Dedication

Dedicated with gratitude to the editorial team that in the process of the Long March toward publication first encouraged, then cajoled, then exhorted, and finally in the last stages, half-dragged us across the finish line: Karen Szall, Martin DelRe, Mitch Tulloch, and Roger LeBlanc.

Woodrow Wilson said, "I not only use all the brains that I have, but all that I can borrow." We had the great good luck to borrow some of the best.
Contents at a Glance

Part I
Preparation
1 Overview of Windows Server 2003 .................................................. 3
2 Introducing Directory Services ...................................................... 17
3 Planning Namespace and Domains .............................................. 29
4 Planning Deployment ................................................................. 43

Part II
Installation and Configuration
5 Getting Started ................................................................. 55
6 Upgrading to Windows Server 2003 ........................................... 105
7 Configuring a New Installation ................................................. 159
8 Installing and Managing Printers .............................................. 187
9 Managing Users and Groups .................................................... 227
10 Managing File Resources ....................................................... 267
11 Administering Group Policy .................................................... 295

Part III
Network Administration
12 Managing Daily Operations ..................................................... 323
13 Using Scripts for Consistent Administration ............................... 351
14 Installing and Configuring Active Directory .............................. 377
15 Managing Active Directory ..................................................... 433
16 Understanding TCP/IP ........................................................... 469
17 Administering TCP/IP ........................................................... 495
18 Implementing Disk Management .............................................. 539
19 Using Clusters ................................................................. 575
20 Managing Storage ............................................................... 613
Part IV
Security
21 Planning for Security ........................................ 703
22 Implementing Security ........................................ 733
23 Patch Management ........................................... 783
24 Using Microsoft Certificate Services ....................... 797
25 Connection Services .......................................... 829
26 Implementing Wireless Security .................. 865

Part V
Support Services and Features
27 Interoperability .............................................. 879
28 Managing Software ........................................ 901
29 Application Compatibility and Virtual Server ........... 955
30 Deploying Terminal Services ................................ 981
31 Using the Indexing Service ................................ 1009

Part VI
Internet Servers and Services
32 Basics of Internet Information Services ........... 1037
33 Advanced Internet Information Services ............... 1069
34 Internet Security and Acceleration Server 2004 .... 1123

Part VII
Tuning, Maintenance, and Repair
35 Performance Monitoring and Tuning ........... 1157
36 Disaster Planning ............................................ 1203
37 Using Backup ................................................. 1221
38 Planning Fault Tolerance and Avoidance .......... 1249
39 Using the Registry ........................................... 1265
40 Troubleshooting and Recovery .................. 1293
Part VIII

Appendixes

A  Interface Changes from Windows 2000 Server.................1331
B  Interface Changes from Windows NT 4 .........................1337
C  Optional Components..............................................1345
D  Using the Microsoft Windows Server 2003 Recovery Console.1353
E  Using the Microsoft Windows Server 2003 Support Tools.....1357
# Table of Contents

_Acknowledgments_ ................................................................. xliii
*Introduction_* ................................................................. xliv
_System Requirements_* .......................................................... li

Part I
_Preparation_

1 **Overview of Windows Server 2003** .............................. 3
   Versions of Windows Server 2003 ........................................ 4
   Deploying Windows Server 2003 and Windows Clients .......... 5
   Network Management ...................................................... 6
      Printer Management ................................................. 7
   Group Policy .............................................................. 7
   IntelliMirror ............................................................... 8
   Terminal Services ......................................................... 8
   Interoperability ........................................................... 9
   System and Network Security ......................................... 9
   Availability and Reliability .......................................... 11
   Active Directory ......................................................... 11
   Storage and File System Support .................................. 13
   Communications ........................................................ 13
   Internet Services and .NET Application Services ............ 14
   Scalability ................................................................. 14
   The Need for Planning ............................................... 15
   Summary ................................................................. 16

2 **Introducing Directory Services** ................................. 17
   Understanding Directory Services .................................. 17
   Active Directory in Microsoft Windows Server 2003 .......... 19
      Terminology and Concepts in Active Directory .......... 20

---

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

Microsoft is interested in hearing your feedback about this publication so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit: [www.microsoft.com/learning/booksurvey/](http://www.microsoft.com/learning/booksurvey/)
# Table of Contents

The Active Directory Architecture ........................................... 23
  The Directory System Agent .................................................. 23
  Naming Formats ...................................................................... 24
  The Data Model ...................................................................... 24
  Schema Implementation ......................................................... 25
  The Security Model ............................................................... 25
  Delegation and Inheritance ..................................................... 26
  Naming Contexts and Partitions ................................................. 26
  The Global Catalog ............................................................... 26

Summary ................................................................................. 27

## 3 Planning Namespace and Domains ........................................ 29

  Analyzing Naming Convention Needs ........................................ 29
    Trees and Forests ............................................................... 29
    Defining a Naming Convention ............................................. 31
    Determining Name Resolution ............................................... 34
  Planning a Domain Structure .................................................... 36
    Domains vs. Organizational Units ......................................... 36
    Designing a Domain Structure ............................................... 38
    Domain Security Guidelines ................................................. 39
    Creating Organizational Units .............................................. 40
  Planning Multiple Domains ...................................................... 40
    Planning a Contiguous Namespace ....................................... 41
    Determining the Need for a Multi-Tree Forest ....................... 41
    Creating the Forest ............................................................ 41

Summary ................................................................................. 42

## 4 Planning Deployment .......................................................... 43

  How Information Technology Functions .................................... 44
  Identifying Business Needs ..................................................... 45
    Getting Specific ............................................................... 45
    Seeing into the Future ......................................................... 46
  Assessing Current Systems ..................................................... 46
    Documenting the Network .................................................... 46
  Making a Roadmap ............................................................... 49
    Defining Goals .................................................................... 50
    Assessing Risk .................................................................... 50

Summary ................................................................................. 52
### Part II

**Installation and Configuration**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5  Getting Started</td>
<td>55</td>
</tr>
<tr>
<td>Designing a Deployment Environment</td>
<td>55</td>
</tr>
<tr>
<td>Choosing an Installation Method</td>
<td>57</td>
</tr>
<tr>
<td>Choosing a Preinstallation Environment</td>
<td>61</td>
</tr>
<tr>
<td>Choosing a Software Update Solution</td>
<td>61</td>
</tr>
<tr>
<td>Choosing an Application Deployment Solution</td>
<td>62</td>
</tr>
<tr>
<td>Understanding Licensing and Product Activation</td>
<td>63</td>
</tr>
<tr>
<td>Designing a Test Lab</td>
<td>65</td>
</tr>
<tr>
<td>Planning Server Configurations</td>
<td>66</td>
</tr>
<tr>
<td>Creating Your Deployment Plan</td>
<td>71</td>
</tr>
<tr>
<td>Creating Your Deployment Environment</td>
<td>72</td>
</tr>
<tr>
<td>Using Setup Manager</td>
<td>72</td>
</tr>
<tr>
<td>Using Unattended Setup with Windows Server 2003 R2</td>
<td>78</td>
</tr>
<tr>
<td>Creating and Modifying a Distribution Share</td>
<td>80</td>
</tr>
<tr>
<td>Using Sysprep with Disk Imaging</td>
<td>89</td>
</tr>
<tr>
<td>Installing Windows</td>
<td>91</td>
</tr>
<tr>
<td>Preparing the System</td>
<td>91</td>
</tr>
<tr>
<td>Performing a Manual Installation of Windows</td>
<td>91</td>
</tr>
<tr>
<td>Initiating Windows Setup Using an Answer File</td>
<td>94</td>
</tr>
<tr>
<td>Initiating Setup Using Command-Line Parameters</td>
<td>95</td>
</tr>
<tr>
<td>Troubleshooting Installations</td>
<td>98</td>
</tr>
<tr>
<td>Setup Freezes or Locks Up</td>
<td>99</td>
</tr>
<tr>
<td>Setup Stops During File Copying</td>
<td>100</td>
</tr>
<tr>
<td>Previous Operating System Will Not Boot</td>
<td>101</td>
</tr>
<tr>
<td>Summary</td>
<td>103</td>
</tr>
</tbody>
</table>

| 6  Upgrading to Windows Server 2003                                     | 105  |
| Architectural Changes Since Windows NT 4.0                             | 106  |
| Domain Controllers and Server Roles                                    | 106  |
| Active Directory                                                       | 107  |
| Hardware Support                                                        | 112  |
| Software Support                                                        | 113  |
Planning a Windows NT Domain Upgrade ................................. 114
Choosing Whether to Upgrade or Migrate ............................. 114
Documenting the Existing Network ......................................... 116
Planning the Active Directory Forest ....................................... 121
Making a Recovery Plan ...................................................... 131
Developing an Upgrade Strategy ........................................... 133
Preparing Domains and Computers ........................................ 137
Reviewing Server Upgrade Requirements ................................. 137
Preparing Windows NT Domains .......................................... 138
Preparing the Computers .................................................... 138
Updating the Active Directory Schema .................................... 140
Testing Active Directory Functionality in Active Directory Domains 140
Updating the Active Directory Forest Schema .......................... 141
Verifying the Forest Schema Update ....................................... 143
Updating the Active Directory Domain Schema ....................... 145
Upgrading Clients to Windows XP ......................................... 147
Upgrading Servers to the Windows Server 2003 Family ............... 149
Installing Windows Server 2003 R2 ...................................... 149
Upgrading a Server to Windows Server 2003 ........................... 150
Switching Forest and Domain Functional Levels ....................... 151
Choosing a Forest Functional Level ...................................... 151
Choosing a Domain Functional Level .................................... 154
Switching Functional Levels ............................................... 157
Summary .............................................................................. 158

7  Configuring a New Installation ........................................ 159
Installing Updates .............................................................. 159
Enabling Remote Administration ............................................ 162
Checking for Setup Problems .............................................. 164
Configuring Devices ........................................................... 164
Using Device Manager ........................................................ 165
Configuring Storage ............................................................ 168
Configuring Networking Settings .......................................... 169
Changing Your Network Identity ............................................ 169
Configuring Network Components ........................................ 170
Configuring TCP/IP ............................................................. 171
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting Up Server Roles</td>
<td></td>
<td>178</td>
</tr>
<tr>
<td>Securing Windows</td>
<td></td>
<td>184</td>
</tr>
<tr>
<td>Summary</td>
<td></td>
<td>185</td>
</tr>
<tr>
<td><strong>8 Installing and Managing Printers</strong></td>
<td></td>
<td>187</td>
</tr>
<tr>
<td>Planning Printer Deployment</td>
<td></td>
<td>187</td>
</tr>
<tr>
<td>Establishing Printer Naming Conventions</td>
<td></td>
<td>188</td>
</tr>
<tr>
<td>Creating Location-Naming Conventions</td>
<td></td>
<td>188</td>
</tr>
<tr>
<td>Enabling Printer Location Tracking</td>
<td></td>
<td>191</td>
</tr>
<tr>
<td>Choosing Whether to Upgrade or Migrate Print Servers</td>
<td></td>
<td>192</td>
</tr>
<tr>
<td>Installing Printers</td>
<td></td>
<td>195</td>
</tr>
<tr>
<td>Managing Printers and Print Servers</td>
<td></td>
<td>199</td>
</tr>
<tr>
<td>Using the Print Management Console</td>
<td></td>
<td>199</td>
</tr>
<tr>
<td>Managing Print Jobs from Windows</td>
<td></td>
<td>204</td>
</tr>
<tr>
<td>Managing Printers from a Web Browser</td>
<td></td>
<td>206</td>
</tr>
<tr>
<td>Managing Printers from a Command Line</td>
<td></td>
<td>207</td>
</tr>
<tr>
<td>Changing Printer Options</td>
<td></td>
<td>208</td>
</tr>
<tr>
<td>Setting Security Options</td>
<td></td>
<td>208</td>
</tr>
<tr>
<td>Changing Printer Availability and Group Priorities</td>
<td></td>
<td>209</td>
</tr>
<tr>
<td>Specifying a Separator Page</td>
<td></td>
<td>210</td>
</tr>
<tr>
<td>Changing Spool Settings</td>
<td></td>
<td>212</td>
</tr>
<tr>
<td>Managing Printer Drivers</td>
<td></td>
<td>214</td>
</tr>
<tr>
<td>Managing Printer Drivers</td>
<td></td>
<td>215</td>
</tr>
<tr>
<td>Creating Printer Pools and Changing Port Settings</td>
<td></td>
<td>216</td>
</tr>
<tr>
<td>Printer Maintenance and Troubleshooting</td>
<td></td>
<td>217</td>
</tr>
<tr>
<td>Optimizing Print Server Performance</td>
<td></td>
<td>218</td>
</tr>
<tr>
<td>Preparing for Print Server Failure</td>
<td></td>
<td>218</td>
</tr>
<tr>
<td>Printing from the Client Machine Experiencing the Problem</td>
<td></td>
<td>219</td>
</tr>
<tr>
<td>Checking the Print Server Status</td>
<td></td>
<td>224</td>
</tr>
<tr>
<td>Checking the Printer</td>
<td></td>
<td>224</td>
</tr>
<tr>
<td>Deleting Stuck Documents</td>
<td></td>
<td>225</td>
</tr>
<tr>
<td>Troubleshooting Printer Location Tracking</td>
<td></td>
<td>225</td>
</tr>
<tr>
<td>Summary</td>
<td></td>
<td>226</td>
</tr>
</tbody>
</table>
Table of Contents

9 Managing Users and Groups .............................................. 227
  Understanding Groups ..................................................... 227
  Assigning Group Scopes .................................................. 228
  Planning Organizational Units ......................................... 230
    Creating Organizational Units ....................................... 231
    Moving Organizational Units ....................................... 232
    Deleting Organizational Units ..................................... 232
  Planning a Group Strategy .............................................. 232
    Determining Group Names ............................................ 233
    Using Global and Domain Local Groups ............................ 233
    Using Universal Groups .............................................. 233
  Implementing the Group Strategy ..................................... 234
    Creating Groups ....................................................... 234
    Deleting Groups ...................................................... 235
    Adding Users to a Group ............................................. 235
  Managing Built-In Groups and User Rights ......................... 237
    Built-In Local Groups ................................................ 237
    Built-In Domain Local Groups ...................................... 239
    Built-In Global Groups .............................................. 241
    Defining User Rights ................................................ 242
  Creating User Accounts ................................................ 247
    Naming User Accounts ............................................... 247
    Account Options ....................................................... 248
    Passwords .............................................................. 249
    Creating a Domain User Account ................................... 250
    Creating a Local User Account ..................................... 251
    Setting User Account Properties ................................... 251
    Testing User Accounts ............................................... 252
  Managing User Accounts ............................................... 253
    Finding a User Account ............................................... 253
    Disabling and Enabling a User Account ........................... 254
    Deleting a User Account ............................................. 255
    Moving a User Account ............................................... 255
    Renaming a User Account ............................................ 256
    Resetting a User’s Password ........................................ 256
    Unlocking a User Account ............................................ 257
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using Home Folders</td>
<td>257</td>
</tr>
<tr>
<td>Creating Home Folders on a Server</td>
<td>257</td>
</tr>
<tr>
<td>Providing Home Folders to Users</td>
<td>258</td>
</tr>
<tr>
<td>Maintaining User Profiles</td>
<td>259</td>
</tr>
<tr>
<td>Local Profiles</td>
<td>261</td>
</tr>
<tr>
<td>Roaming Profiles</td>
<td>261</td>
</tr>
<tr>
<td>Assigning a Logon Script to a User Profile</td>
<td>264</td>
</tr>
<tr>
<td>Summary</td>
<td>265</td>
</tr>
<tr>
<td><strong>10 Managing File Resources</strong></td>
<td>267</td>
</tr>
<tr>
<td>Sharing File Resources</td>
<td>267</td>
</tr>
<tr>
<td>Shared Folders</td>
<td>268</td>
</tr>
<tr>
<td>NFS Shared Folders</td>
<td>268</td>
</tr>
<tr>
<td>Active Directory Shared Folders</td>
<td>268</td>
</tr>
<tr>
<td>DFS Folders</td>
<td>268</td>
</tr>
<tr>
<td>Share Permissions vs. File Permissions</td>
<td>268</td>
</tr>
<tr>
<td>Share Permissions</td>
<td>269</td>
</tr>
<tr>
<td>File Permissions</td>
<td>269</td>
</tr>
<tr>
<td>NTFS Permissions</td>
<td>270</td>
</tr>
<tr>
<td>What Permissions Mean</td>
<td>270</td>
</tr>
<tr>
<td>How Permissions Work</td>
<td>271</td>
</tr>
<tr>
<td>Considering Inheritance</td>
<td>272</td>
</tr>
<tr>
<td>Configuring Folder Permissions</td>
<td>273</td>
</tr>
<tr>
<td>Assigning Permissions to Files</td>
<td>274</td>
</tr>
<tr>
<td>Configuring Special Permissions</td>
<td>274</td>
</tr>
<tr>
<td>Ownership and How It Works</td>
<td>276</td>
</tr>
<tr>
<td>Shared Folders</td>
<td>279</td>
</tr>
<tr>
<td>Using the File Server Management Snap-In</td>
<td>279</td>
</tr>
<tr>
<td>Creating a Shared Folder</td>
<td>281</td>
</tr>
<tr>
<td>Removing a Folder Share</td>
<td>284</td>
</tr>
<tr>
<td>Disconnecting Users</td>
<td>284</td>
</tr>
<tr>
<td>Limiting Simultaneous Connections</td>
<td>284</td>
</tr>
<tr>
<td>Special Shares</td>
<td>285</td>
</tr>
<tr>
<td>The Command Line—Net Share</td>
<td>287</td>
</tr>
</tbody>
</table>
# Table of Contents

NFS Shared Folders ................................................................. 288  
  Initial Configuration ......................................................... 288  
  Creating an NFS Share ..................................................... 290  
  Deleting or Modifying an NFS Share ................................. 292  
  Publishing Shares in Active Directory ......................... 292  
  Summary ................................................................. 293  

11 Administering Group Policy ............................................. 295  
  Components of Group Policy ........................................... 296  
    Group Policy Objects .................................................. 296  
    Default Group Policies ............................................. 298  
  Managing Group Policies .............................................. 298  
    Order of Implementation .......................................... 301  
    Order of Inheritance .............................................. 301  
    Overriding Inheritance .......................................... 302  
  Creating a Group Policy Object .................................. 303  
    Creating a GPO in GPMC ......................................... 304  
    Creating a GPO on a Computer Without GPMC ........... 304  
    Inside the Group Policy Object Editor ..................... 304  
  Managing Group Policy Links ....................................... 305  
    Linking a GPO Using GPMC .................................. 306  
    Linking a GPO Without GPMC .................................. 306  
  Setting the Scope of Group Policy Objects .................... 306  
    Using GPMC to Set the Scope for a GPO ..................... 307  
    Setting the GPO Scope Without GPMC ......................... 308  
  Delegating Permissions on GPOs .................................. 308  
    Delegating Group Policy Using GPMC ......................... 309  
    Delegating Group Policy Without GPMC ...................... 310  
    Disabling a Branch of a GPO .................................. 311  
  Refreshing Group Policy ............................................... 311  
  Backing Up a Group Policy Object ................................ 312  
  Restoring a Group Policy Object ................................ 313  
  Using Group Policy for Folder Redirection .................... 313
Part III

Network Administration

12 Managing Daily Operations ......................... 323
   Using the Microsoft Management Console ........... 323
      Convenience Consoles ......................... 324
      Creating an MMC-Based Console with Snap-Ins .. 324
   Using the Secondary Logon ........................ 331
      Opening Programs Using Run As ................. 332
      Making Shortcuts to Run As .................... 333
      Using Runas for Printers or Control Panel ..... 333
   Administrative Tools .............................. 334
      Installing Administrative Tools Locally ......... 334
      Making Administrative Tools Available Remotely 335
   Support Tools .................................. 335
   Automating Chores with Scripts .................... 335
   Auditing Events .................................. 336
      Audit Settings for Objects ...................... 338
      Viewing Event Logs ............................. 339
      Searching Event Logs ........................... 340
      Filtering Event Logs ............................ 341
      Setting the Size of Event Logs ................. 341
      Archiving Event Logs ........................... 342
   Delegating Control ................................ 343
   Using Task Scheduler .............................. 344
      Changing a Schedule ............................ 345
      Tracking Task Scheduler ......................... 346
      Viewing Tasks on a Remote Computer ............. 347
Using the AT Command ......................................................... 347
Using cron ........................................................................ 348
Summary ............................................................................ 349

13 Using Scripts for Consistent Administration .................. 351
Scripting on Windows Server 2003 ................................... 352
   Windows Server 2003 Scripting Infrastructure .................. 352
   Extending the Infrastructure ........................................... 354
   What’s New in Windows Server 2003 Scripting ................. 355
Scripting Practices ............................................................. 357
   Think from the Command Prompt ................................. 357
   Write WSH Scripts as Console Tools ............................... 357
   Credentials and Scripting ............................................. 362
   Path Management Practices ....................................... 363
   Input and Output Handling ......................................... 366
   Use Good Error Management ...................................... 367
   WMI Scripting Issues .................................................... 370
   Translating Script Languages ...................................... 371
   Noninteractive Scripts: Remote and Scheduled Use ......... 373
The Future of Windows Scripting ...................................... 373
Summary ............................................................................ 376

14 Installing and Configuring Active Directory .................... 377
Using the Active Directory Installation Wizard .................. 378
   Preparing for Installation ............................................ 379
   Promoting Your First Server to a Domain Controller ....... 381
   Choosing Installation Options .................................... 386
   Upgrading Windows NT 4 Domain Controllers ............... 391
   Demoting a Domain Controller ................................... 392
   Changing a Domain Controller Identification ................ 394
   Setting a Global Catalog Server .................................. 394
Using Active Directory Domains and Trusts ...................... 395
   Launching Active Directory Domains and Trusts .......... 395
   Domain and Forest Functionality ................................. 396
   Managing Domain Trust Relationships ....................... 400
   Specifying the Domain Manager ................................. 402
   Configuring User Principal Name Suffixes for a Forest .... 402
   Managing Domains ...................................................... 403
15 Managing Active Directory

Using Active Directory Sites and Services ................................................. 433
    Defining Site Objects ......................................................................... 434
    Understanding Domain Replication ................................................. 436
    Launching Sites and Services ......................................................... 438
Using Active Directory Schema .............................................................. 445
    Examining Schema Security ............................................................ 445
    Launching Active Directory Schema ................................................ 446
    Modifying the Schema ..................................................................... 448
    Modifying Display Specifiers .......................................................... 454
    Performing Batch Importing and Exporting .................................... 457
Using the Ldifde.exe Utility ................................................................. 458
    Understanding Operations Master Roles .......................................... 460
Summary .............................................................................................. 467
16 Understanding TCP/IP ................................................. 469
   The TCP/IP Protocol Suite ........................................ 469
   Internet Protocol .................................................. 470
   Transmission Control Protocol ................................. 470
   User Datagram Protocol ......................................... 471
   Windows Sockets ................................................... 471
   NetBIOS .............................................................. 472
   Requests for Comments ............................................ 472
   IP Addresses and What They Mean. ......................... 474
      Class A Networks ............................................ 474
      Class B Networks ............................................ 475
      Class C Networks ........................................... 475
      Class D and Class E Addresses ........................... 476
   Routers and Subnets .............................................. 477
      What Is a Subnet? ............................................. 477
      Gateways and Routers ....................................... 479
   Address Resolution and Routing Protocols ................ 480
   Name Resolution .................................................. 481
      The Domain Name System ................................ 481
      Dynamic Host Configuration Protocol ................. 487
      Windows Internet Name Service ....................... 489
   IP Version 6 ....................................................... 492
   Summary ............................................................ 494

17 Administering TCP/IP ............................................. 495
   Using DHCP ......................................................... 496
      Designing DHCP Networks ................................ 496
      Installing the DHCP Service ........................... 498
      Creating a New Scope ..................................... 499
      Authorizing the DHCP Server and Activating Scopes ... 503
      Adding Address Reservations ........................... 504
      Enabling Dynamic Updates to a DNS Server for Earlier Clients .... 505
      Using Multiple DHCP Servers for Redundancy ........... 507
      Other DHCP Functions .................................... 510
Setting Up a DHCP Relay Agent .............................................. 511
Backing Up and Restoring the DHCP Database ...................... 513
Using Ipconfig to Release, Renew, or Verify a Lease .............. 514
DHCP Command-Line Administration ..................................... 514
Using DNS Server .................................................................. 515
Installing DNS ....................................................................... 515
Using the Configure A DNS Server Wizard ............................. 516
Creating Zones ................................................................. 521
Creating Subdomains and Delegating Authority ...................... 522
Adding Resource Records .................................................... 524
Configuring Zone Transfers .................................................. 527
Interoperating with Other DNS Servers ................................. 528
Enabling WINS Resolution ................................................... 529
Setting Up a Forwarder ....................................................... 529
Updating Root Hints ............................................................ 531
Setting Up a Caching-Only DNS Server ................................. 531
Setting Up a WINS Server .................................................... 532
Determining Whether You Need WINS ................................. 532
Configuring the Server to Prepare for WINS ......................... 533
Installing WINS ................................................................. 533
Adding Replication Partners ................................................ 534
Miscellaneous WINS Functions ........................................... 536
Compacting the WINS Database ........................................... 537
Summary ............................................................................. 537

18 Implementing Disk Management ........................................ 539
Understanding Disk Terminology ......................................... 539
Overview of Disk Management ............................................. 542
Disk Administration Enhancements ....................................... 543
Remote Management .......................................................... 545
Dynamic Disks ..................................................................... 545
Command Line ................................................................. 545
<table>
<thead>
<tr>
<th>Disk Management Tasks</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding a Partition or Volume</td>
<td>546</td>
</tr>
<tr>
<td>Converting a Disk to a Dynamic Disk</td>
<td>558</td>
</tr>
<tr>
<td>Extending a Volume</td>
<td>559</td>
</tr>
<tr>
<td>Adding a Mirror</td>
<td>561</td>
</tr>
<tr>
<td>Converting a Volume or Partition from FAT to NTFS</td>
<td>566</td>
</tr>
<tr>
<td>Formatting a Partition or Volume</td>
<td>566</td>
</tr>
<tr>
<td>Changing a Drive Letter</td>
<td>569</td>
</tr>
<tr>
<td>Mounting a Volume</td>
<td>570</td>
</tr>
<tr>
<td>NTFS</td>
<td>571</td>
</tr>
<tr>
<td>Encrypting on the File System Level</td>
<td>571</td>
</tr>
<tr>
<td>Disk Quotas, File Screening, and Shadow Copies</td>
<td>574</td>
</tr>
<tr>
<td>Summary</td>
<td>574</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>19 Using Clusters</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What Is a Cluster?</td>
<td>575</td>
</tr>
<tr>
<td>Network Load Balancing Clusters</td>
<td>576</td>
</tr>
<tr>
<td>Server Clusters</td>
<td>576</td>
</tr>
<tr>
<td>Cluster Scenarios</td>
<td>577</td>
</tr>
<tr>
<td>Intranet or Internet Functionality</td>
<td>577</td>
</tr>
<tr>
<td>Terminal Services</td>
<td>578</td>
</tr>
<tr>
<td>Mission-Critical Availability</td>
<td>578</td>
</tr>
<tr>
<td>Requirements and Planning</td>
<td>579</td>
</tr>
<tr>
<td>Identifying and Addressing Goals</td>
<td>579</td>
</tr>
<tr>
<td>Identifying a Solution</td>
<td>579</td>
</tr>
<tr>
<td>Identifying and Addressing Risks</td>
<td>580</td>
</tr>
<tr>
<td>Making Checklists</td>
<td>580</td>
</tr>
<tr>
<td>Network Load Balancing Clusters</td>
<td>580</td>
</tr>
<tr>
<td>NLB Concepts</td>
<td>581</td>
</tr>
<tr>
<td>Choosing an NLB Cluster Model</td>
<td>582</td>
</tr>
<tr>
<td>Creating an NLB Cluster</td>
<td>583</td>
</tr>
<tr>
<td>Planning the Capacity of an NLB Cluster</td>
<td>588</td>
</tr>
<tr>
<td>Providing Fault Tolerance</td>
<td>589</td>
</tr>
<tr>
<td>Optimizing an NLB Cluster</td>
<td>589</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Server Clusters</td>
<td>590</td>
</tr>
<tr>
<td>Server Cluster Concepts</td>
<td>590</td>
</tr>
<tr>
<td>Types of Resources</td>
<td>592</td>
</tr>
<tr>
<td>Defining Failover and Failback</td>
<td>595</td>
</tr>
<tr>
<td>Configuring a Server Cluster</td>
<td>595</td>
</tr>
<tr>
<td>Planning the Capacity of a Server Cluster</td>
<td>597</td>
</tr>
<tr>
<td>Creating a Server Cluster</td>
<td>598</td>
</tr>
<tr>
<td>Compute Clusters</td>
<td>611</td>
</tr>
<tr>
<td>Summary</td>
<td>612</td>
</tr>
<tr>
<td><strong>20 Managing Storage</strong></td>
<td>613</td>
</tr>
<tr>
<td>Using File Server Resource Manager</td>
<td>614</td>
</tr>
<tr>
<td>Setting Global Options</td>
<td>614</td>
</tr>
<tr>
<td>Scheduling Storage Reports</td>
<td>615</td>
</tr>
<tr>
<td>Using Quota Management</td>
<td>618</td>
</tr>
<tr>
<td>Screening Files</td>
<td>624</td>
</tr>
<tr>
<td>Using Disk Quotas</td>
<td>630</td>
</tr>
<tr>
<td>Enabling Disk Quotas</td>
<td>631</td>
</tr>
<tr>
<td>Setting Quota Entries for Users</td>
<td>632</td>
</tr>
<tr>
<td>Exporting and Importing Disk Quotas</td>
<td>633</td>
</tr>
<tr>
<td>Creating Quota Reports</td>
<td>634</td>
</tr>
<tr>
<td>Distributed File System</td>
<td>634</td>
</tr>
<tr>
<td>What’s New in DFS for Windows Server 2003 R2</td>
<td>636</td>
</tr>
<tr>
<td>Concepts and Terminology</td>
<td>637</td>
</tr>
<tr>
<td>Requirements</td>
<td>641</td>
</tr>
<tr>
<td>Installing DFS Management and DFS Replication</td>
<td>644</td>
</tr>
<tr>
<td>DFS Namespaces</td>
<td>644</td>
</tr>
<tr>
<td>DFS Replication</td>
<td>652</td>
</tr>
<tr>
<td>Overview of Storage Manager For SANs</td>
<td>663</td>
</tr>
<tr>
<td>Concepts and Terminology</td>
<td>665</td>
</tr>
<tr>
<td>Installing Storage Manager For SANs</td>
<td>668</td>
</tr>
<tr>
<td>Using the Storage Manager For SANs Console</td>
<td>669</td>
</tr>
<tr>
<td>Managing Server Connections</td>
<td>670</td>
</tr>
<tr>
<td>Managing iSCSI Targets</td>
<td>672</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Managing iSCSI Security</td>
<td>673</td>
</tr>
<tr>
<td>Logging On to iSCSI Targets</td>
<td>674</td>
</tr>
<tr>
<td>Creating and Deploying Logical Units (LUNs)</td>
<td>675</td>
</tr>
<tr>
<td>Extending a LUN</td>
<td>676</td>
</tr>
<tr>
<td>Removable Storage</td>
<td>676</td>
</tr>
<tr>
<td>Concepts and Terminology</td>
<td>677</td>
</tr>
<tr>
<td>Use and Management</td>
<td>680</td>
</tr>
<tr>
<td>Remote Storage</td>
<td>686</td>
</tr>
<tr>
<td>Concepts and System Requirements</td>
<td>687</td>
</tr>
<tr>
<td>Setup and Configuration</td>
<td>690</td>
</tr>
<tr>
<td>Data Recovery and Protection</td>
<td>695</td>
</tr>
<tr>
<td>Summary</td>
<td>699</td>
</tr>
</tbody>
</table>

Part IV

Security

21 Planning for Security ................................................. 703

Security Basics .......................................................... 704
  Authentication ......................................................... 704
  Data Protection ........................................................ 707
  Access Control .......................................................... 709
  Auditing ...................................................................... 710
  Nonrepudiation ............................................................ 710

Smart Cards . .................................................................. 710

Public-Key Infrastructures ............................................... 711
  Public-Key Encryption vs. Symmetric-Key Encryption .................. 713
  Public-Key Certificates and Private Keys ............................ 714
  Certificate Authorities ................................................ 715
  Root and Subordinate Certificate Authorities ....................... 715
  Certificate Registration ............................................... 717
  Certificate Directories ................................................ 718
  Certificate Templates .................................................. 719
  Certificate Revocation .................................................. 719
  Certificate Renewal ...................................................... 720
  Full CRLs and Delta CRLs ............................................... 721
Security-Enabled Protocols ................................................. 721
  Secure Multipurpose Internet Mail Extensions .................. 721
  Kerberos Version 5 .................................................... 722
  Windows NT LAN Manager ............................................ 724
  Secure Sockets Layer .................................................. 724
  Internet Protocol Security .......................................... 725
Virtual Private Networks .................................................. 727
  Remote Access VPNs ................................................... 728
  Router-to-Router VPNs ............................................... 729
Windows Rights Management Services ............................... 729
Security Modules ......................................................... 730
  Cryptographic Application Programming Interface ............ 730
  Cryptographic Service Providers .................................. 730
  CAPICOM .............................................................. 731
  Data Protection API .................................................. 731
Summary ................................................................. 731

22 Implementing Security .................................................. 733
  The Security Configuration Wizard ................................. 734
    Installing the Wizard ............................................... 734
    Using the Wizard .................................................. 735
    Deploying the Policy .............................................. 739
Using Templates to Implement Security Policies .................. 739
  Examining Template Policies ....................................... 741
  Using Predefined Templates ....................................... 741
  Defining New Templates ............................................ 744
  Applying Templates ................................................. 745
Using Security Configuration and Analysis ......................... 746
  Opening a Security Database ..................................... 746
  Importing and Exporting Templates ............................... 747
  Analyzing Security and Viewing the Results ..................... 747
  Configuring Security ................................................ 749
Using Windows Firewall ................................................ 750
Enabling Authentication .................................................. 751
  Obtaining Smart Cards and Certificates .......................... 752
  Logging On with Smart Cards ........................................... 753
  Enabling Remote Certificate or Smart Card Authentication ... 754
  Configuring Authentication for a Remote Access Server ........ 757
Implementing Access Control ............................................. 757
  Establishing Ownership ................................................. 758
  Assigning Permissions ................................................. 759
Managing Certificates ..................................................... 760
  Exporting Certificates and Private Keys ............................ 761
  Importing Certificates .................................................. 762
  Requesting Certificates ................................................. 762
  Enabling Certificates for Specific Purposes ...................... 763
Using Internet Protocol Security Policies .............................. 764
  Defining IPSec Policies ................................................ 764
  Using Predefined IPSec Policies ...................................... 765
  Creating an IPSec Policy ................................................ 767
  Editing an IPSec Policy .................................................. 768
  Assigning IPSec Policies ............................................... 772
Securing Local Data ....................................................... 773
  Creating a Recovery Policy ............................................. 773
  Encrypting Files and Folders ......................................... 775
  Decrypting Files and Folders ......................................... 775
  Sharing Encrypted Files and Folders ................................ 776
  Recovering Files ....................................................... 776
Auditing ................................................................. 778
  Establishing an Audit Policy ......................................... 778
  Auditing Access to Objects ............................................ 779
  Viewing the Security Log ............................................... 780
Using Microsoft Baseline Security Analyzer .......................... 781
What to Do When Hacked ............................................... 782
Summary ............................................................... 782
# Table of Contents

## 23 Patch Management .................................................. 783
- Why It's Important .................................................. 784
- The Patching Cycle .................................................. 785
  - Assess ............................................................. 785
  - Identify ............................................................ 786
  - Evaluate and Plan .................................................. 788
  - Deploy ............................................................... 788
  - Repeat ............................................................... 789
- Deployment Testing .................................................... 789
  - Test Network Deployment ......................................... 789
  - Beta User Deployment ............................................. 791
  - Full Deployment .................................................... 791
- Obtaining Updates ...................................................... 791
  - Automatic Updates .................................................. 791
  - Windows Server Update Services ................................. 792
  - Systems Management Server 2003 ............................... 795
- Third-Party Products .................................................. 795
- Summary ............................................................... 796

## 24 Using Microsoft Certificate Services ............................ 797
- More Vocabulary ...................................................... 798
  - Policy Modules ....................................................... 798
  - Exit Modules ........................................................ 798
  - Certificate Publishers .............................................. 798
  - Certificate Templates .............................................. 799
  - Certificate Authority Types ...................................... 801
- Preinstallation .......................................................... 803
  - Understanding Certificate Authority Roles ...................... 803
  - Preparing for Installation ......................................... 804
- Installation and Configuration ...................................... 805
- The Certification Authority Snap-In ................................ 809
  - Managing the Certification Authority Service .................. 810
  - Configuring the CA's Properties .................................. 812
  - Working with Certificate Templates .............................. 815
  - Managing Revocation and Trust ................................... 817
  - Managing Standalone CAs .......................................... 822
# Table of Contents

The Certificates Snap-In ................................. 822
CAs Linked into a Hierarchy ......................... 823
  Requesting a Certificate if Your Root CA Is Online 824
  Requesting a Certificate if Your Root CA Is Offline 824
Command-Line Utilities ............................... 825
  The Certsrv Tool .................................. 825
  The Certreq Tool ................................. 825
  The Certutil Tool ................................ 827
Summary .............................................. 827

## 25 Connection Services ............................... 829

How Dial-Up Remote Access Works ................... 830
Understanding Virtual Private Networks ............. 831
  How VPNs Work .................................... 831
  Components of a VPN .............................. 833
Common Configurations for Remote Access Servers .... 833
Configuring a Server for Dial-Up Clients .......... 834
Configuring a NAT Server ................................ 835
Setting Remote Access Policies ...................... 836
Understanding the Default Policy .................... 837
Choosing an Administrative Model for Remote Access Policies ............................................. 838
  Administering Access by User .................... 838
  Granting Access by User .......................... 840
  Administering Access by Policy for a Mixed-Mode Domain 840
  Granting or Denying Access by Group Membership for a Mixed Domain 841
  Administering Access by Policy for a Native Domain 843
  Granting or Denying Access by Group Membership for a Native Domain 845
Configuring a Remote Access Policy ................. 848
  Specifying Conditions of Remote Access Policies 848
  Configuring Profiles in Remote Access Policies 850
Configuring a Remote Access Server .................. 852
Configuring a Virtual Private Network .............. 853
  Configuring the Internet Connection .............. 853
  Configuring the Remote Access Server as a Router 854
  Configuring PPTP Ports ............................ 854
<table>
<thead>
<tr>
<th>Configuration</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring PPTP Filters</td>
<td>855</td>
</tr>
<tr>
<td>Elements of a Router-to-Router VPN Connection</td>
<td>855</td>
</tr>
<tr>
<td>Adding a Demand-Dial Interface</td>
<td>857</td>
</tr>
<tr>
<td>Setting Up Static Routes and Routing Protocols</td>
<td>858</td>
</tr>
<tr>
<td>Using the Internet Authentication Service</td>
<td>858</td>
</tr>
<tr>
<td>Installing and Configuring IAS</td>
<td>859</td>
</tr>
<tr>
<td>Installing IAS</td>
<td>859</td>
</tr>
<tr>
<td>Configuring IAS</td>
<td>859</td>
</tr>
<tr>
<td>Configuring Clients for IAS</td>
<td>860</td>
</tr>
<tr>
<td>Using RADIUS for Multiple Remote Access Servers</td>
<td>861</td>
</tr>
<tr>
<td>Configuring a Remote Server for RADIUS Authentication</td>
<td>862</td>
</tr>
<tr>
<td>Configuring the Remote Server for RADIUS Accounting</td>
<td>862</td>
</tr>
<tr>
<td>Configuring the IAS Server for RADIUS</td>
<td>863</td>
</tr>
<tr>
<td>Using the RADIUS Proxy</td>
<td>863</td>
</tr>
<tr>
<td>Summary</td>
<td>864</td>
</tr>
</tbody>
</table>

26 Implementing Wireless Security | 865 |

<table>
<thead>
<tr>
<th>Understanding 802.11 Protocols</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>867</td>
</tr>
<tr>
<td>802.11a</td>
<td>867</td>
</tr>
<tr>
<td>802.11b</td>
<td>867</td>
</tr>
<tr>
<td>802.11g</td>
<td>867</td>
</tr>
<tr>
<td>802.11h</td>
<td>868</td>
</tr>
<tr>
<td>802.11i</td>
<td>868</td>
</tr>
<tr>
<td>802.11e</td>
<td>868</td>
</tr>
<tr>
<td>802.11n</td>
<td>868</td>
</tr>
<tr>
<td>Encryption and Authentication</td>
<td>868</td>
</tr>
<tr>
<td>WPA and WPA2</td>
<td>869</td>
</tr>
<tr>
<td>WPA2</td>
<td>870</td>
</tr>
<tr>
<td>Deployment Scenarios</td>
<td>872</td>
</tr>
<tr>
<td>Enterprise Deployment with 802.1X</td>
<td>872</td>
</tr>
<tr>
<td>Small and Medium Business Deployment with WPA</td>
<td>874</td>
</tr>
<tr>
<td>Summary</td>
<td>875</td>
</tr>
</tbody>
</table>
Part V
Support Services and Features

27 Interoperability ......................................................... 879
  UNIX Interoperability ................................................. 879
  Permissions and Security Concepts ................................ 880
  A UNIX File Listing .................................................. 880
  Symbolic Links ....................................................... 882
  Privilege Levels ..................................................... 882
  Basic Connectivity ................................................... 883
  File Systems .......................................................... 885
  Printing ............................................................... 886
  Microsoft Services for NFS .......................................... 887
  UNIX Identity Management Services ............................... 897
  Windows Subsystem for UNIX-Based Applications ............... 897
  Macintosh Interoperability ......................................... 899
  Novell Netware Interoperability .................................... 899
  Summary ............................................................. 900

28 Managing Software ................................................... 901
  Using the Group Policy Software Installation Extension .......... 901
  Finding the Right Mix of Services .................................. 903
    Natively Authored Windows Installer Packages .................. 904
    Zap Files .......................................................... 904
    Repackaged Applications .......................................... 905
  Setting Up the Group Policy Software Installation Extension .... 908
    Creating a Software Distribution Point ........................... 908
    Creating a GPO for Application Deployment ....................... 909
    Configuring the Group Policy Software Installation Extension . 911
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working with Packages</td>
<td>915</td>
</tr>
<tr>
<td>Adding a Package to a Group Policy</td>
<td>915</td>
</tr>
<tr>
<td>Changing Application Properties</td>
<td>917</td>
</tr>
<tr>
<td>Applying Package Upgrades</td>
<td>919</td>
</tr>
<tr>
<td>Applying Package Modifications</td>
<td>920</td>
</tr>
<tr>
<td>Removing and Redeploying Packages</td>
<td>922</td>
</tr>
<tr>
<td>Using Software Restriction Policies</td>
<td>923</td>
</tr>
<tr>
<td>How Software Restriction Policies Work</td>
<td>923</td>
</tr>
<tr>
<td>Creating Software Restriction Policies</td>
<td>924</td>
</tr>
<tr>
<td>Remote Installation Services</td>
<td>926</td>
</tr>
<tr>
<td>How RIS Works</td>
<td>927</td>
</tr>
<tr>
<td>RIS Requirements and System Recommendations</td>
<td>929</td>
</tr>
<tr>
<td>Installing RIS</td>
<td>930</td>
</tr>
<tr>
<td>Administering RIS</td>
<td>932</td>
</tr>
<tr>
<td>Performing User Installations</td>
<td>948</td>
</tr>
<tr>
<td>Summary</td>
<td>953</td>
</tr>
</tbody>
</table>

29 Application Compatibility and Virtual Server | 955

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Server Overview</td>
<td>955</td>
</tr>
<tr>
<td>Installing Virtual Server</td>
<td>956</td>
</tr>
<tr>
<td>Installing Internet Information Services for Virtual Server</td>
<td>956</td>
</tr>
<tr>
<td>Performing the Installation</td>
<td>958</td>
</tr>
<tr>
<td>Configuring Virtual Server</td>
<td>961</td>
</tr>
<tr>
<td>Configuring Virtual Networks</td>
<td>962</td>
</tr>
<tr>
<td>Configuring Server Properties</td>
<td>965</td>
</tr>
<tr>
<td>Creating Virtual Machines</td>
<td>967</td>
</tr>
<tr>
<td>Initial Configuration of a Virtual Machine</td>
<td>968</td>
</tr>
<tr>
<td>Using Virtual Machine Remote Control</td>
<td>974</td>
</tr>
<tr>
<td>Configuring Virtual Machines</td>
<td>975</td>
</tr>
<tr>
<td>Installing Virtual Machine Additions</td>
<td>977</td>
</tr>
<tr>
<td>Administering Virtual Server</td>
<td>978</td>
</tr>
<tr>
<td>Alternatives to Virtual Server</td>
<td>979</td>
</tr>
<tr>
<td>Virtual PC</td>
<td>979</td>
</tr>
<tr>
<td>VMWare</td>
<td>979</td>
</tr>
<tr>
<td>Summary</td>
<td>980</td>
</tr>
</tbody>
</table>
## 30 Deploying Terminal Services ................................. 981

- Concepts .................................................................. 981
- Remote Access ...................................................... 982
- Central Management .............................................. 982
- Requirements ........................................................ 983
  - RAM .................................................................. 983
  - CPU .................................................................. 983
  - Network Utilization ........................................... 984
  - Capacity Planning .............................................. 984
- Installation ............................................................. 985
  - Enabling Remote Desktop for Administration Mode .... 988
  - Installing Programs ............................................ 988
- Administration ....................................................... 992
  - Terminal Services Manager ................................... 992
  - Terminal Services Configuration ............................ 1000
  - Terminal Services Licensing ................................ 1004
  - Installing Terminal Server Licensing ...................... 1005
  - Remote Desktop Client ........................................ 1007
- Summary ............................................................... 1008

## 31 Using the Indexing Service. ................................. 1009

- Understanding the Indexing Service ......................... 1009
  - Defining Terms .................................................. 1010
  - How Indexing Works .......................................... 1011
- Planning Your Indexing Service ............................... 1012
  - Merging Indexes ................................................ 1013
  - Setting Up an Indexing Console ............................ 1014
- Creating and Configuring Catalogs ......................... 1015
  - Creating a Catalog ............................................. 1015
  - Configuring a Catalog ........................................ 1016
  - Including or Excluding a Directory ....................... 1017
  - Configuring the Property Cache ............................ 1019
  - Adding a Property ............................................. 1019
  - Running a Scan of the Index ................................. 1020
- Registry Entries for the Indexing Service .................. 1021
<table>
<thead>
<tr>
<th>Part VI</th>
<th>Internet Servers and Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>Basics of Internet Information Services</td>
</tr>
<tr>
<td>Protocols Supported</td>
<td>1037</td>
</tr>
<tr>
<td>HTTP</td>
<td>1038</td>
</tr>
<tr>
<td>FTP</td>
<td>1040</td>
</tr>
<tr>
<td>SMTP</td>
<td>1041</td>
</tr>
<tr>
<td>NNTP</td>
<td>1043</td>
</tr>
<tr>
<td>Other Protocols</td>
<td>1043</td>
</tr>
<tr>
<td>Administration Tools</td>
<td>1044</td>
</tr>
<tr>
<td>Adding the Application Server Role</td>
<td>1044</td>
</tr>
<tr>
<td>Internet Information Services</td>
<td>1045</td>
</tr>
<tr>
<td>Remote Administration</td>
<td>1046</td>
</tr>
<tr>
<td>Administration Scripts</td>
<td>1047</td>
</tr>
<tr>
<td>The WWW Publishing Service</td>
<td>1047</td>
</tr>
<tr>
<td>The Default Web Site</td>
<td>1047</td>
</tr>
<tr>
<td>Connecting to a Web Site</td>
<td>1048</td>
</tr>
<tr>
<td>Other Web Sites</td>
<td>1049</td>
</tr>
<tr>
<td>Virtual Directories</td>
<td>1053</td>
</tr>
</tbody>
</table>
### Table of Contents

The FTP Publishing Service .................................................. 1058
  The Default FTP Site ......................................................... 1058
Other FTP Sites ................................................................. 1058
Virtual Directories .............................................................. 1060
Basic Administrative Tasks ................................................... 1062
  Configuring Permissions ..................................................... 1062
Stopping, Starting, and Pausing IIS Services ................................. 1065
Using FrontPage Server Extensions .......................................... 1067
Summary ........................................................................... 1068

#### 33 Advanced Internet Information Services ................................. 1069

Server-Level Administration .................................................. 1071
  Connecting to an IIS Server ................................................. 1071
Creating Configuration Backups .............................................. 1072
Configuring Server Properties ............................................... 1073
Site-Level Administration ..................................................... 1075
Directory-Level Administration .............................................. 1076
File-Level Administration .................................................... 1077
Managing WWW Sites .......................................................... 1078
  Web Site Tab .................................................................. 1078
  Performance Tab .................................................................. 1082
ISAPI Filters Tab ................................................................ 1082
Home Directory Tab ............................................................... 1083
Documents Tab .................................................................... 1085
Directory Security Tab ............................................................ 1086
HTTP Headers Tab ................................................................ 1093
Custom Errors Tab ................................................................ 1094
Managing FTP Sites ............................................................... 1095
  Server-Wide FTP Properties ................................................. 1096
Configuring Individual FTP Site Properties ................................ 1096
Configuring FTP Directory Properties ........................................ 1101
Managing NNTP Virtual Servers .............................................. 1102
  What NNTP Service Does .................................................... 1102
NNTP Service Wizards .......................................................... 1103
Configuring the Default NNTP Virtual Server ............................... 1105
# Table of Contents

- Connecting to the Default NNTP Virtual Server ........................................... 1109
- Displaying NNTP Sessions ................................................................. 1110
- Rebuilding an NNTP Virtual Server .................................................. 1110
- Managing SMTP Virtual Servers ......................................................... 1110
  - What SMTP Service Does .......................................................... 1110
  - SMTP Directories ....................................................................... 1111
  - Configuring the Default SMTP Virtual Server .......................... 1112
  - SMTP Domains .......................................................... 1116
  - The New Domain Wizard ......................................................... 1117
- Web Service Extensions ......................................................................... 1117
- Remote Administration ........................................................................ 1119
  - Administration Web Site ........................................................... 1119
  - Enabling Remote Administration ............................................. 1119
  - Testing Remote Administration .................................................. 1120
- Summary ............................................................................................ 1121

## 34 Internet Security and Acceleration Server 2004 ................................. 1123

- Concepts ............................................................................................ 1123
  - Network Address Translation ....................................................... 1124
  - Packet Filtering and Application Layer Filtering ...................... 1125
  - Caching ......................................................................................... 1126
  - Client Types ............................................................................. 1126
- Installation and Configuration .......................................................... 1127
  - System Requirements ................................................................. 1127
  - Installation ............................................................................... 1128
  - Securing Your ISA 2004 Server ............................................... 1131
  - Initial Configuration of ISA Server 2004 ................................. 1131
- Additional Configuration Tasks ......................................................... 1141
  - Define VPN Access .................................................................... 1141
  - Setup Monitoring ....................................................................... 1144
  - Publishing Servers (Reverse Proxy) ........................................ 1144
  - Additional Configuration ......................................................... 1146
- ISA Firewall Client ........................................................................... 1150
- Import, Export, Backup, and Restore .................................................. 1151
- Summary ............................................................................................ 1153
### Part VII
**Tuning, Maintenance, and Repair**

#### 35 Performance Monitoring and Tuning .......................... 1157

- Documenting the Network, Policies, and Procedures .......................... 1158
  - Documenting the Network ............................................. 1158
  - Evaluating Policies and Procedures ................................ 1159
- Selecting a Monitoring Method ............................................. 1160
  - Determining How Often to Monitor ................................... 1161
  - Monitoring Memory Usage ............................................. 1162
  - Monitoring Processor Activity ...................................... 1163
  - Monitoring Disk Activity ............................................ 1164
  - Monitoring Network Activity ....................................... 1165
- Using Event Viewer ....................................................... 1166
  - Event Log Files ....................................................... 1167
  - Components of an Event .............................................. 1167
  - Viewing an Event Log on Another Computer ......................... 1169
  - Changing Event Log Settings ........................................ 1170
  - Archiving an Event Log .............................................. 1170
- Using the Microsoft Windows Server 2003 Performance Advisor .......... 1171
  - Overview ............................................................... 1171
  - Recording and Viewing Data ......................................... 1173
  - Monitoring Multiple Servers ........................................ 1173
- Using System Monitor .................................................... 1175
  - Adding Counters ....................................................... 1177
  - Matching Counters to Graph Lines .................................. 1178
  - Modifying the Display ................................................ 1178
- Performance Logs and Alerts ............................................. 1180
  - Creating Counter and Trace Logs .................................... 1181
  - Saving Log and Alert File Settings ................................ 1184
  - Using Alerts ............................................................ 1184
- Using Network Monitor ................................................... 1186
  - Capturing Frames ....................................................... 1187
  - Viewing the Capture Window ........................................ 1188
  - Viewing the Frame Viewer Window ................................... 1189
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configuring and Customizing Network Monitor</td>
<td>1190</td>
</tr>
<tr>
<td></td>
<td>Designing a Capture Filter</td>
<td>1192</td>
</tr>
<tr>
<td></td>
<td>Designing a Display Filter</td>
<td>1196</td>
</tr>
<tr>
<td></td>
<td>Setting a Capture Trigger</td>
<td>1198</td>
</tr>
<tr>
<td></td>
<td>Memory and Network Tuning</td>
<td>1199</td>
</tr>
<tr>
<td></td>
<td>Changing File System Cache Settings</td>
<td>1199</td>
</tr>
<tr>
<td></td>
<td>Optimizing the Page File</td>
<td>1201</td>
</tr>
<tr>
<td></td>
<td>Tuning Network Performance</td>
<td>1202</td>
</tr>
<tr>
<td></td>
<td>Summary</td>
<td>1202</td>
</tr>
<tr>
<td>36</td>
<td>Disaster Planning</td>
<td>1203</td>
</tr>
<tr>
<td></td>
<td>Planning for Disaster</td>
<td>1203</td>
</tr>
<tr>
<td></td>
<td>Identifying the Risks</td>
<td>1204</td>
</tr>
<tr>
<td></td>
<td>Identifying the Resources</td>
<td>1205</td>
</tr>
<tr>
<td></td>
<td>Developing the Responses</td>
<td>1206</td>
</tr>
<tr>
<td></td>
<td>Testing the Responses</td>
<td>1209</td>
</tr>
<tr>
<td></td>
<td>Iterating</td>
<td>1210</td>
</tr>
<tr>
<td></td>
<td>Preparing for a Disaster</td>
<td>1211</td>
</tr>
<tr>
<td></td>
<td>Setting Up a Fault-Tolerant System</td>
<td>1211</td>
</tr>
<tr>
<td></td>
<td>Backing Up the System</td>
<td>1212</td>
</tr>
<tr>
<td></td>
<td>Creating Automated System Recovery Disks</td>
<td>1212</td>
</tr>
<tr>
<td></td>
<td>Creating a Boot Disk</td>
<td>1216</td>
</tr>
<tr>
<td></td>
<td>Installing the Recovery Console</td>
<td>1218</td>
</tr>
<tr>
<td></td>
<td>Specifying Recovery Options</td>
<td>1219</td>
</tr>
<tr>
<td></td>
<td>Creating and Using a Recovery Drive</td>
<td>1220</td>
</tr>
<tr>
<td></td>
<td>Summary</td>
<td>1220</td>
</tr>
<tr>
<td>37</td>
<td>Using Backup</td>
<td>1221</td>
</tr>
<tr>
<td></td>
<td>Selecting a Backup Medium</td>
<td>1221</td>
</tr>
<tr>
<td></td>
<td>Using Removable Storage</td>
<td>1222</td>
</tr>
<tr>
<td></td>
<td>Backing Up to Files</td>
<td>1223</td>
</tr>
<tr>
<td></td>
<td>Using CD-ROMs</td>
<td>1223</td>
</tr>
<tr>
<td></td>
<td>Developing a Backup Strategy</td>
<td>1224</td>
</tr>
<tr>
<td></td>
<td>The Backup Window</td>
<td>1224</td>
</tr>
<tr>
<td></td>
<td>Backup Types</td>
<td>1225</td>
</tr>
<tr>
<td></td>
<td>Media Rotation</td>
<td>1227</td>
</tr>
</tbody>
</table>
### Table of Contents

- Backing Up Data ................................................................. 1227
  - Using Windows Server 2003 Backup .................................. 1228
  - Using the Windows Server 2003 Backup Wizard ..................... 1237
  - Executing Jobs from the Command Line ............................. 1237
- Restoring Data ................................................................. 1239
  - Selecting Files to Be Restored ....................................... 1239
  - Selecting Destinations for Restored Files .......................... 1240
  - Setting Restore Options ................................................. 1241
- Planning for Failure .......................................................... 1242
  - Backing Up the System State ........................................... 1242
- Handling Backup and Restore Problems .................................. 1243
  - Backing Up Exchange Servers ......................................... 1243
  - Backing Up Encrypted Files .......................................... 1243
  - Restoring the System State ............................................. 1244
  - Preserving NTFS Permissions ........................................... 1244
- Third-Party Backup Utilities ................................................. 1246
- Summary ............................................................................. 1248

### 38 Planning Fault Tolerance and Avoidance .............................. 1249

- Mean Time to Failure and Mean Time to Recover ..................... 1250
- Protecting the Power Supply ................................................. 1251
  - Local Power Supply Failure ............................................. 1251
  - Voltage Variations ............................................................ 1252
  - Short-Term Power Outages ............................................... 1255
  - Long-Term Power Outages ............................................... 1255
- Disk Arrays ........................................................................... 1256
  - Hardware vs. Software ....................................................... 1256
  - RAID Levels for Fault Tolerance ........................................ 1257
  - Hot-Swap and Hot-Spare Disk Systems ............................... 1262
- Distributed File System ......................................................... 1262
- Clustering ............................................................................. 1263
  - Network Load Balancing .................................................... 1263
  - Server Clusters .................................................................. 1263
- Summary ............................................................................. 1264
### 39 Using the Registry ................................. 1265
- Introducing the Registry .......................... 1265
- The Origins of the Registry ................. 1265
- What Registry Data Is Used For .......... 1267
- Understanding the Registry's Structure .... 1268
  - The Root Keys .............................. 1271
  - Major Subkeys ............................ 1273
  - How Data Is Stored ....................... 1277
- Using the Registry Editors .............. 1279
  - A Whirlwind Tour of the Registry Editor .. 1280
  - A Whirlwind Tour of Reg ................ 1288
- Backing Up and Restoring the Registry ... 1290
  - Choosing a Backup Method ............. 1290
  - Backing Up the Registry ......... 1291
- Summary .................................... 1292

### 40 Troubleshooting and Recovery .............. 1293
- Triaging the Situation ...................... 1293
- Performing a System Recovery .......... 1295
  - Identifying Possible Causes .......... 1295
  - Using the Last Known Good Configuration 1296
  - Using Safe Mode ......................... 1297
  - Using a Boot Disk to Recover the System 1298
  - Booting from Mirrored Boot Partitions 1299
- Performing an In-Place Upgrade ........ 1300
- Using the Automated System Recovery Process 1301
- Fixing the Underlying Problem ......... 1302
  - Rolling Back Recently Installed Drivers 1303
  - Using Help And Support to Gather Basic Information 1304
  - Using System Information to Gather Advanced Information 1306
  - Checking Services ...................... 1307
- Using the System Configuration Utility .... 1309
- Using the System File Checker ........ 1311
- Restoring from a Backup ............... 1311
- Reinstalling Windows ..................... 1312
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency Management Services and Headless Servers</td>
<td>1312</td>
</tr>
<tr>
<td>EMS Overview</td>
<td>1312</td>
</tr>
<tr>
<td>Hardware and Software Requirements</td>
<td>1314</td>
</tr>
<tr>
<td>Setting Up EMS</td>
<td>1315</td>
</tr>
<tr>
<td>Using EMS for Out-of-Band Administration</td>
<td>1321</td>
</tr>
<tr>
<td>Miscellaneous Challenges</td>
<td>1323</td>
</tr>
<tr>
<td>Using the Shutdown Event Tracker</td>
<td>1323</td>
</tr>
<tr>
<td>Adding a Processor to the System</td>
<td>1324</td>
</tr>
<tr>
<td>Troubleshooting Shutdown Problems</td>
<td>1325</td>
</tr>
<tr>
<td>Uninstalling Windows</td>
<td>1326</td>
</tr>
<tr>
<td>Summary</td>
<td>1327</td>
</tr>
</tbody>
</table>

## Part VIII

### Appendixes

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A  Interface Changes from Windows 2000 Server</td>
<td>1331</td>
</tr>
<tr>
<td>B  Interface Changes from Windows NT 4</td>
<td>1337</td>
</tr>
<tr>
<td>Clipboard Viewer</td>
<td>1338</td>
</tr>
<tr>
<td>Compression Agent</td>
<td>1338</td>
</tr>
<tr>
<td>Computers Near Me</td>
<td>1339</td>
</tr>
<tr>
<td>Devices</td>
<td>1339</td>
</tr>
<tr>
<td>Dial-Up Networking</td>
<td>1339</td>
</tr>
<tr>
<td>Disk Administrator</td>
<td>1340</td>
</tr>
<tr>
<td>Find</td>
<td>1340</td>
</tr>
<tr>
<td>MS-DOS Prompt</td>
<td>1340</td>
</tr>
<tr>
<td>My Briefcase</td>
<td>1340</td>
</tr>
<tr>
<td>My Documents</td>
<td>1340</td>
</tr>
<tr>
<td>Network Neighborhood</td>
<td>1341</td>
</tr>
<tr>
<td>Personalized Menus</td>
<td>1341</td>
</tr>
<tr>
<td>Start Menu</td>
<td>1341</td>
</tr>
<tr>
<td>System Information</td>
<td>1341</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>1342</td>
</tr>
<tr>
<td>User Manager</td>
<td>1342</td>
</tr>
<tr>
<td>User Manager for Domains</td>
<td>1342</td>
</tr>
<tr>
<td>View Options</td>
<td>1342</td>
</tr>
<tr>
<td>Windows NT Explorer</td>
<td>1343</td>
</tr>
</tbody>
</table>
C Optional Components .......................................................... 1345
   Accessories and Utilities .................................................. 1346
      Accessibility Wizard ...................................................... 1346
      Accessories .............................................................. 1346
      Communications ........................................................ 1347
      Active Directory Services .............................................. 1347
      Application Server ...................................................... 1347
   Certificate Services ....................................................... 1348
   Distributed File System (DFS) ............................................ 1348
   E-mail Services .............................................................. 1348
   Fax Services ................................................................. 1348
   Indexing Service ............................................................ 1348
   Internet Explorer Enhanced Security Configuration ................. 1349
   Management and Monitoring Tools ....................................... 1349
   Microsoft .NET Framework 2.0 ........................................... 1349
   Networking Services ....................................................... 1350
   Other Network File and Print Services ................................. 1350
   Remote Installation Services ............................................. 1351
   Remote Storage .............................................................. 1351
   Security Configuration Wizard ........................................... 1351
   Subsystem for UNIX-Based Applications ................................. 1351
   Terminal Server ............................................................. 1351
   Terminal Server Licensing ................................................ 1351
   UDDI Services ............................................................... 1351
   Update Root Certificates .................................................. 1352
   Windows Media Services .................................................. 1352
   Windows SharePoint Services ............................................. 1352
Table of Contents

D  Using the Microsoft Windows Server 2003  
Recovery Console ............................ 1353
  Recovery Console Limitations .................. 1353
  Starting the Recovery Console ................. 1354
  Using Recovery Console Commands .............. 1355

E  Using the Microsoft Windows Server 2003 Support Tools .......... 1357
  Glossary ..................................... 1363
  Index ........................................ 1383

What do you think of this book?  
We want to hear from you!  
Microsoft is interested in hearing your feedback about this publication so we can 
continually improve our books and learning resources for you. To participate in a brief 
online survey, please visit: www.microsoft.com/learning/booksurvey/
Acknowledgments

A book of this heft is the product of countless hands. The authors, representing only three sets of hands, have many people to thank.

From Microsoft, we’d like to thank: Darren Canavor and Tom Jones for providing a timely, if unsettling, answer to a critical namespace question, especially since it wasn’t the answer I wanted to hear, but needed to. Gary Wilson and Jeff Davis, MVP Leads Extraordinaire, who provided access to many resources throughout the project. Darrell Gorter, for a last-minute but instant turnaround answer on x64 registry redirection. Ward Ralston for being our gateway into the Server team.

Jason Gerend would like to thank Dan Boldo, Drew McDaniel, and Shobana Balakrishnan for their help with DFS; Anuraag Tiwari, Bart Denison, Keith Hageman, Clyde Law, and Robert Lyon for their help with Storage Manager for SANs; Scott Dickens for his help with RIS; Dara Adekanmbi and Eduardo Melo for their help with R2 Setup; Joan Kelley and James Kahle for sharing their knowledge about unattended Setup; Chris Davis, Kukjin Lee, and Mei Wang for their help with the Server Performance Advisor; Sangeeta Ranjit and Alan Morris for their help with the Print Management Console; and Gary Wilson and Jeff Davis for locating the right members of the product teams. Jason would also like to thank Jeff Middleton for sharing his real-world experiences with disaster recovery during Hurricane Katrina, as well as for his heroic efforts before, during, and after the catastrophe.

We’re very grateful to Paxton Sanders, who did great work on several security and IIS chapters.

Fellow MVP Alex Angelopoulos wrote the core of the scripting chapter and is an outstanding resource for all things scripted.

All three of us appreciate the great work done by the folks at Microsoft Press, including but not limited to project editor Karen Szall; Roger LeBlanc, whose careful and considerate editing was greatly appreciated; Mitch Tulloch, our Technical Editor, who was simply the best (that is, the most annoyingly, irritatingly, fussily, accurate) tech editor we’ve ever worked with; Julie Hatley, indexer; and Elizabeth Hansford, desktop publisher. And last but absolutely not the least, the production and support people at Microsoft Press without whom this book would not exist. It is a pleasure to work with a team of professionals of this caliber. Thank you.

As always, we thank the people from past collaborations whose contributions to every-thing we write can’t be overstated: Rudolph S. Langer and David J. Clark.
Introduction

Change alone is unchanging.

— Heraclitus (c. 535 B.C.–c. 475 B.C.)

Even the ancient Greeks knew that change is inevitable, constant, and inescapable. You can brood about the inevitability of change, or you can take the optimist’s view and assert that at least some change is beneficial. We’re basically optimists, so we’ve changed a lot in this edition. Not only have we gone over the first edition with a fine-tooth comb looking for ways to make it clearer and more concise, but we’ve also added a lot of completely new material covering the new and exciting features that were added to Microsoft Windows Server 2003 with the release of Service Pack 1, and then the release of the R2 editions of Windows Server 2003. Plus we cover the new and exciting architecture in the x64 Editions of Windows Server 2003.

Meet the Family


<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum RAM</td>
<td>4 GB for 32-bit version; 32 GB for 64-bit version</td>
<td>64 GB for 32-bit version; 1 TB for 64-bit versions</td>
<td>128 GB for 32-bit version; 1 TB for 64-bit versions</td>
</tr>
<tr>
<td>Maximum CPU</td>
<td>4</td>
<td>8</td>
<td>64</td>
</tr>
<tr>
<td>Cluster Service</td>
<td>Yes, x64 version only</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Internet Connection Sharing (ICS)</td>
<td>Yes, 32-bit version only</td>
<td>Yes, 32-bit version only</td>
<td>No</td>
</tr>
<tr>
<td>Terminal Server</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Terminal Server Session Directory</td>
<td>Yes, x64 version only</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Hot add memory</td>
<td>No</td>
<td>Yes, 32-bit version only</td>
<td>Yes, 32-bit version only</td>
</tr>
</tbody>
</table>
Introduction

Windows Server 2003, Web Edition, varies enough from the other three editions that we don't attempt to cover it in this book. Windows Server 2003 Compute Cluster Edition is a special version of Windows Server 2003 Standard x64 Edition. It has similar requirements and support but cannot be used as an infrastructure server.

New in Windows Server 2003

Of course, there are many new features in Windows Server 2003, and even more in Windows Server 2003 R2.

Many of the new features in Windows Server 2003 are centered on Active Directory and include the concept of forest and domain functionality levels. Functionality levels allow the introduction of new, non-backward-compatible features, much as Windows 2000 native mode introduced nested groups, Security ID (SID) history, and universal groups.

The Windows Server 2003 interim mode is what you see if you upgrade directly on a Microsoft Windows NT 4 primary domain controller. This gives you enhancements such as linked value replications. For example, if you add a user to a group of 1000, only the new member is replicated; you don't get the 1001 replications required in Windows 2000 Server.

In Windows Server 2003 domain mode, you get domain controller rename, so you can rename domain controllers without first demoting them back to members; and you get the replicated logon timestamp attribute so that the last logon time of a user is replicated to all the domain controllers. That's helpful for troubleshooting account lockout issues.

Windows Server 2003 R2 adds two new Active Directory features: Active Directory Application Mode (ADAM), a limited version of Active Directory that application developers can take advantage of, and Active Directory Federation Services (ADFS), which enables new single sign-on scenarios across completely disparate forests.
To make the configuration of Group Policies less opaque, Windows Server 2003 has Resultant Set of Policy (RSoP). Use this tool to find out what a particular set of policy settings actually means.

Reducing the number of activities that require a server reboot is continuing apace. Now you can extend a storage volume, manage storage dynamically, configure network protocols, and reconfigure Plug and Play hardware without a reboot. It's now possible to administer a completely headless server—a computer without monitor, display adapter, keyboard, or mouse. And from Microsoft Windows XP, Windows Server 2003 adds Remote Assistance and Compatibility Mode.

Die-hard command-line fans will be glad to learn that Windows Server 2003 includes improved command-line management tools that allow administrators to complete most tasks without having to use a graphical user interface.

These improvements and dozens more are detailed in the chapters that follow.

---

**How to Use this Book**

The IT implementer can use this book in several ways. It can be read as a

- Guide to deployment
- Ready reference
- Resource for information when making decisions about network organization and operations
- Thorough introduction to the particulars of Windows Server 2003

We assume the reader has a fundamental understanding of networking and the Microsoft Windows family of operating systems, but we don't expect every reader to be an expert on every subject. We've tried to provide background where appropriate, as well as references to additional information.

---

**What’s in the Book**


Chapters 1 through 4 are all about planning. Perhaps you’ve heard Edison’s famous quote, “Genius is one percent inspiration and ninety-nine percent perspiration.” Modify that slightly and you have a good motto for network building: “A good network is one
percent implementation and ninety-nine percent preparation.” The first chapter is an overview of Windows Server 2003, its components, and its features. This is followed by chapters on directory services and namespace planning. The last chapter in this section covers specific issues that need to be addressed when planning your deployment.

Chapters 5 through 11 cover installation and initial configuration. These chapters take you through the process of installing Windows Server 2003 and configuring hardware. We’ve also included chapters on upgrading existing domains and managing users.

Chapters 12 through 20 cover day-to-day tasks in network administration, including implementing Active Directory and managing storage options.

While every chapter in the book includes important security considerations, Chapters 21 through 26 are focused specifically on security, including patch management and wireless security.

Supporting services and features are described in Chapters 27 through 31. Few networks need all the features Windows Server 2003 offers, but all administrators need to be familiar with managing software, and most need to deal with interoperability with other operating systems. You’ll find chapters on application compatibility, Virtual Server, Terminal Services, and the Index Service.

In Chapters 32 through 34, we cover the components that connect the outside world to you while protecting you from it. Here you’ll find chapters on Internet Information Services, Internet Security, and Acceleration Server 2004.

The final chapters on tuning, maintenance, and repair cover important material on network health. There’s a chapter on the performance monitoring tools included with Windows Server 2003 and how to use them. There are also chapters on the important topics of disaster planning and prevention. If, despite your best efforts, the network falters, here’s where you’ll find information on troubleshooting and recovery. In addition, we include a chapter on the registry—the brains of Windows Server 2003—and some advice if you’re contemplating brain surgery.

At the end of the book, you’ll find a glossary and appendixes that contain information that will prove useful for quick access to important information.

Within the chapters themselves, we’ve tried to make the material as accessible as possible. You’ll find descriptive and theoretical information, as well as many step-by-step examples for how to implement or configure a particular feature. These are supplemented with graphics that make it easy to follow the written instructions.

In addition, we’ve made extensive use of the reader aids common to all books in the Administrator’s Companion series.
**Note** These generally represent alternate ways to perform a task or some information that needs to be highlighted.

**More Info** These refer you to other books and specific sources of information throughout the book.

**Important** Don’t skip over these boxes because they contain important information or warnings about the subject at hand—often critical information about the safety of your system.

**Planning** As we stress throughout the book, proper planning is fundamental to the smooth operation of any network. These boxes contain specific and useful hints to make that process go smoothly.

**On the CD** Look on the companion CD for additional material including scripts that you can use.

**Security Alert** These boxes highlight information you should know to maximize security for your network.

---

**Real World**
Everyone benefits from the experiences of others. Real World sidebars contain elaboration on a particular theme or background based on the adventures of IT professionals just like you.

---

**Under the Hood**
Sometimes you want to know what’s actually happening when a wizard makes a change, or you set a particular configuration. Under the Hood sidebars contain more detailed information about exactly what’s being changed.
We encourage you to take advantage of other books offered by Microsoft Press. In addition to other Windows Server 2003 titles, the Resource Kit series provides in-depth coverage of specific topics. The *Microsoft Windows Server 2003 Resource Kit* is highly recommended for every administrator.

**What’s on the CD?**

For your use, this book includes a companion CD that contains a complete copy of the book in electronic form, sample scripts from throughout the book, and a chapter from the first edition of the book that had to be pulled because of space considerations.

For additional support information regarding this book and the CD (including answers to commonly asked questions about installation and use), visit the Microsoft Press Technical Support Web site at [http://www.microsoft.com/learning/support/books/](http://www.microsoft.com/learning/support/books/).

**Talk to Us**

We’ve done our best to make this book as accurate and complete as a single-volume reference can be. However, because Windows Server 2003 is such a large and complex product, we’re sure that alert readers will find omissions and even errors (though we fervently hope not too many of those). If you have suggestions, corrections, or comments, please write and let us know at WinServer2003R2@scribes.com. We genuinely appreciate hearing from you and sincerely hope you find *Microsoft Windows Server 2003 Administrator’s Companion*, Second Edition, enjoyable and useful.
System Requirements

The following are the minimum hardware and software requirements to run the companion CD and view the eBook that is included on the CD:

- An Intel Pentium II-compatible processor or later
- 133 MHz CPU (550 MHz recommended)
- 128 MB RAM (256 MB recommended)
- 1.5 GB disk space for setup
- CD-ROM drive
- Display monitor capable of 800 × 600 resolution or higher
- Microsoft Mouse or compatible pointing device

You can view the eBook using Adobe Acrobat Reader.
Part I
Preparation

Chapter 1:
Overview of Windows Server 2003 ........................................... 3

Chapter 2:
Introducing Directory Services .............................................. 17

Chapter 3:
Planning Namespace and Domains ....................................... 29

Chapter 4:
Planning Deployment ......................................................... 43
Chapter 1
Overview of Windows Server 2003

Veteran system administrators love to regale newcomers to the field with hair-raising tales of the olden days when everything was much worse (or better, depending on the particular old-timer you speak to). This, of course, is much like the relative who never stops telling stories about walking to school in the snow even if they grew up in Tahiti. What makes computer technology different is that the old days we speak of aren’t very long ago. In computer terms, the year 2000 is pretty far back and 1995 is ancient history.

Those who made the move from Microsoft Windows NT to Microsoft Windows 2000 a few years ago are aware of the lengthy learning curve associated with the new management interfaces in Microsoft Windows 2000 Server and probably have a few spine-tingling tales from that time. Those who then made the move from Windows 2000 Server to Microsoft Windows Server 2003 in the more recent past found it a good deal less onerous—many of the
changes are behind the scenes and don’t affect the administrator’s way of doing things. As a result, although there are improvements in reliability, scalability, security, and the management of large and complicated networks, Windows Server 2003 presents some generally familiar methods of handling networks and users. Adding Windows Server 2003 Service Pack 1 (SP1) and Windows Server 2003 R2 provides additional features and functionality still without making radical changes in how you operate.

However, even if you’re moving directly from Windows NT to Windows Server 2003, this book has everything you need to smooth out what can be a bumpy transition.

### Versions of Windows Server 2003

There are five versions of Windows Server 2003, not including Microsoft Windows Small Business Server, which is in a category by itself. Microsoft Windows Server 2003, Standard Edition is designed to meet the requirements of small-sized to medium-sized businesses, and it includes all the necessary file and printer sharing, secure Internet connectivity, and collaboration capabilities to do so. Microsoft Windows Server 2003, Enterprise Edition is for medium-sized to large-sized businesses and provides a stable enterprise infrastructure, which enables deployment of line-of-business applications and is appropriate for high-performance e-commerce solutions. Microsoft Windows Server 2003, Web Edition is optimized for hosting a Web site, Web services, and applications. Microsoft Windows Server 2003, Datacenter Edition is designed for business-critical solutions that require excellent performance and absolute stability under load, such as the performance required by enterprise database applications and high-volume transaction processing. Microsoft Windows Compute Cluster Server 2003 is a special, x64-only, version of Windows Server 2003 that is designed for easy and automatic deployment of high-performance computing (HPC) clusters. It is based on Windows Server 2003 Standard x64 Edition, but it does not support installation of R2.

**Note** Not all versions of Windows Server 2003 are available on all platforms, and not all versions support installation of R2. The three core editions: Standard, Enterprise, and Datacenter, however, are supported both 32-bit and 64-bit architectures and all support R2.

Underneath, all five are the same stable and powerful platform for .NET technology, which is—in the simplest possible terms—a prebuilt infrastructure for constructing Internet-based applications.

With its improvements to security, network capabilities, and the Active Directory service, Windows Server 2003 is meant to be the center of an organization’s communication hub. The platform can be the network’s router, an Exchange server, or a Web server. There are a number of changes and improvements from the Windows 2000 Server family, ranging from improvements in reliability to the addition of Fibre Channel technology.

Some of the new features apply to both 32-bit and 64-bit operating systems. Table 1-1 identifies which operating systems are 32-bit and which are both.

### Table 1-1 32-bit and 64-bit operating systems

<table>
<thead>
<tr>
<th>Windows Product</th>
<th>32-bit</th>
<th>64-bit x64</th>
<th>64-bit ia64</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2003, Standard Edition</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Windows Server 2003, Enterprise Edition</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Server 2003, Datacenter Edition</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Server 2003, Web Edition</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Windows Computer Cluster Server 2003</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Microsoft Windows XP Home Edition</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Microsoft Windows XP Professional Edition</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Throughout this book, only a few distinctions are made between the versions of Windows Server 2003. Some features available in certain versions of Windows Server 2003 might not be available in others, and that difference is noted where appropriate. With the release of Windows Server 2003 SP1, a whole new 64-bit architecture, “x64,” is added to the Windows product line. This new 64-bit architecture supports full-speed running of 32-bit applications and is based on an extension of the familiar 32-bit x86 instruction set. The ia64 architecture continues to be supported for high-end Windows Servers running Enterprise Edition or Datacenter Edition.

### Deploying Windows Server 2003 and Windows Clients

Deploying Windows Server 2003 together with Microsoft Windows XP Professional is the best way to get the most from technologies that intelligently store user data, applications, system files, and administrative settings from clients to servers. These technologies
help manage software on client machines and transparently provide better availability and safety for users’ data.

For example, Microsoft IntelliMirror is a distributed and highly configurable replication service that allows clients and servers to mirror and share local or distributed file system data. IntelliMirror’s Remote Installation Services (RIS) provides for the installation and configuration of an operating system (such as Windows XP Professional) on a new computer. It can also restore a computer to a known good configuration.

Using the Software Installation feature of Group Policy in Windows Server 2003, you can assign an application to a user or group so that the program appears on the user’s Start menu and is installed the first time a user clicks it. If the application isn’t immediately required, the program can be published so that it appears as an option in Add/Remove Programs for the user to install when needed. When an application upgrade becomes available, the upgrade is automatically applied the next time the user launches the application.

User documents and personal settings can be stored, or mirrored, on a server managed by an administrator. This provides the following benefits:

- **Improved access** Users can log on to any PC on the network; all their documents and personal settings appear on any computer they use.

- **Increased availability** The information mirrored on the server is also on the local machine, so it is available even when users aren’t connected to the network. When a user reconnects, the information on the server is synchronized with the new local information. Because laptop users’ data is synchronized with the server whenever a laptop is connected to the network, network administrators can back up mobile users’ data even when the laptops are not connected.

- **Better protection** All files reside on the server, which can be backed up as part of normal, centralized backup and restore procedures.

Although you can connect machines with any number of operating systems to your Windows Server 2003, using it in conjunction with Windows XP Professional will provide optimal functionality for users and administrators alike. From software installation to IntelliMirror data, coupling the two operating systems will provide the safest and easiest computing experience.

---

**Network Management**

The Microsoft Management Console (MMC) hosts administrative tools displayed as consoles. These tools, composed of one or more applications, are built with modules called snap-ins. This design enables you to customize the tools so that you can delegate specific
administrative tasks to users or groups. Saved as MMC files, these custom tools can be sent by e-mail, shared in a network folder, or posted on the Web. Using system policy settings, you can also assign MMC files to users, groups, or computers. A tool can be scaled up or down, integrated seamlessly into the operating system, repackaged, and customized. In fact, you can do everything with these tools short of adding pinstripes and custom upholstery!

Note Many new command-line tools and utilities were added to improve network management. These command-line tools help automate high-volume or common server administration tasks using Microsoft Visual Basic scripting or command batch files.

Printer Management

New in Windows Server 2003 R2 is the Print Management Console (PMC), which greatly enhances the administrator’s view of printers and print servers in the network. For administrators who have struggled with the previous options for managing printers on Windows Server 2003, the new PMC is a major step forward. Prior to R2, the facilities for managing printers were essentially unchanged since Windows NT. The PMC let’s you scan the network for printers, manage drivers and ports, and deploy printers automatically via Group Policy. For complete details on the new Print Management console, see Chapter 8.

Group Policy

Group Policy is a management technology used to specify options for desktop configurations for groups of computers and users. Group policies are saved as Group Policy Objects (GPOs) that in turn are associated with Active Directory objects such as sites, domains, or organizational units (OUs). Group policies can include security options, software installation and maintenance options, and options for scripts controlling startup and shutdown.

Note In Windows Server 2003, Group Policy has been overhauled to allow more tasks to be assigned using Group Policy settings. Many new policies have also been added, letting an administrator customize and control the performance of Control Panel, Terminal Services, Remote Assistance, networking, error reporting, dial-up connections, network signon, Group Policy, and roaming profiles.

Even better is the addition of the Resultant Set of Policy (RSoP) Wizard. With Group Policy, it’s sometimes hard to discern what is happening as the result of a set of policies—much less perform “what if” scenarios. In logging mode, the RSoP Wizard tells you just
what is happening on a given computer. In planning mode, it analyzes what the result will be of a given set of policies.

Now available for download, the Group Policy Management Console (GPMC) consolidates several Group Policy tools, making policy administration simpler and more efficient.

**IntelliMirror**

IntelliMirror is a powerful technology that helps manage change and configuration. In other words, after the clients and servers are set up, hardware, software, and user changes are handled automatically, using rules and profiles to determine what happens. Administrators can control the rules for the entire network from a single central location. Table 1-2 summarizes some of the centralized network management tasks in Windows Server 2003.

<table>
<thead>
<tr>
<th>Task</th>
<th>What Is Done</th>
<th>Technologies Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage user documents</td>
<td>Mirrors user data to the network and caches network data locally on the client</td>
<td>Active Directory, Group Policy, File Redirection, Offline Files, Synchronization Manager, Disk Quotas, and roaming user profiles</td>
</tr>
<tr>
<td>Manage user settings</td>
<td>Mirrors user settings to the network, and applies administrator-set defaults to the user’s environment</td>
<td>Active Directory, Group Policy user configuration, and roaming user profiles</td>
</tr>
<tr>
<td>Perform remote operating system installation</td>
<td>Installs operating system from network servers</td>
<td>Active Directory, Group Policy, and RIS</td>
</tr>
<tr>
<td>Install software</td>
<td>Provides just-in-time software installation (applications and operating system upgrades)</td>
<td>Active Directory, Group Policy, and Windows Installer</td>
</tr>
</tbody>
</table>

**Terminal Services**

Terminal Services allows Windows-based applications to run on desktops that can’t normally run large Windows applications. All application processing and data storage take place on the server; the client machine needs only to be able to run a “thin client,” which requires very small amounts of memory and disk storage space. (In Windows, a client can simultaneously be a thin client and a fat client.) This allows machines without a lot of power (needed to run enterprise applications independently) to use the resources of the server. With the use of a third-party add-on, even MS-DOS, UNIX, and Apple Macintosh machines can be clients.
With Terminal Services, users log on and see only their own session, which is completely independent of any other client session. The application operates on the server, and the entire process is transparent to the user. The setup and use of Terminal Services and Terminal Services clients is covered in Chapter 30.

Interoperability

The typical network in a medium-sized to large-sized enterprise is completely heterogeneous, so interoperability between and among operating systems is imperative. Windows Server 2003 improves interoperability in the following ways:

- Communicates natively with UNIX and Novell NetWare systems using Transmission Control Protocol/Internet Protocol (TCP/IP)
- Provides services for file and print sharing with UNIX, NetWare, and Macintosh systems
- Provides identity management services to UNIX systems (R2 only)
- Provides the Subsystem for UNIX-Based Applications (SUA) to support UNIX applications running natively on Windows (R2 only)
- Supports Open Database Connectivity (ODBC) software, Microsoft Message Queuing (MSMQ) technology, and many standard communication protocols—such as File Transfer Protocol (FTP), Network News Transfer Protocol (NNTP), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP)—so that new applications can interoperate with existing software and data

Interoperability is covered in Chapter 27.

System and Network Security

Security is available in Windows Server 2003 for every configuration, from a simple workgroup to enterprise server systems. The emphasis on security and the fact that security mechanisms permeate every corner of Windows Server 2003 should not come as a surprise. Security is an increasingly critical issue in virtually every enterprise. Intranets, extranets, and dial-in access, not to mention casual user malfeasance, are all threats to both data and infrastructure. At the same time, an overly complex security apparatus tries the patience of administrators and users alike. Windows Server 2003 attempts to resolve these conflicting needs with a security system that is genuinely secure, yet easy to administer and transparent to the user.
Windows Server 2003 includes full support for the MIT Kerberos version 5 security protocol, providing a single signon to Windows Server 2003–based enterprise resources. As of Windows 2000, Kerberos replaced NT LAN Manager (NTLM), which was used in Microsoft Windows NT 4 as the primary security protocol. For smooth integration, Windows Server 2003 supports both methods of authentication—NTLM when either the client or the server is running a previous version of Windows, and Kerberos for Windows Server 2003 servers and Windows 2000 or Windows XP Professional clients. In addition, there is built-in support for Secure Sockets Layer/Transport Layer Security (SSL/TLS) for users logging on to a secure Web server.

Other security capabilities include the following:

- An X.509-based public-key certificate server integrated with Active Directory, allowing the use of public-key certificates for authentication.
- Support for tamper-resistant smart cards to store passwords, private keys, account numbers, and other security information. Additions to smart card capability include the ability to log on using Terminal Services.
- IPSec, which governs end-to-end secure communication. After IPSec is implemented, communications are secured transparently; no user training or interaction is required.

Many security functions in Windows Server 2003 are innate in Active Directory, and full implementation is available only when Active Directory is used. In addition, some security functions cannot be fully realized in a mixed environment of server domains. For example, Windows Server 2003 includes support for transitive trusts, which means that when a new domain is created in a Windows Server 2003 forest, a two-way, transitive trust relationship is established automatically between the new domain and other domains in the forest. No administrative tasks are required to establish this trust relationship. To set up a trust relationship between a Windows Server 2003 domain and a Windows NT domain, however, you must explicitly establish it.

Security Alert Security enhancements are everywhere in the Windows Server 2003 family. These additions range from the small (security logging is turned ON by default) to the very large.

Security is so firmly integrated into all aspects of Windows Server 2003 that it can’t be quarantined into a single section; hence, security material appears throughout this book. However, all of Part V of this book specifically targets security-related subjects, including basic concepts, implementation, patching, and wireless security.
Availability and Reliability

Availability is the measure of fault tolerance of a software system, where fault tolerance is the ability of a system to maintain data integrity in the event of a catastrophic event. Reliability is the likelihood that the system will continue to work as designed. Taken together, availability and reliability measure the system’s capacity to ensure that data is available and correct under a heavy workload or other adverse conditions.

Windows Server 2003 builds on the foundation Windows 2000 Server created to ensure that computing power is available. Windows 2000 Server added Plug and Play, server clusters (for Enterprise Edition and Datacenter Edition only), Network Load Balancing (NLB), and the ability to start from a mirrored volume. Windows Server 2003 adds Remote Installation Services (RIS) and Emergency Management Services (EMS).

Windows 2000 Server improved on the high reliability offered by Windows NT 4 by improving memory management, providing Windows File Protection, and enhancing the backup utility. Windows Server 2003 adds the Automated System Recovery (ASR) and the Compatibility Mode technology, which allows you to run older applications in an environment that emulates what those applications expect.

Clustering allows the interconnection of multiple computing systems (known as nodes) that act as a single computing entity, or that distribute the processing load across multiple, parallel processors. This provides high fault-tolerance in traditional clusters, and high performance for parallel computer clusters. High-availability server clusters monitor the health of standard applications and servers, and they can automatically recover mission-critical data and applications from many common types of failure—usually in less than a minute. Server clustering is covered in Chapter 19.

Note

Servers that have hardware support for adding memory while the server is operating can have memory added and experience no downtime.

Active Directory

A directory service is a tool that connects the directories across the network and acts like a big phone book for all users. Using general input (for example, “where are the printers?”), a user can receive a listing of resources (for example, printer resources). All versions of Windows Server 2003 except Windows Server 2003, Web Edition include Active Directory as the directory service.
Active Directory combines X.500 naming standards, using the Internet’s Domain Name System (DNS) as a locating device and Lightweight Directory Access Protocol (LDAP) as the core protocol. Active Directory allows a single point of administration for all resources, including users, files, peripheral devices, host connections, databases, Web access, services, and network resources. It supports a hierarchical namespace for user, group, and machine account information, and it can encompass and manage other directories to reduce the administrative burdens and costs associated with maintaining multiple namespaces.

As you can see, there’s a lot of good news about Active Directory—including that it paves the way for eliminating the concept of domains. The actual migration to Active Directory is not difficult, but planning the design of your new directories can be vexatious. Design mistakes can harm the stability and efficiency of the network. Fortunately, you don’t need to get rid of your existing domains to take advantage of Active Directory, and migration can be piecemeal. You can upgrade servers without users being aware of any changes.

Chapter 2 and Chapter 3 explore the concepts behind Active Directory—including namespace design. Specific implementation is discussed in Chapter 14 and Chapter 15.

---

**Note** The new version of the Active Directory Migration Tool (ADMT) allows migrating passwords from Windows NT 4 to Windows 2000 and Windows Server 2003 servers.

ADMT also has a new scripting interface for the migration of users, groups, and computers. All scriptable tasks can be executed directly from a command line or through batch files.

Active Directory has a new feature that provides Windows Management Instrumentation (WMI) classes to monitor whether domain controllers are successfully replicating Active Directory information among themselves. Because Active Directory replication depends on inter-domain trust, this feature also monitors the functioning of trusts.

Another welcome change in Active Directory for Windows Server 2003 is the ability to rename domains. Although it’s not something you want to do casually (because it involves a lot of reboots of both servers and clients), at least now it is possible.

Other new features of Active Directory in Windows Server 2003 R2 include:

- Active Directory Federation Service (ADFS) gives organizations the ability to use federated credentials from partners to provide authenticated access to Web services.

- Active Directory Application Mode (ADAM) is a new, independent mode of Active Directory that application developers can use to provide directory services for applications.
Storage and File System Support

Windows Server 2003 adds features to the extensive storage and file system support offered by Windows 2000 Server. Adding to the list of invaluable features of Windows 2000 Server—such as NTFS 5, Disk Management, and Encrypting File System (EFS)—Windows Server 2003 also provides the capabilities shown in Table 1-3.

Table 1-3 Storage and file system support in Windows Server 2003

<table>
<thead>
<tr>
<th>Feature</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote document sharing</td>
<td>Allows file sharing across the Internet (through firewalls, routers, and so on) to HTTP servers</td>
</tr>
<tr>
<td>Cross-platform document sharing</td>
<td>Provides native support for Network File Systems (NFS)</td>
</tr>
<tr>
<td>File management improvements</td>
<td>The new File Server Resource Manager (FSRM) provides improved file management capabilities including file type screening, per folder quotas</td>
</tr>
<tr>
<td>Distributed File System</td>
<td>Introduced in Windows Server 2003 and greatly improved in Windows Server 2003 R2, provides a single view of a file system that is distributed and replicated across multiple servers</td>
</tr>
<tr>
<td>Command-line support for disk management</td>
<td>New command-line support includes utilities for disk configuration; most notably, this includes the new DiskPart command</td>
</tr>
<tr>
<td>Storage Manager for SANs</td>
<td>The new Storage Manager for SANs provides direct management of LUNs on Fibre Channel and iSCSI SANs</td>
</tr>
<tr>
<td>GUID partition table</td>
<td>New disk partitioning style, the GUID partition table for 64-bit versions of Windows Server 2003; provides improved partition data structure integrity</td>
</tr>
</tbody>
</table>

Communications

Communication is the lifeblood of businesses—and not just network communications, important as they are. Windows Server 2003 includes numerous changes designed to make communicating easier and more reliable. For connections both inside and outside your business, Windows Server 2003 offers the following tools:

- Through the Internet support built into the operating system, users can send e-mail, chat, and view newsgroups.
- Windows SharePoint Services allow groups to share files, participate in discussions, and communicate a variety of information via Web pages. Administrators manage site security and subwebs. (SharePoint Team Services is not installed by default, and Internet Information Services (IIS) is required for installation.)
Windows Server 2003 provides client support for the industry-standard virtual private network (VPN) through two protocols: the Point-to-Point Tunneling Protocol (PPTP) and the Layer Two Tunneling Protocol (L2TP), used with IPSec. These protocols allow clients or branch offices to connect to another network (such as their corporate network) over the Internet.

Users can send, receive, monitor, and administer faxes directly from the desktop. Several easy-to-use utilities are available from the Start menu after Fax Service Administration is installed. (It’s not installed by default during Windows Setup.)

Internet Services and .NET Application Services

With Windows Server 2003, anything you can do on a corporate network you can do in a Web environment as well. Windows Server 2003 incorporates a set of services that provide server-side support for the most popular application-level Internet protocols, enabling a server to function as a Web server, FTP server, SMTP host, POP3 server, or NNTP host, or all of these at once.

Basic Internet services are fully integrated across the whole spectrum of Windows Server 2003 versions. These services are referred to as Internet Information Services 6. You can host multiple Web sites on a single server with only one IP address.

The Microsoft .NET Framework version 2.0 constitutes the underpinnings of Windows and is based on industry standard SOAP and XML. It provides a rich environment for application development, with simplified development and deployment mechanisms and support for multiple programming languages. The .NET Framework enables the developer to create applications using ASP.NET 2.0 (a server-side scripting environment for developing Web applications) and Windows Forms (for building Windows GUI applications).

Scalability

Windows Server 2003 Service Pack 1 adds support for the x64 Editions of Windows Server. These x64 Editions provide support for greatly increased memory address space, greater physical memory, and improved security, while continuing to support 32-bit applications. The Intel Itanium architecture (ia64) of Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition enable high-end processing such as 3-D graphics, e-commerce, and multimedia. The addressable memory limit for all 64-bit versions of Windows Server 2003 is increased to 16 Terabytes (TB), and 64-bit Enterprise and Datacenter Editions support 1 TB of physical random access memory.
(RAM). The management tools are compatible with both 32-bit and 64-bit versions of the operating systems.

Hot Add Memory allows the administrator to add memory to the system’s available memory pool without having to interrupt normal system operation. It does not require a reboot and, hence, results in no downtime. The server hardware has to support this feature, of course, and it is available only on Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition.

As system speed increases, the processor buses can become saturated under load. One way around this is to increase the number of processor buses. Processors and memory are grouped into structures called nodes. Each processor has access to its own node’s memory and that of other nodes. When memory is accessed in its own node, the processor has to wait just a moment for that information to be made available. If memory is accessed in another node, that node might be busy with one of its processor’s requests. This results in a longer delay before the information can be sent to the requestor. This is called nonuniform memory access, or NUMA, because the amount of time access takes varies. Clearly, NUMA can result in a degradation of system performance. Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition try to limit the number of cross-node accesses by assigning same-process threads to processors in the same nodes, and by allocating memory requests to the same node as the processor making the request. The application programmer can harness this technology, which is available in the form of an application programming interface (API).

The Need for Planning

Whether you are designing a new network or making changes to an existing one, planning is the tedious but essential component. Prior to any implementation work, planning must be completed. Few enjoy and many actively dislike this task, but it’s important to understand that every minute and every hour spent planning will later repay you (or your heirs and assigns) a hundredfold.

Sometimes it’s difficult to appreciate the benefits of careful planning—until you’ve had the misfortune of having to support a poorly considered installation. Windows Server 2003 is particularly unforgiving of an offhand approach to planning. As has been mentioned before, you can add Windows Server 2003 or Windows XP Professional to a Windows NT 4 network. The potential of the Windows Server 2003 can go unrealized if it’s tethered to a network that disallows use of advanced features. And in all cases, designing directories, forests, and trees requires considerable thought and the ability to anticipate future needs. Therefore, the wise system administrator spends more time planning than doing.
Summary

This chapter has provided only the briefest overview of the Windows Server 2003 system and a look at just a few of the thousands of changes, large and small, that have been made. Deciding how to implement Windows Server 2003 on your system requires thought and planning. Although planning and design are important elements in nearly every chapter in this book, the next three chapters are devoted exclusively to the subject. Chapter 2 introduces Active Directory. Chapter 3 covers planning namespace and domains. Finally, Chapter 4 covers the matters to be considered before deploying your first copy of Windows Server 2003.
Chapter 2

Introducing Directory Services

Understanding Directory Services .................................................. 17
Active Directory in Microsoft Windows Server 2003 .......................... 19
The Active Directory Architecture .................................................... 23
Summary ......................................................................................... 27

Everyone uses directories—on or off the computer. Defined as a listing that helps you locate things, directories include bus schedules, book indexes, and telephone books. In fact, telephone directories are the source of the analogy for two searching capabilities that are necessary in computer directories. There’s the “white pages” Search By attribute, in which you know a name or some other fact about the object and you search using that piece of information. The second type of search, called a “yellow pages” search, is done by category. Using both types of searches means you don’t have to know much about an object to locate it.

Directories are essential to a computer network’s functioning. The lack of coherent, accessible directories is felt acutely on a network of any size. True directory services—a global catalog of network services and resources—are missing from Microsoft Windows NT networks. Although the directory functions available in version 4 do provide the all-important single logon and single point of administration that corporate environments need, they have serious deficiencies when large numbers of users are involved. Attempts to organize documents in folders and directories work up to a point, but as the number of objects scales up, management becomes both complex and onerous.

Understanding Directory Services

In a typical Windows NT computing environment, a user could log on to the network with a user name, let’s say crussel, and a password. Assuming that permissions are correctly granted, crussel could click Network Neighborhood or open a mapped drive and browse for needed files.

All this works very well until the scope of the network changes. The company adds e-mail, and crussel gains another identity (charlie.russel@example.local). The additional services and databases and administrative tools—each one identifying Charlie Russel slightly
Part I  Preparation

differently—need to be accessible by the same user. When you consider that this is just one of hundreds or even thousands of users, it isn’t hard to see how errors can arise that can be very difficult to resolve. As the number of objects in a network grows, directory services—a centralized place for storing administrative data that is used to manage the entire computer system—becomes essential.

Directory services differ from a directory in that it consists of both the directory information source and the services that make the information available to users. Being both a management tool and an end-user tool, directory services must address the following needs:

■ Access to all the servers, applications, and resources through a single logon point. (User access is granted or blocked using permissions.)
■ Multimaster replication. All information is distributed throughout the system and replicated on multiple servers.
■ “White pages” searches based on attributes—for example, by filename or file type.
■ “Yellow pages” searches based on classification—for example, all the printers on the third floor or all the servers in the Hartford office.
■ The ability to remove dependency on physical locations for purposes of administration. That is, it should be possible to delegate administration of the directory, either partially or completely.

Although Microsoft occasionally used the term “directory services” in connection with Windows NT, Windows NT did not provide a true, hierarchical directory service. In Windows NT, the directory functions were divided among a host of services based on domains. The Domain Name System (DNS) Server provided the translation of names into Internet Protocol (IP) numbers and was integrated with Dynamic Host Configuration Protocol (DHCP) servers used to dynamically allocate Transmission Control Protocol/Internet Protocol (TCP/IP) addresses. The Windows Internet Name Service (WINS) was used for Network Basic Input/Output System (NetBIOS) name resolution and was required on Windows NT networks for file sharing and some applications. Security was implemented through access control lists (ACLs), the Security Accounts Manager (SAM) database, and other services.

Microsoft Windows 2000 Server was the first product in which the Active Directory service replaced the Windows NT collection of directory functions with an integrated implementation that includes DNS, DHCP, Lightweight Directory Access Protocol (LDAP), and Kerberos. (You learn more about these later in this chapter.)
Real World  Directory Services and X.500

X.500 is a standard for directory services established by the International Telecommunications Union (ITU). The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) also publishes the same standard. The X.500 standard defines the information model used in directory services. In this model, all information in a directory is stored in entries, each of which belongs to at least one object class. The actual information in an entry is determined by attributes contained in that entry.

The original 1988 X.500 standard focused heavily on the protocols to be implemented. Directory Access Protocol (DAP) specifies how user applications access the directory information. Directory Service Protocol (DSP) is used to propagate user directory requests between directory servers when the local directory server can’t satisfy the request.

No extant directory service completely implements the X.500 standard, but all are modeled on the basic specifications of X.500, as is Active Directory. An excellent introduction to directories and X.500 can be found at http://www.nlc-bnc.ca/9/1/p1-244-e.html.

Active Directory in Microsoft Windows Server 2003

Active Directory has numerous advantages, not the least of which is that it can handle any size of installation, from a single server with a few hundred objects to thousands of servers and millions of objects. Active Directory also greatly simplifies the process of locating resources across a large network. The Active Directory Service Interfaces (ADSI) and the new Active Directory Application Mode (ADAM) introduced in Windows Server 2003 R2 allow developers to “directory-enable” their applications, giving users a single point of access to multiple directories, whether those directories are based on LDAP, NDS, or NT Directory Services (NTDS).

Active Directory integrates the Internet concept of a namespace with the operating system’s directory services. This combination allows the unification of multiple namespaces in, for example, the mixed software and hardware environments of corporate networks—even across operating system boundaries. The ability to subsume individual corporate directories into a general-purpose directory means that Active Directory can greatly reduce the costs of administering multiple namespaces.
Active Directory is not an X.500 directory. Instead, it uses LDAP as the access protocol and supports the X.500 information model without requiring systems to host the entire X.500 overhead. LDAP is based on TCP/IP and is considerably simpler than the X.500 DAP. Like X.500, LDAP bases its directory model on entries, where the distinguished name (discussed in the next section) is used to refer to an entry without ambiguity. But rather than use the highly structured X.500 data encoding, LDAP adopts a simple, string-based approach for representing directory entries. LDAP uses many of the directory-access techniques specified in the X.500 DAP standard but requires fewer client resources, making it more practical for mainstream use over a TCP/IP link.

Active Directory also directly supports Hypertext Transfer Protocol (HTTP). Every object in Active Directory can be displayed as a Hypertext Markup Language (HTML) page in a Web browser. Directory-support extensions to Microsoft Internet Information Services (IIS) translate HTTP requests for directory objects into HTML pages for viewing in any HTML client.

Active Directory allows a single point of administration for all published resources, which can include files, peripheral devices, host connections, databases, Web access, users, other arbitrary objects, services, and so forth. It uses the Internet DNS as its locator service, organizes objects in domains into a hierarchy of organizational units (OUs), and allows multiple domains to be connected into a tree structure. The concepts of primary domain controller (PDC) and backup domain controller (BDC) no longer exist. Active Directory uses domain controllers only, and all domain controllers are peers. An administrator can make changes to any domain controllers, and the updates will be replicated on all other domain controllers. Starting with Windows Server 2003 R2, the Active Directory Federation Services extends the Active Directory to enable identity management across organizational and platform boundaries.

**Terminology and Concepts in Active Directory**

Some of the terms used to describe concepts in Active Directory have been around for a while in other contexts, so it’s important to understand what they mean when used specifically in reference to Active Directory. This section covers these basic terms and concepts.

**Namespace and Name Resolution**

“Namespace” is perhaps an unfamiliar term for a very familiar concept. Every directory service is a namespace—a circumscribed area in which a name can be resolved. A television listing forms a namespace in which the names of television shows can be resolved to channel numbers. A computer’s file system forms a namespace in which the name of a file can be resolved to the file itself.
Active Directory forms a namespace in which the name of an object in the directory can be resolved to the object itself. *Name resolution* is the process of translating a name into some object or information that the name represents.

**Attribute**
Each piece of information that describes some aspect of an entry is called an *attribute*. An attribute comprises an *attribute type* and one or more *attribute values*. An example of an attribute type might be “telephone number,” and an example of a telephone number attribute value might be “425-707-9790.”

**Object**
An *object* is a particular set of attributes that represents something concrete, such as a user, a printer, or an application. The attributes hold data describing the thing that is identified by the directory object. Attributes of a user might include the user’s given name, surname, and e-mail address. The classification of the object defines which types of attributes are used. For example, the objects classified as “users” might allow the use of attribute types like “common name,” “telephone number,” and “e-mail address,” while the object class “organization” allows attribute types like “organization name” and “business category.” An attribute can take one or more values, depending on its type.

Every object in Active Directory has a unique *identity*. Objects can be moved or renamed, but their identity never changes. Objects are known internally by their identity, not their current name. An object’s identity is a globally unique identifier (GUID), which is assigned by the Directory System Agent (DSA) when the object is created. The GUID is stored in an attribute, *objectGUID*, that is part of every object. The *objectGUID* attribute can’t be modified or deleted. When storing a reference to an Active Directory object in an external store (for example, a database), use *objectGUID* because, unlike a name, it won’t change.

**Container**
A *container* resembles an object in that it has attributes and is part of the Active Directory namespace. However, unlike an object, a container doesn’t represent anything concrete. It is a holder of objects and of other containers.

**Tree and Subtree**
A *tree* in Active Directory is just an extension of the idea of a directory tree. It’s a hierarchy of objects and containers that demonstrates how objects are connected, or the path from one object to another. Endpoints on the tree are usually objects.

A *subtree* is any unbroken path in the tree, including all the members of any containers in that path. Figure 2-1 shows a tree structure for microsoft.com. Any of the unbroken paths
(for example, from nw.sales.seattle.microsoft.com to microsoft.com) is a subtree. Trees and forests are discussed in more detail in Chapter 3.

![Tree structure with subtrees](image)

**Distinguished Name**

Every object in Active Directory has what’s called a *distinguished name* (DN). In this context, “distinguished” means the qualities that make the name distinct. The DN identifies the domain that holds the object as well as the complete path through the container hierarchy used to reach the object. A typical DN might be CN=Charlie Russel, OU=Engineering, DC=example, DC=local. This DN identifies the “Charlie Russel” user object in the Engineering OU, in the example.local domain.

*Note*  
CN translates as common name, OU stands for organizational unit, and DC means domain controller. Some attributes are derived from the X.500 model; an administrator can define others.

Active Directory also uses a *relative distinguished name* (RDN), which is the part of the DN that is an attribute of the object itself. In the previous example, the RDN of the user object is CN=Charlie Russel. The RDN of the parent object is OU=Engineering.

The “DC=” portion of a DN allows X.500 directories to plug in to the DNS namespace, which is also what Active Directory does. The root of the global namespace for Active
Directory is the DNS namespace. Thus, DNS domain names merge within the Active Directory naming scheme. For example, example.local is a valid, internal, DNS domain name and can be the name of an Active Directory domain as well. This DNS integration means that Active Directory fits naturally into Internet and intranet environments. Active Directory servers can be connected directly to the Internet to simplify secure communications and electronic commerce with customers and partners.

**Schema**

“Schema” is a term commonly used in database work. In the context of Active Directory, the schema is definitions of all the pieces that make up your Active Directory: the objects, attributes, containers, and so forth. Active Directory has a default schema that defines the most common object classes, such as users, groups, computers, OUs, security policies, and domains.

The Active Directory schema can be updated dynamically. That is, an application can extend the schema with new attributes and classes and use the extensions immediately. Creating or altering the schema objects stored in the directory causes schema updates. ACLs protect schema objects so that only authorized users (members of the Schema Admins group) can modify the schema.

---

**The Active Directory Architecture**

As mentioned previously, Active Directory isn’t, strictly speaking, an X.500 directory service, although like all existing directory services, it’s derived from that standard. The sections that follow enumerate some characteristics of the Active Directory architecture.

**The Directory System Agent**

The DSA is the process that provides access to the physical store of directory information located on a hard disk. The DSA is part of the Local System Authority (LSA) subsystem in Windows Server 2003 and Windows 2000. Clients access the directory information using one of the following mechanisms:

- LDAP clients connect to the DSA using LDAP. Active Directory supports LDAP v3, defined by RFC 2251; and LDAP v2, defined by RFC 1777. Clients of Microsoft Windows 2000 or later, and clients of Microsoft Windows 95, Windows 98, and Windows Me with the Active Directory client components installed use LDAP v3 to connect to the DSA.

- Messaging Application Programming Interface (MAPI) clients, such as Microsoft Exchange, connect to the DSA using the MAPI remote procedure call (RPC) interface.
Windows clients that use Windows NT connect to the DSA using the SAM interface.

Active Directory DSAs connect to each other to perform replication using a proprietary RPC interface.

**Naming Formats**

Active Directory supports several name formats to accommodate both users and applications:

- **RFC 822 names**  Familiar to most users as Internet e-mail addresses, such as crus-sel@example.local. Active Directory provides a “friendly name” in RFC 822 form for all objects. Thus, a user can use a friendly name both as an e-mail address and as the name used to log on.

- **HTTP URLs**  Familiar to most users who have Web browsers. A typical Uniform Resource Locator (URL) takes the form http://domain/path-to-page, where domain refers to a server running Active Directory services and path-to-page is the path through the Active Directory hierarchy to the object of interest. The URL for Charlie Russel is http://AServer.example.local/Division/Product/Engineering/charlie.russel.

- **LDAP names**  More complicated than Internet names but usually hidden within an application. LDAP names use the X.500 attributed naming convention. An LDAP URL specifies the server holding Active Directory services and the attributed name of the object—for example, ldap://AServer.example.local/CN=charlie.russel,OU=engineering,OU=Product,OU=Division,O=MegaIntl,C=US.

- **UNC names**  The Uniform Naming Convention used in networks based on Windows Server 2003 servers to refer to shared volumes, printers, and files—for example, \example.local\Division.Product.Engineering.Volume\WordDocs\aprilreport.doc.

**The Data Model**

The Active Directory data model is derived from the X.500 data model. The directory holds objects that represent various items, described by attributes. The universe of objects that can be stored in the directory is defined in the schema. For each object class, the schema defines what attributes an instance of the class must have, what additional attributes it can have, and what object class can be a parent of the current object class.
Schema Implementation

The Active Directory schema is implemented as a set of object class instances stored in the directory. This is very different from directories that have a schema but store it as a text file that is read at startup. Storing the schema in the directory itself has many advantages. For example, user applications can read it to discover what objects and properties are available.

The Security Model

Active Directory is part of the Windows Server 2003 and Windows 2000 trusted computing base (TCB) and is a full participant in the security infrastructure. The distributed security model is based on the MIT Kerberos authentication protocol (version 5). Kerberos authentication accommodates both public-key and private-key security, using the same ACL support model as the underlying Windows Server 2003 operating system. ACLs protect all objects in Active Directory. They determine who can see the object, what attributes each user can see, and what actions each user can perform on the object. If a user is not allowed to see an object or an attribute, the fact of its existence is never made known to that user.

An ACL, in turn, is made up of access control entries (ACEs) stored with the object the ACL protects. In Windows 2000 and Windows Server 2003, an ACL is stored as a binary value, called a security descriptor. Each ACE contains a security identifier (SID), which identifies the principal (user or group) to which the ACE applies and provides information about what type of access the ACE grants or denies.

ACLs on directory objects contain ACEs that apply to the object as a whole and ACEs that apply to the individual attributes of the object. This allows an administrator to control not just which users can see an object, but also what properties those users can see. For example, all users might be granted read access to the e-mail and telephone number attributes for all other users, but access to the security properties of users might be denied to all but members of a special security administrators group. Also, individual users might be granted write access to personal attributes such as the telephone and mailing addresses on their own user objects.

Active Directory is the store for the security system, including user accounts, groups, and domains. This store replaces the registry account database and is a trusted component within the LSA.
Delegation and Inheritance

Delegation is one of the most important security features of Active Directory. An administrator can authorize a user to perform a specified set of actions in some identified subtree of the directory. This is called delegated administration. Delegated administration allows very fine-grained control over who can do what and enables administrators to delegate authority without granting elevated privileges. This also eliminates the need for domain administrators with broad authority over large segments of the user population.

Administrators grant rights for specific operations on specific object classes by adding ACEs to the container’s ACL. For example, to allow user Charlie Russel to be an administrator of the Engineering OU, you add ACEs to the ACL in Engineering as follows:

"Charlie Russel";Grant ;Create, Modify, Delete;Object-Class User
"Charlie Russel";Grant ;Create, Modify, Delete;Object-Class Group
"Charlie Russel";Grant ;Write;Object-Class User; Attribute Password

Now Charlie Russel can create new users and groups in Engineering and set the passwords for existing users, but he can’t create other object classes and he can’t affect users in other containers (unless, of course, ACEs grant him that access in the other containers).

Inheritance allows a given ACE to be propagated from the container in which it was applied to all children of the container. Inheritance can be combined with delegation to grant administrative rights to a whole subtree of the directory in a single operation.

Naming Contexts and Partitions

Active Directory is made up of one or more naming contexts or partitions. A naming context is any contiguous subtree of the directory. Naming contexts are the units of partitioning. A single server always holds at least three naming contexts:

- The schema
- The configuration (replication topology and related data)
- One or more user naming contexts (subtrees containing the actual objects in the directory)

The Global Catalog

The DN of an object includes enough information to locate a replica of the partition that holds the object. Many times, however, the user or application does not know the DN of the target object, or which partition might contain the object. The global catalog (GC) allows users and applications to find objects in an Active Directory domain tree, given one or more attributes of the target object.
The global catalog contains a partial replica of every naming context in the directory. It contains the schema and configuration naming contexts as well. This means that the GC holds a replica of every object in Active Directory, but with only a small number of their attributes. The attributes in the GC are those most frequently used in search operations (such as a user’s first and last names, login name, and so on) and those required to find a full replica of the object. The GC allows users to quickly find objects of interest without knowing what domain holds them and without requiring a contiguous extended namespace in the enterprise.

The global catalog is built automatically by the Active Directory replication system. The replication topology for the GC is also generated automatically. The properties replicated into the GC include a base set defined by Microsoft. Administrators can specify additional properties to meet the needs of their installation.

In Windows 2000, when processing a logon event for a user in a native-mode domain, a domain controller has to contact a Global Catalog (GC) server to expand a user’s Universal Group membership. This means that users in a remote office can experience logon failures if the network connection to the rest of the organization is cut off.

In Windows Server 2003, domain controllers can be configured to cache Universal Group membership lookups when processing user logon events, so users can log on even when a GC isn’t available. Specifics on the administration and deployment of Active Directory can be found in Chapter 14 and Chapter 15.

Summary

As you have no doubt gathered, Active Directory is a powerful tool and, like most powerful tools, it can be the source of great trouble if mishandled. Allow time for careful thought and planning before deploying Active Directory. First to be considered is the design of a logical and efficient directory. A poor tree design can negatively affect the productivity and even the stability of the network. Chapter 3 covers how to plan your namespace and domains for both maximum utility and longevity.
Chapter 3
Planning Namespace and Domains

Analyzing Naming Convention Needs.................................29
Planning a Domain Structure..............................................36
Planning Multiple Domains................................................40
Summary.............................................................................42

Few places in your conversion to Microsoft Windows Server 2003 provide more potential for long-term trouble than the initial design of your namespace. This is definitely a case of pay me now or pay me later—so spend some time and energy up front—you’ll be well and thoroughly repaid later with reduced support costs, more flexibility, and less reorganization.

Planning the namespace of a large or even medium-sized organization is an iterative process. You won’t get it right the first, or probably even the second, time. But you need to start somewhere and then consult and collaborate with key players in your organization, and refine and consult again until you have a namespace that will work for your organization. As you work through the process, many of the opinions you receive will be based on company politics and personal agendas, making the whole process more difficult than it should be. Your job is to understand and protect the best interests of the organization as a whole.

Analyzing Naming Convention Needs
To plan your namespace and domain structure, you need to analyze your organization and attempt to understand its underlying naming needs. This requires both a thorough understanding of the type of organization you have and who the players are as well as some educated guesses about where the organization is going.

Trees and Forests
There are two basic namespace types—tree and forest. By understanding the differences between these models, and how they align with your organization, you can choose the model that best reflects the needs of your organization. While it is possible to change
models later, it requires considerable effort and will have an impact on the overall use of names in the namespace. So spend the time here to understand what your organization really needs—which can be different from what the organization thinks it wants.

**Trees**

A tree namespace, like that shown in Figure 3-1, is a single, contiguous namespace, with each name in the namespace directly descended from a single root name. This straightforward naming design is appropriate for an organization that is essentially cohesive and has a single name underlying what can be many divisions and diverse businesses. Many small to midsize businesses fit well within this model. Even very large businesses might be a comfortable fit for a tree structure if the organization is fairly centralized and has a single recognizable name.

![Figure 3-1](image)

**Figure 3-1** A tree structure yields a single, contiguous namespace, with all names derived from a single root

As you can see from the figure, with a tree-structured namespace, each branch of the tree has a name that is directly descended from the root of the tree. This structure makes it easy to find any leaf or branch of the tree by tracing down the structure of its name.

**Forests**

A forest namespace, like that shown in Figure 3-2, is a collection of essentially equal trees, with no single root to the namespace. The forest namespace is appropriate for an organization that has multiple lines of business, each with its own separate and identifiable name. These are usually larger businesses, especially those that have grown by acquisition. They typically don’t have a single, central Information Systems group that manages the
entire organization, and each of the divisions for the most part has a separate identity and infrastructure.

As you can see from the figure, with a forest namespace you have a peer group of trees, each its own contiguous namespace, but the trees do not fit into an overall, contiguous namespace. In other words, you can’t directly trace the names of all the leaves back to a single root.

**Figure 3-2**  A forest is a collection of individual trees that are not part of a contiguous namespace

Defining a Naming Convention

Whether you’re going to have a single tree or a forest of trees for your overall namespace, you first need to decide what to name the various branches of the tree. These are probably the most delicate and politically sensitive decisions you have to make as you lay out your overall naming structure. Be prepared to suffer through some long and painful meetings as you get the critical players involved in the decision process. Nevertheless, spend the time to do this—it will save you untold amounts of grief later.

There are essentially two types of naming conventions—organizational and geographical. Both have their proponents, and an argument can be made for either choice. Keep in
mind that people can get amazingly emotional about what their division or department is called and about its relative weight in the organization. Such political disagreements can be not only bitter but also prolonged beyond any reasonable expectation.

The Organizational Naming Convention
Using an organizational naming convention, you model your namespace on the way your company or organization is structured. Thus, the root of your tree might be microsoft.com, with the first level under that consisting of admin.microsoft.com, finance.microsoft.com, mfg.microsoft.com, eng.microsoft.com, and so forth.

