Contents

Acknowledgments xix
Introduction xxi

Chapter 1  Windows Server 2008 R2 Administration Overview 1
Windows Server 2008 R2 and Windows 7 ......................... 2
Getting to Know Windows Server 2008 R2 ....................... 3
Power Management Options ...................................... 7
Networking Tools and Protocols ................................. 11
  Understanding Networking Options .................. 11
  Working with Networking Protocols ............... 12
Domain Controllers, Member Servers, and Domain Services . . . . 14
  Working with Active Directory ...................... 14
  Using Read-Only Domain Controllers ........... 16
  Using Restartable Active Directory Domain Services 17
Name-Resolution Services .................................. 18
  Using Domain Name System ....................... 18
  Using Windows Internet Name Service .......... 21
  Using Link-Local Multicast Name Resolution .... 23
Frequently Used Tools .................................. 24
  Windows PowerShell 2.0 ......................... 25
  Windows Remote Management .................... 26

Chapter 2  Deploying Windows Server 2008 R2 31
Server Roles, Role Services, and Features for Windows Server
  2008 R2 .................................................. 32
Full-Server and Core-Server Installations of Windows
  Server 2008 R2 ........................................... 39
Installing Windows Server 2008 R2. ........................ 43
  Performing a Clean Installation ................. 44
  Performing an Upgrade Installation .......... 47
  Performing Additional Administration Tasks
    During Installation .......................... 49

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:

microsoft.com/learning/booksurvey
Managing Roles, Role Services, and Features ......................... 56
  Viewing Configured Roles and Role Services 57
  Adding or Removing Roles on Servers 58
  Viewing and Modifying Role Services on Servers 60
  Adding or Removing Features in Windows
  Server 2008 R2 61
Deploying Virtualized Servers ........................................... 62

Chapter 3 Managing Servers Running Windows
  Server 2008 R2 67
Performing Initial Configuration Tasks .................................... 68
Managing Your Servers .................................................... 70
Managing Your Servers Remotely ......................................... 74
Managing System Properties .............................................. 76
  The Computer Name Tab 77
  The Hardware Tab 78
  The Advanced Tab 79
  The Remote Tab 88
Managing Dynamic-Link Libraries ....................................... 88

Chapter 4 Monitoring Processes, Services, and Events 89
Managing Applications, Processes, and Performance .................. 89
  Task Manager 90
  Managing Applications 90
  Administering Processes 91
  Viewing System Services 94
  Viewing and Managing System Performance 95
  Viewing and Managing Networking Performance 97
  Viewing and Managing Remote User Sessions 98
Managing System Services .............................................. 99
  Starting, Stopping, and Pausing Services 101
  Configuring Service Startup 102
  Configuring Service Logon 103
  Configuring Service Recovery 104
  Disabling Unnecessary Services 106
Event Logging and Viewing .............................................. 107
  Accessing and Using the Event Logs 108
  Filtering Event Logs 110
  Setting Event Log Options 112
  Clearing Event Logs 114
  Archiving Event Logs 114
## Monitoring Server Performance and Activity

- Why Monitor Your Server?
- Getting Ready to Monitor
- Using the Monitoring Consoles
- Choosing Counters to Monitor
- Performance Logging
- Viewing Data Collector Reports
- Configuring Performance Counter Alerts

## Tuning System Performance

- Monitoring and Tuning Memory Usage
- Monitoring and Tuning Processor Usage
- Monitoring and Tuning Disk I/O
- Monitoring and Tuning Network Bandwidth and Connectivity

### Chapter 5 Automating Administrative Tasks, Policies, and Procedures

- Understanding Group Policies
- Group Policy Essentials
- In What Order Are Multiple Policies Applied?
- When Are Group Policies Applied?
- Group Policy Requirements and Version Compatibility

## Navigating Group Policy Changes

- Managing Local Group Policies
- Local Group Policy Objects
- Accessing the Top-Level Local Policy Settings
- Local Group Policy Object Settings
- Accessing Administrator, Non-Administrator, and User-Specific Local Group Policy

## Managing Site, Domain, and Organizational Unit Policies

- Understanding Domain and Default Policies
- Using the Group Policy Management Console
- Getting to Know the Policy Editor
- Using Administrative Templates to Set Policies
- Creating and Linking GPOs
- Creating and Using Starter GPOs
- Delegating Privileges for Group Policy Management
- Blocking, Overriding, and Disabling Policies

## Maintaining and Troubleshooting Group Policy

- Refreshing Group Policy
<table>
<thead>
<tr>
<th>Chapter 6</th>
<th>Enhancing Computer Security</th>
<th>189</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing Users and Computers with Group Policy</td>
<td>172</td>
<td></td>
</tr>
<tr>
<td>Centrally Managing Special Folders</td>
<td>172</td>
<td></td>
</tr>
<tr>
<td>User and Computer Script Management</td>
<td>176</td>
<td></td>
</tr>
<tr>
<td>Deploying Software Through Group Policy</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>Automatically Enrolling Computer and User Certificates</td>
<td>185</td>
<td></td>
</tr>
<tr>
<td>Managing Automatic Updates in Group Policy</td>
<td>186</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>----</td>
</tr>
<tr>
<td>Chapter 7</td>
<td>Using Active Directory</td>
<td>211</td>
</tr>
<tr>
<td>Introducing Active Directory</td>
<td>211</td>
<td></td>
</tr>
<tr>
<td>Active Directory and DNS</td>
<td>211</td>
<td></td>
</tr>
<tr>
<td>Read-Only Domain Controller Deployment</td>
<td>212</td>
<td></td>
</tr>
<tr>
<td>New Active Directory Features</td>
<td>213</td>
<td></td>
</tr>
<tr>
<td>Working with Domain Structures</td>
<td>215</td>
<td></td>
</tr>
<tr>
<td>Understanding Domains</td>
<td>215</td>
<td></td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding Domain Forests and Domain Trees</td>
<td>216</td>
</tr>
<tr>
<td>Understanding Organizational Units</td>
<td>218</td>
</tr>
<tr>
<td>Understanding Sites and Subnets</td>
<td>220</td>
</tr>
<tr>
<td>Working with Active Directory Domains</td>
<td>221</td>
</tr>
<tr>
<td>Using Windows 2000 and Later Computers with Active Directory</td>
<td>221</td>
</tr>
<tr>
<td>Working with Domain Functional Levels</td>
<td>222</td>
</tr>
<tr>
<td>Raising Domain and Forest Functionality</td>
<td>225</td>
</tr>
<tr>
<td>Understanding the Directory Structure</td>
<td>227</td>
</tr>
<tr>
<td>Exploring the Data Store</td>
<td>227</td>
</tr>
<tr>
<td>Exploring Global Catalogs</td>
<td>228</td>
</tr>
<tr>
<td>Universal Group Membership Caching</td>
<td>229</td>
</tr>
<tr>
<td>Replication and Active Directory</td>
<td>230</td>
</tr>
<tr>
<td>Active Directory and LDAP</td>
<td>231</td>
</tr>
<tr>
<td>Understanding Operations Master Roles</td>
<td>232</td>
</tr>
<tr>
<td>Using the Active Directory Recycle Bin</td>
<td>233</td>
</tr>
<tr>
<td>Preparing Schema for the Recycle Bin</td>
<td>234</td>
</tr>
<tr>
<td>Recovering Deleted Objects</td>
<td>234</td>
</tr>
</tbody>
</table>

### Chapter 8  Core Active Directory Administration  237

| Tools for Managing Active Directory                                | 237  |
| Active Directory Administration Tools                              | 238  |
| Active Directory Command-Line Tools                                | 238  |
| Active Directory Support Tools                                     | 239  |
| Active Directory Administrative Center and Windows PowerShell       | 240  |

| Using Active Directory Users And Computers                         | 242  |
| Getting Started with Active Directory Users And Computers          | 242  |
| Connecting to a Domain Controller                                  | 243  |
| Connecting to a Domain                                             | 244  |
| Searching for Accounts and Shared Resources                        | 244  |
| Managing Computer Accounts                                         | 246  |
| Creating Computer Accounts on a Workstation or Server              | 246  |
| Creating Computer Accounts in Active Directory Users And Computers | 247  |
| Viewing and Editing Computer Account Properties                     | 248  |
| Deleting, Disabling, and Enabling Computer Accounts                | 248  |
| Resetting Locked Computer Accounts                                 | 249  |
| Moving Computer Accounts                                           | 250  |
Managing Computers
Joining a Computer to a Domain or Workgroup
Using Offline Domain Join
Managing Domain Controllers, Roles, and Catalogs
Installing and Demoting Domain Controllers
Viewing and Transferring Domainwide Roles
Viewing and Transferring the Domain Naming Master Role
Viewing and Transferring Schema Master Roles
Transferring Roles Using the Command Line
Seizing Roles Using the Command Line
Configuring Global Catalogs
Configuring Universal Group Membership Caching
Managing Organizational Units
Creating Organizational Units
Viewing and Editing Organizational Unit Properties
Renaming and Deleting Organizational Units
Moving Organizational Units
Managing Sites
Creating Sites
Creating Subnets
Associating Domain Controllers with Sites
Configuring Site Links
Configuring Site Link Bridges
Maintaining Active Directory
Using ADSI Edit
Examining Intersite Topology
Troubleshooting Active Directory

Chapter 9  Understanding User and Group Accounts
The Windows Server Security Model
Authentication Protocols
Access Controls
Differences Between User and Group Accounts
User Accounts
Group Accounts
Default User Accounts and Groups
Built-in User Accounts
Predefined User Accounts
Contents

Built-in and Predefined Groups ........................................... 285
Implicit Groups and Special Identities ................................. 286
Account Capabilities .......................................................... 286
   Privileges ........................................................................ 287
   Logon Rights ................................................................... 290
   Built-in Capabilities for Groups in Active Directory .............. 291
Using Default Group Accounts .............................................. 293
   Groups Used by Administrators ......................................... 293
   Implicit Groups and Identities .......................................... 294

Chapter 10 Creating User and Group Accounts ....................... 297
User Account Setup and Organization ..................................... 297
   Account Naming Policies .................................................. 298
   Password and Account Policies ......................................... 299
Configuring Account Policies .................................................. 302
   Configuring Password Policies .......................................... 302
   Configuring Account Lockout Policies ............................... 304
   Configuring Kerberos Policies .......................................... 305
Configuring User Rights Policies .......................................... 307
   Configuring Global User Rights ......................................... 307
   Configuring Local User Rights ......................................... 309
Adding a User Account ......................................................... 310
   Creating Domain User Accounts ....................................... 310
   Creating Local User Accounts .......................................... 312
Adding a Group Account ........................................................ 313
   Creating a Global Group ................................................. 314
   Creating a Local Group and Assigning Members .................. 315
Handling Global Group Membership .................................... 316
   Managing Individual Membership ...................................... 316
   Managing Multiple Memberships in a Group ........................ 317
   Setting the Primary Group for Users and Computers .............. 317
Implementing Managed Accounts ........................................... 318
   Creating and Using Managed Service Accounts .................... 319
   Configuring Services to Use Managed Service Accounts ......... 320
   Removing Managed Service Accounts .................................. 321
   Moving Managed Service Accounts .................................... 321
   Using Virtual Accounts .................................................... 322
Chapter 11  Managing User and Group Accounts  323
  Managing User Contact Information ............................ 323
  Setting Contact Information 323
  Searching for Users and Groups in Active Directory 325
  Configuring the User’s Environment Settings .................. 326
    System Environment Variables 327
    Logon Scripts 328
    Assigning Home Directories 329
  Setting Account Options and Restrictions ..................... 330
    Managing Logon Hours 330
    Setting Permitted Logon Workstations 332
    Setting Dial-In and VPN Privileges 333
    Setting Account Security Options 335
  Managing User Profiles ........................................... 336
    Local, Roaming, and Mandatory Profiles 337
    Using the System Utility to Manage Local Profiles 339
  Updating User and Group Accounts ................................ 343
    Renaming User and Group Accounts 344
    Copying Domain User Accounts 345
    Importing and Exporting Accounts 346
    Changing and Resetting Passwords 347
    Enabling User Accounts 348
  Managing Multiple User Accounts ............................... 349
    Setting Profiles for Multiple Accounts 350
    Setting Logon Hours for Multiple Accounts 351
    Setting Permitted Logon Workstations for Multiple Accounts 351
    Setting Logon, Password, and Expiration Properties for Multiple Accounts 351
  Troubleshooting Logon Problems .................................. 352
  Viewing and Setting Active Directory Permissions ............... 353

Chapter 12  Managing File Systems and Drives  357
  Managing the File Services Role ................................ 357
  Adding Hard Disk Drives ......................................... 363
    Physical Drives 363
    Preparing a Physical Drive for Use 365
    Using Disk Management 365
    Removable Storage Devices 368
Installing and Checking for a New Drive 370
Understanding Drive Status 370

Working with Basic, Dynamic, and Virtual Disks 372
Using Basic and Dynamic Disks 372
Special Considerations for Basic and Dynamic Disks 373
Changing Drive Types 374
Reactivating Dynamic Disks 376
Rescanning Disks 376
Moving a Dynamic Disk to a New System 376
Managing Virtual Hard Disks 377

Using Basic Disks and Partitions 378
Partitioning Basics 378
Creating Partitions and Simple Volumes 379
Formatting Partitions 382

Managing Existing Partitions and Drives 384
Assigning Drive Letters and Paths 384
Changing or Deleting the Volume Label 385
Deleting Partitions and Drives 386
Converting a Volume to NTFS 386
Resizing Partitions and Volumes 388
Repairing Disk Errors and Inconsistencies 390
Defragmenting Disks 393
Compressing Drives and Data 395
Encrypting Drives and Data 397
Understanding Encryption and the Encrypting File System 398
Working with Encrypted Files and Folders 400
Configuring Recovery Policy 401

Chapter 13 Administering Volume Sets and RAID Arrays 403
Using Volumes and Volume Sets 404
Understanding Volume Basics 404
Understanding Volume Sets 405
Creating Volumes and Volume Sets 407
Deleting Volumes and Volume Sets 410
Managing Volumes 410

Improving Performance and Fault Tolerance with RAID 411
Implementing RAID on Windows Server 2008 R2 412
Implementing RAID 0: Disk Striping 412
Implementing RAID 1: Disk Mirroring 413
Implementing RAID 5: Disk Striping with Parity 415
Managing RAID and Recovering from Failures 416
  Breaking a Mirrored Set 416
  Resynchronizing and Repairing a Mirrored Set 417
  Repairing a Mirrored System Volume to Enable Boot 418
  Removing a Mirrored Set 418
  Repairing a Striped Set Without Parity 419
  Regenerating a Striped Set with Parity 419
Managing LUNs on SANs 420
  Configuring Fibre Channel SAN Connections 421
  Configuring iSCSI SAN Connections 422
  Adding and Removing Targets 423
  Creating, Extending, Assigning, and Deleting LUNs 423
  Defining a Server Cluster in Storage Manager For SANs 424

Chapter 14 Managing File Screening and Storage Reporting 425
  Understanding File Screening and Storage Reporting 425
  Managing File Screening and Storage Reporting 429
    Managing Global File Resource Settings 430
    Managing the File Groups to Which Screens Are Applied 433
    Managing File Screen Templates 435
    Creating File Screens 438
    Defining File Screening Exceptions 438
    Scheduling and Generating Storage Reports 439

Chapter 15 Data Sharing, Security, and Auditing 441
  Using and Enabling File Sharing 442
  Configuring Standard File Sharing 445
    Viewing Existing Shares 445
    Creating Shared Folders 447
    Creating Additional Shares on an Existing Share 450
  Managing Share Permissions 450
    The Different Share Permissions 451
    Viewing Share Permissions 451
    Configuring Share Permissions 452
    Modifying Existing Share Permissions 453
    Removing Share Permissions for Users and Groups 454
Managing Existing Shares ................................. 454
  Understanding Special Shares 454
  Connecting to Special Shares 455
  Viewing User and Computer Sessions 456
  Stopping File and Folder Sharing 459
Configuring NFS Sharing ................................. 459
Using Shadow Copies ................................. 461
  Understanding Shadow Copies 461
  Creating Shadow Copies 462
  Restoring a Shadow Copy 462
  Reverting an Entire Volume to a Previous Shadow Copy 463
  Deleting Shadow Copies 463
  Disabling Shadow Copies 464
Connecting to Network Drives ................................. 464
  Mapping a Network Drive 464
  Disconnecting a Network Drive 465
Object Management, Ownership, and Inheritance .................. 465
  Objects and Object Managers 466
  Object Ownership and Transfer 466
  Object Inheritance 467
File and Folder Permissions ................................. 468
  Understanding File and Folder Permissions 468
  Setting File and Folder Permissions 471
Auditing System Resources ................................. 473
  Setting Auditing Policies 473
  Auditing Files and Folders 475
  Auditing the Registry 477
  Auditing Active Directory Objects 478
Using, Configuring, and Managing NTFS Disk Quotas ............ 478
  Understanding NTFS Disk Quotas and How
  NTFS Quotas Are Used 479
  Setting NTFS Disk Quota Policies 481
  Enabling NTFS Disk Quotas on NTFS Volumes 484
  Viewing Disk Quota Entries 485
  Creating Disk Quota Entries 486
  Deleting Disk Quota Entries 487
  Exporting and Importing NTFS Disk Quota Settings 488
  Disabling NTFS Disk Quotas 489
Managing Encryption Recovery Policy .................................. 528
  Understanding Encryption Certificates and Recovery Policy 528
  Configuring the EFS Recovery Policy 530
Backing Up and Restoring Encrypted Data and Certificates .......... 531
  Backing Up Encryption Certificates 531
  Restoring Encryption Certificates 532

Chapter 17 Managing TCP/IP Networking 533
  Navigating Networking in Windows Server 2008 R2 ............ 533
  Managing Networking in Windows 7 and Windows Server 2008 R2 ........................................ 537
  Installing TCP/IP Networking .................................... 539
Configuring TCP/IP Networking ........................................ 541
  Configuring Static IP Addresses 541
  Configuring Dynamic IP Addresses and Alternate IP Addressing 543
  Configuring Multiple Gateways 544
  Configuring Networking for Hyper-V 546
Managing Network Connections ...................................... 547
  Checking the Status, Speed, and Activity for Local Area Connections 547
  Enabling and Disabling Local Area Connections 547
  Renaming Local Area Connections 548

Chapter 18 Administering Network Printers and Print Services 549
  Managing the Print and Document Services Role ............. 549
  Using Print Devices 550
  Printing Essentials 550
  Configuring Print Servers 552
  Enabling and Disabling File and Printer Sharing 553
Getting Started with Print Management .......................... 554
Installing Printers ...................................................... 556
  Using the Autoinstall Feature of Print Management 556
Installing and Configuring Physically Attached Print Devices 556
Installing Network-Attached Print Devices 561
Connecting to Printers Created on the Network 563
Deploying Printer Connections 565
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Point and Print Restrictions</td>
<td>566</td>
</tr>
<tr>
<td>Moving Printers to a New Print Server</td>
<td>569</td>
</tr>
<tr>
<td>Monitoring Printers and Printer Queues Automatically</td>
<td>570</td>
</tr>
<tr>
<td>Solving Spooling Problems</td>
<td>571</td>
</tr>
<tr>
<td>Configuring Printer Properties</td>
<td>572</td>
</tr>
<tr>
<td>Adding Comments and Location Information</td>
<td>572</td>
</tr>
<tr>
<td>Listing Printers in Active Directory</td>
<td>572</td>
</tr>
<tr>
<td>Managing Printer Drivers</td>
<td>573</td>
</tr>
<tr>
<td>Setting a Separator Page and Changing Print Device Mode</td>
<td>574</td>
</tr>
<tr>
<td>Changing the Printer Port</td>
<td>574</td>
</tr>
<tr>
<td>Scheduling and Prioritizing Print Jobs</td>
<td>575</td>
</tr>
<tr>
<td>Starting and Stopping Printer Sharing</td>
<td>576</td>
</tr>
<tr>
<td>Setting Printer Access Permissions</td>
<td>577</td>
</tr>
<tr>
<td>Auditing Print Jobs</td>
<td>578</td>
</tr>
<tr>
<td>Setting Document Defaults</td>
<td>579</td>
</tr>
<tr>
<td>Configuring Print Server Properties</td>
<td>579</td>
</tr>
<tr>
<td>Locating the Spool Folder and Enabling Printing on NTFS</td>
<td>579</td>
</tr>
<tr>
<td>Managing High-Volume Printing</td>
<td>580</td>
</tr>
<tr>
<td>Logging Printer Events</td>
<td>580</td>
</tr>
<tr>
<td>Enabling Print Job Error Notification</td>
<td>580</td>
</tr>
<tr>
<td>Managing Print Jobs on Local and Remote Printers</td>
<td>580</td>
</tr>
<tr>
<td>Viewing Printer Queues and Print Jobs</td>
<td>581</td>
</tr>
<tr>
<td>Pausing the Printer and Resuming Printing</td>
<td>581</td>
</tr>
<tr>
<td>Emptying the Print Queue</td>
<td>582</td>
</tr>
<tr>
<td>Pausing, Resuming, and Restarting Individual Document Printing</td>
<td>582</td>
</tr>
<tr>
<td>Removing a Document and Canceling a Print Job</td>
<td>582</td>
</tr>
<tr>
<td>Checking the Properties of Documents in the Printer</td>
<td>582</td>
</tr>
<tr>
<td>Setting the Priority of Individual Documents</td>
<td>582</td>
</tr>
<tr>
<td>Scheduling the Printing of Individual Documents</td>
<td>583</td>
</tr>
</tbody>
</table>

**Chapter 19  Running DHCP Clients and Servers** 585

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding DHCP</td>
<td>585</td>
</tr>
<tr>
<td>Using Dynamic IPv4 Addressing and Configuration</td>
<td>586</td>
</tr>
<tr>
<td>Using Dynamic IPv6 Addressing and Configuration</td>
<td>586</td>
</tr>
<tr>
<td>Checking IP Address Assignment</td>
<td>589</td>
</tr>
<tr>
<td>Understanding Scopes</td>
<td>590</td>
</tr>
</tbody>
</table>
Contents

Installing a DHCP Server .......................................................... 591
  Installing DHCP Components ................................................. 591
  Starting and Using the DHCP Console ................................... 594
  Connecting to Remote DHCP Servers .................................... 595
  Starting and Stopping a DHCP Server ................................... 596
  Authorizing a DHCP Server in Active Directory .................... 596
Configuring DHCP Servers ..................................................... 596
  Binding a DHCP Server with Multiple Network Interface Cards to a Specific IP Address ...................................................... 597
  Updating DHCP Statistics .................................................... 597
  DHCP Auditing and Troubleshooting ..................................... 597
  Integrating DHCP and DNS .................................................. 599
  Integrating DHCP and NAP .................................................... 601
  Avoiding IP Address Conflicts ............................................. 604
  Saving and Restoring the DHCP Configuration ....................... 604
Managing DHCP Scopes ......................................................... 605
  Creating and Managing Superscopes .................................... 605
  Creating and Managing Scopes ............................................. 606
  Creating and Managing Split Scopes ..................................... 616
Managing the Address Pool, Leases, and Reservations .............. 620
  Viewing Scope Statistics ..................................................... 620
  Enabling and Configuring MAC Address Filtering .................... 621
  Setting a New Exclusion Range ............................................ 622
  Deleting an Exclusion Range .............................................. 623
  Reserving DHCP Addresses ................................................ 623
  Modifying Reservation Properties ....................................... 625
  Deleting Leases and Reservations ....................................... 625
Backing Up and Restoring the DHCP Database ....................... 625
  Backing Up the DHCP Database ......................................... 626
  Restoring the DHCP Database from Backup ......................... 626
  Using Backup and Restore to Move the DHCP Database to a New Server ............................................................. 627
  Forcing the DHCP Server Service to Regenerate the DHCP Database ................................................................. 627
  Reconciling Leases and Reservations .................................... 628

Chapter 20  Optimizing DNS .................................................. 629
Understanding DNS .............................................................. 629
  Integrating Active Directory and DNS .................................. 630
  Enabling DNS on the Network ............................................. 631
Understanding DNSSEC ........................................... 633
Configuring Name Resolution on DNS Clients .......... 635
Installing DNS Servers ........................................... 637
  Installing and Configuring the DNS Server Service 637
  Configuring a Primary DNS Server .......................... 639
  Configuring a Secondary DNS Server ....................... 642
  Configuring Reverse Lookups ............................... 642
  Configuring Global Names ................................... 644
Managing DNS Servers ......................................... 645
  Adding Remote Servers to the DNS Manager Console 646
  Removing a Server from the DNS Manager Console .... 646
  Starting and Stopping a DNS Server ....................... 647
  Creating Child Domains Within Zones ................. 647
  Creating Child Domains in Separate Zones ............. 647
  Deleting a Domain or Subnet .................. 648
Managing DNS Records ......................................... 649
  Adding Address and Pointer Records ....................... 650
  Adding DNS Aliases with CNAME .......................... 651
  Adding Mail Exchange Servers ............................ 652
  Adding Name Servers ....................................... 654
  Viewing and Updating DNS Records ....................... 655
Updating Zone Properties and the SOA Record .......... 655
  Modifying the SOA Record ................................ 655
  Allowing and Restricting Zone Transfers ................ 657
  Notifying Secondaries of Changes ........................ 658
  Setting the Zone Type ..................................... 659
  Enabling and Disabling Dynamic Updates ............... 660
Managing DNS Server Configuration and Security .... 660
  Enabling and Disabling IP Addresses for a DNS Server 660
  Controlling Access to DNS Servers Outside the Organization 661
  Enabling and Disabling Event Logging ................. 663
  Using Debug Logging to Track DNS Activity ........... 663
  Monitoring a DNS Server .................................. 664

Index ........................................................................ 667

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:

microsoft.com/learning/booksurvey
Writing *Windows Server 2008 Administrator’s Pocket Consultant* was a lot of fun, and updating the book for Windows Server 2008 Release 2 (R2) was even more so. As I set out to write *Windows Server 2008 Administrator’s Pocket Consultant* and then to update the book for this second edition, my goal was to determine what had changed and what new administration options were available. As with any new release of an operating system, and especially with Windows Server 2008 R2, this meant a great deal of research to determine exactly how things work—and a lot of digging into the operating system internals. I was thankful I’d already written several books on Windows 7 and its new features, so I had a starting point of reference for my research, but by no means a complete one.

When you start working with Windows Server 2008 R2, you’ll see at once that this operating system is different from previous releases of Windows Server. What won’t be readily apparent, however, is just how different Windows Server 2008 R2 is from its predecessors—and that’s because many of the most significant changes to the operating system are under the surface. These changes affect the underlying architecture, not just the user interfaces, and these changes were some of the hardest for me to research and write about.

Because Pocket Consultants are meant to be portable and readable—the kind of book you use to solve problems and get the job done wherever you might be—I had to carefully review my research to make sure I focused on the core of Windows Server 2008 R2 administration. The result is the book that you hold in your hand—a book that I hope you’ll agree is one of the best practical, portable guides to Windows Server 2008 and Windows Server 2008 R2.

It is gratifying to see techniques that I’ve used time and again to solve problems put into a printed book so that others might benefit from them. But no man is an island, and this book couldn’t have been written without help from some very special people. As I’ve stated in all my previous books with Microsoft Press, the team at Microsoft Press is top-notch. Throughout the writing process, Karen Szall and Rosemary Caperton were instrumental in helping me stay on track and in getting the tools I needed to write this book. They did a first-rate job managing the editorial process. Thanks also to Martin DelRe for believing in my work and shepherding it through production.

Unfortunately for the writer (but fortunately for readers), writing is only one part of the publishing process. Next came editing and author review. I must say, Microsoft Press has the most thorough editorial and technical review process I’ve seen anywhere—and I’ve written a lot of books for many different publishers. Bob Hogan was the technical reviewer for the book, Curtis Philips and John Pierce were the project managers, John was also the copy editor, and Andrea Fox was the proofreader.

I hope I haven’t forgotten anyone, but if I have, it was an oversight. Honest. ;–)
Welcome to *Windows Server 2008 Administrator’s Pocket Consultant*, Second Edition. Over the years, I’ve written about many different server technologies and products, but the one product I like writing about the most is Windows Server. From top to bottom, Windows Server 2008 Release 2 (R2) is substantially different from earlier releases of Windows Server. For starters, many of the core components of Windows Server 2008 R2 are built off the same code base as Windows 7 rather than Windows Vista. This means that you can apply much of what you know about Windows 7 to Windows Server 2008 R2. That’s good news, but you still need to learn how Windows Server 2008 R2 is different from previous releases of Windows Server, and while some of these differences are small, others are very important.

Because I’ve written many top-selling Windows Server books, I was able to bring a unique perspective to this book—the kind of perspective you gain only after working with technologies for many years. Long before there was a product called Windows Server 2008 Release 2, I was working with the beta product. From these early beginnings, the final version of Windows Server 2008 R2 evolved until it became the finished product that is available today.

As you’ve probably noticed, a great deal of information about Windows Server 2008 R2 is available on the Web and in other printed books. You can find tutorials, reference sites, discussion groups, and more to make using Windows Server 2008 R2 easier. However, the advantage of reading this book is that much of the information you need to learn about Windows Server 2008 R2 is organized in one place and presented in a straightforward and orderly fashion. This book has everything you need to customize Windows Server 2008 R2 installations, master Windows Server 2008 R2 configurations, and maintain Windows Server 2008 R2 servers.

In this book, I teach you how features work, why they work the way they do, and how to customize them to meet your needs. I also offer specific examples of how certain features can meet your needs, and how you can use other features to troubleshoot and resolve issues you might have. In addition, this book provides tips, best practices, and examples of how to optimize Windows Server 2008 R2. This book won’t just teach you how to configure Windows Server 2008 R2, it will teach you how to squeeze every last bit of power out of it and make the most from the features and options it includes.

Unlike many other books about administering Windows Server 2008 R2, this book doesn’t focus on a specific user level. This isn’t a lightweight beginner book. Regardless of whether you are a beginning administrator or a seasoned professional, many of the concepts in this book will be valuable to you, and you can apply them to your Windows Server 2008 R2 installations.
Who Is This Book For?


- Current Windows system administrators
- Accomplished users who have some administrator responsibilities
- Administrators upgrading to Windows Server 2008 R2 from previous versions
- Administrators transferring from other platforms

To pack in as much information as possible, I had to assume that you have basic networking skills and a basic understanding of Windows Server. With this in mind, I don’t devote entire chapters to explaining Windows Server architecture, Windows Server startup and shutdown, or why you want to use Windows Server. I do, however, cover Windows server configuration, Group Policy, security, auditing, data backup, system recovery, and much more.

I also assume that you are fairly familiar with Windows commands and procedures as well as the Windows user interface. If you need help learning Windows basics, you should read other resources (many of which are available from Microsoft Press).

**NOTE** This book has been completely updated for Windows Server 2008 R2. If you are using Windows Server 2008 RTM, features and procedures will vary slightly. However, you can still use this book to help you with Windows Server 2008 RTM.

