Microsoft®

Windows Server® 2008 Active Directory®

Stan Reimer,
Conan Kezema,
Mike Mulcare, and
Byron Wright, with the
Microsoft Active Directory Team

Resource Kit

How to access your CD files

The print edition of this book includes a CD. To access the CD files, go to http://aka.ms/625150/files, and look for the Downloads tab.

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

Questions? Please contact: mspinput@microsoft.com

Microsoft Press

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

Copyright © 2008 by Stan Reimer and Mike Mulcare

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

Library of Congress Control Number: 2008920569

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 QWT 3 2 1 0 9 8

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

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

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

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

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

Acquisitions Editor: Martin DelRe
Developmental Editor: Karen Szall
Project Editor: Maureen Zimmerman
Editorial Production: Custom Editorial Productions, Inc.
Technical Reviewer: Bob Dean, Technical Review services provided by Content Master, a member of CM Group, Ltd.
Cover: Tom Draper Design

Body Part No. X14-14924

To the three wonderful women in my life–Rhonda, Angela, and Amanda.
Your love and encouragement keep me going.

– Stan Reimer

I dedicate this book to the love of my life, Rhonda, and our precious sons,
Brennan and Liam. Thank you for your continuous support and for
being the reason that I do what I do. I also dedicate this book
to the rest of my family, who are still trying to figure out
what I actually do for a living.

– Conan Kezema

To my family–Nancy, James, Sean, and Patrick. Thanks
always for your encouragement and support.

– Mike Mulcare

Tracey, Samantha, and Michelle, you are the reason I keep
it going. Darrin, thanks for holding down the fort.

– Byron Wright

Contents at a Glance

Part I Windows Server 2008 Active Directory Overview

1 What's New in Active Directory for Windows Server 2008 3
2 Active Directory Domain Services Components 19
3 Active Directory Domain Services and Domain Name System 63
4 Active Directory Domain Services Replication 95

Part II Designing and Implementing Windows Server 2008 Active Directory

5 Designing the Active Directory Domain Services Structure 143
6 Installing Active Directory Domain Services 217
7 Migrating to Active Directory Domain Services 247

Part III Administering Windows Server 2008 Active Directory

8 Active Directory Domain Services Security 273
9 Delegating the Administration of Active Directory Domain Services. 325
10 Managing Active Directory Objects 357
11 Introduction to Group Policy 399
12 Using Group Policy to Manage User Desktops 455
13 Using Group Policy to Manage Security. 513

Part IV Maintaining Windows Server 2008 Active Directory

14 Monitoring and Maintaining Active Directory 551
15 Active Directory Disaster Recovery 583

Part V Identity and Access Management with Active Directory

16 Active Directory Lightweight Directory Services 619
17 Active Directory Certificate Services. 661
18 Active Directory Rights Management Services 703
19 Active Directory Federation Services 745

Table of Contents

Acknowledgments . . . . **xxi**
Introduction . . . . **xxiii**
  Overview of Book xxiii
    Part I – Windows Server 2008 Active Directory Overview xxiii
    Part II – Designing and Implementing Windows Server 2008 Active Directory xxiv
    Part III – Administering Windows Server 2008 Active Directory xxiv
    Part IV – Maintaining Windows Server 2008 Active Directory xxv
    Part V – Identity and Access Management with Active Directory xxv
  Document Conventions xxvi
    Reader Aids xxvi
    Sidebars xxvi
    Command-Line Examples xxvii
  Companion CD xxvii
    Management Scripts xxvii
    Using the Scripts xxviii
  Find Additional Content Online xxviii
  Resource Kit Support Policy xxix

Part I Windows Server 2008 Active Directory Overview

1 What's New in Active Directory for Windows Server 2008 . . . . **3**
  What's New in Active Directory Domain Services 3
    Read-Only Domain Controllers (RODC) 3
    Active Directory Domain Services Auditing 6
    Fine-Grained Password Policies 7
    Restartable Active Directory Domain Services 9
    Database Mounting Tool 9
    User Interface Improvements 10

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

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

www.microsoft.com/learning/booksurvey/

Additional Active Directory Service Roles 11
  Active Directory Certificate Services Role 12
  Active Directory Federation Services Role 13
  Active Directory Lightweight Directory Services Role 15
  Active Directory Rights Management Services Role 16
Summary 18

2 Active Directory Domain Services Components 19

AD DS Physical Structure 19
  The Directory Data Store 20
  Domain Controllers 22
  Global Catalog Servers 23
  Read-Only Domain Controllers 25
  Operations Masters 28
  Transferring Operations Master Roles 32
  The Schema 32
AD DS Logical Structure 41
  AD DS Partitions 42
  Domains 46
  Forests 50
  Trusts 52
  Sites 55
  Organizational Units 57
Summary 60
Additional Resources 61
  Related Tools. 61
  Resources on the CD 61
  Related Help Topics 62

3 Active Directory Domain Services and Domain Name System 63

Integration of DNS and AD DS 64
  Service Location (SRV) Resource Records 64
  SRV Records Registered by AD DS Domain Controllers 66
  DNS Locator Service 69
  Automatic Site Coverage 72
AD DS Integrated Zones 74
  Benefits of Using AD DS Integrated Zones 75
  Default Application Partitions for DNS 76
  Managing AD DS Integrated Zones 78

Integrating DNS Namespaces and AD DS Domains 81
    DNS Delegation 82
    Forwarders and Root Hints 83
    Troubleshooting DNS and AD DS Integration 88
    Troubleshooting DNS. 89
    Troubleshooting SRV Record Registration 91
Summary 92
Best Practices. 92
Additional Resources 92
    Related Information 92
    Related Tools 93
    Resources on the CD 94
    Related Help Topics 94

4 Active Directory Domain Services Replication 95
AD DS Replication Model 96
Replication Process. 97
    Update Types 97
    Replicating Changes 99
Replicating the SYSVOL Directory 105
Intrasite and Intersite Replication 106
    Intrasite Replication 107
    Intersite Replication 108
    Replication Latency 109
    Urgent Replication 110
Replication Topology Generation. 111
    Knowledge Consistency Checker 112
    Connection Objects 112
    Intrasite Replication Topology 114
    Global Catalog Replication 118
    Intersite Replication Topology 119
    RODCs and the Replication Topology 120
Configuring Intersite Replication 122
    Creating Additional Sites. 123
    Site Links 124
    Site Link Bridges 128
    Replication Transport Protocols 129
    Configuring Bridgehead Servers 130

Troubleshooting Replication 133
  Process for Troubleshooting AD DS Replication Failures 133
  Tools for Troubleshooting AD DS Replication 134
Summary 137
Best Practices 137
Additional Resources 138
  Related Information 138
  Related Tools 139
  Resources on the CD 140
  Related Help Topics 140

Part II Designing and Implementing Windows Server 2008 Active Directory

5 Designing the Active Directory Domain Services Structure 143
Defining Directory Service Requirements 144
  Defining Business and Technical Requirements 145
  Documenting the Current Environment 150
Designing the Forest Structure 156
  Forests and AD DS Design 158
  Single or Multiple Forests 159
  Designing Forests for AD DS Security 161
  Forest Design Models 163
  Defining Forest Ownership 166
  Forest Change Control Policies 167
Designing the Integration of Multiple Forests 167
  Designing Inter-Forest Trusts 168
  Designing Directory Integration Between Forests 172
Designing the Domain Structure 172
  Determining the Number of Domains 174
  Designing the Forest Root Domain 176
  Designing Domain Hierarchies 177
  Domain Trees and Trusts 178
  Changing the Domain Hierarchy After Deployment 180
  Defining Domain Ownership 180
Designing Domain and Forest Functional Levels 181
  Features Enabled at Domain Functional Levels 181
  Features Enabled at Forest Functional Levels 183
  Implementing a Domain and Forest Functional Level 183

Designing the DNS Infrastructure 184
Namespace Design. 184
Designing the Organizational Unit Structure. 192
Organizational Units and AD DS Design 192
Designing an OU Structure. 193
Creating an OU Design 195
Designing the Site Topology. 197
Sites and AD DS Design. 198
Creating a Site Design 198
Creating a Replication Design 202
Designing Server Locations 206
Summary 214
Best Practices. 214
Additional Resources 215
Related Information 215
Resources on the CD 216

6 Installing Active Directory Domain Services 217

Prerequisites for Installing AD DS 217
Hard Disk Space Requirements 218
Network Connectivity 219
DNS. 220
Administrative Permissions. 220
Operating System Compatibility 221
Understanding AD DS Installation Options 222
Installation Configuration Tasks and the Add Roles Wizard 222
Server Manager 223
Active Directory Domain Services Installation. 224
Unattended Installation. 225
Using the Active Directory Domain Services Installation Wizard 225
Deployment Configuration. 226
Naming the Domain 227
Setting the Windows Server 2008 Functional Levels 228
Additional Domain Controller Options. 232
File Locations 233
Completing the Installation 234
Verifying Installation of AD DS. 235

Performing an Unattended Installation 236
Installing from Media 237
Deploying Read-Only Domain Controllers 238
Server Core Installation Window Server 2008. 239
Deploying the RODC. 239
Removing AD DS 240
Removing Additional Domain Controllers. 241
Removing the Last Domain Controller. 242
Unattended Removal of AD DS 243
Forced Removal of a Windows Server 2008 Domain Controller 243
Summary 244
Additional Resources 244
Related Information 244
Related Tools. 246
7 Migrating to Active Directory Domain Services 247
Migration Paths 248
The Domain Upgrade Migration Path 249
Domain Restructuring 250
Determining Your Migration Path 252
Upgrading the Domain. 254
Upgrading from Windows 2000 Server and Windows Server 2003 255
Restructuring the Domain 257
Interforest Migration. 258
Intraforest Migration 265
Configuring Interforest Trusts 266
Summary 268
Best Practices 269
Additional Resources 269
Related Information 269
Related Tools. 270

Part III Administering Windows Server 2008 Active Directory

8 Active Directory Domain Services Security 273
AD DS Security Basics 274
Security Principals 274
Access Control Lists 275

Access Tokens . . . 278
Authentication . . . 278
Authorization . . . 279
Kerberos Security . . . 280
Introduction to Kerberos . . . 281
Kerberos Authentication . . . 283
Delegation of Authentication . . . 291
Configuring Kerberos in Windows Server 2008 . . . 293
Integration with Public Key Infrastructure . . . 294
Integration with Smart Cards . . . 297
Interoperability with Other Kerberos Systems . . . 298
Troubleshooting Kerberos . . . 299
NTLM Authentication . . . 303
Implementing Security for Domain Controllers . . . 305
Decrease the Domain Controller Attack Surface . . . 306
Configuring the Default Domain Controllers Policy . . . 308
Configuring SYSKEY . . . 317
Designing Secure Administrative Practices . . . 318
Summary . . . 321
Best Practices . . . 321
Additional Resources . . . 321
Related Information . . . 321
Related Tools . . . 322
Resources on the CD . . . 323
Related Help Topics . . . 323

9 Delegating the Administration of Active Directory Domain Services . . . 325
Active Directory Administration Tasks . . . 326
Accessing Active Directory Objects . . . 327
Evaluating Deny and Allow ACEs in a DACL . . . 329
Active Directory Object Permissions . . . 329
Standard Permissions . . . 330
Special Permissions . . . 331
Permissions Inheritance . . . 336
Effective Permissions . . . 340
Ownership of Active Directory Objects . . . 343

Delegating Administrative Tasks 345
Auditing the Use of Administrative Permissions 348
Configuring the Audit Policy for the Domain Controllers. 348
Configuring Auditing on Active Directory Objects 351
Tools for Delegated Administration 352
Customizing the Microsoft Management Console. 353
Planning for the Delegation of Administration. 354
Summary 355
Additional Resources. 356
Related Information 356

10 Managing Active Directory Objects 357
Managing Users 357
User Objects 358
inetOrgPerson Objects 363
Contact Objects 364
Service Accounts 365
Managing Groups 366
Group Types 366
Group Scope. 367
Default Groups in Active Directory 371
Special Identities 373
Creating a Security Group Design. 374
Managing Computers 377
Managing Printer Objects 379
Publishing Printers in Active Directory. 380
Printer Location Tracking 383
Managing Published Shared Folders 384
Automating Active Directory Object Management 386
Command-Line Tools for Active Directory Management 386
Using LDIFDE and CSVDE. 387
Using VBScript to Manage Active Directory Objects 389
Summary 395
Best Practices 395
Additional Resources. 396
Related Information 396
Related Tools. 397
Resources on the CD 397

11 Introduction to Group Policy 399
- Group Policy Overview 400
  - How Group Policy Works 401
  - What's New in Windows Server 2008 Group Policy? 404
- Group Policy Components 405
  - Overview of the Group Policy Container 405
  - Components of the Group Policy Template 407
  - Replication of the Group Policy Object Components 409
- Group Policy Processing 409
  - How Clients Process GPOs 410
  - Initial GPO Processing 413
  - Background GPO Refreshes 415
  - How GPO History Relates to Group Policy Refresh 416
  - Exceptions to Default Background Processing Interval Times 418
- Implementing Group Policy 423
  - GPMC Overview 424
  - Using the GPMC to Create and Link GPOs 426
  - Modifying the Scope of GPO Processing 427
  - Delegating the Administration of GPOs 436
  - Implementing Group Policy Between Domains and Forests 438
- Managing Group Policy Objects 439
  - Backing Up and Restoring GPOs 439
  - Copying Group Policy Objects 441
  - Importing Group Policy Object Settings 441
  - Modeling and Reporting Group Policy Results 442
- Scripting Group Policy Management 447
- Planning a Group Policy Implementation 450
- Troubleshooting Group Policy 451
- Summary 453
- Additional Resources 453
  - Related Information 453

12 Using Group Policy to Manage User Desktops 455
- Desktop Management Using Group Policy 456
- Managing User Data and Profile Settings 459
  - Managing User Profiles 459
  - Using Group Policy to Manage Roaming User Profiles 466
  - Folder Redirection 469

Administrative Templates 477
  Understanding Administrative Template Files. 478
  Managing Domain-based Template Files 481
  Best Practices for Managing ADMX Template Files 482
Using Scripts to Manage the User Environment 484
Deploying Software Using Group Policy 485
  Windows Installer Technology 486
  Deploying Applications 486
  Using Group Policy to Distribute Non–Windows Installer Applications 490
  Configuring Software Package Properties 491
  Using Group Policy to Configure Windows Installer 498
  Planning for Group Policy Software Installation 500
  Limitations to Using Group Policy to Manage Software 501
Overview of Group Policy Preferences 503
  Group Policy Preferences vs. Policy Settings 503
  Group Policy Preferences Settings 504
  Group Policy Preferences Options 507
Summary 510
Additional Resources 510
  Related Information 510
  On the Companion CD 511

13 Using Group Policy to Manage Security. 513
Configuring Domain Security with Group Policy 513
  Overview of the Default Domain Policy 514
  Overview of the Default Domain Controllers Policy 519
  Recreating the Default GPOs for a Domain. 526
  Fine-Grained Password Policies 527
Hardening Server Security Using Group Policy 532
  Software Restriction Policies. 535
Configuring Network Security Using Group Policy 537
  Configuring Wired Network Security 538
  Configuring Wireless Network Security 541
  Configuring Windows Firewall and IPsec Security 541
Configuring Security Settings Using Security Templates 543
  Deploying Security Templates 545

Summary 547
Additional Resources 548
    Related Information 548

Part IV Maintaining Windows Server 2008 Active Directory

14 Monitoring and Maintaining Active Directory 551
Monitoring Active Directory 551
    Why Monitor Active Directory 553
    Monitoring Server Reliability and Performance 554
    How to Monitor Active Directory 561
    What to Monitor 571
    Monitoring Replication 572
Active Directory Database Maintenance 575
    Garbage Collection 575
    Online Defragmentation 576
    Offline Defragmentation of the Active Directory Database 577
    Managing the Active Directory Database Using Ntdsutil 578
Summary 580
Additional Resources 581
    Related Information 581

15 Active Directory Disaster Recovery 583
Planning for a Disaster 584
Active Directory Data Storage 585
Backing Up Active Directory 587
    The Need for Backups 589
    Tombstone Lifetime 589
    Backup Frequency 591
Restoring Active Directory 591
    Restoring Active Directory by Creating a New Domain Controller 592
    Performing a Nonauthoritative Restore of Active Directory 595
    Performing an Authoritative Restore of Active Directory 599
    Restoring Group Memberships 601
    Reanimating Tombstone Objects 605
    Using the Active Directory Database Mounting Tool 607
    Restoring SYSVOL Information 610
    Restoring Operations Masters and Global Catalog Servers 610

Summary 614
Best Practices 614
Additional Resources 615
    Related Information 615
    Related Tools 615

Part V Identity and Access Management with Active Directory

16 Active Directory Lightweight Directory Services 619
AD LDS Overview 620
    AD LDS Features 620
    AD LDS Deployment Scenarios 620
AD LDS Architecture and Components 622
    AD LDS Servers 622
    AD LDS Instances 623
    Directory Partitions 624
    AD LDS Replication 629
    AD LDS Security 633
Implementing AD LDS 640
    Configuring Instances and Application Partitions 640
    AD LDS Management Tools 643
    Configuring Replication 648
    Backing Up and Restoring AD LDS 651
Configuring AD DS and AD LDS Synchronization 654
Summary 657
Best Practices 657
Additional Resources 658
    Related Tools 658
    Resources on the CD 659
    Related Help Topics 659

17 Active Directory Certificate Services 661
Active Directory Certificate Services Overview 661
    Public Key Infrastructure Components 662
    Certification Authorities 667
    Certificate Services Deployment Scenarios 670
Implementing AD CS 670
    Installing AD CS Root Certification Authorities 671
    Installing AD CS Subordinate Certification Authorities 673

Configuring Web Enrollment 673
Configuring Certificate Revocation 674
Managing Key Archival and Recovery. 681
Managing Certificates in AD CS 685
Configuring Certificate Templates 685
Configuring Certificate Autoenrollment. 690
Managing Certificate Acceptance with Group Policy 692
Configuring Credential Roaming 693
Designing an AD CS Implementation 694
Designing a CA Hierarchy 694
Designing Certificate Templates 697
Designing Certificate Distribution and Revocation. 700
Summary 700
Best Practices. 701
Additional Resources 701
Related Information 701
Related Tools 702

18 Active Directory Rights Management Services 703
AD RMS Overview 704
AD RMS Features 704
AD RMS Components 706
How AD RMS Works 709
AD RMS Deployment Scenarios. 713
Implementing AD RMS 714
Preinstallation Considerations Before Installing AD RMS 714
Installing AD RMS Clusters 715
Configuring the AD RMS Service Connection Point. 720
Working with AD RMS Clients 721
Administering AD RMS 726
Managing Trust Policies. 726
Managing Rights Policy Templates 733
Configuring Exclusion Policies 738
Configuring Security Policies 739
Viewing Reports 741
Summary 742
Additional Resources 742
Related Information 743

19 Active Directory Federation Services 745

AD FS Overview 746

  Identity Federation 746

  Web Services 747

  AD FS Components 749

  AD FS Deployment Designs 753

Implementing AD FS 759

  AD FS Deployment Requirements. 760

  Implementing AD FS in a Federation Web SSO Design 767

  Configuring the Account Partner Federation Service 774

  Configuring Resource Partner AD FS Components 782

  Configuring AD FS for Windows NT Token-based Applications 787

  Implementing a Web SSO Design. 789

  Implementing a Federated Web SSO with Forest Trust Design 790

Summary 791

Best Practices 791

Additional Resources 792

  Resources on the CD 792

  Related Help Topics 792

Index. 795

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

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

www.microsoft.com/learning/booksurvey/

Acknowledgments

by Stan Reimer (for the team):

First of all, I want thank my coauthors for their hard work on this book. When I was first asked to lead this writing project, I looked around for the right people to work with me on this book and I couldn't have picked a better team.

Secondly, I want to thank the folks at Microsoft Press. This team includes Martin DelRe, the program manager, who kept poking us until we agreed to do this project, Karen Szall, the content development manager, and Maureen Zimmerman, the content project manager. I am sure that the problems we had keeping to the schedule on this book caused a few headaches for this group, but they were amazingly supportive and encouraging all the way through. Maureen had an amazing knack for reminding us when materials were due without making it feel like nagging.

Thanks to Bob Dean, the technical reviewer, for his valuable comments. Production for this book was professionally handled by Custom Editorial Productions Inc., with Linda Allen as the project manager, Cecilia Munzenmaier as the copy editor, and many others who toiled away in the background. As writers, we get to have all of the fun at the beginning of the process; these folks are still working on this long after we are done.

A Resource Kit doesn't come together without a lot of interaction with the product groups at Microsoft, as well as other technical experts, such as Directory Services MVPs. All of the chapters in this book have been reviewed by these experts and many of these experts contributed to the Direct from the Source, Direct from the Field, or How It Works sidebars that you will enjoy reading in this book. These reviewers and contributors include:

James McColl, Mike Stephens, Moon Majumdar, Judith Herman, Mark Gray, Linda Moore, Greg Robb, Barry Hartman, Christiane Soumahoro, Gautam Anand, Michael Hunter, Alain Lissoir, Yong Liang, David Hastie, Teoman Smith, Brian Lich, Matthew Rimer, David Fisher, Bob Drake, Rob Greene, Andrej Budja, Rob Lane, Gregoire Guetat, Donovan Follette, Pavan Kompelli, Sanjeev Balarajan, Fatih Colgar, Brian Desmond, Jose Luis Auricchio, Darol Timberlake, Peter Li, Elbio Abib, Ashish Sharma, Nick Pierson, Lu Zhao, and Antonio Calomeni.

by Conan Kezema:

Special thanks to my fellow coauthors for their hard work on this book. I would also like to thank Stan for the many opportunities he has provided over the years; he is a great friend and mentor.

Introduction

Welcome to the *Windows Server 2008 Active Directory Resource Kit*, your complete source for the information you need to design and implement Active Directory in Windows Server 2008.

The *Windows Server 2008 Active Directory Resource Kit* is a comprehensive technical resource for planning, deploying, maintaining, and troubleshooting an Active Directory infrastructure in Windows Server 2008. While the target audience for this Resource Kit is experienced IT professionals who work in medium-sized and large-sized organizations, anyone who wants to learn how to implement and manage Active Directory in Windows Server 2008 will find this Resource Kit invaluable.

One of the new features in Windows Server 2008 Active Directory is that the term *Active Directory* now covers a lot more territory than it did in previous iterations of this directory service. What was previously called Active Directory in Windows 2000 and Windows Server 2003 is now called Active Directory Domain Services (AD DS), and several more directory service components have been included under the Active Directory umbrella. These include Active Directory Lightweight Directory Services (AD LDS), Active Directory Certificate Services (AD CS), Active Directory Rights Management Services (AD RMS), and Active Directory Federation Services (AD FS).

Within this Resource Kit you'll find in-depth technical information on how Active Directory works in Windows Server 2008. In addition, you will find detailed task-based guidance for implementing and maintaining the Active Directory infrastructure. You'll also find numerous sidebars—contributed by members of the Active Directory product team, other directory experts at Microsoft, and directory services MVPs—that provide deep insight into how Active Directory works, best practices for designing and implementing Active Directory, and invaluable troubleshooting tips. Finally, the companion CD includes deployment tools, templates, and many sample scripts that you can use and customize to help you automate various aspects of managing Active Directory in enterprise environments.

Overview of Book

This book is divided into the following five parts with the following chapters:

Part I – Windows Server 2008 Active Directory Overview

- **Chapter 1 – "What's New in Active Directory for Windows Server 2008"** This chapter provides an overview of the new features that are available in Windows Server 2008. If you know Windows Server 2003 Active Directory, this is a good place for you to get a quick overview of some of the new material that will be covered in this book.

- **Chapter 2 – "Active Directory Domain Services Components"** This chapter provides an overview of Active Directory Domain Services—if you are somewhat new to Active Directory, this is a great chapter to get you started on the terms and concepts that make up AD DS.
- **Chapter 3 – "Active Directory Domain Services and Domain Name System"** One of the most critical components that you need in order to make AD DS work efficiently is a properly implemented DNS infrastructure. This chapter provides information on how to do this.
- **Chapter 4 – "Active Directory Domain Services Replication"** In order to work with AD DS, you will need to understand replication. This chapter provides all of the details of how AD DS replication works and how to configure it.

Part II – Designing and Implementing Windows Server 2008 Active Directory

- **Chapter 5 – "Designing the Active Directory Domain Services Structure"** Before deploying AD DS, you need to create a design that meets your organization's requirements. This chapter provides the in-depth information that you will need to do that planning.
- **Chapter 6 – "Installing Active Directory Domain Services"** Installing AD DS on a Windows Server 2008 computer is pretty easy, but there several variations on how to perform the installation. This chapter describes all of the options and the reasons for choosing each one.
- **Chapter 7 – "Migrating to Active Directory Domain Services"** Many organizations are already running a previous version of Active Directory. This chapter provides the details on how to deploy Windows Server 2008 domain controllers in this environment, and how to migrate the Active Directory environment to Windows Server 2008.

Part III – Administering Windows Server 2008 Active Directory

- **Chapter 8 – "Active Directory Domain Services Security"** AD DS provides the core network authentication and authorization services in many organizations. This chapter describes how AD DS security works and the steps you can take to secure your AD DS environment.
- **Chapter 9 – "Delegating the Administration of Active Directory Domain Services"** One of the options in implementing AD DS is that you can delegate many administrative tasks to other administrators without granting them domain level permissions. This chapter describes how AD DS permissions work and how to delegate them.
- **Chapter 10 – "Managing Active Directory Objects"** Most of your time as an AD DS administrator will be spent managing AD DS objects like users, groups and organizational units. This chapter deals with how to manage these objects individually, but also provides details on how to manage large numbers of these objects by using scripts.

- **Chapter 11 – "Introduction to Group Policy"** A central component in a Windows Server 2008 network management system is Group Policy. With Group Policy, you can manage many desktop settings as well as configure security. This chapter begins by explaining what Group Policy objects are and shows how to apply and filter Group Policy objects.
- **Chapter 12 – "Using Group Policy to Manage User Desktops"** One of the important tasks you can perform with Group Policy is configuring user desktops. In Windows Server 2008 and Windows Vista, there are several thousand Group Policy settings available. This chapter describes not only how to apply the policies, but also which policies are most important to apply.
- **Chapter 13 – "Using Group Policy to Manage Security"** Another important task that you can perform with Group Policy is applying security settings. This includes settings that will be applied to all users and computers in the domain as well as settings that can be applied to individual computers or users. This chapter provides the details on how to configure security by using Group Policy.

Part IV – Maintaining Windows Server 2008 Active Directory

- **Chapter 14 – "Monitoring and Maintaining Active Directory"** This chapter prepares you to maintain your Active Directory infrastructure after you deploy it. This chapter covers how to monitor your AD DS environment, and how to maintain the AD DS domain controllers.
- **Chapter 15 – "Active Directory Disaster Recovery"** Because of the central role that AD DS has in many corporations, it is critical that you know how to prepare for and recover from disasters within your AD DS environment. This chapter details how you can do this.

Part V – Identity and Access Management with Active Directory

- **Chapter 16 – "Active Directory Lightweight Directory Services"** AD LDS is one of the new server roles that is included under the Active Directory umbrella in Windows Server 2008. AD LDS is designed to be an application directory—this chapter describes how you can deploy and manage your AD LDS environment.
- **Chapter 17 – "Active Directory Certificate Services"** AD CS can be used to provide the public key infrastructure that provides digital certificates that are so critical for many network security implementations. This chapter describes how to plan and implement AD CS.
- **Chapter 18 – "Active Directory Rights Management Services"** AD RMS provides the tools to apply persistent usage policies to information that stays with the information even as it is moved around or outside the organization. This chapter details how to implement AD RMS.

- **Chapter 19 – "Active Directory Federation Services"** AD FS provides a means to enable users to access multiple Web-based applications in their organization or in other organizations while only authenticating once. This chapter describes the AD FS deployment scenarios and how to implement them.

Document Conventions

The following conventions are used in this book to highlight special features and usage:

Reader Aids

The following reader aids are used throughout this book to point out useful details:

Reader Aid	Meaning
Note	Underscores the importance of a specific concept or highlights a special case that might not apply to every situation
Important	Calls attention to essential information that should not be disregarded
Caution	Warns you that failure to take or avoid a specified action can cause serious problems for users, systems, data integrity, and so on
On the CD	Calls attention to a related script, tool, template, or job aid on the companion CD that helps you perform a task described in the text
More Info	Points out Web sites or other related material that you can access to get more details about a topic described in the text
Security Alert	Emphasizes information or tasks that are essential for maintaining a secure environment or identifies events that indicate a potential security incident

Sidebars

The following sidebars are used throughout this book to provide added insight, tips, and advice concerning Windows Server 2008 Active Directory:

Sidebar	Meaning
Direct from the Source	Contributed by experts at Microsoft to provide "from-the-source" insight into how Active Directory in Windows Server 2008 works, best practices for planning and implementing the Active Directory server roles, and troubleshooting tips
Direct from the Field	Contributed by directory service MVPs to provide real-world insight into best practices for planning and implementing the Active Directory server roles and troubleshooting tips
How It Works	Provides unique glimpses of Windows Server 2008 Active Directory features and how they work

Command-Line Examples

The following style conventions are used in documenting command-line examples throughout this book:

Style	Meaning
Bold font	Used to indicate user input (characters that you type exactly as shown)
Italic font	Used to indicate variables for which you need to supply a specific value (for example, *filename* can refer to any valid file name)
`Monospace font`	Used for code samples and command-line output
%SystemRoot%	Used for environment variables

Companion CD

The companion CD is a valuable addition to this book. Many of the tools and resources mentioned in the chapters are on the CD itself; you can access other tools and resources via links from the CD.

For documentation of the contents and structure of the companion CD, see the Readme.txt file on the CD.

Management Scripts

A set of scripts to manage Active Directory is included on the CD. Among them are scripts to get information about Active Directory objects and scripts to create or modify these objects. These scripts all require Windows PowerShell. The following scripts are included on the CD:

- **AddUserToGroup.ps1** Adds a user account to a group in the same OU
- **CreateAndEnableUserFromCSV.ps1** Creates an enabled user account by reading a .csv file
- **CreateGroup.ps1** Creates a group in Active Directory in the OU and domain specified
- **CreateObjectInAD.ps1** Creates an object in Active Directory
- **CreateOU.ps1** Creates an organizational unit in Active Directory
- **CreateUser.ps1** Creates a user account in Active Directory
- **EnableDisableUserSetPassword.ps1** Enables or disables a user account and sets the password
- **GetDomainPwdSettings.ps1** Obtains the password policy settings for a domain
- **GetModifiedDateFromAD.ps1** Lists the last modified date of a specific user onto a local or remote domain

The CD that accompanies the print edition of this book is not available with this eBook edition, although select CD content is available for download at http://www.microsoftpressstore.com/title/9780735625150.

- **ListUserLastLogon.ps1** Lists the last logon date of a specific user onto a local or remote domain
- **LocateDisabledUsers.ps1** Locates disabled user accounts in a local or remote domain
- **LocateLockedOutUsers.ps1** Locates locked out user accounts a local or remote domain
- **LocateOldComputersNotLogon.ps1** Locates computer accounts in a local or remote domain that have not logged on for a specified number of days
- **LocateOldUsersNotLogOn.ps1** Scans a local or remote domain for user accounts that have not logged onto the domain for an extended period of time that is specified in days
- **ModifyUser.ps1** Modifies user attributes in Active Directory
- **QueryAD.ps1** Queries Active Directory for objects such as users, groups, computers, and so on
- **UnlockLockedOutUsers.ps1** Unlocks user accounts that are locked out

In addition to these scripts, many of the chapters contain references to additional scripts that perform the management tasks included in that chapter.

Full documentation of the contents and structure of the companion CD can be found in the Readme.txt file on the CD.

Using the Scripts

The companion CD includes scripts that are written in VBScript (with a .vbs file extension) and Windows PowerShell (with a .ps1 file extension).

The VBScript scripts on the companion CD are identified with the .vbs extension. To use those scripts, double-click them or execute them directly from a command prompt.

The Windows PowerShell scripts require that you have Windows PowerShell installed and that you have configured Windows PowerShell to run unsigned scripts. You can run the Windows PowerShell scripts on Windows XP SP2, Windows Server 2003 SP1, Windows Vista, or Windows Server 2008. In order for the scripts to work, all computers must be members of a Windows Server 2008 domain.

Note For information about the system requirements for running the scripts on the CD, see the System Requirements page at the end of the book.

Find Additional Content Online

As new or updated material becomes available that complements your book, it will be posted online on the Microsoft Press Online Windows Server and Client Web site. Based on the final build of Windows Server 2008, the type of material you might find includes updates to book content, articles, links to companion content, errata, sample chapters, and more. This Web site will be available soon at *http://www.microsoft.com/learning/books/online/serverclient*, and will be updated periodically.

Digital Content for Digital Book Readers: If you bought a digital-only edition of this book, you can enjoy select content from the print edition's companion CD.
Visit http://www.microsoftpressstore.com/title/9780735625150 to get your downloadable content. This content is always up-to-date and available to all readers.

Resource Kit Support Policy

Every effort has been made to ensure the accuracy of this book and the companion CD content. Microsoft Press provides corrections to this book through the Web at the following location:

http://www.microsoft.com/learning/support/search.asp.

If you have comments, questions, or ideas regarding the book or companion CD content, or if you have questions that are not answered by querying the Knowledge Base, please send them to Microsoft Press by using either of the following methods:

E-mail:

rkinput@microsoft.com

Postal Mail:

Microsoft Press

Attn: Windows Server 2008 Active Directory Resource Kit

One Microsoft Way

Redmond, WA 98052-6399

Please note that product support is not offered through the preceding mail addresses.
For product support information, please visit the Microsoft Product Support Web site at the following address:

http://support.microsoft.com

Chapter 4

Active Directory Domain Services Replication

In this chapter:

AD DS Replication Model 96
Replication Process 97
Replicating the SYSVOL Directory 105
Intrasite and Intersite Replication 106
Replication Topology Generation 111
Configuring Intersite Replication 122
Troubleshooting Replication 133
Summary 137
Best Practices 137
Additional Resources 138

In almost all cases, when you deploy an Active Directory Domain Services (AD DS) domain in Microsoft Windows Server 2008, you should deploy more than one domain controller. Deploying multiple domain controllers in each domain is the easiest and most effective way to provide high availability for the domain controller services. These domain controllers might all be located in one data center at the company head office where they are connected by very fast network connections. Or they might be spread across many locations around the world, with a variety of wide area network (WAN) connections linking the company locations.

Regardless of how many domain controllers a company has or where those domain controllers are located, they must replicate information with each other. If they cannot replicate the information, the directories on the domain controllers will become inconsistent. For example, if a user is created on one domain controller, and that information is not replicated to all the other domain controllers, the user will only be able to authenticate to the domain controller where the account was created.

This chapter describes the process of replication in AD DS. The focus of this chapter is on how replication works; that is, on how the replication topology is created and how domain controllers replicate with each other. By default, when you install AD DS domain controllers, they automatically begin replicating with each other. This default replication topology may not be the most efficient for your organization, so this chapter describes ways that you can modify the replication configuration to meet your company requirements. In addition, this chapter provides guidance on how to troubleshoot AD DS replication.

AD DS Replication Model

As described in Chapter 2, "Active Directory Domain Services Components," AD DS is made up of multiple logical partitions. Replication between the domain controllers with replicas of each partition is handled in exactly the same way for all partitions. When an attribute is changed in the configuration directory partition, it is replicated using the same model and processes as when an attribute is changed in any other partition. The only thing that changes is the list of domain controllers that will receive a copy of the replicated change. Also, replication between domain controllers in the same site is handled differently than it is between domain controllers in different sites, but the essential model does not change. This section describes the replication model used by AD DS.

AD DS uses a multimaster replication model. That means that changes to the AD DS data store can be made on any domain controller except specifically configured read-only domain controllers (RODC). That is, every domain controller except the RODCs has a writable copy of the directory, and there is no single domain controller where all changes have to be made. After a change has been made, it is replicated to all the other domain controllers. This multimaster replication model addresses many important reliability and scalability issues. Because all of the domain controllers provide the same services, no domain controller represents a single point of failure.

Note As discussed in Chapter 2, AD DS has specific operations master roles that can be held by only one domain controller. These roles represent a single point of failure, but the roles can also be easily moved or seized to another domain controller.

The replication model used by AD DS can be described as being loosely consistent, but with convergence. The replication is *loosely consistent* because not all domain controllers with a replica of a partition will always have identical information. For example, if a new user is created on one of the domain controllers, the other domain controllers will not receive that information until the next replication cycle. The replication always moves towards *convergence*, however. If the system is maintained in a steady state, with no new changes made to the directory for a period of time, all domain controllers will reach a state of convergence where they all have identical information.

The replication model also uses a *store-and-forward* replication process. This means that a domain controller can receive a change to the directory and then forward the change to other domain controllers. This is advantageous when multiple domain controllers in a number of company locations are separated by slow WAN links. A change to the directory can be replicated from one domain controller in one site to a single domain controller in another site. The domain controller that receives the update can then forward the changes to other domain controllers in the second site.

AD DS also uses a *state-based* replication model. This means that each domain controller tracks the state of replication updates. As a domain controller receives new updates (either from changes being made on the domain controller or through replicated changes from another domain controller), the domain controller applies the updates to its replica of the AD DS data store. When another domain controller attempts to replicate information that a domain controller already has, the receiving domain controller can determine by the state of its data store that it does not need to get the duplicate information. The current state of the data store includes metadata that is used to resolve conflicts and to avoid sending the full replica on each replication cycle.

Replication Process

Features such as multimaster replication and store-and-forward replication mean that a domain controller could receive AD DS updates from multiple domain controllers and that AD DS replication traffic could take more than one path between domain controllers. For example, if a change is made to AD DS on DC1, the change could be replicated directly to DC2 and DC3. Because of the store-and-forward replication model, DC2, after receiving the update from DC1, may try to replicate the same change to DC3. AD DS replication is designed to ensure that the replication process is efficient while still providing redundancy.

Update Types

Two types of changes can be made to the AD DS information on a particular domain controller. The first type of update is an *originating update*. An originating update is performed when an object is added, modified, or deleted on a domain controller. The second type of update is a *replicated update*. A replicated update is performed when a change made on another domain controller is replicated to the local domain controller. By definition, there can be only one originating update performed for any particular change, and this occurs on the domain controller where the change is made. This originating update is then replicated to all the domain controllers that have a replica of the affected AD DS partition.

Originating updates occur in AD DS under any of the following circumstances:

- **A new object is added to AD DS** Adding a new object to AD DS creates an object with a unique *objectGUID* attribute. As well, all values assigned to attributes that are configured for the object are assigned a version number of *1*.
- **An existing object is deleted from AD DS** When an object is deleted from AD DS, it is marked as deleted, but not immediately removed from the AD DS data store. Only after the tombstone expires on the object is the object actually deleted. For more details, see the section “Replicating Object Deletions” later in this chapter.

- **The attributes for an existing object are modified** This modification can include adding a new value to an attribute, deleting a value for an attribute, or modifying an existing value. When you change an object, the modify request compares the new value for each attribute with the existing value. If the value for an attribute has not changed, the attribute is not updated. If the value has changed, the attribute is updated and the version number for each updated attribute is incremented by one.
- **An object in AD DS is moved to a new parent container** If the parent container is renamed, each object in the container is also moved to the renamed container. When an object is moved to another container in AD DS, the only attribute that changes for the object is the *name* attribute, which is changed to reflect the new location in the LDAP hierarchy.

All originating updates to AD DS are *atomic operations*, which means that when an update is committed to AD DS, either the entire transaction is committed and the change is made to the data store, or no part of the update will be committed. For more information on the process of committing changes to the AD DS data store, see Chapter 14, "Monitoring and Maintaining Active Directory."