The following list shows some advantages and disadvantages of an organizational model:

Advantages
- Reflects company organization
- Is easily understood
- Has a natural growth path
- Permits resources to be organized by business function

Disadvantages
- Is difficult to adjust when organizational structures and names change
- Can be politically sensitive
- Is difficult to support as divisions split and merge
- Can be difficult to implement if divisions of the organization have multiple geographical locations

Real World Sites
Sites, provided by the Active Directory service, can be used to reduce or eliminate the problem the organizational naming structure has with divisions that have multiple locations. A company can create a site for each island of computers with local area network (LAN) connectivity. For example, the main office would be one site while a branch office would be another site. Any domains that span more than one site automatically adjust their replication parameters to optimize the use of the slow wide area network (WAN) link between the sites. Clients are also automatically directed to local domain controllers for service requests, further decreasing the use of your WAN links. For more information about sites and planning your site topology, see Chapter 6.
The Geographical Naming Convention

Using a geographical naming convention, you model your namespace on the geographical divisions of the organization. For example, with the same root of microsoft.com, you might have a first level consisting of noram.microsoft.com, europe.microsoft.com, asia.microsoft.com, africa.microsoft.com, and so on. Underneath this first level, you might break each entry down to the individual country or state/province, depending on the size and complexity of your organization.

The following list shows some advantages and disadvantages of the geographical naming convention:

**Advantages**
- Is apolitical in nature
- Uses names that tend to be persistent
- Offers greater flexibility and granularity

**Disadvantages**
- Doesn’t reflect the nature of the organization
- Might require additional domains to meet security needs

---

**Note**  
Sites can be useful for optimizing the use of slow WAN links on networks using a geographical naming convention. Although there usually aren’t any domains that span multiple sites in networks using the geographical naming convention, using sites further optimizes the use of WAN links by tuning interdomain replication of Active Directory.

Mixed Naming Conventions

Finally, you can opt to use a mixture of the organizational and geographical naming conventions, especially in a forest namespace where different corporate cultures have grown up and have their own agendas. The catch, of course, is that this can lead to confusion and make support more difficult because there is no consistency in how things are done. You should make every effort to rationalize the structure of your namespace when you create it. Your overall support job will be easier in the end.

Even if you adopt a purely geographic naming convention across the whole organization, chances are you’ll find it advantageous at the lowest level of the tree to create organizational units (OUs) or domains that reflect the different business functions of the organization. This is because groups working in similar areas or on related projects tend to need access to resources of a similar nature. The needs on the manufacturing plant floor are different from those in accounting, for example. These common needs identify natural areas of administrative support and control.
Determining Name Resolution

After defining your naming convention, the second decision you need to make is whether you want the namespace you use internally to be the same as the one you present to the outside world. While your initial expectation might be that they should be the same, there can be compelling reasons for using different internal and external namespaces.

Using the Same Internal and External Namespaces
When you have a single namespace, you and your machines have the same names on the internal network as they do on the public Internet. This consistency means you get a single name from the appropriate Internet registration authority and you maintain a single Domain Name System (DNS) namespace, although only a subset of the names is visible from outside the company. Your network structure will end up looking something like Figure 3-3.

When you use the same name for internal and external namespaces, you must ensure that the ability to resolve names from outside your company is limited to machines outside your firewall that are supposed to be externally visible. Make sure that no Active Directory servers reside outside the firewall. However, you also need to make sure your internal machines can resolve names and access resources on both sides of the firewall.

Figure 3-3  With the same internal and external namespace, your DNS must have different zones depending on where the request is coming from.
The following list shows some advantages and disadvantages of using the same internal and external namespace:

**Advantages**
- Provides consistent naming internally and externally
- Allows single name registration
- Enables users to have a single logon identity and e-mail identity

**Disadvantages**
- Needs a complex proxy server configuration
- Requires maintenance of different zones with the same names
- Requires that users be aware of the different views they’ll have of resources, depending on where they are accessing the resources from

**Using Different Internal and External Namespaces**
If you set up different internal and external namespaces, your public presence might be microsoft.com, while internally you use msn.com. All resources that reside outside the company network have names that end in microsoft.com, such as www.microsoft.com. Within the company network, however, you use a separate namespace that has msn.com as its root, as shown in Figure 3-4.
With different internal and external namespaces, your DNS names for machines that are publicly available are different from those that are visible only from inside your firewall. One consideration with this scenario: you must register both the public and private names with the appropriate Internet name registration authority. You might think you don’t need to register the internal-only name because you don’t intend to expose it to the public Internet. What you’re really doing, however, is making sure no one else uses the same name because this can cause name resolution problems for your internal clients.

**Note** One way around the problem of an internal-only name, especially where you might have difficulty gaining control of the domain name because it’s legitimately owned by someone else, is to use a nonexistent root domain name for it, such as .lan (for example, microsoft.lan). This strategy lets you have an internal name that is appropriate for that portion of the namespace without running into a conflict with someone else’s domain name.

The following list shows some advantages and disadvantages of using different internal and external namespaces:

**Advantages**
- Provides a clear distinction between what is internal and what is external
- Offers easier management and proxy configuration
- Makes it easier for users to understand the differences between the internal and external namespaces

**Disadvantages**
- Requires that two names be registered
- Means that users’ logon names are different from their e-mail names

**Planning a Domain Structure**

After you settle on the overall design of your namespace, you need to design your domain structure to support it. Each branch of the namespace can be broken down to either a domain or an OU. Whether a branch is a domain or an OU depends on a variety of considerations, including the need for replication, security policy, resource availability, quality of the connection, and so forth.

**Domains vs. Organizational Units**

Windows Server 2003 network trees are made up of domains and OUs. Each provides for administrative boundaries between branches on the tree, but they have different implications and resource requirements.
Domains
The core unit of the Windows Server 2003 Active Directory is the domain, just as it is in Windows 2000 and Microsoft Windows NT 4. All network objects exist as part of a domain, and the security policy is uniform throughout a domain. Unlike Windows NT, security in Windows 2000 and Windows Server 2003 is based on Kerberos version 5, and the trust relationships are transitive. This means that if domain A trusts domain B and domain B trusts domain C, then domain A also trusts domain C.

Planning One-way Windows NT 4–style trust relationships can still be set up. More importantly, the relationships between Windows 2000 and Windows Server 2003 domains and legacy Windows NT domains are based on the one-way, non-transitive trust relationships inherent in Windows NT. It is essential that you consider these relationships when planning your domain structure.

Starting with Windows 2000, the concept of a primary domain controller (PDC) and one or more backup domain controllers (BDCs) is finally history. Domain controllers in Windows 2000 and Windows Server 2003 are multi-master and peer-based. Each controller of a domain has identical authority over the domain, and if any controller goes offline, the others continue to administer and authenticate the domain. Any domain controller can originate a change to the domain and then propagate the change to the other domain controllers in the domain.

Note Although all domain controllers are created equal in Windows Server 2003, one is more equal than the others if you’re still supporting Windows NT computers on your domain (for example, you’re running in a domain or forest functional level that supports Windows NT 4 domain controllers). In this special case, one domain controller emulates the Windows NT 3.x and Windows NT 4 primary domain controller (PDC) functionality. By default, the first domain controller in a domain gets this job, but you can transfer the PDC Emulator role to another domain controller if you need to. See Chapter 15 for more details about this and other Operations Master roles in the domain.

The domain is also the unit of replication within Active Directory. Changes in the domain are replicated throughout the domain, even when the domain spans multiple sites or locations. This allows domain controllers at distant sites to originate changes to the domain and have the changes replicated across the domain.

Although access rights are transitive across domain boundaries, administrative rights are, by default, limited to the domain. This allows you to grant administrative rights to a key user in a particular domain without worrying about compromising the overall security of the organization, because the administrative rights stop at the domain boundary unless explicitly granted to other domains.
Organizational Units
The OU concept was first introduced in Windows 2000. It has some of the characteristics of a domain, but without the resource overhead of one. An OU is contained within a domain and acts as a container for directory service objects. It forms a branch of the contiguous LDAP namespace (though not necessarily of the DNS namespace), and it can in turn contain other OUs. Thus, the domain corp.microsoft.com can contain other domains, such as finance.corp.microsoft.com, and it can also contain OUs such as the “hr” OU of corp.microsoft.com. Here, the LDAP name would be: “OU=hr,DC=finance,DC=corp, DC=microsoft,DC=com”, but the DNS name, unless explicitly changed, would still be corp.microsoft.com.

The OU provides a convenient administrative boundary, and rights and privileges for administration can be granted to users in an OU without compromising the rest of the domain. However, an OU does not require a separate domain controller, nor is it involved in replication.

The closest analogy to an OU from the Windows NT domain model is the resource domain, but without the domain controller overhead that was required under Windows NT. In cases where there is no particular need for a separate security policy for a given administrative container, the OU provides an appropriate and less resource-intensive boundary.

Designing a Domain Structure
After you design your namespace and everyone involved agrees to it, you’re ready to start designing and implementing your domain structure. The design of your domain structure will closely match the design of your namespace, though you might make a decision that certain namespace boundaries require only OUs, not full domains. Base your choice between an OU and a domain on whether you need a separate security policy (for example, a policy defining account lockout or password complexity) for the entities within the namespace boundary. If a particular namespace boundary doesn’t require a security policy that is different from that of its parent, you’ll probably find an OU to be an appropriate division because it requires fewer resources to implement.

Designing a Single Domain Tree Structure
To create a single, contiguous namespace and therefore a pure domain tree structure, create the domains in hierarchical order, starting at the top of the tree. This top domain is your root domain and has either all the users in it (for smaller, single-domain models) or no users at all (if you use a structural domain as the root domain). For those familiar with the Windows NT 4 domain models, this structure roughly corresponds to the “single
master” domain model, with one important difference. Users need not, and most often should not, reside in a single-master domain, but should reside in their actual appropriate place in the domain hierarchy.

As you branch down the tree of your namespace, you create domains or OUs for each branch of the tree. The decision about whether to create an OU or a domain controller depends on your overall security model, the quality of the connection to the location, and a variety of other factors, including political considerations from the original namespace planning.

---

**Note**  The single tree structure described here is also a forest—a forest with a single tree in it, but a forest nonetheless.

---

### Designing a Multiple Domain Tree Structure

The forest of trees structure is most often used to accommodate an existing namespace that is noncontiguous and can’t easily be made contiguous. You end up with multiple root domains, all on the same level. Below each of these root domains is a contiguous namespace for that tree. Each branch of the LDAP namespace is either a domain (with its attendant requirement of one or more domain controllers) or an OU. You generally create each tree from the top down, and each branch of the tree automatically has a transitive trust relationship with the other branches of the tree.

All trees in a forest share the same schema, configuration, and global catalog, with transitive Kerberos trust relationships among all domains in the forest. The trust hierarchy within each tree follows the DNS naming hierarchy. The trust hierarchy in the forest as a whole, however, follows the order in which trees are joined to the forest, with two-way, transitive trusts created between each pair of trees in the forest. This is transparent to the users but can be modified by the administrator to improve management and referrals.

### Domain Security Guidelines

Within each domain, the security requirements, policy, and configuration are consistent. If you need to change the security requirements and policy for a subunit within a domain, create that subunit as a child domain, not as an OU. Keep this limitation in mind as you plan your overall namespace—you need a separate branch of the namespace to have a separate security policy.
What is meant by security policy? What does it entail? Part Four deals exclusively with security matters, so for the moment, here is a summary of what the security policy includes:

- Logon requirements
- Certificates
- Password-aging and minimum-length requirements
- Smart card or other authentication add-ons
- Machine and time-of-day restrictions

Many of these security measures will be the same throughout your organization, but there can be certain areas that require significantly greater security than that needed in the rest of the organization. If so, plan for areas that require extra care to be in a separate domain so that their more restrictive security isn’t imposed on the entire organization.

Creating Organizational Units

In situations where you don’t need to create separate domains for security reasons but do want to be able to delegate administrative functions, create a separate OU instead of a child domain. Thus, you might have a domain called noram.example.com that you want to divide into business units within the region. You can create separate sales, support, education, human resources, manufacturing, and finance domains under noram.example.com. However, the overhead of separate domains (and their required controllers) for each of these units isn’t necessary—primarily because they all share a single security policy. So, simply create OUs for each of them. If you later need to convert one or more of them to a domain, you can, though the process is not as simple as it should be.

OUs make useful boundaries for administrative purposes. Various administrative tasks and privileges can be delegated to the administrator for a specific OU, freeing up the domain administrator and giving the OU local control of its own resources.

Planning Multiple Domains

When your organization is complex enough, or simply large enough, that you know you’ll have to create multiple domains, spend the extra time up front planning exactly how to implement them. Time spent on the front end will be paid back later 10 times over.

Draw your planned domain structure, and compare it to your planned (or existing) namespace. Decide what simply must be a domain and what can comfortably be an OU. Identify which servers are to be your domain controllers. Keep in mind that the concepts of PDC and BDC from Windows NT are gone. All servers within a domain are of equal
weight and importance. Changes made to any domain controller are propagated to all other controllers within the domain. If simultaneous changes are being made against multiple controllers, Active Directory uses update sequence numbers and the time-stamps of the changes to resolve any conflicts.

**Planning a Contiguous Namespace**

When planning a contiguous namespace, and thus a single tree forest structure, you first create the root domain for the namespace. In this namespace, create the primary administrative accounts but leave the creation of other accounts until later. User and machine accounts should reside in the leaf of the tree where they are going to do the majority of their work. This arrangement is the opposite of Windows NT where, if you were running multiple domains, you often had to create all your user accounts at the highest level of the domain because of the nature of trust relationships.

If you’re migrating from an existing Windows NT environment, you might have your users in a single-master or multiple-master domain. You can continue this arrangement, and it might be the easiest way to migrate from an existing environment. See Chapter 6 for a more detailed discussion about upgrading domains.

**Determining the Need for a Multi-Tree Forest**

If you already have an environment with multiple root domains, or one without a contiguous namespace, you have to create a multi-tree forest rather than a single forest, single tree environment.

The first step is to take a long, hard look at your noncontiguous namespaces. Is there any opportunity to consolidate them into fewer contiguous namespaces? Now is definitely the time to do this. It’s much harder to consolidate them later, and you’ll have a harder political battle as well.

**Creating the Forest**

If you decide there is simply no way to get to a single, contiguous namespace, meaning you need to create a multi-tree forest, decide exactly where the root of each tree in the forest will reside. Think about the physical locations of your potential domain controllers, the layout of your network, the bandwidth to various sites, and the current existence of Windows NT 4 domains and controllers. After you have a good physical and logical map of your network, you’re in a position to plan your domain strategy.
Create your root-level domains first and then start building your trees. This order isn’t an absolute requirement—if you miss a tree or something changes, you can go back and add another tree to your forest. However, it’s generally better to create the roots first, if only to get your tree-to-tree trusts in order.

**Note** After you create the root of a tree, you can’t easily rename or delete it. In Windows Server 2003, you can change domain names using Rndom.exe, but it’s not a task to undertake frequently. So don’t rush into settling on a domain structure—planning it in detail will save you headaches in the long run.


**Summary**

Planning your namespace and domain structure is an essential first step to a successful implementation of Windows Server 2003. It is an iterative process that requires careful planning and a clear understanding of the political realities in the organization. A Windows Server 2003 namespace can have a single, contiguous and hierarchical structure with a forest that is a single tree, or it can be a forest of multiple trees in a noncontiguous namespace. All domain controllers within a domain have the same authority over the domain, and there can be multiple OUs within a domain for delegation purposes. In Chapter 4, you continue to focus on planning; in Chapter 5, you move from planning your installation to actually doing it.
Chapter 4
Planning Deployment

How Information Technology Functions .......................... 44
Identifying Business Needs .......................................... 45
Assessing Current Systems .......................................... 46
Making a Roadmap ..................................................... 49
Summary .................................................................... 52

Contrary to what some system administrators we’ve worked with seem to think, the first step in deployment is not inserting a CD into a brand new server. Inserting the CD is really the last, and easiest, stage of the deployment process, when you've already done all your homework. The real work of deployment is all the planning and negotiating and preparing that comes first.

Deployment involves a good deal more than merely installing an operating system, even a network operating system. We’ll get to the specifics of deployment—application installation and configuration, file and print services, the Active Directory service, communications, security, and other functions—in later chapters. In this chapter, we’ll deal with the work that must be done before that first CD-ROM is ever inserted into a drive—planning the hardware and software infrastructure on which your Microsoft Windows Server 2003 network will be based.

Successful deployment of a network depends primarily on planning. Successful planning, in turn, depends on gathering and analyzing data as well as doing a certain amount of prophesizing and just plain old guessing about what the future of the organization will be. The decisions you make during the early stages of deployment will have your fingerprints all over them, for good or ill. Your vision of the future will prevail for years to come in the operation of the organization, and you’ll undoubtedly be held accountable if the vision turns out to be a nightmare. Therefore, the more planning you devote to deployment, the better off everyone will be.

Three elements are essential for an effective Information Technology (IT) strategy:

- An analysis of how your business requirements and IT capabilities match up today. Where is your technological structure adequate, and where is it lacking?
A projection of your business and IT goals. You need one-year, three-year, five-year, and ten-year plans for business needs, and the IT functionality and services to meet those needs.

A roadmap that provides a path to your business and IT goals.

This chapter discusses all three of these elements and examines how they are interrelated.

Planning  For a more detailed approach to planning deployment of Windows Server 2003, see the volume titled “Planning, Testing, and Piloting Deployment Projects” from the Microsoft Windows Server 2003 Deployment Guide. This guide can be obtained from Microsoft Press and is also available online at http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/DepKit/c283b699-6124-4c3a-87ef-865443d7ea4b.mspx.

How Information Technology Functions

Most people agree that the purpose of an IT department is to serve current business needs as well as to advance long-term goals. Unfortunately, this isn't always clear, for a variety of reasons. Sometimes, communication is poor. Often, no one has given much thought to what it takes, technically speaking, to serve business needs. Many networks appear to have sprouted like mushrooms after a rain, without the benefit of anything resembling an overall vision. Changing the situation is complicated by a number of factors:

- Legacy hardware and software
- Incompatible operating systems and applications that were adopted to solve specific divisional or departmental problems
- Rapidly changing technologies and user requirements
- Resistance to change by those who have grown comfortable with older technologies
- Too little staff, time, and money to plan and execute a network upgrade

This last item is virtually universal. However, if these factors plague your organization, it's time to start struggling against the status quo. The situation can't and won't change overnight, but a carefully thought-out plan with clear priorities can do a great deal to move things forward.
## Identifying Business Needs

Identifying business needs is a topic of such scope that it can seem overwhelming. A good place to start is with individual departments or areas. For example, consider the needs of your sales, human resources, and marketing departments. What does each area need to do now, and what services will be of benefit in the future?

Consider basic operations (such as accounts payable and inventory) that have to be taken care of daily, as well as less frequent operations (the launching of a new product). What kinds of flexibility need to be built into the IT systems? What sorts of changes must be anticipated to deal with increased Internet activity or increased access for users in remote locations?

The research you perform into the organization’s business requirements can also help you overcome resistance—and there’s always some resistance—to changes in the infrastructure. As people participate in your research and share your understanding of the organization’s current issues and opportunities, more of them will come to have a personal stake in supporting your Windows Server 2003 deployment.

## Getting Specific

Start with a list, ranked in order of importance, of enterprise functions that are necessary to meet your organization’s business goals. Include in that list the following items:

- A total cost of ownership (TCO) analysis identifying potential areas where upgrades to the IT infrastructure can result in cost reductions
- A return on investment (ROI) analysis identifying the financial opportunities that can result from upgrades to the IT infrastructure
- Additional business that can result from the infrastructure upgrade
- Potential risks from not updating the IT infrastructure

### Planning

These are complicated issues with much overlap, so you might have to construct this list more than once. Depending on the size of your operation, it might be easier to subdivide the list into manageable bites, each one of which constitutes a project of its own, with the sum of these smaller lists creating an overall planning and justification framework for the entire organization.

**Seeing into the Future**

To make your network successful, you need to take a high-level look at where your organization will be in one, three, five, and even ten years. Will the organization become more centralized or less? Will it expand geographically, or will it contract? Will you have more knowledge workers who require the free flow of information on networks to do their jobs? Will you need to deal with “boundaryless” workers who spend time in the office but who also telecommute, belong to virtual teams, or even work in their clients’ offices? Workers with such needs can make the usual means of information distribution completely inadequate. How will these workers get what they need? How will you balance conflicting demands for access and security?

Computer networks themselves are subject to rapid change because the experience of working on a network changes users’ perceptions of what is possible and therefore their view of what is needed. After it’s possible to have access to real-time sales figures or inventory counts, the demand for access grows rapidly.

Even modest changes can have a substantial impact on your IT infrastructure. By anticipating changes and planning for them, you ensure that your network can evolve to meet future needs.

**Assessing Current Systems**

It’s a rare company that has a complete inventory of its hardware and software. It’s an even rarer company that knows the rate at which its hardware and software infrastructure changes. Grand goals for the future can’t be met without knowing the facts about the present. Even if you’re sure you want to go to Chicago, you don’t have much hope of getting there unless you know whether you’re currently in Savannah or Seattle. The sections that follow detail the steps for analyzing what you have so that you can determine what you need and how to implement changes.

**Documenting the Network**

Knowing what hardware and software you have deployed and how that equipment is being used is vital when designing your network and determining the best way to implement it. After all, you’re probably not tearing out the entire current network and replacing it with brand new, state-of-the-art equipment. (And if you are, that’s not as easy as it sounds, either.)
Instead, you’ll likely be phasing out or repurposing legacy hardware and software over a period of weeks or months, even years. During this time, the existing hardware and software will still have to be supported. A careful and thorough audit of your existing network can be of great use in determining where potential problems (and opportunities) lie.

The Organizational and Physical Infrastructure
Make a drawing of the physical network, including workstations, servers, routers, wiring closets, and hubs. This picture will clarify where the network can be expanded (and where it can’t), the best traffic routing, and whether servers and other hardware are optimally placed. At the same time, an organizational chart showing all members of the IT staff and the responsibilities assigned to each one can help clarify lines of communication and show where they might be lacking. Make sure all critical tasks are assigned at every site, organizational unit (OU), or location. You don’t want to establish a server at a remote location and have no one there who can manage anything beyond a reboot.

Traffic Patterns
Gather network traffic reports to determine the optimum placement of routers, hubs, and switches; bandwidth requirements for workstations and workgroups; and future needs for network management software. Network analysis utilities are available to help you determine your overhead (or background) network traffic. Traffic patterns are also important in determining appropriate wide area network (WAN) connectivity speeds or the speed to be used on risers connecting floors in a building.

Network Addresses
As you upgrade the network using Active Directory, you’ll probably be assigning new network names to most of the nodes on the network. Add the node addresses to the hardware drawing you made earlier so that you can analyze what addresses to assign and what steps will be necessary to make the transition from the old naming system to the new one.

Operating System Connectivity
Many networks might still have Microsoft Windows NT connected to other operating systems such as UNIX and NetWare. You’ll need to determine what tools are necessary to maintain the connectivity you want or migrate these platforms to Windows Server 2003. In addition, hardware placement—routers, switches, and gateways—can all be critical to optimum connectivity and might need upgrading as well.

External Connectivity
Just as most companies don’t know what hardware they have, many networks have undocumented external connectivity. Most know about their Internet, WAN, and fax services, but often there are completely undocumented telephone lines used for dial-up networking or remote network management. Document all connections.
Existing Network Operating Systems
Documenting the operating system on each server and workstation on the network is an essential ingredient to a successful operating system upgrade or migration. You’ll need to determine what the upgrade or migration must support and what preparatory steps are needed.

Existing Applications and Services
You’ll need an inventory of all the software running on all servers and workstations. When you have this list, take a closer look at both the typical resource requirement for each program, as well as the atypical requirements. For example, a particular program might generate a modest amount of traffic most of the time except for weekly downloads of 200 MB from a WAN server, and the accounting department’s requirements are vastly different at year end than they are in midquarter. Where applications are running on servers or operating systems that you will be migrating, make sure you understand the migration path for the application as well as the operating system.

In addition, subdivide and classify the inventory of applications and services into the following categories:

- **Strategic** Software and services that are essential to business operations and that have the most relevance to current and future goals.
- **Tactical** Applications and services that are valuable to the business but that are not providing optimal benefit.
- **Legacy** Software and services that are still used by some groups or departments but that are nearing the end of their useful life. Your plan must call for removing these components before they fall into the obsolete category.
- **Obsolete** Applications and services that are not beneficial to the business and also are a hindrance. The goal of IT is to remove these elements as soon as possible.

Every component belongs in one of these categories, and making the assignments can clarify your thinking and help give shape to your plan. Don’t attempt to make the assignments in a vacuum, however. Involve the parts of the organization that use an application or service in the process. This is especially important if you think the application is either a legacy or obsolete application. An important part of the process of helping your users let go of those legacy applications is getting them to understand where the application fits in the overall strategic direction of the organization and getting them involved in finding a better way to solve the problem that the legacy application is there to solve.
Making a Roadmap

A study commissioned by Microsoft several years ago identified six characteristics of successful IT departments. None of these conclusions are startling, but they bear repeating. Companies with successful IT departments will do the following:

- **Make IT a business-driven line function, not a technology-driven staff function.** In other words, the function of the technology people must be firmly connected to business strategies and the everyday work that advances these strategies.

- **Base technology funding decisions on the same considerations as any other corporate expenditure.** Cost/benefit and ROI analyses must be as much a part of every IT investment decision as they are in the decision to buy a new building.

- **Insist on simplicity and flexibility throughout the technology environment.** Reduce the number of technologies and platforms deployed, and aim for maximum flexibility and ease of implementation.

- **Demand near-term business results from development efforts.** Incremental project rollouts are preferred, as is packaged software over custom software wherever possible. When custom development is necessary, focus on the 20 percent of the functionality that typically adds 80 percent of the value.

- **Drive constant year-to-year operational productivity improvements.** Measure performance against internal and external benchmarks and standards, and strive for constant improvements.

- **Aim for an IT department that is smart about business and a business organization that is smart about IT.** Simply stated, in the better-performing companies the IT and business organization work together. They speak the same language, talk to each other, and understand each other’s capabilities and needs.

These are all grand statements that are difficult to argue with in the abstract but hard to implement in the real world. However, we all have to start somewhere, and keeping these aims in mind and working toward implementing them can only benefit the enterprise overall.

After you analyze your present situation as well as the business goals you need to achieve, the next step is to design a roadmap that will take you where you want to go. The roadmap will include a definition of the goals, a risk assessment, and an implementation plan.
Defining Goals

Your deployment goals must be specific, achievable, and measurable. Spell out the problems that have to be solved and how you will address constraints such as end-user requirements, costs, schedules, and reliability.

Your plan must then address specifically what you want to accomplish at each stage and how you will measure whether you have done what you set out to do. When deploying Windows Server 2003 in a particular department, approach the task as a vendor to that department. At a minimum, you need to do the following:

- Determine who has to agree to the scope of the project and who can sign off at the end of it.
- Determine the scope of the project: what needs to be installed, what needs to be configured, and what the users need to be able to do at the end of the project. Involve as many people in the department as possible.
- Get agreement as to what will constitute completion of the project. For example, a project might be considered complete when all workstations are connected to the network with specified software installed, all users can log on, and data can be retrieved under all conditions in n seconds or fewer. Again, be specific.
- Define a method that will test all areas of the project. Get a sign-off on the method. Allow ample time for testing. Regular, short-loop testing as you go will save much time and aggravation later.
- When the project is complete, get a sign-off that it is in fact complete. Address additions and changes that were not in the original scope as a new project—a different phase of the deployment. It’s very important that every stage have a point of closure.

Some of these steps seem obvious, but it’s surprising how often people have no idea whether their upgrade to the system has actually accomplished anything and, if it has, whether the results are what was wanted and needed. All too often the IT people go away dusting their hands and congratulating themselves, while the actual “customers” are far from satisfied.

Assessing Risk

You can’t predict everything that can go wrong in a deployment, but you can be sure that something will. Typical problems include sudden changes in business needs or user requirements, costs running higher than expected, and the almost inevitable schedule slippage.
Risks can be managed proactively or reactively. Anticipating and preventing a problem is obviously better than reacting to trouble after it pops up. Take time to identify your resources and responses to each risk you identified. Then do the same for the risks that you haven’t identified ahead of time—because there will surely be something you didn’t anticipate. It might be the new server tripping a circuit breaker that you didn’t realize was overloaded or a legacy application that everyone forgot about but that is still running a critical part of the business. It might even be a key member of your team accepting a job offer two weeks before the implementation date. You won’t know what this unanticipated problem is until it’s already on top of you. But if you take the time to identify your resources and responses, you’ll still be better off than if you’re caught totally by surprise and haven’t spent some time thinking through what to do.

Few things can hurt you more during deployment than a poorly thought-out schedule. At the same time, a schedule that considers risks can go a long way toward minimizing the likelihood of serious problems. The following precautions will help you minimize schedule-related perils:

■ **Develop high-risk components first.** Any areas that are already an ongoing tangle—such as messaging or your Web server—must be developed first and independently. New components that haven’t been part of your network before must also be tested separately and understood completely before you install them where they can affect critical operations.

■ **Include a fudge factor for unforeseen circumstances.** Nothing ever works exactly as you expect. The “five-minute install” turns out to require a change in hardware to work correctly. The quick change of hardware requires a half-hour of configuration. Estimate how much time each stage of deployment will take, and then double it.

■ **Update the project plan and schedule.** When circumstances change and milestones are reached, notify everyone involved in the project by updating and distributing the plan and schedule. If you find yourself two days behind after the first stage of the deployment, don’t just plan on working faster to catch up. Instead, update the plan and determine whether the delay is due to a defect in the plan (and therefore likely to multiply over time) or merely a one-time failing. Optimism is a fine quality, but it’s more important to be realistic.

Summary

These first chapters have no doubt given you lots to think about—and certainly plenty to do. Nevertheless, no matter how much groundwork you lay, you must eventually put some of your plans into practice—if only to see where they can be improved. Part II starts with the next chapter; there you will begin the process of actually installing and configuring Windows Server 2003.
Part II
Installation and Configuration

Chapter 5
Getting Started ................................................................. 55

Chapter 6
Upgrading to Windows Server 2003 ..................................... 105

Chapter 7
Configuring a New Installation ........................................... 159

Chapter 8
Installing and Managing Printers ....................................... 187

Chapter 9
Managing Users and Groups ............................................. 227

Chapter 10
Managing File Resources ................................................... 267

Chapter 11
Administering Group Policy ............................................... 295
Chapter 5
Getting Started

Designing a Deployment Environment ........................................... 55
Creating Your Deployment Environment ...................................... 72
Installing Windows ........................................................................ 91
Troubleshooting Installations ........................................................ 98
Summary ....................................................................................... 103

The first four chapters of the book have dealt with abstract planning. This chapter delves into the specific details of planning and implementing a deployment of Microsoft Windows Server 2003 R2, or any other recent version of the Microsoft Windows operating system.

Installing Windows manually is a time-consuming task on a single system; deploying it to a group of computers is a mind-numbing experience unless you automate the process. Fortunately, there are numerous ways to automate the deployment of Windows. These methods range from using simple answer files that run Windows Setup in unattended mode from CD-ROM on a single system to methods that deploy disk images of completely configured systems over the network to any number of target computers.

This chapter discusses how to design a deployment environment suitable to your organization’s needs, how to create an automated deployment environment (if you choose to automate the deployment process), and how to install Windows manually or using an automated method.

Designing a Deployment Environment

It is helpful to design a deployment environment that allows you to deploy Windows efficiently to the client and server systems in your organization. This section discusses how to design a deployment environment that provides the deployment speed and control you need while maintaining an acceptable level of complexity—regardless of whether you want to manually install Windows on a single system or mass deploy it to thousands of computers.


If you use a Windows Server 2003 R2 product key during installation, Windows Server 2003 with Service Pack 1 Setup installs Windows Server 2003 R2 (but no optional components) after Windows Setup (Winnt32.exe or Winnt.exe) is complete by launching Windows Server 2003 R2 Setup (Setup2.exe) from the \Cmpnents\R2 folder of the second CD. If you use a Windows XP Tablet PC Edition 2005 product key during installation, Windows XP Professional with Service Pack 2 Setup installs Windows XP Tablet PC Edition 2005 by installing additional files from the Cmpnents\TabletPC folder on the second CD.

This affects you in four ways:


- When performing an automated installation of Windows Server 2003 R2, you must include the \Cmpnents folder in your installation source, and include a reference to Setup2.exe in the answer file. For more information, see the “Using Unattended Setup with Windows Server 2003 R2” section of this chapter.

- To install optional Windows Server 2003 R2 components such as the new File Server Management console, you must be able to access the \Cmpnents folder and \i386 or \amd64 folders, either locally, on a network share, or on the Windows Server 2003 R2 Disc 2.
Choosing an Installation Method

Windows installation methods fall into one of two broad categories—Setup-based methods and image-based methods. Setup-based methods use Windows Setup (Winnt32.exe or Winnt.exe) to install Windows on the target computer. Image-based methods copy a disk image of a reference computer with Windows already installed on it to the target computer, which must use hardware that is similar to the reference computer.

Choosing a Setup-Based Installation Method

Setup-based installation methods are relatively simple to use, and you can use them on any hardware configuration, making them ideal for organizations with heterogeneous hardware configurations. The following list describes the three different Setup-based installation methods. Table 5-1 lists the key attributes of each method.

- **Manual installation**  
  Performing a manual installation from the Windows CD-ROM or a network share is the simplest way to install Microsoft Windows. Use this method when installing on a single computer and none of the other installation methods are convenient.

- **Unattended installation using an answer file**  
  This method automates the installation of Windows from a CD-ROM, local source, or network share (called a distribution share) by using a text file called an answer file that provides the answers to each question in Windows Setup. Use an answer file to automate Windows Setup and exert more control over Windows default settings than can be provided by a manual installation.

- **Remote Installation Services (RIS)**  
  A Windows server service that enables users to boot a computer over the network from the RIS server and automatically run Windows Setup in unattended mode. Use RIS to automate Setup on any computer that supports booting from the network via Preboot Execution Environment (PXE); to allow users to easily install or reinstall Windows; and to provide central control over the Setup process. For more information about RIS, see Chapter 28.

---

**Note**  
You can increase the number of simultaneous clients that the server hosting the distribution share can handle by copying the installation files from the distribution folder to the target computer’s hard drive and then running Setup locally instead of across the network. Although copying the installation files puts a greater load on the server at first, after Windows finishes downloading the files, no additional load is placed on the server, freeing it to service other clients.
Choosing an Image-Based Installation Method

Image-based installation methods are the fastest methods of installing Microsoft Windows; however, they work best when there is a high degree of hardware similarity between the target computer and the reference computer from which you created the disk image. Too much variation between systems can lead to a multitude of disk images or longer install times when installing additional drivers during Sysprep Mini-Setup. (Sysprep Mini-Setup is an abbreviated version of Windows Setup that runs on the first boot after using Sysprep to reseal a computer for disk imaging.) Finding and maintaining the proper drivers for a disparate set of systems can also be a challenge, which is why many organizations deploy only a few model lines of computers from the same manufacturer.

These characteristics make image-based installation methods ideal for organizations that need to deploy the Windows operating system and applications to large numbers of similar

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Manual Setup</th>
<th>Unattended Setup</th>
<th>RIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>Slow</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Boot method</td>
<td>Windows CD or Windows operating system</td>
<td>Windows CD, Windows operating system, or boot floppy</td>
<td>PXE boot from network, or network boot using RIS boot disk</td>
</tr>
<tr>
<td>Install source</td>
<td>CD, file share, or hard drive</td>
<td>CD, file share, or hard drive</td>
<td>RIS Server</td>
</tr>
<tr>
<td>Supported operating systems</td>
<td>All versions</td>
<td>All versions</td>
<td>Windows Server 2003*; Windows XP Professional*; Windows 2000</td>
</tr>
<tr>
<td>Hardware similarity requirements</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Maximum simultaneous clients</td>
<td>1</td>
<td>Scales with hardware</td>
<td>75 per server</td>
</tr>
<tr>
<td>Configuration information</td>
<td>Manual entry</td>
<td>Unattend.txt</td>
<td>Active Directory and *.sif answer file</td>
</tr>
</tbody>
</table>

* RIS also supports Windows XP Tablet PC Edition and x64 editions of both Windows Server 2003 and Windows XP Professional.
systems that use the same hardware abstraction layer (HAL). The following list discusses the image-based setup methods that are currently available; Table 5-2 lists the key attributes of each method.

- **Sysprep with disk imaging**  Creates an exact copy or “image” of a Windows installation, which can then be copied onto the hard disk of another computer with similar hardware. Use disk imaging in conjunction with the Sysprep tool to rapidly deploy Windows and applications to a large number of computers that use the same HAL and similar hardware devices.

- **RIS with Remote Installation Preparation (RIPrep) images**  Boots a computer over the network from the RIS server and automatically installs a disk image. This Windows server service starts the target computer across the network, downloads a RIPrep disk image from the RIS server, and performs a full Plug and Play (PnP) detection pass. Use RIS with RIPrep images to quickly deploy Windows and applications to any computer that supports starting from the network via Preboot Execution Environment (PXE). For more information about RIPrep, see Chapter 28.

- **Automated Deployment Services (ADS)**  Enables administrators to rapidly deploy Windows Server in a data center. This Windows server service allows the administrator to remotely start a computer over the network and install or reinstall a Windows Server disk image on the computer. Use ADS to centrally manage the deployment of Windows Server in a data center. For more information about ADS, see the Microsoft Web site at [http://www.microsoft.com/windowsserver2003/technologies/management/ads/default.mspx](http://www.microsoft.com/windowsserver2003/technologies/management/ads/default.mspx).

- **SMS 2003 Operating System Deployment Feature Pack**  Enables administrators to centrally manage the deployment of client and server disk images on a network. Using Systems Management Server (SMS), you can advertise an operating system package that SMS installs automatically on targeted systems that already have the SMS client installed. You can also install the operating system package by starting Windows Preinstallation Environment (Windows PE) and connecting to the SMS server. (Windows PE is included with the SMS 2003 Operating System Deployment Feature Pack.) Use the SMS 2003 Operating System Deployment Feature Pack to centrally manage the deployment of Windows on a network that uses SMS to manage systems. For more information about SMS, see the Microsoft Web site at [http://www.microsoft.com/smserver/](http://www.microsoft.com/smserver/).
### Table 5-2 RISrep, ADS, and SMS attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Sysprep and Disk Imaging</th>
<th>RISrep</th>
<th>ADS</th>
<th>SMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>Fast</td>
<td>Fast</td>
<td>Fast</td>
<td>Fast</td>
</tr>
<tr>
<td>Boot method</td>
<td>Windows operating system, Windows PE, or disk-imaging boot floppy</td>
<td>PXE boot from network, or network boot using RIS boot disk</td>
<td>PXE boot from network</td>
<td>Windows operating system, or Windows PE via RIS or CD-ROM</td>
</tr>
<tr>
<td>Install source</td>
<td>Disk image on network share or CD</td>
<td>Disk image on RIS server</td>
<td>Disk image on ADS server</td>
<td>SMS package on SMS server or CD-ROM</td>
</tr>
<tr>
<td>Hardware similarity requirements with reference computer</td>
<td>Same HAL (alternative mass storage drivers must be added manually)</td>
<td>Same HAL</td>
<td>Same HAL (alternative mass storage drivers must be added manually)</td>
<td>Same HAL (alternative mass storage drivers must be added manually)</td>
</tr>
<tr>
<td>Maximum simultaneous clients</td>
<td>Scales with hardware</td>
<td>75 per server</td>
<td>128 per server</td>
<td>Dependent on SMS infrastructure</td>
</tr>
<tr>
<td>Configuration information</td>
<td>Disk image and Sysprep.inf answer file</td>
<td>Disk image, Active Directory, and *.sif answer file</td>
<td>Disk image and Microsoft SQL Server database or Microsoft SQL Server Desktop Edition (MSDE) database</td>
<td>Disk image and Microsoft SQL Server database</td>
</tr>
</tbody>
</table>

* RISrep also supports Windows XP Tablet PC Edition and x64 editions of both Windows Server 2003 and Windows XP Professional.

**Note** You can add support for mass storage devices not included in a reference image by adding the drivers to the Sysprep folder on the target system and using the SysprepMassStorage section of Sysprep.inf. For more information, see the *Microsoft Windows Corporate Deployment Tools User’s Guide*. 
Choosing a Preinstallation Environment

Before you can install Microsoft Windows, you must boot the computer into a suitable operating system (referred to as the *preinstallation environment*). You can use any of the following methods of booting a computer to install Windows:

- Boot from a Windows CD-ROM directly into Windows Setup.
- Boot from a Windows 98– or MS-DOS-based boot disk, and launch 16-bit Windows Setup (Winnt.exe) from a local or network source.
- Boot from an existing operating system such as a “safe OS” installation of Windows created for installation and recovery purposes, and launch 32-bit Windows Setup (Winnt32.exe) from a local or network source.
- Perform a Preinstallation Execution Environment (PXE) boot from the network into Windows Setup via RIS or ADS (or use a RIS boot disk to start from the network).
- Boot Windows PE from a CD-ROM or RIS server and then launch 32-bit Windows Setup (Winnt32.exe) from a local or network source, copy a disk image from a file share, or connect to an SMS server with the SMS 2003 Operating System Deployment Feature Pack.

**Important** Each operating system installation that belongs to a workgroup or Windows domain must have a unique computer name, even if the installations are on the same computer in a dual-boot or a virtual machine configuration.

Choosing a Software Update Solution

To keep your network secure, you must update every Windows installation on your network in a timely manner with the latest software updates. This is especially true for fresh installations of Windows versions earlier than Windows XP with Service Pack 2 or Windows Server 2003 with Service Pack 1; earlier versions of Windows are potential targets for viruses before you can install antivirus software and the latest software updates, even if you enable the Internet Connection Firewall.

This vulnerability highlights the need to select a software update solution when you design your Windows deployment environment, if you have not already. Selecting a software update solution before you create your deployment environment makes it easier for you to integrate important software updates into your deployment process.
There are a number of software update solutions that you can use to install the latest software updates on computers running Microsoft Windows:

- Install updates manually using Microsoft Update or Windows Update.
- Install updates automatically using Automatic Updates, with or without Windows Server Update Services (WSUS) for central control.
- Install updates automatically using SMS for central control.
- Use a third-party patch management program.
- Add updates to the Windows installation process.

Most organizations use more than one of these methods. For example, a common practice when installing Microsoft Windows is to install Windows from a distribution share or disk image with the latest service pack, and script the installation of any critical software updates into the end of the installation process using an answer file. After Setup completes, you can manually run Microsoft Update and enable Automatic Updates, or use SMS or a third-party patch management program to perform future software updates.

For more information on managing software updates, see Chapter 28.

**Choosing an Application Deployment Solution**

A computer is of minimal value in an organization unless it has the applications the user of the computer needs to perform her or his job. You can install applications, drivers, and services during the Windows installation process, or you can install them afterwards. The following list describes a number of methods that you can use to deploy applications:

- **Manual installation**  Performing a manual installation is the simplest way to install an application. Use this method when installing on a single computer and none of the other installation methods are convenient.

- **Group Policy**  Using Group Policy to deploy applications is an efficient way to deploy applications to a large number of computers in an Active Directory environment. To install applications automatically using Group Policy, the applications must use Microsoft Installer (.MSI) packages; otherwise, you can publish any application setup program for manual or semi-automated installation by the user. Use this method when installing applications on many computers in an Active Directory environment, when central management capability is important, and when initial setup time, scheduled installations, managed bandwidth and error reporting are not critical. See Chapter 28 for more information about using Group Policy to deploy applications.
- **SMS** Using SMS to deploy applications provides the highest level of control and reporting when deploying applications to a large number of computers. Use this method on large, complex networks, or when you need the highest level of control over the deployment process and the added complexity and cost of SMS is acceptable.

- **Install or stage applications during Windows Setup** Installing applications via a silent install immediately following Windows Setup, or staging applications by copying the installation files to the target computer’s hard drive for installation later, is a simple method of quickly making applications available to users. Use this method with applications that support unattended installation, and when quick and simple unattended installation of Windows and key applications is more important than central management ability.

- **Install applications prior to disk imaging** Installing applications on the reference computer before using disk-imaging software to duplicate it is the fastest way to deploy a common set of applications. Use this method when you want to minimize the initial setup time for a common set of applications. If you want to manage these applications centrally, install the applications using your chosen application deployment method (for example, SMS).

### Understanding Licensing and Product Activation

There are two licensing issues that administrators must understand with Windows Server 2003—licensing modes and product activation.

#### Licensing Modes

There are two types of licensing modes for Windows servers: Per Server licensing and Per Device Or Per User licensing (formerly called Per Seat). With Per Device Or Per User licensing, each client that accesses the server needs its own Client Access License (CAL). You can purchase CALs for users, for devices, or for a mix of the two. Purchase user CALs for users who connect to servers with more than one device (for example, a user with a desktop, a laptop, and a PDA), and purchase device CALs for devices that are used by more than one user (for example, a kiosk computer). Clients with a CAL can connect to any number of servers, making this method the most common licensing method for companies with more than one Windows server.

Per Server licensing requires the server to have a CAL for each concurrent connection. For example, if you choose the Per Server licensing mode with 50 concurrent connections, the server can support a maximum of 50 simultaneous client connections. This licensing mode works well for companies that use a single Windows server.
If you are unsure which licensing mode to use, visit the Microsoft Web site at http://www.microsoft.com/windowsserver2003/howtobuy/licensing/default.mspx or contact your local Value Added Reseller (VAR) or Microsoft account representative. You can also choose Per Server and switch later to Per Device Or Per User if you made a mistake. You can switch from Per Server to Per Device Or Per User once (without additional cost), but not from Per Device Or Per User to Per Server.

**Note** In Control Panel, click the License icon to keep track of the license purchases and holdings, or to switch licensing modes.

### Real World  Licensing for Terminal Servers and External Users

You must use Per Device Or Per User mode on Terminal Servers, and you must purchase additional Terminal Services CALs for users or devices (though these users or devices do not require a separate Windows CAL unless they also access the server from Windows). Windows 2000 users cannot access Windows Server 2003 Terminal Servers without a CAL, unlike with Windows 2000 Server.

There are three types of Terminal Services CALs: a TS Device CAL, a TS User CAL, and a TS External Connector CAL (for qualified external users who the organization does not employ in any way). For more information about Terminal Server licensing, see the Microsoft Web site at http://www.microsoft.com/windowsserver2003/howtobuy/licensing/ts2003.mspx.

All users that authenticate with the server in any way (or access the server after authenticating) require a CAL—even authenticated Web site users (except in some cases when using Windows Server 2003 Web Edition). You can purchase an External Connector License for servers that external users access. For example, if a Web site user logs on to a front-end Web site for a SharePoint site hosted on another server, you need either a CAL for the user, or an External Connector license for the Web server, **and** the SharePoint server. The External Connector License replaces the Windows 2000 Server Internet Connector License.

### Product Activation

When you install Windows Server 2003, Windows XP, or a variety of other Microsoft programs from retail media, you have 30 days to activate the product. After the grace period, you cannot log on until the product is properly activated (though the computer will run until you restart it). If you change the hardware enough to require activation (which usually entails a motherboard change plus a couple of other devices), Windows gives you three days before it stops working (unless you are using Windows XP without any service packs, in which case you must activate the product immediately).
This is a real pain if you mass deploy systems, because you need a different product key for every computer and must activate each computer separately. Owning a license for each copy is not enough.

To eliminate the hassle of product activation, purchase volume licenses for Windows and Microsoft Office, because copies of Windows and Office bought in volume do not require product activation. Note that volume licenses are less expensive than retail copies, and they are available for as few as five total Office and Windows products—for example, two copies of Windows and three copies of Office. Some volume license agreements also give you access to Windows PE—an invaluable tool for deploying Windows.

**More Info**  For more information about volume licensing, see the Microsoft Licensing Web site at [http://www.microsoft.com/licensing](http://www.microsoft.com/licensing).

### Designing a Test Lab

A test lab provides a safe location in the organization to create and test Windows installations before deploying them to the network at large, and it is an integral component of a medium- or large-sized Windows deployment.

Large organizations that do not already have a test lab should consider creating a dedicated network for testing that closely matches the production network. You can use the deployment test lab for testing a variety of Windows deployment and management scenarios, such as software updates and line of business applications, or you can create separate labs for each of these testing tasks.

Smaller organizations can often use test systems on the production network or use a Microsoft Virtual PC or Microsoft Virtual Server environment for testing. However, when using a virtual test environment it is important to validate against real hardware that is representative of the production environment. You cannot test display card drivers on a virtual machine, for example.

An ideal test lab has the following characteristics:

- Contains test computers that closely represent the computers in the production environment to which you want to deploy Windows.
- Uses the same server configurations as the production network.
- Mirrors the production network environment with respect to network topology, devices, and settings.
- If load testing a server is important, uses similar hardware configurations for the test server and production servers, and provides a method of simulating the typical and maximum loads you expect the servers to encounter during deployment.
■ Is isolated from the production network sufficiently to prevent the lab from affecting the running network.

■ Is well documented and easy to roll back to the reference state after testing a change.


Planning Server Configurations

If the deployment method you select makes use of one or more servers, it is important to plan the server configurations to provide sufficient performance and support the necessary services for the deployment. You must also plan the configurations of any servers that you are deploying to your production network.

Planning Server Roles

The server role has a major impact on the rest of the server configuration. Decide what role a server will play before planning other aspects of the server configuration. Then assess the server’s system requirements, partition layout, and security needs accordingly. Heavily used database servers, for example, usually require extra random access memory (RAM) and fast disk subsystems. RIS servers require multiple partitions, and Web servers have the strictest security requirements.

When creating a deployment environment for Windows, ensure that you fill the following server roles on the deployment network:

■ **File server** If you are using a distribution share to install Windows or store disk images, you need a file server with sufficient capacity to store all files and provide satisfactory performance for the peak number of simultaneous clients you expect to deploy.

You can also use multiple servers to service clients and replicate the distribution share (or other shares) between the servers using Distributed File System (DFS) or the Windows Server 2003 R2 Distributed File Replication Service (DFRS).

■ **Domain controller** If you are using an Active Directory environment for the deployment environment, you need at least one domain controller to service logon requests.
- **DHCP server** You need one or more DHCP servers to provide dynamic IP addresses to client systems, both during and after deployment, unless you choose to use static IP addresses (which is not recommended).

- **DNS server** One or more DNS servers are required to provide adequate Active Directory functionality and make name resolution more convenient.

- **WINS server** If your preinstallation environment is MS-DOS based and you have multiple subnets, you need a WINS server to ensure proper NetBIOS name resolution.

- **RIS, ADS, and SMS servers** If you are using RIS, ADS, or SMS to deploy Windows, set up these servers and size them properly to handle the anticipated load.

- **SQL Servers** If your deployment environment stores configuration data in a SQL Server database, set up these servers and size them properly to handle the anticipated load.

**Note** Take a few moments to think about naming conventions before you commit yourself to a naming scheme. Sometimes system administrators devise arbitrary schemes based on algorithms known only to them, or they attempt to insert charm into the process of computer naming. Block those impulses! It is easy for you to keep a map of what and where the different clients and servers are on the network, but if you make life hard on users, you will pay in the end.

**Note** Usually, short names that indicate the function of the computer or the owner of the computer (for client systems) are best. For example, “Legal_Files” is a good name for a file server in the Legal department.

**Assessing System Requirements**

Make sure that the servers are powerful enough to handle the anticipated load during deployment while providing an adequate response time.

Table 5-3 lists the minimum system requirements for Windows Server 2003 along with some more practical recommendations for the minimum necessary hardware. Before you buy server hardware, check the Windows Server Catalog on the Microsoft Web site ([http://www.microsoft.com/windows/catalog/server](http://www.microsoft.com/windows/catalog/server)).

**Note** The late Duchess of Windsor was fond of saying that you can never be too rich or too thin. Now you can add the axiom that you can never have too much processing power, RAM, or hard disk space on a server. The only restriction is economic. Get the most powerful server you can afford.
Planning Partitions

Before installing Windows, determine how you want to partition the hard drives. A single partition works nicely for client installations but is generally unsuitable for servers. One common practice is to create a 6- to 10-GB partition for the operating system, and another partition with the remaining space. In this way, the operating system is separate from applications and data (especially the Internet Information Services \Inetpub folder), and you can install services that cannot be installed on the system partition, such as RIS. Creating a 6- to 10-GB system partition and a second data and application partition also works well for most servers that use a redundant array of independent disks (RAID) because a hardware RAID appears to the operating system as a single drive.

Note Some administrators like to place the Windows page file on a dedicated partition to reduce page file fragmentation; however, there are easier ways to prevent page file fragmentation, as discussed in Chapter 7.

Windows Setup does not support dynamic volumes well, which can lead to problems when recovering from a serious error or upgrading the operating system. For this reason,
when using dynamic volumes (including software RAID sets), consider leaving the system partition a basic disk and creating dynamic volumes for data and applications only. You can also install a “safe OS” copy of Windows on a basic partition—you can use the “safe OS” copy to restore from backup in case of a disaster. If you install a “safe OS” (or parallel installation, usually of Windows XP), it is important to lock down this installation, because you cannot install software updates without restarting into the installation. You also need a separate license and computer name for this installation.

Note  You cannot perform a clean install on a dynamic volume unless the dynamic volume is “hard-linked.” Only dynamic volumes that you upgraded from basic volumes are hard-linked.

Real World  Just Say “NTFS”

Although FAT16 and FAT32 had their places in the past, there is no place for them anymore on the hard drives of today’s Windows clients and servers. Simply put, NTFS is more reliable, secure, and efficient than FAT and FAT32. With Windows Server 2003, NTFS is also every bit as fast. (FAT previously maintained a slight speed advantage for some tasks.)

If you absolutely must use a legacy version of Microsoft Windows 95, Windows 98, or Windows Me, you can use FAT partitions to perform a dual boot. However, a more powerful, not to mention more secure, solution is to use Microsoft Virtual PC or Virtual Server to run these operating systems in a virtual machine on a system running Windows XP or Windows Server 2003.

Planning Server Security

It is important to ensure adequate security for the servers in the deployment environment as well as the servers you deploy into the production network. Take the following measures to secure the deployment network:

- Create a dedicated user account just for installations that is a member of a new group named Install Users (or something similar). Limit the permissions given to the account, and consider setting the NTFS permissions for this account to Deny on all folders except the distribution share and subfolders.

To deny the account dial-in rights, right-click the account in Active Directory Users And Computers, click Properties, click the Dial-In tab, and then select the Deny Access check box.

- Set the permissions on the distribution share to grant Read and Execute permissions to the Install Users group. Check the NTFS permissions on your folders to ensure that members of the Install Users group do not have access to any other folders.
To secure the servers you deploy, follow these recommendations:

- Unplug the server from the Internet during Windows Setup, even if it is destined for life as a Web server.

- Install Windows to an NTFS partition.

- Create a strong local administrator password during Setup. (Microsoft Windows Server 2003 prompts you automatically for a different password if the one you choose is too simple.) One common practice is to join the computer to a Windows domain, set a random local Administrator password, and then use the domain administrator accounts for all administration tasks.

- Carefully guard any answer files that contain user names and passwords (as described in the “Using Setup Manager” section of this chapter).

- Physically secure the computer as appropriate for its role and contents:
  - Place servers in a locked server room. Give the key or combination only to people with a demonstrated need for it. Create a system that tracks who enters the room and when.
  - Use case locks and do not leave the keys in them.
  - Remove the floppy disk drive if it is not necessary; otherwise, consider floppy disk locks.
  - After you install Windows, set the boot order in the Basic Input Output System (BIOS) to boot only from the hard drive. This prevents someone from using special boot disks or CD-ROMs to access the contents of the hard drive and reset the local administrator password.
  - Set a BIOS password to prevent unauthorized access to the BIOS.
  - Change the operating system selection timeout period to 0 so that Windows boots automatically.

Security Alert All versions of Microsoft Windows prior to Windows XP with Service Pack 2 or Windows Server 2003 with Service Pack 1 are vulnerable to viruses during the period between the completion of Setup and the installation of antivirus software, even if you enable the Internet Connection Firewall. This can be a problem even if the computer is behind a corporate firewall because many private networks have viruses circulating on them. The new Windows Firewall can protect a system until you can install antivirus software and the latest software updates.
Real World  Password Security

To make the system as secure as possible, always assign a password to the administrator account, preferably a password at least seven characters long and consisting of mixed letters and special characters, uppercase letters, and lowercase letters. Use acronyms for phrases that are meaningful to you, easy to remember, and unlikely to be meaningful or memorable to anyone else, such as Uk,Ur?Ue! (which stands for “You know, you are what you eat!”).

Clear the logon history after installing Windows so that would-be hackers must figure out both the password and the user name. To do this on a standalone server, click Start, choose Administrative Tools, and then choose Local Security Policy. Select Local Policies, select Security Options, double-click Interactive Logon: Do Not Display Last User Name, choose Enabled, and then click OK. Use Group Policy to control this on a member server or domain controller.

Because it is possible to disable any administrator account, including the built-in Administrator account, it is wise to have a backup account. Use the built-in Administrator account to make a second account with full administrative privileges, stash the password and user name somewhere safe, and then relegate that account to semiretirement. For extra credit, rename the built-in Administrator account and then create a decoy account named Administrator. Give the decoy account no permissions and disable it. The hackers can pound away at this account as long as they like but it won’t do them any good.

Creating Your Deployment Plan

Before you create your deployment environment and begin the deployment process, it is important to create a deployment plan. This is a document or series of documents that serves as a road map for the deployment process. The deployment plan should include the following items:

- **A budget**  Determine the level of funding available for the project, and keep it up to date as the project progresses.

- **A schedule**  Create a timeline of when to perform each phase of the deployment, and update it as you achieve (or delay) each milestone.

- **A test plan**  Document specific steps that you can perform to verify that an installation performed in your test lab or in a pilot deployment is fully functional.
List of configurations  Create a list of configurations that you need to deploy and the answer files or disk images that support these configurations.

Deployment steps  Document the exact steps that administrators must perform to deploy Windows to your network. Use these steps as the basis for the test plan, and update it with results from testing and pilot deployments.


Creating Your Deployment Environment

This section discusses how to perform common tasks involved with creating a deployment environment, such as using Setup Manager to create answer files and distribution folders for unattended Setup, using unattended Setup with Windows Server 2003 R2, and using Sysprep with disk imaging. For information on using RIS, see Chapter 28.

To perform a manual installation of Windows, go to the “Installing Windows” section of this chapter.

Using Setup Manager

Setup Manager is a Windows program that provides a wizard-driven interface for creating or modifying answer files and distribution folders. This is the fastest, easiest, and least error-prone way to create answer files and distribution folders.

Setup Manager can create the following types of answer files:

- Unattend.txt answer files for automating Windows Setup from a distribution share or a Windows CD-ROM.
- Sysprep.inf answer files for automating Mini-Setup, the abbreviated Windows Setup process that runs the next time the computer starts after using Sysprep to reseal a computer for imaging.
- A RIS .sif answer file for automating the Client Installation Wizard when installing Windows using RIS. (See Chapter 28 for more information about RIS.)

Note  Original equipment manufacturers (OEMs) should use the version of Setup Manager that ships with the OEM Preinstallation Kit (OPK).


To use Setup Manager to create an answer file, and optionally a distribution folder, follow these steps:

1. Insert the CD-ROM with the most up-to-date version of the Windows Server 2003 Support Tools available, or download updated Support Tools from the Microsoft Web site. (Microsoft usually updates the Support Tools with each Service Pack. Do not use the original Windows XP Setup Manager to deploy Windows Server 2003.)

2. Navigate to the \Support\Tools folder, and extract the contents of the Deploy.cab file to a location on the hard drive of the file server on which you want to create the distribution share.

3. Launch Setupmgr.exe from the location on the hard drive to which you copied the contents of the Deploy.cab file. If you want to create a distribution share, launch Setup Manager from the server on which you want to create the distribution share.

4. On the New Or Existing Answer File page, choose Create New to create a new answer file.

5. On the Type of Setup page (shown in Figure 5-1), choose the type of setup for which you want to create an answer file.

7. On the User Interaction page, choose the level of user input you want to allow during Setup. (See Figure 5-2.) Choose Fully Automated to prevent Setup from stopping for user input. See the sidebar “Choosing an Interaction Level” for more information.

![Figure 5-2  The User Interaction page](image)

8. On the Distribution Share page, choose whether to create a distribution share, modify an existing distribution share, or create an answer file for use with a Windows CD-ROM. If you chose Set Up From A CD, skip to step 11.

To create a distribution share for Windows Server 2003 R2, you must perform additional steps after using Setup Manager, as discussed in the “Using Unattended Setup with Windows Server 2003 R2” section of this chapter.

9. On the Location Of Setup Files page, choose On The CD to copy the installation files from a Windows CD-ROM that matches the edition of Windows you want to deploy, or choose In The Following Folder and then specify the location of the \i386 or \amd64 folder.

10. On the Distribution Share Location page, specify the location for the distribution folder and the share name.

11. On the License Agreement page that appears if you chose to fully automate Setup, select the I Accept The Terms Of The License Agreement option to agree to the terms of the End-User License Agreement (EULA) on behalf of the end-user.
12. Use the Setup Manager window (shown in Figure 5-3) to specify additional settings. You do not have to fill out every setting; however, you must use the Name And Organization, Time Zone, Product Key, and Computer Names pages when creating a fully automated answer file.

![Figure 5-3 The Setup Manager window](image)

The following pages are noteworthy:

- **Computer Names**  Use this page to create or import a list of computer names to use for your systems. Setup Manager takes the names (if you have two or more) and creates a uniqueness database file (UDF) that Setup then queries for computer names, using each name only once. Use computer names that are both DNS-compatible and NetBIOS-compatible if pre–Windows 2000 clients connect to these computers over the network.

- **Administrator Password**  Use this page to specify the local Administrator account passwords for the systems. If you choose to specify a password now, select the Encrypt The Administrator Password In The Answer File check box. If you do not select this check box, the password is stored in plain text for anyone with Notepad to read.

- **Workgroup or Domain**  Use this page to specify the domain or workgroup the computers are to join. To join the computers to the domain, choose the Domain option and then type the Windows Server domain name in the text box provided. Windows prompts the user for a valid domain user account and password when he or she logs on to the domain after Setup completes.
Although Windows Setup Manager can encrypt the administrator password, it cannot encrypt the user name and password you specify for creating the computer accounts. Because of this serious security flaw, avoid using answer files to create computer accounts. Instead, create the computer accounts beforehand on the server. See Microsoft Knowledge Base Article 315273 for information about scripting the creation of computer accounts. If you feel you must use an answer file to create computer accounts, guard the file carefully until after installation is completed. (Setup deletes the user name and password from the answer file during the setup process.)

Run Once  Use this page to specify commands to run the first time a user logs on. You can use this page, which corresponds to the [GUIRunOnce] section of the Unattend.txt, to automate Windows Server 2003 R2 Setup (Setup2.exe), or the Active Directory Installation Wizard (as discussed in Chapter 14). You can also use this page to install applications that can be silently installed from a command prompt (and that do not require a reboot). When using this page to install applications, use the When A Destination Computer Starts, Automatically Log On As Administrator check box on the Administrator Password page to force the applications to install during the automated setup process rather than the first time an actual user logs on.

Additional Commands  Use this page to specify commands to run near the end of GUI-mode Setup, before the computer reboots and the $OEM$ folder is deleted. You can use this page to run an application or command that does not require network connectivity, Windows installer support, or a locally logged-in user. Setup Manager ignores this page unless you are creating a new distribution share or modifying an existing one. This page creates a Cmdlines.txt file in the \i386\$OEM$ or \amd64\$OEM$ folder of the distribution share.


13. On the Additional Commands page, click Finish, type the name and location for the answer file, and then click OK.

Setup Manager creates the distribution folder (if you chose to create a new distribution folder) and creates the answer file. It also creates a batch file that starts Setup (Winnt32.exe) in unattended mode using the answer file you created. You can use this batch file or launch Setup with the appropriate parameters, including the parameter pointing to the answer file. (See Tables 5-3 and 5-4 for the appropriate parameters.)
14. If you are creating an answer file for a CD-ROM–based installation, rename the Unattend.txt file to `Winnt.sif`, place it on a floppy disk or USB Flash Device (UFD), and insert the disk or UFD immediately after the computer starts from the Windows CD-ROM.

15. If you plan to start Windows Setup from an MS-DOS environment such as a Windows 98 Startup Disk, modify the batch file that Setup Manager creates to use the 16-bit Setup (Winnt.exe) file by deleting the `32` from the third-to-last line of the file. Also change the `/unattend:` parameter in the second-to-last line to `/u:`.

---

**Real World  Choosing an Interaction Level**

The level of user interaction you require determines how much the person running the installation needs to attend to the process. Here is a more detailed explanation of the interaction levels:

- **User Controlled**   Uses the information in the answer file as default answers during the Windows installation. The user must confirm the defaults or make changes as the installation progresses. (Nothing is automated.)

- **Fully Automated**   Completely automates Setup by using the settings you specify in the answer file. This option is best for quickly setting up multiple systems with identical configurations. If any settings do not work properly (such as might happen if the answer file provides a computer name that is already in use), the installation fails.

- **Hidden Pages**   Automates the parts of Setup for which you provide information, and prompts the user to supply any information you did not include in the answer file. Use this option to set up a system in a specific way, while still allowing the user some limited customization options. (The user sees only the parts of Setup that the answer file does not cover.)

- **Read Only**   Hides the pages for which you provide information, just like the Hidden Pages option. However, if the answer file does not provide information for all settings on a page, Setup displays the page and prompts the user to complete the unanswered portion of the page. You cannot change settings provided in the answer file during installation.

- **GUI Attended**   Automates the text-mode portion of Setup. The person running Setup supplies answers for the Windows Setup Wizard. Use this option when you want to automate the text-mode portion of Setup and allow the person running the installation to provide the settings during the graphical user interface (GUI) portion.
Part II  Installation and Configuration

Note If you create the system partition in a preinstallation environment without restarting the computer, add the `/syspart` and `/tempdrive` parameters to the `Winnt32.exe` command in the Unattend.bat batch file or the command that you use to start Setup.

Using Unattended Setup with Windows Server 2003 R2

To automate Windows Server 2003 R2 Setup using an answer file, you must add the `\Cmpnents` folder from Windows Server 2003 R2 Disc 2 to the distribution share or RIS image, and add commands to the answer file to launch Windows Server 2003 R2 Setup (Setup2.exe). If you do not perform these additional steps, Windows Setup stops after installing Windows Server 2003 with Service Pack 1, and prompts you to insert the second CD-ROM to continue Windows Setup.

To prepare the distribution share for Windows Server 2003 R2, copy the `\Cmpnents` folder from the Windows Server 2003 Disc 2 CD-ROM into a Windows Server 2003 with Service Pack 1 distribution share, at the same level as the `\i386` or `\amd64` folder. For example, if the path to the `\i386` folder on the distribution share is `\srv2\windist\winsrv2003\i386`, copy the `\Cmpnents` folder to `\srv2\windist\winsrv2003\i386\Cmpnents`.

Note To prepare a RIS image for Windows Server 2003 R2, copy the `\Cmpnents` folder into the image at the same level as the `\i386` or `\amd64` folder, associate a new RIS .sif answer file to the Windows Server 2003 with Service Pack 1 image, and then modify the answer as discussed in this section. See Chapter 28 for information about associating answer files to RIS images.

To launch Windows Server 2003 R2 Setup from an Unattend.txt, Sysprep.inf or RIS .sif answer file, follow these steps:

1. Open the appropriate answer file in Setup Manager and then navigate to the Run Once page.

2. If you are running Windows Setup from a distribution share, type the following command in the Command To Add box and then click Add.

   "cmd /c net use \srv2.example.office\windist /user:EXAMPLE\Install Password"

This command connects to the distribution share and authenticates with the server, if necessary. Replace `\srv2.example.office\windist` with the UNC name of the distribution share. Replace `EXAMPLE\Install` with the domain (or computer for workgroup environments) and username of a limited-rights user account with permission to access the share, and `Password` with the password for the user account.
3. If you are creating an Unattend.txt file for installation from a distribution share or local source other than a CD-ROM or DVD-ROM, and you need to copy files from the $OEM$ folder and subfolders during Setup, type the following commands in the Command To Add box. Click Add after each line, and replace source_path with the path to the location of the \i386 or \amd64 and \cmpnents folders:

```
"cmd /c reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Setup /v SourcePath /t REG_SZ /d source_path /f"
"cmd /c reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Setup /v ServicePackSourcePath /t REG_SZ /d source_path /f"
```

These commands ensure that the SourcePath and ServicePackSourcePath registry keys are set to the location of the \Cmpnents and \i386 (or \amd64) folders when Windows Server 2003 R2 Setup runs during the [GUIRunOnce] processing and for subsequent installations of Windows Server 2003 components (including Windows Server 2003 R2 components). Otherwise, the SourcePath and ServicePackSourcePath keys are reset to the drive letter of the CD-ROM drive (usually D).

4. Type the following command in the Command To Add box, and then click Add. This command launches Windows Server 2003 R2 Setup from the [GUIRunOnce] section of the Unattend.txt, Sysprep.inf or .sif answer file.

```
"\srv2.example.office\windist\cmpnents\r2\setup2.exe /q /a"
```

5. If you want to automate the installation of Windows Server 2003 R2 optional components, type the following command in the Command To Add box, and then click Add.

```
"%WINDIR%\system32\sysocmgr.exe /i:%WINDIR%\inf\sysoc.inf /u:\srv2.example.office\windist\Sysocmgr.ini"
```

This command launches Sysocmgr.exe in unattended mode using the Sysocmgr.ini answer file you specify (as described later in this chapter).

6. If you are creating an Unattend.txt file for installation from a distribution share or local source and you do not need to copy files from the $OEM$ folder and subfolders during Setup, open the Unattend.txt file in Notepad or another text editor and change OEMPreinstall = Yes in the [Unattended] section to OEMPreinstall = No.

Doing so prevents Setup from resetting the SourcePath and ServicePackSourcePath registry keys to the drive letter of the first CD-ROM drive (usually D:").

**Note** If you are using the [OEMRunOnce] section of Winbom.ini to install Windows Server 2003 R2 during Sysprep factory mode, you can use the SourcePath entry in Winbom.ini to set the SourcePath and ServicePackSourcePath registry keys during Sysprep factory mode.
Installing Optional Components During Unattended Setup

You can install most optional Windows components during unattended Setup by using the [Components] section of the Unattend.txt file. You cannot install Windows Server 2003 R2 components (or Message Queuing) during Windows Setup, but you can install them automatically after Setup completes by using Sysocmgr.exe and an answer file (Sysocmgr.ini). You can also use Sysocmgr.exe with an answer file to install or uninstall any Windows component at any time after Setup completes.

To install Windows components automatically using Sysocmgr.exe, create a text file named Sysocmgr.ini (or any other name) that includes a listing of the components that you want to install using the following syntax:

```
[Components]
DFSFRSUI = On
DFSR = On
Netfx20 = On
```

Then run the Sysocmgr.exe command with the Sysocmgr.ini file you created, as described in Step 5 of this section. For more information about Sysocmgr.exe and Sysocmgr.ini, see the Microsoft Windows Corporate Deployment Tools User’s Guide (Deploy.chm and Ref.chm) on Windows Server 2003 Disc 2 or at the Microsoft Download Center (http://www.microsoft.com/downloads/).

Creating and Modifying a Distribution Share

A distribution share is a shared folder on a server from which you can install Microsoft Windows. The distribution share must contain the Windows installation files: the \i386 or \amd64 folder from the Windows CD-ROM, the Cmpnents folder (when installing Windows Server 2003 R2), and any device drivers or other files that you want to include during Windows Setup.

This section discusses how to create a distribution share manually, and how to modify a distribution share or RIS image by adding drivers, software updates, and service packs.

Creating a Distribution Share

The easiest way to create a distribution share is to use Setup Manager, as described earlier in this chapter. To create a distribution share for RIS, use the Remote Installation Services Setup Wizard, as described in Chapter 28. However, you can also create a distribution share manually or modify the files contained within it. To do so, follow these steps:
1. Create a folder on the server named \Windist (for example), and share it on the network with the proper share name and permissions. (Keep the share name to eight characters or fewer if it needs to be accessible from an MS-DOS–based or Windows 98–based boot disk.)

Give Administrators Full Access, and give other users Read and Execute permissions.

2. Create a descriptively named subfolder (such as W2K3), and copy the \i386 or \amd64 folder from the Windows CD-ROM into the subfolder.

3. If you are creating a distribution share for Windows Server 2003 R2, copy the \Cmpnents folder from Windows Server 2003 R2 Disc 2 into the same folder in which you copied the \i386 or \amd64 folder.

4. Create a subfolder named $OEM$ in the \i386 or \amd64 folder (or at the same level as the \i386 or \amd64 folder for RIS installations) for any additional drivers or programs that you want to preinstall. Setup copies all files and folders in this folder into the temporary setup folder during installation, and then deletes them near the end of GUI-mode Setup.

You can also place the $OEM$ folder outside the distribution share if you place the path (file or UNC) to the $OEM$ folder after the OEMFilesPath key in the answer file.

5. Create any additional subfolders needed for the installations. Table 5-4 describes the special folders that you can create for use by Setup.

   **Note** If you are using Winnt.exe to launch Windows Setup, all files and folders that you create in the distribution share must have short (8.3) file names. To convert files with short filenames back to long filenames during Setup, see the “Converting Short Filenames Back to Long Filenames” section of this chapter.

<table>
<thead>
<tr>
<th>Folder</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$OEM$1</td>
<td>The folder in which you place files that you want Setup to copy to the drive on which it installs Windows. Equivalent to the %systemdrive% environment variable, you can use the $OEM$1 folder to change drive letters without causing problems for applications that point to a hard-coded drive letter. You can also create subfolders here for the files; Setup copies the entire folder structure to the system drive. If you use the $OEM$1 folder, set OEMPreinstall = Yes in the [Unattended] section of the Unattend.txt answer file.</td>
</tr>
</tbody>
</table>
Table 5-4  Subfolders you can create to store extra files

<table>
<thead>
<tr>
<th>Folder</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$OEM\1\Sysprep</td>
<td>The folder in which you place the files required to run Sysprep, if you want to run Sysprep at the end of unattended installation to reseal the computer or install additional applications using Sysprep Factory mode.</td>
</tr>
<tr>
<td>$OEM$$</td>
<td>The folder that holds any new system files or files that replace existing system files. Setup copies these files into the various subdirectories of the Windows system folder (\Windows).</td>
</tr>
<tr>
<td></td>
<td>This folder must match exactly the structure of the Windows system subfolders for those folders in which you want to add or replace system files. For example, to copy new or replacement files into the %windir%\System32 folder, create an $OEM$$\System32 folder.</td>
</tr>
<tr>
<td>$OEM$Progs</td>
<td>The folder that holds any files that you want to copy to the %PROGRAM FILES% folder during Setup.</td>
</tr>
<tr>
<td>$OEM\textmode</td>
<td>The folder in which you place any hardware-dependent files for use while loading Windows Setup and during the text-mode phase of Setup. These files include updated SCSI, keyboard, video, and pointing device drivers.</td>
</tr>
<tr>
<td></td>
<td>Include the Txtsetup.oem file in this folder to control the loading and installation of these files. To create the Txtsetup.oem file, create a normal text file and list the filenames of all files in this folder. List the Txtsetup.oem file and all files mentioned in the Unattend.txt file, under the [OEMBoot-Files] section.</td>
</tr>
<tr>
<td>$OEM\drive_letter</td>
<td>The folder that specifies additional files and folders that you want Setup to copy into the root folder of the named drive. Create one entry for each drive to which you want to copy files. For example, Setup copies the files located in the $OEM\C folder into the root folder of the C: drive during the text-mode phase of Setup. Setup also copies any subfolders of the $OEM\C folder.</td>
</tr>
</tbody>
</table>

Note  Windows Server 2003, Windows XP, and Windows 2000 do not use the \$OEM\Display and \$OEM\Net subfolders that Windows NT 4 Setup used.

Applying Service Packs to a Distribution Share
You can apply a service pack to a distribution share or standard (non-RIPrep) RIS image so that subsequent installations of Windows are “integrated” installations of Windows that include the latest service pack. To perform this procedure, follow these steps:

1. Make a copy of the distribution share or RIS image so that you do not affect existing clients when you upgrade the distribution share.

   Existing clients that do not have the latest service pack installed might access the distribution share to install optional Windows components, and they must receive the version of the components that corresponds to the service pack level of the client.
2. If the Windows install files are not located in the \i386 or \amd64 folder, move them there before applying the service pack.

3. Open a command prompt, switch to the folder storing the service pack, and then apply the service pack to the distribution share or RIS image.

To do this for Windows Server 2003 Service Pack 1, type `WindowsServer2003-KB889101-SP1-x86-ENU.exe /integrate:path`, where `path` is the path to the distribution share you want to update (for example, e:\windist\winsrv03sp1). The parameters vary depending on the service pack—consult the service pack documentation for further information.

When you run the Update.exe file to update a Windows distribution share with the latest service pack, it creates a Svcpack.log file in the `%systemroot%` of the computer from which you ran Update.exe. If you want to perform more service pack installations from the same computer, rename this log file before performing them.

**Installing Software Updates with an Answer File**

Most organizations choose to deploy software updates after Setup completes using their chosen software update management solution. However, you might want to apply some updates during Setup. For example, you might want to deploy Windows Server 2003 R2 with a set of tested and approved security updates to maximize the security of the server from the moment Setup is complete. This is particularly important when there are viruses on your internal network that can infect new systems before you can install antivirus software and the latest security updates. See Chapter 23 for more information about software updates.

**Important** Install software updates released only after the service pack version you are deploying. For example, if you are deploying Windows Server 2003 R2 (which is based on Windows Server 2003 with Service Pack 1), add only hotfixes that are labeled sp2 (which means they are post–Service Pack 1).

The most flexible method of installing software updates during Setup is to use the following steps to copy the updates into the distribution share and add them to an answer file.

1. Copy the update executable file into the $OEM$ folder.

2. On the Additional Commands page in Setup Manager, type the filename of the update followed by the quiet (/q) and unattended (/u or /m, depending on the update version) parameters. (This adds the commands to the Cmdlines.txt file.) For example, type `KB123456.exe /q /u`.

Some updates use different parameters—to view the parameters supported by an update, type the filename followed by the /? parameter.
To suppress a reboot when installing an update that requires a reboot, add the /z parameter to the software update command. (Not all updates support or require this parameter.)

You can apply software updates to a distribution share in the same way as you apply a service pack: run the update with the /integrate parameter. However, you cannot uninstall software updates applied to a distribution share, so most organizations prefer to add software updates to an answer file or install the updates using the organization’s chosen software update solution after Setup completes.

**Note**  Hotfix chaining (that is, installing multiple software updates with a single restart) is supported in Windows Server 2003, Windows XP, and Windows 2000 Service Pack 3 and later. Previously, you had to restart after each software update installation, or run the Qchain.exe tool after installing the updates before restarting. Install software updates in order by date or Knowledge Base article number when possible.

**Installing Plug and Play Drivers in the Distribution Share**

To add Plug and Play (PnP) drivers to a distribution share or RIS image, follow these steps:

1. Create a subfolder in the \$OEM\$1 folder with a name containing no more than eight characters. This folder remains on the destination computer’s hard drive after Setup completes. If you want to protect these drivers from accidental deletion by end users, instead create it in the \$OEM\$$ folder, which Setup copies to the \Windows folder.

   If you are adding drivers to a RIS image, create the \$OEM\$ folder at the same level as the \i386 or \amd64 folder.

2. Inside the subfolder you created, you can make additional subfolders to categorize the devices. For example, you might have the following directories:

   \$OEM\$1\Drivers\Net
   \$OEM\$1\Drivers\Video
   \$OEM\$1\Drivers\Sound

3. Copy the drivers and .INF files into the appropriate subfolder.

   If you are installing a network driver for a RIS image, copy the driver files into the \i386 or \amd64 folder in addition to the subfolder you created. If this driver replaces an existing driver in the \i386 or \amd64 folder, delete the existing driver’s .pnf file.
4. Add the appropriate lines to the answer files:

- **Standard answer file users** Add each subfolder to the OEMPnPDriversPath entry of the [Unattended] section of the answer file (Unattend.txt or Sysprep.inf), separating each folder reference by a semicolon. For example:

  OEMPnPDriversPath = Drivers\Nic;Drivers\Video;Drivers\Sound

- **Remote Installation Services (RIS) users** Modify the following lines or add them to the [Unattended] section of the default template for the desired image (Risndrd.sif):

  OemPreinstall = Yes
  OEMPnPDriversPath = Drivers\Nic;Drivers\Video;Drivers\Sound

  **Note** Leave the drive letter out of the paths. Setup automatically adds the system drive to the paths.

If you are installing new drivers for a RIS-based operating system image, restart the BINL (Boot Information Negotiation Layer) service on the RIS server after copying the files into the distribution folder. To do so, type the following commands at a command prompt:

- `net stop "boot information negotiation layer"`
- `net start "boot information negotiation layer"`

  **Note** Sysprep and RIS installations postpone installing devices with unsigned drivers until an administrator logs on to the computer. To avoid this (at your own peril), add the `DriverSigningPolicy = Ignore` line to the [Unattended] section of the answer file.

### Installing OEM Drivers in Remote Installation Preparation Images

Although it is tempting to add OEM drivers to a Remote Installation Preparation (RIPrep)-based image by installing them on the source computer before running the RIPrep program on it, this does not work because RIPrep images need to be able to adapt to a wide variety of hardware. Therefore, follow these steps to add drivers to RIPrep-based images:

1. Before running the RIPrep process (described in Chapter 28), create a folder named Sysprep on the C:\ drive of the source computer.

2. Create a C:\Drivers folder to hold OEM drivers, and create any necessary subfolders, such as C:\Drivers\Video or C:\Drivers\Sound.

3. Create a Sysprep.inf file, and place it in the Sysprep folder.
4. Add the following lines to the Sysprep.inf file:

```
[Unattended]
OEMPnPDriversPath = Drivers\Nic;Drivers\Video;Drivers\Sound
```

5. Use Device Manager to remove any devices for which you are installing updated or new drivers. Also, remove any unknown devices.

6. If you are adding mass storage drivers that Windows requires to start, use the “Installing Mass Storage Drivers” section of this chapter to add the drivers to the appropriate RiSetup image (a flat RIS image created using Risetup.exe or the Remote Installation Services Setup Wizard). Add the drivers to the RiSetup image that matches the operating system version (not including service packs) of the RiPrep image and whose folder name is listed first alphabetically.

   For example, when adding mass storage drivers to a Windows Server 2003 R2 RiPrep image on a Windows Server 2003 RIS server that contains RiSetup images in the \Win2K3 and \Win2K3R2 folders, add the drivers to the RiSetup image located in the \Win2K3 folder, because \Win2K3 comes before \Win2K3R2 alphabetically.

7. Run Riprep.exe from the RIS server’s network share, as described in Chapter 28.

8. Stop and restart the BINL service on the RIS server by typing the following commands:

   `net stop "boot information negotiation layer"
   net start "boot information negotiation layer"

---

### Under the Hood  Why RiPrep Images Need RiSetup Images

A RiPrep image does not have a fully populated critical device database, so it uses the critical device database from a matching RiSetup image until the client can load Windows and perform its own enumeration of devices. This is why you must add mass storage drivers to both the RiPrep image and the matching RiSetup image.

RIS determines which RiSetup image to use for a given RiPrep image at runtime by looking at the operating system version and folder name, so the image RIS selects could change if you add or rename image folders.
Installing Mass Storage Drivers

If the hard drive or installation source is attached to a device for which Windows does not have drivers, such as a new network adapter or Serial ATA (SATA) controller, you have a problem. When performing a manual installation, you can always press F6 at the beginning of text-mode setup to install new mass storage drivers from a floppy disk, but this option is cumbersome with unattended installations. To get around this, follow these steps to copy mass storage drivers that are required at boot time to the distribution share or RIS image:

1. Create a folder named \$OEM\Textmode in the \i386 or \amd64 folder of the distribution share. (This step is unnecessary for a RIS image.)

2. Copy the storage drivers into the \$OEM\Textmode folder (or the \i386 or \amd64 folder for a RIS image) as well as the folder specified in the OEMPnPDriversPath entry of the answer file (for example, \$OEM\$1\Drivers\Storage). These files should include at least one .SYS file and the Txtsetup.oem file.

3. In the answer file, add the following lines (refer to the Txtsetup.oem file for the exact syntax):

   [MassStorageDrivers]
   "scsi controller string from txtsetup.oem" = "OEM"

   For example:

   [MassStorageDrivers]
   "DELL PERC 2/3/4 RAID Controller Driver" = "OEM"

   To enable client computers to start from a device connected to an IDE controller for which Windows provides drivers, add the following line to the [MassStorageDrivers] section:

   "IDE CD-ROM (ATAPI 1.2)/PCI IDE Controller" = "RETAIL"

4. Add or modify the [Unattended] section of the answer file to include the following line:

   OemPreinstall = Yes

5. Add or modify the [OEMBootFiles] section of the answer file to include a listing of all files in the $OEM$\Textmode folder. For example:

   [OEMBootFiles]
mraid35x.cat
nodev.inf
Oemsetup.inf
mraid35x.sys
txtsetup.oem
6. Open the Txtsetup.oem file using Notepad. In the [Disks] section, remove any floppy disk references or other path references, and type a backslash (\) at the end of the line (or a period if installing on a FAT partition). For example, change the following line:

   d1 = "Windows Server 2003 Driver Set 1.01", \w23dsk1, \

7. Verify that theTxtsetup.oem file contains a section named [HardwareIds.Scsi.
   device_service_name], where device_service_name is the device service name. If this
   section does not exist, create it using the following syntax, where device_identifier
   is the device identifier:

   [HardwareIds.scsi.device_service_name]
   id = "device_identifier", "device_service_name"

   For example, for a Dell PERC RAID controller, use the following lines:

   [HardwareIds.scsi.DELLPERC]
   id = "PCI\VEN_1000&DEV_0407&SUBSYS_05311028", "mraid35x"

Converting Short Filenames Back to Long Filenames
If you start Windows Setup using the Winnt.exe setup program, or if you use MS-DOS to
copy the distribution share to a local source, all files included in the distribution share
must have MS-DOS–compliant short names. This is because MS-DOS and Winnt.exe will
discard long filenames when copying files. However, you can convert the short filenames
back to long filenames during Setup by creating a renaming file for each folder in which
there are files you want to convert.

The easiest way to create a renaming file ($$Rename.txt) is to copy your files into the
$OEM$ folder (or a subfolder), open the answer file in Setup Manager that corresponds
to the distribution share, and then save the answer file. Setup Manager automatically cre-
ates the necessary $$Rename.txt files for you. You do not need to rename files with long
filenames because Setup Manager lists the short names of each file as MS-DOS would see
them.

To create a renaming file manually, follow these steps:

1. Open Notepad, type the path to the subfolder containing the files you want to
   rename, and enclose the path in brackets (by leaving a blank or using the backslash
   character [\] for the root folder).

2. Underneath the bracketed heading, type each short filename you want to rename
   (not enclosing it in quotes) followed by an equals sign and then the long filename
   in quotes.
3. Repeat step 2 with any additional subfolders in which you have files or folders that you want to rename. A sample renaming file is shown below:

```
[media]
filenm1.txt = "Your long filename here.txt"
ding.wav = "Really loud and annoying ding.wav"
whiz.mpg = "Whizbang Deluxe Video.mpg"

[images]
desktp1.bmp = "corporate logo.bmp"
desktp2.bmp = "division logo.bmp"
```

4. Save the file as $Rename.txt in the folder of the distribution share that contains the files that you want to convert.

**Using Sysprep with Disk Imaging**

One way to increase the speed of the setup process is to create a disk image of an existing reference system and then apply that image to the target system. Installing a disk image created with Sysprep and disk-imaging software usually takes 45 to 60 minutes less time than an unattended Setup-based installation.

More Info For in-depth information about Sysprep, see the Microsoft Corporate Deployment Tools User’s Guide (Deploy.chm).

Disk imaging works like this: first, install Windows and all the applications you need on a single machine that is identical or very similar to the many machines on which you want to deploy Windows. Then prepare this system for imaging by using the reseal functionality of Sysprep (which is available on the Windows CD-ROM in the Deploy.cab file) to clear out the SID and other computer identity information. Image the configuration using a disk-imaging program, such as PowerQuest Drive Image or Norton Ghost, which copies and compresses the disk image to a network share. You can then start a blank system by using Windows PE or the floppy disk created by the disk-imaging program, copy and uncompress the disk image onto the new system, and be up and running in far less time than is required to perform a fully automated Setup-based installation.

However, this solution has some problems. First, the systems must be similar for the disk images to work on them. The computers do not have to be identical because Windows uses Plug and Play (PnP) to detect changes to most system components. However, the systems must share the same HAL—no mixing ACPI systems with non-ACPI systems. If the systems use different mass storage controllers, you must add the drivers to the image by adding the drivers to the \Sysprep folder on the target system and using the [Sysprep-MassStorage] section of Sysprep.inf. In addition, this process does not work for Cluster service servers, Certificate Server servers, or domain controllers (unless you script the DCPROMO process into the disk image).
Because you cannot install a Sysprep-created operating system image on a disk partition smaller than that on which you created the image, install Windows into a partition just large enough for Windows and any necessary applications. The disk-imaging software usually partitions the target computer’s hard disk to the same size as the reference computer’s partition, but you can use the ExtendOemPartition entry in the Sysprep.inf file to extend the destination computer’s system partition to fill the hard disk.

Covering in detail how to use Sysprep and disk-imaging tools to mass deploy computers is outside the scope of this book; however, the following steps summarize how to create a disk image of a reference system and apply it to a target system:

1. Install and customize Windows on the reference system.
2. Install and customize any applications you want to deploy to all systems using this drive image.
3. Copy Sysprep.exe, Factory.exe, and Setupcl.exe from the Deploy.cab file that ships with the version of Windows that you are imaging into the C:\Sysprep folder.
   To automate Mini-Setup, copy a Sysprep.inf answer file you created with Setup Manager to the C:\Sysprep folder. To use Sysprep factory mode to customize an installation after applying the reference image to the target computer, create a Winbom.ini file and copy it to the C:\Sysprep folder.
4. Launch Sysprep, and click Reseal to remove all identity information from the system.
5. Restart the computer into your preinstallation environment and then use a disk-imaging program to save the disk image to the desired network share.

   After using Sysprep to reseal a reference system for imaging, you must restart the computer and run through Mini-Setup (described in step 8) before you can perform additional customizations or use it as a normal system.

6. Boot the target system with Windows PE or a network floppy disk and then connect to the network share containing the drive image.
7. Use the imaging software client tools to expand the image file onto the target system’s hard drive.
8. Restart the target system. Mini-Setup runs, detects any additional PnP devices and hides any missing devices. The wizard generates a new SID, and the system is then fully functional. (To force Mini-Setup to perform a full PnP detection process to eliminate rather than hide any missing devices, run Sysprep with the /PnP switch.)
Important Thoroughly test your disk images before using them to deploy Windows in a production environment.

Installing Windows
The process of manually installing Windows or automating the installation of Windows after creating your deployment environment is straightforward. First, you prepare the system for installation. Then you install Windows, either manually, with an answer file, or via Setup command-line parameters.

Preparing the System
Before you install Windows, several physical tasks remain:

- Back up any existing data on all the drives for which the server is responsible.
- Disable any disk mirroring for the duration of the setup process.
- Disconnect any serial connections to an uninterruptible power supply (UPS). UPS equipment can interfere with the setup program’s ability to detect devices connected to serial ports.
- Upgrade the system BIOS to the latest version available. If the BIOS does not meet Windows’ Advanced Configuration Power Interface (ACPI) standards, set the Plug and Play (PnP) OS setting to NO in the BIOS.
- Change the boot settings in the BIOS to start the computer from the proper location (usually a CD-ROM or PXE-based network boot).
- Locate any mass storage drivers or custom hardware abstraction layer (HAL) files necessary for the system.
- If setting up a headless server without a monitor or any means of input, connect the server to the appropriate terminal concentrator. Before setting up a headless server, refer to Chapter 40 for information about Emergency Management Services (EMS).

Performing a Manual Installation of Windows
The most basic way of installing Windows is to install it manually from the Windows CD or a network share. This method is fine when doing a few installations or when learning the installation process. However, it is a tedious and slow method of deploying systems en masse; so for multiple installations, automate the process using answer files, Sysprep, or RIS.
The Phases of Setup

The Windows Setup process consists of several phases that vary depending on how you initiate the installation.

- **Preinstallation**  This optional phase runs if you launch Setup from a version of the Windows operating system, Windows PE, or an MS-DOS-based boot disk. During this phase, Setup gathers information (if Setup is run from Windows or Windows PE), and then copies the files necessary to boot the computer into text-mode Setup.

- **Text-mode Setup**  During this phase, you select a disk partition and Setup copies the files necessary to start into the graphical user interface (GUI)-based Windows Setup Wizard.

- **GUI-mode Setup (Windows Setup Wizard)**  During this phase, Setup collects more information, installs devices, finishes copying files, processes the Cmdlines.txt file, and then deletes the $OEM$ folder and subfolders from the target computer’s hard drive.

- **First boot**  This is the first boot of Windows after Setup completes, and it is when Setup processes the [GUIRunOnce] section of the Unattend.txt file, followed by the Winbom.ini file if you choose to use Sysprep Factory mode.

To perform a manual installation of Windows, start the computer from the Windows CD-ROM and then follow the instructions on the screen. Following is a list of noteworthy steps:

1. To load mass storage drivers not included with Windows—such as drivers for a Small Computer System Interface [SCSI] or RAID controller—press F6 when the computer starts in Windows Setup. To specify a different HAL manually, press F5.

2. After selecting or creating a hard disk partition, specify whether Setup should convert the partition to NTFS (because it is not an NTFS partition already), format the partition (and perform a Quick NTFS format if there is no existing data on the partition), or leave the disk alone (if there is an existing file system).

   **Note**  Press Shift+F10 at any time during the Windows Setup Wizard to open a command prompt from which you can do various things, such as inspect log files or launch a screen capture program.

4. If you need to specify a static IP address, or change networking settings from the defaults during Setup, choose Custom Settings on the Networking Settings page of the Windows Setup Wizard.

   If you don’t have a DHCP server and don’t assign an Internet Protocol (IP) address to the computer, Windows assigns the computer an automatic private IP address in the 169.254.0.0-169.254.255.255 range with a subnet mask of 255.255.0.0. For more information, see Microsoft Knowledge Base Article 220874 at http://support.microsoft.com/kb/q220874/.

5. Use the Workgroup Or Computer Domain page of the Windows Setup Wizard to join a workgroup or Windows domain. To create a new domain, join a workgroup or an existing domain during Setup and create the new domain later, as discussed in Chapter 7 and Chapter 14.

6. If you are installing Windows Server 2003 R2, Setup prompts you for the Windows Server CD2 the first time an administrator logs in after Setup completes. Insert the CD, or type the location of the \Cmpnents folder. To initiate Windows Server 2003 R2 Setup later, launch Setup2.exe from the \Cmpnents\R2 folder of the installation source.

7. After Setup completes on systems running Windows Server 2003 R2 or Windows Server 2003 with Service Pack 1, the Windows Server Post-Setup Security Updates window appears. Use this window to install the latest software updates and configure Automatic Updates before allowing inbound connections. For more information, see Chapter 7.
Initiating Windows Setup Using an Answer File

To perform an unattended installation of Windows from a distribution share, follow these steps:

1. Start the computer using the preinstallation environment you chose (an MS-DOS boot disk, Windows operating system, or Windows PE).

2. Create an installation partition if there is not one already, mark it active, assign it a drive letter, and format it using the NTFS file system. For example, when using Windows PE or Windows as your preinstallation environment, use the following diskpart.exe commands to erase all data on the first physical drive (and note that you don’t do this on the drive from which you are running Windows), and create a single partition of the maximum size:

   ```
   Select disk 0
   Clean
   Create partition primary
   Select partition 1
   Active
   Assign letter=c
   Exit
   Format c: /fs:ntfs /q
   ```

   When using an MS-DOS-based preinstallation environment, you must format the partition using the FAT32 or FAT16 file system. However, you can convert the partition to NTFS and extend the size during Setup. (For more information, see the Microsoft Windows Corporate Deployment Tools User’s Guide.)

3. Connect to the distribution share, and then launch Windows Setup (Winnt32.exe or Winnt.exe) using the batch file created by Setup Manager or via Setup command-line parameters (as discussed in the next section).

   **Note** If you create the system partition in a preinstallation environment without restarting the computer, add the /syspart and /tempdrive parameters to the Winnt32.exe command in the Unattend.bat batch file or the command that you use to start Setup.

To perform an automated installation of Windows from the Windows CD-ROM, follow these steps:

1. Start the computer from the Windows CD-ROM.

2. Immediately insert the floppy disk that contains the Unattend.txt file (renamed to Winnt.sif).

   If the BIOS boot order lists the CD-ROM before the floppy disk drive, you can insert the floppy disk before starting the computer.
Windows Setup does not support loading mass storage drivers or answer files from USB Flash Devices (such as USB sticks or thumb-drives). If the system BIOS supports floppy emulation, you might be able to use USB Flash Devices to load mass storage drivers or answer files, though the most reliable method is to use a real floppy disk.

### Initiating Setup Using Command-Line Parameters

You can streamline the setup process on a single machine by launching Windows Setup using command-line parameters; you can also use command-line parameters to specify an answer file to automate Setup completely.

To use a command-line parameter on a computer with Windows, boot the computer in Windows and open a command prompt window. Then type `[path]\winnt32.exe[parameter]`, substituting `[path]` with the location of the Windows setup files, and replacing `[parameter]` with the appropriate parameter or parameters you want to use. Table 5-5 shows the available parameters for Winnt32.exe, the 32-bit version of Setup.

---

**Table 5-5 Parameters for the Winnt32.exe command**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>/checkupgradeonly</td>
<td>Runs a compatibility test on the computer to see whether it has any problems that might interfere with upgrading the operating system. It saves a Winnt32.log report in the installation folder for Windows NT upgrades, or an Upgrade.txt report in the Windows folder for Windows 98/Windows Me upgrades.</td>
</tr>
<tr>
<td>/cmd:[command]</td>
<td>Runs the command following the /cmd: parameter after the Windows Setup Wizard completes.</td>
</tr>
<tr>
<td>/cmdcons</td>
<td>Enables the use of the Recovery Mode Console at boot time for repairing failed installations. You can use this parameter only after installing Windows.</td>
</tr>
<tr>
<td>/copydir:[folder name]</td>
<td>Names an additional folder you want Setup to copy into the folder in which it installs Windows (\Windows for Windows Server 2003 and Windows XP, and \WINNT for Windows 2000 and Windows NT). The folder remains after Setup completes, and you can copy additional folders by using the parameter multiple times. The folder might contain drivers or other files needed after setup. For example, create an <code>extra_drivers</code> folder in the <code>\i386</code> or <code>\amd64</code> source folder and use the <code>copydir:i386\extra_drivers\</code> parameter.</td>
</tr>
</tbody>
</table>

---

Note If you have access to Windows PE, you can boot from a CD-ROM to a streamlined version of Windows XP or Windows Server 2003, which you can then use to prepare the computer and launch Setup. Original equipment manufacturers (OEMs) can create customized Windows PE CD-ROMs using the OEM Preinstallation Kit (OPK); enterprise users can use the Windows PE For Corporations Toolkit, available from your account manager.
### Table 5-5 Parameters for the Winnt32.exe command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>/copysource:[folder name]</td>
<td>Names an additional folder you want Setup to copy into the folder in which you install Windows. Setup deletes the folder near the end of GUI-mode Setup.</td>
</tr>
<tr>
<td>/debug[level:filename]</td>
<td>Creates a debug log file with the specified level. The default creates a log file named C:\Windows\Winnt32.log with the level set to 2 (Warning).</td>
</tr>
<tr>
<td>/dudisable=yes</td>
<td>Disables dynamic update during setup, even if an answer file specifies dynamic update locations.</td>
</tr>
<tr>
<td>/duprepare:[folder name]</td>
<td>Extracts any Dynamic Update packages downloaded from the Windows Update Web site that reside in the specified folder, and prepares it for use as a local Dynamic Updates source for clients.</td>
</tr>
<tr>
<td>/dushare:[folder name]</td>
<td>Specifies the location for Setup to search for Dynamic Update files. To create such a share, download and extract Dynamic Update packages from the Windows Update Catalog and then run the /duprepare command on the folder.</td>
</tr>
<tr>
<td>/ems-baudrate:[baudrate]</td>
<td>Specifies the baud rate to use with the EMS serial port. Valid rates are 9600 (default), 19200, 57600, and 115200.</td>
</tr>
<tr>
<td>/emsport:[comport]</td>
<td>Specifies the communications port (COM port) EMS must use for remote troubleshooting. (See Chapter 40 for more information.) Replace comport with com1, com2, off, or usebiossettings. (Com1 and Com2 work only with x86 systems.)</td>
</tr>
<tr>
<td>/m:[folder name]</td>
<td>Specifies the location of a folder containing system file replacements. Setup checks this folder first for files to copy and then checks the installation folder.</td>
</tr>
<tr>
<td>/makelocalsource</td>
<td>Tells Setup to copy all installation files to the local hard disk so that the files are available later during the installation if the Windows CD-ROM or network share is inaccessible.</td>
</tr>
<tr>
<td>/noreboot</td>
<td>Tells Setup not to restart after the initial Windows file copy phase of Setup is complete. This allows you to run additional commands before continuing.</td>
</tr>
<tr>
<td>/s:[sourcepath]</td>
<td>Specifies the location of the Windows Setup files. (The default is the current folder.) This must be a full path—for example, X:\path or \server\share\path. To specify multiple paths for Setup to search for needed files, use multiple /s: parameters. (You can speed transfers by specifying the path to multiple servers that host the same source files.) Setup fails if the first server is not available.</td>
</tr>
</tbody>
</table>
As you can see, many of these parameters piggyback onto other parameters, and pretty soon you can find yourself typing (and sometimes retyping) long strings at the command prompt. If you end up doing this a lot, create a batch file (a text file with the .bat extension) containing the setup command and parameters. Then simply launch the batch file instead of typing all the parameters.

To use a command-line parameter on a computer without an existing copy of Windows, boot the computer with a Windows 98 boot disk (or use Windows PE and Winnt32.exe). Then, at the command prompt, type `\[path]\winnt.exe[parameter]`, substituting the location of the Windows Setup files for [path]. Table 5-6 shows the available parameters for use only with Winnt.exe, the 16-bit version of Setup.

### Table 5-5 Parameters for the Winnt32.exe command

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>/syspart:[drive letter]</td>
<td>Specifies the hard disk to which you want to copy the Setup startup files. Setup makes this disk drive active and then stops, allowing you to remove the disk and insert it in another computer if you want. When you boot the computer next, text-mode Setup automatically starts. You must use the /tempdrive parameter with the /syspart parameter (both pointing to the same drive). You can't run this command from within Windows 98 or Windows Me.</td>
</tr>
<tr>
<td>/tempdrive:[drive letter]</td>
<td>Specifies the drive on which you want to store temporary files during Setup. For clean installations, this also specifies on which drive to install Windows.</td>
</tr>
<tr>
<td>/udf:[id,UDF file]</td>
<td>Specifies the uniqueness database file (UDF) Setup uses to modify an answer file. The ID identifies data in the UDF file that Setup uses in a corresponding section of the answer file. For example, /udf:ComputerName,our_company.udf takes the Computer Name from the UDF instead of from the answer file. If you do not specify a UDF, you are prompted to insert a disk that contains the $Unique$.udf file.</td>
</tr>
<tr>
<td>/unattend</td>
<td>Upgrades the previous version of Windows in unattended mode, taking all settings from the previous installation. OEMs should not use this option on computers sold to end users.</td>
</tr>
<tr>
<td>/unattend:[num:answer file]</td>
<td>Launches Setup in unattended mode by using the answer file you provide. The num parameter specifies the number of seconds to wait after copying files before restarting the computer.</td>
</tr>
</tbody>
</table>
Troubleshooting Installations

Installing Windows is a relatively painless process; however, when Setup fails for some reason or another, life gets more difficult. Fortunately, you can easily solve most installation problems. The follow sections cover the most common problems; you can find additional troubleshooting procedures in Chapter 40.

More Info You can find additional troubleshooting help either in the Windows Help System’s troubleshooters (which is, admittedly, not much good unless you have access to a functioning Windows 2000, Windows XP, or Windows Server 2003 machine) or in the Microsoft Knowledge Base, available at http://support.microsoft.com.
Setup Freezes or Locks Up

Sometimes Windows Setup inexplicably locks up during the installation process. If you receive a Stop Error message, write it down and consult either the Stop Errors troubleshooter in Windows Help or Microsoft technical support.

In general, these failures are intermittent and do not come with anything as helpful as an error message. First, restart the system by pressing Ctrl+Alt+Del. Do this repeatedly, if necessary. If you get no response, press the Reset button on the computer or turn the system off, wait 10 seconds, and then turn it back on. If you see a Boot menu, choose the Windows Setup option to allow Windows Setup to attempt to continue with its installation. If no Boot menu appears, launch Setup again. In either case, do not choose to repair the installation, but instead choose to continue with Setup.

Setup usually detects that an error occurred with its last attempt to install Windows and compensates by using a safer method of installation. If Setup hangs or stops responding again, repeat this process. Sometimes, Setup hangs multiple times before it finishes installing Windows, so be persistent. If installation freezes at a particular part of Setup, try choosing simpler setup options, if applicable.

Other procedures you can use to fix setup problems are as follows:

- Disable the system cache (processor cache) in the BIOS, and then run Setup again. Consult the hardware documentation for information about the correct procedure to do this. After Setup is complete, enable the cache again to avoid a significant performance loss.

- Try adding a wait state to the RAM in the system BIOS. This can help with partially faulty RAM chips. (However, if this server is important, plan on replacing that iffy RAM before doing any critical work on the machine.)

- Verify that the same company manufactures the RAM modules and are of the same speed and type. Although this is not a necessity, it can often eliminate problems.

- Switch the order of the RAM modules, or remove some modules and try installing them again.

- Test the RAM modules for faulty RAM chips with a third-party software program. Replace any faulty modules and run Setup again.

- Check the computer for a Master Boot Record (MBR) virus by booting it from a floppy disk that you have checked for viruses, and then run a virus-checking program and scan the drives for any viruses. If you find any viruses, clean them from the system and run Setup again.
Real World  ACPI BIOS Compatibility Problems

If Setup consistently freezes during the Windows-based Setup Wizard and the system has an ACPI-compatible BIOS dated January 1, 2000 or earlier, the BIOS might not function in ACPI mode with Windows. The freezes can happen at any time during the Setup Wizard, although they most frequently happen during the device-detection phase. If you suspect the BIOS is not working properly with Windows, download the latest version from the system vendor.

If you still have trouble or if no updated BIOS is available, try disabling ACPI during Setup by pressing F5 at the beginning of the text-mode phase of Setup, right after it prompts you to press F6 to install third-party storage drivers. If this does not solve the setup problems, you do not have a problem with the ACPI support in the BIOS. (ACPI support can be added back only by reinstalling Windows, usually by performing a same-version upgrade.)

You can also manually enable or disable ACPI support after the file copy phase of Setup completes, right before the computer restarts in the Windows Setup Wizard. (Sometimes you can do this after the system freezes during the Setup Wizard.) To force Windows to enable or disable ACPI support, follow these steps:

After the text-mode phase of Setup completes but before Windows restarts in the Setup Wizard, go to a command prompt and follow these steps:

1. Type `attrib -r -s -h `c:\txtsetup.sif` at the command prompt.
2. Open the `c:\Txtsetup.sif` file by using the edit command or another text editor, and search for “ACPIEnable=.”
3. To force ACPI support to be enabled, which sometimes fixes setup problems, change the ACPIEnable= value to 1.
4. To disable ACPI support, change the ACPIEnable= value to 0.
5. Save the file, and restart in the Windows Setup Wizard.

Again, if any steps you take reveal questionable hardware, replace the hardware before you rely on the computer to store important data or provide critical functions to users.

Setup Stops During File Copying

If Setup locks up while copying files, you might have a problem with Integrated Device Electronics (IDE) drive configuration. Try one of the following solutions.

Reboot the machine by using Ctrl+Alt+Del or Reset, and go into the system BIOS. Verify that the IDE controllers are enabled and configured properly. Make sure that the BIOS
detects any IDE hard disks or CD-ROMs properly. (You might have to restart the system and watch the display to verify this because often the BIOS does not display drives inside the BIOS.) After doing this, one or more of the following tasks might be useful:

■ Check the physical jumper settings on the drives to make sure they are properly configured to have one master and a maximum of one slave per IDE channel.

■ If the CD-ROM drive is on the same channel as the hard disk, move it to the secondary channel and configure it to be the master.

■ Try lowering the data transfer rate for the drives; for example, configure the drives to use PIO mode 2 instead of Ultra DMA mode or Ultra 66 transfer mode.

■ Check to make sure that the drives are cabled correctly and that the cables are not faulty.

■ Check the hardware settings to make sure the hard disk controller is not conflicting with another device. Try removing all cards from the computer except for the display card and SCSI adapter (if you are using a SCSI drive), and run Setup again. If Setup succeeds, add the cards one by one after installation, and use the Hardware Wizard in Windows 2000 to configure the devices and troubleshoot any hardware conflicts you encounter.

---

**Note** Windows Server 2003 provides a variety of tools you can use to boot a system that does not want to start, including the Safe Mode and Last Known Good Boot options, as well as the Recovery Mode Console, which allows you command-line access to an NTFS or FAT drive that will not boot. (See Chapter 40 for more information.)

If none of this helps, try the recommendations in the previous section or consult the Microsoft Knowledge Base.

**Previous Operating System Will Not Boot**

When you install Windows on a computer that’s already using an operating system and you choose not to upgrade, Setup creates a dual boot so that you can select which operating system you want to use at boot time.

If the computer never displays the Windows Loader menu that allows you to choose the previous operating system, the problem is most likely one of two issues: either the Boot.ini file has a timeout set to 0 (and thus doesn’t display the Boot menu), or the MBR was overwritten during Setup, preventing you from starting the previous operating system even if you have the proper entry in the Boot.ini file.
Changing the Default Operating System and Boot Times

To change which operating system Windows boots by default, as well as to control how long Windows displays a choice of operating systems at boot time, follow these steps:

1. Click Start, choose Control Panel, and then choose System.
2. Click the Advanced tab, and then click the Settings button in the Startup And Recovery section.
3. Select the operating system you want to boot by default from the Default Operating System list.
4. Select the Time To Display List Of Operating Systems check box, and specify the number of seconds you want the Boot menu displayed.

You can also do this by manually changing the timeout value in the Boot.ini file to a value higher than 0. To do this, click the Edit button in the System Startup section of the Startup And Recovery dialog box (described in step 4), or to edit the file from a command prompt, type `bootcfg /timeout N`, where N is the number of seconds you want the Boot menu displayed. (For more information about the Boot.ini file, see Chapter 40.)

**Note** You can force the Windows Boot menu to display at startup by holding down the spacebar after the BIOS displays the power-on self test (POST) screens. This displays the Hardware Profile/Configuration Recovery screen. Press F3 to display the Windows Loader screen with no timeout value.

Restoring the MBR of the Previous Operating System

If the previous operating system still does not boot properly, you might need to re-create the MBR for the operating system that you previously installed. This is risky business, so make sure you have the time to reinstall your operating system and restore a backup if you run into trouble.

**Note** If your previous operating system is Windows NT, Windows 2000, or Windows XP, see the startup troubleshooting section of Chapter 40.

To re-create the MBR for a version of Windows 95, Windows 98, or Windows Me, use the following steps:

1. To restore a version of Windows 95, Windows 98, or Windows Me, boot your computer with a boot disk for the operating system you are unable to boot. (Verify that the disk contains the Sys.com file.)
2. Type `A:\sys c:` at the command prompt to transfer the system files from the floppy disk to the hard disk.
3. Remove your floppy disk and restart your computer. Verify that the operating system you wanted to repair boots properly before performing the next step.


5. When Windows Setup launches, press Enter to begin, and then press R to display the Windows Recovery Console.

6. Choose the Windows installation to log on to and then type the administrator password.

7. Type `fixmbr` to write a valid MBR for your system.

8. Type `bootcfg /list` to display which operating systems the Boot.ini file lists. If the Boot.ini does not list an operating system, type `bootcfg /rebuild` to add operating systems back to the list.

9. Restart your computer, and choose the appropriate operating system from the Windows Loader menu.

10. If the Windows Loader menu still is not available or your current version of Windows still does not boot, return to the Recovery Console (covered in steps 4 through 6) and type `fixboot c:` (where `c:` is the system drive for your current version of Windows). Restart your system, and boot it in the desired operating system.

---

**Summary**

Deploying Windows to clients and servers is an essential task on most networks. You can save time by choosing an installation method that provides the best compromise between speed, control, and complexity. You can perform small deployments quickly and easily using the Windows CD-ROM and an answer file you create using Setup Manager. For larger deployments, you can create a deployment environment that allows you to automate virtually the entire installation process by using distribution shares, RIS, ADS, SMS, or disk imaging.
Chapter 6

Upgrading to Windows Server 2003

Architectural Changes Since Windows NT 4.0 ................................. 106
Planning a Windows NT Domain Upgrade ................................. 114
Preparing Domains and Computers ............................................. 137
Updating the Active Directory Schema ........................................ 140
Upgrading Clients to Windows XP .............................................. 147
Upgrading Servers to the Windows Server 2003 Family ................. 149
Switching Forest and Domain Functional Levels .......................... 151
Summary ................................................................................. 158

The easiest way to install Microsoft Windows Server 2003 on a computer while preserving existing domain information, programs, and computer settings is to perform an upgrade installation. This process is easy for member servers and standalone servers, and even easier when upgrading a Windows Server 2003 server to Windows Server 2003 R2. (The process is akin to installing a Windows feature pack.)

Upgrading domain controllers to Windows Server 2003 is more complex, particularly when upgrading a Windows NT 4.0 domain to Windows Server 2003. Before you upgrade a Windows NT 4.0 domain to Windows Server 2003, document the existing network and plan the upgrade process (including whether to perform a domain restructure). Then prepare the domain and computers, and perform the upgrade according to your plan (which states the order in which to upgrade servers and domains, among other things).

To upgrade a Windows 2000 domain controller to Windows Server 2003, or a Windows Server 2003 domain controller to Windows Server 2003 R2, you must update the Active Directory forest and domain schemas before upgrading the operating system itself.

This chapter discusses all these tasks as well as the architectural changes in Windows since Windows NT 4.0, how to upgrade client computers to Windows XP, and how to upgrade the Active Directory functional level to enable advanced functionality after the upgrade is complete.
To install Windows Server 2003 R2 on a member server or standal-
one serve, skip ahead to the "Upgrading to Windows Server 2003" section; to
upgrade or add a Windows Server 2003 R2 domain controller to an existing
Active Directory forest, first refer to the "Preparing Domains and Computers" sec-
tion of this chapter.

Architectural Changes Since Windows NT 4.0

Windows 2000 and the Windows Server 2003 family introduce numerous architectural
improvements as well as some changes to the way Windows domains work. The following
sections discuss the changes that are relevant to upgrading: the types of server roles avail-
able and the type of domain trusts that are used; new support for devices; Plug and Play
(PnP); Power Management; and of course, the addition of the Active Directory service.

Domain Controllers and Server Roles

In Windows 2000 and the Windows Server 2003 family, the types of server roles are
slightly different from those available in Windows NT. Windows NT 4.0 servers can
have one of four roles: primary domain controller (PDC), backup domain controller
(BDC), member server, and standalone server. Windows 2000 and the Windows Server
2003 servers can have one of three roles: domain controller (DC), member server, and
standalone server.

Note  Windows Server 2003 also uses the term "server role" to describe the
function a server performs—for example, file server, print server, or SharePoint
server.

Server Roles in Windows NT 4.0

Windows NT domains are single-master based, with the PDC serving as the master repos-
itory for a given domain. The PDC must carry out all changes to the domain. BDCs serve
as working backups to the PDC and reduce the load on the PDC by serving client
requests themselves. BDCs maintain a current copy of the domain by synchronizing peri-
odically with the PDC; you can upgrade a BDC to the PDC if the PDC server fails or is
taken out of service.

Member servers are simply Windows NT servers that belong to a Windows NT domain
and are not domain controllers. Member servers usually perform file sharing or print
sharing or run some other type of server software, such as Web, Domain Name System
(DNS), or Dynamic Host Configuration Protocol (DHCP) server software. You can’t
upgrade a Windows NT 4.0 member server to a PDC or BDC without a clean reinstallation of Windows NT, and you can't demote a PDC or BDC to a member server without reinstalling Windows NT.

Standalone servers are Windows NT servers that do not belong to a Windows NT domain and are instead part of a workgroup. It is important to understand that although a standalone server doesn't belong to a Windows NT domain, it isn't limited in its duties as a server. It can still act as a DNS, DHCP, or other type of server, but it can't act as a central repository for user and group data like a PDC or BDC can. To upgrade a standalone server to a PDC or BDC, you must reinstall Windows NT.


The member server and standalone server roles are unchanged for the Windows 2000 Server and Windows Server 2003 families, but Windows 2000 and Windows Server 2003 replace the PDC and BDC roles with a single domain controller role. Domains in Windows 2000 are finally multiple-master based, with all Windows 2000 or Windows Server 2003 domain controllers acting as peers to one another. Any domain controller can make changes to the domain at will. All domain information is stored in Active Directory, which the File Replication Service (FRS) replicates between all domain controllers. The tradeoff is that Windows 2000 and Windows Server 2003 domain controllers cannot exist on a Windows NT domain until you upgrade the PDC of the domain to Windows 2000 or Windows Server 2003. For more information, see the “Planning a Windows NT Domain Upgrade” section of this chapter.

You can promote Windows 2000 and Windows Server 2003 member servers and standalone servers to domain controller status, and you can demote domain controllers to member servers or standalone servers without reinstalling the operating system—the only way to demote a BDC under Windows NT. However, as always, it's preferable not to make more role changes than necessary.

Active Directory

Active Directory is probably the most important new feature in the Windows 2000 Server and Windows Server 2003 family. It is a scalable, easily administered, fault-tolerant directory service that is required by Windows 2000 and Windows Server 2003 domain controllers. Active Directory is also the usual repository for the DNS server database on Windows 2000 and Windows Server 2003 DNS servers.

Chapter 13 and Chapter 14 discuss Active Directory in detail, so this chapter addresses it only briefly to review a few points relevant to upgrading Windows NT domains to Active Directory.
Active Directory Domains

Although Active Directory doesn't make fundamental changes to the way domains work for end users, it does introduce some important domain structures that affect the way you approach domain design. Active Directory, like the directory service in Windows NT, uses domains as the core unit of logical structure. Domains help organize the network structure to match the organization of the company. Each domain requires at least one domain controller (and preferably more) to store the domain information, and each domain controller can make changes to the domain. See Chapter 3 for more about domain planning.

Active Directory domains use DNS names for domain names instead of the Network Basic Input/Output System (NetBIOS) naming structure of Windows NT domains (although Windows 2000 Server and Windows Server 2003 generate NetBIOS names for backward compatibility). Active Directory domains are hierarchically organized—as required by DNS. Active Directory refers to hierarchically organized groups of domains with a contiguous namespace trees, and groupings of trees with noncontiguous namespaces are known as forests. For example, example.local and all subdomains (support.example.local, finance.example.local, and so forth) belong to a single tree; while a different division of the company (example.com, for example) has its own tree in the forest. Because the companies share their networks and administer them together, they belong to the same forest; the suppliers and partners of the companies would have their own forests. You can establish trust relationships between the forests as necessary to allow them to do business with one another more easily.

Active Directory domains are nearly identical between Windows Server 2003 and Windows 2000 Server; however, upgrading the functional level of a forest and relevant domains to one of the Windows Server 2003 functional levels provides enhanced Active Directory management capabilities, including the ability to rename and move domains within or between forests. For more information, see the “Switching Forest and Domain Functional Levels” section of this chapter.

Sites and Organizational Units

Active Directory also introduces the concepts of sites and organizational units (OUs). A site is a group of one or more Internet Protocol (IP) subnets that share local area network (LAN) connectivity. Within a site there can be one or more domains, or a single domain can span multiple sites. See the “Planning the Site Topology” section later in this chapter for further information.

Organizational units (OUs) are similar to domains in that they are containers for network objects such as user accounts and resources. Unlike domains, however, they do not mark a security boundary, and creating OUs doesn’t require adding domain controllers (because OUs exist within a domain and thus make use of the existing domain controller infrastructure). OUs in Active Directory provide an excellent way to provide organization
within a domain without the need for additional security policies and domain controllers. You can easily convert OUs to domains, and domains to OUs, which makes them very flexible. See Chapter 9 for more information about the uses and creation of OUs.

Forest Root Domains
The first domain you create in Active Directory automatically becomes the forest root domain—the top-level domain in the Active Directory hierarchy. If you create additional domain trees (with their own contiguous namespaces), Active Directory creates transitive two-way trusts between the trees and the forest root domain, as if the trees were child domains. Indeed, from a trust and replication perspective, it appears that the subsequent trees are children of the forest root, even though they use completely different namespaces.

Besides its significance as the hub of replication between trees, the forest root domain also contains the Enterprise Admins and Schema Admins groups, which have forest-wide administrative scope.