How This Book Is Organized

Rome wasn’t built in a day, and this book wasn’t intended to be read in a day, in a week, or even in a month. Ideally, you’ll read this book at your own pace, a little each day as you work your way through all the features Windows Server 2008 R2 has to offer. This book is organized into 20 chapters. The chapters are arranged in a logical order, taking you from planning and deployment tasks to configuration and maintenance tasks.

Speed and ease of reference are essential parts of this hands-on guide. This book has an expanded table of contents and an extensive index for finding answers to problems quickly. Many other quick reference features have been added to the book as well, including quick step-by-step procedures, lists, tables with fast facts, and extensive cross references.

As with all Pocket Consultants, Windows Server 2008 Administrator's Pocket Consultant, Second Edition is designed to be a concise and easy-to-use resource for managing Windows servers. This is the readable resource guide that you’ll want on your desktop at all times. The book covers everything you need to perform the core administrative tasks for Windows servers. Because the focus is on giving you maximum value in a pocket-size guide, you don’t have to wade through hundreds of pages of extraneous information to find what you’re looking for. Instead, you’ll find exactly what you need to get the job done, and you’ll find it quickly.
In short, the book is designed to be the one resource you turn to whenever you have questions regarding Windows Server administration. To this end, the book zeroes in on daily administration procedures, frequently performed tasks, documented examples, and options that are representative while not necessarily inclusive. One of my goals is to keep the content so concise that the book remains compact and easy to navigate while at the same time ensuring that it is packed with as much information as possible. This means you get a valuable resource guide that can help you quickly and easily perform common tasks, solve problems, and implement advanced Windows technologies.

Conventions Used in This Book

I’ve used a variety of elements to help keep the text clear and easy to follow. You’ll find code terms and listings in monospace type, except when I tell you to actually type a command. In that case, the command appears in **bold** type. When I introduce and define a new term, I put it in *italics*.

**NOTE** Group Policy now includes both policies and preferences. Under the Computer Configuration and User Configuration nodes, you find two nodes: Policies and Preferences. Settings for general policies are listed under the Policies node. Settings for general preferences are listed under the Preferences node. When referencing settings under the Policies node, I use shortcut references, such as User Configuration\Administrative Templates\Windows Components, or specify that the policies are found in the Administrative Templates for User Configuration under Windows Components. Both references tell you that the policy setting being discussed is under User Configuration rather than Computer Configuration and can be found under Administrative Templates\Windows Components.

Other conventions include the following:

**Best Practices** To examine the best technique to use when working with advanced configuration and administration concepts

**Caution** To warn you about potential problems you should look out for

**More Info** To provide more information on a subject

**Note** To provide additional details on a particular point that needs emphasis

**Real World** To provide real-world advice when discussing advanced topics

**Security Alert** To point out important security issues

**Tip** To offer helpful hints or additional information

I truly hope you find that *Windows Server 2008 Administrator’s Pocket Consultant*, Second Edition provides everything you need to perform the essential administrative tasks on Windows servers as quickly and efficiently as possible. You are welcome to send your thoughts to me at williamstanek@aol.com or follow me at twitter.com/WilliamStanek. Thank you.
Other Resources

No single magic bullet for learning everything you’ll ever need to know about Windows Server 2008 R2 exists. While some books are offered as all-in-one guides, there’s simply no way one book can do it all. With this in mind, I hope you use this book as it is intended to be used—as a concise and easy-to-use resource. It covers everything you need to perform core administration tasks for Windows servers, but it is by no means exhaustive.

Your current knowledge will largely determine your success with this or any other Windows resource or book. As you encounter new topics, take the time to practice what you’ve learned and read about. Seek out further information as necessary to get the practical hands-on know-how and knowledge you need.

I recommend that you regularly visit Microsoft’s Web site for Windows Server (microsoft.com/windowsserver/) and support.microsoft.com to stay current with the latest changes. To help you get the most out of this book, you can visit my corresponding Web site at williamstanek.com/windows. This site contains information about Windows Server 2008 R2 and updates to the book.

Support for This Book

Every effort has been made to ensure the accuracy of this book. As corrections or changes are collected, they will be added to a Microsoft Knowledge Base article accessible via the Microsoft Help and Support site. Microsoft Press provides support for books, including instructions for finding Knowledge Base articles, at the following Web site:

http://www.microsoft.com/learning/support/books/

If you have questions regarding the book that are not answered by visiting this site or viewing a Knowledge Base article, send them to Microsoft Press via e-mail to mspinput@microsoft.com.

Please note that Microsoft software product support is not offered through these addresses.

We Want to Hear from You

We welcome your feedback about this book. Please share your comments and ideas via the following short survey:

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

Your participation will help Microsoft Press create books that better meet your needs and your standards.

NOTE We hope that you will give us detailed feedback via our survey. If you have questions about our publishing program, upcoming titles, or Microsoft Press in general, we encourage you to interact with us via Twitter at twitter.com/MicrosoftPress. For support issues, use only the e-mail address shown above.
CHAPTER 7

Using Active Directory

- Introducing Active Directory 211
- Working with Domain Structures 215
- Working with Active Directory Domains 221
- Understanding the Directory Structure 227
- Using the Active Directory Recycle Bin 233

Active Directory Domain Services (AD DS) is an extensible and scalable directory service that you can use to efficiently manage network resources. As an administrator, you need to be deeply familiar with how Active Directory technology works, and that’s exactly what this chapter is about. If you haven’t worked with Active Directory technology before, you’ll notice immediately that the technology is fairly advanced and has many features. To help manage this complex technology, I’ll start with an overview of Active Directory and then explore its components.

Introducing Active Directory

Since Windows 2000, Active Directory has been the heart of Windows-based domains. Just about every administrative task you perform affects Active Directory in some way. Active Directory technology is based on standard Internet protocols and is designed to help you clearly define your network’s structure.

Active Directory and DNS

Active Directory uses Domain Name System (DNS). DNS is a standard Internet service that organizes groups of computers into domains. DNS domains are organized into a hierarchical structure. The DNS domain hierarchy is defined on an Internet-wide basis, and the different levels within the hierarchy identify computers, organizational domains, and top-level domains. DNS is also used to map host names, such as zeta.microsoft.com, to numeric TCP/IP addresses, such as 192.168.19.2. Through DNS, an Active Directory domain hierarchy can also be
defined on an Internet-wide basis, or the domain hierarchy can be separate from the Internet and private.

When you refer to computer resources in a DNS domain, you use a fully qualified domain name (FQDN), such as zeta.microsoft.com. Here, zeta represents the name of an individual computer, microsoft represents the organizational domain, and com is the top-level domain. Top-level domains (TLDs) are at the base of the DNS hierarchy. TLDs are organized geographically by using two-letter country codes, such as CA for Canada; by organization type, such as com for commercial organizations; and by function, such as mil for U.S. military installations.

Normal domains, such as microsoft.com, are also referred to as parent domains because they’re the parents of an organizational structure. You can divide parent domains into subdomains, which you can then use for different offices, divisions, or geographic locations. For example, the FQDN for a computer at Microsoft’s Seattle office could be designated as jacob.seattle.microsoft.com. Here, jacob is the computer name, seattle is the subdomain, and microsoft.com is the parent domain. Another term for a subdomain is a child domain.

DNS is an integral part of Active Directory technology—so much so that you must configure DNS on the network before you can install Active Directory. Working with DNS is covered in Chapter 20, “Optimizing DNS.”

With Windows Server 2008 R2, you install Active Directory in a two-part process. First you use the Add Roles Wizard to add the Active Directory Domain Services role to the server. Then you run the Active Directory Installation Wizard (click Start, type dcpromo in the Search field, and then press Enter). If DNS isn’t already installed, you are prompted to install it. If no domain exists, the wizard helps you create a domain and configure Active Directory in the new domain. The wizard can also help you add child domains to existing domain structures. To verify that a domain controller is installed correctly, you can:

■ Check the Directory Service event log for errors.
■ Ensure that the SYSVOL folder is accessible to clients.
■ Verify that name resolution is working through DNS.
■ Verify the replication of changes to Active Directory.

NOTE In the rest of this chapter, I’ll use the terms directory and domains to refer to Active Directory and Active Directory domains, respectively, except when I need to distinguish Active Directory structures from DNS or other types of directories.

Read-Only Domain Controller Deployment

As discussed in Chapter 1, “Windows Server 2008 R2 Administration Overview,” domain controllers running Windows Server 2008 R2 can be configured as read-only domain controllers (RODCs). When you install the DNS Server service on an
RODC, the RODC can act as a read-only DNS (RODNS) server. In this configuration, the following conditions are true:

- The RODC replicates the application directory partitions that DNS uses, including the ForestDNSZones and DomainDNSZones partitions. Clients can query an RODNS server for name resolution. However, the RODNS server does not support client updates directly because the RODNS server does not register resource records for any Active Directory–integrated zone that it hosts.

- When a client attempts to update its DNS records, the server returns a referral. The client can then attempt to update against the DNS server that is provided in the referral. Through replication in the background, the RODNS server then attempts to retrieve the updated record from the DNS server that made the update. This replication request is only for the changed DNS record. The entire list of data changed in the zone or domain is not replicated during this special request.

The first Windows Server 2008 R2 domain controller installed in a forest or domain cannot be an RODC. However, you can configure subsequent domain controllers as read-only. For planning purposes, keep the following in mind:

- Prior to adding AD DS to a server that is running Windows Server 2008 R2 in a Windows Server 2003 or Windows 2000 Server forest, you must update the schema on the schema operations master in the forest by running adprep /forestprep.

- Prior to adding AD DS to a server that is running Windows Server 2008 R2 in a Windows Server 2003 or Windows 2000 Server domain, you must update the infrastructure master in the domain by running adprep /domainprep /gpprep.

- Prior to installing AD DS to create your first RODC in a forest, you must prepare the forest by running adprep /rodcprep.

**New Active Directory Features**

Active Directory Domain Service in Windows Server 2008 R2 has many new features that give administrators additional options for implementing and managing Active Directory. When you are using Windows Server 2008 R2 and have deployed the operating system on all domain controllers throughout the domains in your Active Directory forest, your domains can operate at the Windows Server 2008 R2 domain functional level, and the forest can operate at the Windows Server 2008 R2 forest functional level. These operating levels allow you to take advantage of Active Directory enhancements that improve manageability, performance, and supportability, including the following:

- **Active Directory Recycle Bin**  Allows administrators to undo the accidental deletion of Active Directory objects in much the same way as they can
recover deleted files from the Windows Recycle Bin. For more information, see “Using the Active Directory Recycle Bin” later in this chapter.

- **Managed service accounts**  Introduces a special type of domain user account for managed services that reduces service outages and other issues by having Windows manage the account password and related Service Principal Names (SPNs) automatically. For more information, see “Implementing Managed Accounts” in Chapter 10.

- **Managed virtual accounts**  Introduces a special type of local computer account for managed services that provides the ability to access the network with a computer identity in a domain environment. For more information, see “Using Virtual Accounts” in Chapter 10.

**REAL WORLD**  Technically, you can use managed service accounts and managed virtual accounts in a mixed-mode domain environment. However, you must update the Active Directory schema for Windows Server 2008 R2 and you have to manually manage SPNs for managed service accounts.

- **Authentication Mechanism Assurance**  Improves the authentication process by allowing administrators to control resource access based on whether a user logs on using a certificate-based logon method. Thus, an administrator can specify that a user has one set of access permissions when logged on using a smart card and a different set of access permissions when not logged on using a smart card.

Other improvements don’t require that you raise domain or forest functional levels, but they do require that you use Windows Server 2008 R2. These include:

- **Offline domain join**  Allows administrators to pre provision computer accounts in the domain to prepare operating systems for deployment. This allows computers to join a domain without having to contact a domain controller.

- **Active Directory module for Windows PowerShell**  Provides cmdlets for managing Active Directory when you are working with Windows PowerShell. A related option is on the Administrative Tools menu.

- **Active Directory Administrative Center**  Provides a task-orientated interface for managing Active Directory. A related option is on the Administrative Tools menu.

- **Active Directory Web Services**  Introduces a Web service interface for Active Directory domains.

These features are discussed in more detail in Chapter 8, “Core Active Directory Administration.” Also keep in mind that you must prepare Active Directory schema for the Active Directory Recycle Bin. The preparation procedures are the same as those discussed for RODCs in the previous section.
Working with Domain Structures

Active Directory provides both logical and physical structures for network components. Logical structures help you organize directory objects and manage network accounts and shared resources. Logical structures include the following:

- **Organizational units**  A subgroup of domains that often mirrors the organization’s business or functional structure.
- **Domains**  A group of computers that share a common directory database.
- **Domain trees**  One or more domains that share a contiguous namespace.
- **Domain forests**  One or more domain trees that share common directory information.

Physical structures serve to facilitate network communication and to set physical boundaries around network resources. Physical structures that help you map the physical network structure include the following:

- **Subnets**  A network group with a specific IP address range and network mask.
- **Sites**  One or more subnets. Sites are used to configure directory access and replication.

Understanding Domains

An Active Directory domain is simply a group of computers that share a common directory database. Active Directory domain names must be unique. For example, you can’t have two microsoft.com domains, but you can have a parent domain microsoft.com, with the child domains seattle.microsoft.com and ny.microsoft.com. If the domain is part of a private network, the name assigned to a new domain must not conflict with any existing domain name on the private network. If the domain is part of the Internet, the name assigned to a new domain must not conflict with any existing domain name throughout the Internet. To ensure uniqueness on the Internet, you must register the parent domain name before using it. You can register a domain through any designated registrar. You can find a current list of designated registrars at InterNIC (www.internic.net).

Each domain has its own security policies and trust relationships with other domains. Domains can also span more than one physical location, which means that a domain can consist of multiple sites and those sites can have multiple subnets, as shown in Figure 7-1. Within a domain’s directory database, you’ll find objects defining accounts for users, groups, and computers as well as shared resources such as printers and folders.
NOTE User and group accounts are discussed in Chapter 9, “Understanding User and Group Accounts.” Computer accounts and the various types of computers used in Windows Server 2008 R2 domains are discussed in “Working with Active Directory Domains” later in this chapter.

Domain functions are limited and controlled by the domain functional level. Several domain functional levels are available, including the following:


For further discussion of domain functional levels, see “Working with Domain Functional Levels” later in this chapter.

**Understanding Domain Forests and Domain Trees**

Each Active Directory domain has a DNS domain name, such as microsoft.com. One or more domains sharing the same directory data are referred to as a forest. The domain names within this forest can be discontiguous or contiguous in the DNS naming hierarchy.
When domains have a contiguous naming structure, they’re said to be in the same domain tree. Figure 7-2 shows an example of a domain tree. In this example, the root domain msnbc.com has two child domains—seattle.msnbc.com and ny.msnbc.com. These domains in turn have subdomains. All the domains are part of the same tree because they have the same root domain.

If the domains in a forest have discontiguous DNS names, they form separate domain trees within the forest. As shown in Figure 7-3, a domain forest can have one or more domain trees. In this example, the msnbc.com and microsoft.com domains form the roots of separate domain trees in the same forest.

You can access domain structures by using Active Directory Domains And Trusts, shown in Figure 7-4. Active Directory Domains And Trusts is a snap-in for the Microsoft Management Console (MMC). You can also start it from the Administrative Tools menu. You’ll find separate entries for each root domain. In Figure 7-4, the active domain is cpandl.com.
Using Active Directory

Forest functions are limited and controlled by the forest functional level. Several forest functional levels are available, including:


When all domains within a forest are operating in Windows Server 2003 forest functional level, you’ll see improvements over earlier implementations in global catalog replication and replication efficiency. Because link values are replicated, you might see improved intersite replication as well. You can deactivate schema class objects and attributes; use dynamic auxiliary classes; rename domains; and create one-way, two-way, and transitive forest trusts.

The Windows Server 2008 forest functional level offers incremental improvements over the Windows Server 2003 forest functional level in Active Directory performance and features. When all domains within a forest are operating in this mode, you’ll see improvements in both intersite and intrasite replication throughout the organization. Domain controllers can use Distributed File System (DFS) replication rather than File Replication Service (FRS) replication as well. In addition, Windows Server 2008 security principals are not created until the primary domain controller (PDC) emulator operations master in the forest root domain is running Windows Server 2008.

The Windows Server 2008 R2 forest functional level has several new features. These features include the Active Directory Recycle Bin, managed service accounts, and Authentication Mechanism Assurance.

**Understanding Organizational Units**

Organizational units (OUs) are subgroups within domains that often mirror an organization’s functional or business structure. You can also think of OUs as logical containers into which you place accounts, shared resources, and other OUs. For example, you could create OUs named HumanResources, IT, Engineering, and
Marketing for the microsoft.com domain. You could later expand this scheme to include child units. Child OUs for Marketing could include OnlineSales, Channel-Sales, and PrintSales.

Objects placed in an OU can only come from the parent domain. For example, OUs associated with seattle.microsoft.com can contain objects for this domain only. You can’t add objects from ny.microsoft.com to these containers, but you could create separate OUs to mirror the business structure of seattle.microsoft.com.

OUs are helpful in organizing objects to reflect a business or functional structure. Still, this isn’t the only reason to use OUs. Other reasons include:

- OUs allow you to assign group policies to a small set of resources in a domain without applying the policies to the entire domain. This helps you set and manage group policies at the appropriate level in the enterprise.
- OUs create smaller, more manageable views of directory objects in a domain. This helps you manage resources more efficiently.
- OUs allow you to delegate authority and to easily control administrative access to domain resources. This helps you control the scope of administrator privileges in the domain. You could grant user A administrative authority for one OU and not for others. Meanwhile, you could grant user B administrative authority for all OUs in the domain.

OUs are represented as folders in Active Directory Users And Computers, as shown in Figure 7-5. This utility is a snap-in for the MMC, and you can also start it from the Administrative Tools menu.

![Active Directory Users And Computers](image)

**FIGURE 7-5** Use Active Directory Users And Computers to manage users, groups, computers, and organizational units.
Understanding Sites and Subnets

A site is a group of computers in one or more IP subnets. You use sites to map your network’s physical structure. Site mappings are independent of logical domain structures, so there’s no necessary relationship between a network’s physical structure and its logical domain structure. With Active Directory, you can create multiple sites within a single domain or create a single site that serves multiple domains. The IP address ranges used by a site and the domain namespace also have no connection.

You can think of a subnet as a group of network addresses. Unlike sites, which can have multiple IP address ranges, subnets have a specific IP address range and network mask. Subnet names are shown in the form `network/bits-masked`, such as 192.168.19.0/24. Here, the network address 192.168.19.9 and network mask 255.255.255.0 are combined to create the subnet name 192.168.19.0/24.

**NOTE** Don’t worry, you don’t need to know how to create a subnet name. In most cases you enter the network address and the network mask, and then Windows Server 2008 R2 generates the subnet name for you.

Computers are assigned to sites based on their location in a subnet or a set of subnets. If computers in subnets can communicate efficiently with one another over the network, they’re said to be well connected. Ideally, sites consist of subnets and computers that are all well connected. If the subnets and computers aren’t well connected, you might need to set up multiple sites. Being well connected gives sites several advantages:

- When clients log on to a domain, the authentication process first searches for domain controllers that are in the same site as the client. This means that local domain controllers are used first, if possible, which localizes network traffic and can speed up the authentication process.

- Directory information is replicated more frequently within sites than between sites. This reduces the network traffic load caused by replication while ensuring that local domain controllers get up-to-date information quickly. You can also use site links to customize how directory information is replicated between sites. A domain controller designated to perform intersite replication is called a bridgehead server. By designating a bridgehead server to handle replication between sites, you place the bulk of the intersite replication burden on a specific server rather than on any available server in a site.

You access sites and subnets through Active Directory Sites And Services, shown in Figure 7-6. Because this is a snap-in for the MMC, you can add it to any updateable console. You can also open Active Directory Sites And Services from the Administrative Tools menu.
Working with Active Directory Domains

Although you must configure both Active Directory and DNS on a Windows Server 2008 R2 network, Active Directory domains and DNS domains have different purposes. Active Directory domains help you manage accounts, resources, and security. DNS domains establish a domain hierarchy that is primarily used for name resolution. Windows Server 2008 R2 uses DNS to map host names, such as zeta.microsoft.com, to numeric TCP/IP addresses, such as 172.16.18.8. To learn more about DNS and DNS domains, see Chapter 20.

Using Windows 2000 and Later Computers with Active Directory

User computers running professional or business editions of Windows 2000, Windows XP, Windows Vista, or Windows 7 can make full use of Active Directory. These computers access the network as Active Directory clients and have full use of Active Directory features. As clients, these systems can use transitive trust relationships that exist within the domain tree or forest. A transitive trust is one that isn’t established explicitly. Rather, the trust is established automatically based on the forest structure and permissions set in the forest. These relationships allow authorized users to access resources in any domain in the forest.

Server computers running Windows 2000 Server, Windows Server 2003, and Windows Server 2008 or later provide services to other systems and can act as domain controllers or member servers. A domain controller is distinguished from a member server because it runs Active Directory Domain Services. You promote member servers to domain controllers by installing Active Directory Domain Services. You demote domain controllers to member servers by uninstalling Active Directory Domain Services. You use the Add Role and Remove Role wizards to add or remove Active Directory Domain Services. You promote or demote a server through the Active Directory Installation Wizard (Dcpromo.exe).
Domains can have one or more domain controllers. When a domain has multiple domain controllers, the controllers automatically replicate directory data with one another using a multimaster replication model. This model allows any domain controller to process directory changes and then replicate those changes to other domain controllers.

Because of the multimaster domain structure, all domain controllers have equal responsibility by default. You can, however, give some domain controllers precedence over others for certain tasks, such as specifying a bridgehead server that has priority in replicating directory information to other sites. In addition, some tasks are best performed by a single server. A server that handles this type of task is called an operations master. There are five flexible single master operations (FSMO) roles, and you can assign each to a different domain controller. For more information, see “Understanding Operations Master Roles” later in this chapter.

Every Windows 2000 or later computer that joins a domain has a computer account. Like other resources, computer accounts are stored in Active Directory as objects. You use computer accounts to control access to the network and its resources. A computer accesses a domain by using its account, which is authenticated before the computer can access the network.

**REAL WORLD** Domain controllers use Active Directory’s global catalog to authenticate both computer and user logons. If the global catalog is unavailable, only members of the Domain Admins group can log on to the domain because the universal group membership information is stored in the global catalog, and this information is required for authentication. In Windows Server 2003 and later servers, you have the option of caching universal group membership locally, which solves this problem. For more information, see “Understanding the Directory Structure” later in this chapter.

**Working with Domain Functional Levels**

To support domain structures, Active Directory includes support for several domain functional levels, including:


- **Windows Server 2008 mode** When the domain is operating in Windows Server 2008 mode, the directory supports Windows Server 2008 and Windows Server 2008 R2 domain controllers. Windows NT, Windows 2000, and Windows Server 2003 domain controllers are no longer supported. The
good news is that a domain operating in Windows Server 2008 mode can use additional Active Directory features, including the DFS replication service for enhanced intersite and intrasite replication.

- **Windows Server 2008 R2 mode**  When the domain is operating in Windows Server 2008 R2 mode, the directory supports only Windows Server 2008 R2 domain controllers. Windows NT, Windows 2000, Windows Server 2003, and Windows Server 2008 domain controllers are no longer supported. The good news is that a domain operating in Windows Server 2008 R2 mode can use all the latest Active Directory features, including the Active Directory Recycle Bin.

**Using Windows Server 2003 Functional Level**


Before updating Windows 2000 domain controllers, you should prepare the domain for upgrade. To do this, you need to update the forest and the domain schema so that they are compatible with Windows Server 2003 domains. A tool called Adprep.exe is provided to automatically perform the update for you. All you need to do is run the tool on the schema operations master in the forest and then on the infrastructure operations master for each domain in the forest. As always, you should test any procedure in a lab before performing it in a production environment. On Windows Server 2003 installation media, you’ll find Adprep in the i386 subfolder.

**NOTE** To determine which server is the current schema operations master for the domain, open a command prompt and type `dsquery server –hasfsmo schema`. A directory service path string is returned containing the name of the server, such as “CN=CORPSERVER01,CN=Servers,CN=Default-First-Site-Name,CN=Sites, CN=Configuration,DC=microsoft,DC=com.” This string tells you that the schema operations master is CORPSERVER01 in the microsoft.com domain.

**NOTE** To determine which server is the current infrastructure operations master for the domain, start a command prompt and type `dsquery server –hasfsmo infr`.

After upgrading your servers, you can raise the domain and forest level functionality to take advantage of the latest Active Directory features. If you do this, you can use only Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 resources in the domain and you can’t go back to any other mode. You should
use Windows Server 2003 mode only when you’re certain that you don’t need old Windows NT domain structures, Windows NT backup domain controllers (BDCs), or Windows 2000 domain structures.

Using Windows Server 2008 Functional Level


Before updating Windows Server 2003 domain controllers, you should prepare the domain for Windows Server 2008. To do this, you need to use Adprep.exe to update the forest and the domain schema so that they are compatible with Windows Server 2008 domains. Follow these steps:

1. On the schema operations master in the forest, copy the contents of the Sources\Adprep folder from the Windows Server 2008 installation media to a local folder, and then run `adprep /forestprep`. If you plan to install any read-only domain controllers, you should also run `adprep /rodcprep`. You need to use an administrator account that is a member of Enterprise Admins, Schema Admins, or Domain Admins in the forest root domain.

2. On the infrastructure operations master for each domain in the forest, copy the contents of the Sources\Adprep folder from the Windows Server 2008 installation media to a local folder, and then run `adprep /domainprep /gpprep`. You need to use an account that is a member of the Domain Admins group in an applicable domain.

As always, you should test any procedure in a lab before performing it in a production environment.

**NOTE** To determine which server is the current schema operations master for the domain, start a command prompt and type `dsquery server –hasfsmo schema`. To determine which server is the current infrastructure operations master for the domain, start a command prompt and type `dsquery server –hasfsmo infr`.

After upgrading all domain controllers to Windows Server 2008, you can raise the domain and forest level functionality to take advantage of additional Active Directory features. If you do this, you can use only Windows Server 2008 or later resources in the domain and you can’t go back to any other mode. You should use Windows Server 2008 mode only when you’re certain that you don’t need old Windows NT domain structures, Windows NT BDCs, or Windows 2000 or Windows Server 2003 domain structures.
Using Windows Server 2008 R2 Functional Level


Before updating Windows Server 2008 domain controllers, you should prepare the domain for Windows Server 2008 R2. To do this, you need to use Adprep.exe to update the forest and the domain schema so that they are compatible with Windows Server 2008 R2 domains. Follow these steps:

1. On the schema operations master in the forest, copy the contents of the Support\Adprep folder from the Windows Server 2008 R2 installation media to a local folder, and then run adprep /forestprep. If you plan to install any read-only domain controllers, you should also run adprep /rodcprep. You need to use an administrator account that is a member of Enterprise Admins, Schema Admins, or Domain Admins in the forest root domain.

2. On the infrastructure operations master for each domain in the forest, copy the contents of the Support\Adprep folder from the Windows Server 2008 R2 installation media to a local folder, and then run adprep /domainprep /gpprep. You need to use an account that is a member of the Domain Admins group in an applicable domain.

As always, you should test any procedure in a lab before performing it in a production environment.

**NOTE** To determine which server is the current schema operations master for the domain, start a command prompt and type dsquery server –hasfsmo schema. To determine which server is the current infrastructure operations master for the domain, start a command prompt and type dsquery server –hasfsmo infr.

After upgrading all domain controllers to Windows Server 2008 R2, you can raise the domain and forest level functionality to take advantage of the latest Active Directory features. If you do this, you can use only Windows Server 2008 R2 resources in the domain and you can’t go back to any other mode. You should use Windows Server 2008 R2 mode only when you’re certain that you don’t need old Windows NT domain structures; Windows NT BDCs; or Windows 2000, Windows Server 2003, or Windows Server 2008 domain structures.

Raising Domain and Forest Functionality

Domains operating in Windows Server 2003 or higher functional level can use universal groups, group nesting, group type conversion, update logon time stamps, and Kerberos KDC key version numbers. In this mode or higher, administrators can do the following:

- Rename domain controllers without having to demote them first
- Rename domains running on Windows Server 2003 or higher domain controllers
- Create extended two-way trusts between two forests
- Restructure domains in the domain hierarchy by renaming them and putting them at different levels
- Take advantage of replication enhancements for individual group members and global catalogs

As compared to earlier implementations, forests operating in Windows Server 2003 or higher functional level have better global catalog replication and intrasite and intersite replication efficiency, as well as the ability to establish one-way, two-way, and transitive forest trusts.

**REAL WORLD** The domain and forest upgrade process can generate a lot of network traffic as information is being replicated around the network. Sometimes the entire upgrade process can take 15 minutes or longer. During this time you might experience delayed responsiveness when communicating with servers and higher latency on the network, so you might want to schedule the upgrade outside normal business hours. It’s also a good idea to thoroughly test compatibility with existing applications (especially legacy applications) before performing this operation.

You can raise the domain level functionality by following these steps:

1. Click Start, point to Administrative Tools, and then click Active Directory Domains And Trusts.
2. In the console tree, right-click the domain you want to work with, and then click Raise Domain Functional Level.
   
   The current domain name and functional level are displayed in the Raise Domain Functional Level dialog box.
3. To change the domain functionality, select the new domain functional level from the list provided, and then click Raise. You can’t reverse this action. Consider the implications carefully before you do this.
4. Click OK. The new domain functional level is replicated to each domain controller in the domain. This operation can take some time in a large organization.

You can raise the forest level functionality by following these steps:

1. Click Start, point to Administrative Tools, and then click Active Directory Domains And Trusts.
2. In the console tree, right-click the Active Directory Domains And Trusts node, and then click Raise Forest Functional Level.
   
   The current forest name and functional level are displayed in the Raise Forest Functional Level dialog box.
3. To change the forest functionality, select the new forest functional level by using the list provided, and then click Raise. You can’t reverse this action. Consider the implications carefully before you do this.
4. Click OK. The new forest functional level is replicated to each domain controller in each domain in the forest. This operation can take some time in a large organization.

**Understanding the Directory Structure**

Active Directory has many components and is built on many technologies. Directory data is made available to users and computers through data stores and global catalogs. Although most Active Directory tasks affect the data store, global catalogs are equally important because they’re used during logon and for information searches. In fact, if the global catalog is unavailable, standard users can’t log on to the domain. The only way to change this behavior is to cache universal group membership locally. As you might expect, caching universal group membership has advantages and disadvantages, which I’ll discuss in a moment.

You access and distribute Active Directory data by using directory access protocols and replication. Directory access protocols allow clients to communicate with computers running Active Directory. Replication is necessary to ensure that updates to data are distributed to domain controllers. Although multimaster replication is the primary technique that you use to distribute updates, some changes to data can be handled only by individual domain controllers called operations masters. A feature of Windows Server 2008 called *application directory partitions* also changes the way multimaster replication works.

With application directory partitions, enterprise administrators (those belonging to the Enterprise Admins group) can create replication partitions in the domain forest. These partitions are logical structures used to control replication of data within a domain forest. For example, you could create a partition to strictly control the replication of DNS information within a domain, thereby preventing other systems in the domain from replicating DNS information.