The Replication Process in Windows Server 2008

Windows Server 2003 introduced several important changes to the replication process that are also available in Windows Server 2008. One change is the linked value replication. In Windows 2000, the smallest unit of replication is an attribute. This means that in some cases, changing one value in a multivalued attribute can create a significant amount of replication traffic. The most common example of this is what happens with *universal group membership*. Because the entire membership list for the universal group is one attribute, adding a single user to the universal group results in significant replication, especially when the group already has several thousand members. In Windows Server 2003 Active Directory and Windows Server 2008 AD DS, multivalued attributes like *group membership* can be updated by replicating only the change to the attribute by using linked value replication.

AD DS uses linked attributes to enable linked value replication. Linked attributes always include a forward link and backward link to create a link between two AD DS objects. The forward link is the linked attribute on the source object (for example, the *member* attribute on the group object), whereas the backward link is the linked attribute on the target object (for example, the *memberOf* attribute on the user object). A backward link value includes the distinguished names of all the objects that have the object's distinguished name set in their corresponding forward link.

The relationships between linked attributes are stored in a separate table in the directory database as link pairs. The matching pair of *Link IDs* ties the attributes together. For example, the *membe*r attribute has a *link ID* of 2 and the *memberOf* attribute has a *link ID* of 3. Because the *member* and the *memberOf* attributes are linked in the database and indexed for searching, the directory can be examined for all records in which the link pair is *member/memberOf* and the *memberOf* attribute identifies the group.

Another important change in Windows Server 2003 Active Directory is the support for groups of more than 5,000 members. In Windows 2000, groups cannot contain more than 5,000 members because of the attribute-level updates and replication. The practical limit for committing a change to the directory database in one transaction is 5,000. This also defines the maximum number of updates that can be replicated in one update during replication. As a result, the maximum group size in Windows 2000 is 5,000 members. In Windows Server 2008 AD DS, support for modifications of only one value on a multivalued linked attribute removes these restrictions.

Replicating Changes

After an originating update has been committed to AD DS, the change must be replicated to other domain controllers that host a replica of that partition. Within a site, the domain controller where the originating update occurred waits 15 seconds before replicating the changes to its direct replication partners. The 15-second wait occurs so that if multiple updates are committed to the database, they can all be replicated at the same time. This increases the efficiency of the replication. Between sites, the originating update will be replicated to replication partners based on the schedule configured on the site link.

When replicating changes to the directory information, the domain controllers require a mechanism for managing the flow of replication. To optimize AD DS replication, only those changes that need to be replicated between two domain controllers should be sent. To accomplish this, the domain controllers should be able to determine which, if any, changes have not yet been replicated, and then replicate only those changes that are required. AD DS uses a combination of update sequence numbers (USNs), high-watermark values, up-to-dateness vectors, and change stamps to manage directory replication.

Update Sequence Numbers

When an object is updated in the database, an *update sequence number (USN)* is assigned to the update. The USN is specific to the domain controller where the update occurred. For example, if a telephone number update for one user was assigned *USN 5555*, the next change to the domain controller, regardless of which object was modified, would be *USN 5556*. One USN is assigned for each committed change. If multiple attributes are changed with one update (for example, a user's address, telephone number, and office location are all modified at once), only one USN is assigned during the update.

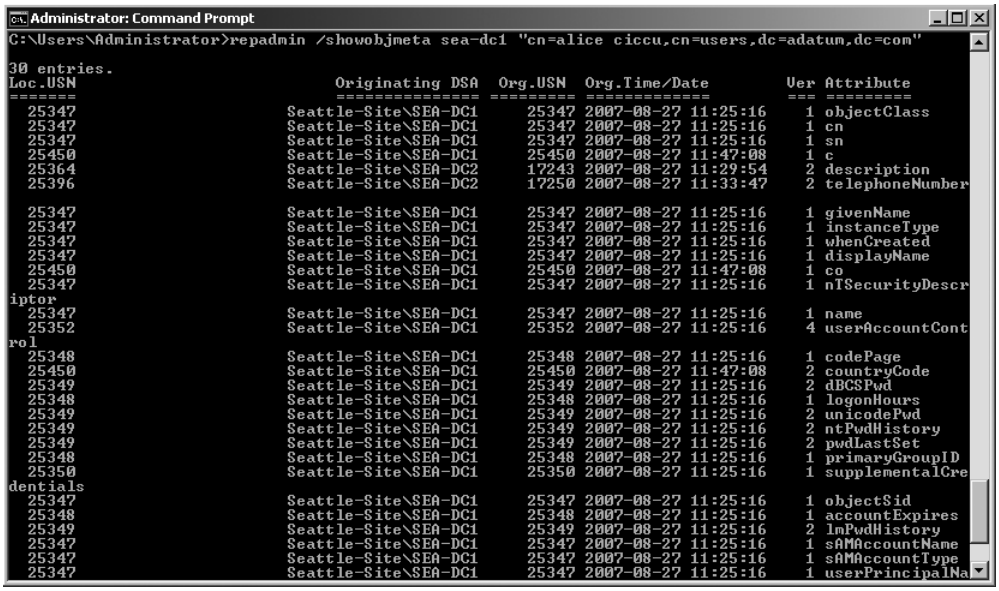
There are three ways that the USN is used when an update is committed. First, the local USN value is stored with the attribute that was updated. The local USN value identifies the USN of the changed attribute. The second way the USN is used is for the object's *uSNChanged* attribute. This attribute is stored with each object and identifies the highest USN for any attribute for the object. For example, suppose a user's telephone number was changed and the USN applied to that change was *5556*. Both the local USN and the *uSNChanged* attribute will be set to *5556*. If the next update applied to the directory on that server were an address change for the same user, the local USN on the address attribute and the *uSNChanged* attribute for the user object would both be changed to *5557*. However, the local USN for the telephone number attribute would remain at *5556,* because that was the USN for the last update that changed that particular attribute.

The local USN and the *uSNChanged* attribute are applied for both originating and replicated updates. The last way the USN is used is as the *originating USN* for the attribute. This value is set only for originating updates and is replicated to all other domain controllers as part of the attribute replication. When the telephone number for a user is changed on a server, the USN for the change is assigned to the originating USN value. When the modified telephone number is replicated to another domain controller, the originating USN is sent along with the update, and this value is not modified on the destination domain controller. The local USN and the *uSNChanged* attribute will be modified on the destination domain controller (and will be specific to that domain controller), but the originating USN is not changed until the attribute itself is updated again. The originating USN is used for propagation dampening, which is described later in this chapter.

Viewing USN Information

The USNs for any object can be viewed through different administrative tools included with Windows Server 2008. The easiest way to view the current and original USN values for an object is to use the Active Directory Users And Computers administrative tool. To view this information, turn on Advanced Features under the View menu and then access the Object tab in the object's Properties sheet. Remember that the USN number is domain controller-specific, so that if you view the USN for an object on two different domain controllers, the USN will be different.

One way to view the local USN, originating domain controller, originating USN, and time stamp for any attribute is by using the Repadmin command-line tool. Type **repadmin /showobjmeta *domaincontrollername objectdistinguishedname*** at a command prompt. Figure 4-1 shows the partial output from this command.



```
C:\Users\Administrator>repadmin /showobjmeta sea-dc1 "cn=alice ciccu,cn=users,dc=adatum,dc=com"

30 entries.
Loc.USN                           Originating DSA  Org.USN  Org.Time/Date        Ver Attribute
=======                           =============== ========= =============        === =========
  25347                      Seattle-Site\SEA-DC1     25347 2007-08-27 11:25:16    1 objectClass
  25347                      Seattle-Site\SEA-DC1     25347 2007-08-27 11:25:16    1 cn
  25347                      Seattle-Site\SEA-DC1     25347 2007-08-27 11:25:16    1 sn
  25450                      Seattle-Site\SEA-DC1     25450 2007-08-27 11:47:08    1 c
  25364                      Seattle-Site\SEA-DC2     17243 2007-08-27 11:29:54    2 description
  25396                      Seattle-Site\SEA-DC2     17250 2007-08-27 11:33:47    2 telephoneNumber

  25347                      Seattle-Site\SEA-DC1     25347 2007-08-27 11:25:16    1 givenName
  25347                      Seattle-Site\SEA-DC1     25347 2007-08-27 11:25:16    1 instanceType
  25347                      Seattle-Site\SEA-DC1     25347 2007-08-27 11:25:16    1 whenCreated
  25347                      Seattle-Site\SEA-DC1     25347 2007-08-27 11:25:16    1 displayName
  25450                      Seattle-Site\SEA-DC1     25450 2007-08-27 11:47:08    1 co
  25347                      Seattle-Site\SEA-DC1     25347 2007-08-27 11:25:16    1 nTSecurityDescr
iptor
  25347                      Seattle-Site\SEA-DC1     25347 2007-08-27 11:25:16    1 name
  25352                      Seattle-Site\SEA-DC1     25352 2007-08-27 11:25:16    4 userAccountCont
rol
  25348                      Seattle-Site\SEA-DC1     25348 2007-08-27 11:25:16    1 codePage
  25450                      Seattle-Site\SEA-DC1     25450 2007-08-27 11:47:08    2 countryCode
  25349                      Seattle-Site\SEA-DC1     25349 2007-08-27 11:25:16    2 dBCSPwd
  25348                      Seattle-Site\SEA-DC1     25348 2007-08-27 11:25:16    1 logonHours
  25349                      Seattle-Site\SEA-DC1     25349 2007-08-27 11:25:16    2 unicodePwd
  25349                      Seattle-Site\SEA-DC1     25349 2007-08-27 11:25:16    2 ntPwdHistory
  25349                      Seattle-Site\SEA-DC1     25349 2007-08-27 11:25:16    2 pwdLastSet
  25348                      Seattle-Site\SEA-DC1     25348 2007-08-27 11:25:16    1 primaryGroupID
  25350                      Seattle-Site\SEA-DC1     25350 2007-08-27 11:25:16    1 supplementalCre
dentials
  25347                      Seattle-Site\SEA-DC1     25347 2007-08-27 11:25:16    1 objectSid
  25348                      Seattle-Site\SEA-DC1     25348 2007-08-27 11:25:16    1 accountExpires
  25349                      Seattle-Site\SEA-DC1     25349 2007-08-27 11:25:16    2 lmPwdHistory
  25347                      Seattle-Site\SEA-DC1     25347 2007-08-27 11:25:16    1 sAMAccountName
  25347                      Seattle-Site\SEA-DC1     25347 2007-08-27 11:25:16    1 sAMAccountType
  25347                      Seattle-Site\SEA-DC1     25347 2007-08-27 11:25:16    1 userPrincipalNa
```

Figure 4-1 Viewing replication metadata using *Repadmin*.

In this output, you can see that the user was created on SEA-DC1, but then the *description* and *telephoneNumber* attributes were modified on SEA-DC2. The originating USNs for all of the attributes except these two are from SEA-DC1, but the originating USNs for the *description* and *telephoneNumber* attributes are from SEA-DC2. However, the local USN numbers are all from SEA-DC1, which is the domain controller where this information was captured. As well, the version number for these two attributes is 2, indicating that the attribute has been modified from the original version.

You can also access the same replication information through the Ldp tool. To do this, connect and bind to a domain controller using Ldp, locate the object, and then right-click the object, select Advanced, and then select Replication Metadata. The replication metadata is the same information as is shown in the Repadmin tool, except that the originating DSA information is shown using the domain controller globally unique identifier (GUID) rather than the display name.

High-Watermark Values

The high-watermark values are used to manage what information is replicated between domain controllers. Each domain controller maintains its own set of high-watermark values for each of its direct replication partners. The high-watermark is just the latest *uSNChanged* value that the domain controller has received from a specific replication partner. When a domain controller sends an update to a replication partner, the *uSNChanged* value is sent along with the update. The destination domain controller retains this *uSNChanged* as the high-watermark value for the replication partner.

The high-watermark values are used during the process of replication. When one domain controller requests updates from another domain controller, the destination domain controller sends its high-watermark value for use by the source domain controller. In effect, the high-watermark is telling the source domain controller which updates the destination domain controller has already received. The source domain controller uses the destination domain controller's high-watermark to filter all of the potential directory updates and sends only the changes with a higher *uSNChanged* value.

Note A separate high-watermark value is maintained for each directory partition on the domain controller and for each direct replication partner.

Up-to-Dateness Vectors and Propagation Dampening

The up-to-dateness vectors are also used to control what information is replicated between domain controllers. The up-to-dateness vectors are used to keep track of all of the originating updates that a domain controller has received from any domain controller. For example, suppose the telephone number for a user is changed on DC1 and the attribute is given the originating USN of *5556*. When this attribute is replicated to DC2, the originating USN is replicated with the updated attribute. Also, the server GUID for DC1 is replicated with the attribute. When DC2 receives this update, it will modify its up-to-dateness vector to show that the latest originating update it received from DC1 is now *5556*.

When a destination domain controller requests updates from a source domain controller, it includes its up-to-dateness vectors with the request. The source domain controller then uses this information to filter the list of all possible updates it could send to the destination domain controller. This option is important when there are more than two domain controllers for a directory partition. For example, if DC3 is added to the scenario described in the preceding paragraph, the telephone number change made on DC1 will be replicated to both DC2 and DC3. Now both DC3 and DC2 will have the updated telephone number, and they will modify their up-to-dateness vector to show that the latest update both of them received from DC1 had an originating USN of *5556*. About 15 seconds after receiving this update, DC2 will notify DC3 that it has updated information. When DC3 requests the directory updates from DC2, it will include its up-to-dateness vector with the request. In this case, DC2 determines that DC3's up-to-dateness vector for DC1 already has the most recent originating USN. If this telephone number update were the only change made to the directory during this time period, no information would be replicated between the DC2 and the DC3 domain controllers.

This process of limiting the updates sent during replication by using the up-to-dateness vector is called *propagation dampening*. This is an important feature because AD DS is designed to create redundant replication connections between domain controllers. One of the problems with creating the redundant links is that the same updates might be sent to a domain controller from multiple replication partners. This could create a significant amount of unnecessary replication traffic, as well as potentially leading to a situation where the same update is sent repeatedly to all domain controllers (resulting in a replication loop). Propagation dampening using the up-to-dateness vector eliminates this possibility.

The high-watermark and up-to-dateness vector are used together to limit replication traffic. The high-watermark identifies the latest change that a domain controller received from another specific domain controller, so the source domain controller does not need to resend changes. The up-to-dateness vector identifies the most recent changes that have been received from all other domain controllers that contain a replica of the partition, so that the source domain controller does not have to send any directory updates that the destination domain controller has received from another replication partner.

Change Stamps and Conflict Resolution

The last property that is used to manage the replication between domain controllers is a *change stamp*. Whenever an attribute is updated, this modification is marked with the change stamp. The change stamp is then sent with the update when it is replicated to other domain controllers. The change stamp is used to determine which change will be accepted in the case of a replication conflict. The change stamp consists of three components:

- **Version number** This is used to track the number of changes that have been made to an attribute on an object. When an object is created, the version number on all attributes is set to *0* if the attribute is left blank. When a blank attribute is assigned a value, the version number is incremented to *1*. Whenever the attribute is updated, the version number increments by one each time.
- **Last write time** This is used to track when the last write occurred to the attribute. The time value is recorded on the server where the attribute is updated and is replicated with the object to other domain controllers.
- **Originating server** This is the GUID for the server where the last originating update to the attribute was applied.

These three components form the change stamp for every modification to an attribute. When the attribute is replicated to another domain controller, this change stamp information is replicated with the attribute. If an attribute is changed on one domain controller and the same attribute is changed on another domain controller before the update is replicated to the second domain controller, this change stamp is used to determine which attribute is accepted as the final change. If a conflict arises, the decision as to which is the final change is made in the following order:

1. **Version number** The change with the highest version number is always accepted. This means that if the change on one domain controller is version 3, and the change on the other domain controller is version 4, the version 4 change will always be accepted.

2. **Last write time** The next value used to determine which value is accepted is the last write time. If the version numbers are identical, the change with the most recent time stamp will be accepted.
3. **Server GUID** If the version numbers are identical and the time stamps are identical, the server database GUID is used to determine which change is accepted. The change coming from the server with the higher GUID will be accepted. These GUIDs are assigned when the domain controllers are added to the domain and the assignment of the GUID is arbitrary.

The AD DS replication process is able to resolve conflicts that are created when the same attribute on an object is modified on two domain controllers at the same time. However, there are at least two other types of conflicts that can arise:

- Adding an object or modifying an object on one domain controller at the same time that the container object for the object is deleted on another domain controller: Take an example in which on one domain controller a new user is added to the Accounting organizational unit (OU). At the same time, on another domain controller, another administrator deletes the Accounting OU. In this case, the container will be deleted on all domain controllers through replication, and the object that was added to the deleted container will be moved to the LostAndFound container in AD DS.
- Adding objects with the same relative distinguished name into the same container: An example of this conflict is when an administrator on one domain controller creates a user object with a relative distinguished name of *Bill* in the Accounting OU, and at the same time, on another domain controller, a user with the same relative distinguished name is moved into the same OU or created in the same OU. In this case, the conflict resolution model will use the GUID assigned to the directory updated to determine which object is kept and which object is renamed. The object with the higher GUID is retained, and the object with the lower GUID is renamed to Bill*CNF:*userGUID*, where the number sign (*) is a reserved character. If the second user object is required, it can be renamed.

Replicating Object Deletions

The replication of object deletions is handled differently in AD DS than other directory updates. When an object like a user account is deleted, the object is not immediately deleted. Rather, a tombstone object is created. The *tombstone object* is the original object where the *isDeleted* attribute has been set to *true*, and most of the other attributes for the object are removed from it. Only a few attributes that are required to identify the object, such as the GUID, SID, SIDHistory, and distinguished name, are retained. Deleted objects are stored in the Deleted Objects hidden container. Every directory partition has a Deleted Objects container.

> **Note** To view the Deleted Objects container in a directory partition, use a tool like Ldp. After connecting and binding to the directory partition, access the Controls option on the Options menu. In the Controls dialog box, add the Return Deleted Objects control. After adding the control, you will be able to view the CN=Deleted Items container when you view the directory tree.

This tombstone is then replicated to other domain controllers in the domain. As each domain controller receives the update, the modifications that were made on the originating domain controller are applied to each domain controller. The tombstone objects remain in the domain database for a specified period of time, called the *tombstone lifetime*. At the end of the tombstone lifetime, set to 180 days by default, each domain controller removes the tombstone from its copy of the database. This process of removing the tombstones from the database is called *garbage collection*. By default, the garbage collection interval for the forest is set at every 12 hours. This means that every 12 hours, the garbage collection process runs and deletes any tombstones that have passed the tombstone lifetime value.

Note The default tombstone lifetime in versions of Active Directory before Windows Server 2008 has varied. In Windows 2000 and Windows 2003 Active Directory, the tombstone lifetime was 60 days. In Windows 2003 SP1, this value was increased to 180 days, but it was changed back to 60 days in Windows Server 2003 R2. If you upgrade an existing domain with a 60-day tombstone to Windows Server 2008, the 60-day tombstone lifetime is retained. The tombstone lifetime and the garbage collection interval can be modified using ADSI Edit or Ldp.exe. These properties are configured on the CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration, DC=*ForestRootDomain* object. The *garbageCollPeriod* and the *tombstoneLifetime* attributes define these settings. In most cases, these values do not need to be modified.

Linked attributes can result in special cases when deleting objects. When an object is deleted, the following changes are made to the linked attributes:

- All of the forward links on the deleted object are removed. For example, if a group object is deleted, all of the member links on the group object are removed. This means that the group is removed from the *memberOf* back-link attribute on each user that was a member of the group.
- All the back-links on the deleted object are removed. For example, if a user is deleted, the user's distinguished name value is removed from the member attributes of each group object that is named in the *memberOf* attribute of the deleted user.

After the linked attribute has been modified on one domain controller, the updates are replicated to other domain controllers just like any other updates.

Important Because of how linked attributes are deleted, you have to treat the authoritative restore of these objects differently than if you are restoring objects without linked attributes. For details, see Chapter 15, "Active Directory Disaster Recovery."

Replicating the SYSVOL Directory

Changes to the AD DS data store are made using the process described previously. However, the System Volume (SYSVOL) folder on each domain controller also contains information that is critical to the correct functioning of AD DS. The SYSVOL shared folder contains the following files and folders that must be available and synchronized between domain controllers in a domain:

- **Group Policy settings** SYSVOL contains a folder with the name of the domain that the domain controller is a member of. In the domain folder is a folder called Policies that contains Group Policy templates and scripts for Windows 2000 or later clients.
- **The NETLOGON shared folder** This includes system policies (Config.pol or Ntconfig.pol files) and user-based logon and logoff scripts for pre-Windows 2000 network clients, such as clients running Windows 98 or Windows NT 4.0. The NETLOGON shared folder is the Scripts folder in the domain folder.

The contents of SYSVOL folder are replicated to every domain controller in a domain. If the domain is at Windows Server 2003 or lower functional level, the File Replication Service (FRS) is responsible for replicating the contents of the SYSVOL folder between domain controllers. When you upgrade the domain functional level to Windows Server 2008, Distributed File System Replication (DFSR) is used to replicate the contents of the SYSVOL folder. In both cases, the connection object topology and schedule that the Knowledge Consistency Checker (KCC) creates for Active Directory replication is used to manage replication between domain controllers.

Note Distributed File System (DFS) Replication is a state-based, multimaster replication engine introduced in Windows Server 2003 R2 that supports replication scheduling and bandwidth throttling. DFS Replication uses a new compression algorithm that is known as Remote Differential Compression (RDC). Using RDC, DFS Replication replicates only the differences (or changes) between the two servers, resulting in lower bandwidth use during replication. For more information on DFSR, see the article "Overview of the Distributed File System Solution in Microsoft Windows Server 2003 R2" at *http://technet2.microsoft.com/windowsserver/en/library/d3afe6ee-3083-4950-a093-8ab748651b761033.mspx?mfr=true*.

Intrasite and Intersite Replication

The description of how AD DS replication works applies to both intrasite and intersite replication. In both cases, the domain controllers use the same processes to optimize the replication process. However, one of the main reasons to create additional sites in AD DS is to manage replication traffic. Because all of the domain controllers within a site are assumed to be connected with fast network connections, replication between these domain controllers is optimized for maximum speed and reduced latency. However, if the replication traffic has to cross a slow network link, conserving network bandwidth is a much more significant issue. Creating multiple sites allows for this conservation of network bandwidth by enabling features such as data compression and scheduled AD DS replication.

Intrasite Replication

The primary goal for replication within a site is to reduce replication latency, that is, to make sure that all domain controllers in a site are updated as quickly as possible. To accomplish this goal, intrasite replication traffic has the following characteristics:

- The replication process is initiated by a notification from the sending domain controller. When a change is made to the database, the sending computer notifies a destination domain controller that changes are available. The changes are then pulled from the sending domain controller by the destination domain controller using a remote procedure call (RPC) connection. After this replication is complete, the domain controller notifies another destination domain controller, which then pulls the changes. This process continues until all the replication partners have been updated.
- Replication occurs almost immediately after a change has been made to the AD DS information. By default, a domain controller will wait for 15 seconds after a change has been made and then begin replicating the changes to other domain controllers in the same site. The domain controller will complete replication with one partner, wait 3 seconds, and then initiate replication with another partner. The reason the domain controller waits 15 seconds after a change is to increase the efficiency of the replication in case additional changes are made to the partition information.
- The replication traffic is not compressed. Because all the computers within a site are connected with fast network connections, the data is sent without compression. Compressing the replication data adds an additional load on the domain controller server. Uncompressed replication traffic preserves server performance at the expense of network utilization.
- Replication traffic is sent to multiple replication partners during each replication cycle. Whenever a change is made to the directory, the domain controller will replicate the information to all direct replication partners, which might be all or some of the other domain controllers in the site.

Modifying Intrasite Replication

In most cases, you will not need to modify how replication works within a site. However, there are some settings that you can modify in specific situations. These settings include:

- **Wait time** If your AD DS forest is running in Windows Server 2003 or Windows Server 2008 functional level, you can modify the time that the domain controller will wait before notifying the first replication partner and before notifying subsequent replication partners. To do this, open the Configuration partition in ADSIEdit and browse to the CN=Partitions,CN=Configuration,DC=*forestname* folder. In the folder, right-click the partition where you want to modify the replication settings. The value for the delay in notifying the first replication partner is stored in the *msDS-Replication-Notify-First-DSA-Delay* attribute. The default value is not displayed but is set at *15 seconds*. The value for subsequent notification delay is stored in the *msDS-Replication-Notify-Subsequent-DSA-Delay* attribute. The default value is *3 seconds*. If your organization contains Windows 2000 Server domain controllers, you must modify the registry on the Windows 2000 Server domain controllers to modify the default settings of *300 seconds* to notify the first replication partner and *30 seconds* for subsequent notifications. You can also use "repadmin *computername* /notifyopt *namingcontext* /first:*timeinseconds* /subs:*timeinseconds*" to set the replication wait times. To reset the wait times to the default values, use the same command with no values assigned to the time settings.

- **Strict replication consistency** Strict replication consistency determines how outdated objects are replicated from reconnected domain controllers that have not replicated in longer than a tombstone lifetime. For example, if a domain controller that is offline while an object is deleted remains offline for the entire tombstone period, the tombstone is never replicated to the server. When the server is reconnected to the network, it will try to replicate the object to other domain controllers. If the destination domain controller has strict replication consistency enabled, it will not accept the inbound replication of an outdated object. By default, Windows Server 2008 enforces strict replication consistency. You can modify this by setting the value of the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\Strict Replication Consistency key to *0*.
- **Amount of data that is replicated in each replication packet** By default, the number of objects Windows Server 2008 domain controllers will replicate in a single packet is 1/1,000,000th the size of RAM, with a minimum of 100 objects and a maximum of 1,000 objects. The maximum size of objects that will be replicated is 1/100th the size of RAM, with a minimum of 1 megabyte (MB) and a maximum of 10 MB. You can modify these settings by creating the Replicator intrasite packet size (objects) and Replicator intrasite packet size (bytes) values in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters path.

Caution Before making any changes to the default settings for intrasite replication, make sure that you test the changes thoroughly. In most cases, these settings do not need to be modified.

Intersite Replication

The primary goal of replication between sites is to reduce the amount of bandwidth used for replication traffic. This means that intersite replication traffic has the following characteristics:

- Replication is initiated according to a schedule rather than when changes are made. To manage replication between sites, you must configure a site link connecting the two sites. One of the configuration options on the site link is a schedule for when replication will occur. Another is the replication interval setting for how often replication will occur during the scheduled time. If the bandwidth between company locations is limited, the replication can be scheduled to happen during nonworking hours.

- Replication traffic is compressed down to about 40 percent of the noncompressed size when replication traffic is more than 32 KB in size. To save bandwidth on the network connection, the bridgehead servers in each site compress the traffic at the expense of additional CPU usage.
- Notifications are not used to alert a domain controller in another site that changes to the directory are available. Instead, the schedule determines when to replicate.

> **Note** You can disable compression for intersite replication and enable notifications. For more details, see the section titled "Configuring Intersite Replication" later in this chapter.

- Intersite replication connections can use either an Internet Protocol (IP) or a Simple Mail Transfer Protocol (SMTP) transport. SMTP can be used as a transport protocol only for the configuration, schema, and application directory partitions, not for the domain partition. The connection protocol you use is determined by the available bandwidth and the reliability of the network that connects company locations.
- Replication traffic is sent through bridgehead servers rather than to multiple replication partners. When changes are made to the directory in one site, the changes are replicated to a single bridgehead server (per directory partition) in that site, and the changes are then replicated to a bridgehead server in the other site. The changes are replicated from the bridgehead server in the second site to all the domain controllers in that site.
- You can easily modify the flow of replication between sites. Almost every component of intersite replication can be changed.

> **Important** One of the key elements in designing AD DS is site design. Site design includes planning the number and location of sites plus the configuration of intersite connections to optimize the use of network bandwidth while minimizing the replication latency. Configuration options for the intersite connections are discussed later in this chapter, and site design issues are discussed in Chapter 5, "Designing the Active Directory Domain Services Structure."

Replication Latency

Because of the way replication works in Windows Server 2008 AD DS, it can take some time for a change made on one domain controller to be replicated to all the other domain controllers in an organization. This time lag is called the *replication latency*. In most cases, the replication latency is easy to calculate, especially within a site. As mentioned earlier, any change made to the data store on one domain controller will be replicated to that domain controller's replication partners in about 15 seconds. The destination domain controller will hold that change for 15 seconds and then pass it on to its replication partners. So the replication latency within a site is about 15 seconds times the number of hops the change has to take before reaching all domain controllers. As explained in the next section, the replication topology within a site never requires more than three hops, so the maximum replication latency within a site will usually be less than one minute.

Determining the replication latency between sites is more difficult. First of all, you must calculate the replication latency within the source site. This replication latency is the amount of time it takes for a change made on a domain controller in the site to be replicated to the source site's bridgehead server. After the information arrives at the originating site's bridgehead server, the site link schedule and replication interval determine the amount of time it takes for the information to get to the destination site. The default configuration for site links is to replicate every three hours. If this configuration is not changed, a maximum of three hours will be added to the replication latency. When the information arrives at the bridgehead server in the destination site, the intrasite replication latency for the destination site must be added. In some cases, this replication latency might be unacceptable. To minimize this, you can shorten the replication interval to a minimum of 15 minutes for intersite replication.

Managing replication latency is a matter of balancing the need for a short latency period and bandwidth limitations. If you want the shortest possible latency period, you should put all the domain controllers in the same site, and the replication latency will be about one minute for all domain controllers. However, if your company locations are separated by WAN connections with limited bandwidth, you will require multiple sites so that you can manage network utilization for AD DS replication, but replication latency will be higher.

Urgent Replication

In some cases, the replication latency described in the previous section is too long. In particular, this is the case when a security-related attribute has been modified in the directory. For these situations, AD DS uses *urgent replication,* in which a domain controller forwards the changes immediately to its replication partners. Any domain controller receiving an urgent update will also immediately forward the change. In this way, all domain controllers in the site are updated within seconds. The following types of changes trigger an urgent replication:

- Modifying the account lockout policy for the domain
- Modifying the domain password policies
- Moving the relative identifier (RID) master to a new domain controller
- Changing a Local Security Authority (LSA) secret, such as when the domain controller machine password is modified
- Locking out a user account when a user attempts to log on too many times using an incorrect password

By default, urgent updates apply only to intrasite replication and not to intersite replication. This default handling of urgent updates can be modified by enabling notification for replication between sites.

User password changes are not replicated using the same urgent replication model. Instead, when a user changes his or her password on a domain controller, the password change is immediately replicated directly to the PDC emulator for the domain. This replication crosses site boundaries and does not make use of the bridgehead servers in each site. Instead, the domain controller where the change was made uses an RPC connection to the PDC emulator to update the password. The PDC emulator then updates all the other domain controllers through the normal process of replication. If the user tries to log on to a domain controller that has not yet received the new password, the domain controller will check with the PDC emulator to see if there are any updated password changes for the user before denying the logon.

Replication Topology Generation

One of the keys to understanding AD DS replication is understanding how the replication topology is created. By default, the process of creating the replication topology is handled automatically by AD DS. Although the replication topology can be manually configured, in most cases the default configuration by the system is the best option.

In order for the replication topology to be successfully created, the following components must be in place:

- **Routable IP infrastructure** In order to configure intersite replication, you need to configure AD DS sites and map the sites to IP subnet address ranges. Domain controllers and client computers use this IP subnet to site mapping when locating domain controllers.
- **DNS** AD DS replication topology requires DNS in order for domain controllers locate replication partners. DNS also stores SRV resource records that provide site affinity information to clients searching for domain controllers.
- **Netlogon service** Netlogon is required for DNS registrations. As well, the Netlogon service must be running for AD DS to function.
- **Remote Procedure Call (RPC) connectivity** AD DS domain controllers must be able to connect to other domain controllers in the same domain by using RPCs. RPCs must be used between domain controllers in the same site and in different sites if the domain controllers are in the same domain. SMTP is an alternative protocol that can be used by domain controllers in different domains and sites.
- **Intersite Messaging** Intersite Messaging is required for SMTP intersite replication and for site coverage calculations. If the forest functional level is Windows 2000, Intersite Messaging is also required for intersite topology generation.

Knowledge Consistency Checker

Knowledge Consistency Checker (KCC) is the process that runs on every domain controller to create the replication topology within a site and between sites. As soon as a domain controller is added to an AD DS forest, KCC begins creating a replication topology that is both efficient and fault tolerant. As additional domain controllers are added to a site or as additional sites are added, KCC uses the information about servers, sites, site links, and schedules to create the optimal replication topology.

The KCC runs on each domain controller. It uses the forest information stored in the configuration directory partition on each domain controller to create a replication topology. Because all domain controllers use the same configuration information and the same algorithm for creating the topology, the topology is created without direct communication between KCC components on different domain controllers. The KCC communicates with other KCCs only to make an RPC request for replication error information.

KCC also dynamically deals with changes or failures within the replication topology. If one of the domain controllers is offline for a period of time, KCC revises the replication topology to work around the unavailable domain controller. By default, KCC on every domain controller recalculates the replication topology every 15 minutes. You can force KCC to recalculate the replication topology at any time through the Active Directory Sites And Services administrative tool by locating the server where you want to check the replication topology, right-clicking the NTDS Settings container in the server container, selecting All Tasks, and then selecting Check Replication Topology. You can also force the domain controller to recalculate the replication topology by using the Repadmin /kcc *domaincontrollername* command.

Connection Objects

When KCC creates the replication topology, it creates a series of connection objects that are stored in the configuration directory partition of AD DS. The connection objects are direct logical connections between domain controllers that are used to replicate directory information. KCC tries to create a replication topology that is both efficient and fault-tolerant. KCC builds as many connection objects as are required to achieve these goals.

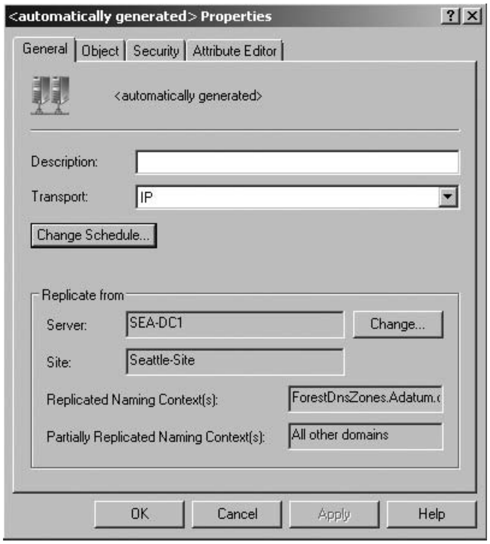
Connection objects are always created as one-way pull connections between two domain controllers. This is because the normal process of replication is always a pull operation where the destination domain controller requests the information from a sending domain controller. In most cases, KCC will build two one-way connections between domain controllers so that information can be replicated either way.

In most cases, the connection objects automatically created by KCC are optimized and you do not need to make any changes. However, in some cases you might want to modify the connection objects. For example, you may need to modify the connection object to aid in troubleshooting AD DS replication.

You can modify the default connection objects in two ways: by modifying some settings on connection objects created by KCC and by adding new connection objects.

Modifying a Connection Object Created by KCC

You can modify the schedule and the source domain controller for a connection object within a site, and you can also modify the transport protocol for connection objects between sites. The connection interface is shown in Figure 4-2. By default, domain controllers within a site will check all their replication partners for missed updates every 15 minutes. You can change that schedule to never check or to check every hour or every half hour. When you modify the connection object, it is renamed from <*automatically generated*> to the object's globally unique identifier (GUID). You can rename the object after modifying it.



<automatically generated> Properties

<automatically generated>

Description:

Transport: IP

Server: SEA-DC1

Site: Seattle-Site

Replicated Naming Context(s): ForestDnsZones.Adatum.c

Partially Replicated Naming Context(s): All other domains

Figure 4-2 Modifying an existing connection object.

Creating a New Connection Object

You can also create an entirely new connection object to force a particular replication topology. When you create a connection object, you are given a choice of which domain controller to pull changes from. You can also modify any of the other settings on the connection agreement.

KCC will not delete or modify any connections that have been manually modified or created. However, KCC will use the manual connection objects as it would use any other connection, and KCC might reconfigure the connection objects in the site to compensate for the manually created connections.

Intrasite Replication Topology

Within a single site, KCC will create a replication topology that includes redundant links. The primary goal for designing AD DS replication is availability and fault tolerance. The unavailability of a single domain controller should not cause AD DS replication to fail. The disadvantage of using redundant links is that a domain controller might receive the same update several times, because each domain controller will have multiple replication partners. As described earlier, AD DS replication uses propagation dampening to avoid multiple updates of the same information.

As domain controllers with replicas of particular AD DS partitions are added to the organization, KCC automatically begins creating the replication topology. This topology forms a replication ring. Figure 4-3 shows an example of a simple network structure with three domain controllers in the same domain and in a single site.

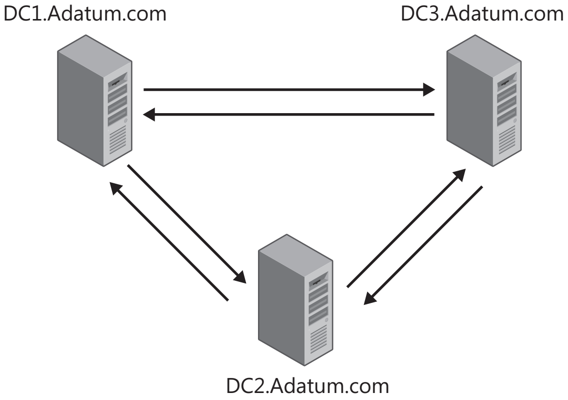


Figure 4-3 A simple replication ring.

As shown in Figure 4-3, KCC creates a replication ring in which every domain controller is configured with two incoming replication connections. If one of the connections is not available, updates can still arrive on the other connection. Also, each domain controller is configured as the source domain controller for two other domain controllers. This creates a redundant ring for each domain controller. As the number of domain controllers with a replica of a particular partition increases, a second principle for creating connections becomes important. KCC will always create a replication topology in which each domain controller in a site is no more than three replication hops away from any other domain controller. As the number of domain controllers with the same directory partition in a site increases beyond seven, extra connection objects are created to decrease the potential number of hops to three or fewer. For example, the site shown in Figure 4-4 has nine domain controllers. It would have a replication topology that would include at least one additional connection.

Replication rings are based on directory partitions. This means that KCC calculates a replication ring for each directory partition. For example, an organization might have multiple domains in a single site and an application directory partition that is replicated to several domain controllers in the site. The configuration could be set up as shown in Figure 4-5.