Because the forest root domain is so important, fault-tolerance and recoverability is critical. If a regional catastrophe wiped out all domain controllers and backups in the forest root domain, the Enterprise Admins and Schema Admins groups would be forever lost, and you would have to re-create the entire forest.

To help reduce the need to alter the forest root domain, you can create a dedicated forest root domain exclusively for forest-level administration and replication, and place the majority of accounts and resources in child domains. Because there are few user accounts and resources in a dedicated forest root domain, Active Directory structures that consist of a dedicated forest root and a single child domain are often said to be using the Single Global Domain Model. Active Directory structures that consist of a dedicated forest root with multiple child domains are referred to as using the Regional Domain Model—a nod to the fact that the child domains are often organized geographically.

Note You cannot easily retire or change the forest root domain, even if the organization changes. However, you can rename the forest root domain if the forest uses the Windows Server 2003 functional level, though you cannot move or delete it.

Trust Relationships
Trust relationships are an important component of large networks that consist of multiple domains. Simply stated, a trust relationship is a policy that enables users from one domain to access resources in another domain.
For example, say that a user, Susan, in the domain Administration, wants to access a resource in the domain Manufacturing, and that the Manufacturing domain trusts the Administration domain. When Susan attempts to access the resource, the resource must verify that she has an account that has permission to access it. To authenticate Susan, the resource in the Manufacturing domain contacts its local domain controller (DC, BDC, or PDC), which in turn queries a domain controller in the Administration domain and verifies that Susan has a valid account and that the account belongs to a group permitted to access the resource.

**Trust Relationships in Windows NT 4.0**

Among and between Windows NT 4.0 and earlier domains, all trusts are nontransitive, meaning that each trust is a one-way relationship between two domains that you must explicitly create. For two domains to trust each other, you must create two separate trust relationships—one for each direction.

A nontransitive trust is also strictly limited. For example, suppose that the domain Finance also trusts the domain Administration (as shown in Figure 6-1). When nontransitive trusts are involved, this statement tells you only that the Finance and Manufacturing domains both allow users from the Administration group access to their domains. It does not tell you anything about the relationship between the Finance and Manufacturing domains, nor does it indicate whether Administration, in turn, allows either Finance or Manufacturing to authenticate users. You must create each trust relationship separately and explicitly.

*Figure 6-1  Three domains under Windows NT 4.0 and under Windows 2000*
Trust Relationships in Active Directory

Active Directory introduces transitive trusts. Transitive trusts are always two-way, and they support pass-through authentication. Creating a trust between the Administration and Manufacturing domains (now probably called administration.example.local and manufacturing.example.local) automatically means that users in each domain can be authenticated and be eligible to access resources in the other domain (though they still need to have proper permissions, of course).

Pass-through authentication comes into play with child domains. With Active Directory domains, users in the child domain can use the parent domain’s trusts by means of the automatic two-way transitive trust that Active Directory creates between the child domain and the parent domain. For example, let’s say you create a widgets.manufacturing.example.local child domain. Users in this domain are automatically eligible to access resources in the manufacturing.example.local domain (the parent domain) as well as the example.local domain (the parent domain of the parent domain—the grandparent domain, if you will).

Transitive trusts become available after you upgrade a domain to Active Directory. Despite some confusion over the matter, they do operate in domains that use the Windows 2000 mixed functional level and work between trees in a forest, but they do not apply to remaining Windows NT domains in your company or to clients connected to Windows NT BDCs. (These domains and clients rely on existing one-way nontransitive trusts.) Explicit one-way trusts are also available between Active Directory–based domains, but you must create them manually.

Windows Server 2003 provides additional capability to set up one-way or two-way transitive trusts between forests, and the ability to rename and move domains within and between forests after you upgrade the forests to the Windows Server 2003 forest functional level.

Real World  Whom Do You Trust?

The question of transitive trusts arises in large multidomained enterprises. Active Directory domain controllers automatically use transitive trusts when communicating with other Active Directory domain controllers, even in domains that use the Windows 2000 mixed functional level. The existing trusts remain in place for use by Windows NT BDCs until you switch the domain to the Windows 2000 native or Windows Server 2003 functional level. Trusts that you add to or take from Windows NT domains are the nontransitive trusts that you explicitly and deliberately set. This means that if you are creating a new Active Directory domain, you must manually create trusts with existing Windows NT domains.
Table 6-1 shows the possible trust relationships between different types of domains.

Table 6-1  Trust relationships between domains of different types

<table>
<thead>
<tr>
<th></th>
<th>Windows NT Domain</th>
<th>Active Directory Domain (Same Forest)</th>
<th>Active Directory Domain (Different Forest)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows NT Domain</td>
<td>One-way trust*</td>
<td>One-way trust*</td>
<td>One-way trust*</td>
</tr>
<tr>
<td>Active Directory Domain (Windows 2000)</td>
<td>One-way trust*</td>
<td>Two-way transitive trust (One-way trust available)</td>
<td>One-way trust*</td>
</tr>
<tr>
<td>Active Directory Domain (Windows Server 2003 forest functional level)</td>
<td>One-way trust*</td>
<td>Two-way transitive trust (One-way trust available)</td>
<td>Two-way transitive forest trust (One-way trust available)</td>
</tr>
</tbody>
</table>

* You can establish one-way trusts in both directions, simulating a two-way trust.

**Hardware Support**

Hardware support for the Microsoft business operating systems has come a long way. Windows 2000 shed the Windows NT legacy of nonexistent drivers, device configuration nightmares, and poor support for modern technologies by introducing top-of-the-line hardware support for the whole alphabet soup: Plug and Play (PnP), Universal Serial Bus (USB), Institute of Electrical and Electronics Engineers (IEEE) 1394 (Firewire), and Advanced Configuration Power Interface (ACPI) device configuration and power management.

**Note**  An up-to-date, ACPI-compatible BIOS is required for full use of PnP and power management. The ACPI BIOS should support the Advanced Programmed Interrupt Controller (APIC) standard, which raises the 15 interrupt request (IRQ) limit and enhances IO performance as well. (All multiprocessor systems support APIC, as do all systems certified for use with Windows Server 2003 or Windows XP.) If the system doesn't boot after upgrading a standard Programmed Interrupt Controller (PIC) BIOS to APIC operation, restore the old BIOS or reinstall the operating system. Windows Server 2003 supports legacy Advanced Power Management (APM) and PnP BIOSs, but their features are limited.

Device drivers in Windows 2000 also changed to enhance system stability and to increase the number of devices supported. Windows 2000 supports the Win32 Driver Model (WDM), enabling most WDM drivers to work interchangeably with Windows 2000, Windows XP, Windows Server 2003, Windows 98, and Windows Me. Device Driver Signing triggers an alert when you install drivers that Microsoft hasn't tested and
digitally signed. (Administrators can create policies blocking the installation of unsigned drivers.) Microsoft also fine-tuned the driver model to reduce system instability and to facilitate PnP and power management. Windows XP added device driver rollback, and support for CD-RW drives and USB 2.0 devices. Windows Server 2003 added support for Fibre Channel, Hot Plug PCI, and storage area networks (SANs), among other technologies.

However, broad device driver availability is only part of the equation for servers. Because device drivers are one of the leading causes of system instability, simply having a driver isn’t enough. It is very important that servers use only device drivers that are Microsoft certified and digitally signed.

**Note** The vast majority of Windows 2000 drivers work fine in Windows XP and Windows Server 2003. Although many Windows NT 4.0 drivers work in Windows Server 2003, they do not support power management or Plug and Play and can more easily decrease the stability of the operating system. For this reason, most companies use Group Policy to block the installation of Windows NT 4.0 drivers.

Windows 98 and Windows Me WDM drivers often work fine on Windows XP systems, but avoid them on servers for stability reasons—drivers are a leading cause of system crashes. Windows 95, Windows 3.x, and MS-DOS drivers absolutely don’t work in Windows 2000, Windows XP, or Windows Server 2003.

**Software Support**

Software support, like hardware support, is another area where Windows has made great advances since Windows NT 4.0, which is largely incapable of running applications written for other versions of Windows, such as Windows 98. Windows Server 2003 and Windows XP run many popular Windows 98 and Windows Me applications out of the box and support many more with Application Compatibility Updates, which are available from Microsoft Update (http://update.microsoft.com/microsoftupdate).

Windows XP and Windows Server 2003 also provide special compatibility modes that simulate key aspects of the Windows 95, Windows 98, Windows NT, or Windows 2000 operating systems, allowing end users to take additional steps to run incompatible programs. Microsoft also provides the Application Compatibility Toolkit (see http://www.microsoft.com/technet/prodtechnol/windows/appcompatibility/default.mspx) that administrators can use to inventory deployed applications, evaluate any compatibility problems, and create custom compatibility fixes for the applications. See Chapter 29 for more information about application compatibility technologies.
Note Upgrading an existing Windows 98–based or Windows Me–based system presents additional complexities. Vendors often have one version of their software for Windows 98 and Windows Me, and another for Windows NT, Windows 2000, and Windows XP. Furthermore, the same application is installed differently depending on the operating system involved. Consequently, many applications require vendor-provided migration files (upgrade packs) during the operating system upgrade, or they must be uninstalled and then reinstalled after the upgrade completes.

Planning a Windows NT Domain Upgrade

Upgrading a Windows NT 4.0 domain to Active Directory isn’t quite the three-click process that you perform when upgrading a single Windows NT 4.0 workstation to Windows XP. In fact, considerable planning is necessary before you even start Windows Setup on the first computer. You must upgrade some computers, such as the PDC and BDCs, in a specific order, while you can upgrade other computers, such as client computers and Windows NT member servers, at any time.

The following sections are essential for anyone planning a Windows NT 4.0 domain upgrade. They cover documenting an existing network, making a recovery plan, planning the Active Directory forest, and developing an upgrade strategy. Subsequent sections cover preparing for the upgrade, the actual upgrade process, and finally, switching an upgraded domain into native Windows 2000 or Windows Server 2003 mode.

Note You must upgrade the Active Directory schema before adding Windows Server 2003 domain controllers to an existing Windows 2000 Active Directory forest or before adding Windows Server 2003 R2 domain controllers to a Windows Server 2003 or Windows 2000 Active Directory forest. See the “Updating the Active Directory Schema” section of this chapter for more information.

Choosing Whether to Upgrade or Migrate

If your current domain structure is unsatisfying, it might be tempting to start from scratch, migrating accounts and resources into a fresh Active Directory domain. Resist this impulse if possible.

When migrating to a new domain, you must select a new domain name (a political nightmare in its own right), update all existing links and e-mail addresses, and educate users how to log on and find resources in the new domain. In addition, it’s important to realize that everyone needs to sign off on a decision of this magnitude, and that can be tough. The decision to migrate to a new domain structure is political, not technical.
With that said, it makes sense to look at migrating to a new domain or domain tree if doing so makes it possible to merge two or three separate domains or trees into a single domain or tree. Just remember to carefully weigh the pros and cons and get everyone’s approval before tackling this complex issue. If you choose to migrate to a new domain, refer to the Active Directory for Microsoft Windows Server 2003 Technical Reference for information about the Active Directory Migration Tool (ADMT) and other tools that can help make migration easier.

**Note**  
An *in-place* domain upgrade is a domain upgrade that you perform while leaving the domain intact. You can also upgrade domains by removing the PDC from the domain, and upgrading it offline. Meanwhile, the BDCs provide services to the existing domain. After testing the upgraded PDC, bring it back into the production domain and upgrade the remaining BDCs.

### An Overview of the Active Directory Migration Tool (ADMT)

The Active Directory Migration Tool (ADMT) is a powerful program that you can use to migrate accounts, groups, trusts, profiles, and passwords from an existing Windows NT 4.0, Windows 2000, or Windows Server 2003 domain structure to a new Active Directory forest. This is useful when you want to perform a major domain restructure while minimizing downtime.

Before you can use ADMT to migrate to a new Active Directory forest, you must document the existing domains, trusts, groups, user accounts, service accounts, and computers: Then you must design and create the new Active Directory forest and domain trees. Once the new forest is operating properly, prepare for the migration by performing the following tasks (see the Active Directory Migration Tool Help system for a complete list):

- Enable remote registry access on all computers that you want to migrate.
- Switch the functional level of the target domain to Windows 2000 native or Windows Server 2003 functional level. (The source domain can be a Window NT 4.0 domain or an Active Directory domain with any functional level.)
- Create a temporary two-way trust between the source and target domains. A two-way trust allows you to use an administrator account from the source domain, which is more likely to have the proper permissions on the source objects. At a minimum, the source domain must trust the target domain.
Add a common administrator account to the local administrators group on every workstation and member server that you want to migrate. (You can use Active Directory Service Interfaces [ADSI] scripts to automate this.) Then use this account in ADMT to migrate these computers.

Disconnect any mapped network drives or connections between the source and target domains.

Identify or create a user account for the migration that has administrative privileges in the source and target domains, as well as Exchange Administrator privileges if you want to use the Exchange Directory Migration Wizard.

After preparing the source and target domains, install ADMT on a domain controller in the new forest and then use the ADMT wizards to perform the following tasks (ADMT installs the necessary agents on the source computers if you created the appropriate trusts and permissions):

- Perform a test run of each migration task, such as migrating user or computer accounts. ADMT allows you to perform a test migration without modifying the actual domains.
- Create migration reports for each migration test run, and analyze the reports for any problems.
- Fix any problems, and rerun the tests.
- Perform the migration in stages, and test the results of each migration stage.
- Use the Security Translation Wizard to update the access control lists (ACLs) for migrated objects to grant them appropriate permissions in the target forest.

See the Active Directory Migration Tool Help for additional information about migrating and restructuring domains using ADMT. You can download ADMT from the Microsoft Web site at http://www.microsoft.com/downloads by searching for “ADMT”.

Documenting the Existing Network

The first step in planning an in-place domain upgrade is to document the current network structure. To do so, take an inventory of the following network attributes:

- The existing domain model
- Existing trust relationships
- Account and resource domains
The sections that follow describe how to document each of these features.

**Important** Windows Server 2003 digitally signs all server message block (SMB) protocol communications by default for greater network security. Because of this, Windows 9x systems must install the DS Client Pack (found on a Windows 2000 Server CD-ROM in the \clients\win9x folder) and Windows NT 4.0 systems must be running Service Pack 4 or newer to access Windows Server 2003 domain controllers. Computers running Microsoft Windows for Workgroups or Mac OS X do not at present support SMB signing. If you can’t upgrade or retire these systems, you can disable this setting using Group Policy—the location is Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft Network Server: Digitally Sign Communications.

### The Existing Domain Model

The type of domain structure, or model, that the existing Windows NT domains use determines how you implement Active Directory trees and forests. Table 6-2 summarizes the types of domain models that might be in use.

**Table 6-2  Domain models available in Windows NT**

<table>
<thead>
<tr>
<th>Domain Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-domain</td>
<td>A single Windows NT domain</td>
</tr>
<tr>
<td>Single-master</td>
<td>One account domain and multiple resource domains</td>
</tr>
<tr>
<td>Multiple-master</td>
<td>Multiple account domains with two-way trusts between them and multiple resource domains that trust all master domains</td>
</tr>
<tr>
<td>Complete trust</td>
<td>Every domain is a resource domain and an account domain, with each domain trusting every other domain</td>
</tr>
</tbody>
</table>

### Existing Trust Relationships

Document existing trust relationships, and determine whether all trusts are still necessary. Windows preserves existing trust relationships during an upgrade to maintain compatibility with Windows NT 4.0 BDCs. However, Windows doesn’t import trusts with Windows NT 4.0 domains into Active Directory. Re-create these trusts in Active Directory before upgrading or taking the last BDC in the domain offline.

If you upgrade any domains into separate forests and want to maintain trust relationships between the forests, delete the existing trusts (which use NetBIOS domain names) after upgrading the PDC and re-create them using fully qualified DNS domain names. See Chapter 14 for information about working with trusts in Active Directory.
Account Domains and Resource Domains
Record the current number of account domains and resource domains. Also think about whether you want to restructure your domains, either before or after you upgrade the network to Active Directory.

DNS Namespaces
If the company has already deployed DNS, carefully document the namespaces currently in use. You cannot easily rename domains after you create them, and they must be unique on the network.

Server Software and Compatibility Issues
A crucial and sometimes forgotten step in documenting a network is to make an inventory of the servers. Record the server names, hardware capabilities, locations, operating system version, and service pack levels of the following types of servers, and evaluate any compatibility issues or problems with the servers before you begin the upgrade process:

- Domain Controllers You must upgrade the Windows NT 4.0 PDC before upgrading any other domain controllers in the domain or adding any Windows 2000 or Windows Server 2003 domain controllers if you want to maintain the existing domain. You can upgrade the BDCs after that.

Windows Server 2003 and Windows 2000 replace the LAN Manager Replication Service feature of Windows NT with the file replication service (FRS), which Windows installs automatically on all domain controllers. If you must maintain compatibility with the LAN Manager Replication Service, see Microsoft Knowledge Base Article 248358 or refer to the Microsoft Windows Server 2003 Resource Kit.

Note The preferred way to upgrade a domain is to purchase a new server to use as the PDC to upgrade. (Install Windows as a BDC, and then promote it to PDC.) This ensures that the computer is modern, compatible, and fast enough to adequately run Windows Server 2003. It also minimizes the amount of junk residing on the hard drive and in the registry, providing the “closest-to-clean installation” experience possible.

- File and Print Servers You can easily upgrade file and print servers to Windows Server 2003 or migrate the server settings and data to a server running Windows Server 2003. Migrating to a new server can yield performance gains from newer hardware and can also help consolidate servers. Use the Microsoft File Server Migration Toolkit (available for download at http://www.microsoft.com/windowsserver2003/upgrading/nt4/tooldocs/msfsc.mspx) or Print Migrator to streamline the migration process. (See Chapter 8 for information about migrating print servers.)
■ DNS, DHCP, and Windows Internet Name Service (WINS) Servers  Upgrade Windows NT 4.0 DNS, DHCP, and WINS servers to Windows Server 2003 or Windows 2000 Server to maximize functionality and to minimize problems.

■ Windows NT RRAS Servers  Windows NT 4.0 Routing and Remote Access Service (RRAS) servers need access to a real BDC for user information. They work erratically while on a mixed-mode Active Directory domain, and cease to work entirely after you upgrade the last BDC. For this reason, upgrade any Windows NT 4.0 RRAS servers before you start the domain upgrade process (if practical), or immediately after stabilizing the newly upgraded domain with two or more domain controllers.

Note  When setting up an Active Directory domain, the Active Directory Setup Wizard gives you the option of weakening the security settings for Active Directory to support pre–Windows 2000 clients. (They’re talking about Windows NT 4.0 RRAS servers here.) Don’t do it—instead upgrade or replace these servers with Windows 2000 or Windows Server 2003 RRAS servers.

■ Windows NT 3.51 Servers  If there are still Windows NT 3.51 servers or clients on your network, upgrade them or get rid of them. If you absolutely can’t part with your Windows NT 3.51 (or earlier) computers, leave an existing domain running under Windows NT 4.0 (or create one if necessary) and establish the appropriate trust relationship between this domain and your Active Directory structure. Just keep them off Active Directory domains.

Security Alert  Windows NT 3.51 computers joined to an Active Directory domain can deny access to user or group logon events, or they can incorrectly grant access to users or groups to which you have denied access. These difficulties and security breaches occur because of the way in which Windows NT 3.51 generates access tokens when a user logs on to the server.

■ NetWare Servers  Determine whether you want to synchronize Active Directory with Novell Directory Services (NDS). Check the release notes included on the Windows Server 2003 CD-ROM for any compatibility issues with NetWare. (Chapter 27 discusses interoperability.)
Samba Servers  Samba servers might require access to a real Windows NT 4.0 domain controller (instead of a Windows Server 2003 running the PDC emulator). Record the location and capabilities of any Samba servers on the network, and make a special note of whether they require access to Windows NT domain controllers. (If they do, postpone switching the network to a native mode until this issue is cleared up.) Many Samba servers also do not support SMB signing.

Other Application Servers  Evaluate all application servers carefully for known issues with Windows 2000, Windows Server 2003, and Active Directory.

Important  Windows NT 4.0 Enterprise Edition clusters cannot perform a rolling upgrade directly to Windows Server 2003. (A rolling upgrade allows the cluster to stay online while you upgrade each node one at a time.) To deal with this, either take the cluster offline and upgrade each node, or perform a rolling upgrade to Windows 2000, and then Windows Server 2003.

Choosing Whether to Upgrade Individual Servers
Upgrading a server preserves all settings and, when upgrading the PDC, allows you to keep the domain and all its user accounts and resources. However, performing a clean install yields the best performance and reliability. Here’s how you can balance these tradeoffs:

- Upgrade the PDC and any application servers that are difficult to set up.
- Retire any aging Windows NT servers, or repurpose them as desktop machines running Windows XP.
- Back up any relevant data, and then perform clean installs of Windows Server 2003 on any other Windows NT servers that are powerful enough to run Windows Server 2003. After installation is complete, restore the data. The File Server Migration Toolkit and Print Migrator tools can help with this process. (You can download them from http://www.microsoft.com/downloads.)
- Replace any retired servers with new Windows Server 2003 systems that serve whatever role you need.
Planning the Active Directory Forest

There are several steps to take when planning the Active Directory forest for your organization, including designing the Active Directory structure, choosing DNS names, and planning the site topology. This section briefly covers these steps. See Chapter 3 for additional information about planning the namespace and the domain structure. Refer to the Windows Server 2003 Resource Kit for more in-depth planning help.

Designing the Active Directory Domain Structure

When designing the Active Directory structure for an existing Windows NT–based network, take into consideration the current Windows NT domain model: single domain, single-master domain, multiple-master domain, or complete trust. (See Table 6-2 for a summary.) This section guides you through designing an Active Directory domain structure appropriate for your existing network model.

Note  When designing your Active Directory structure, start simple. If it’s possible to end up with a single domain, begin with that plan. Explore designs that are more complex than necessary, but go with the simplest design that fits—it’ll be easier to understand, administer, and troubleshoot (especially when you start using Group Policy).

Single-Domain Model

The Windows NT single-domain model consists of a single domain, with all accounts and resources stored together.

The single-domain model is easy to upgrade: the single domain under Windows NT becomes the forest root domain in Active Directory. You can then use OUs to organize the accounts and resources and to delegate some of the administrative burden.

Large domains and networks that might be reorganized at some point should consider creating a dedicated forest root domain (as described in the Real World sidebar “Using Dedicated Forest Roots”), and then upgrading the Windows NT domain as a child domain of the forest root. This requires additional resources and adds some complexity, but not as much as adding a normal domain would.

Single-Master–Domain Model

The Windows NT single-master–domain model consists of one master domain that contains all user accounts, and one or more resource domains that trust the master domain and contain only computer accounts and other resources.

If you have a single-master–domain model, create a dedicated forest root domain (discussed in the Real World sidebar “Using Dedicated Forest Roots”), and make the former master domain the first child domain. Then add the resource domains as second-level child domains.
If the company has a centralized network structure, after upgrading the domains to Active Directory and switching the master domain to Windows 2000 or Windows Server 2003 native mode, consider restructuring the domains into a single child domain. You can use OUs either to mimic the resource domains or to organize them more logically with the accounts and resources grouped and organized according to the company’s structure.

**Note** If you want to restructure or consolidate your domains, do so before using Group Policy.

Merging the resource domains back into a single child domain under the dedicated forest root offers a number of advantages. Because there are fewer domains to manage, the administrative burden is less. You can use OUs to create a detailed network structure without dealing with trusts. In addition, you can delegate administrative authority to the OUs, giving you the flexibility to handle the administrative tasks the way you want. You can also perform Active Directory queries faster and more efficiently in a single domain. Finally, because OUs don’t require domain controllers, there is the potential to free up some underused computing resources for other tasks. Figure 6-2 shows a single-master Windows NT domain converted to an Active Directory tree using a dedicated forest root domain, with a resource domain converted to an OU after switching the account domain to Windows 2000 or Windows Server 2003 native mode.

![Diagram](image)

**Figure 6-2** A single-master Windows NT domain converted to an Active Directory

A company with a more decentralized organization, or one with different business units, might want to keep multiple domains but convert its resource domains into full-fledged domains, with both resources and user accounts. (With Active Directory, there is no rea-
son to keep distinct resource domains.) This arrangement allows users to be in the same
domain as the resources they use, reducing traffic and making it easier for users to find
and access the resources they need. However, you must wait until you upgrade all rele-
vant domains and switch the target domain to Windows 2000 or Windows Server 2003
native mode before you can move the accounts. This is because an object that is moved
between domains loses its ability to access resources to which it formerly had access,
unless the native mode SIDHistory feature can provide the resources with the object’s old
security identifier (SID).

Note Third-party solutions can provide much of this organizational flexibility in
Windows NT 4.0, with the intent of permitting companies to restructure their
domains in a way that works well with Active Directory before they upgrade.

Real World Using Dedicated Forest Roots

Creating a dedicated forest root domain that consists solely of users and resources
involved in forest-wide administration has a number of advantages over a forest
root domain that does double-duty as a normal production domain. Advantages
include the following:

- The Domain Admins group exists to delegate administration of a domain;
  however, in the forest root domain this group can exert forest-wide control,
  which might not be a good thing. In a dedicated forest root domain, this isn’t
  a problem because the forest administrators (Enterprise Admins) also handle
  the domain administration tasks (normally performed by separate Domain
  Admins). Domain Admins in child domains do not have forest-wide control.

- A dedicated forest root domain provides a permanent, unchanging root for
  the Active Directory forest, facilitating future reorganization.

- Because a dedicated forest root domain contains an extremely small number
  of users and resources, it’s easily replicated and backed up. (Remember, if all
  domain controllers in the forest root domain are permanently lost, so are the
  Enterprise Admins and Schema Admins groups.)

- You can transfer the ownership of the forest root without affecting data and
  users in a production environment—they remain safely in one or more child
  domains.

As you can see, there are some good reasons Microsoft recommends using a dedi-
cated forest root domain. However, smaller networks should weigh these options
against the additional resources required by the domain—the forest root domain is
vital to Active Directory, and therefore is not a domain to neglect.
Multiple-Master–Domain Model
The multiple-master–domain model in Windows NT consists of a network with two or more master domains that contain all the user accounts, and multiple resource domains that trust each master domain and contain all the computer accounts and other resources. Large networks use this model to circumvent the Windows NT limit of 40,000 objects per domain.

Because of the flexibility and simplicity the Active Directory single-domain or single global domain models offer, many companies with a multiple-master–domain model choose to consolidate their domains into a single Active Directory domain (with or without a dedicated forest root domain) and use OUs to hierarchically structure their network. If you choose to consolidate the domains, create the forest root domain first (if applicable) and then perform the domain upgrades just as if you were going to preserve the existing domain structure. After you upgrade the domains and switch the target domain to a native-mode functional level, you can move all accounts into the single domain without the need to reassign permissions on the objects.

**Note** If you want to restructure or consolidate your domains, do so before using Group Policy.

To create a single-domain tree (with a contiguous namespace) during the domain upgrade, create a dedicated forest root domain and stabilize it with a couple of domain controllers. (See the Real World sidebar “Using Dedicated Forest Roots,” in the previous section.) Then upgrade the master domains one by one, adding them to the Active Directory tree as children of the forest root, which also serves as the tree root domain in this example. Figure 6-3 shows a multiple-master Windows NT domain converted to an Active Directory tree, with two resource domains converted to OUs after switching the account domains to native mode. After you upgrade the account domains, upgrade the resource domains and add them to the tree as children of the account domains (grandchildren of the forest root). Once the upgrade is complete, switch the account domains to a Windows 2000 or Windows Server 2003 native mode, and consider consolidating the resource domains into the account domains, using OUs when applicable.
Figure 6-3  A multiple-master Windows NT domain converted to an Active Directory tree

If you want to keep each master domain in an authoritative role, create a multiple-tree forest. First, create a dedicated forest root domain to serve as the root for the forest. Dedicate this domain exclusively to forest administration; do not create your users or resources in this domain. Then seed each master domain as the root for a new tree in the forest. (This is called the tree root domain.) In this case, it doesn’t matter which master domain you upgrade first, but you must upgrade the master domain for each tree before upgrading the resource domains.
Real World  Multiple-Master Domains and the Case for Domain Consolidation

The Windows NT multiple-master–domain model is widely used in larger organizations for several reasons. First, it allows the network to grow beyond the limitations of the single Security Accounts Manager (SAM) that single domains and single-master domains use. The SAM in Windows NT is stored in the system registry, and after it grows past 40 MB, performance degradation is noticeable. This means that the practical limit for a domain is 40,000 objects, with a maximum of 20,000 user accounts. To create more user accounts or objects than this in Windows NT 4.0, you must use a multiple-master–domain model.

The second reason that companies use a multiple-master–domain model in Windows NT is to allow for physically different network sites that don’t possess wide area network (WAN) connections that are fast and reliable enough to allow domain controller replication to take place without consuming an inappropriate amount of the WAN bandwidth. Using a master domain in each site gets around this lack of adequate connectivity because no replication takes place between master account domains and all the WAN bandwidth is available for other uses.

The third reason to use a multiple-master Windows NT domain structure is to reflect the company’s organization in cases where different parts of the company need to control their own resources and users. Each master account domain can have its own administrator, or you can use an administrator account in the dedicated forest root domain that belongs to the Enterprise Admins group, depending on the desires of the company.

Active Directory deals with these issues effectively, permitting many companies to move to a single-domain model (or at least to reduce the number of domains) and gain the advantages that model has to offer. Active Directory stores all domain information in its database (which is external to the registry and free to grow in size), and each domain stores only its part of the directory instead of one server storing the entire network schema. This enables you to scale the domain to millions of objects. No other domain is necessary; you can perform all organization with OUs. You can also create multiple physical sites, with a single domain spanning all sites and intersite replication set up to make the best use of slow WAN links. For help with consolidating domains, see the Solution Accelerator for Domain Server Consolidation and Migration: Windows NT 4.0 to Windows Server 2003, a set of documentation that provides prescriptive, tested, and supported help on planning, designing, deploying, and verifying a domain migration project. You can obtain this tool from the Microsoft Download Center at http://www.microsoft.com/downloads.
Using Structural Domains Elsewhere in an Active Directory Tree

A structural domain is simply a domain without user accounts or resources—it exists purely to form the structure of the domain (hence the name) as well as to aid in easy and efficient interdomain replication. The dedicated forest root domain is a type of structural domain (albeit one with the additional role of forest-wide administration, which does entail some user accounts and resources).

You can use structural domains elsewhere in the forest to create a domain hierarchy that is well suited to further restructuring. For example, by using a structural domain as a tree root domain (in addition to the forest root domain), you provide an unchanging anchor in the domain tree, under which you can move child domains without altering the higher-level domain structure.

Structural domains are also useful for replication between sites, especially when accessing or replicating the global catalog (GC), which is the master catalog for all objects in the host domain’s portion of Active Directory and a partial catalog of objects stored in other domains. If you have more than one site, you might choose to create a structural domain at the root that spans all sites and maintains a copy of the GC at each site. (You can also store a copy of the GC in the top-level local domain at each site and just use the structural domain as a link between the sites.) Having an on-site GC permits the local domains at all sites to concentrate on intrasite data processing and replication, with all intersite replication performed by the structural domain.

Using structural domains for replication also makes setting up and maintaining replication links easier. Child domains simply replicate upward to the parent domain, obviating the need to know the name of each domain you need to replicate with.

As you can see, using structural domains has a number of advantages; however, you must balance these advantages with the increased complexity and resources required for additional domains. A simple Active Directory structure makes administration and reorganization easier, and it permits the more efficient placement of domain controllers.
Complete-Trust Model
The Windows NT complete-trust model involves multiple domains that all trust each other.

Highly decentralized companies or companies that implemented domains in a piecemeal fashion and gradually connected them often use the Windows NT complete-trust model. The model provides a lot of autonomy and flexibility for each master domain, but it also results in a large administrative burden.

When upgrading an enterprise that uses the complete trust model to Active Directory, many companies try to consolidate their domains into a single tree or even a single domain. If you want to maintain the autonomy of the current domain structure of the complete-trust model, set up each current master domain as a new tree root domain. When you create the Active Directory structure like this, you automatically reduce the amount of administration necessary, as all trusts between domains in an Active Directory tree or forest are automatically transitive. (If this is undesirable, create multiple forests.)

When you upgrade the network, first create the forest root domain, preferably by creating a dedicated forest root. (You could also upgrade an existing domain and seed it as the forest root, although Microsoft discourages this.) When you have the forest root domain up and running with a couple of domain controllers, you can upgrade the account domains and add them as children of the forest root or as roots in new trees. If necessary, after upgrading domains, you can replace any transitive trusts with Windows NT–style one-way trusts to limit access within a forest.

Note A one-way trust can also be set up to permit a legacy Windows 3.51 or Windows NT 4.0 domain or a child domain of another forest (such as one belonging to a business partner) to access a specific domain in the tree or forest. When you set up an explicit one-way trust in Active Directory, it works identically to trusts in Windows NT—that is, the trust is not transitive. If you grant a domain access to a single domain in the tree or forest, the trusted domain cannot access any other domain in the tree, even though the tree is linked with transitive trusts.

Choosing DNS Names
After conceiving an Active Directory structure, it’s time to name the baby. If you haven’t read Chapter 3 yet, you might want to refer to it for namespace planning information. After you settle on a naming convention and decide whether to use separate internal and external domain names, it’s time to choose the DNS names for the forest root domain and any additional trees. To do so, use the following steps as a guide—just remember that domain names are highly political in nature, so if you’re fond of your job, don’t create the domain structure and namespace without first getting the approval of the authorities in your organization.
1. Identify what domain names are currently in use with your company. If you use separate domain names for the corporate network and the company’s Internet presence, choose the one in use for the corporate network. This name should be a registered, Internet-valid DNS name so that it’s guaranteed to be unique.

2. Choose a domain name suffix to use for the forest root domain, and by extension, the entire forest. Windows uses .local by default, but if you plan to include any Mac OS X clients in the forest, choose a different suffix such as .office or .lan. (Note that .local conflicts with the Rendezvous feature of Mac OS X, though there are some workarounds.)

3. Choose what domain name prefix or full domain name to use for the forest root domain name. This is a crucial decision because the forest root can’t be deleted or easily changed, and if you’re creating a single tree forest, the forest root name (corp.example.local) also serves as the root name for the tree. (Child domains append their names to the front of the root domain name—for example, marketing.corp.example.local.)

This prefix should conform to the following specifications:

- Not currently in use on the network (if you’re going to use a dedicated forest root domain).
- Isn’t used on the Internet. It’s fine to use your company’s Internet domain name (for example, example.local). Just remember to add a prefix to it so that local clients don’t get confused trying to access your company Web site (for example, use corp.example.local).
- Isn’t likely to ever become outdated. (Broad geographical names work well unless you live in Turkey or Russia.)
- Is 15 characters or fewer, and consists only of Internet standard characters (A-Z, a-z, 0-9, and “.”). This allows legacy clients to use the prefix as the NetBIOS domain name.
- Is easy to remember and makes sense.

4. If you’re creating multiple trees, decide what DNS names to use as the root for each tree. Once again, get explicit buy-in from all decision-makers on the project on each of these names because they’re difficult to change and users see them every day.

5. Arrange to have the forest root DNS prefix ownership, along with the domain names of any additional trees, delegated to the forest administrator, which is likely you. When the actual Active Directory domains are set up or upgraded, you can delegate the ownership of any additional DNS domains to the administrator responsible for DNS in that domain. (See Chapter 14 and Chapter 16 for help with this.)
Planning the Site Topology
Sites, an important new feature of Active Directory, define the boundaries of LAN connectivity, making WAN links more efficient. When you set up sites that mark the sections of the network that have high-speed symmetrical connectivity (10 Mbps is a good number to use), Active Directory tunes the way it uses the WAN links. It reduces the frequency of replication between sites and directs clients' service requests, such as client logon events or directory searches, to domain controllers that are available locally.

Sites are independent of domains. Whereas domains typically mirror a company’s logical organizational structure, sites mirror the physical network structure of a company. A single site might consist of one or more domains, trees, or even forests; or a single domain might span multiple sites. A site can consist of a single IP subnet (which is often the case because subnets frequently mark physical network boundaries) or multiple IP subnets, but all subnets must share reliable, high-speed connectivity to be a part of a single site.

Note  It is becoming increasingly common for a company’s WAN link to be as fast as an internal LAN. However, the WAN link charge might be based on usage, or a company might use the link heavily for real-time, bandwidth-intensive tasks such as video, reducing the available bandwidth. In such cases, you might still want to set up a site structure for the Active Directory forest to avoid burdening the WAN link with excessive replication and service requests.

When planning to upgrade a Windows NT domain to Active Directory, it is important to plan the site topology so that you can set up the site structure promptly after upgrading. Ask yourself the following questions and record your answers:

■ What sites do you need to create in the Active Directory forest?
■ What links are available between these sites, and how fast and expensive are they? Are they already heavily utilized, or is an abundance of bandwidth available?
■ Are you planning to create additional links between the sites?
■ Are there any domains that span physical sites, and if so, are the links between the sites fast enough to support this?

Note  Sites are easy to reconfigure, so be sure to tune them as your network links change.

Two types of connections are available for intersite replication: point-to-point synchronous low-speed remote procedure call (RPC) and Simple Mail Transfer Protocol (SMTP). Any domains that span multiple sites must have at least a point-to-point synchronous low-speed RPC connection between the sites within the domain. This connection is
required because you can’t use SMTP for intersite replication between domain controllers in the same domain; you can use SMTP links only for schema, configuration, and global catalog (GC) information replication. Therefore, if you have multisite domains, double-check the link between the sites to make sure you have adequate connectivity for this setup.

You would be wise to have a global catalog server on each site to allow a local domain controller to service requests for any resource in the forest without having to use the WAN link. However, the global catalog server shouldn’t be the same server as the infrastructure master unless there are no other domain controllers in the domain, because this configuration breaks the infrastructure master’s ability to update other domain controllers in the domain. (See Chapter 15 for information about the infrastructure master role.)

Place at least one DNS server in each site, and have a minimum of two domain controllers per site for redundancy. (This isn’t as important for remote sites with a small number of clients.)

---

**Note**  Place at least one Windows Server 2003 domain controller in each site. Doing so allows Windows Server 2003 to take over the topology generator role, improving intersite replication efficiency and scalability, even when the rest of the domain controllers are running Windows 2000. Switching to Windows Server 2003 functional level results in additional efficiency and scalability improvements, including automatically selecting bridgehead servers and allowing the maximum number of sites per domain to increase to 3000. (The limit is 300 otherwise.)

---

**Making a Recovery Plan**

Upgrading a Windows NT 4.0 domain involves a fair amount of risk. If the PDC fails the upgrade and there aren’t any BDCs available, the entire domain fails. To protect your network from this unhappy possibility (and others), you need a recovery plan.

The following sections provide specific recommendations for safeguarding a network from disasters.

**Make Sure All Domains Have at Least One BDC**

Be sure all domains you plan to upgrade have at least one BDC in addition to the PDC. This prevents the domain from being orphaned (or lost entirely) if the PDC fails the upgrade. Having a working and recently synchronized BDC allows the network to function (almost) normally while you upgrade the PDC. (Some programs or services such as WINS don’t like it when the PDC is gone.)
Back Up Each Computer Before Upgrading
Back up each system before upgrading it. This is perhaps overly cautious on some desktop systems that do not store any data locally, but it’s important on servers, especially domain controllers. Also, make sure you test the backups by restoring randomly selected data from the backup, or even performing a full restoration into a Microsoft Virtual Server environment. (See Chapter 29 for information about Microsoft Virtual Server.)

Synchronize All BDCs with the PDC
Synchronize the PDC with all its replication partners before upgrading it. If the PDC fails the domain upgrade, you can promote a BDC to the PDC and the domain won’t lose any changes.

Take a BDC Offline for Backup
Freshly synchronized BDCs and new tape backups of the PDC protect you from most disasters. However, it’s good insurance to take a freshly synchronized BDC offline before upgrading the PDC. This provides you with a quickly available, working backup of the domain as it existed before you started the upgrade process. If the upgraded PDC replicates bad domain information to the BDCs or the domain becomes damaged in some other way, having an offline backup allows you to go back to a healthy copy of the domain.

To prepare a BDC to act as an offline domain backup, synchronize the BDC with the PDC domain, back up the BDC, and then disconnect the network cable to the BDC. If a major disaster occurs after upgrading the PDC and it is necessary to restore the domain to its pre–Active Directory state, use the following steps:

1. Demote any Windows 2000 or later domain controllers on the network back to member server status.
2. Reconnect the offline BDC to the network.
3. Promote the formerly offline BDC to a PDC.
4. Synchronize the new PDC with the other BDCs on the network. This returns the domain to the state it was in immediately before you took the BDC offline.

**Important** All changes to the domain performed after taking the backup BDC offline are lost if you bring the BDC back online and promote it to a PDC. Because of this, keep a record of any changes you make (such as creating or deleting accounts, and changing group memberships or trust relationships). By doing so, in the event of a disaster you can manually re-create the lost changes.
Relax
Don’t let all these warnings dissuade you from performing an upgrade. If you take precautions and the upgrade goes faultlessly, you won’t have to resort to restoring backups or using other recovery mechanisms. However, if you do encounter problems, you will be prepared.

Developing an Upgrade Strategy
After documenting the existing network infrastructure, making a recovery plan, and designing the Active Directory trees and sites, you’re ready to put it all together and create an actual upgrade plan. This section presents some general guidelines that apply to all domain upgrades, as well as some tips for specific domain models.

Upgrading or Replacing Windows NT RAS Servers
As mentioned earlier in this chapter, Windows NT 4.0 RAS servers don’t play well with Active Directory networks. Because of this, upgrade or replace any Windows NT 4.0 RAS servers with Windows Server 2003 or Windows 2000 member servers running Routing and Remote Access (RRAS) before upgrading the PDC and starting the domain upgrade. If this isn’t feasible, put all Windows NT 4.0 RAS servers near the top of the list of servers to upgrade after you upgrade the PDC and a few BDCs.

Making Sure the PDC Is Sufficiently Powerful
Start the domain upgrade by carefully examining the current PDC. Although Active Directory uses peer-based, multiple-master domain controllers, the first domain controller retains extra services that in some cases you cannot easily move to other domain controllers. These services include the global catalog server, the Operations Master, and the PDC emulator. (The PDC emulator provides services for Windows NT, Windows 95, Windows 98, and Windows Me clients, and also performs some tasks in a pure Windows 2000, Windows XP, and Windows Server 2003 environment.)

Because of these additional roles the upgrade PDC must perform, the first PDC should be especially fast, powerful, and reliable. The best way to ensure that the PDC is fast enough is to buy a powerful new server and install Windows NT 4.0 Server on it as a BDC with Service Pack 6a and the latest hot fixes. Promote the server to your PDC, let it sit for a little while, and then take it offline and perform the upgrade to Windows Server 2003. This ensures that your first domain controller is on the most powerful and up-to-date hardware you have available, and it provides the closest-to-clean install experience possible from an upgrade.
Creating the Dedicated Forest Root Domain
Before Upgrading the PDC
If you want to create a dedicated forest root domain, you need to do this before you upgrade the PDC. After you have the new domain up and running with a couple of domain controllers, you can upgrade the PDC and join it to this new tree as a child domain.

Upgrading or Retiring Any Incompatible Clients and Servers
If you have any Windows NT 4.0 RAS servers or computers running Windows NT 3.51 or earlier, upgrade or retire these systems as discussed earlier in this chapter.

Disable the LAN Manager Replication Service on all Windows NT 4.0 servers because it’s incompatible with Active Directory networks. The file replication service (FRS) feature of Windows 2000 and Windows Server 2003 domain controllers replaces it. (Note that the new DFS Replication service of Windows Server 2003 R2 does not replace FRS for domain controller replication.)

More Info
If you want to synchronize FRS with LAN Manager Replication Service, see the “Synchronize File Replication Services” topic in the Windows Server 2003 Deployment Guide at http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/DepKit/6e81e1f0-7d13-480b-be24-5887f8bfa3cc.mspx. This topic discusses a workaround using tools from the Windows Server 2003 Deployment Kit companion CD.

Upgrading the PDC First
The first server you upgrade must be the Windows NT PDC in the account domain you want to use as the root of the new Active Directory tree. This is true whether the tree you’re creating is the first in the forest or the twentieth in the third forest—upgrade the PDC first if you want to upgrade the Windows NT domain instead of creating a new domain.

Note
If you’re going straight from Windows NT to Windows Server 2003–based domain controllers without passing “Go” (Windows 2000), consider using the Windows Server 2003 Interim functional level. This mode offers a number of advantages over Windows 2000 mixed mode, and it still allows Windows NT BDCs (but no Windows 2000 domain controllers) to operate in the domain. For more information, see the “Switching Forest and Domain Functional Levels” section later in this chapter.
Upgrading or Replacing the BDCs Quickly

It’s important to get another Windows Server 2003 or Windows 2000 domain controller online quickly after you upgrade the PDC. If the sole Windows Server 2003 domain controller goes down, you’ll have to promote a BDC to PDC and start over again (though most changes will survive, except any changes incapable of being stored on a Windows NT BDC).

Another reason that it’s important to quickly add additional domain controllers is because computers running Windows 2000, Windows XP, or Windows Server 2003 authenticate preferentially with Windows Server 2003 and Windows 2000 domain controllers. If there are too few Windows Server 2003 or Windows 2000 domain controllers available, clients might not be able to authenticate during busy times. (Most clients can log on using cached credentials, but you should nonetheless add domain controllers quickly.) If you can’t add additional Windows Server 2003 or Windows 2000 domain controllers in a prompt manner, configure the Windows Server 2003 domain controllers to appear to all clients as Windows NT 4.0 domain controllers. To do so, refer to the Windows Server 2003 Resource Kit or Knowledge Base Article 298713.

Because the master copy of the domain information is stored in Active Directory after you upgrade the PDC, you don’t need to upgrade BDCs. Instead, you can replace them with new Windows Server 2003 or Windows 2000 domain controllers, or perform clean installations on BDCs and then install Active Directory when finished.

If you do choose to upgrade BDCs, do so one at a time, and pause before upgrading or retiring the last BDC. Verify that you’ve dealt with all incompatible clients and servers, recreate in Active Directory any trusts in that are established with Windows NT 4.0 domains, and to be extra safe, take the last BDC offline for a week or more before upgrading or retiring it. If nothing erupts in flames, go ahead with your plan.

Important  Make sure that the first domain controller is visible on the network when upgrading a BDC. When you upgrade a BDC, it replicates only with the PDC emulator. If the former PDC isn’t available, the BDC takes over the PDC emulator and other roles, creating serious problems when the first domain controller comes back online.
Real World  Upgrading BDCs on Remote Sites Using Backup Media

To reduce the amount of replication traffic generated when upgrading or deploying a new domain controller on the far end of a slow WAN link, back up the system state information from an existing domain controller and physically ship the backup media to the remote site. Then upgrade the BDC to Windows Server 2003 (or perform a clean install) and, before running the Active Directory Installation Wizard, restore the files to a local hard drive (by specifying Restore Files To: Alternate Location In Backup). Then run the Active Directory Wizard (Dcpromo.exe) with the /adv switch and specify the location of the restored files. This seeds the new or upgraded domain controller with a slightly out-of-date copy of the Active Directory database, which Active Directory updates during the first replication. This first replication is significantly faster than if you replicated the entire Active Directory database.

Upgrading Member Servers and Clients Independently

Upgrade member servers and workstations whenever you want—either before or after you upgrade the domain. Windows 2000, Windows XP, and Windows Server 2003 clients and member servers work perfectly well with Windows NT domains; however, the benefits of Active Directory aren’t available to clients and member servers until you upgrade the domain.

Scheduling the Domain Upgrade Appropriately

Schedule the domain upgrade at a time that has the lowest impact on the user population. It’s best to avoid upgrades during major projects and during the busiest times of year if possible. Even perfect upgrades produce some impact on the users, especially if you perform any domain restructuring or consolidation.

Creating a Testing Criteria

It’s important to ascertain whether Active Directory is functioning properly after a domain upgrade, before it’s too late to back out and restore the Windows NT 4.0 domain. Use these criteria as a starting point:

- Users can log on successfully.
- Users can access e-mail.
Users and groups can access resources for which they have permissions, including resources in other domains (when applicable).

- Active Directory is functioning properly. (Use Dcdirname.exe.)
- Replication works properly. (Use Repadmin.exe and Nltest.exe to verify this.)

## Preparing Domains and Computers

The first step in the actual upgrade process for servers running Windows NT 4.0 or Windows 2000 Server is to prepare the domains and computers for the upgrade. This important step streamlines the upgrade process and makes it go as smoothly as possible.

## Reviewing Server Upgrade Requirements

You can upgrade to Windows Server 2003, Standard Edition, from the following operating systems:

- Windows 2000 Server
- Windows NT 4.0 Server with Service Pack 5 or later
- Windows NT 4.0 Terminal Services with Service Pack 5 or later

To upgrade to Windows Server 2003, Enterprise Edition, you must be running one of the following operating systems:

- Windows 2000 Advanced Server
- Windows NT 4.0 Enterprise Edition

You can install Windows Server 2003 R2 on a server running Windows Server 2003 with Service Pack 1 without performing an operating system upgrade.

**Note** You must perform a clean install to switch editions, unless you want to upgrade from Standard Edition to Enterprise Edition, in which case you can perform an upgrade installation. You cannot upgrade from an x86 edition of Windows to an x64 edition of Windows.
Preparing Windows NT Domains

Perform the following actions to prepare a Windows NT–based domain for upgrading to Active Directory:

■ Verify that all PDCs and BDCs that you plan to upgrade are running Windows NT Server 4, or Windows NT Server 4 Enterprise Edition with Service Pack 6a.

■ Clean up the directories and user accounts to eliminate old baggage. When you upgrade the domain, Windows moves all user accounts into Active Directory. Although Active Directory is extremely scalable, disused accounts do take up hard disk space and make identifying valid accounts more difficult. There’s no point in storing and replicating disused accounts indefinitely, so delete them before you upgrade.

■ Clean out unused directories, and uninstall outdated software.

■ Disable trusts that you don’t want to preserve.

■ Synchronize the PDC with all the BDCs, and then implement the recovery plan described earlier in the “Making a Recovery Plan” section, including taking one of the BDCs offline and disconnecting it from the network.

Preparing the Computers

To prepare the computers for the upgrade, perform these tasks for each computer involved:

■ Check the system requirements for the version of Windows to which you're upgrading to make sure the computer meets them. See Chapter 5 for more information.

■ Check the Windows Server Catalog on the Microsoft Web site (http://www.microsoft.com/windows/catalog/server/). If possible, replace components that the Windows Catalog doesn’t list as 100-percent compatible.

■ Insert the Windows Server 2003 or Windows XP CD-ROM (if you're upgrading a client), and check the system for compatibility problems.

■ If you're upgrading from Windows NT 4.0, install Windows NT 4.0 Service Pack 6a.
- If you're upgrading a Windows 2000 server running Microsoft Internet Security and Acceleration (ISA) Server 2000, make sure ISA Server 2000 Service Pack 1 or later is installed.

- If you're upgrading a Windows 2000 domain controller that has the Server for NIS component of Services For UNIX 2.0 installed, see Microsoft Knowledge Base Article 293783 at http://support.microsoft.com for information about a supported hotfix.

- Read the Read1st.txt and Relnotes.doc files on the Windows 2000 CD-ROM to check for application or hardware issues.

- Check the Event Viewer. Fix any problems before you upgrade.

- Uninstall any virus protection programs you have installed, unless you know that they work under Windows Server 2003 without modification.

- Perform and verify a full system backup, including the system state, and create or update the emergency repair disk.

  **Important** Windows NT 4.0 DHCP servers sometimes lose data during the upgrade process. To mitigate this issue, export the DHCP database and settings using the Dhcpxem.exe tool from the Windows Server 2003 Resource Kit, and then restore the file after the upgrade is complete.

- Record the hardware configuration of the system for reference in case of a hardware conflict or problem. Include installed devices, interrupt requests (IRQs), jumper settings, and the hard disk configuration.

- Disable any Windows NT 4.0 software-based disk mirrors, volume sets, stripe sets, or stripe sets with parity:
  - If you're using a software-based mirror set, break the mirror.
  - If you're using any volume sets, stripe sets, or stripe sets with parity, back up the data and then delete the set (deleting all data). After you install Windows Server 2003, restore the data to the appropriate basic disk or dynamic disk. (See Chapter 18.)

  **Note** If you absolutely must access a Windows NT volume set, stripe set, stripe set with parity, or mirror set after upgrading to Windows Server 2003, use the Ftonline tool included with the Windows Server 2003 Support Tools.

- Uncompress all hard disks (unless they make use of NTFS compression).
■ Disconnect the serial cable to any serial port uninterruptible power supply (UPS) devices. (You can leave USB UPS devices plugged in.)
■ Locate all drivers and get the Windows CD-ROM, or connect to the network share with the Windows installation files.

### Updating the Active Directory Schema

You must update the Active Directory schema before performing the following actions:

■ Adding a Windows Server 2003 or Windows Server 2003 R2 domain controller to an existing Windows 2000 forest or domain
■ Adding a Windows Server 2003 R2 domain controller to an existing Windows Server 2003 forest or domain

This section discusses how to test Active Directory before updating the schema, as well as how to update the forest schema, verify the update, and update the domain schema for each domain in which you want to install Windows Server 2003 or Windows Server 2003 R2 domain controllers.

**Important** If you use any third-party Active Directory applications or have made any custom changes to the Active Directory schema, verify that they are compatible with the Windows Server 2003 or Windows Server 2003 R2 schema revision levels before updating the forest schema. This is rarely a problem, but it is nearly impossible to undo a schema update once it has propagated, so it's best to err on the side of caution.

### Testing Active Directory Functionality in Active Directory Domains

Perform the following actions before updating the Active Directory schema, adding any Windows Server 2003 domain controllers to an existing Windows 2000 Active Directory domain, or upgrading any Windows 2000 domain controllers in the domain to Windows Server 2003:

■ Verify that all domain controllers in the domain have Netlogon and Sysvol shares by using Dcdiag.exe from the Windows Support Tools. To do so, open a command prompt window, switch to the folder storing Dcdiag.exe, and then type `dcdiag /e /test:frssysvol`. All domain controllers should pass the tests.
If you see the error message “There are errors after the SYSVOL has been shared”, try restarting the File Replication Service on the affected domain controller, check the File Replication Service log in Event Viewer for any additional errors, and then rerun Dcdiag.exe.
- View the operations master roles in the forest by using the `dcdiag /test:FSMO-CHECK` command, and transfer any operation master roles that reside on non-existent or unhealthy domain controllers to healthy domain controllers. See Chapter 15 for information on transferring operation master roles.

- Verify replication using the Windows Server 2003 version of Repadmin.exe on a Windows XP or Windows Server 2003 member server in the forest. To do so, open a command prompt window, switch to the folder storing Repadmin.exe, and then type `repadmin /replsum /bysrc /bydest /sort:delta`.

  All domain controllers should show 0 in the Fails column, and the largest deltas should be less than or roughly equal to the replication frequency on the site links used by the domain controllers for replication. The default replication frequency between sites is 180 minutes; you can change this setting by using the Active Directory Sites And Services MMC snap-in. See Chapter 15 for more information.


### Updating the Active Directory Forest Schema

You must update the Active Directory schema before you can add a Windows Server 2003 or Windows Server 2003 R2 domain controller to a Windows 2000 Active Directory forest, or add a Windows Server 2003 R2 domain controller to a Windows Server 2003 Active Directory forest. This also applies to domain controllers upgraded to Windows Server 2003 or Windows Server 2003 R2.

To prepare a forest for Windows Server 2003 or Windows Server 2003 R2 domain controllers, use the following procedure to update the schema in your test lab. This is an important step because you cannot undo a forest schema update. After testing the schema updates, use the procedure in your production network.

1. Update all Windows 2000 domain controllers and servers running Exchange Server 2000 or later to Windows 2000 Service Pack 4 or later.

   Domains with more than 10 domain controllers consume additional network bandwidth during replication unless all domain controllers are running Windows 2000 with Service Pack 3 or later. See Microsoft Knowledge Base Article 331161 at [http://support.microsoft.com](http://support.microsoft.com) for more information about this and other issues with Windows 2000 domain controllers running service pack revisions earlier than Service Pack 4.
Important If you have implemented the Exchange Server 2000 schema changes in the forest prior to updating the forest schema to Windows Server 2003 or Windows Server 2003 R2 levels, you must perform a special schema update to prevent Adprep from mangling attributes. See Microsoft Knowledge Base Article 325379 at http://support.microsoft.com for information about how to prep the schema and for help with fixing mangled attributes. You can safely update the schema for Exchange Server 2000 after updating the forest schema to Windows Server 2003 or Windows Server 2003 R2 level.

2. Identify the servers with the schema master and infrastructure master roles, and install the appropriate version of the Windows Support Tools on the schema master.

Note If you’re updating a Window 2000 Active Directory forest to support Windows Server 2003 domain controllers, update the schema to the Windows Server 2003 R2 revision, even if you don’t plan to immediately use Windows Server 2003 R2 domain controllers. This eliminates the hassle of updating the schema a second time when you decide to deploy Windows Server 2003 R2 domain controllers.

3. On the server designated the schema master, use the Run As feature (discussed in Chapter 12) to open a command prompt window on the schema master using an account that belongs to the Enterprise Admins and Schema Admins groups (or has delegated authority). Or log on to the server using an account that belongs to the Enterprise Admins and Schema Admins groups (or has delegated authority), and open a command prompt window.

4. Switch to the folder in which you installed the Windows Support Tools, and run the repadmin /showreps command to verify that the last inbound replication succeeded. If the last replication failed, troubleshoot replication before proceeding.

5. Temporarily disable outbound Active Directory replication by typing repadmin /options +DISABLE_OUTBOUND_REPL.

6. Switch to the folder in which Adprep.exe is located.

   To update the forest schema to Windows Server 2003 R2 level, use the Adprep.exe file located in the \Cmpnents\R2\Adprep folder of the Windows Server 2003 R2 Disc 2 CD-ROM.
Best Practices  Use either the Windows Server 2003 R2 version of Adprep.exe (to upgrade the forest schema to Windows Server 2003 R2 level) or the Windows Server 2003 Service Pack 1 version of Adprep.exe (to upgrade the forest schema to Windows Server 2003 level). These versions of Adprep.exe offer increased error checking and reporting, and provide more control over updating the domain schema. The Windows Server 2003 Service Pack 1 version of Adprep.exe is located in the \i386 or \amd64 folder of the Windows Server 2003 with Service Pack 1 CD, and is available for download from Microsoft Product Support Services via Microsoft Knowledge Base Article 324392 at http://support.microsoft.com.

7. Type adprep /forestprep, and watch for any error messages.

8. If the schema upgrade completed successfully and without errors (see the next section for information about how you can verify that the update proceeded properly), switch to the folder in which you installed the Windows Support Tools, and type repadmin /options −DISABLE_OUTBOUND_REPL to enable outbound replication of the schema master to the network. Then update the schema in each domain in which you want to install Windows Server 2003 or Windows Server 2003 R2 domain controllers.

Otherwise, follow the instructions provided by the error messages, if possible, or restore from backup and research the problem before trying again.

Verifying the Forest Schema Update

To verify that the schema update operation succeeded for the forest, perform the following steps:

1. Check the system log in Event Viewer for any errors. (You can safely ignore errors with event ID 1153.)

2. Install the Windows Support Tools and then use the Dcdiag.exe command from the Windows Support Tools to verify Active Directory functionality. (Ignore any replication errors—the server is disconnected from the network.)

   To do so, click Start, choose All Programs, Windows Support Tools, Command Prompt and then type Dcidiag in the command prompt window.

3. Open ADSI Edit from the Windows Support Tools.

   To do so, click Start, choose All Programs, Windows Support Tools, Command Prompt and then type Adsiedit.msc in the command prompt window.
4. In the ADSI Edit window under the Configuration node, navigate to CN=Configuration, DC=forest_root_domain, where forest_root_domain is the DNS name of the forest root domain, and then navigate to CN=ForestUpdates.

5. Right-click the CN=Windows2003Update object (shown in Figure 6-4), choose Properties from the shortcut menu, and then view the value for the Revision attribute (or property in Windows 2000). The value should read 9 after updating the forest schema for Windows Server 2003 or Windows Server 2003 R2. (See Table 6-3 for a listing of schema revision numbers.)

![Figure 6-4 The ADSI Edit window](image)

6. Under the Schema node of ADSI Edit, right-click the CN=Schema,CN=Configuration,DC=forest_root_domain object, where forest_root_domain is the DNS name of the forest root domain, and then choose Properties from the shortcut menu.

7. View the value for the objectVersion attribute (or property in Windows 2000), as shown in Figure 6-5. The value should read 31 after updating the forest schema for Windows Server 2003 R2. (See Table 6-3 for a listing of schema version numbers.)

**Note** Adprep.exe stores its log files in the SYSTEMROOT\System32\Debug\Adprep\Logs folder.
Figure 6-5  The ADSI Edit window

Table 6-3  Schema revision and version levels

<table>
<thead>
<tr>
<th></th>
<th>Schema Revision</th>
<th>Schema Version (ObjectVersion)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000</td>
<td>(none)</td>
<td>13</td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td>9</td>
<td>30</td>
</tr>
<tr>
<td>Windows Server 2003 R2</td>
<td>9</td>
<td>31</td>
</tr>
</tbody>
</table>

Updating the Active Directory Domain Schema

To prepare a domain for Windows Server 2003 or Windows Server 2003 R2 domain controllers, you must update the domain schema to the Windows Server 2003 or Windows Server 2003 R2 levels. Use the following procedure on each domain before adding Windows Server 2003 or Windows Server 2003 R2 domain controllers to the domain:

1. If you recently updated the forest schema and different computers perform the infrastructure master role and schema master role, wait for Active Directory to replicate the changes to the infrastructure master. Wait 15 minutes if the infrastructure master is in the same site; half a day or a day if it’s in another site.

If your domain controllers are running Windows 2000 Server with Service Pack 2 or earlier, the adprep /forestprep command delays replication. (See Microsoft Knowledge Base Article 331161 at http://support.microsoft.com for more information.)
2. Open a command prompt window on the infrastructure master using an account that belongs to the Domain Admins or Enterprise Admins group (or has delegated authority).

3. Temporarily disable outbound Active Directory replication by typing `repadmin /options +DISABLE_OUTBOUND_REPL`.

4. Switch to the folder in which Adprep.exe is located.

To update the forest schema to Windows Server 2003 R2 level, use the Adprep.exe file located in the `\Components\R2\Adprep` folder of the Windows Server 2003 R2 Disc 2 CD-ROM.

---

**Best Practices**

Use either the Windows Server 2003 R2 version of Adprep.exe (to upgrade the schema to Windows Server 2003 R2 level) or the Windows Server 2003 Service Pack 1 version of Adprep.exe (to upgrade the schema to Windows Server 2003 level). These versions of Adprep.exe offer increased error checking and reporting, and they provide more control over updating the domain schema. The Windows Server 2003 Service Pack 1 version of Adprep.exe is located in the `\i386` or `\amd64` folder of the Windows Server 2003 with Service Pack 1 CD, and is available for download at [http://support.microsoft.com](http://support.microsoft.com) via Microsoft Knowledge Base Article 324392.

5. Type `adprep /domainprep`, and watch for any error messages.

6. Confirm that Adprep upgraded the schema properly by doing the following:
   - Use Dcdiag from the Windows Support Tools.
   - Check the system log in Event Viewer for any errors.
   - Check the Adprep.exe log files in the `systemroot\System32\Debug\Adprep\Logs` folder.

7. If the domain preparation completed without errors, switch to the folder in which you installed the Windows Support Tools, and type `repadmin /options -DISABLE_OUTBOUND_REPL` to enable outbound replication of the schema master to the network. Otherwise, follow the instructions provided by the error messages, if possible, or restore from backup and research the problem before trying again. Do not proceed until you can confirm that the domain was prepared properly.

8. Find a time when the network is quiet enough to synchronize all Group Policy Objects (GPOs) between all domain controllers on the domain, and then type `adprep /domainprep /gpprep` and watch for any error messages.

This step ensures that Resultant Set of Policy (RSoP) works properly with site-based GPOs.
9. Wait for the changes to replicate to other domain controllers before upgrading any
domain controllers to Windows Server 2003 or Windows Server 2003 R2. Allow at
least 15 minutes. If there are domain controllers in remote sites, allow half a day or
a day.

Note A domain can run indefinitely after performing this procedure without
the need to upgrade any domain controllers to Windows Server 2003 or Win-
dows Server 2003 R2, though there are no benefits to doing so.

Upgrading Clients to Windows XP

Although this book concentrates on Windows Server 2003 issues, in all likelihood you’ll
spend more time performing client upgrades than server upgrades.

Upgrading to Windows XP is easy, but the results vary depending on the starting oper-
Windows NT 4.0 systems usually upgrade flawlessly, although they might end up with
some legacy device drivers.

Computers running Windows 98 or Windows Me are the most difficult to upgrade to
Windows XP. Because of these difficulties, perform clean installations instead of
upgrades whenever possible. If you need to migrate user settings and data, use the User
State Migration Toolkit (USMT), available from the Microsoft Web site at http://
deciding whether to upgrade or to perform new installations, test the upgrade or migra-
tion on some clients that are representative of the client population. (Chapter 5 covers
performing clean installations of Windows.)

Note You can automate the upgrading of Windows 2000 clients using the Soft-
ware Installation feature of Group Policy. To do so, see Chapter 28. You can also
automate upgrades using command-line switches. (See Chapter 5 for more infor-
mation.)

To upgrade a client computer to Windows XP, use the following procedure:

1. While running Windows 2000, Windows NT 4.0, Windows Me, or Windows 98,
close all open programs and disable all virus-protection programs.

2. Insert the Windows XP CD-ROM, and in the Welcome To Microsoft Windows XP
window, click the Install Windows XP link.
3. Select the Upgrade option, click Next, and then follow the instructions onscreen to upgrade Windows. This upgrades the computer to Windows XP while keeping the settings and programs intact.

- If Setup finds hardware or software that isn’t compatible with Windows XP, it lists it on the Report System Compatibility page.
- If prompted, select Yes to upgrade your drive to NTFS, unless you want to dual-boot with Windows 98 or Windows Me, or anticipate that you might uninstall Windows XP.

---

**Under the Hood  Why Windows 98 and Windows Me Upgrades Are Tough**

A direct upgrade from Windows 98 or Windows Me to Windows XP is possible, but it is usually better to perform a clean installation. The difficulty lies in a fundamental difference in architectures: Windows XP is based on Windows NT and Windows 2000, while Windows 98 and Windows Me (and Windows 95) are heirs to the MS-DOS and Windows 3.x compost heap (although obviously all the later operating systems include huge amounts of new code). To further complicate matters, Windows 98 and Windows Me might not use the same drivers as Windows XP (unless you use WDM drivers), and applications are often coded differently for Windows 95, Windows 98, and Windows Me than they are for Windows XP. These are major obstacles to overcome.

The fact is that some Windows 95, Windows 98, and Windows Me applications won’t run in Windows XP without modification. Thus, when performing an upgrade from Windows 98 or Windows Me, it is important either to uninstall applications that don’t run without modification on both Windows 98 and Windows XP or to obtain an upgrade pack (also called a migration DLL) during the upgrade process or from the application vendor beforehand.

With that said, you can upgrade a Windows 98–based or Windows Me–based system to Windows XP and you can make it work. However, a prudent person performs a few upgrades on representative systems before deciding on the upgrade strategy.
Upgrading Servers to the Windows Server 2003 Family

After you plan the domain upgrade and prepare the computer (as discussed earlier in this chapter), you’re ready to begin the upgrade. Use this section to install Windows Server 2003 R2 on a server running Windows Server 2003, or to upgrade a server running Windows NT 4.0, Windows 2000, or Windows Server 2003 to Windows Server 2003 or Windows Server 2003 R2.

Note Instead of upgrading an existing Windows 2000 domain controller to be the first Windows Server 2003 domain controller in the domain, add a Windows Server 2003 member server and then install Active Directory on it after it’s been up and running for a week or so. This allows your network to continue operating without being affected by the upgrade process.

Installing Windows Server 2003 R2

To install Windows Server 2003 R2 on a server running Windows Server 2003, use the following steps:

1. If you haven’t yet installed Windows Server 2003 Service Pack 1, install the service pack from Windows Update or another source and then restart the server.

2. Close all open programs, disable all virus protection programs, and then insert Windows Server 2003 R2 Disc 2.

3. In the Welcome To Windows Server 2003 R2 window, click the Continue Windows Server 2003 R2 Setup link, and then follow the instructions onscreen in the Windows Server 2003 R2 Setup Wizard.

Note You must update the Active Directory schema to the Windows Server 2003 R2 revision before you can install Windows Server 2003 R2 on any domain controllers in the forest. See the “Updtaing the Active Directory Schema” section of this chapter for more information.
Upgrading a Server to Windows Server 2003

To upgrade a server to Windows Server 2003, use the following steps:

1. If you’re upgrading a PDC, synchronize with the domain’s BDCs one last time.
   When upgrading a Windows NT 4.0 multiple domain network, make sure that you follow your upgrade plan to upgrade the Windows NT 4.0 domains in the proper order.

2. Close all open programs, and disable all virus-protection programs. Then insert the Windows Server 2003 CD-ROM.

3. In the Welcome To Windows Server 2003 window, click the Install Windows Server 2003 link.

4. Select the Upgrade option (shown in Figure 6-6), click Next, and then follow the instructions onscreen to upgrade Windows. This upgrades the computer to Windows Server 2003 while keeping the settings and programs intact.
   - If Setup finds hardware or software that isn’t compatible with Windows Server 2003, it lists it on the Report System Compatibility page.
   - If prompted, select Yes to upgrade your drive to NTFS.

5. Windows Setup copies files to the hard drive and then restarts the computer for the text-based part of Setup. (You might need to remove the CD-ROM temporarily to boot into Setup properly.)
6. If you are upgrading a PDC or BDC, the Active Directory Installation Wizard starts after Setup completes. If you’re installing Windows Server 2003 R2, finish the Windows Server 2003 R2 Setup process before using the Active Directory Installation Wizard. See Chapter 14 for information about how to use this wizard to install Active Directory and a DNS server if you want to deploy both services on the domain controller (a good idea). Refer to the next section for help in choosing a forest functional level.

**Note** Windows doesn’t import existing trusts between Windows NT 4.0 domains into Active Directory when upgrading a Windows NT 4.0 PDC, though the trusts continue to function as long as a BDC is available. Because of this, you must recreate all trusts with Windows NT 4.0 domains in Active Directory before upgrading or taking the last BDC in the upgraded domain offline.

---

### Switching Forest and Domain Functional Levels

Active Directory has a number of functional levels that dictate what features are available and what versions of Windows can serve as domain controllers. In a forest that includes any Windows Server 2003 domain controllers, there are three forest functional levels, and four domain functional levels. This is an increase from the single forest functional level and two domain functional levels available in Windows 2000.

The following sections help you sort out this increased complexity and figure out what functional levels are appropriate for your network.

**Note** Windows Server 2003 R2 does not add any functional levels to Active Directory, though it does require a schema update, as discussed in the “Updating the Active Directory Schema” section of this chapter.

---

### Choosing a Forest Functional Level


- **Windows 2000** The baseline forest functional level that supports Windows Server 2003 and Windows 2000 domain controllers, as well as Windows NT 4.0 BDCs. The Windows 2000 forest functional level permits domains to use any functional level—Windows 2000 mixed or higher—and is the default forest functional level.
Windows Server 2003 interim  A special functional level that is available when upgrading from Windows NT 4.0. The Windows Server 2003 interim functional level supports only Windows Server 2003 domain controllers and Windows NT 4.0 BDCs. It allows group membership changes (instead of the entire group membership list) to be replicated, and it improves the generation of intersite replication topologies. When you choose the Windows Server 2003 interim forest functional level, you must use the Windows Server 2003 interim domain functional level or higher for all domains in the forest.

Windows Server 2003  The native functional level of a forest where all domain controllers run Windows Server 2003. The Windows Server 2003 forest functional level provides the features of the interim functional level, along with other new features such as the ability to rename domains and create two-way, transitive trusts between forests. When you choose the Windows Server 2003 forest functional level, you must use the Windows Server 2003 domain functional level for all domains in the forest.

Start with the Windows 2000 forest functional level if you have any Windows 2000 domain controllers in your forest or if you anticipate that you might. Switching forest or domain functional levels is a one-way process (there’s no going back), and old servers have a surprising knack for sticking around and making themselves useful. For example, you can put an aging Windows 2000 domain controller to good use as a second or third domain controller at a remote site.


If you’re upgrading directly from Windows NT 4.0 and you know that you’ll never want to add a Windows 2000 domain controller to the forest (in any domain), choose the Windows Server 2003 interim functional level when performing the upgrade. (This option appears in the Active Directory Installation Wizard.) If you forgo this option when upgrading the PDC, you can make the switch later, although you’ll have to use a script to do so. (See the Windows Server 2003 Resource Kit for more information.) If your Windows NT 4.0 domains make use of groups with more than 5000 members, you must choose the Windows Server 2003 interim functional level or divide the groups into two or more groups of 5000 members or less (except for the Domain Users group, which is exempt from this limitation).
Note  You can raise the domain functional levels of all domains in the forest to Windows Server 2003 native level without touching each domain, as long as all domains are already at the Windows 2000 native functional level (or Windows Server 2003 native). Simply raise the forest functional level to Windows Server 2003 native level, and all domains follow suit.

When you raise the forest functional level to Windows Server 2003 functional level, you automatically raise the domain functional level for all domains in the forest to the Windows Server 2003 functional level. If there are any Windows 2000 domain controllers, Windows generates a report listing the offending servers and blocks the increase until you upgrade or remove the domain controllers. If there are any domains using Windows 2000 mixed or Windows Server 2003 interim functional levels, Windows blocks the increase until you raise the functional level of the domains to Windows 2000 or Windows Server 2003.

Table 6-4 summarizes the differences between the different forest functional levels. (For a more complete list, see the Windows Server 2003 Help and Support Center.)

Table 6-4  Some differences among forest functional levels

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Efficient Group Member Replication</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Improved Replication Topology Generation</td>
<td>Limited; requires Windows Server 2003 domain controller</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td>Linked value replication</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Global catalog replication improvements</td>
<td>When both domain controllers are Windows Server 2003</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum number of group members</td>
<td>5000 (except Domain Users group, which can be higher)</td>
<td>5000+</td>
<td>5000+</td>
</tr>
<tr>
<td>Domain rename</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Transitive forest trusts</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Defunct schema objects</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Application Group</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Choosing a Domain Functional Level


- **Windows 2000 mixed**  The default mode of all newly created domains, as well as upgraded Windows NT domains. While a domain is in mixed mode, Windows NT 4.0 BDCs, Windows 2000 domain controllers, and Windows Server 2003 domain controllers can all coexist on the network.


- **Windows 2000 native**  A functional level for Windows 2000 and newer domain controllers that permits domains to scale past the Windows NT 40,000 account limit, enables the SIDHistory feature (which makes domain restructuring much less painful), and provides the additional Universal and Domain Local groups. When using Windows Server 2000 native functional level, you can only use Windows 2000 and Windows Server 2003 domain controllers.

- **Windows Server 2003**  A functional level for Windows Server 2003 domain controllers only that provides all the features of Windows 2000 functional level, as well as domain controller renaming and a higher maximum number of sites per domain, among other things.

Start with the Windows 2000 mixed domain functional level if you have any Windows 2000 domain controllers in your forest or if you anticipate that you might. Otherwise, choose the Windows Server 2003 Interim functional level. Most companies find themselves remaining in Windows 2000 mixed or Windows Server 2003 interim functional level for some time to ensure compatibility with existing Windows NT 4.0 BDCs or other servers that need access to a “real” Windows NT 4.0 BDC. However, there are advantages to using the Windows 2000 and Windows Server 2003 native functional levels, as described in Table 6-5, especially when restructuring or consolidating domains.
Table 6-5  The differences among domain functional levels

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Objects per domain</td>
<td>Fewer than 40,000 (20,000 user accounts) recommended</td>
<td>Fewer than 40,000 (20,000 user accounts) recommended</td>
<td>Millions</td>
<td>Millions</td>
<td>Millions</td>
</tr>
<tr>
<td>Multimaster replication</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Group types</td>
<td>Global, Local</td>
<td>Global, Local</td>
<td>Universal, Domain Global, Domain Local</td>
<td>Global, Local Universal, Domain Global, Domain Local, Local</td>
<td></td>
</tr>
<tr>
<td>Domain controller rename</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Nested groups</td>
<td>No</td>
<td>Distribution groups and local groups that can store global groups only</td>
<td>Yes</td>
<td>Distribution groups and local groups that can store global groups only</td>
<td>Yes</td>
</tr>
<tr>
<td>Convert groups</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cross-domain administration</td>
<td>Limited</td>
<td>Limited</td>
<td>Full</td>
<td>Limited</td>
<td>Full</td>
</tr>
<tr>
<td>Group membership replication</td>
<td>Only membership changes</td>
<td>Entire group membership list</td>
<td>Entire group membership list</td>
<td>Only membership changes</td>
<td>Only membership changes</td>
</tr>
<tr>
<td>Maximum sites per domain</td>
<td>N/A</td>
<td>300</td>
<td>300</td>
<td>300</td>
<td>300</td>
</tr>
<tr>
<td>SIDHistory</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Microsoft recommends a rapid switch to Windows 2000 functional level; however, consider taking a more cautious approach when upgrading from a Windows NT 4.0 network. Running in Windows 2000 mixed or Windows Server 2003 interim functional level allows nervous network administrators a chance to start using Active Directory in a limited manner without losing their Windows NT 4.0 safety net. Wait until it’s clear there is no need for Windows NT 4.0 BDCs before making the domain functional level upgrade because, after you upgrade the domain mode, there is no going back. There is less incentive for most networks to move to the Windows Server 2003 functional level, although large networks should evaluate it more closely, as the increased scalability and replication efficiency can be invaluable.

### Table 6-5 The differences among domain functional levels

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Password filters</td>
<td>Installed manually on each PDC and BDC</td>
<td>Installed manually on each domain controller</td>
<td>Installed automatically on all domain controllers</td>
<td>Installed manually on each domain controller</td>
<td>Installed automatically on all domain controllers</td>
</tr>
<tr>
<td>Queries using Desktop Change/Configuration Management</td>
<td>No</td>
<td>Only on Windows 2000 domain controllers</td>
<td>Yes</td>
<td>Only on Windows Server 2003 domain controllers</td>
<td>Yes</td>
</tr>
<tr>
<td>Authentication protocols</td>
<td>NTLM</td>
<td>NTLM, Kerberos</td>
<td>Kerberos</td>
<td>NTLM, Kerberos</td>
<td>Kerberos</td>
</tr>
<tr>
<td>lastLogonTimestamp user/computer attributes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>inetOrgPerson user password</td>
<td>N/A</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Redirect the Users and Computers containers</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Real World  Existing Clients Still Work in Native Mode

It’s important to understand that not all systems in the domain need to run Windows 2000, Windows XP, or Windows Server 2003 to operate in a Windows Server 2003 functional level domain. Functional levels affect only the operation of the domain controllers.

The issue of legacy systems (Windows NT, Windows 95, Windows 98, Windows Me, MS-DOS, or Windows 3.x) in the domain is important, however, when it comes to planning WINS server deployment. As long as you have legacy clients and servers in the domain, you need WINS servers for NetBIOS name resolution (unless you have a small, nonrouted network that can handle NetBIOS name resolution using broadcast). In addition, don’t turn off NetBIOS over Transmission Control Protocol/Internet Protocol (NetBIOS over TCP/IP), even if your network consists entirely of Windows 2000, Windows XP, and Windows Server 2003 systems, because legacy applications (which are many) may still rely on NetBIOS calls for network communication, as does network Browsing.

Switching Functional Levels

Before switching functional levels, take the last Windows NT 4.0 BDC or Windows 2000 domain controller offline and test whether there are any remaining legacy applications or servers that break as a result. This step is important because you cannot undo a functional level switch. Once you are sure that you don’t need any legacy domain controllers on the network, and will never again need any, log on to a domain controller using an administrator account and follow these steps to raise the forest or domain functional level:

1. Click Start, choose Administrative Tools, and then select Active Directory Domains And Trusts.

2. To raise the forest functional level, right-click Active Directory Domains And Trusts and then choose Raise Forest Functional Level. To raise the domain functional level, right-click the domain for which you want to change the functional level and choose the Raise Domain Functional Level option.

You can also upgrade forests from a command line. (See the Help menu for the procedure.)
3. Select the functional level, as shown in Figure 6-7, and then click Raise.

![Figure 6-7 The Raise Domain Functional Level dialog box](image)

4. When Windows asks you to verify the switch, click OK. Click OK in the next dialog box also.

**Important** You can upgrade the functionality of a forest only after all domains within the forest use the Windows 2000 or Windows Server 2003 functional levels. After you upgrade a forest, you can add only domains operating in the same mode or higher. To add a domain with a lower functionality level, you have to create a whole new forest.

---

**Summary**

Upgrading a computer’s operating system to Windows Server 2003 or Windows XP is relatively easy, but upgrading domains to Active Directory is considerably more complex. You must perform a lot of planning before you can upgrade a Windows NT domain, and some preparation is necessary for Windows 2000 domains as well. This planning includes steps such as documenting the network, devising a recovery plan, creating a suitable Active Directory structure, and then putting it all together into a plan of attack. Despite all the work involved, upgrading domains is usually the least painful way of moving to Active Directory.

The next chapter moves on to the initial configuration steps to take after you complete the Windows Server 2003 installation process.
Chapter 7
Configuring a New Installation

Installing Updates. ................................................................. 159
Enabling Remote Administration. ............................................. 162
Checking for Setup Problems .................................................. 164
Configuring Devices ............................................................... 164
Configuring Networking Settings ............................................. 169
Setting Up Server Roles ......................................................... 178
Securing Windows ................................................................. 184
Summary ................................................................................. 185

The goal of this chapter is to help get your system in basic working order after Microsoft Windows Server 2003 Setup completes. This involves verifying that Setup completed properly, adding and possibly troubleshooting devices, configuring the server’s network settings, and setting up the server to fulfill its role in life (or at least, its role on your network). It’s also of vital importance that you properly secure the server before placing it into service. Most of the tasks in this chapter are short and simple so that you can get the server up and running quickly after Setup completes.

Installing Updates

The Windows Server Post-Setup Security Updates window (shown in Figure 7-1) is the first thing that you see when you log on to a server as an administrator after performing a clean install of Windows Server 2003 with Service Pack 1 or Windows Server 2003 R2. Until you click Finish in the Windows Server Post-Setup Security Updates window, Windows blocks all inbound connections to the server (except port 3389 if you enabled Remote Desktop during automated Setup). This prevents viruses or hackers from compromising the security of the server while you install the latest software updates and an antivirus program. The Windows Server Post-Setup Security Updates window does not appear if you explicitly enable or disable the Windows Firewall during Setup using an Unattend.txt file or after Setup using Group Policy. If the window does not appear, update your server manually using Windows Update and also configure Automatic Updates manually.
The Windows Server Post-Setup Security Updates window appears automatically every time an administrator logs in until you click Finish. Simply closing the window does not allow inbound connections.

To use the Windows Server Post-Setup Security Updates window, follow these steps:

1. Click Update This Server in the Windows Server Post-Setup Security Updates window to launch Windows Update and install the latest software updates.
   
   Perform this step even if you automate the deployment of software updates so that you close all known vulnerabilities before you open any ports in the Windows Firewall software firewall.

2. Install an antivirus program, and then restart the server if required by the antivirus program or any of the software updates you installed.

3. After restarting, click Configure Automatic Updating For This Server in the Windows Server Post-Setup Security Updates window to enable or disable Automatic Updates.

   If you use Automatic Updates by itself or in conjunction with Windows Server Update Services (WSUS), set Automatic Updates to automatically download and install updates. If you use a different software update tool such as Systems Management Server (SMS), disable Automatic Updates. For more information on software updates, see Chapter 23.
4. Click Finish in the Windows Server Post-Setup Security Updates window to turn off Windows Firewall and allow inbound connections. After clicking Finish, you can re-enable Windows Firewall by clicking Start, Control Panel, and then Windows Firewall.

**Note**  Windows Firewall blocks Resultant Set of Policy (RSoP) and other remote administration tools by default. Test Windows Firewall for compatibility issues with your network and applications before deploying it on your network. For more information see the Microsoft Web site at http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2maint.mspx#EFAA and http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/Operations/73ee2e78-4b34-4683-b662-7e0f8582fffc3.mspx.

**Security Alert**  When you click Finish in the Windows Server Post-Setup Security Updates window, Windows creates a REG_DWORD value named DontLaunchSecurityOOBE with no data in the following registry key: HKLM\Software\Microsoft\Windows\Current Version\ServerOOBE\SecurityOOBE. This registry key blocks the Windows Server Post-Setup Security Updates window from appearing in the future.

If you have not changed the Windows Firewall settings, Windows also stops and disables the Windows Firewall/Internet Connection Sharing service after you click Finish in the Windows Server Post-Setup Security Updates window. If you enabled Internet Connection Sharing after Setup completed, Windows disables the Windows Firewall but does not stop or disable the shared Windows Firewall/Internet Connection Sharing service.

**Documenting Installations**

Human memory is fallible, which is why effective administrators take good notes. Documenting server installations helps you remember what tasks you have performed on a server, and makes it possible for other administrators to administer the server (for example, if you decide to go on vacation). If you’re a consultant, you can include a copy of your documentation along with your bills to foster trust and goodwill with clients.

Use the following list as a starting point for your documentation:

- Server hardware, including expansion capabilities
- Operating system version and service pack revision
Enabling Remote Administration

Unless you prefer the server room to your office, enable Remote Desktop after installing Windows and then relocate to a more comfortable location. Remote Desktop permits you to administer remotely virtually everything you need, as if you were sitting in front of the computer.

Security Alert  A server is only as secure as the least secure computer from which you administer it. For example, if you administer a server from a computer that has been compromised by attackers, viruses, or spyware, the server is probably now compromised as well. This is especially scary if you log on from a public terminal with a keystroke logger! To mitigate this security risk, administer servers only from computers that you secure to the same level as the servers, and do not use these computers for Web browsing and checking e-mail—and even use a separate nonadministrator account.
To enable Remote Desktop automatically, use the [TerminalServices] section of Unattend.txt. (See the Microsoft Windows Corporate Deployment Tools User’s Guide for more information.) To enable Remote Desktop manually after Setup completes, use the following procedure:

1. Click Start, choose Control Panel, and then choose System.
2. Click the Remote tab and then select the Enable Remote Desktop On This Computer check box (shown in Figure 7-2).

![Figure 7-2 Enabling Remote Desktop](image)

3. Click Select Remote Users, and optionally click Add to allow additional users or groups to administer the server remotely. (Members of the Administrators group are automatically given permission to connect remotely after Remote Desktop is enabled.)

Be extremely selective to whom you give permission to log on to a server. Consider using the default permissions (Administrators only). If you must add other users, as always, assign permissions to groups (creating new groups as necessary) rather than individual users.

4. If you enabled the Windows Firewall, you must also enable the Remote Desktop exception. To do so, click Start, choose Control Panel, choose Windows Firewall, click Exceptions, and then select the Remote Desktop check box. This enables the exception on all network connections.

To access the Windows Firewall settings for a specific network connection, right-click the network connection in the Network Connections folder, choose Properties, click Advanced, and then click Settings.
Security Alert  You can enable Remote Assistance by selecting the Turn On Remote Assistance check box in the System Properties dialog box. However, enabling Remote Assistance allows a logged-on user to give another user (who doesn’t have explicit permission to access the computer) the ability to view and even control the computer remotely. Control this capability carefully by disabling it entirely, using Group Policy to limit it, or configuring your firewall to block Remote Assistance invitations from leaving your company (block TCP port 3389). For more information about using Remote Assistance with Windows Server 2003, see http://support.microsoft.com/kb/301527/.

Checking for Setup Problems
After your Windows installation is complete, check the system for setup errors or device problems. Here’s a quick list of actions to perform:

1. Click Start, choose Administrative Tools, and then choose Computer Management.
2. Select Event Viewer and then System.
3. Review the System event log and other logs, such as Application, Directory Service and DNS Server, as necessary.
4. Select Device Manager, and check for any problem devices (or any missing devices).
5. Select Disk Management, and verify that all hard disk drives and partitions are properly recognized.
6. Review setup errors. To do so, open the \Windows\setuperr.log file. If this file is empty or does not exist, there were no errors during Setup.

Configuring Devices
One of the first things to do after installing an operating system is make sure devices are recognized and properly installed. Although Windows Server 2003 Setup usually does a superb job of detecting and configuring devices, Setup isn’t able to resolve resource conflicts or overcome a lack of drivers. You also need to enable any devices that you disconnected or disabled before starting the installation, such as an uninterruptible power supply (UPS).

To add a Plug and Play (PnP) device, plug it in and provide the drivers, if necessary. To check for device configuration problems, use Device Manager.
Using Device Manager

Device Manager is a central repository for device information in Windows. Use it to view or print the configuration and drivers loaded for any device on your system, as well as to disable, uninstall, or change the configuration for a device.

**Note** To administer devices from a command line, you can use Devcon.exe, the Windows Management Instrumentation Command-line (WMIC), or scripts. (See Chapter 13 for more information about WMIC and Windows scripts.) Devcon.exe is a command-line version of Device Manager that is part of the Windows Support Tools found in the \Support\Tools folder on your product CD. Devcon also works in Windows PE, but not in the Recovery Console. For more information, see http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/0f087656-fb2e-4828-9630-e76051a0a608.mspx.

Working with Device Manager

After opening Device Manager as part of the Computer Management (Compmgmt.msc) console or on the Hardware tab of the System tool in Control Panel, you see a list of all the devices that Windows has detected on your system. (See Figure 7-3.) Device Manager displays any nonfunctioning devices with an exclamation point, indicating that a problem exists with the device; disabled devices are displayed with a small red “x” over the icon.

![Figure 7-3 The Device Manager snap-in](image)
Note To use the Computer Management snap-in to remotely administer another computer running Microsoft Windows 2000, Windows XP, or Windows Server 2003, select Computer Management in the console tree and then choose Connect To Another Computer from the Action menu. Select the computer you want to manage, and click OK. You cannot perform some actions remotely, such as defragmenting disks or enabling Remote Desktop. In addition, Device Manager works on remote computers in read-only mode—you can diagnose problems, but you must make changes locally or using Remote Desktop.

On the far right side of the toolbar, icons are available according to the device you selected. In Figure 7-3, the following buttons are available (reading from left to right):

- **Scan For Hardware Changes** Click this button to tell the system to look for changes in hardware. Use this button after adding new PnP devices or after swapping hardware.
- **Update Driver** Click this button to open the Hardware Update Wizard, which you can use to install updated or new drivers for a device.
- **Uninstall** Select a device and click this button to uninstall it. Uninstalling a device doesn’t remove its drivers from the hard disk.
- **Disable/Enable** Select a device and click this button to disable it or enable it, depending on its current status. When a device is disabled, its resources are freed and its drivers remain but are not loaded during startup. Take care not to disable something you need to start the machine.

To change the Device Manager display, choose a setting from the View menu. (See Table 7-1.) Use the different view settings for Device Manager to organize your system’s devices in a way that makes it easy to find the information you need.

### Table 7-1 View settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices By Type</td>
<td>Shows devices categorized by device type; usually the most useful view</td>
</tr>
<tr>
<td>Devices By Connection</td>
<td>Shows all devices in relation to how they are connected to other devices</td>
</tr>
<tr>
<td>Resources By Type</td>
<td>Shows all system resources, organized by type of resource</td>
</tr>
<tr>
<td>Resources By Connection</td>
<td>Shows all system resources, organized and grouped by the device to which they’re connected</td>
</tr>
<tr>
<td>Show Hidden Devices</td>
<td>Includes devices that are not PnP, devices that might have been physically removed but still have their drivers installed, and kernel drivers that do not correspond to physical devices</td>
</tr>
</tbody>
</table>
Working with Device Properties

To display a device’s properties (as shown in Figure 7-4), select the device and then click the Properties toolbar button or double-click the device.

![Figure 7-4  The General tab of the Device Properties dialog box](image)

In the Device Properties dialog box, there are several tabs. You can view the status and configuration information—as well as the device manufacturer, device type, and location—in the upper portion of the General tab. For more information about a message displayed in the Device Status box, check Microsoft Help and Support at [http://support.microsoft.com](http://support.microsoft.com). Other tabs include the Driver tab, which displays the details of the driver and lets you update, rollback, or uninstall the driver, and the Resources tab, which displays the hardware resources for the driver. Along with these tabs, some devices have additional advanced settings or tabs for device-specific settings.

**Note**  
The device name shown in Device Manager is the name of the driver that Windows is using for the device and can be incorrect if the wrong driver is loaded for the device.
Troubleshooting Devices
Troubleshooting devices is not an exact science. Devices in Windows XP and Windows Server 2003 usually just work. If they don’t, it’s often difficult to make them work. With that said, here are some of the troubleshooting techniques gleaned from many years of device-induced headaches:

■ Open the properties for the device and see whether the cause of the problem is listed in the General tab or the Resources tab. If there are any conflicts, remove or disable the conflicting device, or plug the device into a different slot (if possible).

■ Select the device in Device Manager, and click the Uninstall toolbar button. Click Scan For Changes, and let Windows redetect the device. You can also uninstall the device and then restart Windows for a more thorough but time-consuming attempt.

■ Try plugging external devices into a different port or directly into the computer instead of through a hub. Connect high-power, bus-powered Universal Serial Bus (USB) or Firewire devices such as bus-powered external hard drives only to self-powered hubs (hubs with external power supplies). To check the power consumption of USB devices, open the device properties for the USB hub and click the Power tab.

■ If the problem is persistent, remove all unnecessary devices from the system and see whether the device works. If not, try the device in another system to see whether it’s faulty or whether there is a conflict unique to your system. If the device works, add the removed devices back one by one until a device fails, and then assess the situation. (You might need to leave some cards or devices unplugged.)

**Note** If you disable something essential—like the mouse or keyboard—you can return to the previous hardware profile by restarting with the last good hardware profile. When the Loader menu appears, press F8 and choose Last Known Good Configuration. Then choose the version of Windows you installed from the Loader menu and press Enter. This action enables the last good hardware profile.

Configuring Storage
Partition and format only the system partition during Windows installation. The Disk Management snap-in (or the new diskpart command) is a much more elegant and efficient way of partitioning and formatting disks and volumes than is Windows Setup, and it is best for you to perform as many of your disk management chores as possible after Setup completes. Here are some of the tasks that you might need to complete (see Chapter 18 for complete procedures):
■ Partition and format any additional hard disk drives.
■ Set up any software-based redundant array of independent disks (RAIDs).
■ Check the Direct Memory Access (DMA) status of any Integrated Device Electronics (IDE) devices. (To do so, in Device Manager, select IDE ATA/ATAPI Adapters, select Primary IDE Channel, and then click Properties. Click the Advanced Settings tab, and select the Transfer Mode boxes. Repeat this procedure for the secondary channel as well.)
■ Defragment all disk drives. See Chapter 18 for more information about using the Defrag.exe command and scheduling the disk defragmenter to run regularly.
■ Implement an appropriate backup strategy (as discussed in Chapter 37).

**Configuring Networking Settings**

Although most computers are properly set up for network access during Windows Setup, you might need to change these settings at some point—possibly immediately if the settings are wrong or incomplete. This section explains how to get a server running properly on a network.

**Changing Your Network Identity**

To change the identity of a server that isn’t a domain controller, log on using an account with administrator permissions and follow these steps:

1. Open the System tool in Control Panel, and then click the Computer Name tab.
2. Optionally, enter a description for the server in the Computer Description box and then click Change. (The description appears next to the computer name when browsing the local network or searching for a computer in Active Directory.)
3. Type the new name for your computer in the Computer Name text box.
4. To change the domain or workgroup to which you belong, choose either the Domain option or the Workgroup option, and then type the domain or workgroup name in the text box.
5. Click More to manually specify the domain name for your computer and to preview the Network Basic Input/Output System (NetBIOS) name for your system. Click OK when you’re finished.
Real World  Naming Computers

It’s a good idea to use a computer name that is both DNS-compatible and NetBIOS-compatible so that all types of clients see the same name for your computer. To do this, keep the name to 15 characters or fewer and don’t use asterisks or periods. To obtain the best application compatibility, use dashes instead of spaces or underscores.

Configuring Network Components

To add or change the settings for core network components such as clients, services, and protocols, open the Network Connections folder (found in Control Panel), right-click the Local Area Connection icon, and choose Properties from the shortcut menu. This procedure opens the familiar Local Area Connection Properties dialog box shown in Figure 7-5, which you can use to view and change your server’s networking components. The top of the General tab of the dialog box shows the network adapter to which you are binding networking services.

Figure 7-5  The General tab of the Local Area Connection Properties dialog box
To install a network component, click Install, choose the type of component you want to install (Client, Service, or Protocol), and then click Add. Select the component from the list presented and click OK. To configure the component (if the component has a configurable option), select the component and click Properties.

Security Alert  If you have a multihomed server (a server with more than one network adapter) and one of the connections is to the Internet, disable everything but Transmission Control Protocol/Internet Protocol (TCP/IP) (and optionally QoS Packet Scheduler) on the Internet connection to increase security. Then give your local area connections names indicating to which network the adapters are connected. To do so, right-click the connections in the Network Connections folder and choose Rename.

Configuring TCP/IP

TCP/IP is the most important protocol in today’s networks, and it’s the backbone for modern Microsoft networks. The protocol is well suited to enterprise networking, and it’s required for accessing the Internet. If you’re unfamiliar with TCP/IP, see Chapter 16 and Chapter 17 for more information.

Using Dynamic Addressing

The easiest and most reliable way to set up addressing on a network running the TCP/IP suite is to use a DHCP server to automatically distribute IP addresses. DHCP can also inform clients of the appropriate DNS servers and gateways to use. A DHCP server not only simplifies client configuration, but also simplifies server administration by managing the database of available IP addresses dynamically and automatically. (With static IP addressing, you must manually keep track of all IP addresses.)

Windows Server 2003 automatically connects to a DHCP server to obtain an IP address unless the server is a domain controller, in which case Windows prompts you to specify a static IP address. To toggle between dynamic and static IP addressing, follow these steps:

1. Select the Internet Protocol (TCP/IP) component in your Local Area Connection Properties dialog box. (Click Add to install TCP/IP if it’s not already installed.) Then click Properties. The Internet Protocol (TCP/IP) Properties dialog box appears (as shown in Figure 7-6).
2. Select the Obtain An IP Address Automatically option. Do not select this option on a DHCP server—a DHCP server must have a fixed, static IP address.

3. Select the Obtain DNS Server Address Automatically option if your DHCP server is set up to provide the DNS server addresses to clients; otherwise, select the Use The Following DNS Server Addresses option, and type the IP addresses for the DNS servers you want to use.

Real World  Assigning IP Addresses for WINS and DNS Servers

Most administrators use static IP addresses for WINS and DNS servers, and we prefer this method because it ensures that each server is at a known address, and it allows for easy configuration of specific and consistent IP addresses for DNS and WINS servers across multiple segments of the network. Some administrators, however, prefer to use DHCP reservations for their WINS and DNS servers, and this is technically feasible. It does have certain advantages—specifically it enables the DHCP administrator to easily change TCP/IP options that are included in the DHCP reservation without touching every affected server. It also allows the administrator to take back the address if the server is moved or decommissioned. See Chapter 17 for information about creating reservations on a DHCP server.
Using Static Addressing
If your network doesn’t have a DHCP server or if you’re setting up a DHCP server, use a static IP address and DNS information by using the following steps:

1. Obtain an IP address from the person who maintains the database of IP addresses that your organization can use.

2. If the network also uses DHCP servers, add an exclusion for your IP address to all DHCP servers that service the address range in which your IP address is located.

3. Select the Internet Protocol (TCP/IP) component in the Local Area Connection Properties dialog box, and click Properties.

4. Select the Use The Following IP Address option, type the address you obtained in the IP Address text box, and then press Tab to automatically fill in the default subnet mask. If the network is using a specific subnet mask, type it in the Subnet Mask text box.

5. Type the IP address for the default gateway or router in the Default Gateway text box. The default gateway forwards, or routes, any traffic destined for hosts outside the local subnet, possibly to another portion of the wide area network (WAN) or to the Internet.

6. Choose the Use The Following DNS Server Addresses option to specify the IP addresses of the DNS servers. Type the primary and secondary DNS server addresses in the text boxes provided. Click OK when you are finished.

Setting Advanced TCP/IP Options
If you need to specify advanced TCP/IP options such as WINS servers, NetBIOS over TCP/IP, or multiple IP addresses per connection, click Advanced in the TCP/IP Properties dialog box. This opens the Advanced TCP/IP Settings dialog box.

Configuring IP Settings
The Advanced TCP/IP Settings dialog box contains four tabs, the first of which is the IP Settings tab. Use this tab to add the IP address and subnet mask for a network connection as well as the gateways the server must use. To change the options on this tab, follow these steps:
1. Use the Add, Edit, and Remove buttons in the IP Addresses box (shown in Figure 7-7) to modify the computer’s IP address and subnet mask settings. You can use multiple IP addresses and subnet masks for your network connection—either to access different logical IP networks or to use different IP addresses in a single, logical IP network.

![Figure 7-7 The IP Settings tab of the Advanced TCP/IP Settings dialog box](image)

2. To add a default gateway or router, click Add and type the IP address for the router.

**Note** A router metric is a measurement of relative “cost” of the connection. Because most companies pay a flat fee for their network connections, this “cost” is usually a performance cost. As such, when you select the Automatic Metric check box, Windows automatically assigns the gateway a metric based on the performance of the gateway. To manually specify a metric, type a lower number (such as 10) for gateways that you want to use preferentially. Windows calculates the route metric for the default gateway based on the speed of the network link: 10 for a 200 Mb or faster link; 20 for an 81 Mb or faster link; 25 for a 21 Mb or faster link; 30 for a 4 Mb or faster link; 40 for a 501 Kb or faster link, or 50 for a 500 Kb or slower link. To view the routing table, type route print at a command prompt.
Configuring DNS Settings

Click the DNS tab to access the advanced DNS settings for your network connection, as shown in Figure 7-8.

![Figure 7-8 The DNS tab of the Advanced TCP/IP Settings dialog box](image)

Use the following procedure to specify your DNS settings:

1. Use the Add, Edit, and Remove buttons in the DNS Server Addresses box to add or modify the DNS servers you want to use for this connection. Use the up and down arrows next to the box to change the order in which your server queries the DNS servers.

2. Select the appropriate options for resolution of unqualified names (such as srv1).
   - Append Primary And Connection Specific DNS Suffixes  Limits the resolution for unqualified names to the domain suffixes and connection-specific suffixes. If your primary DNS suffix is eng.example.com and you type `ping srv4` at a command prompt, DNS looks for srv4.eng.example.com. If you also specify a connection-specific name (in the DNS Suffix For This Connection text box), such as dev.example.com, DNS queries srv4.eng.example.com and srv4.dev.example.com.
❑ **Append Parent Suffixes Of The Primary DNS Suffix**  Includes parent suffixes up to the second-level domain in the resolution of unqualified names. So if the primary DNS suffix is eng.uk.corp.example.com and you type `ping srv4` at a command prompt, DNS queries for the following:

```
srv4.eng.uk.corp.example.com
srv4.uk.corp.example.com
srv4.corp.example.com
srv4.example.com
```

❑ **Append These DNS Suffixes (In Order)**  Specifies the only domain suffixes to be appended to unqualified domain names during the name resolution process. If you specify domain suffixes here, Windows does not use the primary and connection-specific suffixes.

3. To override the parent DNS domain name specified for the computer in the Network Identification tab of the System Properties Control Panel tool, type the DNS domain name you want to use in the DNS Suffix For This Connection text box. (You can overrule this using Group Policy.)

4. To prevent the server from registering its IP address with the DNS server, clear the Register This Connection’s Addresses In DNS check box.

5. To force the server to register its fully qualified domain name (FQDN), including the DNS suffix listed in the DNS Suffix For This Connection text box (or taken from the DHCP server), select the Use This Connection’s DNS Suffix In DNS Registration check box.

**Configuring WINS Settings**

To specify the WINS settings for your computer, click the WINS tab in the Advanced TCP/IP Settings dialog box (shown in Figure 7-9). If WINS servers are operating on the network, add their addresses here. This enables the server to communicate via NetBIOS with hosts on other subnets that are running Microsoft operating systems earlier than Windows 2000, and it minimizes broadcast traffic. For a more thorough discussion of when to use WINS servers on your network, see Chapter 17.
To enable the use of an Lmhosts file for resolving NetBIOS names to IP addresses, select the Enable LMHOSTS Lookup check box, and click Import LMHOSTS to import an Lmhosts file. Use Lmhosts files only when absolutely necessary because trying to keep them up to date can be tricky—the miniscule reduction of network traffic that Lmhosts files offer isn’t worth it.

Note When you set up a WINS server, use the Ipconfig command at a command prompt to obtain your current IP address and then type that address in the WINS Addresses field. Don’t type any other WINS server in this field; you don’t want your WINS server registering its NetBIOS name with another WINS server if the WINS service hasn’t started in time to respond at bootup.

Make sure the Enable NetBIOS Over TCP/IP option is selected. Disable this only if you communicate exclusively with other computers running Windows 2000, Windows XP, and Windows Server 2003, or computers that rely solely on DNS for name resolution services (for example, UNIX). Also, note that any applications that use NetBIOS (and there are many of these) don’t work if you select Disable NetBIOS Over TCP/IP, so use this setting with caution.

Configuring TCP/IP Options
If you need to specify any TCP/IP options, click the Options tab in the Advanced TCP/IP Settings dialog box. Select an option you want to modify, and then click Properties. For more information about TCP/IP properties and secure TCP/IP connections, see Chapter 16.
Setting Up Server Roles

After you click Finish in the Windows Server Post-Setup Security Updates window, the Manage Your Server window (shown in Figure 7-10) appears. You can use the Manage Your Server window to perform the following tasks:

- View what roles, such as domain controller or file server, you have assigned the server.
- Add or remove roles using the Configure Your Server Wizard.
- Launch administrative tools relevant to the roles you have assigned the server.
- Get additional information about server management.

Although you can perform all these tasks using MMC consoles, the Manage Your Server window provides a central location from which you can manage a server. The Configure Your Server Wizard streamlines the role configuration process and guides you through some steps that aren't included in other wizards.

To add or remove roles from the server, use the Configure Your Server Wizard, as described in the following steps:

1. Click the Add Or Remove A Role link in the Manage Your Server window, or click Start, choose Administrative Tools, and then Configure Your Server Wizard.
2. Verify that the server is connected to the network and is properly configured, and then click Next.
The Configure Your Server Wizard scans the network looking for other servers, checks for Internet connectivity, and searches for locally attached peripherals such as printers or external hard drives.

If you enabled the Windows Firewall on the server, Windows asks whether you want to create an exception for the Configure Your Server Wizard. Doing so adds the Configure Your Server Wizard to the list of exceptions in Windows Firewall for all network connections for which the Windows Firewall is enabled.

3. If the wizard can’t find any other servers on the network, the Configuration Options page appears, which gives you the choice of configuring the server with roles typical for the first server on a network (as discussed in the “Configuring the First Server on a Network” sidebar) or choosing roles individually.

**Important** Don’t add any Windows Server 2003 domain controllers to an existing Windows 2000 or Microsoft Windows NT domain until you properly upgrade or prepare the domain. For more information, see Chapter 6.

4. If the wizard finds other servers on the network, if you have previously set up roles on the server, or if you chose Custom Configuration on the Configuration Options page, the wizard displays a list of server roles you can choose. Choose a server role from the list, as shown in Figure 7-11 and described in Table 7-2, and then follow the instructions onscreen.

If you enabled the Windows Firewall, verify that the proper exceptions are enabled in the firewall (for example, File and Printer Sharing) after setting up a role.
### Table 7-2 Server role choices in the Configure Your Server Wizard

<table>
<thead>
<tr>
<th>Role</th>
<th>Windows Server 2003</th>
<th>Windows Server 2003 R2</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Server</td>
<td>Configures disk quotas and the Indexing service; installs the File Server Management console and launches the Share A Folder Wizard.</td>
<td>Upgrades the File Server Management console; installs the File Server Resource Management and DFS Management consoles; and allows you to optionally install the DFS Replication Service, the Storage Manager for SANs (and the Virtual Disk Service version 1.1), Microsoft Services for NFS, and File Services For Macintosh components. Might require a restart. See Chapter 10 for more information.</td>
</tr>
<tr>
<td>SharePoint Services</td>
<td>Not available.</td>
<td>Installs Internet Information Service (IIS), ASP.NET and Windows SharePoint Services 2.0 with Microsoft SQL Server Desktop Engine (WMSDE) using the default settings.</td>
</tr>
<tr>
<td>Print Server</td>
<td>Launches the Add Printer Wizard and Add Printer Driver Wizard. See Chapter 8 for more information.</td>
<td>Installs the Print Management console. See Chapter 8 for more information.</td>
</tr>
<tr>
<td>Application Server</td>
<td>Installs IIS and optionally enables Microsoft FrontPage Server extensions and/or ASP.NET with the .NET Framework. Also enables COM+ for remote transactions and Microsoft Distributed Transaction Coordinator (DTC) for remote access.</td>
<td>Unchanged.</td>
</tr>
<tr>
<td>Mail Server</td>
<td>Installs and configures a lightweight POP3 mail server software and the SMTP service of IIS. See Chapter 33 for more information about the SMTP service, or Windows Help for information about the POP3 server.</td>
<td>Unchanged.</td>
</tr>
<tr>
<td>Terminal Services</td>
<td>Installs Terminal Services (not Remote Desktop). Requires a restart and a Terminal Services License Server on the network. See Chapter 30 for more information.</td>
<td>Unchanged.</td>
</tr>
</tbody>
</table>
Table 7-2  Server role choices in the Configure Your Server Wizard

<table>
<thead>
<tr>
<th>Role</th>
<th>Windows Server 2003</th>
<th>Windows Server 2003 R2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Controller</td>
<td>Starts the Active Directory Installation Wizard (dcpromo), and optionally installs and configures DHCP and DNS. Also installs Routing And Remote Access (RRAS) on multihomed servers. See Chapter 14 for more information.</td>
<td>Unchanged.</td>
</tr>
<tr>
<td>DNS Server</td>
<td>Installs the DNS server software, and starts the Configure A DNS Server Wizard. See Chapter 17 for more information.</td>
<td>Unchanged.</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>Installs the DHCP server software, and starts the New Scope Wizard. See Chapter 17 for more information.</td>
<td>Unchanged.</td>
</tr>
<tr>
<td>WINS Server</td>
<td>Installs the WINS server software. See Chapter 17 for more information.</td>
<td>Unchanged.</td>
</tr>
</tbody>
</table>

**Note**  You can also install components manually using the Windows Components Wizard, or from a command prompt using Sysocmgr.exe. For information about Sysocmgr.exe, see the Microsoft Windows Corporate Deployment Tools User’s Guide (Deploy.chm and Ref.chm) on Windows Server 2003 R2 Disc 2 or at the Microsoft Download Center (http://www.microsoft.com/downloads/).

**Configuring the First Server on a Network**

If you are setting up the first server in a new domain, choose the Typical Configuration For A First Server option in the Configure Your Server Wizard (as described in step 3 of the procedure under “Setting Up Server Roles”). Doing so instructs the Configure Your Server Wizard to guide you through the configuration process of setting up Active Directory, DNS, and DHCP, as described in the following steps:

1. If you have not done so already, specify a static IP address for the server in the appropriate address range. See Chapter 16 for information about choosing an appropriate network address.
2. After choosing the Typical Configuration For A First Server option in the Configure Your Server Wizard, type the domain name you want to use in the first text box, as shown in Figure 7-12, and then click Next.

Use a domain name that is different from your Internet domain name, and/or uses the .local, .office, or .lan suffix, which are not valid Internet top-level domains. Using separate internal and external domain names reduces confusion for end-users, simplifies the DNS server configuration, and can increase security by preventing DNS from making internal host names available to Internet DNS servers. For more information about namespace planning, see Chapter 3.

3. If the server is multihomed (has multiple network adapters) and you have enabled the Windows Firewall/Internet Connection Sharing service, stop it and disable it using the Services console in the Administrative Tools folder. RRAS cannot install properly while the Windows Firewall/Internet Connection Sharing service is running.

4. Verify that the DNS domain name and NetBIOS domain name are correct, click Next, verify the settings, and then click Next again.

5. If the server is multihomed, the Routing and Remote Access Server Setup Wizard appears. Select the network adapter that connects to the Internet, choose whether to enable the RRAS Basic Firewall, click Next, and then click Finish.
6. At this point, Windows installs RRAS (if the server has multiple enabled network cards), DNS, DHCP, and Active Directory and then restarts the computer. After you log on again, the Configure Your Server Wizard assigns the server a static IP address (192.168.0.1) if the server does not already have one, attempts to assign a DNS forwarder, creates a scope of IP addresses for DHCP (192.168.0.10–192.168.0.254 if the static IP address is 192.168.0.1), and authorizes the DHCP server in Active Directory.

7. Configure all systems and devices on your network to use DHCP or to use a static IP address in the range of 192.168.0.2–192.168.0.9 (if the static IP address for the server is 192.168.0.1). (You can expand the reserved address range by making the DHCP scope smaller or adding reservations—see Chapter 17 for more information.) If you did not assign a static IP address to the server before performing this procedure and you use a router to share your Internet connection, make sure that the router does not use 192.168.0.1 as its IP address, and disable its DHCP server.

8. Change the DHCP options (as described in Chapter 17) to provide the appropriate IP address of your Internet router (the default gateway).

---

**Real World  Special Facts About Domain Controllers**

Although it’s true that all domain controllers are peers, the first domain controller in a domain is special. The first Active Directory domain controller in a domain automatically assumes the role of Global Catalog server. There must be at least one Global Catalog server in every domain. The global catalog is a database that contains a full replica of all directory objects in its host domain, plus a partial replica of all directory objects in every domain in the forest. The global catalog’s role is to locate in which domain a resource is located and to provide universal group membership information during a logon event. After you install additional controllers, you can reassign the role of Global Catalog server or designate more than one machine as a Global Catalog server. (This is necessary only in multidomain forests and in some branch-office scenarios.) This process is described in Chapter 14.

The first domain controller also takes the operations master roles. A single controller must perform each of these roles because they are functions that cannot be executed in different places at the same time. (For example, a single controller must handle the creation of security identifiers to ensure that each identifier is unique.) Under most circumstances, you don’t have to change the location for any of the operations master roles, but it is helpful to understand each of the roles and what happens in the case of failure. See Chapter 15 for information about operations master roles.
Securing Windows

Entire books could be (and have been) written about securing Windows Server 2003, and rightly so; it’s an important topic. In the meantime, here are some security precautions to take before considering your server “online” (for more information, see Chapter 21 and Chapter 22):

■ Use the Security Configuration Wizard (SCW) to create and apply policies that lock down the server and disable unneeded services (but be careful not to lock down the server so much that clients cannot communicate with it).


■ Implement appropriate physical security—if an attacker gains physical access to a system, it is no longer your system.

■ Enable security auditing. (The SCW can automatically configure an appropriate audit policy.)

■ Eliminate FAT. (Make sure all hard disk partitions are using NTFS.)

■ Rename the administrator account, and create a strong password for it.

■ Do not install unnecessary applications such as e-mail, Microsoft Office, or utilities.

■ Disable unnecessary accounts.

■ Check folder permissions.

■ Remove unnecessary file shares.

■ Install antivirus software and the latest virus definition files.

■ Set appropriate password policies and account lockout policies for your network using Group Policy.
Real World  Protecting the Administrator Account

A good precaution after installation is to use the built-in Administrator account to make a second account with full administrative privileges. This account can have a generic name, or you can call it something descriptive. Use it for all the day-to-day administrative work.

Then rename the default Administrator account and relegate it to semi-retirement. If your other administrator account gets disabled for some reason, you still have the original uncontaminated, known-to-be-good administrator account to which you can resort, just in case.

For bonus points, create another account, named Administrator, and disable it. Enable the Audit Account Logon Events setting in Group Policy, and then scan the Event Log for failures to log on with the decoy Administrator account. This tells you how much “action” the account is seeing from internal hackers (or at least, how forgetful the administrators are).

**Note** Clear the logon history after installing Windows so that would-be hackers must figure out both the password and the user name. To do this on a standalone server, click Start, choose Administrative Tools, and then Local Security Policy. Select Local Policies and then Security Options, double-click Interactive Logon: Do Not Display Last User Name, choose Enabled, and then click OK. Use Group Policy to control this on a member server or domain controller.

Summary

After installing Windows Server 2003, you have some important configuration steps to perform. These tasks include documenting the installation, installing the latest software updates, enabling remote administration, and configuring devices and network settings. You also need to set up the server to fulfill its intended role on the network, which is made easier by the useful Manage Your Server window and the Configure Your Server Wizard. The last part of a server’s post-installation shakedown is securing the server as appropriate for its roles.

In the next chapter, the topic is how to manage print servers.
Chapter 8
Installing and Managing Printers

Planning Printer Deployment .................................................. 187
Installing Printers ................................................................. 195
Managing Printers and Print Servers ........................................ 199
Changing Printer Options ....................................................... 208
Managing Printer Drivers ....................................................... 214
Printer Maintenance and Troubleshooting ............................... 217
Summary ................................................................................. 226

Back in the early, heady days of desktop personal computers, people talked a lot about the coming “paperless office.” This vision of the future has not come to pass. In fact, today the paper-recycling box is the biggest receptacle in an average office!

The cost of basic printers has declined over the years, but increasingly, companies have invested in sophisticated high-speed printers that enable users to handle jobs that once required an outside print shop. These are expensive both to buy and to use. Therefore, printer sharing remains an important function of enterprise networks. Setting up multiple users to share printers reduces cost and can increase printing output. You can direct routine work to low cost-per-page printers, schedule long print jobs for off hours, and limit access to high-end printers.

Planning Printer Deployment

Before you deploy printers and Microsoft Windows Server 2003 print servers, it is important to establish printer-naming and location-naming conventions, evaluate whether to upgrade or migrate existing print servers, and prepare for print server failures.

\section*{Establishing Printer Naming Conventions}

An effective printer-naming convention is important if you want to ensure that users can easily identify printers on the network. When creating a printer naming convention, use the following guidelines:

- Obtain management support for the convention so that you can establish a naming scheme that is enforceable in the company.

- The \textit{printer name} can be any length up to 220 characters, but it should be much shorter than this for readability and so that users can remember the printer name.

- The \textit{share name} can be up to 80 characters long, but it should be shorter than this for readability and compatibility. The share name is the name that all clients see when they browse for a printer, use the Add Printer Wizard, or use the Net Use command.

Some older applications cannot print to printers with fully qualified printer share names (the computer name and printer share name combined) that exceed 31 characters, or to print servers where the default printer's share name exceeds 31 characters. MS-DOS and Microsoft Windows 3.x clients cannot access printers with share names longer than eight characters followed by a three-character extension. Clients using other operating systems might also have trouble with names longer than 31 characters or names containing spaces or other special characters.

- The printer name and share name should convey as much relevant information about the printer as possible without exceeding a reasonable length.

Most companies use a variant of the printer model name followed by a number if multiple identical printers exist in the same location. Some companies also include the location of the printer in the printer name, for example, LaserJet8100_Floor10_1.

\section*{Creating Location-Naming Conventions}

In small organizations, finding printers is easy: stand up and look around, or ask the person sitting next to you. This does not work as well in larger organizations where printers are widely scattered and of varying capabilities. A much easier way is to browse or search for printers in Active Directory based on the criteria you want, including printer features and printer location.
Location names are similar in form to domain names and use the name/name/name... syntax. They start with the most general location name and become progressively more specific. For example, a multinational corporation might have the location name structure shown in Figure 8-1. Each part name can be a maximum of 32 characters and can contain any characters except the forward slash (/), which Windows reserves as a delimiter. The entire location name cannot be longer than 260 characters, with a maximum of 256 levels.

Figure 8-1  A sample location name structure

Note  As with choosing domain names, creating a printer location-naming scheme is political, so get the appropriate sign-off from management. Keep the naming convention simple and easy to understand for end users—after all, they need to be able to look at the location name and answer the age-old question “Where’s my printout?” A sample location name is NorthAmerica/Seattle/HQ/Floor10/ConferenceRoom. (You can be more precise than just naming the location of the subnet.)

After creating a printer location-naming convention, enable printer location tracking in Active Directory, as discussed in the “Enabling Printer Location Tracking” section of this chapter.
If you are not using the printer location-tracking feature of Active Directory, you can still include location information with printers, although this approach has some limitations. To enter location information, type the location name in the General tab of the printer’s Properties dialog box. Be careful and consistent with location names. Make sure that all administrators use the same name for a particular location, and keep the names short and easy to remember: users need to know the exact location names when they search for printers if Active Directory’s location-browsing capabilities are unavailable.