An application directory partition can appear as a child of a domain, a child of another application partition, or a new tree in the domain forest. Replicas of the application directory partition can be made available on any Active Directory domain controller running Windows Server 2008 or Windows Server 2008 R2, including global catalog servers. Although application directory partitions are useful in large domains and forests, they add overhead in terms of planning, administration, and maintenance.

**Exploring the Data Store**

The data store contains information about objects such as accounts, shared resources, OUs, and group policies. Another name for the data store is the *directory*, which refers to Active Directory itself.

Domain controllers store the directory in a file called Ntds.dit. This file’s location is set when Active Directory is installed, and it should be on an NTFS file system.
drive formatted for use with Windows Server 2008 or later. You can also save directory data separately from the main data store. This is true for group policies, scripts, and other types of public information stored on the shared system volume (SYSVOL).

Sharing directory information is called publishing. For example, you publish information about a printer by sharing the printer over the network. Similarly, you publish information about a folder by sharing the folder over the network.

Domain controllers replicate most changes to the data store in multimaster fashion. Administrators for small or medium-size organizations rarely need to manage replication of the data store. Replication is handled automatically, but you can customize it to meet the needs of large organizations or organizations with special requirements.

Not all directory data is replicated. Instead, only public information that falls into one of the following three categories is replicated:

- **Domain data**  Contains information about objects within a domain. This includes objects for accounts, shared resources, organizational units, and group policies.
- **Configuration data**  Describes the directory’s topology. This includes a list of all domains, domain trees, and forests, as well as the locations of the domain controllers and global catalog servers.
- **Schema data**  Describes all objects and data types that can be stored in the directory. The default schema provided with Windows Server 2008 R2 describes account objects, shared resource objects, and more. You can extend the default schema by defining new objects and attributes or by adding attributes to existing objects.

### Exploring Global Catalogs

When universal group membership isn’t cached locally, global catalogs enable network logon by providing universal group membership information when a logon process is initiated. Global catalogs also enable directory searches throughout the domains in a forest. A domain controller designated as a global catalog stores a full replica of all objects in the directory for its host domain and a partial replica for all other domains in the domain forest.

**NOTE**  Partial replicas are used because only certain object properties are needed for logon and search operations. Partial replication also means that less information needs to be circulated on the network, reducing the amount of network traffic.

By default, the first domain controller installed on a domain is designated as the global catalog. If only one domain controller is in the domain, the domain controller and the global catalog are the same server. Otherwise, the global catalog is on the domain controller that you’ve configured as such. You can also add global catalogs...
to a domain to help improve response time for logon and search requests. The recommended technique is to have one global catalog per site within a domain.

Domain controllers hosting the global catalog should be well connected to domain controllers acting as infrastructure masters. The role of infrastructure master is one of the five operations master roles that you can assign to a domain controller. In a domain, the infrastructure master is responsible for updating object references. The infrastructure master does this by comparing its data with that of a global catalog. If the infrastructure master finds outdated data, it requests updated data from a global catalog. The infrastructure master then replicates the changes to the other domain controllers in the domain. For more information on operations master roles, see “Understanding Operations Master Roles” later in this chapter.

When only one domain controller is in a domain, you can assign the infrastructure master role and the global catalog to the same domain controller. When two or more domain controllers are in the domain, however, the global catalog and the infrastructure master must be on separate domain controllers. If they aren’t, the infrastructure master won’t find out-of-date data and will never replicate changes. The only exception is when all domain controllers in the domain host the global catalog. In this case, it doesn’t matter which domain controller serves as the infrastructure master.

One of the key reasons to configure additional global catalogs in a domain is to ensure that a catalog is available to service logon and directory search requests. Again, if the domain has only one global catalog and the catalog isn’t available, and there’s no local caching of universal group membership, standard users can’t log on and those who are logged on can’t search the directory. In this scenario, the only users who can log on to the domain when the global catalog is unavailable are members of the Domain Admins group.

Searches in the global catalog are very efficient. The catalog contains information about objects in all domains in the forest. This allows directory search requests to be resolved in a local domain rather than in a domain in another part of the network. Resolving queries locally reduces the network load and allows for quicker responses in most cases.

**TIP** If you notice slow logon or query response times, you might want to configure additional global catalogs. But more global catalogs usually means more replication data being transferred over the network.

**Universal Group Membership Caching**

In a large organization, having global catalogs at every office location might not be practical. Not having global catalogs at every office location presents a problem, however, if a remote office loses connectivity with the main office or a designated branch office where global catalog servers reside. If this occurs, standard users won’t be able to log on; only members of Domain Admins will be able to log on.
This happens because logon requests must be routed over the network to a global catalog server at a different office, and this isn’t possible with no connectivity.

As you might expect, you can resolve this problem in many ways. You can make one of the domain controllers at the remote office a global catalog server by following the procedure discussed in “Configuring Global Catalogs” in Chapter 8. The disadvantage of this approach is that the designated server or servers will have an additional burden placed on them and might require additional resources. You also have to manage more carefully the uptime of the global catalog server.

Another way to resolve this problem is to cache universal group membership locally. Here, any domain controller can resolve logon requests locally without having to go through a global catalog server. This allows for faster logons and makes managing server outages much easier because your domain isn’t relying on a single server or a group of servers for logons. This solution also reduces replication traffic. Instead of replicating the entire global catalog periodically over the network, only the universal group membership information in the cache is refreshed. By default, a refresh occurs every eight hours on each domain controller that’s caching membership locally.

Universal group membership caching is site-specific. Remember, a site is a physical directory structure consisting of one or more subnets with a specific IP address range and network mask. The domain controllers running Windows Server and the global catalog they’re contacting must be in the same site. If you have multiple sites, you need to configure local caching in each site. Additionally, users in the site must be part of a Windows domain running in Windows Server 2003 or higher functional mode. To learn how to configure caching, see “Configuring Universal Group Membership Caching” in Chapter 8.

**Replication and Active Directory**

Regardless of whether you use FRS or DFS replication, the three types of information stored in the directory are domain data, schema data, and configuration data.

Domain data is replicated to all domain controllers within a particular domain. Schema and configuration data are replicated to all domains in the domain tree or forest. In addition, all objects in an individual domain and a subset of object properties in the domain forest are replicated to global catalogs.

This means that domain controllers store and replicate the following:

- Schema information for the domain tree or forest
- Configuration information for all domains in the domain tree or forest
- All directory objects and properties for their respective domains

However, domain controllers hosting a global catalog store and replicate schema information for the forest, configuration information for all domains in the forest, a subset of the properties for all directory objects in the forest that’s replicated only
between servers hosting global catalogs, and all directory objects and properties for their respective domain.

To get a better understanding of replication, consider the following scenario, in which you’re installing a new network:

1. Start by installing the first domain controller in domain A. The server is the only domain controller and also hosts the global catalog. No replication occurs because no other domain controllers are on the network.

2. Install a second domain controller in domain A. Because there are now two domain controllers, replication begins. To make sure that data is replicated properly, assign one domain controller as the infrastructure master and the other as the global catalog. The infrastructure master watches for updates to the global catalog and requests updates to changed objects. The two domain controllers also replicate schema and configuration data.

3. Install a third domain controller in domain A. This server isn’t a global catalog. The infrastructure master watches for updates to the global catalog, requests updates to changed objects, and then replicates those changes to the third domain controller. The three domain controllers also replicate schema and configuration data.

4. Install a new domain, domain B, and add domain controllers to it. The global catalog hosts in domain A and domain B begin replicating all schema and configuration data as well as a subset of the domain data in each domain. Replication within domain A continues as previously described. Replication within domain B begins.

**Active Directory and LDAP**

The Lightweight Directory Access Protocol (LDAP) is a standard Internet communications protocol for TCP/IP networks. LDAP is designed specifically for accessing directory services with the least amount of overhead. LDAP also defines operations that can be used to query and modify directory information.

Active Directory clients use LDAP to communicate with computers running Active Directory whenever they log on to the network or search for shared resources. You can also use LDAP to manage Active Directory.

LDAP is an open standard that many other directory services use. This makes interdirectory communications easier and provides a clearer migration path from other directory services to Active Directory. You can also use Active Directory Service Interface (ADSI) to enhance interoperability. ADSI supports the standard application programming interfaces (APIs) for LDAP that are specified in Internet standard Request for Comments (RFC) 1823. You can use ADSI with Windows Script Host to create and manage objects in Active Directory.
Understanding Operations Master Roles

Operations master roles accomplish tasks that are impractical to perform in multi-master fashion. Five operations master roles are defined, and you can assign these roles to one or more domain controllers. Although certain roles can be assigned only once in a domain forest, other roles must be defined once in each domain.

Every Active Directory forest must have the following roles:

- **Schema master**  Controls updates and modifications to directory schema. To update directory schema, you must have access to the schema master. To determine which server is the current schema master for the domain, start a command prompt and type `dsquery server –hasfsmo schema`.

- **Domain naming master**  Controls the addition or removal of domains in the forest. To add or remove domains, you must have access to the domain naming master. To determine which server is the current domain naming master for the domain, start a command prompt and type `dsquery server –hasfsmo name`.

These forestwide roles must be unique in the forest. This means that you can assign only one schema master and one domain naming master in a forest.

Every Active Directory domain must have the following roles:

- **Relative ID master**  Allocates relative IDs to domain controllers. Whenever you create a user, group, or computer object, domain controllers assign a unique security ID to the related object. The security ID consists of the domain’s security ID prefix and a unique relative ID allocated by the relative ID master. To determine which server is the current relative ID master for the domain, start a command prompt and type `dsquery server –hasfsmo rid`.

- **PDC emulator**  When you use mixed-mode or interim-mode operations, the PDC emulator acts as a Windows NT PDC. Its job is to authenticate Windows NT logons, process password changes, and replicate updates to BDCs. The PDC emulator is the default time server, and as such also performs time synchronization in a domain. To determine which server is the current PDC emulator master for the domain, start a command prompt and type `dsquery server –hasfsmo pdc`.

- **Infrastructure master**  Updates object references by comparing its directory data with that of a global catalog. If the data is outdated, the infrastructure master requests updated data from a global catalog and then replicates the changes to the other domain controllers in the domain. To determine which server is the current infrastructure operations master for the domain, start a command prompt and type `dsquery server –hasfsmo infr`.

These domainwide roles must be unique in each domain. This means that you can assign only one relative ID master, one PDC emulator, and one infrastructure master in each domain.
Operations master roles are usually assigned automatically, but you can reassign them. When you install a new network, the first domain controller in the first domain is assigned all the operations master roles. If you later create a child domain or a root domain in a new tree, the first domain controller in the new domain is automatically assigned operations master roles as well. In a new domain forest, the domain controller is assigned all operations master roles. If the new domain is in the same forest, the assigned roles are relative ID master, PDC emulator, and infrastructure master. The schema master and domain naming master roles remain in the first domain in the forest.

When a domain has only one domain controller, that computer handles all the operations master roles. If you’re working with a single site, the default operations master locations should be sufficient. As you add domain controllers and domains, however, you’ll probably want to move the operations master roles to other domain controllers.

When a domain has two or more domain controllers, you should configure two domain controllers to handle operations master roles. Here, you would make one domain controller the operations master, and you would designate the second as your standby operations master. The standby operations master could then be used if the primary one fails. Be sure that the domain controllers are direct replication partners and are well connected.

As the domain structure grows, you might want to split up the operations master roles and place them on separate domain controllers. This can improve the responsiveness of the operations masters. Pay particular attention to the current responsibilities of the domain controller you plan to use.

**BEST PRACTICES** Two roles that you should not separate are schema master and domain naming master. Always assign these roles to the same server. For the most efficient operations, you usually want the relative ID master and PDC emulator to be on the same server as well. But you can separate these roles if necessary. For example, on a large network where peak loads are causing performance problems, you would probably want to place the relative ID master and PDC emulator on separate domain controllers. Additionally, you usually shouldn’t place the infrastructure master on a domain controller hosting a global catalog. See “Exploring Global Catalogs” earlier in this chapter for details.

**Using the Active Directory Recycle Bin**

When your Active Directory forest is operating in the Windows Server 2008 R2 mode, you can use the Active Directory Recycle Bin. The Active Directory Recycle Bin adds an easy-to-use recovery feature for Active Directory objects. When you enable this feature, all link-valued and non-link-valued attributes of a deleted object are preserved, allowing you to restore the object to the same state it was in before it was deleted. You can also recover objects from the recycle bin without having to
initiate an authoritative restore. This differs substantially from the previously available technique, which used an authoritative restore to recover deleted objects from the Deleted Objects container. Previously, when you deleted an object, most of its non-link-valued attributes were cleared and all of its link-valued attributes were removed, which meant that although you could recover a deleted object, it was not restored to its previous state.

Preparing Schema for the Recycle Bin
Before you can make the recycle bin available, you must update Active Directory schema with the required recycle bin attributes, as discussed earlier in “Using Windows Server 2008 R2 Functional Level.” When you do this, the schema is updated, and then every object in the forest is updated with the recycle bin attributes as well. This process is irreversible once it is started.

After you prepare Active Directory, you need to upgrade all domain controllers in your Active Directory forest to Windows Server 2008 R2 and then raise the domain and forest functional levels to the Windows Server 2008 R2 level.

After these operations, you can access the recycle bin. From now on, when an Active Directory object is deleted, the object is put in a state referred to as logically deleted, moved to the Deleted Objects container, and its distinguished name is altered. A deleted object remains in the Deleted Objects container for the period of time set in the delete object lifetime value, which is 180 days by default.

REAL WORLD The msDS-deletedObjectLifetime attribute replaces the tombstone-Lifetime attribute. However, when msDS-deletedObjectLifetime is set to $null, the lifetime value comes from the tombstoneLifetime. If the tombstoneLifetime is also set to $null, the default value is 180 days.

Recovering Deleted Objects
You can recover deleted objects from the Deleted Objects container by using an authoritative restore. The procedure has not changed from previous releases of Windows Server. What has changed, however, is the fact that the objects are restored to their previous state with all link-valued and non-link-valued attributes preserved. To perform an authoritative restore, the domain controller must be in Directory Services Restore Mode.

Rather than using an authoritative restore and taking a domain controller offline, you can recover deleted objects by using the Ldp.exe administration tool or the Active Directory cmdlets for Windows PowerShell. Keep in mind that Active Directory blocks access to an object for a short while after it is deleted. During this time, Active Directory processes the object’s link-value table to maintain referential integrity on the linked attribute’s values. Active Directory then permits access to the deleted object.
Using Ldp.exe for Basic Recovery

You can use Ldp.exe to display the Deleted Objects container and recover a deleted object by following these steps:

1. Click Start, type **Ldp.exe** in the Search box, and then press Enter.
2. On the Options menu, click Controls. In the Controls dialog box, select Return Deleted Objects in the Load Predefined list, and then click OK.
3. Bind to the server that hosts the forest root domain by choosing Bind from the Connection menu. Select the Bind type, and then click OK.
4. On the View menu, click Tree. In the Tree View dialog box, use the BaseDN list to select the appropriate forest root domain name, such as DC=Cpandl,DC=Com, and then click OK.
5. In the console tree, double-click the root distinguished name and locate the CN=Deleted Objects container.
6. Locate and right-click the Active Directory object that you want to restore, and then click Modify. This displays the Modify dialog box.
7. In the Edit Entry Attribute text box, type **isDeleted**. Do not enter anything in the Values text box.
8. Under Operation, click Delete, and then click Enter.
9. In the Edit Entry Attribute text box, type **distinguishedName**. In Values, type the original distinguished name of this Active Directory object.
10. Under Operation, click Replace. Select the Extended check box, click Enter, and then click Run.

Using Windows PowerShell for Basic and Advanced Recovery

You can also use the Active Directory cmdlets for Windows PowerShell to recover deleted objects. You use Get-ADObject to retrieve the object or objects you want to restore, pass that object or objects to Restore-ADObject, and then Restore-ADObject restores the object or objects to the directory database.

**NOTE** The Active Directory module is not imported into Windows PowerShell by default. You need to import the module before you can use the cmdlets it provides. For more information, see “Active Directory Administrative Center and Windows PowerShell” in Chapter 8.

To use the Active Directory cmdlets for recovery, you need to open an elevated, administrator PowerShell prompt by right-clicking the Windows PowerShell entry on the menu and clicking Run As Administrator. The basic syntax for recovering an object is as follows:

```
Get-ADObject -Filter {ObjectId} -IncludeDeletedObjects | Restore-ADObject
```
ObjectId is a filter value that identifies the object you want to restore. For example, you could restore a deleted user account by display name or SAM account name as shown in these examples:

```
Get-ADObject -Filter {DisplayName -eq "Rich Haddock"} -IncludeDeletedObjects | Restore-ADObject

Get-ADObject -Filter {SamAccountName -eq "richh"} -IncludeDeletedObjects | Restore-ADObject
```

It’s important to note that nested objects must be recovered from the highest-level of the deleted hierarchy to a live parent container. For example, if you accidentally deleted an OU and all its related accounts, you need to restore the OU before you can restore the related accounts.

The basic syntax for restoring container objects such as an OU is as follows:

```
Get-ADObject -ldapFilter: "(msDS-LastKnownRDN=ContainerID)" -IncludeDeletedObjects | Restore-ADObject
```

ContainerID is a filter value that identifies the container object you want to restore. For example, you could restore the Corporate Services OU as shown in this example:

```
Get-ADObject -ldapFilter: "(msDS-LastKnownRDN=Corporate_Services)" -IncludeDeletedObjects | Restore-ADObject
```

If the OU contains accounts you also want to restore, you can now restore the accounts by using the technique discussed previously, or you can restore all accounts at the same time. The basic syntax requires that you establish a search base and associate the accounts with their last known parent, as shown here:

```
Get-ADObject -SearchBase "CN=Deleted Objects,ForestRootDN" -Filter {lastKnownParent -eq "ContainerCN,ForestRootDN"} -IncludeDeletedObjects | Restore-ADObject
```

ForestRootDN is the distinguished name of the forest root domain, such as DC=Cpandl,DC=Com, and ContainerCN is the common name of the container, such as OU=Corporate_Services or CN=Users. The following example restores all the accounts that were in the Corporate Services OU when it was deleted:

```
Get-ADObject -SearchBase "CN=Deleted Objects,DC=Cpandl,DC=com" -Filter {lastKnownParent -eq "OU=Corporate_Services,DC=Cpandl,DC=com"} -IncludeDeletedObjects | Restore-ADObject
```
Managing File Systems and Drives

- Managing the File Services Role 357
- Adding Hard Disk Drives 363
- Working with Basic, Dynamic, and Virtual Disks 372
- Using Basic Disks and Partitions 378
- Managing Existing Partitions and Drives 384

A hard disk drive is the most common storage device used on network workstations and servers. Users depend on hard disk drives to store their word-processing documents, spreadsheets, and other types of data. Drives are organized into file systems that users can access either locally or remotely.

Local file systems are installed on a user’s computer and can be accessed without remote network connections. The C drive available on most workstations and servers is an example of a local file system. You access the C drive using the file path C:\.

On the other hand, you access remote file systems through a network connection to a remote resource. You can connect to a remote file system using the Map Network Drive feature of Windows Explorer.

Wherever disk resources are located, your job as a system administrator is to manage them. The tools and techniques you use to manage file systems and drives are discussed in this chapter. Chapter 13, “Administering Volume Sets and RAID Arrays,” looks at volume sets and fault tolerance.

Managing the File Services Role

A file server provides a central location for storing and sharing files across the network. When many users require access to the same files and application data, you should configure file servers in the domain. In earlier releases of the Windows
Server operating system, all servers were installed with basic file services. With Windows Server 2008 R2, you must specifically configure a server to be a file server by adding the File Services role and configuring this role to use the appropriate role services.

Table 12-1 provides an overview of the role services associated with the File Services role. When you install the File Services role, you might also want to install the following optional features, available through the Add Features Wizard:

- **Windows Server Backup** The backup utility included with Windows Server 2008 R2.
- **Storage Manager for SANs** Allows you to provision storage for storage area networks (SANs).
- **Multipath I/O** Provides support for using multiple data paths between a file server and a storage device. Servers use multiple I/O paths for redundancy in case of the failure of a path and to improve transfer performance.

**Table 12-1 Role Services for File Servers**

<table>
<thead>
<tr>
<th>ROLE SERVICE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>BranchCache For Network Files</td>
<td>Enables computers in a branch office to cache commonly used files from shared folders.</td>
</tr>
<tr>
<td>Distributed File System (DFS)</td>
<td>Provides tools and services for DFS Namespaces and DFS Replication. DFS Replication is a newer and preferred replication technology. When a domain is running in Windows 2008 domain functional level, domain controllers use DFS Replication to provide more robust and granular replication of the SYSVOL directory.</td>
</tr>
<tr>
<td>DFS Namespaces</td>
<td>Allows you to group shared folders located on different servers into one or more logically structured namespaces. Each namespace appears as a single shared folder with a series of subfolders. However, the underlying structure of a namespace can come from shared folders on multiple servers in different sites.</td>
</tr>
<tr>
<td>DFS Replication</td>
<td>Allows you to synchronize folders on multiple servers across local or wide area network connections using a multimaster replication engine. The replication engine uses the Remote Differential Compression (RDC) protocol to synchronize only the portions of files that have changed since the last replication. You can use DFS Replication with DFS Namespaces or by itself.</td>
</tr>
</tbody>
</table>
### Role Service | Description
--- | ---
File Server Resource Manager (FSRM) | Installs a suite of tools that administrators can use to better manage data stored on servers. Using FSRM, administrators can generate storage reports, configure quotas, and define file-screening policies.

Indexing Service | Allows indexing of files and folders for faster searching. Using the related query language, users can find files quickly. You cannot install Indexing Service and Windows Search Service on the same computer.

Services for Network File System | Provides a file sharing solution for enterprises with a mixed Windows and UNIX environment. When you install Services for Network File System (NFS), users can transfer files between Windows Server 2008 R2 and UNIX operating systems by using the NFS protocol.

Windows Search Service | Enables fast file searches of resources on the server from clients that are compatible with Windows Search Service. This feature is designed primarily for desktop and small office implementations.


You can add the File Services role to a server by following these steps:

1. In Server Manager, select the Roles node in the left pane, and then click Add Roles. This starts the Add Roles Wizard. If the wizard displays the Before You Begin page, read the Welcome text, and then click Next.

   **Note** During the setup process, shared files are created on the server. If you encounter a problem that causes the setup process to fail, you need to resume the setup process using the Add Role Services Wizard. After you restart Server Manager, select the File Services node under Roles. In the main pane, scroll down and then click Add Role Services. You can continue with the installation starting with step 3. If you were in the process of configuring domain-based DFS, you need to provide administrator credentials.

2. On the Select Server Roles page, select File Services, and then click Next twice.

3. On the Select Role Services page, select one or more role services to install. A summary of each role service is provided in Table 12-1. To allow for interoperability with UNIX, be sure to add Services for Network File System. Click Next.
4. A DFS namespace is a virtual view of shared folders located on different servers. To install DFS Namespaces, you work with several additional configuration pages:

- On the Create A DFS Namespace page, set the root name for the first namespace or elect to create a namespace later, as shown in the following screen. The namespace root name should be something that is easy for users to remember, such as CorpData. In a large enterprise, you may need to create separate namespaces for each major division.

- On the Select Namespace Type page, specify whether you want to create a domain-based namespace or a stand-alone namespace, as shown in the following screen. Domain-based namespaces can be replicated with multiple namespace servers to provide high availability, but they can have only up to 5,000 DFS folders. Stand-alone namespaces can have up to 50,000 DFS folders, but they are replicated only when you use failover server clusters and configure replication.

- If you are creating a domain-based namespace, on the Provide Credentials To Create A Namespace page, click Select, and then specify the user name and password for an account that is a member of the Domain Admins groups. This account is used to create the namespace.

- On the Configure Namespace page, you can add shared folders to the namespace as well as namespaces that are associated with a DFS folder, as shown in the following screen. Click Add. In the Add Folder To Namespace dialog box, click Browse. In the Browse For Shared Folders dialog box, select the shared folder to add, and then click OK. Type a
name for the folder to add, and then click OK. Next, type a name for the folder in the namespace. This name can be the same as the original folder name or a new name that will be associated with the original folder in the namespace. After you type a name, click OK to add the folder and complete the process.

**NOTE** You do not have to configure DFS Namespaces at this time. Once you install DFS Namespaces, DFS Replication, or both, you can use the DFS Management console to manage the related features. This console is installed and available on the Administrative Tools menu. See Chapter 15, “Data Sharing, Security, and Auditing,” for more information.

5. With File Server Resource Manager, you can monitor the amount of space used on disk volumes and create storage reports. To install File Server Resource Manager, you work with two additional configuration pages:

- On the Configure Storage Usage Monitoring page, select disk volumes for monitoring as shown in the following screen. When you select a volume and then click Options, you can set the volume usage threshold and choose the reports to generate when the volume reaches the threshold value. By default, the usage threshold is 85 percent.
On the Set Report Options page, you can select a save location for usage reports, as shown in the following screen. One usage report of each type you select is generated each time a volume reaches its threshold. Old reports are not automatically deleted. The default save location is %SystemDrive%\StorageReports. To change the default location, click Browse, and then select the new save location in the Browse For Folder dialog box. You can also elect to receive reports by e-mail. To do this, you must specify the recipient e-mail addresses and the SMTP server to use.

![Screen shot of Set Report Options page](image.png)

**NOTE** You do not have to configure monitoring and reporting at this time. After you install FSRM, you can use the File Server Resource Manager console to manage the related features. This console is installed and available on the Administrative Tools menu.

6. To install Windows Search Service, you work with an additional configuration page that allows you to select the volumes to index. Indexing a volume makes it possible for users to search a volume quickly. However, indexing entire volumes can affect service performance, especially if you index the system volume. Therefore, you may want to index only specific shared folders on volumes, which you can do later on a per-folder basis.

**NOTE** You do not have to configure indexing at this time. After you install Windows Search Service, you can use the Indexing Options utility in Control Panel to manage the related features.

7. After you complete the optional pages, click Next. You’ll see the Confirm Installation Options page. Click Install to begin the installation process. When Setup finishes installing the server with the features you selected, you’ll see the Installation Results page. Review the installation details to ensure that all phases of the installation were completed successfully.

If the File Services role is installed already on a server and you want to install additional services for a file server, you can add role services to the server by using a similar process. In Server Manager, expand the Roles node, and then select the File
Adding Hard Disk Drives

Before you make a hard disk drive available to users, you need to configure it and consider how it will be used. With Windows Server 2008 R2, you can configure hard disk drives in a variety of ways. The technique you choose depends primarily on the type of data you’re working with and the needs of your network environment. For general user data stored on workstations, you might want to configure individual drives as stand-alone storage devices. In that case, user data is stored on a workstation’s hard disk drive, where it can be accessed and stored locally.

Although storing data on a single drive is convenient, it isn’t the most reliable way to store data. To improve reliability and performance, you might want a set of drives to work together. Windows Server 2008 R2 supports drive sets and arrays using redundant array of independent disks (RAID) technology, which is built into the operating system.

Physical Drives

Whether you use individual drives or drive sets, you need physical drives. Physical drives are the actual hardware devices that are used to store data. The amount of data a drive can store depends on its size and whether it uses compression. Typical drives have capacities of 500 gigabytes (GB) to 2 terabytes (TB). Many drive types are available for use with Windows Server 2008 R2, including Small Computer System Interface (SCSI), Parallel ATA (PATA), and Serial ATA (SATA).

The terms SCSI, PATA, and SATA designate the interface type used by the hard disk drives. This interface is used to communicate with a drive controller. SCSI drives use SCSI controllers, PATA drives use PATA controllers, and so on. When setting up a new server, you should give considerable thought to the drive configuration. Start by choosing drives or storage systems that provide the appropriate level of performance. There really is a substantial difference in speed and performance among various drive specifications.

You should consider not only the capacity of the drive but also the following:

- **Rotational speed**  A measurement of how fast the disk spins
- **Average seek time**  A measurement of how long it takes to seek between disk tracks during sequential input/output (I/O) operations

Generally speaking, when comparing drives that conform to the same specification, such as Ultra320 SCSI or SATA II, the higher the rotational speed (measured in thousands of rotations per minute) and the lower the average seek time (measured in milliseconds, or msecs), the better. As an example, a drive with a rotational speed...
of 15,000 RPM gives you 45–50 percent more I/O per second than the average
10,000 RPM drive, all other things being equal. A drive with a seek time of 3.5 msec
gives you a 25–30 percent response time improvement over a drive with a seek time
of 4.7 msec.

Other factors to consider include the following:

- **Maximum sustained data transfer rate**  A measurement of how much
data the drive can continuously transfer

- **Mean time to failure (MTTF)**  A measurement of how many hours of
operation you can expect to get from the drive before it fails

- **Nonoperational temperatures**  Measurements of the temperatures at
which the drive fails

Most drives of comparable quality have similar transfer rates and MTTF. For
example, if you compare Ultra320 SCSI drives with 15,000 RPM rotational speed
from different vendors, you will probably find similar transfer rates and MTTF. For
example, the Maxtor Atlas 15K II has a maximum sustained data transfer rate of up
to 98 megabytes per second (MBps). The Seagate Cheetah 15K.4 has a maximum
sustained data transfer rate of up to 96 MBps. Both have an MTTF of 1.4 million
hours. Transfer rates can also be expressed in gigabits per second (Gbps). A rate of
1.5 Gbps is equivalent to a data rate of 187.5 MBps, and 3.0 Gbps is equivalent to
375 MBps. Sometimes you'll see a maximum external transfer rate (per the speci-
fication to which the drive complies) and an average sustained transfer rate. The
average sustained transfer rate is the most important factor. The Seagate Barracuda
7200 SATA II drive has a rotational speed of 7,200 RPM and an average sustained
transfer rate of 58 MBps. With an average seek time of 8.5 msec and an MTTF of
1 million hours, the drive performs comparably to other 7,200 RPM SATA II drives.
However, most Ultra320 SCSI drives perform better and are better at multiuser read/
write operations, too.

**NOTE**  Don’t confuse MBps and Mbps. MBps is megabytes per second. Mbps is
megabits per second. Because there are 8 bits in a byte, a 100 MBps transfer rate is
equivalent to an 800 Mbps transfer rate. With SATA, the maximum data transfer rate
is usually around 150 MBps or 300 MBps. With PATA, the maximum data transfer
rate is usually around 100 MBps.

Temperature is another important factor to consider when you’re selecting a
drive, but it’s a factor few administrators take into account. Typically, the faster a
drive rotates, the hotter it runs. This is not always the case, but it is certainly some-
thing you should consider when making your choice. For example, 15K drives tend
to run hot, and you must be sure to carefully regulate temperature. Both the Maxtor
Atlas 15K II and the Seagate Cheetah 15K.4 can become nonoperational at tempera-
tures of 70 degrees Centigrade or higher (as would most other drives).
Preparing a Physical Drive for Use

After you install a drive, you need to configure it for use. You configure the drive by partitioning it and creating file systems in the partitions as needed. A partition is a section of a physical drive that functions as if it were a separate unit. After you create a partition, you can create a file system in the partition.