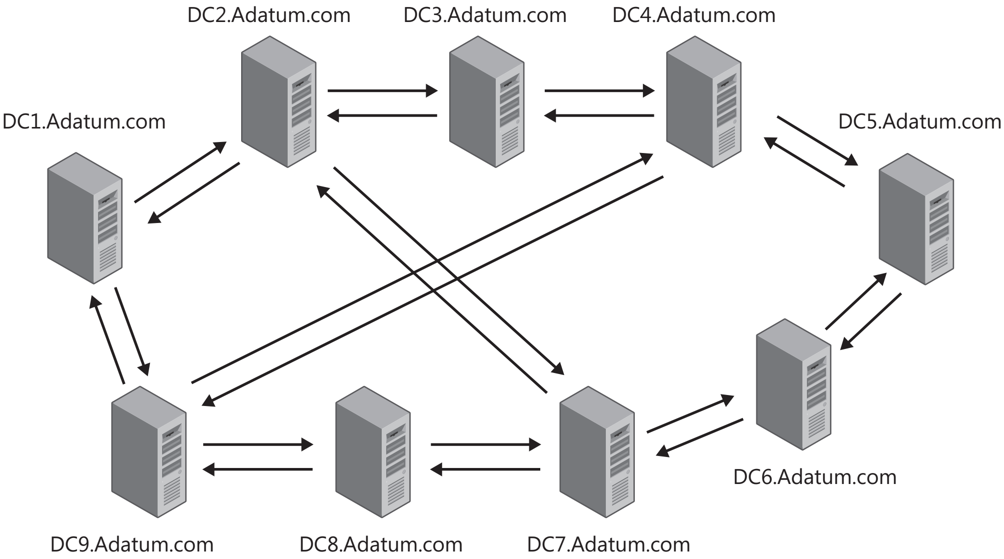
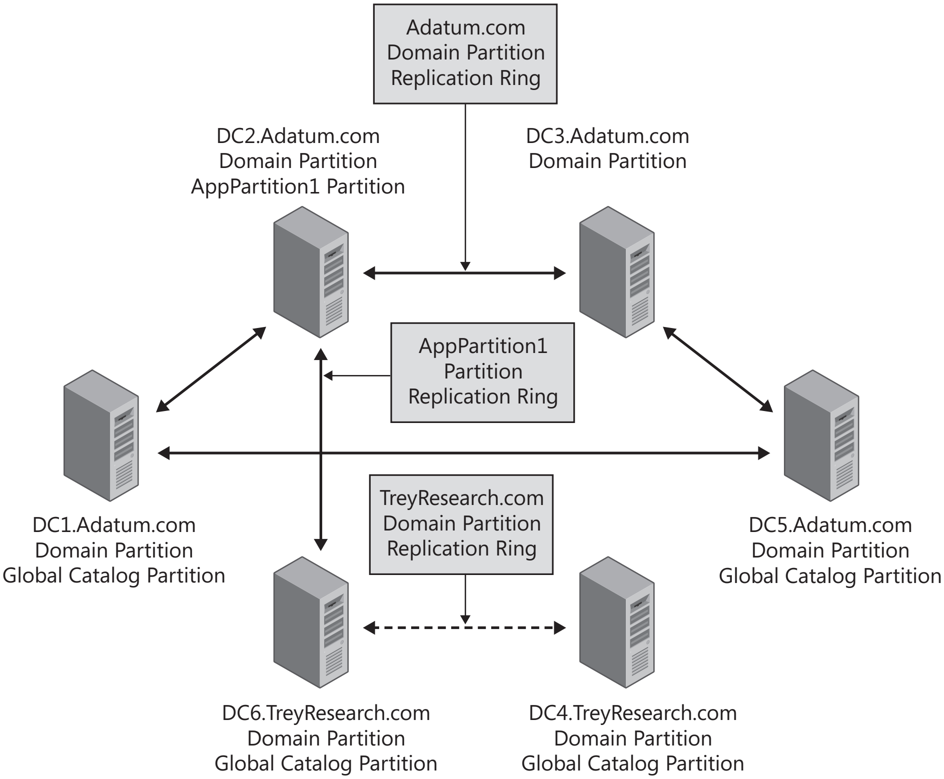

DC2.Adatum.com
DC3.Adatum.com
DC4.Adatum.com
DC1.Adatum.com
DC5.Adatum.com
DC6.Adatum.com
DC9.Adatum.com
DC8.Adatum.com
DC7.Adatum.com

Figure 4-4 A replication ring with more than seven domain controllers.


Adatum.com
Domain Partition
Replication Ring
DC2.Adatum.com
Domain Partition
AppPartition1 Partition
DC3.Adatum.com
Domain Partition
AppPartition1
Partition
Replication Ring
DC1.Adatum.com
Domain Partition
Global Catalog Partition
TreyResearch.com
Domain Partition
Replication Ring
DC5.Adatum.com
Domain Partition
Global Catalog Partition
DC6.TreyResearch.com
Domain Partition
Global Catalog Partition
DC4.TreyResearch.com
Domain Partition
Global Catalog Partition

Note: All domain controllers also host a replica of the Configuration and Schema Partitions. The replication ring for the Configuration and Schema Partitions would include all the domain controllers.

Figure 4-5 Replication rings created for each directory partition.

In the scenario illustrated in Figure 4-5, the replication rings shown in Table 4-1 would be created.

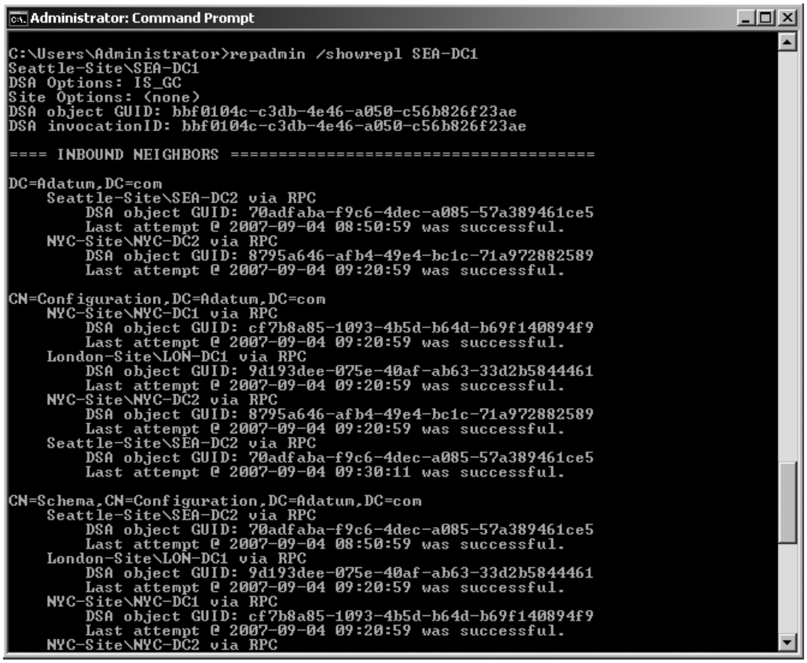
Table 4-1 Replication Rings in a Complex Site

Directory Partition	Replication Partners
Configuration directory partition, schema directory partition	All the domain controllers would be included in the replication ring for both the configuration directory partition and the schema directory partition.
ADatum.com domain directory partition	DC1.ADatum.com, DC2.ADatum.com, DC3.ADatum.com, DC5.ADatum.com
TreyResearch.com domain directory partition	DC4.TreyResearch.com, DC6.TreyResearch.com
Global catalog partition	DC1.ADatum.com, DC4.ADatum.com, DC4.TreyResearch.com
AppPartition1 application directory partition	DC2.ADatum.com, DC6.TreyResearch.com

> **Note** The Domain Name System (DNS) application directory partitions (ForestDnsZones and DomainDnsZones) are also included in the replication topology. To keep the Figure 4-5 scenario from getting too complicated, these partitions are not included in that figure nor in the associated table. As discussed in Chapter 3, "Active Directory Domain Services and Domain Name System," these partitions are treated exactly like other domain directory partitions. Also, the global catalog replication topology is not shown in Figure 4-5. The process of creating a global catalog replication ring is slightly different than for other partitions and will be described in the next section.

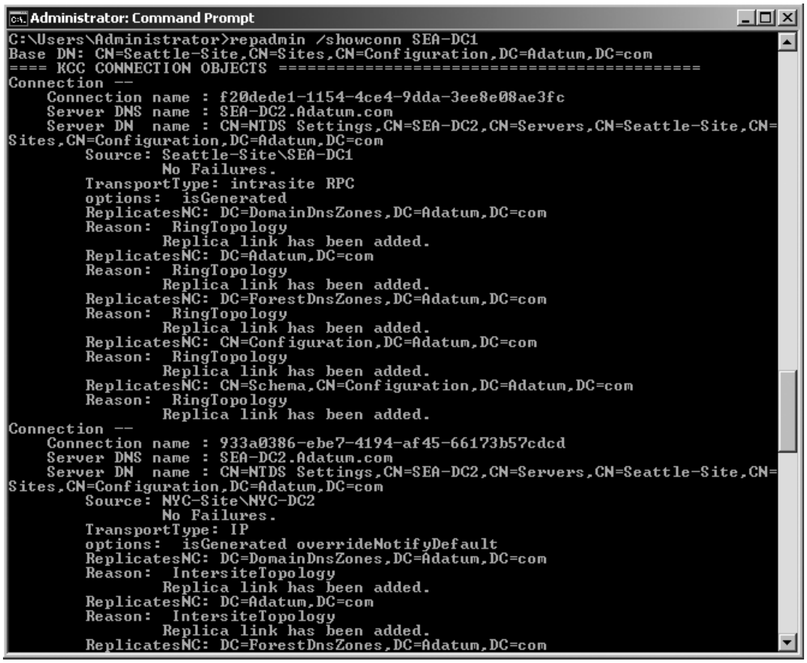
The replication connections and replication status can be viewed by using the Repadmin command-line tool with the */showrepl* parameter. Figure 4-6 shows the partial output when running this command on a domain controller in a forest with multiple domains and sites.

The replication ring is a logical concept; the actual replication topology as implemented with the connection objects does not duplicate the replication rings exactly. Although a separate replication ring is created for each directory partition, KCC will not create additional connection objects for each replication ring. Instead, KCC reuses connection objects to use as few connection objects as possible while still creating a replication topology that provides redundancy for each partition. For example, in the scenario illustrated in Figure 4-5, DC2.ADatum.com has a connection object with DC6.TreyResearch.com. This single connection object could be used to replicate the schema partition, the configuration partition, and the AppPartition1 partition, as well as the DNS application directory partitions. You can see which directory partitions are replicated by each connection object by viewing the connection object in Active Directory Sites And Services and Repadmin. As shown in Figure 4-6, you can view the Replicated Naming Context(s) setting on each connection object. You can also use the Repadmin /showconn *servername* to show the partitions that are being replicated by each connection object. Partial output of this command is shown in Figure 4-7. In this figure, you can see that the connection object with SEA-DC2.ADatum.com is being used to replicate the DomainDnsZones, ForestDnsZones, ADatum.com, Configuration, and Schema partitions.



```
C:\Users\Administrator>repadmin /showrepl SEA-DC1
Seattle-Site\SEA-DC1
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: bbf0104c-c3db-4e46-a050-c56b826f23ae
DSA invocationID: bbf0104c-c3db-4e46-a050-c56b826f23ae

==== INBOUND NEIGHBORS ======================================

DC=Adatum,DC=com
    Seattle-Site\SEA-DC2 via RPC
        DSA object GUID: 70adfaba-f9c6-4dec-a085-57a389461ce5
        Last attempt @ 2007-09-04 08:50:59 was successful.
    NYC-Site\NYC-DC2 via RPC
        DSA object GUID: 8795a646-afb4-49e4-bc1c-71a972882589
        Last attempt @ 2007-09-04 09:20:59 was successful.

CN=Configuration,DC=Adatum,DC=com
    NYC-Site\NYC-DC1 via RPC
        DSA object GUID: cf7b8a85-1093-4b5d-b64d-b69f140894f9
        Last attempt @ 2007-09-04 09:20:59 was successful.
    London-Site\LON-DC1 via RPC
        DSA object GUID: 9d193dee-075e-40af-ab63-33d2b5844461
        Last attempt @ 2007-09-04 09:20:59 was successful.
    NYC-Site\NYC-DC2 via RPC
        DSA object GUID: 8795a646-afb4-49e4-bc1c-71a972882589
        Last attempt @ 2007-09-04 09:20:59 was successful.
    Seattle-Site\SEA-DC2 via RPC
        DSA object GUID: 70adfaba-f9c6-4dec-a085-57a389461ce5
        Last attempt @ 2007-09-04 09:30:11 was successful.

CN=Schema,CN=Configuration,DC=Adatum,DC=com
    Seattle-Site\SEA-DC2 via RPC
        DSA object GUID: 70adfaba-f9c6-4dec-a085-57a389461ce5
        Last attempt @ 2007-09-04 08:50:59 was successful.
    London-Site\LON-DC1 via RPC
        DSA object GUID: 9d193dee-075e-40af-ab63-33d2b5844461
        Last attempt @ 2007-09-04 09:20:59 was successful.
    NYC-Site\NYC-DC1 via RPC
        DSA object GUID: cf7b8a85-1093-4b5d-b64d-b69f140894f9
        Last attempt @ 2007-09-04 09:20:59 was successful.
    NYC-Site\NYC-DC2 via RPC
```

Figure 4-6 Using *Repadmin* to view the replication connections.



```
C:\Users\Administrator>repadmin /showconn SEA-DC1
Base DN: CN=Seattle-Site,CN=Sites,CN=Configuration,DC=Adatum,DC=com
==== KCC CONNECTION OBJECTS ============================================
Connection --
    Connection name : f20dede1-1154-4ce4-9dda-3ee8e08ae3fc
    Server DNS name : SEA-DC2.Adatum.com
    Server DN  name : CN=NTDS Settings,CN=SEA-DC2,CN=Servers,CN=Seattle-Site,CN=
Sites,CN=Configuration,DC=Adatum,DC=com
        Source: Seattle-Site\SEA-DC1
                No Failures.
        TransportType: intrasite RPC
        options:  isGenerated
        ReplicatesNC: DC=DomainDnsZones,DC=Adatum,DC=com
        Reason:  RingTopology
                Replica link has been added.
        ReplicatesNC: DC=Adatum,DC=com
        Reason:  RingTopology
                Replica link has been added.
        ReplicatesNC: DC=ForestDnsZones,DC=Adatum,DC=com
        Reason:  RingTopology
                Replica link has been added.
        ReplicatesNC: CN=Configuration,DC=Adatum,DC=com
        Reason:  RingTopology
                Replica link has been added.
        ReplicatesNC: CN=Schema,CN=Configuration,DC=Adatum,DC=com
        Reason:  RingTopology
                Replica link has been added.
Connection --
    Connection name : 933a0386-ebe7-4194-af45-66173b57cdcd
    Server DNS name : SEA-DC2.Adatum.com
    Server DN  name : CN=NTDS Settings,CN=SEA-DC2,CN=Servers,CN=Seattle-Site,CN=
Sites,CN=Configuration,DC=Adatum,DC=com
        Source: NYC-Site\NYC-DC2
                No Failures.
        TransportType: IP
        options:  isGenerated overrideNotifyDefault
        ReplicatesNC: DC=DomainDnsZones,DC=Adatum,DC=com
        Reason:  IntersiteTopology
                Replica link has been added.
        ReplicatesNC: DC=Adatum,DC=com
        Reason:  IntersiteTopology
                Replica link has been added.
        ReplicatesNC: DC=ForestDnsZones,DC=Adatum,DC=com
```

Figure 4-7 A single connection object used to replicate multiple directory partitions.

Global Catalog Replication

The global catalog is a different partition than the other partitions in that it is built from all the domain databases in the entire forest. The global catalog itself is read-only on all domain controllers, which means that the information in the global catalog cannot be directly modified by the administrator. The global catalog is just a list of all the attributes that are moved into the global catalog because their *isMemberOfPartialAttributeSet* attribute is set to *true*.

The fact that the global catalog is created from the domain databases also affects the replication ring for the global catalog. Each global catalog server must get the global catalog information from the domain controllers in all domains. For a simple example, see Figure 4-8, which shows a company with two domains and one domain controller in each domain in the same site. Only the DC1.ADatum.com domain is configured as a global catalog server. The global catalog server is also the only domain controller for the ADatum.com domain, so it will extract the global catalog information for ADatum.com from its own domain database. The domain controller in the TreyResearch.com domain has the only copy of that domain directory partition, so DC1.ADatum.com collects the global catalog information for the TreyResearch.com domain from DC2.TreyResearch.com. To extract the information from the TreyResearch.com domain, a connection object is created from DC2.TreyResearch.com to DC1.ADatum.com. This connection is then used to replicate the global catalog information to DC1.ADatum.com.

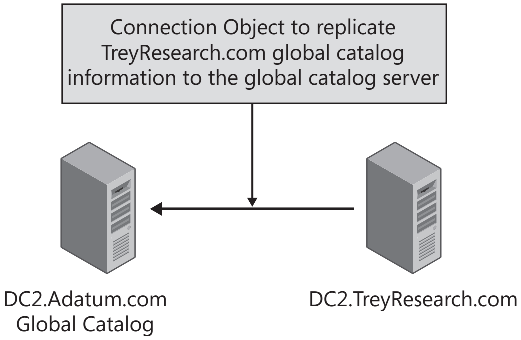

Connection Object to replicate TreyResearch.com global catalog information to the global catalog server
DC2.Adatum.com
Global Catalog
DC2.TreyResearch.com

Figure 4-8 An example of simple global catalog replication.

Figure 4-9 shows a more complicated example of how the global catalog is created and replicated. In this scenario, a connection object is configured from a domain controller in every domain to each global catalog server. For example, DC1.ADatum.com will have an inbound connection object from DC2.ADatum.com, DC4.TreyResearch.com, and DC6.Contoso.com. This connection object is used to build the global catalog on DC1.ADatum.com. Each of the other global catalog servers will have a similar set of connection objects created. Also, a separate replication ring is created for the global catalog partition with all of the global catalog servers.

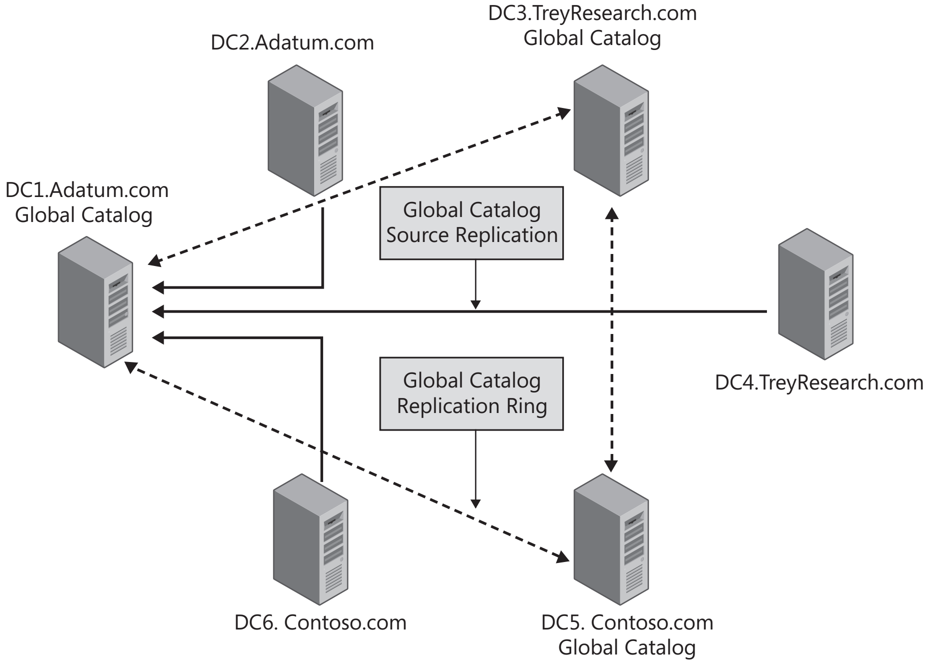

DC3.TreyResearch.com
Global Catalog
DC2.Adatum.com
DC1.Adatum.com
Global Catalog
Global Catalog
Source Replication
Global Catalog
Replication Ring
DC4.TreyResearch.com
DC6. Contoso.com
DC5. Contoso.com
Global Catalog

Figure 4-9 An example of a more complicated global catalog replication.

Intersite Replication Topology

When additional sites are added to a forest, the replication topology becomes increasingly complex. In a multisite scenario, a replication topology must be created for each site, and a replication topology must be created for replication between sites. To deal with this complexity, the process for creating connection objects changes for the intrasite replication. Within a site, KCC on each domain controller is responsible for creating the connection objects that it needs to ensure that it has the required replication redundancy for all of its partitions; it then replicates the information about the connection objects to the other domain controllers. Also, the domain controller receives information about the connection objects that have been created by other domain controllers. The next time KCC runs, connection objects might be added, modified, or deleted based on the information the domain controller has received about other connection objects in the site. Eventually, KCCs on all the domain controllers in a site determine the optimal replication configuration.

A similar approach is used when determining the replication topology between sites, except that one domain controller in each site is responsible for developing the intersite topology. KCC on one domain controller in the site is designated as the Inter-Site Topology Generator (ISTG) for the site. There is only one ISTG per site regardless of how many domains or other directory partitions there are in the site. ISTG is responsible for calculating the ideal replication topology for the entire site. This process consists of the following two actions:

- Identifying the bridgehead servers for each directory partition that is present in the site. Replication between sites is always sent from a bridgehead server in one site to a bridgehead server in another site. This means that information is replicated only once across the network connection between the sites.
- Creating the connection objects between the bridgehead servers to ensure that the information is replicated between the sites. Because the replication is configured between bridgehead servers, there are no redundant connection objects configured as there are within a site. However, the ISTG will create connection objects with bridgehead servers in multiple sites if the site links are configured to enable the connections.

When a new site is added to the forest, ISTG in each site determines which directory partitions are present in the new site. ISTG then calculates the new connection objects that will be needed to replicate the required information from the new site. Also, ISTG designates one domain controller to be the bridgehead server for each directory partition. ISTG creates the required connection agreement in its directory, and this information is replicated to the bridgehead server. The bridgehead server then creates a replication connection with the bridgehead server in the remote site, and replication begins.

To see how the replication topology is created between sites, see Figure 4-10. In this example, the forest contains two sites and two domains with domain controllers for each domain in each site. There is also at least one global catalog server in each site. This means that each site contains a directory partition for each of the domains and a global catalog partition, as well as the schema directory partition and the configuration directory partition. Two bridgehead servers would be designated in each site, because each of these partitions must be replicated between the sites. One of the bridgehead servers in each site will be a domain controller in the Adatum.com domain. Another bridgehead server in each site must be a domain controller in the TreyResearch.com domain. In the Figure 4-10 example, DC1.ADatum.com and DC6.TreyResearch.com are also global catalog servers. This means that they will become bridgehead servers to replicate global catalog information between sites. Because the schema directory partition and the configuration directory partition are shared by all domain controllers, one of the existing connection objects can be used to replicate these partitions.

> **Note** This discussion of the replication topology is based on the default behavior for AD DS domain controllers. Administrators can modify the default behavior, especially for replication between sites. These modifications and the effect of these changes are discussed later in this chapter.

RODCs and the Replication Topology

RODCs also participate in normal AD DS replication, and connection objects must be created between RODCs and other domain controllers. However, because RODCs have read-only copies of the AD DS database, the KCC will only create single one-way connection objects from a domain controller with a writable copy of the database to the RODC. The RODC can only pull changes from other domain controllers; it can never be configured as a replication source for any connection object.

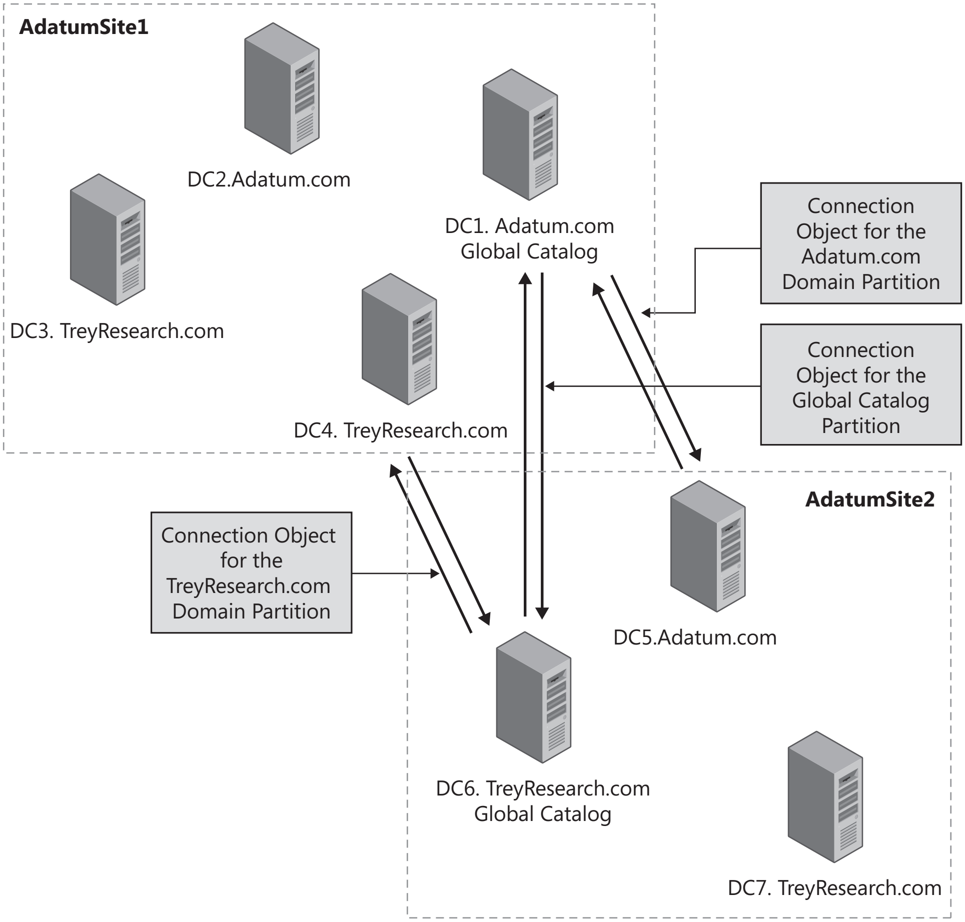

AdatumSite1
DC2.Adatum.com
DC1. Adatum.com
Global Catalog
DC3. TreyResearch.com
DC4. TreyResearch.com
Connection Object for the Adatum.com Domain Partition
Connection Object for the Global Catalog Partition
AdatumSite2
Connection Object for the TreyResearch.com Domain Partition
DC5.Adatum.com
DC6. TreyResearch.com
Global Catalog
DC7. TreyResearch.com

Figure 4-10 Intersite connection objects.

RODC replication is also limited by which domain controllers can be direct replication partners. RODCs can replicate all AD DS partitions except the domain partition from Windows Server 2003 domain controllers. RODCs can also replicate all partitions from another Windows Sever 2008 domain controller, but they must replicate the domain partition from a domain controller running Windows Server 2008. This means that each RODC must have a connection object with a Windows Server 2008 domain controller with a writable copy of the database for the RODC's domain. This also means that when you upgrade a domain from Windows Server 2003, the first Windows Server 2008 domain controller cannot be an RODC.

If the RODC is deployed in a separate site, the Windows Server 2008 should be placed in the nearest site in the topology. Figure 4-11 provides an example of a possible RODC deployment and the connection objects that would be configured.

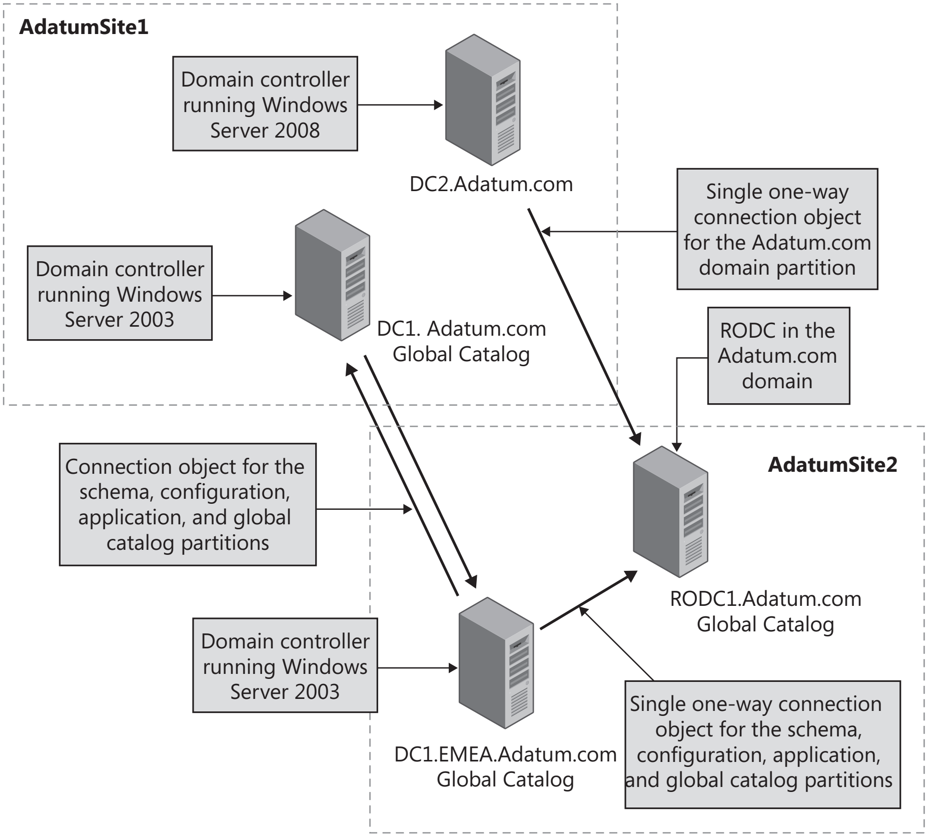

AdatumSite1
Domain controller running Windows Server 2008
DC2.Adatum.com
Single one-way connection object for the Adatum.com domain partition
Domain controller running Windows Server 2003
DC1. Adatum.com Global Catalog
RODC in the Adatum.com domain
AdatumSite2
Connection object for the schema, configuration, application, and global catalog partitions
RODC1.Adatum.com Global Catalog
Domain controller running Windows Server 2003
DC1.EMEA.Adatum.com Global Catalog
Single one-way connection object for the schema, configuration, application, and global catalog partitions

Figure 4-11 Replication connection objects with RODCs.

Configuring Intersite Replication

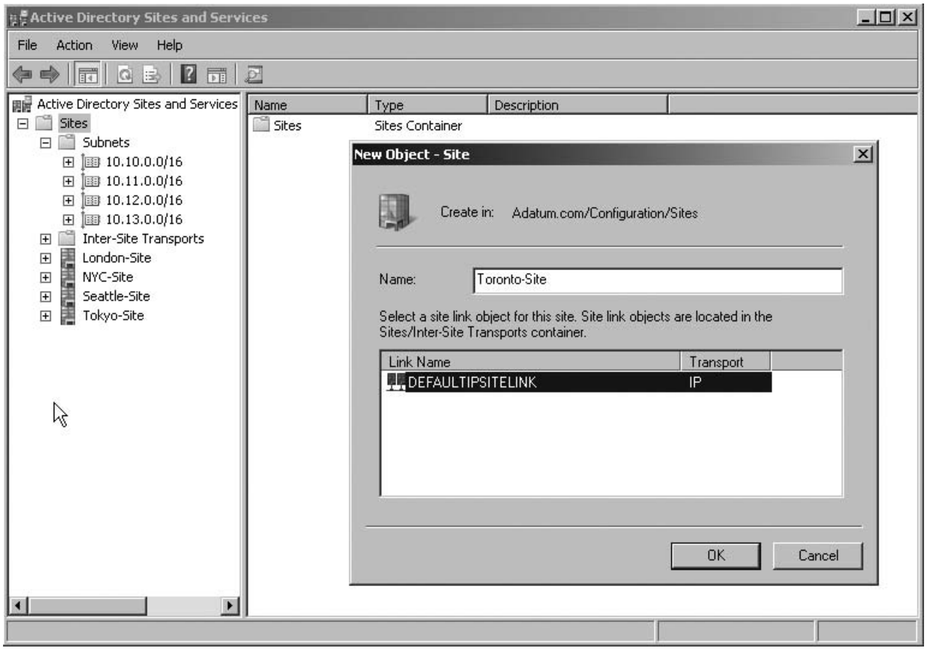
The most important reason for creating multiple sites in AD DS is to control replication traffic between company locations, especially between locations that are separated by slow WAN connections. As described in Chapter 2, an AD DS site is a network location in which all the domain controllers are connected to each other with fast and reliable network connections. One of the tasks of setting up an AD DS network is determining where to draw the site boundaries and then connecting the sites together.

> **Note** Defining clear criteria for when to create an additional site is difficult because of the large numbers of variables that have to be included in this decision. Chapter 5 goes into detail about when you should consider creating additional sites. That chapter also covers many of the other design issues that you must consider when designing the site topology.

Creating Additional Sites

When AD DS is installed, a single site called the Default-First-Site-Name (the site can be renamed) is created. Because sites are usually based on the company location, you can rename this site to more accurately reflect the location where the domain controllers in the site are located. If additional sites are not created, all subsequent domain controllers will be added to this site as they are installed. However, if your company has multiple locations with limited bandwidth between the locations, you will almost certainly want to create additional sites.

Additional sites are created using the Active Directory Sites And Services administrative tool (see Figure 4-12). To create a new site, right-click the Sites container and then click New Site.


Active Directory Sites and Services
File
Action
View
Help
Active Directory Sites and Services
Sites
Subnets
10.10.0.0/16
10.11.0.0/16
10.12.0.0/16
10.13.0.0/16
Inter-Site Transports
London-Site
NYC-Site
Seattle-Site
Tokyo-Site
Name
Type
Description
Sites
Sites Container
New Object - Site
OK
Cancel

Create in: Adatum.com/Configuration/Sites

Name: Toronto-Site

Select a site link object for this site. Site link objects are located in the Sites/Inter-Site Transports container.

Link Name	Transport
DEFAULTIPSITELINK	IP

Figure 4-12 Creating a new site in Active Directory Sites And Services.

When you create a new site, you must link the site with an existing site link. This ensures that the site will automatically be included in the replication topology. From the Link Name list, choose which site link will be used to connect this site to other sites.

Each site is associated with one or more IP subnets in AD DS. By default, no subnets are created in AD DS, so you will normally begin by creating all of the subnets associated with the Default-First-Site-Name site. As you create additional sites, also create additional subnets in the Subnets container in Active Directory Sites And Services and associate the subnets with the new site.

On the Disc As you modify the site configuration, ensure that you document all of the changes you make. You can use the ADDSSites.xlsx job aid on the CD as a template for documenting the site configuration. You can use the ListADDSSites.ps1 Windows PowerShell script on the CD to display information about all of the sites in your forest. Remember that you need to provide the full path when running a Windows PowerShell script, and you may need to modify the PowerShell script execution policy before you can run a script.

For examples of Visual Basic Scripting Edition (VBScript) scripts that you can use to obtain site information, see the Script Center Script Repository Web site at *http://www.microsoft.com/technet/scriptcenter/scripts/default.mspx?mfr=true*.

To move an existing domain controller into the site, right-click the domain controller object in its current Servers container and select Move. You are then given a choice about which site you want to move the domain controller into. If you install a new domain controller and you have more than one site in your forest, you are given a choice about which site to install the new domain controller. The default selection in the Active Directory Domain Services Installation Wizard is to locate the domain controller in the site where the IP subnet matches the domain controller's IP address.

Important When you move a domain controller to a new site, ensure that you modify the domain controller IP configuration to reflect the new site location. You will also need to refresh the host record in DNS by using the *IPConfig /refreshDNS* command and update the SRV records by stopping and starting the Netlogon service. Verify that you can ping all domain controllers in the domain by fully qualified domain name after completing the domain controller move.

Site Links

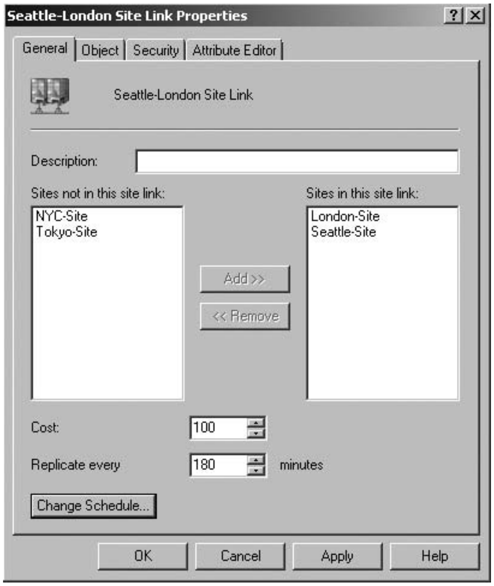
The AD DS objects that connect sites together are called *site links*. When AD DS is installed, a single site link—called DEFAULTIPSITELINK—is created. If you do not create any additional site links before you create additional sites, each site is included in this default site link. If all of the WAN connections between your company locations are equal in terms of bandwidth and cost, you can just accept this default configuration. If all the sites are connected by one site link, the replication traffic between all sites will have exactly the same properties. If you make a change on this site link, the replication configuration for all sites will be modified.

On the Disc As part of documenting your site configuration, ensure that you also document the site link configuration. You can use the ADDSSites.xlsx job aid on the CD. The ListADDSSites.ps1 script on the CD lists the site links associated with each site.

However, in many cases, you might not want to have the replication between all sites configured the same way. For example, if your company locations are linked by different network connections, you may want to replicate AD DS information across network connections with limited available bandwidth less frequently than you do across network connections with more available bandwidth. If you want to be able to configure different replication settings between sites, you must create additional site links and assign the appropriate sites to the site links.

> **Note** Creating a site link does not replace the work of ISTG; all it does is make it possible for ISTG to do its work. After a site link is in place, ISTG will use the site link to create the required connection objects to replicate all the AD DS partitions between each site.

The following are the configuration options on all site links. Figure 4-13 shows the interface for configuring site links:



Seattle-London Site Link

Description:

Sites not in this site link:
NYC-Site
Tokyo-Site

Sites in this site link:
London-Site
Seattle-Site

Cost: 100

Replicate every 180 minutes

Figure 4-13 Configuring site links.

- **Cost** The cost for a site link is an administrator-assigned value that defines the relative cost of the site link. The cost will usually reflect the speed of the network connection and the expenses associated with using the connection. This cost is important if there are redundant site links in the organization, that is, if there is more than one path for replication to travel from one site to another. In all cases, the lowest-cost route will be chosen as the replication path.

Important Creating redundant site links between sites and configuring costs on the site links is only useful if you have multiple WAN connections between the sites. If you only have one network connection between company locations, adding site links provides no benefit.

- **Replication schedule** The replication schedule defines what times during the day the site link is available for replication. The default replication schedule allows for replication to occur 24 hours a day. However, if the available bandwidth to a site is very limited, you might want to have replication occur only during nonworking hours.
- **Replication interval** The replication interval defines the intervals at which the bridgehead servers check with the bridgehead servers in the other sites to see if there are any directory updates. By default, the replication interval for site links is set at *180 minutes*. The replication interval is only applied during the replication schedule. If the replication schedule is configured to allow replication from 22:00 to 05:00, by default, the bridgehead servers will check for updates every three hours during that time.
- **Replication transports** The site link can use either RPC over IP or SMTP as the replication transport. See "Replication Transport Protocols" later in this chapter for more details.

These options provide significant flexibility for configuring replication between sites. However, there are also some mistakes to avoid. To understand how these options work together, consider a company network like that shown in Figure 4-14.

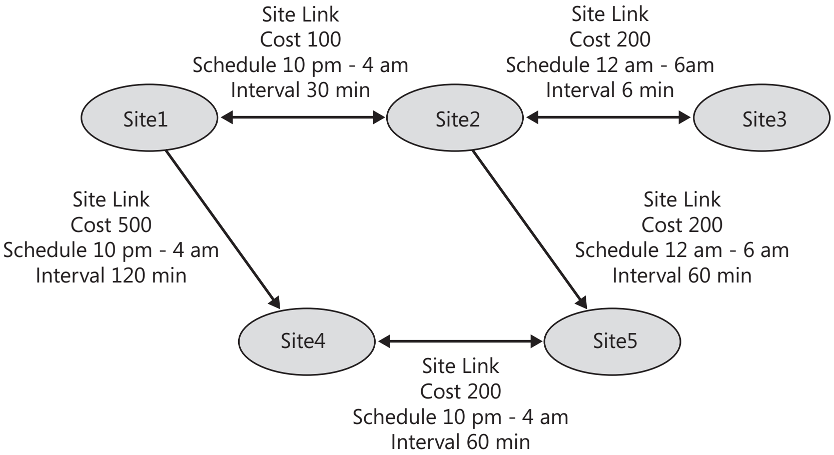

Site Link
Cost 100
Schedule 10 pm - 4 am
Interval 30 min
Site Link
Cost 200
Schedule 12 am - 6am
Interval 6 min
Site1
Site2
Site3
Site Link
Cost 500
Schedule 10 pm - 4 am
Interval 120 min
Site Link
Cost 200
Schedule 12 am - 6 am
Interval 60 min
Site4
Site5
Site Link
Cost 200
Schedule 10 pm - 4 am
Interval 60 min

Figure 4-14 A site link configuration.