### Meeting the Requirements for Printer Location Tracking

Printer location tracking requires a few conditions to work properly. These conditions are easy for most organizations to meet, but the network infrastructure of some companies might require modification. To use printer location tracking, the network must meet the following conditions:

- The network must have an IP addressing scheme that approximates the network’s physical layout.
- The Active Directory structure must contain more than one site or more than one subnet. If you do not have multiple IP subnets, you can use the Active Directory Sites and Subnets console to create subnets from address ranges within a subnet that correspond to physical locations.
- The client computers must be able to query Active Directory. (They must support Lightweight Directory Access Protocol version 2 or later.) To use printer location tracking on computers running Windows 98 or Windows NT 4.0, install the Active Directory Client Extensions.
- Each site should be on a separate subnet.
- Each subnet that clients need to access should have its own subnet object in Active Directory.
- You have defined a printer location-naming convention.

For information about how to install Active Directory and create the appropriate subnets for the enterprise using Active Directory Sites and Services, see Chapter 14.

---

**Note**  
Try to keep printers and print servers on the same network segment as the users of the printer if you expect a high print volume. This approach minimizes the impact to users on other parts of the network. In any case, try to minimize the number of network hops a print job needs to take to get from users to their default printer. Deploy print servers to branch offices to prevent Windows from sending print jobs across a WAN link to the print server and then back across the WAN link to the printer. You can centrally manage print servers using the new Print Management Console.
Enabling Printer Location Tracking

To enable users to search Active Directory easily for printers by location, create a location-naming convention as discussed in the “Creating Location-Naming Conventions” section of this chapter, and then follow these steps to set up printer location tracking:

1. Open Active Directory Sites and Services from the Administrative Tools menu.
2. In the Sites folder, right-click the first site and choose Properties from the shortcut menu.
3. Click the Location tab, and type the location name for the site, as shown in Figure 8-2, or click Browse to select the location from the location tree for the enterprise.

4. Click OK, and repeat steps 2 and 3 for each site and subnet on the network.
5. Create a new Group Policy object that applies to all computers on which you enable printer location tracking. To do this, open the Group Policy Management Console (available from the Microsoft Web site at http://go.microsoft.com/fwlink/?linkid=21813), right-click the domain, and then choose Create And Link A GPO Here.
6. Right-click the GPO, and choose Edit. The Group Policy Object Editor appears.
7. In the console tree, click Computer Configuration, the Administrative Templates folder, and finally Printers (shown in Figure 8-3).
8. Double-click the Pre-Populate Printer Search Location Text policy, select Enabled, and click OK. Close the Group Policy window, and then close the domain’s Properties dialog box. When searching Active Directory, this automatically fills in the location of the user’s subnet.

9. Open the Print Management Console or Printers And Faxes folder for your print server, right-click a printer, choose Properties, and then type the location in the Location text box, or click Browse to select the location from the location tree for the enterprise. Repeat this for all printers in Active Directory, or use the Prncnfg.vbs script to automate this procedure. (For help using this script, type `cscript %windir%\system32\prncnfg.vbs /?` at a command prompt.)

Note You probably want to be more specific in the Location box for printers than simply providing the location of the subnet. For example, you might add a room number or name.

10. Test printer location tracking by searching Active Directory by location from a client machine.

Choosing Whether to Upgrade or Migrate Print Servers

If you still have Microsoft Windows NT 4 print servers deployed in your organization, it is time to upgrade or replace them with Windows Server 2003 print servers. Doing so increases reliability, manageability, and performance. You can also consolidate several Windows NT 4 print servers into a single Windows Server 2003 print server (when appropriate), providing further savings in operating costs.
There are three ways of dealing with existing Windows NT 4 (and Windows 2000) print servers:

■ **Perform an in-place upgrade**  Upgrading the server to Windows Server 2003 preserves all settings, printer drivers, ports, and print queues, saving reconfiguration time, which can be significant for print servers with a large number of installed printers. Windows Server 2003 attempts to upgrade existing drivers to a native level 3 version, but it preserves existing Windows NT 4 printer drivers (level 2 drivers) if it cannot locate a native driver. (Windows NT 4 printer drivers run in kernel mode and can destabilize the operating system or force a reboot if they crash.)

Upgrading Windows 2000 print servers does not require updating drivers.

■ **Perform a clean install**  A clean install provides the most stable and high-performance environment, but it takes the most time to set up and install all printers.

■ **Migrate settings to a new server**  The Print Migrator version 3.1 utility makes it possible to save all relevant print server settings (drivers, ports, queues, and preferences) from a Windows NT 4.0, Windows 2000 Server, or Windows Server 2003 print server and then apply them to a server running Windows Server 2003. This saves time as compared to a normal clean install. If you choose this approach, replace as many of the Windows NT printer drivers as possible with native level 3 drivers.

If print server downtime is an issue, set up a new Windows Server 2003 print server before taking the existing print server offline. Then switch users to the new print server, using one of the methods discussed in the “Preparing for Print Server Failure” section later in this chapter. You can also migrate the print server to a Windows Server 2003 print server by using the Print Migrator utility, as discussed in the following sidebar.

---

**Note**  Before you upgrade or migrate a Windows NT 4 print server, use the Fixprnsv.exe utility (located in the \Printers\Fixprnsv folder on the Windows Server 2003 CD-ROM) to identify incompatible drivers. After the upgrade or migration is finished, you can use the utility again to identify any incompatible drivers that made it through, and possibly upgrade them.

---

**Using Printer Migrator to Back Up or Migrate Print Servers**

Printer Migrator is a useful tool that you can use to back up print server settings, drivers, and print queues from a print server running Windows NT 4, Windows 2000, or Windows Server 2003 system, and restore the data to any server running Windows Server 2003.
You can download Printer Migrator from the Microsoft Web site at http://www.microsoft.com/WindowsServer2003/techinfo/overview/printmigrator3.1.mspx, and then use the following list to back up or migrate print server settings after installing and opening the program (which is shown in Figure 8-4).

- To view the printer settings of a remote server, choose Target from the View menu and type the UNC name of the remote print server.

- To back up a print server, choose Backup from the Actions menu, type the computer name of the server that you want to back up in the Target Server box, type a name for the backup file, and then click Open. This saves the configuration to a compressed .CAB file.

- To restore a backup file, choose Restore from the Actions menu, type the name of the server on which you want to restore the configuration in the Target Server box (or leave it blank to restore to the local machine), specify the backup file, and then click Open.

To attempt to convert Line Printer Remote (LPR) printer ports to the faster Windows Server 2003 standard Transmission Control Protocol/Internet Protocol (TCP/IP) printer port (SPM) during a restore operation, select the Attempt LPR To SPM Conversion check box. To migrate LPR printer ports to a new print server without converting them to SPM ports, install Print Services for UNIX on the target machine before migrating the LPR ports and do not select the Install The Active Directory Client Extensions check box.  

---

**Figure 8-4** The Printer Migrator program
If you attempt to restore the configuration of a Windows NT 4.0 print server on a Windows Server 2003 server, Print Migrator warns you that kernel-mode drivers (Windows NT 4.0 drivers) are blocked. Click Cancel to install the Windows NT 4.0 drivers anyway, or click OK to exit without installing the drivers. After restoring the Windows NT 4.0 drivers, upgrade the drivers to level 3 (Windows Server 2003/Windows 2000/Windows XP) if possible.

Installing Printers

Installing a printer is a familiar task for most computer users—if the printer uses a USB or IEEE 1394 (Firewire) connection, plug it in to the server and insert the driver disk. If the printer uses a network connection (the best way to connect a printer), use the Add Printer Wizard to install the printer, as described in this section, or use the new automatic detection feature of the Windows Server 2003 R2 Print Management Console, as described in the “Using the Print Management Console” section of this chapter.

To set up a network-based printer through a standard TCP/IP printer port, follow these steps:

1. Connect the printer to the network, and set up the printer with the proper TCP/IP settings for the network. If you configure the printer to use DHCP, create a DHCP reservation for the printer so that its address does not change.

   **Note** You can connect Windows Server 2003 to printers shared by other Windows servers or clients, and then share these connections. To do so, choose the network printer option in the Add Printer Wizard and then follow the instructions onscreen.

2. Select the appropriate print server in the Print Management Console and choose Add Printer from the Action menu, or open the Printers And Faxes folder and choose Add Printer from the File menu. The Add Printer Wizard appears.

3. On the Local Or Network Printer page, select the Local Printer Attached To This Computer option, and clear the Automatically Detect And Install My Plug And Play Printer check box.

4. On the Select A Printer Port page, select Create A New Port, select Standard TCP/IP Port from the drop-down list, and then click Next. Windows launches the Add Standard TCP/IP Printer Port Wizard.
Under the Hood  The Standard Port Monitor and LPR

Windows Server 2003 includes an improved version of the standard TCP/IP port monitor (Tcpmon.dll), which supports the majority of network printers, provides more status information than a Line Printer Remote (LPR) port, and is 50 percent faster than the LPR Port Monitor (Lprmon.dll). By default, Windows uses the raw printer protocol with the standard port monitor for the highest performance. However, if the printer requires LPR support, you can configure the standard port monitor to use an LPR-compatible mode, which offers increased compatibility with Line Printer Daemon (LPD) print servers and printers that implement the LPD service, while still providing better print performance than the LPR port monitor.

If you cannot get a network printer to work using the standard port monitor, you can install Print Services For UNIX and install the printer using a fully RFC 1179 compliant LPR monitor. To do so, on the Select A Printer Port page of the Add Printer Wizard, select LPR Port instead of Standard TCP/IP Port. For more information about the differences between the standard port monitor and the LPR port monitor, see Microsoft Knowledge Base article 814586 on the Microsoft Web site at http://support.microsoft.com/kb/814586/.

5. On the Add Port page, shown in Figure 8-5, type the IP address of the printer in the first text box and then click Next. Windows attempts to connect to the printer.

![Figure 8-5 The Add Port page of the Add Standard TCP/IP Printer Port Wizard](image)
6. If Windows cannot detect the printer, the Additional Port Information Required page appears. Accept the Generic Network Card device type (which works for most printers), select a specific device type, or click Custom to specify the port settings manually. Click Next to continue.

Most device types in the list configure the printer port to use the Line Printer Remote (LPR) protocol, which is slower than the raw protocol. If the device type that matches your printer uses the LPR protocol, try selecting Generic Network Card instead or try choosing Custom and manually specifying the RAW protocol and port 9100 (the default port for the raw protocol).

7. If you select Custom, the Configure Standard TCP/IP Port Monitor dialog box appears, as shown in Figure 8-6. Specify the appropriate settings and then click OK.

- Choose Raw to use the raw protocol, or choose LPR to use a slower LPR-compatible protocol to communicate with a printer that uses the LPD service.
- Type the port number for the printer if you are using the raw protocol. Use the default port number (9100) unless the printer documentation specifies that you must use a different port.
- If you choose the LPR protocol, type the queue name in the box provided.
- If the printer supports Simple Network Management Protocol (SNMP) as defined in RFC 1759, select the SNMP Status Enabled check box and type the Community Name (usually “public”) and SNMP Device Index.

![Figure 8-6 The Configure Standard TCP/IP Port Monitor dialog box of the Add Standard TCP/IP Printer Port Wizard](image)
8. If Windows does not detect the printer, choose the printer model on the Install Printer Software page.

9. On the Name Your Printer page, type a name for the printer in the Printer Name text box.

10. On the Printer Sharing page, type a share name for the printer.

    **Note** For maximum compatibility and readability, choose a printer name with 31 characters or fewer that does not contain any spaces or special characters. For compatibility with MS-DOS and Windows 3.x clients and software, use an eight-character or shorter share name.

11. On the Location And Comment page, type the location name for the printer in the Location box. (See the “Creating Location-Naming Conventions” section earlier in this chapter for information about choosing a location-naming scheme.) Describe the capabilities of the printer in the Comment text box.

12. Print a test page by clicking Yes on the Print Test Page page, and then click Next to display a summary of the printer installation. Click Finish to complete the installation.

### How Printers Are Published in Active Directory

Windows publishes printers automatically to whatever domain controller the print server contacts first. The domain controller then replicates the new printer objects (printQueue objects in Active Directory-speak) with the other domain controllers so that clients can find the printers regardless of which domain controller they query. The maximum propagation delay within a single site is about 30 minutes, but it is usually closer to 5 to 10 minutes.

When a print server updates the characteristics of its printers, the print server automatically updates Active Directory. If a print server goes offline, Windows removes (prunes) the printers shared by the print server from Active Directory until the server comes back online, at which point the print server republishes its printers.
Ideally, Active Directory should list all printers that are available to clients. For this to happen, you must manually publish printer shares of a Windows NT 4.0 print server. To do so, launch Active Directory Users and Computers from the Administrative Tools folder; right-click the domain, subnet, or organizational unit in which you want to publish the printer; and choose New Printer from the shortcut menu. Type the path of the printer you want to publish in the Network Path Of The Pre-Windows 2000 Print Share box, and then click OK.

Managing Printers and Print Servers

This section focuses on some common management chores such as connecting to a printer and viewing the print jobs; managing print jobs in the queue; and transferring print jobs from one printer to another using the new Windows Server 2003 R2 Print Management Console, the Printers and Faxes folder, a Web browser, or a command prompt.

Using the Print Management Console

The Print Management Console (PMC) is a new MMC management console that makes it possible to centrally manage and monitor print servers. You can use the PMC to manage a single print server or hundreds of print servers with thousands of printers across the world, all without consuming a significant amount of network bandwidth or ever touching the Printers and Faxes folder.

To install the Print Management Console, install Windows Server 2003 R2 and then install or upgrade the Print Server role, as discussed in Chapter 7, or download and install the PMC setup files for Windows XP from http://www.microsoft.com/downloads. You cannot install the Print Management Console on a computer running Windows XP.

Important To deploy printer connections via Group Policy, you must update the Active Directory schema to Windows Server 2003 R2 level, although you do not need to deploy any Windows Server 2003 R2 domain controllers. For more information about updating the Active Directory schema, see Chapter 6.

After you install the Print Management Console, you can open it from the Manage Your Server window or from the Administrative Tools folder. You can monitor print servers using any account, but you must use an account with Administrator privileges to administer printers or server.

Use the following list to perform common tasks using the Print Management Console:

- To add print servers to the console, right-click the Servers container and then choose Add/Remove Servers. You can manage any Windows Server 2003, Windows XP, or Windows 2000 print server, and you can view the queue status of any SAMBA print...
server with which you can authenticate. You can also manage Windows NT 4.0 print servers, although Microsoft does not officially support this scenario and the functionality might differ from that of newer versions of Windows.

**Note** If you cannot see any printers on a remote server, open Windows Firewall from Control Panel, click the Exceptions tab, select the File And Printer Sharing check box, and click Edit. Use the Edit A Service dialog box to change the scope of each port to Any Computer. Before changing the scope to Any Computer in a production environment, evaluate the potential security risks and verify that other firewalls on the network block these ports from distrusted networks such as the Internet.

- Use the Drivers, Forms, Ports, and Printers containers to view and manage drivers, forms, ports, and printers on a print server.

**Note** Set the default print settings to a standard-size paper (most likely letter size) and the lowest quality setting that is acceptable to the users to increase printing speed, reduce waste, and lower costs.

- Choose Add/Remove Columns from the View menu to add or remove additional columns from a view. Click a column heading to sort the view by that heading.

- To view print jobs and the printer configuration Web page for each printer (when available), right-click a Printers container and choose Show Extended View. Figure 8-7 shows the Extended View of Print Management Console.

- To perform a task on a group of printers, select the printers, right-click them, and choose the appropriate command from the shortcut menu. You can perform the following tasks on a group of printers:
  - Pause printing
  - Resume printing
  - Publish printers in Active Directory
  - Unpublish printers in Active Directory
  - Cancel all print jobs
  - Delete the printers

- To manage the print server options, right-click the print server and then choose Properties.

- To automatically add printers on a local subnet, right-click Local Print Server (you cannot perform this procedure on a remote print server), and then choose Automatically Add Network Printers. If Windows cannot find the proper driver for a printer it detects, specify the location of the proper driver.

- To manage Integrated Color Management (ICM) color profiles, right-click the appropriate printer, choose Properties, and then click the Color Management tab.
Creating Filtered Printers Folders

You can create virtual folders in the Print Management Console called filtered printers folders that display printers that match the criteria you specify—for example, printers with errors. You can also use filtered printers folders to send e-mail notifications or launch scripts when Windows finds printers that match the criteria that you specify—this is invaluable if you want Windows to notify you when a printer goes offline, for example.

To create a filtered printers folder, which appears in the Print Management Console under the top-level Printers container, use the following steps:

1. Right-click the Custom Printer Filters container, and choose Add New Printer Filter.

2. On the Printer Filter Name and Description page, type a name and optionally a description for the folder, and then select the Display The Total Number Of Printers Next To The Name Of The Printer Filter to display in the console tree how many printers the folder contains.

3. On the Define A Printer Filter page, specify what criteria to use when selecting printers to display in the folder.
4. On the Set Notifications page, choose whether you want to receive an e-mail notification or launch a script when Windows detects printers that match the criteria you specify.

---

**Note** You can save a Print Management Console window that you customize as a new Microsoft Management Console (MMC) file (.msc) by choosing Save As from the File menu. This is the fastest way to duplicate the Print Management Console settings, including server connections and filtered printers folders, on another server.

---

**Note** To create a Server Notification that e-mails you or launches a script when Windows loses contact with the Spooler service of a remote print server, right-click the print server and choose Set Notifications.

### Deploying Printer Connections

To deploy printer connections to users automatically, you have three options. You can connect a computer to shared printers during unattended Setup, as discussed in Chapter 5. You can write a custom logon script and deploy it via Group Policy. Or you can use the Print Management Console in Windows Server 2003 R2 to deploy printer connections to users via Group Policy.

Using the Print Management Console to deploy printer connections is the most convenient method of deploying printer connections to computers running Windows XP Professional, Windows Server 2003, or Windows 2000. However, on computers running Windows 2000 you can deploy printer connections only by using user-based Group Policy—not computer-based Group Policy.

To deploy printer connections using the Print Management Console, use the following steps:

1. Update the Active Directory schema to the Windows Server 2003 R2 revision, as discussed in Chapter 6.

2. Copy the Pushprinterconnections.exe script (located in the %WINDIR%\Pmcsnap folder) to a network share that is accessible by all users and computers to which you want to deploy printer connections.

Create a new Group Policy object that applies to all computers or users to which you want to be able to deploy printer connections. To do so, open the Group Policy Management Console (available from the Microsoft Web site at http://go.microsoft.com/fwlink/?linkid=21813), right-click the domain or OU in which you want to deploy the startup script, and then choose Create And Link A GPO Here. See Chapter 11 for more information about Group Policy.
3. Right-click the GPO, and choose Edit. The Group Policy Object Editor appears.

4. To deploy printer connections to users, click User Configuration in the console tree, Windows Settings, and finally Scripts.
   To deploy printer connections to computers, instead click Computer Configuration, Windows Settings, and finally Scripts.

5. Double-click Logon or Startup as appropriate, and then use the Logon Properties dialog box (shown in Figure 8-8) or Startup Properties dialog box to add the network path to the Pushprinterconnections.exe script. Close the Group Policy Object Editor when you are finished.

   ![Figure 8-8 The Logon Properties dialog box](image)

   **Important** The Pushprinterconnections.exe script must execute during every Windows startup when deploying printer connections to computers, or during every user logon when deploying printer connections to users. Executing the Pushprinterconnections.exe script at Windows startup does not enable you to deploy printer connections to users—you must run it as a logon script. If the script does not run, new or updated printer connections that you deploy via Group Policy do not appear on the client computers.

6. In the Print Management Console, right-click the printer you want to deploy to clients and then choose Deploy With Group Policy.
7. In the Deploy With Group Policy dialog box (shown in Figure 8-9), click Browse to select the GPO you created to deploy printer connections.

![Deploy With Group Policy dialog box](image)

Figure 8-9  The Deploy With Group Policy dialog box

8. In the Deploy With Group Policy dialog box, select whether to deploy printer connections to users and/or computers in the GPO:

   - To deploy the printer connections to users in the GPO, select the The Users That This GPO Applies To (Per User) check box.
   - To deploy the printer connections to computers in the GPO, select the The Computers That This GPO Applies To (Per Machine) check box.
   - To remove a printer connection, select the connection and click Remove.

9. Click OK when you are finished. The Print Management console adds the Deployed Printers node to the Computer Configuration and User Configuration nodes of the appropriate Group Policy Object, adds the specified printers to the appropriate Deployed Printers node, and then displays the results of the operation in the Print Management Console dialog box. Verify that the operation succeeded and then click OK.

   Windows installs or removes the printer connections the next time the user logs on (for per-user deployments), or the next time the computer restarts (for per-machine deployments).

Managing Print Jobs from Windows

The easiest way to manage print servers is to use the Print Management Console. However, if you do not yet have a Windows Server 2003 R2 print server on your network, you can manage printers from any machine running Windows Server 2003, Windows XP, or
Windows 2000 using the Printers And Faxes folder. Regardless of the method you use to manage printers, the tasks are identical and simple.

To manage print jobs, double-click the printer in the Print Management Console or the Printers And Faxes folder and then use the following list:

- To temporarily stop a document from printing, right-click the selected document and choose Pause from the shortcut menu. To resume printing, right-click the document and then choose Resume.
- To temporarily stop all documents from printing, choose Pause Printing from the Printers menu. To resume printing all documents, select Pause Printing a second time from the Printer menu.
- To cancel one or more print jobs, select the documents, right-click, and choose Cancel from the shortcut menu. (You can also cancel print jobs by selecting them and pressing Delete.)
- To cancel all print jobs in the print queue, select Cancel All Documents from the Printer menu.
- To restart a print job (that is, force the document to print from the beginning again), right-click the document and choose Restart from the shortcut menu.

Sometimes a print job appears stuck in the queue and you cannot delete it. If this occurs, turn the printer off and then on again, or stop the Print Spooler service on the print server and restart it.

- To change the priority or scheduling of a print job, right-click the print job, choose Properties, and then use the Priority slider to adjust the priority of the document, with 1 being the lowest priority and 99 the highest priority.

To specify that the document should be printed only during a certain period, select the Only From option and choose the time range to allow the document to print.

**Note**  Use the Schedule feature to set a large document to print only during times when you anticipate the printer to be available.

- To move all documents from one printer to another printer that can use the same printer driver, right-click the printer, choose Properties, click the Ports tab, select the port that the second printer is on, and then clear the check box next to the original port.

To install a new replacement printer, click Add Port and then add the appropriate port for the second printer. If another print server hosts the printer, choose Local
Port and add the printer using the `\printserver\printersharename` format. (See “Installing Printers” earlier in this chapter for help.)

**Note** You cannot move the currently printing document when you move print jobs from one printer to another. To move the first print job, you must restart it.

### Managing Printers from a Web Browser

If you have Internet Information Server (IIS) with Internet Printing support installed on the print server, you can manage printers from any browser, provided you have sufficient privileges. (Set the permissions on the Printers node of the Default Web Site in IIS, as described in Microsoft Knowledge Base Article 323428.)

**Security Alert** Do not install IIS and Internet Printing unless you have a strong need to manage printers using a Web browser—installing IIS exposes the server to additional security risks. Instead, use the Print Management Console, the Printers And Faxes folder, Remote Desktop, or command-line tools to manage a print server remotely. You can disable Internet printing support on Windows 2000 print servers using Group Policy—to do so, disable the Web-based Printing setting in the Computer Configuration, Administrative Templates, Printers folder of the appropriate Group Policy object. This policy setting does not apply to Windows Server 2003.

To manage a print server using a Web browser from a computer running Windows Server 2003, Windows XP, Windows 2000, or Windows 9x with the Internet Print Services client (available on the Microsoft Web site at [http://www.microsoft.com/windows98/downloads/contents/WUPreviews/IPP/Default.asp](http://www.microsoft.com/windows98/downloads/contents/WUPreviews/IPP/Default.asp)), type the URL of the print server followed by `/printers` in the browser’s Address window. Then use the following list:

- To display the printer’s queue, click the printer you want to manage.
- To pause, resume, or cancel the printing of all documents in the print queue, click a hyperlink under the Printer Actions heading.
- To pause or cancel a specific print job, select the option button to the left of the document, and then click the Pause hyperlink or the Cancel hyperlink under the Document Actions heading.
- To view the properties for the printer, click the Properties hyperlink under the View heading. Note that you can use a Web browser only to view properties, not to change them.
Connecting to a Print Server Using a Web Browser

You can connect to a printer share on a Windows print server with Internet Printing support using Microsoft Internet Explorer 4.01 or later. To do so, browse to the printer and click the Connect hyperlink. If the printer share is in a Medium-High or Medium security zone, the client downloads the appropriate printer drivers and connects to the printer using Internet Printing Protocol (IPP). If the printer share is in a Medium-Low security zone, the client connects to the printer using RPC, which is faster than IPP. The best way to ensure that the client connects to the printer using RPC is to add the printer share to the Trusted Sites zone in Internet Explorer (configurable using the Internet Options tool in Control Panel).

Managing Printers from a Command Line

Windows Server 2003 makes command-line administration practical for Windows administrators. You can now perform almost any administration task from a command line—printers included. Hallelujah! Use the following list of commands and scripts to get started.

- **Print**  Prints the specified text file to the specified printer.
- **Lpr**  Prints the specified text file to the specified LPD print queue.
- **Net print**  Displays information about the specified print queue or print job. Can also hold, release, or delete print jobs.
- **Lpq**  Displays information about the specified LPD print queue.
- **Net start**  Starts the specified service. You can use the **Net start spooler** and **Net stop spooler** commands to start or stop the spooler service.

More Info  To view a list of parameters, type the command followed by `/?` at a command prompt, or use the Windows Server 2003 Help and Support Center.

- **Cscript %WinDir%\System32\Prnmngr.vbs**  Adds, deletes, or lists printers on a Windows print server.
- **Cscript %WinDir%\System32\Prnjobs.vbs**  Lets you view and manage the print jobs of printer shares on a Windows print server.
- **Cscript %WinDir%\System32\Prncfg.vbs**  Allows you to view and change the settings of printers on a Windows print server.
- `Cscript %Windir%\System32\Prnqctl.vbs` Pauses or resumes printing, clears the print queue, or prints test pages.
- `Cscript %Windir%\System32\Prnport.vbs` Administers all things related to printer ports.
- `Cscript %Windir%\System32\Prndrvr.vbs` Adds, deletes, or lists printer drivers on a Windows print server.
- `Cscript %Windir%\System32\Pubprn.vbs` Publishes shared printers on computers running Windows NT 4.0 or Windows 98 to Active Directory.

**Note** You can administer printers and print servers from a command-line with the help of the Windows Management Instrumentation (WMI) API and the Windows Scripting Host. Together, these technologies provide you with the ability to administer Windows Server 2003 using the scripts Microsoft provides or with scripts that you write yourself. This section does not go into depth about how to use the Windows Scripting Host and WMI—for help with that, see Chapter 13 or the Microsoft Script Center at http://www.microsoft.com/technet/scriptcenter.

---

**Changing Printer Options**

There are myriad printer options that you can configure; some of the most relevant options for an administrator are the security options, availability and group priority settings, separator pages, and print spooler settings.

**Setting Security Options**

Security can be an important factor to consider with printing. For example, you might not want everyone to print to the five-dollar-a-page dye sublimation printer purchased for the art staff. At a more basic level, you probably do not want most users to modify printer properties or change the priorities of documents in the print queue.

Setting permissions on a print queue is no different from setting permissions on a folder. To set permissions on a printer, right-click the printer, choose Properties, and then use the Security tab to assign permissions to groups of users. Click Advanced to exert finer control over permissions or to enable auditing. You can view the results of the audit settings in the security log.

There are three levels of control permissions for a printer: Print, Manage Documents, and Manage Printers:

- **Print** Users or groups with Print permission can connect to the printer, print documents, and pause, restart, or delete their own documents from the print queue. Windows by default grants members of the Everyone group the Print permission (which in Windows Server 2003 does not include Anonymous Logon).
Manage Documents  Users or groups with Manage Documents permission have the Print permissions along with the ability to change the settings for all documents in the print queue and to pause, restart, and delete any user’s documents from the print queue. Windows grants the Creator/Owner group the Manage Documents permission level by default.

Manage Printers  Users or groups with Manage Printers permission have the Manage Documents and Print permissions along with the ability to modify printer properties, delete printers, change printer permissions, and take ownership of printers. The Manage Printers permission level is the equivalent of Full Control permission in Windows NT. Windows grants this permission level to print operators, server operators, and administrators by default.

Changing Printer Availability and Group Priorities

You can set up a printer in a way that the print jobs submitted by some users or groups print before print jobs submitted by other groups; for example, you can give priority to managers or groups with tight deadlines. You can also reserve a printer for exclusive use by certain groups during certain times; for example, you can reserve a printer outside of normal business hours so that the groups you specify can print large, high-priority print jobs.

To control availability or group priority, create two or more logical printers for a single physical printer, give each logical printer a different priority and/or make it available at different times, and give different sets of users or groups permission to print to each logical printer.

To perform this procedure, use the following steps:

1. Create two or more logical printers for the physical printer by using the Add Printer Wizard to install the printer multiple times on the same port.

   Give each printer a descriptive name that describes the printer’s purpose or who is allowed to print to it. For example, LaserPrinter1_OvernightJobs or LaserPrinter1_Executives.

2. In the Print Management Console or the Printers And Faxes folder, right-click the first logical printer for the physical printer you want to control, select Properties, and then click the Advanced tab.

3. Click the Security tab, and assign permissions only to the groups to which you want to give special priority or allow to print during the times you specify.

4. Click the Advanced tab, shown in Figure 8-10.
5. To make the logical printer available only during specific hours, select the Available From option and then select the earliest and latest times the printer is to be available to users.

6. To change the priority of the users and groups that use this logical printer, type a number in the Priority text box. The priority range goes from 1, which is the lowest priority, to 99, which is the highest priority.

7. Click OK, and repeat the process for all other logical printers you created for the printer.

Specifying a Separator Page

Use a separator page with busy printers to help prevent one user from picking up the next user’s print job in addition to their own. Windows Server 2003 comes with four default separator pages located in the `%systemroot%\System32` folder:

- **Pcl.sep** Switches the printer to Printer Control Language (PCL) and then prints a separator page.
- **Pscript.sep** Switches the printer to PostScript and does not print a separator page.
- **Sysprint.sep** Switches the printer to PostScript and then prints a separator page.
- **Sysprintj.sep** Switches the printer to PostScript with Japanese character support and then prints a separator page.
If your printer does not support these languages, create a custom separator page, as discussed in the “Custom Separator Pages” sidebar. To specify a separator page, use the following steps:

1. In the Print Management Console or the Printers And Faxes folder, right-click the printer you want to modify and select Properties.
2. Click the Advanced tab.
3. Click Separator Page to select a page to insert between printed documents to help separate the print jobs.

### Real World Custom Separator Pages

To create a custom separator page, create a text file in Notepad or any text editor, save it with the .sep file extension, and then create your separator page. On the first line, type the escape character you want to use (for example “\”), and then the text that you want to appear on the separator page. (See Table 8-1 for a listing of commands you can use on a separator page.) Following is an example of a simple print separator page that prints the user name, job number, date, and time of the print job, using the “\” character as the escape character:

```plaintext
\ \U\LUser Name: \N
\U\LJob : \I
\U\LDate: \D
\U\LTime: \T
\E
```

### Table 8-1 Separator page commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>Escape character used by the separator file interpreter to delimit commands. Can be any character, but this table uses “\” as an example.</td>
</tr>
<tr>
<td>\Hn</td>
<td>Sends the n control sequence to the printer. See your printer manual for the correct control sequence to use with your printer.</td>
</tr>
<tr>
<td>\Wn</td>
<td>Specifies the width of the separator page, beyond which Windows omits all characters. The default width is 80, and the maximum width is 256.</td>
</tr>
<tr>
<td>\n</td>
<td>Skips the number of lines you specify by n. Valid numbers are 0 through 9, with 0 acting as a carriage return, moving printing to the next line.</td>
</tr>
<tr>
<td>\Fpathname</td>
<td>Prints the contents of file specified by pathname directly to the printer. The file must be rendered in the appropriate language for the printer.</td>
</tr>
<tr>
<td>\L</td>
<td>Prints all characters following the \L command until the next escape character.</td>
</tr>
</tbody>
</table>
Changing Spool Settings

Print spooling, or storing a print job on disk before printing, affects how clients perceive printing performance and the actual printing speed. You can change the way print spooling works to correct printing problems or to hold printed documents in the printer queue in case a user needs to print the document again.

To change the spool settings for a printer, right-click the printer you want to modify, select Properties, and then use the following settings on the Advanced tab to modify the spool settings:

- **Spool Print Documents So Program Finishes Printing Faster**  
  Spools the print documents to the print server, freeing the client to perform other tasks more quickly.
  
  - To reduce the time it takes to print a document, select Start Printing Immediately.
  
  - To ensure that the entire document is available to the printer when printing begins, select Start Printing After Last Page Is Spooled. This step might correct some printing problems, and it helps high-priority documents print before low-priority documents.

- **Print Directly To The Printer**  
  Turns off spooling, causing a performance hit on the server (though it might fix some printing problems).

- **Hold Mismatched Documents**  
  Holds documents in the queue that do not match the current printer settings (for example, documents that require legal-size paper when letter paper is currently in the printer). Other documents in the print queue are unaffected by held documents.

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>\N</td>
<td>Prints the user name of the user that submitted the print job.</td>
</tr>
<tr>
<td>\I</td>
<td>Prints the print job number.</td>
</tr>
<tr>
<td>\D</td>
<td>Prints the date when the print job is printed, using the date format used by the print server.</td>
</tr>
<tr>
<td>\T</td>
<td>Prints the time when the print job is printed, using the time format used by the print server.</td>
</tr>
<tr>
<td>\U</td>
<td>Disables block printing of characters in the separator file until explicitly enabled.</td>
</tr>
<tr>
<td>\B\S</td>
<td>Prints characters in single-width block text until the separator file interpreter encounters a \U command.</td>
</tr>
<tr>
<td>\B\M</td>
<td>Prints characters in double-width block text until the separator file interpreter encounters a \U command.</td>
</tr>
<tr>
<td>\E</td>
<td>Ejects the current page.</td>
</tr>
</tbody>
</table>
Chapter 8  Installing and Managing Printers  213

- **Print Spooled Documents First**  Prints the highest priority document that is already spooled first, ahead of higher priority documents that are still spooling. This step speeds overall printer throughput by preventing the printer from waiting for documents to spool.

- **Keep Printed Documents**  Keeps a copy of print jobs in the printer queue in case users need to print the document again. In this circumstance, the user can resubmit the document directly from the queue rather than printing from his or her application a second time.

  **Note**  For optimal performance, place the spool folder for the print server on a separate drive from Windows, its applications, and especially its swap file. Also, make sure the drive is big enough to hold all the documents in the print queue. (If you choose to hold printed documents, use a large drive or disk array and use the File Server Resource Manager to create a quota for the print queue that notifies you if the print queue grows too large.) To change the spool settings for the print server, right-click the server in the Print Management Console and choose Server Properties, or open the Printers And Faxes folder, choose Server Properties from the File menu, and then click the Advanced tab.

**Under the Hood  Printer Data Types**

After a print job reaches the beginning of the print queue, the local print provider polls the print processor to determine whether the print job is in the correct data type for the printer. If the print job is in the incorrect format, the print processor needs to convert it. The data type that Windows uses to represent a print job is important not only because the data type must match a data type supported by the printer, but also because of performance considerations. Therefore, you need to understand the differences between the two main data types supported by the default Windows print processor. (Third-party print processors occasionally—but not often—supply additional data types.)

The most commonly used printer data type supported by Windows is *enhanced metafile* (EMF). This is the default data type for Windows XP, Windows 2000, or Windows NT clients printing to logical printers that use the PCL page description language. The EMF data type is a metafile format that allows better portability, smaller print jobs, and faster client print performance. EMF files generally consume less network bandwidth, but they do require more processing on the print server than do raw print jobs.

The second most commonly used data type is the *raw* data type (which is different from the raw protocol used by a standard TCP/IP printer port), which is the default
data type for PostScript printers and all clients running Windows 9x. Client computers perform all processing of raw print jobs, which reduces client print performance but does consume less resources on the server.

The Windows XP (and Windows 2000) print processor (Winprint) supports three other data types, which Windows uses infrequently. The data types are raw (FF appended), raw (FF auto), and text. Raw (FF appended) appends a form-feed character to the print job, which is required by some applications that otherwise do not print the last page when using the raw data type with PCL printers. The raw (FF auto) data type automatically checks for the presence of a trailing form-feed character and adds one if necessary. The text data type encodes the entire print job as plain American National Standards Institute (ANSI) text, and then adds any additional print specification using the printer’s factory default settings. This data type is useful for printers that do not operate properly with other data types.

To change the print processor or data types, click Print Processor on the Advanced tab of the printer’s Properties dialog box. To set up a printer that supports multiple printer languages (usually PostScript and PCL), create two logical printers for the printer, one for each data type. Users with PostScript documents can use the PostScript-enabled logical printer, whereas users with PCL documents can use the PCL logical printer.

Managing Printer Drivers

When you install a printer, Windows installs the Windows Server 2000, Windows XP, and Windows Server 2003 version of the driver that corresponds to the processor architecture used by the server (x86, x64, or Itanium). To use the printer from a client computer that runs an older version of Windows or uses a different processor architecture than the server, you must install additional drivers. For example, if the server is running a 32-bit version of Windows but the client computer is running Windows XP Professional x64 Edition, you must install x64 drivers on the server for all printers to which you want the client computer to be able to print.

You might also need to remove or reinstall problematic drivers, or set up a printer pool where two or more printers act as one printer to improve speed and availability.

Under the Hood 64-Bit and 32-Bit Driver Support

Windows Server 2003, Windows XP, and Windows 2000 can use only drivers written specifically for the processor architecture of the computer on which Windows is installed. For example:

- You cannot use a 64-bit x64 driver on a 32-bit edition of Windows.
You cannot use a 32-bit driver on a 64-bit edition of Windows.

You cannot use an x64 driver on an Itanium-based system, and vice-versa.

You can (and should!) add printer drivers for different architectures to a print server because the print server merely distributes the drivers—it does not use them itself.

Managing Printer Drivers

To install printer drivers that Windows automatically downloads onto a client machine when a user connects to the printer, follow these steps:

1. In the Print Management Console, right-click the Drivers folder on the appropriate print server and choose Manage Drivers. Or open the Printers And Faxes folder, choose Server Properties from the File menu and then click the Drivers tab of the Print Server Properties dialog box.

2. Use the Drivers tab of the Print Server Properties dialog box to manage drivers:
   - To install drivers, click Add and then use the Add Printer Driver Wizard to install drivers for the appropriate operating system and processor architecture.
   - To remove an obsolete or problematic driver, select it and click Remove.
   - To reinstall a driver, select it and click Reinstall.
   - To view the details of a printer driver, select the driver and click Properties.

Note When installing new drivers for multiple operating system versions and/or processor architectures, use drivers that are designed to work together so that printer settings you specify on the print server can be applied to client computers when they connect to the printers. Some printer manufacturers provide multiple-platform driver packages just for this purpose.

Under the Hood Windows Automatically Checks for New Drivers

Windows automatically downloads printer drivers when it connects to a Windows printer share. Windows XP, Windows 2000, and Windows NT 4 clients automatically check for updated versions of the printer drivers at startup and download newer versions from the print server, if present. Microsoft Windows 95, Windows 98, and Windows Me clients do not automatically check for updated drivers—you must update them manually.
Creating Printer Pools and Changing Port Settings

A printer pool is useful for handling a large volume of printing at a single location, particularly when there is a mix of large and small documents. For example, someone with a single-page memo probably does not want to be stuck in the queue behind a print job that is the corporate equivalent of the *Encyclopedia Britannica*.

If multiple printers share a single driver, you can add them to a printer pool, which appears to users as one printer. The advantage of using a printer pool is that clients simply print to the single logical printer on the print server, which then sends the print job to the first available printer. If one printer in a printer pool goes offline, Windows sends the print jobs to the other printers in the printer pool, eliminating downtime for users. Printer pools also simplify administration because you manage all printers in a printer pool with one logical printer; if you modify the properties for the single logical printer, all physical printers in the printer pool use the same settings.

**Note** Locate printers in a printer pool near each other to make finding a completed print job easier.

To set up a printer pool or change the port settings for a printer, follow these steps:

1. In the Print Management Console or the Printers And Faxes folder, right-click the logical printer on which you want to enable printer pooling, and choose Properties.
2. Click the Ports tab.
3. Select the Enable Printer Pooling check box.
4. To add an additional printer to the printer pool, select the port to which the printer is connected.
   
   If the printer is a network printer and you have not yet added it to the print server, click Add Port to add a new Standard TCP/IP printer port for the printer. (See the “Installing Printers” section of this chapter for more information.)
5. To change the transmission retry settings for a port, select the port and click Configure Port.

**Important** All printers in a printer pool must be able to use the same printer driver—if you add an incompatible printer to a printer pool, documents might print incorrectly.
Printer Maintenance and Troubleshooting

This section discusses how to perform two common print server maintenance tasks—optimize a print server and prepare for a print server failure—as well as how to troubleshoot common printer problems.

The goal in troubleshooting printing problems, as in troubleshooting any type of problem, is first to isolate and identify the problem and then to determine a course of action to fix it. This section helps you diagnose your printer problems and locate the printing subsystem where the error is occurring, and it gives you specific tips for solving your problems.

Printing problems usually fall into the following categories:

- **Physical problems** Including problems with the printer and the transmission media.
- **Print server problems** Including problems with printer drivers, permissions levels, and software status.
- **Network connectivity problems** Including not being able to communicate between the server and the clients because of incorrect protocols, network settings, or hardware failures. (You can troubleshoot these problems on either the client or the server, depending on where the connectivity problem exists.)
- **Client problems** Including problems with printer drivers, permissions, and applications.

Try to determine which category the problem is in before getting into details. A process of elimination usually works. Start by printing from a couple of client machines. If only one does not work, you narrowed the problem down to that client machine; if all clients fail, try printing from the print server. If this succeeds, you know that the problem lies either in the print server configuration or in network connectivity. Keep trying alternatives until you isolate the problem as precisely as possible, and then apply the most common fixes until you solve the problem.

If you already know where the problem is, jump straight to the heading in this section that applies and continue.

**More Info** If you cannot resolve the problems by using the information provided here, use the Microsoft Knowledge Base on the Microsoft Web site at [http://support.microsoft.com](http://support.microsoft.com).
Optimizing Print Server Performance

For best performance, use a fast, dedicated drive or disk array just for the print spool folder, and do not place any system files—especially the swap file—on this drive. Windows Server 2003 gives file sharing a higher priority than printer sharing, so expect reduced print performance if you use the print server for both services. Also, place the print server on the same network segment as the users and printers.

To monitor the performance of print servers to determine whether they are performing optimally, launch the Performance snap-in from the Administrative Tools folder and add counters from the new Print Queue object under the Performance category.

Preparing for Print Server Failure

Many companies have a secondary print server in case the primary print server fails. When the primary print server fails, the administrator has three options:

- Send e-mail instructing users to choose ReserveServer2 (for example) for printing. This option is easiest for the administrator but, inevitably, some users have difficulty connecting to another printer. If you planned the print server downtime, you can use the Print Management Console to deploy printer connections to the backup server and remove connections to the offline server.

- If your network requires an extremely high level of print performance and reliability, set up a print server cluster. This provides additional capacity and automatic failover should one server stop responding. For information about clustering, see Chapter 19.

- Create an alias on a backup print server so that clients see the backup server instead of the primary server. The backup print server must connect to the same network printers as the primary print server and use the same share names. (Use Print Migrator to copy the configuration of the primary server to the backup server.)

To switch users to the backup server instead of the primary server, follow these steps:

1. Open Registry Editor (Regedit.exe) on the backup print server, and navigate to the following registry key:

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters

2. Create a new String Value named OptionalNames with the primary server name as the data.

3. Create a new DWORD Value named DisableStrictNameChecking with a value of 1.
Security Alert  The DisableStrictNameChecking registry value makes it possible for someone on the internal network to use the OptionalNames parameter to impersonate a computer, although name resolution would be unreliable unless they also “poisoned” the DNS and/or WINS server. Remove this registry value as soon as the primary print server is back online; otherwise, you push new printer connections to all clients and remove connections to the offline server.

4. Create a DNS Alias (CNAME) record mapping the primary server’s DNS name to the backup server’s DNS name.

5. If you are using WINS on the network, create a DHCP reservation for the backup print server so that its IP address does not change, and then create a new static mapping in WINS that maps the primary print server’s NetBIOS name to the backup print server’s IP address. See Chapter 17 for more information about administering WINS, DHCP, and DNS.

6. Restart the server.

7. To bring the primary print server back online, delete the new registry values, DNS alias, and WINS registration and then restart the server.

Note  If a printer fails on the print server but the server itself does not, you can easily move users to another printer that can use the same printer driver. (Recent printers in the same model line can often use the same driver.) To do so, right-click the printer, choose Properties, click Ports, and then select the port of the printer to which you want to redirect users of the failed printer. This port can be a local port, network port, or printer share on another print server. You can also create a printer pool to automate the failover of one printer to another that uses the same driver.

Printing from the Client Machine Experiencing the Problem

Print from the client machine, and observe any error messages that appear. These messages often uncover the cause of the problem or at least indicate some possibilities. If the document prints properly, you probably have a user error, in which case you might need to educate the users as to the proper printing procedure. Otherwise, you might have a problem with a particular program, or there might be a compatibility problem with the printer driver.

Note  Many administrators use this step later in their troubleshooting process to minimize the number of times they need to visit client systems. To understand whether the problem affects only the client or clients reporting the problem or whether it is generalized, check the print server or print from another client computer such as your own computer.
Under the Hood  What Happens When You Print a Document

When a Windows XP or Windows 2000 client prints a document, the following sequence of events occurs, as illustrated by Figure 8-11:

1. The application calls the Windows Graphical Device Interface (GDI), which calls the locally installed printer driver for the remote print device.

2. The GDI and the printer driver cooperate to render the document in the printer language of the printer.

3. Windows sends the rendered document with enhanced metafile (EMF) data type, to the client side of the spooler (Winspool.drv).

4. Winspool.drv then makes a remote procedure call (RPC) connection with the Windows print server’s spooler service (Spoolsrv.exe).

5. The print server’s spooler service makes an application programming interface (API) call to the print server’s print router (Spools.dll).

6. The print router communicates with the client’s remote print provider (Win32spl.dll), which then establishes an RPC connection directly with the print server’s spooler service and sends the print job over the network.

7. The document is saved in the print queue as an .SPL (spool) file by the local print provider.

8. When the print job reaches the front of the queue, the local print provider on the print server polls the print processor to determine whether it needs to convert the print job to a different data type before printing.

9. The print job moves to the Separator Page Processor (SPP) for the insertion of a separator page, if required.

10. Windows despoils the job to the language monitor and, from there, through the appropriate printer port (most likely a standard TCP/IP port) to the printer itself.

11. The printer receives the print job either in its entirety or gradually as the print monitor feeds the printer at the appropriate rate to keep the printer’s buffers full. The printer converts each page to a bitmap format and then prints the document.
Figure 8-11 Interaction of Windows XP with various services to print a document
Document Prints Incorrectly
When a document prints but appears garbled or has some other defect, a compatibility problem exists between the client, printer driver, and printer. Make sure that the client is using the proper client printer driver and that the server is using the proper printer driver. If the client is using an x64 edition of Windows, obtain a native x64 version of the printer driver for the specific printer model you are using instead of using a printer driver written for a similar model.

You might want to try installing a duplicate logical printer to test whether the printer driver is corrupt. If this is not the problem, try changing the spool settings on the client driver. If multiple clients experience the same problem, change the server’s printer driver. Specifically, try changing the following options on the Advanced tab of the printer’s Properties dialog box. (See “Changing Spool Settings” earlier in this chapter for a more detailed procedure.)

- To ensure that the entire document is available to the printer when printing begins, select the Start Printing After Last Page Is Spooled option.
- If you continue to have printing problems, choose the Print Directly To The Printer option to turn off spooling. This action causes a performance reduction on the server.
- Clear the Enable Advanced Printing Features check box on the print server to turn off metafile spooling, which disables some printer options such as page order, booklet printing, and pages per sheet (if available on the printer).

Note If the printer has multiple trays with different forms, match the form to the tray so that documents using the form always print properly. Under the Form To Tray Assignment heading, select each tray and choose the form that the tray holds. If the printer supports Page Protection and has 1 MB or more of available optional memory, click the Device Settings tab and turn on this option to ensure that complex pages print properly. When you turn this option on, the printer creates each page in memory before beginning to print.

Document Fails to Print
If the document does not print at all, perform the troubleshooting tasks described in the following list:

- If you receive an error stating that the appropriate printer driver is not available for download, install the printer drivers on the print server that correspond to the client computer’s operating system and processor architecture. (See the “Managing Printer Drivers” section of this chapter for more information.)
■ If you receive an error stating that the print device was unavailable, you might have a network connectivity problem, or the user might not have Print permissions on the printer. (See the “Setting Security Options” section of this chapter for more information.)

■ If you experience a lot of disk access and the document fails to print, verify that the drive holding the client’s spool folder contains enough free disk space to hold the spooled document. (See the “Changing Spool Settings” section of this chapter for more information.)

■ Determine whether you can see and connect to the print server across the network. Try copying a file to the print server to see whether you can access the print server. (Generally, if you cannot access the print server, you cannot access any attached printers.)

■ Print a test document from Microsoft Notepad. If you can print with Notepad, the printer drivers are correct and the application is likely the problem.

■ If you cannot print with Notepad, you can also try printing from the command line by typing the following command: `echo test > [printer port name]`, using the share name of the network printer as the `printer port name`.

Printing from Some Applications Fails

Some applications experience problems when printing in Windows. Some of the issues you might encounter are listed here:

■ **Printing from Microsoft Outlook on a system with multiple languages is slow**  
  This occurs if languages are installed on the client that are not available on the server. To remedy this, copy the fonts to the `%SystemRoot%\Fonts` folder on the print server, and open the Fonts folder (or restart the server).

■ **“Access denied” error message occurs when configuring a printer inside an application**  
  This occurs when you do not have sufficient privileges to change the printer’s configuration. To change advanced printer settings, you need to have Manage Printers permissions.

■ **“Out-of-memory” error message occurs on application load on Windows 3.x client**  
  This can occur if the user has not selected a default printer. Install a printer, and set it as the default printer.

■ **MS-DOS program does not print**  
  Try quitting the program—some MS-DOS programs do not print until you close them. Also, use the `net use` command to map a local port to the shared printer. (For more information, see Microsoft Knowledge Base Article 314499 on the Microsoft Web site at [http://support.microsoft.com/kb/314499](http://support.microsoft.com/kb/314499).)
More Info  For other issues, consult the Printers.txt file on the installation CD-ROM for the client operating system if the system is Windows XP, Windows 2000, Windows NT 4, Windows 95, or Windows 98. You might also want to check the Microsoft Knowledge Base at http://support.microsoft.com.

Checking the Print Server Status

Administrators often check the print server status before actually going to the client machine because they can do it remotely. Use the following list to check the print server status:

■ Check for stalled documents or error messages in the print queue or on the printer configuration Web page (if present). If the printer is out of paper or toner or if there is a paper jam, an error message frequently appears here.

■ Check that sufficient free disk space exists on the drive holding the spool folder.

■ If documents print garbled, the printer might be using the wrong data type (EMF or raw). Try using the raw data type to see whether this corrects the problem. You might also want to clear the Enable Advanced Printing Features check box in the Advanced tab of the printer’s Properties dialog box. (See the “Changing Spool Settings” section earlier in this chapter for more information.)

■ Check to see whether any documents are printing. If no documents exist in the print queue to observe, print a test page or document from the print server to verify that the print server is printing properly.

■ If some documents in the print queue do not print and you cannot delete them, the print spooler might be stalled. Restart the Print Spooler service to see whether this corrects the problem. You might also want to add another logical printer (printer driver) for the printer to try to rule out the possibility of a corrupt printer driver.

Note  To prevent documents with certain languages from printing slowly, install on the print servers the fonts for all languages that the clients will use to print. To do this, copy the fonts to the %SystemRoot%\Fonts folder on the print server and open the Fonts folder (or reboot the server).

Checking the Printer

If you ruled out the clients and the server as the source of the problem but you still cannot print any documents on the printer, take a close look at the printer. Pause the print queue, and then go check the actual printer. Are any errors reported on the printer? If you
find any paper jams or if the printer is low on toner or needs servicing, the printer usually reports an error message. Make sure that the ready or online light is illuminated and that the printer cable is securely attached, or that the network cable is properly plugged in and the light next to the network port is illuminated (if available).

If you still cannot print to the printer, attempt to print a test page directly from the printer. Most printers support this capability. If this works, try configuring a different print server with the printer. If you can print from a different print server, you have a problem with the original print server. If this does not work, use the ping.exe program to see if you can access the printer’s IP address.

**Deleting Stuck Documents**

If you cannot delete documents in the print queue or if documents do not print, the print spooler might be stalled. This also affects any fax services the server is running. To restart the Print Spooler service, follow these steps:

1. Launch the Services snap-in from the Administrative Tools folder.

2. Select the Print Spooler service in the right pane, and then click the Restart Service toolbar button.

3. To specify a recovery process to perform if the Print Spooler service fails, click the Recovery tab, and then specify whether you want to restart the service, restart the computer, or run a program after each print spooler failure.

   Restarting the service is usually a good option—it saves time. Automatically restarting the computer is a last option because of other processes that might be interrupted or stopped by a restart.

4. To view the services (such as remote procedure call) on which the print spooler depends, double-click the Print Spooler service and then click the Dependencies tab. You can also use this tab to view the services that depend on the print spooler to function properly.

   **Note** To restart the print spooler from a command prompt, type `net stop "print spooler"` and then `net start "print spooler"`.

**Troubleshooting Printer Location Tracking**

Printer location tracking can have its own set of problems, although these are usually related to the way your printers and network are set up.
Clients Cannot Locate Some Printers in Active Directory
This problem usually occurs when you do not name a printer according to the printer location name conventions the company decided to implement. When you have printer location tracking enabled, clients by default can locate only printers with location attributes that match the naming convention. To fix the problem, type the correct location name in the missing printer’s Location field.

Naming Scheme Needs to Be Changed
If the company changes its organizational structure or if you find that the current location-naming scheme needs to be changed, use Active Directory Sites and Services to update the sites and subnet names and then type the new location names in the Location field of each printer that is affected by the location name restructuring. You can also do this with an Active Directory Services Interface (ADSI) script.

Summary
Almost all networks need comprehensive and reliable print services. You must plan how to meet present printing needs while also preparing for expansions and changes. Contingency plans are essential because even a brief disruption in printing is inconvenient and costly. The next chapter covers the day-to-day tasks that network administrators perform and how to customize the tools in Windows Server 2003 to make your work easier and more efficient.
The central task of a network is to provide the customers (the users) with everything they need and clear away the clutter that hampers their progress. What they need includes access to the files, folders, applications, printers, and Internet connections that they require to do their jobs. What they don’t need is any trouble getting at what they do need.

The network administrator has additional needs, including shielding need-to-know material from those who don’t need to know, protecting the network from malicious or otherwise dangerous users, and protecting the users from themselves. The key to meeting all these needs is the configuration of organizational units, groups, users, and Group Policies—the topic of this chapter and Chapter 11.

Understanding Groups

By definition, groups in the Microsoft Windows Server 2003 family are Active Directory directory service or local computer objects that can contain users, contacts, computers, or other groups. In general, though, a group is usually a collection of user accounts. The point of groups is to simplify administration by allowing the network administrator to assign rights and permissions to groups rather than individual users.
Windows Server 2003 allows two group types: security and distribution. Almost all groups used by Windows Server 2003 and Microsoft Windows 2000 Server are security groups because they’re the only groups through which permissions can be assigned. Each security group is also assigned a group scope, which defines how permissions are assigned to the group’s members. Programs that can search Active Directory can also use security groups for nonsecurity purposes, such as sending e-mail to a group of users. Distribution groups, on the other hand, are not security-enabled and can be used only with e-mail applications to send e-mail to sets of users.

Later in the chapter, you find sections on user rights and how they are defined and assigned to groups. Chapter 10 follows with a discussion on permissions and how they are assigned.

**Assigning Group Scopes**

When a group is created, it is assigned a group scope that in turn defines how permissions are assigned. The three possible group scopes—global, domain local, and universal—are defined in the following sections.

**Global Scope**

A group with a global scope is truly global in the sense that permissions can be granted for resources located in any domain. However, members can come only from the domain in which the group is created, and in that sense it is not global. Global groups are best used for directory objects that require frequent maintenance, such as user and computer accounts. Global groups can be members of universal and domain local groups in any domain, and they can have the following members:

- Other global groups in the same domain
- Individual accounts from the same domain

**Domain Local Scope**

A domain local group is the inverse of a global group in that members can come from any domain but the permissions can only be assigned for resources in the domain in which the group is created. The members of a domain local group have a common need to access certain resources in a particular domain. Domain local groups can have one or more of the following members:

- Other domain local groups in the same domain
- Global groups from any domain
- Universal groups from any domain
- Individual accounts from any domain
Note  The nesting rules apply fully only in domains with a Windows 2000 native or higher domain functional level—that is, when all the controllers in the domain are servers running at least Microsoft Windows 2000 or Windows Server 2003. In domains with a Windows 2000 mixed domain functional level, security groups with global scope can contain only individual accounts, not other groups. Security groups with domain local scope can contain both global groups and accounts. For more about domain functional levels, see Chapter 6.

Universal Scope
A universal security group can have members from any domain and can be assigned permissions to resources in any domain. Although the universal scope sounds like an ideal solution in a multiple-domain enterprise, it’s available only in domains that are running in Windows 2000 native domain functional level and higher. Universal groups can have the following members, which can be drawn from any domain:

- Other universal groups
- Global groups
- Individual accounts

Even in a Windows 2000 native or higher domain functional level, universal groups must be used with discretion because of the negative impact they can have on network performance, as described in the Real World sidebar, “How Groups Affect Network Performance.”

Real World  How Groups Affect Network Performance
The importance of planning groups becomes even more apparent when you consider the negative effect your group organization can have on network performance. When a user logs on to the network, the domain controller determines the user’s group memberships and assigns a security token to the user. The token includes the security identifiers (SIDs) of all the groups that the user belongs to, in addition to the user account ID. The more security groups the user belongs to, the longer it takes to assemble the token and the longer it takes the user to log on.

In addition, the security token, once assembled, is sent to every computer the user accesses. The target computer compares all the SIDs in the token against the permissions for all the shared resources available at that computer. A large number of users added to a large number of shared resources (including individual folders) can take up a lot of bandwidth and processing time. One solution is to limit membership in security groups. Use distribution groups for categories of users that don’t require specific permissions or rights.
Groups with universal scope have a performance impact of their own because all such groups, along with their members, are listed in the global catalog. When there’s a change to the membership in a group with universal scope, this fact must be relayed to every global catalog server in the domain tree, adding to the replication traffic on the network. New to Windows Server 2003 is the ability to enable universal group caching for remote domain controllers. This improves logon performance and limits replication traffic when changes are made to universal group membership on a remote domain controller. Groups with global or domain local scope are also listed in the global catalog, but their individual members are not, so the solution is to limit the membership of universal groups primarily to global groups.

### Planning Organizational Units

Organizational units (OUs) are, as their name implies, organizing tools for collections of objects within a domain. An OU can contain any collection of Active Directory objects such as printers, computers, groups, and so forth.

In the past, a domain that got very complicated was usually sorted out by splitting the domain into multiple domains. OUs provide an alternative administrative substructure that is infinitely more flexible. They can be arranged hierarchically within a domain, and administrative control can be delegated for functions in a single OU or an entire subtree of OUs. (An OU is the smallest entity over which you can delegate administrative control.) At the same time, OUs can be modified, moved, renamed, and even deleted easily. Another plus is that, unlike a domain, a subtree of OUs doesn’t require a separate domain controller.

#### Real World  Organizational Units or New Domain?

Unfortunately, there’s no firm rule you can apply to decide when an expanding network should be divided into separate domains and when new OUs are called for. If any of the following applies, multiple domains might be the answer:

- Decentralized administration is needed.
- The network encompasses competing business units or joint ventures.
- Parts of the network are separated by very slow links (analog modems, for example), so complete replication would create severe traffic problems. (If the link is merely slow, you can use multiple sites within a single domain because replication is less frequent.)
- Different account policies are needed. Because account policies are applied at the domain level, greatly differing policies might call for separate domains.
The following list describes situations that call for the use of OUs:

- Localized and/or tightly controlled administration is needed.
- The structure of the organization requires the arrangement of network objects into separate containers.
- The structure that you want to separate is likely to change at some point.

So, in general, when the situation calls for a flexible, even fluid structure, OUs are the answer.

OUs are containers only. They don’t confer membership and aren’t security principals. Rights and permissions are granted to users through group membership. After your groups are constructed, use OUs or organize group objects and assign Group Policy settings. The use of Group Policy is covered in Chapter 11.

**Creating Organizational Units**

OUs are easily created and appear as folders in a domain structure. The following steps describe how to create an OU:

1. Choose Active Directory Users And Computers from the Administrative Tools menu.
2. Right-click the domain, and select New and then Organizational Unit to open the dialog box shown in Figure 9-1.
3. In the Organizational Unit dialog box, type the name for the unit and then click OK.
Moving Organizational Units

One of the most useful aspects of OUs is that they can be moved from one container or even one domain to another. The following steps describe how to move an OU:

1. Choose Active Directory Users And Computers from the Administrative Tools menu.
2. Right-click the OU to be moved, and select Move from the shortcut menu.
3. In the Move dialog box, select the new location for the OU and click OK.

**Important** Moving OUs is easy in Windows Server 2003, but moving OUs that have Group Policy Objects linked to them can have unexpected results. Carefully consider the consequences of an OU move to the overall design of your Group Policy and verify the final behavior after the move.

Deleting Organizational Units

OUs can also be deleted easily. However, exercise caution when deleting an OU because the contents of the OU are also removed. That means you can inadvertently delete all the resources and user accounts contained in an OU if you act too hastily. The following steps describe how to delete an OU:

1. Choose Active Directory Users And Computers from the Administrative Tools menu.
2. Right-click the OU, and select Delete.
3. Confirm the deletion by clicking Yes twice.

Planning a Group Strategy

Looking at your network and the various group types, and then factoring in your specific needs, you can end up feeling as though you’re working on some infernal logic puzzle: Claire lives in a blue house, Luisa collects stamps, Sam drives a Toyota, and Ross eats cheese. Which one has red hair?

Nevertheless, as in so many other aspects of network administration, planning is the essential step. The domain mode determines the types of groups available to you. A domain having Windows 2000 mixed domain functional level, for example, can’t support groups with universal scope. Thus, as long as you have Microsoft Windows NT backup domain controllers, you are limited to groups with global and domain local scopes.
Determining Group Names

In planning your groups, determine a naming scheme that is appropriate for your organization. Two factors have to be considered:

- **Group names must be instantly recognizable** Administrators searching Active Directory don’t have to guess at their meaning.

- **Comparable groups must have similar names** In other words, if you have a group for engineers in each domain, give all the groups parallel names, such as NorAmer Engineers, SoAmer Engineers, and Euro Engineers.

Using Global and Domain Local Groups

Develop a strategy for using the different groups. For example, users with common job responsibilities belong in a global group. Thus, add user accounts for all graphic artists to a global group called Graphic Artists. Other users with common needs are assigned to other global groups. Then you must identify resources to which users need access and create a domain local group for that resource. If, for example, you have several color printers and plotters that are used by specific departments, you can make a domain local group called Printers&Plotters.

Next, decide which global groups need access to the resources you identified. Continuing the example, you add the global group Graphic Artists to the domain local group Printers&Plotters, along with other global groups that need access to the printers and plotters. Permission to use the resources in Printers&Plotters is assigned to the Printers&Plotters domain local group.

Keep in mind that global groups can complicate administration in multiple-domain situations. Global groups from different domains must have their permissions set individually. Also, assigning users to domain local groups and granting permissions to the group does not give members access to resources outside the domain.

---

**Note** Remember that the nesting rules apply only in Windows 2000 native and higher domain functional level. In environments with Windows 2000 mixed domain functional level, security groups with global scope can contain only individual accounts, not other groups. Security groups with domain local scope can contain global groups and accounts.

Using Universal Groups

When you’re able to use universal groups (that is, when your domain is running in Windows 2000 native or higher domain functional level), keep the following guidelines in mind:

- Avoid adding individual accounts to universal groups, to keep replication traffic down.
Add global groups from multiple domains to universal groups to give members access to resources in more than one domain.

Universal groups can be members of domain local groups and other universal groups, but they can't be members of global groups.

Implementing the Group Strategy

After you plan your strategy and test it using a variety of scenarios, you're ready to begin putting the structure into place.

Creating Groups

Use Active Directory Users And Computers to create and delete groups. Create groups in the Users container or in an OU that you create for the purpose of containing groups. The following steps demonstrate how to create a group in the Quality Assurance OU:

1. Choose Active Directory Users And Computers from the Administrative Tools menu.
2. Expand the domain in which the group is to be created.
3. Right-click the Quality Assurance OU, point to New, and choose Group from the shortcut menu to open the dialog box shown in Figure 9-2.

4. Fill in the required information:
   - The group name must be unique in the domain.
The group name as it will be seen by pre-Windows 2000 operating systems is filled in automatically. (In Windows 2000 native and higher domain functional level, this field is Downlevel Name Of New Group, but it is still filled in automatically based on the name you provide as the group name.)

For Group Scope, click Domain Local, Global, or Universal.

For Group Type, click Security or Distribution.

5. Click OK when you're finished. The new group appears in the Quality Assurance OU. You might have to wait a few minutes for the group to be replicated to the global catalog before adding members.

---

**Note** Groups that are created directly in the Users container (the default behavior) can’t have Group Policies applied to them. By using OUs and managing your groups within them, you have much greater control over how Group Policy is applied.

### Deleting Groups

Don’t create groups you don’t need, and when groups are no longer necessary be sure to promptly delete them from the system. Unnecessary groups are a security risk because it is all too easy to unintentionally grant permissions where you shouldn’t.

Each group, like each user, has a unique security identifier (SID). The SID is used to identify the group and the permissions assigned to the group. When the group is deleted, the SID is deleted and not used again. If you delete a group and decide later to re-create it, you have to configure the users and permissions as if for a new group.

To delete a group, right-click its name in Active Directory Users and Computers and choose Delete from the shortcut menu. Deleting a group deletes only the group and the permissions associated with the group. It has no effect on the accounts of users who are members of the group.

### Adding Users to a Group

After you create a group, you need to add members to it. As was mentioned earlier in the chapter, groups can contain users, contacts, other groups, and computers. The following steps show how to add members to a group:

1. Choose Active Directory Users And Computers from the Administrative Tools menu.
2. In the console tree, click the container that includes the objects you want to add to the group.
3. Highlight the accounts you want to add. (You can use the Shift and Ctrl keys to select multiple accounts.)
4. Right-click the highlighted accounts, and select Add To A Group from the shortcut menu. This opens the Select Group dialog box. Click Look For and Look In to narrow the search.

5. Type the first few letters of the group name and click OK. All matches are displayed. Highlight the correct group name and click OK.

You can also approach adding users to a group from another angle by following these steps:

1. Right-click a group name, and select Properties.

2. Click the Members tab and then click Add. Make sure the Object Types and Locations fields are pointing to the positions you want.

3. Click Advanced, and then click Find Now. All the potential group members appear in the lower pane.

4. Highlight the accounts to be added and click OK.

---

**Note** A contact is an account without security permissions and is typically used to represent external users for the purpose of e-mail. You can't log on to the network as a contact.

---

**Changing the Group Scope**

Over time, you might find that you need to change the scope of a particular group. For example, you might need to change a global group to a universal group so that users from another domain can be part of the group. However, the types of changes that can be made to a group scope are quite limited, and you might need to delete the group and create a new one to get the configuration you need.

To change a group scope, right-click the group name in Active Directory Users And Computers and choose Properties from the shortcut menu. Make the necessary changes on the General tab, and click OK when you're finished. There are several rules for changing a group scope, as described here:

- In Windows 2000 mixed domain functional level, a security group cannot have universal scope.

- A global group can be changed to a universal group if the global group is not already a member of another global group.

- A domain local group can be changed to a universal group if the domain local group does not already contain another domain local group.

- A universal group can be converted to a global group, as long as no other universal groups are members.
Creating Local Groups

A local group is a collection of user accounts on a single computer. The user accounts must be local to the computer, and members of local groups can be assigned permissions for resources only on the computer where the local group was created.

Local groups can be created on any computer running Windows Server 2003 except a domain controller. In general, you don’t want to use local groups on a computer that’s part of a domain or, at least, you want to do so sparingly. Local groups don’t appear in Active Directory, so you must administer local groups separately on each computer. The following steps describe how to create a local group:

1. Right-click the My Computer icon on the desktop, and choose Manage from the shortcut menu.
2. In the console tree, expand System Tools and then Local Users And Groups.
3. Right-click the Groups folder, and select New Group from the shortcut menu.
4. In the New Group dialog box, type the group name. You can include a description if you want.
5. Click Add to add members to the group. (You can add members now or later.)
6. Click Create when you’re finished, and the new group is added to the list of groups in the details pane.

Managing Built-In Groups and User Rights

When you create an Active Directory domain with one or more Windows Server 2003 domain controllers, built-in groups are automatically created in both the Users and Built-In containers. Many of these groups also have built-in rights that are automatically assigned to members of the group.

Built-In Local Groups

Member servers and standalone servers running Windows 2000 Server (Service Pack 3 or later) and computers running Microsoft Windows 2000 Professional (Service Pack 3 or later) or Microsoft Windows XP Professional (Service Pack 1 or later) have built-in local groups that give rights to perform tasks on a single computer. Install Adminpak.msi from the Windows Server 2003 installation disk on these computers as needed. Table 9-1 shows the built-in local groups on a standalone server. Many are common to clients and servers alike, but some, where noted, are only on member servers and standalone servers.
<table>
<thead>
<tr>
<th>Local Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators</td>
<td>Members can perform all administrative tasks on the computer. The built-in Administrator account that’s created when the operating system is installed is a member of the group. When a server (not a domain controller) or a client running Windows XP Professional or Windows 2000 Professional joins a domain, the Domain Admins group (described in Table 9-3) is made part of this group.</td>
</tr>
<tr>
<td>Backup Operators</td>
<td>Members can log on to the computer, back up and restore the computer’s data, and shut down the computer. Members cannot change security settings but can override them for purposes of backup and restore. No default members.</td>
</tr>
<tr>
<td>DHCP Users (installed with DHCP Server service)</td>
<td>Members of this group can read DHCP information stored at a specific server for troubleshooting purposes. No default members.</td>
</tr>
<tr>
<td>DHCP Administrators (installed with DHCP Server service)</td>
<td>Members of this group can administer DHCP Server service but do not have access to other parts of the server. No default members.</td>
</tr>
<tr>
<td>Guests</td>
<td>Members can perform only tasks for which an administrator has granted rights. Members can use only resources for which an administrator has specifically granted permission. The guest account is a default member of this group.</td>
</tr>
<tr>
<td>HelpServicesGroup</td>
<td>No users are assigned to this group. The only member should be the account associated with support applications.</td>
</tr>
<tr>
<td>Network Configuration Operators</td>
<td>Members can change TCP/IP settings, and renew and release addresses. No default members.</td>
</tr>
<tr>
<td>Performance Monitor Users</td>
<td>Members can monitor performance counters on a specific server locally and remotely. No default members.</td>
</tr>
<tr>
<td>Performance Log Users</td>
<td>Members can administer performance logs, counters, and alerts on a specific server, locally or remotely. No default members.</td>
</tr>
<tr>
<td>Power User</td>
<td>Members can create and modify user accounts and install programs on the local computer but cannot view other users’ files. Members can create and delete local groups, and add or remove users from the groups they have created. Members can add or remove users from the Power Users, Users, and Guests groups. No default members.</td>
</tr>
<tr>
<td>Print Operators</td>
<td>Members can manage printers and print queues on a specific server. No default members.</td>
</tr>
<tr>
<td>Remote Desktop Users</td>
<td>Members are allowed to connect remotely. No default members.</td>
</tr>
</tbody>
</table>
Note If you don’t want members of the Domain Users group to have access to a particular workstation or member server, remove Domain Users from that computer’s local Users group. Similarly, if you don’t want the members of Domain Admins to administer a particular workstation or member server, remove Domain Admins from the local Administrators group.

Built-In Domain Local Groups

The Windows 2000 and Windows Server 2003 built-in domain local groups provide users with rights and permissions to perform tasks on domain controllers and in Active Directory. The domain local groups have predefined rights and permissions that are granted to users and global groups that you add as members. Table 9-2 shows the most commonly used built-in domain local groups.

Table 9-2 Commonly used built-in domain local groups

<table>
<thead>
<tr>
<th>Domain Local Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Operators</td>
<td>Members can create, delete, and manage user accounts and groups. Members cannot modify the Administrators, Domain Admins, and Domain Controllers groups, or any of the Operators groups. Members can log on locally to domain controllers and shut them down. No default members.</td>
</tr>
<tr>
<td>Administrators</td>
<td>Members are automatically granted every right and permission on all domain controllers and the domain itself. The Administrator account, Enterprise Admins group, and Domain Admins group are members.</td>
</tr>
<tr>
<td>Domain Local Group</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Backup Operators</td>
<td>Members can back up and restore data on all domain controllers, and they can log on to domain controllers and shut them down. There are no default members, and membership should be granted with care. This group is not the same as the Built-In Local Group Backup Operators.</td>
</tr>
<tr>
<td>Cert Publishers</td>
<td>Members can publish certificates for users and computers. No default members.</td>
</tr>
<tr>
<td>DnsAdmins (installed with DNS)</td>
<td>Members have administrative access to DNS servers. No default members.</td>
</tr>
<tr>
<td>Guests</td>
<td>Members can perform only tasks for which an administrator has granted rights. Members can use only resources for which an administrator has specifically granted permission. The Guest User and Domain Guests groups are members by default.</td>
</tr>
<tr>
<td>Incoming Forest Trust Builders</td>
<td>Members can allow an incoming forest trust to let users in another forest access resources in the home forest. No default members.</td>
</tr>
<tr>
<td>Network Configuration Operators</td>
<td>Members can change TCP/IP settings, and they can renew and release addresses on domain controllers. No default members.</td>
</tr>
<tr>
<td>Performance Monitor Users</td>
<td>Members can monitor performance counters on domain controllers either locally or from remote clients without being Administrators or members of the Performance Log Users group. No default members.</td>
</tr>
<tr>
<td>Performance Log Users</td>
<td>Members can manage performance logs, counters, and alerts on domain controllers either locally or remotely without being Administrators.</td>
</tr>
<tr>
<td>Pre–Windows 2000 Compatible Access</td>
<td>Provided for backward compatibility for computers running Windows NT 4. Add users to this group only if they are running Windows NT 4 or earlier. No default members.</td>
</tr>
<tr>
<td>Print Operators</td>
<td>Members can manage all aspects of domain printer operation and configuration.</td>
</tr>
<tr>
<td>RAS and IAS Servers</td>
<td>Servers in this group have access to the remote access properties of users. No default members.</td>
</tr>
<tr>
<td>Remote Desktop Users</td>
<td>Members can remotely log on to domain controllers. No default members.</td>
</tr>
<tr>
<td>Server Operators</td>
<td>Members can perform most administrative tasks on domain controllers, except the manipulation of security options.</td>
</tr>
<tr>
<td>Users</td>
<td>Members can log on to the computer, access the network, save documents, and shut down the computer. Members cannot install programs or make system changes. The Domain Users group is a member by default.</td>
</tr>
</tbody>
</table>
Security Alert  In Windows NT, all domain users are members of the Everyone group. This group is controlled by the operating system and appears on any network with Windows NT servers. In Windows 2000 Server and Windows Server 2003, the equivalent group is called Authenticated Users. Unlike Everyone, Authenticated Users contains no anonymous users or guests. The Everyone group survives as a special identity. You don’t see it when you administer groups, and it cannot be placed in a group. When a user logs on to the network, the user is automatically added to Everyone. You can’t see or change the membership of the special identities, which also include the Network and Interactive groups.

Built-In Global Groups

Built-in global groups are created to encompass common types of accounts. By default, these groups do not have inherent rights; an administrator must assign all rights to the group. However, some members are added to these groups automatically, and you can add more members based on the rights and permissions you assign to the groups. Rights can be assigned directly to the groups or by adding the built-in global groups to domain local groups. Table 9-3 describes the built-in global groups that are commonly used.

Table 9-3  Commonly used built-in global groups

<table>
<thead>
<tr>
<th>Global Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DnsUpdateProxy</td>
<td>Members are DNS clients that can provide dynamic updates to DNS on behalf of other clients. No default members.</td>
</tr>
<tr>
<td>Domain Admins</td>
<td>This group is automatically a member of the domain local Administrators group, so members of Domain Admins can perform administrative tasks on any computer in the domain. The Administrator account is a member of this group by default.</td>
</tr>
<tr>
<td>Domain Computers</td>
<td>All controllers and workstations in the domain are members.</td>
</tr>
<tr>
<td>Domain Controllers</td>
<td>All domain controllers in the domain are members.</td>
</tr>
<tr>
<td>Domain Guests</td>
<td>The Guest account is a member by default. This group is automatically a member of the domain local Guests group.</td>
</tr>
<tr>
<td>Domain Users</td>
<td>All domain users and the Administrator accounts are members. The Domain Users group is automatically a member of the domain local Users group.</td>
</tr>
<tr>
<td>Enterprise Admins</td>
<td>This group is for users who are to have administrative rights for the entire network. Enterprise Admins is automatically a member of the Administrators group on all domain controllers in the forest.</td>
</tr>
<tr>
<td>Group PolicyCreator Owners</td>
<td>Members can create and modify group policy for the domain. The Administrator account is a default member of the group.</td>
</tr>
<tr>
<td>Schema Admins</td>
<td>Members can alter the Active Directory Schema. (appears only in forest root domain)</td>
</tr>
</tbody>
</table>
Note If you have users with fewer rights and permissions than the typical user, add these users to Domain Guests and remove them from Domain Users.

Defining User Rights

What users can and cannot do depends on the rights and permissions that have been granted to them. Rights generally apply to the system as a whole. The ability to back up files or to log on to a server, for example, is a right that the administrator giveth or taketh away. Rights can be assigned individually, but most often they are characteristics of groups, and a user is assigned to a particular group on the basis of the rights that the user needs.

Permissions indicate the access that a user (or group) has to specific objects, such as files, directories, and printers. For example, the question of whether a user can read a particular directory or access a network printer is a permission. Permissions are discussed at length later in this chapter.

Rights, in turn, are divided into two types: privileges and logon rights. Privileges include such functions as the ability to run security audits or force shutdown from a remote system—obviously not tasks that are done by most users. Logon rights are self-explanatory; they involve the ability to connect to a computer in specific ways. Rights are automatically assigned to the built-in groups in Windows Server 2003, although they can be assigned to individual users as well as groups. Assignment by group is preferred, so whenever possible, assign rights by group membership to keep administration simple. When membership in groups defines rights, rights can be removed from a user by simply removing the user from the group. Tables 9-4 and 9-5 list the logon rights and privileges and the groups to which they are assigned by default.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Groups Assigned the Right on Domain Controllers</th>
<th>Groups Assigned the Right on Workstations and Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access this computer from the network</td>
<td>Permits connection to the computer through the network</td>
<td>Administrators, Authenticated Users, Everyone</td>
<td>Administrators, Backup Operators, Power Users, Users, Everyone</td>
</tr>
<tr>
<td>Allow logon locally</td>
<td>Permits logging on to the computer interactively</td>
<td>Administrators, Account Operators, Backup Operators, Print Operators, Server Operators</td>
<td>Administrators, Backup Operators, Power Users, Users, Guest</td>
</tr>
<tr>
<td>Allow logon through Terminal Services</td>
<td>Allows logging on as a Terminal Services client</td>
<td>Administrators</td>
<td>Administrators, Remote Desktop Users</td>
</tr>
</tbody>
</table>
Table 9-5 Privileges assigned to groups by default

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Groups Assigned the Privilege by Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Act as part of the operating system</td>
<td>Allows a process to authenticate as any user. A process that requires this privilege must use the LocalSystem account, which already includes this privilege.</td>
<td>None</td>
</tr>
<tr>
<td>Add workstations to domain</td>
<td>Allows a user to add new workstations to an existing domain.</td>
<td>Authenticated Users on domain controllers</td>
</tr>
<tr>
<td>Adjust memory quotas for a process</td>
<td>Allows user to set the maximum amount of memory a process can use.</td>
<td>Administrators</td>
</tr>
<tr>
<td>Back up files and directories</td>
<td>Allows backing up the system; overrides specific file and folder permissions.</td>
<td>Administrators, Backup Operators</td>
</tr>
<tr>
<td>Bypass traverse checking</td>
<td>Allows a user to go through directory trees (folder structures) even if the user doesn’t have permission to access the directories being passed through.</td>
<td>Administrators and Authenticated Users on domain controllers; on servers and workstations, Administrators, Backup Operators, Power Users, Users, and Everyone</td>
</tr>
<tr>
<td>Change the system time</td>
<td>Allows the setting of the computer’s internal clock.</td>
<td>Administrators and Server Operators on domain controllers; Administrators and Power Users on servers and workstations</td>
</tr>
<tr>
<td>Create a pagefile</td>
<td>Allows the creation and modification of a pagefile.</td>
<td>Administrators</td>
</tr>
<tr>
<td>Create global objects</td>
<td>Allows the creation of global objects in a Terminal Services session.</td>
<td>Administrators</td>
</tr>
<tr>
<td>Debug programs</td>
<td>Allows the user to attach a debugger to a process.</td>
<td>Administrators</td>
</tr>
<tr>
<td>Enable computer and user accounts to be trusted for delegation</td>
<td>Permits a user to set the Trusted for Delegation setting on an object.</td>
<td>Administrators on domain controllers; not assigned on member servers or workstations</td>
</tr>
<tr>
<td>Force shutdown from a remote system</td>
<td>Allows the shutdown of a computer from a remote location on the network.</td>
<td>Administrators and Server Operators on domain controllers; Administrators on member servers and workstations</td>
</tr>
<tr>
<td>Privilege</td>
<td>Description</td>
<td>Groups Assigned the Privilege by Default</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Impersonate a client after authentication</td>
<td>Allows an account to impersonate another account.</td>
<td>Administrators</td>
</tr>
<tr>
<td>Increase quotas</td>
<td>Allows a process with write property access to another process to increase the processor quota assigned to that process.</td>
<td>Administrators</td>
</tr>
<tr>
<td>Increase scheduling priority</td>
<td>Allows the use of Task Manager to change the scheduling priority of a process.</td>
<td>Administrators</td>
</tr>
<tr>
<td>Load and unload device drivers</td>
<td>Install and remove device drivers.</td>
<td>Administrators</td>
</tr>
<tr>
<td>Manage auditing and security log</td>
<td>Allows a user to specify auditing options and to view and clear the security log in Event Viewer. Audit Directory Service Access must be turned on for object access auditing to be performed. (See Chapter 11.) Administrators can always view and clear the security log.</td>
<td>Administrators</td>
</tr>
<tr>
<td>Modify firmware environment variables</td>
<td>Allows the configuration of nonvolatile RAM on computers that support such function.</td>
<td>Administrators</td>
</tr>
<tr>
<td>Profile a single process</td>
<td>Allows performance sampling on a process.</td>
<td>Administrators and Power Users on member servers and workstations; Administrators on domain controllers</td>
</tr>
<tr>
<td>Profile system performance</td>
<td>Allows performance sampling of the system.</td>
<td>Administrators</td>
</tr>
<tr>
<td>Remove computer from docking station</td>
<td>Allows the removal of a laptop from a docking station using Eject PC on the Start menu.</td>
<td>Administrators, Power Users, and Users (default setting for this is Disabled, not enforcing any limitations)</td>
</tr>
</tbody>
</table>
Assigning User Rights to a Group

Rights are assigned and removed most easily at a domain level using Group Policy. Suppose you have a group of users who should be able to log on locally to servers running Windows Server 2003 but you don’t want them to be members of any groups that have this logon right by default. One way to approach this situation is to create a group called Logon Rights, add the users to the group, and assign the right to log on locally to the Logon Rights group. The following steps describe how to assign a right to a particular group:

1. Choose Active Directory Users And Computers from the Administrative Tools menu. Right-click the domain name, and select Properties.

2. Click the Group Policy tab, and then click Edit. Select Computer Configuration, and then choose Windows Settings.

3. Under Security Settings, click Local Policies and then click User Rights Assignment. (See Figure 9-3.) In the details pane, double-click Allow Log On Locally.

4. Select Define These Policy Settings and then click Add.

---

Table 9-5 Privileges assigned to groups by default

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Groups Assigned the Privilege by Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore files and directories</td>
<td>Allows restoring files and folders to a system; overrules specific file and folder permissions.</td>
<td>Administrators, Backup Operators, and Server Operators on domain controllers; Administrators and Backup Operators on workstations and servers</td>
</tr>
<tr>
<td>Shut down the system</td>
<td>Shuts down the local computer.</td>
<td>Administrators, Account Operators, Backup Operators, Print Operators, and Server Operators on domain controllers; Administrators, Backup Operators, and Power Users on member servers; Administrators, Backup Operators, Power Users, and Users on workstations</td>
</tr>
<tr>
<td>Synchronize directory service data</td>
<td>Allows a user to initiate a synchronization of Active Directory.</td>
<td>None</td>
</tr>
<tr>
<td>Take ownership of files or other objects</td>
<td>Allows a user to take ownership of any security object, including files and folders, printers, registry keys, and processes.</td>
<td>Administrators</td>
</tr>
</tbody>
</table>
5. Type the name of the group to be granted this right (or click Browse to search for the group). Click OK twice, and close Default Domain Policy.

![Figure 9-3 User rights listed under Group Policy](image)

The same process can remove rights, except that you click Remove, rather than Add, in step 4. Rights can also be assigned to an individual user by using this method.

**Note** Rather than set this as a Default Domain Group Policy, use a different Group Policy Object to link this change to an OU.

**Assigning Rights Locally**

Rights can be assigned or removed locally, though you must bear in mind that a defined domain-level policy overrides a local policy setting. The following steps describe how to assign a policy locally:

1. Choose Local Security Policy from the Administrative Tools menu.
2. Under Security Settings, click Local Policies and then click User Rights Assignment.
3. In the detail pane, double-click the policy you want to assign to open the policy’s properties window.
4. Click Add User Or Group to select an individual or a group in the Select Users Or Groups dialog box. Make sure the Look For and Look In fields are pointing to the locations you want. Click Advanced, and then click Find Now. All the potential group members appear in the lower pane.
5. Highlight the accounts to be added and click OK.

If the Add User Or Group and Remove buttons aren’t available in the Properties window as shown in Figure 9-4, it means the policy has been set at the domain level and can’t be overridden locally.
Creating User Accounts

Every person who has access to the network requires a user account. A user account makes it possible to do the following:

- Authenticate the identity of the person connecting to the network
- Control access to domain resources
- Audit actions performed using the account

Windows Server 2003 creates only two normal predefined accounts on a domain controller: the Administrator account, which is granted all rights and permissions, and the Guest account, which has limited rights. On domain controllers, there is also a KRBTGT key distribution account; on non-domain controllers, there are built-in special accounts for Help and Support and Remote Assistance. All other accounts are created by an administrator and are either domain accounts (which are valid throughout the domain by default) or local accounts (which are usable only on the machine on which they are created).

Naming User Accounts

In Active Directory, each user account has a principal name. The name consists of two parts, the security principal name and the principal name suffix. For existing Windows NT user accounts, the security principal name is by default the same as the name used to log on to the Windows NT domain. For new Windows Server 2003 user accounts, an administrator assigns the security principal name. The default principal name suffix is the DNS name of the root domain in the domain tree. So a user identified as EduardoP in
a Windows NT domain has a principal name such as EduardoP@example.com in Windows Server 2003 (as well as Windows 2000 Server).

**Account Options**

Planning account options for users simplifies the process of creating accounts. Consider the following account options:

- **Logon Hours**  By default, a user can log on at any hour of the day or night. For security reasons, you might want to restrict access by some or all users to certain times of the day or certain days of the week.

- **Log On To**  By default, users can log on to all workstations. For security reasons, you can limit logon access to a particular machine or machines if you have the NetBIOS protocol installed in the domain. Without NetBIOS, Windows 2000 is unable to determine a specific logon location.

- **Account Expiration**  You can decide whether you want to set accounts to expire. For obvious reasons, it makes sense to set an expiration date for temporary employees to coincide with the end of their contracts.

Other options—*many* other options—can be set in user accounts and are detailed in the section “Setting User Account Properties.” The three options just listed are the most likely to be applied across large numbers of users.

---

**Real World  Establishing a Naming Convention**

Assign the security principal name using a consistent naming convention so that you and your users can remember user names and find them in lists. The following list describes some options for user names:

- **First name plus last initial**  Examples are MichaelG and SusanM. In the case of duplicate first names, you can add numbers (MichaelG1 and MichaelG2) or enough letters to provide identification (IngridMat and IngridMur).

- **First name plus a number**  Examples are Dave112 and Dave113. This approach can be a problem, especially for people with first names that appear frequently in the population. This approach can make it hard to remember your own user name much less any others.

- **First initial plus last name**  An example is MSmith. If you have both a Linda Smith and a Louise Smith, you could use LiSmith and LoSmith or LSmith1 and LSmith2.
Last name plus an initial  This convention is useful in a large network. When you have multiple users with the same last name, add a few letters as in SmithLi or SmithLo.

No matter which approach you choose, you must not only accommodate the existing users on your network but you must also be able to integrate future users. Then, whether the company’s next hire is U Ti or Chomondely St. J. Montmorency-Glossup, your user-name convention can still handle it.

Passwords

All your users must have well-chosen passwords and be required to change them periodically. Passwords should be chosen according to the guidelines in the Real World sidebar “Rules for Good Passwords.” Set accounts to lockout when invalid passwords are entered. (Allow three attempts, to leave room for typographical errors by the user.)

Real World  Rules for Good Passwords

A good password has the following characteristics:

- It is not a rotation or reuse of the characters in a logon name. (How many brain cells does it take to figure this one out?)
- It contains at least two alphabetic characters and one nonalphabetic character.
- It is at least seven characters long.
- It isn’t the user’s name or initials, the initials of his or her children or significant other, or any of these items combined with other commonly available personal data such as a birth date, telephone number, or license plate number.

Among the best passwords are alphanumeric acronyms of phrases that have a meaning to the user but are not likely to be known to others. This makes the password easy for the user to remember, while at the same time making it hard for an outsider to guess. Another good password isn’t a word at all but a “passphrase”—an entire phrase or sentence, complete with spaces and punctuation.

It pays to educate your users about passwords and password privacy, but most of all, it pays to heed your own advice: make sure the password you select for administration is a good password, and change it frequently. Doing so will help you avoid the consequences of having somebody break into your system and wreak havoc in your very own kingdom. If users dial in to the network from home or other remote sites, include more security than domain-level password authorization.
Administrators should have two accounts on the system: one administrative account and one normal user account. Use the normal user account unless you are performing administrative tasks like installing software or configuring accounts. Because of the privileges associated with administrative accounts, they are prime targets for intruders. Chapter 12 includes details about using the secondary logon feature to keep the administrative account safe.

Creating a Domain User Account

Domain user accounts can be created in the default Users container, or you can make an OU to hold domain user accounts. The following steps describe how to add a domain user account:

1. Choose Active Directory Users And Computers from the Administrative Tools menu.
2. Right-click the container in which you want to create the account, point to New, and then choose User from the shortcut menu.
3. Provide the user’s first and last name. The Full Name box is filled in automatically. The full name must be unique in the OU where the user account is created.
4. Provide the user logon name based on your naming convention. (See Figure 9-5.) This name must be unique in Active Directory. The pre–Windows 2000 logon name is filled in automatically. This is the name used to log on from computers running older Windows operating systems such as Windows NT. Click Next.

![Figure 9-5 Creating a new user](image)
5. Provide a password, and set password policies. Click Next. A confirmation screen appears.

6. If the details of the account you are about to create are correct, click Finish. Otherwise, click Back to make corrections.

At this point, the new user account is added to the OU with default settings. It’s unlikely that the default settings are exactly what you want, so you need to adjust the properties of the new account, as described in the section “Setting User Account Properties.”

Creating a Local User Account
A local account can’t log on to the domain and therefore has access only to the resources on the computer where it’s created and used. The following steps describe how to create a local user account:

1. Right-click My Computer, and choose Manage from the shortcut menu.
2. In the console tree, click Local Users And Groups. Right-click Users, and choose New User from the shortcut menu.
3. In the New User dialog box, supply the user name, full name, and description.
4. Provide a password, and set password policies. Click Create. At this point, the new user account is created with default settings. Local accounts can belong to locally created groups (on the single computer).

Setting User Account Properties
The Properties window for a domain user can have up to 13 tabs, depending on the domain’s setup; Table 9-6 describes these tabs. Information entered in the Properties window can be used as the basis for a search in Active Directory. For example, you can find a user’s telephone number or department by searching for the user’s last name. The following steps describe how to set the properties for a domain user account:

1. Choose Active Directory Users And Computers from the Administrative Tools menu.
2. Open the OU where the domain user account was created.
3. Double-click the user account to open the Properties window.
4. Click the tab for the properties you want to set. Make the changes, and click OK when you’re finished.
Note There are even more tabs visible if you have Advanced Features enabled in your Active Directory Users and Computers console. The additional tabs are Published Certificates, Object, and Security.

Testing User Accounts

As you develop different types of user accounts, it’s advisable to test them. Create a dummy account with the memberships and restrictions you’re planning on using. Then log on to a client machine and see whether the account produces the results you expect by doing the following:

- Test restrictions to logon hours and passwords by attempting to bypass them.
- Test home folders and profiles (discussed in “Using Home Folders,” later in this chapter) to see whether they are actually created.
Test roaming profiles by logging on from various machines.
Test group memberships by performing a task that membership in the group is supposed to allow (or deny), such as logging on to a server.

The time to discover an unfortunate setting is in a test environment. Test Group Policy settings using Resultant Set of Policy, discussed in Chapter 11.

Managing User Accounts
On a large, busy network, managing user accounts is a continual process of additions, deletions, and changes. Although these tasks aren’t difficult, they can be time-consuming and need to be managed carefully.

Finding a User Account
On small networks, it’s easy enough to locate a user under Active Directory Users And Computers. On a larger network, more advanced search techniques must be brought to bear.

To search for a particular user account, choose Active Directory Users And Computers from the Administrative Tools menu and on the toolbar, click the Find icon, shown here:

This opens the Find Users, Contacts, And Groups dialog box. Click the drop-down arrow in the Find box and you see that you can also use this tool to search for computers, printers, shared folders, OUs, and more. (See Figure 9-6.)

Figure 9-6  The Find tool allows for fairly specific searches
Select the scope of your search in the In box. Type a name or part of a name, and click Find Now. A search for a portion of a name returns all users, contacts, and groups with that element in their names.

Choose another option in Find and the possible search parameters adjust. For example, choose Common Queries in the Find list and you have an easy way to search for disabled accounts or users with nonexpiring passwords.

For even more in-depth searches, click the Advanced tab and select criteria from the Field drop-down list. Searches can be made on virtually every bit of information in a user, contract, group, or other object record. Figure 9-7 shows a search for a printer that can print double-sided on legal-sized paper and can staple and can print at least four pages per minute and has a resolution of 600 dpi or greater. A tall order, but if it exists, it will be found.

![Figure 9-7 Searching for printers in Active Directory using specific criteria](image)

**Disabling and Enabling a User Account**

If you need to deactivate a domain user account for some period of time but not delete it permanently, you can disable it. Find the user account, right-click the user name, and select Disable Account from the shortcut menu (as shown in Figure 9-8).

An informational box opens telling you that the object has been disabled, and a red circle with an “X” appears over the user account’s icon. Enable a disabled account by reversing the process, choosing Enable Account from the shortcut menu.
Deleting a User Account

Each user account in the domain has an associated SID that is unique and never reused, which means that a deleted account is completely deleted. If you delete Jeremy's account and later change your mind, you have to re-create not only the account but also the permissions, settings, group memberships, and other properties that the original user account had. For that reason, if there’s any doubt about whether an account might be needed in the future, it’s best to disable it and not perform the deletion until you’re sure it won’t be needed again.

However, accounts do have to be deleted at regular intervals. Just find the user account, right-click the user name, and select Delete from the shortcut menu. An Active Directory dialog box prompts you to confirm the deletion. Click Yes and the account is deleted.

Moving a User Account

Moving a user account from one container to another is similarly easy. Find the user account in Active Directory. Right-click and select Move from the shortcut menu. In the Move dialog box, select the destination container and click OK. Or just drag and drop the account into its new destination container.

Using the Ctrl and Shift keys, you can select multiple user accounts to move at once.
Renaming a User Account

On occasion, a user account might need to be renamed. For example, if you have an account configured with an assortment of rights, permissions, and group memberships for a particular position and a new person is taking over that position, you can change the first, last, and user logon names to fit the new person. The following steps describe how to rename an existing user account:

1. Find the existing user account. Right-click the user name, and choose Rename from the shortcut menu. (You can also slowly click the user name twice.)
2. Press the Delete key and then the Enter key to open the Rename User dialog box.
3. Type the changes, and click OK. The account is renamed, and all permissions and other settings remain intact. Other data in the account’s Properties window—such as address, phone number, and so forth—have to be changed as well. If a home folder exists, it will not be renamed for the new user and will have to be created separately.

Resetting a User’s Password

For passwords to be effective, they must not be obvious or easy to guess. However, when passwords are not obvious or easy to guess, they are often forgotten. When a user forgets his or her password, you can reset it. The best practice is to reset it to a simple password and require the user to change the password the next time he or she logs on to the network.

The following steps describe how to reset a password:

1. Find the user account whose password you need to reset.
2. Right-click the account name and choose Reset Password from the shortcut menu.
3. In the Reset Password dialog box (shown in Figure 9-9), type the new password twice, and select the User Must Change Password At Next Logon option. Click OK to implement the change.

![Figure 9-9  Resetting a user’s password](image-url)
Unlocking a User Account

If a user violates a group policy, such as exceeding the limit for bad logon attempts or failing to change an expired password, Active Directory locks the account. When an account is locked, it cannot be used to log on to the system. When the penitent comes pleading for reinstatement and after you deliver a few firm words on the importance of following rules, take the following steps to unlock the user account:

1. Find the locked account in Active Directory. Right-click the account and choose Properties from the shortcut menu.
2. In the Properties window, click the Account tab.
3. Clear the check box next to Account Is Locked Out. Click OK.

By default, Group Policy does not lock accounts because of failed logon attempts—you make this setting for security reasons. See Chapter 11 for more about Group Policy.

Note For instructions about how to delegate the right to unlock locked accounts, see Chapter 12.

Using Home Folders

Home directories or folders are repositories you can provide on a network server for users’ documents. Placing home folders on a network file server has several advantages:

■ Backup of user documents is centralized.
■ Users can access their home folders from any client computer.
■ Home folders can be accessed from clients running any Microsoft operating system (including MS-DOS and all versions of Windows).

The contents of home folders are not part of user profiles, so they don’t affect network traffic when users log on. (A home folder can also be on a client computer, but that defeats much of its purpose.)

Creating Home Folders on a Server

The following steps describe how to create a home folder on a network file server:

1. On the server, create a new folder for the home folders. Name it Home Folders. Right-click the new folder, and choose Sharing And Security from the shortcut menu.
2. Click the Sharing tab, and select the Share This Folder option.
3. Click the Security tab, and assign Full Control to the Users group (as shown in Figure 9-10).

![Figure 9-10 Giving full control to Users](image)

**Security Alert** Store home folders on a partition formatted with NTFS. Home folders on a FAT partition can be secured only by assigning shared folder permissions on a user-by-user basis.

**Providing Home Folders to Users**

To provide a user with a home folder, you must add the path for the folder to the user account’s properties. Follow these steps to give a user access to a home folder:

1. Find the user account in Active Directory. Right-click the user name, and choose Properties from the shortcut menu.

2. Click the Profile tab. In the Home Folder area, click the Connect option and specify a drive letter to use to connect to the file server.

3. In the To box, specify the UNC name for the connection—for example, `\server_name\shared_folder\user_logon_name`. If you use the variable `%username%`, as shown in Figure 9-11, a home folder is given the user’s logon name.
Maintaining User Profiles

A profile is an environment specifically customized for a user. The profile contains the desktop and program settings for the user. Every user has a profile, whether the administrator configures one or not, because a default profile is automatically created for each user who logs on to a computer. Profiles offer a number of advantages:

- Multiple users can use the same computer, with the settings for each user restored at logon time to the same state as when he or she logged off.
- Desktop changes made by one user do not affect any other user.
- If user profiles are stored on a server, they can follow users to any computer on a network running Windows Server 2003, Windows XP Professional, Windows 2000, or Windows NT 4.

From an administrator’s standpoint, the information in the profile can be a valuable tool for setting up default user profiles for all users on the network or for customizing default profiles for different departments or job classifications. You can also set up mandatory profiles that allow a user to make changes to the desktop while logged on but not to save any of the changes. A mandatory profile always looks exactly the same every time a user logs on. There are three types of profiles:

- **Local profiles** Profiles made on a computer when a user logs on. The profile is specific to a user, local to that computer, and stored on the local computer’s hard disk.
- **Roaming profiles**  Profiles created by an administrator and stored on a server. These profiles follow a user to any computer on a network running Windows Server 2003, Windows XP Professional, Windows 2000, or Windows NT 4.

- **Mandatory profiles**  Roaming profiles that can be changed only by an administrator.

### Real World  What's Stored in a Profile?

All profiles start out as a copy of the Default User profile that is installed on every computer running Windows Server 2003, Windows XP Professional, Windows 2000, and Windows NT 4. Registry data for Default User is in the Ntuser.dat file contained in the Default User profile. Inside each profile are the following folders:

- **Application Data**  Program-specific settings determined by the program manufacturer plus specific user security settings

- **Cookies**  Messages sent to a Web browser by a Web server and stored locally to track user information and preferences (not in Windows NT 4)

- **Desktop**  Desktop files, folders, shortcuts, and the desktop appearance

- **Favorites**  Shortcuts to favorite locations, particularly Web sites

- **Local Settings**  Application data, History, and Temporary files (not in Windows NT 4)

- **My Documents**  User documents and My Pictures, which contains user graphics files (not in Windows NT 4)

- **NetHood**  Shortcuts to My Network Places

- **PrintHood**  Shortcuts to items in the Printers folder

- **Recent**  Shortcuts to the most recently accessed folders and files

- **SendTo**  Items on the Send To menu

- **Start Menu**  Items on the user’s Start menu

- **Templates**  Application templates

By default, only the Cookies, Desktop, Favorites, My Documents, and Start Menu folders are visible in Microsoft Windows Explorer. The other folders are hidden; to see them select Folder Options, click the View tab, and select Show Hidden Files And Folders.
Local Profiles

Local profiles are created on computers when individual users log on. On a computer upgraded from Windows NT 4, the profile is stored in the Profiles folder on the system root partition. On a computer with a new installation of Windows Server 2003, Windows XP Professional, Windows 2000 Server, or Windows 2000 Professional, the user profile is in the Documents And Settings folder (as shown in Figure 9-12).

![Figure 9-12 A user’s local profile set up at the first logon event](image)

The first time a user logs on to a computer, a profile folder is generated for the user, and the contents of the Default User folder are copied into it. Any changes made to the desktop by the user are saved in that user’s profile when he or she logs off.

If a user has a local account on the computer as well as a domain account and logs on at different times using both accounts, the user will have two profile folders on the local computer: one for when the user logs on to the domain using the domain user account and one for when the user logs on locally to the computer. The local profile is shown with the logon name. The domain profile is also shown with the logon name but has the domain name appended to it.

Roaming Profiles

Roaming profiles are a great advantage for users who frequently use more than one computer. A roaming profile is stored on a server and, after the user’s logon attempt is authenticated in the directory service, the profile is copied to the local computer. This allows a user to have the same desktop, application configuration, and local settings at any machine running Windows Server 2003, Windows XP Professional, Windows 2000, or Windows NT 4.

Here’s how it works. You assign a location on a server for user profiles and create a folder shared with users who are to have roaming profiles. You type a path to that folder in the user’s Properties window. The next time the user logs on to a computer, the profile from the
server is downloaded to the local computer. When the user logs off, the profile is saved both locally and in the user profile path location. Specifying the user profile path is all it takes to turn a local profile into a roaming profile, available anywhere in the domain.

When the user logs on again, the profile on the server is compared to the copy on the local computer, and the more recent copy is loaded for the user. If the server isn’t available, the local copy is used. If the server isn’t available and this is the first time the user has logged on to the computer, a user profile is created locally using the Default User profile. When a profile isn’t downloaded to a local computer because of server problems, the roaming profile is not updated when the user logs off.

Security Alert  It’s best to put user profiles on a member server rather than on a domain controller to speed up the process of authentication and to avoid using a domain controller’s processing power and bandwidth for the downloading of profiles. In addition, place the profiles on a server that is backed up regularly so that copies of roaming profiles are as recent as possible.

Setting Up Roaming Profiles

Setting up roaming profiles is easy—you assign a location on a server and complete the following steps:

1. Create a shared folder for the profiles on the server.
2. On the Profile tab in the user account Properties window, provide a path to the shared folder, such as `\server_name\shared_profile_folder\%username%`.

Figure 9-13 shows an example of a path for a roaming profile. When you use the variable `%username%`, Windows Server 2003 automatically replaces the variable with the user account name.

Figure 9-13  Setting a path for a roaming profile
After you create a shared profile folder on a server and supply a profile path in the user account, a roaming profile is enabled. The user’s configuration of his or her desktop is copied and stored on the server and is available to the user from any computer. Most of the time, though, you don’t want to send your users off to fend for themselves. Life is easier for them, and for you, if users are assigned a customized profile that is already set up with appropriate shortcuts, network connections, and Start menu items. For this, you need to set up customized profiles.

**Creating Customized Roaming Profiles**

Creating customized roaming profiles is a simple—albeit multistep—process:

1. Create a user account with a descriptive name such as District Managers or Sales Staff. This is just a “blank” user account that you use to create a template for the customized configuration.

2. Log on using the template account, and create the desktop settings you want, including applications, shortcuts, appearance, network connections, printers, and so forth.

3. Log off the template account. Windows Server 2003 creates a user profile on the system root drive in the Documents And Settings folder.

4. Log on again using an administrator account. Find the accounts that are going to have this customized roaming profile.

5. In each account, click the Profile tab, and in the Profile Path box, type `\server_name\profile_folder\%username%`. Click OK.


7. Click the Advanced tab, and then in the User Profiles section, click Settings. Highlight the template account—in this case TeamLeaders—and click Copy To.

8. In the Copy To dialog box, type the path of the profiles folder on the server, `\server_name\roaming_profiles_folder\username`. Note that this time you must use the actual name of the roaming profile or the profile will be stored under the name of whoever is logged on.

9. In the Permitted To Use area, click Change to give the appropriate group permission to use the profile. (See Figure 9-14.) Click OK to copy the template profile.
Using Mandatory Profiles
If you’re going to all the trouble of assigning customized profiles, you undoubtedly want to make the profiles mandatory. To change a profile into a mandatory profile, you need only rename the hidden file Ntuser.dat to Ntuser.man.

Note
If you don’t see the Ntuser file in the individual’s profiles folder, choose Folder Options from the Tools menu and click the View tab. In Advanced Settings, select Show Hidden Files And Folders.

Assigning a Logon Script to a User Profile
Logon scripts can be assigned by profile or through Group Policy. (Group Policy is covered in Chapter 11.) The following steps describe how to assign a script to a profile:

1. Choose Active Directory Users And Computers from the Administrative Tools menu.
2. In the console tree, click Users. Right-click the user account, and choose Properties.
3. Click the Profile tab, and type the name of the logon script in the Logon Script box.
4. Click OK when you’re finished.

Windows Server 2003 always looks for logon scripts in the same place—on the authenticating domain controller at the path %SystemRoot%\SYSVOL\sysvol\domain_name\scripts. Scripts in this folder can be typed in the Logon Script path by name only, as shown in Figure 9-15. If you use folders inside the Scripts folder, you must show that part of the path in the Logon Script path. Table 9-7 shows the special variables that can be used when creating logon scripts. Logon scripts can also be created in VBScript and JScript. Replication
of logon scripts to all domain controllers is automatic on NTFS volumes on servers running Windows Server 2003 and Windows 2000 Server. Scripts on FAT16 and FAT 32 partitions must be replicated manually.

![User profile: Profile path: \Home\Shared\Profiles\Profile\Logon script: \Scripts](image)

**Figure 9-15** A logon script that’s located inside the Scripts folder

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%homedrive%</td>
<td>Letter of the drive containing the user’s home directory on the user’s local workstation</td>
</tr>
<tr>
<td>%homepath%</td>
<td>Full path of the user’s home directory</td>
</tr>
<tr>
<td>%os%</td>
<td>User’s operating system</td>
</tr>
<tr>
<td>%processor_architecture%</td>
<td>Processor type on the user’s workstation</td>
</tr>
<tr>
<td>%processor_level%</td>
<td>Processor level of the user’s workstation</td>
</tr>
<tr>
<td>%userdomain%</td>
<td>Domain where the user’s account is defined</td>
</tr>
<tr>
<td>%username%</td>
<td>Account user name</td>
</tr>
</tbody>
</table>

Writing and using scripts is covered in Chapter 13. For additional information about scripting and sample scripts, the TechNet Script Center at [http://www.microsoft.com/technet/scriptcenter/default.mspx](http://www.microsoft.com/technet/scriptcenter/default.mspx) is an excellent resource.

**Summary**

The success of a network operation is measured by both the availability of some information and resources and the restriction and protection of others. Windows Server 2003 offers the network administrator the tools and functionality to meet the information needs of users, while protecting sensitive information stored on or passed through the network. This chapter has explored the options available to the administrator for configuring groups, group scope, and user accounts through Windows Server 2003. The next chapter covers the use of group policy, shares, and permissions to provide accessibility and security for any network—from the simplest to the most complex.
As we’ve said in previous chapters, the whole point of a network is to share resources among the users. Your goal as a system administrator is to make sure everyone can find and use the resources they need without compromising security. Sharing and permissions are extensions of the security features that begin with user accounts and passwords and are at the heart of an administrator’s responsibilities.

Sharing File Resources

Windows Server 2003 supports four kinds of file resource sharing:

- Shared Folders
- Network File System (NFS) Shared Folders
- Active Directory Shared Folders
- Distributed File System (DFS) Folders

In this chapter, we’ll cover the basics of the first three of these, but we’ll leave the discussion of DFS for Chapter 20, where we talk about advanced storage technologies. For NFS shares, we’ll cover the mechanics of doing the actual file sharing here but leave the more in-depth discussion of setting up authentication and such for Chapter 27, where we cover interoperability. But first, let’s provide some basic descriptions of each of the types and note the situations in which they are important.
Shared Folders
These are essentially the same old shared folders that we've all used and seen since at least Microsoft Windows for Workgroups. In Windows Server 2003 SP1 and later, there is an important change, however. The default share permissions for a folder are read-only for the Everyone group. And in Windows Server 2003, the Everyone group does *not* include anonymous users.

NFS Shared Folders
Starting in Windows Server 2003 R2, the Microsoft Services for NFS are an installable component of Windows. Services for NFS includes NFS Server and NFS Client, along with the various supporting utilities, including the User Name Mapping Server. The NFS Server component allows you to share folders using the platform-independent NFS protocol. NFS Server supports both NFSv2 and NFSv3 protocols. The default permissions for an NFS share are read-only, with no anonymous access and no root access.

Active Directory Shared Folders
Active Directory Shared Folders are any shared folders that are published in Active Directory. To create an Active Directory Shared Folder, the underlying folder must first be shared on the host machine.

DFS Folders
DFS folders are another way to mask the underlying complexities of the network and file locations to simplify the user's view of file resources. They are discussed in Chapter 20.

Share Permissions vs. File Permissions
Before we explain the details of how to manage and configure shares in Windows Server 2003, let's take a moment to understand how permissions work with shared folders.

There are two kinds of permissions involved in any shared folder—those on the actual share, and those imposed by the underlying file system. These permissions are *subtractive*. This means that only the most restrictive permission will win. Managing permissions on both the share and the file system at the same time can often be quite confusing, and it's difficult to keep track of the details of both. We generally recommend using the underlying NTFS file permissions to control access and setting the share permissions to Full Control for everyone for most normal shares. The NTFS file permissions give much greater granularity and control over exactly what level of access is granted. However, there might be cases when using a more restrictive share permission is useful. We suggest, however, that when you do that you indicate in the share name that the share is restricted.
Share Permissions

Shares can be entire volumes or a folder tree. Until a volume or folder is shared over the network, users can’t see it or gain access to it. By default, the Everyone group is granted read access to all files in the folder, to all subfolders of that folder, and so on, assuming they have sufficient file system permissions. After a volume or folder is shared, restrictions can be added or removed in the form of share permissions. These permissions apply only at the drive or folder level—not at the file level—and are limited to allowing or denying Full Control, Read, and Change, as shown in Table 10-1.

<table>
<thead>
<tr>
<th>Share Permission</th>
<th>Type of Access</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>Allows viewing of file and subfolder names, viewing data in files, running programs</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>Allows the access under Read, plus allows adding files and subdirectories to the shared folder, changing data in files, and deleting files and subdirectories</td>
<td></td>
</tr>
<tr>
<td>Full Control</td>
<td>Allows all the access under Change, plus allows changing file permissions (NTFS volumes only) and taking ownership (NTFS volumes only)</td>
<td></td>
</tr>
</tbody>
</table>

Share permissions determine the maximum access allowed over the network. They don’t affect a user who logs on locally or a terminal server user of the computer. Share permissions are the only restrictions available for shares on a FAT volume (yet another reason to convert your FAT volumes to NTFS).

File Permissions

File permissions, unlike share permissions, control user access regardless of where it originates. Local users, Terminal Services users, and network users are all treated equally. Because FAT and FAT32 file systems don’t support any restriction on access to files, you should always use NTFS file systems to protect sensitive information. NTFS uses access control lists (ACLs) to limit access to resources. NTFS permissions can be assigned to both files and folders, and they apply network-wide and locally.

On an NTFS volume, you can set permissions down to the file level. This means that for any file you can give individual users different types of access. Although you can set such detailed permissions, this way lies madness for all but the most meticulous control freaks (who are, arguably, already mad).

Always try to operate with the simplest possible permissions. Set as few restrictions as possible. Assign permissions to groups, not individuals. Don’t set file-by-file permissions unless doing so is unavoidable. Managing the minutiae of permissions can easily and quickly soak up all your time and much of your life’s blood as well, unless you guard against it.
NTFS Permissions

As we noted earlier, the underlying ability to assign enforceable permissions to files and folders is part of the NTFS file system. As you work with files and folders on NTFS, you need to understand how the permissions work and how they are different for a file and for the folder that contains the file.

What Permissions Mean

Windows 2003 Server has a set of standard folder permissions that are combinations of specific kinds of access. The individual permissions are Full Control, Modify, Read & Execute, List Folder Contents, Read, and Write. Each of these permissions consists of a group of special permissions. Table 10-2 shows the special permissions and the standard permissions to which they apply.

<table>
<thead>
<tr>
<th>Special Permission</th>
<th>Full Control</th>
<th>Modify</th>
<th>Read &amp; Execute</th>
<th>List Folder Contents</th>
<th>Read</th>
<th>Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traverse Folder/Execute File</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>List Folder/Read Data</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Read Attributes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Read Extended Attributes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Create Files/Write Data</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Create Folders/Append Data</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Write Attributes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Write Extended Attributes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Delete Subfolders and Files</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Delete</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Read Permissions</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Change Permissions</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Take Ownership</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Synchronize</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Standard file permissions include Full Control, Modify, Read & Execute, Read, and Write. As with folders, each of these permissions controls a group of special permissions. Table 10-3 shows the special permissions associated with each standard permission.
**Important** Any user or group assigned Full Control on a folder can delete files and subfolders no matter what the permissions are on the individual files or subfolders.

Any user or group assigned Take Ownership can become the owner of the file or folder and then change permissions and delete files or even entire subfolder trees, no matter what the permissions are before they become the owner.

### How Permissions Work

If you take no action at all, the files and folders inside a shared folder have the same permissions as the share. Permissions for both directories and files can be assigned to the following:

- Groups and individual users on this domain
- Global groups, universal groups, and individual users from domains that this domain trusts
- Special identities, such as Everyone and Authenticated Users

The important rules for permissions can be summarized as follows:

- By default, a folder inherits permissions from its parent folder. Files inherit their permissions from the folder in which they reside.

<table>
<thead>
<tr>
<th>Special Permission</th>
<th>Full Control</th>
<th>Modify</th>
<th>Read &amp; Execute</th>
<th>Read</th>
<th>Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traverse Folder/Execute File</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>List Folder/Read Data</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Read Attributes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Read Extended Attributes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Create Files/Write Data</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Create Folders/Append Data</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Write Attributes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Write Extended Attributes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Delete Subfolders and Files</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Delete</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Read Permissions</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Change Permissions</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Take Ownership</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Users can access a folder or file only if they were granted permission to do so or they belong to a group that has been granted permission.

Permissions are cumulative, but the Deny permission trumps all others. For example, if the Technical Writers group has Read access to a folder, the Project group has Modify permission for the same folder, and Alex is a member of both groups, Alex has the higher level of permission, which is Modify. However, if the Technical Writers group permission is changed to explicitly Deny, Alex is unable to use the folder despite his membership—and ostensibly higher level of access—in the Project group.

The user who creates a file or folder owns the object and can set permissions to control access.

An administrator can take ownership of any file or folder.

Members of the Administrators, Backup Operators, and Server Operators groups can take ownership and reassign ownership.

Considering Inheritance

Just to complicate matters a bit more, there are two types of permissions: explicit and inherited. *Explicit permissions* are the ones you set on files or folders you create. *Inherited permissions* are those that flow from a parent object to a child object. By default, when you create a file or a subfolder, it inherits the permissions of the parent folder.

If you don’t want the child objects to inherit the permissions of the parent, you can block inheritance at the parent level or child level. Where you block inheritance is important. If you block at the parent level, no subfolders will inherit permissions. If you block selectively at the child level, some folders will inherit permissions and others will not.

To block a file or folder from inheriting permissions, right-click the folder, select Properties, and then click the Security tab. Click Advanced, and clear the check box for Allow Inheritance From The Parent To Propagate To This Object And All Child Objects.

If the check boxes for permissions appear shaded, the permissions are inherited from a parent object. If the boxes are shaded and have a check mark (as shown in Figure 10-1), some permissions are inherited and others have been added. There are three ways to change this situation:

- Click Advanced, and clear the check box for Allow Inheritance From The Parent To Propagate To This Object And All Child Objects. When the check box is cleared, you can make changes to the permissions or change the users or groups in the list.
Change the permissions of the parent folder.

Select the opposite permission—Allow or Deny—to override the inherited permission.

![Figure 10-1 A folder with inherited and noninherited permissions](image)

**Note** If neither Allow nor Deny is selected, the users or groups might have acquired the permission through a group membership. Otherwise, failure to explicitly configure Allow or Deny effectively denies the permission.

**Configuring Folder Permissions**

Before sharing a folder on an NTFS volume, set all the permissions on the folder. When you set folder permissions, you’re also setting permissions on all the files and subfolders in the folder. To set the permissions on the folder, perform one or more of the following actions:

- To assign permissions to a folder, right-click the folder in Explorer and choose Properties from the shortcut menu. Then click the Security tab.

- To remove an individual or group from the list, just select the name and click Remove.

- To add a user or group to the list of those with permissions, click Add. This opens the Select Users, Computers, Or Groups dialog box. Optionally, click Advanced to perform a more sophisticated search, as shown in Figure 10-2. Click OK when you’re done.
Assigning Permissions to Files

Permissions for individual files are assigned in the same way as permissions for folders. There are, however, some special considerations:

- Remember to grant permissions to groups rather than to individuals.
- Create domain-based groups, and assign file permissions to them rather than assigning permissions directly to local groups.

Configuring Special Permissions

In some circumstances, you might find it necessary to set, change, or remove special permissions on either a file or folder. To access special permissions, follow these steps:

1. Right-click the file or folder, and choose Properties from the shortcut menu. For this example, we’re working on a folder named VCD, which will appear in the various steps and screen shots. Your folder name will be different.

2. Click the Security tab, and then click Advanced.
   - To add a user or group, click Add. Double-click the user or group name to open the Permission Entry dialog box.
To view or modify existing special permissions, select the name of the user or group and click Edit.

To remove special permissions, select the name of the user or group and click Remove. If the Remove button is dimmed, clear the check box for Allow Inheritance Permissions From Parent To Propagate To This Object, and skip to step 6.