Two partition styles are used for disks: master boot record (MBR) and GUID partition table (GPT). The MBR contains a partition table that describes where the partitions are located on the disk. With this partition style, the first sector on a hard disk contains the master boot record and a binary code file called the master boot code that’s used to boot the system. This sector is unpartitioned and hidden from view to protect the system.

With the MBR partitioning style, disks support volumes of up to 4 terabytes (TB) and use one of two types of partitions—primary or extended. Each MBR drive can have up to four primary partitions or three primary partitions and one extended partition. Primary partitions are drive sections that you can access directly for file storage. You make a primary partition accessible to users by creating a file system on it. Although you can access primary partitions directly, you can’t access extended partitions directly. Instead, you can configure extended partitions with one or more logical drives that are used to store files. Being able to divide extended partitions into logical drives allows you to divide a physical drive into more than four sections.

GPT was originally developed for high-performance Itanium-based computers. GPT is recommended for disks larger than 2 TB on x86 and x64 systems or any disks used on Itanium-based computers. The key difference between the GPT partition style and the MBR partition style has to do with how partition data is stored. With GPT, critical partition data is stored in the individual partitions, and redundant primary and backup partition tables are used for improved structural integrity. Additionally, GPT disks support volumes of up to 18 exabytes and as many as 128 partitions. Although the GPT and MBR partitioning styles have underlying differences, most disk-related tasks are performed in the same way.

Using Disk Management

You use the Disk Management snap-in for the Microsoft Management Console (MMC) to configure drives. Disk Management makes it easy to work with the internal and external drives on a local or remote system. Disk Management is included as part of the Computer Management console and the Server Manager console. You can also add it to custom MMCs. In Computer Management and in Server Manager, you can access Disk Management by expanding the Storage node and then selecting Disk Management.

Regardless of whether you are using Computer Management or Server Manager, Disk Management has three views: Disk List, Graphical View, and Volume List. With remote systems you’re limited in the tasks you can perform with Disk Management. Remote management tasks you can perform include viewing drive details, changing
drive letters and paths, and converting disk types. With removable media drives, you can also eject media remotely. To perform more advanced manipulation of remote drives, you can use the DiskPart command-line utility.

**NOTE** Before you work with Disk Management, you should know several things. If you create a partition but don’t format it, the partition is labeled as Free Space. If you haven’t assigned a portion of the disk to a partition, this section of the disk is labeled Unallocated.

In Figure 12-1, the Volume List view is in the upper-right corner and Graphical View is used in the lower-right corner. This is the default configuration. You can change the view for the top or bottom pane as follows:

- To change the top view, select View, choose Top, and then select the view you want to use.
- To change the bottom view, select View, choose Bottom, and then select the view you want to use.
- To hide the bottom view, select View, choose Bottom, and then select Hidden.

![Figure 12-1](image-url)

**FIGURE 12-1** In Disk Management, the upper view provides a detailed summary of all the drives on the computer and the lower view provides an overview of the same drives by default.

Windows Server 2008 R2 supports four types of disk configurations:

- **Basic**  The standard fixed disk type used in previous versions of Windows. Basic disks are divided into partitions and can be used with previous versions of Windows.

- **Dynamic**  An enhanced fixed disk type for Windows Server 2008 R2 that you can update without having to restart the system (in most cases). Dynamic disks are divided into volumes and can be used only with Windows 2000 and later releases of Windows.
Removable  The standard disk type associated with removable storage devices. Removable storage devices can be formatted with exFAT, FAT, FAT32, or NTFS.

Virtual  The virtual hard disk (VHD) disk type associated with virtualization can be used when a computer is running Windows 7, Windows Server 2008 R2, or later releases. Computers can use VHDs just like they use regular fixed disks and can even be configured to boot from a VHD.

**REAL WORLD**  Windows Vista with SP1 or later, Windows 7, and Windows Server 2008 or later all support exFAT with removable storage devices. The exFAT file system is the next generation file system in the FAT (FAT12/16, FAT32) family. While retaining the ease-of-use advantages of FAT32, exFAT overcomes the 4-GB file size limit on FAT32 and its 32-GB partition size limit on Windows systems. The exFAT file system also supports allocation unit sizes of up to 32,768 KB.

The exFAT file system is designed so that it can be used with any compliant operating system or device. This means you can remove an exFAT storage device from a compliant camera and insert it into a compliant phone or vice versa without having to do any reformatting. It also means that you can remove an exFAT storage device from a computer running Mac OS or Linux and insert it into a computer running Windows.

From the Disk Management window, you can get more detailed information on a drive section by right-clicking it and then selecting Properties. When you do this, you see a dialog box. With fixed disks, the dialog box is much like the one shown on the left in Figure 12-2. With removable disks, the dialog box is much like the one shown on the right in Figure 12-2. This is the same dialog box that you can open from Windows Explorer (by selecting the top-level folder for the drive and then choosing Properties from the File menu).

**FIGURE 12-2**  The General tab of the Properties dialog box provides detailed information about a drive.
If you've configured remote management through Server Manager and MMCs, as discussed in Chapter 3, “Managing Servers Running Windows Server 2008 R2,” you can use Disk Management to configure and work with disks on remote computers. Keep in mind, however, that your options are slightly different from when you are working with the disks on a local computer. Tasks you can perform include:

- Viewing limited disk properties but not volume properties. When you are viewing disk properties, you’ll see only the General and Volumes tabs. You won’t be able to see volume properties.
- Changing drive letters and mount paths.
- Formatting, shrinking, and extending volumes. With mirrored, spanned, and striped volumes, you are able to add and configure related options.
- Deleting volumes (except for system and boot volumes)
- Creating, attaching, and detaching VHDs. When you create and attach VHDs, you need to enter the full file path and won’t be able to browse for the .vhd file.

Some tasks you perform with disks and volumes depend on the Plug and Play and Remote Registry services.

Removable Storage Devices

Removable storage devices can be formatted with NTFS, FAT, FAT32, or exFAT. You connect external storage devices to a computer rather than installing them inside the computer. This makes external storage devices easier and faster to install than most fixed disk drives. Most external storage devices have either a universal serial bus (USB) or a FireWire interface. When working with USB and FireWire, the transfer speed and overall performance of the device from a user’s perspective depends primarily on the version supported. Currently, several versions of USB and FireWire are used, including USB 1.0, USB 1.1, USB 2.0, FireWire 400, and FireWire 800.

USB 2.0 is the industry standard, and it supports data transfers at a maximum rate of 480 Mbps, with sustained data transfer rates usually from 10–30 Mbps. The actual sustainable transfer rate depends on many factors, including the type of device, the data you are transferring, and the speed of a computer. Each USB controller on a computer has a fixed amount of bandwidth, which all devices attached to the controller must share. The data transfer rates are significantly slower if a computer’s USB port is an earlier version than the device you are using. For example, if you connect a USB 2.0 device to a USB 1.0 port or vice versa, the device operates at the significantly reduced USB 1.0 transfer speed.

USB 1.0, 1.1, and 2.0 ports all look alike. The best way to determine which type of USB ports a computer has is to refer to the documentation that comes with the computer. Newer LCD monitors have USB 2.0 ports to which you can connect devices as well. When you have USB devices connected to a monitor, the monitor acts like a USB hub device. As with any USB hub device, all devices attached to the
hub share the same bandwidth, and the total available bandwidth is determined by the speed of the USB input to which the hub is connected on a computer.

FireWire (IEEE 1394) is a high-performance connection standard that uses a peer-to-peer architecture in which peripherals negotiate bus conflicts to determine which device can best control a data transfer. Like USB, several versions of FireWire currently are used, including FireWire 400 and FireWire 800. FireWire 400 (IEEE 1394a) has maximum sustained transfer rates of up to 400 Mbps. FireWire 800 (IEEE 1394b) has maximum sustained transfer rates of up to 800 Mbps. As with USB, if you connect a FireWire 800 device to a FireWire 400 port or vice versa, the device operates at the significantly reduced FireWire 400 transfer speed.

FireWire 400 and FireWire 800 ports and cables have different shapes, making it easier to tell the difference between them—if you know what you’re looking for. FireWire 400 cables without bus power have four pins and four connectors. FireWire 400 cables with bus power have six pins and six connectors. FireWire 800 cables always have bus power and have nine pins and nine connectors.

Another option is External Serial ATA (eSATA), which is available on newer computers and is an ultra-high-performance connection for data transfer to and from external mass storage devices. eSATA operates at speeds up to 3 Gbps. You can add support for eSATA devices by installing an eSATA controller card.

When you are purchasing an external device for a computer, you’ll also want to consider what interfaces it supports. In some cases, you may be able to get a device with a dual interface that supports USB 2.0 and FireWire 400, or a triple interface that supports USB 2.0, FireWire 400, and FireWire 800. A device with dual or triple interfaces gives you more options. There also are devices with quadruple interfaces.

Working with removable disks is similar to working with fixed disks. You can do the following:

- Right-click a removable disk and select Open or Explore to examine the disk’s contents in Windows Explorer.
- Right-click a removable disk and select Format to format a removable disk as discussed in “Formatting Partitions” later in this chapter. Removable disks generally are formatted with a single partition.
- Right-click a removable disk and select Properties to view or set properties. On the General tab of the Properties dialog box, you can set the volume label as discussed in “Changing or Deleting the Volume Label” later in this chapter.

When you work with removable disks, you can customize disk and folder views. To do this, right-click the disk or folder, select Properties, and then click the Customize tab. You can then specify the default folder type to control the default details displayed. For example, you can set the default folder type as Documents or Pictures And Videos. You can also set folder pictures and folder icons.

Removable disks support network file and folder sharing. You configure sharing on removable disks in the same way that you configure standard file sharing. You
can assign share permissions, configure caching options for offline file use, and limit the number of simultaneous users. You can share an entire removable disk as well as individual folders stored on the removable disk. You can also create multiple share instances.

Removable disks differ from standard NTFS sharing in that they don’t necessarily have an underlying security architecture. With exFAT, FAT, or FAT32, folders and files stored on a removable disk do not have any security permissions or features other than the basic read-only or hidden attribute flags that you can set.

Installing and Checking for a New Drive

Hot swapping is a feature that allows you to remove devices without shutting off the computer. Typically, hot-swappable drives are installed and removed from the front of the computer. If your computer supports hot swapping of drives, you can install drives without having to shut down. After you do this, open Disk Management, and then choose Rescan Disks from the Action menu. New disks that are found are added with the appropriate disk type. If a disk that you’ve added isn’t found, reboot.

If the computer doesn’t support hot swapping of drives, you must turn the computer off and then install the new drives. Then you can scan for new disks as described previously. If you are working with new disks that have not been initialized—meaning they don’t have disk signatures—Disk Management will start the Initialize Disk dialog box as soon it starts up and detects the new disks.

You can initialize the disks by following these steps:

1. Each disk you install needs to be initialized. Select the disk or disks that you installed.
2. Disks can use either the MBR or GPT partition style. Select the partition style you want to use for the disk or disks you are initializing.
3. Click OK. If you elected to initialize disks, Windows writes a disk signature to the disks and initializes the disks with the basic disk type.

If you don’t want to use the Initialize Disk dialog box, you can close it and use Disk Management instead to view and work with the disk. In the Disk List view, the disk is marked with a red downward pointing arrow icon, the disk’s type is listed as Unknown, and the disk’s status is listed as Not Initialized. You can then right-click the disk’s icon and select Online. Right-click the disk’s icon again, and select Initialize Disk. You can then initialize the disk as discussed previously.

Understanding Drive Status

Knowing the status of a drive is useful when you install new drives or troubleshoot drive problems. Disk Management shows the drive status in Graphical View and Volume List view. Table 12-2 summarizes the most common status values.
<table>
<thead>
<tr>
<th>STATUS</th>
<th>DESCRIPTION</th>
<th>RESOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
<td>The normal disk status. It means the disk is accessible and doesn’t have problems. Both dynamic disks and basic disks display this status.</td>
<td>The drive doesn’t have any known problems. You don’t need to take any corrective action.</td>
</tr>
</tbody>
</table>
### Statuses and Resolutions

<table>
<thead>
<tr>
<th>STATUS</th>
<th>DESCRIPTION</th>
<th>RESOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unrecognized</td>
<td>The disk is of an unknown type and can’t be used on the system. A drive from a non-Windows system might display this status.</td>
<td>If the disk is from another operating system, don’t do anything. You can’t use the drive on the computer, so try a different drive.</td>
</tr>
<tr>
<td>Not Initialized</td>
<td>The disk doesn’t have a valid signature. A drive from a non-Windows system might display this status.</td>
<td>If the disk is from another operating system, don’t do anything. You can’t use the drive on the computer, so try a different drive. To prepare the disk for use on Windows Server 2008 R2, right-click the disk, and then click Initialize Disk.</td>
</tr>
<tr>
<td>No Media</td>
<td>No media has been inserted into the CD-ROM or removable drive, or the media has been removed. Only CD-ROM and removable disk types display this status.</td>
<td>Insert a CD-ROM, a floppy disk, or a removable disk to bring the disk online. With FireWire and USB card readers, this status is usually (but not always) displayed when the card is removed.</td>
</tr>
</tbody>
</table>

### Working with Basic, Dynamic, and Virtual Disks

Windows Server 2008 R2 supports basic, dynamic, and virtual disk configurations. This section discusses techniques for working with each disk configuration type.

*NOTE* You can’t use dynamic disks on portable computers or with removable media.

### Using Basic and Dynamic Disks

Normally, Windows Server 2008 R2 disk partitions are initialized as basic disks. You can’t create new fault-tolerant drive sets using the basic disk type. You need to convert to dynamic disks and then create volumes that use striping, mirroring, or striping with parity (referred to as RAID 0, 1, and 5 respectively). The fault-tolerant features and the ability to modify disks without having to restart the computer are the key capabilities that distinguish dynamic disks from basic disks. Other features available on a disk depend on the disk formatting.

You can use both basic and dynamic disks on the same computer. However, volume sets must use the same disk type and partitioning style. For example, if you want to mirror drives C and D, both drives must have the dynamic disk type and use...
the same partitioning style, which can be either MBR or GPT. Note that Disk Management allows you to start many disk configuration tasks regardless of whether the disks you are working with use the dynamic disk type. The catch is that during the configuration process Disk Management will convert the disks to the dynamic disk type. To learn how to convert a disk from basic to dynamic, see “Changing Drive Types” on the next page.

You can perform different disk configuration tasks with basic and dynamic disks. With basic disks, you can do the following:

- Format partitions and mark them as active
- Create and delete primary and extended partitions
- Create and delete logical drives within extended partitions
- Convert from a basic disk to a dynamic disk

With dynamic disks, you can do the following:

- Create and delete simple, striped, spanned, mirrored, and RAID-5 volumes
- Remove a mirror from a mirrored volume
- Extend simple or spanned volumes
- Split a volume into two volumes
- Repair mirrored or RAID-5 volumes
- Reactivate a missing or offline disk
- Revert to a basic disk from a dynamic disk (requires deleting volumes and restoring from backup)

With either disk type, you can do the following:

- View properties of disks, partitions, and volumes
- Make drive letter assignments
- Configure security and drive sharing

**Special Considerations for Basic and Dynamic Disks**

Whether you’re working with basic or dynamic disks, you need to keep in mind five special types of drive sections:

- **Active** The active partition or volume is the drive section for system caching and startup. Some devices with removable storage may be listed as having an active partition.

- **Boot** The boot partition or volume contains the operating system and its support files. The system and boot partition or volume can be the same.

- **Crash dump** The partition to which the computer attempts to write dump files in the event of a system crash. By default, dump files are written to the %SystemRoot% folder, but they can be located on any partition or volume.
- **Page file**  A partition containing a paging file used by the operating system. Because a computer can page memory to multiple disks, according to the way virtual memory is configured, a computer can have multiple page file partitions or volumes.

- **System**  The system partition or volume contains the hardware-specific files needed to load the operating system. The system partition or volume can’t be part of a striped or spanned volume.

**NOTE**  You can mark a partition as active using Disk Management. In Disk Management, right-click the primary partition you want to mark as active, and then click Mark Partition As Active. You can’t mark dynamic disk volumes as active. When you convert a basic disk containing the active partition to a dynamic disk, this partition becomes a simple volume that’s active automatically.

### Changing Drive Types

Basic disks are designed to be used with previous versions of Windows. Dynamic disks are designed to let you take advantage of the latest Windows features. Only computers running Windows 2000 or later releases of Windows can use dynamic disks. However, you can use dynamic disks with other operating systems, such as UNIX. To do this, you need to create a separate volume for the non-Windows operating system. You can’t use dynamic disks on portable computers.

Windows Server 2008 R2 provides the tools you need to convert a basic disk to a dynamic disk and to change a dynamic disk back to a basic disk. When you convert to a dynamic disk, partitions are changed to volumes of the appropriate type automatically. You can’t change these volumes back to partitions. Instead, you must delete the volumes on the dynamic disk and then change the disk back to a basic disk. Deleting the volumes destroys all the information on the disk.

### Converting a Basic Disk to a Dynamic Disk

Before you convert a basic disk to a dynamic disk, you should make sure that you don’t need to boot the computer to other versions of Windows. Only computers running Windows 2000 and later releases of Windows can use dynamic disks. With MBR disks, you should also make sure that the disk has 1 MB of free space at the end of the disk. Although Disk Management reserves this free space when creating partitions and volumes, disk management tools on other operating systems might not. Without the free space at the end of the disk, the conversion will fail.

With GPT disks, you must have contiguous, recognized data partitions. If the GPT disk contains partitions that Windows doesn’t recognize, such as those created by another operating system, you can’t convert to a dynamic disk.
With either type of disk, the following holds true:

- There must be at least 1 MB of free space at the end of the disk. Disk Management reserves this free space automatically, but other disk management tools might not.
- You can’t use dynamic disks on portable computers or with removable media. You can configure these drives only as basic drives with primary partitions.
- You shouldn’t convert a disk if it contains multiple installations of the Windows operating system. If you do, you might be able to start the computer only using Windows Server 2008 R2.

To convert a basic disk to a dynamic disk, follow these steps:

1. In Disk Management, right-click a basic disk that you want to convert, either in the Disk List view or in the left pane of the Graphical View. Then click Convert To Dynamic Disk.

2. In the Convert To Dynamic Disk dialog box, select the check boxes for the disks you want to convert. If you’re converting a spanned, striped, mirrored, or RAID-5 volume, be sure to select all the basic disks in this set. You must convert the set together. Click OK to continue.

   The Disks To Convert dialog box shows the disks you’re converting. The buttons and columns in this dialog box contain the following information:
   - **Name**  Shows the disk number.
   - **Disk Contents**  Shows the type and status of partitions, such as boot, active, or in use.
   - **Will Convert**  Specifies whether the drive will be converted. If the drive doesn’t meet the criteria, it won’t be converted, and you might need to take corrective action, as described previously.
   - **Details**  Shows the volumes on the selected drive.
   - **Convert**  Starts the conversion.

3. To begin the conversion, click Convert. Disk Management warns you that after the conversion is complete, you won’t be able to boot previous versions of Windows from volumes on the selected disks. Click Yes to continue.

4. Disk Management restarts the computer if a selected drive contains the boot partition, system partition, or a partition in use.

**Changing a Dynamic Disk Back to a Basic Disk**

Before you can change a dynamic disk back to a basic disk, you must delete all dynamic volumes on the disk. After you do this, right-click the disk and select Convert To Basic Disk. This changes the dynamic disk to a basic disk. You can then create new partitions and logical drives on the disk.
Reactivating Dynamic Disks

If the status of a dynamic disk is Online (Errors) or Offline, you can often reactivate the disk to correct the problem. You reactivate a disk by following these steps:

1. In Disk Management, right-click the dynamic disk you want to reactivate, and then click Reactivate Disk. Confirm the action when prompted.

2. If the drive status doesn’t change, you might need to reboot the computer. If this still doesn’t resolve the problem, check for problems with the drive, its controller, and the cables. Also make sure that the drive has power and is connected properly.

Rescanning Disks

Rescanning all drives on a system updates the drive configuration information on the computer. Rescanning can sometimes resolve a problem with drives that show a status of Unreadable. You rescan disks on a computer by choosing Rescan Disks from the Action menu in Disk Management.

Moving a Dynamic Disk to a New System

An important advantage of dynamic disks over basic disks is that you can easily move them from one computer to another. For example, if after setting up a computer you decide that you don’t really need an additional hard disk, you can move it to another computer where it can be better used.

Windows Server 2008 R2 greatly simplifies the task of moving drives to a new system. Before moving disks, you should follow these steps:

1. Open Disk Management on the system where the dynamic drives are currently installed. Check the status of the drives and ensure that they’re marked as Healthy. If the status isn’t Healthy, you should repair partitions and volumes before you move the disk drives.

   **NOTE** Drives with BitLocker Drive Encryption cannot be moved using this technique. BitLocker Driver Encryption wraps drives in a protected seal so that any offline tampering is detected and results in the disk being unavailable until an administrator unlocks it.

2. Check the hard disk subsystems on the original computer and the computer to which you want to transfer the disk. Both computers should have identical hard disk subsystems. If they don’t, the Plug and Play ID on the system disk from the original computer won’t match what the destination computer is expecting. As a result, the destination computer won’t be able to load the right drivers, and boot might fail.

3. Check whether any dynamic disks that you want to move are part of a spanned, extended, or striped set. If they are, you should make a note of which disks are part of which set and plan on moving all disks in a set
together. If you are moving only part of a disk set, you should be aware of the consequences. For spanned, extended, or striped volumes, moving only part of the set will make the related volumes unusable on the current computer and on the computer to which you are planning to move the disks.

When you are ready to move the disks, follow these steps:

1. On the original computer, start Computer Management. Then, in the left pane, select Device Manager. In the Device list, expand Disk Drives. This shows a list of the physical disk drives on the computer. Right-click each disk that you want to move, and then click Uninstall. If you are unsure which disks to uninstall, right-click each disk and click Properties. In the Properties dialog box, click the Volumes tab, and then select Populate. This shows you the volumes on the selected disk.

2. Next, on the original computer, select the Disk Management node in Computer Management. If the disk or disks that you want to move are still listed, right-click each disk, and then click Remove Disk.

3. After you perform these procedures, you can move the dynamic disks. If the disks are hot-swappable disks and this feature is supported on both computers, remove the disks from the original computer and then install them on the destination computer. Otherwise, turn off both computers, remove the drives from the original computer, and then install them on the destination computer. When you have finished, restart the computers.

4. On the destination computer, access Disk Management, and then choose Rescan Disks from the Action menu. When Disk Management finishes scanning the disks, right-click any disk marked Foreign, and then click Import. You should now be able to access the disks and their volumes on the destination computer.

**NOTE** In most cases, the volumes on the dynamic disks should retain the drive letters that they had on the original computer. However, if a drive letter is already used on the destination computer, a volume receives the next available drive letter. If a dynamic volume previously did not have a drive letter, it does not receive a drive letter when moved to the destination computer. Additionally, if automounting is disabled, the volumes aren’t automatically mounted, and you must manually mount volumes and assign drive letters.

### Managing Virtual Hard Disks

Using Disk Management, you can create, attach, and detach virtual hard disks. You can create a virtual hard disk by choosing Create VHD from the Action menu. In the Create And Attach Virtual Hard Disk dialog box, click Browse. Use the Browse Virtual Disk Files dialog box to select the location where you want to create the .vhd file for the virtual hard disk, and then click Save.
In the Virtual Hard Disk Size list, enter the size of the disk in MB, GB, or TB. Specify whether the size of the VHD dynamically expands to its fixed maximum size as data is saved to it or uses a fixed amount of space regardless of the amount of data stored on it. When you click OK, Disk Management creates the virtual hard disk.

The VHD is attached automatically and added as a new disk. To initialize the disk for use, right-click the disk entry in Graphical View, and then click Initialize Disk. In the Initialize Disk dialog box, the disk is selected for initialization. Specify the disk type as MBR or GPT, and then click OK.

After initializing the disk, right-click the unpartitioned space on the disk and create a volume of the appropriate type. After you create the volume, the VHD is available for use.

Once you’ve created, attached, initialized, and formatted a VHD, you can work with a virtual disk in much the same way as you work with other disks. You can write data to and read data from a VHD. You can boot the computer from a VHD. You are able to take a VHD offline or put a VHD online by right-clicking the disk entry in Graphical View and selecting Offline or Online, respectively. If you no longer want to use a VHD, you can detach it by right-clicking the disk entry in Graphical View, selecting Detach VHD, and then clicking OK in the Detach Virtual Hard Disk dialog box.

You can use VHDs created with other programs as well. If you created a VHD using another program or have a detached VHD that you want to attach, you can work with the VHD by completing the following steps:

1. In Disk Management, click the Attach VHD option on the Action menu.
2. In the Attach Virtual Hard Disk dialog box, click Browse. Use the Browse Virtual Disk Files dialog box to select the .vhd file for the virtual hard disk, and then click Open.
3. If you want to attach the VHD in read-only mode, select Read-Only. Click OK to attach the VHD.

Using Basic Disks and Partitions

When you install a new computer or update an existing computer, you often need to partition the drives on the computer. You partition drives using Disk Management.

Partitioning Basics

In Windows Server 2008 R2, a physical drive using the MBR partition style can have up to four primary partitions and one extended partition. This allows you to configure MBR drives in one of two ways: by using one to four primary partitions, or by using one to three primary partitions and one extended partition. A primary partition can fill an entire disk, or you can size it as appropriate for the workstation or server you’re configuring. Within an extended partition, you can create one or
more logical drives. A logical drive is simply a section of a partition with its own file system. Generally, you use logical drives to divide a large drive into manageable sections. With this in mind, you might want to divide a 600-GB extended partition into three logical drives of 200 GB each. Physical disks with the GPT partition style can have up to 128 partitions.

After you partition a drive, you format the partitions to assign drive letters. This is a high-level formatting that creates the file system structure rather than a low-level formatting that sets up the drive for initial use. You’re probably very familiar with the C drive used by Windows Server 2008 R2. Well, the C drive is simply the designator for a disk partition. If you partition a disk into multiple sections, each section can have its own drive letter. You use the drive letters to access file systems in various partitions on a physical drive. Unlike MS-DOS, which assigns drive letters automatically starting with the letter C, Windows Server 2008 R2 lets you specify drive letters. Generally, the drive letters C through Z are available for your use.

**NOTE** The drive letter A is usually assigned to a system’s floppy disk drive. If the system has a second floppy disk drive, the letter B is assigned to it, so you can use only the letters C through Z. Don’t forget that CD-ROMs, Zip drives, and other types of media drives need drive letters as well. The total number of drive letters you can use at one time is 24. If you need additional volumes, you can create them by using drive paths.

Using drive letters, you can have only 24 active volumes. To get around this limitation, you can mount disks to drive paths. A drive path is set as a folder location on another drive. For example, you might mount additional drives as E:\Data1, E:\Data2, and E:\Data3. You can use drive paths with basic and dynamic disks. The only restriction for drive paths is that you mount them on empty folders that are on NTFS drives.

To help you differentiate between primary partitions and extended partitions with logical drives, Disk Management color codes the partitions. For example, primary partitions might be color coded with a dark-blue band and logical drives in extended partitions might be color coded with a light-blue band. The key for the color scheme is shown at the bottom of the Disk Management window. You can change the colors in the Settings dialog box by choosing Settings from the View menu.

**Creating Partitions and Simple Volumes**

Windows Server 2008 R2 simplifies the Disk Management user interface by using one set of dialog boxes and wizards for both partitions and volumes. The first three volumes on a basic drive are created automatically as primary partitions. If you try to create a fourth volume on a basic drive, the remaining free space on the drive is converted automatically to an extended partition with a logical drive of the size you designate by using the new volume feature in the extended partition. Any subsequent volumes are created in the extended partitions as logical drives automatically.
In Disk Management, you create partitions, logical drives, and simple volumes by following these steps:

1. In Disk Management’s Graphical View, right-click an unallocated or free area, and then click New Simple Volume. This starts the New Simple Volume Wizard. Read the Welcome page, and then click Next.

2. The Specify Volume Size page, shown in Figure 12-3, specifies the minimum and maximum size for the volume in megabytes and lets you size the volume within these limits. Size the partition in megabytes in the Simple Volume Size In MB field, and then click Next.

![New Simple Volume Wizard](image)

**FIGURE 12-3** Set the size of the volume on the Specify Volume Size page.

3. On the Assign Drive Letter Or Path page, shown in Figure 12-4, specify whether you want to assign a drive letter or path, and then click Next. The following options are available:

   - **Assign The Following Drive Letter** Choose this option to assign a drive letter. Then select an available drive letter in the list provided. By default, Windows Server 2008 R2 selects the lowest available drive letter and excludes reserved drive letters as well as those assigned to local disks or network drives.

   - **Mount In The Following Empty NTFS Folder** Choose this option to mount the partition in an empty NTFS folder. You must then type the path to an existing folder or click Browse to search for or create a folder to use.

   - **Do Not Assign A Drive Letter Or Drive Path** Choose this option if you want to create the partition without assigning a drive letter or path. If you
later want the partition to be available for storage, you can assign a drive letter or path at that time.

**NOTE** You don’t have to assign volumes a drive letter or a path. A volume with no designators is considered to be unmounted and is for the most part unusable. An unmounted volume can be mounted by assigning a drive letter or a path at a later date. See “Assigning Drive Letters and Paths” later in this chapter.

![Assign Drive Letter Or Path page](image)

**FIGURE 12-4** On the Assign Drive Letter Or Path page, assign the drive designator or choose to wait until later.

4. On the Format Partition page, shown in Figure 12-5, determine whether and how the volume should be formatted. If you want to format the volume, select Format This Volume With The Following Settings, and then configure the following options:

- **File System** Sets the file system type as FAT32 or NTFS. NTFS is selected by default in most cases. If you use FAT32, you can later convert to NTFS with the Convert utility. You can’t, however, convert NTFS partitions to FAT32.

- **Allocation Unit Size** Sets the cluster size for the file system. This is the basic unit in which disk space is allocated. The default allocation unit size is based on the size of the volume and is set dynamically prior to formatting by default. To override this feature, you can set the allocation unit size to a specific value. If you use many small files, you might want to use a smaller cluster size, such as 512 or 1,024 bytes. With these settings, small files use less disk space.

- **Volume Label** Sets a text label for the partition. This label is the partition’s volume name and is set to New Volume by default. You can
change the volume label at any time by right-clicking the volume in Windows Explorer, clicking Properties, and typing a new value in the Label field provided on the General tab.

- **Perform A Quick Format**  Tells Windows Server 2008 R2 to format without checking the partition for errors. With large partitions, this option can save you a few minutes. However, it’s usually better to check for errors, which enables Disk Management to mark bad sectors on the disk and lock them out.

- **Enable File And Folder Compression**  Turns on compression for the disk. Built-in compression is available only for NTFS. Under NTFS, compression is transparent to users and compressed files can be accessed just like regular files. If you select this option, files and directories on this drive are compressed automatically. For more information on compressing drives, files, and directories, see “Compressing Drives and Data” later in this chapter.

5. Click Next, confirm your options, and then click Finish.

**Formatting Partitions**

Formatting creates a file system on a partition and permanently deletes any existing data. This is a high-level formatting that creates the file system structure rather than a low-level formatting that initializes a drive for use. To format a partition, right-click the partition and then click Format. This opens the Format dialog box, shown in Figure 12-6.
You use the formatting fields as follows:

- **Volume Label**  Specifies a text label for the partition. This label is the partition’s volume name.