In Windows Server 2008 AD DS, all site links are considered transitive by default. This means that connection objects can be created between domain controllers that are not in adjacent sites. For example, in Figure 4-14, Site1 has a site link to Site2 and to Site4, and Site2 has a site link to Site3 and Site5. Because of the transitive nature of the site links, this means that domain controllers in Site1 can also replicate directly with domain controllers in Site3 and Site5.

The site link costs define the path that replication traffic will take through the network. When KCC is creating the routing topology, it uses the accumulated costs for all site links to calculate the optimal routing. In the example shown in Figure 4-14, there are two possible routes between Site1 and Site5: the first route is through Site2; the second route is through Site4. The cost to route through Site2 is 300 (100 + 200), and the cost through Site4 is 700 (500 + 200). This means that all replication traffic will be replicated through Site2 unless the connection is not available.

When replication traffic crosses multiple site links, the site link schedules and replication intervals for each site link combine to determine the effective replication window and interval. For example, effective replication will occur between Site1 and Site3 only during the hours of 00:00 to 4:00 (the overlapping time in the schedules), and the effective replication will happen every 60 minutes (the replication interval for the Site2–Site3 site link).

Note If the schedules for site links do not overlap, it is still possible for replication to occur between multiple sites. For example, if the Site1–Site2 site link is available from 02:00 to 06:00, and the Site2–Site3 site link is available from 22:00 to 01:00, changes to the directory will still flow from Site1 to Site3. The changes will be sent from Site1 to Site2, and then from Site2 to Site3. However, the replication latency would be almost a day in this case, because changes replicated to Site2 at 02:00 would not be replicated to Site3 until 22:00.

Additional Site Link Configuration Options

In addition to the site link configuration options available in Active Directory Sites And Services, you can also configure other site link settings by using ADSIEdit, or by modifying the registry on the domain controllers. For example, you configure the following settings:

- **Turn off compression for intersite replication** By default, all replication traffic between sites is compressed. However, compressing the traffic places an extra load on the domain controller's processor. If you have sufficient bandwidth between the AD DS sites, you can disable the compression in Windows Server 2008 AD DS.
- **Enable notification for intersite replication** By default, replication between sites is based on the schedule and replication frequency configured on the site link. You have the option to enable notification for intersite replication. If notification is enabled, the bridgehead server in a site where a change has occurred notifies the bridgehead server in the destination site, and the changes are pulled across the site link. This can greatly reduce replication latency between sites, but will also increase the network traffic between sites.

To turn off compression or to turn on notification for intersite replication, you must use a tool such as ADSI Edit to modify the Options attribute on either the site link object or the connection object. To turn off compression, set the value of the Options attribute to *4*; to turn on notification, set the value to *1*.

- **Modify the amount of data that is replicated** You can modify the amount of data that is replicated in each replication packet. By default, the number of objects Windows Server 2008 domain controllers will replicate in a single packet is 1/1,000,000th the size of RAM, with a minimum of 100 objects and a maximum of 1,000 objects. The maximum size of objects that will be replicated is 1/100th the size of RAM, with a minimum of 1 megabyte (MB) and a maximum of 10 MB. You can modify these settings by creating the Replicator inter site packet size (objects) and Replicator inter site packet size (bytes) values in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters path.

Site Link Bridges

In some cases, you might want to turn off the transitive nature of site links by turning off site link bridging and manually configuring site link bridges. When you configure site link bridges, you define which site links should be seen as transitive and which site links should not. Turning off the transitive nature of site links can be useful when you do not have a fully routed network, that is, if all segments of the network are not available at all times (for example, if you have a dial-up or scheduled-demand dial connection to one network location). Site link bridges can also be used to configure replication in situations where a company has several sites connected to a fast backbone with several smaller sites connecting to each larger center using slow network connections. In such cases, site link bridges can be used to manage the flow of replication traffic more efficiently.

More Info Chapter 5 provides details about when and how to use site link bridges.

When you create a site link bridge, you must define which site links are part of the bridge. Any site links you add to the site link bridge are considered transitive with each other, but site links that are not included in the site link bridge are not transitive. In the example used earlier, a site link bridge could be created for the site links connecting Site1, Site2, Site4, and Site5. All of these site links would then be considered transitive, which means that a bridgehead server in Site1 could replicate directly with a bridgehead server in Site5. However, because the site link from Site2 to Site3 is not included in the site link bridge, it is not transitive. That means that all replication traffic from Site3 would flow to Site2, and from there it would flow to the other sites.

To turn off the transitive site links, expand the Inter-Site Transport container in Active Directory Sites And Services, right-click IP, click Properties, and then clear the Bridge All Site Links option on the General tab of the IP Properties sheet.

> **Caution** The site link bridging setting affects all site links using the transport protocol where you disable site link bridging. This means that all site link bridging is disabled, and you will now have to configure site link bridges for all site links if you want transitive site connections.

Replication Transport Protocols

Windows Server 2008 AD DS can use one of three different transport protocols for replication:

- **RPC over IP within a site** All replication connections within a site must use an RPC-over-IP connection. This connection is synchronous, which means that the domain controller can replicate with only one replication partner at any one time. The RPC connection uses dynamic port mapping. The first RPC connection is made on the RPC endpoint mapper port (TCP port 135). This connection is used to determine which port the destination domain controller is using for replication.

> **Note** If you are replicating the directory information through a firewall or are using routers with port filtering enabled, you can specify the port number that the domain controllers will use for replication. To do this, create the following registry key as a DWORD value and specify any valid port number: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS \Parameters\TCP/IP Port.

- **RPC over IP between sites** Replication connections between sites can also use RPC over IP. This RPC connection is the same as the intrasite connection with one important exception: by default, all traffic sent between sites is compressed.

> **Note** When you look at the two types of RPC-over-IP connections in the Active Directory Sites And Services administrative tool, you will notice that they are identified differently in the interface. The RPC over IP within a site is called *RPC*, and the RPC over IP between sites is called *IP*.

- **SMTP between sites** Replication connections between sites can also use SMTP to replicate information between sites. SMTP can be a good choice as a replication protocol if the WAN links between company locations have very high latency. SMTP uses an asynchronous connection, which means that the domain controller can replicate with multiple servers at the same time.

Configuring SMTP Replication

Configuring SMTP replication is significantly more complicated than configuring RPC over IP replication between sites. With RPC-over-IP replication, domain controllers use built-in components and Kerberos authentication to automatically configure and secure replication.

To configure SMTP replication, complete the following steps:

1. Install the SMTP Server feature on the bridgehead servers in both sites. When you install the SMTP Server feature, required components from the Web Server (IIS) server role are also installed.
2. Install Active Directory Certificate Services and configure the Certification Authority (CA) as an Enterprise CA. The CA will be used to issue certificates to the domain controllers that will be used to sign and encrypt the SMTP messages that are exchanged between domain controllers. When you install an Enterprise CA, it automatically issues domain controller certificates to domain controllers in the same domain as the Enterprise CA. These domain controllers can use the certificates to secure SMTP data. For domain controllers in other domains in the forest, you must manually request a Domain Controller certificate or a Directory Email Replication certificate.

> **Note** You can also purchase certificates from public CAs to be used for SMTP replication.

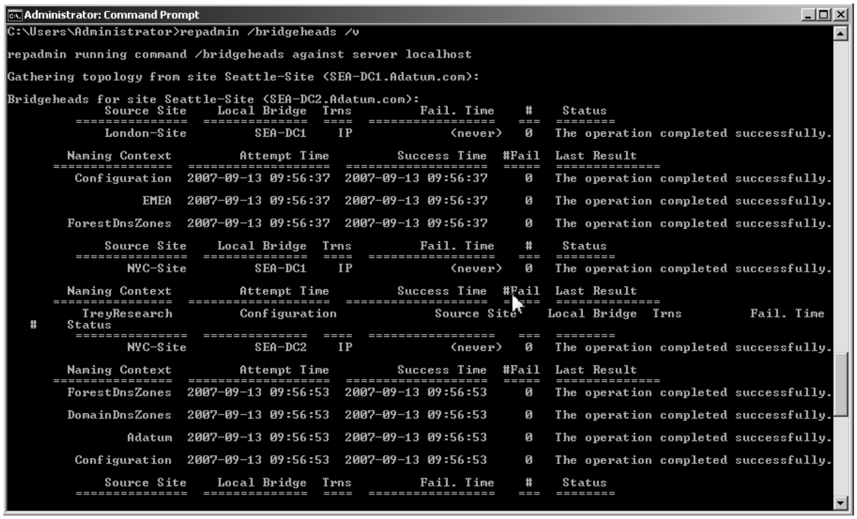
3. Configure SMTP site links with a cost that is less than any RPC over IP site link connecting between the two sites. The two sites must not have any domain controllers in the same domain.
4. Ensure that SMTP e-mail can be sent between the domain controllers. If the domain controllers can communicate directly by using port 25, no further configuration is required. However, in some cases, the domain controllers may need to forward the SMTP messages to a SMTP bridgehead server rather than directly to the destination bridgehead server.

Configuring Bridgehead Servers

As mentioned earlier, replication between sites is accomplished through bridgehead servers. By default, ISTG automatically identifies the bridgehead server as it calculates the intersite replication topology. To view which domain controllers are operating as bridgehead servers, you can use the *Repadmin /bridgeheads* command. The command output lists all of the current bridgehead servers in each site, including the directory partitions each bridgehead server is responsible for. The command output also displays whether or not the last replication with each bridgehead server was successful.

If you run the *Repadmin /bridgeheads /v* command, the command output displays the last attempted replication for each directory partition on the bridgehead server, as well as the last successful replication time. Figure 4-15 shows the partial output from this command.

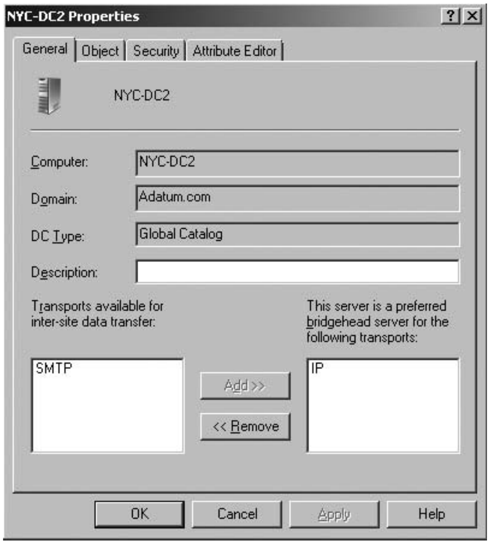
In some cases, you might want to control which domain controllers are going to operate as bridgehead servers. Bridgehead server may require additional server resources if there are many changes to the directory information, replication is set to occur frequently, and the organization has hundreds of sites. To configure which servers will be the bridgehead servers, access the computer objects in the Active Directory Sites And Services administrative tool, right-click the server name, and then select Properties. (Figure 4-16 shows the interface.) You are given the option of configuring the server as a preferred bridgehead server for either IP or SMTP transports.



```
C:\Users\Administrator>repadmin /bridgeheads /v

repadmin running command /bridgeheads against server localhost

Gathering topology from site Seattle-Site (SEA-DC1.Adatum.com):

Bridgeheads for site Seattle-Site (SEA-DC2.Adatum.com):
             Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ===============  ==============  ====  =================   ===  ========
             London-Site         SEA-DC1    IP             (never)   0   The operation completed successfully.

        Naming Context         Attempt Time         Success Time  #Fail  Last Result
      ================  ===================  ===================  =====  ==============
         Configuration  2007-09-13 09:56:37  2007-09-13 09:56:37      0   The operation completed successfully.

                  EMEA  2007-09-13 09:56:37  2007-09-13 09:56:37      0   The operation completed successfully.

        ForestDnsZones  2007-09-13 09:56:37  2007-09-13 09:56:37      0   The operation completed successfully.

             Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ===============  ==============  ====  =================   ===  ========
                NYC-Site         SEA-DC1    IP             (never)   0   The operation completed successfully.

        Naming Context         Attempt Time         Success Time  #Fail  Last Result
      ================  ===================  ===================  =====  ==============
          TreyResearch         Configuration             Source Site    Local Bridge  Trns         Fail. Time
   #    Status
         ===============  ==============  ====  =================   ===  ========
                NYC-Site         SEA-DC2    IP             (never)   0   The operation completed successfully.

        Naming Context         Attempt Time         Success Time  #Fail  Last Result
      ================  ===================  ===================  =====  ==============
        ForestDnsZones  2007-09-13 09:56:53  2007-09-13 09:56:53      0   The operation completed successfully.

        DomainDnsZones  2007-09-13 09:56:53  2007-09-13 09:56:53      0   The operation completed successfully.

                Adatum  2007-09-13 09:56:53  2007-09-13 09:56:53      0   The operation completed successfully.

         Configuration  2007-09-13 09:56:53  2007-09-13 09:56:53      0   The operation completed successfully.

             Source Site    Local Bridge  Trns         Fail. Time    #    Status
         ===============  ==============  ====  =================   ===  ========
```

Figure 4-15 Viewing bridgehead server status using *Repadmin*.

> **On the Disc** If you configure a bridgehead server and then forget that you configured it, you may spend a lot of time troubleshooting AD DS replication if the bridgehead server fails. Ensure that you document preferred bridgehead servers for both types of replication transports in the ADDSSites.xlsx job aid on the CD.



NYC-DC2

Computer: NYC-DC2

Domain: Adatum.com

DC Type: Global Catalog

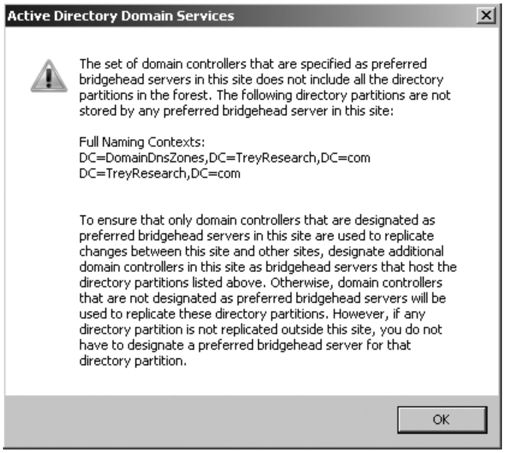
Description:

Transports available for inter-site data transfer: SMTP

This server is a preferred bridgehead server for the following transports: IP

Figure 4-16 Configuring a preferred bridgehead server.

The advantage of configuring preferred bridgehead servers is that you can ensure that the domain controllers you choose will be selected as the bridgehead servers. If you want complete control over which servers are used as bridgehead servers, you must configure a preferred bridgehead server for each partition that needs to be replicated into a site. For example, if a site contains replicas of the ADatum.com domain directory partition, the TreyResearch.com domain directory partition, the global catalog partition, and an application directory partition, you will need to configure at least one domain controller with a replica of each of these partitions. If you do not configure bridgehead servers for all of the partitions, you will get a warning message like the one shown in Figure 4-17, and ISTG will log an event in the event log and then choose a preferred bridgehead server for the partition. You can also configure multiple preferred bridgehead servers. If you do, ISTG will choose one of the identified servers as the bridgehead server.



The set of domain controllers that are specified as preferred bridgehead servers in this site does not include all the directory partitions in the forest. The following directory partitions are not stored by any preferred bridgehead server in this site:

Full Naming Contexts:
DC=DomainDnsZones,DC=TreyResearch,DC=com
DC=TreyResearch,DC=com

To ensure that only domain controllers that are designated as preferred bridgehead servers in this site are used to replicate changes between this site and other sites, designate additional domain controllers in this site as bridgehead servers that host the directory partitions listed above. Otherwise, domain controllers that are not designated as preferred bridgehead servers will be used to replicate these directory partitions. However, if any directory partition is not replicated outside this site, you do not have to designate a preferred bridgehead server for that directory partition.

Figure 4-17 Warning message to configure bridgehead servers for each directory partition.

You should configure this option with caution. Configuring preferred bridgehead servers limits the ability of ISTG to choose the bridgehead server—it will always select a server that is configured as a preferred bridgehead server. If this server fails and no other servers have been designated as bridgehead servers for that directory partition, ISTG will not select another bridgehead server and replication will cease until the server is again available or until you have reconfigured the preferred bridgehead server options. If the preferred bridgehead server does fail, you can either remove the server as a preferred bridgehead server and allow ISTG to identify a bridgehead server or choose another preferred bridgehead server.

Caution If the preferred bridgehead server does fail, and you choose to reconfigure the preferred bridgehead server, you need to make any configuration changes in both sites. Because the bridgehead servers are not available, no information will be replicated between the sites until the configuration changes are made in both sites. To make changes in a remote site, connect to a domain controller in the site in Active Directory Sites And Services.

Troubleshooting Replication

If AD DS replication fails, domain controllers will not be updated with changes made on other domain controllers. This may lead to inconsistent experiences for users and administrators, depending on which domain controller they are connecting to. If password or configuration changes for users are not replicated, users may not be able to log on to the network. If group policy settings or the SYSVOL directory are not replicated, users may experience different group policy settings. Because of the importance of AD DS replication, you should be prepared to troubleshoot AD DS replication issues.

Process for Troubleshooting AD DS Replication Failures

The first step in troubleshooting AD DS replication failures is to identify the reason for the failure. In many cases, it can be difficult to immediately identify why AD DS replication fails, so often troubleshooting is a matter of eliminating possible reasons for failure. As general guidance, complete the following steps:

1. Verify network connectivity. As is the case with most troubleshooting scenarios, start by verifying that the domain controllers can communicate with each other on the network. The network connection might be unavailable or network settings may not be configured properly.
2. Verify name resolution. One of the most common causes for replication errors is that DNS name resolution is failing. If you receive error messages indicating that the RPC server is not available or "Target account name is incorrect" errors, verify that the domain controllers can resolve the target server's FQDN.
3. Test for authentication and authorization errors. If you are receiving access denied errors during replication, then there is a problem with authentication or authorization. To identify the cause of the security error, run the *dcdiag /test:CheckSecurityError /s:DomainControllerName* command, where *DomainControllerName* is the name of the domain controller that you want to test. To test the connection between two domain controllers for replication security errors, run the *dcdiag /test:CheckSecurityError /ReplSource:SourceDomainControllerName* command. This command tests the connection between the domain controller on which you run the command and the source domain controller (identified by *SourceDomainControllerName*). The output from these commands identifies the security issues between the domain controllers. Fix the issues and then rerun the command to verify that you have addressed the issue.
4. Check the Event Viewer on the affected domain controllers. When replication fails, events describing the nature of the failure are written to the Event Viewer.
5. Check for domain controller performance issues. If a domain controller does not have enough server resources, replication may fail, or the replication queues may back up. For example, if the domain controller runs out of hard disk space on the drive where the AD DS data store is located, the domain controller will not accept replication changes.

In some cases, the domain controller performance may be the cause of delayed replication. To address domain controller performance issues, consider the following:

a. Move applications or services to another server. If the domain controller is performing multiple roles or running other applications, consider moving the roles or applications to another server on the network.

b. Distribute AD DS and DNS roles across multiple servers. AD DS integrated DNS zones provide benefits, but running both AD DS services and DNS services on a single computer can cause performance issues. By distributing the load of these services, you may be able to minimize the server performance impact.

c. Deploy domain controllers with 64-bit hardware. Computers with 64-bit hardware provide significant performance gains over domain controllers with 32-bit hardware.

6. Review and modify the replication topology. In large organizations with thousands of sites, calculating the replication topology can consume the processor resources on the domain controller performing the Inter-Site Topology Generator role. Consider decreasing the number of sites in the organization or configuring dedicated bridgehead servers. Also verify that the AD DS site link configuration corresponds with the actual WAN link configuration in your network. AD DS replication should use the WAN connections with maximum available bandwidth whenever possible.

More Info Two excellent resources for troubleshooting specific AD DS replication errors are the Troubleshooting Active Directory Replication Problems Web page (*http://technet2.microsoft.com/windowsserver/en/library/4f504103-1a16-41e1-853a-c68b77bf3f7e1033.mspx?mfr=true*) and the How to Troubleshoot Intra-Site Replication Failures Web page (*http://support.microsoft.com/kb/249256*).

Tools for Troubleshooting AD DS Replication

Windows Server 2008 provides several tools for troubleshooting AD DS replication. All of these tools are installed on Windows Server 2008 when the server is configured as a domain controller.

Active Directory Sites And Services

In addition to using Active Directory Sites And Services to configure sites and replication, you can also use it perform some basic troubleshooting tasks. These tasks include:

- **Forcing the KCC to recalculate the replication topology** To do this, expand the domain controller object in the AD DS site servers container, right-click NTDS Settings, point to All Tasks, and click Check Replication Topology. This forces the KCC to run immediately rather than waiting for the next scheduled update.

- **Forcing a domain controller to pull replication changes** Locate the domain controller to which you want to pull changes in the site servers container. In the NTDS Settings container under the domain controller, right-click the connection object with the domain controller from which you want to pull changes and then click Replicate Now. If both domain controllers are in the same site, you will get an error message or get a message the replication was successful. If the domain controllers are in different sites, you will get a message telling you that the domain controller will attempt immediate replication. Check the Event Viewer for replication errors.
- **Forcing the replication of the configuration partition from or to a domain controller** When you right-click the NTDS object under a domain controller other than the domain controller that is the current focus for Active Directory Sites And Services, you can choose to Replicate configuration from the selected DC or Replicate configuration to the selected DC. One of the benefits of using these commands is that the configuration information will be replicated even if no connection object exists between the domain controllers. This option is useful when a replication partner was removed from the domain while a domain controller was offline and the domain controller cannot locate other domain controllers to create new connection objects.

Repadmin

The most useful tool for monitoring and troubleshooting replication is Repadmin. You can use the Repadmin.exe command-line tool to view the replication topology from the perspective of each domain controller. You can also use Repadmin.exe to manually create the replication topology, force replication events between domain controllers, and view the replication metadata and up-to-date state of vectors.

To run the Repadmin command-line tool, use the following syntax:

```
repadmin command arguments [/u:[domain\]user /pw:{password|*}]
```

You need to provide the user account information only if the current logged-on user is not a member of the Domain Admins group.

The following examples use some of the available command arguments for the Repadmin command-line tool:

- To export the replication information on a domain controller to a .csv file, use this syntax:

  ```
  Repadmin /showrepl DC1.Adatum.com /csv>filename.csv
  ```

  This command is useful because you can open the .csv file by using an application like Microsoft Office Excel and search the file.
- To display the replication partners of the domain controller named DC1, use this syntax:

  ```
  repadmin /showreps DC1.Adatum.com
  ```

- To display the highest USN on the domain controller named DC2, use this syntax:

  ```
  repadmin /showvector dc=Adatum,dc=com DC2.Adatum.com
  ```

- To display the connection objects for the domain controller named DC1, use this syntax:

  ```
  repadmin /showconn DC1.Adatum.com
  ```

- To initiate a replication event between two replication partners, use this syntax:

  ```
  repadmin /replicate DC2.Adatum.com DC1.Adatum.com dc=Adatum,dc=com
  ```

- To initiate a replication event for a specified directory partition with all of its replication partners, use this syntax:

  ```
  repadmin /syncall DC1.Adatum.com dc= Adatum,dc=com
  ```

  Running this command will result in the domain controller requesting updates for all directory partitions from all direct replication partners. If you want to force the domain controller to initiate replication of local changes, add the */p* parameter at the end of the command.

Dcdiag

The Dcdiag.exe tool performs a number of tests that check domain controllers for issues that might affect replication. These tests include connectivity, replication, topology integrity, and intersite health tests.

To run the Dcdiag command-line tool, use the following syntax:

```
dcdiag command arguments [/v /f:LogFile /ferr:ErrLog ]
```

In the command, the optional switch */v* directs the command to produce detailed output, */f* directs the output to the log file, and */ferr* redirects fatal error output to a separate log file. To run all of the dcdiag tests on a local computer and display the results in the command prompt window, just type **DCdiag** and press Enter. To check a remote domain controller, run DCDiag /s:*Servername,* where *Servername* is the remote domain controller name.

Following are a few of the tests that can be run using DCDiag:

- **Connectivity** Tests whether domain controllers are DNS registered, can be pinged, and have LDAP/RPC connectivity.
- **Replications** Checks for timely replication and any replication errors between domain controllers.
- **NetLogons** Checks that the appropriate logon privileges exist to allow replication to proceed.
- **Intersite** Checks for failures that would prevent or temporarily hold up intersite replication and tries to predict how long it will take before the KCC is able to recover. Results of this test are often not valid, especially in atypical site or KCC configurations or at the Windows Server 2008 forest functional level.

- **FSMOCheck** Checks that the domain controller can contact a KDC, a Time Server, a Preferred Time Server, a PDC, and a global catalog server. This test does not test any of the servers for operations master roles.
- **Services** Checks if the appropriate domain controller services are running.
- **Kccevent** Checks that the Knowledge Consistency Checker is completing without errors.
- **Topology** Checks that the KCC has generated a fully connected topology for all domain controllers.

> **Note** For detailed information on how to use the Repadmin and DCDiag command-line tools, type the command name followed by **/?**.

Additional Tools

Two standard server administrative tools are also useful for monitoring and troubleshooting replication. The first tool is the Event Viewer. One of the event logs added to all domain controllers is a Directory Service event log. Most of the directory replication-related events are logged in this event log, and this should be one of the first places you look when replication fails.

The Reliability and Performance Monitor tool is useful for monitoring the amount of replication activity happening on the server. When a server is promoted to be a domain controller, the *DirectoryServices* performance object and several file replication performance objects are added to the list of performance counters. These performance counters can be used to monitor the level of replication traffic as well as a wide variety of other AD DS–related activities.

Summary

One of the key aspects to managing Windows Server 2008 AD DS is understanding how replication works. A stable replication environment is crucial in maintaining an up-to-date copy of all directory information on all the domain controllers in the forest, which is essential to ensure consistent user logon and directory search performance. By understanding how replication works within a site and between sites, you can also design and implement the optimal replication configuration.

Best Practices

- Replication within a single site happens automatically and quickly and rarely fails. If all of your company's domain controllers are connected by fast network connections, you should implement a single site.

- On the other hand, if your company has multiple locations where you install domain controllers, creating additional sites is the easiest and best way to manage AD DS–related traffic across WAN links with limited available bandwidth. Not only do multiple sites limit replication traffic, but they also keep client authentication traffic local.
- Develop a regular practice of monitoring AD DS replication. Consider using a tool such as the Active Directory Management Pack with System Center Operations Manager to monitor replication on all domain controllers in your site. If you do not have a tool like this, regularly monitor the Directory Service event log and either the DFS Replication event log (if your AD DS forest is at the Windows Server 2008 functional level) or the File Replication Service event log.
- In most organizations, the most important cause of AD DS replication errors is DNS lookup errors. By integrating DNS with AD DS and taking advantage of the DNS directory partitions, you can minimize the chances of DNS errors.

Additional Resources

These resources contain additional information related to this topic:

Related Information

- Chapter 14, “Monitoring and Maintaining Active Directory,” provides details on using monitoring tools such as Event Viewer and Reliability and Performance Monitor to monitor AD DS domain controllers, including monitoring replication.
- Chapter 5, “Designing the Active Directory Domain Services Structure,” goes into detail on designing the AD DS site configuration.
- “Troubleshooting Active Directory Replication Problems” is located at *http://technet2.microsoft.com/windowsserver/en/library/4f504103-1a16-41e1-853a-c68b77bf3f7e1033.mspx?mfr=true*. This Web site provides detailed steps for troubleshooting Active Directory replication issues and links to Knowledge Base articles that address specific Event IDs.
- The “How to Troubleshoot Intra-Site Replication Failures” Knowledge Base article at *http://support.microsoft.com/kb/249256* provides details on how to troubleshoot intrasite replication errors. This KB article, as well as many of the other KB articles listed next, refers to Windows Server 2003. Many of the steps in troubleshooting AD DS replication have not changed in Windows Server 2008.
- The “Active Directory Replication Troubleshooter” located at *http://blogs.technet.com/rbeard47/pages/active-directory-replication-troubleshooter.aspx* provides a detailed step-by-step process for troubleshooting Active Directory replication.

- "Fixing Replication DNS Lookup Problems (Event IDs 1925, 2087, 2088)" at *http://technet2.microsoft.com/windowsserver/en/library/43e6f617-fb49-4bb4-8561-53310219f9971033.mspx?mfr=true* provides detailed information on how to troubleshoot replication errors related to DNS.
- "How to Troubleshoot RPC Endpoint Mapper Errors" (*http://support.microsoft.com/kb/839880*) provides detailed information on how to troubleshoot replication errors related to RPC connectivity.
- "Service Overview and Network Port Requirements for the Windows Server System" (*http://support.microsoft.com/kb/832017*) describes the ports required by most Windows Server services, including AD DS replication. This information is very useful when configuring firewalls between domain controllers.
- "Replication Not Working Properly Between Domain Controllers After Deleting One from Sites and Services" (*http://support.microsoft.com/kb/262561*) describes how to use the Repadmin tool to create manual connection objects to domain controllers that have been removed from Active Directory Sites And Services.
- "Active Directory Replication Technologies" at *http://technet2.microsoft.com/windowsserver/en/library/53998db6-a972-495e-a4e7-e3ca3f60b5841033.mspx* provides detailed information on how AD DS replication works.
- The Script Repository: Active Directory Web site, located at *http://www.microsoft.com/technet/scriptcenter/scripts/ad/default.mspx*, has several scripts that can be used to enumerate and modify the AD DS site and site link configuration.

Related Tools

Windows Server 2008 provides several tools that can be used when managing and troubleshooting replication. Table 4-2 lists some of these tools and explains when you would use each of the tools.

Table 4-2 AD DS Replication Tools

Tool Name	Description and Use
Dnslint.exe	This tool is a free download from Microsoft. (See *http://support.microsoft.com/kb/321045* for the download location.) This tool can be used to help diagnose common DNS name resolution issues and to verify that DNS records used specifically for AD DS replication are correct.
Nslookup.exe	This tool is included in all Microsoft Windows server and client operating systems. Nslookup is used to query DNS servers and to obtain detailed responses. The information obtained using Nslookup can be used to diagnose and solve name resolution problems, verify that resource records are added or updated correctly in a zone, and debug other server-related problems.
Active Directory Sites And Services	This tool can be used to configure sites and replication and to perform some basic AD DS replication troubleshooting tasks.

Table 4-2 AD DS Replication Tools *(continued)*

Tool Name	Description and Use
Repadmin.exe	Use this command-line tool to view the replication topology from the perspective of each domain controller. You can also use Repadmin.exe to manually create the replication topology, force replication events between domain controllers, and view the replication metadata and up-to-date state of vectors.
DCDiag.exe	Use this tool to perform tests that check domain controllers for issues that might affect replication.

Resources on the CD

- ADDSSite.xlsx is a spreadsheet template for documenting AD DS site information.
- ListADDSSites.ps1 is a simple Windows PowerShell script for listing information about all of the sites in your forest.

Related Help Topics

- "Checklist: Configure an Additional Site" in Active Directory Sites And Services help.
- "Checklist: Configure the Intersite Replication Schedule" in Active Directory Sites And Services help.
- "Troubleshooting Active Directory Domain Services Replication" in Active Directory Sites And Services help.

Chapter 9

Delegating the Administration of Active Directory Domain Services

In this chapter:

Active Directory Administration Tasks 326
Accessing Active Directory Objects 327
Active Directory Object Permissions. 329
Delegating Administrative Tasks 345
Auditing the Use of Administrative Permissions. 348
Tools for Delegated Administration 352
Planning for the Delegation of Administration 354
Summary 355
Additional Resources. 356

Active Directory Domain Services (AD DS) is typically deployed as a common directory service shared between various business divisions within an organization. Using a common directory service helps reduce the costs associated with maintaining the infrastructure, but introduces a number of other considerations:

- How to manage users and resources independently between divisions when decentralized administration is required
- Ensuring that administrators or users can only perform permitted tasks within their own business division
- Ensuring that specific objects or information stored within the directory is only available to administrators with the appropriate permissions

These considerations can be addressed by a thorough understanding of how to delegate administrative tasks. Delegation involves a higher-level administrator granting permissions to other users to perform specific administrative tasks within the Active Directory structure. The Active Directory structure provides a hierarchical view of the directory service: first at the site and domain level, and then at the organizational unit (OU) level within a domain. This hierarchy provides powerful options for managing permissions and delegating administrative tasks at various levels throughout the logical infrastructure.

This chapter describes administrative delegation, starting with a discussion of the various types of tasks that might be delegated within an enterprise. Then it describes object access, the types of permissions that can be assigned to objects residing within the directory, and how to use these permissions for delegation of administration. Finally, the chapter provides information about auditing changes to objects residing within AD DS.

Active Directory Administration Tasks

Active Directory administration tasks typically fall into one of two categories–data management or service management. Data management tasks relate to the management of content that is stored within the Active Directory database. Service management tasks relate to the management of all aspects that are required to ensure a reliable and efficient delivery of the directory service throughout the enterprise.

Table 9-1 describes some of the tasks that are related to each of these categories.

Table 9-1 Active Directory Administration

Category	Tasks
Data management	■ **Account management**—includes creating, maintaining, and removing user accounts ■ **Security group management**—includes creating security groups, provisioning security groups to grant access to network resources, managing memberships of security groups, and removing security groups ■ **Resource management**—includes all aspects of managing network resources such as end-user workstations, servers, and resources hosted on servers such as file shares or applications ■ **Group Policy management**—includes all aspects of creating, assigning, and removing Group Policy objects within the Active Directory structure ■ **Application-specific data management**—includes all aspects of managing Active Directory-integrated or enabled applications such as Microsoft Exchange Server
Service management	■ **Installation and trust management**—includes aspects such as the creation and deletion of domains, the deployment of domain controllers, and the configuration of appropriate Active Directory functional levels ■ **Domain controller and directory database management**—includes aspects related to the management of domain controller hardware, database maintenance, and the application of service packs and security updates ■ **Schema management**—includes the extension or modification of the schema to support the deployment of Active Directory-enabled applications

Table 9-1 Active Directory Administration *(continued)*

Category	Tasks
	■ **Operations master roles management**—includes tasks that ensure the proper assignment and configuration of operations master roles ■ **Backup and restore management**—includes all tasks related to performing regular backups of the directory database and restore procedures when required ■ **Replication management**—includes all tasks related to the creation, maintenance, and monitoring of the replication topology ■ **Security policy management**—includes all tasks related to the management of the default domain controller security policy and managing the password, account lockout, and Kerberos account policies

More Info For more information about the tasks related to data management and service management, refer to “Best Practices for Delegating Active Directory Administration” found at *http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/actdid1.mspx*.

Delegating data and service management tasks within an organization requires an understanding of the administrative needs of all business units. This understanding ensures the most effective delegation model used to provide a more effective, efficient, and secure networking environment. To deploy the delegation model, you need to understand Active Directory object permissions, delegation methods, and auditing. These concepts are discussed in the next few sections.

Accessing Active Directory Objects

To effectively delegate administrative tasks, you need to know how Active Directory controls access to objects stored within the directory service. Access control involves the following:

- Credentials of the security principle attempting to perform the task or access the resource
- Authorization data used to protect the resource or authorize the task being performed
- An access check that compares the credentials against the authorization data to determine if the security principle is permitted to access the resource or perform the task

When a user logs on to an AD DS domain, authentication takes place and the user receives an access token. An access token includes the security identifier (SID) for the user account, SIDs for each security group of which the user is a member, and a list of privileges held by the user and the user’s security groups. The access token helps to provide the security context and credentials needed to manage network resources, perform administrative tasks, or access objects residing in Active Directory.

Security is applied to a network resource or an Active Directory object by authorization data that is stored in the *Security Descriptor* of each object. The Security Descriptor consists of the following components:

- **Object owner** The SID for the current owner of the object. The owner is typically the creator of the object or a security principal that has taken over ownership of an object.
- **Primary group** The SID for current owner's primary group. This information is only used by the Portable Operating System Interface for UNIX (POSIX) subsystem.
- **Discretionary access control list (DACL)** A list of access control entries (ACEs) that define the permissions each security principle has to an object. Each security principal that is added to the access control list obtains a set of permissions that specify the extent to which that user or group can manipulate the object. If a user does not appear in an ACE, either individually or as a member of a group, that user has no access to the object.
- **System access control list (SACL)** Defines the audit setting on an object including which security principle is to be audited and the operations that are to be audited.

Figure 9-1 illustrates the architecture of a user's access token and an object's security descriptor. When a user tries to access a network resource or an Active Directory object, an access check is performed and each ACE is examined until a User or Group SID match is found. Access is then determined by the permissions configured on the ACE.

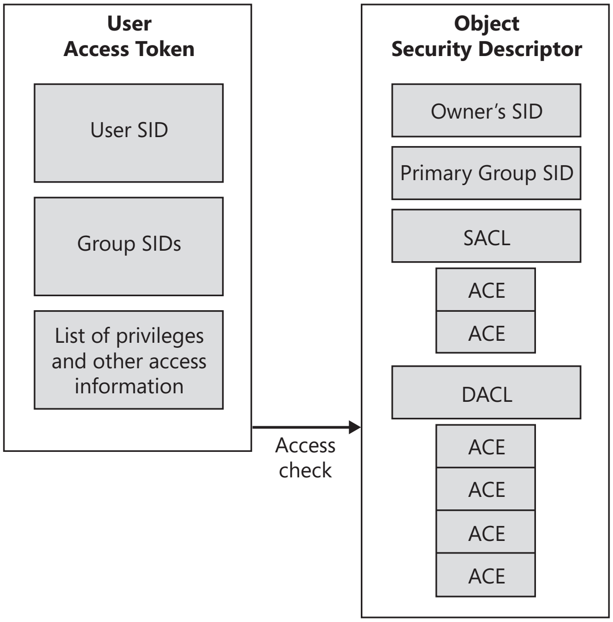


Figure 9-1 Access check between a user's access token and an object's security descriptor.

Evaluating Deny and Allow ACEs in a DACL

ACEs are listed within a DACL in a specific order, which has a direct affect on the outcome of the access check. During an access check, ACEs are evaluated in sequence. The evaluation sequence is listed as follows:

- ACEs that have been explicitly assigned are evaluated before inherited ACEs.
- For each set of explicit or inherited ACEs, Deny ACEs are always evaluated before Allow ACEs.

Figure 9-2 illustrates how Allow and Deny permissions are evaluated for both explicit and inherited ACEs.

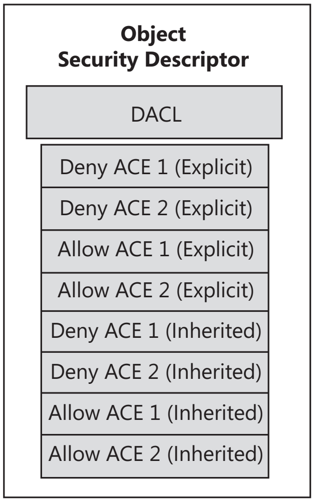

Object
Security Descriptor
DACL
Deny ACE 1 (Explicit)
Deny ACE 2 (Explicit)
Allow ACE 1 (Explicit)
Allow ACE 2 (Explicit)
Deny ACE 1 (Inherited)
Deny ACE 2 (Inherited)
Allow ACE 1 (Inherited)
Allow ACE 2 (Inherited)

Figure 9-2 Evaluating Allow and Deny ACEs.

Active Directory Object Permissions

Every object in Active Directory has an access control list (ACL), which means that you can modify the permissions on that object. This includes objects visible through the Active Directory Users And Computers administrative console as well as objects visible through the Active Directory Sites and Services administrative console, ADSI Edit, or Ldp.exe. The most common tool used to modify Active Directory object access is Active Directory Users And Computers. However, each of the previously mentioned tools can be used to perform the common task of managing object access within the directory service.