3. In the Permission Entry For VCD dialog box shown in Figure 10-3, select from the Apply Onto drop-down list where you want the permissions applied. (See Table 10-4 and Table 10-5 for explanations of the choices in this drop-down box.) Apply Onto is available for folders only.

![Figure 10-3  Setting special permissions for a folder](image)

4. In Permissions, select Allow or Deny for each permission.

5. To prevent subfolders and files from inheriting these permissions, select Apply These Permissions To Objects And/Or Containers Within This Container Only.

6. Click OK to close the dialog box.

In the Permission Entry For VCD dialog box for folders, you can choose how and where the special permissions are applied. Table 10-4 and Table 10-5 demonstrate the application of the special permissions depending on whether Apply These Permissions To Objects And/Or Containers Within This Container Only is selected.
Ownership and How It Works

As you’ve seen, Administrators and members of a few other select groups are the only ones who can grant and change permissions. The exception is when a user is the owner of the folder or file in question. Every object on an NTFS partition has an owner, and the owner is the person who created the file or folder. The owner controls access to the file or folder and can keep out anyone he or she chooses.

<table>
<thead>
<tr>
<th>Selected in Apply Onto</th>
<th>Applies to Current Folder?</th>
<th>Applies to Subfolders in Current Folder?</th>
<th>Applies to Files in Current Folder?</th>
<th>Applies to Subsequent Subfolders?</th>
<th>Applies to Files in Subsequent Subfolders?</th>
</tr>
</thead>
<tbody>
<tr>
<td>This folder only</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>This folder, subfolders, and files</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>This folder and subfolders</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>This folder and files</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Subfolders and files only</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Subfolders only</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Files only</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 10-5 Application of special permissions when Apply These Permissions To Objects And/Or Containers Within This Container Only is not selected

<table>
<thead>
<tr>
<th>Selected in Apply Onto</th>
<th>Applies to Current Folder?</th>
<th>Applies to Subfolders in Current Folder?</th>
<th>Applies to Files in Current Folder?</th>
<th>Applies to Subsequent Subfolders?</th>
<th>Applies to Files in Subsequent Subfolders?</th>
</tr>
</thead>
<tbody>
<tr>
<td>This folder only</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>This folder, subfolders, and files</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>This folder and subfolders</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>This folder and files</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Subfolders and files only</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Subfolders only</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Files only</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Here's how it works. Let's say a user named Maxwell creates a folder on his computer named Max's Private Stuff. To check the settings on his new folder, Maxwell right-clicks the folder, chooses Properties, and then clicks the Security tab. (See Figure 10-4.)

Figure 10-4  Viewing the NTFS permissions for a new folder

He sees that the Administrators group has full access to his folder, but because Maxwell is the owner of the folder, he can change the permissions so that he has the folder all to himself. To do so, he clicks Advanced to open the Advanced Security Settings dialog box and clears the Inherit From Parent option. (See Figure 10-5.)

Figure 10-5  Removing inheritance from a permission entry
Maxwell gets a security warning, and he can choose to either copy the current (inherited) permissions to the folder, making them explicit, or remove all permissions from the folder. He clicks Copy and returns to the Security Properties dialog box, where he then highlights the Administrators group, and clicks Remove. After this is done, even the administrator sees an Access Denied message when trying to open the folder.

Of course, nothing on the network can be *completely* beyond the reach of administrators, so an administrator can right-click the folder and choose Properties from the shortcut menu. When the administrator clicks the Security tab, the information box shown in Figure 10-6 opens.

![Figure 10-6](image)

**Figure 10-6** The administrator tries to view permissions for a folder owned by a user

In the Security Properties dialog box, no changes can be made. However, if the administrator clicks Advanced and then clicks the Owner tab (shown in Figure 10-7), he or she can change the owner of the folder to an administrator.

![Figure 10-7](image)

**Figure 10-7** Changing the ownership of a folder

Regardless of the status of the folder, the administrator can take ownership. When Maxwell logs on the next time, he still has access to Max’s Private Stuff, but when he clicks Advanced and then Owner, he sees that he’s no longer the owner of the folder. Changing
the ownership of the folder doesn’t automatically give Administrators access to the contents of the folder, but ownership does grant the ability to read and change permissions. With that, an administrator can change permissions and attain access to the folder contents.

---

**Note** The owner of a file or folder can also grant the Take Ownership special permission to others, allowing those users to take ownership at any time.

---

### Shared Folders

As with most things in Windows Server 2003, there are several ways to configure and administer shared folders. You can right-click a folder in Windows Explorer and choose Sharing And Security from the shortcut menu; you can use the Shared Folders snap-in, either stand alone or as part of the Computer Management MMC snap-in; you can use the new File Server Management MMC snap-in introduced in R2; or you can use the command line.

---

**Note** For some useful shared folders script examples that you use as is, or modify for your own needs, see the Microsoft TechNet Script Center at: http://www.microsoft.com/technet/scriptcenter/scripts/storage/shares.

Each approach has its advantages, but we recommend that you use the command line when you want to quickly create or modify a share, or that you use the File Server Management MMC snap-in when you want access to more management functions in a single place. The File Server Management snap-in not only gives you a place to create and manage shared folders, it provides quick access to the Disk Defragmenter and Disk Management snap-ins. We’ll use the File Server Management snap-in and the command line in this section, and we’ll use Windows Explorer in the “Creating an NFS Share” section and when we cover NFS shares. The command prompt is actually our first choice for most share management tasks, so we’ll try to integrate command lines into the whole process.

---

### Using the File Server Management Snap-In

The new File Server Management tool, introduced in Windows Server 2003 R2 is a useful addition to the administrator’s tool chest. It takes advantage of the improvements in the Microsoft Management Console introduced with MMC v3.0. Its biggest shortcoming, in our opinion, is that it fails to integrate NFS share management into the console. Ah, well, maybe in the next version.
To make the File Server Management tool available in R2, you need to add or upgrade the File Server role using Manage Your Server.

**Note**  An earlier version of the File Server Management snap-in was used in versions of Windows Server 2003 prior to R2. This snap-in is still available in R2, and it can be started by typing `filesvr.msc` from the Run dialog box or a command prompt.

To use the File Server Management tool, follow these steps:

1. Open the File Server Management MMC snap-in from the Administrative Tools folder on the Start menu, or type `fs.msc` in the Run dialog box or at a command prompt to open the File Server Management console shown in Figure 10-8.

![Figure 10-8  The File Server Management console in Windows Server 2003 R2](image)

2. Expand Share Folder Management, and expand Shared Folders in the tree pane.

3. Use the Shares, Sessions, and Open Files folders to view the current file shares on the system you’re managing and to see how much activity the shares are getting, as shown in Figure 10-9.
4. To see the same information from the command line, open a command window and type the following command, as shown in Figure 10-10:

```
net share
```

![Figure 10-10  Viewing available Shares using the command line](image)

**Creating a Shared Folder**

To share a folder or volume, open the File Server Management console and follow these steps:

1. Highlight the Shares folder, and click New Share from the More Actions menu in the Actions pane, as shown in Figure 10-11, to open the Share A Folder Wizard.
2. Click Next, and then type the folder path in the Folder Path box as shown in Figure 10-12, or click Browse to locate or create the folder you want to share. Click Next to continue.

3. Type the name you want to give the file share. For the best interoperability with earlier versions of Windows and non-Microsoft clients, choose a name that is both DNS and NetBIOS compatible.

4. Type a description for the shared folder in the Share Description box.

5. Optionally, click Change to control whether clients should use the offline files feature with the shared folder, and then click Next.

6. Specify the Share Level permissions for the folder, and then click Finish. (You can also set NTFS permissions here by choosing the Use Custom Share And Folder Permissions option and clicking Customize.)
7. To create the same share from the command line, open a command window and type

```
net share Docs=D:\Pub\Documents /grant:Everyone,Full
   /Remark:"Generally available documents" /cache:documents
```

as shown in Figure 10-13.

![Figure 10-13 Creating a share from the command line](image)

**Real World Setting Permissions**

It is generally best to use NTFS file permissions *instead* of share-level permissions to control access to shared resources over the network. Using share-level permissions alone gives you significantly less control over the specific permissions being granted, and it's less secure than file system permissions because it applies only to users connecting over the network.

However, there are some exceptions to this rule; for example, you might want to permit all authenticated users to access a volume in a certain subfolder but allow only a certain group to access the root directory. In this instance, you can create two file shares: one at the subfolder level with no share-level security (Full Control for Everyone), and one at the root folder level with share-level security to allow only the specified group access.

Somewhat more useful is the ability to hide file shares by adding the dollar sign ($) character to the end of the share name. This notation allows any user to connect to the share—provided he or she knows the share name. After users connect, they're still bound by NTFS security permissions, but this approach can be handy for storing useful power tools so that an administrator can access them from a user's system and user account. File security isn't really an issue—you just don't want users mucking around with the files.
Removing a Folder Share

It’s easy to stop sharing a folder without removing the underlying folder or files. From the File Server Management console, highlight the share, right-click, select Stop Sharing, and click Yes to confirm. Or, from the command line type

```
net share <sharename> /delete
```

From the command line, you won’t even get prompted to confirm. Use caution when you remove a share. It will disconnect any open files that users might be using and potentially cause loss of data.

Disconnecting Users

If you need to disconnect users from the server for some reason—say, to close off the server while you update the files—follow these steps:

1. Open the File Server Management console, and then open the Sessions subfolder.
2. Right-click the user you want to disconnect, and click Close Session from the shortcut menu.
3. To disconnect all sessions, click Disconnect All Sessions.
4. To close an open file, click the Open Files folder, select the file you want to close, and then click Close Open File.
5. To close all open files, click Disconnect All Open Files.
6. To close sessions from the command line, type `net session /delete`.
7. To see what files are open on the network prior to closing a session, type `net file`.

**Important** Be kind to your users and warn them before disconnecting them. Disconnecting a user who is working on a file can cause data loss and ill feelings (and Help desk calls).

Limiting Simultaneous Connections

You can limit the number of simultaneous user connections you want to allow to a shared folder so that a given shared folder doesn’t overburden the server with user connections. To do so, follow these steps:

1. Open the File Server Management console, and then open the Shares subfolder.
2. Right-click the shared folder you want to limit access to, and then choose Properties from the shortcut menu.

3. To place no limit on the number of connections you allow to the shared folder (other than the limit set by the number of licenses you have), select the Maximum Allowed option in the General tab, as shown in Figure 10-14.

4. To manually limit the number of connections you want to allow to the shared folder, type the maximum number of connections you want to allow in the Allow This Number Of Users box and then click OK.

5. To do this from the command line, type `net share /users:<number>`.

**Special Shares**

In addition to shares created by a user or administrator, the system creates a number of special shares that shouldn’t be modified or deleted. These include the administrative shares: the `ADMIN$` share, and the hidden shares for each hard drive volume (`C$`, `D$`, `E$`, and so on). These shares allow administrators to connect to drives that are otherwise not shared. These shares are not visible by default and can be connected to only by an administrator.
Special shares exist as part of the operating system’s installation. Depending on the computer’s configuration, some or all of the following special shares might be present (and none of them should be modified or deleted):

- **ADMIN$**  Used during the remote administration of a computer. The path is always the location of the folder in which Windows was installed (that is, the system root). Only Administrators, Backup Operators, and Server Operators can connect to this share.

- **driveletter$**  The root folder of the named drive. Only Administrators, Backup Operators, and Server Operators can connect to these shares on Windows 2003 Server or a Windows 2000 server. On Microsoft Windows XP Professional and Windows 2000 Professional computers, only Administrators and Backup Operators can connect to these shares.

- **IPC$**  Used during remote administration and when viewing shared resources. This share is essential to communication and can’t be deleted.

- **NETLOGON**  Essential to all domain controllers. Do not remove.

- **SYSVOL**  Required on all domain controllers. Do not remove.

- **PRINT$**  A resource that supports shared printers.

To connect to an unshared drive on another computer, you need to be logged on using an account with the necessary rights. Use the address bar in any window and type the address using the syntax

```
\<computer_name\>[driveletter]$```

To connect to the system root folder (the folder in which Windows is installed) on another computer, use the syntax

```
\<computer_name\>\admin$```

Figure 10-15 shows a connection made to the Windows directory on a client machine (xmpl-vpc-01) using the special share admin$.

Other special shares such as IPC$ and PRINT$ are created and used solely by the system. NETLOGON is a special share on Windows Server 2003, Windows 2000, and Windows NT servers and is used while processing domain logon requests.
Chapter 10  Managing File Resources  287

Figure 10-15  Connecting to an administrative share on a remote computer

Note  Adding a dollar sign ($) to the end of a share name hides the share from all users. To access a hidden share, you need to specify it explicitly; you can’t browse the network for the share.

The Command Line—Net Share

As we’ve seen throughout this chapter so far, it’s easy to create and manage shares at the command line by using the net share command. The syntax of the net share command is

NET SHARE

sharename=drive:path [/GRANT:user,[READ | CHANGE | FULL]]
[/USERS:number | /UNLIMITED]
[/REMARK:"text"]
[/CACHE:Manual | Documents | Programs | None ]

sharename [/USERS:number | /UNLIMITED]
[/REMARK:"text"]
[/CACHE:Manual | Documents | Programs | None]

{sharename | devicename | drive:path} /DELETE

Simply typing net share at the command line with no parameters will give you a list of currently shared folders. Typing net share <sharename> will give you the parameters in effect for the sharename.
Two other useful **net** commands for dealing with shares are **net view** and **net session**. Typing **net view** will give you a list of computers on the network or the resources available on a particular computer, while typing **net session** will list the sessions on the current computer or the details of a session with a particular computer. The syntax for these two **net** commands are:

```
NET VIEW
[\computername [/CACHE] | /DOMAIN[:domainname]]
```

```
NET VIEW /NETWORK:NW [\computername]
```

```
NET SESSION
[\computername] [/DELETE]
```

**Note** The **net** commands work with both NetBIOS names and IP addresses, and where the user is specified, they can use both DOMAIN\User and e-mail address formats. This makes it a flexible and useful tool, and one that should be a part of your normal repertoire.

---

**NFS Shared Folders**

For the first time in a Microsoft operating system, Windows Server 2003 R2 includes built-in support for NFS, the cross-platform choice for sharing of network resources. We’ll discuss the setup and configuration of NFS in greater detail in Chapter 27, but in this section we’ll show you how to share folders using the NFS protocol.

**Initial Configuration**

Before you can use Microsoft Server for NFS to share folders to NFS clients, you’ll need to make several configuration changes on your server. You’ll need to set up and specify a User Name Mapping server and open some ports on Windows Firewall if you’re using it, at a minimum. Well, actually, you can go ahead and share folders without doing any of that, but no one will be able to use them. The graphical tool for configuring and administering NFS is the %windir%\msnfs\nfsmgmt.msc, and the command-line tool is %windir%\msnfs\nfsadmin.exe.

**Specify a User Name Mapping Server**

Windows Server 2003 supports direct mapping of UNIX user ID (UID) and group ID (GID) in Active Directory using RFC 2307, as well as the User Name Mapping service. You can specify the User Name Mapping server to use from the command line:

```
nfsadmin mapping mapsrv=<servername>
```
To specify the User Name Mapping server graphically, open the MS NFS Administration console and follow these steps:

1. Right-click MSNFS Administration and select Properties, as shown in Figure 10-16.

![Figure 10-16 Using MSNFS Administration to specify the User Name Mapping server](image)

2. Enter the name or IP address of the User Name Mapping server.

3. Optionally, select Active Directory Lookup and specify the Active Directory Domain to use.

**Windows Firewall Configuration**

To share folders using NFS on a computer that is protected by Windows Firewall, you must create port exceptions in the firewall. There is no automatic way to configure these exceptions, unfortunately. For more details on configuring Windows Firewall, see Chapter 22. The ports that need to be opened for NFS are shown in Table 10-6.

<table>
<thead>
<tr>
<th>NFC Component</th>
<th>Port to Open</th>
<th>Protocols Used</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username Mapping Server and Server for NFS</td>
<td>Portmapper</td>
<td>TCP, UDP</td>
<td>111</td>
</tr>
<tr>
<td>Server for NFS</td>
<td>Network Status Manager</td>
<td>TCP, UDP</td>
<td>1039</td>
</tr>
<tr>
<td>Server for NFS</td>
<td>Nlockmgr (file locking manager)</td>
<td>TCP, UDP</td>
<td>1047</td>
</tr>
</tbody>
</table>
Creating an NFS Share

The creation of NFS shares is directly integrated into Windows Explorer, and the steps are very similar to the steps for creating traditional Windows shares. To share a folder using NFS, open Windows Explorer and follow these steps:

1. Highlight the folder you want to share, right-click, and select Sharing And Security from the context menu.
2. Click the NFS Sharing Tab, as shown in Figure 10-17.
3. Click Share This Folder, and type in a share name to use for the folder.
4. Optionally, change the encoding used. The default is ANSI, which is appropriate for most situations.
5. Select Allow Anonymous Access if you want to allow unauthenticated users to access the share.

Table 10-6 Open ports for NFS

<table>
<thead>
<tr>
<th>NFS Component</th>
<th>Port to Open</th>
<th>Protocols Used</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server for NFS</td>
<td>Mount (mounting daemon)</td>
<td>TCP, UDP</td>
<td>1048</td>
</tr>
<tr>
<td>Server for NFS</td>
<td>Server for NFS</td>
<td>TCP, UDP</td>
<td>2049</td>
</tr>
</tbody>
</table>

More Info For full information on configuring UNIX interoperability components—including NFS Server and Client, User Name Mapping, and UNIX ID Management—see Chapter 27.
6. Click the Permissions button to set the share permissions on the new share, as shown in Figure 10-18.

![Figure 10-18 Setting share permissions](image)

7. You can specify different permissions for each machine that accesses the share, or you can specify by groups of machines. (See Chapter 27 for how to set up client groups.) The default permissions are Read-Only for all machines, with no root access.

8. Click your way out of the dialog boxes.

9. To configure the same share from the command line, open a command window and type
   
   `nfsshare source=d:\Source -o ro -o noroot -o anon=yes`
   
   as shown in Figure 10-19.

![Figure 10-19 Creating an NFS share from the command line](image)
Deleting or Modifying an NFS Share

Deleting or modifying an existing NFS share is essentially the same process as creating it in the first place. Open Windows Explorer, highlight the shared folder, and select Sharing And Security from the context menu. Make your changes on the NFS Sharing tab, and click OK the necessary number of times. You're done. Existing connections will not see the changes until the next time they connect to the share.

The command line process is also the same. The full syntax of the `nfsshare.exe` command is

```
nfsshare
    sharename=drive:path
    [-o ro[=client[:client ...]]]
    [rw[=client[:client ...]]]
    na
    root[=client[:client ...]]
    noroot[=client[:client ...]]
    anon=yes|no
    anonuid=[Unmapped UID]
    anongid=[Unmapped GID]
    encoding={euc-jp|euc-tw|euc-kr|shift-jis|big5|ksc5601|gb2312-80|ansi }
    {euc-jp|euc-tw|euc-kr|shift-jis|big5|ksc5601|gb2312-80|ansi}=client1[:client2...]

    sharename
    [-o ro[=client[:client ...]]]
    [rw[=client[:client ...]]]
    na
    root[=client[:client ...]]
    noroot[=client[:client ...]]
    anon=yes|no
    anonuid=[Unmapped UID]
    anongid=[Unmapped GID]
    encoding={euc-jp|euc-tw|euc-kr|shift-jis|big5|ksc5601|gb2312-80|ansi }
    {euc-jp|euc-tw|euc-kr|shift-jis|big5|ksc5601|gb2312-80|ansi}=client1[:client2...]
    removeclient=client[[:client ...]]

    {sharename | drive:path} /delete
```

Publishing Shares in Active Directory

You can publish relatively permanent file shares in Active Directory, making them easier for users to find in a large network. To do so, use the following steps:

1. Open the File Server Management console and then select Shares.
2. Right-click the shared folder for which you want to set permissions, and then choose Properties from the shortcut menu.

3. Click the Publish tab and then select the Publish This Share In Active Directory check box. (See Figure 10-20.)

![Figure 10-20 Publishing a share in Active Directory](image)

4. In the Description box, type a description for the file share.

5. Type the e-mail address of the person responsible for the file share in the Owner box. (That would probably be you.)

6. Click Edit, add any keywords relevant to the share, and then click OK.

---

**Summary**

The success of a network is judged both by the availability of needed information and resources and by the restriction and protection of those using the network. This chapter has explored the options available to the administrator for managing the file resources of a network in Windows Server 2003. The next chapter covers day-to-day administrative tasks and how to simplify and streamline these tasks for maximum efficiency.
Chapter 11
Administering Group Policy

Components of Group Policy ........................................... 296
Managing Group Policies .................................................. 298
Creating a Group Policy Object ........................................... 303
Managing Group Policy Links ............................................. 305
Setting the Scope of Group Policy Objects ......................... 306
Delegating Permissions on GPOs .......................................... 308
Refreshing Group Policy .................................................... 311
Backing Up a Group Policy Object ....................................... 312
Restoring a Group Policy Object ........................................... 313
Using Group Policy for Folder Redirection ............................ 313
Using Resultant Set of Policy (RSoP) ..................................... 317
Summary ........................................................................ 320

For many small to medium networks, the groups built into Microsoft Windows Server 2003 can, with perhaps a little tweaking, provide perfectly adequate security. However, larger networks and those with special needs might not be able to alter the groups to provide all the levels of security needed. In those instances, Group Policy can give administrators a degree of control that is as granular as anyone could wish for.

Group Policy can reduce lost productivity caused by the usual suspects—users who accidentally delete system configuration files, misplace vital folders, or inadvertently introduce a virus to the network. Also, Group Policy can help increase productivity by making it easier for users to find what they need to work more efficiently. Group Policy accomplishes this by allowing the administrator to delineate the elements of the user’s desktop environment by specifying which programs are available, which programs appear on the desktop, and which options are available on the Start menu.
Components of Group Policy

Group Policy consists of several configurable components. The first is administrative templates, which set registry-based policy. Administrative templates provide policy information for the items that appear under the Administrative Templates folder in the console tree of the Group Policy Object Editor (GPOE) and in the Group Policy Management Console (GPMC). (These tools will be discussed in further detail later in the chapter.)

The other main components of Group Policy are as follows:

- **Security Settings**  Configures security for users, computers, and domains.
- **Scripts**  Specifies scripts for computer startup and shutdown, as well as for user logon and logoff events.
- **Folder Redirection**  Places special folders such as My Documents or specified application folders on the network.
- **Software Settings**  Assigns applications to users. (See Chapter 28 for more about publishing software on the network.)

Group Policy Objects

A collection of policy settings is called a Group Policy Object (GPO). A GPO contains both policies that affect computers and policies that affect users. Computer-related policies include security settings, application settings, assigned applications, and computer startup and shutdown scripts. User-related policies define application settings, folder redirection, assigned and published applications, user logon and logoff scripts, and security settings. In cases of conflicting policies, computer-related settings usually override user-related settings.

Note  Group Policy is the successor to the System Policy Editor in Windows NT and was first introduced in Windows 2000.

GPOs are stored at the domain level and are associated with an Active Directory object—a site, domain, or organizational unit (OU). One or more GPOs can apply to a site, domain, or OU, just as a single GPO can be linked to multiple sites, domains, and OUs.

Important  Linking a GPO to another site or another domain can seriously diminish performance.
Windows NT 4 Policies and Windows Server 2003

System policies set in Windows NT 4 do not migrate to Windows 2000 or to Windows Server 2003. A Windows NT client upgraded to Windows 2000 Professional or Windows XP Professional has only Active Directory–based group policies; no Windows NT 4 policies survive the upgrade. The primary difference between Windows NT system policies and Windows 2000 group policies lies in where the policies are written. Windows 2000 and Windows Server 2003 use the following four trees of the registry:

- HKEY_LOCAL_MACHINE\Software\Policies
- HKEY_CURRENT_USER\Software\Policies
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

The first two locations are preferred. When a group policy changes, these trees are essentially deleted and their contents are rewritten. Although none of the templates that come with Windows Server 2003 include values that write to other places in the registry, it’s possible for them to do so. (Windows NT 4 policies can write to any part of the registry.) However, it’s inadvisable to employ Windows NT–style policies that write to other parts of the registry for the following reasons:

- Only the four trees just listed are secure. Applications, the operating system, or users can modify other parts of the registry.
- After a policy is set in another part of the registry, it persists until the registry is edited or the policy is specifically reversed.
- Sticking with the Active Directory Group Policy gives you considerably more control over when and how policies change.

Windows NT 4 Workstation and Server clients don’t employ Active Directory, so you have to continue to use System Policy Editor (Poledit.exe) to set policy for those clients. Group policies do not apply to them. Similarly, run Poledit.exe on Windows 95 and Windows 98 clients, and copy the resulting Config.pol file to the SYSVOL folder of the Windows 2003 domain controller.

GPOs store information in two locations: in a folder structure called a Group Policy template (GPT) and in a Group Policy container (GPC) in Active Directory.
The GPT is in the SYSVOL folder of all domain controllers. It contains information about software policy, file and application deployments, scripts, and security settings. A GPC contains GPO properties, including the Active Directory class information related to application deployment. The information stored in a GPC changes infrequently.

**Note** A GPO that applies locally is stored in the local computer’s %SystemRoot%\System32\GroupPolicy folder. A computer can have only one local Group Policy.

**Group Policy Templates**

When you create a GPO, the corresponding GPT folder structure is created automatically. The actual name of the folder for the GPT will be the globally unique identifier (GUID) for the GPO—a number that is useful to the computer but is otherwise incomprehensible. However, to see the policy folder, look in %SystemRoot%\SYSVOL\ domain\Policies.

**Group Policy Containers**

Group Policy Objects also have an Active Directory component called a GPC that includes subcontainers with version information, status information, and a list of which Group Policy extensions are employed in the GPO. GPCs have no direct relevance to administration.

**Default Group Policies**

When Active Directory is set up, two domain GPOs are created. The Default Domain Policy is linked to the domain and affects all computers and users in the domain. The Default Domain Controllers Policy is linked to the Domain Controllers organizational unit and applies to all domain controllers in the domain.

**Managing Group Policies**

Group Policy can be created and modified using the Group Policy Object Editor (GPOE) snap-in for the Microsoft Management Console (MMC) plus additional snap-ins such as Active Directory Users and Computers, Active Directory Sites and Services, and Resultant Set of Policy. Different aspects of Group Policy functionality is provided by these additional snap-ins. If this is how you’ve been managing Group Policy until now and are content with the results, you can continue in the same way.

However, you should consider adding the new Group Policy Management Console (GPMC) to your repertoire. The GPMC provides a comprehensive overview of group policy across the enterprise in a single console. All Group Policy management tasks can be
performed from the GPMC except configuring individual policies in GPOs. And when
you want to configure individual policies from within a GPO, right-click the GPO and
select Edit, and the Group Policy Object Editor will launch with the GPO loaded.

As compared with the default Group Policy tools of Windows Server 2003, GPMC adds
the following new features:

- Back up and restore Group Policy objects
- Import and export GPOs and Windows Management Instrumentation (WMI) filters
- Copy and paste GPOs and Windows Management Instrumentation (WMI) filters
- Easier management of Group Policy–related security
- HTML reporting for GPO settings and Resultant Set of Policy (RSoP) data

Note Download GPMC at http://www.microsoft.com/downloads. If you have at
least one valid license of Windows Server 2003 or Windows 2000 Server, you can
use an unlimited number of copies of GPMC.

GPMC manages Windows Server 2003 as well as Windows 2000–based Group Policy
implementations.

Table 11-1 lists some common Group Policy tasks and how they’re performed on com-
puters with and without GPMC.

Table 11-1 Comparison of tasks with and without GPMC

<table>
<thead>
<tr>
<th>Task</th>
<th>On a computer without GPMC</th>
<th>With Group Policy Management snap-in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a Group Policy Object</td>
<td>Navigate to the Group Policy Properties tab for a site, domain, or organizational unit; click the tab, and then click New.</td>
<td>Open GPMC, navigate to Group Policy Objects, right-click it, and then click New.</td>
</tr>
<tr>
<td>Create a Group Policy object (GPO) and a link to it</td>
<td>On the Group Policy tab for a site, domain, or organizational unit, click New.</td>
<td>In GPMC, right-click the domain, site, or OU; select Create; And Link A GPO Here. For more information, see the “Creating a Group Policy Object” section later in this chapter.</td>
</tr>
<tr>
<td>Create an unlinked GPO</td>
<td>Go to the Group Policy Properties tab for a site, domain, or organizational unit, and click Add. On the All tab, right-click the Name pane and then click New.</td>
<td>Open GPMC, and navigate to Group Policy Objects. Right click Group Policy Objects, and select New. For more information, see the “Creating a Group Policy Object” section later in this chapter.</td>
</tr>
</tbody>
</table>
Table 11-1  Comparison of tasks with and without GPMC

<table>
<thead>
<tr>
<th>Task</th>
<th>On a computer without GPMC</th>
<th>With Group Policy Management snap-in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit a GPO</td>
<td>Navigate to the Group Policy Properties tab for the relevant domain, site, or OU. Select the GPO, and then click Edit.</td>
<td>Open GPMC, navigate to Group Policy Objects, right-click the GPO, and then click Edit. The Group Policy Object Editor will open with the GPO loaded. For more information, see the “Creating a Group Policy Object” section later in this chapter.</td>
</tr>
<tr>
<td>Link an existing GPO to a site, domain, or organizational unit</td>
<td>Go to the Group Policy Properties tab for a site, domain, or organizational unit; click Add; and then select a GPO.</td>
<td>In GPMC, navigate to a site, domain, or organizational unit; right-click it; and then click Link An Existing GPO Here.</td>
</tr>
<tr>
<td>Disable a branch of a GPO</td>
<td>Navigate to the Group Policy Properties tab for the relevant domain, site, or OU. Make your selection on the General tab.</td>
<td>Open GPMC, and navigate to the GPO. Right click, and select Edit, which will launch the Group Policy Object Editor. Right click the GPO, and select Properties. Make your selection on the General tab. See the “Disabling a Branch of a GPO” section later in this chapter.</td>
</tr>
<tr>
<td>Use security groups to filter the scope of policy</td>
<td>Open the GPO in the Group Policy Object Editor. Right-click the GPO, select Properties, and then click the Security tab.</td>
<td>In GPMC, click a GPO or GPO Link and then click the Scope tab. Use Add and Remove buttons to set the groups, users, and computers to which the GPO applies. For more information, see the “Setting the Scope of GPOs” section later in this chapter.</td>
</tr>
<tr>
<td>Delegate permissions on GPOs</td>
<td>Navigate to the properties of a GPO, and select the Security tab. In the Permissions For Authenticated Users pane, select the permissions you want to grant.</td>
<td>In GPMC, click the GPO, click the Delegation tab, and then click the Add or Remove button. For more information, see the &quot;Delegating Permissions on GPOs&quot; section later in this chapter.</td>
</tr>
<tr>
<td>Determine Resultant Set of Policy with Group Policy Results</td>
<td>In the Resultant Set of Policy snap-in, right-click Resultant Set of Policy and then select Generate RSoP Data. Select Logging Mode or Planning Mode in the Resultant Set of Policy Wizard.</td>
<td>In GPMC, right-click Group Policy Results and then click Group Policy Results Wizard. For more information, see the “Using Resultant Set of Policy (RSoP)” section later in this chapter.</td>
</tr>
<tr>
<td>Add a WMI filter</td>
<td>Navigate to the Properties of a Group Policy Object, and click the WMI Filter tab.</td>
<td>In GPMC, right-click WMI Filters and click New.</td>
</tr>
</tbody>
</table>
Order of Implementation

Group policies are processed in the following order:

1. Local group policy object.
2. GPOs linked to the site, in the order specified by the administrator. See the Linked Group Policy Objects tab for the site in the Group Policy Management Console (GPMC). The GPO with the lowest link order is processed last and therefore has the highest precedence.
3. Domain GPOs in the order specified by the administrator. See the Linked Group Policy Objects tab (shown in Figure 11-1) in the Group Policy Management Console (GPMC). The GPO with the lowest link order is processed last and therefore has the highest precedence.
4. Organizational unit Group Policy Objects, from largest to smallest organizational unit (parent to child organizational unit).

In this sequence, the last writer wins. If multiple GPOs attempt contradictory settings, the GPO with highest precedence wins.

Order of Inheritance

As a rule, Group Policy settings are passed from parent containers down to child containers. This practice means that a policy applied to a parent container applies to all the containers—including users and computers—that are below the parent container in the Active Directory tree.
Directory tree hierarchy. However, if you specifically assign a Group Policy for a child container that contradicts the parent container policy, the child container’s policy overrides the parent Group Policy.

If two policies are not contradictory, both can be implemented. For example, if a parent container policy calls for an application shortcut to be on a user's desktop and the child container policy calls for another application shortcut, both appear. Policy settings that are disabled are inherited as disabled. Policy settings that are not configured in the parent container are not inherited.

**Overriding Inheritance**

Several options are available for changing how inheritance is processed. One option prevents child containers from overriding any policy setting set in a higher level GPO. On a computer with GPMC, this option is known as enforcing the GPO link. On computers without GPMC, the same function is called No Override. This option is not set by default and must be turned on in each GPO where it’s wanted.

**Enforcing a GPO Link in GPMC**

Open GPMC and follow these steps:

1. Select the GPO in the console tree.
2. On the Scope tab, right-click the link and select Enforced on the shortcut menu to enable or disable enforcement for the link.
3. Click OK.

**Setting No Override**

On a computer without GPMC, set the No Override option by following these steps:

1. Open the GPO you want to administer.
2. Right-click the GPO, and choose No Override from the shortcut menu (as shown in Figure 11-2). A check mark appears next to the GPO under No Override.
3. Click OK.

A second option is Block Inheritance. When you select this option, the child container does not inherit any policies from parent containers. If there is a conflict between these two options, the Enforced/No Override option always takes precedence.

Simply stated, Enforced/No Override is a link property, Block Policy Inheritance is a container property, and Enforced takes precedence over Block Policy Inheritance.
Chapter 11  Administering Group Policy  303

Figure 11-2  Preventing inheritance from overriding settings on a GPO

**Setting Block Inheritance in GPMC**
In the console tree, navigate to the domain or organizational unit for which you want to block inheritance. Right click the domain or OU, and select Block Inheritance.

**Blocking Inheritance on Computers Without GPMC**
In the Group Policy Object Editor, right-click the GPO for which you want to block inheritance. Select Properties from the shortcut menu. On the Group Policy tab, select the box for Block Policy Inheritance. (The check box can be seen in Figure 11-2.)

**Note**  Explicit permissions take precedence over inherited permissions—even an inherited Deny. So if you explicitly grant access to an object, the inherited Deny will not prevent access.

---

**Creating a Group Policy Object**
Creating an Active Directory domain also creates a Default Domain Policy and a Default Domain Controllers Policy. With a few judicious adjustments to meet the needs of your own situation, you might never need anything else., though most organizations will likely need a few OUs with Group Policy Objects linked to them. When the time comes to set up a GPO of your own, follow the procedure in “Creating a GPO in GPMC” or the steps in “Creating a GPO on a Computer without GPMC.”
Creating a GPO in GPMC
Open GPMC, and navigate to the container to which you want the new GPO to apply. Right-click the domain, site, or OU; select Create; And Link A GPO Here from the shortcut menu.

Creating a GPO on a Computer Without GPMC
To create a Group Policy Object using a computer without GPMC, follow these steps:

1. Launch Active Directory Users and Computers (for domain or OU Group Policy Objects) or Active Directory Sites and Services (for site GPOs).
2. Right-click the object for which you want to create a GPO, and choose Properties from the shortcut menu.
3. Click the Group Policy tab, and then click New.
4. Type a name for the new GPO, and choose from the following buttons:
   - Add To add a link to the new policy.
   - Edit To open the new GPO in the Group Policy Object Editor.
   - Options To set No Override or to disable the GPO.
   - Delete To remove the GPO permanently or remove it from the list. If you choose Remove The Link From The List, the GPO remains in Active Directory but is no longer applied to the particular Active Directory container.
   - Properties To set filtering for the GPO through security groups.
5. Click OK when you're finished.

Inside the Group Policy Object Editor
When you click Default Domain Policy in the Group Policy console tree, the Group Policy Object Editor (GPOE) displays two nodes: Computer Configuration and User Configuration. When you click these nodes, you find that each displays extensions for Software Settings, Windows Settings, and Administrative Templates.

**Note** In GPMC, right-click the Default Domain Policy and select Edit to open GPOE with the policy loaded.

Use the Computer Configuration folders to customize policies for computers on the network. These policies go into effect when the computer is turned on and the operating system starts. Settings in these folders apply to any user who logs on to the computer. For
example, if you have machines in a training room for which you want to enforce a strict environment, the Computer Configuration node is where you make those settings.

The User Configuration node contains settings for customizing environments or setting policies for users on the network. User Configuration policies come into play when a specific user logs on to the network.

**Note**  These settings come into play only when the container being linked to actually contains user or computer accounts. For example, user settings in a GPO linked to an OU that contains only computer accounts will not be applied to users who log on to these computers.

## Managing Group Policy Links

With numerous GPOs on a network, it’s important to keep track of links between GPOs and Active Directory containers such as a domains or OUs. To find out what links exist for a particular GPO, open the Group Policy Object Editor, right-click the GPO, and choose Properties from the shortcut menu. Click the Links tab and then click Find Now to see a list of links to the GPO.

Using GPMC, navigate to Group Policy Objects and select the GPO to view. In the details pane, click the Scope tab to display links. (See Figure 11-3.)
Linking a GPO Using GPMC

To link a Group Policy Object using GPMC, open the Group Policy Management Console. In the console tree, locate the site, domain or organizational unit to which you want to link a GPO and then select one of the following options:

- To link an existing GPO, right-click the domain or organizational unit in the domain, and then select Link An Existing GPO from the shortcut menu. In the Select GPO dialog box, click the GPO that you want to link and then click OK.
- To link a new GPO, right-click the domain or OU and then select Create And Link A GPO Here on the shortcut menu. In the Name box, type a name for the new GPO and then click OK.

Note The Create And Link A GPO Here option is not available for sites because it is unclear in which domain to create the GPO. The user must first create a GPO in any domain in the forest, and then use the Link An Existing GPO option to link it to the site.

Linking a GPO Without GPMC

To link an existing GPO to a domain or organizational unit, open Active Directory Users and Computers. To link to a site, open Active Directory Sites and Services. Right-click the domain, OU, or site to which you want to link a GPO and then follow these steps:

1. Select Properties, and then click the Group Policy tab.
2. To add the Group Policy object to the Group Policy Object Links list, click Add. This opens the Add A Group Policy Object Link dialog box.
3. Click the All tab, click the Group Policy object that you want, and then click OK.
4. In the properties dialog box for the site, domain, or OU, click OK.

Note To link a new GPO, follow the steps in the “Creating a GPO on a Computer without GPMC” section earlier in this chapter.

Setting the Scope of Group Policy Objects

The settings of a GPO are implemented when the GPO is linked to a site, domain, or OU. The sum total of the users and computers to which a GPO applies is called the scope.

A GPO applies to all the users and computers in the Active Directory container to which the GPO is linked unless the user or computer portion of the GPO is disabled. Active
Directory containers being what they are, there are inevitably users and computers in the container that should not have a particular GPO applied. In addition, policies for a particular GPO apply only to users or computers who have Read and Apply Group Policy permissions for that GPO. To filter the application of a GPO, create security groups and assign Read and Apply Group Policy permissions only to the groups to which the GPO applies.

Filtering the scope of a GPO using security groups involves using the Access Control List (ACL) Editor to allow or deny access to the GPO for particular groups.

Table 11-2 shows the settings needed to have a GPO apply or not apply to a security group. The location of the security group doesn’t matter when making the settings. What matters is the location of the users or computers that are members of the security group. If a user or computer doesn’t belong to the Active Directory container that the GPO is associated with (directly, through a link, or by inheritance), no combination of permissions or membership in a security group can force the GPO to apply to that user or computer.

<table>
<thead>
<tr>
<th>Intended Result</th>
<th>Permissions Needed</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>This group policy will be applied to the members of this group.</td>
<td>Apply Group Policy: Allow, Read: Allow</td>
<td>Group Policy will be applied to all members except members who belong to another group with Apply Group Policy or Read set to Deny.</td>
</tr>
<tr>
<td>This group policy will not be applied to members of this group.</td>
<td>Apply Group Policy: Deny, Read: Deny</td>
<td>Group Policy will not be applied to any members of this group, no matter what other groups they belong to.</td>
</tr>
<tr>
<td>Membership in this group should not be a relevant factor in whether this Group Policy is applied.</td>
<td>Apply Group Policy: No setting, Read: No setting</td>
<td>Application of this Group Policy to members of this group will depend on whether members belong to other security groups with Allow or Deny settings.</td>
</tr>
</tbody>
</table>

### Using GPMC to Set the Scope for a GPO

In GPMC, click a GPO or GPO Link, and then select the Scope tab. Under the Security Filtering heading, click Add. In the Enter The Object Name To Select box, type the name of the group, user, or computer that you want to add to the security filter. Click OK.

**Note** If Authenticated Users appears in the Security Filtering section of the Scope tab, select this group and click Remove to ensure that only members of the group or groups you added can receive the settings in this GPO.
Setting the GPO Scope Without GPMC

To set the scope of a GPO when you’re not using GPMC, follow these steps:

1. Open the GPO you want to administer in the Group Policy Object Editor.
2. Right-click the GPO, and choose Properties from the shortcut menu.
3. Click the Security tab as shown in Figure 11-4.
4. Add or remove groups, or edit the settings.
5. Click OK several times when you’re done to close all the open windows.

Delegating Permissions on GPOs

Not every network is of such size and complexity as to require delegation of permissions on GPOs. However, many networks are this complicated, so if you’re considering handing off some of the responsibility for GPOs, here are issues to bear in mind:

- If permission is set to inherit to all child containers, authority delegated at the domain level will affect all objects in the domain.
- Permissions granted at the OU level can affect just that OU or that OU plus its child OUs.
■ Control delegated at the site level is likely to span domains and can influence objects in domains other than the domain where the GPO is located.

■ Always assign control at the highest OU level possible.

Delegating Group Policy Using GPMC

Just about every chore connected with Group Policy can be delegated, including creating, editing, and managing GPOs. However, the right to edit, delete, or modify security is delegated separately from the right to link GPOs. And both of those are separate from permission to create GPOs.

Delegating Permission to Create

Open GPMC, and navigate to the domain where you want to grant permission. In the console tree, select Group Policy Objects. Click the delegation tab (shown in Figure 11-5), and then select the Add button to identify the user or group you want to permit to create GPOs.

![Figure 11-5 Viewing the delegation settings of a GPO](image)

Delegating Permission to Link

Open GPMC, and navigate to the domain where you want to grant permission. In the console tree, click the domain. In the details pane, click the Delegation tab. In the drop-down list, select Link GPOs and click the Add button to identify the user or group you want to give link permission to.
Delegating Permission to Edit, Delete, or Modify Security
Open GPMC, and navigate to the domain where you want to grant permission. In the console tree, select the specific Group Policy Object. In the details pane, click the Delegation tab. Click the Add button to locate the user or group. In the Add Group Or User dialog box (shown in Figure 11-6), select the range of permissions you want to delegate.

Delegating Group Policy Without GPMC
By default, only Domain Administrators, Enterprise Administrators, Group Policy Creator Owners, and SYSTEM can create new Group Policy Objects. So if you want a non-administrator user or group to be able to create GPOs, add that user or group to the Group Policy Creator Owners security group. A nonadministrator member of the Group Policy Creator Owners group can create GPOs and edit those GPOs, but the user has no additional rights regarding other GPOs.

In addition, members of the Group Policy Creator Owners group can’t link GPOs to containers unless they have been explicitly granted the right to do so on a particular site, domain, or OU.

Delegating Permission to Create
To allow a nonadministrator to create new Group Policy Objects, follow these steps:

1. Open Active Directory Users and Computers. In the console tree, click Users.
2. In the details pane, double-click Group Policy Creator Owners.
3. In the Group Policy Creator Owners Properties dialog box, click the Members tab.
4. Click Add, type the name of the user or group of users, and then click OK.

Delegating Permission to Link, Edit, Delete, or Modify Security
Navigate to the properties of a GPO, click Permissions for Authenticated Users, and select the check boxes that correspond to the permissions you want to give.
Disabling a Branch of a GPO

If a GPO has an entire node under User Configuration or Computer Configuration that’s not configured, disable the node to avoid processing those settings. This speeds startup and logon for all users subject to that GPO.

Disabling a Node Using GPMC

Open Group Policy Management Console, and follow these steps:

1. In the console tree, navigate to the domain or OU that contains the GPO.
2. Double-click the domain or OU.
3. Right-click the GPO that contains the user or computer settings you want to disable, point to GPO Status, and then choose one of the following options:
   - Click User Settings Disabled to disable user settings for the GPO.
   - Click Computer Settings Disabled to disable computer settings for the GPO.

   A check mark next to User Settings Disabled or Computer Settings Disabled indicates that the option is in effect.

Disabling a Node without GPMC

To disable either the computer or users portion of a Group Policy, follow these steps:

1. In the Group Policy Object Editor, right-click the GPO and choose Properties from the shortcut menu.
2. On the General tab, select the option to disable the User Configuration or Computer Configuration settings for this GPO.
3. Click OK when you’re finished.

The settings you’ve chosen to disable no longer affect any Active Directory container to which the GPO is linked.

Refreshing Group Policy

Policy changes are immediate, but they are not instantly propagated to clients. Client computers process a policy each time one of the following events happen:

- The computer starts
- A user logs on
- An application requests a refresh
- A user requests a refresh
- The Group Policy refresh interval has elapsed
By default, client computers receive policy updates every 90 minutes, though to prevent multiple computers refreshing at the same time, the actual refresh interval can vary from 90 to 120 minutes.

The value of shorter times between policy refreshes must be measured against the increase in network traffic that’s generated as a result.

To change a Group Policy refresh interval, follow these steps:

1. Open the Group Policy Object in the Group Policy Object Editor.
2. In the console tree, expand Computer Configuration, Administrative Templates, and then System, until you reach Group Policy.
3. In the details pane, double-click Group Policy Refresh Interval For Users.
4. Click Enabled, specify the refresh interval and then click OK.

Because policy can be set at several levels, when you click a policy object, you see both local policy and the policy in effect on the system. These might not be the same if the computer is inheriting settings from domain-level policies. If you make a policy setting and it isn’t reflected in effective policy, a policy from the domain is overriding your setting.

It’s also possible that the policy change hasn’t been refreshed since you made it. To force a policy refresh for the local computer, open a command window and type:

```bash
gpupdate [/target:{computer | user}] /force
```

Use the Target parameter if you want only computer settings or only user policy settings to be refreshed.

---

**Backing Up a Group Policy Object**

A valuable feature, new in Group Policy Management Console, is the ability to back up and restore Group Policy Objects. Regular backups of all GPOs should be part of your overall disaster planning strategy. To back up a GPO, follow these steps:

1. Open Group Policy Management. In the console tree, navigate to Group Policy Objects in the domain that contains the GPO to be backed up.
2. To back up a single GPO, right-click the GPO, and select Back Up from the shortcut menu. To back up all GPOs in the domain, right-click Group Policy Objects and select Back Up All.
3. In the Back Up Group Policy Object dialog box, type the path to the backup location and then click Back Up.
4. After the operation completes, click OK.
Best Practices  Because the only reason to back up GPOs—or anything else for that matter—is to protect data that might have to be restored one day, be sure the back up folder is secure and can be accessed only by authorized administrators.

Restoring a Group Policy Object

Using GPMC, you can restore GPOs that have been backed up. If you back up all the GPOs in a container, you can restore all, some, or one of them at a time.

To restore backed-up GPOs, follow these steps:

1. Open Group Policy Management Console. In the console tree, navigate to Group Policy Objects in the domain that contains the GPO that you want to restore.

2. To restore a previous version of an existing GPO or to restore a deleted GPO, right-click Group Policy Objects and select Manage Backups.

3. In the Manage Backups dialog box, select the GPO to restore and click the Restore button.

When you have a lot of GPOs to sort through, select the box to display only the latest versions of the backed-up GPOs. If you’re unsure which GPO to restore, highlight them one at a time and click View Settings.

Note  A deleted GPO can’t be restored if it’s never been backed up, which is why it’s wise to back up GPOs on a regular schedule. And don’t wait for the schedule when you make major changes in a GPO. Back it up at once.

Using Group Policy for Folder Redirection

Folder Redirection is an extension to Group Policy that allows you to place folders that you choose on the network. For example, you might want to redirect users’ My Documents folders that can become quite large over time. There are real benefits to using this feature, including:

■ Users can log on to different computers and still have access to the redirected folders.

■ If you use roaming profiles, only the network path to the redirected folders is part of the user profile, making logging on and off much faster.
Folders on a network server can be backed up as part of routine maintenance without the users having to do anything extra.

Folders can be redirected to one location for everyone in the Active Directory container affected by the GPO. They can also be redirected to different locations according to security group membership.

**Redirecting to One Location**

By far, the most common form of redirection is to send everyone’s My Documents folder to a single location on a network server. The following steps show how to do this (you can substitute other Windows special folders in the steps to redirect them as well):

1. Create a shared folder on the server.

**Best Practices** Insert a dollar sign ($) at the end of the share name for the folder on the server to prevent the folder from appearing in My Network Places. It will also hide the folder from casual browsers.

2. Open the GPO linked to the Active Directory container containing the users whose folders are to be redirected.

3. In the console tree, click User Configuration, and then Windows Settings, and finally Folder Redirection.

4. Right-click My Documents, and choose Properties from the shortcut menu. (See Figure 11-7.)

![Figure 11-7 Setting Folder Redirection in the GPO](image-url)
5. On the Target tab, select Basic—Redirect Everyone’s Folder To The Same Location. Choose the Target folder location that coincides with the new shared folder on the server and provide a root path, as shown in Figure 11-8.

![Figure 11-8 Settings for the redirection of My Documents folders](image)

6. Click the Settings tab. The following settings are enabled by default:

   - **Grant The User Exclusive Rights To My Documents** The user and the local system have exclusive rights to the folder. No administrative rights are enabled. If this setting is disabled, the permissions that exist on the folder in its present position remain.

   - **Move The Contents Of My Documents To The New Location** The contents of the user’s current My Documents folder are sent to the new location. If this option is disabled, the user has a new, but empty, My Documents folder at the new location.

   - **Policy Removal** The default is to leave the folder in the new location when the policy is removed. If you choose to redirect the folder back to the local user, see the “Removing Redirection” section later in this chapter.

   - **My Pictures Preferences** The My Pictures folder will follow My Documents as a subfolder by default.

7. Click OK when you’re finished.
Redirecting by Group Membership

Special folders can also be redirected based on the user’s membership in security groups. To do so, follow these steps:

1. Create the shared folders at the locations to which the folders will be redirected.
2. Open the GPO linked to the site, domain, domain controller, or OU containing the users whose folders are to be redirected.
3. In the console tree, click User Configuration, and then Windows Settings, and finally Folder Redirection.
4. Right-click the special folder (in this case, My Documents), and choose Properties from the shortcut menu.
5. In the drop-down list, select Advanced – Specific Locations For Various User Groups, and then click Add.
6. In the Specify Group And Location box, type the security group and the location for the redirected folders. Always use a UNC path, even if the folders are to be on the local computer, so that roaming users will be able to see their folders.
7. Click OK. Add more groups and locations as needed.
8. Click the Settings tab. The following settings are enabled by default:
   - **Grant The User Exclusive Rights To My Documents** The user and the local system have exclusive rights to the folder. No administrative rights are enabled. If this setting is disabled, the permissions that exist on the folder in its present position remain.
   - **Move The Contents Of My Documents To The New Location** The contents of the user’s current My Documents folder will be sent to the new location. If this option is disabled, the user will have a new, but empty, My Documents folder at the new location.
   - **Policy Removal** The default is to leave the folder in the new location when the policy is removed. If you choose to redirect the folder back to the local user, see the “Removing Redirection” section.
   - **My Pictures Preference** My Pictures will follow My Documents as a sub-folder.
9. Click OK when you’re finished.

Removing Redirection

When folders have been redirected and later the policy changes, the effect on the folders depends on the combination of choices made on the Settings tab in the special folder’s
Properties dialog box. Table 11-3 shows the various combinations of settings and the outcome when the policy is changed. (Software policy settings are covered in Chapter 28.)

<table>
<thead>
<tr>
<th>Policy Removal Option</th>
<th>Move Contents of Folder to New Location</th>
<th>Outcome When Policy Is Removed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect the folder back to the local user profile location when policy is removed.</td>
<td>Enabled</td>
<td>The folder returns to its user profile location; the contents of the folder are copied back to the original location; the contents are not deleted from the redirected location.</td>
</tr>
<tr>
<td>Redirect the folder back to the local user profile location when policy is removed.</td>
<td>Disabled</td>
<td>The folder returns to its user profile location; the contents of the folder are not moved or copied back to the original location. Warning: this means the user cannot see the folder contents.</td>
</tr>
<tr>
<td>Leave the folder in the new location when policy is removed.</td>
<td>Enabled or Disabled</td>
<td>The folder and its contents remain at the redirected location; the user has access to the contents at the redirected location.</td>
</tr>
</tbody>
</table>

**Using Resultant Set of Policy (RSoP)**

The Resultant Set of Policy (RSoP) tool is a welcome addition to Group Policy because a hazard of creating and configuring GPOs is that the results are sometimes unpredictable and very difficult to troubleshoot. RSoP gathers information on all existing policies to determine the policies in effect and the order in which they are applied.

RSoP has two modes: logging mode and planning mode. In planning mode, RSoP helps construct a “what if” scenario so that you can test the effect of a new policy or test policy precedence. In logging mode, RSoP can tell you what policies are being applied to a particular user and can help you discover policies that should be removed or repaired.

**Running an RSoP Query**

An RSoP query can be run on a site, a domain, a computer account, a user account, or an OU. Both planning mode and logging mode have options to assist in configuring your query.

For a query using the Group Policy Object Editor, Add the RSoP snap in to a Microsoft Management Console. In the console tree, right-click Resultant Set of Policy and select Generate RSoP data to launch the Resultant Set of Policy Wizard. On the Mode Selection page, select the mode.
If you’re using GPMC, right-click Group Policy Modeling and select Group Policy Modeling Wizard. You’ll need to specify the domain controller on which the query is to be run, and then follow the steps in the next sections based on the operation you’re performing.

---

**Note** To query a site, open Active Directory Sites and Services, right-click the site and select All Tasks and then Resultant Set of Policy.

**A Planning RSoP**

The planning mode in RSoP simulates what the effect will be of change in your system. If you’re thinking of moving, adding, or deleting a group or making any changes to group policy, RSoP tells you what the result of proposed changes will look like. When you select Planning Mode as described in the previous section, the Resultant Set of Policy Wizard starts. Follow these steps:

1. In the User And Computer Selection window use the Browse buttons to specify the user, computer, or container to be analyzed, and then click Next. The following simulation options are on the Advanced Simulation Options page.
   - **Slow network connection** Some policies do not apply when a dial-up or other slow connection is used. Choose this option to simulate a slow connection.
   - **Loopback processing** If you’re in a situation where you must modify the user policy based on the computer the user logs on to, loopback processing simulates the application of the GPOs to any user who logs on to a computer controlled by alternate user policy settings. You can choose to replace the user’s usual policies or merge the new with the existing policies.
   - **Site** Specifies the site and physical location of the subnet to use. Use this setting to test startup or logon events on a different subnet.

   After making your selections, click Next.

2. To simulate changes to the user or computer location, enter the new location and click Next.

3. In the list of Security groups, add or remove groups to simulate the result of policies based on changes in security group membership. Click Next.

4. The next page is Computer Security Groups. Here you can simulate changes to the computer’s security group memberships. Click Next.

5. On the WMI Filters For Users page, you can link Windows Management Instrumentation (WMI) filters to arrive at resulting policy based on whether the user meets the criteria specified in all or some WMI filters. Click Next.
6. On the WMI Filters For Computers page, you can link Windows Management Instrumentation (WMI) filters to arrive at resulting policy based on selected information such as installed software. Click Next.

7. The next page summarizes the selections made so far. Review it carefully. There are a lot of steps in this wizard, and one misstep can make the results useless.

8. Click Next. When the operation is complete, select Finish.

The RSoP will appear in a Microsoft Management Console (as shown in Figure 11-9), which you can examine, compare to other RSoP planning results, and save for future reference.

Figure 11-9  The output of a planning RSoP

Note  To change a setting in an existing RSoP, right-click the query in the console tree and select Change Query.

A Logging RSoP
In logging mode, RSoP reports on current policy settings as they apply to users and computers. Planning mode shows the administrator the outcome of a possible future change, but logging mode is all about what's going on now. A logging RSoP is what you need to discover which policies are applied to a particular user or computer or to investigate why certain policies are not working as expected.
When using Group Policy Object Editor, just choose Logging mode on the Mode Selection page of the Resultant Set of Policy Wizard.

In the Group Policy Management Console, right-click Group Policy Results to launch the Group Policy Results Wizard.

**Note** To run RSoP on a remote computer, you must be a member of Domain Admins, be a member of Enterprise Admins, or have had the right to generate RSoP delegated to you. You must be a member of Enterprise Admins to cross domain boundaries in a forest.


**Summary**

The success of a network is judged by both the availability of needed information and resources and the restriction and protection of others. This chapter has explored the options available to the administrator for configuring shares, permissions, and group policy through Windows Server 2003. The next chapter covers day-to-day administrative tasks and how to simplify and streamline these tasks for maximum efficiency.
Part III
Network Administration

Chapter 12
Managing Daily Operations .................................................. 323
Chapter 13
Using Scripts for Consistent Administration ............................. 351
Chapter 14
Installing and Configuring Active Directory ............................ 377
Chapter 15
Managing Active Directory .................................................. 433
Chapter 16
Understanding TCP/IP .......................................................... 469
Chapter 17
Administering TCP/IP ......................................................... 495
Chapter 18
Implementing Disk Management ............................................ 539
Chapter 19
Using Clusters ..................................................................... 575
Chapter 20
Managing Storage ............................................................... 613
A network administrator’s job consists of masses of details, and if you’re to cope, you must find ways of handling and tracking them. Microsoft Windows Server 2003 supplies plenty of tools for doing this, including ones that allow you to delegate tasks to other users or groups, use scripts to automate tasks, and schedule tasks to run periodically. Nevertheless, administering a network is still largely a process of planning and organization, and in that area there’s no substitute for brain power. This chapter discusses some of the tools that can help in the daily business of network management.

Using the Microsoft Management Console

The Microsoft Management Console (MMC) is a powerful addition to the system administrator’s arsenal. The MMC works as a packager of system tools, enabling the system administrator to create specialized tools that can then be used to delegate specific administrative tasks to users or groups. Saved as MMC (.msc) files, these custom tools can be sent by e-mail, shared in a network folder, or posted on the Web. With system policy
settings, they can also be assigned to users, groups, or computers. The tools are flexible enough to be modified, scaled up or down, and generally shaped for any use to which you might want to put them.

**Convenience Consoles**

Windows Server 2003 comes with three Convenience Consoles, which are ready-made packages of tools. All three of these are listed in the Administrative Tools menu. If you haven’t installed Administrative Tools, see the “Administrative Tools” section later in this chapter. Following are the names and descriptions of the three consoles:

- **Active Directory Management** This console contains all the tools commonly used to administer Active Directory. These tools are Active Directory Users and Computers, Active Directory Domains and Trusts, Active Directory Sites and Services, and Domain Name System (DNS).

- **IP Address Management** This console consists of the tools used to manage IP address resolution and assignment: Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and Windows Internet Naming Service (WINS).

- **Public Key Management** This console includes the tools to manage certificates, certification authorities, and registration authorities that are part of your public-key infrastructure. The tools are Certificate Authority, Certificate Templates, Certificates for Local Computer, and Certificates for Current User.

In addition, you’ll probably create your own Convenience Consoles based on the needs of your network. To build a custom MMC, you can either start with an existing console and modify it or start from scratch.

**Creating an MMC-Based Console with Snap-Ins**

Building your own tools with the MMC standard user interface is a straightforward process. The next few sections walk you through the creation of a new console and describe how to arrange its administrative components into separate windows.

**Note** In the following steps, you should not have the console window or any other window in the MMC you are creating maximized.

1. Click Start and select Run. In the Open text box, type `mmc` and then click OK. An empty MMC window opens, as shown in Figure 12-1, ready for you to add snap-ins.
2. From the File menu, select Add/Remove Snap-In. (The menu commands on the menu bar at the top of the MMC window apply to the entire console.) The Add/Remove Snap-In dialog box opens. Here you can choose which snap-ins to place in the console file and enable extensions. In the Snap-Ins Added To box, accept the default, Console Root.

3. Click Add. This opens a dialog box listing the snap-ins installed on your computer. (See Figure 12-2.)
4. Select a snap-in to see a description of its function. Double-click a snap-in to add it to the console. For this example, we’ll add Computer Management. Select the computer to manage, as shown in Figure 12-3.

5. Select the Local Computer option, and select the Allow The Selected Computer To Be Changed When Launching From The Command Line check box. These options are common to many of the snap-ins. Click Finish.

6. From the Add Standalone Snap-In dialog box, select Event Viewer and click Add. As you did before, select the Local Computer option and select the Allow The Selected Computer To Be Changed When Launching From The Command Line check box. Click Finish, and then close the list of available snap-ins. The Add/Remove Snap-In dialog box lists two snap-ins: Computer Management (Local) and Event Viewer (Local).

7. Click the Extensions tab. By default, the Add All Extensions check box is selected, which means that when this console is opened on a particular machine, all extensions that are locally installed on that machine will be used. If this check box isn’t selected, only extensions that are selected on the list of available extensions will be loaded.

8. Click OK to close the Add/Remove Snap-In dialog box. The Console Root window now has two snap-ins, rooted at the Console Root folder.

9. Save the console by choosing Save from the Console menu. You are prompted for a name—be as descriptive as possible. The file is saved in the Administrative Tools
folder by default. This folder is part of your profile, so an added benefit is that if you use roaming profiles, any tools you create go with you. See Chapter 9 for information on creating roaming profiles.

Note Windows Server 2003 R2 includes a new version of MMC – MMC v3. By default, the new interface is turned off, and you’ll see the screens described above when you go to create your own console. You can enable the new, three pane, interface by adding the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MMC\UseNewUI. Frankly, we don’t see any particular reason to do so, but go ahead and try it. The one area where we see a definite improvement is in the new UI for adding and removing snap-ins, but the new action pane doesn’t improve anything for us.

Customizing the Layout of a Console
After you’ve added the snap-ins, you can provide different administrative views in the console by adding windows. To create one window for each of the snap-ins, follow these steps:

1. In the left pane of the console window, right-click the Computer Management folder and select New Window From Here from the shortcut menu. This opens a new Computer Management window rooted at the Computer Management snap-in. Click the Show/Hide Console Tree toolbar button, shown in Figure 12-4.

![Figure 12-4 The Show/Hide Console button](image)

2. In the Console Root window, right-click the Event Viewer folder and select New Window From Here. Click the Show/Hide Console Tree toolbar button.

3. Close the original Console Root window. From the Window menu, choose Tile Horizontally. The console window will look like Figure 12-5.
Figure 12-5 A customized console

Note that the buttons and menus apply only to the active window. Remember to save your console file after completing the changes.

Setting Options for a Console File
When creating consoles for workgroup managers or other users, you can restrict how the console is used. Console options can be set so that users can access only the tools that the administrator allows. To set console file options, follow these steps:

1. With the console open, select Options from the File menu. This opens the Options dialog box.

2. Click the Console tab. Choose one of the following console modes:

   - **Author Mode** This mode has no restrictions. The user can access all parts of the console tree as well as change this console file at will.

   - **User Mode—Full Access** The user can access all parts of the console tree but cannot make changes that affect functionality. Cosmetic changes, such as the arrangement of windows, are saved automatically.

   - **User Mode—Limited Access, Multiple Windows** The user can access only the parts of the console that were visible at the time the console file was saved. Users can create new windows but can’t close existing ones.

   - **User Mode—Limited Access, Single Window** The same as the previous mode, except that only one window is visible. Users cannot create new windows.
3. In all but author mode, you can also select the Do Not Save Changes To This Console option, so that the console always opens in the same view. You can also select the Allow The User To Customize Views option. This allows the user to add windows rooted in the tools in the MMC.

4. Click OK, and save the console file.

Modifying Console Files

After you’ve saved a console file in any mode other than author mode, the Console menu no longer includes options for disallowed actions, such as adding another snap-in. This prevents the user from changing the settings.

To modify a console file, open a command-prompt window and type `mmc /a`. The `/a` switch specifies author mode, overriding any user mode setting, and opens the console window, from which you can open any console file and make changes.

---

**Note**  
The system administrator can and should set user profiles to disallow the use of the `/a` switch to ensure that inappropriate modifications can’t be made. Or use Group Policy to disable it by enabling the Restrict The User From Entering Author Mode policy in User Configuration\Administrative Templates\Windows Components\Microsoft Management Console.

Distributing and Using Consoles

As mentioned earlier, the default location for saved console files is the Administrative Tools folder. Console files can be distributed in a variety of ways. You can copy a console file to a shared folder on the network, or you can mail it to another person by right-clicking the file, pointing to Send To, and selecting Mail Recipient. When you assign a console to be used by a particular person, be sure that the person’s user profile includes permission to access the tools and services in the console. The user also has to have any administrative permissions necessary to use the system components administered by the console.

If you know the location of a console, you can open it using Windows Explorer by clicking it as you would any other file. You can also open it from the command line. For example, to open the DHCP management console from the command line, type `dhcpmgmt.msc`. (For consoles that are not on your path, you’ll need to specify the path to the console.)

Using MMC for Remote Administration

MMC-based tools are admirably suited for remote administration. You can easily construct a console to administer a number of computers or a single machine. This section describes how to create a console that can be used to remotely administer another
computer. The console includes the Services snap-in, which manages system services, and the Event Viewer snap-in, which allows access to the various event logs. To create this remote administration console, follow these steps:

1. Click Start, and then select Run. In the Open text box, type `mmc` and then click OK. An empty MMC window opens.

2. From the File menu, select Add/Remove Snap-In. The Add/Remove Snap-In dialog box opens.

3. Click Add to open the Add Standalone Snap-In dialog box.

4. Select Services, and then click Add.

5. In the This Snap-In Will Always Manage area, select Another Computer and then click Browse. This opens another Select Computer dialog box.

6. Highlight the computer you want this snap-in to manage, and then click OK. Click Finish.

7. Repeat steps 4 through 6, except choose the Event Viewer snap-in. Close the Add Standalone Snap-In dialog box. Click OK in the Add/Remove Snap-In dialog box.

8. At this point, the console will look like the one in Figure 12-6. Save it under a descriptive name. You can use this console to view events on the remote machine and to start and stop services.

![Figure 12-6](image-url) A console to remotely administer another computer

As you can see, consoles can be configured in dozens, if not hundreds, of different ways and then distributed. Snap-ins for every imaginable function will increasingly be available from Microsoft as well as third-party suppliers.
Note Because consoles are excellent tools for organizing and delegating administrative chores, examples of their use can be found in many other chapters of this book.

Using the Secondary Logon

Recommended administrative practice dictates that an administrator be logged on to a privileged account (one with administrative rights) only while doing chores that require privileges. For ordinary work, the administrator is supposed to log off from the privileged account and then log on again to an ordinary account. Of course, 10 minutes later a situation usually arises requiring use of the privileged account, making it necessary to log off from the ordinary account and log back on to the administrator account, with the process reversed again a few minutes later when the administrative chore is completed.

After a few days of this, even the most security-conscious person begins to toy with the idea of logging on to the administrator account and staying there. In time, most administrators succumb to the temptation and stay in the privileged account most of the time.

This practice makes Microsoft Windows 2000 and Windows Server 2003 systems highly susceptible to Trojan-horse attacks. Using an administrator account while running any browser exposes your entire network to potential problems. Even with the very best antivirus and antispyware protection, and a full-featured firewall, it is a bad idea to browse the Internet with an administrative account. A Web page with Trojan-horse code can be downloaded to the system and executed. The execution, done in the context of administrative privileges, can cause considerable harm, including a reformatted hard disk, the capture of critical user and customer financial information, or the creation of a new user with administrative access. It’s like handing the keys to your network to a complete (and known to be malicious) stranger.

Note For an excellent discussion of the reasons why users should not run programs using administrator credentials, and how to work around the problem of installing and running programs that require administrator credentials in order to work, see the weblog of Aaron Margosis at http://blogs.msdn.com/aaron_margosis/default.aspx.

This problem was finally addressed in Windows 2000 with the Run As feature (enabled by the Runas service, which is on by default). This feature, also included in Windows Server 2003, allows you to work in a normal, nonprivileged account and launch applications or tools while using the credentials of a different account (most likely your administrator account) without logging off and then logging back on again.
To use the Run As feature, create an ordinary user account for your own use (if you don’t have one already). Make sure that the user account has the right to log on locally at the machine you want to use.

**Note**  Windows Server 2003 views all domain controllers as special cases. On a domain controller, by default, users can’t log on locally. Chapter 9 includes more information on creating user accounts and granting rights.

### Opening Programs Using Run As

To open a program or system tool using a user account (most likely an account with Administrator privileges) different than the one you are in, use the following steps:

1. Right-click the desired program, Control Panel tool, or Administrative Tools icon.
2. Choose Run As from the shortcut menu. (See Figure 12-7.)
3. Select The Following User, and enter the user name and password for the account you want to use.
4. Click OK to open the program or tool using the specified account’s credentials.

![Figure 12-7 Choosing the Run As options](image)

You can also choose to run the program using your current account but with restricted access by selecting the Protect My Computer And Data From Unauthorized Program Activity box.

**Note** Some administrative tasks, such as setting system parameters, require an interactive logon and do not support Run As.
Making Shortcuts to Run As

The idea of Run As is to encourage administrators to work outside the administrator's account; configuring useful shortcuts makes this more likely to happen. Perform this task using an account without administrative rights. Right-click an open area of the desktop, choose New, and then choose Shortcut. Table 12-1 shows some examples of useful shortcuts.

Table 12-1 Useful Run As shortcuts

<table>
<thead>
<tr>
<th>A Shortcut to</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>A command prompt with local administrative privileges.</td>
<td>runas /user:AdministratorAccountName@Computer-Name cmd</td>
</tr>
<tr>
<td>A command prompt with domain administrative privileges but no profile.</td>
<td>runas /user:DomainAdminAccountName@Domain /noprofile cmd</td>
</tr>
<tr>
<td>A command prompt with domain administrative privileges. This command prompt also loads the account profile.</td>
<td>runas /user:DomainAdminAccountName@Domain cmd</td>
</tr>
<tr>
<td>Active Directory Users and Computers with domain administrative credentials.</td>
<td>runas /user:DomainAdminAccountName@Domain &quot;mmc %windir%\system32\dsa.msc&quot;</td>
</tr>
<tr>
<td>Performance Monitor with enterprise administrative credentials.</td>
<td>runas/user:EnterpriseAdminAccountName@Domain &quot;mmc %windir%\system32\perfmon.msc&quot;</td>
</tr>
<tr>
<td>Command prompt to administer server in another forest.</td>
<td>Runas /netonly/user:Domain\AdministratorAccountName cmd</td>
</tr>
</tbody>
</table>

Keep a few of the most frequently used shortcuts on your desktop and you'll find it easier to stay in your less-privileged account most of the time.

Using Runas for Printers or Control Panel

Some applications, such as the Printers folder and Control Panel, are launched from the shell at the time of logon, so if you’re logged on as an ordinary user, the Control Panel functions stay in that context (although you can open individual tools with a different account using the runas command as shown in Table 12-1).

To stop the shell and start it again as an administrator so that you can use functions such as the Printers folder, follow these steps:

1. Right-click the taskbar, and choose Task Manager from the shortcut menu.
2. Click the Processes tab. Select Explorer.exe, and click End Process. A warning message appears. Click Yes. The entire desktop, except for Windows Task Manager and any active applications, disappears.
3. Select the Applications tab in Windows Task Manager, and then click New Task.

4. In the Create New Task box, type `runas /user:<domain\username> explorer.exe`. As before, `username` is the account with administrative privileges. If you’re logged on locally, use the command `runas /user:<machinename\username> explorer.exe`.

5. Enter the password for the user name. The desktop, along with the taskbar, returns. This desktop is in the security context of the user name you specified in the command.

To return to the ordinary user’s desktop, use Task Manager again to shut down Explorer.exe. Then start a new instance by typing `explorer.exe` (without runas, so that Internet Explorer is restarted in the original security context) in the Create New Task dialog box.

---

**Important** Don’t close Task Manager while you’re working in the desktop’s administrative context—just minimize it to the taskbar. Closing Task Manager can have unpredictable results.

---

**Note** You can start a separate copy of Windows Explorer using the `/separate` switch. Combine this with runas to open Explorer in a different user context. Or, if you’re on an x64 machine and want to run a copy of 32-bit Explorer, use it to run the 32-bit version of Explorer.exe that is in the `%windir%\SysWOW64` directory.

---

**Administrative Tools**

Most tools you’ll need for managing a Windows Server 2003 network come as part of the Windows Server 2003 package, but only a few of them are automatically installed along with the operating system.

**Installing Administrative Tools Locally**

To install the full set of Administrative Tools locally, double-click the Adminpak.msi file in your `%windir%\System32` folder on a 32-bit version of Windows Server 2003, or in the `%windir%\SysWOW64` folder on a 64-bit version. (It’s also in the \i386 folder on the Windows Server 2003 CD-ROM.) This starts the Administrative Tools Setup Wizard, which installs the tools (and later removes them and reinstalls them, if you wish). Click Next to proceed with the installation.

---

**Note** The latest version of the Adminpak.msi is always available for direct download from the Download Center on Microsoft.com. Also, see Knowledge Base article 304718 for which versions of Adminpak.msi work in which environments.
Making Administrative Tools Available Remotely

To make Administrative Tools available to others on your network, you can assign the tools to other computers or publish them in Active Directory. Chapter 28 covers the process of assigning and publishing software to users using Group Policy.

Support Tools

The Windows Server 2003 Support Tools are immensely valuable because they provide functionality not otherwise available in the operating system. You’ll probably never use some of the tools, but a few will undoubtedly turn out to be priceless. This section discusses a few of these utilities. You can view a complete list by choosing Tools Help from the Windows Support Tools menu.

If you don’t see the Support Tools on your Programs menu, you’ll need to install them. To install the Windows 2003 Support Tools, insert the Windows Server 2003 CDROM. Open the Support folder and then the Tools folder. Double-click Suftools.msi to start the installation.

Note: The latest version of the Support Tools is always available from the Download Center on http://www.microsoft.com/downloads/.

Note: If your environment includes multiple server architectures, be sure to use the appropriate CD-ROM for the architecture of the server on which you are installing the tools.

Tools have been both added to and removed from Support Tools. To view the list, search for New And Removed Support Tools in the Help and Support Center.

Automating Chores with Scripts

Out of necessity, most network administrators quickly acquire scripting skills. There aren’t enough hours in the day to do everything manually, even if that were desirable. In addition, good scripts are like any program: once the information is entered correctly, there’s no need to worry about it until something external changes.

Through ActiveX, Windows Server 2003 enables scripting options using Microsoft Visual Basic, Scripting Edition (VBScript); JScript; or Perl. Previously, the only native scripting language supported by Windows was the MS-DOS batch language, and many administrators undoubtedly continue to use batch scripts because they’re very small and very
fast. Why use anything else if a batch file will do the job? You shouldn’t. However, in a large enterprise or for more complicated scripts, a more sophisticated scripting language is in order.

The Windows Script Host (WSH) is built into Windows Server 2003, Windows 2000, Windows XP Professional, and Windows 98. In addition, Windows 95 and Windows NT can run WSH, so scripts are portable across the Windows spectrum. Scripts run under WSH using Wscript.exe and Cscript.exe. Wscript.exe runs in the background, and Cscript.exe runs at the command prompt. To run a script from the command line, the syntax is

```
Cscript <scriptname.extension> [options] [arguments]
```

To view the entire list of host options, type `Cscript //?` at a command prompt. The most important options are listed here:

- `/B` Specifies batch mode; script errors and prompts are not displayed.
- `/D` Enables active debugging.
- `/T:nn` Indicates the maximum time in seconds that the script is permitted to run.

WSH is useful for logon and logoff scripts that can be assigned to users—individually or as a group—or to computers. The other important use for WSH is the creation of user accounts, a tedious process at best and, in a large enterprise, quite impossible without scripts.

Chapter 13 is all about using scripts.

---

**Auditing Events**

Auditing certain computers, users, and operating system events is a necessary part of network administration. You choose what is to be audited and then, by reviewing the event logs, track usage patterns, security problems, and network traffic trends. Beware of the impulse to audit everything, however. The more events you audit, the bigger the logs. Reviewing huge event logs is a painful chore, and eventually no one looks at them anymore. These logs can take up enormous amounts of space. Therefore, it’s critical to decide on an auditing policy that protects your network without creating a large administrative burden. Also bear in mind that every audited event results in a small increase in performance overhead.

By default, all auditing categories are turned off when Windows Server 2003 SP1 or later is installed except for success audits of logon events. Table 12-2 lists the categories of events that can be audited.
Every audited event tells you something, but it’s not always something you need to know. For example, auditing successful logons and logoffs might reveal the use of a stolen password, or it might just produce countless pages showing that your duly authorized users are logging on and off as expected. Auditing logon failures, however, will definitely be rewarding if someone is trying a random password hack.

Before you can audit access to Active Directory objects (which is described in the next section), you must turn on the Audit Policy setting by using Group Policy. To enable auditing of any of the categories in Table 12-2, open the Default Domain Policy MMC if you have one; otherwise, follow these steps to enable auditing for all computers in the domain:

1. Launch Active Directory Users and Computers.
2. Right-click the domain name in the console tree, and choose Properties from the shortcut menu.
3. Click the Group Policy tab and then click Edit.
4. In the console tree, click your way through Computer Configuration, Windows Settings, Security Settings, and Local Policies to reach Audit Policy, as shown in Figure 12-8.

### Table 12-2 Auditing categories

<table>
<thead>
<tr>
<th>Event Category</th>
<th>Activated When</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account logon events</td>
<td>A domain controller receives a logon request</td>
</tr>
<tr>
<td>Account management</td>
<td>A user account or group is created or changed</td>
</tr>
<tr>
<td>Directory service access</td>
<td>An Active Directory object is accessed</td>
</tr>
<tr>
<td>Logon events</td>
<td>A user logs on or logs off</td>
</tr>
<tr>
<td>Object access</td>
<td>An object is accessed</td>
</tr>
<tr>
<td>Policy change</td>
<td>A policy affecting security, user rights, or auditing is modified</td>
</tr>
<tr>
<td>Privilege use</td>
<td>A user right is used to perform an action</td>
</tr>
<tr>
<td>Process tracking</td>
<td>An application executes an action that is being tracked</td>
</tr>
<tr>
<td>System events</td>
<td>A computer is rebooted or shut down or another event occurs that affects security</td>
</tr>
</tbody>
</table>

Every audited event tells you something, but it’s not always something you need to know. For example, auditing successful logons and logoffs might reveal the use of a stolen password, or it might just produce countless pages showing that your duly authorized users are logging on and off as expected. Auditing logon failures, however, will definitely be rewarding if someone is trying a random password hack.

Before you can audit access to Active Directory objects (which is described in the next section), you must turn on the Audit Policy setting by using Group Policy. To enable auditing of any of the categories in Table 12-2, open the Default Domain Policy MMC if you have one; otherwise, follow these steps to enable auditing for all computers in the domain:

1. Launch Active Directory Users and Computers.
2. Right-click the domain name in the console tree, and choose Properties from the shortcut menu.
3. Click the Group Policy tab and then click Edit.
4. In the console tree, click your way through Computer Configuration, Windows Settings, Security Settings, and Local Policies to reach Audit Policy, as shown in Figure 12-8.

![Figure 12-8 Categories of events for auditing](image-url)
5. Right-click the event category you want to audit, and choose Properties from the shortcut menu.

6. In the dialog box that opens, select the check box to define the setting and select the option to audit successful attempts, failed attempts, or both.

**Audit Settings for Objects**

Assuming that you’ve turned on a policy setting for auditing an Active Directory object, create audit settings for objects by following these steps:

1. Right-click the object you want to audit, and choose Properties from the shortcut menu. Click the Security tab.

2. Click Advanced, and then click the Auditing tab.

3. Click Add to set up auditing for a new group or user. Make your selection and click OK.

4. Select the events you want to audit, as shown in Figure 12-9. Table 12-3 lists the options and their definitions.

![Figure 12-9 Selecting events to be audited](image)

5. Click OK when finished.

**Note** By default, audit settings are inherited by child objects. The Auditing tab of the Access Control Settings dialog box includes a check box for allowing inheritable auditing entries. Clear this check box and the audit settings for the object remain constant, even if the parent object’s audit settings are changed. In addition, clearing this check box removes any audit settings that have already been inherited. The second check box in this tab resets existing auditing and allows audit entries to be inherited from the parent object once again.
Auditing Advisory

Windows Server 2003 allows such granularity that it’s possible—actually easy—to create a real morass when selecting audit settings. So many items can show up in the event log that really important issues might be lost in the crowd. Be very careful when deciding what events need to be audited, and audit as few as is reasonable. You can always add events later as circumstances dictate.

Viewing Event Logs

Event logs must be viewed with regularity for auditing to have any effect. To view the security log, open Event Viewer from the Administrative Tools folder and then click Security. Double-click any entry to see more information about it. The security entries in Figure 12-10 occurred in the span of about a minute because the object being audited was set to audit successful events. Of course, you’ll generally learn more from auditing failed events than from auditing successful ones, but this does demonstrate the need to choose your auditing battles carefully.
Figure 12-10  Viewing the security log

Searching Event Logs

No matter how selective you are, the event logs will mix all sorts of information together, making searches for specific information difficult. To search for a specific type of event, select the log in Event Viewer, and choose Find from the View menu. In the Find dialog box, shown in Figure 12-11, select the type or types of events you want returned. Table 12-4 describes the filtering options for the event logs.

Figure 12-11  Searching for specific events in a log
Filtering Event Logs

If you don’t have enough specific information to locate what you need, you can filter an event log for certain types of information. To use event log filtering, follow these steps:

1. Launch Event Viewer from the Administrative Tools folder.
2. Right-click the log you want to search, and choose Properties from the shortcut menu.
3. Click the Filter tab. Table 12-4 describes the fields in this tab. Click OK when you’re ready to start filtering.
4. The log appears, filtered as you requested. To view the full, unfiltered log again, return to the Filter tab and click Clear.

Table 12-4 Options for filtering event logs

<table>
<thead>
<tr>
<th>Option</th>
<th>Use to Search or Filter for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>Notification that some major operation has been performed successfully.</td>
</tr>
<tr>
<td>Warning</td>
<td>Notification of some problem or potential problem. Warnings might or might not be significant. For example, replication performed after repeated tries will generate a warning.</td>
</tr>
<tr>
<td>Error</td>
<td>Notification of an important event. Errors signify a loss of data or a loss of function. For example, failure of a service to start during bootup will generate an error.</td>
</tr>
<tr>
<td>Success Audit</td>
<td>Events audited for success.</td>
</tr>
<tr>
<td>Failure Audit</td>
<td>Events audited for failure.</td>
</tr>
<tr>
<td>Event Source</td>
<td>A source for an event, such as a system component or a program.</td>
</tr>
<tr>
<td>Category</td>
<td>Events by category, such as logon/logoff, policy change, or process tracking.</td>
</tr>
<tr>
<td>Event ID</td>
<td>The specific ID number assigned to each logged event.</td>
</tr>
<tr>
<td>User</td>
<td>A specific user.</td>
</tr>
<tr>
<td>Computer</td>
<td>A specific computer.</td>
</tr>
<tr>
<td>From</td>
<td>Events after a specific date. The default is the first date in the log. You can click the drop-down box to select events on a specific date.</td>
</tr>
<tr>
<td>To</td>
<td>Events before a specific date. The default is the last date in the file.</td>
</tr>
</tbody>
</table>

Setting the Size of Event Logs

When an event log is full, a dialog box pops up to notify you. If this happens often, you might want to reduce the number of items being reported or increase the size of the log. To set event log options, follow these steps:

1. Launch Event Viewer from the Administrative Tools folder.
2. Right-click the log you want to configure and choose Properties.

3. In the General tab, set the options you want. Under When Maximum Log Size Is Reached, there are three options:
   - If you don’t archive this log, select Overwrite Events As Needed.
   - If you archive this log at regular intervals, you can select the Overwrite Events Older Than option. Fill in the appropriate number of days.
   - Do Not Overwrite Events, the last option, means that the log must be cleared manually. When the maximum log size is reached, new events are simply not recorded.

4. Click OK when you’re finished.

---

**Note** To set limits for a large number of machines—a department or a whole domain—use Group Policy.

---

**Calling a Halt When the Log Is Full**

Maybe you are so security-conscious that none of the event log options are acceptable. If you absolutely, positively must not lose a single security event, you can set the computer to halt when the security log is full. A registry change is necessary to make this happen. First, set Event Log Wrapping to either Do Not Overwrite Events or Overwrite Events Older Than \( n \) Days. Then start Regedit.exe, proceed to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\CrashOnAuditFail, and change the value to 1.

This setting takes effect after a reboot; then, when the log is full, the system simply stops. After restarting, only administrators are able to log on until the security log is cleared. This is obviously a drastic measure, but if you absolutely must retain an audit trail on a particular server, this is one way to ensure that.

---

**Archiving Event Logs**

If you will be using event logs to track system usage trends, you must save them. To archive an event log, launch Event Viewer from the Administrative Tools folder and click the log you want to archive. Then, from the Action menu, choose Save Log As. If you save the file in the event log format (.evt), it can be reopened in Event Viewer, and all the binary data for each event is retained. You can also save logs as .txt files or in
Delegating Control

Obviously, one of the simplest ways to minimize your administrative chores is to delegate them. In a Windows NT network, the usual way to grant broad administrative rights was to make users members of the Domain Admins group. You could also parcel out administrative rights through some combination of other groups such as Print Operators or Server Operators.

These groups are still available, but Windows Server 2003 makes delegation even simpler, allowing you to assign responsibility for management of some portion of the namespace to another user or group. The recipient of the delegated authority can have complete administrative control within the area chosen but not the sweeping administrative rights inherent in being a member of the Domain Admins group.

Assign control by organizational unit (OU) whenever possible, because assigning permissions at the object level quickly becomes too complicated to be worthwhile. Records of security assignments are critical, so keep track of all delegations. To delegate control, use the Delegation of Control Wizard, which always assigns permissions at the OU level. (Detailed descriptions of permissions are provided in Chapter 10. For more on the planning and deployment of security policies, see Chapter 21 and Chapter 22.) To use the wizard, follow these steps:

1. Launch Active Directory Users and Computers from the Administrative Tools folder.
2. Expand the domain node, right-click the container for which you want to delegate control, and choose Delegate Control from the shortcut menu. This starts the Delegation of Control Wizard. Click Next.
3. Click Add to select the user or group to be granted control. Make your selection from the Select Users, Computers, Or Groups page.
4. In the Tasks To Delegate page, shown in Figure 12-12, select the tasks that you want to delegate. Select predefined tasks, or click Create A Custom Task To Delegate. Click Next.
5. If you selected a predefined task, you’re essentially finished. Review the summary and click Finished.
Figure 12-12 Choosing the tasks to be delegated

If you selected Create A Custom Task To Delegate, you’re presented with more specific choices about what objects you’re delegating control on and the specific permissions to be granted. When those choices are made, you’ll see a summary of the delegation. Click Finished.

Using Task Scheduler

It’s true that you could—and still can—schedule tasks using the AT command, as described later in this chapter, but Task Scheduler provides a graphical interface and is much easier to use. Tasks can be scheduled during off-hours to run repeatedly. The Task Scheduler service is started at bootup and runs in the background. To use Task Scheduler, open Control Panel, double-click the Scheduled Tasks folder, and then follow these steps:

1. In the Scheduled Tasks window, double-click the Add Scheduled Task entry. This starts the Scheduled Task Wizard. Click Next.

2. Select a program from the page, or click Browse to locate another program. Click Next.

3. Supply a name for the task, and then indicate how often you want it performed. Click Next.

4. Select the time of day you want the task performed. Depending on the timing you’ve selected, you’ll also need to specify one of the following:

   - **Daily Task** Every day, every n days, or weekdays only.
❑ **Weekly Task**  Every \( n \) weeks; supply the day of the week.

❑ **Monthly Task**  Select the day of the month, and select which months.

5. Supply the user name and password for the user who will be scheduling tasks. Note that the account you specify must have the privileges necessary to run the task. For example, if you’re scheduling a backup program, the user must have backup rights. Click Next.

6. If you need to specify parameters for the task being scheduled, select the Open Advanced Properties check box and then click Next.

7. Make the necessary changes and click OK.

---

**Important**  For tasks to run as expected, it’s important that the computer’s date and time be set correctly.

Many programs will start to run in Task Scheduler and then pause, waiting for input that never comes—or input that comes much later, when someone looks at the machine to see what’s going on. To make sure you have all the parameters for a task to be able to run successfully, open a command prompt and type `program_name /?`. Then right-click the task in the Scheduled Tasks window and choose Properties from the shortcut menu. Enter the necessary parameters in the Run text box and click OK.

You might want to schedule a task to run right away so that you can test its performance. If a task is scheduled by a user and that user isn’t logged on at the scheduled time, the task still runs in the background and is not visible.

---

**Note**  Unfortunately, the Windows Server 2003 disk defragmenter utility doesn’t support scheduled operation. To schedule a defrag operation, you can either purchase a commercial defrag program that supports scheduling, such as Raxco’s PerfectDisk, which runs on both 32-bit and x64 versions of Windows Server 2003, or you can create a little batch file that runs the command-line version (Defrag.exe) and use the Windows Task Scheduler to run the batch file.

---

**Changing a Schedule**

Even the best schedule can run up against reality now and again, so you need to be able to adjust your planned events. Here are your options:

- To run a task immediately, right-click the task’s icon in the Scheduled Tasks window and choose Run from the shortcut menu.
To stop a task that’s running, right-click the task’s icon in the Scheduled Tasks window and choose End Task. If the scheduled task has been set up to start another task, the End Task command halts only the original scheduled task.

To temporarily halt all Task Scheduler actions, open the Advanced menu in the Scheduled Tasks window and choose Pause Task Scheduler. Any tasks that do not start because Task Scheduler is paused will run again only at their next scheduled time. To start Task Scheduler again, click the same menu and choose Continue Task Scheduler.

To stop using Task Scheduler, open the Advanced menu in the Scheduled Tasks window and choose Stop Using Task Scheduler. No scheduled tasks will run, and the Task Scheduler service no longer starts automatically when the system is rebooted.

Tracking Task Scheduler

The system maintains a detailed log of Task Scheduler’s activities. To view the log, double-click Scheduled Tasks in Control Panel. From the Advanced menu, choose View Log. This opens a log, like the one shown in Figure 12-13, with the most recent entry at the bottom of the window. The Details view in the Scheduled Tasks window displays information about each task.

![Figure 12-13  The Task Scheduler log](image)

If a scheduled task doesn’t execute as expected, right-click that task in the Task Scheduler window and choose Properties from the shortcut menu. Verify that the task is in fact enabled. (The Enabled check box in the Task Properties dialog box should be selected.)
Viewing Tasks on a Remote Computer

If you are an administrator of a remote computer running Windows 2000 Server, Windows 2000 Professional, Windows XP Professional, Windows NT 4 Server, or Windows NT 4 Workstation, you can view and edit the Task Scheduler settings on that computer. Find the computer in the My Network Places window or in the Network Neighborhood window, right-click, and select Explore from the shortcut menu. In the left pane, open Control Panel and double-click Scheduled Tasks.

To view and edit scheduled tasks, the remote computer must meet the following requirements:

- Have remote administration enabled
- Specify your user account as having remote administrative access
- Share the hard disk on which the Scheduled Tasks folder resides

Using the AT Command

You can also use the AT command to schedule tasks. By default, the AT command is run using the LocalSystem account, which requires administrative privileges. To specify another account as the user of the AT command, follow these steps:

1. Open Control Panel and double-click Scheduled Tasks.
2. In the Scheduled Tasks window, open the Advanced menu and then choose AT Service Account.
3. Click This Account, and specify a particular user and password. Click OK.

The command structure for the AT command is as follows:

```
AT [\computername] [id] [/delete] /delete [/yes]
AT [\computername] time [/interactive] [/every:date[,..] | /next:date[,..]] command
```

The following parameters can be used with the AT command. Used without parameters, the AT command returns a list of scheduled commands.

- `\computername` Specifies a remote computer. Without this parameter, the local computer is assumed.
- `id` Indicates the identification number, if one is assigned.
- `/delete` Cancels a scheduled command. If no identification number is specified, all scheduled commands on the computer will be canceled.
- `/yes` Forces a yes answer to all system queries when canceling all commands.
■ **time**  Specifies when the command is to run, expressed as *hours:minutes* in 24-hour notation.

■ /interactive  Allows the task to interact with the desktop of the user logged on at the time the job is run.

■ /every:date[,...]  Runs the command on the date specified. The date can be specified as one or more days of the week (M, T, W, Th, F, S, Su) or as one or more days of the month (numbers 1 through 31). Separate multiple dates with commas. If this parameter is omitted, the current day of the month is assumed.

■ /next:date[,...]  Runs the command on the next occurrence of the specified day. If this parameter is omitted, the current day of the month is assumed.

■ **command**  Indicates the program, batch file, or command to be run. If a path is required, use the Uniform Naming Convention (UNC) path.

Here are some important facts to keep in mind about the AT command:

■ The AT command doesn’t automatically load Cmd, the command interpreter. Therefore, if the command parameter doesn’t point to an executable file, you must explicitly specify Cmd, followed by the /c switch, at the beginning of the command.

■ Commands scheduled using AT run as background processes, so there is no displayed output. To redirect output to a file, use the redirection symbol (>). The redirection symbol must be preceded by the escape symbol (^), so a sample command would be at `retrieve.bat ^>c:\daylog.txt`.

■ If you have to use a drive letter to connect to a shared directory, include an AT command to disconnect the drive when the task is completed. Otherwise, the assigned drive letter will be neither available nor seen at the command prompt.

**Note**  You can switch back and forth between the AT command and Task Scheduler, although there are some limitations. For example, if you schedule a task using AT and later modify that same task using Task Scheduler, the task is then “owned” by Task Scheduler and you can no longer access it using AT.

---

**Using cron**

If you are running Windows Server 2003 R2, you have one other scheduler available to you, the UNIX cron daemon that is included as part of the Subsystem for UNIX Applications (SUA). This is a full implementation of cron that behaves exactly as any UNIX system administrator would expect. For more details on SUA, see Chapter 27.
Autocompletion on the Command Line

Windows Server 2003 includes a number of improvements in command-line functions, such as file and folder autocompletion. Windows Server 2003 SP1 and later has the feature turned on by default, with the Tab key as the autocompletion key.

To turn this feature on in earlier versions of Windows Server 2003, open a command-line window and type cmd /f:on. Now you can avoid typing long file or folder names at the command line. For example, to navigate into the Program Files folder from the root of the system drive (typically C), you’d type c:\cd p and then press Ctrl+D. The command expands immediately to c:\cd “Program Files”. Press Enter to invoke that path.

Autocompletion also works with files. Let’s say you’re in C:\Program Files\Windows Media Player and you would like to execute Mplayer.exe. At the command line, type mp and then press the Tab key. The path expands to include Mplayer.exe. Press Enter to actually execute the file.

Another useful autocompletion method is the use of wildcards. You can use multiple wildcards in a single command line, so you could type cd/d pro*86\com* to change to the C:\Program Files (x86)\Common Files directory on an x64 Edition server.

Another command-line feature re-creates the functions of DOSKEY. Press the up and down arrows on the keyboard to navigate through recently used commands. Press F7 for a GUI-based display of recently used commands from which you can choose, also using the up and down arrows. Press Enter when you’ve arrived at the command you want to reuse.

For complete documentation on the command prompt, open a command window and type help cmd.

Summary

Windows Server 2003 supplies plenty of tools to help in the management of daily operations, including ones that handle delegation, scripts, and task scheduling. However, it’s still up to humans to do the planning and decide which tools are appropriate for which chores. Every network has its own quirks and needs, and only experience can show you the optimal path. The next chapter covers the scripting support provided in Windows Server 2003. It discusses how to use your favorite scripting language to automate many time-consuming tasks.
Chapter 13

Using Scripts for Consistent Administration

Scripting on Windows Server 2003 ........................................... 352
Scripting Practices ............................................................... 357
The Future of Windows Scripting ............................................ 373
Summary ............................................................................. 376

The Microsoft Windows scripting infrastructure has grown dramatically since the late 1990s, and available documentation, administrator knowledge, and the number of books dedicated to the subject have grown along with it. Given the breadth of documentation available, it might be argued that a one-chapter discussion of how to script is superfluous, and we agree—we have no intention here to teach you how to script. But scripting is fundamentally important to Windows administration, and our goal is to show you ways it can simplify and improve the quality of your system administration by allowing you to implement customized, highly automated solutions to many problems. Furthermore, we want to distinguish the ways that server scripting is different from, and has different needs than, the general run of Windows scripting.

We’ll start by showing how some scripting elements fit together. We’ll introduce the elements of the Windows Server 2003 scripting infrastructure in general terms and point out significant enhancements—notably Perl and Services for UNIX (or Subsystem for UNIX Applications in Windows Server 2003 R2)—to the base installation of Windows Server 2003 that add useful functionality and extend your options. The heart of our discussion is core conceptual practices for writing and using server scripts. Although most of our focus is on the core command shell and WSH scripting environments, many of the key concepts and scripting examples also apply to using Perl and UNIX-derived commands.

People often speak of scripting without defining it explicitly. Because it is used in so many contexts and usually includes some concept of intent, it is difficult to provide a technically precise definition that is always true. For practical purposes, we define scripting as a “gluing” activity: although superficially similar to programming, it focuses on gluing together pre-existing tools to solve problems rather than building solutions from the ground up.
Many administrators, especially if they’ve ever worked in a large organization, understand the need for scripting to improve efficiency and reduce the number of mouse clicks it takes to get a task accomplished. A fact that often gets missed, however, is that scripting is an essential first step to providing consistent, repeatable, and standardized administration.

The first step to improving a process of any kind is to be able to standardize and document how it is now. Scripts are an essential part of that process—they ensure that everyday tasks are always done exactly the same way. No administrator using GUI administrative tools will always perform even a fairly simple task exactly the same way every time. And when multiple administrators are involved, the problem increases. By using well-designed scripts, all administrators will use the same script to perform the task, and the task will always be performed in the same way.

Once you have your core processes standardized, you can start improving them. Awkward or inefficient scripts can be modified, and additional tasks can be added to the scripting library.

---

**Scripting on Windows Server 2003**

Windows Server 2003 scripting is not a monolithic structure; it consists of several elements that have converged, usually including additions that didn’t come with Windows. To make it easier for you to understand how it all fits together, we’ll look at the infrastructure and some additions separately and then cover the extensions specific to Windows Server 2003.

**Windows Server 2003 Scripting Infrastructure**

The Windows Server 2003 scripting infrastructure, as we view it and use it, has three major elements that provide progressively deeper reach into the operating system:

- Command shell
- Active Scripting
- Active-Scripting-accessible Component Object Model (COM) interfaces, including Active Directory Services Interface (ADSI) and Windows Management Instrumentation (WMI)
Command Shell
The familiar Windows command shell (Cmd.exe) is a distinct shell from the Windows Explorer interface. While it is still sometimes called the “DOS” prompt, it has been changed and improved well beyond its original DOS roots. In addition to having a significantly improved internal command set, it even supports primitive looping and error detection and can invoke any console-mode application available. While not as cute or obviously full featured as Windows Explorer, the command shell provides critical interactive task composition abilities missing from the GUI. You can rapidly recall and repeat commands, and you can create new tools by chaining old tools together instantly using its internal pipelining system.

To see a list of internal commands supported by Cmd.exe, open a command shell window and type **help**. External command-line tools are not shown in this listing but can typically be investigated using standard command-line help switches; although the help switches vary, most console applications on Windows use /?, /h, or -? to invoke help.

**Note** For a (nearly) complete list of command-line tools in Windows Server 2003, open Help and Support, Quick Guide for Finding Tools, Command-Line Reference A-Z.

In contrast, although windowed applications are easy to invoke by clicking and often have internal task-specific time-saving conveniences, there is no way to record individual command sequences and repeat them. Nor is there a way to chain commands together in an immediate, ad-hoc fashion. You can mimic this with some third-party applications, but there is no easy or standard method for combining multiple graphical applications or actions into a single, repeatable, sequence of steps—which is something that the command shell and batch files make simple and easy. The command shell can use any tool that will provide console output, including graphical applications.

Active Scripting
Active Scripting is the Microsoft COM-based open scripting interface technology. It enables users to mix scriptable applications and different scripting languages. Microsoft includes scripting engines for two Active Scripting languages with Windows Server 2003: VBScript and JScript. Windows Server 2003 also includes several host applications, including the Windows Scripting Host (WSH). WSH has both a console host, Cscript.exe, and a GUI mode host, Wscript.exe. WSH provides a core set of facilities to support application-like use, including input/output handling, argument parsing, and an optional help system.
COM Interfaces
Windows Script Host uses the Component Object Model, or COM, for real work. COM, from a scripting perspective, is a standard for software component interfaces. If a component implements the proper COM interfaces, scripts can talk to it without worrying about whether the component is a compiled library or application, a service, or another script. A typical Windows Server install has hundreds of scriptable components. Two technologies with COM interfaces are particularly critical. The Active Directory Services Interface (ADSI) acts as a scripting gateway to directory services. Windows Management Instrumentation (WMI) provides a standard model for accessing fine-grained information about system elements and, in many cases, lets you manipulate those elements as well.

Extending the Infrastructure
Many administrators find the built-in scripting infrastructure in Windows Server 2003 to be sufficient for their needs, and it certainly has the ability to accomplish many tasks without any enhancement. But one of its biggest strengths is that it can be extended and enhanced. The two scripting infrastructure elements that offer the most scope for enhancement are the command shell itself and the supported scripting languages.

Even though the Cmd.exe in Windows Server 2003 is a significant improvement over the MS-DOS-compatible command.com interpreter, it still is severely limited compared to the shells that a UNIX or Linux system administrator takes for granted. It’s also missing the rich set of console applications that UNIX provides. Windows Services for UNIX (SFU) includes the Interix subsystem and the UNIX Korn and C shells, in addition to many standard UNIX tools that are available from the command line. Windows Server 2003 R2 integrates and enhances this with the Subsystem for UNIX Applications (SUA), which supports both 32-bit and 64-bit Windows Server 2003. SFU is available for Windows 2000, Windows Server 2003, and Windows XP Professional as a free download from http://www.microsoft.com/windowsserversystem/sfu/default.mspx.

More Info  SUA and the interoperability tools built into Windows Server 2003 are covered in detail in Chapter 27.

The Active Scripting tools are pluggable, and you can install and run several other scripting engines for WSH. You can also install additional scripting hosts that happily run alongside WSH. The first addition you should probably install is Perl. Perl is included with Services for UNIX or available directly from http://www.activestate.com. For many years, Perl has been the UNIX administrator’s scripting language of choice and has been widely used by Windows administrators as well. Installing Perl gives you immediate access to a wealth of scripts and Perl packages.
Perl is not the only additional choice to enhance Windows Server scripting. While they might not have quite as many already tested and readily available scripts available, several other useful scripting engines are available that plug into Active Scripting, including those for Python, KiXtart, IBM Rexx, and Tcl. Alternative shells are also available, from the Cmd-like shells (such as JPSoft 4NT and TakeCommand) to classic UNIX-style shells (such as Cygwin). Table 13-1 lists some alternative shells and where they can be obtained. Many don’t require commercial license purchases, and even those that do are reasonably priced for a small number of servers if you consider the savings in administrative time. If you’re familiar with a scripting system that is sufficiently stable and secure for server use, you should consider adding it; familiarity is the primary factor in making it easy to automate administration.

### Table 13-1  Some commonly used scripting systems or enhancements

<table>
<thead>
<tr>
<th>Scripting Enhancement</th>
<th>Where to Find It</th>
</tr>
</thead>
<tbody>
<tr>
<td>KiXtart</td>
<td><a href="http://www.kixtart.org/">http://www.kixtart.org/</a></td>
</tr>
<tr>
<td>Tcl</td>
<td><a href="http://www.tcl.tk/">http://www.tcl.tk/</a></td>
</tr>
<tr>
<td>JPSoft (4NT and TakeCommand)</td>
<td><a href="http://www.jpsoft.com/">http://www.jpsoft.com/</a></td>
</tr>
</tbody>
</table>

### What’s New in Windows Server 2003 Scripting

Although the conceptual architecture of Windows Server 2003 scripting has not changed from earlier versions of Windows, the details have. The command shell, scripting host, and COM-related systems have all had changes made to them. Documenting all the possibilities would require an entire book, so we’ll simply provide an overview and point you to appropriate sources of additional information. Following are the major areas of change:

- The command shell—specifically, Cmd.exe and console-based tools
- Windows Scripting Host (WSH)
- Distributed COM (DCOM)
- ADSI and WMI

The Windows Command Shell—Cmd.exe
The Windows Server 2003 command shell has additions, changes, and usage details documented in its help file. You can access these by typing `%WINDIR%\Help\ntcmds.chm` at a command prompt. There are 64 documented new external command-line tools. These include several WSH scripts focused on IIS and printer management, a large set of Active Directory tools, and miscellaneous other tools, including sc (services); tasklist and taskkill (process management); and takeown, inuse, and openfiles (file management). Help for these and other commands is available by invoking the command with its help switch, usually `/?`. Some new tools use the POSIX-style `-?` for their help switch instead.

Windows Scripting Host
Windows Server 2003 uses version 5.6 of WSH, VBScript, and JScript. This version has been available since 2001 for all supported operating systems, and WSH and the scripting engines are part of the updateable core feature set of Windows, so it technically has no new unique features. WSH scripts have been affected, however, by significant changes in default Distributed COM (DCOM) security.

Distributed COM
All remote COM access, including ADSI and WMI, is affected by DCOM’s increased authentication security and the presence of firewalls. The default security level used for authenticating clients has changed from connection-level to packet-level. Because the authentication level is negotiated, the changes don’t affect tools unless one side insists on a lower security level than the other system will accept. Client-side firewalls affect asynchronous connections because they require a separate connection and an exclusion for the specific remote host or the ports used.

ADSI and WMI
There are roughly 350 new classes and 4000 distinct new properties and methods in WMI’s `root/cimv2` namespace on a default Windows Server 2003 domain controller. Unfortunately, there is no system-based help on these new elements. We’ve included Scriptomatic on the CD, which will allow you to browse through classes and properties on a Windows Server 2003 system as a useful starting point. You can search class names on MSDN at `http://msdn.microsoft.com` for specifics of the class or search the TechNet
Script Center at http://www.microsoft.com/technet/scriptcenter/default.mspx. The TechNet Script Center will usually provide code samples as well.

**On the CD**  Look for the Scriptomatic tool on the CD in the Tools folder.

---

**Scripting Practices**

Writing and using scripts requires a clear understanding by both the script writer and the script user of the intended use and the designed use. A script that will be scheduled to run automatically, for example, can’t have any GUI elements in it because it will fail if it is run when no one is logged in. If you’re running a script interactively from the console, it will fail if you don’t provide the correct input and syntax to the script.

**Think from the Command Prompt**

The most important step you can take to improve your Windows automation work is to think in terms of the command prompt. Good command-prompt tools can use the command prompt’s special abilities such as pipelining and batching. They can run correctly from the Task Scheduler. They work properly when run without a graphical session. And they function properly when they are run unattended. By focusing on these requirements, you’ll create good scripts that can be used in a broad range of conditions.

**Write WSH Scripts as Console Tools**

Making WSH scripts act as true command-line tools that can write to both the standard output and standard error streams and even read an input pipeline is a commitment that involves both script writing and use, but the effort pays off immediately in both cases.

**More Info**  See the “Input and Output Handling” section for more on the standard streams.

Writing WSH scripts as console tools means designing them to run totally automated with no user intervention after invocation. This means users need to be able to completely configure the tool and supply data to it from the command line. The most convenient way to do this is to use general defaults for tool configuration and implement named arguments for them. If you need to accommodate a large quantity of data, you can read it from standard input (WScript.StdIn.ReadLine, for example).
Although WSH allows you to set the default script host to the console-mode cscript host, it still breaks console input pipes during the host selection. For example, suppose you use a script like this simple VBScript Len function wrapper that tells us the length of lines:

```vbs
' Len.vbs
If WScript.Arguments.UnNamed.Count > 0 Then
    For Each uarg in WScript.Arguments.UnNamed
        WScript.StdOut.WriteLine Len(WScript.StdIn.ReadLine)
    Next
Else
    Do While Not WScript.StdIn.AtEndofStream
        WScript.StdOut.WriteLine Len(WScript.StdIn.ReadLine)
    Loop
End If
```

You first set the default WSH host to cscript by entering `cscript //H:cscript //S` at a command prompt, and then you perform a quick test using `ipconfig | len`. This will immediately return the console error `len.vbs(7, 5) (null)`—which indicates that the handle is invalid.

One solution is to invoke cscript explicitly with the script as an argument—a cumbersome and not terribly practical solution, especially if you need to chain multiple scripts together. Not only do you have to add cscript to each command line you type, but you also need an explicit path to the script file. A better solution is to use wrapper scripts that invoke the script properly. For the len.vbs script, we create a command shell script len.cmd with the following single line in it:

```bash
@cscript "len.vbs" %* || @exit
```

---

**Important** For this to work properly, the command shell script must be in the same folder as your WSH script, and as it is by default, .cmd must precede .vbs in your `%PATH%` shell variable.

The following script can be used to automatically create a shell wrapper for any WSH scripts you create:

```xml
<?xml version="1.0" encoding="ISO-8859-1" ?>
<job>
<runtime>
<description><![CDATA[
Name: New-ConsoleWrapper.wsf
Name: New-ConsoleWrapper.wsf
DESCRIPTION
Given one or more paths to WSH scripts as arguments or as standard input data, this script will generate a wrapper CMD script in the same directory to allow direct execution of the script as a pipelineable script tool and shut down the pipeline if the script is terminated.

LIMITATIONS
```
+ This script should always be executed with cscript as the host.
+ If the %PATHEXT% environment variable has been modified so that the CMD
extension comes after the WSH script type you wish to wrap, wrapper scripts will
not work.
]]></description>
<example><![CDATA[
USAGE SCENARIO
To create wrapper scripts in the current directory and all directories underneath
it for all files with the .wsf or .vbs extensions, use this:
   dir /s /b *.wsf *.vbs | cscript New-ConsoleWrapper.wsf
Drag-and-Drop:
Do NOT drag and drop onto this script. Drag and drop onto this script's wrapper
script (New-ConsoleWrapper.cmd or New-ConsoleWrapper.bat).
]]></example>

<named name="?" helpstring="returnsthis help message" type="simple"
required="false"/>
<named name="A"
helpstring="Always create wrapper script, whether or not the specified script
exists" type="string" required="false"/>
<named name="Force"
helpstring="Overwrite pre-existing wrapper script files. If not specified, prior batch scripts with the
same name will not be overwritten." type="simple" required="false"/>
<named name="B"
helpstring="Generates wrappers with a .bat extension instead of the default.cmd
extension." type="simple" required="false"/>
<named name="T"
helpstring="Turns on tracing. This causes various extra information about the
process to be echoed to stderr." type="simple" required="false"/>
<unnamed name="scriptpath"
helpstring="one or more scripts to create wrapper scripts for." many="true"
required="false"/>

]]></example>

<object id="fso" progid="Scripting.FileSystemObject"/>
<reference object="Scripting.FileSystemObject"/>
<object id="sh" progid="Wscript.Shell"/>

<script language="VBScript"> <![CDATA[
Option Explicit
Dim StdIn, StdOut, StdErr, UARGS(), Named, UnNamed, TRACING
set Named = WScript.Arguments.Named
Set UnNamed = WScript.Arguments.UnNamed

' declare and initialize some data we may change based on named args.
dim ALWAYS_CREATE, OVERWRITE, EXT
ALWAYS_CREATE = false: OVERWRITE = false: EXT = ".cmd"

Script_Initialize true
ProcessArguments
dim arg: for each arg in UARGS
   TraceLine "script to wrap from argument list: " & arg
CreateWrapper arg
next
If UBound(UARGS) < 0 then
    TraceLine "No unnamed args found; iterating over the input stream"
    ' if we didn't have any scripts specified on the command line, read them from StdIn
    do while not StdIn.AtEndOfStream
        CreateWrapper StdIn.ReadLine
    loop
end if

Sub CreateWrapper(byval scriptname)
    if TRACING Then StdErr.WriteLine "wrapping " & scriptname
    if not(FSO.FileExists(scriptname)) or ALWAYS_CREATE then
        StdErr.WriteLine "script not found: " & scriptname
        exit sub
    end if
    dim WrapperPath
    WrapperPath = StemNameFromFileSpec(scriptname) & EXT
    dim WrapperCmd: WrapperCmd = "@cscript " & FSO.GetExtensionName(scriptname) & "," & FSO.GetExtensionName(scriptname) & ","
    If FSO.FileExists(WrapperPath) and not(OVERWRITE) then
        StdErr.WriteLine "wrapper script found, not overwritten: " & WrapperPath
        exit sub
    end if
    dim file: set file = FSO.OpenTextFile(WrapperPath, ForWriting, True)
    file.Write WrapperCmd
    file.Close
    StdOut.WriteLine "wrapper script created: " & WrapperPath
end sub

Function StemNameFromFileSpec(byval filespec)
    ' given a filespec as an argument, turns it into a "stem" - full path to parent directory + the base name.
    StemNameFromFileSpec = FSO.BuildPath( _
        FSO.GetParentFolderName(filespec), _
        FSO.GetBaseName(filespec) )
end function

Sub ProcessArguments()
    ' General argument processor template routine.
    ' Insert other handlers below.
    Dim i
    If Named.Exists("A") Then
        ALWAYS_CREATE = True
    Else
        ALWAYS_CREATE = False
end sub
End If
If Named.Exists("Y") Then OVERWRITE = True Else OVERWRITE = False
If Named.Exists("B") Then EXT = ".bat" Else EXT = ".cmd"
If Named.Exists("T") Then TRACING = True Else TRACING = False
TraceLine "Tracing script execution now."
' get unnamed arguments into an array
redim UARGS(UnNamed.Length - 1)
TraceLine "found " & UnNamed.Length & " unnamed arguments."
for i = 0 to ubound(UARGS)
    UARGS(i) = UnNamed(i)
next
End sub

Sub Script_Initialize(byval bFailOnGUI)
' Set up global StdIn, StdOut, StdErr
if bFailOnGUI And _
    lcase( right(WScript.FullName, 11) ) <> "cscript.exe" then
    WScript.Echo "Must be run with cscript as the script host"
    WScript.Arguments.ShowUsage: WScript.Quit 1
end if
Set StdIn = WScript.StdIn
Set StdOut = WScript.StdOut
Set StdErr = WScript.StdErr
End Sub

Sub TraceLine( s )
    If TRACING then WScript.StdErr.WriteLine s
End Sub

On the CD   This script (New-ConsoleWrapper) is on the companion CD.

The command shell wrapper for this script is a one liner:
@cscript "%~dpn0.wsf" %* || @exit

Some comments on the specifics of the command shell script are useful for understanding how to make WSH scripts work as console tools. The leading “@” turns off echoing for that line only. This is simpler than an “echo off” statement in a very short script. The quotes around the file name aren’t always required, but they ensure that script names with spaces in them are correctly invoked.

The “%~dpn0.wsf” is an example of using batch parameters in a script. The “%~” identifies that special batch parameter modifiers will be used to modify the “%0” parameter. “%0” is argument zero, the name of the called script, the “d” expands to the drive (as in
“C:\”), the “p” expands to the path, and the “n” to the base name of the file (without the extension). The “.wsf” is then appended to this.

The “%*” passes on all command-line arguments without affecting them. The rest of the line is technically a new command. The doubled vertical line characters, ||, mean “if the command fails to run properly” perform the command that follows. The net effect of || @exit is to tell the CMD script to exit if the command fails. The exit statement ensures that the script stops processing data immediately on a failure rather than repeatedly asking you whether you want to terminate the script until the end of the input stream.

---

**Important** Remember, if you don’t use a workaround like the console wrapper, you must explicitly execute WSH scripts with cscript on the command line to make them read standard input properly. Setting the default WSH host to Cscript.exe isn’t sufficient.

---

**Credentials and Scripting**

One of the critical security and reliability issues for Windows scripts is credential use. There are two main problem areas:

- **Secure password handling** Where scripts require passwords, how do we manage those passwords and securely transmit them?
- **Session credentials** Administrators should normally operate with limited privileges and then elevate them as required to handle specific tasks. Handling privilege elevation with scripts introduces a new range of issues with both security and troubleshooting.

---

**Use RunAs and Scheduled Tasks**

One solution that has some fringe benefits is to not handle authentication within the script, but to use the RunAs command or schtasks alternate credentials arguments instead. By using this approach, you don’t need to write or maintain code for managing the user’s credentials, or worry about specifying the user’s credentials explicitly within the script. Troubleshooting problems is also simplified because it’s clear that everything is happening with permissions derived from the executing account.

---

**Avoid Specifying Passwords on the Command Line**

Many tools that handle alternative authentication allow you to specify a password on the command line. This is a bad practice and should be avoided. If someone has permission to enumerate processes, he or she can also read the entire command line of processes running on a server. Further, even momentary access to your console will let a user see the clear-text password as typed on the command line.
Most tools that provide this kind of support will automatically prompt for a password if it isn’t provided or if you enter the password switch with no argument.

**Use Obfuscated Password Entry**

Windows XP and Windows Server 2003 have a new COM object written specifically to allow hidden password entry. You must be running the script from the command line for this to work, but this new COM object allows you to enter the password on the command line with no visible text, as shown in the following three examples:

**VBScript**

```vbscript
dim ScriptPW, pw
set ScriptPW = CreateObject("ScriptPW.Password")
pw = ScriptPW.GetPassword
```

**JScript**

```javascript
var ScriptPW, pw;
ScriptPW = new ActiveXObject("ScriptPW.Password");
pw = ScriptPW.GetPassword();
```

**Perl**

```perl
use Win32::OLE;
$ScriptPW = Win32::OLE->CreateObject("ScriptPW.Password");
$pw = $ScriptPW->GetPassword();
```

**Path Management Practices**

When you invoke an application by any means other than specifying an explicit qualified name for it, Windows performs a search for the tool. This includes every single tool you invoke in any context.

**How Command Discovery Works**

When you type a command such as `regedit` at the command prompt, the command processor (Cmd.exe) first checks for an internal match—this is how names of internal commands such as `dir` are found. The command processor next looks in the current directory for files with the base name `regedit` and one of the file extensions listed in the `%PATHEXT%` command shell variable, in the order they are listed in the variable. If it isn’t found, it looks through each folder listed in the `%PATH%` variable in the order they are listed, and in each folder it checks against that base name plus the list of file extensions listed in `%PATHEXT%`. This process continues until it finds a matching name or it runs out of folders to search.

**Making Changes to the Shell Working Directory**

Executables always use the shell’s search mechanism for discovery. This applies to WSH scripts launching an external process using WScript.Shell’s Run method, for example,
because the external process is just inheriting the shell. Because the local directory will always be searched first for commands, you need to exercise caution when changing your working directory in a script. Any arbitrary path might contain malicious executables with names of commands you are likely to invoke. An equally serious problem is that there are often multiple versions of files on a system, and invoking an external command after a directory change can pick up the wrong version of a file. To avoid this problem, you have two basic solutions:

- Always use a working directory that has controlled access so that only Administrators can write into it.
- Use explicit, fully qualified command paths. (This is the preferred solution.)

**Use Fully Qualified Command Paths**

To prevent accidental executable substitution, you should qualify executable paths rather than using just bare names. At its simplest, qualification can just specify executable type by including the file suffix—for example, you would use Regedit.exe instead of regedit to ensure you don't find regedit.com instead. For increased control, you can specify a fully qualified path and use well-known environment variables in the path to make the invocation work on nonstandard system configurations. For example, %SYSTEMROOT%\system32\regedit.exe will always find regedit.exe, even if Windows is installed in D:\WinSafe instead of C:\Windows.

**Real World  Making Sure %PATH% Is Limited and Has Strong Permissions**

As we've mentioned, the command processor searches for commands by looking in all the folders listed in %PATH%. The only three standard folders in the path are the system folder, Windows itself, and the WMI folder; if your system drive is C they will be: C:\WINDOWS\system32;C:\WINDOWS;C:\WIN- DOWS\System32\Wbem.