- **File System**  Specifies the file system type as FAT32 or NTFS. NTFS is the native file system type for Windows NT and later releases of Windows.

- **Allocation Unit Size**  Specifies the cluster size for the file system. This is the basic unit in which disk space is allocated. The default allocation unit size is based on the size of the volume and is set dynamically prior to formatting. To override this feature, you can set the allocation unit size to a specific value. If you use lots of small files, you might want to use a smaller cluster size, such as 512 or 1,024 bytes. With these settings, small files use less disk space.

- **Perform A Quick Format**  Tells Windows Server 2008 R2 to format without checking the partition for errors. With large partitions, this option can save you a few minutes. However, it’s more prudent to check for errors, which allows Disk Management to mark bad sectors on the disk and lock them out.

- **Enable File And Folder Compression**  Turns on compression for the disk. Built-in compression is available only for NTFS. Under NTFS, compression is transparent to users, and compressed files can be accessed just like regular files. If you select this option, files and directories on this drive are compressed automatically. For more information on compressing drives, files, and directories, see “Compressing Drives and Data” later in this chapter.

When you’re ready to proceed, click OK. Because formatting a partition destroys any existing data, Disk Management gives you one last chance to cancel the procedure. Click OK to start formatting the partition. Disk Management changes the drive’s status to reflect the formatting and the percentage of completion. When formatting is complete, the drive status changes to reflect this.
Managing Existing Partitions and Drives

Disk Management provides many ways to manage existing partitions and drives. Use these features to assign drive letters, delete partitions, set the active partition, and more. In addition, Windows Server 2008 R2 provides other utilities to carry out common tasks such as converting a volume to NTFS, checking a drive for errors, and cleaning up unused disk space.

**NOTE** Windows Vista, Windows 7, Windows Server 2008, and later releases of Windows support hot-pluggable media that use NTFS volumes. This new feature allows you to format USB flash devices and other similar media with NTFS. There are also enhancements to prevent data loss when ejecting NTFS-formatted removable media.

Assigning Drive Letters and Paths

You can assign drives one drive letter and one or more drive paths, provided that the drive paths are mounted on NTFS drives. Drives don’t have to be assigned a drive letter or path. A drive with no designators is considered to be unmounted, and you can mount it by assigning a drive letter or path at a later date. You need to unmount a drive before moving it to another computer.

Windows cannot modify the drive letter of system, boot, or page file volumes. To change the drive letter of a system or boot volume, you need to edit the registry as described in Microsoft Knowledge Base article 223188 ([support.microsoft.com/kb/223188/en-us](support.microsoft.com/kb/223188/en-us)). Before you can change the drive letter of a page file volume, you might need to move the page file to a different volume.

To manage drive letters and paths, right-click the drive you want to configure in Disk Management, and then click Change Drive Letter And Paths. This opens the dialog box shown in Figure 12-7. You can now do the following:

- **Add a drive path** Click Add, select Mount In The Following Empty NTFS Folder, and then type the path to an existing folder, or click Browse to search for or create a folder.
- **Remove a drive path** Select the drive path to remove, click Remove, and then click Yes.
- **Assign a drive letter** Click Add, select Assign The Following Drive Letter, and then choose an available letter to assign to the drive.
- **Change the drive letter** Select the current drive letter, and then click Change. Select Assign The Following Drive Letter, and then choose a different letter to assign to the drive.
- **Remove a drive letter** Select the current drive letter, click Remove, and then click Yes.
**NOTE** If you try to change the letter of a drive that’s in use, Windows Server 2008 R2 displays a warning. You need to exit programs that are using the drive and try again or allow Disk Management to force the change by clicking Yes when prompted.

**FIGURE 12-7** You can change the drive letter and path assignment in the Change Drive Letter And Paths dialog box.

**Changing or Deleting the Volume Label**

The volume label is a text descriptor for a drive. With FAT32, the volume label can be up to 11 characters and can include spaces. With NTFS, the volume label can be up to 32 characters. Additionally, although FAT32 doesn’t allow you to use some special characters, including * / \ [ ] : ; | = , + , ?, NTFS does allow you to use these special characters.

Because the volume label is displayed when the drive is accessed in various Windows Server 2008 R2 utilities, including Windows Explorer, it can provide information about a drive’s contents. You can change or delete a volume label using Disk Management or Windows Explorer.

Using Disk Management, you can change or delete a label by following these steps:

1. Right-click the partition, and then click Properties.
2. On the General tab of the Properties dialog box, type a new label for the volume in the Label text box or delete the existing label. Click OK.

Using Windows Explorer, you can change or delete a label by following these steps:

1. Right-click the drive icon, and then click Properties.
2. On the General tab of the Properties dialog box, type a new label for the volume in the Label text box or delete the existing label. Click OK.
Deleting Partitions and Drives

To change the configuration of a drive that’s fully allocated, you might need to delete existing partitions and logical drives. Deleting a partition or a drive removes the associated file system, and all data in the file system is lost. Before you delete a partition or a drive, you should back up any files and directories that the partition or drive contains.

**NOTE**  To protect the integrity of the system, you can’t delete the system or boot partition. However, Windows Server 2008 R2 does let you delete the active partition or volume if it is not designated as boot or system. Always check to be sure that the partition or volume you are deleting doesn’t contain important data or files.

You can delete a primary partition, a volume, or a logical drive by following these steps:

1. In Disk Management, right-click the partition, volume, or drive you want to delete, and then click Explore. Using Windows Explorer, move all the data to another volume or verify an existing backup to ensure that the data was properly saved.
2. In Disk Management, right-click the partition, volume, or drive again, and then click Delete Partition, Delete Volume, or Delete Logical Drive as appropriate.
3. Confirm that you want to delete the selected item by clicking Yes.

The steps for deleting an extended partition differ slightly from those for deleting a primary partition or a logical drive. To delete an extended partition, follow these steps:

1. Delete all the logical drives on the partition following the steps listed in the previous procedure.
2. Select the extended partition area itself and delete it.

Converting a Volume to NTFS

Windows Server 2008 R2 provides a utility for converting FAT volumes to NTFS. This utility, Convert (Convert.exe), is located in the %SystemRoot% folder. When you convert a volume using this tool, the file and directory structure is preserved and no data is lost. Keep in mind, however, that Windows Server 2008 R2 doesn’t provide a utility for converting NTFS to FAT. The only way to go from NTFS to FAT is to delete the partition by following the steps listed in the previous section and then to re-create the partition as a FAT volume.

**The Convert Utility Syntax**

Convert is run at the command prompt. If you want to convert a drive, use the following syntax:

```
convert volume /FS:NTFS
```
where *volume* is the drive letter followed by a colon, drive path, or volume name. For example, if you want to convert the D drive to NTFS, use the following command:

```
convert D: /FS:NTFS
```

If the volume has a label, you are prompted to enter the volume label for the drive. You are not prompted for a volume label if the disk doesn’t have a label.

The complete syntax for Convert is shown here:

```
```

The options and switches for Convert are used as follows:

- `volume` Sets the volume to work with
- `/FS:NTFS` Converts to NTFS
- `/V` Sets verbose mode
- `/X` Forces the volume to dismount before the conversion (if necessary)
- `/CvtArea:filename` Sets the name of a contiguous file in the root directory to be a placeholder for NTFS system files
- `/NoSecurity` Removes all security attributes and makes all files and directories accessible to the group Everyone

The following sample statement uses Convert:

```
convert C: /FS:NTFS /V
```

### Using the Convert Utility

Before you use the Convert utility, determine whether the partition is being used as the active boot partition or a system partition containing the operating system. You can convert the active boot partition to NTFS. Doing so requires that the system gain exclusive access to this partition, which can be obtained only during startup. Thus, if you try to convert the active boot partition to NTFS, Windows Server 2008 R2 displays a prompt asking if you want to schedule the drive to be converted the next time the system starts. If you click Yes, you can restart the system to begin the conversion process.

**TIP** Often, you will need to restart a system several times to completely convert the active boot partition. Don’t panic. Let the system proceed with the conversion.

Before the Convert utility actually converts a drive to NTFS, the utility checks whether the drive has enough free space to perform the conversion. Generally, Convert needs a block of free space that’s roughly equal to 25 percent of the total space used on the drive. For example, if the drive stores 200 GB of data, Convert needs about 50 GB of free space. If the drive doesn’t have enough free space, Convert
aborts and tells you that you need to free up some space. On the other hand, if the drive has enough free space, Convert initiates the conversion. Be patient. The conversion process takes several minutes (longer for large drives). Don’t access files or applications on the drive while the conversion is in progress.

You can use the /CvtArea option to improve performance on the volume so that space for the master file table (MFT) is reserved. This option helps to prevent fragmentation of the MFT. How? Over time, the MFT might grow larger than the space allocated to it. The operating system must then expand the MFT into other areas of the disk. Although the Disk Defragmenter utility can defragment the MFT, it cannot move the first section of the MFT, and it is very unlikely that there will be space after the MFT because this will be filled by file data.

To help prevent fragmentation in some cases, you might want to reserve more space than the default (12.5 percent of the partition or volume size). For example, you might want to increase the MFT size if the volume will have many small or average-size files rather than a few large files. To specify the amount of space to reserve, you can use FSUtil to create a placeholder file equal in size to that of the MFT you want to create. You can then convert the volume to NTFS and specify the name of the placeholder file to use with the /CvtArea option.

In the following example, you use FSUtil to create a 1.5-GB (1,500,000,000 bytes) placeholder file named Temp.txt:

```
fsutil file createnew c:\temp.txt 1500000000
```

To use this placeholder file for the MFT when converting drive C to NTFS, you would then type the following command:

```
convert c: /fs:ntfs /cvtarea:temp.txt
```

Notice that the placeholder file is created on the partition or volume that is being converted. During the conversion process, the file is overwritten with NTFS metadata and any unused space in the file is reserved for future use by the MFT.

### Resizing Partitions and Volumes

Windows Server 2008 R2 doesn’t use Ntldr and Boot.ini to load the operating system. Instead, Windows Server 2008 R2 has a preboot environment in which Windows Boot Manager is used to control startup and load the boot application you’ve selected. Windows Boot Manager also finally frees the Windows operating system from its reliance on MS-DOS so that you can use drives in new ways. With Windows Server 2008 R2, you can extend and shrink both basic and dynamic disks. You can use either Disk Management or DiskPart to extend and shrink volumes. You cannot shrink or extend striped, mirrored, or striped-with-parity volumes.

In extending a volume, you convert areas of unallocated space and add them to the existing volume. For spanned volumes on dynamic disks, the space can come from any available dynamic disk, not only from those on which the volume was
originally created. Thus, you can combine areas of free space on multiple dynamic disks and use those areas to increase the size of an existing volume.

**CAUTION** Before you try to extend a volume, be aware of several limitations. First, you can extend simple and spanned volumes only if they are formatted and the file system is NTFS. You can’t extend striped volumes. You can’t extend volumes that aren’t formatted or that are formatted with FAT32. Additionally, you can’t extend a system or boot volume, regardless of its configuration.

You can shrink a simple volume or a spanned volume by following these steps:

1. In Disk Management, right-click the volume that you want to shrink, and then click Shrink Volume. This option is available only if the volume meets the previously discussed criteria.
2. In the field provided in the Shrink dialog box, shown in Figure 12-8, enter the amount of space to shrink.

![Shrink Dialog Box](image)

**FIGURE 12-8** Specify the amount of space to shrink from the volume.

The Shrink dialog box provides the following information:

- **Total Size Before Shrink In MB** Lists the total capacity of the volume in megabytes. This is the formatted size of the volume.

- **Size Of Available Shrink Space In MB** Lists the maximum amount by which the volume can be shrunk. This doesn’t represent the total amount of free space on the volume; rather, it represents the amount of space that can be removed, not including any data reserved for the master file table, volume snapshots, page files, and temporary files.

- **Enter The Amount Of Space To Shrink In MB** Lists the total amount of space that will be removed from the volume. The initial value defaults to the maximum amount of space that can be removed from the volume. For optimal drive performance, you’ll want to ensure that the drive has at least 10 percent of free space after the shrink operation.
- **Total Size After Shrink In MB** Lists what the total capacity of the volume will be (in megabytes) after the shrink. This is the new formatted size of the volume.

3. Click Shrink to shrink the volume.

You can extend a simple volume or a spanned volume by following these steps:

1. In Disk Management, right-click the volume that you want to extend, and then click Extend Volume. This option is available only if the volume meets the previously discussed criteria and free space is available on one or more of the system’s dynamic disks.

2. In the Extend Volume Wizard, read the introductory message, and then click Next.

3. On the Select Disks page, select the disk or disks from which you want to allocate free space. Any disks currently being used by the volume are automatically selected. By default, all remaining free space on those disks is selected for use.

4. With dynamic disks, you can specify the additional space that you want to use on other disks by performing the following tasks:
   - Click the disk, and then click Add to add the disk to the Selected list.
   - Select each disk in the Selected list, and then, in the Select The Amount Of Space In MB list, specify the amount of unallocated space to use on the selected disk.

5. Click Next, confirm your options, and then click Finish.

### Repairing Disk Errors and Inconsistencies

Windows Server 2008 R2 includes feature enhancements that reduce the amount of manual maintenance you must perform on disk drives. The following enhancements have the most impact on the way you work with disks:

- Transactional NTFS
- Self-healing NTFS

Transactional NTFS allows file operations on an NTFS volume to be performed transactionally. This means programs can use a transaction to group sets of file and registry operations so that all of them succeed or none of them succeed. While a transaction is active, changes are not visible outside the transaction. Changes are committed and written fully to disk only when a transaction is completed successfully. If a transaction fails or is incomplete, the program rolls back the transactional work to restore the file system to the state it was in prior to the transaction.

Transactions that span multiple volumes are coordinated by the Kernel Transaction Manager (KTM). The KTM supports independent recovery of volumes if a transaction fails. The local resource manager for a volume maintains a separate
transaction log and is responsible for maintaining threads for transactions separate from threads that perform the file work.

Traditionally, you have had to use the Check Disk tool to fix errors and inconsistencies in NTFS volumes on a disk. Because this process can disrupt the availability of Windows systems, Windows Server 2008 R2 uses self-healing NTFS to protect file systems without requiring you to use separate maintenance tools to fix problems. Because much of the self-healing process is enabled and performed automatically, you might need to perform volume maintenance manually only when you are notified by the operating system that a problem cannot be corrected automatically. If such an error occurs, Windows Server 2008 R2 notifies you about the problem and provides possible solutions.

Self-healing NTFS has many advantages over Check Disk, including the following:

- Check Disk must have exclusive access to volumes, which means system and boot volumes can be checked only when the operating system starts up. On the other hand, with self-healing NTFS, the file system is always available and does not need to be corrected offline (in most cases).
- Self-healing NTFS attempts to preserve as much data as possible if corruption occurs and reduces failed file system mounting that previously could occur if a volume was known to have errors or inconsistencies. During restart, self-healing NTFS repairs the volume immediately so that it can be mounted.
- Self-healing NTFS reports changes made to the volume during repair through existing Chkdsk.exe mechanisms, directory notifications, and update sequence number (USN) journal entries. This feature also allows authorized users and administrators to monitor repair operations through Verification, Waiting For Repair Completion, and Progress Status messages.
- Self-healing NTFS can recover a volume if the boot sector is readable but does not identify an NTFS volume. In this case, you must run an offline tool that repairs the boot sector and then allow self-healing NTFS to initiate recovery.

Although self-healing NTFS is a terrific enhancement, at times you may want to (or may have to) manually check the integrity of a disk. In these cases, you can use Check Disk (Chkdsk.exe) to check for and (optionally) repair problems found on FAT, FAT32, and NTFS volumes. Although Check Disk can check for and correct many types of errors, the utility primarily looks for inconsistencies in the file system and its related metadata. One of the ways Check Disk locates errors is by comparing the volume bitmap to the disk sectors assigned to files in the file system. Beyond this, the usefulness of Check Disk is rather limited. For example, Check Disk can’t repair corrupted data within files that appear to be structurally intact.
Running Check Disk from the Command Line

You can run Check Disk from the command prompt or within other utilities. At a command prompt, you can test the integrity of the E drive by typing the following command:

```bash
chkdsk E:
```

To find and repair errors that are on the E drive, use the following command:

```bash
chkdsk /f E:
```

**NOTE** Check Disk can’t repair volumes that are in use. If a volume is in use, Check Disk displays a prompt that asks if you want to schedule the volume to be checked the next time you start the system. Click Yes to schedule this.

The complete syntax for Check Disk is shown here:

```bash
```

The options and switches for Check Disk are used as follows:

- **volume**: Sets the volume to work with.
- **[path]filename**: FAT/FAT32 only: Specifies files to check for fragmentation.
- **/F**: Fixes errors on the disk.
- **/V**: On FAT/FAT32: Displays the full path and name of every file on the disk. On NTFS: Displays cleanup messages, if any.
- **/R**: Locates bad sectors and recovers readable information (implies /F).
- **/X**: Forces the volume to dismount first if necessary (implies /F).
- **/I**: NTFS only: Performs a minimum check of index entries.
- **/C**: NTFS only: Skips checking of cycles within the folder structure.
- **/L:size**: NTFS only: Changes the log file size.

Running Check Disk Interactively

You can run Check Disk interactively by using Windows Explorer or Disk Management. Follow these steps:

1. Right-click the drive, and then click Properties.
2. On the Tools tab of the Properties dialog box, click Check Now.
3. As shown in Figure 12-9, you can now do the following:
   - Check for errors without repairing them. Click Start without selecting either of the check boxes.
   - Check for errors and fix them. Make the appropriate selections in the check boxes to fix file system errors, recover bad sectors, or both, and then click Start.
Defragmenting Disks

Any time you add files to or remove files from a drive, the data on the drive can become fragmented. When a drive is fragmented, large files can’t be written to a single continuous area on the disk. As a result, the operating system must write the file to several smaller areas on the disk, which means more time is spent reading the file from the disk. To reduce fragmentation, Windows Server 2008 R2 can manually or automatically defragment disks using Disk Defragmenter. The more frequently data is updated on drives, the more often you should run this tool.

You can manually defragment a disk by following these steps:

1. In Server Manager, select the Storage node and then the Disk Management node. Right-click a drive, and then click Properties.
2. On the Tools tab, click Defragment Now. In the Disk Defragmenter dialog box, select a disk, and then click Analyze Disk. Disk Defragmenter then analyzes the disk to determine whether it needs to be defragmented. If so, it recommends that you defragment now.
3. In the Disk Defragmenter dialog box, select a disk, and then click Defragment Disk.

**NOTE** Depending on the size of the disk, defragmentation can take several hours. You can click Stop Operation at any time to stop defragmentation.

When you enable automatic defragmentation, Windows Server 2008 R2 runs Disk Defragmenter automatically on a specific schedule, such as at 1:00 A.M. every Wednesday. As long as the computer is powered on at the scheduled run time, automatic defragmentation occurs. You can configure and manage automated defragmentation by following these steps:

1. In Server Manager, select the Storage node and then the Disk Management node. Right-click a drive, and then click Properties.
2. On the Tools tab, click Defragment Now. This displays the Disk Defragmenter dialog box, shown in Figure 12-10.
FIGURE 12-10 Disk Defragmenter analyzes and defragments disks efficiently.

3. To cancel automated defragmentation, click Configure Schedule, clear Run On A Schedule, and then click OK. Click Close, and skip the remaining steps.

4. To enable automated defragmentation, click Turn On Schedule. In the Modify Schedule dialog box, shown in Figure 12-11, select Run On A Schedule, and then set the run schedule. In the Frequency list, you can choose Daily, Weekly, or Monthly. If you choose a weekly or monthly run schedule, you need to select the run day of the week or month from the Day list. Finally, the Time list lets you set the time of the day that automated defragmentation should occur.

5. If you want to modify the run schedule, click Configure Schedule. In the Modify Schedule dialog box, shown in Figure 12-11, set the run schedule as discussed in the previous step.

6. If you want to manage which disks are defragmented, click Select Disks. In the Select Disks For Schedule dialog box, select which disks should be defragmented. By default, all disks installed within or connected to the computer are defragmented, and any new disks are defragmented automatically as well. In the Disks To Include In Schedule list, select the check boxes for disks that should be defragmented automatically and clear the check boxes for disks that should not be defragmented automatically. Click OK.

7. Click OK, and then click Close to save your settings.

**NOTE**  Windows Vista with SP1 or later, Windows 7, and Windows Server 2008 or later releases of Windows automatically perform cyclic pickup defragmentation. With this feature, when a scheduled defragmentation pass is stopped and rerun, the computer automatically picks up the next unfinished volume in line to be defragmented.
Compressing Drives and Data

When you format a drive for NTFS, Windows Server 2008 R2 allows you to turn on the built-in compression feature. With compression, all files and directories stored on a drive are automatically compressed when they’re created. Because this compression is transparent to users, compressed data can be accessed just like regular data. The difference is that you can store more information on a compressed drive than you can on an uncompressed drive.

REAL WORLD Although compression is certainly a useful feature when you want to save disk space, you can’t encrypt compressed data. Compression and encryption are mutually exclusive alternatives for NTFS volumes, which means you have the choice of using compression or using encryption. You can’t use both techniques. For more information on encryption, see “Encrypting Drives and Data” later in this chapter. If you try to compress encrypted data, Windows Server 2008 R2 automatically decrypts the data and then compresses it. Likewise, if you try to encrypt compressed data, Windows Server 2008 R2 uncompresses the data and then encrypts it.

Compressing Drives

To compress a drive and all its contents, follow these steps:

1. In Windows Explorer or Disk Management, right-click the drive that you want to compress, and then click Properties.

2. On the General tab, select Compress Drive To Save Disk Space, and then click OK.

3. In the Confirm Attribute Changes dialog box, select whether to apply the changes to subfolders and files, and then click OK.
Compressing Directories and Files

If you decide not to compress a drive, Windows Server 2008 R2 lets you selectively compress directories and files. To compress a file or directory, follow these steps:

1. In Windows Explorer, right-click the file or directory that you want to compress, and then click Properties.

2. On the General tab of the Properties dialog box, click Advanced. In the Advanced Attributes dialog box, select the Compress Contents To Save Disk Space check box, as shown in Figure 12-12. Click OK twice.

![Advanced Attributes](image)

**FIGURE 12-12** With NTFS, you can compress a file or directory by selecting the Compress Contents To Save Disk Space check box in the Advanced Attributes dialog box.

For an individual file, Windows Server 2008 R2 marks the file as compressed and then compresses it. For a directory, Windows Server 2008 R2 marks the directory as compressed and then compresses all the files in it. If the directory contains subfolders, Windows Server 2008 R2 displays a dialog box that allows you to compress all the subfolders associated with the directory. Simply select Apply Changes To This Folder, Subfolders, And Files, and then click OK. Once you compress a directory, any new files added or copied to the directory are compressed automatically.

**NOTE** If you move an uncompressed file from a different drive, the file is compressed. However, if you move an uncompressed file to a compressed folder on the same NTFS drive, the file isn’t compressed. Note also that you can’t encrypt compressed files.

Expanding Compressed Drives

You can remove compression from a drive by following these steps:

1. In Windows Explorer or Disk Management, right-click the drive that contains the data you want to expand, and then click Properties.
2. Clear the Compress Drive To Save Disk Space check box, and then click OK.
3. In the Confirm Attribute Changes dialog box, select whether to apply the change to subfolders and files, and then click OK.

**TIP** Windows always checks the available disk space before expanding compressed data. You should too. If less free space is available than used space, you might not be able to complete the expansion. For example, if a compressed drive uses 150 GB of space and has 70 GB of free space available, you won’t have enough free space to expand the data.

**Expanding Compressed Directories and Files**

If you decide that you want to expand a compressed file or directory, follow these steps:

1. Right-click the file or directory in Windows Explorer, and then click Properties.

With files, Windows Server 2008 R2 removes compression and expands the file. With directories, Windows Server 2008 R2 expands all the files within the directory. If the directory contains subfolders, you also have the opportunity to remove compression from the subfolders. To do this, select Apply Changes To This Folder, Subfolders, And Files when prompted, and then click OK.

**TIP** Windows Server 2008 R2 also provides command-line utilities for compressing and uncompressing data. The compression utility is called Compact (Compact.exe). The uncompression utility is called Expand (Expand.exe).

**Encrypting Drives and Data**

NTFS has many advantages over other file systems that you can use with Windows Server 2008 R2. One of the major advantages is the capability to automatically encrypt and decrypt data using the Encrypting File System (EFS). When you encrypt data, you add an extra layer of protection to sensitive data, and this extra layer acts as a security blanket blocking all other users from reading the contents of the encrypted files. Indeed, one of the great benefits of encryption is that only the designated user can access the data. This benefit is also a disadvantage in that the user must remove encryption before authorized users can access the data.

**NOTE** As discussed previously, you can’t compress encrypted files. The encryption and compression features of NTFS are mutually exclusive. You can use one feature or the other but not both.
Understanding Encryption and the Encrypting File System

File encryption is supported on a per-folder or per-file basis. Any file placed in a folder marked for encryption is automatically encrypted. Files in encrypted format can be read only by the person who encrypted the file. Before other users can read an encrypted file, the user must decrypt the file or grant special access to the file by adding a user’s encryption key to the file.

Every encrypted file has the unique encryption key of the user who created the file or currently has ownership of the file. An encrypted file can be copied, moved, or renamed just like any other file, and in most cases these actions don’t affect the encryption of the data. (For details, see “Working with Encrypted Files and Folders” later in this chapter.) The user who encrypts a file always has access to the file, provided that the user’s public-key certificate is available on the computer that he or she is using. For this user, the encryption and decryption process is handled automatically and is transparent.

EFS is the process that handles encryption and decryption. The default setup for EFS allows users to encrypt files without needing special permission. Files are encrypted using a public/private key that EFS automatically generates on a per-user basis.

Encryption certificates are stored as part of the data in user profiles. If a user works with multiple computers and wants to use encryption, an administrator needs to configure a roaming profile for that user. A roaming profile ensures that the user’s profile data and public-key certificates are accessible from other computers. Without this, users won’t be able to access their encrypted files on another computer.

**SECURITY ALERT** An alternative to a roaming profile is to copy the user’s encryption certificate to the computers that the user uses. You can do this by using the certificate backup and restore process discussed in “Backing Up and Restoring the System State” in Chapter 16. Simply back up the certificate on the user’s original computer and then restore the certificate on each of the other computers the user logs on to.

EFS has a built-in data recovery system to guard against data loss. This recovery system ensures that encrypted data can be recovered in the event that a user’s public-key certificate is lost or deleted. The most common scenario for this is when a user leaves the company and the associated user account is deleted. A manager might have been able to log on to the user’s account, check files, and save important files to other folders, but if the user account has been deleted, encrypted files will be accessible only if the encryption is removed or if the files are moved to a FAT or FAT32 volume (where encryption isn’t supported).

To access encrypted files after the user account has been deleted, you need to use a recovery agent. Recovery agents have access to the file encryption key necessary to unlock data in encrypted files. To protect sensitive data, however, recovery agents don’t have access to a user’s private key or any private key information.
Windows Server 2008 R2 won’t encrypt files without designated EFS recovery agents. Therefore, recovery agents are designated automatically, and the necessary recovery certificates are generated automatically as well. This ensures that encrypted files can always be recovered.

EFS recovery agents are configured at two levels:

- **Domain** The recovery agent for a domain is configured automatically when the first Windows Server 2008 R2 domain controller is installed. By default, the recovery agent is the domain administrator. Through Group Policy, domain administrators can designate additional recovery agents. Domain administrators can also delegate recovery agent privileges to designated security administrators.

- **Local computer** When a computer is part of a workgroup or in a standalone configuration, the recovery agent is the administrator of the local computer by default. Additional recovery agents can be designated. Further, if you want local recovery agents in a domain environment rather than domain-level recovery agents, you must delete the recovery policy from Group Policy for the domain.

You can delete recovery agents if you don’t want them to be used. However, if you delete all recovery agents, EFS will no longer encrypt files. One or more recovery agents must be configured for EFS to function.

### Encrypting Directories and Files

With NTFS volumes, Windows Server 2008 R2 lets you select files and folders for encryption. When a file is encrypted, the file data is converted to an encrypted format that can be read only by the person who encrypted the file. Users can encrypt files only if they have the proper access permissions. When you encrypt folders, the folder is marked as encrypted, but only the files within it are actually encrypted. All files that are created in or added to a folder marked as encrypted are encrypted automatically.

To encrypt a file or directory, follow these steps:

1. Right-click the file or directory that you want to encrypt, and then click Properties.
2. On the General tab of the Properties dialog box, click Advanced, and then select the Encrypt Contents To Secure Data check box. Click OK twice.

**NOTE** You can’t encrypt compressed files, system files, or read-only files. If you try to encrypt compressed files, the files are automatically uncompressed and then encrypted. If you try to encrypt system files, you get an error.

For an individual file, Windows Server 2008 R2 marks the file as encrypted and then encrypts it. For a directory, Windows Server 2008 R2 marks the directory as encrypted and then encrypts all the files in it. If the directory contains subfolders, Windows Server 2008 R2 displays a dialog box that allows you to encrypt all the
subfolders associated with the directory. Simply select Apply Changes To This Folder, Subfolders, And Files, and then click OK.

**NOTE** On NTFS volumes, files remain encrypted even when they’re moved, copied, or renamed. If you copy or move an encrypted file to a FAT or FAT32 drive, the file is automatically decrypted before being copied or moved. Thus, you must have proper permissions to copy or move the file.

You can grant special access to an encrypted file or folder by right-clicking the file or folder in Windows Explorer and then selecting Properties. On the General tab of the Properties dialog box, click Advanced. In the Advanced Attributes dialog box, click Details. In the Encryption Details For dialog box, users who have access to the encrypted file are listed by name. To allow another user access to the file, click Add. If a user certificate is available for the user, select the user’s name in the list provided, and then click OK. Otherwise, click Find User to locate the certificate for the user.

**Working with Encrypted Files and Folders**

Previously, I said that you can copy, move, and rename encrypted files and folders just like any other files. This is true, but I qualified this by saying “in most cases.” When you work with encrypted files, you’ll have few problems as long as you work with NTFS volumes on the same computer. When you work with other file systems or other computers, you might run into problems. Two of the most common scenarios are the following:

- **Copying between volumes on the same computer** When you copy or move an encrypted file or folder from one NTFS volume to another NTFS volume on the same computer, the files remain encrypted. However, if you copy or move encrypted files to a FAT or FAT32 volume, the files are decrypted before transfer and then transferred as standard files. FAT and FAT32 don’t support encryption.

- **Copying between volumes on a different computer** When you copy or move an encrypted file or folder from one NTFS volume to another NTFS volume on a different computer, the files remain encrypted as long as the destination computer allows you to encrypt files and the remote computer is trusted for delegation. Otherwise, the files are decrypted and then transferred as standard files. The same is true when you copy or move encrypted files to a FAT or FAT32 volume on another computer. FAT and FAT32 don’t support encryption.