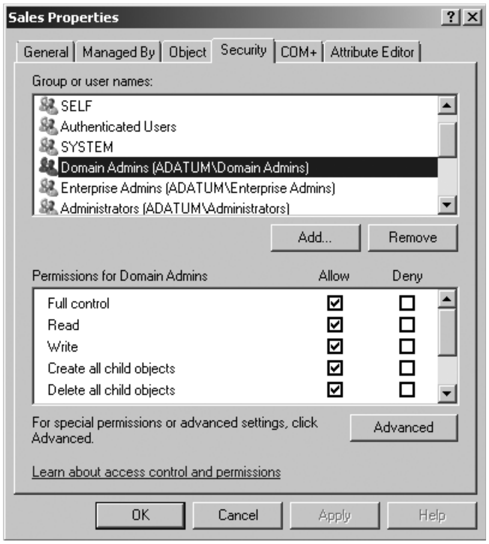
Access control permissions on an Active Directory object are separated into two categories: *standard permissions* and *special permissions*. Special permissions are granular options that can be applied to an object. A standard permission is made up of a group of special permissions to allow or deny a specific function. For example, the Read standard permission is made up of the Read permissions, List contents, and Read all properties special permission entries.

Standard Permissions

To view the standard permissions for any Active Directory object in the domain directory partition, access the Security page for that object's Properties sheet in the Active Directory Users And Computers administrative console.

> **Note** If the Security page is not visible, select Advanced Features on the View menu and then reselect the object and open its Properties sheet.

The Security page displays the group or user names that are assigned permissions to the object. As you select a group or user entry, the associated allow or deny permissions for that entry are shown. Figure 9-3 illustrates the permissions for the Domain Admins group on the Sales organizational unit. Notice that, by default, the Allow box is checked for each permission to provide the Domain Admins group full control over the Sales OU.



Group or user names:

- SELF
- Authenticated Users
- SYSTEM
- Domain Admins (ADATUM\Domain Admins)
- Enterprise Admins (ADATUM\Enterprise Admins)
- Administrators (ADATUM\Administrators)

Permissions for Domain Admins	Allow	Deny
Full control	☑	☐
Read	☑	☐
Write	☑	☐
Create all child objects	☑	☐
Delete all child objects	☑	☐

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

Figure 9-3 Viewing the Security page on an Organizational Unit object.

Depending on the type of object being secured, you will notice that different permissions may be visible on the security page. For example, the following standard permissions are common with all objects:

- Full control
- Read
- Write
- Create all child objects
- Delete all child objects

Some Active Directory objects also have standard permissions that are applied to grouped sets of properties. For example, a user object has several read-and-write property sets such as General Information, Personal Information, Phone And Mail Options, and Web Information. Each of these property sets refers to a set of object attributes, so granting access to a single property set provides access to a set of attributes. For example, the Personal Information property set includes attributes such as *homePhone*, *homePostalAddress*, and *streetAddress*. Using the property sets to assign access to groups of attributes simplifies the process of assigning permissions without having to modify at the granular attribute level.

Note The Active Directory schema defines which attributes are part of each property set by using the *rightsGuid* value for the property category (in the Configuration directory partition) and the *attributeSecurityGUID* for the *schema* object. For example, the *rightsGuid* value for cn=Personal-Information, cn=Extended-Rights, cn=configuration, dc=*forestname* is equivalent to the *attributeSecurityGUID* for cn=Telephone-Number, cn=Schema, cn=Configuration, dc=*forestname*. This means that the telephone number is included in the Personal Information property set.

In addition to the standard permissions, the Security page may also show extended rights related to the object being secured. Depending on the object, these rights include options such as Allowed To Authenticate, Generate Resultant Set Of Policy, Receive As, Send As, Send To, Change Password, and Reset Password.

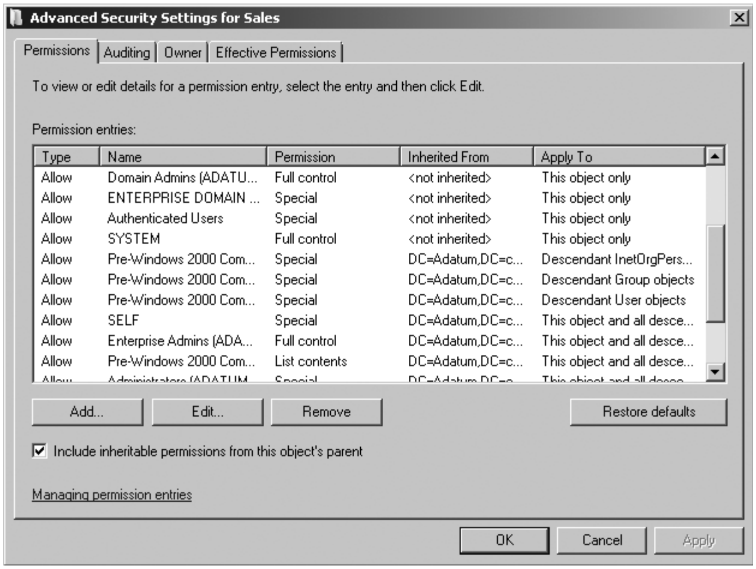
Special Permissions

One of the entries in the permissions list on the Security page is Special Permissions. In addition to being able to grant standard permissions, you can also grant special permissions to Active Directory objects.

Note You can determine if special permissions are applied to an object by viewing the Allow or Deny check boxes located next to the Special Permissions entry. If a check mark is visible, special permissions have been assigned.

As mentioned previously, special permissions are much more granular and specific than standard permissions. To simplify management, you would typically use standard permissions on an object; however, there may be specific needs that require you to modify the special permission entries.

To get access to special permissions, click Advanced on the Security page and then ensure that the Permissions page is selected. Figure 9-4 shows the interface. Table 9-2 explains the options available on the Permissions page.



To view or edit details for a permission entry, select the entry and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Domain Admins (ADATU...	Full control	<not inherited>	This object only
Allow	ENTERPRISE DOMAIN ...	Special	<not inherited>	This object only
Allow	Authenticated Users	Special	<not inherited>	This object only
Allow	SYSTEM	Full control	<not inherited>	This object only
Allow	Pre-Windows 2000 Com...	Special	DC=Adatum,DC=c...	Descendant InetOrgPers...
Allow	Pre-Windows 2000 Com...	Special	DC=Adatum,DC=c...	Descendant Group objects
Allow	Pre-Windows 2000 Com...	Special	DC=Adatum,DC=c...	Descendant User objects
Allow	SELF	Special	DC=Adatum,DC=c...	This object and all desce...
Allow	Enterprise Admins (ADA...	Full control	DC=Adatum,DC=c...	This object and all desce...
Allow	Pre-Windows 2000 Com...	List contents	DC=Adatum,DC=c...	This object and all desce...
Allow	Administrators (ADATUM	Special	DC=Adatum,DC=c	This object and all desce

☑ Include inheritable permissions from this object's parent

Figure 9-4 Viewing the Advanced Security Settings for an object.

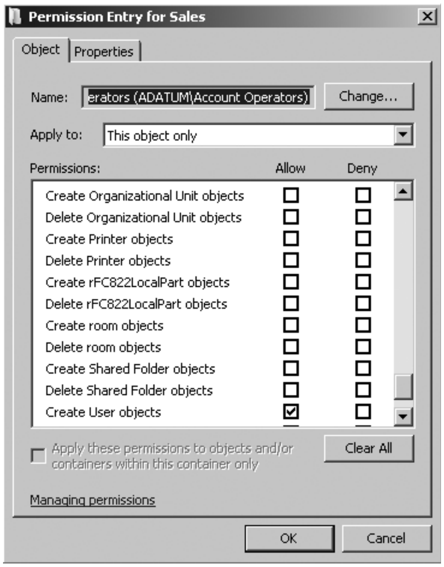
Table 9-2 Special Permissions Configuration

Option	Explanation
Type	This value is set to either *Allow* or *Deny*. Normally, the interface sorts the permissions so that all Deny permissions are listed first, but the sort order can be changed by clicking any column header. Regardless of the order of appearance in this column, the Deny permissions are always evaluated first.
Name	This is the name of the security principal to which each ACE applies.
Permission	This column lists the level of permission granted for the security principal. Levels of permission can be standard rights, such as Full Control; special permissions such as Create/Delete User Objects; or just Special. The types of permissions available depend on the type of object and how granular the permission entry is.
Inherited From	This column lists the location where this permission is set and if the permission is inherited from a parent container.
Apply To	This column specifies the depth to which this permission applies. It has a variety of settings, including This Object Only, This Object And All Descendant Objects, All Descendant Objects, as well as many others.
Include Inheritable Permissions From This Object's Parent	This option allows you to specify if parent permission entries are to be applied to the object.
Add/Edit/Remove buttons	These buttons allow you to add new ACEs, remove existing ACEs, or edit a specific ACE to provide more granular permission settings.

Note The Restore Defaults button on the Permissions page resets the permissions on the object to the default permission settings as indicated in the Default Security settings of the object class in the Active Directory Schema.

In many cases, the same security principals may be listed in multiple ACEs. For example, the Account Operators group has multiple Create/Delete entries for Computer objects, Group objects, User objects, Printer objects, and InetOrgPerson objects in separate ACEs. This happens whenever you specify a combination of permissions that cannot be stored within a single ACE. In this example, each ACE can only contain focus on one type of object (Computer, User, etc.), and cannot be combined into a single ACE.

If you add or edit the permissions granted to a security principal, you are provided two different options for applying permissions. Figure 9-5 shows the first option, which is applying permissions to the object.



Name: erators (ADATUM\Account Operators)

Apply to: This object only

Permissions:

Permissions	Allow	Deny
Create Organizational Unit objects	☐	☐
Delete Organizational Unit objects	☐	☐
Create Printer objects	☐	☐
Delete Printer objects	☐	☐
Create rFC822LocalPart objects	☐	☐
Delete rFC822LocalPart objects	☐	☐
Create room objects	☐	☐
Delete room objects	☐	☐
Create Shared Folder objects	☐	☐
Delete Shared Folder objects	☐	☐
Create User objects	☑	☐

☐ Apply these permissions to objects and/or containers within this container only

Figure 9-5 Assigning special permissions to Active Directory objects.

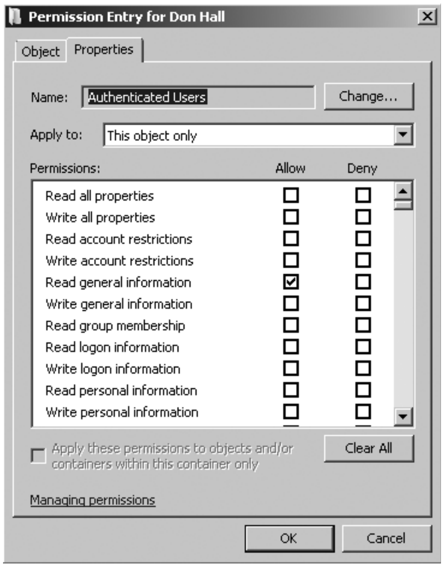
The Object tab is used to apply permissions to various object scopes:

- **This object only** Permissions only apply to the object being secured or modified.
- **This object and all descendant objects** Permissions will apply to both the object being secured and all child objects within the object.
- **All descendant objects** Permissions will only apply to child objects within the object being modified.

- **Individual descendant objects** Windows Server 2008 provides a large selection of individual descendant objects that can be granularly secured. For example, if you are assigning permissions at the OU level, you may choose to only apply permissions to computer objects within the Sales OU. These options provide the capability to delegate permissions at a granular object level.

The second option for applying permissions is to control access to the object properties. Figure 9-6 shows the interface.

The Properties page is used to apply permissions for the security principal listed in the Name field to the individual properties for the object. For example, if you are applying permissions to a user object, you are given the option of assigning Read and Write permissions to each attribute available on the object class, such as *general information, group membership,* and *personal information.*



Name: Authenticated Users

Apply to: This object only

Permissions:	Allow	Deny
Read all properties	☐	☐
Write all properties	☐	☐
Read account restrictions	☐	☐
Write account restrictions	☐	☐
Read general information	☑	☐
Write general information	☐	☐
Read group membership	☐	☐
Read logon information	☐	☐
Write logon information	☐	☐
Read personal information	☐	☐
Write personal information	☐	☐

☐ Apply these permissions to objects and/or containers within this container only

Figure 9-6 Configuring an object's property permissions.

How It Works: Viewing the ACE Using Ldp.exe

Ldp.exe is a graphical user interface (GUI) tool that is used to perform operations such as connect, bind, search, modify, add, or delete against any LDAP-compatible directory service. LDP can be used to view advanced Active Directory metadata such as security descriptors and replication metadata.

To view the ACL using Ldp.exe:

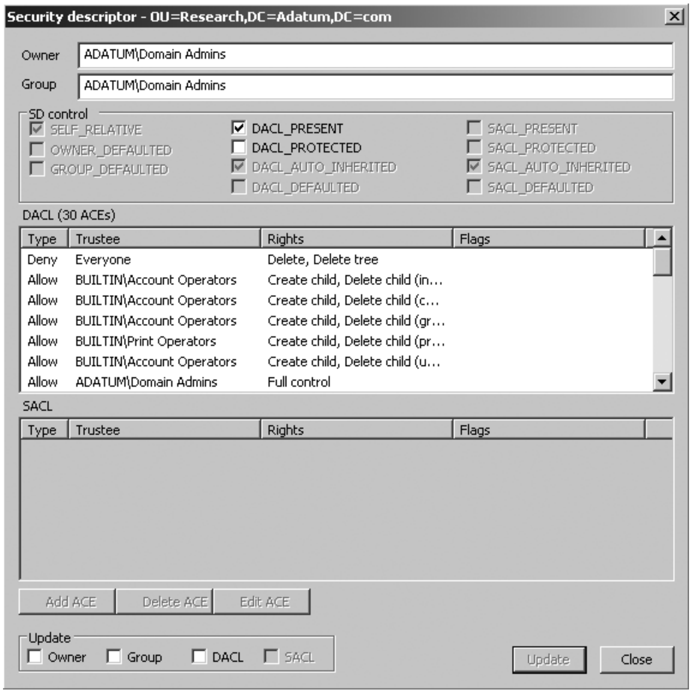
1. Open the Run dialog box, type **ldp**, and then press **Enter**.
2. Click the Connection menu and then click Connect.

If you leave the server box empty, the server will connect to the local computer. You can also type in the server name.

3. After you are connected to the server, click the Connection menu and then click Bind. If you are not logged in with a user account that has administrative rights, type in alternate credentials. Otherwise, leave the logon information blank.
4. After binding to the domain, click the View menu and then click Tree.
5. To view the entire domain, click OK. The domain OU structure will be listed in the left pane.

To view the ACL for any object, locate the object in the tree view in the left pane. Right-click the object, point to Advanced, click Security Descriptor, and finally, click OK.

As shown in Figure 9-7, a number of advanced options are available such as modifying DACL and SACL rights and modifying the security descriptor controls such as DACL and SACL protection.



Security descriptor - OU=Research,DC=Adatum,DC=com

Owner: ADATUM\Domain Admins

Group: ADATUM\Domain Admins

SD control

☑ SELF_RELATIVE
☐ OWNER_DEFAULTED
☐ GROUP_DEFAULTED
☑ DACL_PRESENT
☐ DACL_PROTECTED
☑ DACL_AUTO_INHERITED
☐ DACL_DEFAULTED
☐ SACL_PRESENT
☐ SACL_PROTECTED
☑ SACL_AUTO_INHERITED
☐ SACL_DEFAULTED

DACL (30 ACEs)

Type	Trustee	Rights	Flags
Deny	Everyone	Delete, Delete tree	
Allow	BUILTIN\Account Operators	Create child, Delete child (in...	
Allow	BUILTIN\Account Operators	Create child, Delete child (c...	
Allow	BUILTIN\Account Operators	Create child, Delete child (gr...	
Allow	BUILTIN\Print Operators	Create child, Delete child (pr...	
Allow	BUILTIN\Account Operators	Create child, Delete child (u...	
Allow	ADATUM\Domain Admins	Full control	

SACL

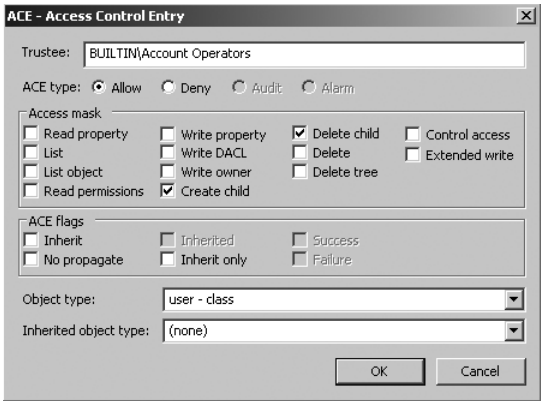
Type	Trustee	Rights	Flags

Update

☐ Owner ☐ Group ☐ DACL ☐ SACL

Figure 9-7 Using Ldp.exe to modify the security descriptor.

When you add or edit an ACE using Ldp.exe, you are able to modify specific permissions and ACE flags on various object types and specify object inheritance. Figure 9-8 shows an illustration of the ACE editor provided with Ldp.exe.



ACE - Access Control Entry

Trustee: BUILTIN\Account Operators

ACE type: ● Allow ○ Deny ○ Audit ○ Alarm

Access mask
☐ Read property ☐ Write property ☑ Delete child ☐ Control access
☐ List ☐ Write DACL ☐ Delete ☐ Extended write
☐ List object ☐ Write owner ☐ Delete tree
☐ Read permissions ☑ Create child

ACE flags
☐ Inherit ☐ Inherited ☐ Success
☐ No propagate ☐ Inherit only ☐ Failure

Object type: user - class

Inherited object type: (none)

Figure 9-8 Modifying an ACE using Ldp.exe.

Permissions Inheritance

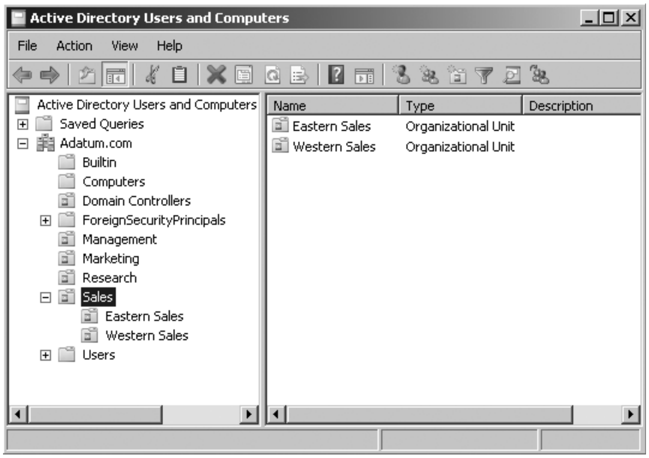
AD DS uses a static permissions inheritance model. That is, when permissions are changed on a container object in the Active Directory structure, the changes are calculated and applied to the security descriptor for all objects in that container. Consequently, if permissions are changed higher in the Active Directory structure and these permissions are applied to all descendant objects, calculating the new ACL for each object can be a processor-intensive process. However, this initial effort means that the permissions do not need to be recalculated when a user or process tries to access the object.

There are two primary methods that are used to control inheritance of permissions:

- **Configuring inheritable permissions on the object** By default, when an object is created in Active Directory, inheritable permissions are included from the object's parent. You can determine if a permission entry is inherited by looking to see whether the check box on the Security page is shaded or not, or by viewing the Inherited From column of the Advanced Security Settings box.
- **Configuring the scope of how permissions are applied** As described previously, another way to control inheritance is to specify how permissions apply to descendant objects when security is applied to an object. By default, when a new group or user name is manually added to the ACE, the entry has permissions that apply to *this object only*. To force inheritance to a child object, you need to modify the scope to apply to descendant objects in addition to the current object.

Note If you use the Delegation Of Control Wizard, inheritance will automatically be set to This Object And All Descendant Objects. More information about the Delegation Of Control Wizard is provided in the "Delegating Administrative Tasks" section later in this chapter.

If you have designed your OU structure with the goal of delegated administration, you will have created an OU structure in which top-level administrators that require permissions to all Active Directory objects are granted permissions high in the hierarchy with delegated permissions to all descendant objects. As you move further down the hierarchy, you may be delegating permissions to other administrators who should only have control over a smaller part of the domain. For example, Figure 9-9 shows the Sales OU. Within the Sales OU are two child OUs called Eastern Sales and Western Sales. The manager who is in charge of the entire Sales division may be delegated permissions to the entire Sales OU object and all descendant objects, whereas the Eastern Sales or Western Sales managers may be delegated permissions to their own specific OU only.

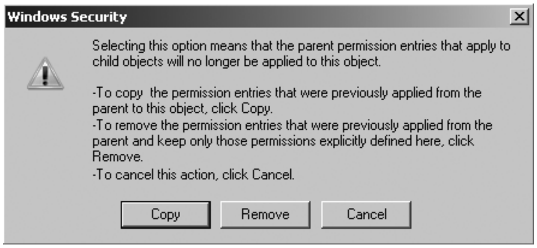

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Computers
Saved Queries
Adatum.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Management
Marketing
Research
Sales
Eastern Sales
Western Sales
Users

Name	Type	Description
Eastern Sales	Organizational Unit	
Western Sales	Organizational Unit	

Figure 9-9 Delegating management of the Sales OU.

In some cases, however, you may want to block higher-level administrators from having any administrative permissions to a specific child OU. For example, if you create a child OU for a branch office in your company, you may assign a local administrative group full control of the OU. However, you may not want those local administrators to have access to any executive user accounts in the OU. To limit their access, you can create an Executives OU within the branch office OU and then remove the option to include inheritable permissions from the object's parent. This, in effect, blocks permissions inheritance at the Executives OU level.

To block the inheritance of permissions on an Active Directory object, access the Advanced Security Settings dialog box for the object (shown in Figure 9-4). Then clear the Include Inheritable Permissions From This Object's Parent option. When you clear this option, you are presented with the choice to copy the existing permissions or remove all permissions before explicitly assigning new permissions, as shown in Figure 9-10.



Selecting this option means that the parent permission entries that apply to child objects will no longer be applied to this object.

-To copy the permission entries that were previously applied from the parent to this object, click Copy.
-To remove the permission entries that were previously applied from the parent and keep only those permissions explicitly defined here, click Remove.
-To cancel this action, click Cancel.

Figure 9-10 Selecting the option to copy or remove permissions when blocking permissions inheritance.

Blocking inheritance has the following implications:

- The permissions are blocked for the object and any descendant objects. This means that you cannot block the permissions inheritance at a container level and then reapply the inheritance from a higher container at a lower level.
- Even if you decide to copy the permissions before modification, permissions inheritance begins where you block the permissions. If you modify the permissions at a higher level, the permissions will not be inherited past the blocked permissions.
- You cannot be selective about which permissions are blocked. When you block permissions, all inherited permissions are blocked. Permissions that have been explicitly assigned to the object or child objects are not blocked.

Note One of the possible concerns with blocking inherited permissions is that you might create an orphaned object where no one has any permissions. For example, you can create an OU, block all permissions inheritance to that OU, and assign the permissions to only one administrative group. You can even remove the Domain Admins group from the ACL of the OU so that the Domain Admins does not have any permissions under normal circumstances. If that administrative group gets deleted, the OU would have no group with administrative control. In this case, the Domain Admins group would have to take ownership of the object and reassign permissions.

Direct from the Source: Delegating Control of an OU Model

There are many schools of thought on how one should design an OU model and perform delegation within the model. The most common OU model starting points are based on business function, geography, or a hybrid of the two. A delegation model can be centralized, decentralized, or centralized with decentralized execution, but ultimately its design is a result of how a customer wants to provide operational support.

Anyone considering delegation is at one of two points in the Active Directory life cycle—either he or she is considering migrating to Active Directory, or else he or she has migrated to Active Directory and has the opportunity to revisit earlier decisions to provide a more effective and efficient environment.

For those considering migrating to Active Directory, the lesson learned is to engage early and often in discussions with the customers. Understanding how customers run their business is critical in developing an infrastructure that will work for them. If you are an employee of a company and have been tasked with migrating the environment to Active Directory, the same advice stands—talk early and often to upper management to gain a better understanding of how they want to run the business. When deciding on how to architect the solution, keep in mind that Active Directory can provide infinite granularity (depth) as well as infinite scope (breadth) because of the flexible nature of the product. One could conceivably define groups for every imaginable role (depth) and groups to cover every scope (breadth), resulting in an environment that would be difficult to manage and maintain. There is balance point between depth and breadth, and that point may be different for every customer. Factors such as number of sites and support personnel are critical in designing an effective delegation model. This is why it is critical, as an architect, to have thorough planning and design sessions with the customer or upper management from the beginning of the design process, so that there is a clear understanding of how operational support will be provided.

For those who already have an established Active Directory environment and have the ability to revisit the existing delegation model, I would recommend looking at the way you are currently maintaining operational support. You may be able to streamline your operations by scaling back the depth and breadth of your current model. It has been my experience that sometimes less is more when dealing with operational support.

Finally, communication is critical to be truly effective and meet customer or upper management expectations. I have been involved in many customer discussions in which IT professionals are discussing a topic such as delegation within Active Directory with the customer or upper management, and the terminology used has caused frustration for both sides. Before engaging in technical discussions, you should consider the following topics:

- **Who is my audience?** Your audience may differ depending on whether it is a meeting or if you are writing a white paper or proposal.
- **How do I make my audience more knowledgeable?** Take a few minutes to go through your delivery strategy. Are there words, phrases, or topics that may have a different meaning or connotation, depending on your audience?
- **Consider developing two or three different strategies for discussion.** Using analogies is a great method for removing the technical nature from a discussion and placing the subject in a context that most non-IT professionals can understand.

Barry Hartman

Senior Consultant

Microsoft Consulting Services

Effective Permissions

As discussed so far in this chapter, a user can obtain permissions to a specific object in Active Directory in several ways:

- The user account may be granted explicit permissions to an object.
- One or more groups that the user belongs to may be granted explicit permissions to an object.
- The user account or one or more groups that the user belongs to may be given permissions at a container-object level and permissions inherited by lower-level objects.

All of these permissions are cumulative; that is, the user is granted the highest level of permissions from any of these configurations. For example, if a user is explicitly given Read permission to an object, the user belongs to a group that is explicitly given Modify permissions, and the user belongs to a group that is given Full Control at the container level, the user will have Full Control. When a user attempts to access an object, the security subsystem examines all of the ACEs that are attached to the object. All of the ACEs that apply to the security principal (based on user account or group SIDs) are evaluated and the highest level of permission is set. However, in addition to ACEs that grant permissions, Active Directory also supports Deny permissions. Deny permissions can be applied at two levels:

- The user object or one or more of the groups that the user belongs to may be explicitly denied permission to an object.
- The user object or one or more groups that the user belongs to may be denied permissions at a container level, and this denial of permission may be inherited to lower-level objects.

Deny permissions almost always override Allow permissions. For example, if a user is a member of a group that is given Modify permissions to an Active Directory object, and the user is explicitly denied Modify permissions to the object, the user will not be able to modify the object. This is because the ACEs that deny permissions are evaluated before the ACEs that allow permissions. If one of the ACEs denies permission to the security principal, no other ACEs are evaluated for the object.

The one situation in which Allow permissions do override Deny permissions is when the Deny permissions are inherited and the Allow permissions are explicitly assigned. For example, you can deny a user the permission to modify any user accounts in a container. But, if you explicitly allow Modify permissions to an object within the container, the user account will have Modify permissions on that object.

Deny Permissions: Use Carefully

Using the Deny option to deny permissions can make your Active Directory security design very difficult to manage. There are a number of different scenarios in which you may think about using the Deny permission. One is a situation in which you may want to use the Deny option to remove some permissions that are being inherited. For example, you may grant Modify permissions at a container level but may want to change that to Read-Only farther down the hierarchy. In this case, you could deny the Write permission on any objects or properties farther down the hierarchy.

Another scenario in which you may think of using the Deny option is when you want to create a container that requires higher security. For example, you may have a container for all of the executives, and you may want to make sure that a normal user cannot read the executive account properties. You may choose to deny Read permissions on the container using the Domain Users group. Unfortunately, this denies everyone the right to read the directory objects, including all administrators. Because of the complications that can result from using the Deny option, you should use it with care.

In most cases, rather than denying permissions, you can just ensure that a user or group has not been given permissions. If a user has not been granted any permissions and is not a member of any group that has been granted permissions, the user will not have any access and will be implicitly denied. You do not need to explicitly apply the Deny permission to prevent users from accessing objects in Active Directory.

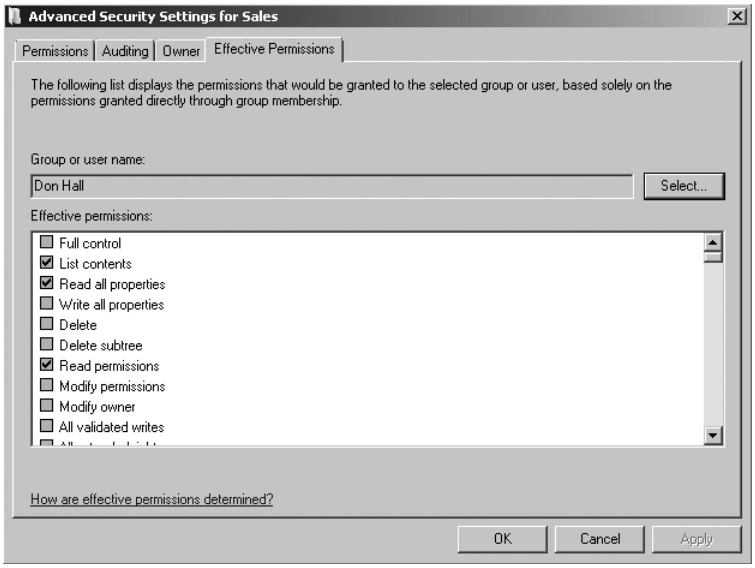
One of the few scenarios in which it can be beneficial to use the Deny option is if you have a case where a group should be given permissions, but one or more users in the same group should have a lower level of permissions. For example, you may have a group called Account Admins that is responsible for managing all user accounts in the domain. Some members of this group may be temporary employees who need to be able to manage all user accounts in the domain, but who should not be able to modify any properties on executive accounts. In this case, you could assign the Account Admins group permission to manage all user accounts in the domain. Next, create an OU for the executive accounts, and create a group for the temporary members of the Account Admins group. Then, deny the temporary users the right to modify any user accounts in the Executive OU.

As you can see, configuring security on Active Directory objects can involve managing a large number of interrelated variables. Many companies may start out with a fairly simple security design in which a small group of administrators are given all the permissions in Active Directory. Most of the time, the initial Active Directory security configuration is clearly documented. However, as time goes by, this simple initial configuration often becomes much messier. Sometimes another group of administrators is given a set of permissions for a specific task and for a specific period of time. Granting the permissions is easy to do, but often the permissions are never removed. Often these security modifications made after the initial deployment are also not clearly documented.

For any Active Directory structure that has been deployed for some time, the current security configuration is likely more complex than was initially designed. Sometimes this results in users having more permissions than they should have. Fortunately, Windows Server 2008 provides a tool that can be used to easily determine the effective permissions a security principal has to any object in Active Directory.

To determine the effective permissions that a security principal has on an Active Directory object, access that object's properties through the appropriate Active Directory administrative tool. Click the Security page, click Advanced, and then click the Effective Permissions page. To determine the effective permissions for a specific user or group account, click Select and then search for the user or group name. After you have selected the name, click OK. The Effective Permissions page displays all of the permissions the security principal has to the Active Directory object. Figure 9-11 shows the interface for the Active Directory Users And Computers administrative tool. Notice that the Effective Permissions page for the Sales OU displays the overall permissions assigned to the *Don Hall* user object.

Note This tool has some limitations that may affect the effective permissions displayed. The tool determines the effective permissions based on inherited and explicitly defined permissions for the user account and the user's group memberships. However, the user may also get some permissions based on how the user logs on and connects to the object. For example, in Windows Server 2008, you can assign permissions to the interactive group (that is, anyone logged on to the computer) or the network login group (that is, anyone accessing the information across the network). This Active Directory administrative tool cannot determine the permissions granted to a user based on these types of groups. Also, the tool can only determine permissions by using the permissions of the person running the tool. For example, if the user running the tool does not have permission to read the membership of some of the groups that the evaluated user object belongs to, the tool will not be able to determine the permissions accurately.


Advanced Security Settings for Sales
Permissions
Auditing
Owner
Effective Permissions
Select...
How are effective permissions determined?
OK
Cancel
Apply

The following list displays the permissions that would be granted to the selected group or user, based solely on the permissions granted directly through group membership.

Group or user name: Don Hall

Effective permissions:

- ☐ Full control
- ☑ List contents
- ☑ Read all properties
- ☐ Write all properties
- ☐ Delete
- ☐ Delete subtree
- ☑ Read permissions
- ☐ Modify permissions
- ☐ Modify owner
- ☐ All validated writes

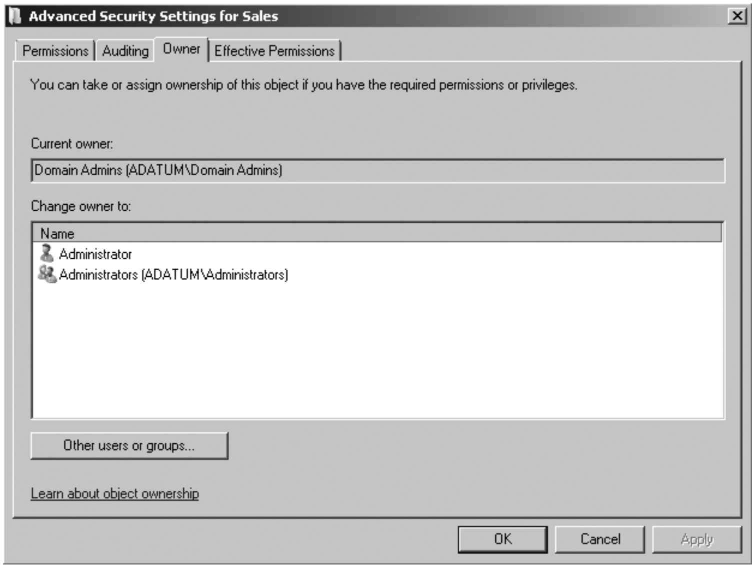
Figure 9-11 Displaying the effective permissions for an Active Directory object.

Ownership of Active Directory Objects

Every object in Active Directory has an owner. By default, the user who created an object is the owner. The owner of an object has the right to modify permissions on the object, which means that, even if the owner does not have full control of an object, the owner can always modify the permissions on the object. In most cases, the owner of an object is a specific user account rather than a group account. One exception to this is when an object is created by a member of the Domain Admins group; the ownership of the object is then assigned to the Domain Admins group. If the owner of the object is a member of the local Administrators group but not a part of the Domain Admins group, the ownership of the object is assigned to the Administrators group.

To determine the owner of an Active Directory object, access that object's properties using the appropriate Active Directory administrative tool. Select the Security page, click Advanced, and then select the Owner page. Figure 9-12 shows the interface for the Active Directory Users And Computers administrative tool.

If you have the Modify owner permission to the object, you can use this interface to modify the owner of the object. You can chose either to take ownership for your own account or to assign the ownership to another user or group. This last option is unique in Windows Server 2003 And Windows Server 2008 Active Directory. In Microsoft Windows 2000 Active Directory, you could only take ownership of an object; you could not assign the ownership to another security principal.



You can take or assign ownership of this object if you have the required permissions or privileges.

Current owner:
Domain Admins (ADATUM\Domain Admins)

Change owner to:

Name
Administrator
Administrators (ADATUM\Administrators)

Figure 9-12 Viewing the ownership of an Active Directory object.

Administrative Privileges

The administrative permissions discussed so far have to do with specific permissions on Active Directory objects and define what actions the administrator can perform on those objects. In addition to these permissions, a user may also be able to perform some tasks in Active Directory because of the privileges assigned to him or her. The permissions discussed so far are based on the ACLs that are attached to each Active Directory object. User privileges are different because user privileges are applied to user accounts. User privileges are something that the user has because of who he or she is, not because he or she has permission to modify a particular Active Directory object. For example, there are two ways that you can give a user or group the right to add workstations to the domain. One option is to give the user or group permission to Create Computer Objects either at an OU level or at the Computers container level. This allows the user to add as many workstations as needed to the domain in the specified container.

Another way to allow a user to add workstations to the domain is to ensure that the user has the *Add workstations to domain* privilege. This user right is a part of the Default Domain Controllers Policy. Any user who has this privilege can add up to 10 workstations to the domain. By default, the Authenticated Users group is granted this permission.

Delegating Administrative Tasks

This chapter has thus far discussed how to ensure the security of Active Directory objects. This has been in preparation for this section, which applies the security options to delegate administrative tasks. Because every object in Active Directory has an ACL, you can control administrative access down to any property on any object. This means that you can grant other Active Directory administrators very precise permissions so that they can perform only the tasks they need to do.

Although you can get extremely specific about delegating administrative permissions, you should maintain a balance between keeping things as simple as possible and meeting your security requirements. In most cases, delegating administrative permissions in Active Directory falls under one of the following scenarios:

- **Assigning full control of one OU** This is a fairly common scenario when a company has multiple offices with local administrators in each office who need to manage all objects in the local office. This option also may be used for companies that have merged multiple resource domains into OUs in a single Active Directory domain. The former resource domain administrators can be given full control of all objects in their specific OU. Using this option means that you can almost completely decentralize the administration of your organization while still maintaining a single domain.
- **Assigning full control of specific objects in an OU** This is a variation on the first scenario. In some cases, a company may have multiple offices, but local administrators should have permission to manage only specific objects in the office OU. For example, you may want to allow a local administrator to manage all user and group objects, but not computer objects. In a situation in which resource domains have become OUs, you may want OU administrators to manage all computer accounts and domain-local groups in their OU, but not to manage any user objects.
- **Assigning full control of specific objects in the entire domain** Some companies have highly centralized user and group administration, in which only one group has permission to add and delete user and group accounts. In this scenario, this group can be given full control of user and group objects regardless of where the objects are located within the domain. This is also a fairly common scenario for a company with a centralized desktop and server administration group. The desktop team may be given full control of all computer objects in the domain.
- **Assigning rights to modify only some properties for objects** In some cases, you may want to give an administrative group permission to manage a subset of properties on an object. For example, you may want to give an administrative group permission to reset passwords on all user accounts, but not to have any other administrative permissions. Or the Human Resources department may be given permission to modify the personal and public information on all user accounts in the domain, but not permission to create or delete user accounts.

It is possible to use all of these options, and any combination of these options, with Windows Server 2008 AD DS. As mentioned previously, one way to configure delegated permissions is by directly accessing the ACL for an object and configuring the permissions. The problem with this option is that it can get quite complex because of the number of options available and the real possibility of making a mistake.

Direct from the Source: Delegating Control

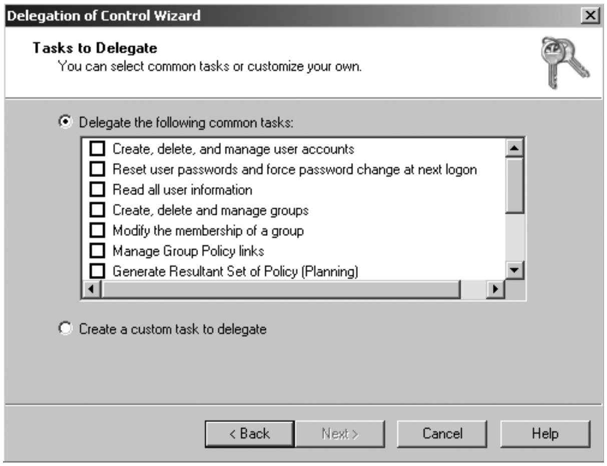
When delegating control to create users and groups, it is imperative to maintain a tracking system for changes that are made. This will make not only daily administration easier, but will be of great use when troubleshooting access issues.