Unfortunately, some applications will add themselves to your search path automatically without asking; sometimes they are added at the front of the path, so they are searched first. This can cause slowdowns as a result of extra folders being searched first. If an application that adds itself to your path has an incompatible version of a critical dynamic-link library (DLL) in its folder, it might even cause other applications to fail when they try to use the incompatible version. Even worse, some applications open security holes by adding paths that other users might have permission
to write to. A malicious file with a common name such as “regedit” in one of these
locations can easily be invoked by an administrator, opening the entire system to
possible exploitation.

To guard against this, take the following precautions:

■ Whenever you install new software, after a reboot check the system path by
typing path at a command prompt. If an application has added itself, consider
removing it; at the very least, make sure it is added to the tail end of the path.

■ Carefully check the security settings on folders that you do want to remain in
your path. Only privileged users who normally should be able to administer
the computer should have permission to write or modify files. (Permission for
reading and executing is fine.)

Monitor the %PATHEXT% Variable
The pathext variable is also occasionally modified by application installs, and it might not
need some elements that it contains by default. For example, encoded JScript (.JSE) and
VBScript (.VBE) files are considered executables, but Windows does not have any tools
shipped in this form. If you don’t use encoded scripts, you can remove .JSE and .VBE
from the %PATHEXT% variable to prevent invoking encoded scripts. Another simple
security trick that can shut down some attack vectors is to reverse the order of .EXE and
.COM on %PATHEXT%. This will prevent a malicious program from inserting itself
higher in the executable order by adding a .COM version of a common .EXE file. As with
removing encoded scripts from known executable types, you should check the effects of
switching .COM and .EXE files against your supported systems; some application suites
use a .COM file as a launch wrapper for their .EXE and might have critical impairments
if the .EXE is launched directly.

Add a Tools Directory to Your Path
If you use many command-line tools and want them consistently available from a predict-
able location, you should put the standard tools you use in a folder that is added to your
path. This isn’t an exception to the general practices for path management; rather, it
should be a directory modifiable by administrators only and one that follows the core sys-
tem directories in the path statement. For consistent access across several machines such
as a group of servers, you can use Distributed File System (DFS) to synchronize content,
or you can create the folder on a single server and then share the folder. Map the folder
as a drive letter and then add the map to your logon script to make it consistently avail-
able. (We like to store our generally available scripts in a folder we share as “Tools” and
have that automatically mapped to the T: drive.) As obsolete as we might wish drive-mapping
to be, drive letters are still necessary for many command-line tools that refer to their
Input and Output Handling

Reading and presenting data is usually an afterthought in light-duty scripting, an oversight that causes scripts to misbehave or fail when used for batch processing or in non-interactive sessions. There are some simple practices you can apply to make scripts handle I/O properly in the console environment and even account for special output needs such as logging.

WSH: Use Text Streams for Input and Output

Console WSH scripts have three objects automatically available for input and output operations: WScript.StdIn, WScript.StdOut, and WScript.StdErr. These objects correspond to the familiar UNIX streams of STDIN, STDOUT, and STDERR, respectively. These objects are actually text streams, functionally identical to the TextStream object used for file reading and writing in WSH. Use WScript.StdIn to read data you are processing, WScript.StdOut to write new data you create, and WScript.StdErr to emit error or tracing information. These streams will work correctly in all contexts where you use console script invocation. Your script won’t care whether it is reading input from a file or a previous command; you can log output information by redirecting it to a file and still get console output. In the most extreme case of redirection, you’re actually getting to use three files without all the messy coding to open them from the Scripting.FileSystemObject:

```
cscript myscript.vbs < in.txt 2> err.log 1> out.log
```

Limit MsgBox Use

The MsgBox function in VBScript supports optional parameters for displaying different buttons, selecting a default, setting a window icon and window modality, and providing a clickable reference to a help file topic. This is the real point behind MsgBox: providing necessary context-sensitive information to a user that needs confirmation and possibly needs to make a decision. If you really need this functionality at multiple points in the script, MsgBox is the function you want and the script would be a poor candidate for full automation anyway.

In any other roles, MsgBox is bad news. If a script is running in batch processing mode with WSH’s //B option, MsgBox will always cause a failure when encountered. MsgBox will cause a script to hang or fail if it’s used when a GUI can’t be presented—such as when running as a scheduled task, in a service account, or remotely via a console session. With arbitrarily large amounts of data coming out of it, MsgBox is even useless for interactive roles; users must click repeatedly to continue processing.
If a MsgBox-using script doesn’t use the return button-click information for anything, you can generally fix it instantly by replacing MsgBox with WScript.StdOut.WriteLine. If the message was customized with other arguments, you can comment those out. If you don’t need the message for your output, just comment out the whole line.

**WScript.Echo: Flexible but Suppressed in Batch Mode**

If you want a script to write to your console window when run from Cscript.exe and pop up a box when run from Wscript.exe, and if you don’t care whether output is displayed when using scripts in batch mode, WSH’s native Echo method allows this. The WScript.Echo statement will pop up a message window if run from the GUI WSH host Wscript.exe, and it will write output to the standard output stream if run from the console WSH host Cscript.exe. If WSH is run in batch mode, WScript.Echo output is always suppressed no matter what host you are using; this makes it a bad choice for output redirection from a noninteractive script.

WScript.Echo statements are usually straightforward to convert to WScript.StdOut.WriteLine statements, but Echo has a special feature that the StdOut WriteLine doesn’t: Echo will take multiple comma-separated arguments and output them with an automatic space. To adapt WScript.Echo statements for use with WScript.StdOut.WriteLine, you need to replace each argument-separating comma with & " " & in VBScript or + " " + in JScript.

**Use the WScript.Shell LogEvent for Critical Information Logging**

Scripts that run periodically on a schedule or that make significant changes that might not be otherwise recorded explicitly are candidates for logging. Too much detail can be useless, but a single event containing a critical piece of information can be useful at each standard exit point from these key scripts; at the least, you will know when the script was run and where. LogEvent always writes to the application log; its first argument is the event type. Use 0 for an information event, 2 for a warning, and 1 for an actual error. You can use the following generic code for almost any script to track normal exit events by placing this at the end of the script code or before any explicit WScript.Quit statements:

VBScript:
```vbnet
Set WshShell = CreateObject("WScript.Shell")
WshShell.LogEvent 0, "script exit: " & WScript.ScriptFullName
```

JScript:
```jscript
new ActiveXObject("WScript.Shell").LogEvent(0,
   "script exit: " + WScript.ScriptFullName);
```

Perl:
```perl
use Win32::OLE;
Win32::OLE->CreateObject("WScript.Shell")->
   LogEvent(0, "script exit: ". Win32::GetFullPathName( $0 ));
```
Use Good Error Management

Error-handling standards for desktop scripts are generally more lax than for enterprise scripts, but all scripts benefit from good error handling except those quick “one off” scripts that you never intend for anyone but yourself to see.

Use VBScript’s On Error Resume Next Carefully

With VBScript in particular, it is common to see the statement On Error Resume Next at the start of scripts, which effectively tells WSH to ignore all runtime errors regardless of the consequences. This is a bad practice and lazy coding, and it can cause completely unpredictable consequences.

If you expect your script to encounter error events, handle them if at all possible. And if it will be normal to encounter reasonable errors in particular sections of the script, you should turn on error suppression immediately before it is needed, and then continue the current task only if errors are known and can clearly be handled. Whatever you do, you should turn error suppression back off immediately.

Console Scripts Should Handle Most Errors as Normal Events

GUI-focused or single-run scripts typically treat errors that prevent core operation as critical errors. Console scripts designed for batch use might not work well with this model. For example, a script for changing an account password on a specific computer needs to connect to the computer, authenticate, get an account reference, and then set the new password. Any error in this process means the password change failed, so there’s no point in continuing. However, if we’re handling dozens of password updates at once, we don’t want to halt the whole chain of events for reasonable errors such as specific machines being unavailable or the particular user not being present on one of the machines. The following simplified code for a password update script demonstrates this approach. We suppress errors just long enough to try connecting and get an error result. If there is no error, we set the password. If we get a normal error—such as insufficient permissions, no machine available, or the account doesn’t exist—we write a message to the error stream. If we get any other error whatsoever, it represents an unknown situation, possibly even a major problem, and we actually quit after writing an error.

Function ChangePassword (computer, name, newpass)
  On Error Resume Next
  Dim user: Set user = GetObject("WinNT://" & computer & "/" & name & ",user")
  Dim result: result = Err.Number
  On Error Goto 0
  Select Case result
  Case 0
    user.SetPassword(newpass): user.SetInfo
  Case &H46, &H80070035, &H800708AD
    WScript.StdErr.WriteLine "Failure: " & computer
  Case Else
WScript.StdErr.WriteLine computer_ & " FAILURE Unknown error returned: 0x" & Hex(result)
WScript.Quit 999
End Select
ChangePassword = result
End Function

Return Error Information to the Shell
If you choose to make a script terminate as a result of a critical failure, give it a non-zero exit code. In the case of WSH scripts, it’s a good idea to make the exit code something other than 1. Some invoking applications will handle more process shutdown details for you if they see a nonzero exit code. You should avoid using an exit code of 1 for a WSH script because WSH returns an error of 1 if it chooses to shut down on its own. One option is to pass along the script error, which we could have done by using the WScript.Quit result. Because high-numeric codes such as ADSI errors might not be rendered correctly, we used 999 as a generic unknown error code.

Log Errors in Noninteractive Scripts
When a script is running noninteractively, you won’t see what problems it encountered unless you take explicit steps to log the errors. If you want to log errors when a script is run noninteractively but just let them go to the screen from an interactive session, you can test the interactive status of your script. The WScript.Interactive property is false if the script is running noninteractively, so you can then use LogEvent as detailed in the “Input and Output Handling” section to log the error.

Assume Everyone Can Read Your Scripts
Scripts are human-readable and editable—that’s the good news. But that also means anyone with access to the script can see what it does in explicit detail and modify its operation if they have appropriate permissions. Tools such as the Microsoft Script Encoder are not useful for securing data or preventing editing. The Script Encoder, for example, is exactly what the name says: an encoder, not an encryption tool. Tools are available, however, that will decode encoded scripts flawlessly.

The best solution for protecting script code from being tampered with is to make sure that only administrators, or users with a need to modify the script, have permission to edit it. If you have a certificate server or at least a known certificate and are willing to deploy the support infrastructure to make only signed scripts run, you can also use script signing as a possible solution, but this requires substantial overhead and infrastructure support.

Securing data inside a script is more difficult. You need to set the permissions on the script (or the folder it resides in) to only allow read access to specific groups of
users. This doesn’t, however, prevent an authorized user from accidentally copying the script or some data within it to an area where it will be exposed. You should always assume that it is possible for users to gain read access to the script, and therefore you should never encase sensitive information within a script.

WMI Scripting Issues

The learning curve to get started with WMI scripting is fairly steep, but once you learn to use WMI, you’ll find it a very useful tool. A few practices can help with understanding it and preventing or resolving errors.

Use Scriptomatic to Explore WMI

WMI’s endless classes and properties change in every release of Windows; it’s impossible to document them in detail without creating an entire reference work. Fortunately, you can explore them directly using Scriptomatic from the Scripting Center. Version 2.0 of Scriptomatic is available at: http://www.microsoft.com/technet/scriptcenter/tools/scripto2.mspx and on the CD that accompanies this book. Scriptomatic gives you a complete list of all WMI classes available on a specific computer and can automatically generate scripts to sample output data.

Use WMIC for Interactive Exploration and One-Shot WMI Calls

One of the reasons WMI has a bad reputation is the sheer mass of code required for the simplest invocations. A better alternative for immediate use is the `wmic` command-line tool. WMIC provides many conveniences, including short aliases that help with the lengthy WMI calls, but at first glance it might appear difficult to use. If you’re used to script-based WMI calls and already know a specific class and property you want information from, you can get what you want with a command of the form `wmic path <class> get <property>`. For example, `wmic path win32_operatingsystem get buildnumber` would return the `BuildNumber` property exposed by the WMI `Win32_OperatingSystem` class.

Note Even on a Windows Server 2003 x64 Edition computer, you still use “Win32_operatingsystem” as the class. In fact, all the familiar WMI classes in `root/cimv2` that begin with `Win32_` are still exactly the same in x64 Edition. That might make no sense, but that’s how it is.

Avoid Authentication and Impersonation Settings

Many WMI sample scripts explicitly set authentication and impersonation levels. In scripting examples, this is typically used following the `winmgmts:` moniker in curly brackets `{}`. For example, a call that sets both of these levels might look like this:

```vbscript
Set wmi = GetObject("winmgmts:{impersonationLevel=impersonate," & "authenticationLevel=pktPrivacy}!root/cimv2")
```

Although you might occasionally want to change these security settings, if you don’t have a specific reason for doing so, it’s usually best to eliminate them. This allows WMI to use
the systemwide default impersonation level settings and negotiate the authentication level with the remote system. If you specify levels too low (as some legacy scripts do), WMI scripts might fail. This also makes WMI calls much more compact, because the line of script just shown reduces to

```vbs
Set wmi = GetObject("winmgmts:!root/cimv2")
```

## Translating Script Languages

All good scripters learn early on that there are many excellent examples of good scripts to use as the basis for their own scripting needs. It’s almost never necessary to start completely from scratch—someone has usually had to do something similar before, and scripters have traditionally made many of their scripts available for others to read and use. Unfortunately, if the script you want to borrow from isn’t written in your preferred language, you’re going to have to do some translation. And that isn’t very simple.

There are good sample scripts in just about any language you might choose to use, but there are certainly more of them in VBScript than in any other. So, if your preferred language isn’t VBScript, sooner or later you’ll probably have to translate a script or section of script from VBScript to your preferred language. The most common need is when administrators are researching COM, WMI, or ADSI properties. The documentation on these properties is frequently arcane, but there are usually code samples available somewhere—and they are almost always written in VBScript. The result is usually an impromptu attempt to translate a couple of lines of working VBScript into JScript or Perl. Because VBScript syntax has several historic peculiarities, this can be almost as difficult as starting from scratch. While we can’t tell you everything you need to know to translate some unknown script, what we can do is provide a sample of how to access COM objects directly in VBScript, JScript, and Perl. This won’t equip you for high-powered COM use, but seeing the general process for all three languages side–by–side should get you started.

## Creating and Getting

Working with COM objects might involve either accessing a pre-existing instance of an object or creating a new instance. In general, most components are created by you when needed and then shut down when you’re done with them (sometimes automatically). ADSI and WMI are both exceptions because you access them through running services. Creating a new instance in any scripting language works out to calling an underlying `CoCreateInstance` API; getting access to a running object such as the WMI interface reduces to calling the `GetActiveObject` API. To illustrate how this is done, we’ll demonstrate working with both a common COM class and WMI.

The COM class we’ll use as an example is `WshShell`, which has a common name or programmatic identifier used in WSH scripts of “WScript.Shell”. One of its properties is `CurrentDirectory`, which can be used to both read and set the current shell directory. It also has a method named `LogEvent` for writing to the Windows Application event log. To get
the running instances of COM objects, we’ll use the WMI winmgmts moniker and the path to a WMI namespace. We’ll create a reference to the namespace used most commonly by administrators, the root/cimv2 namespace, and then query WMI for the name and startup mode of all services.

**VBScript**

First, let’s look at an example in VBScript:

```vbscript
Dim WshShell: Set WshShell = CreateObject("WScript.Shell")
WshShell.CurrentDirectory = "C:\temp"
Dim wmi: Set wmi = GetObject("winmgmts://./root/cimv2")
Dim results: Set results = wmi.execQuery("
   "select Name,PathName,ProcessId from Win32_Service"

Note that when not capturing a result from a method as shown next, VBScript does not use parentheses around the method’s argument list:

```vbscript
WshShell.LogEvent 0, "Started in directory " & dir
```

VBScript uses physical line endings for statement terminations. To put two statements on one line, you use the colon (:); and to break a single line across two physical lines, you insert an underscore (_) at the end of the physical line. It uses the ampersand (&) to append one string to another. One final peculiarity that is very important is that it is not case-sensitive. The WMI method ExecQuery was written in the preceding code as execQuery, but it still works.

**JScript**

The JScript requirements are somewhat different than VBScript’s. VBScript’s CreateObject maps to the new ActiveXObject syntax. In addition, JScript uses the backslash (\) as an escape character, so literal backslashes in strings need to be doubled to escape them. Either double quotes or single quotes can be used as quoting characters, as long as they are correctly paired. Finally, when you call a method it must have its arguments enclosed by parentheses.

```javascript
var WshShell; WshShell = new ActiveXObject("WScript.Shell");
var dir = WshShell.CurrentDirectory;
WshShell.CurrentDirectory = 'C:\\temp';
var wmi = GetObject('winmgmts://./root/cimv2');
var results = wmi.ExecQuery(
   'select Name,PathName,ProcessId from Win32_Service');
WshShell.LogEvent(4, "Start in directory: " + dir);
```
Perl

Perl uses `CreateObject` (though with a rather different syntax) just as VBScript does, but first you need to “use” the Win32::OLE module. Backslashes are an escape character again, and statement termination uses semicolons just as JScript does. Finally, when setting a property on a COM object (such as WshShell’s `CurrentDirectory` property), you use the same bracket notation as you would with setting a hashtable value.

```perl
use Win32::OLE;
$WshShell = Win32::OLE->CreateObject("WScript.Shell");
$dir = $WshShell->CurrentDirectory;
$WshShell->{CurrentDirectory} = 'C:\temp';
$wmi = Win32::OLE->GetObject("winmgmts://./root/cimv2");
$results = $wmi->ExecQuery("select Name,PathName,ProcessId from Win32_Service");
$WshShell->LogEvent(4, "Start in directory: $dir");
```

Noninteractive Scripts: Remote and Scheduled Use

Scripts that run as scheduled or remote tasks have many shared issues as a result of their lack of a console or other visible interactive session. Although a well-written script can control this behavior, if your script invokes a component which doesn’t behave correctly, you’ll have problems. Using scripting conventions that don’t require interaction with the GUI and that don’t require user input can simplify the problem. And designing your scripts to recognize when they are being run from a noninteractive session allows you to redirect output, for example, to a log file or to use an input file as a source.

**Important** It’s possible to work around needing a graphical session on a remote system by using Remote Desktop, but be careful. If you disconnect, the GUI session halts to restrict resource use and continues its work only when you reconnect.

The Future of Windows Scripting

Windows has a broad repertoire of scripting tools and interfaces available. However, legacy support requirements within specific tools, new basic technologies such as .NET, convergence of environments such as WSH and the command shell, and the emergence of issues based on real-world use have all shown us clear limitations. The standard command shell has limited usability compared to UNIX command shells. The scripting environment lacks interactivity and is tied to using COM for interoperation, with no way to talk to the new .NET runtime environment. The plethora of command-line arguments used for invoking help in the console shell and the workarounds required for using WSH scripts as command-line tools highlight both poor standardization and major interoperability issues.
Since 2001, Microsoft has been working on a new hybrid command line/scriptable shell system codenamed Monad, or MSH. MSH allows users to create and manipulate objects and use scripts with data flow managed by pipelines that support objects instead of simple text. Although the msh.exe shell is console-based, this isn’t a requirement for Monad use. Tools such as Microsoft Management Console will be able to create queries as Monad scripts, for example, and these queries can be reused elsewhere and even modified. The shell language is heavily informed by several existing shells and scripting systems, notably including Perl and ksh, and also supports classic stream-based interaction with the current Windows command shell. It also has direct access to .NET types, allowing you to use objects interactively, much like you could if you could type WSH script code at a command prompt.

The management infrastructure we’ve accessed for the last few years via WMI is also being extended. Web Services for Management (also known as WS-Management or just WS-Man) is a new specification for management via Web services. From a scripter’s viewpoint, it brings new accessibility: you can use HTTPS connections for remote access to management data, and you can even (with appropriate hardware support) talk to a non-functioning system that cannot even boot Windows. WS-Man automatically exposes existing WMI providers for use. Most of the information about WS-Man that has been available up to now has been focused on developers. A good starting point is the MSDN portal site for WS-Man at http://msdn.microsoft.com/library/en-us/wsman/wsman/portal.asp.

**References and Resources**

Although there are hundreds of books and online resources that deal with aspects of scripting languages used on Windows, there are a few that stand out for their particular use in server scripting:

- *Microsoft Windows 2000 Scripting Guide* (Microsoft Press, 2002) The *Microsoft Windows 2000 Scripting Guide* provides initial deep background on using WSH-related technologies such as COM Automation, WMI, and ADSI. While originally written for Windows 2000, it is still very valid for Windows Server 2003. The core tools and concepts are the same. Most of the critical differences are specific extensions to WMI and ADSI classes that are new in Windows Server 2003. The authors are all applied administrative scripters with an intimate knowledge of how WSH works in practice. Much of this material is free from Microsoft Press and the Scripting Center (http://www.microsoft.com/technet/scriptcenter/default.mspx).
■ Windows NT Shell Scripting by Tim Hill (Sams, 1998). Windows NT Shell Scripting is the best-known reference available for working with the Cmd.exe shell. Although it predates Windows 2000 and thus doesn’t document some of the more recent command shell enhancements such as “!” expansion and the automatic %CD% and %DATE% variables, it is completely focused on the command shell and provides exhaustive example-based treatment of syntax and usage issues.

■ Windows Scripting Solutions, located at http://www.windowsitpro.com/windowsscripting. Windows Scripting Solutions is the only print periodical we’re aware of that specifically targets Windows administrative scripters. The publisher, Penton Media, allows even nonsubscribers to access much of their electronic content.

■ Roth Consulting, located at http://www.roth.net. Although Dave Roth is generally known as the author of Win32 Perl Programming: The Standard Extensions, we mention his site because it is a significant resource center for administration-focused Perl scripting.


■ Perl. The ActiveState distribution of Perl is available from http://www.activestate.com/Products/ActivePerl.

■ Services for UNIX v3.5. The final version of SFU is available from http://www.microsoft.com/windowsserversystem/sfu/default.mspx.


■ Sample scripts are included on the CD. They include: New-ConsoleWrapper.wsf, Generic WSF Template, ping-wmi.wsf, new-aduser.wsf, and get-wmi.wsf. These include some wrapper batch files.
SFU’s Win32 Console Tools. A Word document showing usage for the executables from SFU is included on the CD. This covers the tools that can be run directly in cmd sessions.

New Windows Server 2003 Console Tools. A Word document showing usage for the new command-line applications is included on the CD.

Summary

In this chapter, we covered scripting in Windows Server 2003. We’ve covered both the reasons why we think scripting is an essential part of any good administrator’s toolbox, and some of the challenges of writing scripts. In the next chapter, we start our coverage of directory services by showing you how to install and configure Active Directory.
Managing Microsoft Active Directory service is an important part of the Microsoft Windows Server 2003 administration process, and familiarity with the various tools provided for this purpose is essential. Nearly all the tools use Microsoft Management Console (MMC) snap-ins to provide the user interface. The Administrative Tools program group on the Start menu includes some snap-ins, but you must add others manually by using the MMC’s Add Snap-In function.

You’ll find that some Active Directory management tools are programs you run every day, whereas others are needed only during Active Directory installation or occasionally thereafter. The MMC snap-ins that provide Active Directory management functions are:

- **Active Directory Domains and Trusts**  Changes the domain mode, manages domain trust relationships, and configures user principal name (UPN) suffixes
- **Active Directory Users and Computers**  Creates, manages, and configures Active Directory objects
- **Active Directory Sites and Services**  Creates and configures domain sites, and manages the domain controller replication process
- **Active Directory Management**  Combines the three core Active Directory snap-ins just listed with the DNS snap-in to make a single management console with all the important tools
- **Active Directory Schema**  Modifies the schema that defines Active Directory objects and properties
In addition to the MMC snap-ins, Microsoft Windows Server 2003 includes separate utilities for importing data to and exporting it from Active Directory, as well as the Active Directory Installation Wizard that is used to promote and demote domain controllers and create domains and forests. There are also command-line tools for automating various Active Directory administration tasks. This chapter examines the tasks Active Directory administrators typically perform using the Active Directory Installation Wizard, the Active Directory Domains and Trusts snap-in, and the Active Directory Users and Computers snap-in. The next chapter examines the Active Directory Sites and Services snap-in and the Active Directory Schema Administrator snap-in.

Using the Active Directory Installation Wizard

Unlike Microsoft Windows NT Server version 4 and earlier, Windows Server 2003 doesn’t designate a system as a domain controller during the operating system installation. Every Windows Server 2003 server installs as either a standalone system or a member of a domain. After the installation is complete, you can promote the server to domain controller status using the Windows Server 2003 Active Directory Installation Wizard (or “dcpromo.exe” from the command line). This tool provides a great deal of additional flexibility to Active Directory administrators because servers can be promoted or demoted at any time, while Windows NT 4 servers are irrevocably designated as domain controllers during the installation process.

Also gone is the distinction between primary and backup domain controllers. Windows 2000 and Windows Server 2003 domain controllers are all peers in a multiple-master replication system. This means that administrators can modify the contents of the Active Directory tree on any server functioning as a domain controller, and the system will replicate the changes to all the other controllers on the domain. This is a major advance from the Windows NT 4 single-master replication system, in which an administrator can change only the primary domain controller (PDC), after which the changes are replicated to all the backup domain controllers (BDCs).

Another advantage is that you can use the Active Directory Installation Wizard (or dcpromo.exe from the command line) to demote a domain controller back to a standalone or member server. In Windows NT 4, after you install a server as a domain controller, you can demote it from a PDC to a BDC, but you can’t remove its domain controller status completely, except by reinstalling the operating system.

The basic function of the Active Directory Installation Wizard is to configure a server to function as a domain controller, but depending on the current state of Active Directory on your network, this task can take several forms. If this is the first Windows Server 2003 or Windows 2000 server that you promote to a domain controller on your network, you
create an entirely new Active Directory with that computer hosting the first domain in the first tree in the first forest.

---

**Note**  Be sure to read Chapter 3, which discusses planning namespaces and domains, before launching into Active Directory. Unless you have an independent test network where you can make mistakes without serious consequences, it's essential that you know where you're going before you get on the train.

---

### Preparing for Installation

To promote a Windows Server 2003 server to a domain controller, first complete the entire operating system installation process. If you are installing Windows Server 2003 R2, you can do the promotion either before or after you complete the R2 installation portion. After the final reboot, you then log on to the machine using an administrator account. (You can log on either locally or across the network by using Remote Desktop for Administration.)

---

**NTFS**

To host Active Directory, the server must have an NTFS partition. If you choose to install Windows Server 2003 on a system with only FAT partitions, you must convert at least one partition to NTFS before promoting the server to be a domain controller. You can do this by using the Convert.exe utility from the command prompt.

---

**Note**  Converting the Windows Server 2003 boot partition (the partition on which Windows Server 2003 is installed) requires a reboot of the system. Because the conversion can’t actually occur while the Windows Server 2003 GUI is loaded, a registry flag is used to schedule the conversion to take place the next time the machine restarts. You can then restart the Active Directory Installation Wizard and begin the installation sequence again.

---

**Security Alert**  FAT and FAT32 partitions are a serious security hole. Avoid them on Windows Server 2003 computers, especially domain controllers. In fact, just avoid them entirely. The time when they made sense is gone.

---

### DNS Server

The last requirement for installing Active Directory is that the server must have access to a Domain Name System (DNS) server. Active Directory uses DNS to store information about the domain controllers on the network. Client systems locate a domain controller for authentication by sending a query to the DNS server identified in their TCP/IP client
configurations. The DNS server that Active Directory uses need not be running on the computer being converted to a domain controller, nor does it have to run the Microsoft DNS service, though both are a good idea. However, the DNS server you use must support the Service Location resource record defined in the RFC 2052 document and the Dynamic Update protocol defined in RFC 2136.

More Info  RFCs (requests for comments) are the TCP/IP specification documents published by the Internet Engineering Task Force (IETF). All the documents are in the public domain and available for viewing at http://www.rfc-editor.org.

A DNS server is essentially a database composed of individual elements called resource records that contain information about the computers on a TCP/IP network. Various types of resource records are defined in the DNS specifications, and Active Directory requires a new type of resource record—the SRV (the DNS resource record for specifying the location of services)—to store information about Active Directory domain controllers. In addition, a DNS server used by Active Directory requires the ability to dynamically update its records, based on the availability of the domain controllers on the network. More information about DNS and dynamic DNS can be found in Chapter 16.

Originally, network administrators configured DNS servers by manually creating the resource records that identify the computers on the network. Each time a system was added or taken out of service, the administrator had to add, remove, or modify the resource record associated with it. A Windows Server 2003 network running Active Directory uses multiple domain controllers to provide fault tolerance and load balancing. If a domain controller fails or becomes unavailable to clients for any reason, another domain controller takes over its duties automatically.

Unfortunately, traditional DNS servers have no such automatic self-configuration capabilities. A network administrator has to manually modify the appropriate SRV resource record every time a domain controller goes offline and another takes its place. The Dynamic Update protocol defined in RFC 2136, on the other hand, enables DNS servers to receive messages from domain controllers containing their availability status. The server modifies its own resource records based on the contents of these messages, thus ensuring that all the domain controllers identified in the resource records are available and that all the available domain controllers are listed in the DNS server.

The Microsoft DNS Server version included with Windows Server 2003 products supports both new specifications, as does the UNIX-based DNS Server BIND versions 8.1.2 and later. If you already have a DNS server supporting these features on your network, specify its IP address in the new server’s TCP/IP configuration before you begin the Active Directory installation process. You need not install a DNS server on your new
domain controller in this case because the Active Directory Installation Wizard will locate the specified server and create the appropriate SRV resource records in it.

**Security Alert** See Chapter 17 for details about DNS poisoning attacks. If you are using BIND, you should not use a version prior to 8.4.4, and the latest version greater than BIND 9 is preferred.

However, if a DNS server supporting the new features isn’t available on the network, the wizard offers to install and configure Microsoft DNS Server on the system automatically. You can refuse the offer and install a DNS server on another system, but your new server must be able to access that DNS server to install Active Directory and promote the system to a domain controller.

**Real World  The Case for On-Site DNS Servers**

If your network currently uses off-site DNS servers for name resolution, such as those provided by your Internet service provider (ISP), install at least one new DNS server on your local network to support Active Directory. Although your ISP’s DNS servers might support the Service Location resource record and the Dynamic Update protocol, it’s unlikely that your Windows Server 2003 servers will be authorized to dynamically update the ISP’s DNS server records. Even if that were permitted, it is neither practical nor secure for your client systems to traverse a wide area network (WAN) link just to request information about local resources. You can set up internal DNS servers, that you control, to support your Active Directory, and then enable these servers to forward to your ISP’s DNS servers if you trust them to be protected with the latest patches, or turn off forwarding completely. Turning off forwarding will cause locally unresolved names to be forwarded to the root DNS servers. That way you maintain control of your network and Active Directory, while forwarding the heavy lifting of all the rest of the Internet to your ISP or the root DNS servers.

**Promoting Your First Server to a Domain Controller**

Assuming you already designed the Active Directory hierarchy that you’re going to use on your network (as discussed in Chapter 3), the process of actually installing Active Directory and promoting a server to a domain controller is quite simple. The following sections examine the process of installing Active Directory on the first server of a Windows Server 2003 network. In “Choosing Installation Options” later in this chapter, you find the various Active Directory installation options you can use when installing subsequent servers.
Launching the Active Directory Installation Wizard

Following the standard wizard pattern, installing Active Directory on a server is a matter of responding to prompts in a sequence of screens. Windows Server 2003 incorporates links to the wizard on the Manage Your Server Wizard that is displayed automatically after the operating system installation, as shown in Figure 14-1. This page is designed to guide you through all the processes needed to add and configure new roles to the server by asking questions in wizard fashion and linking to the appropriate tools for each task.

![Figure 14-1 The Windows Server 2003 Manage Your Server Wizard](image)

For users new to Windows Server 2003, this page functions as a combination mini-tutorial and checklist of server configuration procedures. To launch the Active Directory Installation Wizard from here, select Add Or Remove A Role and acknowledge that everything is connected, attached, and ready to go. If there are no other roles defined yet, the server is not yet a member of another domain, and there are no domain controllers present on the local subnet, the wizard will prompt you to configure the server as a typical first server in a domain, or it will allow you to select a custom configuration as shown in Figure 14-2. If this is the first server, by all means use this option—it will ask the right questions to automatically set up DHCP (if required), DNS, and Active Directory in one pass and with only a single reboot.
Figure 14-2 The Configure Your Server Wizard lets you choose a typical first server configuration

Note You can bypass all these steps and go directly to the Active Directory Installation Wizard by typing Dcpromo at the command line.

When you upgrade a Windows NT 4 primary domain controller to Windows Server 2003, the system launches the Active Directory Installation Wizard automatically after the operating system installation finishes.

If this isn’t the first server in your domain, or if you choose Custom, you can then select the Domain Controller (Active Directory) role to add. You’ll get warned about compatibility with other operating systems, and then you’ll be prompted for information about what kind of domain controller this will be. As shown in Figure 14-3, you can choose from one of the following options:

- **Domain Controller For A New Domain** Installs Active Directory, including the Global Catalog, on the server, and designates it as the first domain controller in a new domain

- **Additional Domain Controller For An Existing Domain** Installs Active Directory on the server, and replicates the directory information from an existing domain (Creating replicas is covered later in this chapter.)
Creating a New Domain

When you install the first Active Directory server on your network, use the Configure Your Server Wizard to select a first server configuration. You’ll get prompted to specify the following items:

- An Active Directory domain name
- A DNS domain name and NetBIOS domain name

Everything else will get automatically configured, including setting up and authorizing your DHCP server if one isn’t detected on the network, and configuring DNS correctly for Active Directory.

Specifying Domain Names

To identify the domain controller on the network, you must specify a valid DNS name for the domain you’re creating. This name doesn’t have to be the same as the domain your organization uses for its Internet and probably shouldn’t be. Nor does the name have to be one registered with a domain registrar such as Network Solutions—one of the organizations responsible for maintaining the registry of DNS names in the com, net, org, and edu top-level domains. If you do choose to use your public domain name as your internal Active Directory domain name, you should ensure that it is correctly registered with an official domain registrar.
Note  When using a different domain name from your public, registered, domain name, it’s a good idea to use a different top-level domain than the officially supported public ones. In this chapter, “.local” is used as the top-level domain, allowing complete control of the domain on the internal network and no chance of confusion with names in the public Internet.

Planning  Using .local can create issues with Macintosh computers. If your network includes Macs, choose a different top-level domain, such as “.lan” to avoid complications.

The NetBIOS name is for use by clients that don’t support Active Directory. Windows 2000 and later systems don’t require NetBIOS, but legacy systems such as Windows NT 4 and Microsoft Windows 9.x systems, as well as Samba clients, use NetBIOS names for all network resources, including domains. If you create cross-forest trusts, you’ll also need NetBIOS names because the trust process uses them. Unfortunately, we can’t completely get rid of NetBIOS yet, even though we should be able to by now.

If you have any legacy clients on your network, they’ll be able to see only the NetBIOS name. The wizard automatically fills in a suggested name you can use, based on the DNS name you specified, or you can replace it with a name of your own selection that is 15 characters or fewer.

Important  Avoid the temptation to have a different NetBIOS name than the one specified. Doing so will lead to confusion for users and administrators alike.

At this point, the Active Directory Installation Wizard has all the configuration information it needs to install Active Directory and promote the server to a domain controller.

Under the Hood  What Configuring a First Server Does

When you run the Configure Your Server Wizard and select the option to configure this server as a first server on the network, many of the prompts you would see if you were to manually configure each of the elements are bypassed. The wizard makes intelligent decisions based on basic information about your network that you provide, plus Microsoft’s best practices. Here’s what gets done automatically:

- Active Directory is installed with all roles assigned to the current server, and the global catalog database is created.
Log file and database locations are configured to the standard locations on the root drive.

The Sysvol folder is created, and replication is enabled.

Permissions are set on accounts and on the server. Permission levels are configured to support Windows 2000 or later clients.

The Directory Restore password is set to the current Administrator password.

The local Administrator account is disabled.

DNS is installed on the server.

Networking is configured to point to this server as the primary DNS server.

DNS A and SRV records are created for the server.

If no DHCP server was identified on the network, the following gets done:

- The DHCP service is installed.
- A DHCP scope of 10 to 254 on the local subnet is created.
- The DHCP server is authorized and started.

If you opt to create your first server manually, be sure all the steps just listed are completed. Many are handled by the individual wizards, but one that’s often forgotten is the authorization of the DHCP server.

Finally, a note of caution. The wizard does not create a reverse DNS zone for your local subnet. While technically this isn’t absolutely required, we think it’s a good thing to do, and the first thing we do on a new domain is add the reverse DNS zone for the local subnet.

The procedure for installing additional domain controllers on your network is similar to that for the manual installation of the first domain controller. The following sections examine the other options provided by the Active Directory Installation Wizard and how you use them to build a Windows Server 2003 network with Active Directory.

**Choosing Installation Options**

Planning an effective directory service strategy is an essential element of an Active Directory deployment. As stated earlier, before running the Installation Wizard on any Windows Server 2003 server, have in mind a directory structure that outlines which domains, trees, or forests you intend to create in Active Directory and how they should be configured. As you create additional domain controllers on the network, you can use the Installation Wizard to specify any of the Active Directory installation options.
Creating Additional (Replica) Domain Controllers

Replicas provide fault tolerance and load balancing for an Active Directory domain, and they can reduce internetwork traffic by enabling network clients to authenticate using a domain controller on the local segment. When a domain controller malfunctions or is unavailable for any reason, the other domain controllers automatically take over. Even a small domain should have at least two domain controllers to maintain this fault tolerance.

To create an additional domain controller in an existing domain, you run the Active Directory Installation Wizard on a newly installed Windows Server 2003 server after joining the domain. For the computer to join the domain, you can either join the domain for the first time and supply the administrative credentials that enable the system to create a computer object in the domain, or create the computer object manually using Active Directory Users and Computers. After joining the domain, log on to the system using the local administrator account and launch the wizard from the Manage Your Server page or by running Dcpromo.exe directly.

When the Domain Controller Type page appears in the wizard, select Additional Domain Controller For An Existing Domain and specify the DNS name of the domain to be replicated. You must then supply the user name, password, and domain name of an account with administrative privileges in the domain.

The rest of the process is straightforward. You’ll need to specify locations for log and database files, and for the Sysvol directory. The wizard installs Active Directory on the server; creates the database, logs, and the system volume in the locations you specify; registers the domain controller with your DNS server; and replicates the data from an existing domain controller for that domain. It does not install a copy of the global catalog on the server, nor does it assign any of the special roles to the server.

When the new domain controller is up and running, it is essentially indistinguishable from the existing domain controller, as far as client functionality is concerned. All domain controllers function as peers, unlike Windows NT servers, which are designated as primary and backup domain controllers. Administrators can modify Active Directory contents (either objects or schema) from any domain controller, and the changes are replicated to all the other controllers for that domain.

Note  The first domain controller in a domain is assigned certain Operations Master roles for the domain. These roles are not duplicated to the additional or replica domain controllers as they are created, but remain with the original domain controller unless you explicitly move them. For more information about the various roles domain controllers can play in the domain and how to manage those roles, see Chapter 15.
When creating a replica, the Active Directory Installation Wizard automatically config-
ures the replication process between the domain controllers. You can customize the rep-
lication process using Active Directory Sites and Services, included with Windows Server
2003. (See Chapter 15.)

Creating a Child Domain in an Existing Tree
When you create the first Windows Server 2003 domain on your network, you’re also cre-
at ing the first tree in a forest. You can populate the tree as you create additional domains
by making them children of existing domains. A child domain is one that uses the same
namespace as a parent domain. This namespace is established by the DNS name of the
parent domain, to which the child adds a preceding name for the new domain.

For example, if you create a domain called example.local, a child of that domain would be
called something like finance.example.local. Typically, child domains reflect the geo-
ographical, departmental, or political divisions of an organization, but you can use any tree
design principle you want, although it’s usually desirable to create domains based on
administrative boundaries when possible. A parent domain can have any number of chil-
dren, and the tree structure can extend through any number of generations, which
enables you to use a single namespace to create a domain tree that reflects the structure
of your entire organization.

More Info Before implementing any tree structure, read Chapter 3 for impor-
tant considerations in planning your namespace.

To install Active Directory and create a child domain, you must first join your Windows
Server 2003 server to the parent domain by joining that domain and supplying adminis-
trative credentials or by manually creating a computer object in the domain using Active
Directory Users and Computers. Then log on to the system using the local administrator
account and launch the Active Directory Installation Wizard.

A child domain is not a replica; it is a completely separate domain located in the same
tree. Therefore, when the wizard displays the Domain Controller Type page, you must
select Domain Controller For A New Domain. In the Create New Domain dialog box, you
select Child Domain In An Existing Domain Tree. The wizard then prompts you for your
Network Credentials to ensure you have sufficient privileges, and then it prompts you for
the DNS name of the domain that is to be the parent of the child and the short name for
the child domain, as shown in Figure 14-4. The short name is the name that will be added
to the parent domain’s DNS name to form the full name of the child domain. For exam-
ple, to create a child domain called Finance.example.local, you specify example.local as
the parent domain name and Finance as the short name of the child.
As with the creation of the first domain in the tree, you must supply a NetBIOS name for the new domain of no more than 15 characters. (See Figure 14-5.) In the preceding example, the domain is called FINANCE. The wizard then completes the Active Directory installation, following the same steps as the first domain in a forest, and prompts you for a system reboot.
Creating a New Tree in an Existing Forest

In addition to creating child domains in an Active Directory tree, you can also create entirely new trees, thus forming a forest. Each tree in a forest has its own separate namespace, but the trees all share the same schema and configuration. If, for example, you modify the schema to add customized attributes to a particular object in one tree, those attributes will be present in the same object type in all the other trees in the forest.

Before you create a new tree in an existing forest, your new Windows Server 2003 must join the root domain of that forest. The root domain is the first domain created in the forest, and you join the system to that domain by logging on to it and specifying credentials for an administrative account in the domain or manually creating a computer object in the domain using Active Directory Users and Computers.

When the computer has an account in the forest’s root domain, log on to the system using the local administrator account and launch the Active Directory Installation Wizard from the Manage Your Server page or by executing Dcpromo.exe directly. When the Domain Controller Type dialog box appears, select Domain Controller For A New Domain. Then select Domain Tree In An Existing Forest in the Create New Domain dialog box.

To create the new tree, you must first specify the appropriate network credentials to proceed, and then the DNS name of the new tree in the forest. This DNS name must not be a part of any existing namespace in the forest. That is, if a tree already uses example.com as the DNS name of its root domain, you can’t use the name engineering.example.com for the root domain in your new tree, even if that exact domain name doesn’t exist in the example.com tree.

After supplying the DNS name, you furnish a NetBIOS equivalent in the usual manner. The wizard then completes the installation process as in previous installations and prompts you to reboot the system.

Creating a New Forest

The fundamental difference between creating a new tree and creating a new forest is that forests each have their own individual schema and configuration, whereas trees do not. The most obvious scenario in which a network has multiple forests is when two organizations with existing Active Directory installations merge, and sufficient schema and configuration differences exist between the two to make joining them into one forest impractical.

The procedure for creating a new forest is the same as that for creating the first domain on the network, as described in “Promoting Your First Server to a Domain Controller” earlier in this chapter.
Upgrading Windows NT 4 Domain Controllers

Windows Server 2003 simplifies the process of converting the domains from a Windows NT 4 network to Windows Server 2003 Active Directory domains by enabling you to upgrade the servers gradually. Windows NT domain controllers can coexist on the same network as Windows 2000 or Windows Server 2003 domain controllers and can even function in the same domain. The only special rule for the upgrade process is that you must upgrade the PDC of a Windows NT 4 network before any of the BDCs.

When you install the Windows Server 2003 operating system on the PDC, the Active Directory Installation Wizard launches automatically after the final reboot and begins the promotion process. After the server is promoted to a domain controller, the system can host your existing domain, using the Windows NT 4 BDCs as replicas. You can then upgrade or decommission the BDCs at your own pace.

When all the domain controllers are running Windows Server 2003, you can then use the Active Directory Domains and Trusts snap-in to convert the domain from Windows Server 2003 interim mode to Windows Server 2003 mode, enabling you to take full advantage of Active Directory’s grouping capabilities. See “Domain and Forest Functionality” later in this chapter, for more information about switching the domain operational mode.

Real World Upgrading from Windows NT 4 Domains

If you’re still using Windows NT 4 domains, the chances are that the computers acting as your domain controllers have been around for a while and might well be ready to be decommissioned. You really don’t want an underpowered server as the first domain controller in your new environment, especially if it’s a machine that is reaching the end of its life. One solution is to use a new machine that will be your core domain controller in the new world, and first install Windows NT 4 on it, selecting Backup Domain Controller as the role for the server. Then promote it to Primary Domain Controller on your Windows NT 4 domain, and upgrade it directly to Windows Server 2003. Your existing Windows NT 4 domain controllers can be upgraded or decommissioned as time and resources permit.

The other way to manage the process, if your existing Windows NT 4 domain controllers are at least of the minimum level to run Windows Server 2003, is to go ahead and upgrade your current PDC, and then add any new servers to the domain that will be domain controllers. You can then transfer the Operations Master roles to one of the new servers before you decommission the server that had been the PDC in your Windows NT 4 domain. Don’t forget to also designate at least one other Global Catalog server before you pull the old PDC off the network.

For details on transferring roles and creating a Global Catalog server, see Chapter 15.
Demoting a Domain Controller

A major difference between Windows Server 2003 domain controllers and Windows NT domain controllers is that you can demote a Windows Server 2003 domain controller to a standalone or member server. When you launch the Active Directory Installation Wizard, the program ascertains that the system is already functioning as a domain controller and provides only the option to demote the server, as shown in Figure 14-6.

Demoting a domain controller erases the Active Directory database from the machine, removes all references to it from the DNS server, and returns the system’s security accounts to a state identical to that of a newly installed Windows Server 2003 computer. If the domain to which the system belongs has additional domain controllers on the network, the server remains a member of that domain after the demotion.

If the server is the sole domain controller for a particular domain, the demotion causes that domain to be erased completely from Active Directory, and the system becomes a standalone server until you join it to another domain. If the server is the only controller of a forest’s root domain, you must destroy all the other domains in the forest before you can proceed with the demotion of the root domain controller. To demote the controller, follow these steps:

1. Open the Active Directory Installation Wizard by running Dcpromo.exe. You see the page shown in Figure 14-6. Click Next.

2. If you see a message box like the one in Figure 14-7, don’t proceed with the demotion of the server until you’re sure at least one other Global Catalog server exists in
the domain, or unless this is the last domain controller in the domain and you are removing the domain entirely. (See “Setting a Global Catalog Server” later in this chapter.)

Figure 14-7   A warning message when demoting a Global Catalog server

3. If this is the last domain controller in the domain, select the appropriate box on the Remove Active Directory page, as shown in Figure 14-8.

Figure 14-8   The Remove Active Directory page

4. If you're removing the last domain controller in the domain, you get additional prompts to delete the application directory partitions on the domain controller.

5. Provide a password for the server administrator account. You then see a summary showing what you selected and what the result will be if you proceed.

The Configuring Active Directory page opens and provides a running description of the processes being performed. This takes at least a few minutes, and sometimes considerably longer, depending on the machine. When the configuration is complete, the server is no longer a domain controller and you're prompted to click Finish and then Restart Now.
Changing a Domain Controller Identification

Changing a domain controller’s network identity can be accomplished in a single step if the domain is a pure Windows Server 2003 domain. If there are still Windows NT 4 BDCs or Windows 2000 domain controllers in the domain, the domain controller can be renamed only by demoting it, changing the name, and promoting it again.

Important When changing a domain controller’s name, exercise caution, especially in a mixed environment with earlier clients. References to your server’s old domain name can be perpetuated by WINS servers, causing browsing problems as well as preventing the reuse of the computer name, and clearing out WINS databases to correct the problem can be tricky.

To change the domain controller’s identity, do the following:

1. If the domain still contains earlier domain controllers, demote the domain controller.
2. Open the System tool in Control Panel, and click the Computer Name tab.
3. Click Advanced to open the Identification Changes dialog box. Type the new name for your computer.

Note Try to use a computer name that is both DNS-compatible and NetBIOS-compatible so that all types of clients see the same name for your computer. To do this, keep the name shorter than 15 characters in length and don’t use asterisks or periods. It’s also preferable to avoid using spaces or underscores for the best application compatibility.

After you make the change to the computer’s network identity, if you had to demote the domain controller initially, you can promote it once more to a domain controller.

Setting a Global Catalog Server

The first Windows Server 2003 domain controller in a forest is automatically a Global Catalog server. The Global Catalog (GC) contains a full replica of all directory objects in its host domain plus a partial replica of all directory objects in every domain in the forest. The point of a GC is to provide authentication for logon events. In addition, because a GC contains information about all objects in all the domains in the forest, finding information in the directory doesn’t require unnecessary queries across domains. A single query to the GC produces the information about where you can find the object.

Note As long as your enterprise has any Windows NT domain controllers, each domain must have at least one Global Catalog server.
By default, there will be one GC, but any domain controller can be configured as a Global Catalog server. If you need additional logon and search services, you can have multiple Global Catalog servers in the domain.

To make a domain controller into a Global Catalog server, follow these steps:

1. Launch Active Directory Sites and Services from the Administrative Tools folder.
2. Open Sites and select the applicable site.
3. Open Servers and then select the domain controller you want to make into a Global Catalog server.
4. Select NTDS Settings from the right-hand pane, and choose Properties from the Action menu.
5. In the General tab, select the Global Catalog Server check box.

---

**Using Active Directory Domains and Trusts**

Windows Server 2003 Active Directory Domains and Trusts is an MMC snap-in you can use to view a tree display containing all the domains in your forest. With this snap-in, you can manage the trust relationships between the domains, change the domain mode, and configure the user principal name (UPN) suffixes for the forest. Active Directory Domains and Trusts also provides access to Active Directory Users and Computers for each domain that you use to view and modify the properties of individual objects.

**Launching Active Directory Domains and Trusts**

Windows Server 2003 adds the Active Directory Domains and Trusts Manager snap-in to the Start menu by default, so after logging on using an account with administrative privileges, you can run the utility by selecting Active Directory Domains and Trusts from Administrative Tools in the Start menu’s Programs group. The MMC snap-in file is called Domain.msc, so you can also launch the manager from the Run dialog box by executing that filename.

When the Active Directory Domains and Trusts Manager loads, the console tree (on the left side of the screen shown in Figure 14-9) displays all the domains in the forest in expandable tree fashion, stemming from a root labeled Active Directory Domains and Trusts. The result pane (on the right) displays the children of the currently selected domain, or if you select the root, the root domains of all the trees in the forest. The functions provided by Active Directory Domains and Trusts are accessible from the Action menus produced by clicking a domain name or the root object, as well as within the Properties dialog box for a domain.
Domain and Forest Functionality

Windows Server 2003 expands on the Windows 2000 Server concept of domain functionality modes to also add functionality based on the mode of the forest. By default, when you create a new domain in a new forest, the functionality level is set to mixed mode for the domain, and Windows 2000 mode for the forest. These levels allow Windows NT 4, Windows 2000, and Windows Server 2003 domain controllers in both the domain and forest.

As you replace or upgrade earlier domain controllers in your forest, you are able to raise the functionality level to support additional features and functionality in the domain and forest. Table 14-1 lists domain functionality levels, while Table 14-2 lists forest functionality levels.

Table 14-1  Domain functionality levels

<table>
<thead>
<tr>
<th>Domain Functionality Level</th>
<th>Domain Controllers Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000 Mixed</td>
<td>Windows NT 4</td>
</tr>
<tr>
<td></td>
<td>Windows 2000</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003</td>
</tr>
<tr>
<td>Windows 2000 Native</td>
<td>Windows 2000</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003</td>
</tr>
<tr>
<td>Windows Server 2003 Interim</td>
<td>Windows NT 4</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003</td>
</tr>
</tbody>
</table>
By default, newly installed domain controllers operate in Windows 2000 mixed functional level for the domain, and Windows 2000 functional level for the forest. This means you can use Windows NT BDCs as domain controllers and Windows 2000 Servers as domain controllers in the Windows Server 2003 domain. This allows you to upgrade an existing Windows NT domain to Windows Server 2003 gradually by first upgrading the Windows NT PDC to Windows Server 2003. You can then use Active Directory to store information about your domain and modify the directory using the Active Directory snap-ins included with Windows Server 2003.

When Windows Server 2003 is operating in Windows 2000 mixed functional level or Windows Server 2003 interim functional level, the Windows NT BDCs are fully functional domain controllers in the Active Directory domain, and maintain a full copy of the domain database. The primary drawback to using mixed mode is that you can’t take advantage of the Windows Server 2003 advanced grouping features, such as the ability to nest groups and create groups with members in different domains or the ability to rename domain controllers or whole domains.

What’s the difference in functionality among the different modes? Table 14-3 provides a quick summary of the domain functionality differences, while Table 14-4 provides a summary for forest functionality differences.

### Table 14-2 Forest functionality levels

<table>
<thead>
<tr>
<th>Forest Functionality Level</th>
<th>Domain Controllers Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000</td>
<td>■ Windows NT 4</td>
</tr>
<tr>
<td></td>
<td>■ Windows 2000</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2003</td>
</tr>
<tr>
<td>Windows Server 2003 Interim</td>
<td>■ Windows NT 4</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2003</td>
</tr>
</tbody>
</table>

### Table 14-3 Domain functionality features

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain controller rename</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Update logon timestamp</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>User password on InetOrgPerson object</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Universal Groups</td>
<td>■ Distribution Groups—Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Note  Windows Server 2003 interim domain functional level is not listed. Use this functional level only when upgrading an entire forest to Windows Server 2003 directly from Windows NT 4. It does not support any Windows 2000 domain controllers in the forest. Its functionality is similar to the Windows 2000 functional level.

When you complete upgrading all the Windows NT BDCs in your domain to at least Windows 2000, you can switch the computer to Windows 2000 native functional level, which enables the advanced grouping capabilities. When all the domain controllers in the domain are running Windows Server 2003, you can upgrade to Windows Server 2003 domain functional level and Windows Server 2003 forest functional level, enabling advanced features such as domain renaming and domain controller renaming. A caution, however. After you switch the operational functional level for the domain or forest to a
higher level, you can’t switch it back without reinstalling Active Directory and completely re-creating the domains. Be sure you have no further need for earlier controllers on your network before changing the functional level.

**Important** After the forest functionality level is raised to Windows Server 2003, no domain controller anywhere in the forest can be at a level below Windows Server 2003. This means you cannot install any earlier servers and promote them to be domain controllers, though they can still be member servers. Be very sure you no longer require earlier domain controllers before taking the final step to bring your forest up to full Windows Server 2003 functionality.

**Changing the Domain Functionality Levels**

To change the domain functionality level, use the following steps:

1. Open the Active Directory Domains and Trusts console.
2. Right-click the domain you want to upgrade, and select Raise Domain Functional Level from the shortcut menu to open the dialog box shown in Figure 14-10.

![Figure 14-10](image)

3. Select the functionality level desired from the Select An Available Domain Functional Level drop-down menu. Only levels that are possible for the selected domain are displayed. Click Raise to bring up a final confirmation dialog box.
4. If you’re sure you want to raise the domain functional level, click OK. (There’s no going back without an arduous restoration of the Active Directory domain from a backup, so make sure you’re ready for this step.)
Note The functional level of the domain refers only to the domain controllers in a particular domain. After raising the functional level, you can still use earlier domain controllers in the same tree, as long as they are located in different domains.

Changing the Forest Functionality Levels
To change the forest functionality level, use the following steps:

1. Open the Active Directory Domains and Trusts console.
2. Right-click at the root (top) of the tree, on Active Directory Domains and Trusts. Select Raise Forest Functional Level from the shortcut menu.
3. Select the functionality level desired from the Select An Available Forest Functional Level drop-down list. Only levels that are possible for the forest are displayed. Click Raise to bring up a final confirmation dialog box. If your current forest cannot be raised, you see the dialog box shown in Figure 14-11.

4. If you’re sure you want to raise the forest functional level, click OK. (There’s no going back, so make sure you’re ready for this step.)

Managing Domain Trust Relationships
The trust relationship between domains is managed in the Trusts tab of a domain’s Properties dialog box. (See Figure 14-12.) When you establish a trust relationship between two domains, users in one domain can access resources located in another trusted domain. An Active Directory domain tree is a collection of domains that share not
only the same schema, configuration, and namespace, but are also connected by trust relationships.

![Figure 14-12  The Trusts tab of the Properties dialog box for a domain](image)

Windows Server 2003 supports three types of trust relationships: the explicit, one-way trusts used by Windows NT; the transitive, hierarchical trusts provided in Active Directory domains; and forest trust relationships that allow you to create transitive or nontransitive trust relationships between two Windows Server 2003 forests. The explicit, one-way trust relationships of Windows NT function in only one direction. For example, when domain A trusts the users in domain B, it doesn’t automatically follow that B trusts the users in A. An administrator must explicitly create the trusts in both directions to achieve a mutual relationship between the domains.

Active Directory automatically creates trust relationships in all the domains in a tree and between all trees in a forest; they run in both directions, and they are transitive. A transitive trust relationship is one that is propagated throughout a tree hierarchy. For instance, when domain A trusts domain B and domain B trusts domain C, domain A trusts domain C. The creation of each new domain in a forest includes the establishment of trust relationships with all the other domains in the tree, enabling users to access resources in any one of the tree’s domains (assuming they have the appropriate permissions) without manual configuration by an administrator.
To provide domain access to users from a domain in another forest or to grant the users in your domain access to another forest, you can manually establish trust relationships by clicking one of the Add buttons in the Trusts tab and specifying the name of a domain. These are one-way relationships; you must establish a trust for each domain to create a bidirectional trust. Depending on the nature of the domain to trust or be trusted, the relationship might or might not be transitive. You can establish a transitive trust relationship with Windows Server 2003 and Windows 2000 domains in another tree or forest, but relationships with Windows NT domains can’t be transitive.

To establish a trust relationship with another domain, you specify the name of the domain in the Add Trusted Domain dialog box and supply a password. To complete the process, an administrator of the other domain must specify the name of your domain in the Add Trusting Domain dialog box and furnish the same password. Both domains must approve before the systems can establish the trust relationship.

**Specifying the Domain Manager**

The third tab in a domain’s Properties dialog box identifies the individual who is the designated manager for the domain. This tab provides contact information about the manager derived from the associated user account in Active Directory. You can change the manager by clicking Change and selecting another user account from the Active Directory display shown. The information is informative, but doesn’t actually do anything.

**Configuring User Principal Name Suffixes for a Forest**

A UPN is a simplified name users can supply when logging on to Active Directory. The name uses the standard e-mail address format consisting of a user name prefix and a domain name suffix, separated by an at sign (@), as defined in RFC 822 (for example, user@example.com). UPNs provide network users with a unified logon name format that insulates them from the Active Directory domain hierarchy and the need to specify the complex Lightweight Directory Access Protocol (LDAP) name for their user objects when logging on.

By default, the suffix of the UPN for users in a particular forest is the name of the first domain created in the first tree of that forest, also called the forest DNS name. Using Active Directory Domains and Trusts Manager, you can specify additional UPN suffixes that users can employ in place of the forest DNS name when logging on. To do this, select the root object in the console tree of the main Active Directory Domains and Trusts display (that is, the object labeled Active Directory Domains and Trusts), and choose Properties from the Action menu. In the UPN Suffixes tab, click Add to specify additional suffixes. These suffixes apply to the entire forest and are available to any user in any domain of any tree in that forest.
Managing Domains
The Active Directory Domains and Trusts snap-in also provides access to the Active Directory Users and Computers snap-in that you use to view and modify the objects in a domain and their properties. When you select a domain in the console tree of the main display and choose Manage from the Action menu, the MMC opens the Active Directory Users and Computers snap-in with the focus on the selected domain.

Using Active Directory Users and Computers
The Active Directory Users and Computers snap-in is the primary tool for Active Directory administrators, and it’s the tool you use most often for day-to-day directory maintenance. Active Directory Users and Computers displays all the objects in a domain by using a Windows Explorer–style expandable tree display. Dialog boxes for each object provide access to the object’s properties, which you can modify to update user information and account restrictions.

You also use Active Directory Users and Computers to create new objects and model the tree hierarchy by creating and populating container objects such as organizational units (OUs). The following sections examine the most common tasks administrators perform using Active Directory Users and Computers.

Launching Active Directory Users and Computers
Active Directory Users and Computers, like most of the Active Directory administration tools, is a snap-in for the MMC. The snap-in file is called Dsa.msc, and you can launch the manager in any one of these three ways:

- Launch Active Directory Users and Computers from the Administrative Tools folder in the Start menu’s Programs group.
- Select a domain in the console tree of the Active Directory Domains and Trusts snap-in, and choose Manage from the Action menu. This opens a new MMC dialog box called Active Directory Users And Computers, leaving the existing Domains And Trusts window intact.
- Open the Run dialog box from the Start menu, and execute the Dsa.msc snap-in file.

To perform many of the functions provided by the Active Directory Users and Computers snap-in, you must be logged on to the domain using an account that has administrative privileges. You can use the Delegation Of Control Wizard to delegate administration tasks for specific objects to other users without giving them full administrative access to the domain, as discussed in “Delegating Object Control” later in this chapter.
Viewing Active Directory Objects

The main Active Directory Users And Computers dialog box (Figure 14-13) contains many of the standard MMC display elements. The console tree (on the left) lists an Active Directory domain and the container objects within it in an expandable display. The result pane (on the right) displays the objects within the highlighted container. The manager includes a specialized toolbar providing quick access to commonly used functions and a description bar that provides information about the manager’s status or the currently highlighted object. The program displays the actions you can perform on each object in the Action menu after you click the objects.

Figure 14-13 The main Active Directory Users And Computers dialog box

Active Directory Object Types

The objects in the Active Directory Users And Computers dialog box represent both physical entities, such as computers and users, and logical ones, such as groups and organizational units. The default object types in a newly created Active Directory domain are listed in Table 14-5.

Table 14-5 Object types created in a new Active Directory domain

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>![Domain Icon]</td>
<td>Root object of Active Directory Users and Computers display; identifies the domain currently being administered by the manager.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>![Organizational Unit Icon]</td>
<td>Container object used to create logical groupings of computer, user, and group objects.</td>
</tr>
</tbody>
</table>
By modifying the schema that controls the directory service structure, you can create new object types in Active Directory and modify the attributes of existing types. For more information, see Chapter 15.

**Normal Mode vs. Advanced Mode**

By default, the Active Directory Users and Computers snap-in is displayed in normal mode with only the objects that administrators use most often visible. This also hides certain tabs in an object’s Properties dialog box from view, including the Object tab and the Security tab that you use to set permissions for the object.

When you choose Advanced Features from the manager’s View menu, however, the display changes to include all the system objects in Active Directory, which represent policies, DNS records, and other directory service elements, as well as the LostAndFound container, as shown in Figure 14-14.

From this interface, you can view information about the system objects and control access to them by modifying the associated permissions. Because access to these objects isn’t required as frequently, you can suppress their appearance by leaving the manager in normal mode. However, when you want to modify the permissions for standard objects such as organizational units, users, and groups, you must enable Advanced Features to see the Security tab in an object’s Properties dialog box.
Changing the Domain

You can use the Active Directory Users and Computers snap-in to administer any domain on the network. To change the currently displayed domain in the manager, select the root or domain object in the console tree and choose Connect To Domain from the Action menu. This displays the Connect To Domain dialog box, where you can type the name of the domain or browse to another domain.

From the Action menu, you can also choose Connect To Domain Controller to access the selected domain by using a specific domain controller on the network. Unless your domain controllers are out of sync, the information should be the same on all the replicas, but sometimes you might want to select a domain controller at a different location to avoid a slow or expensive WAN connection.

Using Filters to Simplify the Display

When you begin to populate Active Directory with new objects, it can rapidly grow to an unwieldy size. The sheer number of objects in the display can make locating the specific object you need difficult. To temporarily suppress the display of objects you don’t need to see, you can apply a filter to the Active Directory Users and Computers snap-in based on object types or based on the contents of specific object attributes.

When you choose Filter Options from the View menu, the Filter Options dialog box appears, as shown in Figure 14-15. Here you can opt to display all object types, select specific object types to display, or build a custom filter based on object attributes.
Figure 14-15  The Filter Options dialog box of Active Directory Users and Computers

When you select the Create Custom option and click Customize, you see a Find Custom Search dialog box like the one shown in Figure 14-16. In this dialog box, you can select an object type, choose an attribute of that object, and specify a full or partial value for that attribute.

For example, you can display only the user objects that have the value Sales in the Department attribute (as shown in the figure), or you can choose to display only the users that have a particular area code in the Telephone Number attribute. This enables you to quickly zero in on the objects you need to use without scrolling through an unnecessarily cluttered display.

Figure 14-16  The Find Custom Search dialog box of Active Directory Users and Computers
Finding Objects
You can also search for specific objects in the entire Active Directory without modifying the manager’s display. By selecting the domain object and choosing Find from the Action menu, you display the Find Users, Contacts, And Groups dialog box (shown in Figure 14-17), in which you can specify the type of object you want to locate, a specific domain, or the entire directory, and the name and description of the object.

![The Find Users, Contacts, and Groups dialog box of Active Directory Users and Computers](image)

Figure 14-17  The Find Users, Contacts, And Groups dialog box of Active Directory Users and Computers

The program then searches the Global Catalog to locate the desired object. The GC is a subset of the entire Active Directory, containing only the most commonly used attributes, which makes it easier to search for a specific object. Without the GC, the task of searching an Active Directory installation that includes domain controllers in remote locations can require extensive WAN traffic that is both slow and expensive.

**Note** Although Active Directory always creates the GC on the first domain controller for a domain, you can change its default location by modifying the NTDS settings in the Active Directory Sites and Services snap-in. You can also specify additional attributes that are to be stored in the GC by using the Active Directory Schema snap-in.

The Advanced tab in the Find Users, Contacts, And Groups dialog box uses the same interface as the Custom Filter feature discussed in the previous section. In the same way, you can search for objects based on any of their attributes. If an attribute you select isn’t part of the GC, the search proceeds by looking through the actual contents of the domain controllers on your network. In some cases, this can slow down the search process considerably.
Default Active Directory Objects

A newly created Active Directory domain contains organizational unit, computer, user, and group objects that the Active Directory Installation Wizard creates by default. These objects provide access to the system at several levels and include groups that enable administrators to delegate specific network maintenance tasks to others. Even if you don’t expect to use these objects in the future, you must use them to create other objects with the appropriate permissions for your network.

If, for example, you don’t want to have any single user with the full control granted to the Administrator account, you must still log on as administrator to create new user objects with the rights and permissions you want. With Active Directory, you can “orphan” parts of the directory structure if you modify, delete, or disable the Administrator account without first creating other user objects and granting them equivalent permissions to the various parts of the directory.

The default objects created in an Active Directory domain, along with their functions and their locations in the domain hierarchy, are listed in Table 14-6.

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Object Type</th>
<th>Location</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Builtin</td>
<td>Container</td>
<td>Domain root</td>
<td>Default container for groups providing access to server administration functions.</td>
</tr>
<tr>
<td>Computers</td>
<td>Container</td>
<td>Domain root</td>
<td>Default container for upgraded computer accounts.</td>
</tr>
<tr>
<td>Users</td>
<td>Container</td>
<td>Domain root</td>
<td>Default container for upgraded user accounts.</td>
</tr>
<tr>
<td>Domain Controllers</td>
<td>Organizational Unit</td>
<td>Domain root</td>
<td>Default container for new Windows Server 2003 domain controllers.</td>
</tr>
<tr>
<td>Account Operators</td>
<td>Security Group—Builtin Local</td>
<td>Builtin</td>
<td>Members can administer domain user and group accounts.</td>
</tr>
<tr>
<td>Object Name</td>
<td>Object Type</td>
<td>Location</td>
<td>Function</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Administrators</td>
<td>Security Group—</td>
<td>Builtin</td>
<td>Members can fully administer the computer or domain.</td>
</tr>
<tr>
<td></td>
<td>Builtin Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup Operators</td>
<td>Security Group—</td>
<td>Builtin</td>
<td>Members can bypass file security to back up files.</td>
</tr>
<tr>
<td></td>
<td>Builtin Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guests</td>
<td>Security Group—</td>
<td>Builtin</td>
<td>Users are granted guest access to the computer or domain.</td>
</tr>
<tr>
<td></td>
<td>Builtin Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Print Operators</td>
<td>Security Group—</td>
<td>Builtin</td>
<td>Members can administer domain printers.</td>
</tr>
<tr>
<td></td>
<td>Builtin Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replicator</td>
<td>Security Group—</td>
<td>Builtin</td>
<td>Supports file replication in a domain.</td>
</tr>
<tr>
<td></td>
<td>Builtin Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Operators</td>
<td>Security Group—</td>
<td>Builtin</td>
<td>Members can administer domain servers.</td>
</tr>
<tr>
<td></td>
<td>Builtin Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>Security Group—</td>
<td>Builtin</td>
<td>Ordinary users.</td>
</tr>
<tr>
<td></td>
<td>Builtin Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Domain Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP Administrators</td>
<td>Security Group—</td>
<td>Users container</td>
<td>Members who can administer a DHCP server.</td>
</tr>
<tr>
<td></td>
<td>Domain Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP Users</td>
<td>Security Group—</td>
<td>Users container</td>
<td>Members who have read-only access to DHCP server.</td>
</tr>
<tr>
<td></td>
<td>Domain Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DnsAdmins</td>
<td>Security Group—</td>
<td>Users container</td>
<td>DNS administrators.</td>
</tr>
<tr>
<td></td>
<td>Domain Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAS and IAS Servers</td>
<td>Security Group—</td>
<td>Users container</td>
<td>RAS and IAS servers.</td>
</tr>
<tr>
<td></td>
<td>Domain Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WINS Users</td>
<td>Security Group—</td>
<td>Users container</td>
<td>Members that have read-only access to WINS. (Created only if WINS is installed on the network.)</td>
</tr>
<tr>
<td></td>
<td>Domain Local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DnsUpdateProxy</td>
<td>Security Group—</td>
<td>Users container</td>
<td>DNS clients that are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).</td>
</tr>
<tr>
<td></td>
<td>Global</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Admins</td>
<td>Security Group—</td>
<td>Users container</td>
<td>Designated administrators of the domain.</td>
</tr>
<tr>
<td></td>
<td>Global</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Computers</td>
<td>Security Group—</td>
<td>Users container</td>
<td>All workstations and servers joined to the domain.</td>
</tr>
<tr>
<td></td>
<td>Global</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Creating an Organizational Unit

The directory service schema dictates which objects you can create in an Active Directory domain, where they can be located, and which attributes they are permitted to have. Active Directory Users and Computers lets you create objects only in locations appropriate to the object type. For example, you can’t create an organizational unit (OU) object that is subordinate to a user object, but a user object can be subordinate to an OU object.

OUs can be subordinate to each other, however, and the number of OU layers you can create in your Active Directory domain is unlimited. To create an OU, click the domain object or another OU in the Active Directory Users and Computers scope or result pane,
choose New from the Action menu, and select Organizational Unit. You can also click Create New Organizational Unit on the Active Directory Users and Computers toolbar to achieve the same effect. After you specify a name for the new object in the Create New Object dialog box, the manager creates an icon with the appropriate name and inserts it into the Active Directory Users and Computers display.

After you create an OU, you can populate it with other objects, such as users, computers, groups, and other OUs, or you can modify its attributes by opening the Properties dialog box from the Action menu.

**Configuring OU Objects**

The Properties dialog box for an OU includes three tabs: General, Managed By, and Group Policy. The General tab and the Managed By tab enable you to specify information about the OU such as a descriptive phrase and an address for the location of the object, as well as the identity of the person responsible for managing the OU. The information you include in these tabs (if any) depends on the criteria you use to design your Active Directory. An OU can be associated with a particular department within an organization; a physical location such as a room, a floor, or a building; or even a branch office in a particular city or country.

The Group Policy tab is where you create and manage the links to Group Policy objects in Active Directory. Group Policy objects are collections of system settings that control the appearance and functionality of network clients. When you apply group policies to OUs, domains, and sites, all the objects contained in those entities inherit the system settings. You can link OUs to multiple Group Policy objects in this tab, and you can control the priorities with which the policies are applied. When you use the Edit button in the Group Policy tab to modify a Group Policy object, Active Directory Users and Computers launches the Group Policy snap-in for the MMC. (For more about setting group policy and using the Group Policy snap-in, see Chapter 11.)

---

**Note** If you install the Group Policy Management Console (GPMC) described in Chapter 11, the tab will change accordingly.

When you enable Advanced Features in the Active Directory Users and Computers View menu, the OU’s Properties dialog box also displays the Object tab (shown in Figure 14-18) and the Security tab (shown in Figure 14-19). The Object tab displays the full path to the object in the domain hierarchy, the dates and times of its creation and last modification, and the update sequence numbers from when it was created and last modified.
Figure 14-18  The Object tab of an OU's Properties dialog box

Figure 14-19  The Security tab of an OU's Properties dialog box
The Security tab enables you to control access to the object by assigning permissions to users and groups. When you click Advanced, you see the Permissions tab (shown in Figure 14-20), and by selecting the Allow Inheritable Permissions check box, you can also control whether the object inherits permissions that have been assigned to its parent object.

![Figure 14-20 The Permissions tab](image)

**Delegating Object Control**

Active Directory is designed to support much larger enterprise networks than Windows NT domains, and larger networks naturally require more attention and maintenance from administrators. Active Directory makes it possible for administrators to delegate control over specific tasks to other users without giving them full access to the domain. To do this, launch the Delegation Of Control Wizard by choosing Delegate Control from the Action menu for a domain or organizational unit.

The wizard first prompts you to specify the users, groups, or both to whom you want to delegate control. After you do this, the wizard displays the Tasks To Delegate page (shown in Figure 14-21) that you use to specify which types of tasks in the container the selected users or groups should be able to control. This list of tasks is object sensitive and is different for different objects.
After you supply the wizard with the appropriate information, it configures the selected object with the appropriate permissions.

**Real World  Think Before You Delegate**

The Delegation Of Control Wizard makes it easy to delegate control over Active Directory tasks—too easy sometimes. Before you start delegating away your administrative authority, take the time to sit down and come up with a maximum of three or four types of administrators to whom you’d like to delegate control, and create the appropriate groups. Then use the Delegation Of Control Wizard to delegate control to the appropriate groups. (Don’t delegate to individual users.) Some suggested groups and their functions are as follows:

- **Help Desk Admins**  Reset passwords (after all, what’s the Help desk for?)
- **Active Directory Admins**  Manage users, groups, and computer accounts
- **Domain Admins**  Windows Server 2003 built-in group for administration within a domain
- **Enterprise Admins**  Windows Server 2003 built-in group for administering domains, forests, trusts, and replication

If you need to provide an even finer grained control over specific objects and specific permissions on those objects within the container, you can create a custom task. Just select Create A Custom Task To Delegate on the Tasks To Delegate page to bring up the Active Directory Object Type page, shown in Figure 14-22.
Security Alert Creating a custom delegation task gives you great freedom and power. But most organizations will find the preconfigured tasks in the Delegation Of Control Wizard are sufficient. Resist the temptation to create a custom task unless you have a thorough understanding of both the Active Directory objects you’re modifying and the business need you’re solving. You can easily delegate more control than you intend, creating a security problem that will be difficult to identify.

![Delegation of Control Wizard](image)

**Figure 14-22** The Active Directory Object Type page

From here, you can select the individual objects that the task will apply to. When you have the objects selected, click Next to bring up the Permissions page to set the specific permissions you want to grant as part of this task.

Whether you use one of the preconfigured tasks or create a custom task, you have one last chance to see all your changes and confirm them before the delegation takes place. Make sure you have correctly identified the objects and permissions you want to grant, especially if you created a custom task, before clicking Finish to make the actual changes.

**Note** If you check out the Security tab in the object’s Properties dialog box (which is visible only when Advanced Features is enabled in the Active Directory Users and Computers View menu), you can see the permissions that the wizard has assigned to the users or groups you selected.
Creating a User Object

A typical Active Directory installation usually consists of more user objects than any other type, and the creation and management of user objects accounts for much of the Active Directory administration burden. The task of manually creating a user object is just like that of creating an organizational unit or any other object. After selecting the container in which the user object will reside (usually an OU), you select the container and choose New from the Action menu and select User or click Create New User on the Active Directory Users and Computers toolbar, producing the dialog box shown in Figure 14-23.

Figure 14-23  The New Object - User dialog box

In the New Object - User dialog box, you specify the first and last name of the user and the logon name that the user will supply when connecting to the network. The earlier logon name for the user (that is, the name with which the user will log on at Windows NT, Windows 95, or Windows 98 workstations) then appears automatically. The next dialog box provides a field for the user object’s password and enables you to set basic password and account options for the user, as follows:

- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled

After presenting a summary screen confirming your input, Active Directory Users and Computers creates the user object in the container you selected.
Using the Command Line to Add a User

Manually creating users using the GUI just doesn't make a lot of sense if your network has more than a few users. You can, however, easily add users via the command line with the NET USER command, and manage what groups users are in with the NET GROUP command. Unfortunately, the NET USER command, a legacy from the Windows NT days, doesn't really understand OUs and will put newly created users in the main Users container. To go beyond NET USER and NET GROUP, you'll need to use tools such as the “ds*” tools (dsadd, dsget, and so on) which are, frankly, painful and awkward to use. To add the user “charlie” and assign him to the groups “Domain Admins” and “Domain Users”, you would type the following at the command prompt:

```
net user charlie * /add /expires:never /passwordchg:yes /domain
net group "Domain Admins" Charlie /add
```

The first line creates a domain user account and will prompt for the password for the account, and then repeat the prompt to ensure it was typed correctly. The password is displayed as * as it's typed. The second line adds the user to the “Domain Admins” group. New accounts are automatically added to the Domain Users account.

**Note** You can also predetermine the Active Directory containers in which new user and computer accounts will be created by using Rediruser.exe and Redircomp.exe, which are described in Microsoft Knowledge Base Article 324949 ([http://support.microsoft.com/kb/324949](http://support.microsoft.com/kb/324949)).

Use Template Objects and Copy Them

Although you certainly *can* create each of your user objects discretely, it is a pain if you have a lot of configuration to do afterward to ensure they're in the right groups, have the right home directories and profiles, and so on. A better way is to create templates of the different kinds of user you'll have and then copy the template user to create new users. This ensures that each user is created with the same settings and configuration as all the other users created from a particular template, greatly reducing the chance of error.

Configuring User Objects

After you create a user object, you can proceed to the configuration process, in which you add information about the user to the Active Directory database and define the user’s access to the network. The Action menu that Active Directory Users and Computers generates when you click a user object contains several of the commands most commonly
used by administrators, as well as access to the Properties dialog box for the user. These commands are as follows:

■ **Copy**  Copies an existing user as a template for a new user.

■ **Add To A Group**  Generates a dialog box from which you can select the groups to which the user will belong.

■ **Name Mappings**  Enables administrators to map X.509 certificates and Kerberos names to the user object. This command is visible only when Advanced Features is enabled.

■ **Disable Account**  Prevents the user from logging on to the network using the account until it is manually enabled by an administrator.

■ **Reset Password**  Generates a dialog box with which you can modify the user account's logon password.

■ **Move**  Enables administrators to move the user object to another container object (that is, domain or organizational unit) in Active Directory.

■ **Open Home Page**  Opens the default browser on the system, and displays the URL listed in the Home Page field on the General tab of the user object’s Properties dialog box.

■ **Send Mail**  Opens the default e-mail client on the system, and addresses a message using the e-mail address listed in the E-Mail field on the General tab of the user object’s Properties dialog box.

Active Directory Users and Computers provides these functions on the Action menu for the sake of convenience, but you can also access most of them through the user object’s Properties dialog box, which provides a complete interface to the object’s attributes. The following sections examine the 13 tabs in this dialog box and the functions located on each one. If you have Advanced Features enabled from the View Menu, you have at least 16 tabs.

---

**Note**  The attributes appearing on the tabs of the Properties dialog box are those included in the default schema used by Active Directory. You can modify the schema to create additional attributes or change existing ones using the MMC Active Directory Schema Manager snap-in. See Chapter 15 for more information about using this tool.

---

**The General Tab**  
The General tab contains basic information about the user, including the first and last names you specified when creating the object. This tab also has fields for a descriptive phrase about the user, office location, and the user’s telephone number, e-mail address,
and home page URL. Apart from the \textit{name} fields, the information on this tab is optional and is used solely for reference purposes. Users can search Active Directory using the values of the attributes on this (and other) tabs and automatically insert the user’s e-mail address and home page URL into the appropriate client applications, but these fields don’t affect the user’s access to the network in any palpable way.

\textbf{The Address Tab}

On the Address tab, you find fields where you can insert mailing address information for the user. As on the General tab, these are reference fields that don’t play a major role in the object’s configuration, but they do provide a way to centralize the information storage for individuals in your organization. As with all the information in Active Directory, you can search on the fields, insert the value into other objects, and generally do all the things you’d expect to be able to do with a database.

\textbf{The Account Tab}

The Account tab contains the user logon name you specified during the creation of the object, as well as its earlier user name.

The Logon Hours button and the Logon To button provide access to dialog boxes that enable you to restrict the hours and days of the week that the user is permitted to log on to the network and the workstations from which the user can log on to the network.

The Account Locked Out check box is selected whenever the user account has been disabled, either deliberately by an administrator or because of repeated logon failures. Clearing this check box releases the account and permits the user to log on again. The Account Options area contains the password and account options settings. When creating new user accounts, the following options must be selected or cleared:

- **User Must Change Password At Next Logon**  
  Presents the user with a dialog box during the next logon event requiring a new password

- **User Cannot Change Password**  
  Prevents the user from changing his or her own password

- **Password Never Expires**  
  Prevents the user account from being subject to expiration policies defined in the Account Expires box

- **Account Disabled**  
  Prevents the user from logging on using this account until it is cleared by an administrator

Finally, the Account Expires area lets you set an expiration date for the user account. The default is for the account to never expire, but you can use the expiration feature to easily manage accounts for temporary workers or automatically expire the accounts of departing users.
The Profile Tab
On the Profile tab, you can specify the location of the user profile associated with the object. By default, every user who logs on to a Windows Server 2003 system has a profile directory created in the Documents And Settings folder on the system drive. When you specify a profile path on this tab, the system stores a copy of the profile in the specified directory. If this directory is located on a shared network drive, the user can access the profile from any system on the network. The Logon Script field specifies the name of the script that the workstation should execute when the user logs on to the network.

From the Home Folder box, you can create a personal folder on a network drive over which the user has full control. Storing data files on a network drive makes it easier to protect them from tampering and accidental erasure, as well as simplifying backup strategies. You can configure the workstation to map a drive to the shared drive automatically during the logon process by specifying a drive letter and the UNC name of a network share in the Connect fields.

The Telephones Tab
The Telephones tab contains fields for all the various phone numbers associated with a user, including pager, mobile, fax, and IP phone numbers. A multiline Notes field provides a general-purpose area for notes.

The Organization Tab
The Organization tab provides fields in which you can specify the user’s title, department, and company. In the Manager box, you can identify the user’s superior by selecting another user object from Active Directory. There is also a multiline Direct Reports field.

The Member Of Tab
The Member Of tab is where you specify the groups that the user should be a member of. Clicking Add displays an object listing from which you can select the appropriate groups. The Set Primary Group button is enabled only if the user belongs to several groups. The primary group doesn’t have a significant impact on Windows Server 2003 users but is important for Macintosh and UNIX users. Windows Services for Macintosh recognizes a single group affiliation—usually the group with which the Macintosh user shares documents on a server—while Windows Services for UNIX can map Windows groups to UNIX groups and uses the Primary group for the logon group in UNIX.

Note You can also add a user to a group from the Members tab of the group object’s Properties dialog box.
The Dial-In Tab
On the Dial-In tab, you control whether the user should be permitted access to the network through a dial-in Remote Access Service (RAS) connection. You can also set whether the user must use callback or a verified caller ID for security verification, and you can assign a static IP address and static routes for the connection.

The Environment Tab
The Environment tab has settings for controlling the user experience when connecting via Terminal Services. You can set a specific startup program, connect client drives and printers, or set the default printer to the client default.

The Sessions Tab
The Sessions tab has settings for controlling Terminal Services idle timeout and reconnection settings.

The Remote Control Tab
The Remote Control tab has settings for managing the remote control settings on a Terminal Services session. You can enable or disable remote control, set it to require or not require user permission, and set whether you are able to only view a user’s session or actually interact with it.

The Terminal Services Profile Tab
The Terminal Services Profile tab allows you to set a different user profile when logged on to a Terminal Services session. Any settings that aren’t explicitly set here default to the regular profile. Also on this tab you can enable or disable Terminal Services for the user.

The COM+ Tab
The COM+ tab allows you to designate the user’s COM+ partition set.

The Published Certificates Tab
The Published Certificates tab, which is visible only when you enable the Active Directory Users and Computers Advanced Features display option, lets you manage the X.509 certificates linked to the user object. From this page, you can view the certificates published for the user account, add new certificates, remove certificates, and export certificates to files.

The Object Tab
The Object tab, visible only when Advanced Features is enabled, displays the full pathname of the user object, the dates it was created and last modified, and the update sequence numbers (USNs) from when it was created and last modified.
The Security Tab

The Security tab, also visible only when Advanced Features is enabled, lets you assign permissions that control access to the user object. The tab is virtually identical to the same tab in the Properties dialog boxes for other object types. Chapter 9 has more information about the creation and configuration of user accounts.

Creating a Group

Groups make it possible to assign permissions and other attributes to multiple users in a single operation, as well as to distribute e-mail to a large number of addresses (when Microsoft Exchange Server is installed). When you assign permissions to an Active Directory object (or to an NTFS file or directory), you can add groups to the object’s access control list (ACL), which causes the permissions to be propagated to all the group’s members. You create group objects in Active Directory Users and Computers just as you do any other object type, and then you select the objects you want to be members of the group.

Group objects can exist in organizational units, in other groups (when the domain is no longer operating at the Windows 2000 mixed functionality level), or directly beneath the domain root. When you select one of these container objects in Active Directory Users and Computers, choose New from the Action menu, select Group, and you will see the New Object - Group dialog box, shown in Figure 14-24.

![Figure 14-24 The New Object - Group dialog box](image)

Chapter 14 Installing and Configuring Active Directory 423
As with other objects, you must first specify a name (up to 64 characters long) for the new
group and an earlier NetBIOS name equivalent (up to 15 characters long). Then in the
Group Scope area, select one of the following options:

- **Domain Local**  A Domain Local group can contain user objects, other Domain
  Local groups in the same domain, Global groups from any domain in the forest,
  and Universal groups. You can insert Domain Local groups into the ACL for any
  object in that domain but not for objects in other domains. Domain Local groups
don’t appear in the GC.

- **Global**  A Global group can contain user objects and other Global groups from the
  same domain. Unlike Domain Local groups, you can insert Global groups into the
  ACL for any object in the forest. Global groups are included in the GC, but their
  members are not; Global group memberships are replicated only within their
domain.

- **Universal**  The most comprehensive group scope, a Universal group can contain
  other Universal groups, Global groups, and users from any domain in the forest.
  Like Global groups, you can insert Universal groups into the ACL for any object in
  the forest. Universal groups appear in the GC with their members; using Global
  groups as members of the Universal group lessens the update traffic to the GC
  because changes to the Global group memberships (which aren’t included in the
  catalog) are far more frequent than changes to the Universal group memberships.

---

**Note**  Group nesting (that is, the storage of groups within other groups) is an
Active Directory feature that is available only when the domain is running at least
at the Windows 2000 native functional level (except, of course, the ability to place
Global groups in Local groups as was possible with Windows NT 4). To operate at
the Windows 2000 native functional level, all the domain’s controllers must be
running Windows 2000 Server or Windows Server 2003. For more information
about raising the functional level of a domain, see “Domain and Forest Function-
ality” earlier in this chapter.

After selecting the group scope, select one of the following group types:

- **Security**  Security groups are intended for inclusion in the ACLs of network
  resources such as files and printers. They can also serve as distribution lists for
  e-mail.

- **Distribution**  Distribution groups are intended solely for use as e-mail distribution
  lists.

When you click OK, the manager creates the group object in the container you selected.
Configuring Group Objects

The Properties dialog box for a group object contains up to six tabs (depending on whether Advanced Features is enabled), as discussed in the following sections.

**The General Tab**
The General tab provides fields into which you can insert a description of the group object. It specifies the group’s type and scope, and includes a multiline field for comments.

**The Members Tab**
The Members tab is where you specify the objects that are to be the members of the group. Clicking Add produces a dialog box in which you can browse Active Directory and select the desired objects.

**The Member Of Tab**
When no longer operating at the Windows 2000 mixed functionality level, Active Directory group objects can be members of other objects. On the Member Of tab, you can select the groups that the new group is to be a member of.

**The Managed By Tab**
The Managed By tab enables you to specify information about the person responsible for administering the group object.

**The Object Tab**
The Object tab (which appears only when Advanced Features is enabled in Active Directory Users and Computers) displays the full canonical name of the group object, the dates of its creation and last modification, and its USNs at its creation and last modification.

**The Security Tab**
The Security tab (which appears only when Advanced Features is enabled in Active Directory Users and Computers) enables you to set the permissions that specify which objects will have access to the group object and how much access they will have.

Creating a Computer Object

In addition to container objects, group objects, and user objects, Active Directory also has objects representing computers. To log on to a domain, a Windows Server 2003 computer must have an object representing it in the Active Directory hierarchy. When you promote a system to a domain controller or log on to a domain for the first time, Windows Server 2003 automatically creates a computer object. (In the case of a first-time
logon event, the system prompts for the user name and password of an account with sufficient privileges to create new objects. However, you can also create computer objects manually, just as you create any other object.

Selecting a container, choosing New from the Action menu, and selecting Computer produces a New Object—Computer dialog box in which you supply the DNS and NetBIOS names for the new computer object. You can also specify the particular user or group that is authorized to join the computer to the domain and whether this account is for a pre–Windows 2000 computer, or if this account should be for a backup domain controller.

Note The Active Directory Users and Computers snap-in creates objects one at a time, but sometimes administrators have to create a great many objects, and this tool becomes impractical. For more information about creating objects en masse, see Chapter 15.

Configuring Computer Objects

After Active Directory Users and Computers creates the computer object, you can configure its attributes using the following nine properties: General, Operating System, Member Of, Delegation, Location, Managed By, Object, and Security, and Dial-in. Almost all the tabs have the same purpose as those in other objects. The four that are unique to the computer object are Operating System, Location, Delegation, and Dial-in.

The Operating System tab identifies the operating system running on the computer, the version, and the currently installed service pack. These fields are not editable; they are blank when you manually create a computer object and are filled in when the computer joins a domain. The Location tab enables you to specify which locations are served by the site in the directory setup, the Delegation tab allows you to set a computer as trusted for delegation, and the Dial-in tab allows you to set the Dial-in policy for this computer account.

Security Alert Enabling Trusted For Delegation on a computer account can open up the possibility of sophisticated security attacks to your network. Be sure you thoroughly understand the implications of enabling delegation, and restrict the services and computers that are trusted for delegation.

Using Remote Computer Management

Active Directory Users and Computers provides administrative access to remote computers represented by objects in Active Directory. When you click a computer object and choose Manage from the Action menu, the manager opens the MMC Computer
Management snap-in with that computer as its focus. With this capability, you can read the remote system’s event logs, manipulate its services, and perform many of the other tasks provided by the Computer Management snap-in.

**Note** For more full-featured remote administration of Windows 2000 Servers, Windows Server 2003 servers, or Microsoft Windows XP Professional desktops, use Terminal Services (also known as Remote Desktop), as described in Chapter 30.

### Publishing a Shared Folder

Shared folder objects enable you to publish shared network directories in Active Directory, allowing users to access them directly by browsing in the Network Neighborhood for the object. This eliminates the need for users to know the exact location of the shared folder. Creating a shared folder object doesn’t actually create the share; you must do this manually on the Sharing tab of the drive or folder’s Properties dialog box in the Windows Explorer window or the My Computer window. You can also create shared folder objects from Distributed file system (Dfs) folders (which are discussed in Chapter 20).

To create a shared folder object, click a container object in Active Directory Users and Computers and choose New from the Action menu, and then select Shared Folder. In the Create New Object dialog box, specify a name for the new object and type the UNC pathname to the share. After the manager creates the object, you can configure it using the tabs in the object’s Properties dialog box.

**Note** The permissions you set on the Security tab of the shared folder’s Properties dialog box don’t control access to the shared folder itself, only to the shared folder object. To access the folder using Active Directory, a user must have permission to access both the share and the object. The same is true for a printer object.

### Publishing a Printer

Creating a printer object enables users to access the printer through Active Directory in much the same way that they can access shared folders. You create a printer object just as you do a shared folder object, by selecting a container and choosing New\Printer from the Action menu and specifying the UNC path to the shared printer. The manager then creates the object, combining the name of the host system and the share to form the object name. For more information about printer administration, see Chapter 8.
Moving, Renaming, and Deleting Objects

After you create objects in Active Directory, you can use Active Directory Users and Computers to remodel your tree at any time by moving objects to different containers, renaming them, and deleting them. The Action menu for nearly every Active Directory object contains a Move command that opens a dialog box in which you can browse for a container where you want to place the object. You can also select several objects by holding down the Ctrl key while clicking them and moving them all to the same container. Or simply use the Drag and Drop procedure to move objects around as you want.

Moving a container object to a new location automatically moves all the objects within the container at the same time and also modifies the references to that object in all other Active Directory objects. If, for example, User X is a member of Group Y and you move the organizational unit containing X’s user object to a new location, X remains a member of Y, and Group Y’s member list is automatically updated to show X in its new location. In the same way, when you rename an object using the Rename command on the Action menu or by clicking the object once, all the references to that object throughout Active Directory change to reflect the new name. When you delete a container object, all the objects in the container are deleted as well.

Important Moving user and computer objects when Group Policy is being used to manage and deploy features can have unexpected side effects.

Renaming a Domain Controller or a Whole Domain

No matter how carefully you choose a naming convention on your network, sooner or later you wish you named one or more areas of the network differently. Maybe the division the network serves has had a major name change, or you consolidated all your West Coast operations into your Oakland office, but there are still compelling security reasons why you don’t want to consolidate domains, at least not yet. Or maybe, with all the planning you did, you still made an essential mistake in the naming of your domain controllers and you’d really like to fix it.

In a Windows 2000 domain or forest, there wasn’t a whole lot you could do about it without experiencing substantial pain. A domain really couldn’t be renamed or moved around in the forest, and even changing the machine name of a domain controller required demoting the domain controller (one reboot), changing the name (another reboot), and then promoting the machine to be a domain controller again (reboot number three). In short, it was a bit more work than it should have been and a procedure that would seriously affect your network while you did it.
Renaming a Domain Controller

In a domain that is at the Windows 2000 native functionality level, the only way you can rename a domain controller is to demote the domain controller, rename the machine, and then repromote the machine to be a domain controller again. A tedious task at best, and one that requires three reboots. In Windows Server 2003, however, if your domain functionality level has been raised to Windows Server 2003 level, which requires that all domain controllers in the domain are Windows Server 2003 servers, you can rename a domain controller without first demoting it, and with only a single reboot. This makes it much more feasible and simplifies the overall management of your network.

To rename a domain controller, take the following steps:

1. Log on to the domain controller to be renamed with an account with either Domain Admins or Enterprise Admins authority, or use runas to get to the necessary administrative level.
2. Open a command window.
3. Add a new name to the domain controller machine using netdom:
   
   ```
   netdom computername <CurrentName> /add:<NewName>
   ```

4. Make the new name the primary one using netdom:
   
   ```
   netdom computername <CurrentName> /makeprimary:<NewName>
   ```

5. Restart the computer.
6. Remove the original name using netdom:
   
   ```
   netdom computername <NewName> /remove:<CurrentName>
   ```

**Important** It takes a finite amount of time for changes to Active Directory and DNS records to propagate to all the places they need to propagate. How long depends on a variety of factors, but mostly on how you have your network configured. Allow sufficient time at each step for changes to propagate.

If changes have not propagated thoroughly, some clients might have problems accessing the domain or logging on, especially after the /makeprimary step.

Renaming Domains

Windows Server 2003 adds a completely new functionality to the Active Directory—the ability to rename an entire domain, restructuring the forest. This is a powerful new tool in the enterprise administrator’s arsenal, but one that should be used with extreme caution.
The latest versions of these tools, along with full documentation on using them, and all the steps that need to be performed to restructure your domain can be found at: http://www.microsoft.com/windowsserver2003/downloads/domainrename.mspx. Always check this site for the most current version of the tools and for updated documentation about this procedure.

Using Active Directory Federation Services

Windows Server 2003 R2 includes the new Active Directory Federation Service (ADFS) as an optional installation. ADFS enables federated identity management between Active Directory forests that have no trust relationship. ADFS uses the WS-Federation specification of Web Services Security (WS-Security) specifications. In its initial release, ADFS supports only the Passive Requestor Profile (WS-F PRP).

That's all nice, but what does it mean and why do you care? Let's start by looking at the problem it's trying to solve: how to securely identify a user without directly knowing anything about the user except the organization that the user comes from. Let's look at a typical scenario. You have an extranet that you need to allow business partners access to, in a secure way, without actually creating domain accounts for them. This is a common scenario these days, and one that had all sorts of complications before ADFS. If you provided a generic or even user-specific account that your partner could use, you have the problem of somehow keeping the account database up to date and accurate—a hard enough task with your own employees.

ADFS resolves the problem by providing a secure way for your extranet application to get confirmation from your partner's Active Directory that the individual requesting access is a valid and authenticated user. And it does so without having to establish a trust relationship between the two Active Directory forests.

To install ADFS, you'll need to first install IIS6, and enable Secure Sockets Layer (SSL) with an appropriate certificate. And you'll also need ASP .NET 2.0 installed (though the wizard will actually manage to do the ASP .NET installation automatically). Because running a Web server on your domain controller is not generally a good idea, ADFS should normally not be installed on a domain controller. Your publicly visible Web server installs the ADFS Web Agent, which can connect to the Federation Service.

Once installed, ADFS adds a new management console, the Active Directory Federation Services console, as shown in Figure 4-25. From this console, you can configure your organization's settings and establish partner accounts. ADFS recognizes two kinds of partners:

- **Account Partners**  
  External organizations whose accounts you use and enable

- **Resource Partners**  
  External organizations whose resources your organization uses
Figure 14-25  The Active Directory Federation Services console


Summary

This chapter has covered the basic tools and techniques for administering Active Directory in Windows Server 2003. Active Directory Users and Computers, in particular, is a tool that administrators use frequently to perform day-to-day maintenance tasks. The next chapter covers Active Directory tools that you’ll use far less often.
Chapter 15
Managing Active Directory

Using Active Directory Sites and Services ................................................. 433
Using Active Directory Schema ................................................................. 445
Summary .................................................................................................. 467

 Tasks such as promoting domain controllers and creating and configuring users and other objects are required in every Active Directory installation, but many administrators of smaller networks never have to deal with the more advanced features of Active Directory. This chapter discusses Active Directory management tools that administrators use only once in a great while, and some administrators never use at all. Tasks such as modifying the Active Directory schema and dividing a large network into sites are not to be taken lightly. You should fully understand the ramifications of your actions before you even load tools such as Active Directory Sites and Services or Active Directory Schema snap-ins.

Using Active Directory Sites and Services

Active Directory Sites and Services is a snap-in for the Microsoft Management Console (MMC) that administrators use to create and manage the sites that make up a Microsoft Windows Server 2003 network as well as to establish links between sites. A site, in Active Directory terminology, is defined as a group of computers on one or more Internet Protocol subnets that are well connected. A subnet is a network that is a component of a larger network. For more information about subnets, see Chapter 16.

Well connected means that the systems share a network transport that provides low-cost, high-speed communications between the machines, and it typically refers to systems in a single location that are connected by local area networks (LANs). Systems that aren’t well connected are those that use relatively slow, expensive communications. Active Directory consists of one or more sites, but sites aren’t part of the namespaces you deal with when you create the Active Directory hierarchy.

When designing trees and forests for Active Directory installation, the boundaries between forests, trees, domains, and organizational units (OUs) are often politically motivated. For example, Active Directory for a large corporation might consist of separate trees corresponding to corporate divisions, domains for individual departments, and
OU s for workgroups. Sites, on the other hand, are always based on geographical locations and the types of connections between those locations.

As an example, suppose this imaginary corporation has two divisions, each of which has its own Fast Ethernet LAN running at 100 Mbps. If the two divisions are located in separate buildings on the same campus, they might have a high-speed fiber-optic connection between the two LANs, also running at 100 Mbps. In this case, because all the computers in the two divisions are equally well connected, they can be said to form a single site. If, on the other hand, the two divisions are located in separate cities and are connected by a T1 line operating at only 1.544 Mbps, the divisions would form two separate sites because all the computers on the network aren’t equally well connected.

Sites don’t appear as objects in the Active Directory namespace; they’re completely separate from the hierarchy of forests, trees, and domains. A site can contain objects from different domains, and a domain’s objects can be split among different sites. The basic reason for dividing an enterprise network into sites is to take advantage of the efficient communications between well-connected systems while regulating the traffic over slower, costlier connections. Specifically, Active Directory uses sites during authentication and replication:

- **Authentication** When a user logs on to the network from a workstation, the system authenticates the user with a domain controller at the same site whenever possible. This speeds up the authentication process and helps reduce wide area network (WAN) traffic.

- **Replication** Domain controller replication activities that must cross site boundaries are subject to special conditions because of the need to use slower WAN connections.

Sites in Active Directory are associated with one or more particular IP subnets used by your network. During the authentication process, the workstation transmits information about the subnet on which it resides. Domain controllers use this information to try and locate an Active Directory server on the same subnet as the workstation.

The use of sites during replication is more complex. When two domain controllers are located at the same site, replication takes place at full LAN speed: usually from 100 Mbps to 1 Gbps. Two domain controllers located in different buildings or cities, on the other hand, are likely to be connected using WAN technology that is far slower and also far more expensive than LAN technology. Therefore, maximizing the efficiency of the communications between sites is typically a matter of when and how often replications that use WAN links occur.

**Defining Site Objects**

When you create the first Windows Server 2003 domain controller on your network, the Active Directory Installation Wizard creates your first site, names it Default-First-Site-Name
(yes, that’s actually the name), and associates it with the server you just promoted. You can supply a more descriptive name for this site if you want or leave it as is. If all the Active Directory servers on your network will be located near enough to each other to communicate by using LAN connections, you don’t need any other sites or the Sites and Services snap-in. As you promote each server on the network to a domain controller, Active Directory adds it to the site and automatically configures the replication topology between the servers.

If you will have servers at remote locations, however, you can create additional sites using Sites and Services. By creating subnet objects and associating them with specific sites, you give Active Directory the information it needs to automatically add each server that is subsequently promoted to a domain controller to the appropriate site, based on the subnet where the machine is located. If you move a server to a new location at a different site, however, you must also manually move the server object to the new site object. Thus, if you plan to install and configure a domain controller at the home office and then ship it to a remote location, you have to use Sites and Services to move the server object to the appropriate site.

To move a server to a new site, follow these steps:

1. Open Active Directory Sites and Services.
2. Click the plus sign (+) next to Sites to open the list of available sites.
3. To open the list of servers, click the site where the server currently is.
4. Right-click the server you want to move, and choose Move from the shortcut menu (as shown in Figure 15-1).
5. In the Move Server window, select the new site for the server and click OK.

**Note** You can use the Install From Media feature to install a new domain controller directly, and place it in the site it will reside in all at once. For details on how to do this, see the Microsoft Knowledge Base Article 311078.
Subnet Objects
Active Directory uses subnet objects to define the boundaries of a site. Subnet objects each consist of a network address and a subnet mask used by some or all of the computers in a site. You can associate a site with multiple subnet objects so that if your network has multiple subnets in a single location you can include all of them in a single site. On a network with two or more sites, subnet objects are needed for the Active Directory Installation Wizard to place the server objects for newly promoted domain controllers into the correct sites. Without subnet objects, the wizard is likely to create the server object in the wrong place. If this occurs, you can manually move the server object to the proper site using the method described in the previous section.

Server Objects
Server objects are always children of site objects and are created by the Installation Wizard whenever it promotes a server to a domain controller. Don’t confuse an Active Directory server object with the computer object that the wizard also creates during the promotion process. The two, although linked, are completely separate objects with different purposes. You can manually create server objects in the Sites and Services snap-in, but this shouldn’t be necessary.

When Active Directory installation includes two or more sites, the Installation Wizard uses the subnets associated with the site objects to determine which site is appropriate for the server object. If no site is associated with the subnet used by a new domain controller, the wizard still creates the server object. Afterward, you have to create the site where the server belongs and move the server to it, or you’ll need to create a new subnet object and associate it with an existing site.

Understanding Domain Replication
Replication is the process of copying Active Directory data between domain controllers to ensure that they all have the same information. The Windows Server 2003 multiple-master replication capabilities make the entire replication process more complex than it was in Microsoft Windows NT. On a Windows NT network, servers wrote all domain directory changes to the primary domain controller first, which then propagated the information to the backup domain controllers. This process was an example of single-master replication. In Windows Server 2003, administrators can modify Active Directory by writing to any domain controller. All the domain controllers execute periodic replication events that copy their modifications to all the other domain controllers. The schedule and topology for these replication events differ depending on whether the domain controllers are at the same or different sites. The following sections examine these two replication scenarios.
Intrasite Replication

Replication between domain controllers in the same site is known as *intrasite replication* and is completely automatic and self-regulating. A module known as the *knowledge consistency checker* (KCC) creates connections between the domain controllers in the site and triggers replication events whenever anyone modifies the directory information on a domain controller. Because all the domain controllers in the site are assumed to be well connected, the replication process is designed to keep *latency* (that is, the delay between directory writes and their propagation to the other domain controllers) to a minimum, even at the expense of network bandwidth.

The KCC dynamically creates connection objects in Active Directory; when communication between domain controllers in the same site is disrupted, the KCC immediately creates new connections to ensure timely contact between the systems. *Timely contact* within a site means that no domain controller is more than three connections (or *hops*) away from any other domain controller. Administrators can create additional connection objects, which can improve communication between controllers and reduce latency further by decreasing the maximum number of hops allowed, but this approach also increases the system resources used by the replication process, including processor cycles, disk accesses, and network bandwidth. As a general rule, the replication topology within a site requires no administrative maintenance.

Intersite Replication

When you create multiple sites in Active Directory, the domain controllers assume that the network connections between the sites are slower than those within a site, more expensive, or both. As a result, the domain controllers use *intersite replication* to attempt to minimize the replication traffic between sites and also to provide administrators with a much more flexible replication topology.

When you have domain controllers in multiple sites, Active Directory still creates a default replication topology automatically during the installation process. However, distinct differences exist between the default replication patterns for intrasite and intersite topologies. These differences include the following:

- **Number of connections** The KCC still automatically creates connections between domain controllers in different sites, but it creates fewer of them. The three-hop-maximum rule isn’t observed between sites, in the interests of minimizing the bandwidth used.

- **Replication schedule** Replication activities within a site are triggered by changes to the Active Directory database on a domain controller. Replication between sites takes place at scheduled times and intervals—the default is every 180 minutes.
across each site link. Administrators can customize the schedule to take advantage of time periods when traffic is low and bandwidth is less expensive.

- **Compression**  Domain controllers transmit replication data uncompressed within a site, thus saving the processor cycles needed to decompress the data at the destination. Traffic between sites is always transmitted in compressed form to conserve bandwidth.

One of the primary functions of the Sites and Services snap-in is to configure the replication pattern between sites. To do this, you create site link and site link bridge objects that specify how and when replication data should be transmitted between sites. The following sections examine the functions of Sites and Services and how you use it to create a customized domain controller replication topology for your network.

**Launching Sites and Services**

The Sites and Services tool is a standard snap-in for the MMC application, which you launch by selecting Active Directory Sites and Services from the Administrative Tools folder in the Start menu’s Programs group. The snap-in module is called Dssite.msc; you can also launch Sites and Services by executing that filename from the command line or the Run dialog box.

**Viewing Replication Objects**

The Sites and Services interface uses the same console tree and result panes as many of the other Active Directory administration tools. The Sites container in the console tree contains the *Default-First-Site-Name* object automatically created by the Active Directory installation, and two other containers called the Inter-Site Transports container and the Subnets container. When you create additional sites, they appear as separate objects in the Sites container. Administrator-created objects appear in the containers under Sites, subnet objects appear in the Subnets container, and site link and site link bridge objects appear in the Inter-Site Transports container.

**Creating Site Objects**

Creating additional site objects in Active Directory is simply a matter of right-clicking the Sites container and choosing New Site from the shortcut menu. When the New Object – Site dialog box appears (as shown in Figure 15-2), you supply a name for the site object and select a site link it should use to define the transport mechanism for the site. The Active Directory Installation Wizard creates the *Defaultipsitelink* object during the installation process, so this object is always available if you haven’t yet created any other site links. After the site object is created, you can move server objects into it and associate them with the subnets on which they’re located.
Each site object in Active Directory has a Servers container holding objects representing the servers in the site, a Licensing Site Settings object, and an NTDS Site Settings object. The site object’s Properties dialog box enables you to specify a description for the site and its location, as well as containing the standard Object, Security, and Group Policy tabs found in the dialog boxes of so many other Active Directory objects.

The Licensing Site Settings object specifies the computer and domain licensing the site. In the Properties dialog box for the NTDS Site Settings object, you can set the schedule for replication, and enable or disable the Universal Group Membership caching. In the NTDS Settings object for an individual server, you can manually configure replication if necessary.

Creating Server and Connection Objects
Server objects are created during the installation of Active Directory on each domain controller, in the site associated with the subnet on which the server is located. Each server object contains an NTDS Settings object, which in turn contains the objects that represent that server’s connections to other domain controllers on the network. These connections must exist for domain controllers to replicate their Active Directory data. All connections, whether created automatically by the KCC or manually by an administrator, appear as objects associated with a server. A connection object is a unidirectional conduit to another domain controller on the network, either in the same site or another site. For replication traffic to travel in both directions, separate connection objects must exist for each of the two servers.
The KCC automatically creates connection objects that ensure the continued replication of Active Directory data to all the functioning domain controllers in each domain. When the status of your network changes—such as when a domain controller goes down and forces the replication traffic between any other two domain controllers in the site to travel over more than three hops—the KCC creates new connection objects to reduce that traffic path to three hops or fewer. When the nonfunctioning domain controller becomes operational again, the KCC can remove connection objects to bring the replication traffic back to its recommended topology.

Normally, the only reason you manually create connection objects is to customize your network’s replication topology. If, for example, you want replication activities to occur only at specific times, you can create a connection object and configure its schedule. You can also create connection objects to decrease the number of hops between specific domain controllers.

The major difference between manually created connection objects and those created by the KCC is that the manual objects remain in place until you remove them manually; the KCC doesn’t remove them no matter how the replication topology changes. Connection objects created by the KCC, however, are removed automatically as the replication topology changes. To create a connection object, follow these steps:

1. Right-click a server’s NTDS Settings object in the Sites and Services console tree, and choose New Active Directory Connection from the shortcut menu. This displays the Find Domain Controllers dialog box.

2. Select the domain controller you want to create a connection to, and click OK to open the New Object Connection dialog box.

3. Supply a name for the new connection, and click OK. The program adds a connection object to the details pane.

The Properties dialog box for a connection object contains the familiar Object tab and Security tab, as well as a General tab, as shown in Figure 15-3. In the General tab, you can supply a descriptive phrase for the connection, select the mode of transport for the replication messages (IP, RPC, or SMTP), and schedule the replication events.

The dialog box displayed when you click Change Schedule (shown in Figure 15-4) enables you to specify the hours of the day during which replication should occur and the interval between replication events (once, twice, or four times an hour). Keep in mind that this connection controls only the replication messages traveling from the server under which the object appears to the server you selected as the destination when creating the object. Traffic going in the other direction is controlled by the other server’s connection object (if it exists).
Creating Subnet Objects
Administrators create objects representing the IP subnets on the network and associate them with specific site objects in the Subnets container. When you promote the first server to a domain controller, the Active Directory Installation Wizard creates a site and places the server object in that site. If you create additional sites, subnet objects are used to ensure that each subsequent domain controller you install is placed in the appropriate
site. During the promotion process, the wizard identifies the subnet on which the server resides and searches Active Directory for a corresponding subnet object. When the wizard finds the subnet object, it reads its properties to determine the site with which that subnet is associated, and it creates the new server object in that site.

Subnet objects aren’t essential to Active Directory’s replication topology. You can create sites and move the server objects into them manually. However, if you’ll be installing a lot of servers, subnet objects automate the construction of the replication topology and make the entire site deployment process more manageable. To create a subnet object, follow these steps:

1. Right-click the Subnets container in the console tree of the Sites and Services snap-in, and choose New Subnet from the shortcut menu.

2. In the New Object – Subnet dialog box (shown in Figure 15-5), specify the subnet’s network address and number of masked bits.

3. Select the site with which that subnet is to be associated, and click OK.

Any servers on that subnet that you promote to domain controllers are automatically added to this site. You can associate multiple subnets with a single site to support a network of almost any size.
Note  The network address is the portion of the IP address that identifies the network on which a computer resides. The number of bits masked refers to how many of each IP address's 32 bits the system uses to identify the network. The design of the network and the IP addresses you use for workstations determine the value for this number. For example, if your organization has a class B network address (which uses 16 bits to identify the network) and uses a further 8 bits to identify subnets, the result is a total of 24 out of 32 bits that are devoted to the network address. The value for the subnet object's name field is therefore something like 172.16.2.0/24.

Creating Site Link Objects
The Inter-Site Transports container is where you create the site link and site link bridge objects that dictate how replication traffic is to be transmitted between sites. Two containers within Inter-Site Transports represent the two transport protocols supported by Active Directory: IP and Simple Mail Transfer Protocol (SMTP).

A site link object represents the WAN mechanism used to transmit data between two sites, such as a leased T1 connection or an Asynchronous Transfer Mode (ATM) backbone, in the case of IP, or any means by which systems send e-mail using SMTP. Active Directory creates a default site link object called Defaultipsitelink when it creates the network’s first site during the promotion of the first server to a domain controller. If all your sites are linked using technologies with exactly the same speed, you don’t need to create additional site links. When you have different technologies connecting sites, however, you create multiple site link objects to have different replication schedules for each one.

When creating a site link object, you select two or more sites that are connected by the transport mechanism and specify a cost value for the link. The cost value enables you to assign priorities to the various WAN connections, based on their relative speeds. A higher cost value indicates that a connection is more expensive to use, and the KCC schedules less frequent replications on its connections between those two sites as a result.

To create a site link object, follow these steps:

1. Right-click either the IP or SMTP transport in the console tree of Sites and Services, and choose New Site Link from the shortcut menu.

2. In the New Object – Site Link dialog box, specify a name for the object and select the sites that the link connects. If the link is to represent a point-to-point connection such as a T1, you select only two sites. For a technology such as an ATM backbone, which can connect several sites, you select more than two site objects. When the site link object connects more than two site objects, you can assume that any one of the chosen sites can transmit to any other chosen site.

3. Click OK, and the manager creates the link object.
Configuring Site Links

Right-click the new link object, and select Properties to configure its properties. The Site Link Properties dialog box for a site link object (shown in Figure 15-6) contains the standard Object tab and Security tab, as well as a General tab in which you can provide a description of the object and specify the sites connected by the link. You can add new sites to the link as needed after creating the object.

![Site Link Properties dialog box]

Figure 15-6  The General tab of the Site Link Properties dialog box

The General tab also contains fields with which to specify the cost for the link (from 1 to 32,767) and the interval between replication events (from 15 to 10,080 minutes). Clicking Change Schedule enables you to specify the time periods that replication is or is not permitted. If you want to limit replication activities to nonpeak traffic hours, for example, you can specify that replication events not occur between 9 A.M. and 5 P.M. The KCC observes the site link object’s scheduling limitations when it dynamically creates connections between domain controllers.

Creating Site Link Bridge Objects

Site link bridge objects function much like site links, except that instead of grouping sites, they group site links. A site link bridge object typically represents a router in the network infrastructure. You create a site link bridge object to enable route replication traffic between linked sites. Site link bridges are normally not required in a Windows Server 2003 forest because the site links are transitive. Windows 2000 Server domains had non-transitive site links.

The procedure for creating a site link bridge object is virtually identical to that of creating a site link object, except that you select two or more site links instead of sites. You don’t need to specify a routing cost for a site link bridge because Active Directory automatically
computes it by adding the routing costs of all the bridge's sites. Thus, a site link bridge object containing two sites with routing costs of 3 and 4 has a routing cost of 7.

**Using Active Directory Schema**

The *schema* is the blueprint of Active Directory, dictating what kinds of objects can exist in the database and what the attributes of those objects are. To customize Active Directory for use on a network, you can modify the schema to create new object types, add new attributes to existing object types, and modify the type of information installed on an attribute. To do this, use the MMC snap-in called Active Directory Schema.

Modifying the schema is a task that the average administrator never has to perform. At most, you change the schema occasionally or perhaps only once. Modifying the schema is subject to the same cautions as modifying a Windows Server 2003 system's registry, except on a larger scale. Just as improper registry modifications can adversely affect a single system, improper schema modifications can have a devastating effect on the entire network.

---

**Note** Before you can add any Microsoft Windows Server 2003 family domain controllers to an existing Windows 2000 forest, you must upgrade the schema using Forestprep.exe on the Windows Server 2003 CD-ROM.

**Examining Schema Security**

Because modifying the Active Directory schema isn’t something to do casually, Windows Server 2003 uses several safety mechanisms to prevent the schema from being modified accidentally or injudiciously. You can modify the schema only when the requirements of all three safety mechanisms have been satisfied.

**Schema Administrator Permissions**

To modify the schema, you must be logged on to a server or workstation in the Windows Server 2003 domain using an account that is a member of the Schema Admins group. This is a built-in group created during Active Directory installation that grants its members permission to write to the schema object. The Administrator account in the forest root domain is automatically made a member of the Schema Administrators group, but members of the Domain Admins group are not automatically part of the Schema Admins group. Users who aren’t members of this group can also modify the schema if an administrator has granted them the appropriate permissions to the schema object.
Security Alert  It is a good practice to strictly limit the members of the Schema Admins group. Don’t automatically add new administrators to the group, and don’t routinely log on with an account that is a member of the Schema Admins group.

Flexible Single-Master Operations
Active Directory uses a multimaster replication system for modifications of the database contents, but for schema modifications, it uses a single-master system. This means that only one domain controller can modify the schema at once. Unlike most single-master replication models, which require all modifications to be written to one designated system and subsequently copied to the other replicas, administrators can modify the Active Directory schema from any domain controller. The mechanism that makes this possible is called Flexible Single-Master Operations (FSMO). While an administrator is modifying the schema on one domain controller, write access requests to the schema on all other domain controllers are denied.

To move the Schema Master FSMO role, see the “Transferring the Schema Master” section later in this chapter. For more about the different FSMO roles, see the “Understanding Operations Master Roles” section later in this chapter.

Read-Only Schema Access
Finally, all domain controllers are configured by default during Active Directory installation to permit read-only access to the schema. To enable write access, you must create a new entry in the registry or register the Scmmgmt DLL. Using the Windows Server 2003 registry editor (Regedit.exe), browse to this key:

HKEY_LOCAL_MACHINE\System\Current Control Set\Services\NTDS\Parameters

Create a new DWORD entry called Schema Update Allowed. Assign the entry a value of 1 to enable write access to the schema. Change the value to 0 to disable write access again after the modifications are complete.

Alternately, open a command prompt and type:

Regsvr32 scmmgmt.dll

This will add the Active Directory Schema to the list of MMC snap-ins and enable schema modifications.

Launching Active Directory Schema
Because of its infrequent use and potential dangers, the Schema Manager is two removes from the Administrative Tools menu. To view or change the schema, you must first install
the Administrative Tools (as described in Chapter 12). Then run the Active Directory Schema snap-in in an MMC console by following these steps:

1. Click Start and select Run. Type `mmc` and press Enter.
2. Select Add/Remove Snap-In from the Console menu.
3. Click Add, and select Active Directory Schema from the list of snap-ins provided. When the snap-in is loaded, you can save the console screen to a file to provide easy access to the snap-in in the future. When the view pane opens, you see two containers in the console tree, which hold the object classes and the attributes that make up those classes, shown in Figure 15-7. Selecting either of these two containers displays Active Directory’s classes or attributes in the result pane.

![Figure 15-7](image)

**Figure 15-7** Schema Manager object classes and attributes stored in Active Directory

However, before changing the schema, be sure the schema snap-in is accessing the Active Directory database on the domain controller that is currently functioning as the Schema Master (that is, the one domain controller to which write access to the schema is permitted). To determine which domain controller you are currently accessing, follow these steps:

1. Select Active Directory Schema, and choose Change Domain Controller from the shortcut menu. In the Change Domain Controller dialog box (shown in Figure 15-8), you see the current domain controller and are able to change the focus to any other domain controller, or you can specify a particular controller. Click OK or Cancel when you are finished.
2. Right-click the Active Directory Schema object in the console tree, and choose Operations Master from the shortcut menu.

3. In the Change Operations Master dialog box, you see which domain controller is the operations master and specify whether the schema can be modified on that system. To change the schema, either change the schema master to the domain controller you’re currently using or change your connection to the current schema master.

![Image of Change Domain Controller dialog box]

**Figure 15-8** The Change Domain Controller dialog box

### Modifying the Schema

The process of modifying the Active Directory schema involves creating or modifying the classes and attribute object types displayed in Schema Manager. *Classes* are essentially collections of attributes that either form an Active Directory object type by themselves or contribute certain attributes to another object type. The latter instance is known as an *auxiliary class*. To add attributes to an existing object type, the best method is to create a new class containing the new attributes and add it to the object type as an auxiliary. This method is more manageable and less dangerous than modifying the class representing the object type itself.

Third-party software products might supply their own schema modifications that create entirely new object types, but adding attributes to an existing object type is the most common form of schema modification manually performed by administrators—for example, adding attributes to the user object type that enable you to store additional information about the user in Active Directory. This relatively easy process consists of the following steps, which are examined in more detail in the following sections:

- Creating new attribute objects corresponding to the information fields you want to add to the object
- Creating a new class object to be used as an auxiliary to the existing object type
- Adding the newly created attributes to the new auxiliary class
- Adding the auxiliary class to the existing object class
Creating Attributes
Creating an attribute is a matter of supplying a name by which the attribute will be identified and specifying the type of data that will be stored there. The data can be text or numerical, and you can apply constraints that limit the data to a particular length or value type. For example, to add an attribute to hold the user’s employee ID number, you specify that the attribute’s data should be in integer form and limited to nine digits. To create an attribute object, follow these steps:

1. Right-click the Attributes container in Schema Manager’s console tree, and choose Create Attribute from the shortcut menu. This first produces a warning that creating an object permanently modifies the Active Directory, and then it produces the Create New Attribute dialog box shown in Figure 15-9.

![](image)

**Figure 15-9** The Create New Attribute dialog box

2. In the Identification area, specify the name for the new object. The Common Name field should contain the name by which the attribute will be listed in standard dialog boxes, and the LDAP Display Name field should contain the name by which it is known in the LDAP directory hierarchy. (LDAP stands for Lightweight Directory Access Protocol.) Often, these two names are the same. The Unique X.500 Object ID field must contain a numerical string that uniquely identifies the attribute object in the X.500 namespace. Standards organizations such as the International Telecommunications Union issue Object IDs (OIDs) to ensure that they have unique values. In the Description box, fill in a description of the object and its function.
More Info  Object Identifiers can be obtained either directly from an ISO Name Registration authority, or from Microsoft. If you intend to extend the Active Directory schema and want to apply for the Certified for Windows logo, the OID must be registered with Microsoft. For more information about obtaining an OID from an ISO Name Registration Authority, see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ad/ad/obtaining_a_root_oid_from_an_iso_name_registration_authority.asp. To obtain a base OID directly from Microsoft, see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ad/ad/obtaining_an_object_identifier_from_microsoft.asp.

3. In the Syntax And Range area, define the nature of the data to be stored in the attribute. The Syntax field provides more than a dozen options that define the types of information that can be stored in an attribute. The Minimum and Maximum fields enable you to define a range of possible values. You can also specify whether the attribute should be able to have multiple values.

4. Click OK, and the manager creates the new attribute object.

Important  Don’t be tempted to make up your own OIDs. Even if you’re running Active Directory on an isolated network, it’s all too easy to supply an OID for a new attribute or class that duplicates one of the hundreds of other OIDs already assigned to Active Directory objects.

Configure the new (or any other) attribute object by opening the Properties dialog box from its shortcut menu, shown in Figure 15-10. From this window, you can specify a description for the object, modify its range of possible values, and enable any of the following options:

- Deactivate this attribute
- Index this attribute in Active Directory
- Ambiguous Name Resolution (ANR)
- Replicate this attribute to the Global Catalog (GC)
- Attribute is copied when duplicating a user
- Index this attribute for containerized searches in Active Directory
Creating Object Classes

Attribute objects by themselves are useless until they belong to an object class. You can add the attribute objects you created to an existing class, but creating a new class object for them is generally more practical. To create a class object, right-click the Classes container in the schema snap-in and choose Create Class from the shortcut menu. This displays the Create New Schema Class dialog box shown in Figure 15-11.

Figure 15-11  The Create New Schema Class dialog box
As with an attribute object, you must first specify a common name, an LDAP display name, and a unique X.500 object ID. Then, in the Inheritance And Type area, specify the parent class for the new object (that is, the class from which the new object should be derived), and choose one of the following three class types:

- **Structural class** The typical directory objects you work with in programs such as Active Directory Manager. A structural class object can have either an abstract class or another structural class as its parent object.

- **Abstract class** Objects from which structural class objects are derived. You can also specify an existing abstract class as the parent of a new abstract class object.

- **Auxiliary class** Collections of attributes you can add to either an abstract or structural class object to augment its capabilities. New auxiliary class objects can be derived only from abstract classes.

To hold your new attributes, create an auxiliary class type.

**Adding Attributes to a Class**

After you create the attribute objects and the class object to contain them, you must add the attributes to the class. You do this by opening the Properties dialog box for the newly created class object. The dialog box for a class object has four tabs, including the standard Security tab. On the General tab, supply a description for the object and specify whether the object class should show while browsing. You can also disable the object by selecting the Deactivate This Class check box.

In the Attributes tab (shown in Figure 15-12), add your newly created attribute objects to the class by clicking Add for either the Mandatory or Optional list and then selecting the objects by name. When an attribute is mandatory, you must supply a value for the attribute when creating a new object of that class. For example, if you create an Employee ID Number attribute, add it to your auxiliary class as a mandatory attribute, and then add the auxiliary class to the user class; the next time a new user object is created, an employee ID number will be required for the user. Values for optional attributes aren’t required.

**Adding an Auxiliary Class to a Structural Class**

An auxiliary class object can’t store attribute information until you add the auxiliary class object to a structural class object, such as a user or computer. To do this, open the structural class object’s Properties dialog box and select the Relationship tab. (See Figure 15-13.)

On this tab, click Add Class for the Auxiliary Classes list, and select the class object you just created. This causes Active Directory to add the attributes in the auxiliary class to the structural class. In the Possible Superior list, specify which other object classes can contain the current object class. For example, the user object class has the organizational
unit object class in its Possible Superior list, which enables the creation of new users in OUs. The opposite is not true, however; you can't create an OU beneath a user, so the user object isn't a possible superior of the OU object.
Modifying Display Specifiers

After you add new attributes to a class, the attributes exist in the Active Directory database, but you can't see them in utilities such as Active Directory Users and Computers. To view, add, or modify the values of the new attributes, you must first alter the display specifiers that control how attributes appear in applications. Display specifiers are Active Directory objects that define the labels for the attributes that appear in a dialog box and control the contents of the shortcut menu that appears when you right-click an object of a modified class.

For example, you might create a new attribute intended to store users' employee ID numbers and name it EmployeeIDNumber. You probably don't want the attribute name to appear this way in Active Directory Users and Computers, so you create the display name Employee ID Number and make it the equivalent of EmployeeIDNumber. To modify the display specifier objects, you can use a Microsoft Visual Basic script and execute it from the Windows Server 2003 command prompt.

The following script assumes that two new attributes, called SalaryLevel and EmployeeIDNumber, were created and added to an auxiliary class called HumanResources, which, in turn, was added to the user object class. The first section connects to the DisplaySpecifiers container in Active Directory.