After you transfer a sensitive file that has been encrypted, you might want to confirm that the encryption is still applied. Right-click the file and then select Properties. On the General tab of the Properties dialog box, click Advanced. The Encrypt Contents To Secure Data option should be selected.
Configuring Recovery Policy

Recovery policies are configured automatically for domain controllers and workstations. By default, domain administrators are the designated recovery agents for domains, and the local administrator is the designated recovery agent for a stand-alone workstation.

Through the Group Policy console, you can view, assign, and delete recovery agents. To do that, follow these steps:

1. Open the Group Policy console for the local computer, site, domain, or organizational unit you want to work with. For details on working with Group Policy, see “Understanding Group Policies” in Chapter 5.

2. Open the Encrypted Data Recovery Agents node in Group Policy. To do this, expand Computer Configuration, Windows Settings, Security Settings, and Public Key Policies, and then select Encrypting File System.

3. The pane at the right lists the recovery certificates currently assigned. Recovery certificates are listed according to who issued them, who they are issued to, expiration data, purpose, and more.

4. To designate an additional recovery agent, right-click Encrypting File System, and then click Add Data Recovery Agent. This starts the Add Recovery Agent Wizard, which you can use to select a previously generated certificate that has been assigned to a user and mark it as a designated recovery certificate. Click Next.

5. On the Select Recovery Agents page, you can select certificates published in Active Directory or use certificate files. If you want to use a published certificate, click Browse Directory, and then, in the Find Users, Contacts, And Groups dialog box, select the user you want to work with. You’ll then be able to use the published certificate of that user. If you want to use a certificate file, click Browse Folders. In the Open dialog box, use the options provided to select and open the certificate file you want to use.

SECURITY ALERT Before you designate additional recovery agents, you should consider setting up a root certificate authority (CA) in the domain. Then you can use the Certificates snap-in to generate a personal certificate that uses the EFS Recovery Agent template. The root CA must then approve the certificate request so that the certificate can be used.

6. To delete a recovery agent, select the recovery agent’s certificate in the right pane, and then press Delete. When prompted to confirm the action, click Yes to permanently and irrevocably delete the certificate. If the recovery policy is empty (meaning that it has no other designated recovery agents), EFS will be turned off so that files can no longer be encrypted.
Decrypting Files and Directories

If you want to decrypt a file or directory, follow these steps:

1. In Windows Explorer, right-click the file or directory, and then click Properties.


With files, Windows Server 2008 R2 decrypts the file and restores it to its original format. With directories, Windows Server 2008 R2 decrypts all the files within the directory. If the directory contains subfolders, you also have the option to remove encryption from the subfolders. To do this, select Apply Changes To This Folder, Subfolders, And Files when prompted, and then click OK.

**TIP** Windows Server 2008 R2 also provides a command-line utility called Cipher (Cipher.exe) for encrypting and decrypting your data. Typing `cipher` at a command prompt without additional parameters shows you the encryption status of all folders in the current directory.
Symbols and Numbers

32-bit operating systems, upgrading not allowed from, 47
64-bit systems only, no 32-bit option, 4, 44

A
access control entries (ACEs), 277
access permissions. See permissions
Account Lockout policy, 352
Account Operators group, 291–292
account policies. See also Group Policy
changing with security templates, 192–193
Default Domain Policy
GPO management of, 146
global user rights configuration, 307–309
Kerberos policies, 305–307
lockout policies, 304–305
password policies, 302–304
setting, 300–301
user rights policies, configuring, 307
accounts
Administrator account, 284–285, 293–294
computer. See computer accounts
domain. See domain user accounts
group. See group accounts
Guest accounts, 285
importing and exporting, 346–347
local. See local accounts
LocalService account, 284
LocalSystem account, 283–284
lockout policy, GPO for, 146
managed service accounts, 318–322
managed virtual accounts, 318, 322
NetworkService account, 284
policies for. See account policies
user. See user accounts
ACLs (access control entries), 277
ACPI (Advanced Configuration and Power Interface), 7–10
Action Center, 519
activation, 45, 69, 76
active cooling mode, 7–8
Active Directory accessing data of, 227
adding items with Dsadd, 239
Adprep, 238–239
ADSI Edit for maintenance, 231, 240, 269–270
application directory partitions, 227
audit policies, setting, 474–475, 478
authentication mechanism assurance, 16, 214
Certificate Services, 14–15, 33
change tracking by, 273
command-line tools, 238–239
certificate information, user, 323–325
data stores, 14, 227–228
dcpromo command, 212
DHCP server authorization, 596
directories. See data stores
directory structure overview, 227
displaying item properties, 239
dns integration, 19–20, 211–212, 630–631
Domain Services. See AD DS (Active Directory Domain Services)
domains, 14
domains, relationships of, 215–216
dsadd, 239
dsget, 239
dsmod, 239
dsmove, 239
dsqury, 232, 239, 265, 352
dsrm, 239
exporting objects, 346–347
Federation Services. See AD FS (Active Directory Federation Services)
global catalogs, 222, 228–229
Group Policy, relationship to, 136–137
importing objects, 346–347
Installation Wizard, 221, 254–255
installing, 212
legacy server operating systems with, 221
Lightweight Directory Services, 15, 33
maintenance of, 269–272
managed service accounts, 16, 214
managed virtual accounts, 214
modifying item properties, 239
multimaster replication model, 222
new features for R2, 15–16, 213–214
non-server operating systems with, 221
Ntdsutil, 239, 523
offline domain join feature, 16, 214
overview of, 14–18
permissions, setting, 353–355
ports used by, 273
printer listings, 572
queries, saved, 242
recovery of, 523
Recycle Bin, 16, 213–214, 233–236
removing objects from, 239
replication. See replication of directory data
replication partitions, 227
Restartable Active Directory Domain Services, 16–18
restore mode, 18
Rights Management Services (AD RMS), 15, 33
schema data, 228
schema master role transfers, 257
Active Directory Administration Tool

Active Directory, continued
searching for users or
groups, 325–326
searching with Users And
Computers, 244–246
service dependencies
of, 273
Service Interface (ADSI),
231
Sites And Services. See
Active Directory Sites
And Services
Started state, 17
states of domain control-
lers, 17–18
Stopped state, 17–18
support tools, table of,
240
SYSVOL share, 455
tools for managing, over-
view of, 237–240
troubleshooting, 272–274
universal group mem-
bership caching, 229–230
Users And Computers
tool. See Active
Directory Users And
Computers
USNs (update sequence
numbers), 273
Web Services, 16, 214,
241
Windows PowerShell
module, 214, 241–242
Windows Web Server
2008 R2 with, 6
Active Directory Administra-
tion Tool, 240
Active Directory Administra-
tive Center
ADWS required for, 241
capabilities of, 240
defined, 16, 214
modules required for, 16
Active Directory Domains And
Trusts
accessing domain struc-
tures, 217
raising domain or forest
functionality levels, 226–227
transferring domain nam-
ing master roles, 257
Active Directory Installation
Wizard, 221, 254–255
Active Directory Schema snap-
in, 257
Active Directory Sites And
Services
global catalogs, configur-
ing, 260–261
ISTG identification, 271
moving domain control-
lers to sites, 265
purpose of, 220
site link bridge configura-
tion, 267–268
site link creation, 266–268
site links, changing
sites associated with,
267–268
sites, creating, 263
subnets, creating, 264
universal group mem-
bership caching, 260–261
Active Directory Users And
Computers
adding members to
groups, 316–317
advanced options fold-
ers, 243
common queries
searches, 245
computer account cre-
ation, 247–248
Computer Management
tool, opening, 250
copying domain user
accounts, 345–346
disabled accounts, 348,
352
domain controllers, con-
ecting to, 243–244
domain user accounts,
278
domains, connecting
to, 244
domainwide operations
masters role manage-
ment, 255–256
Exchange Server groups,
242
expiration options,
351–352
expired accounts, 348
ForeignSecurityPrincipals
folder, 242
global catalogs, listing
domain controllers
with, 244
global groups, creating,
314–315
home directory specifica-
tion, 330, 345
locked-out accounts, 348
Logon Hours, restrict-
ing, 351
logon options, 351–352
LostAndFound folder, 243
managing computer
accounts, 248–250
multiple accounts, editing
method, 347, 349–352
NTDS Quotas folder, 243
object security permis-
sions, setting, 353–355
OUs folders, 243
OUs (organizational
units), managing, 262
password options,
351–352
Profile tab settings,
326–330
Program Data folder, 243
recommended as primary
AD tool, 242
renaming user accounts,
344–345
Saved Queries folder, 242
searching with, 244–246
standard folder set,
242–243
System folder, 243
updating user and group
accounts, 343–348
user profile creation,
338–339
viewing computer
accounts, 248
workstations, restricting
logons to, 351, 353
Active partitions
converting to NTFS, 387
defined, 373
drive letters for, 379
marking partitions as, 374
AD. See Active Directory
AD CS (Active Directory Cer-
tificate Services)
CA (certificate authority)
types, 14–15
role services provided
by, 33
AD DS (Active Directory
Domain Services). See also
Active Directory
defined, 15, 211
directory service logs,
108
domain controllers cre-
ated by installing, 221
functionality provided
by, 33
Group Policy based on,
145–147
preparations for installa-
tion, 213
Restartable Active Direc-
tory Domain Services,
16–18
Stopped state, 17–18
AD FS (Active Directory Fed-
eration Services)
purpose of, 15
role services provided
by, 33
single sign-on with, 276
AD LDS (Active Directory
Lightweight Directory
Services), 15, 33
AD RMS (Active Directory
Rights Management Ser-
vices), 15, 33
AD WS (Active Directory Web
Services), 16, 214, 241
Add Features Wizard, 61–62,
70
Add Role Services Wizard, 359, 363
Add Roles Wizard
AD DS, adding with, 221
DNS Server creation, 637–639
File Services role, 359–363
installing domain controllers, 254
Add Workstations To The Domain right, 251
Add/Remove Windows Components, 61
address book entries, 323–325
Administrative Center, Active Directory. See Active Directory Administrative Center
administrative shares, 454–456
administrative templates, 149–151
Administrative Tools program group accessing, 24
Active Directory tool access, 238
Administrative wizards, 24. See also Server Manager
Administrator account group memberships of, 293–294
security issues for, 284–285
Administrators and Non-Administrators local Group Policy, 142, 144–145
Administrators group
Administrator account membership in, 285
comparison table for, 293
LocalSystem account, 283–284
rights of, 291–292
administrators, groups used by, 293–294
ADMX, 140–141
ADSI (Active Directory Service Interface)
Edit tool, 240, 269–270
WSH and LDAP with, 231
Advanced Boot Options, 524–526
Advanced Configuration and Power Interface (ACPI), 7–10
ADWS (Active Directory Web Services), 16, 241
AES (Advanced Encryption Standard), 336, 528
affinity setting power management issues, 9
allocation unit size, 381, 383
AMD-V (AMD Virtualization), 62
Anonymous Logon identity, 294
AppData(Roaming) folder, redirecting, 172–176
Apple Macintosh computer groups, 317–318
application directory partitions, 227
Application Server role, 33
applications
data backup options, 510
deploying with Group Policy, 180–185
logs of, 107–108
performance settings for, 80
processes associated with, finding, 91
recovery from hangs, 519
shortcut menu options in Task Manger, 91
starting from Task Manager, 90
status of, viewing, 91
stopping, 90
switching between, 90
architecture of domains, 214
architecture of Windows Server 2008 R2, 2
archive attribute, 497
archives, event log, 114–116
ARP command, 49
Assign User Rights, 291
ASSOC command, 49
ATTRIB command, 49
auditing
Active Directory objects, 478
audit events, 109
Audit Policy, setting security policies, 207–208
file and folder use, 475–477
file screening, configuring, 433
logons, 352
policies, setting, 473–475
print jobs, 578
purpose of, 473
registries, 477
authentication
Authenticated Users group, 251
Authenticated Users identity, 294
Kerberos as default protocol, 276. See also Kerberos
logon process component of, 276
mechanism assurance, Active Directory, 16, 214
network authentication component of, 276
NTLM authentication, 276
security policies for, 207
single sign-on, 276
timing synchronization of servers, 353
two-part process for, 276
Windows PowerShell 2.0, configuring for, 27–30
authoritative restores, 523
autoenrollment for certificates, 185–186
autoloader tape systems, 499–500
automatic restarts on system failure, 521
Automatic Updates. See also updates configuration overview, 133–134
enabling, 69
Group Policy configuration of, 186–188

B
Background Intelligent Transfer Service (BITS), 36
background, processes in, 89–90
backup domain controllers, 14
backups
application data options, 510
archive attribute, 497
autoloader tape systems for, 499–500
automatic disk management, 502
command-line tool for. See Wbadmin configuring scheduled backups, 511–514
copy backups, 497
critical vs. noncritical volumes, 511
daily, 498
DAT (digital audio tape) drives for, 499
differential, 497–498, 501
disk drives for, 500
DVDs for, 501–502, 511
encryption certificate backups, 531–532
extended backup sets, 498
Group Policy backups, 164
hardware for, 496, 499–500
Hyper-V, strategies for, 66
incremental, 497–498
media issues, 500–501
modifying scheduled backups, 514–515
normal/full, 497
Ntbackup.exe recoveries, 503
off-site storage of, 496
plan creation for, 495–497
remote shared folders for, 511
Balanced power management plan

backups, continued
repair options to, 501
scheduling, 496
shadow copies for. See shadow copies
storage location issues, 511
system state, 508
tape drives for, 499–501, 502
tools for, selecting, 501–502
virtual library systems, 500
Windows Firewall exceptions for, 510
Windows Server Backup for. See Windows Server Backup
Balanced power management plan, 7
bandwidth performance counters, 132
basic disks
capabilities of, 373
converting to dynamic disks, 374–375, 408
deﬁned, 366
inadvertent conversion to dynamic disks, 373
limitations of, 372, 404
partition creation on, 379–382
volume creation on, 379–382
Batch identity, 294
biometrics, 38
BitLocker Drive Encryption, 36, 134
BitLockerToGo, 134
BITS (Background Intelligent Transfer Service), 36
B-node (broadcast), WINS, 22
boots
boot partitions
defined, 373
mirrored, booting issues, 418
mirroring, 413
striped sets, excluding from, 412
BOOTP (Bootstrap Protocol), 615
bots
dual booting, 404, 412
enable boot logging option, 521
failure overview, 518–520
last known good conﬁguration, 521
mirrored volume errors, 418
recovery options during, 524–526
safe mode, 520–522
Startup And Recovery dialog box, conﬁguring from, 86–87
Windows Preboot Environment, 2
BranchCache, 36, 358
bridgehead servers, 220, 271–272
built-in capabilities of user accounts, 286
built-in groups, 283, 285
built-in local groups, 280
built-in user accounts, 283–284
Bypass Traverse Checking privilege, 287
CALL command, 49
callback setup, 334
CAPI2 (CryptoAPI Version 2), 538
CAs (certiﬁcate authorities)
autoenrollment conﬁguration, 185–186
recovery agents, required to create, 530
types of, 14–15
CD/CHDIR command, 49
CEIP (Customer Experience Improvement Program), 73
certiﬁcates
AD CS (Active Directory Certiﬁcate Services), 14–15
autoenrollment group policies, 185–186
backups of, 531–532
CAs. See CAs (certiﬁcate authorities)
CryptoAPI Version 2, 538
EFS, 398
moving between computers, 532
OCSP (Online Certiﬁcate Status Protocol), 538
recovering, 528–532
user accounts, for, 278
Change share permission, 451
Check Disk, 390–392
child domains, 19, 212, 630
children, object, 467
Chkdsk, 49, 390–392
CHKNTFS command, 49
CHOICE command, 49
Cipher.exe, 530
clean installations, 44–47
CLS command, 49
clusters, SAN access by, 424
CMAK (Connection Manager Administration Kit), 36
CMD command, MINWINPC, 49
Cmd.exe, 25
cmdlets, 25–26, 241–242. See also Windows PowerShell 2.0
COLOR command, 49
command prompts, opening, 41
command-line utilities, 24–25.
See also Windows PowerShell 2.0
Comma-Separated Value Directory Exchange (CSVDE), 346–347
compression
directories or ﬁles, of, 396
encryption, exclusivity of, 395
hard disk drives, of, 395
option during formatting, 382–383
Remote Differential Compression, 37
removing, 396–397
computer accounts
auditing ﬁle access, 475–477
creating, 246–248
disabling and enabling, 248–249
editing, 248
listing all, 344
moving, 250
password management issues, 249
permissions, setting, 353–355
purpose of, 246
resetting, 249
share permissions, adding to, 452–453
standard vs. managed, 247–248
computer assignment software deployment method, 180–185
Computer Management tool
closing open shared ﬁles, 458–459
disk quota management, 484–489
ﬁle sharing sessions, viewing, 456–457
launching for a selected computer, 250
shared folders, creating shares, 447–450
shared folders, viewing, 445–446
viewing currently open shared ﬁle information, 458
computer scripts
assigning, 177–178
permissions for, 469
types of, 176
WSH, 176, 231
Conﬁguration data collector type, 123, 125–126
Conﬁguration node of Server Manager, 71
Connection Manager Administration Kit (CMAK), 36
device drivers, continued
improved error recovery of, 518
Pnputil.exe, 42
printer, 550–551, 557, 559–560, 562, 573–574
Sc query type=driver command, 42
DFS (Distributed File System)
DFS Namespaces services, 358, 360–361
files services, for, 358
replication logs, 108
Replication Service, 141, 273, 358
utility, 240
DHCP (Dynamic Host Configuration Protocol)
Active Directory authorization for, 596
auditing, 597–599
binding specific network connections, 597
capabilities of, 585
connecting to remote DHCP servers, 595
console for managing, 594–595
core-server installations, default for, 47
database files for managing, 625–628
DHCP Server role, 34
DHCPv4 clients, 586
DHCPv6 clients, 586–589
DHCPv6 messages, 589
DNS, integration with, 599–600, 632
DNS/Active Directory integration issues, 19–20
installing servers, 591–594
IPV4 address conflicts, 604
leases, 586, 590, 615, 624–625, 627–628. See also scopes, DHCP
MAC address filtering, 621–622
NAP integration, 601–603
Network Policy Servers with, 602–603
relay agents, 589, 591
reservations, 590, 614, 623–625, 628
restoring, 604–605
saving configurations for, 604–605
scopes. See scopes, DHCP
starting DHCP servers, 596
stopping DHCP servers, 596
updating statistics for, 597
WINs with, 22
Diagnostics node of Server Manager, 71
dial-in privileges, 333–335
Dial-Up identity, 295
differential backups, 497–498, 501
DIMs (Digital ID Management Service), 337, 528
DIR command, 50
Direct Access Management Console, 36
directories, file. See also folders
  compressing, 396
decompressing, 397
RD/RMDIR command, 52
directory access protocols, 227
directory service logs, 108
Directory Services Access Control Lists Utility, 240
Directory Services Restore Mode, 523
desktop.log, 370
DirectoryQuota.exe utility, 26
Directory services logs, 108
discovery, network, 12, 534–535
disk drives. See hard disk drives
disk duplexing, 413
disk imaging, 2
disk mirroring
  advantages of, 411–412
  booting issues, 418
  breaking mirrored sets, 416–417
defined, 411
  Failed Redundancy status, 417
  implementing, 413–415
  removing mirrored volumes, 418–419
  repairing, 417–418
disk quotas
  NTFS. See NTFS disk quotas
  Resource Manager. See Resource Manager disk quotas
disk striping, 411–413, 419–420
disk striping with parity
  advantages of, 411
  implementing, 415–416
  repairing, 419–420
DiskPart utility
  creating partitions, 55
  deleting partitions during installations, 56
  extending, 56
  formatting, 54–55
  MINWINPC command for, 50
  removing partitions, 53–54
Diskraid.exe command, 42
DISM command, 50
display names, user accounts, 298, 310
DNS (Domain Name System)
  AAAA records, 649–650
  Active Directory integration with, 19–20, 211–212, 630–631
  adding records, 650–655
  aliases, 651–652
  child domains, 19, 630, 647–648
  client configuration, 631–633, 635–636
  CNAME records, 649, 651–652
  defined, 629
  deleting domains or subnets, 648–649
  DHCP integration with, 599–600, 632
  DHCP Server role, 34
  DNS Manager console, 645
  DNS Server logs, 108
  DNS Server role, 34
DNSSEC, 633–634
domains, deleting, 648–649
dynamic updates of, 19–20, 660
event logging, 663–664
forward lookup zones, setting up, 639–642
forwarding restrictions configuration, 661–663
full vs. partial integration, 630
fully qualified domain names, 19
GlobalNames zone, 633, 644–645
installation of, 19–20, 637–639
IP addresses, selectively disabling for DNS, 660–661
IPv6 support in R2, 632
mail exchange server identification, 652–654
management tasks, 647
monitoring DNS servers, 664–665
MX records, 649, 652–653
notifying secondaries of changes, 658–659
NS records, 649, 654–655
operational overview, 18–19
organization of computers by, 629–630
IP addresses, selectively disabling for DNS, 660–661
IPv6 support in R2, 632
mail exchange server identification, 652–654
management tasks, 647
monitoring DNS servers, 664–665
MX records, 649, 652–653
notifying secondaries of changes, 658–659
NS records, 649, 654–655
operational overview, 18–19
organization of computers by, 629–630
parent domains, 19, 630
primary server configuration, 639–641
primary vs. secondary servers, 637
PTR records, 649–651
query resolution order, 645
record management overview, 649
remote servers, adding to console, 646
replication dependence on, 273
reverse lookup configuration, 642–644
RODCs with, 20, 632–633
root domains, 19, 629–630
secondary server configuration, 642
Security Extensions (DNSSEC), 20
separate zones, creating child domains in, 647–648
server restart time issue, 631
server types, 637
SOA records, 649, 655–657
startup tasks of DNS servers, 631
structure of domain hierarchies, 211–212
subnets, deleting, 648–649
viewing records, 655
well-known site-local addresses of servers, 631–632
zone transfer control, 657–658
zone types, settings, 659–660
zones, 632–634
zones, configuring, 639–644
DNS Server Troubleshooting Tool, 240
DNSSEC (DNS Security Extensions), 20
domain accounts. See domain user accounts
Domain Admins group, 285, 293–294
Domain Computers group, 316
domain controllers
Active Directory domains, 14
Active Directory Users And Computers, connecting to, 243–244
AD DS for creating, 221
backup domain controllers, 14
backup media, installing from, 255
bridgehead servers, 220
computer account passwords, resetting, 249
data stores of. See data stores
defined, 14
demoting, 221, 254–255
dNS servers, installation on, 637–639
functionality levels, advantages of raising, 225–226
global catalogs of. See global catalogs installing, 253–255
integration of DNS and Active Directory, 19
multimaster replication model, 14, 19, 222
primary, 14
promoting servers to, 221
raising functionality levels, 226
read-only. See RODCs (read-only domain controllers)
recovery of, 523
renaming, 254
replication of data, 230–231
Restartable Active Directory Domain Services, 16–18
sites, associating with, 265
states of, 17–18
universal group membership caching, 229–230
verifying installation of, 212
Domain Controllers group, 316
domain functional levels raising, 225–227
requirements for, 213
versions of, 216
Windows Server 2003 mode, 222–224
Windows Server 2008 mode, 222–224
Windows Server 2008 R2 mode, 223, 225
Domain Guests group, 285
domain local groups, 280–283
Domain Name System. See DNS (Domain Name System)
domain naming master role required for each forest, 232
seizing roles, 258–260
transferring, 257
transferring roles, command line for, 258
domain trees, 215–217
domain user accounts changing passwords, 347
copying, 345–346
creating, 310–312
defined, 278
expired, 348
logons, troubleshooting, 352–353
managed service accounts, 318–322
multiple accounts, editing method, 349–352
single sign-on, 276
Domain Users group, 316
domains
accounts. See domain user accounts
Active Directory domains, 14
Adprep, 238–239
child domains, 19, 212, 630
controlling servers. See domain controllers
defined, 6, 215
deleting from DNS servers, 648–649
DNS structuring of, 18–19
domain functional levels, 15–16
forest functional level, 16
functionality of. See domain functional levels
GPMC, node for, 147–148
group policies for, 145–147
inheritance of group policies, 137
domains, continued
joining computers to, 78, 250–253
naming master role. See domain naming master role
Netdom commands, 42
network type, as a, 11
offline domain join feature, 16
parent domains, 19, 212, 630
place in site architecture, 136
registrars for, 215
relationships of, 215–216
root domains, 19, 629–630
structures of, 214
subdomains, 212
TLDs (top-level domains), 212
trees, 215–217
domainwide roles, managing, 255–256
DOSKEY command, 50
drive letters
assigning, 380–381, 384–385
assigning to volumes while creating, 409
hidden shares for, 455
moved disks, 377
partitions, for, 379
removing, 384
drive paths
adding or removing, 384
function of, 379
drives
DVD, 501–502, 511
hard disk. See hard disk drives
partitioning. See partitions, drive
tape drives, 499–502
volumes. See volumes
Dsadd, 239
Dsget, 239
Dsmod, 239
Dsmove, 239
Dsquery, 232, 239, 265, 352
Dsmr, 239
dual booting
operating systems not supporting RAID, 412
volumes enabling, 404
dump files
flash dump partitions, 373
recovery dumps, options for, 87–88
DVDs for backups, 501–502, 511
dynamic assignment of IP addresses
BOOTP (Bootstrap Protocol), 615
configuring, 541, 543–544
DHCP for. See DHCP (Dynamic Host Configuration Protocol)
dynamic disks
capabilities of, 373
compared to basic disks, 372–373
converting basic disks to, 374–375
converting to basic disks, 375
defined, 366
extending volumes, 388–390
Foreign status, 377
moving to a new system, 376–377
NTFS for. See NTFS
Offline status, 376
Online (Errors) status, 376
reactivating, 376
restrictions on, 372
UNIX compatibility of, 374
dynamic virtual machine storage, 63
dynamic volumes, 404
ECHO command, 50
editions of Windows Server 2008 R2
Datacenter, 3–5
descriptions of, 3–4
Enterprise, 3–5
Foundation, 3–5
Itanium-Based. See Itanium-Based Systems, edition for
Standard, 3–5
table of features for, 4–5
Web edition. See Windows Web Server 2008 R2
EFS (Encrypting File System)
access to files, 398
advantages of, 397
certificates, 337, 398
copying files, 400
decryption, 402
deleted user accounts, effects of, 398
keys, 398
recovery agents, 529–530
recovery system of, 398–399, 401
steps for encryption, 399–400
user profiles for, 398
e-mail
distribution groups, 280
file screening notifications by, 430–431
mail exchange server identification, 652–654
Enable- cmdlet verb, 26
external disk encryption
access to encrypted files, 398
account security settings for, 336
AES (Advanced Encryption Standard), 336, 528
certificates for. See certificates
compression, exclusivity of, 395
decrypting files or folders, 402
deleted user accounts, effects of, 398
EFS. See EFS (Encrypting File System)
keys, 398
recovery agents, 398–399, 401
recovery process, 528–532
standards for, 336
steps for encrypting files or folders, 399–400
user profiles for, 398
ENDLOCAL command, 50
Enforce Password History policy, 302
Enforce User Logon Restrictions policy, 306
Enterprise Admins group, 293–294
Enterprise Domain Controllers identity, 295
Enterprise edition, 3–5
terms of possession, 75–76
environment variables. See system environment variables
EPT (extended page tables), 63
ERASE command, 50
error events, 109
errors
Action Center for resolving, 519
details, logging of, 518–519
paging file size for Stop error dumps, 82
eSATA (External Serial ATA), 369
ETL (Event Trace Log) files, 539
event logging
applications and services logs, 107, 108
archiving logs, 114–116
clearing logs, 114
data available from, 110
descriptions of events, 109
DNS events, 663–664
error details in, 518–519
Event Viewer, 108–110
file screening events, 436
filtering logs, 110–112
forwarded events logs, 107
levels, event, 109
maximize sizes for, setting, 113
options for, setting, 112–113
overwriting options, 113
saving log files, 114
security templates for changing policy settings, 192–193
Windows logs, 107–108
Event Trace Log (ETL) files, 539
event tracing, 123, 125
events
descriptions of, 109
IDs of, 110
logging. See event logging
task categories of, 110
Wecutil.exe, 43
Wevtutil.exe, 43
Everyone group
Everyone identity, 295
Guest account membership in, 285
Guest group rights identical to, 291
Exchange Server
Active Directory Users And Computers view of, 242
managed service accounts for, 318–322
Windows Server Backup with, 503
exFAT file system, 367
EXIT command, 50
EXPAND command, 50
exporting accounts, 346–347
extended partitions capabilities of, 378–379
deleting, 386
extending volumes, 388–390
external storage devices. See removable disks