Greg Robb

Microsoft Premier Field Engineer

To make this task easier, AD DS includes the Delegation Of Control Wizard. To use the Delegation Of Control Wizard, follow these steps:

1. Open the Active Directory Users And Computers administrative console and identify the parent object where you want to delegate control. In most cases, you will be delegating control at an OU level, but you can also delegate control at the domain or container level (for example, the Computers or Users container). Right-click the parent object and click Delegate Control. Click Next.
2. On the Users Or Groups page, add the users or groups to which you want to delegate control. Click Add to search Active Directory for the appropriate users or groups.
3. Next, select the tasks that you want to delegate. The interface (shown in Figure 9-13) enables you to select from a list of common tasks or to create a custom task to delegate.



Tasks to Delegate
You can select common tasks or customize your own.

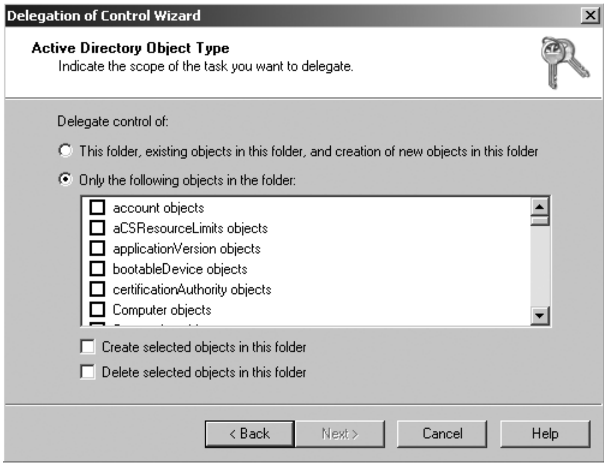
● Delegate the following common tasks:

☐ 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)

○ Create a custom task to delegate

Figure 9-13 Using the Delegation Of Control Wizard to select a common task or create a custom task to delegate.

4. If you choose to create a custom task, you can choose the type or types of objects to which you want to delegate administrative permissions. (Figure 9-14 shows the interface.)



Active Directory Object Type
Indicate the scope of the task you want to delegate.

Delegate control of:

○ This folder, existing objects in this folder, and creation of new objects in this folder

● Only the following objects in the folder:

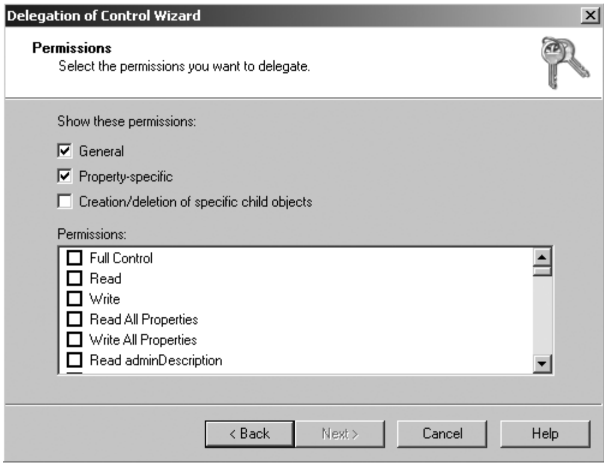
- ☐ account objects
- ☐ aCSResourceLimits objects
- ☐ applicationVersion objects
- ☐ bootableDevice objects
- ☐ certificationAuthority objects
- ☐ Computer objects

☐ Create selected objects in this folder

☐ Delete selected objects in this folder

Figure 9-14 Selecting the type of object or objects to which permissions will be delegated.

5. After you have selected the type of object to which to delegate permissions, you can choose what levels of permissions you want to apply to the object. You can choose full control over the object, or you can delegate permissions to specific properties. (The interface is shown in Figure 9-15.)



Permissions
Select the permissions you want to delegate.

Show these permissions:

☑ General

☑ Property-specific

☐ Creation/deletion of specific child objects

Permissions:

- ☐ Full Control
- ☐ Read
- ☐ Write
- ☐ Read All Properties
- ☐ Write All Properties
- ☐ Read adminDescription

Figure 9-15 Selecting the specific permissions to delegate.

The Delegation Of Control Wizard makes it much easier to delegate control in a consistent manner than when configuring permissions through the ACL. However, the effect of either method is the same; that is, the ACL on the objects is modified to provide the appropriate level of access.

Direct from the Source: The Delegation Of Control Wizard

You are able to use the Delegation Of Control Wizard to delegate many common tasks by giving control to individual users or to groups. These tasks can be set to certain predefined items such as Create, Delete, And Manage User Accounts and Reset User Passwords And Force Password Change At Next Logon. In addition to the predefined items, it is possible to delegate custom tasks using very granular choices, such as account objects, computer objects, or group objects. This makes the Delegation Of Control Wizard a very powerful tool for enabling the share of control throughout Active Directory.

Greg Robb

Microsoft Premier Field Engineer

Auditing the Use of Administrative Permissions

Delegating administrative tasks in AD DS results in the need to be able to monitor and audit the use of administrative permissions throughout the directory structure. Auditing serves at least two primary purposes. First of all, it provides evidence for changes that have been made to the directory. If a change has been made to the directory, you may need to track down who has made the change. This is especially important if an incorrect or malicious change has been made to the domain information. A second purpose for auditing is to provide an additional check on the administrative permissions being exercised throughout the domain. By examining audit logs occasionally, you can determine if someone who should not have administrative rights is in fact exercising such rights.

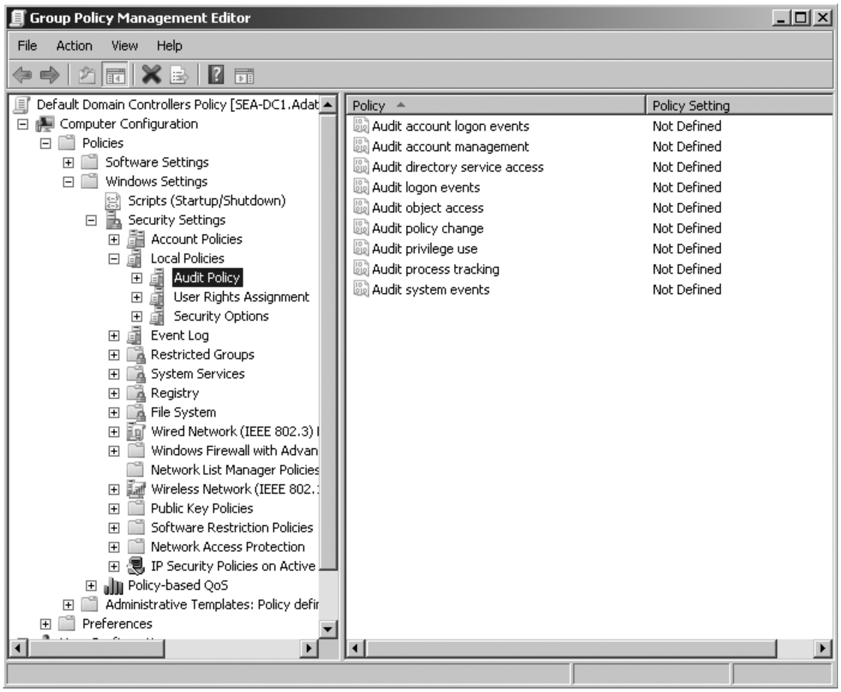
When AD DS events are audited, entries are written to the Security log on the domain controller. You can then use the Event Viewer to view events that Windows Server 2008 logs in the Security log. You can also save events to an event file that can be used to archive and track trends over time.

There are two steps involved in enabling auditing of changes made to Active Directory objects—configuring the audit policy for domain controllers and configuring the SACL on specific Active Directory objects which are to be audited. These two steps are discussed in the following sections.

Configuring the Audit Policy for the Domain Controllers

Your first step for enabling auditing is to configure the audit policy for the domain controllers. This can be configured on the Default Domain Controllers Policy found within the Group Policy Management console. When you open the Group Policy Management console, browse to the Group Policy Objects container. In the details pane, you can right-click Default

Domain Controllers Policy and then click Edit to open the Group Policy Management Editor. From the Group Policy Management Editor, you can browse to Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies and then click Audit Policy. Figure 9-16 shows the default auditing configuration in Windows Server 2008 AD DS.


Group Policy Management Editor
File
Action
View
Help
Default Domain Controllers Policy [SEA-DC1.Adat
Computer Configuration
Policies
Software Settings
Windows Settings
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) I
Windows Firewall with Advan
Network List Manager Policies
Wireless Network (IEEE 802.
Public Key Policies
Software Restriction Policies
Network Access Protection
IP Security Policies on Active
Policy-based QoS
Administrative Templates: Policy defir
Preferences

Policy	Policy Setting
Audit account logon events	Not Defined
Audit account management	Not Defined
Audit directory service access	Not Defined
Audit logon events	Not Defined
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

Figure 9-16 Configuring auditing on the Default Domain Controllers OU.

To audit changes to Active Directory objects, you need to enable and configure the Audit Directory Service Access policy. When this policy is enabled and configured, all modifications made to Active Directory objects are reported in the Security log. You can audit both successful changes to Active Directory objects and failed attempts at modifying Active Directory objects.

In Windows 2000 Server and Windows Server 2003, the Audit Directory Service Access policy was the primary option used to audit directory service events. Windows Server 2008 divides this policy into four subcategories:

- Directory Service Access
- Directory Service Changes
- Directory Service Replication
- Detailed Directory Service Replication

Dividing the Audit Directory Service Access policy into four subcategories provides more granular control on what is or is not audited in relation to directory service events. Enabling the Audit Directory Service Access policy enables all the directory service policy subcategories. To modify the subcategories, you cannot use the Group Policy Object Editor. You can only view and modify the subcategories with the command-line tool Auditpol.exe. For example, if you want to view all of the possible categories and subcategories, type the following line at the command prompt, and then press Enter:

```
auditpol /list /subcategory:*
```

Note For a list of commands that can be used with Auditpol.exe, open a command prompt and type the following: **Auditpol.exe /?**

Auditing Changes to Objects Using the Directory Service Changes Subcategory

The Directory Services Changes subcategory provides the ability to audit changes to objects in AD DS. This subcategory audits the following types of changes:

- When a modify operation is successfully performed on an attribute, AD DS logs both the previous and current values of the attribute.
- When a new object is created, all values of the attributes that are populated during the creation are logged. Note that any default values to attributes that are assigned by AD DS are not logged.
- When an object is moved within the domain, both the previous and new location is logged.
- If you undelete an object, the location where the object is moved to is logged as well as any additions or modifications to attributes while performing the undelete operation.

To enable the Directory Service Changes audit subcategory, you can type the following line at the command prompt, and then press Enter:

```
auditpol /set /subcategory:"directory service changes" /success:enable
```

When you enable the Directory Services Changes audit subcategory, AD DS logs various types of events in the Security event log, as shown in Table 9-3.

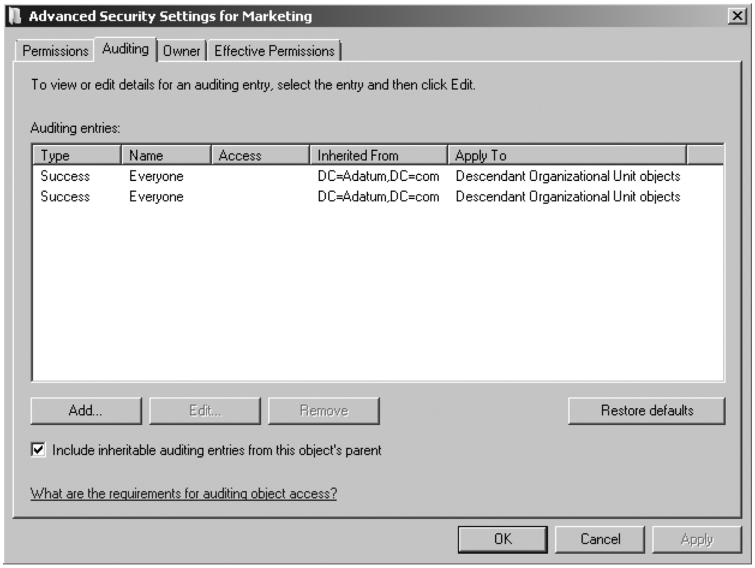
Table 9-3 Directory Services Changes Events

Event ID	Type	Description
5136	Modify	Logged when a modification is made to an attribute in AD DS.
5137	Create	Logged when a new object is created in AD DS.
5138	Undelete	Logged when an object is undeleted in AD DS.
5139	Move	Logged when an object is moved within the domain.

Configuring Auditing on Active Directory Objects

The second step to configuring Active Directory object auditing is to enable auditing directly on the SACL of each Active Directory object to be audited. To enable Active Directory object auditing, access the object's Properties sheet through the appropriate Active Directory administrative tool. Then, click the Security page, click Advanced, and click the Auditing page. Figure 9-17 shows the interface for the Active Directory Users And Computers administrative console and the default audit setting for an OU in Active Directory.

To add additional auditing entries, click Add and select which users or groups and what actions you want to audit. In most cases, you should select the Everyone group so that modifications made by anyone can be audited. Then you can select which activities you want to audit. You can audit all modifications made to any object in the container, to specific types of objects, or to specific properties. You can enable the auditing of all successful modifications, of all failed attempts to make modifications, or both. If you audit all successful modifications, you will have an audit trail for all changes made to the directory. If you enable failed attempts, you will be able to monitor any illicit attempts to modify directory information. After auditing is enabled, all of the audit events are recorded in the Security log accessible through the Event Viewer.


Advanced Security Settings for Marketing
Permissions
Auditing
Owner
Effective Permissions
Add...
Edit...
Remove
Restore defaults
What are the requirements for auditing object access?
OK
Cancel
Apply

To view or edit details for an auditing entry, select the entry and then click Edit.

Auditing entries:

Type	Name	Access	Inherited From	Apply To
Success	Everyone		DC=Adatum,DC=com	Descendant Organizational Unit objects
Success	Everyone		DC=Adatum,DC=com	Descendant Organizational Unit objects

☑ Include inheritable auditing entries from this object's parent

Figure 9-17 Configuring auditing on Active Directory objects.

Enabling auditing is easy. Managing auditing is much more difficult. If you enable the auditing of all directory modifications at the domain controller OU level, the Security log will grow very rapidly. Almost all of the events will be legitimate changes and thus of no interest to you except as an audit trail. However, interspersed among the legitimate changes may be a small number of changes that you need to be aware of. The problem is finding the few interesting audit events among the large number of routine events. In some companies, one administrator may be given the task of reviewing the event logs every day. A better way to deal with this is to create some automated way of centralizing and analyzing the event logs. Another way is to use a tool such as Microsoft System Center Operations Manager (a separate product available for purchase) to filter the events and raise alerts only on the interesting events.

More Info If you want to find out more about Microsoft System Center Operations Manager, you can go to the following Web site: *http://www.microsoft.com/systemcenter/opsmgr/default.mspx*. Operations Manager provides a great deal of functionality that goes far beyond just monitoring Security logs.

Direct from the Source: Consider Event Log Settings Carefully

Always think through the ramifications of enabling an option that will increase the amount of information being sent to the event logs. Many customers will customize the event logs to meet their specific security requirements but never revisit the settings to determine if the additional logging will cause them problems. I have seen many instances in which auditing was enabled and the policy setting Audit: Shut Down System Immediately If Unable To Log Security Audits was also enabled, resulting in a denial of service attack. Another setting that many IT professionals change is the maximum log size. Before changing event log sizes to high values, do some preliminary analysis to determine if the system on which you are enabling this setting has enough memory available. Information about the event log and memory constraint can be found at *http://support.microsoft.com/kb/183097.*

Barry Hartman

Senior Consultant

Microsoft Consulting Services

Tools for Delegated Administration

AD DS provides powerful options for delegating administrative tasks and assigning only the precise permissions that users need to have to perform specific tasks. To complement this delegation, Windows Server 2008 also makes it easy to develop administrative tools that fit the user's task. For example, if you delegate the right to reset passwords for a single OU, you can also provide a very simple administrative tool that can only be used to reset passwords in the specified OU. Windows Server 2008 provides the ability to create a customized view of the Microsoft Management Console (MMC) administrative snap-in in order to allow delegated administrators effective tools to complete their tasks.

Direct from the Source: Working with Third-Party Delegation Tools

Many customers use third-party products to perform delegation. These products usually provide a Web interface and allow administrators to develop custom Web views for daily administrative functions versus creating customized MMCs. When working with customers dealing with branch office scenarios, make sure you understand the business and branch office operational requirements in the event of an extended communications outage. If a customer has highly reliable communication links to the branch office, then this topic isn't as much of a concern; however, for those customers who don't have highly reliable communications, it is a subject that needs to be addressed.

In the event of a communications outage, you must understand what the branch office requires to continue to function. In the case of delegation, if the branch office needs to continue to function and system administrative actions still need to occur, but the Web interface required to perform some of these functions is unavailable because it is hosted from headquarters, how will the people at the branch office perform their jobs? If the third-party product instantiated the delegation model natively into Active Directory Users and Computers, then the same restrictions that applied through the Web interface would apply when using native tools. It is important that you, the trusted advisor, have an understanding of how third-party products interface and interact with Active Directory. Having this type of knowledge will allow you to advise and prepare your customers so they are still able to maintain operations when situations such as a communications outage occur.

Barry Hartman

Senior Consultant

Microsoft Consulting Services

Customizing the Microsoft Management Console

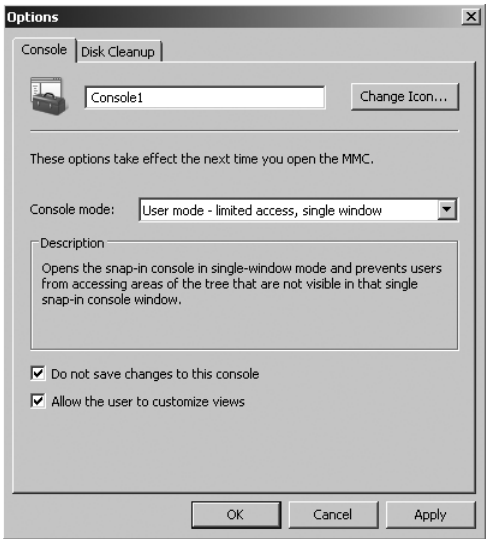
One option for developing an administrative tool is to create a customized MMC using one of the default snap-ins and then modify what the user can see in the MMC.

Caution Simply creating the customized MMC does not grant or limit the user's rights to perform administrative tasks. Before creating the customized administrative interface, you must first delegate the correct level of permissions. For example, if you give a user the right to create user accounts at a domain level, and then you create an MMC that only allows the user to view one OU, the user can still create user accounts in any OU in the domain. If the user loads the regular Active Directory Users And Computers administrative tool or sits down at another desk with a different MMC, the user will be able to create the account anywhere.

To create the customized MMC, open the Run dialog box and type **mmc**. This opens an empty MMC. From the File menu, add the appropriate Active Directory administrative tool snap-in. If you create a custom MMC using the Active Directory Users And Computers snap-in, you would then expand the domain and locate the container object where you have delegated permissions. In the left pane, right-click on the container object and select New Window From Here.

This opens a new window with just the container object and all child objects visible. You can then switch back to the window that displays the entire domain and close the window. Finally, save the administrative tool and provide it to the users, who will administer only the part of the domain that is visible in the MMC. The MMC can be provided to the user in a number of ways. For example, you may install the MMC on his or her desktop, or you may create a shortcut to the administrative tool on a network share.

To make sure that the administrators do not modify the custom MMC after you have given it to them, you can modify the MMC options by selecting Options from the File menu. You can configure the MMC to be saved in User Mode and modify the permissions on the MMC so that the end user cannot save any changes to the MMC. Figure 9-18 shows the interface. For full details on how to create customized MMCs, see Windows Help And Support.



Console1

These options take effect the next time you open the MMC.

Console mode: User mode - limited access, single window

Description

Opens the snap-in console in single-window mode and prevents users from accessing areas of the tree that are not visible in that single snap-in console window.

☑ Do not save changes to this console

☑ Allow the user to customize views

Figure 9-18 Configuring a custom MMC to prevent changes to the MMC.

Planning for the Delegation of Administration

As shown in this chapter, Windows Server 2008 AD DS provides the tools you need to delegate administrative permissions in your domain. However, with all of the positive things you can do in delegating permissions, you also take the risk of assigning incorrect permissions. Incorrect permissions may result in allowing users to do things in Active Directory that they should not be able to do. Incorrect permissions can also mean assigning too few permissions, so that users cannot do the work they need to do. Creating a delegation structure that will provide users with the precise permissions they need requires a significant amount of planning. The following are several suggestions to help with your administrative delegation planning:

- Carefully document the administrative requirements for all potential administrators. In most companies, you will find that there are various users and groups that need some administrative permissions in the domain. Many of these users could be members of the Domain Admins group. As you document the administrative tasks that users need to perform, you will usually find that they really need a much lower level of access. Often the only way to document the level of administrative permissions each group needs is to document all of the administrative work they do every day. By documenting the activities they have to perform, you can design the precise permissions they need to have.
- Before making any changes to the production environment, test all security modifications in a test environment. Making a wrong security configuration can have serious implications for your network. Use the test lab to ensure that the modifications meet the permission requirements but do not give any additional permissions that are not needed.
- Use the Effective Permissions page in the Advanced Security Settings window to monitor and test the users' permissions. The Effective Permissions page can be used to determine the precise permissions a user or group has in AD DS. Use the tool in the test environment to ensure that your configuration is accurate and use it again in the production environment to make sure that your implementation followed the plan.
- Document all the permissions that you assign. Of all the tasks assigned to network administrators, documenting changes made to the network appears to be the most disliked because it can be very tedious and not seem important. As a result, documentation is often incomplete or out of date. The only way to effectively manage the security configuration on your network is to document the initial configuration and then to make a commitment to keep the documentation updated whenever one of the original settings is modified.

Summary

The option to delegate administrative permissions in Windows Server 2008 AD DS provides a great deal of flexibility in how your domain can be administered. The delegation of administrative rights is based on the Active Directory security model, in which every object and every attribute on every object has an ACL that controls what permissions security principals have to a specific object. According to the security model, all permissions are, by default, inherited from container objects to objects within the container. These two basic features of the security model mean that you can assign almost any level of permission to any Active Directory object. This flexibility can also mean a great deal of complexity if the security for Active Directory is not kept as simple as possible. This chapter provided an overview of security permissions, Active Directory object access, delegation of administration, and auditing changes made in Active Directory.

Additional Resources

The following resources contain additional information and tools related to this chapter.

Related Information

- Chapter 5, "Designing the Active Directory Domain Services Structure," provides details on planning the structure of Active Directory such as site, domain, organizational unit, and forest designs.
- Chapter 6, "Installing Active Directory Domain Services," provides details on delegating administration for Read-Only Domain Controllers.
- Chapter 8, "Active Directory Domain Services Security," provides additional details on Active Directory security basics and authentication.
- "Best Practices for Delegating Active Directory Administration" located at *http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/actdid1.mspx.*
- "Best Practices for Delegating Active Directory Administration Appendices" located at *http://www.microsoft.com/downloads/details.aspx?FamilyID=29dbae88-a216-45f9-9739-cb1fb22a0642&DisplayLang=en.*
- "Delegating Authority in Active Directory" located at *http://www.microsoft.com/technet/technetmag/issues/2007/02/ActiveDirectory/default.aspx.*
- "Using Scripts to Manage Active Directory Security" located at *http://www.microsoft.com/technet/scriptcenter/topics/security/exrights.mspx.*
- "Sample Scripts to Manage Active Directory Delegation and Security" located at *http://www.microsoft.com/technet/scriptcenter/scripts/security/ad/default.mspx?mfr=true.*
- "Step-by-Step Guide to Using the Delegation Of Control Wizard" located at *http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/stepbystep/ctrlwiz.mspx.*
- "Default Security Concerns in Active Directory Delegation" located at *http://support.microsoft.com/?kbid=235531.*

Index

A

Access control entries (ACEs)
  description of, 274–275
  in Active Directory object access, 328–329
  in AD LDS, 647
  Ldp.exe to view, 334–336
Access control lists (ACLs)
  dynamic DNS and, 79
  for GPO settings, 406–407
  groups and, 366
  in AD LDS, 646–648
  integrated zones and, 75
  of organizational units, 59
  overview of, 273–275
  schema objects and, 626
  security filtering and, 433
  selective authentication and, 169
  Web server resources secured by, 785
Access denied errors, 133
Access tokens
  authentication from, 327
  for security, 276, 282
  in AD LDS, 636
  migration and, 251
Account administrative model, 155
Account domains, 178
Account lockout, 110
  attributes of, 7
  Default Domain Policy control of, 7
  domain number and, 175
  fine-grained password policies and, 528
  in AD LDS, 638
  policy for, 516
  security policy boundaries and, 47
Account management, 326
Account Operators group, 317
Account partner in AD FS, 773–781
  account store in, 776–777
  adding, 783
  claims extractions in, 778
  cookies for, 761
  definition of, 750
  federation service configured as, 750
  in federation Web SSO scenario, 755–756, 768
  organization claims in, 775–776
  outgoing claims mappings in, 780–781
  resource partner in, 778–780
  trust policy in, 773–774
Account policies, 514–518
Account properties for user object, 360–361
Account store
  adding, 776–777
  Federation Services requirements for, 761–762
  forest as, 790
Accounts organizational units, 197
Activation
  file extension, 487, 496–497
  overriding RMS cluster, 723
  Windows Process Activation Service for, 673
Active Directory Application Mode (ADAM), 15, 750, 762
Active Directory Application Mode Setup Wizard, 626, 632
Active Directory Certificate Services (AD CS), 130, 294, 762
Active Directory Client Extension, 301
Active Directory Diagnostic tool, 256–257
Active Directory Domain Services (AD DS), 3–11. *See also* Administration, delegating; also Domain Name System (DNS); also Installing AD DS; also Migrating to AD DS
  account partner and, 761–762
  accounts stored in, 750
  AD LDS synchronization with, 654–657
  auditing of, 6
  database mounting tool in, 9
  fine-grained password policies in, 7–8
  read-only domain controllers (RODC) in, 3–5
  restartable, 9
  Rights Management Services (RMS) and, 708
  user interface improvements of, 10–11
Active Directory Domain Services (AD DS), components of, 19–62
  data store, 20–22
  domain controllers, 22
  domains, 46–50
  forests, 50–51

  - global catalog servers, 23–25
  - operations masters, 28–32
    - domain naming, 29–30
    - infrastructure, 31
    - PDC (primary domain controller) emulator, 30–31
    - RID (relative ID), 30
    - schema, 29
    - transferring roles of, 32
  - organizational units, 57–60
  - partitions, 42–46
  - read-only domain controllers, 25–28
  - related tools for, 61
  - schema, 32–41
    - components of, 33–34
    - deactivating objects of, 40–41
    - modifying, 34–36
    - new attributes in, 36–40
  - sites, 55–57
  - trusts, 52–55
- Active Directory Domain Services (AD DS), structure of, 143–216
  - best practices for, 214–215
  - DNS infrastructure in, 184–192
    - integration with, 190–192
    - internal and external namespaces in, 184–186
    - options for, 186–190
  - domain functional levels in, 181–184
  - domain structure in, 172–181
    - domain number and, 174–176
    - forest root, 176–177
    - hierarchy changes after deployment in, 180
    - ownership of, 180–181
    - trees and trusts in, 178–180
  - Exchange Server 2007 and, 204–214
    - DNS server location and, 206–207
    - domain controller location and, 208–209
    - global catalog server location and, 209–210
    - operations master server locations and, 213–214
    - overview of, 204–206
    - read-only domain controller design and, 210–213
  - forest design in, 156–167
    - change control policies in, 167
    - for security, 161–163
    - integration of multiple, 167–172
    - models of, 163–166
    - overview of, 158–159
    - ownership of, 166
    - single or multiple, 159–161
  - forest functional levels in, 183–184
  - organizational unit structure in, 192–197
  - service requirements in, 144–156
    - business, 145–146
    - documenting, 150–156
    - functional, 146
    - legal, 147–148
    - project constraints in, 149–150
    - security, 148–149
    - service level agreements in, 146–147
  - site topology design in, 197–204
- Active Directory Domain Services Installation Wizard, 225–236
  - completing installation and, 234–235
  - delegation record and, 83, 88
  - deployment configuration and, 226–227
  - DNS configuration errors and, 232
  - domain controller location and, 124
  - domain controller options and, 232–233
  - domain upgrading and, 254
  - file locations and, 233–234
  - fully qualified domain name and, 227
  - Ntds.dit file and, 22
  - operations masters and, 32
  - option selections and, 234
  - password policy enforcement by, 234
  - RODCs and, 27
  - to start AD DS installation, 222–224
  - uninstalling AD DS by, 240
  - verifying installation and, 235–236
  - Windows Server 2008 functional levels and, 228–232
- Active Directory Domains and Trusts tool, 30, 61, 259, 265, 362
- Active Directory Federation Services. *See* Federation Services
- Active Directory Lightweight Directory Services (AD LDS), 148, 619–659
  - account partner and, 762
  - accounts stored in, 750
  - Active Directory Domain Services synchronization with, 654–657
  - best practices for, 657
  - directory partitions in, 624–629
    - application, 627–629
    - configuration, 624–625
    - schema, 626–627

- implementing, 640–654
  - backing up and restoring in, 651–654
  - configuring instances and partitions in, 640–643
  - management tools for, 643–648
  - replication configuration in, 648–650
- instances in, 623–624
- overview of, 620–622
- replication of, 629–633
- security for, 633–639
  - authentication for, 637–639
  - default groups for, 634–635
  - permissions for, 635–636
  - security principals in, 633–634
- servers in, 622–623
- tools for, 658

Active Directory Lightweight Directory Services Setup Wizard, 627, 640–643, 648–649, 658
Active Directory Management Pack, 137
Active Directory Migration tool (ADMT), 249, 252, 259–260
Active Directory Schema MMC snap-in, 23, 32, 36, 255
Active Directory Service Interface (ADSI), 36, 61, 390
Active Directory Services, 11–18
- certificate services role as, 11–13
- federation services role in, 13–15
- lightweight services role in, 15–16
- rights management services role in, 16–18

Active Directory Sites and Services tool, 61
- AD LDS and, 650, 658
- for replication troubleshooting, 139
- for troubleshooting replication, 134–135
- knowledge consistency checker (KCC) and, 112
- object visible through, 329
- RPC-over-IP connections and, 129

Active Directory Users and Computers tool
- AD database mounting tool and, 609
- attributes shown by, 37
- auditing enabled in, 309
- cached credentials and, 26
- credential caching and, 212
- domain configuration and, 61
- domain directory partition and, 43
- for GPC object, 407
- in migration, 260
- inetOrgPerson object created by, 364
- infrastructure operations masters and, 256
- MMC administrative snap-in customized by, 354
- object visible through, 329
- PDC emulator role seizure and, 612
- resultant PSOs and, 531
- RODC deployment and, 239
- to map certificates, 295
- to modify object access, 329
- to verify installation, 235
- user profiles and, 464, 466

ActiveX Data Objects (ADO), 390
Adamsync synchronization, 654–657
Add Application Wizard, 782
Add Features Wizard, 404
Add Printer Wizard, 383
Add Resource Partner Wizard, 779
Add Roles Wizard, 10, 222–223
ADDS DesignDocument.xlsx, 167, 184, 197, 204
Administration, delegating, 59, 181, 325–356
- auditing, 348–352
- object access in, 327–329
- object permissions in, 329–348
  - effective, 340–343
  - inheritance of, 336–339
  - ownership of, 343–348
  - special, 331–336
  - standard, 329–331
- of read-only domain controllers, 211
- organizational unit design and, 194
- planning for, 354–355
- tasks, 326–327
- tools for, 352–354

Administrative autonomy, 162–163, 174, 252
Administrative isolation, 162–163, 165, 214
Administrative permissions, 220–221
Administrative templates. *See* Templates
Administrator Role Separation, 5, 27
Administrators group, 163
ADML files, 479
ADMT Group Account Migration Wizard, 260–261
ADMX files, 404, 479–481. *See also* Templates
ADMX Migrator, 483
Adprep.exe command-line tool, 8, 250, 255, 363
AdRestore tool, 606, 615
ADSchemaAnalyzer, 655
ADSI Edit tool, 76, 329
- AD database mounting tool and, 609
- for Active Directory objects, 358, 395, 397
- for GPC object, 407

  for PSOs, 529, 531
  in AD LDS, 634, 643–645
  in disaster recovery, 616
  in garbage collection, 575
  scripts and, 574
  site links and, 127–128
  tombstone lifetime modified by, 590
Advanced Encryption Services (AES), 182
Advertising applications, 488
AES Algorithm, 686
Aging, record, 78, 80
Alert Tasks, 559
Allow access control entries (ACEs), 275, 329
Allow Cryptography Algorithms Compatible With Windows NT 4.0, 221–222
Allow permissions, 340
Allowed RODC Password Replication Group, 213
American National Standards Institute (ANSI), 39–40
Anonymous authentication, 637
Anonymous SID-Name translation, 518
Application Policies extension, 698
Application programming interfaces (APIs), 663
Application-facing role, 3
Applications
  AD FS configuration of, 782–783
  AD LDS directory partitions for, 627–629
  basic groups for, 366–367
  claims-aware, 752, 781
  compatibility of, 213
  default partition, 76–77
  directory partitions for, 29, 44–46, 116, 240, 634
  directory-enabled, 155
  DNS partitions for, 78–79
  domain controllers backup and, 589
  event viewer and, 569
  Group Policy for deployment of, 486–489
  in Federation Web SSO scenario, 769
  internal Web, 670
  organizational units based on, 197
  public key-enabled, 667
  site-aware, 489
  specific data management for, 326
  Windows NT token-based, 752, 757, 759, 785–787
  zero Administration for Windows (ZAW) down-level applications package (.zap) for, 490–491
Archived rights policy template, 733
ASP.NET applications, 14
Assigning applications, 488
Asymmetrical encryption, 661
Asynchronous processing, for GPOs, 413–414
Atomic operations, originating updates as, 98
Attack surface decrease, for security, 303–306
Attribute Editor, 407
Attributes
  claims extractions and, 778
  classSchema object specified, 33
  creating in schema, 36–40
  displayName, 34
  fSMORoleOwner, 30
  global catalog and, 23
  in user objects, 358
  indexing, 35–36
  isDeleted, 104
  LdapDisplayName, 40
  linked, 98, 105
  modifying, for objects, 98
  msDS-AuthenticatedToAccountList, 26
  msDS-DnsRootAlias, 29
  msDS-NeverRevealGroup, 26
  msDS-RevealedList, 26
  msDS-Reveal-OnDemandGroup, 26
  msDS-UpdateScript, 29
  name, 98
  of account lockout settings, 7
  of crossRef class, 50
  of Password Settings objects (PSOs), 8, 530
  RODC filtered, 4
  schema definitions of, 33
  SIDHistory, 170
  userAccountControl, 8
  USNChanged, 100–101
Auditing
  administration delegating, 348–352
  administrator accounts, 317
  administrator actions, 163
  audit policy for, 304, 518
  configuring, 351–352
  domain controllers
    archiving logs for, 310
    Directory Service Changes subcategory of, 308
    policy for, 348–350
    settings for, 308–309
    subcategories of, 307
  domain services, 6
  in interforest migration, 260

  settings for, 307–309
  user rights assignment and, 524
  Version 3 templates and, 686
Auditpol.exe command-line tool, 6, 308, 349–350
Authenticated Users group, 79, 169
Authentication. *See also* Kerberos authentication; also Kerberos security
  account partner, 762
  across boundaries, 287–288
  AD DS infrastructure and, 143
  challenge-response mechanisms for, 301–303
  computer objects for, 377
  cookies for, 760–761
  delegated, 289–291
  digital certificates for, 661
  domain controllers for, 22
  domain number and, 176
  extranet store for, 15, 621
  Federation Services and, 13
  federation trusts and, 749
  firewalls for, 169
  forest-wide, 268
  in AD LDS, 632, 637–639
  in wired network security, 540
  LAN Manager level of, 525
  NTLM, 301–303
  overview of, 276–277
  perimeter network and, 148
  read-only domain controller, 212
  security policy boundaries and, 47
  selective, 165, 168–170, 182
  site-specific service locator (SRV) records and, 56
  SSL client certificates for, 764
  SSL server certificates for, 764
  troubleshooting, 133, 298–301
  trusts as, 52
  two-factor, 149, 670
  universal groups and, 25, 370
Authentication Service (AS), 280, 282
Authoritative name server, 82
Authoritative restores, 591, 599–601
Authority Information Access (AIA), 672
Authorization
  AD DS infrastructure and, 143
  in access control, 327–328
  overview of, 277–278
  resource partner for, 750
  troubleshooting, 133
Authorization Manager
  application groups for, 367
  group claims and, 775
  LDAP query groups and, 366
  policies for, 182
Authorizer, 375
Autoenrollment of certificates, 527, 680, 690–692, 698, 701
Automatic Certificate Request Service (ACRS), 527, 690
Automatic named control flags, 275
Automatic site coverage, 210
Automating object management, 386–395
  command-line tools for, 386–387
  LDIFDE and CSVDE for, 387–389
  VBScript for, 389–395
Autonomy, administrative, 162–163, 174, 252
Availability, requisite, 145–146

B

Background zone loading, 80–81
Backing up and restoring. *See also* Disaster recovery
  Active Directory Lightweight Directory Services (AD LDS), 651–654
  best practices for, 614
  database mounting tool and, 9
  default domain GPOs, 526
  documenting, 155
  frequency of, 591
  Group Policy objects, 439–440
  management of, 326
  media for, 10
  need for, 589
  overview of, 587–589
  security media for, 318
  tombstone lifetime and, 589–590
Backlinks, 602
Backup Operators group, 163
Backward compatibility, 278, 301
Backward linked attributes, 98, 105
Bandwidth
  documenting, 151
  domain creation and, 178
  Exchange Server 2007 and, 205
  for replication, 75, 198–199
  Group Policy software deployment and, 489–490
  install from media (IFM) feature and, 588
  intersite replication and, 108, 110

  monitoring and, 554
  multicasting and, 502
  network frame analysis tool for, 246
  Network Location Awareness Service (NlaSvc) and, 404, 419
  site link costs and, 202–203
  site links and, 125
Bandwidth throttling, 106
Base certificate revocation lists (CRLs), 675
Base schema objects, 40
Batch files, for managing Active Directory, 386, 389, 392
Best practices
  for AD DS structure, 214–215
  for AD LDS, 657
  for Certificate Services (CS), 701
  for disaster recovery, 614–615
  for Domain Name System (DNS), 92
  for Federation Services, 790
  for forest-wide authentication, 169
  for Group Policy templates, 482–484
  for Kerberos policy settings, 292
  for LAN Manager (LM) password hash values, 302
  for migrating to AD DS, 269
  for object management, 395–396
  for replication, 137–138
  for RODC deployment, 239
  for security, 170, 319
  for service administrators, 162
  for universal group design, 376
Binary Large Object (BLOB), 684–685
BIND DNS infrastructure, 190–192
Bind redirection authentication, 638–639
Blocking device installation, 401
Blocking inheritance of permissions, 338
Boot Configuration Data (BCD), 588
Bootmgr files, 588
Boundaries
  authenticating across, 287–288
  domain, 46–47, 172–173
  Exchange Server, 158
Branch offices, 3, 5, 27, 206–207, 238. *See also* Read-only domain controllers (RODCs)
Bridgehead servers, 4, 28
  configuring, 130–132
  in intersite replication, 109–110, 120
  replication interval for, 126
  site link bridges and, 128
  site link costs and, 203
  SMTP replication and, 130
Bridging, site link, 128–129
Built-in groups, 371–372
Bulk operations, 388–389, 396
Business service requirements in AD DS, 145–146
Business units, 155, 178
Business-to-business (B2B) identity federation scenario, 746, 750
Business-to-consumer (B2C) identity federation scenario, 747
Business-to-employee (B2E) identity federation scenario, 747