```vbscript
Dim oRoot
Dim oDisp
Dim oCont
Dim aMenu
Dim iCount
Dim sNewMenu
Dim oFileSystem
Dim sOutFile
Dim sSystemFolder
Set oFileSystem = WScript.CreateObject("Scripting.FileSystemObject")
sSystemFolder = oFileSystem.GetSpecialFolder(1)
Set oRoot = GetObject("LDAP://RootDSE")
Set oCont = GetObject("LDAP://&" & CN=409,CN=DisplaySpecifiers," & _
   oRoot.get("configurationNamingContext"))
Set oDisp = oCont.GetObject("displaySpecifier","cn=user-Display")
MsgBox "Display Specifier: " & oDisp.Name

The following routine assigns display names to the two new attributes. These names appear in all dialog boxes providing access to these attributes.

oDisp.PutEx 3, "attributeDisplayNames", _
   Array("SalaryLevel,Annual Salary", _
   "EmployeeIDNumber,Employee ID Number")
```

oDisp.SetInfo
The next routine creates a new entry, called *HR Info*, on the shortcut menu that appears when you right-click a user object in the My Network Places window. When you access this shortcut menu item, the program executes another Visual Basic script called Hrshell.vbs that enables users to view the values for the new attributes.

```
MsgBox "Adding Shell Context Menu item"
iCount = 0
If Not IsEmpty(oDisp.shellContextMenu) Then
    aMenu = oDisp.GetEx("shellContextMenu")
    For iCount = LBound(aMenu) To UBound(aMenu)
        MsgBox "Existing Menu item: " & aMenu(iCount)
    Next
    iCount = iCount + 1
End If
sNewMenu = CStr(iCount) & ",&HR Info...,hrshell.vbs"
oDisp.PutEx 3, "shellContextMenu", Array(sNewMenu)
oDisp.SetInfo
```

This next routine creates the Hrshell.vbs script:

```
MsgBox "Adding Shell Context Menu Program"
Set sOutFile = oFileSystem.CreateTextFile(sSystemFolder & _
    "\hrshell.vbs",True)
sOutFile.WriteLine "Dim Args"
sOutFile.WriteLine "Dim oUser"
sOutFile.WriteLine "Set Args = Wscript.Arguments"
sOutFile.WriteLine "MsgBox " & Chr(34) & " LDAP Path: " & Chr(34) & _
    " & Args(0)"
sOutFile.WriteLine "MsgBox " & Chr(34) & " Object Class: " & _
    Chr(34) & " & Args(1)"
sOutFile.WriteLine "Set oUser = GetObject(Args(0))"
sOutFile.WriteLine "MsgBox " & Chr(34) & " HR Info" & Chr(34) & _
    " & vbCRLF & " & _ Chr(34) & " Salary: " & Chr(34) & _
    " & oUser.SalaryLevel & vbCRLF & " & Chr(34) & " Employee ID: " & _
    Chr(34) & " & oUser.EmployeeIDNumber"
sOutFile.WriteLine "Set oUser = Nothing"
sOutFile.WriteLine "WScript.Quit"
sOutFile.Close
```

The following routine adds a similar entry to the user shortcut menu in Active Directory Users and Computers, causing the application to execute the Hradmin.vbs script. This script creates a dialog box in which administrators can modify the values for the new attributes.

```
MsgBox "Adding Admin Context Menu item"
iCount = 0
If Not IsEmpty(oDisp.adminContextMenu) Then
    aMenu = oDisp.GetEx("adminContextMenu")
    For iCount = LBound(aMenu) To UBound(aMenu)
        MsgBox "Existing Menu item: " & aMenu(iCount)
    Next
    iCount = iCount + 1
```
End If
sNewMenu = CStr(iCount) & ",&HR Admin...,hradmin.vbs"
oDisp.PutEx 3, "adminContextMenu", Array(sNewMenu)
oDisp.SetInfo

The next section creates the Hradmin.vbs script and terminates the script:

MsgBox "Adding Admin Context Menu Program"
Set sOutFile = oFileSystem.CreateTextFile(sSystemFolder & _
   "\hradmin.vbs",True)
sOutFile.WriteLine "Dim Args"
sOutFile.WriteLine "Dim oUser"
sOutFile.WriteLine "Dim temp"
sOutFile.WriteLine "Set Args = Wscript.Arguments"
sOutFile.WriteLine "MsgBox " & Chr(34) & "LDAP Path: " & Chr(34) & _
   " & Args(0)"
sOutFile.WriteLine "MsgBox " & Chr(34) & "Object Class: " & _
   Chr(34) & " & Args(1)"
sOutFile.WriteLine "Set oUser = GetObject(Args(0))"
sOutFile.WriteLine "temp = InputBox(" & Chr(34) & "Old Salary: " & _
   Chr(34) & " & oUser.SalaryLevel & vbCRLF & " & Chr(34) & _
   "New Salary" & Chr(34) & ")"
sOutFile.WriteLine "if temp <> " & Chr(34) & Chr(34) & _
   " then oUser.Put " & Chr(34) & "SalaryLevel" & Chr(34) & ",temp"
sOutFile.WriteLine "temp = InputBox(" & Chr(34) & _
   "SOC Sec Number: " & Chr(34) & " & oUser.EmployeeIDNumber & _
   vbCRLF & " & Chr(34) & "New Number" & Chr(34) & ")"
sOutFile.WriteLine "if temp <> " & Chr(34) & Chr(34) & _
   " then oUser.Put " & Chr(34) & "Employee ID" & _
   Chr(34) & ",temp"
sOutFile.WriteLine "oUser.SetInfo"
sOutFile.WriteLine "Set oUser = Nothing"
sOutFile.WriteLine "WScript.Quit"
sOutFile.Close
MsgBox "Quit... "
Set oDisp = Nothing
Set oCont = Nothing
Set oRoot = Nothing
Set oFileSystem = Nothing
WScript.Quit

When you save this script to a text file with a .VBS extension and execute it from the command prompt, Windows Server 2003 adds the shortcut menus to the My Network Places window and the Active Directory Users and Computers snap-in and creates the scripts that selecting those shortcut menus executes. This part of the schema modification process is obviously the most complex. After you create your own scripts, carefully test and debug them on a non-production network before executing them on live domain controllers.
Note  Microsoft Virtual Server 2005 R2 is an excellent tool for creating a safe test network that you can use to test any changes to Active Directory. Or any other changes on your network. For more information about using and configuring Virtual Server, see Chapter 29.

Performing Batch Importing and Exporting

MMC snap-ins such as Active Directory Users and Computers make it easy to create and configure new objects in Active Directory, but deploying the directory service on a large scale might require the creation of thousands of objects. In cases like these, manually creating individual objects is impractical. Anticipating the need for the mass creation of Active Directory objects, and particularly user objects, Windows Server 2003 includes tools that enable administrators to perform batch imports and exports of Active Directory objects. Among these tools is Ldifde.exe, a command-line utility for importing, exporting, and modifying Active Directory objects using the LDAP Data Interchange Format (LDIF).

Using the Ldifde.exe Utility

Active Directory uses LDAP to define its namespace, and it supports LDIF. LDIF is a standardized format for saving directory service information in text files. If you’re running another directory service that also supports LDIF on the network, you can import its data into Active Directory by using the Ldifde.exe utility. You can also use Ldifde.exe to export Active Directory objects to LDIF files and modify existing objects.

The syntax for using the Ldifde.exe utility is as follows:

```
Ldifde [-a username password] [-b username domainname password]

[-a username password] – specifies the user name and password for simple authentication to the LDAP directory.
[-b username domainname password] – specifies the user name, domain name, and password for the SSPI bind method (by default, the utility logs in to the LDAP directory as the current user, with the SSPI bind method).
[-c FromDN ToDN] – replaces all occurrences of FromDN with ToDN.
[-d RootDN] – specifies the root object where the utility should commence its search (default = current naming context).
[-e] – prevents lazy commits
[-f filename] – specifies the name of the LDIF file that the utility will import data from or export data to.
[-g] – disables paged search.
```
[-h] – enables SASL encryption
[-i] – causes the utility to operate in import mode (default = export mode).
[-j] – specifies the location of the utility's log file.
[-k] – causes the program to ignore "constraint violation" and "object already exists" errors.
[-l attributes] – specifies the attributes that the utility should look for during a search of an LDAP directory.
[-m] – enables Windows NT's Service Account Manager (SAM) logic during export operations.
[-n] – prevents the utility from exporting binary values.
[-o attributes] – specifies the attributes that the utility should omit from inputting.
[-p scope] – specifies the search scope (Base, OneLevel, or Subtree).
[-q threadcount] – enables multithreaded import with threadcount number of threads
[-r filter] – specifies the objects for which the utility will search (default = "(objectClass=*)").
[-s servername] – specifies the name of the server to which the utility will bind (default = domain controller of the currently logged on domain).
[-t] – specifies a port number to use when communicating with the LDAP service (default = 389).
[-v] – causes the program to operate in verbose mode.
[-w timeout] – sets the timeout period
[-y] – the default. Forces lazy commits
[-"] – displays help information for the program.

Exporting Objects
To export Active Directory information to an LDIF file, execute a command like the following:

```
ldifde -f research.ldif -s cz2 -d "ou=Research,dc=example,dc=com"
    -p subtree -r "(objectClass=*")"
```

The -f parameter specifies the name of the LDIF file that the utility will create. The -s and -d parameters identify the server that the utility should use to access Active Directory and the OU where the export process should begin. The -p parameter specifies that the utility should export the entire subtree below the Research OU, and -r specifies that the program should export only person (that is, user) objects. When you execute the command, Ldifde.exe searches Active Directory, starting in the Research OU and traveling down the subtree to the bottom, writing the information about each user object it finds to the Research.ldif file. A typical LDIF entry for a user object (in this case, the Administrator object) appears as follows:

```
dn: CN=Administrator,CN=Users,DC=example,DC=com
changetype: add
accountExpires: 9223372036854775807
badPasswordTime: 0
badPwdCount: 0
```
Importing Objects
To import users or other objects from another LDAP directory service, you must first export the information using whatever tools the other product provides, and then import the LDIF file into Active Directory using a command like the following:

```
Ldifde -i -f newusers.ldif
```

In this example, the `-i` parameter puts the program into import mode, and the `-f` parameter specifies the name of the LDIF file you created from the other directory service.

Modifying Objects
You can also use Ldifde.exe to modify the information stored in Active Directory objects, albeit in a roundabout way. After exporting Active Directory object information to an LDIF file, modify the attribute values in the file using any text editor, and then import it back into Active Directory. The new information overwrites the old, effectively modifying the Active Directory object information. If faced with a situation in which you have to make many similar changes to the directory, such as a company move requiring new mail addresses for all users, use Ldifde.exe and a text editor with search and replace capabilities to quickly modify thousands of objects in the Active Directory database.
Understanding Operations Master Roles

Domain controllers must handle five operations master roles in every Active Directory forest, called Flexible Single Master Operations roles, or FSMO roles. Some of the operations master roles are critical to your network, and if the machine providing them fails, you'll know about it at once. Others can be unavailable for a long time without you or your users being any the wiser. The five FSMO roles are as follows:

- **Primary domain controller (PDC) emulator** Acts as a Windows NT primary domain controller in domains that have Windows NT backup domain controllers or computers without Windows 2000 client software. This role also:
  1. Acts as the root time server for the domain.
  2. Acts as the Group Policy originator. All GPO changes are initially made to the PDC emulator, and then replicated to the rest of the domain controllers.
  3. Acts as the password change and account lockout originator to ensure consistency across the domain.

- **Schema master** Controls all updates and modifications to the schema.

- **Domain naming master** Controls the addition or removal of domains.

- **Relative identifier (RID) master** Allocates relative IDs to each domain controller.

- **Infrastructure master** Updates changes to group-to-user references when memberships in groups are changed.

Normally, you have no reason to interfere with the operations master roles. On the typical network, they reside where they were created, on the first domain controller in the network. If you need to transfer the roles, either for performance reasons or because you will be decommissioning the server, the actual transfer is relatively trivial. Just try to make a transfer when the original role holder is available—it's easier and less painful. In serious circumstances when the controller holding the role is unavailable, you can seize a role, but it's a drastic measure and one that's not to be taken lightly. In all cases, except with the PDC emulator, when an operations master role is seized (rather than transferred), you must not bring the original holder of the seized role back online without completely reformatting the boot disk and reinstalling Windows Server 2003. The next several sections explain the operations master roles in more detail.

**Important** If you must seize an operations master role because the holder of the role is no longer available, you must not bring the machine that held the role back online without completely erasing and reformatting the machine. If two machines try to claim ownership of an operations master role, you will not have a happy network and data corruption and logon failures can and will occur. You've been warned.
Primary Domain Controller Emulator

When upgrading a Windows NT domain, only one domain controller can create users, groups, and computer accounts—the basics of security. This Windows Server 2003 domain controller is configured as the PDC operations master and emulates a Windows NT primary domain controller. The PDC emulator supports the Kerberos and NTLM protocols, allowing Windows NT domain controllers to synchronize with a Windows Server 2003 environment running in Windows 2000 mixed mode or Windows 2003 transitional mode.

Every domain must have a domain controller that acts as a PDC emulator as long as the domain contains either clients without Windows 2000 or Windows XP client software or Windows NT backup domain controllers. If the controller acting as the PDC emulator isn’t available, it will affect users because the network itself will be disrupted. So if you know that the controller acting as the PDC emulator will be unavailable, transfer this role.

Transferring the PDC Emulator

To transfer the role of PDC emulator, follow these steps:

1. Launch Active Directory Users and Computers from the Administrative Tools folder.
2. Right-click the domain node, and choose Connect To Domain Controller from the shortcut menu.
3. Select the domain controller you want to give the role of PDC emulator. Click OK.
4. Right-click the domain node, and choose Operations Masters from the shortcut menu. Click the PDC tab to see the current focus (the controller that will become the PDC emulator) and the controller that is the current operations master.
5. Click Change and then click OK.
6. You can also transfer the roles from the command line, using Ntdsutil.exe, as described in the “Seizing the PDC Emulator” section. However, instead of typing “seize PDC,” you’ll type transfer PDC.

Seizing the PDC Emulator

If the PDC emulator becomes unavailable unexpectedly and it can’t be returned to service quickly, you need to seize the role of the PDC emulator and force it to another domain controller. To seize the PDC emulator, follow these steps:

1. Choose Run from the Start menu (or open a command window), type ntdsutil, and press Enter.
2. At each prompt, supply the following information and then press Enter:
   a. At ntdsutil, type roles.
   b. At fsmo maintenance, type connections.
c. At server connections, type **connect to server** followed by the fully qualified domain name of the controller that is to be the new PDC emulator. (See Figure 15-14.)

d. At server connections, type **quit**.

e. At fsmo maintenance, type **seize PDC**.

f. At ntdsutil, type **quit**.

![Figure 15-14 Using Ntdsutil to seize and move the PDC emulator role to a new server](image)

When the original PDC emulator becomes available again, you can use the same procedure to return the PDC emulator role.

**Schema Master**

Not surprisingly, the schema master handles all updates to the schema. Only one schema master exists in an entire forest. The schema master role is assigned to the first domain controller in the first domain in the forest and remains there unless you change it. Because modifications of the schema are uncommon, the schema master can be nonfunctional for an extended period without affecting users.

**Transferring the Schema Master**

To transfer the schema master role, follow these steps:

1. Open the Active Directory Schema snap-in.
2. Right-click Active Directory Schema in the console window, and choose Change Domain Controller from the shortcut menu. Change the focus to the controller that will assume the schema master role.
3. Right-click Active Directory Schema in the console window, and choose Operations Master from the shortcut menu. Click Change and then click OK.

---

**Note** You can also use the Ntdsutil.exe command-line utility to transfer any of the operations master roles, using a similar syntax to that for seizing a role.
Seizing the Schema Master
Don’t seize the schema master unless there’s no hope of returning the original controller to service. Before seizing the schema master role, the original schema master must be disconnected from the network. To seize the schema master role, follow these steps:

1. Choose Run from the Start menu (or open a command window), and then type `ntdsutil` and press Enter.
2. At each prompt, supply the following information and then press Enter:
   a. At ntdsutil, type `roles`.
   b. At fsmo maintenance, type `connections`.
   c. At server connections, type `connect to server` followed by the fully qualified domain name of the controller that is to be the new schema master.
   d. At server connections, type `quit`.
   e. At fsmo maintenance, type `seize schema master`.
   f. At ntdsutil, type `quit`.

**Important**  Seizing the schema master role is a radical step. Don’t do it unless the original schema master is permanently out of service. Before you can bring the original schema master back online, you must reformat its boot disk and reinstall Windows Server 2003 to prevent serious problems with the updating of the schema.

Domain Naming Master
Only one server in the enterprise performs the role of domain naming so that the domain naming master is created in the first domain and the role remains there no matter how large the forest. The domain naming master can be unavailable for some time, and the network is unaffected until there’s a need to establish a new domain. Therefore, unless the controller playing this role is to be permanently removed from the network, you usually don’t need to either transfer or seize this role.

Transferring the Domain Naming Master
If you need to transfer this role to another controller, follow these steps:

1. Launch Active Directory Domains and Trusts from the Administrative Tools folder.
2. Right-click Active Directory Domains and Trusts, and choose Connect To Domain Controller from the shortcut menu.
3. Select the domain controller you want to give the role of domain naming master. Click OK.

4. Right-click Active Directory Domains and Trusts again, and select Operations Master from the shortcut menu. A dialog box opens, showing the current domain naming master and the computer that will become the domain naming master.

5. Click Change and then click OK.

Seizing the Domain Naming Master
If the domain naming master must be unexpectedly and permanently removed from the network, you can seize the domain mastering role and reassign it to another domain controller. To seize the role, follow these steps:

1. Choose Run from the Start menu (or open a command window), and then type `ntdsutil` and press Enter.

2. At each prompt, supply the following information and then press Enter:
   a. At ntdsutil, type `roles`.
   b. At fsmo maintenance, type `connections`.
   c. At server connections, type `connect to server` followed by the fully qualified domain name of the controller that is to be the new master.
   d. At server connections, type `quit`.
   e. At fsmo maintenance, type `seize domain naming master`.
   f. At ntdsutil, type `quit`.

Important Before seizing the domain naming master, the controller holding the domain naming master role must be disconnected completely from the network. Seizing the domain naming master role is a radical step, and do not do it unless the original domain naming master is permanently out of service. Before you can bring the original domain naming master back online, you must first reformat its boot disk and reinstall Windows Server 2003.

Relative Identifier Master
When a domain controller creates a security object—a user, a group, or a computer account—it assigns a unique security identifier (SID) to the object. The SID is made up of two parts: the domain security ID that is common to all security objects in the domain, and the relative ID that is unique to each object. The RID master is the controller in each domain that allocates and tracks the sequences of relative IDs.
Users won’t notice the temporary loss of the RID master. Administrators are also unlikely to notice unless they’re creating security objects and the domain runs out of relative ID numbers. So transferring the RID master role isn’t usually necessary unless the RID master is to be removed permanently from the network.

**Transferring the RID Master**

If you need to transfer this role to another controller, follow these steps:

1. Launch Active Directory Users and Computers from the Administrative Tools folder.
2. Right-click the domain node, and choose Connect To Domain Controller from the shortcut menu.
3. Select the domain controller you want to give the role of RID master. Click OK.
4. Right-click the domain node, and choose Operations Masters from the shortcut menu. A dialog box opens. On the RID tab, the current focus (the controller that will become the RID master) is shown, as well as the current operations master.
5. Click Change and then click OK.

**Seizing the RID Master**

If the RID master must be unexpectedly and permanently removed from the network, you can seize the RID mastering role and reassign it to another domain controller. To seize the role, follow these steps:

1. Choose Run from the Start menu (or open a command window), and then type `ntdsutil` and press Enter.
2. At each prompt, supply the following information and then press Enter:
   a. At `ntdsutil`, type `roles`.
   b. At `fsmo maintenance`, type `connections`.
   c. At `server connections`, type `connect to server` followed by the fully qualified domain name of the controller that is to be the new master.
   d. At `server connections`, type `quit`.
   e. At `fsmo maintenance`, type `seize RID master`.
   f. At `ntdsutil`, type `quit`.

**Important** Before proceeding with the seizure, the controller holding the RID master role must be disconnected completely from the network. Seizing the RID master role is a radical step. Don’t do it unless the original RID master is permanently out of service. Before you can bring the original RID master back online, you must first reformat its boot disk and reinstall Windows Server 2003.
Infrastructure Master

The infrastructure master is responsible for keeping up with the changes in group membership and distributing updates to other domains. One infrastructure master exists in each domain. If the controller holding the infrastructure master role becomes unavailable, it won’t affect users. Even administrators won’t notice until a number of user account changes don’t show up in other domain controllers. Therefore, it’s best not to transfer the infrastructure master role unless the controller is going to be unavailable for a considerable period.

Real World  Placing the Infrastructure Master Role

Unless the domain has only one domain controller, or your forest has only a single domain, don’t assign the infrastructure master role to the controller hosting the global catalog (GC). To find out whether changes need to be distributed to other domains, the infrastructure master looks to a GC and updates itself using the GC information. If the GC and the infrastructure master are on the same controller, the infrastructure master will never find any outdated data, so nothing is replicated to other domains. See Chapter 14 for more about the GC.

Transferring the Infrastructure Master

To transfer the infrastructure master role to another controller, follow these steps:

1. Launch Active Directory Users and Computers from the Administrative Tools folder.
2. Right-click the domain node, and choose Connect To Domain Controller from the shortcut menu.
3. Select the domain controller you want to give the role of infrastructure master. Click OK.
4. Right-click the domain node, and choose Operations Masters from the shortcut menu. Click the Infrastructure tab to see the current focus (the controller that will become the infrastructure master) as well as the controller that is the current operations master.
5. Click Change and then click OK.

Seizing the Infrastructure Master

If the infrastructure master is unexpectedly and permanently removed from the network, you can seize the infrastructure master role and reassign it to another domain controller. To seize the role, follow these steps:

1. Choose Run from the Start menu (or open a command window), and then type `ntdsutil` and press Enter.
2. At each prompt, supply the following information and then press Enter:
   a. At ntdsutil, type `roles`.
   b. At fsmo maintenance, type `connections`.
   c. At server connections, type `connect to server` followed by the fully qualified domain name of the controller that is to be the new master.
   d. At server connections, type `quit`.
   e. At fsmo maintenance, type `seize infrastructure master`.
   f. At ntdsutil, type `quit`.

**Important** Before proceeding with the seizure, the controller holding the infrastructure master must be disconnected completely from the network. Seizing the infrastructure master role is a drastic step. Don’t do it unless the original infrastructure master is permanently out of service. Before you can bring the original infrastructure master back online, you must first reformat its boot disk and reinstall Windows Server 2003.

**Summary**

Active Directory is a major part of the Windows Server 2003 enterprise network infrastructure, and planning, deploying, and maintaining it is a major part of the network administrator’s burden. Learning to use the Active Directory tools included with Windows Server 2003 makes it possible to create and maintain a directory service infrastructure that is efficient and largely self-regulating. With Active Directory solidly in place, you can move on to other administrative responsibilities, which are discussed in following chapters. Chapter 16 covers network addresses and Internet protocols.
The protocol wars have ended, and TCP/IP is the winner. After years of proprietary protocols vying for popularity, TCP/IP has emerged as the only protocol needed by most networks. Every modern computer supports TCP/IP, as do a growing number of other devices such as printers, network appliances, personal digital assistants (PDAs), and cell phones. Additionally, Novell NetWare, Microsoft Windows, and Apple Mac operating systems have been using TCP/IP as their preferred network protocol for some time now.

Although the basics of setting up TCP/IP on a server are covered in Chapter 7, in this chapter we cover some of the theory behind TCP/IP and the tools you use to handle IP addresses on your network. In the next chapter, we'll cover the details of day-to-day administration of TCP/IP.

**The TCP/IP Protocol Suite**

Whole books have been written about TCP/IP, and justifiably so. Although most administrators don't need to know every detail of programming a TCP connection or what to expect as a return value from a `gethostbyname` call, they do need to understand enough to configure the protocol and make it work properly.

The key thing to remember about TCP/IP is that it isn't a single entity. TCP/IP is short for Transmission Control Protocol/Internet Protocol, but these are only two of the protocols included in the TCP/IP suite. There are a variety of other protocols, each with its own specialized area of importance and use.

TCP/IP isn't proprietary and isn't controlled by any one company or vendor, unlike other protocols such as Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)
and the now-obsolete NetBIOS Extended User Interface (NetBEUI) protocol. TCP/IP is an open standard controlled by the Internet Engineering Task Force (IETF) and by the users of the Internet itself in the form of RFCs (requests for comments). Anyone can submit an RFC for consideration and inclusion into the written definitions of the protocols and policies of the Internet and TCP/IP.

Internet Protocol
IP is the core protocol of the TCP/IP suite. To quote from RFC 791, “The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks.” IP performs only one basic function: it delivers a packet of bits (called a datagram) from point A to point B over any network “wire” it happens to encounter along the way.

Note The term wire is used loosely here and elsewhere to indicate the actual—usually physical—network connection between two points. In fact, that wire can just as easily be a piece of optical fiber or even a radio or infrared signal. In all cases, it functions as the transmission medium through which the packets travel.

IP doesn’t in and of itself know anything about the information in the datagram it carries, nor does it have any provision beyond a simple checksum to ensure that the data is intact or that it has reached its destination. That is left to the other protocols in the TCP/IP suite.

Transmission Control Protocol
According to RFC 793 (the defining RFC for the protocol), TCP is “a connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols which support multinetwrok applications.” That’s nice, but what does all that really mean? The following list should help:

- **Connection-oriented** TCP provides for the communication of packets between two points, sending the datagram specifically from one computer or device to another, and sending an acknowledgment back to the sending computer on receipt of intact packets.

- **End-to-end** Each TCP packet designates a specific endpoint as its destination. Packets are passed along the wire and ignored except by the actual endpoint of the packet and any device that needs to direct it.

- **Reliable** This is the key point of TCP. When a program or application layer protocol such as File Transfer Protocol (FTP) uses TCP for its transport protocol, TCP takes responsibility for the reliability of the communications. The protocol itself provides for interprocess communication to ensure that packets that are sent out
not only get there, but also that they get there in the order in which they were sent. If a packet is missed, the protocol communicates with the sending device to ensure the packet is resent.

Because TCP has to create a reliable connection between two devices or processes, each packet involves substantially more overhead than is needed with other, less reliable protocols within the suite. But by the same token, the programmer writing the application that uses TCP doesn’t have to include a lot of error checking and handshaking in the application itself.

User Datagram Protocol

The User Datagram Protocol (UDP), another protocol in the TCP/IP suite, is a connectionless, transaction-oriented protocol designed to send packets with a minimum of protocol overhead. It provides no guarantee that its intended recipient received the packet, or that packets were received in the order in which they were sent. UDP is frequently used in broadcast messages where there is no specific intended recipient, such as Boot Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) requests, but it can also be used by applications that prefer to ensure reliable delivery internally rather than in an underlying protocol. UDP is defined in RFC 768.

Many parts of the TCP/IP suite of protocols and programs can use either TCP or UDP as their transport protocol. The choice of which to use will depend on the reliability and security of the network you’re on and whether there are routing issues. An example of a protocol that can use either TCP or UDP is the Network File System (NFS) Protocol.

Windows Sockets

Windows Sockets (commonly referred to as Winsock) is a Microsoft technology that provides a consistent way for application programs to communicate with a TCP/IP stack without having to consider any underlying variations in the TCP/IP stack implementation.

In the distant past, there were many vendors of TCP/IP protocol and applications suites for MS-DOS–based computers, each slightly different from the others. This situation made it extremely difficult to write an application that required TCP/IP and yet worked with all the TCP/IP implementations that existed. Winsock was designed to get around this problem by providing a uniform set of application programming interface (API) calls that would be the same regardless of the underlying differences in the actual implementation of TCP/IP.

The original Winsock version 1 had a fair number of difficulties, and version 1.1 was released soon after its initial implementation. The current version of Winsock supported by Microsoft Windows Server 2003 and Windows XP is version 2, which provides for full
backward compatibility with earlier versions while offering improved functionality and support for additional features and expandability. Note that Winsock 2 has been around since Microsoft Windows NT 4, so applications are widely available that use this API—something that will become more important as IP version 6 (discussed later in the chapter) is rolled out.

**NetBIOS**

Network Basic Input/Output System (NetBIOS) is a networking API used by legacy applications and operating systems to communicate across a network using the NWLink (IPX/SPX compatible), NetBEUI, or TCP/IP protocols.

Until the advent of Microsoft Windows 2000, NetBIOS was the primary networking API used by all Microsoft operating systems. NetBIOS names were used for name resolution within Windows-based networks. Any time a computer wanted to communicate with another computer on the network, the computer had to resolve the NetBIOS name for the other computer either by querying a Windows Internet Naming Service (WINS) server, using a NetBIOS broadcast, or referring to the computer’s local Lmhosts file.

With Windows 2000, Microsoft changed the Windows networking infrastructure to one based on TCP/IP, with no NetBIOS support required. Networks based on Windows Server 2003 or Windows 2000 can use DNS to resolve network names, and network applications can use the Winsock interface to communicate using a network.

Unfortunately, because earlier versions of Windows require NetBIOS support to function properly on a Windows-based network, most companies still need to support NetBIOS over TCP/IP and provide WINS services for earlier clients and servers. Even in a pure Windows Server 2003 and Windows XP network, NetBIOS and WINS might be required, depending on other applications and servers that are on the network.

**Requests for Comments**

Requests for comments (RFCs) come in many guises, but all of them have the same intent and a somewhat similar format. They are designed to provide a way for an extremely diverse group—the users of the Internet—to communicate and agree on the architecture and functionality of the Internet. Some RFCs are official documents of the IETF, defining the standards of TCP/IP and the Internet; others are simply proposals trying to become standards; and others fall somewhere in between. Some are tutorial in nature, others are quite technical, and some are even humorous (such as RFC 2324, “Hyper Text Coffee Pot Control Protocol”). But all are a way for the Internet, an essentially anarchic entity, to organize and communicate information.
There’s no need to list all the RFCs here, and you certainly don’t need to read them all, but you should know where to find them and be aware of the most important ones. You can find listings of RFCs in a number of places, including http://www.ietf.org/rfc.html; an excellent site we use that we find friendlier and more accessible is http://www.cse.ohio-state.edu/cs/Services/rfc/index.html. The RFCs at this location are organized and linked logically to make it easy to find the information you’re looking for. This site, however, isn’t necessarily as up–to date as the official RFC editor site, http://www.rfc-editor.org. If you want to be sure you have the most current information, use the latter site. Table 16-1 lists some important RFCs and their subject matter.

Table 16-1  Some key RFCs and what they cover

<table>
<thead>
<tr>
<th>RFC Number</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 768</td>
<td>User Datagram Protocol (UDP)</td>
</tr>
<tr>
<td>RFC 791</td>
<td>Internet Protocol (IP)</td>
</tr>
<tr>
<td>RFC 792</td>
<td>Internet Control Message Protocol (ICMP)</td>
</tr>
<tr>
<td>RFC 793</td>
<td>Transmission Control Protocol (TCP)</td>
</tr>
<tr>
<td>RFC 821</td>
<td>Simple Mail Transfer Protocol (SMTP) (Obsoleted by RFC 2821)</td>
</tr>
<tr>
<td>RFC 822</td>
<td>Standard for the Format of Advanced Research Project Agency (ARPA) Internet Text Messages (Obsoleted by RFC2822)</td>
</tr>
<tr>
<td>RFC 854, 855</td>
<td>Telnet Protocol</td>
</tr>
<tr>
<td>RFC 959</td>
<td>File Transfer Protocol (FTP)</td>
</tr>
<tr>
<td>RFC 1001, 1002</td>
<td>Network Basic Input/Output System (NetBIOS) over TCP/IP</td>
</tr>
<tr>
<td>RFC 1011</td>
<td>Official Internet Protocols</td>
</tr>
<tr>
<td>RFC 1034</td>
<td>DNS Concepts and Facilities</td>
</tr>
<tr>
<td>RFC 1035</td>
<td>DNS Implementation and Specification</td>
</tr>
<tr>
<td>RFC 1166</td>
<td>Internet Numbers</td>
</tr>
<tr>
<td>RFC 1542</td>
<td>Clarifications and Extensions for the Bootstrap Protocol</td>
</tr>
<tr>
<td>RFC 1886</td>
<td>DNS Extensions to Support IP version 6 (Obsoleted by RFC 3596)</td>
</tr>
<tr>
<td>RFC 1918</td>
<td>Address Allocation for Private Internets</td>
</tr>
<tr>
<td>RFC 2131</td>
<td>Dynamic Host Configuration Protocol (DHCP)</td>
</tr>
<tr>
<td>RFC 2136</td>
<td>Dynamic Updates in the DNS System (Dynamic DNS)</td>
</tr>
<tr>
<td>RFC 2251</td>
<td>Lightweight Directory Access Protocol (LDAP)</td>
</tr>
<tr>
<td>RFC 2460 through 2463</td>
<td>Internet Protocol version 6 (IPv6) Specifications</td>
</tr>
<tr>
<td>RFC 2661</td>
<td>Layer Two Tunneling Protocol (L2TP)</td>
</tr>
<tr>
<td>RFC 2782</td>
<td>A DNS Resource Record (RR) for Specifying the Location of Services (DNS SRV)</td>
</tr>
</tbody>
</table>
**IP Addresses and What They Mean**

Your IP address is to the Internet (or to the other computers on your local network) what your street address is to your mail carrier. It uniquely identifies your computer by using a simple, 32-bit (or 128 bits with IPv6) addressing scheme. This scheme, which originated in the late 1960s and early 1970s, uses four octets separated by dots, in the form \textit{w.x.y.z} (we'll use these letters to represent each octet throughout the chapter), to describe both the network’s address and the local machine’s address on that network. Each octet is represented by a single decimal number but is called an octet because it requires eight bits to describe.

In terms of IP addresses, most networks fall into one of three classes: A, B, or C. These different classes describe networks (sometimes referred to as licenses) of different sizes and complexities. The licenses to use a range of IP addresses are controlled by Internet Corporation for Assigned Names and Numbers (ICANN).

**Class A Networks**

A class A network has an address that begins with a number from 1 through 127 for the first octet—the \textit{w} portion of the address. This octet describes the network itself, and the remainder of the address is the actual local device’s address on that network. A class A network with the network address of 10 (the \textit{w} portion) contains all IP addresses from 10.0.0.0 to 10.255.255.255.

The class A address 127 has a special meaning and isn’t available for general use. This means there are a total of 126 possible usable class A addresses in the world (from 1 through 126), and that each class A network can contain more than 16 million unique network devices.
The class A addresses were spoken for long ago and are assigned to such entities as the United States Department of Defense, Stanford University, and Hewlett-Packard.

**Real World 127: The Loopback Address**

All IP addresses that begin with the network number 127 are special. Your network card interprets them as loopback addresses. Any packet sent to an address beginning with 127 is treated as if it got to its intended address, and that address is the local device. So packets addressed to 127.0.0.1 are treated the same as packets to 127.37.90.17; both are actually addressed to your current machine, as are all the other 16 million addresses in the 127 class A network. (You too can have your very own class A network. Of course, you can talk only to yourself, but who cares?)

**Class B Networks**

A class B network uses the first two octets, w and x, to describe the network itself, and the remainder of the address is the actual local device’s address on that network. The first octet in a class B network must begin with a number from 128 through 191, resulting in 16,384 class B networks, each of which can have 65,534 unique addresses. This is still a pretty large network, and most of the class B networks were assigned long ago to large organizations or companies such as Rutgers University and Toyota Motor Corporation.

Many addresses in the class B address space have subsequently been divided into smaller groups of addresses and reassigned. Large Internet service providers (ISPs), for example, use this technique to more efficiently use the available address space.

**Class C Networks**

A class C network has an address that begins with a number from 192 through 223 for the w octet of the address and uses the first three octets (w.x.y) to describe the network itself. The last octet, z, describes the actual local device’s address on that network. This arrangement makes for roughly 2 million class C networks, each of which can have a maximum of 254 devices on the network. That’s enough for a small business or a department, but not for a major corporation.

**Note** Because Internet-accessible IP addresses are in such short supply these days, a new method of dividing up Internet IP addresses was created—Classless Internet Domain Routing (CIDR). CIDR allows IP addresses to be leased out in smaller chunks than entire classes so that companies can lease a more suitable number of IP addresses than if they had to lease an entire class A, B, or C network. CIDR uses variable length subnet masks to accomplish these smaller address chunks.
Class D and Class E Addresses

An IP address with a number from 224 through 239 for the w octet of the address is known as a class D address, which is used for multicast addresses. With multicast addresses, a number of computers can share a single multicast address, in addition to their normal IP addresses. This makes it easy to send identical data to multiple hosts simultaneously—just send the data to the shared multicast address and every member of the multicast group receives it.

The IP address space that uses the numbers 240 through 247 for the w octet is referred to as a class E address. This space is reserved for future use.

Real World  IP Addresses for Networks that Use Firewalls or Internet Gateways

Organizations and companies today use routers, proxy servers, and firewalls between the computers in their organization and the public Internet. The addresses of the computers within the organization are translated by that router or firewall and never directly propagated onto the Internet. Addresses within the organization, then, need to be unique within the organization, but not necessarily globally unique, because no other organization will see them. Should you use just any old address then? No, you really shouldn’t. There is a special set of network addresses reserved for just such uses. These addresses are defined in RFC 1918, and by using these addresses you can comfortably employ a substantially larger address space than you are otherwise able to access.

Using these special network addresses also protects the integrity of the Internet. Because these special addresses are designated exclusively for private networks, they are automatically filtered at routers, protecting the Internet. The following is a list of these special addresses:

- 10.0.0.0 through 10.255.255.255 (a single 24-bit block of addresses or a class A network)
- 172.16.0.0 through 172.31.255.255 (16 contiguous 20-bit blocks of addresses or class B networks)
- 192.168.0.0 through 192.168.255.255 (256 contiguous 16-bit blocks of addresses or class C networks)

You should always use addresses from this group of addresses for your internal network. Only machines directly connected to the public Internet should use globally
unique IP addresses. All other devices on your network should use these RFC 1918 addresses, which will be hidden by the router or firewall from public view using Network Address Translation (NAT). Microsoft Windows Server 2003 can provide NAT directly, or you can choose to use a full-featured firewall such as Microsoft Internet Security and Acceleration Server 2004 (ISA 2004). When you use a firewall or proxy server, you require “real” IP addresses only for machines that are outside your firewall and are visible to the Internet as a whole, which helps conserve the global IP address space.

Routers and Subnets

If every computer on the Internet had to know the location of every other computer on the Internet and how to get from here to there, the entire Internet would have come to a grinding halt long ago. Early on, it became apparent that some method was needed to filter and route packets to allow users to not only print to their network printers easily, but also reach any other computer on the Internet without having to know a whole lot about how to get there. Enter subnets, routers, and gateways.

What Is a Subnet?

A subnet is simply a portion of the network that operates as a separate network, without regard to what happens outside and without affecting the rest of the network. A subnet is usually a separate physical “wire” that has only a single point of contact with other areas of the network, through a router or bridge—although even when two subnets share the same physical wire, they still require a router to connect to each other.

Setting up a subnet involves using what is known as a subnet mask to allow computers in a subnet to see and directly communicate only with other computers in the same subnet. A subnet mask is a special number, again in w.x.y.z form, that masks or blocks areas outside the subnet from sight. The mask works by letting you see only those portions of the IP address space that aren’t masked by a 1. (Remember that each octet is actually an 8-bit binary value. To “mask by 1” means to ensure that the appropriate bit has been set to a value of 1.) For example, if you have a class C address of 192.168.222.17, and your subnet mask is 255.255.255.0 (a typical class C subnet), as shown in Figure 16-1, you can see only addresses in the last octet of the address (the z portion).

If your IP address is 192.168.222.17, the address at 192.168.223.25 is hidden from you by your subnet mask of 255.255.255.0. You can send a packet to that address only by first passing that packet to a gateway or router that knows both where you are and either
where the other network is or how to find it. If, on the other hand, you send a packet to a printer with the IP address 192.168.222.129 or to a computer at 192.168.222.50, you have no problem. The system can see that address, and the packet goes directly to its destination.

Figure 16-1  Subnet masking

If you can assign an entire class of addresses to a subnet, it’s easy to figure out what your mask is; however, if you can assign only a portion of a class (as is the case when leasing Internet IP addresses using CIDR), you need to sit down with your binary-to-decimal conversion tables and determine exactly what the correct subnet mask should be. (Remember that this is all done in binary.) If you understand how it works, you can customize your subnet mask or figure out what the one you have is actually doing. Custom subnet masks are also called variable length subnet masks, and are often referred to in so-called slash notation, where the network number is specified, followed by the number of bits used in the subnet mask. For example, 192.168.1.0/26 has a subnet mask of 255.255.255.192, allowing a single class C network to be broken into 4 subnets, with a maximum of 62 hosts per subnet.

Note  Use the default subnet mask for your network class unless you have a specific reason not to. For a class A network, this is 255.0.0.0; for a class B network, it’s 255.255.0.0; and for a class C network, use 255.255.255.0. For in-depth information about subnet masks, see the Microsoft Windows Server 2003 Resource Kit (Microsoft Press, 2005).

All the subnet masks on a single portion of your network must be the same. If they aren’t, this causes all sorts of problems. One machine might be able to send a packet to another, but the other might not be able to send the packet back.
Under the Hood  Physical vs. Logical

Throughout this chapter, we talk about subnets as being separate physical segments on the network. And usually that is the case. But there can be occasions when different subnets need to share the same physical segment of “wire.” Sometimes that’s an actual Ethernet cable they’re sharing, but it could also be a wireless network. You can have different physical networks even with wireless, by using different frequencies. For example, 802.11a and 802.11g are on different wireless frequencies and cannot see each other. Thus, an 802.11a and 802.11g network have some of the same characteristics as two separate Ethernet cables. Regardless of whether two subnets are on the same physical wire, however, they can’t see each other because of the subnet masking without the intervention of a router. But in this case, the router would have two connections (virtual or physical) to the same physical network.

Often you’ll have two different wireless networks sharing the same “wire”—that is, the same frequency and same general physical location. But even here, subnets and subnet masks help to hide one network from another. If you have a public, unsecured, 802.11g wireless network and a private, secured, 802.11g wireless network, you should assign a different subnet to each network. Traffic that must cross from one to the other will still need the services of a router.

Gateways and Routers

A gateway can have different functions on a network, but for the moment you’re going to focus on the subnet and routing functions. As already mentioned, if you have a subnet mask of 255.255.255.0 and the y octet of your IP address is 222, you can’t see an IP address on the network with a y octet of 223.

How, then, do you get to an IP address on another subnet? The answer is a gateway or router. A router is a device (usually an external box, but sometimes a computer with more than one network adapter) that connects to more than one physical segment of the network and sends packets between those segments as required. It takes your packets from the 222 subnet and sends them over to the 223 subnet for delivery to the address on that subnet. Thus, it acts as a gatekeeper between the two separate portions of the network, keeping the traffic with 222 addresses in the 222 subnet and letting only traffic with 223 addresses cross over to the 223 segment.

If a router doesn’t know where to direct a packet, the router knows which entity to ask for directions—another router. It constantly updates its routing tables with information from other routers about the best way to get to various parts of the network.
Although the terms *gateway* and *router* are often used interchangeably, strictly speaking a gateway is a device or computer that translates between networks of different architectures, such as IPX/SPX and TCP/IP. A router is a device or computer that sends packets between two or more network segments as necessary using logical network addresses (typically IP addresses).

In addition to gateways and routers, there are also *bridges*. These are devices or computers that direct traffic between two network segments based on physical (media access control) addresses, and they are generally used to isolate two sections of a network to improve performance. Bridges are cheaper and less capable than routers.

### Address Resolution and Routing Protocols

Detailed information about how address resolution and routing protocols work and the algorithms involved in routing and address resolution are beyond the scope of this book, but it’s useful to know what some of the protocols are, if only to recognize acronyms when they’re thrown about. In that spirit, the following list consists of the most common TCP/IP address resolution and routing protocols:

- **Address Resolution Protocol (ARP)** Maps the IP address to the physical hardware address (the media access control (MAC) address) corresponding to that IP address, permitting you to send something to an IP address without having to know what physical device it is.

- **Routing Information Protocol (RIP)** A distance vector-based routing protocol that is mostly provided for backward compatibility with existing RIP-based networks. As with most distance vector-based routing protocols (which make extensive use of broadcasts to discover which other devices and routers are nearby), RIP is being replaced by newer routing protocols that scale better and have lower network traffic overhead.

- **Open Shortest Path First (OSPF)** A link-state routing protocol that is suitable for use in large and very large networks, such as those common in large enterprises. Link-state routing protocols maintain a map of the network topology that they share with other routers. As the topology changes, routers update their link-state database and then inform neighboring routers of the topology change, reducing the amount of network bandwidth consumed when compared to vector-based routing protocols.
Real World  Routing Flaps

The Internet has grown exponentially in the last few years, stretching the technology for resolving addresses to the limit, and sometimes past the limit. When a major router on the Internet goes down—even momentarily—all the other routers on the Internet have to tell one another about it and recalculate new routes that bypass that router. This adjustment results in large numbers of packets passing back and forth, causing traffic to become so heavy that the routing updates can’t occur properly because the information doesn’t make it through the traffic. Such a situation is called a routing flap, and it can cause a large portion of the Internet to come to a virtual halt.

Routing flaps don’t happen very often, but they are becoming more and more of a problem. In addition, current router technology is reaching the limit of its ability to calculate the best route from all the possible routes when major changes are caused by the failure of a key router. The next generation of TCP/IP (known as IP version 6, and discussed later in this chapter) will help, as will new algorithms for performing the routing calculations.

Name Resolution

As useful as the 12-decimal–digit IP numbers (192.168.101.102) are when it comes to computers recognizing other computers, they’re not the sort of information that human minds process very well. Not only is there a limit to how many 12-digit numbers one can memorize, but such numbers can easily change.

Even worse, IP version 6 (IPv6) addresses are 128 bits expressed in strings that can have as many as 32 hexadecimal characters, although they’re often shorter. (Actually, IPv6 addresses can even be written as 128 ones and zeroes, but that’s not likely to catch on.) Obviously, easy-to-remember names are preferable to strings of numbers or strings of characters and numbers. This section looks at how names are handled in the TCP/IP and Internet world.

The Domain Name System

The Domain Name System (DNS) was designed in the early 1980s, and in 1984 it became the official method for mapping IP addresses to names, replacing the use of “hosts” files. With Windows 2000, DNS became the method clients use to locate domain controllers using the Active Directory service. (Clients use LDAP to actually access the data stored in
the Active Directory database.) Although there have been modifications to the overall structure of DNS, the overall result is still remarkably like the original design.

More Info  See RFC 1591 for an overall description of DNS, and RFCs 1034 and 1035 for the actual specification. RFCs 3007, 4033, 4034, and 4035 provide the specification for dynamic updates (Dynamic DNS), with which Windows Server 2003, Windows XP, and Windows 2000 comply.

The Domain Namespace
The domain namespace describes the tree-shaped structure of all the domains from the root (".") or "dot") domain down to the lowest level leaf of the structure. It is a hierarchical structure in which each level is separated from those above and below with a dot, so you always know where you are in the tree.

Before the Internet moved to DNS, a single master file (Hosts.txt) had to be sent using FTP to everyone who needed to convert from numbers to names. Every addition or change required a revised copy to be propagated to every system. This obviously created enormous overhead even when the Internet was still quite small.

DNS overcomes the limitations of Hosts.txt files by maintaining a distributed database that is extensible to add information as needed. It permits local administration of local names while maintaining overall integrity and conformance to standards.

Top Level Domains
The top level domains are the first level of the tree below the root. They describe the kinds of networks that are within their domain in two, three, or now four letters, such as .com for commercial domains and .edu for educational domains. The original top level domains were functionally based and had a decidedly American slant. That’s not surprising, given that most of the namespace was originally set up and administered by the U.S. Department of Defense.

As the Internet grew, however, this approach made less and less sense, especially with a distributed database such as DNS that allowed for local administration and control. Geographical top level domains were added to the functionally based ones, such as .it for Italian domains, and so on.

How Names Are Resolved into Addresses
When you click a link to http://www.microsoft.com and your browser attempts to connect to that site, what actually happens? How does it find www.microsoft.com? The short answer is that it asks the primary DNS server listed in the TCP/IP Properties dialog box on your workstation. But how does that DNS server know where the site is?
Real World  Where Domain Names Come from and How You Get One

These days, virtually every business (and many individuals) wants its own domain. The keeper and distributor of domain names used to be Network Solutions, formerly called InterNIC. Recently this task was opened up to competition, and there are now a myriad of companies that will register your domain name for you. The list is too big and volatile to include here—for a complete listing, visit the Internet Corporation for Assigned Names and Numbers (ICANN) Web site at http://www.icann.org/registrars/accredited-list.html. You can link to any of the accredited registrars from this site and perform a search to find out if your chosen name is taken.

Have alternative names in mind as well; you’ll probably need them. After you research existing names and choose one that isn’t taken, register the name with your chosen registrar. Pay between $15 and $35 (US) per year or you lose the name.

After you acquire a domain name from a registrar such as Network Solutions, you need to properly set up the DNS hosting for the domain name. If you acquired the domain name through your Web hosting company, this is probably done automatically for you. Otherwise, follow the directions provided by your registrar to enter the addresses of two DNS servers that have DNS records for your domain name. If you’re using a Web hosting company, these are probably that company’s DNS servers. If you’re hosting your Web site on your own server or servers, you’ll need to either host your own DNS records or contract with a company that specializes in DNS to host them for you. This could be your ISP, or a company such as ZoneEdit (www.zoneedit.com) that specializes in DNS.

Long ago, domain names were free and forever, but those days are gone. If you don’t pay your bill from your chosen registrar, your domain name is put up for grabs, and chances are that someone else will claim it before you’re able to reregister it. The available short names are disappearing at a rapid rate, and many people are finding that they need to think up longer versions to find something that isn’t taken.

When a TCP/IP application wants to communicate with or connect to another location, it needs the address of that location. However, it usually knows only the name it’s looking for, so the first step is to resolve that name into an IP address. The first place it looks for the name is in the locally cached set of names and their IP addresses that it has resolved recently. After all, if you asked about http://www.microsoft.com just a few minutes ago,
why should it go through all the trouble of looking up that name again? It’s not likely that the IP address will have changed in that time.

Suppose, however, that you haven’t been on the Internet for a couple of days, and your computer doesn’t have the address for http://www.microsoft.com cached. In this case, Windows queries your primary DNS server (specified in the connection properties for your Internet connection). If your DNS server doesn’t have any recent information about http://www.microsoft.com, the DNS server asks around to see whether anyone else knows the IP address.

This can happen in a couple ways. The default method is to use recursion, in which the DNS server queries the root server of the domain, which passes back the location of the DNS server that is authoritative regarding the next level down in the domain, which the original DNS server then queries. This process recurs until it reaches a DNS server that contains the IP address of the desired host in its zone data.

Note You might want to disable the use of recursion on your DNS server if it is in use on an internal network and you want your clients to fail over to a secondary DNS server that handles name resolution for hosts outside your local network.

If you disable recursion on the DNS server, or if the client doesn’t request the use of recursion, the DNS entry for the desired host is found by iteration. When using iteration, the DNS server checks its zone and cache data, and when it finds that it cannot complete the request, it sends the client a list of DNS servers that are more likely to have the host name in their zones. The client then contacts those servers, which might in turn respond with their own list, possibly even to the point that the client might query the Internet root servers looking for the appropriate DNS server.

**Reverse Lookups**

In most cases, you have a host name for which you need to locate the IP address, but in some instances you might have only an IP address for which you need to look up the host name. Reverse lookup was added to the DNS specification for this reason. The only problem with creating reverse lookups is the difference between the way the DNS namespace is organized and the way in which IP addresses are assigned. DNS names go from specific to general, beginning with the host name and ending with the root of the domain [the period at the end of a fully qualified domain name (FQDN)]. IP addresses work in reverse fashion, so to facilitate the lookup of a host name from an IP address, a special domain, the in-addr.arpa domain, was created.
In the in-addr.arpa domain, the octets of an IP address are reversed, with in-addr.arpa appended to the address. For example, the IP address 10.230.231.232 is queried as 232.231.230.10.in-addr.arpa.

The reverse lookup zone is maintained as a separate database within the DNS database. The resource records (RRs) in the reverse lookup zone are of the type PTR (pointer). Much like pointers in common programming languages, or shortcuts in Windows, these PTR RRs refer to a different record—the associated A (address) record in the forward lookup zone. For example, the following list describes two records that a host might have:

- **A record (forward lookup zone)**  
xmpl-svr3.example.local IN A 192.168.51.3

- **PTR record (reverse lookup zone)**  
3.51.168.192.in-addr.arpa. IN PTR xmpl-svr3.example.local

You can perform a reverse lookup of an IP address by typing `nslookup` followed by the IP address you want to look up at a command prompt. For example, if you type `nslookup 192.168.51.3`, the DNS server responds with the name and address of the DNS server, followed by the name and address of the host.

### Dynamic DNS and Active Directory Integration

Dynamic DNS, which was new to Windows 2000 Server, makes DNS more flexible by permitting clients to update their DNS records dynamically. This capability eliminates the need to update DNS entries manually when clients change IP addresses. Unfortunately, the standard dynamic DNS service described in RFC 2136 allows for only a single-master model, in which a single primary DNS server maintains the master database of zone data (the addresses and host names for a particular domain). This database can be replicated with secondary DNS servers, but only the primary server can manage dynamic updates to the zone. If the primary server goes down, client updates to the zone aren’t processed.

The dynamic DNS server in Windows 2000 Server can overcome the limitations of a single-master model and use Active Directory to store its zone data, permitting a multiple-master model. Because the Active Directory database is fully replicated to all Active Directory–enabled domain controllers, any domain controller in the domain can update DNS zone data. Using Active Directory to store the zone data also allows for added security features and simplified planning and management, as well as faster directory replication than is possible using a single-master model, because Active Directory replicates only relevant changes to the zone.
Zone Storage and Active Directory

A DNS server is required to support the use of Active Directory, so if a DNS server can’t be found on the network when a server is being promoted to domain controller, the DNS service is installed by default on the domain controller. After Active Directory is installed, the storage and replication of your zones can be done in one of two ways:

- **Standard zone storage using a text-based file**  With this method, zones are stored in .DNS text files located in the %SystemRoot%\System32\DNS folder. The filename is the same as the zone name you chose when creating the zone. Figure 16-2 shows part of a text DNS zone file.

- **Directory-integrated zone storage**  Zones are stores in a dnsZone container object located in the Active Directory tree.

![Figure 16-2 Zone storage in a text file](image)

The second method is preferred, not only because integrated zones are automatically replicated and synchronized whenever a new domain controller comes online, but also for reasons of administrative simplicity. Keeping a DNS namespace separate from the Active Directory namespace doubles your work (and your chances for error) when testing replication or modifying your domain, for example.

However, it is important to realize that using directory-integrated zone storage decreases the number of dynamic updates per second that the DNS server can process by a factor of two, and secure dynamic updates decrease this number by an additional 25 percent. Although performance varies widely depending on the hardware in question and what services are running, Microsoft found that a dual-processor Pentium III 733-MHz system with 256 MB of RAM running Windows Server 2003 can process 9500 queries per second.
and 1300 dynamic updates per second with 75 percent processor usage when using a standard primary zone storage.


For more information about monitoring DNS server performance, see [http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/5e81fbe2-764a-47c4-bc7a-0da6f447897b.mspx](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/5e81fbe2-764a-47c4-bc7a-0da6f447897b.mspx).

Lightweight Directory Access Protocol
LDAP is used to access data in the Active Directory database. Once again, DNS is used to locate domain controllers, and LDAP is used to access the Active Directory data. LDAP runs on top of TCP/IP, and Active Directory supports both versions 2 and 3 of LDAP. Any LDAP product complying with these specifications can be used to access data in Active Directory. For more information about Active Directory and LDAP, see Chapter 2.

Dynamic Host Configuration Protocol
One of the problems facing organizations using TCP/IP these days is deciding how to manage internal IP addresses. The chore of managing and maintaining all the IP addresses in your organization can quickly become an administrator’s nightmare, especially if you deal with intermittently connected computers such as laptops and remote computers. DHCP provides a simple way to handle addresses for computers, and it allows for greatly simplified administration and management of addresses and configuration. If you need to make a change to the TCP/IP settings for your entire organization, you need to make the change only to the DHCP server and it will be automatically propagated to all the DHCP clients. This is a lot simpler than having to go around to every computer in the organization and change their settings.

DHCP allows the administrator to assign IP addresses only as required. A mobile user can connect a laptop to the network when necessary and be assigned an appropriate address automatically. Likewise, a dial-in user doesn’t need a permanent IP address; one can be assigned when the connection is made to the network, and when the connection is broken the address is made available for someone else’s use.

How DHCP Works
To receive an IP address, the client computer sends a DHCP discover broadcast, which a DHCP server picks up and responds to by offering the client an IP address for its use. The client responds to the first offer it receives and sends back to the DHCP server a
request for the IP address offered. The DHCP server sends an acknowledgment telling the client that it succeeded in leasing the IP address for the amount of time specified by the DHCP server.

DHCP clients attempt to renew their leases at boot-up, as well as after 50 percent of the lease time has passed. In this renewal process, the discover stage is skipped and the client simply begins with a request. If the renewal of the lease fails at the 50 percent mark, the client waits until 87.5 percent of the lease has passed and then attempts to acquire a new IP address by sending out a DHCP discover broadcast and starting the IP lease process again.

Using Multiple DHCP Servers
Because DHCP uses UDP broadcasts, your DHCP servers don’t see (and thus don’t respond to) client requests on a different subnet unless the router between the two is configured to forward broadcasts. In most large establishments, this means separate DHCP servers for each subnet because broadcast traffic is an unnecessary burden on your routing capacity. If your DHCP server properly supports RFC 3011, it can handle requests from multiple subnets, assigning the correct address for each subnet. You can also configure a second DHCP server for each subnet to provide for redundancy and to give your network a way to issue addresses if the main DHCP server fails.

If you do opt to allow your routers to pass along broadcasts, they must support RFC 1542 and be configured to forward BOOTP broadcasts. Check the documentation for your router for configuration information; most new routers (and newer versions of router software) support this. If your router doesn’t support RFC 1542 and you have clients that don’t have access to a local DHCP server, you must configure a DHCP relay agent to forward client broadcasts to a DHCP server on another network segment.

---

**Note** Although you can use DHCP remotely with supported routers, it’s best to situate your DHCP servers on-site. WAN failures do occur, and even a brief one can keep clients from being able to acquire or maintain an IP address. Letting a WAN be in a position to put your LAN out of business is a bad idea.

Windows Server 2003 supports integration of DHCP with dynamic DNS to facilitate the updating of a client’s DNS record when the client receives a new IP address from a DHCP server.

DNS servers in a DHCP managed network should support dynamic DNS. The Windows Server 2003 or Windows 2000 Server DNS will properly support dynamic updates, as will BIND version 8 or later.
Note Zone transfers between Windows 2000 and BIND version 9.x DNS servers might not work unless the Windows 2000 server is running Service Pack 3 or later. Zone transfers between Windows Server 2003 and BIND version 9.x work fine.

Typically, you need one DHCP server for every 10,000 clients, though this number can be higher if you have large disk capacity and a fast CPU, or lower if your IP address class or network layout prevents this kind of server utilization. DHCP is very disk-intensive, so make sure that if your server will be handling a significant number of clients you have sufficient hardware, such as a large and fast redundant array of independent disks (RAID), adequate memory, and one or more fast CPUs. For information about evaluating the performance of your current system, see Chapter 35.


Real World DHCP and Availability

DHCP itself does not support synchronization with other DHCP servers. If your network demands increased reliability, have a backup DHCP server offline with the same scope as the primary server, so if the primary server goes down you can bring the backup online immediately. (You can also use the Windows Server 2003 or Windows 2000 Server Cluster service to create a DHCP cluster.)

You might also want to split the address space between two DHCP servers, with the primary server handling 80 percent of the address space and the secondary server handling 20 percent. If the primary server fails, the secondary server handles all client leases from its 20 percent of the address space until the primary server is brought back online. If both servers are down, clients maintain their IP addresses until their leases run out.

If server reliability is a problem on your network, consider increasing the lease time to allow more time to bring servers back online before clients lose their addresses.

Windows Internet Name Service

NetBIOS is an interface originally developed to allow applications to access network resources in the Microsoft MS-DOS operating system. As such, it was the primary networking API and naming method for Microsoft networks until the release of Windows 2000.
NetBIOS host names are up to 15 characters long and part of a flat namespace, so all names on a given network must be unique. Normally, host names are resolved by broadcast—not the most efficient means in terms of either time or network bandwidth. Routers also usually do not forward NetBIOS broadcasts, eliminating the ability to resolve host names on a different subnet.

WINS was created to provide a solution to this problem by maintaining a dynamic database of IP addresses and their associated NetBIOS names. However, WINS is still limited in many ways by the underlying architecture of NetBIOS, and it is now an optional service in a Windows Server 2003 or Windows 2000 network.

Although many of us might be eager to do away with WINS, it is still used by many companies to provide NetBIOS name resolution services to earlier Microsoft operating systems, such as Microsoft Windows 98 and Windows NT, that don’t function properly in a NetBIOS-free network. (Windows Server 2003, Windows XP, and Windows 2000 don’t require NetBIOS support.)

---

**Note**  WINS is usually deployed in conjunction with DNS to provide optimal support for newer clients. Although BIND 8 and newer versions can be used adequately as a DNS server for Windows Server 2003 and Windows 2000 Server networks, BIND doesn’t support WINS records, which can cause issues with DNS zone transfers. For this reason, stick with Windows 2000 or newer DNS servers if you need to use WINS servers on your network (although there are workarounds, as discussed in Chapter 17).

When deploying WINS servers on your network, deploy only the minimum number necessary to provide adequate service to your clients. WINS servers can be a pain to replicate, so keeping the number of servers down can be a big plus. (Microsoft itself, for example, used no more than about 12 WINS servers worldwide before moving to Windows 2000.) If you’re doing any major restructuring of your network, consider upgrading older clients to Windows XP (or at least Windows 2000) and eliminating WINS from your network.

---

**Important**  Don’t install WINS on a multihomed server. WINS has enough replication problems without complicating the situation by placing the server on two subnets.

To make WINS and Browsing (explained in the “Browsing vs. browsing” sidebar) work correctly when you are in an enterprise environment with subnets and multiple domains,
keep a few tricks in mind. There are three possible scenarios listed here, and each is discussed in the sections that follow:

- Single domain across a subnet boundary
- Multiple domains within a subnet boundary
- Multiple domains across a subnet boundary

**Single Domain Across a Subnet Boundary**

To see the resources of a single domain across a subnet boundary, with only TCP/IP as your protocol, you need to set up WINS servers on both sides of the router or mess around with Lmhosts files. Avoid Lmhosts files like the plague: they’re a pain to get right in the first place and have to be manually edited every time there is a change anywhere. They also don’t deal well with DHCP, under which IP addresses are subject to change. However, if you’re setting up a virtual private network with Internet-connected clients, you might not be able to avoid Lmhosts because these clients don’t have an available WINS server.

In general, it’s a good idea to have a domain on each side of your router. The alternative is much more traffic across the router than you want, because every authentication request has to cross over. The obvious choice is to put a WINS server in each domain. No special requirements need to be met for this to work because Browsing doesn’t need to be told about another domain.

**Real World  ** _Browsing vs. browsing_

A source of possible confusion in any discussion about Microsoft networking is the subtle distinction between the common meaning of the word “browsing” and the very specific meaning that the word has in Microsoft networking. Many texts use “browsing” to mean looking for or at the resources available, which is a reasonable use of the word. However, “Browsing” in the Microsoft networking sense refers to the Computer Browser service used by Windows-based computers to maintain browse lists of all shared resources on the network. It’s easy to get confused, so to avoid that here, “Browsing” is always capitalized when used in the Microsoft networking sense.

With the growth of networks and the introduction of directories such as Active Directory, Browsing has become much less important. Most networks are too large to browse for resources, and Active Directory helps alleviate this issue by permitting you to query Active Directory for the resources you want. This makes finding resources easier, and also reduces the network traffic caused by Browsing.
Multiple Domains Within a Subnet Boundary
If you're running a forest within a single subnet, you might want a WINS server in each domain, but you don’t need to do anything special with Browsing. You can set up and explicitly add the other domains to browse, but this step isn’t required.

Multiple Domains Across a Subnet Boundary
Now you get to the tricky one. For everything to work in multiple domains across a subnet boundary, you need to set up everything very carefully. Because the Browsing packets don’t cross the subnet boundary unless they know where they’re going, you need to explicitly set the Computer Browsing service to browse the domain on the far side of the router. Each domain in the forest or tree needs to be configured to browse any domains on the far side of the router.

For the technical details of WINS and Browsing, see the *Microsoft Windows Server 2003 Resource Kit*. When you have a network free of Microsoft clients earlier than Windows 2000, you might be able to happily turn off WINS and make your life a lot easier. However, before disabling WINS on your network, you should carefully test your existing applications and servers to ensure that there isn’t a dependency on NetBIOS names that you aren’t aware of.

**IP Version 6**
As pointed out earlier, the explosive growth of the Internet has pushed it to the limits of the original design. The number of IP addresses has grown almost exponentially in recent years, leading to the fear that there will soon not be enough addresses to connect all the devices and computers that people want to connect. If that weren’t bad enough, routers are being overloaded by the increasing inadequacy of the IPv4 standard.

To find a solution to the limitations of the 32-bit address space and the limits to the routing protocols in the current structure of TCP/IP, the IETF and others began working on a new version of IP several years ago. Different working groups originally proposed different solutions, but over time these groups have arrived at a consensus on the next generation of IP, IP version 6 (often shortened to IPv6). It was formally accepted by the IETF in December 1994, and the current specification is in RFC 2460.

IPv6 defines a 128-bit IP address space compatible with the current implementation of TCP/IP (version 4, or IPv4). The specifications call for packets to include additional information for improved routing and handling of mobile devices. IPv6 will not only enlarge the address space available, but it will also improve network performance, ease configuration issues, and provide enhanced security via required IPSec support. (See Chapter 22 for more information about IPSec and other TCP/IP-related security protocols.)
IPv6 addresses have four times the number of bits that IPv4 addresses do (128 vs. 32), but what does that actually mean? The 32-bit address structure can enumerate more than 4 billion hosts on as many as 16.7 million networks, but the number of potential IPv6 addresses totals $2^{96}$ times the size of the IPv4 address space ($4 \times 2^{96}$). This works out to $340,282,366,920,938,463,463,374,607,431,768,211,456$ possible addresses. Of course, given routing and hierarchical requirements, this theoretical address space is diminished greatly when making practical estimates. The mathematically minded should consult RFC 1715, in which Christian Huitema analyzes other addressing schemes (including the French and U.S. telephone systems) and concludes that 128-bit addressing will suffice for another 25 years of Internet growth.

Despite the benefits, many are not looking forward to the deployment of IPv6. After all, most companies try to minimize the number of protocols they need to support. Supporting yet another protocol is regarded with less enthusiasm than Friday afternoon performance audits. The transition will be gradual, however, and there is an incredible amount of work in progress to ensure that it is painless as well.

Although the impending shortage of IP addresses has been pushed off somewhat by companies that use a small number of Internet-accessible IP addresses to provide Internet access to an internal private network (which is free to use a class A network), the time for IPv6 is approaching. Some companies, such as ISPs and cellular phone networks, are already deploying IPv6, although it will still be some time before IPv6 actually replaces IPv4.

Windows Server 2003 ships with built-in support for IPv6. Before deploying IPv6, however, you should test your environment and key applications to ensure full compatibility. With that said, here are some facts about the IPv6 implementation in Windows Server 2003:

- IPv6 support is installed and uninstalled like any other protocol—by right-clicking the desired network connection and choosing Properties.

- Internet Explorer 6 and IIS 6 support IPv6, as does the Windows Server 2003 versions of FTP, Telnet, and other select network applications (though Internet Explorer can’t browse IPv6 Web sites when using a non-IPv6-compatible proxy server and both Internet Explorer and IIS don’t support literal IPv6 addresses).
The IPv6 protocol stack in Windows Server 2003 and Windows XP is independent of the IPv4 protocol stack, which means existing functionality won’t be altered. However, there is no support in Windows Server 2003 for IPv6-only operation—that is, IPv4 must also be available together with IPv6, even in networking environments where only IPv6 is used for communication.

Limited IPSec for IPv6 support is included, but it relies on static keys and isn’t suitable for using outside your test labs yet.


**Summary**

Although it’s not necessary to become an expert on TCP/IP to run a network, some basic knowledge is required. TCP/IP and DNS in particular are worth studying in some depth because so many network difficulties can be traced to the misconfiguration of one or the other. The next chapter covers the administration of the TCP/IP server programs DNS, DHCP, and WINS.
Now that you understand some of the underlying principles of TCP/IP (which were covered in Chapter 16), it’s time to deal with the day-to-day issues of managing and administering TCP/IP.

The three basic network features that virtually all TCP/IP-based networks need to use are:

- Dynamic Host Configuration Protocol (DHCP), to dynamically provide clients with IP addresses and configuration information
- Domain Name System (DNS), to translate IP addresses into friendly names that are easier to deal with and vice versa
- Windows Internet Naming Service (WINS), to translate NetBIOS names and IP addresses for clients that still use NetBIOS

Although Active Directory and Microsoft Windows clients function with standards-based DHCP and DNS servers, such as those available for UNIX systems (nobody other than Microsoft makes WINS servers), Active Directory works best with the DHCP and DNS servers provided as a part of Microsoft Windows Server 2003 and Microsoft Windows 2000 Server. There are a few additional capabilities available when you deploy Active Directory in conjunction with DHCP and DNS servers running Windows Server 2003 or Windows 2000 Server, such as secure dynamic updates for legacy clients and multi-master replication between DNS servers.

This chapter shows you how to install and manage DHCP, DNS, and WINS servers running Windows Server 2003.

Using DHCP

If you’ve ever managed more than a very small number of computers on a network, you’ve probably used DHCP. DHCP can provide both an IP address and all the essential configuration information that any client on the network needs to connect and communicate with other computers, both on the network and outside on the Internet. By providing a central location for address management and disbursement, the DHCP service of Windows Server 2003 makes it easy to configure and manage your TCP/IP network.

The DHCP server provided with Microsoft Windows Server 2003 is truly excellent—it works predictably, reliably, and properly. The following sections describe how to use it. If you need to get up to speed about how DHCP works, see Chapter 16.

Designing DHCP Networks

It’s important to design the deployment of DHCP servers in a way that fits the network. Small, nonrouted networks can use a single DHCP server. If you have a larger network, consider the subnets and routers in use, and also split the address space between two servers or host your DHCP service on a cluster to improve fault tolerance. Use the following checklist as part of your planning:

- Draw a map of the network, showing each physical and logical subnet and the routers joining the subnets.
- If the network uses routers to subnet the network, determine whether the routers support forwarding DHCP broadcasts. (Most newer routers do, although this option usually needs to be turned on.)
- Plan on sectioning the IP address range between two DHCP servers to provide fault tolerance. (DHCP servers can’t communicate with each other, so they can’t share the same addresses.) Give 80 percent of the addresses to one server, and 20 percent to the other server. (This is called “the 80/20 rule.”) If one server goes down, clients can still receive IP addresses from the other server. Alternatively, you can set up a DHCP server cluster to handle 100 percent of the addresses.
- If the link between the subnets is fast and reliable and the routers in between can be configured to forward DHCP broadcasts (or if you add a DHCP relay agent), you can place the second DHCP server on a different physical subnet. Otherwise, deploy a pair of DHCP servers to each physical subnet.
- Don’t run a DHCP server on a domain controller if you plan on using the DHCP server to update DNS records for legacy clients. Doing so creates an additional security risk. (Consult the DNS Help topic in the Windows Server 2003 Help system for more information—specifically, check the Dynamic Updates topics.)
Size the servers appropriately. A single DHCP server can service no more than 10,000 clients and 1000 scopes.

Upgrade any Microsoft Windows NT 4 domain controllers to Windows Server 2003 or Windows 2000 Server. (See Chapter 6 for more information about upgrading.)

Use a disk drive with fast access time, or better yet, use a redundant array of independent disks (RAID). DHCP servers frequently access the disk drives, and a fast storage subsystem means better DHCP performance.

**Note** Another method of protecting against DHCP server failure is to have a hot backup. To do this, set up a DHCP server identically to the primary DHCP server, except with its own scope, that encompasses 20 percent of the address space (or possibly less). Don’t activate this server. (It could be serving other roles that you don’t want to slow down except in the case of an emergency.) If the primary DHCP server goes down, manually bring the backup server online by activating its scope. However, splitting the address range between two live servers or using a DHCP server cluster is a superior solution because it provides automatic fault tolerance—no manual intervention is required.

**DHCP Security Considerations**

Although DHCP servers aren’t high-value targets for hackers, there are nonetheless a number of vulnerabilities inherent to DHCP servers. Because the number of IP addresses in a scope is limited, an unauthorized user can launch a denial-of-service (DoS) attack on the network by acquiring a large number of IP addresses from the DHCP server. A DoS attack on the DNS server can also be initiated by performing a large number of DNS dynamic updates via DHCP. Similarly, a user with physical access to the network can easily use a non-Microsoft DHCP server to set up a rogue DHCP server that provides improper IP addresses to other clients.

To round off the list of DHCP security vulnerabilities, any user that obtains an IP address from the DHCP server will probably also obtain the addresses for company DNS and WINS servers. A hacker can then obtain further information about the network configuration from these servers or attack them.

To minimize these risks, limit physical access to your network. If a hacker can plug into your network, his or her job is immensely easier than trying to break through a firewall. The use of 802.1x across the entire physical network to control access can significantly reduce the risk. Also make sure to maintain and regularly review DHCP audit logs (stored by default in the %windir%\System32\Dhcp folder).
Plan the IP Address Range and Exclusions
Besides determining how to place the DHCP servers into the network structure, you also need to plan the IP address ranges you’ll use, as well as which IP addresses to reserve or exclude from this pool of addresses. Use the following list to help plan the IP address ranges to use and exclude:

- Determine the range of IP addresses that the DHCP server will manage. Most likely, this will be a private address range such as 10.x.x.x or 192.168.x.x.

- Make a list of any IP addresses to exclude to support hosts with static IP addresses. Only DHCP servers and hosts that don’t work as DHCP clients need static IP addresses, although you might want to use static addresses for DNS servers as well.

  Note  Consider switching all hosts with statically assigned IP addresses to DHCP assigned addresses. If any servers need unchanging addresses, create client reservations for the servers using DHCP. (Lease reservations are covered later in this chapter.) This allows the servers to use an unchanging address and yet still have all TCP/IP options configured automatically through DHCP. It also makes it easier to track and manage IP addresses, and it will make your life much easier if your company ever needs to change its addressing, as might happen after a merger. The fewer static addresses, the better.

- Make a list of servers that need to have unchanging IP addresses, such as DNS and WINS servers, and then decide whether you can use a DHCP reservation or whether bona fide static addresses are needed.

- If the DHCP server will be using Internet-registered IP addresses (which it probably won’t), register the IP addresses with the Internet service provider (ISP).

Installing the DHCP Service
The easiest way to set up the DHCP service is by using the Manage Your Server Wizard (also called the Configure Your Server Wizard) to install the DHCP server role and create a new scope. (The Configure Your Server Wizard is discussed in Chapter 7; creating scopes is covered in the next section.) However, you can also do this manually by installing the Dynamic Host Configuration Protocol (DHCP) component, accessible through the Add/Remove Programs tool.

  Note  Configure the server with a static IP address before setting up the DHCP server service. See Chapter 7 for help with this.
Real World  DHCP Options

There are four levels at which you can configure DHCP options in a Windows Server 2003 DHCP server:

- **Server options.** These options apply to all clients of the DHCP server you’re managing. Because of this, use server options sparingly—specify server options only for parameters common across all scopes on the server.

- **Scope options.** These are the most often used type of options—they apply to all clients within a scope and override any server options set on the DHCP server.

- **Client options.** These options are specified for individual clients. This is useful if specific computers need special options. Client options override all other options, including class options.

- **Class options.** These options provide DHCP parameters to clients based on the type of client they are—either using vendor classes such as all Microsoft Windows 95 or Windows 98 clients, or with user classes that specify clients with particular needs, such as RRAS clients, “mobile clients,” or any other user-defined class. For more information about creating and using class options, consult the Help system or the Microsoft Windows Server 2003 Resource Kit.

Creating a New Scope

After installing the DHCP service, the next thing you must do to get the DHCP server up and running is create a new scope of IP addresses for the DHCP server to manage. (A scope is a range of IP addresses that the DHCP server can manage.) Before you do this, make sure you know which range of IP addresses is approved, which IP addresses need to be excluded for systems with static IP addresses, and which IP addresses need to be reserved for DNS or WINS servers.

Important  If you use the Manage Your Server Wizard to create a default first server, it will automatically create and activate a DHCP scope for your network. Carefully review the settings it made, and make any necessary changes. If there are already DHCP servers on your network do not run this wizard.
Scopes, Superscopes, and Multicast Scopes

A scope is simply the range of possible IP addresses on a network. To add more clients to a network where the scope is exhausted, you can add another scope as long as the scope doesn’t overlap with an existing scope. An excellent source of information about the complex subject of choosing subnet masks and other TCP/IP issues is Microsoft Windows Server 2003 TCP/IP Protocols and Services Technical Reference by Thomas Lee and Joseph Davies (Microsoft Press, 2003).

When you create multiple scopes, it’s important to understand that clients from one logical subnet aren’t able to obtain IP addresses from a different scope than the one they currently belong to, because the other scope is in a different logical subnet. If this is the behavior you want, great. However, if you want clients to be able to use addresses from other scopes, use a superscope.

A superscope is a collection of scopes grouped together into a single administrative whole. There are three primary reasons you might want to use superscopes:

- One scope is running out of IP addresses.
- You need to renumber the IP network, and therefore move clients from one set of addresses to another.
- You want to use two DHCP servers on the same subnet for redundancy.

When you create a superscope, you enable clients to obtain or renew leases from any scope within the superscope, even if they contain addresses from a different logical subnet.

A multicast scope is simply a scope of multicast addresses (class D addresses) that are then shared by many computers (members of the multicast group).

To create the new scope, follow these steps (or if you’re using the Configure Your Server Wizard to set up DHCP, you can jump to Step 4):

1. Launch DHCP from the Administrative Tools folder on the Start menu.
2. If the DHCP server you want to administer isn’t listed in the DHCP console tree, choose the Add Server command from the Action menu to locate the server you want to administer.
3. Select the appropriate DHCP server in the console tree. Select the Action menu, and choose New Scope to launch the New Scope Wizard.
4. Click Next, and type a name and description for the scope to use for distinguishing this scope from others. (See Figure 17-1.) Click Next.

![Figure 17-1](image)

**Figure 17-1** The Scope Name page of the New Scope Wizard

5. Type the IP address that the scope begins with in the Start IP Address field, and type the IP address that the scope ends with in the End IP Address field, as shown in Figure 17-2.

![Figure 17-2](image)

**Figure 17-2** The IP Address Range page of the New Scope Wizard
6. Type the network’s subnet mask in the Subnet Mask box, or use the Length box to adjust the length of the subnet mask. Then click Next.

7. To exclude a range of addresses from the scope, in the Start IP Address box, type the start IP address for the exclusion range; in the End IP Address box, type the end IP address for the exclusion range. (To add a single address, enter it in the Start IP Address box and then click Add.) Then click Add. Add as many exclusions as needed, and click Next when you’re finished.

8. Specify the lease duration for the clients, and then click Next. For more information, see the “Setting Lease Durations” sidebar.

9. To configure DHCP options, choose Yes; otherwise, choose No, and then click Next. If you select No, click Finish to complete the setup of the scope.

10. If you chose to specify DHCP options for this scope, type the routers (default gateways) you want clients to use in the Router (Default Gateway) page, clicking Add after typing each one. When you’re finished adding gateways, click Next.

   **Note** Set only the options you know you need. If you’re uncertain about an option, leave it alone.

11. Type the domain name of the domain in the Parent Domain box, and add the IP addresses for the DNS servers in the IP Address box, as shown in Figure 17-3, clicking Add after entering each one. Click Next when you’re done.

   ![New Scope Wizard](image)

   **Figure 17-3** The Domain Name And DNS Servers page of the New Scope Wizard
12. In the WINS Server Address box, type the addresses of any WINS servers you configured on the network for resolving NetBIOS names into IP addresses for down-level clients. Click Next.

13. To activate the scope immediately, choose Yes; otherwise, choose No to activate the scope later. Click Next, and then click Finish to complete the scope configuration.

**Real World  Setting Lease Durations**

Use longer leases for networks without redundant DHCP servers to permit more time to recover an offline DHCP server before clients lose their leases, or to minimize network traffic at the expense of less frequent address turnover. You can also use longer leases if scope addresses are plentiful (at least 20 percent available), the network is stable, and computers are rarely moved.

In contrast, scopes that support dial-up clients or mobile clients such as laptops or personal digital assistants (PDAs) can have shorter leases and therefore function well with fewer addresses.

If you’re planning a major network change, change the scope lease duration to be quite short. This will allow you to make the changes you need to the DHCP Scope properties and have them rapidly deployed to all clients. After the network change is made, don’t forget to set the DHCP back to a more reasonable duration to minimize the amount of network traffic and resource utilization on the DHCP server.

Lease durations are set in the scope’s Properties dialog box. Scopes are listed in the DHCP administration console.

**Authorizing the DHCP Server and Activating Scopes**

After you set up the DHCP server and create the scopes, you must authorize the server to give leases and activate the scopes. DHCP servers that are also domain controllers are automatically authorized when added to the DHCP Manager console.

Authorizing a DHCP server is an important step that Windows Server 2003 provides to reduce the occurrence of unauthorized (rogue) servers set up to hand out false IP addresses to clients. Although rogue DHCP servers that use UNIX or a hardware-based DHCP server can still be set up, Windows Server 2003–based and Windows 2000–based DHCP servers can’t be used in a Windows domain without authorization.

To authorize the DHCP server after installing the service, select the server in the DHCP console and then choose Authorize from the Action menu. To manage the list of authorized
servers, right-click DHCP at the root of the console tree and choose Manage Authorized Servers from the shortcut menu.

To activate a scope, right-click the scope in the console tree, and then choose Activate from the shortcut menu. Don’t activate a scope until you finish selecting all the options you want. When you activate a scope, the Activate command on the menu changes to Deactivate.

---

**Under the Hood  Scope Deactivation**

When you deactivate a scope, the assumption is that those addresses are not being used by the network and the DHCP server will not accept those addresses as valid. Any existing clients will be unable to renew their addresses, and when they try, they’ll cause DHCP negative acknowledgement messages to be sent from the server to the client. This is the correct method if your intent is to never use those addresses as part of a DHCP scope again, and you should deactivate a scope prior to deleting it. But if what you want to do is temporarily stop handing out addresses in a particular scope, the preferred method is to add an exclusion that covers the entire address range of the scope. This way, any existing addresses already given out are retained by the clients and are considered valid. When you’re ready to re-enable the scope, you simply remove the exclusion.

---

**Adding Address Reservations**

Reservations are used to provide a consistent and unchanging IP address to servers and other hosts that need to be at a predictable IP address. The only servers that can’t use a reservation are DHCP servers—they must be at a fixed IP address. Using reservations instead of static addresses guarantees that a server has a consistent IP address, while giving you the ability to easily change settings as required, and to recover the IP address in the future if the server is decommissioned or moved.

To add an address reservation to a scope, right-click the Reservations folder under the desired scope, and choose New Reservation from the shortcut menu. Walk through the wizard, and add the new reservation. You’ll need to know the MAC address for the DHCP client you want a reservation for, and the IP address you want to assign to it.

---

**Important**  When reserving an address for a client, make the reservation on all DHCP servers that potentially service that client. You can create reservations outside the address range of the scope on the server, allowing you to use the same set of reservations even when you’re using multiple servers.
Note To obtain the MAC address, go to the client computer (or make a remote desktop connection) and type `ipconfig /all` at the command prompt. The MAC address is listed as the physical address. Or check the current DHCP lease for the client—the MAC address is shown in the Unique ID column. Yet another way to get the MAC address is to use the new `getmac` command in Windows Server 2003. From a command prompt, type: `getmac /s computer` where `computer` is the IP address, hostname, or DNS name of the remote computer you want the MAC address for.

Enabling Dynamic Updates to a DNS Server for Earlier Clients

Microsoft Windows Server 2003, Windows XP, and Windows 2000 clients automatically update their forward lookup records with the DNS server after obtaining a new IP address from a DHCP server, while explicitly requesting that the DHCP server update their reverse lookup (PTR) records on the DNS server. This second step requires communication between the DHCP server and the DNS server.

Because legacy and non-Windows clients don't automatically update their own resource records, you can configure the DHCP server to update the legacy client's forward and reverse lookup records whenever the client obtains a new IP address.

To enable legacy client support for DHCP and dynamic DNS, use the following procedure:

1. Select the scope or DHCP server on which you want to permit dynamic DNS updates.
2. From the Action menu, choose Properties, and then click the DNS tab.
3. Select the Enable DNS Dynamic Updates option, as shown in Figure 17-4.
The other options available on the DNS tab are:

- **Dynamically Update DNS A And PTR Records Only If Requested By The DHCP Clients**  
  This option allows Windows XP, Windows 2000, and other Windows clients to decide whether to update the DNS server themselves or have the DHCP server update their DNS address (A) and reverse lookup (PTR) records.

- **Always Dynamically Update DNS A And PTR Records**  
  This option forces the DHCP server to update the A and PTR records for all DHCP clients, even if they request permission to update the DNS server themselves.

- **Discard A and PTR Records When Lease Is Deleted**  
  This option forces the DHCP server to delete the A record as well as the PTR record of a client whose lease has expired or is deleted. (The PTR record is always deleted at lease expiration, regardless of this setting.)

- **Dynamically Update DNS A And PTR Records For DHCP Clients That Do Not Request Updates**  
  This option enables the DHCP server to update the forward and reverse lookup records for clients that can’t update their own forward lookup records (Windows Me and all other versions of Windows prior to Windows 2000). If you don’t select this check box, the DNS records of pre–Windows 2000 clients aren’t dynamically updated.

---

**Note**  
Although Windows Server 2003 can interoperate with Berkeley Internet Name Domain (BIND) DNS servers, mixing and matching DHCP and DNS servers can cause trouble, particularly when it comes to DHCP–DNS communication, secure dynamic updates, and updating DNS records for clients running earlier versions of Windows. Because of this, it’s best to use Microsoft DHCP and DNS servers for internal addressing and name resolution on Windows-based networks. (You can reference BIND DNS servers for external name resolution without issues.)

---

**Real World  
DHCP, Stale Records, and Secure Dynamic Updates**

There is a problem that arises when using DHCP in combination with DNS zones that make use of secure dynamic updates. When DHCP creates a DNS record for a client running an earlier version of Windows, the DHCP server becomes the owner of the record. As the owner of the record in a zone with secure dynamic updates enabled, only the DHCP server is allowed to update the record. This is usually fine; however, the DNS records of clients running earlier versions of Windows become stale.
stale (outdated) and orphaned (unable to be updated by anyone) under the following conditions:

- If the DHCP server is replaced by a backup server, or its scope is migrated to another server (in which case the records are still owned by the original server)
- If the client is upgraded to Windows 2000, Windows XP, or Windows Server 2003 (in which case the records are still owned by the DHCP server, which will no longer update the records because the client is now theoretically capable of doing so)

The best solution is to upgrade all clients running earlier versions of Windows, but this is obviously impractical for some networks. Another solution is to add all DHCP servers to the DnsUpdateProxy group. When a member of this group creates or updates a DNS record, no security information is recorded. (The record is unsecured.) This prevents the record from becoming orphaned. When any other computer modifies one of these unsecured records, it then becomes the owner. (This is intended to allow upgraded clients to take possession of their DNS records.) However, astute readers will notice that this means that all DNS records recorded by the DHCP servers are unsecured and can be modified by anyone who changes their DNS name to the name of an unsecured record. (They also acquire ownership in doing so.) This also includes the DNS record of the DHCP server itself. To protect against this risk, create a dedicated DHCP service account that is used exclusively for dynamic DNS updates. For more information about this, see Microsoft Knowledge Base Article 816592.

To add a DHCP server to the DnsUpdateProxy group, in the Active Directory Users And Groups snap-in, right-click the DHCP server, and then choose Properties from the shortcut menu. Click the Member Of tab, click Add, type DnsUpdateProxy in the box, and then click OK.

Windows Server 2003, Windows XP, and Windows 2000 clients are exempt from this issue. (They can directly communicate with the DNS server and securely update their DNS records.)

Using Multiple DHCP Servers for Redundancy

Computers don’t lose network connectivity immediately when a DHCP server goes down, but new computers, returning laptops, or little-used systems that haven’t recently logged on might not be able to obtain network access until a DHCP server is available.
To ensure that there will continue to be an available DHCP server, even if the primary DHCP server is down, configure multiple DHCP servers. The traditional solution is to set up redundant servers with a split scope across the servers. Windows Server 2003 Enterprise Edition gives you the option of configuring DHCP onto a cluster for high availability.

**Splitting the Address Space Between Two Servers**

To employ two DHCP servers for load balancing and redundancy, use the following procedure:

1. Create identical scopes on each server for all valid IP addresses that the DHCP servers you’re setting up will manage. This might mean creating a single scope (if you have a single subnet), or multiple scopes encompassing a number of subnets.

2. Set up exclusions so that the primary DHCP server handles 80 percent of the address pool and the secondary server handles the other 20 percent of the addresses. Thus, each server excludes the addresses available on the other server so that no address appears in both servers’ address pools.

3. Create a superscope on both servers that contains all valid scopes for the physical subnet. To do so, select the appropriate DHCP server from the console tree, choose the New Superscope command from the Action menu, name the superscope, and then select the member scopes to include.

   **Note** You can delete a superscope without affecting the member scopes by selecting the superscope and pressing Delete. However, **deactivating** a superscope deactivates all member scopes as well.

   **Best Practices** If you have a routed network with DHCP relay agents or routers that forward DHCP broadcasts between the physical subnets, you can use DHCP servers on other subnets as secondary servers. However, unless the DHCP server has at least one scope with available addresses from the client’s own subnet, the client isn’t able to obtain or renew an IP address lease. To make sure this doesn’t happen, create two superscopes on each server, one for each logical subnet. Thus, each server owns 80 percent of the address pool for its local subnet, and 20 percent of the address pool for the other DHCP server’s local subnet.

**Setting Up a DHCP Server Cluster**

Although splitting the address space between two DHCP servers is an adequate way to provide redundancy and load balancing, an even more powerful solution is to set up the DHCP service to run on a Windows Server 2003 cluster. The members of the cluster equally share the DHCP service workload, and if one of the servers fails, the other servers
Chapter 17  Administering TCP/IP  509

continue to provide addresses to clients as if nothing had happened. Instead of an
address space split between servers, each server in the cluster has access to the complete
address space.

Using the Windows Server 2003 Cluster service is discussed in detail in Chapter 19, but
the basic steps to get a DHCP server up and running in a cluster are as follows:

1. Install DHCP (as described earlier in this chapter), and set up the server cluster (as
described in Chapter 19).

   **Note**  You should not create or activate any DHCP scopes until the DHCP
   service is set up on the cluster, as described in the following steps.

2. Launch Cluster Administrator from the Administrative Tools folder on the Pro-
   grams menu.

3. Select the cluster you want to use to host the DHCP service.

4. Choose the Configure Application command from the File menu to open the Con-
   figure Application Wizard.

5. Click Next in the first page, and then choose the Use An Existing Virtual Server
   option and select the appropriate group. If you haven’t already created a virtual
   server, choose the Create A New Virtual Server option and use the wizard to create
   a new virtual server (as discussed in Chapter 19).

6. In the Create Application Cluster Resource page, choose the Yes, Create A Cluster
   Resource For My Application Now option, choose the DHCP resource type, and
   then click Next.

7. Type a name and, optionally, a description for the DHCP resource and then click
   Next.

8. Click Advanced Properties, click the Dependencies tab, and then click Modify.

9. Double-click the IP address, physical disk, and network name you want to use for
   the DHCP server cluster. These resources then appear as dependencies. Click OK
   when finished, optionally modify the properties of the resource, and then click OK.

10. Click Next in the Application Resource Name And Description page, specify where
    the DHCP database should be stored (most likely the physical disk you specified in
    Step 9), and then click Next. If you select a different disk, make sure that it belongs
    to the group and that a dependency has been created for it.

11. Review the settings, and click Finish to complete the wizard.
12. Verify that the resource is displayed in the correct group, and then right-click the resource and choose Bring Online from the shortcut menu to enable the DHCP server to begin servicing clients.

13. Authorize the DHCP server in Active Directory (if on an Active Directory network), as discussed earlier in this chapter.

Note Right-click the group to which the DHCP resource belongs, and choose Move Group from the shortcut menu to verify that the resource has been properly created on the cluster. If the group moves properly, the resource setup is fine.

Other DHCP Functions
The DHCP snap-in provides a single point from which to administer all the properties and functionality of the DHCP servers.

Modifying Scopes
Modify a scope’s properties by right-clicking the scope in the console tree and choosing Properties from the shortcut menu. This displays the Scope Properties dialog box shown in Figure 17-5.

Figure 17-5 The General tab of the Properties dialog box for a DHCP scope
To deactivate a scope, right-click the scope in the DHCP console and choose Deactivate from the shortcut menu. To return the scope to use, right-click the scope again and choose Activate.
Note To temporarily stop distribution of leases from a scope, adjust the exclusion range so that no new addresses are available rather than deactivating the scope. This avoids forcing clients currently using addresses in the scope to prematurely obtain a new IP address from a different DHCP server or a different scope.

To exclude a range of IP addresses from a scope, right-click the Address Pool folder under the appropriate scope and choose New Exclusion Range from the shortcut menu. Type the range of addresses you want to exclude, and then click Add.

**Enabling Server-Based Conflict Detection**

The Windows Server 2003 DHCP server provides the ability to enable server-based conflict detection, which is a technique that pings an IP address before leasing it to a client to ensure that it’s not already in use by a static IP client. Windows Server 2003, Windows XP, and Windows 2000 clients automatically verify that the IP address offered by the DHCP server is available before accepting it, so conflict detection is useful only for earlier clients. In the interest of conserving network bandwidth and reducing client startup times, leave this option disabled unless you’re having problems with duplicate IP addresses, as might be the case if you have undocumented static IP addresses on the network.

To enable server-based conflict detection, right-click the DHCP server in the console tree and choose Properties from the shortcut menu. Click the Advanced tab, and then set the Conflict Detection Attempts number to 1. Don’t increase this number beyond 2; this results in additional searches and needlessly increases the time it takes a client to obtain an IP address.

**Setting Up a DHCP Relay Agent**

If you have a routed network, deploy DHCP servers on both sides of routers to maximize reliability and minimize bandwidth usage. However, there are instances in which you want to allow DHCP to work across a router; for example, if the routed network is very reliable and fast, as might be the case with a partitioned local network or municipal area network (MAN), you might want to simply allow clients to cross the router to reach a DHCP server.

You can configure most routers manufactured in the last several years to pass DHCP broadcasts (because they’re BOOTP-compliant), but if the router doesn’t support forwarding DHCP broadcasts, you can set up a server running Windows Server 2003 or Windows 2000 Server as a DHCP relay agent using the following procedure:

1. Launch Routing and Remote Access from the Administrative Tools folder on the Programs menu.
2. If the server you want to make a DHCP relay agent isn’t listed in the console tree, choose the Add Server command from the Action menu to locate the server you want to administer.

3. If the appropriate server isn’t already enabled, select it, choose the Configure And Enable Routing And Remote Access command from the Action menu, and then click Next (otherwise, skip to Step 5).

4. Choose Custom Configuration in the wizard, click Next, select LAN Routing, click Next, and then click Finish.

5. In the Routing and Remote Access window, select the IP Routing object on the desired server, right-click the General object, and then choose New Routing Protocol from the shortcut menu.

6. Select DHCP Relay Agent and then click OK.

7. Right-click the DHCP Relay Agent object, and then choose New Interface from the shortcut menu.

8. Select the network adapter connected to the network with the wayward DHCP clients, and then click OK. As shown in Figure 17-6, change the Hop-Count Threshold and Boot Threshold values, if necessary, and then click OK. (The hop count determines the maximum number of relay agents a DHCP request can pass through, and the boot threshold introduces a forwarding delay so that local DHCP servers can get first crack at servicing clients.)

Figure 17-6 Setting up a DHCP relay agent
9. Right-click the DHCP Relay object again, and choose Properties from the shortcut menu.

10. Type the address of a DHCP server you want to forward DHCP requests to, and then click Add.

**Backing Up and Restoring the DHCP Database**

Windows Server 2003 automatically backs up the DHCP database every 60 minutes to the `\%Systemroot%\System32\Dhcp\Backup` folder. Everything but registry and configuration settings (such as audit log settings) are saved during this backup.

To manually force a backup, use the following procedure:

1. Select the DHCP server you want to back up from the console tree.
2. Choose Backup from the Action menu.
3. Select the folder you want to store the backup files in, and click OK.

**Real World  Migrating and Consolidating with the Command Prompt**

Windows Server 2003 provides an enhanced version of the Netsh command that you can use to migrate DHCP scopes. This technique can also be used to consolidate DHCP servers, because existing scopes are preserved on the destination server. (Simply export the scopes from the source servers and then import them all into the destination server.)

To do so, type the following command, where `\\servername` is the source server, `c:\dhcpdatabase` is the filename you want to use (no file extension needed), and `10.0.0.0` is the scope you want to export (noting that to export multiple scopes, separate with spaces, and to export all scopes, type all):

```
netsh dhcp server \servername export c:\dhcpdatabase 10.0.0.0
```

To import the scope on the destination server, copy the file to a local hard drive and then type the following command (noting that you can import all the exported scopes or just select scopes):