F
Failover Clustering, 36
FAT
converting to NTFS, 49, 386–388
exFAT, 367
fault tolerance
disk mirroring for, 413
disk striping with parity for, 412, 415–416
Fax Server role, 34
features
adding, 61–62, 70
defined, 32
dependencies of, 32
Features node of Server Manager, 71
Features Summary section of Server Manager, 73
removing, 62
table of, 35–39
federated servers, single sign-on for, 276
Federated Web Single Sign-On, 276
Fibre Channel SANs, 421–422
file and folder permissions, 468–473
deleting, 386
file handles, 92
File Replication Services logs, 108
file screening
active vs. passive, 425
auditing reports, 433
creating new templates, 436
creating screens, 438
e-mail notification configuration, 430–431, 436
event logging, 436
exception creation, 438
exception paths, 427, 430
file groups for, 426–427, 429, 433–435
file screen paths, 425
file screens, 429
File Server Resource Manager role service requirement, 425
global options for, 429, 430–433
notification limit configuration, 431–432
purpose of, 425
shared folders, summaries for, 447
storage reports for. See storage reports templates for, 426, 429
templates, modifying, 435–437
types of notification, 431–432
variables for, 436–437
File Server Resource Manager. See FSRM (File Server Resource Manager)
file servers
installing, 359–363
purpose of, 357–358
role for. See File Services role
File Services role
adding additional services, 362–363
adding to servers, 359–363
BranchCache For Network Files, 358
DFS services for, 358
File Server Resource Manager role service, 425
FSRM with, 358
Indexing Service with, 359
MPIO (Multipath I/O) option, 358
not installed by default, 357–358
optional features for, 358
role services associated with, 34, 358–359
Services for Network File System with, 359
Storage Manager for SANs with, 358
Windows Server Search Service, 359, 362
Windows Server 2003 File Services, 359
Windows Server Backup with, 358
file sharing
public file method. See public file sharing
standard method for files. See standard file sharing
file systems
allocation unit size, 381, 383
Check Disk for error checking, 390–392
encrypting. See EFS (Encrypting File System)
exFAT, 367
FAT, converting to NTFS, 386–388
importance of, 357
NTFS. See NTFS
security templates for paths, 196–199
setting types during formatting, 381
files
classification management, 429
compressing, 396
decompressing, 397
encryption keys of, 528
permissions, 468–473
server services. See file servers; File Services role
sharing, public. See public file sharing
sharing, standard. See standard file sharing
special permissions, table of, 470
subsets of, managing, 429
filtering event logs, 110–112
FIND command, 50
finding users or groups, 325–326
fingerprint devices, 38
FireWire, 369
flexible single master operations roles. See operations masters
folder redirection
Folder Redirection setting, 138
with Group Policy, 172–176
folders
compressing, 396
file screen paths, 425
permissions, 468–473
RD/RMDIR command, 52
special permissions, table of, 471
FOR command, 50
Force Logoff When Logon Hours Expire policy, 332
foreground, processes in, 89
ForeignSecurityPrincipals, 242
forest functional level
defined, 16
raising, 225–227
requirements for, 213
versions of, 218
forests
Adprep, 238–239
defined, 215
DNS server replication in, 634
ForestDNSZones, 632
functional level of. See forest functional level
preparing for AD DS installation, 213
replication partitions of, 272
replication strategy for, 640, 643, 645
structure of, 216–217
FORMAT command, 50
formatting drives
allocation unit size, 381, 383
compression option, 382, 383
file system selection, 381, 383
quick formats, 382, 383
volume creation, during, 409
forward lookup zones, 639–642
Foundation edition, 3–5
FQDNs (fully qualified domain names), 19, 212, 278, 279
free space partitions, 366
FRS (File Replication Service), 273
FSMO (flexible single master operations) roles. See operations masters
FSRM (File Server Resource Manager)
capabilities of, 429
creating file screens, 438
e-mail notification configuration, 430–431, 436
file groups for file screening, 433–435
file screen audit option, 433
file screen exception creation, 438
file screen support, 425
generating on-demand storage reports, 440
notification limit configuration, 431–432
purpose of, 359, 361–362
scheduling storage reports, 439–440
storage report settings, 432–433
template modification for file screening, 435–437
FSUtil, 388
FTP command, 50
FTYPE command, 50
Full Control permission, 469
Full Control share permission, 451
full integration of Active Directory and DNS, 19–20
full-server installations
core-server installations compared to, 39–40
defined, 31
option during installations, 45
upgrade installations, choosing during, 48
user interfaces for, 39–40
fully qualified domain names (FQDNs), 19, 212, 279
G
gateways, multiple default, 544–545
Get- cmdlet verb, 26
global catalogs
configuring, 260–261
domain controller use of, 222
infrastructure master requirements, 229
logon errors from unavailable servers, 353
logon function of, 228–229
recommended number of, 229
global groups
creating, 314–315
core, 280–282
when to use, 283
global power states, 10
global unicast addresses, 590
global user rights configuration, 307–309
GlobalNames zone, 633, 644–645
GOTO command, 50
GPMC (Group Policy Management Console)
Active Directory connection mechanism, 148
ADMX format, 140–141
backing up GPOs, 164
blocking inheritance, 156
copying GPOs, 163
deleting GPOs, 169
disabling unused parts of GPOs, 165
editors for, 139–140
enforcing inheritance, 156
folder redirection, 172–176
GPO editing, 148–149
importing GPOs, 163–164
link order, changing, 154–157
loopback processing settings, 165
modeling policies, 160–162
nodes of, 147–148
pasting GPOs, 163
refresh interval, configuring, 158–160
restoring GPOs from backup, 164–165
Results Wizard, 165, 170–171
slow-link detection settings, 166–169
software deployment with, 180–185
starting, 147
GPOE (Group Policy Object Editor), 140–141, 143
GPOs (Group Policy objects)
ADMX format, 140–141
Adprep domain preparation, 239
backing up, 164
copying, 163
creating, 151–152
Dcgpofix, 171
Default Domain Controllers Policy GPO, 146–147, 171
Default Domain Policy GPO, 146–147, 171
defined, 137
deleting, 169
deploying security policies to multiple computers, 210
determining sources of settings, 170–171
disabling unused parts of, 165
depleting GPOs, 163–164
inheritance with, 137, 154–157
linking to containers, 151–152
local layers of, 142–143
loopback processing settings, 166
pasting, 163
permissions for managing, 154
removing links, 169
restoring from backups, 164–165, 171
RSoP (Resultant Set of Policy), 165, 170–171, 239
script assignments in, 177–179
security templates, importability of, 190
security templates, importing into, 202–203
Software Installation policy, 180–185
starter GPOs, 152
WMI filters, linking to, 162
GPT (GUID partition table) partitions, 365
gpupdate command, 160
graphical administrative tools, 24
graphical interfaces, settings for, 79
group accounts
adding members to, 316–317
adding multiple members to, 349
advantages of, 279
auditing file access, 475–477
built-in capabilities of, 293–297
built-in groups, 283, 285, 347
built-in local groups, 280
Create And Delete Groups right, 291
creating, 313–316
default, 293–294
deleting, 347
distribution groups, 280, 282, 315
domain local groups, 280–281
global groups, 280–283
global user rights configuration, 308–309
guidelines for types to create, 313–314
implicit groups, 283, 294–295
listing all, 344
local groups, 279
local groups, creating, 315–316
local user rights configuration, 309–310
logon rights for, 290
Macintosh computer groups, 317–318
name issues, 279
naming, 314
permissions, setting, 353–355
predefined groups, 283, 285
primary groups, 317–318
Properties dialog box for managing, 317, 325
purpose of, 275
redirecting folders based on membership, 174–175
removing members from, 316
renaming, 344–345
restricted accounts, 291
scopes of, 280–281, 315
searching for, 325–326
security groups, 280
share permissions, adding to, 452–453
SIDs of, 281–282, 344
user accounts compared to, 277
Group Policy
Active Directory, relationship to, 136–137
Active Directory-based, 145–147
administrative templates, 149–151
ADMX, 140–141
application order, 137
auditing, setting, 473–475
autoenrollment for certificates, 185–186
Automatic Updates configuration, 186–188
backups of, 164
capabilities of, 136
changes from previous versions, 135–136
compatibility issues, 139
computer startup and shutdown scripts, 177–178
configuration options, 154
containers, 137
defined, 136
deleting GPOs, 169
deploying security policies to multiple computers, 210
deploying security templates, 202–203
deploying software with, 180–185
determining GPO sources of settings, 170–171
DFS Replication Service for, 141
disabling local group policies, 143
domains, for, 145–147
editing with GPMC, 148–149
EFS recovery agents, 529–530
event messages from, 141
folder redirection, 172–176
gpupdate command, 160
Group Policy Management feature, 36
importance of, 135
inheritance with, 137, 154–157
language specification, 140–141
link order, 154–157
local group policies, 136
local Group Policy Editor, 140
logging, 141
loopback processing settings, 166
Machine folders, 146
Manage Group Policy Links right, 292
Management Console. See GPMC (Group Policy Management Console)
modeling, 160–162, 165
Network Location Awareness with, 141
networking policies, 533, 537
nodes and notation for, 135–136
objects. See GPOs (Group Policy objects)
OUs, for, 145–147
permissions for managing, 154
Point And Print Restrictions, 566–568
printer related, 552, 565–568
propagation of, 157–160
replication mechanism for, 141
restoring from backups, 164–165, 171
RSoP (Resultant Set of Policy), 165, 170–171
script assignment with, 176–179
security settings, 158, 162, 171
security templates, 158, 162, 171
security templates for. See security templates sites, for, 145–147
Group Policy Management Editor

slow-link detection, 166–169
software deployment with, 180–185
Supported On field, 139
timing of application of, 138
troubleshooting, 170–171
upating at startup issues, 138
User folders, 146
user logon and logoff scripts, 178–179
User vs. computer policies, 138, 166
version differences in, 139
Windows Vista policy settings, 140

Group Policy Object Editor (GPOE), 140–141, 143
Group Policy Starter GPO Editor, 139–140
groups. See group accounts
Guest accounts, 285
Guests group
Guest account membership in, 285
rights identical to Everyone group, 291

H
handles, statistics for, 92, 96–97
hard disk drives
allocation unit size, 381, 383
average seek times, 363
basic. See basic disks
capacities of, 363
characteristics of, 363–364
Check Disk utility, 390–392
compression of, 382, 395
converting to NTFS, 386–388
crash dump partitions, 373
decompressing, 396–397
defragmenting, 393–395
device drivers for, loading during installations, 54
disk duplexing, 413
Disk Usage statistics in Resource Monitor, 118
dynamic. See dynamic disks
eSATA (External Serial ATA), 369
errors, repairing, 390–392
failure detection, 520
Foreign status, 371, 377
hot swapping, 370
initialization of new drives, 370
installing, 370
installing the OS onto, 46
local vs. networked drives, 363
logical drive partitions. See logical drives
management tool for. See Disk Management master file tables, 388
maximum sustained data transfer rates, 364
mounting disks to drive paths, 379
moving dynamic disks to a new system, 376–377
MTTF (mean time to failure), 364
No Media status, 372
Not Initialized status, 372
offline status, 371, 376
Online (Errors) status, 371, 376
paging files. See paging partitioning. See partitions, drive performance counters for, 131
physical drive issues, 363–364
power management issues, 7
preparing for use, overview of, 365
RAID implementations. See RAID: RAID 0; RAID 1; RAID 5
reactivating, 376
RECOVER command, 52
rescanning, 376
rotational speeds, 363
SANs of. See SANs (storage area networks)
space requirements for installing R2, 44
status of, viewing, 370–372
Storage node of Server Manager, 71
temperature ranges for, 364
troubleshooting volume status issues, 406–407
tuning I/O performance, 131
Unreadable status, 371
Unrecognized status, 372
virtual. See VHDS (virtual hard disks)
hard page faults, 129
hardware
CPUs. See processors
events logs for, 108
failures, overview of recovery issues, 518–520
memory. See memory (RAM)
storage. See drives
hardware independence, 2
hibernation, 2
hidden shares, 454–456
H-node (hybrid), WINS, 22
home directories, user, 329–330, 345
home folders
assigning, 326
multiple accounts, setting for, 350–351
home network type, 12
%HomeDrive%, 327
%HomePath%, 327
HOSTNAME command, 50
hot swapping drives, 370
hotfixes, 43
Hyper-V, 34, 62–66

I
IE ESC (Internet Explorer Enhanced Security Configuration), 72–73
IF command, 50
IIS (Internet Information Services)
Intranet Update Service Locations policy for, 187–188
managed service accounts for, 318–322
Web Server role, 35
WinRM IIS Extension, 39
implicit groups, 286
importing accounts, 346–347
incident reports, 427
incremental backups, 497–498
Indexing Service, 359
InetOrgPerson object, 277
informational events, 109
infrastructure master role
function of, 232
seizing roles, 258–260
transferring, 256
transferring roles, command line for, 258
viewing, 255–256
infrastructure masters, 229
inheritance
ACEs, enabled by default, 277
GPOs, of, 137, 154–157
objects, of, 467–468
overriding, 137
Initial Configuration Tasks console, 67–70
Ink and Handwriting Services, 37
leases, DHCP, 586, 590, 615, 624–625, 627–628
licensing, 42
link order of group policies, 154–157
link-layer filtering, 621–622
Link-Local Multicast Name Resolution. See LLMNR (Link-Local Multicast Name Resolution)
link-local unicast IPv6 addresses, 590
links, configuring for sites, 265–268
List Folder Contents permission, 469
live migration, 63
LLMNR (Link-Local Multicast Name Resolution) disabling, 24
DNS client computer use of, 632
name resolution without DNS, 23–24
PNRP for, 37
load balancing, 37
local accounts
authentication of, 276
managed virtual accounts, 318, 322
local area connections. See connections, network
local group policies
accessing settings for, 143 Administrators and Non-Administrators, 142, 144–145
defined, 136
disabling, 143
folders for, 144
layers of GPOs, 142
Local Group Policy GPO, 142
rights assignments, viewing, 291
security templates, changing settings with, 192–193
user rights policies, configuring, 307, 309–310
user-specific, 142, 144–145
Local Group Policy Editor, 291
Local Group Policy Object Editor, 140
local groups
adding users to, 40
creating, 315–316
defined, 279
policies for. See local group policies
local profiles, 337–342
local user accounts
changing passwords, 347
creating, 312–313
defined, 278
rights configuration, 307, 309–310
Local Users And Groups utility changing passwords, 347
creating local groups, 315–316
local user account creation, 278
LocalAccountTokenFilterPolicy key, 74
LocalService account, 284
LocalSystem account, 283–284, 288
lockout policy, 352
logging
Active Directory logs, 108
application logs, 107–108
archiving logs, 114–116
data collectors for. See
data collector sets
data collector reports, 122, 126–127
event. See event logging
Group Policy logs, 141
logical drives
deleting, 386
purpose of, 379
local processor idling, 8–10
logoffs
audit policies, setting, 474–475
default nature of, 6
Force Logoff When Logon Hours Expire policy, 332
user logoff scripts, 178–179
Logon Locally user right, 353
logon names
creating, 310, 312
FQDNs, 278
naming schemes for, 299
parts of, 278
Pre-Windows 2000 vs. R2, 343
rules for, 298
logon rights
defined, 286
table of, 290
logon scripts
assignment methods for, 178–179
creating, 328–329
multiple accounts, setting for, 350–351
names, changing, 345
paths to, setting, 326
logons
audit policies, setting, 474–475
authentication of. See authentication
disabled accounts preventing, 352
failure auditing of, 352
Group Policy application during, 138
hour restrictions on user accounts, 330–332, 351
lockout policy preventing, 352
mandatory profile issues, 337
names. See logon names
passwords for. See passwords
rights, 286, 290
scripts for. See logon scripts
single sign-on, 276
timing synchronization of servers, 353
Windows Logon, displaying, 41–42
workstation restrictions, 332–333, 351, 353
loopback processing settings, 166
LPR Port Monitor, 37
managed virtual accounts, 214, 318, 322
mandatory accounts, 337, 353
Map Network Drive, Windows Explorer, 357
mapping drive letters, 53
mapping network drives, 464–465
master boot code, 365
master file tables (MFTs), 388
maximum lifetimes for tickets policies, 306
Maximum Password Age policy, 302–303
maximum processor state, 8
Maximum Tolerance For Computer Clock Synchronization policy, 306–307
MBR (master boot record) partitions, 365
MD/MKDIR command, 50
Mdsched.exe, 520
member servers, 14
memory (RAM)
adding, criteria for, 97
built-in diagnostics for, 520
DEP (Data Execution Prevention), 83–84
dump file options, 87–88
Kernel Memory statistics, 96
Memory Usage statistics, Resource Monitor, 118
nonpaged pool, 93
paged pool, 93
paging files, 80–82, 374
peak working sets, 93
Physical Memory statistics, 96
process utilization of, viewing, 91
tuning performance of, 128–130
usage graphs, 95–96
Windows Memory Diagnostics, 44
Message Queuing, 37
messages, warning, 519
MFTs (master file tables), 388
Microsoft Exchange Server. See Exchange Server
Microsoft Update, 133–134.
See also updates
Microsoft Windows logs, 108
migration issues, 47
Mini Windows PC environment (MINWINPC), 49–53
Minimum Password Age policy, 303
Minimum Password Length policy, 303
minimum processor state, 8
MINWINPC commands, table of, 49–53
mirrored volumes
basic disks, limitations of, 404
breaking mirrored sets, 416–417
dynamic drive requirement, 372–373
Failed Redundancy status, 417
RAID 1, 411–419
removing, 418–419
repairing, 417–418
M-node (mixed), WINS, 22
Modify An Object Label privilege, 289
Modify permission, 469
modularization of architecture, 2
monitoring servers
baselines, establishing, 116–117
importance of, 116
Performance Monitor
for, 119
plans for, 117
Reliability Monitor for, 119–120
Resource Monitor for, 117–118
tools for, overview of, 117
MORE command, 50
mounting partitions, 380
MOUNTVOL command, 50
MOVE command, 51
MPIO (Multipath I/O)
File Services role, option for, 358
function of, 37
requirement for SAN access, 421
.msi files, 181
multicast addresses, 590, 611–612
Multipath I/O (MPIO), 37
multiple default gateways, 544–545
multiple operating system servers, 87. See also dual booting
multiple-core processor power management, 8–10

Name resolution services
DNS. See DNS (Domain Name System)
LLMNR (Link-Local Multicast Name Resolution), 23–24, 37, 632
reverse lookup configuration, 642–644
supported services list, 18
WINS (Windows Internet Name Service), 21–22
name servers, 654–655
naming computers, 47, 69, 77–78
naming contexts, managing, 269–270
NAP (Network Access Protection), 601–603
NAT (Network Address Translation), 538
NBTSTAT command, 51
NDF (Network Diagnostic Framework), 447, 539
Network Awareness, 534–535
Network Diagnostics, 534
network direct memory access (NetDMA), 13
Network Discovery, 534–535
network drives, 464–465
Network Explorer
Network Discovery with, 535
purpose of, 533
Network identity, 295
Network Location Awareness, 141
Network Map, 534
Network Policy and Access Services (NPAS), 34, 333–335
Network Policy Servers, 602–603
networking
adapters for. See network adapters
addressing for. See IP addresses
administrative template for, 150
networking, continued
authentication protocols for, 276
categories of networks, 12, 534–535
configuring IP addresses, 541–544
configuring with Initial Configuration Tasks console, 69
collections. See connections, network counters for, 132
diagnostics, 537
discovery options, 12
dynamic addressing for. See DHCP (Dynamic Host Configuration Protocol)
connections.
See connections, network
counters for, 132
diagnostics, 537
discovery options, 12
dynamic addressing for. See DHCP (Dynamic Host Configuration Protocol)
Hyper-V, configuring for, 546
IPv4. See IPv4
IPv6. See IPv6
latency issues, 132
Manage Network Configuration right, 292
multiple default gateways, 544–545
NDF (Network Diagnostic Framework), 539
Network Configuration Operators group, 292
Network Usage statistics, Resource Monitor, 118
OCSP (Online Certificate Status Protocol), 538
performance statistics in Task Manager, 97–98
pinging addresses, 542
policy settings for, 533, 537
prefix notation, 264
print services. See printers protocols overview, 12–13
RDP (Remote Desktop Protocol), 539
security policies for, 207
SRA (Secure Remote Access), 538
SSL (Secure Sockets Layer), 538
SSTP, 538
subnet masks, 541–542
TCP Chimney offloading, 538–539
TCP/IP for. See TCP/IP
Teredo, 538
tools for, list of, 11, 533–534
tracing networks, 539
VPNs for. See virtual private networks
NetworkService account, 284
New-cmdlet verb, 26
New Object—User Wizard, 310–312
Next Generation TCP/IP stack, 13
NFS (Network File System) Services for Network File System, 359
sharing, 459–461
NICs (network interface cards). See network adapters
NLB (Network Load Balancing), 37
No Access share permission, 451
nonpaged pool, 93, 130
normal/full backups, 497
Notepad launch methods, 41
NPS (Network Policy and Access Services), 34, 333–335
NTFS (Network Policy Server) Network Policy, 333–335
NPT (nested page tables), 63
Ntbackup.exe, 503
Ntds.dit, 227–228
Ntdsutil, 239, 523
NTFS compression, 395–397
disk quotas. See NTFS disk quotas
encrypted files, 397–401
FILE, converting from, 386–388
quotas. See NTFS disk quotas
resizing volumes, 388–390
self-healing NTFS, 390–391
Transactional NTFS, 390–391
volume formatting, recommended for, 407
NTFS disk quotas administrators exempt from, 480
configuring, 481–483
creating entries, 486–487
default limits, setting, 485
deleting entries, 487–488
disabling disk quotas, 489
disk quota limits, 479
disk quota warnings, 479
enabling, 480
enabling volumes for, 484–485
exporting settings, 488–489
Group Policy for, 481
importing settings, 488–489
independence of user quotas, 480
local volume management, 480
managing files of deleted users, 487–488
overhead from, 481
potential problems with, 479
recommendations for, 480
refreshing information for, 481
remote volume management, 480
Resource Manager quotas compared to, 478
rights required to set, 481
setting without enforcing, 480
SIDs for, 481
viewing entries, 485–486
NTFSC D dispensation authentication, 276
NX (no-execute page-protection), 83–84
objects
audit policies, setting, 474–475
directories. See objects, directory
file and folder. See objects, file and folder
inclusion and exclusion for, 467–468
management tools for, 466
ownership of, 466–467
parent-child structures of, 467
types of, 465–466
objects, directory. See also Active Directory
access controls for, 277
computer accounts, 246–250
importing and exporting, 346–347
InetOrgPerson object, 277
searching for, 244–246
security permissions, setting, 353–355
Self identity, 295
objects, file and folder
ownership, editing, 467
permissions for, 465
Windows Explorer for managing, 466
Oclist.exe, 42
Ocsetup.exe, 42
OCSP (Online Certificate Status Protocol), 538
offline domain join, Active Directory, 214, 252–253
offline work, shared folder
options for, 449
on-demand reports, 427
operations masters defined, 222
domain naming master role, 232, 257
domainwide roles, managing, 255–256
FSMO roles, 222, 255
infrastructure masters. See infrastructure master role
listing, 258
Netdom commands for, 258–260
PDC emulator. See PDC emulator master role
relative ID masters. See relative ID master role
role requirements, 232
schema master role, 232, 257
seizing roles, 258–260
transferring roles at command lines, 258
organizational units. See OUs (organizational units)
OUs (organizational units) Active Directory Users
And Computers folder for, 243
advantages of, 219
creating, 261–262
defined, 136, 215
deploying security policies to multiple
computers, 210
group policies for, 145–147
inheritance of group policies, 137
managing, 262
relationships of, 218–219
security templates with, 202–203

page faults
counter for, 129
peer process, viewing, 93
paged pool, 93, 130
paging
automatic management of, 82
configuring, 81–82
defined, 80
page file partitions, 374
parent domains, 19, 212, 630
parents, object, 467
partial integration of Active Directory and DNS, 19
partitions, drive
active partitions, 373, 374
boot, 373
clean installation options for, 44
crash dump partitions, 373
creation with Disk Management, 379–382
deleting, 54, 56, 386
effects on installing the OS, 46
extended partition capabilities, 378–379
extending, 54, 56
formatting, 54–55, 381–383
free space, 366
GPT vs. MBR partitions, 365
installations, configuring during, 54–55
logical drives in. See logical drives
mounting, 380
new, creating, 54–55
number of allowed partitions, 378–379
overview of, 378–379
page file partitions, 374
primary partitions, 378–379
removal during installations, forcing, 53–54
resizing, 388–390
system partitions, 374
unallocated, 366
partitions, replication. See replication partitions
passive cooling mode, 7–8
passwords
changing, 347
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
creating for user accounts, resetting, 249
defined, 80
defining, 80
define, 80
page file partitions, 374
parent domains, 19, 212, 630
parents, object, 467
partial integration of Active Directory and DNS, 19
partitions, drive
active partitions, 373, 374
boot, 373
clean installation options for, 44
flash dump partitions, 373
creation with Disk Management, 379–382
deleting, 54, 56, 386
effects on installing the OS, 46
extended partition capabilities, 378–379
extending, 54, 56
formatting, 54–55, 381–383
free space, 366
GPT vs. MBR partitions, 365
installations, configuring during, 54–55
logical drives in. See logical drives
mounting, 380
new, creating, 54–55
number of allowed partitions, 378–379
overview of, 378–379
page file partitions, 374
primary partitions, 378–379
removal during installations, forcing, 53–54
resizing, 388–390
system partitions, 374
unallocated, 366
partitions, replication. See replication partitions
passive cooling mode, 7–8
passwords
changing, 347
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
creating for user accounts, resetting, 249
define, 80
define, 80
definition, 80
define, 80
page file partitions, 374
parent domains, 19, 212, 630
parents, object, 467
partial integration of Active Directory and DNS, 19
partitions, drive
active partitions, 373, 374
boot, 373
clean installation options for, 44
flash dump partitions, 373
creation with Disk Management, 379–382
deleting, 54, 56, 386
effects on installing the OS, 46
extended partition capabilities, 378–379
extending, 54, 56
formatting, 54–55, 381–383
free space, 366
GPT vs. MBR partitions, 365
installations, configuring during, 54–55
logical drives in. See logical drives
mounting, 380
new, creating, 54–55
number of allowed partitions, 378–379
overview of, 378–379
page file partitions, 374
primary partitions, 378–379
removal during installations, forcing, 53–54
resizing, 388–390
system partitions, 374
unallocated, 366
partitions, replication. See replication partitions
passive cooling mode, 7–8
passwords
changing, 347
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
counter for, 129
creating for user accounts, resetting, 249
definition, 80
definition, 80
definition, 80
definition, 80
page file partitions, 374
parent domains, 19, 212, 630
parents, object, 467
partial integration of Active Directory and DNS, 19
partitions, drive
active partitions, 373, 374
boot, 373
clean installation options for, 44
flash dump partitions, 373
creation with Disk Management, 379–382
deleting, 54, 56, 386
effects on installing the OS, 46
extended partition capabilities, 378–379
PDC emulator master role
function of, 232
seizing roles, 258–260
transferring, 256
transferring roles, command line for, 258
viewing, 255–256
peak working sets, 93
Peer Name Resolution Protocol (PNRP), 37
performance. See also Performance Monitor
applications, system settings for, 80
baselines, establishing, 116–117
built-in diagnostics for, 520
counters for. See counters
data collector sets, 122–127
event tracing data, 123, 125
I/O handle statistics, 96–97
monitoring. See monitoring servers
networking statistics in Task Manager, 97–98
Physical Memory statistics, 96
Resource Monitor for tuning, 117–118
Task Manager Performance tab, 95–97
tools for monitoring, overview of, 117
virtual memory, configuring, 81–82
visual effects settings, 79
Performance Monitor accessing, 119
alerts, configuring counters for, 127–128
counters, adding, 120–122
counters for, 119
data collector reports, 122, 126–127
data collector sets, 122–127
graphs of, 119
memory counters, 129–130
paging counters, 130
remote access requirements, 121
view types, choosing, 120
permissions
Active Directory, setting, 353–355
file and folder objects, for, 465, 468–473
network drive connections, for, 464
object inheritance of, 467–468
permissions, continued
printer, 577–579
setting for files and folders, 471–473
sharing folders, for, 449–454
special file permissions, table of, 470
special folder permissions, table of, 471
special identities, 294–295
user, defined, 286
physical drives
Physical Memory statistics, 96
PIDs (process IDs), 93
PING command, 52
pinging addresses, 542
planning
backups and recovery, 495–497
deployments. See deploying Windows Server 2008 R2
modeling Group Policy, 160–162
P-node (peer-to-peer), WINS, 22
Pnputil.exe, 42
PNRP (Peer Name Resolution Protocol), 37
policy editors, 140
policy, group. See Group Policy
POPD command, 52
ports, printer, 574
power management
ACPI, 6–10
active vs. passive system cooling, 7–8
Balanced plan, 7
changing plans for, 6–7
firmware compliance issues, 9
global power states, 10
options for, 7
Powercfg.exe command-line utility, 7
sleep states, processor, 10
Powershell.exe. See Windows PowerShell 2.0
preboot environment, 2
predefined groups, 283, 285
predefined user accounts, 283–285
preinstallation environment, 2
primary domain controllers defined, 14
PDC emulator master role, 232, 255–260
primary groups, 317–318
primary partition limitations, 378–379
printers
Active Directory, listing in, 572
administrative template for, 150
autostart feature, 556
canceling jobs, 582
canceling to network printers, 563–564
deploying connections with Group Policy, 565–566
detection issues, 558–559
Distributed Scan Server service, 552
document default settings for, 579
document priority, setting, 582–583
document properties, viewing, 582
drivers for, 550–551, 557, 559–560, 562, 573–574
filtering views of, 570–571
Group Policy affecting, 552
high-volume printing management, 580
installing network-attached printers, 561–563
installing physically attached printers, 556–560
Internet Printing service, 552
job error notifications, 580
jobs, 551
local vs. network devices, 550
logging events, 580
LPD (Line Printer Daemon) Service, 552
LPR Port Monitor, 37
management techniques, 580–581
monitoring, 570–571
monitors, 551–552
moving to new print servers, 569–570
objects for, 466
pausing, 581–582
permissions for, 577–579
Point And Print Restrictions, 566–568
port configuration, 574
Print and Document Services, 34
Print and Document Services role services, 34, 552–553
PRINT command, 52
Print Management tool, 554–555
Print Server Properties dialog box, 579–580
print server services, 552
print servers vs. network-attached printers, 550
PRINT$ share, 455
Printer Migration Wizard, 569–570
Printer Operators group rights, 291–292
prioritizing jobs, 575–576
properties of, setting, 572
queues, 551, 582
remote user access to, 560
resuming printing after pauses, 581–582
scheduling jobs, 575–576, 583
separator pages, 574
sharing for, 553, 557–558, 576–577
spool folder permissions, 579
spoolers for, 551, 575–576
spooling issues, 571–572
viewing, 554–555
priority, scheduling, 288
privileges. See also permissions
assignment of, 286
audit policies, setting, 474–475
table of, 287–289
processes
application initiation of, 89
audit policies, setting, 474–475
background, in the, 89–90
CPU Time, 92
CPU utilization for, 91
dependencies of, 93
descriptions of, 91
foreground, in the, 89
handles, 92
Increase A Process Working Set privilege, 288
I/O reads and writes, 92
memory usage, 91
names of, 91
nonpaged pool, 93
number in use, viewing, 97
page faults of, 93
paged pool, 93
peak working sets, 93
PIDs (process IDs), 93
priorities, 92
remote users, visibility of, 91
session IDs, 93
stopping, 94
System Idle Process, 93
Task Manager administration of, 91–94
thread counts of, 93
processors
64-bit only supported, 44
affinity settings, 9
CPU Usage category of Resource Monitor, 117
CPU usage counters, 131
CPU Usage graphs, 95–96
logical processor idling, 8–10
NX (no-execute page-protection), 83–84
power considerations, 7–9
processes, utilization for, 91
%Processor_Architecture% variable, 327
sleep states, 10
throttling for power savings, 7–8
tuning performance of, 130–131
product keys, 45, 48, 76
profiles, user. See user profiles
PROMPT command, 52
Proxy identity, 295
p-states, 8–9
public file sharing
access options for, 443
accessing public folders, 442–443
disabling, 445
enabling, 444
less secure than standard file sharing, 443
net session command, 457
overview of, 442
Public folder subfolders, 443
remote user accessibility of, 442
share objects, 466
public network type, 12
publishing directory information, 228
PUSHD command, 52
Quality Windows Audio Video Experience, 37
queries, Active Directory, 242
RAID
0 level. See RAID 0
1 level. See RAID 1
5 level. See RAID 5
Diskraid.exe command, 42
levels, comparison of, 411
levels supported by R2, 403
overview, 411
purpose of, 403
RAID 0
defined, 411
implementing, 412–413
repairing, 419–420
RAID 1
advantages of, 412–413
booting issues, 418
breaking mirrored sets, 416–417
defined, 411
Failed Redundancy status, 417
implementing, 413–415
removing mirrored volumes, 418–419
repairing, 417–418
RAID 5
advantages of, 412
basic disks, limitations on, 404
defined, 411
implementing, 415–416
regenerating status, 407
repairing, 419–420
RAM. See memory (RAM)
Rapid Virtualization Indexing (RVI), 62
RDP (Remote Desktop Protocol), 99, 539
RD/RMDIR command, 52
Read & Execute permission, 469
Read permission, 469
Read share permission, 451
reads, I/O counters for, 129, 131
processes, viewing in Task Manager, 92
Receive-side scaling (RSS), 13
Recenyle.exe, 524
RECOVER command, 52
recovery
Active Directory Recycle Bin for, 233–236
Advanced Boot Options, 524–526
application restores, 526–528
boots, options during, 524–526
core-server installation system recovery, 524
corrupted system files, 519–520
domain controllers, of, 523
encrypted file recovery, 528–532
file and folder restores, 526–528
GPOs, restoring, 164–165
hardware failure overview, 518–520
last known good configuration, 521
ntbackup.exe recoveries, 503
NTFS permissions of, 398–399, 401
Recovery Wizard,
Windows Server Backup, 526–528
Repair Your Computer installation option, 525–526
RPO (recovery point objective), 497
RTO (recovery time objective), 497
safe mode, 520–522
services, options for, 104–106
setting options for, 87–88
startup failure overview, 518–520
Startup Recovery Options, 524
Startup Repair Options, 524
Startup Repair Wizard, 524
system images, of, 524–526
System Recovery Options Wizard, 525–526
system state files, of, 522–523
Wbadmin for, 509–510
Windows Error Recovery mode, 522
Windows Firewall exceptions for, 510
Recycle Bin, Active Directory, 16, 213–214, 233–236
redirection of folders with Group Policy, 172–176
registry
auditing, 477
changes, recording with data collector sets, 125–126
REG commands, table of, 52
Regedit, 41
security templates for paths, 196–198
REGSVR32 command, 52
Regsvr32 utility, 88
relative ID master role function of, 232
seizing roles, 258–260
transferring, 256, 258
viewing, 255–256
Reliability Monitor, 119–120
REM command, 52
remote access
dial-in privileges, 333–335
management. See remote management
printers, enabling for, 560
SRA (Secure Remote Access), 538
users, 91, 98–99
Remote Assistance
defined, 37
managing, 134
remote computers
PowerShell, configuring for, 27–30
shared folders, viewing, 446–447
remote control sessions, 99
Remote Desktop
Initial Configuration Tasks
console, enabling from, 70
managing, 134
Remote Desktop Services
User identity, 295
Server Manager, Configure Remote Desktop option, 71
service for, 35
Remote Desktop Protocol (RDP), 99
Remote Differential Compression, 37
remote management
ADMIN$ share, 455
connecting to remote computers, 75
LocalAccountTokenFilterPolicy key, 74
PowerShell command for configuring, 75
requirements for, 74
Server Manager for, 72
services management requirements, 100
Windows Firewall settings for, 74–75
Windows PowerShell for, 75–76
WinRM for. See WinRM (Windows Remote Management)
remote monitoring, 121
Remote Procedure Call (RPC) over HTTP Proxy, 38
remote users
viewing processes of, 91
viewing sessions with Task Manager, 98–99
removable disks
characteristics of, 368–369
configuring, 369–370
defined, 367
eSATA (External Serial ATA), 369
file system options for, 368
FireWire connections, 369
USB connections, 368–369
Remove- cmdlet verb, 26
Remove Role Wizard, 221
REN command, 52
renaming computers, 47, 77–78
Repadmin, 273–274
Repair Your Computer installation option, 525–526
replication of directory data commands, table of, 274
Inter-Site Topology Generator, 271–272
monitoring with Repadmin, 273–274
multimaster replication model, 222
network installation scenario for, 230–231
recovery from, 272
Replication Diagnostics Tool, 240
service dependencies of, 273
site link bridges, 268–269
site links, 265–266
troubleshooting, 272–274
types of data replicated, 228
replication partitions
bridgehead server requirements, 272
purpose of, 227
reports
data collector reports, 122, 126–127
storage. See storage reports
Reset Passwords On User Accounts right, 292
Resource Exhaustion Detection And Recovery, 519
Resource Manager disk quotas
creating new quota templates, 492–493
creating quotas, 493
limits, 490
modifying quota templates, 491–492
NTFS disk quotas compared to, 478
NTFS disk quotas in parallel with, 489
quota types, 490
templates for, 490
Resource Monitor, 117–118
Restart Manager, 519
Restartable Active Directory Domain Services, 16–18
restoring backups. See recovery
Restricted identity, 295
Resultant Set of Policy (RSoP), 165, 170–171
reverse lookup configuration, 642–644
RIDs (relative IDs)
RID masters. See relative ID master role
user accounts of, 278–279
rights. See also privileges
logon, 286, 290
user. See user rights
roaming profiles
changing from or to, 343
creating, 338–339
defined, 337
encryption recovery for, 528–532
RODCs (read-only domain controllers)
deployment of, 212–213
DNS services on, 20, 632–633
purpose of, 16–17
role services
AD CS (Active Directory Certificate Services), 14–15, 33
AD DS. See AD DS (Active Directory Domain Services)
AD FS (Active Directory Federation Services), 15, 33, 276
AD LDS (Active Directory Lightweight Directory Services), 15, 33
AD RMS (Active Directory Rights Management Services), 15, 33
AD WS (Active Directory Web Services), 16, 241
Add Role Services Wizard, 359
Add Roles wizard. See Add Roles Wizard adding, 61
configuring in Server Manager, 59
defined, 32
dependencies of, 32
File Server Resource Manager. See FSRM (File Server Resource Manager)
File Services. See File Services role
Hyper-V, 34, 62–66
NPAS, 34, 333–335
Print and Document Services, 34
Remote Desktop, 35
remote management, 74
roles, server. See server roles
root domains, 19, 629–630
ROUTE command, 52
RPC (Remote Procedure Call)
Remote Procedure Call (RPC) over HTTP Proxy, 38
replication dependence on, 273
RPC over IP for site links, 266
RPO (recovery point objective), 497
RSAT (Remote Server Administration Tools)
purpose of, 38, 133
required for remote management, 74
RSoS (Resultant Set of Policy), 165, 170–171, 239
RSS (receive-side scaling), 13
RTO (recovery time objective), 497
RVI (Rapid Virtualization Indexing), 62