C

Caching
  certificate revocation lists (CRLs), 676–677
  credential, 26–27, 212–213
  domain controller information, 72
  names, 298
  schema, 38
  universal group membership, 25, 209, 370–371, 376
CAPolicy.inf file, 672–673
Catalog. *See* Global catalog; Global catalog servers
Centralized administration, in forest design, 159
Certificate revocation lists (CRLs). *See also* Revocation
  caching of, 676–677
  configuration of, 675–678
  distribution of, 701
  distribution point paths for, 667, 672
  for SSL server authentication certificates, 764
  importing, 677–678
  overview of, 12–13
  publication intervals for, 672
Certificate Services (CS), 661–702
  best practices for, 701
  certificate autoenrollment for, 690–692
  certificate templates for, 685–689, 697–699
  certification authorities and, 667–669
  credential roaming in, 693–694
  deployment scenarios for, 670
  distribution procedures for, 700
  Group Policy certificate acceptance in, 692–693
  hierarchy for, 694–697

  - implementing, 670–685
    - certificate revocation in, 674–681
    - key archival and recovery in, 681–685
    - root certification authorities in, 671–673
    - subordinate certification authorities in, 673
    - Web enrollment in, 673–674
  - overview of, 11–13
  - PKI (public key infrastructure) components of, 662–667
  - revocation procedures for, 700
  - tools for, 702
- Certificates
  - authentication model based on, 293
  - Automatic Request Settings for, 527
  - Client Licensor, 710–711
  - digital, 293
  - federation proxy server client, 771–773
  - federation server, 763
  - for account partner authentication, 762
  - Group Policy settings for, 13
  - in Rights Management Services (RMS), 709–711
  - Privilege Attribute, 282, 284, 299
  - root certification authority, 763
  - self-signed, 766, 790
  - software restriction policies and, 535
  - SSL server authentication, 764
  - token-signing, 763, 767, 771, 773
  - user account mapping of, 294–295
  - verification, 763
- Certification Authorities (CA), 293–294
  - account partner and, 762
  - Certificate Services (CS) and, 667–669
  - choosing, 765–766
  - configuring, 679
  - description of, 666
  - enterprise, 13, 701
  - in STMP replication, 130
  - internal, 767
  - management tools for, 662
  - MMC snap-in for, 702
  - offline root, 701
  - root, 671–673, 763
  - stand-alone, 13, 689
  - subordinate, 673
  - troubleshooting, 12
  - trusted root, 527
  - Web enrollment of, 671
- Certification practice statement (CPS), 672
- Certreq.exe command-line utility, 662, 664, 702
- CertUtil.exe command-line utility, 675
- Challenge-response authentication mechanism, 301
- Change control policies, 156, 159, 167
- Change injection, 574
- Change stamps, in replication, 99, 103–104
- Checkpoint file, 586
- Child domains, 48–49, 221
- Circular logging, 584, 587
- Claims
  - agent aware of, 14
  - applications aware of, 752, 782
  - extractions of, 778
  - federation, 751
  - identity, 779, 782
  - incoming mappings of, 783–785
  - organization, 775–776, 781
  - outgoing mapping of, 780–781
  - transformation module DLL for, 773
- Classes
  - crossRef, 50
  - dynamicObject, 182
  - inheritance of, 34
  - User, 33–34, 36
- classSchema objects, 33
- Client Access server role, 205
- Client Licensor Certificate (CLC), 710–711
- Client Service Discovery, 722–723
- Clients
  - domain controllers availability and, 70–71
  - federation proxy server, 771–773
  - Rights Management Services (RMS), 708–709, 721–726
  - site of, 71
  - SSL authentication certificates for, 764
  - Web browser requirements for AD FS, 760–761
- Client-side extensions (CSEs), 405
  - for scripts, 416
  - in Group Policy, 409–410
    - dynamic link libraries of, 411
    - GUIDs associated with, 411–413
    - storage of, 411
    - viewing, 411
  - preferences versus, 509, 534
  - slow link detection default behavior and, 421
- Cloning, 248, 501
- Closed set, in intraforest migration, 266
- Cluster key passwords, 717, 740–741

Cluster service information, 588
Clusters, RMS, 706–707, 715–720
Cmdlet syntax, in PowerShell, 393–395
Comma Separated Value Directory Exchange (CSVDE) tool, 36
Comma-separated values file (CSV), 387
Common name claims, 775–776
Compatibility, 221–222, 278, 301
Compatibility, application, 213
Compression, intersite replication and, 127
Computer accounts, 263–265
Computer Group Policy, 414
Computer Migration Wizard, 263–264
Computer MMC snap-in, 9, 378
Computer objects, 377–379
Conditional forwarders, 84–86, 152
Confidentiality, 147–148
Configuration directory partitions
  domain naming operations master and, 29
  in AD DS structure, 44
  in AD LDS structure, 624–625
  in forest design, 50, 158
  replication of, 135
Configuration store, for distributed applications, 15
Conflict resolution, in replication, 103–104, 629
Connection objects, 112–115
Connection points, RMS, 719–721
Connectivity
  for installing AD DS, 219–220
  for remote procedure calls (RPCs), 111
  forced domain controller removal and, 243
  in AD FS deployment, 760
  in Group Policy troubleshooting, 453
  troubleshooting, 133, 136
Constrained delegation, 289–290
Constraints, 149–150, 152
Contact objects, 364–365
Containerized indexes, 35
Containers
  Group Policy, 457–458
  in AD LDS configuration directory partition, 625
  parent, 98
  Password Setting, 528
Control Panel settings, 506–507
Convergent replication, 96
Cookies, 760–761
Copying, in migration, 250
Costs
  of internal certification authorities (CA), 666
  of monitoring, 553–554
  site link
    bandwidth links to, 202
    formula for, 202–203
    KCC routing topology and, 127
    redundancy and, 125
    RPC-over-IP and, 130
CPU utilization, KCC, 572
Credential Manager, 520
Credentials
  AD DS and, 149, 220
  AD DS Installation Wizard and, 10
  caching of, 4–5, 26–27, 212–213
  for sensitive accounts, 317
  in access control, 327
  in AD LDS, 649
  in federation trust, 14
  roaming and, 693–694, 701
  RODC administrative, 211
Cross-business unit communication, 156
Cross-domain copying wizard, 441
Cross-domain group-to-user references, 31
Cross-forest trusts, 169, 364
Cross-reference objects, 29, 49–50, 242
CryptoAPI 2.0 diagnostic logging, 663–664
CryptoAPI Next Generation (CNG) algorithm, 685–687
Cryptographic identifier, 535
Cryptographic service provider (CSP), 671, 717
Cryptography Next Generation (CNG), 12
Cscript.exe run time, 390
CSVDE command-line utility, 358, 387–389, 394, 396
CurrentNetworkEnvironment.xlsx, 152, 154, 184
Custom claims, 776, 778
Custom Installation Wizard, 493

D

Data
  confidentiality of, 147–148
  management of, 326
  Privilege Attribute Certificate (PAC), 299
  replication of, 128
  storage of, 585–587
Data collector sets and reports, 559–562
Data recovery agent (DRA), 526

Data store
  as AD DS component, 20–22
  dynamic application, 29
  for AD LDS, 622–623
  indexing, 35–36
Databases, 22
  certification authority, 671
  data store and, 22
  defragmentation of, 576–578
  directory management for, 326
  in AD LDS, 623
  integrity of, 579
  locations of, 580
  mounting tool for, 9, 607–610, 615
  NTDS, 219
  read-only AD DS, 4
  Rights Management Services (RMS) and, 708, 717
  schema attributes and, 38
  Security Accounts Manager (SAM), 21, 234
  semantic analysis of, 579–580
  SQL Server, 17
  storage monitoring for, 571
Dcdiag.exe tool
  for authentication status, 298
  for monitoring, 572–573
  for replication troubleshooting, 136–137, 140
  for verifying AD DS installation, 235
  in forest preparation, 256
Dcgpofix.exe command-line tool, 526–527
Dcpromo.exe tool, 224, 236, 240, 243
Dctlog.txt file, 264
Deactivating objects, 40–41
Debug Logging option, 90
Decentralized administration, 325. *See also* Administration, delegating
Dedicated domain controllers, 319
Dedicated root domain, 47, 176–177, 181
Default display name, 362, 364
Default Domain Controllers Policy. *See* Domain controllers
Default domain policy, 291, 514–519. *See also* Domains
  account lockout settings and, 7
  account policies in, 514–518
  local policies in, 518–519
  Password Settings objects and, 7–8
Default trust configuration, 179
Default-First-Site-Name, 56, 123
Defragmentation
  offline, 577–578
  online, 576–577
Delegated subdomains, 87
Delegation. *See also* Administration, delegating
  documenting, 152–153
  for new domains, 220
  namespace design and, 189
  of administrative rights, 181
  of authentication, 279, 289–291
  of read-only domain controller administration, 211
  of signing key, 679
  organizational unit design and, 194
  records of, 82–83, 88
Delegation of Control Wizard, 336, 346–348, 436–437
Delete number command, 609
Delta certificate revocation lists (CRLs), 675
Demilitarized zone, 14
Denied RODC Password Replication Group, 213
Deny access control entries (ACEs), 275, 329
Deny permissions, 340–341
Dependent services, stopping, 9
Designated File Types object, 537
Desktops. *See* Group Policy for user desktops
Device installation, blocking, 401
DFS Replication event log, 137
DHCP Client service, 89
Diagnostic logging, 663–664
Differentiated Services Code Point (DSCP), 400
Digest authentication, 279
Digital certificates, 293, 661, 665
Digital signatures, 13, 293, 295, 763
Digitally signed security token, 751
Dir command, 462
Direction of forest trusts, 168
Directory partitions
  application, 634
  in AD LDS, 620, 624–629
    application, 627–629
    configuration, 624–625
    schema, 626–627
  names of, 628
Directory Service Agent (DSA), 21, 280, 623
Directory service auditing, 6
Directory Service Changes subcategory, 308, 350

Directory Service event log, 137, 572–573
Directory Services Restore Mode (DSRM)
  for monitoring, 579–580
  in AD DS installation, 234, 243
  in disaster recovery, 595–596, 600–601
  overview of, 9
Directory-enabled applications, 155
Disaster recovery, 583–616
  AD DS data files and, 20
  backing up for, 587–591
    frequency of, 591
    need for, 589
    overview of, 587–589
    tombstone lifetime and, 589–590
  best practices for, 614–615
  data storage and, 585–587
  documenting, 145
  operations masters locations and, 214
  planning for, 584–585
  restoring Active Directory in, 591–614
    authoritative, 599–601
    database mounting tool for, 607–610
    domain controller creation in, 591–595
    group memberships in, 601–605
    nonauthoritative, 595–599
    operations masters and global catalog in, 610–614
    SYSVOL information in, 610
    tombstone object reanimation in, 605–607
  rollback in, 250
  service level agreements (SLAs) for, 147
  tools for, 615–616
Discretionary access control lists (DACLs). *See also* Dsacls command-line tool
  in Active Directory object access, 328–329
  in AD LDS, 636, 648
  in migration, 251, 263
  security and, 274–275, 278
Disk cloning, 501
Dispatch agent log file, 264
Display names, 34, 361–362
Display Specifier schema, 625
DisplayADLDSInstances.ps1 script, 629
DisplayMachineVersionLGPO.vbs script, 417
DisplayUserVersionLGPO.vbs script, 417
Distinguished name tag (DNT), 602
Distinguished names, 43, 50, 575
Distributed applications, 15
Distributed File System (DFS)
  for SYSVOL folder, 610
  in AD DS structure, 198
  network utilization managed by, 489
  replication and, 4, 409
  security of, 56
  shared folder publishing and, 385
Distributed File System Replication (DFSR) service, 106, 182, 571
Distributed rights policy template, 733–735
Distribution groups, 366–367
Distribution of certificates, 667, 700
DNS Console tool, 93
DNS locator service, 69–72
DNS Manager, 76–77
DNSCmd tool, 76
Dnscmd.exe command-line tool, 93
DNSDomainname 600 IN AAAA IPv6Address record, 68
DNSDomainname 600 IN IPv4Address record, 68
Dnslint.exe tool, 93, 139
dnsRoot attribute, 50
Documenting
  administrative delegation, 355
  current environment, 150–156
    Active Directory infrastructure in, 152–154
    administrative models and processes in, 155–156
    backup and recovery infrastructure in, 155
    directory-enabled applications in, 155
    Exchange Server implementation in, 154
    name resolution infrastructure in, 152
    network infrastructure in, 151–152
Documents, RMS and, 704. *See also* Printers
Domain administrator account, 317
Domain Admins group, 135
  AD DS structure and, 162–163, 166
  application directory partitions and, 46
  blocking permissions and, 338
  database mounting tool and, 609
  different user types and, 7
  domain controller removal and, 242
  domain controller security and, 316
  in new domains, 373
  migration and, 256
  permissions and, 330, 375
  read-only domain controllers and, 3, 239
Domain Controller Diagnostics tool, 235

Domain controllers. *See also* PDC (primary domain controller) emulator operations masters; also Read-only domain controllers (RODCs)
  Adprep command-line tool and, 8
  as AD DS components, 22
  audit policy for, 348–350
  availability of, 70–71
  backing up, 589
  computer objects for, 378
  database management for, 326
  default policy for, 519–525
    overview of, 401, 416
    security options for, 525
    user rights assignment in, 519–525
  disaster recovery of, 591–595
  documenting, 153
  domain name information stored in, 79
  Domain Name System and, 63
  dynamic port mapping and, 129
  Exchange Server 2007 and, 205
  for AD DS logon, 199
  forced removal of, 243–244
  forest root, 209
  fully qualified domain name for, 227
  in troubleshooting replication, 135
  installing AD DS and, 218, 232–233
  location of, 208–209
  management interface for, 21
  migrating, 269
  monitoring of, 571
  partition integration with, 163
  password resetting and, 377
  permissions of, 28–29
  promotion to, 217
  pruning service on, 381
  rebooting, 371
  redundancy of, 584
  removing, 241–242
  replication and, 56, 114–116
  security for, 199, 303–316
    attack surface decrease as, 303–306
    audit policy settings for, 307–309
    event log policy settings for, 309–310
    option policy settings for, 312–313
    SMB signing for, 314–315
    SYSKEY configuration for, 315–316
    user rights assignment policy settings for, 311–312
  source, 10
  SRV records registered by, 66–69
  states of, 9
Domain identifier, 272
Domain Name System (DNS), 63–94
  AD DS installation and, 220, 232
  AD DS integrated zones and, 74–81
    benefits of, 75
    default application partitions for, 76–77
    managing, 78–81
  AD DS integration with, 64–74
    automatic site coverage for, 72–74
    DNS locator service for, 69–72
    service location (SRV) resource records for, 64–69
  best practices for, 92
  domain controller restoring and, 594
  in AD FS deployment, 760
  infrastructure of, 184–192
    AD DS integration with, 190–192
    internal and external namespaces in, 184–186
    options for, 186–190
  lookup errors in, 138
  monitoring of, 571
  namespaces of, 81–91
  delegation in, 82–83
    forwarders in, 83–86
    root hints in, 86
    stub zones in, 86–88
    troubleshooting, 88–91
  read-only, 5
  replication and, 111, 569
  server for, 206–207, 569–570
  server service of, 45
  tools for, 93–94
  troubleshooting, 133
  updating, 242
Domain naming operations masters, 29–30, 32, 214, 613
Domain services. *See* Active Directory Domain Services (AD DS)
Domain tree root domain, 88
Domain trees, 48–49
DomainDnsZones, 5, 45, 76, 78–79, 235
Domains. *See also* Default domain policy
  Active Directory Domains and Trusts tool for, 61
  decommissioning source, 265
  default Group Policy objects (GPOs) for, 526–527

  default policy for, 401
  directory partitions for, 43–44
  functional levels of, 153, 181–184, 228, 230–231
  Group Policy implementation for, 438–439
  Group Policy templates based in, 481–482
  in AD DS, 46–50
  in Group Policy Management Console (GPMC), 424–425
  numbers of, 174–176
  recovering groups in remote, 603–604
  restructuring of, 250–252. *See also* Interforest migration
  RMS trusted publishing, 729–731
  RMS trusted user, 727–729
  structure of, 172–181
    domain number and, 174–176
    forest root, 176–177
    hierarchy changes after deployment in, 180
    ownership of, 180–181
    trees and trusts in, 178–180
  upgrading in migrating to AD DS, 249–250, 254–257
Down-level client computers, 221
Drive mapping, 385
Dsacls command-line tool, 636, 646–648
Dsadd.exe tool, 387
Dsadd.exe utility, 379
Dsamain.exe tool, 607–609. *See also* Databases, mounting tool for
Dsdbutil.exe command-line tool, 61
  for AD LDS instance backup, 651–653
  for AD LDS instance restore, 653
  for AD LDS management, 645–646, 658
  for AD LDS service account, 624
DSGET command-line tool, 532
Dsget.exe tool, 387
DsGetDcName API, 69–70
Dsmgmt.exe command-line tool, 27, 638
Dsmod.exe tool, 387
Dsmove.exe tool, 387
Dsquery.exe tool, 387
Dsrm.exe tool, 387
Duration, of account lockout settings, 7
Dynamic application data, 29
Dynamic DNS, 79–80, 89
Dynamic Host Configuration Protocol (DHCP), 9, 79
Dynamic Link Libraries (DLLs), 411
Dynamic port mapping, 129
Dynamic updates, 90–91, 190
dynamicObject class, 182

E

Edge Transport Server, 16, 654–655
Effective permissions, 340–343, 355
Electronic data interchange (EDI), 746
Elliptic-Curve Diffie-Hellman (ECDH) Algorithm, 686
Elliptic-Curve Digital Signature Algorithm, 686
E-mail claims, 775
Emergency escalation notification processes, 156
Empty root domain, 47
Encrypting file system (EFS), 13, 526, 661, 665, 670
Encryption, 7–8, 12, 661
Enforcement object, 537
Enterprise Admins group, 51
  AD DS structure and, 159, 162–163, 166
  database mounting tool and, 609
  domain controller removal and, 242
  domain controller security and, 316
  domain creation and, 221
  forest trust creation and, 267–268
  in new domains, 373
  migration and, 256
Enterprise Certification Authorities (CA), 130, 294, 668–669, 673, 701
Enterprise directory store, 15, 621
Enterprise PKI MMC snap-in, 12, 664–665, 702
Enterprise Trust settings, 527
Errors, 133, 138–139. *See also* Troubleshooting
Escalation, emergency, 156
European Union Data Protection Directive (EUDPD), 148
Event logs
  for security hardening, 533
  for troubleshooting Kerberos, 298
  of super users, 740
  policy settings for, 309–310
  settings for, 352
Event trace data, 559–560
Event Viewer
  AD DS installation and, 235
  delegating administration and, 348
  for monitoring, 569–570
  Group Policy and, 451

  - in AD LDS, 624
  - migration and, 256–257
  - replication and, 56, 133
- Everyone group, 464
- Exchange Management Shell, 394, 396
- Exchange Server 2007, 16, 204–214
  - Adamsync synchronization and, 654–655
  - DNS and, 92, 206–207
  - documenting implementation of, 154
  - domain controller location and, 208–209
  - Domain Name System and, 63
  - forest boundaries and, 158
  - global catalog server location and, 209–210
  - ldf files and, 655
  - operations master server locations and, 213–214
  - overview of, 204–206
  - read-only domain controller design and, 210–213
  - schema modification and, 35
  - sites and, 56, 199
- Exclusion policies, RMS, 738–739
- Extended Key Usage (EKU) extension, 698
- Extensible Markup Language (XML), 747
- Extensible Storage Engine (ESE), 22, 623
- Extensible storage engine transaction (ESENT) log files, 218
- Extension activation, 487
- External Certification Authorities (CA), 666
- External trusts, 54–55, 165
- Extranet authentication store, 621

F

- Fast Logon Optimization feature, 414
- Federal Privacy Act (Australia), 147
- Federation Service Proxy, 14–15
- Federation Services, 167, 621, 745–791
  - account partner configuration in, 773–781
    - account store in, 776–777
    - claims extractions in, 778
    - organization claims in, 775–776
    - outgoing claims mappings in, 780–781
    - resource partner in, 778–780
    - trust policy in, 773–774
  - best practices for, 790
  - components of, 749–752
  - deployment scenarios for, 752–759
    - federation Web single sign-on (SSO), 753, 755–757
    - federation Web single sign-on (SSO) with forest trust, 753, 757–759
    - Web single sign-on (SSO), 752–755
  - identity federation and, 746–747
  - implementation as federation Web single sign-on (SSO) with forest trust, 788–790
  - implementation as federation Web SSO implementation, 766–773
    - installing federation proxy servers in, 771–772
    - installing federation servers in, 769–771
    - overview of, 766–769
  - implementation requirements for, 759–766
    - account store, 761–762
    - client Web browser, 760–761
    - network, 760
    - PKI (public key infrastructure), 762–766
    - Web server, 762
  - overview of, 13–15
  - resource partner components in, 781–785
  - rights management integration with, 17
  - RMS and, 716, 731–733
  - Web services in, 747–749
  - Windows NT token-based applications and, 785–787
- File extension activation, 487, 496–497
- File junctions, 407
- File Replication Service (FRS), 106, 137, 571, 610
- Filtered attribute set, RODC, 4
- Filtering, 55
  - of security identifier (SID), 170–171
  - of User Principal Name (UPN) suffix, 171
  - replication and, 129
  - security, 432–434, 451–452
  - Windows Management Instrumentation (WMI) and, 428, 434–435
- Financial Modernization Act (USA), 147
- Find command, 11
- Fine-grained password policies, 7–8, 527–532
  - domain functional level and, 182
  - domain number and, 175
  - implementing, 528–531
  - overview of, 7
  - planning for, 528
  - resultant PSOs in, 531–532
  - resultant set of policy for, 8
  - security policy boundaries and, 47
  - storing, 7–8

Firewalls
  authentication, 169
  configuring, 304
  documenting, 151
  forwarders and, 188
  Kerberos authentication ports and, 297
  replication and, 129
Flags
  DsGetDcName values for, 69–70
  for GPO state, 406
  Kerberos ticket, 286–287
  named control, 275
Folder redirection, 469–477
  computer startup and, 416
  configuring, 470–474
  Group Policy implementation and, 439
  Group Policy object copying and, 441
  Group Policy processing order and, 428
  Group Policy settings for, 60, 400, 475–477
  offline files for, 459, 474–475
  synchronous Group Policy processing and, 413, 415
Foreign Security Principals container, 235
Forest root domains
  as AD DS components, 47, 54
  creating, 221, 226
  distribution of, 209
  Domain Name System and, 88
  in verifying installation, 235
  structure of, 176–177
Forest trusts, 54–55
ForestDnsZones
  creation of, 45
  Domain Name System and, 68, 76, 78–79
  in verifying installation, 235
  overview of, 5
Forests. *See also* Interforest migration; also Intraforest migration
  cross-reference objects and, 29
  data store and, 20
  default tombstone lifetime for, 590
  design of, 156–167
    change control policies in, 167
    for security, 161–163
    integration of multiple, 167–172
    models of, 163–166
    overview of, 158–159
    ownership of, 166
    single or multiple, 159–161
  federated trust between, 14
  federation Web single sign-on (SSO) with forest trust and, 753, 757–759
  federation Web single sign-on (SSO) with forest trust implementation and, 788–790
  functional levels of, 4, 153, 183–184, 228–229, 231, 602
  Group Policy implementation for, 438–439
  in AD DS, 50–51
  monitoring of, 571
  Windows Server 2008 upgrade of, 255–256
Forward linked attributes, 98, 105
Forward Lookup Zones page, 235
Forwardable Kerberos ticket flag, 286
Forwarded events, 569
Forwarded Kerberos ticket flag, 287, 289
Forwarders, 83–86, 152, 188, 232
Forward links, 602
FSMO (flexible single-master operation) roles, 20, 28, 241, 243, 602, 612
FSMOCheck test, 55
fSMORoleOwner attribute, 29–31, 61
Fully qualified domain name (FQDN), 89, 227, 290
Functional service requirements in AD DS, 146

G

Garbage collection, for maintenance, 105, 575–576
gc SRV record, 67
gc. msdcs.DnsForestName record, 69
Global Address List (GAL), 21, 158, 204, 362
Global audit policy, 6
Global catalog
  common forest, 50
  contact objects and, 364
  disaster recovery and, 610–614
  gc SRV record for, 67
  in forest design, 158
  monitoring of, 571
  partition for, 44
  replication of, 118–119
  universal group membership lists in, 369
Global Catalog LDAP, 298
Global catalog servers, 10, 20
  authoritative restore of, 603
  data store and, 20
  documenting, 153
  Exchange Server 2007 and, 204–205
  first domain controller as, 232

  - forced domain controller removal and, 243
  - in AD DS, 23–25, 199, 218
  - in single domain, 174
  - infrastructure operations masters and, 214
  - location of, 209–210
  - restoring, 593, 614
- Global groups, 369
- Global security group membership, 8
- Globally Unique Identifiers (GUIDs)
  - client-side extensions (CSEs) and, 411–413
  - Domain Name System and, 68
  - for Group Policy container (GPC), 406
  - of deleted objects, 575
  - PSOs and, 531
  - replication and, 101–104
- GMPC
  - GPOs created and linked by, 426–427
  - overview of, 424–425
- GPLogView.msi script, 452
- GPMC (Group Policy Management Console), 404, 702
  - description of, 423
  - global audit policy enabled by, 6
  - GPO creation and linking by, 426–427
  - overview of, 424–425
- GPMCSampleScripts.msi, 447–450
- Gpresult.exe tool, 445–446
- GPU command-line tool, 489
- Gpupdate command-line tool, 418–419
- Gramm-Leach-Bliley Act (USA), 147
- Graphic Identification and Authentication (GINA) dynamic-link library (DLL), 276
- Graphical utilities, 386
- “Green field” environments, 247
- Group claims, 775
- Group claims extractions, 778
- Group nesting, 181
- Group Policy, 399–454. *See also* Security, Group Policy for
  - Automatic Certificate Request Service (ACRS) and, 690
  - certificate-related settings in, 13
  - components of, 405–409
  - computer objects and, 378
  - documenting, 153
  - domain number and, 174–175
  - domain-level, 181
  - for authentication protocols acceptance, 302
  - for certificate acceptance, 692–693
  - for DNS Locator records, 211
  - for DNS registration, 73–74
  - for domain controller security, 306–307
  - for printers, 380–382, 384
  - implementing, 423–439
    - between domains and forests, 438–439
    - GMPC overview in, 424–425
    - GMPC to create and link GPOs in, 426–427
    - GPO administration in, 436–438
    - GPO processing scope in, 427–436
    - planning, 450–451
  - Kerberos policy settings and, 291–292
  - management of, 326
  - objects of, 439–446
    - backing up and restoring, 439–440
    - copying, 441
    - default domain, 526–527
    - importing settings for, 441
    - modeling and reporting, 442–446
  - organizational units and, 59, 192–195, 197
  - overview of, 400–405
  - processing of, 409–423
    - background GPO refreshes and, 415–416
    - client GPO, 410–413
    - initial GPO, 413–415
    - interval times for background, 418–423
  - registry settings deployed through, 737
  - scripting management of, 447–450
  - SCW policy and, 306
  - setting types for, 60
  - SYSVOL directory and, 106
  - troubleshooting, 451–453
  - trusted root certificate distribution by, 666
- Group Policy containers (GPCs), 405–407, 457–458
- Group Policy Creator Owners group, 436
- Group Policy for user desktops, 428, 432, 455–511
  - administrative templates and, 477–484
    - best practices for, 482–484
  - domain-based, 481–482
    - overview of, 478–481
  - folder redirection and, 469–477
    - configuring, 470–474
    - Group Policy settings for, 475–477
    - offline files for, 474–475
  - individualized versus centralized control of, 456
  - overview of, 456–458

- preferences in, 503–510
  - in Control Panel settings, 506–507
  - in Windows settings, 504–505
  - options for, 507–510
  - settings versus, 503–504
- scripts and, 484–485
- software deployment and, 485–503
  - application, 486–489
  - file extension activation configuration for, 496–497
  - limitations to, 501–503
  - network bandwidth and, 489–490
  - non-Windows Installer, 490–491
  - package property configuration for, 491–496
  - planning, 500–501
  - removing, 497–498
  - Windows Installer technology for, 485–486, 498–500
- user profiles and, 459–469
  - in Windows versions, 461
  - junction points and, 461–462
  - local, 463
  - mandatory and super mandatory, 465–466
  - overview of, 459–460
  - roaming, 463–469

Group Policy Management Console. *See* GPMC (Group Policy Management Console)
Group Policy Management Editor, 307
Group Policy Modeling Wizard, 424, 437, 442
Group Policy Object Editor, 383–384
Group Policy Results Wizard, 425
Groups
- AD LDS default, 635
- best practices for, 396
- for object management, 366–377
  - default, 371–373
  - scope of, 367–371
  - security, 374–377
  - special identities for, 373–374
  - types of, 366–367
- nested, 181, 368–369
- primary, 274–275, 328
- resource, 787
- restoring, 601–605
- restricted, 423, 534
- special identities for, 235
- tombstone reanimation and, 605

Group-to-UPN mapping, 787

H

Hard disk space, AD DS installation and, 218–219
Hardening, security. *See* Security, Group Policy for
Hardware Security Module (HSM), 673
Hash values, 4, 518, 535, 537
Health Insurance Portability and Accountability Act (HIPAA) of 1996 (USA), 147
High-watermark values, 99, 101–103
HTTP, 747
Hub Transport server role, 205
HW Auth Kerberos ticket flag, 287

I

Identifier authority, in SID, 272–273
Identity claims, 775, 779, 782
Identity federation, 746–747
Identity Integration Feature Pack, 172
id-kp-PCSPSigning enhanced key usage, 679
id-pkix-ocsp-nocheck extension, 679
IEEE 802.11 standard, 541
IEEE 802.3 standard, 538–540
Import-Csv cmdlet, 394
Incoming claims mappings, 783–785
Indexing
- Extensible Storage Engine (ESE) for, 22
- for searching, 35–36
- in AD LDS, 623

inetOrgPerson object, 182, 363–364
Infrastructure operations masters, 31, 214
- global catalog server versus, 32
- migration and, 256
- phantom objects and, 602
- restore of, 612–613
- tools for, 32

Inheritance, 34, 336–339
Initial Configuration Tasks Wizard, 222–223
Initial Kerberos ticket flag, 287
Install from media (IFM) feature
- disaster recovery and, 588, 592
- for AD DS, 217, 224, 237–238

Installation, blocking, 401
Installing AD DS, 217–246
- options for, 222–225
- prerequisites for, 217–222
  - administrative permissions, 220–221
  - Domain Name System (DNS), 220
  - hard disk space, 218–219
  - network connectivity, 219–220
  - operating system compatibility, 221–222

- read-only domain controller deployment in, 238–239
- removing AD DS and, 240–244
- tools for, 246
- unattended, 236–238
- wizard for, 225–236
  - completing installation and, 234–235
  - deployment configuration and, 226–227
  - domain controller options and, 232–233
  - file locations and, 233–234
  - fully qualified domain name and, 227
  - verifying installation and, 235–236
  - Windows Server 2008 functional levels and, 228–232

Instances
- authoritatively restoring AD LDS
- backing up AD LDS, 651–652
- in AD LDS, 620, 623–624, 640–643
- restoring AD LDS

Integrated authentication, 291, 638

Integrated zones, of AD DS, 74–81
- benefits of, 75
- default application partitions for, 76–77
- managing, 78–81

Interfaces
- data store and, 21
- for AD LDS, 622
- for schema modifying, 36
- new features in, 10–11
- resultant PSOs and, 531
- Security Configuration Wizard (SCW) user, 304
- Security Support Provider (SSPI), 277

Interforest migration, 257–265
  - Active Directory migration tool for, 259–260
  - auditing in, 260
  - computer accounts in, 263–265
  - decommissioning source domains in, 265
  - global and domain local group accounts in, 260–261
  - migration account creation in, 259
  - pristine forest creation in, 258
  - service accounts in, 262–263
  - trust configuration for, 266–268
  - trust creation in, 259
  - user accounts in, 261–262

Interforest trusts, 167–171

Internal Certification Authorities (CA), 666, 670, 765, 767

International Organization for Standardization (ISO), 39, 362, 482

International Telecommunications Union (ITU), 362

Internationalized domain names, 228

Internet Explorer, 17, 401, 421

Internet Information Services (IIS), 17, 279, 295, 304

Internet name resolution, 188

Internet Protocol (IP), 109, 111, 219–220, 298

Internet Protocol (IP) subnets, 55, 123, 151, 199–201

Internet Protocol Security (IPsec), 13, 538, 541–543

Internet, RMS deployment over, 714

Inter-realm session keys, 287

Intersite replication, 122–132
- additional sites and, 123–124
- bridgehead servers in, 130–132
- compression and, 127
- in AD LDS, 630
- intersite messaging for, 111
- notification of, 127
- overview of, 108–109
- site link bridges and, 128–129
- site links and, 124–128
- topology generation for, 119–120
- transport protocols for, 129–130
- troubleshooting, 136

Inter-Site Topology Generator (ISTG), 119–120, 125, 130, 134, 206–207, 630

Inter-Site Transport container, 128

Interval, replication, 126

Intraforest migration, 257, 259, 265–266

Intranets, RMS deployment in, 713

Intrasite replication, 106–108, 114–117, 630

Invalid Kerberos ticket flag, 287

IPconfig.exe tool, 93

IPv4 address, 68, 71

IPv6 address, 68, 71

isDeleted attribute, 104

isMemberOfPartialAttributeSet attribute, 23

Isolation, administrative, 162–163, 165, 214

Issuance policies, for certificates, 699

J

Japan's Personal Information Protection Act, 148

JScript, 390, 447

Junction points, user profiles and, 461–462

K

Kccevent test, 55
Kerberos authentication
  access tokens and, 276
  Advanced Encryption Services (AES) for, 182
  as best practice, 319
  domain number and, 175
  dynamic updates based on, 90
  in AD LDS, 638
  password resetting and, 377
  security policy boundaries and, 47
  Security Support Provider (SSP) for, 277
  SRV record example for, 67
Kerberos password-change servers, 67
Kerberos security, 278–301
  authentication delegation in, 289–291
  authentication in, 281–288
  configuring, 291–292
  for AD LDS replication, 632–633
  interoperability of, 296–297
  overview of, 278–280
  policy for, 517
  public key infrastructure integration with, 292–295
  smart card integration with, 295–296
  troubleshooting, 297–301, 320–321
  user principal names in, 775
Kerberos ticket flags, 286–287
Kerberos Token Size tool, 321
Kerberos Tray tool, 286, 320
Key Distribution Center (KDC)
  description of, 279
  encryption and, 282
  in authorization process, 277
  Kerberos SRV identification of, 67
  PAC data from, 299
  password resetting and, 377
  shared secrets management by, 279–280
Key performance indicators (KPIs), 561
Key recovery agents (KRAs), 682, 685
Keys, archival and recovery of, 681–685
KList.exe tool, 286, 320
Knowledge Consistency Checker (KCC)
  AD LDS and, 630
  branch office locations and, 206
  connection objects created by, 106, 113, 120
  CPU utilization by, 572
  description of, 112
  domain functional level and, 182
  in troubleshooting replication, 134
  Kccevent test for, 55
  site link costs and, 127, 202
  topology test for, 55
kpassword SRV record, 67
krbtgt accounts, 4, 26, 212, 280
Ksetup.exe tool, 296, 321
Ktpass.exe tool, 321

L

LAN Manager (LM) authentication, 301–303
LanMan, 304
Last Interactive Logon Information, 182, 361
Last write time, 103–104
Latency, 107, 109–110, 127, 151, 574
LDAP directory interchange format (LDIF), 387
LDAP query groups, 366–367
LdapDisplayName attribute, 40
Ldf files, 626–627, 655
LDIF files, 603, 642
LDIFDE command-line utility
  for managing objects, 358, 387–389, 396
  for PSOs, 529
  in disaster recovery, 616
Ldp.exe tool, 43, 76, 101
  access control entries view by, 329, 334–336
  AD database mounting tool and, 609
  for managing objects, 395, 397
  in AD LDS, 636–637, 644–645, 647, 658
  in disaster recovery, 606, 616
Legacy applications, migrating, 16
Legal service requirements in AD DS, 147–148
Licenses, RMS, 711
Licensing-only clusters, RMS, 707
Life cycle management, of software, 485
Lifetime, tombstone, 105
Lightweight Directory Access Protocol (LDAP). *See also* Active Directory Lightweight Directory Services (AD LDS)
  Active Directory Domain Services and, 43
  Data Interchange Format Directory Exchange (LDIFDE) tool of, 36, 38
  database mounting tool and, 9, 607
  domain attack surface reduction and, 304
  domain controller security options and, 525
  Federation Services and, 15

  - in installing AD DS, 217
  - inetOrgPerson object and, 363
  - interface of, 21
  - ports for, 298
  - referral response of, 4
  - SRV record example for, 65, 67
- Linked attributes, 98, 105
- Linked-value replication, 369–370, 602–603
- Link-local IPv6 Address, 68, 71
- Links
  - as bridges to sites, 128–129
  - group membership and, 602
  - Group Policy Management Console for, 426–427
  - Group Policy object order of, 428–429
  - of Password Settings objects (PSOs), 8
  - site, 124–128
  - speed of, 151
  - to GPOs., 426–427
  - to Internet Protocol (IP) subnets, 199
- Linux, 247
- ListADDSDomains.ps1 script, 51
- ListADDSSites.ps1 script, 55, 124
- ListADDSSites.xlsx job aid, 124
- ListAppPartitions.ps1 script, 77
- ListDomainControllers.ps1 script, 28
- ListFSMOs.ps1 script, 31
- LMHosts files, 63
- Load balancing, 65, 134, 205, 651
- Local area networks (LANs), 55
- Local Group Policy object (LGPO), 402, 405
- Local policies, 518–519
- Local Security Authority (LSA), 110, 276–277, 287, 289, 320
- Local System Authority (LSA) account, 262
- Local user profiles, 463, 467, 471
- Logging
  - circular, 584, 587
  - CryptoAPI 2.0 diagnostic, 663–664
  - debug, 90
  - directory service auditing and, 6
  - Group Policy, 404
  - resultant set of policy (RSoP) mode for, 442
  - transactions, 579–580, 586–587
- Logon Locally permissions, 59
- Logon time stamp, 182
- Lookup errors, DNS, 139
- Loopback processing, 422–423, 453
- Loosely consistent replication, 96

M

- Machine Certificate, 710–711
- Mailbox server, 205
- Maintenance, 575–580
  - garbage collection for, 575–576
  - Ntdsutil.exe for, 578–580
  - of group memberships, 602
  - offline defragmentation for, 577–578
  - online defragmentation for, 576–577
- Management tools for AD DS, 11
- Mandatory attributes, 358
- Mandatory user profiles, 459, 465–466
- Mapping
  - certificates, 294–295
  - drives to shared folders, 385
  - group-to-UPN, 787
  - incoming claims, 783–785
  - many-to-one, of certificates, 294
  - outgoing claims, 780–781
  - ports, 129
- Massachusetts Institute of Technology (MIT), 278
- Mathematical hash, in digital signatures, 293
- May postdate Kerberos ticket flag, 287
- mayContain attributes, 33
- Memory allocation errors, 299
- Message routing topology, 56
- Messaging API (MAPI), 21
- Messaging, intersite, 111
- Metadirectory, 621
- Microsoft Download Center, 404
- Microsoft Identify Lifecycle Manager (ILM), 787
- Microsoft Identity Integration Server 2003 (MIIS), 172, 364, 621
- Microsoft Identity Lifecycle Manager 2007 (ILM), 172, 364, 621
- Microsoft Management Console (MMC), 15, 239, 352–354, 393
- Microsoft Office, RMS and, 723–726
- Microsoft Root Certificate Program, 666
- Microsoft Simple Certificate Enrollment Protocol, 671
- Microsoft System Center Operations Manager, 351–352
- Microsoft Systems Management Server (SMS), 501
- Migrating to AD DS, 247–270
  - best practices for, 269
  - domain restructuring in, 250–252
  - domain upgrading in, 249–250, 254–257
  - interforest, 257–265
  - Active Directory migration tool for, 259–260

  auditing in, 260
  computer accounts in, 263–265
  decommissioning source domains in, 265
  global and domain local group accounts in, 260–261
  migration account creation in, 259
  pristine forest creation in, 258
  service accounts in, 262–263
  trust configuration for, 266–268
  trust creation in, 259
  user accounts in, 261–262
  intraforest, 265–266
  legacy applications, 16
  overview of, 248–249
  path determination in, 252–254
  tools for, 270
Migration paths, 175
Mixed operating systems environment, 483–484
Mobile users, as security risk, 148. *See also* Roaming user profiles
Mobile-based Messaging API (MAPI), 205
Modeling, Group Policy, 424, 442–443
Monitoring, 551–574
  overview of, 551–552
  process of, 561–570
    baselines and thresholds in, 562–563
    Event Viewer in, 569–570
    overview of, 561–562
    performance counters and thresholds in, 563–569
  reasons for, 553–554
  servers, 554–561
    data collector sets and reports for, 559–561
    Performance Monitor for, 555–557
    Reliability Monitor for, 557–559
    Resource Monitor for, 555
  what to include in, 571–574
Moving, in migration, 250
msDS-AuthenticatedToAccountList attribute, 26
msDS-DnsRootAlias attribute, 29
msDS-NeverRevealGroup attribute, 26
msDS-RevealedList attribute, 26
msDS-Reveal-OnDemandGroup attribute, 26
msDS-UpdateScript attribute, 29
Msgina.dll, 276
MSI installer package, 557
Multimaster DNS server configuration, 75
Multimaster replication, 22, 28, 96–97, 106, 629
mustContain attributes, 33
Mutual authentication, 278, 284

N

Named control flags, 275
Names
  anonymous SID-Name translation for, 518
  attribute of, 98
  cache for, 298
  common name claims and, 775–776
  default display, 362, 364
  Default-First-Site, 56–57
  display, 361
  distinguished, 43, 50, 575
  distinguished name tag (DNT) for, 602
  documenting resolution infrastructure of, 152
  domain, 29–30
  fully qualified domain, 227, 290
  in renaming domains, 180, 182
  NetBIOS, 63–64, 290
  of AD LDS directory partitions, 628
  of Certification Authorities, 671
  of user objects, 361–362
  RFC 2822-style e-mail, 775
  servers for, 5
  service principal (SPN), 283, 285, 300–301, 321
  subject name of certificates, 698–699
  Universal Naming Convention (UNC) for, 380, 384
  User Principal (UPN), 171, 283, 295, 362–363, 395, 775, 779
  Windows Internet Naming Service (WINS) server and, 220
  X.500 OID structure for, 39
Namespaces, Domain Name System (DNS), 81–91
  delegation in, 82–83
  Distributed File System (DFS) and, 385
  domain number and, 175
  forwarders in, 83–86
  internal and external, 184–188
  root hints in, 86
  stub zones in, 86–88
  troubleshooting, 88–91
Naming context heads, 573
ncName attribute, 50
Negotiated authentication, 291, 638
Nested groups, 181, 368–369
NetBIOS names, 63–64, 290

NetDom command-line tool, 377, 396, 599
NETLOGON
  service for, 111
  shared folder for, 106
  troubleshooting, 136
  user profiles in, 463–465
Network Access Protection (NAP), 538, 541
Network connectivity
  Federation Services requirements for, 760
  for installing AD DS, 219–220
  in Group Policy troubleshooting, 453
  troubleshooting, 133
Network Device Enrollment Service (NDES), 12, 695
Network List Manager policies, 538
Network Location Awareness service (NlaSvc), 404, 419–420
Network Monitor, 90, 93, 246, 299
Network perimeter, 14
Network security, Group Policy for, 537–543
  for Windows firewall and IPsec, 541–543
  settings for, 518, 538
  wired, 538–540
  wireless, 541
Network Service account, 642, 657
Network Zones, 536
New Trust Wizard, 171, 267, 297
Nltest.exe tool, 94
Nonauthoritative restore of Active Directory, 591, 595–599
Non-dedicated root domain, 47
Non-Domain Naming Context (NDNC), 44
Nonobject access control entries, 275
Nontechnical constraints, 152
Nontransitive external trusts, 54
North American Industry Classification System, 748
Notification of intersite replication, 127
Novell Directory Services, 247
Nslookup.exe tool, 89, 94, 139, 298
Ntbackup.exe tool, 587
NTDS database, 219
NTDS Settings, 112, 135, 242
Ntds.dit file, 218, 585
Ntdsai.dll, 22
Ntdsdbutil.exe tool, 651
Ntdsutil.exe tool
  AD DS components and, 30, 61
  for AD snapshots, 608
  in AD DS installation, 237
  in disaster recovery, 593–595, 600–601, 616
  in maintenance, 578–580
  install from media (IFM) feature and, 588, 592
  linked value replication and, 602–603
  overview of, 9
NTLM (NT LAN Manager) authentication
  disaster recovery and, 599
  for security, 277–278, 301–303
  in AD LDS, 638
NTLM version 1 authentication, 302
NTLM version 2 authentication, 302

O

Object access control entries, 275
Object identification model, LDAP as, 43
Object-based persistent usage policy, 16
Objects
  ActiveX Data (ADO), 390
  administrative access to, 327–329
  Adsiedit.msc tool for, 395
  as originating updates, 97–98
  attributeSchema, 33
  auditing changes in, 350
  Binary Large (BLOB), 684–685
  classSchema, 33
  client Group Policy, 410–413
  computer, 263
  configuring auditing of, 351–352
  connection, 112–115
  cross-reference, 29, 242
  deactivating schema, 40–41
  default domain Group Policy, 526–527
  deletion of, 104–105, 589
  Designated File Types, 537
  dynamicObject class for, 182
  enforcement, 537
  Group Policy, 60, 153
    managing, 439–446
    processing scope of, 427–436
  inetOrgPerson, 182
  initial Group Policy, 413–415
  Ldp.exe tool for, 395
  Local Group Policy (LGPO), 402, 405
  locating in other domains, 49–50
  NTDS Settings, 242
  organizational units to administer, 59–60
  ownership quotas for, 318
  packet replication of, 108
  Password Setting, 528

  permissions in, 329–348
    effective, 340–343
    inheritance of, 336–339
    ownership of, 343–348
    special, 331–336
    standard, 329–331
  phantom, 602
  PowerShell scripts and, 392–394
  resultant password settings (PSOs), 531–532
  rootDSE, 628–629, 643
  Security Descriptors of, 328
  security principal, 272
  site link, 124
  tombstone, 589–590, 605–607, 614
  Trusted Publishers, 537
  VBScript and, 391–392
  X.{five hundred}500 object IDs for, 39–40
Objects, managing, 357–398
  automating, 386–395
    command-line tools for, 386–387
    LDIFDE and CSVDE for, 387–389
    VBScript for, 389–395
  best practices for, 395–396
  computer, 377–379
  contact, 364–365
  groups for, 366–377
    default, 371–373
    scope of, 367–371
    security, 374–377
    special identities for, 373–374
    types of, 366–367
  inetOrgPerson, 363–364
  printer, 379–384
  published shared folder, 384–385
  service accounts and, 365
  tools for, 397
  user, 358–363
Office SharePoint Server 2007, 15, 705
Offline Certification Authorities, 669
Offline files, for folder redirection, 459, 474–475
Offline root certification authorities, 701
OK As Delegate Kerberos ticket flag, 287
One-to-one mapping of certificates, 294
One-way forest trusts, 165
One-way trusts, 168, 268
Online Certification Status Protocol (OCSP), 12, 671, 678–680, 700
Online Responder service, 12–13, 678–681, 701–702
Operating system, performance counters for, 567–569
Operations masters, 28–31
  common forest, 51
  disaster recovery and, 610–614
  domain naming, 29–30
  flexible single, 20, 28
  infrastructure, 31, 256, 602
  monitoring of, 571
  PDC (primary domain controller) emulator, 30–31
  restoring, 593
  RID (relative ID), 30
  RODCs and, 27
  roles management for, 326
  schema, 29
  server locations for, 213–214
  single point of failure and, 96
  transferring roles of, 32
Organization claims, 781
Organizational administrative model, 155
Organizational forest model, 164–165
Organizational Units (OUs), 192–197. *See also* Administration, delegating
  administrative autonomy and, 252
  authoritative restore for, 599
  designing, 193–195
  documenting, 153
  domain top-level structure for, 181
  Group Policy and, 436
  in AD DS, 57–60
  in PowerShell scripts, 43
  lockdown and, 423
  password policies and, 7
  security templates deployed to, 545
  structure overview of, 192–193
Originating server, 103
Originating updates, 97, 102
Orphaned objects, 338
OU Admins group, 162
Outgoing claims mapping, 780–781
Outlook clients, 204–205
Ownership
  in security descriptors, 274–275
  object quotas for, 318
  of domain structure, 180–181
  of forest design, 166
  of groups, 375

  - of permissions, 343–348
  - of services and data, 161–162

P

- Parent containers, 98
- Parent-child domain configuration, 48
- Parent-child trust, 179
- Partial attribute set (PAS), 23
- Partitions
  - application directory, 29, 116, 240
  - configuration directory, 29, 50, 158
  - cross-reference objects and, 50
  - default application, 76–77
  - DNS application, 78–79
  - domain controller integration with, 163
  - in AD DS, 42–46
  - in AD LDS, 624–629, 640–643
  - multiple logical, in AD DS, 96
  - read-only, 3
  - redundant rings based on, 114
  - replication of configuration, 135
- Passport authentication, 279
- Password Export Server (PES), 262
- Password Replication Policies, 5
- designing, 212–213
  - for RODCs, 10–11, 26–27, 224, 239
- Password Settings Containers (PSCs), 7, 528
- Password Settings Objects (PSOs), 7
  - attributes of, 8
  - resultant, 528, 531–532
  - resultant set of policy (RSOP) and, 8
- Passwords
  - cluster key, 717, 740–741
  - complex policy for, 319
  - custom filters for, 516
  - disaster recovery resetting of, 596, 599
  - domain number and, 175
  - fine-grained, 7–8
    - overview of, 7
    - resultant set of policy for, 8
    - storing, 7–8
  - for Directory Services Restore Mode (DSRM), 234
  - for krbtgt account, 280
  - for SYSKey, 315–316
  - in AD LDS, 638, 657
  - Kerberos password-change servers and, 67
  - LAN Manager (LM) hash values for, 302
  - migration and, 262, 265
  - PDC (primary domain controller) emulator operations master and, 31, 111
  - permission to reset, 345
  - policy for, 514–515
  - read-only domain controllers and, 3
  - resetting, 377
  - security policy boundaries and, 47
  - split, 317
  - storing, 4
  - uninstalling AD DS and, 241
  - urgent replication and, 110
- Path rules, software restriction policies and, 535–536
- Patriot Act of 2001 (USA), 147
- PDC (primary domain controller) emulator operations masters
  - description of, 30–31
  - disaster recovery and, 594
  - domain-based template file storage on, 481
  - Group Policy Management Console and, 425
  - location of, 213
  - passwords and, 111
  - restore of, 612
  - tools for, 32
- Peer domains, 48
- Performance. *See also* Monitoring
  - counters and thresholds for, 559, 561, 563–569
  - service level agreements (SLAs) for, 147
- Performance Monitor, 56, 551, 555–557
- Perimeter networks
  - AD LDS in, 654
  - as security risk, 148
  - forest deployment in, 159
  - in business-to-employee (B2E) identity federation scenario, 747
  - Windows NT token-based application in, 757
- Period Group Policy, 414
- Permissions, 329–348
  - access tokens and, 276
  - administrative, 27
  - Allowed to Authenticate, 170
  - application directory partitions and, 46
  - delegating, 194
  - documenting, 153
  - Domain Admins group and, 375
  - domain number and, 175
  - effective, 340–343, 355
  - for delegation record creation, 83

  for domain controllers, 28–29
  for installing AD DS, 220–221
  for restricted data, 16
  in access control lists, 274
  in AD LDS, 635–636
  in folder redirection, 472–473
  in forest root domain, 51
  inheritance of, 336–339
  Logon Locally, 59
  migration and, 252, 259
  named control flags and, 275
  of security principals, 272
  ownership of, 343–348
  principal of least privilege for, 317, 319, 395
  Rights Management Service (RMS) and, 723–726
  RODC administrative, 211
  special, 331–336
  standard, 329–331
Persistent usage policy, object-based, 16
Personal identification number (PIN), 670
Personal Information Protection and Electronic Documents Act, The (Canada), 147
Phantom objects, 602
PIN (personal identification number), 295
Ping utility, 219
PKI (public key infrastructure), 12
  cross-certification hierarchy and, 696
  Federation Services requirements for, 762–766
  in AD FS applications, 782
  in Certificate Services (CS), 661–667
  in security, 292–295
  policy settings for, 538
PKIView, 12
Planning mode, for RSoP, 442
Policy-based Quality of Service (QoS), 400
PolicyDefinitions folder, 482
Portals, 621
Portquery tool, 298
Ports, 129, 297–298
POSIX (Portable Operating System Interface for UNIX) subsystem, 274, 328
Power management, 401, 534
Power users group, 7
PowerShell scripts
  best practices for, 396
  DisplayADLDSInstances.ps1, 629
  Exchange Management Shell from, 394–395
  ListADDSDomains.ps1, 51
  ListADDSSites.ps1, 55, 124
  ListAppPartitions.ps1, 77
  ListDomainControllers.ps1, 28
  ListFSMOs.ps1, 31
  object management by, 392–394
  organizational unit references in, 43
Precedence, of Password Settings objects (PSOs), 8
Preferences, Group Policy and, 401, 405
  in Control Panel settings, 506–507
  in server security hardening, 534
  in Windows settings, 504–505
  logon scripts versus, 485
  options for, 507–510
  settings versus, 503–504
Preferred DNS server setting, 232
Primary domain controller (PDC) emulator. *See* PDC (primary domain controller) emulator operations masters
Primary groups, 274–275, 328
Principal of least privileges, 317
Printers
  Group Policy for, 401
  objects of, 379–384, 396
Pristine forest, 257–258
Privilege Attribute Certificate (PAC) data, 282, 284, 299
Privileges, 317, 344, 395
Project constraints, 149–150
Projects, organizational units based on, 197
Promotion to domain controller (dcpromo), 217
Propagation dampening, 102–103
Protected named control flags, 275
Proxiable Kerberos ticket flag, 287, 289
Proxy Kerberos ticket flag, 287, 289
Pruning service, on domain controllers, 381
Public Certification Authorities, 765–766
Public key authentication, 278
Public key certificates, 12. *See also* PKI (public key infrastructure)
Publishing
  applications, 487–488
  RMS trusted domains for, 729–731
  shared folder objects, 384–385
Pubprn.vbs script, 380

Q

Quality of Service (QoS), policy-based, 400

R

Read-only domain controllers (RODCs)
  account creation for, 225
  as AD DS components, 25–28
  design of, 210–213
  DNS and, 81
  installing AD DS and, 238–239
  overview of, 3–5
  Password Replication Policy for, 10–11, 26–27, 224
  replication and, 120–122
  SRV records and, 69
  SYSKey settings versus, 316
  unique roles for, 20
  Windows Server 2008 run by, 182
Read-only domain name servers, 5
Realm trusts, 55, 297
Rebooting, 371, 578–579
Redircmp.exe utility, 378
Redundancy
  for root domain, 215
  in disaster recovery planning, 584
  in site links, 126
  replication for, 97, 102
Redundant rings, for domain controllers, 114–116
Registry-based parameter, 60
Regsvr32 Schmmgmt.dll command, 36
Relative distinguished name (RDN), 43
Reliability Monitor, 56, 551, 557–559
Reliability, requisite, 145
Remote Administration exception, 445
Remote Desktop, 318
Remote Differential Compression (RDC), 106
Remote domains, group restoration in, 603–604
Remote procedure calls (RPCs)
  connectivity for, 111
  Domain Name System and, 69, 81
  for password updating, 111
  in AD LDS, 622
  in intrasite replication, 107
  over IP connection, 129
  replication interface and, 21
  RID (relative identifier) operations master and, 214
Remote Server Administrator Tools, 482
Renaming domains, 29, 180, 182
Rendom.exe, 29
Renewable Kerberos ticket flag, 287
Repadmin.exe tool
  as bridgeheads command, 130
  for monitoring, 572–573
  for replication troubleshooting, 140
  in disaster recovery, 616
  in replication, 100, 116, 135–136
Replicated Naming Contexts settings, 116
Replicated updates, 97
Replication, 95–140
  AD LDS security in, 657
  bandwidth for, 199
  best practices for, 137–138
  boundaries for, 46, 50, 172
  compression of, 198
  credentials caching and, 213
  delaying, in installation, 234–235
  design of, 202–204
  directory, 620–621
  Distributed File System, 182
  forced, 599
  GPOs and, 409, 452
  in multiple domains, 175
  in Windows Server 2008, 98–99
  interface for, 21
  intersite, 108–109, 122–132
    additional sites and, 123–124
    bridgehead servers in, 130–132
    site link bridges and, 128–129
    site links and, 124–128
    transport protocols for, 129–130
  intrasite, 106–108
  Kerberos troubleshooting and, 299
  latency of, 109–110
  linked-value, 182, 369–370, 602–603
  management of, 326
  migration and, 256
  model of, 96–97
  monitoring of, 571–574
  multimaster, 22, 28
  network traffic associated with, 10
  of AD LDS, 629–633, 648–650
  of changes, 99–105
    change stamps and conflict resolution in, 103–104
    in high-watermark values, 101–102
    in sequence numbers, 99–101
    in up-to-dateness vectors and propagation dampening, 102–103
    object deletions as, 104–105
  of RODC filtered attributes, 4

- of SYSVOL folder, 105–106, 610
- password, 10
- Password Replication Policy for, 5, 26–27
- performance counters for, 566
- sites and, 56
- synchronization of, 44
- tools for, 139–140
- topology generation for, 111–122
  - components of, 111
  - connection objects for, 112–113
  - global catalog, 118–119
  - intersite, 119–120
  - intrasite, 114–117
  - knowledge consistency checker for, 112
  - RODCs and, 120–122
- troubleshooting, 11, 133–137
  - Active Directory Sites and Services tool for, 134–135
  - Dcdiag.exe tool for, 136–137
  - failures, 133–134
  - Repadmin.exe tool for, 135–136
- unidirectional, 4
- update types for, 97–98
- urgent, 110–111
- zone transfer process versus, 75

Reports, RMS, 741–742

Request for Comments (RFC) 2798-compliance, 363

Resetting
- account lockout settings, 7
- passwords, 345, 377, 596, 599

Resource access boundaries, 47, 173

Resource accounts, 787

Resource domains, 178

Resource forest model, 165, 168

Resource groups, 787

Resource Kit tools, 493

Resource locator service, DNS as, 220

Resource management, 326

Resource Monitor, 555

Resource partner in AD FS
- adding, 783
- configuring, 781–785
- definition of, 750
- federation service configured as, 751
- in Federation Web SSO scenario, 768–769

Resource user accounts, 790

Resources organizational units, 197

Restartable AD DS, 9

Restore Group Policy Object Wizard, 440

Restoring. *See* Backing up and restoring; Disaster recovery

Restricted access forest model, 165–166

Restricted enrollment agent, 12, 670

Restricted Group Policy, 316

Restricted groups, 423, 534

Resultant password settings objects (PSOs), 531–532

Resultant Set of Policy (RSoP), 8, 437, 442, 444

Results, Group Policy, 425, 444–446

Retention methods for archiving logs, 310

Reversible encryption, 7–8

Revision level, in SID, 272–273

Revocation of certificates
- certificate revocation lists (CRLs) for, 667, 672, 701, 764
- configuring, 674–681
- designing, 700
- status of, 12

RFC 2822-style e-mail names, 775

RID (relative identifier) operations masters
- disaster recovery and, 214
- for security, 272–273
- purpose of, 30
- restoring, 613
- RODC limitations and, 27
- tools for, 32
- urgent replication and, 110

Rights
- assignment of, 518–525
- delegating administrative, 59, 181

Rights account certificate (RAC), 710–711

Rights Management Services (RMS), 703–743
- administering, 726–741
  - exclusion policies in, 738–739
  - reports in, 741–742
  - rights policy templates in, 733–738
  - security policies in, 739–741
- trust policies in, 726–733
- certificates in, 709–711
- components of, 706–709
- deployment of, 713–714
- features of, 704–706
- implementing, 714–726
  - clients in, 721–726
  - cluster installation in, 715–720
  - connection point configuration in, 720–721
  - preinstallment considerations for, 714–715
- licenses in, 711
- operations of, 711–713
- overview of, 16–18

Ring topology, 630
Rings, replication, 114–116
Roaming user profiles, 459, 463–469, 693
Roaming, credential, 693–694, 701
Rollback, in disaster recovery, 250
Root Certification Authorities, 671–673, 763
Root cluster, RMS, 706–707
Root domain, 209, 215
Root hints, 86, 188, 232
rootDSE object, 628–629, 643
Routable IP infrastructure, 111
Routers, with port mapping, 129
RSA Algorithm, 686

S

Safe mode, 596
Sarbanes-Oxley Act of 2002 (USA), 147
SASL Bind authentication, 638–639
Scavenging, record, 78, 80
Scheduled tasks, 386
Scheduling replication, 106, 126
Schema
  AD LDS directory partitions for, 626–627
  common forest, 50
  directory partition for, 44
  Display Specifier, 625
  extensible, 620
  global catalog and, 23
  in AD DS, 32–41
    components of, 33–34
    deactivating objects of, 40–41
    modifying, 34–36
    new attributes in, 36–40
  management of, 326
  migration and, 255–256
  of forest domains, 158, 160
  operations masters for, 27, 29, 32, 214, 612–613
Schema Admins global group, 36
Schema Admins group, 51
  AD DS structure and, 159, 162, 166
  domain controller security and, 316
  in new domains, 373
Script Center Script Repository Web site, 28, 124
Scriptomatic.exe, 434
Scripts. *See also* JScript; also PowerShell scripts; also VBScript
  ADSI-based, 574
  client-side extension for, 416
  for Group Policy for user desktops, 484–485
  for Group Policy management, 447–450
  for version numbers, 417
  Group Policy for, 400
  Group Policy settings for, 60
  preferences versus, 485, 503
  synchronous logon, 414
  user management by, 484–485
Scwcmd command-line tool, 305–306
Searching, 35–36, 383–384
Secedit.exe tool, 546
Secure attention sequence (SAS), 276
Secure channel network traffic signing, 221
Secure Hypertext Transfer Protocol (HTTPS) session cookies, 760–761
Secure Sockets Layer (SSL), 624, 641, 661, 670, 761
Secure Sockets Layer-Transport Layer Security (SSL-TLS), 13, 279
Secure wireless networks, 13
Secure-Multipurpose Internet Mail Extensions (S-MIME), 13
Security, 271–321. *See also* Rights Management Services (RMS)
  access control lists for, 273–275
  access tokens for, 276
  administrative delegation and, 341
  administrative practices for, 316–319
  as service requirement in AD DS, 148–149
  authentication for, 276–277
  authorization for, 277–278
  best practices for, 170, 319
  boundaries for, 50
  delegation records and, 83
  digitally signed tokens for, 751
  domain-level policies for, 181
  dynamic DNS and, 79
  event viewer and, 569
  for AD LDS, 632–639
    authentication for, 637–639
    default groups for, 634–635
    permissions for, 635–636
    replication, 632–633, 657
    security principals in, 633–634
  for domain controllers, 199, 221, 303–316
    attack surface decrease as, 303–306
    audit policy settings for, 307–309
    event log policy settings for, 309–310
    options policy settings for, 312–313
    SMB signing for, 314–315

    - SYSKEY configuration for, 315–316
    - user rights assignment policy settings for, 311–312
  - for Rights Management Services (RMS), 739–741
  - for RODCs, 3, 25, 212
  - Foreign Security Principals container and, 235
  - forest design and, 161–163
  - forwarders for, 188
  - group management for, 326
  - Group Policy for, 60, 400
  - groups for, 366–367
  - Hardware Security Module for, 673
  - in Certificate Services deployment, 670
  - in forest root domain, 51
  - integrated zones for, 75
  - issuance, 699
  - Kerberos, 278–301
    - authentication delegation in, 289–291
    - authentication in, 281–288
    - configuring, 291–292
    - interoperability of, 296–297
    - overview of, 278–280
    - public key infrastructure integration with, 292–295
    - smart card integration with, 295–296
    - troubleshooting, 297–301, 320–321
  - NTLM authentication for, 301–303
  - object management and, 374–377
  - object-based persistent usage policy for, 16
  - of internal DNS server, 185–186
  - Password Settings objects (PSOs) and, 8
  - performance counters for, 567
  - physical, 163
  - policy boundaries for, 47, 173
  - policy management for, 326
  - resource user accounts and, 790
  - security principals for, 272–273
  - testing modifications to, 355
  - Version 3 templates for, 686
- Security Accounts Manager (SAM) database, 21, 234, 242
- Security Configuration and Analysis tool, 545–546
- Security Configuration Database, 305
- Security Configuration Wizard (SCW), 304–306, 314, 546–547
- Security Descriptor, 274–275, 328
- Security filtering, 432–434, 451–452
- Security identifiers (SIDs), 163, 327
  - Dcdiag.exe tool for, 573
  - external trusts and, 55
  - filtering of, 170–171
  - history of, 181
  - in migration, 251–252
  - overview of, 272–273
  - RID operations master and, 30
- Security log, 348
- Security principals, 294
  - AD DS migration of, 250
  - domain resource access of, 52
  - forest trusts and, 54
  - in access control, 273
  - organizational units versus, 60
  - overview of, 272–273
  - RID master creation of, 30
  - selective authentication and, 169
- Security Support Provider (SSP), 277
- Security Translation Wizard, 264–265
- Security, Group Policy for, 513–548
  - default domain controllers policy and, 519–525
    - security options for, 525
    - user rights assignment in, 519–525
  - default domain GPOs in, 526–527
  - default domain policy and, 514–519
    - account policies in, 514–518
    - local policies in, 518–519
  - fine-grained password policies in, 527–532
    - implementing, 528–531
    - planning for, 528
    - resultant PSOs in, 531–532
  - hardening server, 532–537
    - preferences in, 534
    - settings for, 533–534
    - software restriction policies in, 535–537
  - network, 537–543
    - for Windows firewall and IPsec, 541–543
    - settings for, 538
    - wired, 538–540
    - wireless, 541
  - templates for, 543–547
- Selected Objects hidden container, 104
- Selective authentication, 165, 168–170, 182
- Self-signed certificates, 766, 790
- Semantic database analysis, 579–580
- Separation, of administrator roles, 5
- Server Core installation, 218, 224, 239
- Server Licensor Certificate (SLC), 710

Server Manager, 12, 16, 223–224
Server message block signing. *See* SMB (server message block) signing
Server Operators group, 163
Servers
  bridgehead, 4
  for Federation Services, 769–771
  for Federation Services proxy, 771–772
  in AD LDS, 622–623
  security hardening for, 532–537
    preferences in, 534
    settings for, 533–534
    software restriction policies in, 535–537
  Web, 762, 769
Server-side extensions (SSEs), of Group Policy, 409
Service Account Migration Wizard, 263
Service accounts, 262–263, 365
Service administrators, 318
Service location (SRV) resource records. *See* SRV (service location) resource records
Service management, 326
Service principal names (SPNs), 21, 283, 285, 300–301, 321
Service proxy, federation, 751–752
Service requirements in AD DS, 144–156
  business, 145–146
  documenting, 150–156
  functional, 146
  legal, 147–148
  project constraints in, 149–150
  security, 148–149
  service level agreements in, 146–147
Services test, 55
Set-ExecutionPolicyRemoteSigned command, 28, 77
Setspn.exe tool, 321
Shadow accounts, 757
Shadow groups, 7
Shared folder objects, 384–385
Shared trust configuration, 51
Shared-secret authentication model, 293, 295
Shortcut trusts, 53, 179–180, 287–288
SIDHistory attribute, 170
Sign-out cookies, 761
Simple LDAP bind authentication, 637–638
Simple Mail Transfer Protocol (SMTP), 21
  domain number and, 175
  replication and, 109, 111, 129–130
  user principal name and, 362
Single point of failure, 96
Single sign-on (SSO) access, 14, 143, 621
Single sign-on deployment. *See* Federation Services
Single-label DNS names, 228
Site-aware applications, 489
Site-aware network services, 56
Sitename parameter, 70
Sites. *See also* Intersite replication; also Intrasite replication
  Active Directory Sites and Services tool for, 61
  AD DS, 55–57
  AD LDS, 650
  automatic coverage of, 72–74, 210
  clients belonging to, 71
  design of, 109
  documenting, 153
  in Group Policy Management Console (GPMC), 424
  link bridges for, 128–129
  links for, 124–128, 202
  replication based in, 630
  SRV resource records and, 67
  topology design of, 197–204
Site-specific service locator (SRV) records, 56
SLAs (service-level agreements), 146–147, 553
Slow link detection policy settings, 419–422, 453, 467–468
Smart cards
  certificates and, 12, 670
  logon for, 13
  security and, 295–296, 317
SMB (server message block) signing
  as best practice, 319
  for domain controller security, 221, 314–315, 525
  migration and, 269
  overview of, 304
Snapshot volume, 9
SOAP (Simple Object Access Protocol) HTTP, 747
Software deployment, 60, 415–416, 485–503
  application, 486–489
  file extension activation configuration for, 496–497
  limitations to, 501–503
  network bandwidth and, 489–490
  non-Windows Installer, 490–491
  package property configuration for, 491–496
  planning, 500–501

  Reliability Monitor for, 557–559
  removing, 497–498
  restriction policies for, 534–537
  Windows Installer technology for, 485–486, 498–500
Source domain controller, 10
Spanning tree, 202
Special identities, for groups, 235
Special permissions, 331–336
SQL Server database, RMS and, 17
SRV (service location) resource records
  authentication and, 56
  DNS and AD DS integration and, 190
  Domain Name System (DNS) and, 64–69, 220
  removing, 242
  site-specific, 210
  troubleshooting, 91
SSL client authentication certificates, 764
SSL server authentication certificates, 764
Stand-alone Certification Authorities, 668–669, 675, 689
Standard Industrial Classification, 748
Standard permissions, 329–331
State-based replication model, 97
Static permissions inheritance model, 336
Store-and-forward replication process, 96–97
Storing fine-grained passwords, 7–8
Strict replication consistency, 108
String attributes, 35
Stub zones, 86–88, 152
Subauthority, in SID, 272–273
Subdomains, delegated, 87
Subject name of certificates, 698–699
Subordinate Certification Authorities, 673
Subtree indexes, 35
Suffix routing, name, 171
Super mandatory user profiles, 465–466
Super users, 739–740
Supernets, 200
Svchost service, 410
Synchronization
  folder redirection and, 475
  identity, 621
  in legacy application migration, 16
  of AD DS and AD LDS, 654–657
  of certificates, 693
  of directories, 172
  of directory service data, 525
  of startup scripts, 485
Synchronous connections, 129
Synchronous logon scripts, 414
Synchronous processing, for GPOs, 413–415
SYSKEY configuration, 315–316
System Access Control Lists (SACLs), 6, 274–275, 309, 328
System Center Configurations Manager (SCCM), 501–502
System Center Operations Manager, 137, 554
System container, 7
System Monitor, 556
System Stability Report, 557–559
systemmayContain attributes, 33
systemmustContain attributes, 33
SYSVOL folder
  ADMX files on, 404
  backing up, 588
  Distributed File System Replication for, 182
  Group Policy container on, 405, 407
  installation of, 219
  replication of, 105–106
  restoring Active Directory and, 610
  storage location for, 233–234
  uninstalling AD DS and, 241
  verifying installation and, 235

T

Tasks
  alert, 559
  delegating administrative, 326–327, 345–346
  scheduled, 386
Technical service requirements in AD DS, 145–146
Templates
  administrative, 60, 477–484
    best practices for, 482–484
    domain-based, 481–482
    in Group Policy, 401, 404–405, 407–409
    overview of, 478–481
  certificate, 681–699
    configuring, 683
    deployment of, 688
    description of, 667
    designing, 697–699
    implementing, 685–689
    MMC snap-in for, 702
    security configuration for, 687–688
    updating, 688–689
  OCSP Response Signing certificate, 679

  rights policy, 733–738
  security, 543–547
  version 3, 686–687
Temporary user profiles, 468
Terminal Services, 521–522
Test environment, 355
Test forest, for schema changes, 36
Thawte certificate authority, 294
Third-party delegation tools, 353
Threshold, of account lockout settings, 7
Ticket-Granting Service (TGS). *See also* Kerberos security; also Kerberos ticket flags
  Exchange protocol for, 284
  Kerberos policy settings for, 292
  responsibility of, 280
  session keys of, 282–283, 287
  troubleshooting, 298
Token-signing certificates, 763, 767, 771, 773
Tokensz.exe tool, 299, 321
Tombstone objects
  best practices for, 614
  lifetime of, 589–590
  maintenance and, 575
  reanimation of, 605–607
  replication and, 104–105
Topology test, 55
Tracking
  printer locations, 383–384, 396
  to control delegation, 346
Transaction logs, 579–580, 586–587
Transform files, 493–494
Transitive site links, 126, 128
Transitive trusts, 49, 158, 160, 168
Transitive two-way trusts, 52–53, 158, 160
Transmission Control Protocol (TCP) ports, 43
Transmission Control Protocol-Internet Protocol (TCP-IP) network, 64, 297–298, 760
Transport Layer Security (TLS), 761
Transport protocols, replication, 126, 129–130
Tree root trusts, 52, 179
Trees, domain
  as AD DS component, 48–49
  in root domain, 88, 221
  spanning, 202
  structure of, 178–180
Troubleshooting
  Certification Authorities (CAs), 12
  documenting processes of, 156
  Domain Name System (DNS), 88–91
  Group Policy, 407, 444, 451–453
  Kerberos security, 297–301
  logon scripts, 503
  replication, 11, 112, 133–137
    Active Directory Sites and Services tool for, 134–135
    Dcdiag.exe tool for, 136–137
    failures in, 133–134
    Repadmin tool for, 135–136
  slow link detection, 421
Troubleshooting Active Directory Replication Problems Web site, 134
Trusted administrators, 159, 163
Trusted Publishers object, 537
Trusted Root Certification Authorities, 527
Trusts
  Active Directory Domains and Trusts tool for, 61
  AD DS, 52–55
  boundaries for, 47
  Certification Authorities (CA) and, 666
  cross-forest, 364
  disaster recovery and, 599–600
  documenting, 153
  domain number and, 176
  federation, 749–750
  forest, 167–171, 183. *See also* Federation Services
  in interforest migration, 259, 266–268
  Kerberos authentication and, 278
  management of, 326
  New Trust Wizard for, 171, 297
  parent-child, 179
  policy for, 14
  realm, 297
  Rights Management Services (RMS) policies for, 726–733
  selective authentication for, 165
  shared, in forests, 51
  shortcut, 179–180, 287–288
  structure of, 178–180
  transitive, 49, 168
  transitive two-way, 52–53, 158, 160
  tree root, 179
  two-way, 179, 267
Tuple indexes, 35
Two-factor authentication, 149, 670
Two-phase migration, 248
Two-way forest trusts, 165
Two-way transitive trusts, 52–53, 158, 160
Two-way trusts, 179, 267

U

Unattended installation of AD DS, 225, 236–238
Unattended removal of AD DS, 243
Unidirectional replication, 4
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001, 147
Universal Description Discovery and Integration (UDDI), 748
Universal groups, 25, 98, 209
  authentication and, 370
  availability of, 368
  best practices for, 376
  caching of, 370–371
  global catalog storage of, 369
Universal Naming Convention (UNC), 380, 384, 471, 490
UNIX, 190–191, 247, 274, 328
Unmount number command, 609
Update sequence numbers (USNs), 99–101, 599
Update types, for replication, 97–98
Updates, dynamic, 90–91, 190
Upgrading
  as best practice, 319
  in migrating to AD DS, 249–250, 254–257
  installing AD DS as, 219
  software, 495–496
Up-to-dateness vectors, 99, 102–103
Urgent replication, 110–111
USA Patriot Act of 2001, 147
User Account Migration Wizard, 264, 270
User accounts
  certificate mapping to, 294–295
  in AD LDS, 634
  in interforest migration, 261–262
  privileges applied to, 344
  resource, 790
  urgent replication and, 110
User class, 33–34, 36
User datagram protocol (UDP), 65, 299
User desktops. *See* Group Policy for user desktops
User Group Policy, 414
User Group Policy Loopback Processing Mode, 422
User interface, AD DS features in, 10–11
User objects, 358–363
User Principal Names (UPNs), 25
  claims of, 775
  in multidomain environments, 395
  object management and, 362–363
  security and, 283, 295
  suffix filtering of, 171
  suffix mapping of, 779
User profiles, 459–469
  folder redirection and, 476–477
  in Windows versions, 461
  junction points and, 461–462
  local, 463
  mandatory and super mandatory, 465–466
  overview of, 459–460
  roaming, 463–469, 693
User rights, assignment of, 311–312, 518–525
userAccountControl attribute, 8
Users container, 372–373
Users, super, 739–740
uSNChanged attribute, 100–101

V

VBScript
  best practices for, 396
  for AD DS information, 28
  for automating object management, 389–395
  for Group Policy management, 447
  printers added by, 380
  replication and, 124
  to extend schema, 36
Verification certificates, 573, 763, 773
Verifying AD DS installation, 235–236
Verisign Certificate Authority, 294
Version numbers, 103
  for Group Policy components, 409
  for Group Policy container (GPC), 406
  for Group Policy objects (GPOs), 416–417
  Windows user profiles and, 461
Virtual private networks (VPNs), 13, 149, 269, 501–502
Visual Basic, 447
Volume Shadow Copy Service (VSS), 9, 587

W

W32tm.exe tool, 321
Wait time, in replication, 107
Wake-on LAN technology, 502
Wbadmin command-line tool, 237, 587–588, 595, 601, 616

Web agents, AD FS, 752, 754, 756, 759, 761, 764, 767, 772–773, 785
Web enrollment of Certification Authorities, 12, 671, 673–675, 678
Web server, 673, 762, 769
Web Services Description Language (WSDL), 747
Web services in AD FS, 747–749
Web single sign-on (SSO) AD FS implementation, 752–755, 787–788
Web-Based Enterprise Management (WBEM) initiative, 390
Wevutil.exe command-line tool, 663–664, 702
Where-Object cmdlet, 394
Wide Area Networks (WANs), 27, 55, 95–96
Wi-Fi Protected Access, 541
Windows Deployment Services (WDS), 501
Windows Explorer, 219, 462
Windows firewall, 538, 541–543
Windows Installer technology, 467, 485–486, 498–500
Windows Internet Naming Service (WINS), 63–64, 220
Windows Management Instrumentation (WMI), 390, 424, 428, 434–435, 445
Windows NT 4.0 upgrade, 249
Windows NT token-based applications, 782, 785–787
Windows Process Activation Service, 673, 678
Windows Recovery Environment (Windows RE), 598, 614, 616
Windows Resource Protection, 588
Windows Script Host (WSH), 390, 484
Windows Server 2008, 98–99
Windows Server 2008 Server Core Installation, 3, 25
Windows Server Backup tool, 237, 587–588, 616
Windows token-based agent, 14
Windows token-based applications, 752, 757, 759
Windows Vista, RMS and, 17
Wired network security, 538–540
Wireless networks, 13, 538, 541, 670
Workstations organizational units, 197
Wscript.exe run time, 390
WS-Federation Passive Requestor Profile (WS-FPRP), 14, 748
WS-Federation specification, 748

X

X.500 directories, 363
X.500 object IDs, 16, 39–40

Z

Zero Administration for Windows (ZAW) down-level applications package (.zap), 490–491
Zone loading, background, 80–81
Zone Properties sheet, 78