S
safe mode, 520–522
SANs (storage area networks)
clusters, defining, 424
creating LUNs, 423
deleting LUNs, 424
Fibre Channel SAN configuration, 421–422
iSCSI Initiator options, 420
iSCSI SAN configuration, 422–423
LUN management, 420–424
Manage iSCSI Targets, 422–423
MPIO requirement, 421
Storage Manager for SANs, 38, 358, 420–424
types of LUNs, 420
VDS (Virtual Disk Service), 420
Sc query type=driver command, 42
scanning service, 552
scheduled reports, 427
schema data, Active Directory, 228
schema master role
forests, required for, 232
seizing roles, 257, 258
Sconfig (Server Configuration)
core-server installation
network configuration, 47
remote management configuration, 75
starting, 68
tasks available in, 41
scopes, DHCP
activating, 615
BOOTP support, 615–616
class network address ranges for, 590
creating normal scopes, 606–611
deactivating, 615
defined, 590
deleting, 616
exclusion ranges in, 622–623
global unicast addresses, 590
link-local unicast IPv6 addresses, 590
modifying existing, 615
multicast addresses, 590
multicast scope creation, 611–612
multiple on a single network, 616
normal, 590, 606–611
setting options for, 612–614
split, 591, 616–620
statistics for, viewing, 620
supercscopes, 591, 605–606
types of, 590–591
scopes, group, 280–281, 315
scripts
computer scripts, assigning, 177–178
permissions needed to run, 469
types of, 176
user scripts, assigning, 178–179
WSH, 176, 231
SCSI (Small Computer System Interface) drives, 364–365.
See also iSCSI
searching
Active Directory with Users And Computers, 244–246
users or groups, for, 325–326
Windows Search Service, 359, 362
Windows TIFF IFilter, 39
Secedit, 201–202
second-level address translation (SLAT), 63
Secure Remote Access (SRA), 538
Secure Socket Tunneling Protocol (SSTP), 538
Secure Sockets Layer (SSL), 538
security configuration wizard. See Security Configuration Wizard
DEP (Data Execution Prevention), 83–84
event logs, 107
file screening capability. See file screening
Group Policy for. See Group Policy passwords for. See passwords
permissions for. See permissions policies. See security policies
templates. See security templates
UAC (User Account Control), 2–3
user account security for, 335–336
Windows File Protection, 88
Windows Server security model, 275–277
Security Configuration And Analysis snap-in
analyzing security templates, 190, 199–200
applying security templates, 191–192, 202
changing database settings, 200–201
disadvantages of, 199
Security Configuration Wizard
applying security policies, 209
Audit Policy options, 207–208
authentication options, 207
baseline server selection, 205
configuration sections, 204
creating security policies, 204–208
defaults, 208
network security rules, 207
purpose of, 203–204
rolling back security policies, 209
Server Manager, running from, 72
server role selection, 205
services, selecting, 206–207
SMB Security Signatures, 207
starting, 204
security descriptors, 277
security groups
creating, 314–315
defined, 280
security identifiers. See SIDs (security identifiers)
security permissions, setting, 353–355
security policies
applying, 209
Audit Policy, 207–208
authentication options, 207
baseline server selection, 205
client feature selection, 206
creating, 204–208
defined, 203
deploying to multiple computers, 210
editing, 208
location specification for, 208
network security rules, 207
security templates

security policies, continued
registry settings affected by, 207
rolling back, 209
security templates with, 204, 208. See also security templates
server role selection, 205
service selection, 206–207
SMB Security Signatures, 207

security templates
analyzing, 199–200
applying, 202
blank templates, 190
changing database settings, 200–201
changing settings for, 192–193
configuring, 199–200
creating templates, 191
deploying to multiple computers, 199, 202–203
file system paths, configuring, 196–199
OU organization issues, 202–203
paths for templates, 191
policies affected by, 189
registry paths, configuring, 196–198
rollback templates, 201–202
Security Configuration And Analysis snap-in, 190–192
security policies, incorporating in, 204, 208. See also security policies
snap-in for managing, 190–191
steps for working with, 190
system services, configuring, 194–195
User Configuration not included by, 190
security zones, Internet Explorer, 72–73
Self identity, 295
self-healing NTFS, 390–391
Server Configuration utility. See Sconfig (Server Configuration)
Server Core installations. See core-server installations
Server Manager
adding role services, 61
adding server roles, 58–60
capabilities of, 67
Change System Properties option, 71
Check For New Roles option, 72
clearing event logs, 114
command-line counter-part, 57
Configure Remote Desktop top option, 71
connecting to remote computers, 75
customer experience improvement options, 73
details pane, 71–72
event log access, 108–110
event logging options, setting, 112–113
features, adding and removing, 61–62
Features Summary section, 73
filtering event logs, 110–112
installing domain controllers, 254
layout of window for, 70
nodes of console tree, 70–71
purpose of, 32
remote management with, 72, 100
removing role services, 61
removing server roles, 60
reporting options, 59
Resources And Support section, 73
role management with, 56–61
role services, viewing current, 60–61
Roles node, 70–71
Roles Summary section, 73
Security Configuration Wizard, starting, 72
Security Information section, 72
server roles, viewing current, 57–58
Services node, 99–106
starting, 70
View Network Connections option, 71
Windows Error Reporting options, 73
Windows Firewall, launching from, 72
Windows Update, launching, 72
Server Operators group, 291–292
server roles
Add Roles Wizard, 70
adding, 58–59
Application Server role, 33
dependencies of, 32
DHCP Server role, 34
DNS Server role, 34
Fax Server role, 34
new, checking for, 72
Oclist.exe, 42
removing, 60
Roles node of Server Manager, 70–71
Roles Summary section of Server Manager, 73
selection for security policies, 205
Server Manager for configuring, 32
table of, 33–35
viewing, 57–58
Web Server (IIS), 35
Servermanagercmd.exe, 32
service accounts, 318
services
account management feature of Active Directory, 16
managed service accounts for, 318–322
managed virtual accounts for, 318, 322
objects and managers for, 466
recovery policies for, 519
restrictions, viewing, 94
roles, server. See role services
security policies for, 206–207
Service identity, 295
stopping with Task Manager, 94–95
Svchost.exe associated contexts, 94–95
system. See system services
Services console, restartable
Active Directory Domain Services, 17–18
Services for Macintosh, 317–318
Services for Network File System, 359, 459–461
sessions, IDs of, 93
Set- cmdlet verb, 26
SET command, 52
SETLOCAL command, 52
setup logs, 107
Setup program
clean installations with, 44–45
command-line administration in, 49–53
existing settings, using, 46
installation process, 46
recovery options, 44
upgrade installations, performing, 47–49
Where Do You Want To Install page, 46
SFC command, 52
shadow copies
creating, 462
default schedule for, 461
deleting, 463–464
disabling, 464
restoring, 462–463
reverting entire volumes
to previous copies, 463
shared folders, summaries
for, 447
substituting for backups,
496
viewing settings for, 462
VSS, 501
Share And Storage Manage-
ment, 446–447
sharing
NFS (Network File System)
sharing, 459–461
printer sharing, 553,
557–558, 576–577
public files. See public file
sharing
share objects, 466
special shares, 454–456
standard method for
files. See standard file
sharing
SHIFT command, 53
shortcuts, access permissions
for, 469
shrinking volumes, 388–390
shutdown script assignment,
177–178
SIDs (security identifiers)
disk quotas, tracking
with, 481
group accounts, of,
281–282
relative ID master role,
232
renamed accounts, 344
user accounts, of,
278–279
Simple Mail Transfer Protocol
(SMTP), 266
Simple Network Management
Protocol (SNMP) Services, 38
Simple TCP/IP Services, 38
single sign-on, 276
sites
collection steps, 262–263
default site creation, 262
defined, 136, 215
domain controllers, associating with, 265
GPMC, node for, 147–148
group policies for,
145–147
independence from
domain structures, 220
inheritance of group poli-
cies, 137
intersite replication, 220
link bridge configuration,
268–269
link configuration, 
265–268
link costs, 267
link creation, 263
link replication schedule,
267
subnet creation for, 264
transport protocols,
266–269
SLAT (second-level address
translation), 63
sleep states, computer, 2
sleep states, processor, 10
Slmgr commands, 42
slow-link detection settings,
166–169
smart cards, requiring, 335
SMB (Server Message Block),
447
SMB Security Signatures, 207
SMTP (Simple Mail Transfer
Protocol), 266
SNMP (Simple Network
Management Protocol)
Services, 38
soft page faults, 129
Software Installation policy,
180–185
spanned volumes. See also
volume sets
basic disks, limitations
of, 404
creating, 408–409
defined, 403
NTFS, recommended
for, 407
resizing, 388–390
special identities, 283, 286,
294–295
special shares, 454–456
split scopes, 591, 616–620
SQL Server 2005 Embedded
Edition, 39
SQL Server managed service
accounts, 318–322
SRA (Secure Remote Access),
538
SSL (Secure Sockets Layer), 538
SSTP (Secure Socket Tunneling
Protocol), 538
stand-alone servers, 14
standard edition, 3–5
standard file sharing
advantages over public
file sharing, 443
closing open shared files,
458–459
creating shares for folders,
447–450
descriptions for folders,
448
enabling, 444
ending user sessions,
457–458
hiding shared folders, 448
membership required to
set folder shares, 447
names of shares, 448
net session command, 457
net share command, 445
NFS (Network File System)
for, 447
offline use options, 449
overview of, 441–442
permission settings,
449–454
security-setting depen-
dence of user access,
442
share objects, 466
SMB (Server Message Block), 447
special shares, 454–456
stopping sharing, 459
viewing currently open
file information, 458
viewing existing shares,
445–447
viewing sharing sessions,
456–457
START command, 53
Start menu, 6
StartRep.exe, 524
Startup Recovery Options, 524
Startup Repair Wizard, 524
startups, system
audit policies, setting,
474–475
computer startup script
assignment, 177–178
DHCP availability for, 586
failure overview, 518–520
Group Policy application
during, 138
last known good configu-
ration, 521
safe mode, 520–522
Startup And Recovery
dialog box, configuring
from, 86–87
StR (Startup Repair Tool),
519–520
Stop errors
details, logging of,
518–519
paging file size required
to record, 82
stopping applications, 90
Storage Manager for SANs,
358
storage reports
auditing reports, 433
configuring parameters,
432–433, 436
generating on-demand, 440
global options for, 429
location configuration,
432–433
scheduling, 439–440
table of standard reports,
428
types of, 427
StR (Startup Repair Tool),
519–520
striped sets, 411–413, 416,
419–420
striped volumes

basic disks, limitations of, 404
creating, 408–409
disk striping, 411–413, 419–420
RAID 0, implementing, 412–413
stripes, 411–412
SUA (Subsystem for UNIX-based Applications), 38
subdomains, 212
subnet masks, 541–542
subnets
creating, 264
defined, 215
deleting from DNS servers, 648–649
place in site architecture, 136
well-connected goal for, 220
SUBST command, 53
superscopes, 591, 605–606
support service summary, 134–135
symbolic links, privilege for creating, 288
System console, 76–77
system crashes
backup partitions, 373
degraded recovery, options for, 87–88
Stop errors, 82, 518–519
system environment variables configuring, 84–86
most commonly used, 327
multiple accounts, setting for, 350–351
user account creation with, 327–328
system event audit policy settings, 474–475
system failure options, 87–88
system files, corrupted, 519–520
System identity, 295
System Idle Process, 93
system images, corrupted, 44, 524–526
system logs, 107
system partitions
defined, 374
mirrored, booting issues, 418
mirroring, 413
striped sets, excluding from, 412
System Properties dialog box accessing from System console, 77
Advanced tab, 79–88
applications, performance settings for, 80
Computer Name tab, 77–78
DEP (Data Execution Prevention), 83–84
device drivers, downloading, 78–79
environment variables, configuring, 84–86
Hardware tab options, 78–79
joining computers to domains, 78
names of computers, changing, 78
performance settings, 79–80
System Recovery Options Wizard, 525–526
system services accounts of, security issues for, 104
descriptions of, 100
disabling by operating systems, 100
disabling manually, 102
failed start notifications, 101
logon accounts for, 100
logon configuration options, 103–104
managing with Server Manager, 99–106
names of, 100
pausing, 101
recovery options for, 104–106
resuming and restarting, 101
security templates for configuring, 194–195
starting, 101
startup configuration, 102–103
startup types, 100
status of, viewing, 100
stopping, 101
unnecessary services, 106
viewing with Task Manager, 94–95
system settings administrative template for, 150
System folder, Active Directory Users And Computers, 243
system startup. See startups, system
system state backups, 508, 522–523
recoveries, 510
System utility capabilities of, 68
user profile management, 339–343
SystemInfo, 43
%SystemRoot%, 327
SYSVOL share, 455
Tape drives, 499–502
Task Manager
application control with, 90–91
Applications tab, 90–91
Base Priority tab, 92
columns, adding more, 92–93
CPU Time tab, 92
Handles tab, 92
I/O tab, 92
launching, 90
networking performance statistics, 97–98
New Task command, 41
nonpaged pool, 93
page faults of processes, 93
paged pool, 93
peak working sets, 93
Performance tab, 95–97
PIDs (process IDs), 93
process administration with, 91–94
remote user session management, 98–99
session IDs, 93
stopping processes, 94
system services, viewing, 94–95
System statistics, 96–97
thread counts, 93
Task Scheduler
viewing, 134
Wbadmin, scheduling backups using, 516–517
TCP Chimney offloading, 538–539
TCP/IP. See also IP addresses configuring IP addresses, 541–544
installing, 539–540
multiple default gateways, 544–545
Next Generation TCP/IP stack, 13
overview, 12–13
Simple TCP/IP Services, 38
TCP Chimney Offload feature, 13
Telnet, 38
templates administrative templates, 149–151
security. See security templates
Teredo, 538
threads
number in use, viewing, 97
processor, viewing number of, 93
queueing performance counter, 130
throttling, processor, 8
tickets, account policy for, 305–307
time
logon hour restrictions on user accounts, 330–332
TIME command, 53
time zones, setting, 69
Windows Time, 135
TITLE command, 53
tls (transport layer security), 538
TLDs (top-level domains), 212
TPM (trusted platform module), 36
trace data collector type, 123, 125
TRACERT command, 53
treading networks, 539
transactional NTFS, 390–391
transitivity of links, 268–269
trees, domain, 215–217
trusted platform module (TPM), 36
tuning system performance
disk I/O, 131
memory, 128–130
networks, 132
processors, 130–131
TYPE command, 53
up time statistics, 97
updates
automatic, enabling, 69
marking of in-use files for, 518
Microsoft Update, 133–134
options during clean installations, 45
software update deployment, 183–184
Windows Update not enabled by default, 69
Windows Update to configure Automatic Updates, 134
Wusa.exe Patchname.msu command, 43
upgrade installations
32-bit operating systems, upgrading not allowed from, 47
core vs. full-server option, 48
defined, 43
migration issues, 47
performing, 47–49
upgrades, application, 184–185
USB (universal serial bus)
power management issues, 7
removable disk characteristics, 368–369
USER flash drives, 384
user account control (UAC), 2–3
user accounts
account lockout policies, 304–305
Administrator account, 284–285
auditing file access, 475–477
built-in, in, 283–284, 347
capability types granted to, 286–287
contact information of, 323–325
Create And Delete Groups right, 291
Create, Delete, And Manage User Accounts right, 292
creating domain user accounts, 310–312
creating local user accounts, 312–313
deleting, 347
disabled, 348, 352
display name creation, 310, 312
display name guidelines, 298
domain accounts. See domain user accounts
domain vs. local user, 278
enabling, 348–349
environment settings for, 326–330
expiration options, 351–352
expired, 348
fQDNs (fully qualified domain names), 278
global user rights configuration, 307–309
group accounts compared to, 277
Guest accounts, 285
guidelines for organizing, 297–301
home directories, 329–330, 345
home folders, 326
hour restrictions for logons, 330–332, 351
InetOrgPerson object, 277
Kerberos policies, 305–307
listing, 343–344
local user rights configuration, 309–310
LocalService account, 284
LocalSystem account, 283–284
locked out, 348
logon hour restrictions on, 330–332
logon names for. See logon names
logon options, 351–352
logon rights, 286, 290
logon workstations restrictions, 332–333, 351
moving, 349
multiple accounts, editing method, 347, 349–352
naming schemes, 299
NetworkService account, 284
password policies, 302–304
passwords of. See passwords
permissions, setting, 353–355
privileges for. See privileges
profiles. See user profiles
Properties dialog boxes for, accessing, 325
property configuration, 349–352
public certificates for, 278
purpose of, 275
renaming, 344–345
reset passwords on user accounts right, 292
restricted accounts, 291
searching for, 325–326
security options, 335–336
share permissions, adding to, 452–453
SIDs of, 278–279, 344
single login system, 276
system environment variables for, 327–328
upgrading, 343–348
user assignment software deployment method, 180–185
user contact information, 323–325
Virtual Network Manager, 63
Virtual PC, 63
Virtual Server, 63
virtualizing servers, 34, 62–66
visual effects settings, 79
VOL command, 53
volume sets
creating, 408–409
deleting, 410
failed drives, data loss from, 405
NTFS, recommended for, 407
purpose of, 403
status of, viewing, 405–407
striped sets, 411–413
volumes
active, 373, 374
boot, 373
capabilities of, 404
creation with Disk Management, 379–382,
408–409
defined, 404
deleting, 386, 410
drive letter assignment, 409
dual-boot capability, 404
dynamic, advantages of, 404.
See also dynamic disks
formatting options, 409
labels for, 381–382, 385
layouts of, 404
master file tables, 388
mirroring, 414–415
NTFS recommended for, 407
properties of, 404
recovering, 391
resizing, 388–390
sets. See volume sets
size specification, 380, 408
statuses of, table of,
406–407
troubleshooting, 406–407
unmounted, 381
viewing information on, 404–405
VPNs (virtual private networks)
privileges, 333–335
protocols for, 538
VSS (Volume Shadow Copy Service), 501

W
waking on timed events, 7
warning events, 109
warning messages, 519
Wbadmin
backup information, listing, 508
compared to other backup tools, 501–502
configuring scheduled backups, 514
creating manual backups, 515–516
deleting system state backups, 508
disabling scheduled runs, 508
disks, listing available, 508
enable backup command, 507, 509, 514
listing available commands for, 506
modifying scheduled backups, 515
start backup command, 515–516
starting, 506
starting one-time backups, 509
starting recoveries, 509
stopping jobs, 509
syntax of, 506
system state backups, 522–523
table of commands, 507
Task Scheduler with, 516–517
WCF (Windows Communication Foundation) Activation Components, 37
WDS (Windows Deployment Services), 35
Web edition. See Windows Web Server 2008 R2
Web Server (IIS) role, 35
Wecutil.exe, 43
WER (Windows Error Reporting), 42, 73
Wevtutil.exe, 43
WIM (Windows Imaging Format), 2
Windows 7
differences from R2, 2
features shared with R2, 1–2
joining computers to domains, 250–251
Windows 95 and 98, 250–251
Windows 2000, 250–251
Windows Biometric Framework, 38
Windows Boot Manager
implications for resizing volumes, 388
Startup And Recovery dialog box, configuring from, 86–87
Windows command shell
CMD command for launching during Setup, 49
Windows PowerShell 2.0, opening from, 25
Windows components, administrative templates for, 150
Windows Defender, 134–135
Windows Deployment Services (WDS), 35
Windows Domain Manager, 240
Windows Error Recovery mode, 522
Windows Error Reporting (WER), 42, 73
Windows Experience Index scores, 2
Windows Explorer
  Check Disk, running from, 392
  file and folder object management, 466
  object inheritance, setting, 468
  object ownership, editing, 467
  Public folder access, 442–443
  setting permissions for files and folders, 471–473
Windows File Protection, 88
Windows Firewall
  advanced firewall option, 135
  backup and recovery exceptions, 510
  opening for configuration, 70
  remote management, settings for, 74–75, 238
  Server Manager, launching from, 72
  user rights assignment blocked issue, 308–309
Windows Imaging Format (WIM), 2
Windows Installer Packages, 181
Windows Internal Database, 39
Windows Logon, 41–42
Windows Memory Diagnostics, 44, 520, 524
Windows Network Diagnostics, 537
Windows NT, 250–251
Windows PE (Preinstallation Environment) 3.0, 2
Windows PowerShell 2.0
  Active Directory module for, 214, 241–242
  authentication, 27–30
  cmdlets, 25–26, 241–242
  configuring, 27–30
  deleted object recovery with, 235–236
  installing graphical environment for, 25
  listing cmdlets, 241–242
  logs of events, 108
  opening, 25
  Powershell.exe, 25
  remote computers, working with, 75–76
remote management, requirement for, 74
roles and services, viewing with, 57
Run As Administrator remoting requirement, 28
Sconfig, installing with, 41
scripts, 176
ServerManager module, 57
windows for, opening, 41
WinRM for, 26–30
Winrm quickconfig command, 43
Windows Preboot Environment, 2
Windows Process Activation Services, 39
Windows Remote Management. See WinRM (Windows Remote Management)
Windows Script Host (WSH), 176
Windows Search Service, 359, 362
Windows Server 2000, 139, 213
Windows Server 2003 domain functional level of, 216, 222–224
File Services, 359
forest functional level, 218
Group Policy compatibility issues, 139
joining computers to domains, 250–251
R2 Active Directory install issues, 213
Windows Server 2008 domain functional level of, 216, 222–224
forest functional level, 218
joining computers to domains, 250–251
Windows Server Backup advantages of, 502
application data, 504, 510
application restores, 526–528
automatic disk management feature, 502
Bare Metal Recovery option, 512
compared to other backup tools, 501–502
configuring performance settings, 505
configuring scheduled backups, 511–514
core installations, limitations, 502
destination options, 513, 518
differential backups not available in, 501
DVD backup limitations, 501–502
features, 39
file and folder restores, 526–528
installing, 502–503
limitations of, 504
manual backups, 517–518
media for backups, 501–502
Microsoft Exchange Server with, 503
modifying scheduled backups, 514
no backup warnings, 503
noncritical volume backups, 511
Ntbackup.exe recoveries, 503
operating system only (critical) backups, 511
recommended for file servers, 358
Recovery Wizard, 526–528
remote computers, connecting to, 504
rights and permissions for, 504
system state data, 504
tape backups not available, 502
VSS basis of, 501
Windows Server Migration tools, 47
Windows Server security model, 275–277
Windows Server Update Services (WSUS), 187
Windows Software Licensing Management tool Simg commands, 42
Windows System Resource Manager (WSRM), 39
Windows TIFF IFilter, 39
Windows Time, 135
Windows Update configuring Automatic Updates from, 134
not enabled by default, 69
Server Manager, launching from, 72
Windows Vista
joining computers to domains, 250–251
policy editors for computers, 140
Windows Web Server 2008 R2 Active Directory issues, 6
features for, 4–5
Windows XP
  connecting to network printers, 563–564
  joining computers to domains, 250–251
  profiles and logons issues, 338
WinRM

WinRM (Windows Remote Management)
Administrative Center, required for, 16
authentication, 27–30
configuring, 27–30
IIS Extension, 39
listener configuration, 29
PowerShell with, 26–30
quickconfig command, 43
remote management, required for, 74
WINS (Windows Internet Name Service)
configuring name service with, 21–22
WINS Server service, 39
Wireless LAN Service, 39
WMI filters, linking to GPOs, 162

Wmic commands, 43
workgroups
defined, 6
joining computers to,
250–253
joining computers to with
System Properties, 78
Write permission, 469
writes, I/O
counters for, 131
processes, viewing in Task
Manager, 92
WSH (Windows Script Host),
176, 231
WS-Management
requirement for remote
server management, 26
Winrm quickconfig com-
mand, 43

WSRM (Windows System Resource Manager), 39, 135
WSUS (Windows Server Update Services), 187
Wusa.exe Patchname.msu
command, 43

X
x64 architecture, 4
X.500 directory services, 277
XPS Viewer, 39

Z
ZAP (ZAW Down-Level Application Packages) files, 181
zones, DNS, 632–634, 639–641
WILLIAM R. STANEK (williamstanek.com) has more than 20 years of hands-on experience with advanced programming and development. He is a leading technology expert, an award-winning author, and a pretty-darn-good instructional trainer. Over the years, his practical advice has helped millions of programmers, developers, and network engineers all over the world. He has written more than 100 books. Current books include *Active Directory Administrator's Pocket Consultant*, *Windows Group Policy Administrator's Pocket Consultant*, *Windows 7 Administrator's Pocket Consultant*, and *Windows Server 2008 Inside Out*.

William has been involved in the commercial Internet community since 1991. His core business and technology experience comes from more than 11 years of military service. He has substantial experience in developing server technology, encryption, and Internet solutions. He has written many technical white papers and training courses on a wide variety of topics. He frequently serves as a subject matter expert and consultant.

William has a BS in computer science, magna cum laude, and an MS with distinction in information systems. He is proud to have served in the Persian Gulf War as a combat crewmember on an electronic warfare aircraft. He flew on numerous combat missions into Iraq and was awarded nine medals for his wartime service, including one of the United States of America’s highest flying honors, the Air Force Distinguished Flying Cross. Currently, he resides in the Pacific Northwest with his wife and children.

William recently rediscovered his love of the great outdoors. When he’s not writing, teaching, or making presentations, he can be found hiking, biking, backpacking, traveling, or trekking in search of adventure.

Follow William on Twitter at twitter.com/WilliamStanek.