```
netsh dhcp server \servername import c:\dhcpdatabase 10.0.0.0
```

It is important to note that both export and import of very large DHCP databases can take a substantial amount of time. During the process, the DHCP service is stopped and the server cannot service DHCP requests.
To restore the DHCP database from a backup, either to the same system or a different one, use the following procedure:

1. Select the DHCP server you want to back up from the console tree.
2. Choose Restore from the Action menu.
3. Select the folder where the backup files are stored, and click OK.
4. Click Yes when asked whether you want to stop and restart the DHCP service. No clients are able to obtain or renew leases during this time.

**Note** To change the folder in which the DHCP database is automatically backed up, right-click the DHCP server in the console tree, choose Properties from the shortcut menu, and then click the Advanced tab.

To back up DHCP’s configuration settings, open the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer subkey in the Registry Editor and save the desired keys to a registry file. To back up, restore, or move a Windows Server 2003 DHCP server, see Microsoft Knowledge Base article 325473.

### Using Ipconfig to Release, Renew, or Verify a Lease

On any Windows computer without a static IP address, you can run a command-line utility to release, renew, or verify the client’s address lease. At a command prompt, use one of the following commands:

- To release a client’s lease, type `ipconfig /release`.
- To renew a lease, type `ipconfig /renew`.
- To verify the client’s lease, type `ipconfig /all`.

The Ipconfig program is useful when troubleshooting problems because it displays every detail of the current TCP/IP configuration. You can find more troubleshooting information in Chapter 40.

### DHCP Command-Line Administration

The DHCP server in Windows Server 2003 provides full command-line administration capabilities with the rather unfriendly, but powerful, `netsh` command. To use these capabilities, do the following:

1. Open a command prompt window.
2. Type `netsh` at the command prompt. The prompt changes to `netsh>.
3. Type `dhcp`. The prompt changes to `netsh dhcp>`.
4. Type server followed by the server name or IP address to connect to the desired DHCP server—for example, server \srv1 or server 192.168.0.1.

5. Type list to view a list of the available commands. To obtain help with a particular command, type the command name followed by /?.

Using DNS Server

Modern TCP/IP networks use DNS for name resolution, and DNS is a requirement for Active Directory. Active Directory supports the DNS server included with Windows 2000 Server and Windows Server 2003, either standalone or integrated directly into Active Directory, and it also supports BIND version 8.2.2 or later.

If you’re using Active Directory–integrated DNS, you can skip the next section because DNS is automatically set up during the Active Directory Setup Wizard. (See Chapter 14.)

Installing DNS

To install DNS, use the Configure Your Server Wizard to set up Active Directory on the server and let Windows install DNS at the same time. (See Chapter 7.) This provides domain controller functionality and also lets DNS benefit from Active Directory integration. You can also use the Configure Your Server Wizard to set up DNS completely independent of Active Directory. If you want to set up DNS service the old-fashioned way (by installing the service), follow these steps:

1. Click Start, choose Control Panel, and then select Network Connections. Right-click the connection you want, and choose Properties from the shortcut menu.

2. Select the Internet Protocol (TCP/IP) entry, and then click Properties. To specify a static IP address, type the IP address, subnet mask, and default gateway that you’re using. Be sure the Use The Following DNS Server Addresses option is selected. In the Preferred DNS Sever box, type the computer’s assigned IP address.

   Note An alternative to using a static IP address is to use automatic addressing and make a client reservation with the DHCP server so that the DNS server is always guaranteed the same IP address. However, this can lead to problems if you forget to make the address reservation, and Windows Server 2003 strongly discourages you from using a dynamically assigned address, so proceed with caution.

3. Click Start, choose Control Panel, and then click System.

4. In the Computer Name tab, click Change. In the Identification Changes box, click More. (You aren’t able to perform this procedure on domain controllers.)
5. In the Primary DNS Suffix Of This Computer dialog box, type the DNS domain name and click OK. Reboot the server to implement the DNS suffix changes, if any. (Otherwise, no reboot is necessary.)

6. Open the Add/Remove Programs Control Panel tool, and then click Add/Remove Windows Components to launch the Windows Components Wizard.

7. Select Networking Services from the list of components, and then click Details.

8. Select the check box next to the Domain Name System (DNS) component, and then click OK.

9. Click Next to install the service. All the necessary files are copied to the hard disk.

**Using the Configure A DNS Server Wizard**

Windows Server 2003 provides a handy wizard to help you set up a DNS server. The following sections guide you through the wizard, while later sections delve into more detail about individual tasks that the wizard accomplishes.

**Setting Up a DNS Server**

Both large and small networks have similar DNS requirements, although many small networks will usually function well without Reverse Lookup zones. If your internal domain name is different from your public, Internet domain name (that is, internally you use “example.local” or “example.lan”, but externally you use “example.com”), you must configure an internal DNS server to support your internal network.

If your DNS domain name is the same on your local network as it is on the Internet (that is, example.com is your Active Directory domain name as well as your Internet domain name), you could, theoretically, have only external DNS records, but this is a bad practice because it exposes your internal network topology and names to the world. In this case, it is better to maintain an internal DNS server that supports your internal network, while the publicly visible DNS server or servers for your domain should only have records for publicly visible servers.

**Real World  The Need (or Lack Thereof) for Secondary DNS Servers**

Because of the pivotal role DNS plays in any TCP/IP-based network, it's vital for it to be reliable. Small networks can often make do with a single DNS server, but medium and large networks must have fault-tolerant DNS service.

One way of providing DNS redundancy is to set up secondary DNS servers using standard zone files to provide redundancy if the primary DNS server (of which there can be only one) doesn’t respond to client queries. Secondary DNS servers
Another approach is to add another Active Directory–integrated DNS server. Because Active Directory uses a full multiple-master model, all DNS servers using Active Directory–integrated zones can be primary servers—no secondary zones are required.

If you are going to use standard primary and secondary DNS servers, set up secondary DNS servers for both forward and reverse lookup zones. Fewer secondary servers are required for reverse lookup zones because of their infrequent use. They are usually placed outside the network and subnet that the reverse zone serves.

The Configure A DNS Server Wizard makes it easy to set up a DNS server. To use the wizard, do the following:

1. Launch DNS from the Administrative Tools folder on the Programs menu.
2. Select the DNS server you want to configure. (Choose the Connect To Server command from the Action menu if the server isn’t displayed in the console tree.)
3. Choose the Configure A DNS Server command from the Action menu.
4. Click Next in the first screen. (Optionally, click DNS Checklists to review background material about DNS and the DNS configuration process.)
5. Choose the Create Forward And Reverse Lookup Zones option in the Select Configuration Action page as shown in Figure 17-7, and then click Next.

![Figure 17-7](image-url) Choose what types of zones to create
6. Select Yes, Create A Forward Lookup Zone Now and then click Next.

7. In the Zone Type page shown in Figure 17-8, choose one of the following options, and then click Next to continue:

- **Primary zone**  Use this option if the DNS server is to be authoritative for the zone you want to create. Only authoritative servers can update the DNS database.

- **Secondary zone**  Use this zone if the DNS server is hosted on UNIX servers. Also, use it if this server is to have read-only privileges in the zone with all data obtained from the primary DNS server.

- **Stub zone**  Use this type of zone to create a pseudo-zone that allows the server to directly query DNS servers from a specific zone without having to locate the zone’s DNS servers by querying the root servers or Internet DNS servers.

  **Note**  For primary zones, select the Store The Zone In Active Directory check box to take advantage of Active Directory–integrated zone storage. This option is available only on domain controllers.

*Figure 17-8*  Choosing a zone type
8. If you’re creating an Active Directory–integrated zone, specify with which servers the zone information should be replicated and then click Next. (You’ll probably want to choose To All DNS Servers In The Active Directory Domain to reduce replication traffic.)

9. If you chose to create a secondary zone, type a name for the zone and then click Next. Then type the IP addresses of the master servers from which you want to copy the zone data. Click Add after typing or locating each one. Click Up and Down to arrange the IP addresses in the order you want to contact them. Click Next when you’re done.

10. If you’re creating a standard zone, type a filename for the zone file on the Zone File page. To use an existing file, copy the file to the %SystemRoot%\System32\Dns folder, select the Use This Existing File option, type the filename in the box provided, and then click Next.

11. On the Dynamic Update page (available only for primary zones), choose how you want to configure dynamic updates and then click Next. The options are:
   - **Allow Only Secure Dynamic Updates** This is the default for Active Directory–integrated zones (and is available only for Active Directory–integrated zones), and it provides the best security. However, clients running earlier versions of Windows might end up with orphaned DNS records under certain circumstances. (See the “DHCP, Stale Records, and Secure Dynamic Updates” sidebar earlier in this chapter.)
   - **Allow Both Secure and Unsecure Dynamic Updates** This is the recommended setting for standard zones.
   - **Do Not Allow Dynamic Updates** This setting disables dynamic updates entirely.

12. To create a reverse lookup zone, click Next; otherwise, choose the No I Don’t Want To option first and then click Next.

13. If you chose to create a reverse lookup zone, choose the type of zone to create and then click Next.

14. If you’re creating an Active Directory–integrated zone, specify with which servers the zone information should be replicated and then click Next.

15. Type the address of the network in the Network ID box and then click Next. The wizard automatically creates the reverse lookup zone name for you from this information, as shown in Figure 17-9.
16. If you’re creating a standard zone, click Next to approve the filename provided.

17. On the Dynamic Update page, choose how you want to configure dynamic updates and then click Next.

18. To set up the server to forward unresolved DNS queries to another DNS server (which might either resolve the query from its cache or contact an external DNS server to resolve the query), type the IP address of the forwarding server and then click Next. Alternatively, choose the No, It Should Not Forward Queries option and then click Next.

19. Review the summary of the DNS server configuration, and then click Finish to complete the initial configuration of the DNS server.

Note Use the Nslookup command from a command prompt to test the functionality of the DNS server. However, the command’s functionality is limited without a reverse lookup zone. (You aren’t be able to perform reverse lookups to obtain DNS names from IP addresses.) Consult online Help for command reference information.

Real World DNS Poisoning Attacks
The standard setup for most DNS servers that supported only internal network clients was to set up your DNS server as a primary zone, and then configure it to forward all other requests to your ISP’s designated DNS servers. This resulted in fast and private support for internal name resolution, while providing the fastest resolution of names outside your private network and reducing overall traffic for your ISP and the
Internet as a whole. Unfortunately, this exposes your network to DNS poisoning attacks such as the widespread cache corruption attack that affects all versions of BIND before version 9. If some malicious program manages to subvert the DNS servers maintained by your ISP because your ISP hasn’t gotten around to updating them, your DNS server would pass that problem on to your internal clients.

The problem is especially a concern if your ISP is somewhat slow to apply patches to its DNS servers, as seems to be the case for many ISPs, both large and small. BIND is the most common DNS server software used by ISPs, and several vulnerabilities have been identified against BIND, especially versions before BIND 9. Patches to correct these vulnerabilities are available, but if your ISP is slow to apply the patch, you could be exposed.

If you don’t specify a server to forward to, your DNS server will use root hints to directly resolve the address. This might be somewhat slower, and it certainly increases the overall traffic on the Internet, but if the root servers are poisoned then we’re all in trouble. If you trust your ISP to maintain its servers adequately, continue to forward to their servers. Personally, we’ve stopped doing so.

## Creating Zones

Zones allow you to store portions of the DNS namespace so that a single DNS server can serve a portion of the namespace.

### Planning

When setting up the domains, start with the top-level domain. Then create subdomains and delegate control of the domains to other DNS servers as necessary.

The two types of zones concerned are forward lookup zones and reverse lookup zones. Forward lookup zones are the types of zones normally associated with DNS servers; they return an IP address when given a DNS name. Reverse lookups are used less often, but they are still important. They provide the ability to resolve an IP address into a DNS name, something that Internet Information Services (IIS) can use for its log files. (Troubleshooting tools such as Nslookup rely on reverse lookup zones as well.)

When you first set up a DNS server, you’ll probably want to use the Configure A DNS Server Wizard (discussed in the previous section), which guides you through creating the first forward lookup zone. However, if you didn’t use the wizard to set up the zones or you need to create additional zones, use the following procedure:

1. Launch DNS from the Administrative Tools folder on the Programs menu.
2. Select the DNS server you want to configure. (Choose the Connect To Server command from the Action menu if the server isn’t displayed in the console tree.)
Note If you select the Forward Lookup Zone container in the console before choosing New Zone from the Action menu, the New Zone Wizard assumes that you intend to create a forward lookup zone and skips several steps.

3. Choose New Zone from the Action menu to start the New Zone Wizard. Click Next to start using the wizard. (See the “Setting Up a DNS Server” section for help with this.)

Creating Subdomains and Delegating Authority

In most large network environments, you need to create subdomains and delegate their management to other DNS zones hosted by other DNS servers. Doing so eliminates the undesirable situation of having a large namespace hosted in a single zone by a single server. Thus, you might have a zone containing the root domain example.local as well as the subdomain marketing.example.local; however, you might have the subdomain eng.example.local and its subdomains delegated to a separate zone managed by another DNS server, as shown in Figure 17-10.

![Figure 17-10] A domain tree with zones identified

Important Be sure you have a host record created for the DNS server in the forward lookup zone and a pointer record for the DNS server in the reverse lookup zone. DNS might not automatically create these (especially the pointer record), so double-check them—otherwise, the server might not work.

Note Zones must have a contiguous namespace, so it isn’t possible to combine subdomains from different branches of the namespace and place them in a single zone. Create separate zones for each noncontiguous part of the domain.
To create a new subdomain in an existing zone and then delegate authority over the domain to another DNS server, perform the following steps:

1. Select the domain in which you want to create a new subdomain, and then choose New Domain from the Action menu.

2. Type the name of the subdomain in the dialog box that appears, and then click OK. This name must not be fully qualified. For example, if you were creating the subdomain eng.example.com under the domain example.com, type only eng in this dialog box.

   **Note**  Subdomains don't have to be delegated to a different DNS server. Subdomains can even be created in new zone files and still be managed by the same server. This is useful if you want to host the domains on the same computer yet manage them differently.

3. To delegate authority over the subdomain, select the parent domain of the subdomain, choose New Delegation from the Action menu, and then click Next to start the New Delegation Wizard.

4. Type the name for the subdomain you want to delegate, as shown in Figure 17-11. Check that the fully qualified name of the subdomain displayed is correct and then click Next.

![New Delegation Wizard](image)

   **Figure 17-11**  Delegating a subdomain

5. Click Add to specify the servers to which you want to delegate the subdomain.
6. Type the name of the server to which you want to delegate authority and then click Resolve, or click Browse to locate its resource record in the DNS server’s zone files. Alternatively, type the IP address or addresses for the server, clicking Add after typing each one. Click OK when you’re done.

7. Add any other DNS servers that will host the delegated subdomain. Click Next to continue.

**Note** When you delegate control over a subdomain to multiple DNS servers, Windows automatically monitors the round-trip times to the servers and selects the closest (fastest) one.

8. Review the summary window, and click Finish to complete the delegation process.

**Adding Resource Records**

After creating zones and subdomains, add resource records for the domain server and any other servers with static IP addresses or IP reservations (DHCP servers, WINS servers, routers, and so on). The steps that follow are for adding new host records, but the process to add new pointer records, Alias (CNAME) records, mail exchangers, or other resource records is similar. (Note that the DNS server doesn’t work properly without a host record and a pointer record, which might not be created automatically for you.)

1. Select the zone and domain or subdomain to which the host belongs, and then choose New Host from the Action menu. Alternatively, choose New Alias, New Mail Exchanger, or another type of record from the Action menu. Table 17-1 lists the records supported by Windows Server 2003 DNS server.

**More Info** For more information about each of these record types and what they mean, refer to the related RFC or see the *Microsoft Windows Server 2003 Resource Kit* (2005), available from Microsoft Press.

2. In the Name box, type the host name (and only the host name—the name must not contain any periods), or leave the Name box blank to use the name of the parent domain. Type the host’s IP address.

3. Select the Create Associated Pointer (PTR) Record to create a resource record for the host in the reverse lookup zone.

4. If you want to allow any authenticated user to update the resource record you’re creating, select the Allow Any Authenticated User To Update DNS Records With The Same Owner Name check box.

5. Click Add Host, and then fill out the fields for any additional host records you want to create, or click Done.
Real World  Changing DNS Records

When you make a change to the DNS records, make sure you choose the Update Server Data Files command from the Action menu after making the changes. This option increments the serial number, letting other DNS servers know that you made a change and that they need to update their information.

If you’re using conventional DNS zones, add or change DNS records only from the primary DNS server for a zone. If you’re using Active Directory–integrated DNS, you can make the changes to any Active Directory–based DNS and it propagates correctly to the other Active Directory DNS servers and notifies secondary servers that there are updated records.

Table 17-1  Supported DNS record types

<table>
<thead>
<tr>
<th>Record Type</th>
<th>Common Name</th>
<th>Function</th>
<th>RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Address record</td>
<td>Maps a fully qualified domain name (FQDN) to a 32-bit IPv4 address</td>
<td>128</td>
</tr>
<tr>
<td>AAAA</td>
<td>IPv6 Host</td>
<td>Maps an FQDN to a 128-bit IPv6 address</td>
<td>1886</td>
</tr>
<tr>
<td>AFSDB</td>
<td>Andrews file system (AFS) or distributed computing environment (DCE) record</td>
<td>Maps a DNS domain name to a server subtype that is either an AFS version 3 volume or an authenticated name server (NS) using DCE or network computing architecture (NCA)</td>
<td>1183</td>
</tr>
<tr>
<td>ATMA</td>
<td>Asynchronous Transfer Mode (ATM) address</td>
<td>Maps a host name to an ATM address</td>
<td>“ATM Name System Specification Version 1.0”</td>
</tr>
<tr>
<td>CNAME</td>
<td>Canonical name or alias record</td>
<td>Maps a virtual domain name (alias) to a real domain name</td>
<td>1035</td>
</tr>
<tr>
<td>HINFO</td>
<td>Host information record</td>
<td>Specifies the CPU and operating system type for the host</td>
<td>1700</td>
</tr>
<tr>
<td>ISDN</td>
<td>ISDN information record</td>
<td>Maps an FQDN to an ISDN telephone number</td>
<td>1183</td>
</tr>
<tr>
<td>KEY</td>
<td>Public key resource record</td>
<td>Contains a public key for a DNS zone</td>
<td>2535</td>
</tr>
</tbody>
</table>
### Table 17-1  Supported DNS record types

<table>
<thead>
<tr>
<th>Record Type</th>
<th>Common Name</th>
<th>Function</th>
<th>RFC</th>
</tr>
</thead>
<tbody>
<tr>
<td>MB</td>
<td>Mailbox name record</td>
<td>Maps a domain mail server name to the actual host name of the mail server</td>
<td>1035</td>
</tr>
<tr>
<td>MG</td>
<td>Mail group record</td>
<td>Maps a domain mailing group to the actual mailbox (MB) resource records of its members</td>
<td>1035</td>
</tr>
<tr>
<td>MINFO</td>
<td>Mailbox information record</td>
<td>Specifies a mailbox for the person who maintains the mailbox or list, and can also specify a mailbox for related errors</td>
<td>1035</td>
</tr>
<tr>
<td>MR</td>
<td>Mailbox renamed record</td>
<td>Maps an old mailbox name to a new mailbox name for forwarding purposes</td>
<td>1035</td>
</tr>
<tr>
<td>MX</td>
<td>Mail exchange record</td>
<td>Provides routing information to reach a given mailbox</td>
<td>974</td>
</tr>
<tr>
<td>NS</td>
<td>Name server record</td>
<td>Specifies that the name server listed has a zone starting with the owner name</td>
<td>1035</td>
</tr>
<tr>
<td>NXT</td>
<td>Next record</td>
<td>Specifies the nonexistence of the specified name</td>
<td>2035</td>
</tr>
<tr>
<td>OPT</td>
<td>Option resource record</td>
<td>Specifies optional data with a DNS request or reply</td>
<td>2671</td>
</tr>
<tr>
<td>PTR</td>
<td>Pointer resource record</td>
<td>Points to another DNS resource record—most often used in reverse lookup to point to the A record</td>
<td>1035</td>
</tr>
<tr>
<td>RP</td>
<td>Responsible person information record</td>
<td>Provides information about the person responsible for a server</td>
<td>1183</td>
</tr>
<tr>
<td>RT</td>
<td>Route-through record</td>
<td>Provides routing information for hosts lacking a direct WAN address</td>
<td>1183</td>
</tr>
<tr>
<td>SIG</td>
<td>Signature resource record</td>
<td>Digitally signs a host name</td>
<td>2535</td>
</tr>
<tr>
<td>SOA</td>
<td>Start of authority</td>
<td>Specifies the beginning of a zone, and indicates the authoritative server</td>
<td>1034</td>
</tr>
</tbody>
</table>
Configuring Zone Transfers

Because the DNS service is so important to a modern TCP/IP-based network, and because it’s essential to the operation of Active Directory, always configure multiple DNS servers in each zone to provide fault tolerance.

Windows Server 2003 supports several ways of achieving zone transfers between DNS servers managing a zone. If the DNS servers are using Active Directory to store their zone data, Active Directory handles the zone replication, allowing for a full multimaster model in which all servers are peers and any can make changes to the DNS database. Additionally, zone transfers are incremental so that only changed records are synchronized.

Windows Server 2003 also supports RFC 1995–compliant incremental zone transfers when using standard zone files. This incremental zone transfer method permits a secondary DNS server to pull only the zone changes that it needs to synchronize its copy of the zone data with the primary server’s. If the serial number of the primary DNS server’s zone file matches that of the secondary DNS server’s serial number, no changes were made, so no zone transfer need take place.

Incremental zone transfers occur only if both servers support this feature. When performing zone transfers with Windows NT 4 DNS servers or other DNS servers that don’t support this feature, a full zone transfer occurs. In a full zone transfer, the entire contents of the zone file are pulled from the primary DNS server by the secondary server.
Real World  Controlling Zone Transfers

The default configuration for Active Directory-integrated DNS is to not allow zone transfers. It’s a potential security issue to allow uncontrolled zone transfers, but you do want to allow them to your secondary servers. If you use secondary DNS servers in a zone, you should first create a Name Server resource record for the secondary server, as described previously under “Adding Resource Records.” Then configure the properties of the zone to perform zone transfers only to servers listed in the Name Servers tab of the zone properties, as shown in Figure 17-12. This will ensure that a rogue DNS server can’t download records from your server.

Interoperating with Other DNS Servers

Windows Server 2003 and Windows 2000 DNS servers perform fast zone transfers with data compression and multiple resource records sent in each message when transferring zones to other Windows DNS servers. This zone transfer method works with all Windows DNS servers, and BIND DNS servers version 4.9.4 or later. Note that Windows 2000 DNS servers must run Service Pack 3 or newer if receiving zone information from BIND 9.x servers.

Important  Although you can use Windows Server 2003 DNS servers and Active Directory in conjunction with Windows NT 4 Service Pack 4 DNS servers and BIND servers later than version 4.9.4, there are serious compatibility and security issues for all older versions of BIND. You should upgrade BIND to the latest version for maximum security, and in all cases you should be using version 8.4.4 or later. For the current state of BIND versions and vulnerabilities, see http://www.isc.org/index.pl?/sw/bind/bind-security.php.
Enabling WINS Resolution

WINS allows NetBIOS names to be resolved into IP addresses. This capability is important for networks that support large numbers of pre–Windows 2000 Microsoft clients. DNS can work with WINS to search the entire combined DNS and NetBIOS namespace, if necessary, when a client attempts to resolve a host name.

In Windows NT 4, enabling WINS resolution within DNS was essential to successfully resolving hosts that might have recently changed IP addresses—the dynamic WINS database provided an up-to-date IP address when the static DNS zone file couldn’t. However, with Windows Server 2003, Windows XP, and Windows 2000, dynamic updates to the DNS server have nearly eliminated the need to use WINS servers to keep the namespace up to date, and WINS is gradually being phased out. Not a moment too soon, in our opinion.

To enable WINS resolution in a zone, follow these steps:

1. Select the zone in which you want to enable WINS resolution, and then choose Properties from the Action menu.
2. Click the WINS tab, and select the Use WINS Forward Lookup check box.
3. If you’re not using Microsoft DNS servers as secondary servers, select the Do Not Replicate This Record check box to prevent compatibility problems. (Only Windows DNS servers support WINS records.)
4. Type the IP address of each WINS server you want to query, clicking Add after typing each one.

You find more about setting up WINS in the “Setting Up a WINS Server” section later in this chapter.

Setting Up a Forwarder

No name server is able to answer the queries of all clients; sometimes clients request a DNS name that isn’t in a zone managed by the DNS server, let’s say example.microsoft.com. The DNS server goes to the Internet to the top level of the DNS domain tree. The top-level DNS servers then provide the address of the DNS server for the first level (.com). This server in turn provides the address of the microsoft.com DNS server, which then provides the address of the example.microsoft.com DNS server.

This process is called recursion, and it takes time and a number of trips out to the Internet by the DNS server. In a network with multiple DNS servers and domains, it can be advantageous to have DNS servers forward their unresolved queries to another DNS server. This server then either replies with the desired record from its own DNS zone or
hunts down the unresolved query and reports back to the DNS server that forwarded the request. This can reduce WAN link usage in two ways:

- If the server is authoritative for the zone containing the requested DNS record, the DNS server can reply directly without having to hunt for the appropriate DNS server.

- If the server isn’t hosting the zone with the requested record, it still might be able to answer the query from its cache of recent DNS queries.

Security Alert  See the “DNS Poisoning Attacks” sidebar earlier in this chapter before deciding whether to enable forwarders. There are serious security implications you should understand before taking this step.

To configure the DNS server to forward unresolved queries to another DNS server, follow these steps:

1. In the console tree, select the DNS server on which you want to enable forwarding, and then choose Properties from the Action menu and then click the Forwarders tab.

2. To forward all unresolved queries to another DNS server, select All Other DNS Domains in the DNS domain box, and then type the IP addresses of the DNS server or servers to which you want to forward unresolved queries, clicking Add after typing each one.

3. To change the default timeout before DNS will try the next forwarder in the list, change the Number Of Seconds Before Forward Queries Time Out from the default of 5 seconds.

4. To disable recursion for a particular domain, select the domain and then select the Do Not Use Recursion For This Domain check box. If the DNS server that is the target of the forwarded queries doesn’t respond and the Do Not Use Recursion For This Domain check box is selected, the DNS server fails the query, and the client fails over to a secondary DNS server if it’s configured to do so. A DNS server that’s configured to use forwarders and not perform recursion is called a slave server.

To enable forwarding queries for a specific domain to a specific DNS server (conditional forwarding) follow these steps:

1. In the console tree, select the DNS server on which you want to enable forwarding, choose Properties from the Action menu, and then click the Forwarders tab.

2. Click New in the DNS Domain, type the DNS domain for which to use conditional forwarding, and click OK.
3. With the domain highlighted, type the IP addresses of the DNS server or servers to which you want to forward unresolved queries, clicking Add after typing each one.
4. Click OK to close the dialog box and implement the changes.

**Updating Root Hints**

Root hints tell a DNS server where to look to find the DNS servers authoritative for the top level of the domain structure. Root hints for the Internet’s root servers are automatically installed in the Cache.dns file located in the %SystemRoot%\System32\Dns folder.

If the DNS server needs only to resolve names in the private network, you must provide the locations of the top-level DNS servers for the network, either through the DNS console (as described next) or by manually editing the Cache.dns file. Alternatively, you can import root hints from another server.

**Note** If the server is the root of the network’s namespace and doesn’t resolve Internet host names, you can delete the Cache.dns file.

To update root hints on the server, use the following procedure:

1. In the console tree, select the DNS server on which you want to update the root hints, and then choose Properties from the Action menu.
2. Click the Root Hints tab and then click Add to manually add a name server record for a root DNS server. Alternatively, click Copy From Server, type the IP address for the DNS server from which you want to copy root hints, and then click OK.

**Setting Up a Caching-Only DNS Server**

Caching-only servers are DNS servers that don’t host any zones and aren’t authoritative for any domains—they simply cache the queries that they perform on behalf of the clients that use the server. Caching-only servers are useful for sites that use a slow WAN link to other DNS servers. By simply caching queries instead of holding its own zone files, a caching-only server reduces network traffic because it never performs any zone transfers.

To set up a caching-only server, follow these steps:

1. Install the DNS service, using the Add/Remove Windows Components section of the Add/Remove Programs tool.
2. Configure the caching server with a static IP address.
3. Launch DNS from the Administrative Tools folder on the Programs menu, select The Following Computer in the Select Target Computer dialog box, type the name of the DNS server from which you want to cache, and click OK. (If this dialog box doesn’t appear, choose Connect To Computer from the Action menu in the DNS window.)
The DNS server is added to the DNS console on the caching server. The caching server performs recursive queries on behalf of its clients and over time accumulates resource records for answering future queries. You can clear the cache on a caching server by right-clicking the server’s name in the DNS console and selecting Clear Cache from the shortcut menu.

### Setting Up a WINS Server

WINS is an essential part of any large network with earlier Windows clients and network applications. It provides the equivalent function of a DNS server—except for the NetBIOS namespace. WINS servers resolve NetBIOS names into IP addresses by using the WINS dynamic database to call up the appropriate name records. If all your systems are Windows 2000 or later, it is possible for them to function without WINS.

### Determining Whether You Need WINS

If you’re asking yourself whether you need WINS at this point, the answer is probably yes. Most large networks need WINS to provide NetBIOS name resolution for their earlier Windows clients. There are two instances in which you don’t need WINS servers (though you might still choose to use one):

- All clients on the network support name resolution through dynamic DNS. Windows XP, Windows 2000, and Windows Server 2003 are the only Microsoft operating systems that can rely exclusively on DNS for name resolution. If you have any down-level clients at all, you need WINS. If you have a mixed environment with other clients such as UNIX clients, make sure they’re all configured to properly use DNS.

- The network is small (fewer than 50 clients) and not subnetted. If the entire network consists of a single network segment, clients that require NetBIOS name resolution can effectively resolve NetBIOS names by broadcast—a technique that doesn’t work across routers or on large networks where the NetBIOS broadcasts would generate too much network traffic.

The following WINS clients are supported by WINS in Windows Server 2003:

- Windows Server 2003
- Windows XP
- Windows 2000
- Microsoft Windows NT 3.5 or later
- Windows Me
Non-WINS clients aren't resolvable by WINS unless static entries are added for them—don't do it. This practice is strongly discouraged because static entries are extremely difficult to eliminate from the WINS database after replication takes place. Instead, clients should be configured to use DNS to resolve names that aren't in the WINS database.

**Configuring the Server to Prepare for WINS**

After you determine that you need WINS on your network, it's time to configure the server. The most common cause of WINS problems is improper TCP/IP configuration on the server. Follow these steps to properly configure the TCP/IP settings for the WINS server before you install the service:

1. Right-click the Local Area Connection icon in the Network Connections folder, and choose Properties from the shortcut menu.
2. Select the Internet Protocol (TCP/IP) component, and click Properties.
3. Configure the server to use a static IP address, or make sure that an address reservation for the server is configured on the DHCP server.
4. Click Advanced, and then click WINS.
5. Select any WINS servers listed on the tab, and click Remove. Failure to do this can cause the WINS server to register its own address with another WINS server instead of with itself, which you don't want.
6. Click Add, and type the IP address of your own server. Do not use the loopback address, 127.0.0.1; use the real address. Then click OK.

**Installing WINS**

After the TCP/IP settings are correct, you're ready to install the WINS component. Use the Windows Component Wizard, accessible either from the Configure Your Server tool or from Add/Remove Programs in Control Panel. If you installed WINS during Windows Setup, you can skip this section. Otherwise, use these steps to install WINS:

1. Open the Add/Remove Programs Control Panel tool, and click the Add/Remove Windows Components icon in the frame on the left (the Places bar) to launch the Windows Component Wizard.
2. Click Next, select Networking Services from the list of components, and click Details.

3. Select the Windows Internet Name Service (WINS) component check box, click OK, and then click Next.

**Important** Don’t install WINS on a multihomed server. You can physically do it, but it often causes dreadful replication problems, especially if the server is on two different subnets.

### Adding Replication Partners

WINS servers are easy to set up and require little management, except for replication partners. WINS replication is an important and somewhat delicate issue that you must examine closely before setting up. Deploy as few WINS servers as possible to minimize management migraines. For example, the entire Microsoft Corporation used only 12 WINS servers worldwide during the height of NetBIOS. Just about every enterprise can get by with a handful of WINS servers at most. A good rule of thumb is one WINS server for every 10,000 users, plus one WINS server for redundancy.

**Planning** Set up replication between WINS servers in a hub (star) pattern, with a single-master WINS server in the center and all other WINS servers replicating only with this server, using the push/pull method. Using a double hub with two master servers in the center can provide additional redundancy, but the replication problems that can arise generally outweigh the added reliability. For additional planning details, see the *Windows Server 2003 Resource Kit* (Microsoft Press, 2005).

To set up a replication partner and configure its settings after planning your WINS deployment, follow these steps:

1. Launch WINS from the Administrative Tools folder, and in the console tree expand the WINS server that you want to set up for replication.

2. Select the Replication Partners folder, and then choose New Replication Partner from the Action menu.

3. Type the IP address for the WINS server you want to enable replication with, and click OK.

4. To modify the replication parameters for the new replication partner, if necessary, double-click the server in the Replication Partners folder, and then click the Advanced tab.
5. To change the way you replicate with the server, choose an option from the Replication Partner Type drop-down list (Figure 17-13).

![Figure 17-13 The Advanced tab of the Properties dialog box](image)

6. To configure a permanent connection for pull or push replication, select the Use Persistent Connection For Replication check box in the Pull Replication section, the Push Replication section, or both.

7. In the Start Time fields, type the time you want pull replication to begin in hours, minutes, and seconds.

8. In the Replication Interval fields, type the frequency—days, hours, and minutes—with which you want to replicate with the replication partner.

9. Use the Number Of Changes In Version ID Before Replication box to type the number of changes to the local copy of the WINS database that you will allow before the server pushes changes to the replication partner.

**Note** Use push/pull replication on the entire WINS namespace to make troubleshooting replication problems easier. In addition, primary and backup WINS servers must use push/pull replication.
Miscellaneous WINS Functions

The WINS snap-in lets you manage all the functionality of WINS on multiple servers from the same application. The following are some functions you can perform with the WINS snap-in:

■ To view the status of your WINS servers, click Server Status in the console tree. The status of your servers appears in the pane on the right.

■ To view records in the WINS database, right-click the Active Registrations folder in the console tree under the desired server. Choose either Find By Name to search for a particular name or Find By Owner from the Action menu to display the Find By Owner dialog box, which shows all the records in the WINS database. When viewing records, you can use the Record Types tab of the Find By Owner dialog box to filter the type of records displayed.

■ To add a static entry to the database, right-click the Active Registrations folder and choose New Static Mapping from the shortcut menu.

---

**Important** Add static entries only for computers that do not support WINS and only if absolutely necessary. Static entries are notoriously difficult to eliminate after replication and can be deleted only by the owner.

■ To initiate scavenging, which purges the WINS database and does general cleanup on it, select the WINS server you want to scavenge and choose Scavenge Database from the Action menu. When initiating scavenging, don’t attempt to alter the scavenging parameters for WINS. These parameters have been extensively tested and optimized by Microsoft. Any change you make will be for the worse.

■ To modify the properties for the WINS server, select the server you want to work on, and then choose Properties from the Actions menu. This displays the Properties dialog box shown in Figure 17-14, which you can use to modify the path to the backup copy of the WINS database, change the length of name leases, and modify logging and other options.

---

**More Info** If you’re fortunate enough to have outgrown WINS on your network, it’s time to decommission the WINS servers. For information about doing so, consult the Windows Server 2003 Help system or the *Windows Server 2003 Resource Kit* (Microsoft Press, 2005) for specific issues about working with a NetBIOS-less network.
Compacting the WINS Database

You should compact the WINS database whenever the database approaches 30 MB in size to maximize performance and stability.

To do so, follow these steps:

1. Open a command prompt window.
2. Type the following commands:

   ```
   cd %systemroot%\system32\wins
   net stop wins
   jetpack wins.mdb tmp.mdb
   net start wins
   ```

More Info  For more information about the Jetpack.exe command, see Microsoft Knowledge Base article 145881.

Summary

DHCP and DNS servers are essential to any TCP/IP-based network with more than a few clients, as are WINS servers for routed TCP/IP networks with legacy Windows clients. Windows Server 2003 provides powerful, easy-to-use, and reliable DHCP, DNS, and WINS servers.

The next chapter covers the configuration of hard disks for maximum security and efficiency.
Chapter 18

Implementing Disk Management

Understanding Disk Terminology ............................................... 539
Overview of Disk Management .................................................... 542
Disk Management Tasks .............................................................. 546
NTFS ................................................................. 571
Summary ................................................................. 574

Under normal circumstances, this would be a combined chapter about disk management and storage. However, with Microsoft Windows Server 2003, the subject of computer and network storage has become more complex for the administrator while at the same time becoming simpler for the user. Windows Server 2003 provides for both local and remote storage and for storage on removable media—all in a way that is completely transparent to the user. After all, the user doesn’t care whether a program or file is stored on a local or remote disk, on tape, or somewhere on the intranet, as long as it’s available when needed.

This chapter covers the more traditional disk management tasks that are possible under Windows Server 2003, and Chapter 20 takes a look at some of the less traditional methods of storage that are now possible.

Understanding Disk Terminology

Before going into the details of managing disks and storage, let’s review some definitions:

- **Physical drive**  The actual hard disk itself, including the case, electronics, platters, and all that stuff. This is not terribly important to the disk administrator.

- **Partition**  A portion of the hard disk. In many cases, this is the entire hard disk space, but it needn’t be.

- **Allocation unit**  The smallest unit of managed disk space on a hard disk or logical volume. It’s also called a *cluster*. 
- **Primary partition**  A portion of the hard disk that’s been marked as a potentially bootable logical drive by an operating system. MS-DOS can support only a single primary partition, but Windows Server 2003 can support multiple ones. There can be only four primary partitions on any hard disk.

- **Extended partition**  A nonbootable portion of the hard disk that can be subdivided into logical drives. There can be only a single extended partition per hard disk, but it can be divided into multiple logical drives.

- **Extended volume**  Similar to, and sometimes synonymous with, a spanned volume. This is any dynamic volume that has been extended to make it larger than its original size. When it uses portions of more than one physical disk, it is more properly referred to as a spanned volume.

- **Logical drive**  A section or partition of a hard disk that acts as a single unit. An extended partition can be divided, for example, into multiple logical drives.

- **Logical volume**  Another name for a logical drive.

- **Basic disk**  A traditional disk drive that is divided into one or more partitions, with a logical drive in the primary partition, if present, and one or more logical drives in any extended partitions. Basic disks do not support the more advanced functions of Disk Management, but they can be converted to dynamic disks in many cases.

- **Dynamic disk**  A managed hard disk that can be used to create various volumes.

- **Volume**  A unit of disk space composed of one or more sections of one or more dynamic disks.

- **Simple volume**  The dynamic equivalent of a partition. A portion of a single dynamic disk, it can be assigned either a single drive letter or no drive letter and can be attached (mounted) on zero or more mount points.

- **RAID (redundant array of independent [formerly “inexpensive”] disks)**  The use of multiple hard disks in an array to provide for larger volume size, fault tolerance, and increased performance. RAID comes in different levels, such as RAID-0, RAID-1, RAID-5, and so forth. Higher numbers don’t necessarily indicate greater performance or fault tolerance, just different methods of doing the job.

- **Spanned volume**  A collection of portions of hard disks combined into a single addressable unit. A spanned volume is formatted like a single drive and can have a drive letter assigned to it, but it will span multiple physical drives. A spanned volume—occasionally referred to as an extended volume—provides no fault tolerance and increases your exposure to failure, but it permits you to make more efficient use of the available hard disk space.
■ Striped volume   Like a spanned volume, a striped volume combines multiple hard disk portions into a single entity. A striped volume uses special formatting to write to each of the portions equally in a stripe to increase performance. A striped volume provides no fault tolerance and actually increases your exposure to failure, but it is faster than either a spanned volume or a single drive. A stripe set is often referred to as RAID-0, although this is a misnomer because plain striping includes no redundancy.

■ Mirror volume   A pair of dynamic volumes that contain identical data and appear to the world as a single entity. Disk mirroring can use two drives on the same hard disk controller or use separate controllers, in which case it is sometimes referred to as duplexing. In case of failure on the part of either drive, the other hard disk can be split off so that it continues to provide complete access to the data stored on the drive, providing a high degree of fault tolerance. This technique is called RAID-1.

■ RAID-5 volume   Like a striped volume, this combines portions of multiple hard disks into a single entity with data written across all portions equally. However, it also writes parity information for each stripe onto a different portion, providing the ability to recover in the case of a single drive failure. A RAID-5 volume provides excellent throughput for read operations, but it is substantially slower than all other available options for write operations.

■ SLED (single large expensive disk)   Now rarely used, this strategy is the opposite of the RAID strategy. Rather than using several inexpensive hard disks and providing fault tolerance through redundancy, you buy the best hard disk you can and bet your entire network on it. If this doesn’t sound like a good idea to you, you’re right. It’s not.

■ JBOD   Just a bunch of disks. The hardware equivalent of a spanned volume, this has all the failings of any spanning scheme. The failure of any one disk will result in catastrophic data failure.

---

Under the Hood   Disk Technologies for the Server

The first time we wrote a chapter about disk management, there were basically three possible technologies available: Modified Field Modification (MFM), Pulse Frequency Modulation (PFM), and Small Computer System (or Serial) Interface (SCSI). Unless you were a total geek (and had oodles of money), your systems used either MFM or PFM, and RAID wasn’t even an option. Over time, SCSI became the only real choice for the vast majority of servers and even became mainstream on high-end workstations. Servers at the high end might use fiber, but SCSI had the vast majority of the server disk market.

Integrated Device Electronics (IDE), later called Advanced Technology Attachment (ATA), became the standard on the personal computer. However, IDE never made a
serious inroad into the server market because, while fast for single tasks, it lacked the inherent multitasking support and bus mastering that a server disk interface technology required, and there were no real hardware RAID solutions that supported it.

Recently, the introduction of Serial ATA (SATA) technology has made serious inroads into the lower end of the server marketplace. With SATA RAID controllers built into many motherboards, and standalone SATA RAID boards that support 8 or more SATA drives and have substantial battery backed RAM cache onboard, many low to mid-range servers are finding SATA RAID solutions to provide a cost effective alternative to SCSI. While most SATA RAID controllers lack the ability to hot-swap a failed drive, and generally don’t have the ultimate performance potential of SCSI, they are still quite attractive alternatives where cost is a primary factor.

On the horizon are newer and even faster technologies for interfacing with disks. We think that Serially Attached SCSI (SAS) is the most interesting addition to the server market, but it’s still early yet. With the main bottleneck for servers continuing to be I/O in general, and especially disk I/O, there will continue to be pressure to find new and faster methods to access disk-based storage. Especially with 64-bit servers becoming mainstream and the enormous datasets being supported on 64-bit Windows Server 2003, the need for fast and easily expandable disk storage will increase dramatically.

Overview of Disk Management

Hard disk storage has been the usual long-term storage method for modern computers, from the mainframe to the desktop, and that’s not likely to change, even considering the richer storage options that have been added to Windows Server 2003. This section looks at each of the new facilities.

RAID

RAID (redundant array of independent disks) is a term used to describe a technique that has gone from an esoteric high-end solution to a normal procedure on most servers. Seven or eight years ago, RAID was mostly unheard of, although the original paper defining RAID was written in 1988. In the past, most server systems relied on expensive, higher-quality hard disks—backed up frequently. Backups are still crucial, but now you can use one form or another of RAID to provide substantial protection from hard disk failure. Moreover, this protection costs much less than those big server drives did.
RAID can be implemented at a software or hardware level. When it is implemented at the hardware level, the hardware vendor provides an interface to administer the arrays and the drivers to support the various operating systems it might need to work with. Although there are performance and often redundancy advantages to using a hardware RAID solution, it's generally substantially more expensive than the software RAID built into Windows Server 2003.

Windows Server 2003 includes an excellent and flexible implementation of RAID levels 0, 1, and 5 in software. It doesn't cover all the possibilities by any means, but it is certainly sufficient for many purposes.

**Disk Administration Enhancements**

The task of disk management in Windows Server 2003 brings not only a brand new interface, based on the Microsoft Management Console (MMC), but also a whole new set of capabilities. Anyone who has spent much time with Windows NT will probably not miss the old Disk Administrator at all.

The MMC's Disk Management snap-in (shown in Figure 18-1), which is provided for managing your physical disks, is divided into two panes. By default, the top pane shows the drive letters (volumes) associated with the local disks and gives their properties and status, while the bottom pane has a graphical representation organized by physical drive. It can be used as a standalone snap-in or as part of the Computer Management console, shown in Figure 18-2.

![Figure 18-1  Disk Management with an MMC interface](image-url)
Figure 18-2 The Computer Management console and the Disk Management snap-in

Hardware RAID

Although Disk Management provides an excellent software RAID solution, hardware RAID is also now widely available, from either the original server vendor or from third parties, and it provides substantial advantages over software RAID. Hardware RAID solutions range from a simple RAID controller to fully integrated, standalone subsystems. Their features vary, as does their cost, but all claim to provide superior performance and reliability over a simple software RAID solution such as that included in Windows Server 2003. In general, they do. Some advantages they offer include the following:

- Hot-swap and hot-spare drives, allowing for virtually instantaneous replacement of failed drives
- Integrated disk caching for improved disk performance
- A separate, dedicated system that handles all processing, for improved overall performance
- Increased flexibility and additional RAID levels, such as RAID-10 (also called RAID 0+1), a combination of striping (RAID-0) and mirroring (RAID-1) that provides for fast read and write disk access with full redundancy

Not all hardware RAID systems provide all these features, but all have the potential to improve the overall reliability and performance of your hard disk subsystem. As such, definitely consider them for any mission-critical server.
Remote Management

The new Disk Management snap-in in Windows Server 2003 lets you manage not only the local hard disks but also drives on other computers running Windows 2000, Windows XP, and Windows Server 2003, enabling the administrator to manage disk tasks and space allocations from a workstation without having to sit at the machine that is being administered. This capability is a boon for remote site management and—using the MMC—makes it easy to delegate authority and administrative responsibilities for a group of computers to others without having to give them full administrative privileges.

Dynamic Disks

Dynamic disks were introduced in Windows 2000 Server. By converting a disk to a dynamic disk, you give Disk Management the ability to manage it in new ways, without requiring a reboot in most cases. You can extend a disk volume, span a volume across multiple physical disks, stripe the volume for improved performance, mirror it, or add it to a RAID-5 array—all from the MMC and all without a reboot, after the disk is converted to a dynamic disk. The initial creation or conversion of the first of your basic disks to a dynamic disk requires a reboot, unfortunately, but when you get over that hurdle, you’ll breeze through the remaining tasks. When combined with the new remote management functionality, dynamic disks give the system administrator powerful tools for managing the type and configuration of hard disk storage across the enterprise.

Command Line

Windows Server 2003 adds a complete command-line interface for managing disks to the system administrator’s toolkit—Diskpart.exe. This command-line utility is scriptable or it can be used interactively. Here is a simple script to create a volume on an existing dynamic disk and assign it to the next available drive letter:

REM Filename: MakeVol.txt
REM
REM This is a DiskPart.exe Script. Run from the command line
REM or from another script, using the syntax:
REM
diskpart /s MakeVol.txt > logfile.log
REM
REM to run this script and dump the results out to a log file.
REM
REM This script creates a simple volume of 4 Gb on disk #5, and then
REM assigns a drive letter to it. Note that this does NOT format
REM the volume -- that requires using the format command, not part
REM of diskpart.exe
REM First, list out our disks. Not required for scripting, but useful
REM to show the overall environment if we need to troubleshoot problems
list disk

REM Next, select which disk will have the simple volume created on it.
select disk 5

REM Now, create the volume...
create volume simple size=4096

REM Assign without parameters will choose the next available HD letter.
Assign

Windows Server 2003 also includes a useful command-line utility for managing various
file system functionality —Fsutil.exe. Fsutil.exe is covered in Chapter 20.

---

**Disk Management Tasks**

Like all MMC snap-ins, the Disk Management snap-in can be opened in a number of
ways. One of the most direct ways is to right-click the My Computer icon in the upper left
corner of your desktop and choose Manage from the menu. This opens a local version of
the Computer Management snap-in, containing the System Tools, Storage, and Services
and Applications snap-ins. Click Storage to access the Removable Storage (if you have
removable storage drives installed), Disk Defragmenter, Logical Drives, and Disk Man-
agement snap-ins, and then click Disk Management to open the Disk Management win-
dow. To open the Disk Management snap-in only, double-click the file Diskmgmt.msc in
the %WinDir%\System32 directory.

When you open the Computer Management snap-in, you have the ability to manage not
only the resources of the local computer but also those of remote computers. This makes
it easy to manage the disks on a remote computer. If you run the Disk Management snap-
in only, you're limited to managing disks on your local computer, unless you create a cus-
tom MMC. The Disk Management snap-in can be customized to change the view settings
available in a variety of ways. See Chapter 12 for information about creating and custom-
izing MMCs.

**Adding a Partition or Volume**

Adding a new drive or partition to a Windows 2000 or Windows Server 2003 server is
straightforward. First, obviously, you need to physically install and connect the drive. If
you have a hot-swappable backplane and array, you don't even have to shut the system
down to accomplish this task. If you're using conventional drives, however, you need to
shut down and power off the system.
After the drive is installed and the system is powered up again, Windows Server 2003 automatically recognizes the new hardware and makes it available. If the disk is a basic disk that is already partitioned and formatted, you’re able to use it immediately. If it’s a brand new disk that has never been partitioned or formatted, you need to prepare it first. And if it’s a dynamic disk or disks, but from another machine, you’re able to use it as soon as you import it. If the disk is a basic disk that has already been formatted, you don’t get prompted to upgrade it to a dynamic disk, but do so anyway. If the disk has never been used before, you’re prompted by the Initialize and Convert Disk Wizard.

Note  If you’re adding a drive to your server that uses a different technology than existing drives, or simply a different controller, it might require a new driver before the disk is recognized by the system.

Adding a New Disk Using the Initialize And Convert Disk Wizard

If you install a new hard drive, it is automatically recognized if the driver for the disk is already present on the system, and the Initialize And Convert Disk Wizard starts automatically when you open Disk Management. To add a new disk after the logon event is complete, follow these steps:

1. Open the Computer Management console by right-clicking the My Computer icon on your desktop and choosing Manage from the shortcut menu.
2. On the Storage menu, choose Disk Management. If the disk is new, you see the first page of the Initialize And Convert Disk Wizard, shown in Figure 18-3. This wizard allows you to upgrade the new disk to a dynamic disk. Click Next.

Figure 18-3  The first page of the Initialize And Convert Disk Wizard
3. You see a confirmation of the disk (or disks, if you added more than one) that can be selected for initializing, shown in Figure 18-4.

![Select Disks to Initialize](image1.png)

**Figure 18-4**  The Select Disks To Initialize page of the Initialize And Convert Disk Wizard

4. Make sure there is a check mark to the left of the disk or disks to be upgraded and then click Next again.

5. Now select the disks you want to convert to dynamic disks from the list, as shown in Figure 18-5.

![Select Disks to Convert](image2.png)

**Figure 18-5**  The Select Disks To Convert page of the Initialize And Convert Disk Wizard
6. You get a confirmation message. If all the options are correct, click Finish and the
disk will be initialized and converted to a dynamic disk.

7. When the wizard finishes, you’re at the main Disk Management console, shown in
Figure 18-6. Notice that the disk is still not formatted or allocated and is highlighted
in black (if you haven’t changed the default color settings for the Disk Management
console).

![Figure 18-6](image)

**Figure 18-6** The main Disk Management console, showing the new disk (Disk 2)

**Creating a Volume**

To create a new volume (the dynamic-disk equivalent of a partition), complete these
steps:

1. In the Disk Management console, right-click the unallocated disk and choose
Create Volume from the shortcut menu. The New Volume Wizard opens to guide
you through the process of creating the new volume on the dynamic disk. Click
Next.

2. Select the type of volume you’ll be creating (Figure 18-7). Depending on the num-
ber of available unallocated volumes, you see one or more options for the type of
volume. These options include Simple, Spanned (the Windows NT 4 Volume Set),
Striped (RAID-0), Mirrored (RAID-1), and RAID-5. Click Next.

3. Select the dynamic disks to use for the new volume. The choices available and the
selections you need to make depend on the type of volume you’re creating and the
number of available unallocated disks. Figure 18-8 shows a RAID-5 volume being
created.
4. On the same page, adjust the size of the new volume. By default, the new volume will use the maximum available space from each of the selected disks. For spanned volumes, this will be the sum of the free space on the selected disks; for other types of volumes, it will be the number of disks multiplied by the available space on the smallest of the selected disks. Click Next.

5. Select either a drive letter or a mount point for the new volume (as shown in Figure 18-9), or opt not to assign a drive letter or path at this time. With Windows Server 2003, you can “mount” a volume on an empty subdirectory, minimizing the number of drive letters and reducing the complexity of the storage that is displayed.
to the user. If you want to take advantage of this feature, click Browse to locate the directory where you will mount the new volume. Click Next. See the Real World sidebar “Mounted Volumes” for more about this subject.

6. Select the formatting options you want (shown in Figure 18-10). Even when mounting the volume rather than creating a new drive, you can choose your format type without regard to the underlying format of the mount point. Click Next.

7. You see a confirmation page. If all the options are correct, click Finish to create and format the volume. You return to the Disk Management console, where you see the new volume (shown in Figure 18-11).

Figure 18-9  Select a drive letter or mount point for the new volume

Figure 18-10  Set the formatting options for the new volume
Mounted Volumes

Windows Server 2003 borrows a concept from the UNIX world by adding the ability to mount a volume or partition on a subfolder of an existing drive letter. A mounted volume can also have a drive letter associated with it, although it does not need to, and it can be mounted at more than one point, giving multiple entry points into the same storage.

A volume must be mounted on an empty subfolder of an existing NTFS volume or drive. FAT and FAT32 drives do not support mounted volumes. You can, however, mount a FAT or FAT32 volume at any mount point. You can mount only a single volume at a given mount point, but you can then mount further volumes on top of an existing mounted volume, with the same rules and restrictions as any other mount. The properties of a drive do not show all the available disk space for that drive, because they do not reflect any volumes mounted on the drive.

Mounted volumes can be used to provide a mix of redundant and nonredundant storage in a logical structure that meets the business needs of the enterprise while hiding the complexities of the physical structure from the users. Unfortunately, mounted volumes are not handled correctly by Network File System (NFS) shares and should be avoided in environments where Server for NFS is used.

Creating a Partition

You can create partitions only on basic disks, not on dynamic disks. To create a new partition, follow these steps:

1. In the Disk Management console, right-click the unallocated basic disk and select New Partition. The New Partition Wizard, shown in Figure 18-12, opens to guide you through the process of creating the new partition on the basic disk. Click Next.
2. Select the type of partition you’ll be creating. (See Figure 18-13.) If this is a removable drive, you see only an option for a primary partition, but with a nonremovable disk you’re able to choose either a primary or an extended partition. A basic disk can hold up to four primary partitions or three primary partitions and one extended partition. Click Next.

3. Specify how much of the available space on the disk you want to use for this partition. (See Figure 18-14.) Click Next.
4. If you’re creating an extended partition, continue with Step 6. If you’re creating a primary partition, select either a drive letter or mount point for the new partition, as shown in Figure 18-15. You can also choose to defer giving the new partition a mount point or drive letter. However, it is unavailable to your users until you do. Click Next.

5. Select the formatting options you want, or opt to defer formatting until later. Click Next.

6. You see a confirmation page. If all the options are correct, click Finish to create the partition. If it is a primary partition, it will be formatted and the drive letter or
mount point will be assigned. If it is an extended partition, you’ll need to format it and choose the drive letters and mount points for it, as discussed in the next section, “Creating Logical Drives in an Extended Partition.”

**Real World  Formatting Options**

Windows Server 2003 supports three file system formats: FAT, FAT32, and NTFS. However, only NTFS should be used on a server. NTFS is required for all the advanced features of Windows Server 2003 and is inherently more secure than FAT or FAT32.

Before any disk or volume can be used, it must be partitioned and formatted. You can choose to quick-format a drive to make it available more quickly, but this option simply removes the file entries from the disk and does no checking for bad sectors. Select this choice only when recycling a disk that has already been formatted and when you are confident it hasn’t been damaged.

On an NTFS volume or partition, you can specify the allocation unit size. This option lets you tune the disk for a particular purpose, depending on the disk’s size and intended function. A database storage volume that will contain large database files that are managed by the database program might lend itself to large allocation units (also called clusters), while a disk that must hold many small files is a candidate for smaller clusters. However, the default sizes are an excellent compromise for most situations—modify them only with caution and with a clear understanding of the consequences for your environment.

You can also choose to enable disk and folder compression on NTFS volumes and partitions. This causes all files and folders on the volume to be compressed, as opposed to individual files or folders you select. Compression can minimize the amount of hard disk space used by files, but it can have a negative impact on performance. Given the low cost of hard-drive space today, compression hardly seems worth the risk and effort, and certainly it is not a good option to use for frequently updated data.

Finally, a cautionary note. Formatting a disk doesn’t actually remove the data on it. If you are removing a disk from service, don’t just format it and throw it away or recycle it. If there is any chance that the disk might contain sensitive data, you need to wipe the disk completely with a program that will make it difficult or impossible for others to read the data on the disk. There are commercial third-party products with cute interfaces to do this, or you can use the built in Windows Server 2003 command Cipher with the /w (for wipe) switch. To erase a disk completely, first format it, then use cipher /w. If the disk has multiple volumes or partitions on it, do this for each volume, then remove the partitions with diskpart.
Creating Logical Drives in an Extended Partition

If you created a new extended partition, the next step is to create logical drives in the partition. You can assign one or more logical drives in an extended partition, and each of those logical drives can be assigned a drive letter and one or more mount points. Each of the logical drives can be formatted with any of the supported file systems, regardless of the format of other logical drives. To create a logical drive, follow these steps:

1. In the Disk Management console, right-click the Free Space portion of the extended partition and select Create Logical Drive from the menu to open the New Partition Wizard (shown earlier in Figure 18-12). Click Next.

2. You see the Select Partition Type page, shown in Figure 18-16, with the Logical Drive option selected and the only choice active. Click Next and specify the size of the logical drive you’ll be creating, as shown in Figure 18-17. You can specify the entire partition for a single drive, or you can divide the partition into multiple logical drives. Click Next.

3. Select the drive letter or mount point for the new logical drive, as shown in Figure 18-18. You can also choose not to assign a letter or mount point at this time. Click Next.

4. Select the formatting options you want. Click Next again, and you see the final confirmation page. If all the options are correct, click Finish to create and format the new logical drive. If you need to create additional logical drives on the partition, you can repeat these steps as many times as required to create the number of logical drives desired.
Deleting a Partition, Volume, or Logical Drive

Deleting a partition, deleting a logical drive, and deleting a volume are essentially the same task, with one important exception. When you delete a logical drive, you end up with free space in the partition, but other logical drives in the partition are untouched. When you delete a partition or volume, the entire volume or partition is deleted. You cannot, however, delete an extended partition until all the logical drives
in the partition have first been deleted. You can directly delete a primary partition or a volume.

In all cases, when you delete a volume, logical drive, or partition, you end up with free or unallocated space and no data on the volume, drive, or partition when you’re done, so make sure you have a good backup if there’s a chance you might later need any of the data. To delete a partition, logical drive, or volume, follow these steps:

1. Right-click the partition, logical drive, or volume and choose Delete Partition, Delete Logical Drive, or Delete Volume.

2. If you’re deleting a volume or partition, you see a warning message similar to the one shown in Figure 18-19. Deleting an extended partition involves extra steps, because you must first delete the logical drives in the partition before you can delete the partition itself.

When the volume or partition is completely deleted, the space it occupied will be unallocated. Space that is unallocated on dynamic disks can be used to create mirrors, extend an existing volume, create a RAID array, or otherwise manage the storage on your server. Space that is unallocated on basic disks can be partitioned.

**Converting a Disk to a Dynamic Disk**

The advantages of dynamic disks are significant. Even if you use hardware RAID controllers and hot-swappable disks to manage your hard disks, you might find it useful to use dynamic disks. There is a caveat, however. Because you can’t boot from or even see a dynamic disk from any other operating system except Windows 2000 Server and later, and because manipulating dynamic disks from the recovery console will cause data corruption, you should leave your boot drive as a basic drive. If you need to provide for redundancy on that drive, use a hardware RAID controller to provide RAID level 1 on your boot drive. This will make recovery from a failed hard disk or other disaster as painless as possible. To convert a basic disk to a dynamic disk, follow these steps:

1. Right-click the disk’s icon on the left side of the Disk Management console, and choose Upgrade To Dynamic Disk from the shortcut menu.
2. You see a dialog box like the one shown in Figure 18-20, listing the available basic disks on your machine. The disk you clicked is selected, and you can select other disks to upgrade at the same time. Click OK to continue with the upgrade.

3. You get a warning message stating that no other version of Windows can use these disks. Click Next.

![Figure 18-20](image)

You can select more than one disk to upgrade

4. If there are no file systems on the disks you chose to upgrade, that's all there is to it. However, if there are file systems on any of the disks, you get a warning message stating that the file systems will be dismounted. Click Yes and the upgrade proceeds. You can now manage the disks dynamically, and they can be part of mirrors, RAID-5 arrays, or other enhanced disk configurations that aren't supported by basic disks.

**Important** If there are any open files on the disk to be upgraded, you might experience data loss. Perform disk upgrades only during quiet times when no users are logged on to or using the server.

---

**Extending a Volume**

You can add space to a volume without having to back up, reboot, and restore your files if the volume is on a dynamic disk and if it is a simple volume or a spanned volume. You do this by converting the volume to a spanned or extended volume that incorporates unallocated space on any dynamic disk. Unfortunately, you can’t increase the size of a RAID-5 or RAID-0 (striped) volume simply by adding disks to the array, unless you’re using a version of hardware RAID that supports this functionality. To extend a volume, follow these steps:

1. In the Disk Management console, right-click the volume you want to extend. Choose Extend Volume from the menu to open the Extend Volume Wizard. Click Next.
2. Highlight one or more disks from the list of dynamic disks that are available and have unallocated space. Click Add to add the selected disk or disks, and indicate the amount of space you want to add. (See Figure 18-21.) Click Next.

3. The Extend Volume Wizard displays a final confirmation page before extending the volume. Click Finish to extend the volume, or click Cancel if you change your mind.

---

**Important** A spanned (extended) volume is actually less reliable than a simple disk. Unlike a mirror or RAID-5 volume, in which there is built-in redundancy, a spanned or striped volume will be broken and all its data lost if any disk in the volume fails.

---

**Real World** **Extending—Administrator’s Friend or Foe?**

Most administrators have wished at some point that they could simply increase the users’ home directory space on the fly without having to bring the system offline for several hours while the entire volume is backed up and reformatted to add the additional hard disks, the backup is restored, and the share points are re-created. Fun? Hardly. Risky? Certainly. And definitely a job that means coming in on the weekend or staying late at night—in other words, something to be avoided if at all possible.
All this makes Windows Server 2003’s ability to create additional space on a volume without the need to back up the volume, reformat the disks, and re-create the volume a seductive feature. However, if you’re using conventional hard disks without hardware RAID, you might want to think twice before jumping in. Only spanned or striped volumes allow you to add additional storage on the fly, and, because neither is redundant, using them exposes your users to the risks of a failed drive. Yes, you have a backup, but even under the best of circumstances, you’ll lose some data if you need to restore a backup. Further, using spanned volumes actually increases your risk of a hard-disk failure. If any disk used as part of the spanned volume fails, the entire volume is toast and will need to be restored from backup.

Why, then, would anyone use spanning? Because they have hardware RAID to provide the redundancy. This combination offers the best of both worlds—redundancy provided by the hardware RAID controller and flexibility to expand volumes as needed, using Windows Server 2003 Disk Management. Yet another compelling argument for hardware RAID, in case you needed any more.

---

**Note** Windows Server 2003 uses the terms “extended” and “spanned” nearly interchangeably when describing volumes. Technically, however, a spanned volume must include more than one physical disk, while an extended volume can also refer to a volume that has had additional space added to the original simple volume on the same disk.

---

**Adding a Mirror**

When your data is mission critical and you want to make sure that no matter what happens to one of your hard disks the data is protected and always available, consider mirroring the data onto a second drive. Windows Server 2003 can mirror a dynamic disk onto a second dynamic disk so that the failure of either disk does not result in loss of data. To mirror a volume, you can either select a mirrored volume when you create the volume (as described in the “Creating a Volume” section earlier in this chapter) or add a mirror to an existing volume. To add a mirror to an existing volume, follow these steps:

1. In the Disk Management console, right-click the volume you want to mirror. If a potential mirror is available, the shortcut menu lists the Add Mirror command.
2. Choose Add Mirror to display the Add Mirror dialog box, shown in Figure 18-22, where you can select the disk to be used for the mirror.

![Add Mirror dialog box](Image)

**Figure 18-22** The Add Mirror dialog box

3. Highlight the disk that will be the mirror, and click Add Mirror. The mirror is created immediately and starts duplicating the data from the original disk to the second half of the mirror, as shown in Figure 18-23. This process is called *regeneration* or sometimes *resynching*. (The process of regeneration is also used to distribute data across the disks when a RAID-5 volume is created.)

**Note**  Regeneration is both CPU intensive and disk intensive. When possible, create mirrors during slack times or during normally scheduled downtime. Balance this goal, however, with the equally important goal of providing redundancy and failure protection as expeditiously as possible.

![Disk Management](Image)

**Figure 18-23** A newly created mirrored disk in the process of regeneration
To improve your overall data security and reliability, mirror your volumes onto disks that use separate controllers whenever possible. This process is known as *duplexing*, and it eliminates the disk controller as a single point of failure for the mirror while actually speeding up both reading and writing to the mirror, because the controller and bus are no longer potential bottlenecks.

**Drive Failure in a Mirrored Volume**

If one of the disks in a mirrored volume fails, you continue to have full access to all your data without loss. Windows Server 2003 marks the failed disk as missing and takes it offline, as shown in Figure 18-24, while sending alerts to the alert log. However, it continues to read and write from the other half of the mirrored volume as though nothing had happened. Be warned, however, that you no longer have any fault tolerance on that volume, and any additional failure will result in catastrophic data loss.

After you replace the failed disk or correct the problem and reactivate it, the mirror automatically starts regenerating. If the problem can be solved without powering down the system, you can regenerate the mirror on the fly. To reactivate the failed disk, follow these steps:

1. Right-click the icon for the failed disk on the left side of the Disk Management console to get the menu shown in Figure 18-25.
2. Choose Reactivate Disk. Windows Server 2003 warns you about running chkdsk on any affected volumes, brings the disk back online, and starts regenerating the failed mirror, as shown in Figure 18-26. When the mirror has been regenerated, the disk status changes from Resynching to Healthy.

![Figure 18-26 Data being regenerated on a reactivated mirrored disk]

**Removing a Mirror**

If you need to make additional disk space available on your system and you have no additional disks available, you can remove the mirror from a mirrored volume. When you remove a mirror, the data on one of the disks is untouched, but the other disk becomes unallocated space. Of course, you will have lost all redundancy and protection for the data, so you need to take steps to restore the mirror as soon as possible. Until then you might want to modify your backup schedule for the remaining disk. To remove a mirror, follow these steps:

1. In the Disk Management console, right-click either half of the mirror. Choose Remove Mirror from the menu, and the Remove Mirror dialog box opens, as shown in Figure 18-27.

2. Highlight the disk you want to remove from the mirror. Click Remove Mirror. You get one last chance to change your mind. Click OK and the disk you highlighted becomes unallocated space.
Breaking a Mirror

If a disk fails and you can’t replace it with an identical one, break the mirror until a replacement becomes available. Breaking a mirror severs the connection between the two disks, allowing the remaining disk to continue to function normally until a replacement disk becomes available. You might also find it useful to break a mirror even when both disks are still functioning, because you then end up with two identical copies of the same data. One of the halves of the broken mirror continues to have the same drive letter or mount point, while the second half of the broken mirror is assigned the next available drive letter. To break a mirror, follow these steps:

1. In the Disk Management console, right-click either disk of the mirrored volume.
2. Choose Break Mirror from the shortcut menu. You’re asked to confirm that you really want to break it.
3. Click Yes, and the mirror is broken. You’ll have two disks. One retains the drive letter or mount point of the original mirror, and the other is assigned the next available drive letter. They will both contain exact duplicates of the data at the instant of the break but will immediately start to diverge as they are modified.

Real World  Backing Up Active Files

One of the most difficult tasks faced by the system administrator is to get a reliable, sure backup of a file that is in constant active use. An example of this is a data file for a database such as Microsoft SQL Server or Oracle. Although there are third-party solutions that back up active database files on the fly, they’re not free. The Break Mirror command can be used to get around this problem. You can momentarily stop the database, break the mirror, and restart the database. Now you have a copy of the data.
file that is no longer in active use and can be safely and effectively backed up. When the backup is complete, you can delete the broken volume and re-create the mirror. Note, however, that the creation of a mirror involves substantial overhead and might adversely affect system performance until the regeneration is complete. And while your mirror is broken, you don’t have any redundancy on the active disk.

Converting a Volume or Partition from FAT to NTFS

You can convert a volume or partition from the FAT or FAT32 file system to NTFS without losing data or interrupting the availability of the rest of the server. However, Windows Server 2003 offers no graphical way to do this—you have to run a command-line utility. To convert a volume or partition, open a command window and type

```convert <volumename | mountpoint | driveletter:/> /fs:ntfs [/v]
```

This command converts the volume or drive from either FAT or FAT32 to NTFS. If you use the `/v` command-line switch, the conversion will be fairly noisy, listing the name of each file and directory that’s converted. If someone has a file open on the volume and the program cannot gain exclusive access to it, you’re offered the opportunity to schedule the conversion for the next time you reboot. This option is all right if you have a planned maintenance reboot coming anyway, but otherwise you probably shouldn’t schedule the conversion, because it might end up taking a fairly long time if the drive is large and contains a lot of files.

Real World NTFS Conversion Planning

If you schedule a conversion to NTFS for the next reboot before you’re actually ready to reboot the server and your server needs to be rebooted unexpectedly, you simply have to wait while the conversion happens. There is no way to bypass the conversion after you commit to it. This can turn minor downtime into a major headache if it happens in the middle of the production day. Don’t commit to a conversion unless you are sure you can afford the downtime if Windows Server 2003 unexpectedly decides it needs to reboot. Or better yet, don’t use FAT or FAT32 drives in the first place—they really have no place on a server.

Formatting a Partition or Volume

Before a partition, logical drive, or volume can be used, it must be formatted. Formatting lays down the necessary structure to support the file system you choose for the volume. You must format a volume or drive when it is first created, and at any later point if you want to clear it off. You can also use Format to change the type of file system on a drive, partition, or volume, but all data on the target is deleted during the formatting. (The
command-line `convert` command—which allows conversion of FAT and FAT32 targets to the NTFS format only—preserves any data on the target.) The file systems supported by Windows 2000, Windows XP, and Windows Server 2003 are FAT, FAT32, and NTFS.

In general, use NTFS unless you have a compelling reason not to. One case in which some would argue that you would not use NTFS is when log files will reside on the volume or partition. A FAT32 volume tends to be faster and more appropriate for large files that grow constantly in small increments, as log files do. However, even with log files, use extreme caution before opting for FAT32—there are no quotas, no volume shadow copies, and most importantly, no security on a FAT32 file system. If your applications are written to take advantage of it, the new Common Log File System (CLFS) provides a far better alternative without the impact on security that FAT32 has.

**Under the Hood  Common Log File System (CLFS)**

Windows Server 2003 R2 includes a new type of file system—the Common Log File System. CLFS is a specialized file system driver designed specifically for writing log files efficiently. It must be implemented by the application writing the log files—you can’t suddenly get all your applications to use CLFS by creating a CLFS disk. Both Kernel mode and User mode applications can be written to use the CLFS driver.

CLFS is a performance optimized driver. All writes are buffered until an explicit flush or the buffer is filled. Or another application using CLFS forces a write—CLFS is smart enough to piggyback writes. Logs are written directly to disk from the buffer, and multiple streams of data can be written during a single I/O operation, reducing disk seeks. Disk reads are cached to reduce disk accesses as well.

**Real World  Assigning Volume Names**

The name you assign to a volume, partition, or drive should tell you something about it rather than simply mimicking the drive letter. A volume name like “Big70GBSCSI” tells you pretty conclusively that it’s that big new SCSI drive you just bought—unless, of course, you already have half a dozen of them on your server, in which case you’ll need a more effective name. On the other hand, a volume name of C_DRIVE is just about useless, because the drive letter is available from anywhere that the volume name is. A common scheme is to assign volume names based on the primary use of the volume. For example, “UserHome” or “DB_STORE” make it pretty clear what the volume is from a logical (but not necessarily physical) view.
Another reason to use FAT or FAT32 is to allow the computer to support dual booting into other operating systems. NTFS is not visible or accessible from other operating systems, while FAT can be used by a variety of operating systems and FAT32 can be used by Microsoft Windows 95, Windows 98, and Windows Me in addition to Windows 2000 and Windows XP. But again, unless this is a test lab machine, dual booting doesn’t make a whole lot of sense on a server. To format a logical drive, partition, or volume, follow these steps:

1. In the Disk Management console, right-click the logical drive, partition, or volume you want to format, and choose Format from the menu. You see the dialog box shown in Figure 18-28. Select the file system you want to use: FAT, FAT32, or NTFS.

![Figure 18-28 The Format dialog box](image)

2. Select the allocation unit size (also called the cluster size). Normally, you simply accept the default here. See the Real World sidebar “Optimum Cluster Size” for a discussion of this issue.

3. Type a name for the volume, logical drive, or partition. The default name is New Volume.

4. Select the Perform A Quick Format box if you want to format the drive quickly. Do not do this, however, unless you have a strong need to make the volume available immediately. The full, long version of the format checks the entire drive for defects. It can take a while on a large drive, and the overall system performance will tend to suffer while the format is going on, but the greater sense of confidence in the volume should be worth the wait.

5. If the entire drive will be compressed, select Enable File And Folder Compression. Note, however, that you can choose to compress individual folders and even individual files regardless of whether you check this option now. And with the size and cost of drives these days, this option is much less useful than it once was.

6. Click OK and the formatting begins. Windows Server 2003 can handle only one format at a time, so you’re unable to format any other partition or volume until this one finishes.
Real World  Optimum Cluster Size
A discussion of the best cluster size for a particular application or need is beyond the scope of this chapter and can be fairly heated, with an enormous amount of unsubstantiated and generally false statements being bandied about. Suffice it to say that the defaults are good for almost all situations and that decisions to choose something other than the default allocation size should be made only when there is a specific, clearly understood reason and a compelling need to do so. You can choose cluster sizes from 512 bytes up to 256 KB. You cannot enable file and folder compression on NTFS if you go beyond 4 KB for your allocation unit size.

If you seriously think you need to change the cluster size for a particular volume, first make the change in a controlled lab environment and perform confidence and performance tests to ensure that the change meets your needs and doesn’t cause unintended side effects.

Changing a Drive Letter
You can change the drive letter of a volume or partition at any time, and you can even have multiple paths to a given drive. In addition, Windows Server 2003 allows you to change the drive letter of a removable drive, such as a Jaz or Zip drive. To change a drive letter, follow these steps:

1. Right-click the drive in the Disk Management console, and choose Change Drive Letter And Path.

2. A dialog box displaying the current drive letter and any mount-point paths for the disk appears, as shown in Figure 18-29. Highlight the drive letter shown, and click Change. Select the new drive letter from the drop-down list. Click OK.

![Figure 18-29  Changing the drive letter and path of a logical drive](image-url)
3. You see a confirmation message warning that the change could affect the ability of some programs to run. Click Yes and the drive letter change takes place immediately, unless there are open files on the drive. If there are open files on the drive, the drive temporarily has two drive letters, the old one and the new one. You see the warning shown in Figure 18-30. Click Yes to confirm the change.

![Figure 18-30](image)  
**Figure 18-30**  Message warning that a drive has a dual identity

### Mounting a Volume

Starting with Windows 2000, Microsoft added a new feature to the disk and storage management process. You can mount a dynamic volume—or any partition or logical drive in an extended partition—on any empty directory that resides on a drive that is both NTFS formatted and nonremovable. The volume being mounted can be formatted as FAT, FAT32, or NTFS, and appears to users as a simple directory. This feature makes it possible to create larger file systems that use multiple hard disks without the inherent risks of using spanned volumes, because the failure of any one of the mounted volumes affects only the directories that were part of that volume. You can also easily support multiple formats from a single drive letter. To mount a volume, follow these steps:

1. From the Disk Management console, right-click a volume or partition. Choose Change Drive Letter And Path from the menu. The Change Drive Letter And Paths dialog box, shown previously in Figure 18-29, opens.

2. Click Add; the Add New Drive Letter Or Path dialog box opens, shown in Figure 18-31.

![Figure 18-31](image)  
**Figure 18-31**  The Add New Drive Letter Or Path dialog box, used to mount a volume
3. You can type the mount point or click Browse to select or create a mount point. Any empty directory that resides on a nonremovable NTFS volume or drive can be the mount point.

4. After you select or type the mount point, click OK, and the volume or partition is mounted.

**Important**  It's actually easy to get yourself into trouble with this new feature. Disk Management lets you make multiple levels of mounted volumes, including ones that are recursive. You're well advised to mount volumes only at the root level of a drive. Trying to mount below that point can lead to confusion and make management and documentation difficult. Also, do not use mounted volumes in areas of the file system that are shared with Server for NFS. Server for NFS does not currently support mounted volumes correctly.

---

**NTFS**

The NTFS format had been around, essentially unchanged, since the original version of Windows NT. Beginning with Windows 2000, and continuing with Windows Server 2003, Microsoft has made substantial changes to NTFS to support the new features that administrators and users have been asking for. These new features include shadow copies, disk quotas—finally—and the ability to encrypt files and whole file systems at the physical disk level.

**Note**  The new version of NTFS, introduced in Windows 2000, is a logical extension of the original NTFS but is not completely compatible with it. If you're going to use NTFS in a dual-boot configuration with Windows NT 4 on the same machine as Windows Server 2003, you must install Windows NT 4 Service Pack 4 or later to permit your Windows Server 2003 NTFS partitions to be seen when booted into Windows NT 4. Also keep in mind that the quotas and encryption available in Windows Server 2003 are not supported under Windows NT 4 and will not be enforced or available in it. Do not enable shadow copies on a machine that dual boots. Any changes made to files from an alternate boot are not properly updated and shadowed and can become corrupted.

**Encrypting on the File System Level**

With the introduction of Windows 2000, Microsoft added the ability to encrypt individual files or entire subdirectories stored on an NTFS in a totally transparent way. To their creator, encrypted files look exactly like regular files—no changes to applications are required to use them. However, to anyone except the creator/encryptor, the files are unavailable, and even if someone did manage to gain access to them, they would be gibberish because they're stored in encrypted form.
Encryption is simply an advanced attribute of the file, as compression is. However, a file cannot be both compressed and encrypted at the same time—the attributes are mutually exclusive. Encrypted files are available only to the encryptor, but they can be recovered by the domain or machine recovery agent if necessary. Encrypted files can be backed up by normal backup procedures if the backup program is Windows 2000–aware or Windows Server 2003–aware. Files remain encrypted when backed up, and restored files retain their encryption.

Under normal circumstances, no user except the actual creator of an encrypted file has access to the file. Even a change of ownership does not remove the encryption. This prevents sensitive data—such as payroll information, annual reviews, and so on—from being accessed by the wrong users, even ones with administrative rights.

**Important** Encryption is available only on the NTFS beginning with Windows 2000. If you copy the file to a floppy disk or to any other file system, the file is no longer encrypted. This is true even of NTFSs on earlier versions of Windows NT, or of file systems accessed using Client for NFS.

When you encrypt a folder, all new files created in that folder are encrypted from that point forward. You can also elect to encrypt the current contents when you perform the encryption. However, be warned that if you choose to encrypt the contents of a folder when it already contains files or subfolders, those files and subfolders are encrypted for the user performing the encryption only. This means that even files that are owned by another user are encrypted and available for your use only—the owner of the files will no longer be able to access them.

When new files are created in an encrypted folder, the files are encrypted for use by the creator of the file, not the user who first enabled encryption on the folder. Unencrypted files in an encrypted folder can be used by all users who have security rights to use files in that folder, and the encryption status of the file does not change unless the filename itself is changed. Users can read, modify, and save the file without converting it to an encrypted file, but any change in the name of the file triggers an encryption, and the encryption makes the file available only to the person that triggers the encryption.

**Important** If you use EFS, it is essential that you back up EFS certificates and designate a Recovery Agent to protect against irreversible data loss. EFS certificates and recovery agents are covered in Chapter 22.

To encrypt a file or folder, follow these steps:

1. In Windows Explorer, right-click the folder or files you want to encrypt, and choose Properties from the shortcut menu.
2. Click Advanced on the General tab to open the Advanced Attributes dialog box shown in Figure 18-32.

![Advanced Attributes dialog box](image)

**Figure 18-32** The Advanced Attributes dialog box

3. Select the Encrypt Contents To Secure Data option, and click OK to return to the main Properties window for the folder or file. Click OK or Apply to enable the encryption. If any files or subfolders are already in the folder, you're presented with the dialog box shown in Figure 18-33.

![Confirm Attribute Changes dialog box](image)

**Figure 18-33** Choosing whether to encrypt the files already in a folder or just new files

4. If you choose Apply Changes To This Folder Only, all the current files and subfolders in the folder remain unencrypted, but any new files and folders are encrypted by the creator as they are created. If you choose Apply Changes To This Folder, Subfolders, And Files, all the files and folders below this folder are encrypted so that only you can use them, regardless of the original creator or owner of the file.

5. Click OK and the encryption occurs.
Disk Quotas, File Screening, and Shadow Copies

Windows Server 2003 adds three new capabilities to NTFS—quotas (enhanced in R2), file screening (R2 only), and shadow copies of shared folders. Quotas and file screening give you additional flexibility in managing the use of file system resources on your server by allowing you to control how much space is available to each user or group of users and what kinds of files can be stored. Shadow copies of shared folders allow you to create backup snapshots of the files in shared folders on an NTFS volume. These snapshots are created automatically on a schedule you control, enabling easy, user-initiated, fallback to older versions of a particular file in the event of corruption, deletion, or inadvertent and undesired changes. These new storage capabilities are covered in detail in Chapter 20.

Summary

Windows Server 2003 provides the system administrator with a much richer set of disk management tools than any previous version of Windows. The addition of dynamic volumes has materially reduced the number of reboots required to manage disk resources. The administrator can now reconfigure arrays on the fly, adding disks and extending volumes to manage disk space without having to reboot for every change. When combined with hardware RAID controllers and hot-swappable drives, these tools finally give the administrator the ability to manage a 24-hour-7-day operation.

The features added to NTFS, including quotas, file screening, shadow copies, and file system encryption give the administrator additional flexibility and options to control file system abuse, to protect users and the enterprise from undesired changes and deletions, and to protect sensitive data so that even administrators don’t have inappropriate access to confidential information. And it is all done in a way that is transparent to the user.

The next chapter looks at clustering, a way to use more than one machine to improve the scalability and fault tolerance of your critical applications and services. Windows Server 2003, Enterprise Edition supports two distinct types of clustering—network load balancing and server clustering.
Microsoft Windows Server 2003 supports two high availability clustering technologies: Network Load Balancing (NLB) clusters and server clusters. Microsoft does not support combining NLB clustering with server clustering. This chapter describes the two types of clustering supported by Windows Server 2003, their place in the enterprise, and their configuration and requirements. Finally, we'll take a brief look at a new Microsoft clustering technology that is designed to support high-performance computing (HPC)—Microsoft Compute Cluster Server 2003.

**What Is a Cluster?**

A *cluster* is a group of two or more computers functioning together to provide a common set of applications or services with a single apparent identity to clients. The computers are physically connected by hardware in the form of either a network or shared storage. The clustering software provides a common interface externally while managing the resources and load internally.
Windows Clustering provides the following benefits:

- **High availability**  When a clustered application or service fails or a computer in the cluster fails, the cluster responds by restarting the application or service on another member of the cluster or by distributing the load from the failed server to the rest of the cluster.

- **Scalability**  For cluster-aware applications, adding more machines to the cluster adds capabilities.

- **Manageability**  Administrators can move applications, services, and data from computer to computer within the cluster, allowing them to manually balance loads and to offload machines scheduled for maintenance.

### Network Load Balancing Clusters

NLB—known as the Windows Load Balancing Service in Microsoft Windows NT 4—gives TCP/IP-based services and applications high availability and scalability by combining up to 32 servers running Windows Server 2003 in a single cluster. By combining NLB with round-robin DNS, NLB clustering can scale well beyond 32 servers. Client requests for applications and services provided by the cluster are distributed across the available servers in the cluster in a way that is transparent to the client. NLB clusters are supported in all versions of Windows Server 2003.

If a server fails or is taken offline, the cluster is automatically reconfigured and the client connections are redistributed across the remaining servers. If additional servers are added to the cluster, they are automatically recognized and the load is reconfigured and distributed.

### Server Clusters

Server clusters distribute the workload among the servers in a cluster, with each server running its own workload. Like other types of clusters, server clusters are scalable and highly available. In the event of a failure, applications and services that can be restarted, such as print queues and file services, are restarted transparently. Ownership of shared resources passes to the remaining servers. When the failed server becomes available again, the workload is automatically rebalanced.

Windows Server 2003 supports server clusters only in the Enterprise and Datacenter Editions. There are three basic types of server clusters supported by Windows Server 2003: single node clusters, single quorum device clusters, and majority node set clusters, as shown in Figure 19-1.
Cluster Scenarios

In deciding whether and how to implement clustering, you first need to understand what problem is being solved and how best to solve it using the available technologies. Then you can make a business case for the particular solution or combination of solutions that best solves the particular problem. This section describes various scenarios and the type of clustering appropriate for each.

Intranet or Internet Functionality

An intranet or Internet server is a prime candidate for an NLB cluster. By enabling an NLB cluster across multiple servers, you provide your site with both redundancy and increased capacity. If a server should fail, the load is distributed transparently among the remaining servers.
Each Web server in the cluster runs its own Web server and accesses only local Web pages. This version is “shared nothing” clustering—there are no shared disks and no shared applications or data, with the possible exception of a common back-end database. NLB clusters are an appropriate and relatively inexpensive way to achieve both redundancy and high availability for your Web site, whether it’s internal or external. Clients that need access to the Web pages are distributed among the servers in the cluster according to the load at each server. What makes this work is that most Web pages change infrequently, allowing manual updates of all Web servers with the same information when you need to make changes.

Terminal Services
Starting with Windows Server 2003, Terminal Services now supports clustering using NLB clusters and the new Session Directory to distribute Terminal Services sessions across a farm of servers running Terminal Services, allowing for high availability and load balancing and presenting a single face to Remote Desktop clients. If you have large numbers of Terminal Services users, moving to Windows Server 2003 and enabling NLB clustering for your servers running Terminal Services gives you additional flexibility, redundancy, and improved user experience for your Terminal Services users. For more information about Terminal Services Session Directory, see http://www.microsoft.com/windowsserver2003/techinfo/overview/sessiondirectory.mspx.

Mission-Critical Availability
If your business absolutely, positively can’t be run without a certain application or set of applications, you need a highly reliable server to make sure that the application is always available. A server cluster is a good solution in this scenario, providing both high availability and scalability. With a server cluster, you organize your critical applications into groups, one group to a server. All the resources for each group are self-contained on the server, but if any server in the cluster fails, the others pick up the services and applications from the failed server, allowing for continuous availability of critical services and applications. You can control the failover and fallback actions for each server and clustered resource.

Server clusters require a substantially greater investment in hardware than NLB clusters. In addition, with the exception of majority node set clustering, they aren’t suitable for “shared nothing” clustering, because they use a shared disk array to keep resources in sync. When a server fails, the other server picks up the applications that had been running on the failed server. Because the disks are shared, the remaining server has access to the same set of data as the failed server, and thus there is no loss of functionality. The exception to this is majority node set (MNS) clustering, which does not use a shared disk quorum resource but rather replicates data across the cluster to local quorum disks. Majority node set clustering is appropriate for geographically diverse clusters and requires specialized support from original equipment manufacturers (OEMs) and
independent software vendors (ISVs). For a TechNet support webcast on MNS clustering, see http://support.microsoft.com/kb/838612.

Requirements and Planning
Before you attempt to implement any form of clustering, you need to clearly understand the business reason for doing so. You also need to be aware of the costs and benefits of the implementation, as well as the resource requirements for a successful implementation. Treat the implementation of a Windows Server 2003 cluster as you would any other major project. Clearly state the business case for the cluster, and obtain a commitment from all levels before you expend substantial resources on the project.

Identifying and Addressing Goals
The first step in planning your cluster is to identify your goals for the implementation and the needs that using clusters will meet. This sounds obvious, but it is actually the part of the process that is most often overlooked. The implementation of any technology should always be first and foremost a business decision, not a technology decision. Creating and maintaining clusters is not a trivial task, and it requires both technological and financial resources. You'll have a hard time selling your project if you haven't clearly identified one or more needs that it will meet.

In identifying the needs to be met and the goals of your project, you need to be as objective as possible. Always keep in mind that what you might view as “cool” technology can look remarkably like scary, unproven gobbledygook to those in the organization who are less technically savvy than you are. This doesn’t mean that those individuals won’t support your project, but it does mean that you need to make the case for the project on a level that they can understand and identify with.

Start by clearly identifying the business goals that you’re trying to accomplish. State the general goals, but provide enough detail to make the success of the project clearly measurable. Identify the specific gains you expect and how those gains will be measured. Be sure to clearly indicate how the needs you’ve identified are currently being met. This step is critical because it lets you point out both the costs of your suggested method and the risks associated with it.

Identifying a Solution
Once you know the business needs you’re trying to meet, you can identify some solutions. If you’ve clearly laid out your goals and objectives for the project, the technology that achieves those goals will be driven by those needs, not the other way around. This is also the time to use your best political judgment. You need to identify not only the best
way to meet the business needs, but also how much you can realistically sell and implement in a single shot. If you think that ultimately you will need a fully integrated, three-tiered, multiple-cluster solution, you might want to build your plan around a phased approach that allows you to distribute the risks and costs over a broader period.

In addition, if you’re proposing a clustering solution to the problem, spend some time and energy identifying methodologies that might be considered alternatives to clustering and clearly laying out the strengths and weaknesses of those alternatives. This effort will short-circuit objections and diversions as you build support for your project.

**Identifying and Addressing Risks**

As you plan your schedule, be sure to identify the risks at each step of the process and plan solid fallback positions if problems arise. Selling the project is also much easier if it’s clear that you’ve actually thought about the risks. For example, if your goal is to replace an existing manual methodology, have you left yourself a way to fall back to it if there are problems? Or are the two mutually incompatible? If you’re replacing an existing client/server application with a clustered, Web-based, distributed, n-tiered application, have you drawn a clear roadmap for how you will make the transition from one to the other? What are the risks of that transition?

Spend some time identifying failure points in your project. If you’re building a server cluster to provide 24-hour, 7-day access to your Microsoft Exchange messaging, have you identified redundant network connections to the cluster? It does little good to create a highly available server if the network connection to it is questionable.

**Making Checklists**

Take the time to identify all the possible pieces of your cluster implementation ahead of time. Use this to build a checklist of steps that you need to take and the dependencies at each point. At each major step, identify the hardware, software, knowledge, and resources required, and create a checklist of the prerequisites for that step. Use the checklists in the Windows Help for Cluster Administrator as a starting point, but build onto them with the details for your implementation and your environment. The time you spend planning your clustering implementation will easily be saved in the actual installation and implementation, and it greatly reduces your risks of failure.

**Network Load Balancing Clusters**

NLB provides a highly available and scalable solution for TCP/IP-based network applications such as a Web server or FTP server. By combining the resources of two or more servers into a single cluster, NLB can provide for redundancy of information and resources while servicing far more clients than a single server alone could handle.
NLB Concepts

NLB is a Windows Server 2003 networking driver. It acts independently of the TCP/IP networking stack and is transparent to that stack. The NLB driver (Wlbs.sys) sits between the TCP/IP stack and the network card drivers, with the Windows Load Balancing Service (Wlbs.exe)—the necessary NLB control program—running on top, alongside the actual server application. (See Figure 19-2.)

![Figure 19-2 NLB as a network driver](Image)

**Note**  The Windows Load Balancing Service (Wlbs.exe) has been renamed in Windows Server 2003 to the Network Load Balancing Service (Nlb.exe). However, Wlbs.exe can continue to be used interchangeably with Nlbs.exe to provide full compatibility with existing scripts and applications. New scripts and applications should reference Nlb.exe to avoid future deprecation of Wlbs.exe.

Optimally, each server participating in an NLB cluster should have two network interface cards (NICs), although this is not an absolute requirement. Communications and management are materially improved with two NICs, however, especially in unicast mode. (Unicast mode, as opposed to multicast mode, allows each NIC to present only a single address to the network.) Overall network throughput is also improved, as the second network adapter is used to handle host-to-host traffic within the cluster. NLB clustering is not a place to try to cut costs on network cards. Server-grade NICs will provide full network throughput while minimizing the load on the servers.

NLB supports up to 32 computers per cluster. Each server application can be balanced across the entire cluster or can be primarily hosted by a single computer in the cluster, with another computer in the cluster providing directed failover redundancy. For fully distributed applications, the failure of any single host causes the load currently being serviced by that host to be transferred to the remaining hosts. When the failed server comes back online, the load among the other hosts is redistributed to include the restored server. While NLB clustering does not provide the failover protection appropriate for databases, it does provide for high availability and scalability of TCP/IP-based applications.
Note NLB is supported across the Windows Server 2003 family and requires that TCP/IP be installed. It works over Fiber Distributed Data Interface–based or Ethernet-based networks (including Wireless) from 10 megabits per second (Mbps) to 1 gigabit per second (Gbps). It uses from 250 KB to 4 MB of RAM and roughly 1 MB of disk space.

Choosing an NLB Cluster Model
A host in an NLB cluster can use one of four models, each with its own merits and drawbacks. These models are as follows:

■ Single network adapter in unicast mode
■ Single network adapter in multicast mode
■ Multiple network adapters in unicast mode
■ Multiple network adapters in multicast mode

The choice of model for a given host and cluster varies depending on the circumstances, requirements, and limitations imposed on the design of the cluster. The sections that follow provide details on each of the models.

Note NLB in Windows Server 2003 does not support a mixed unicast mode and multicast mode environment. All hosts in the cluster must be either multicast or unicast. Some hosts, however, can have a single adapter, whereas others have multiple adapters. In addition, NetBIOS cannot be supported in a single-adapter-only configuration.

Single Network Adapter in Unicast Mode
A single network adapter running in unicast mode is in some ways the easiest type of host to set up, and with only a single adapter, it is cheaper than one with multiple network adapters. It does, however, impose significant limitations:

■ Overall network performance is reduced.
■ Ordinary communications among cluster hosts are disabled.
■ NetBIOS support is not available within the cluster.

Single Network Adapter in Multicast Mode
Using multicast mode in clusters in which one or more hosts have a single network adapter means that normal communications are possible between hosts within the
cluster. This capability overcomes one of the most awkward limitations of the single adapter in unicast mode. However, there are still the following significant disadvantages:

- Overall network performance is reduced.
- Some routers do not support multicast media access control (MAC) addresses.
- NetBIOS support is not available within the cluster.

**Multiple Network Adapters in Unicast Mode**

Using multiple network adapters in unicast mode is generally the preferred configuration. It does impose the cost of a second network adapter per host, but given the relatively low cost of network adapters, including the per-port cost of hubs, this is a relatively minor price to pay for the resulting advantages:

- No limitations are imposed on ordinary network communications among cluster hosts.
- Ordinary NetBIOS support is available through the first configured adapter.
- No bottlenecks occur as a result of a single network adapter.
- The model works with all routers.

**Multiple Network Adapters in Multicast Mode**

If you are forced by circumstances to use some hosts within a cluster that have only a single network adapter and you must be able to maintain normal network communications among the hosts in the cluster, you must run all the hosts in multicast mode, even those with multiple adapters, because you can’t run some hosts in unicast mode and some in multicast mode. This limitation could cause a problem with some routers, but otherwise it is a viable solution.

**Creating an NLB Cluster**

Creating an NLB cluster requires using the Network Load Balancing Manager, shown in Figure 19-3. This new manager simplifies the creation and management of NLB clusters, bringing all the pieces into a single management interface. You can connect to the NLB with the NLB Manager on any address in the cluster, including private addresses or the shared public address.

**New NLB Cluster**

To create a new NLB cluster, follow these steps:

1. Open the Network Load Balancing Manager from the Administrative Tools folder, as shown in Figure 19-3.
2. Right-click Network Load Balancing Clusters in the left pane and select New Cluster, as shown in Figure 19-4.

3. In the Cluster Parameters screen, shown in Figure 19-5, you need to enter an IP address, subnet mask, and the fully qualified domain name (FQDN) that the cluster will be known by. This IP address is a fixed IP address, so it can’t be a DHCP address.
4. Select whether the cluster will be unicast or multicast and whether you will allow remote control. Then click Next.

**Important** Allowing remote control of a cluster is a significant security issue. Before you decide to enable this, carefully consider the consequences and understand the risks. If you do decide to enable remote control of your cluster, you should enforce sound password rules on the remote password. For more information about NLB security, see [http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/clustering/nlbsecbp.mspx](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/clustering/nlbsecbp.mspx).

5. If the cluster will have additional IP addresses, enter them in the Cluster IP Address screen, and then click Next.

6. You can enter port rules in the next screen, or wait to configure these after you get the cluster up and running. Port rules can be used to control the behavior of various types of TCP/IP traffic. Windows Server 2003 allows you to configure different port rules for different IP addresses. Click Next when you have configured any rules you want to configure at this point.

7. Enter the name or IP address of the first host that will be joined to the cluster in the Connect screen, shown in Figure 19-6. Click Connect to connect to the server and bring up a list of network interfaces available. Highlight the interface that will host the public traffic of the cluster (as opposed to private, node-to-node traffic).
8. Click Next to bring up the Host Parameters screen, shown in Figure 19-7. Here you set the priority for this host of the cluster and the dedicated IP address that will be used to connect to this specific server (as opposed to the cluster as a whole). This IP address must be a fixed IP address, not a DHCP address. Finally, set the initial state of this host when Windows is started.
Chapter 19  Using Clusters 587

9. Click Finish to start up the NLB service and configure the server into the new cluster.

Adding a Node to an NLB Cluster
To add another node to an existing NLB cluster, follow these steps:

1. Open the Network Load Balancing Manager from the Administrative Tools folder.
2. Right-click the cluster you want to add a node to in the left pane, and select Add Host To Cluster, as shown in Figure 19-8.

3. Enter the name or IP address of the host that will be joined to the cluster in the Connect screen, shown previously in Figure 19-6. Click Connect to connect to the server and bring up a list of network interfaces available. Select the interface that will host the public traffic of the cluster (as opposed to private, node-to-node traffic).

4. Click Next to bring up the Host Parameters screen, shown earlier in Figure 19-7. Here you set the priority for this host of the cluster and the dedicated IP address that will be used to connect to this specific server (as opposed to the cluster as a whole). This IP address must be a fixed IP address, not a DHCP address. Finally, set the initial state of this host when Windows is started.

5. Click Finish to start up the NLB service on the new node and configure the server into the existing cluster. When the node is up and part of the cluster, it shows a status of Converged in the NLB Manager, as shown in Figure 19-9.
Removing a Host from an NLB Cluster

To remove a host from an NLB cluster, follow these steps:

1. Open the Network Load Balancing Manager from the Administrative Tools folder.
2. Connect to the cluster you want to remove a node from by right-clicking Network Load Balancing Clusters in the left pane and selecting Connect To Existing.
3. Right-click the node you want to remove in the left pane, and select Delete Host.

Planning the Capacity of an NLB Cluster

In general, an NLB cluster should contain as many hosts as needed to handle the client load for the applications being run in the cluster. The exception to this would be cases in which the sole function of the cluster is to provide failover tolerance for a critical TCP/IP application—that is, when a single server can handle the load and the second server is there simply for fault tolerance.

The maximum number of hosts in a given cluster is 32. If your application requires more than 32 hosts, you can set up multiple clusters, using round-robin DNS to distribute the load among the clusters. The effective limitation, however, is likely to be the network saturation point. If you do run multiple clusters in a subnet, you should host each on its own network switch to minimize the network bottleneck.

Although fewer and more powerful servers might look cost-effective for a given application, you should consider how the failure of a server will affect the application and the remaining servers. If the remaining servers can’t handle the resulting load, you could potentially have...
a cascading failure, bringing down the entire application. Always provide sufficient server capacity within the cluster to handle the expected load when a single server is down. Also consider ways to limit the load to the application when there has been a failure.

When determining the expected cluster capacity, you also need to consider the application being clustered and the type of load it imposes on the cluster. Plan your servers according to where the limitation and stress will be greatest. Web serving and FTP applications are input/output (I/O) intensive, whereas Terminal Services can be very CPU intensive, depending on the types of applications your user community uses.

**Providing Fault Tolerance**

Although NLB clusters provide overall fault tolerance for your TCP/IP application, they are not a complete solution for all possible failures. Because they are “shared nothing” clusters, there is always some data lag between servers. For fully fault-tolerant, high-availability clustering that can run any application, you should probably use server clustering, which provides the greatest level of fault tolerance.

One thing you can do to improve the overall fault tolerance of the cluster is to make the hard disks fault tolerant, whether physically attached to the server or as Network-Attached Storage (NAS). Both hardware and software RAID solutions are viable options for improving the fault tolerance of an NLB cluster. For more on RAID and fault tolerance in general, see Chapter 18 and Chapter 38.

**Optimizing an NLB Cluster**

Optimizing an NLB cluster calls for clearly understanding where the bottleneck in your clustered application is likely to be. An application such as a Web front end that is essentially a file server, for example, tends to be a heavy user of both disk I/O and network bandwidth, and such an application can be a RAM hog if you’re going to do effective caching. Terminal Services, on the other hand, can put a heavy load on the CPU, and to a somewhat lesser extent, on RAM, depending on your user community. Focus your optimization efforts on the bottleneck and you’ll get the most gain for your effort.

One area that can be a problem is running an NLB cluster in a switched environment without planning your network load carefully. If each of the servers in your cluster is connected to a different switched port, you can easily end up flooding your switched ports because every client request to the cluster passes through all switched ports to which a member of the cluster is attached. Running in multicast mode can exacerbate the problem. If you’re running in a switched environment, you should follow these guidelines:

1. Use a top-quality hub to connect the servers in the cluster to one another, and uplink the hub to a single switched port. If you do use switches, separate each cluster onto its own VLAN.
2. Use unicast mode. If you enabled multicast mode during setup, change it. (You'll need to change this on all servers in the cluster.) It is possible to use multicast mode, but this requires enabling Internet Group Multicast Protocol (IGMP) support, introduced in Windows Server 2003. Given the other limitations multicast mode, however, unicast is preferred.

3. Edit the registry on each of the hosts in the cluster, changing the following key from the default parameter of 1 to 0:

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WLBS\Parameters\MaskSourceMAC

   This change allows the switch to tell which MAC address is really the source of traffic, helping it to do its switching job properly. You'll need to restart the servers after making this change.

---

**Server Clusters**

A server cluster is a group of independent nodes that work together as a single system. They share a common cluster database that enables recovery in the event of the failure of any node. A traditional server cluster uses a jointly connected resource, generally a disk array on a shared SCSI bus or Fibre Channel, which is available to all nodes in the cluster. Each Windows Server 2003 Enterprise Edition node in the cluster must have access to the array, and each node in the cluster must be able to communicate at all times with the other nodes in the cluster.

Windows Server 2003 supports server clusters only on machines running Enterprise Edition or Datacenter Edition. Both editions support up to eight node clusters and can be configured in three different models: single node clusters, single quorum device clusters, and majority node set clusters. We focus on single quorum device clusters in this chapter. Single node clusters are primarily used for creating virtual servers and for proof of concept and development of cluster-aware applications. Majority node set server clusters require specialized support from both the hardware and software vendors involved.

**Server Cluster Concepts**

To understand and implement server clusters, it is important to understand several new concepts and their ramifications, as well as specialized meanings for certain terms.

**Networks (Interconnects)**

A cluster has two distinct types of networks: the *private network* that's used to maintain communications between nodes in the cluster and the *public network* that clients of the cluster use to connect to the services of the cluster. Each of these networks can share the
same network card and physical network cabling, but it is a good practice to keep them separate. This gives you an alternate path for interconnection between the nodes of the cluster. Because the interconnect between the nodes of a cluster is a potential single point of failure, it should always be redundant. The cluster service uses all available networks, both private and public, to maintain communications between nodes.

**Real World  Always Have at Least Two Interconnects**

If you have only a single method of communication in a cluster, the failure of that interconnect has a 50 percent chance (in a two-node cluster) of causing the entire cluster to become unavailable to its clients—hardly why you opted for a highly available technology like clustering. Here's what happens when the nodes of a cluster can no longer communicate. When the communications fail, each node recognizes that it is no longer able to talk to the other nodes of the cluster and decides that the other nodes in the cluster have failed. Each node therefore attempts to take over the functions of the cluster by itself. The nodes are “partitioned,” and as each node attempts to enable itself to take over the functions of the entire cluster, it starts by trying to gain control of the quorum resource (discussed later in the “Types of Resources” section) and, therefore, the shared disk on which the quorum resides. Because only one node is able to gain control of the quorum resource, the other nodes are automatically shut down while the single node attempts to maintain the processes of the cluster. However, because any given node has an equal chance of gaining control of the quorum resource, there's a 50 percent chance in a two-node cluster that the node with a failed network card wins, leaving all the services of the cluster unavailable.

**Nodes**

A node is a member of a server cluster. It must be running Windows Server 2003, Enterprise Edition or Windows Server 2003, Datacenter Edition, and Windows Clustering. It must also be running TCP/IP, be connected to the shared cluster storage device, and have at least one network interconnect to the other nodes in the cluster.

**Groups**

Groups are the units of failover. Each group contains one or more resources. Should any of the resources within the group fail, all fail over together according to the failover policy defined for the group. A group can be owned by only one node at a time. All resources within the group run on the same node. If a resource within the group fails and must be moved to an alternate node, all other resources in that group must be moved as well. When the cause of failure on the originating node is resolved, the group falls back to its original location, based on the failback policy for the group.
Resources
Any physical or logical entity that can be brought online or offline can be a server cluster resource. It must be able to be owned by only one node at a time and will be managed as part of the cluster. The quorum resource is a special resource that serves as the repository of the configuration data of the cluster and the recovery logs that allow recovery of the cluster in the event of a failure. The quorum resource must be able to be controlled by a single node, it must provide physical storage for the recovery logs and cluster database, and it must use the NTFS file system. The only resource type supported for a quorum resource in single quorum device clustering is the Physical Disk resource as shipped with Windows Server 2003 (which along with other resource types are described in the next section), but it is possible that other quorum resource types will be developed and certified by third parties.

Types of Resources
Windows Server 2003 Enterprise Edition includes several resource types; the sections that follow examine each of these resource types and the role they play in a server cluster. The available cluster resource types are as follows:

- Physical Disk
- Dynamic Host Configuration Protocol (DHCP)
- Windows Internet Naming Service (WINS)
- Print Spooler
- File Share
- Internet Protocol Address
- Local Quorum
- Majority Node Set
- Network Name
- Generic Application
- Generic Script
- Generic Service
- Volume Shadow Copy Service Task

Physical Disk
The Physical Disk resource type is the central resource type required as a minimum for all server clusters. It is used for the quorum resource that controls which node in the cluster
is in control of all other resources. The Physical Disk resource type is used to manage a shared cluster storage device. It has the same drive letter on all cluster servers.

**DHCP and WINS**
The DHCP service provides IP addresses and various other TCP/IP settings to clients, and WINS provides dynamic resolution of NetBIOS names to IP addresses. Both can be run as a resource of the cluster, providing for high availability of these critical services to network clients. For failover to work correctly, the DHCP and WINS databases must reside on the shared cluster storage.

**Print Spooler**
The Print Spooler resource type lets you cluster print services, making them fault tolerant and saving a tremendous number of help desk calls when the print server fails. It also ameliorates the problem of people simply clicking Print over and over when there’s a problem, resulting in a long and repetitious print queue.

To be clustered, a printer must be connected to the server through the network. Obviously, you can’t connect the printer to a local port such as a parallel or Universal Serial Bus (USB) port directly attached to one of the nodes of the cluster. The client can address the printer either by name or by IP address, just as it would a nonclustered printer on the network.

In the event of a failover, all jobs that are currently spooled to the printer are restarted. Jobs that are in the process of spooling from the client are discarded.

**File Share**
You can use a server cluster to provide a high-availability file server using the File Share resource type. The File Share resource type lets you manage your shared file systems in three different ways:

- As a standard file share with only the top-level folder visible as a share name.
- As shared subfolders, where the top-level folder and each of its immediate subfolders are shared with separate names. This approach makes it extremely easy to manage users’ home directories, for example.
- As a standalone Distributed file system (Dfs) root. You cannot, however, use a cluster server File Share resource as part of a fault-tolerant Dfs root.

**Internet Protocol Address and Network Name**
The Internet Protocol Address resource type is used to manage the IP addresses of the cluster. When an Internet Protocol Address resource is combined with a Network Name resource and one or more applications, you can create a virtual server. Virtual servers allow clients to continue to use the same name to access the cluster even after a failover.
has occurred. No client-side management is required because, from the client perspective, the virtual server is unchanged.

**Local Quorum**
The Local Quorum resource type is used to manage the system disk on the local node of a single node server cluster. The Local Quorum resource type cannot fail over to another node.

**Majority Node Set**
The Majority Node Set resource type is used to manage cluster configuration data that might or might not reside on a cluster storage device. It is used to ensure that the data remains consistent across nodes that may be geographically dispersed. Only a single Majority Node Set resource can exist in a server cluster.

**Generic Application**
The Generic Application resource type allows you to manage regular, cluster-unaware applications in the cluster. A cluster-unaware application that is to be used in a cluster must, at a minimum:

- Be able to store its data in a configurable location
- Use TCP/IP to connect to clients
- Have clients that can reconnect in the event of an intermittent network failure

When you install a generic, cluster-unaware application, you have two choices: you can install it onto the shared cluster storage, or you can install it individually on each node of the cluster. The first method is certainly easier because you install the application only once for the whole cluster. However, if you use this method you won’t be able to perform a rolling upgrade of the application, because it appears only once. (A rolling upgrade is an upgrade of the application in which the workload is moved to one server while the application on the other server is upgraded and then the roles are reversed to upgrade the first server.)

To give yourself the ability to perform rolling upgrades on the application, you need to install a copy onto each node of the cluster. You need to place it in the same folder and path on each node. This method uses more disk space than installing onto the shared cluster storage, but it permits you to perform rolling upgrades, upgrading each node of the cluster separately.

**Generic Script**
Similar to the Generic Application resource, the Generic Script resource type is used to manage operating system scripts as a cluster resource. The Generic Script resource type provides limited functionality.
Generic Service
Finally, server clusters support one additional type of resource—the Generic Service resource. This is the most basic resource type, but it does allow you to manage your Windows Server 2003 services as a cluster resource.

Volume Shadow Copy Service Task
The Volume Shadow Copy Service Task resource type allows you to create jobs in the Scheduled Task folder that will be run against whatever node is currently hosting a particular resource group, allowing the task to fail over with the resource. As shipped, this resource type is used only to support Shadow Copies of Shared Folders in a server cluster.

Defining Failover and Failback
Windows Server 2003 server clusters allow you to define the failover and failback (sometimes referred to as fallback) policies for each group or virtual server. This ability enables you to tune the exact behavior of each application or group of applications to balance the need for high availability against the overall resources available to the cluster in a failure situation. Also, when the failed node becomes available again, your failback policy determines whether the failed resource is immediately returned to the restored node, maintained at the failed-over node, or migrated back to the restored node at some predetermined point in the future. These options allow you to plan for the disruption caused when a shift in node ownership occurs, limiting the impact by timing it for off-hours.

Configuring a Server Cluster
When planning your server cluster, you’ll need to think ahead to what your goal is for the cluster and what you can reasonably expect from it. Server clusters provide for extremely high availability and resource load balancing, but you need to make sure your hardware, applications, and policies are appropriate.

High Availability with Load Balancing
The most common cluster configuration is static load balancing. In this scenario, the cluster is configured so that some applications or resources are normally hosted on one node whereas others are normally hosted on another node. If one node fails, the applications or resources on the failed node fail over to another node, providing high availability of your resources in the event of failure and balancing the load across the cluster during normal operation. The limitation of this configuration is that in the event of a failure, your applications will all attempt to run on fewer nodes, and you need to implement procedures either to limit the load by reducing performance or availability, or to not provide some less critical services during a failure. Another possibility for managing the reduced
load-carrying capacity during a failure scenario is to have “at risk” users and applications that can be shut off or “shed” during periods of reduced capacity, much like power companies do during peak load periods when capacity is exceeded.

It’s important to quickly take steps to manage load during periods of failure when you configure your cluster for static load balancing. Failure to shed load can lead to catastrophic failure, or such extreme slowdown as to simulate it, and then no one will have access to the cluster’s resources and applications.

**Maximum Availability Without Load Balancing**

The cluster configuration with the highest availability and reliability for critical applications is to run one node of the cluster as a hot spare. This scenario requires that the hot spare node be sufficiently powerful to run the entire load of any other node in the cluster. You then configure all the applications and resources to run on the other nodes, with the one node sitting idle. In the event of failure on one of the primary nodes, the applications fail over to the idle node and continue with full capability. After the primary node is back online it can continue as the new hot spare, or you can force the applications back to the primary node, depending on the needs of your environment.

This scenario provides full and complete fault tolerance in the event of the failure of one of the nodes, but it has the greatest hardware cost. It also does not provide for full and complete fault tolerance in the event of multiple node failures—that would take essentially one hot spare for each primary node. Use this clustering configuration only where your applications or resources are critical and you can afford the extra hardware expense far more than any limits to the load in case of a failure.

**Partial Failover (Load Shedding)**

Another cluster configuration is called load shedding or partial failover. In this configuration, critical applications and resources are designed to fail over to the other nodes in the cluster in the event of a failure, but noncritical applications and resources are unavailable until the cluster is back to full functionality. The critical resources and applications are thus protected in a failure situation, but noncritical ones simply run as though they were on a stand-alone server.

In this configuration, you might, depending on capacity and load conditions, have to configure the noncritical applications and resources on all nodes to be unavailable in the event of a failure on other nodes. This allows you to maintain a high level of performance and availability for your most critical applications while shedding the load from less critical applications and services when necessary. This strategy can be very effective when you must, for example, service certain critical applications or users under any and all circumstances but can allow other applications and users with a lower priority to temporarily fail.
Virtual Server Only
You can create a server cluster that has only a single node, which allows you to take advantage of the virtual server concept to simplify the management and look of the resources on your network. For example, the File Share resource lets you create automatic subdirectory shares of your primary share and control their visibility, a perfect way to handle users’ home directories. Having a single node doesn’t give you any additional protection against failure or any additional load balancing over that provided by simply running a single standalone server, but it allows you to easily manage groups of resources as a virtual server.

This scenario is an effective way to stage an implementation. You create the initial virtual server, putting your most important resources on it in a limited fashion. Then, when you’re ready, you add another node to the server cluster and define your failover and failback policies, giving you a high-availability environment with minimal disruption to your user community. In this scenario, you can space hardware purchases over a longer period while providing services in a controlled test environment.

Planning the Capacity of a Server Cluster
Capacity planning for a server cluster can be a complicated process. You need to thoroughly understand the applications that will be running on your cluster and make some hard decisions about exactly which applications you can live without and which ones must be maintained under all circumstances. You’ll also need a clear understanding of the interdependencies of the resources and applications you’ll be supporting.

The first step is to quantify your groups or virtual servers. Applications and resources that are in the same group will fail over together onto the same server. This means you’ll need to plan out which applications are dependent on each other and will need to function together. Make a comprehensive list of all applications in your environment, and then determine which ones need to fail over and which ones can be allowed to simply fail but still should be run on a virtual server.

Next, determine the dependencies of the applications and the resources they need to function. This allows you to group dependent applications and resources in the same group or virtual server. Keep in mind that a resource can’t span groups, so if multiple applications depend on a resource, such as a Web server, they must all reside in the same group or on the same virtual server as the Web server and thus share the same failover and failback policies.

A useful mechanism for getting a handle on your dependencies is to list all your applications and resources and draw a dependency tree for each major application or resource. This helps you visualize not only the resources that your application is
directly dependent on, but also the second-hand and third-hand dependencies that might not be obvious at first glance. For example, a cluster that is used as a high-availability file server uses the File Share resource. And it makes perfect sense that this File Share resource is dependent on the Physical Disk resource. It’s also dependent on the Network Name resource. However, the Network Name resource is dependent on the IP Address resource. Thus, although the File Share resource isn’t directly dependent on the IP Address resource, when you draw the dependency tree you will see that they all need to reside in the same group or on the same virtual server. Figure 19-10 illustrates this dependency tree.

![dependency tree for a File Share resource]

**Figure 19-10** The dependency tree for a File Share resource

Finally, as you’re determining your cluster capacity, you need to plan for the effect of a failover. Each server must have sufficient capacity to handle the additional load imposed on it when a node fails and it is required to run the applications or resources owned by the failed node.

The disk capacity for the shared cluster storage must be sufficient to handle all the applications that will be running in the cluster and to provide the storage that the cluster itself requires for the quorum resource. Be sure to provide enough RAM and CPU capacity on each node of the cluster so that the failure of one node won’t overload the other node to the point that it too fails. This possibility can also be managed to some extent by determining your real service requirements for different applications and user communities and reducing the performance or capacity of those that are less essential during a failure. However, such planned load shedding might not be sufficient and frequently takes a significant amount of time to accomplish, so give yourself some margin to handle that initial surge during failover.

**Creating a Server Cluster**

Once you’ve thoroughly researched and planned your implementation of server clusters, you’re ready to actually create the cluster. The mechanism to create and manage server clusters is the Cluster Administrator application, part of the Administrative Tools folder.
New Server Cluster

To create a new server cluster, follow these steps:

1. Open the Cluster Administrator from the Administrative Tools folder. Select Create New Cluster from the drop-down list in the Open Connection To Cluster dialog box, as shown in Figure 19-11.

![Figure 19-11 The Open Connection To Cluster dialog box](image)

2. Click OK to launch the New Server Cluster Wizard, shown in Figure 19-12. The New Server Cluster Wizard walks you through testing to see if the cluster can be successfully created. It also gives you an opportunity to correct issues it discovers during the test, and then actually creates the cluster.

![Figure 19-12 The New Server Cluster Wizard](image)

3. Click Next to bring up the Cluster Name And Domain page, as shown in Figure 19-13. The domain is generally already filled in with the current domain. Fill in the name for the cluster. You can make this a name that means something to you, as opposed to your user community, because you'll likely be creating virtual servers for it.
4. Click Next to bring up the Select Computer page, shown in Figure 19-14. Enter the name of the computer that will be the first computer in the new cluster in the Computer Name field.

5. Click Next to bring up the Analyzing Configuration page. The wizard automatically analyzes the configuration and highlights any problems, as shown in Figure 19-15. If the bar is green, the problems it found are nonfatal and you could go ahead and create the cluster. However, you should attempt to correct any problems before proceeding.
6. To view details on the problems found, click View Log. A typical problem is shown in Figure 19-16. You can correct the problem (in this case, one of the network adapters was configured for DHCP, a nonrecommended configuration) and then click Re-analyze to run the analysis again.

7. Once the Analyzing Configuration Wizard gives you a clean bill of health, click Next to open the IP Address page, shown in Figure 19-17. Enter the IP address that will be used by clustering management tools to connect to the cluster.

![Figure 19-15](image1.png)

**Figure 19-15**  The Analyzing Configuration page of the New Server Cluster Wizard

![Figure 19-16](image2.png)

**Figure 19-16**  The Task Details page, showing that one adapter is configured for DHCP
8. Click Next to bring up the Cluster Service Account page shown in Figure 19-18. This can be an existing account or a new account. The account will be given local administrative privileges on all nodes of the cluster. Click Next.

9. The final confirmation page is shown in Figure 19-19. Spend a moment here to verify that this is really what you want to do and that everything agrees with your checklist. You can go back and fix anything before continuing, if necessary, so take the time now now.
10. When you're ready, click Next to start creating the cluster. When the process is complete, you'll see a status page as shown in Figure 19-20. Click View Log to see a log of the process, or click Details to see more detailed steps than those shown. If there were problems, you'll be able to go back and correct them and try again. Click Next.

11. This brings you to the final page of the New Server Cluster Wizard. You can view the log from here by clicking View Log or change from Local Quorum to Majority Node Set by clicking the Quorum button. Click Finish and the New Server Cluster...
Wizard exits, leaving you in the Cluster Administrator application, as shown in Figure 19-21.

Creating a Clustered Resource
Once you have your cluster created, you can take advantage of the management capabilities of Cluster Administrator to create cluster resources. We’ll walk through the steps to create a File Share cluster resource in a new group on a virtual server called HOME. Referring to Figure 19-10, you’ll see the list of dependencies we need to deal with. Although we could put these resources in the main Cluster group, we prefer to group items into more logical units, especially because failover policies are controlled at the group level. Therefore, to create our File Share resource, we’ll need to do the following:

- Create a group to hold the necessary resources
- Create a Physical Disk resource
- Create an IP Address resource
- Create a Network Name resource
- Create the File Share resource

New Cluster Group
To create a new cluster group, follow these steps:

1. Open the Cluster Administrator from the Administrative Tools folder, and connect to the cluster where you will be creating the resource.
2. Right-click the Active Groups folder of the server that will host the File Share resource, and select Group from the New menu, as shown in Figure 19-22.

![Figure 19-22](image)

The shortcut menu to create a new group

3. This opens the New Group Wizard shown in Figure 19-23. Give your new cluster group an appropriate name and description.

![Figure 19-23](image)

The New Group Wizard

4. Click Next to bring up the Preferred Owners dialog box shown in Figure 19-24. This allows you to control which nodes are the preferred owners of this share, and
the order of preference. Select the nodes to be used for this group, and click Add to move them to the right pane. Use the Move Up and Move Down buttons to arrange their order of precedence.

![Preferred Owners dialog box of the New Group Wizard](image)

**Figure 19-24** The Preferred Owners dialog box of the New Group Wizard

5. Click Finish to create the group. The group is created and is initially offline, because it has no active resources associated with it.

**New Physical Disk Resource**

To create a new Physical Disk resource, continue with the following steps:

1. Right-click the group just created and select Resource from the New menu to open the New Resource Wizard, shown in Figure 19-25.

![New Resource Wizard](image)

**Figure 19-25** The New Resource Wizard
2. Fill in the Name and Description fields, and select Physical Disk from the Resource Type drop-down list. The Group should be the one you just created.

3. Click Next to open the Possible Owners page, as shown in Figure 19-26. Specify which machines in the cluster can host this resource.

![Possible Owners page of the New Resource Wizard](image1)

Figure 19-26 The Possible Owners page of the New Resource Wizard

4. Click Next to open the Dependencies page. This will be blank because this is the first resource in this group.

5. Click Next to open the Disk Parameters page, shown in Figure 19-27. The Disk drop-down list will include all Physical Disk resources that can be managed by the cluster service.

![Disk Parameters page of the New Resource Wizard](image2)

Figure 19-27 The Disk Parameters page of the New Resource Wizard
Note The cluster service can manage only basic disks, not dynamic disks, and all partitions on the disk must be formatted with NTFS. Windows Server 2003 server clusters do support volume mount points.

6. Select the disk that will be the Physical Disk resource, and click Finish to create the resource.

New IP Address Resource
To add a new IP address resource, continue with the following steps:

1. Right-click the group just created and select Resource from the New menu to open the New Resource Wizard, shown earlier in Figure 19-25.

2. Fill in the Name and Description fields, and select File Share from the Resource Type drop-down list. The Group should be the one you just created.

3. Click Next to open the Possible Owners page, shown earlier in Figure 19-26. Specify which machines in the cluster can host this resource.

4. Click Next to open the Dependencies page. This will have the Physical Disk resource we just created, but referring to our dependency tree in Figure 19-10, we see that there is no dependency for the IP Address resource type.

5. Click Next to open the TCP/IP Address Parameters page, shown in Figure 19-28. Fill in the IP address and parameters that will be used for this share.

6. Click Finish to create the IP Address resource.
New Network Name Resource
To add a new network name resource, continue with the following steps:

1. Right-click the group just created and select Resource from the New menu to open the New Resource Wizard shown earlier in Figure 19-25.

2. Fill in the Name and Description fields, and select Network Name from the Resource Type drop-down list. The Group should be the one you just created.

3. Click Next to open the Possible Owners page, shown earlier in Figure 19-26. Specify which machines in the cluster can host this resource.

4. Click Next to open the Dependencies page, shown in Figure 19-29. We’ll now see both the Physical Disk and IP Address resources on the list of available resources. By looking at the dependency tree, we see that the Network Name resource has a dependency on the IP Address resource, so select the IP Address resource in the left plane and click Add to move it to the right dependencies pane.

5. Click Next to open the Network Name Parameters page, and enter the name for the virtual server.

6. Click Finish to create the Network Name resource.

New File Share Resource
Finally, we’re ready to create the File Share resource, because we’ve made all the dependencies.

1. Right-click the group just created and select Resource from the New menu to open the New Resource Wizard shown earlier in Figure 19-25.
2. Fill in the Name and Description fields, and select IP Address from the Resource Type drop-down list. The Group should be the one you just created.

3. Click Next to open up the Possible Owners page, shown earlier in Figure 19-26. Specify which machines in the cluster can host this resource.

4. Click Next to open the Dependencies page. We'll now see all three of the resources we've just created. We know that all of them are required for the File Share resource to work, so we'll move them all to the rightmost dependency pane.

5. Click Next to open the File Share Parameters page shown in Figure 19-30.

![Figure 19-30 The File Share Parameters page](image)

6. Fill in the Share Name and Path fields, and add a description in the Comment text box. If you click Finish now, you'll end up with a simple File Share.

7. Click Advanced to open the Advanced File Share Properties dialog box shown in Figure 19-31. Select Share Subdirectories and Hide Subdirectory Shares, and click OK.

![Figure 19-31 Advanced File Share Properties dialog box](image)

8. Click Finish to create the File Share resource, and click OK to acknowledge the success.
9. Finally, right-click the group you created and select Bring Online to make the resource actually online and available.

**Note** The File Share resource will, by default, set the file system permissions to Read Only. Click Permissions in the File Share Parameters screen to change that as required.

### Compute Clusters

As this edition of the book is being written, Microsoft is beta testing a new kind of Windows Server clustering—High Performance Computing (HPC) clusters, also called compute clusters. Unlike NLB or server clusters, compute clusters are not designed to provide high availability for critical applications, but rather to distribute highly parallel and complex computing tasks across multiple nodes. Windows Compute Cluster Server 2003 (CCS) enables super-computer functionality on the desktop.

CCS is a combination of a special version of Windows Server 2003 x64 Edition; the Compute Cluster Edition (CCE); and a package of interfaces, management tools, and utilities known as the Compute Cluster Pack. The Compute Cluster Pack is available separately and can be installed on any x64 Edition of Windows Server 2003, including R2 versions. CCE is at the SP1 level and does not support installation of R2.

**Note** Windows Compute Cluster Server 2003 is supported only on x64 Editions of Windows Server 2003. It is not available on 32-bit Windows Server 2003, nor on Itanium 64-bit editions.

CCS supports configurations that have one, two, or three NICs per node. The preferred configuration is a head node with a public (internal network LAN) interface, a private intra-cluster communications interface, and a high-speed Message Passing Interface (MPI). Each compute node in the cluster would have at least a private communications interface and the MPI interface. Figure 19-32 shows this topology.

CCS includes Remote Installation Services (RIS) that allows the easy setup and deployment of compute nodes on demand. Once the head node is created and configured, individual compute nodes are simply connected to the network and powered up. RIS then deploys Windows Server 2003 Compute Cluster Edition to the new node and configures it to be part of the compute cluster.

CCS includes the Microsoft Message Passing Interface (MS MPI), a highly compatible implementation of the Argonne National Labs MPICH2 specification. Because the MS MPI implementation is completely compatible with MPICH2 at the API level, existing HPC applications that use MPICH2 will easily migrate to CCS.
More Info  For additional information on CCS, including details of MPI, migration of existing parallel applications, and parallel debugging, see http://www.microsoft.com/windowsserver2003/ccs/default.mspx.

Summary

Windows Server 2003, Enterprise Edition provides two high-availability clustering models: Network Load Balancing clusters (formerly known as the Windows Load Balancing Service) and server clusters. Clusters provide a highly available and scalable environment. Network Load Balancing clusters use standard hardware to distribute TCP/IP applications across a cluster. Server clusters use specialized shared disk resources to provide failover and static load balancing for a variety of applications. A new type of Windows Server 2003 cluster, the compute cluster, supports high-performance computing and highly parallel computing tasks. The next chapter covers configuring your storage as well as planning for fault tolerance and flexibility in managing your storage needs.
Chapter 20
Managing Storage

Hard-drive prices have plummeted, capacities have soared, and demand has risen accordingly. While some administrators manage storage crises by simply adding more storage, this approach can lead to an unmanageable amount of storage and devices, complicating backup and archival tasks, and leading to backwaters of the network where vast quantities of data sit unused or where users store their personal music and movie collections, consuming yet more resources.

By managing your storage more wisely, you can manage the growth in storage on the network, avoid storage crises such as file shares that run out of disk space, and increase reliability and performance.

To help manage storage on the network, Microsoft provides new tools in Windows Server 2003 R2, such as File Server Resource Manager, Storage Manager For SANs (storage area networks), and a much more useful and high-performance Distributed File System (DFS), as well as the Windows Server 2003 Removable Storage and Remote Storage tools, which are unchanged since Windows Server 2003.

More Info For information about Shared Folders, see Chapter 10; for information about disk management, see Chapter 18.
Using File Server Resource Manager

File Server Resource Manager (FSRM) is a collection of three tools that provides administrators the ability to view all their local storage resources from a single console, as well as to create and apply policies that control these resources. The three tools included in File Server Resource Manager are

- Storage Reports Management
- Quota Management
- File Screening Management

Specifically, these tools allow administrators of Windows Server 2003 R2 file servers to keep track of storage growth and usage on the local server, as well as create hard or soft policies limiting the amount and type of files that users can save in specific folders.

To use the File Server Resource Manager MMC snap-in (Fsrm.msc) of the File Server Management console (Fs.msc), install or upgrade the File Server role on a server running Windows Server 2003 R2, open the File Server Management console from the Administrative Tools folder, and then use the following sections to apply settings appropriate for your situation.

Note  The File Server Resource Manager can manage only a single server at a time, and it works only on servers running Windows Server 2003 R2 that have the File Server Resource Manager installed. To manage multiple servers, use Microsoft Operations Manager (MOM) in conjunction with the File Server Resource Manager Management Pack.

Setting Global Options

Before you can create notifications in FSRM, you need to specify the e-mail settings. This is also a good time to configure other global options, such as where Windows stores storage reports and whether to audit file screening.

To set global options, right-click File Server Resource Manager in the File Server Management or File Server Resource Manager console, and choose Configure Options.

- Use the E-mail Notifications tab (or the Storept Admin Options command at a command prompt) to specify the e-mail settings:
  - The SMTP server to use when sending storage reports and notifications. This is most likely the server name of a nearby Microsoft Exchange Server.
❑ The administrator e-mail address or addresses to which Windows should send storage reports and notifications by default. (You can specify other addresses when creating storage reports and notifications.)

❑ The e-mail address that File Server Resource Manager should use as the “From” address for e-mails it sends. Use the e-mail address of the server administrator, or another address to which administrators or users can respond if they have questions (for example, about quotas).

❑ Click Send Test E-mail to test the e-mail settings.

■ Use the Storage Reports tab (or the Storreport Reports command) to edit and review storage reports. (You can also do this when creating storage reports, as discussed in the “Scheduling Storage Reports” section of this chapter.)

■ Use the Report Locations tab (or the Storreport Admin Defaults command) to specify where Windows should store storage reports.

■ Use the File Screen Audit tab (or the Filescrn Admin Options command) to enable auditing for files that Windows blocks according to file screens you create (as discussed in the “Screening Files” section of this chapter). To view the audited events, use the File Screening Audit storage report. (See the “Scheduling Storage Reports” section for more information.)

Note Windows stores File Server Resource Manager global settings in the %WINDIR%\system32\srm\defaults\SrmGlobalSettings.xml file.

Scheduling Storage Reports
FSRM supports reporting in Dynamic Hypertext Markup Language (DHTML), HTML, Extensible Markup Language (XML), Comma-Separated Values (CSV) text, or plain text, making it easy to view reports or process them using scripts, Microsoft Excel, or other applications.

File Server Resource Manager includes the following storage reports:

■ Large files
■ Files by owner
■ Files by file group
■ Duplicate files
■ Least recently accessed files
■ Most recently accessed files
Quota usage

File screening audit

To schedule a storage report, use the following steps:

1. In the File Server Management console tree, click File Server Resource Manager, and then click Storage Reports Management.
2. Right-click Storage Reports Management, and choose Schedule A New Report Task. The Storage Reports Task Properties dialog box appears, as shown in Figure 20-1.

3. In the Scope section of the dialog box, click Add to select the local folders that you want to monitor.
4. In the Report Data section of the dialog box, select the reports that you want to generate.
   
   To view the settings for all selected reports, click Review Selected Reports. To adjust the settings for a report, select the report and then click Edit Parameters.
5. In the Report Formats section of the dialog box, select the formats in which you want to generate the reports.
6. Click the Delivery tab, select the Send Reports To The Following Administrators check box, and type the e-mail addresses of the administrators who should receive the storage reports, separating each address with a semicolon.
7. Click the Schedule tab, and then click Create Schedule. The Schedule dialog box appears, which you can use to schedule the storage reports.
8. After you finish creating the scheduled report task, click OK in the Storage Reports Task Properties dialog box. The new scheduled report task appears in the File Server Resource Manager node of the File Serve Management console, as shown in Figure 20-2.

![Figure 20-2](image)

**Figure 20-2** The Storage Reports Management node in the File Server Management console

*Note* You can add or remove reports from multiple storage report tasks by right-clicking Storage Reports Management, and then choosing Add Or Remove Reports For A Report Task.

9. To run the scheduled report immediately, right-click it and choose Run Report Task Now. The Generate Storage Reports dialog box appears, asking whether you want to view the reports immediately or whether File Server Resource Manager should generate the reports in the background for viewing later from the %SystemDrive%:\StorageReports\Scheduled folder.

10. To schedule a storage report from a command prompt, use the **Schtasks /Create** command to create a task in the Scheduled Tasks folder for the report and then use the **Storage Reports Add** command to create the report. For example, open a command prompt window and then type the following commands:

```
Schtasks /Create /S Srv1 /SC Monthly /MO First /D Sun /TN
"Monthly Large Files Storage Report"
/TR "C:\Windows\System32\Storrept.exe Reports Generate /Scheduled /Task:"Monthly Large Files Storage Report"
/RU "SYSTEM"
Storrept Reports Add /Report:LargeFiles
/Task:"Monthly Large Files Storage Report"
/Scope:"E:\Projects|E:\Legal"
/Name:"Monthly Large Files Storage Report"
/Format:DHTML /Remote:Srv1
```
Note When viewing a storage report in DHTML format, you can sort the listing by columns, as long as Internet Explorer can display active content. (You might need to use the Information Bar in Internet Explorer to allow blocked content.)

**Under the Hood  Storage Reports, Snapshots, and Performance**

To create a storage report, Windows creates a Scheduled Task in the Scheduled Tasks folder that uses the Volume Shadow Copy Service to take a snapshot of the specified storage volumes. Windows then creates the storage report from this snapshot using XML style sheets stored in the `%WINDIR%\system32\srm\xslt` folder. This process minimizes the performance impact on the server but does degrade file server performance temporarily.

To minimize the performance impact of storage reports, schedule storage reports outside of normal business hours or during times when few users need to access the server. Consolidate storage report tasks to minimize the number of snapshots Windows must take. (All storage reports in a storage report task use the same snapshot.)

**Using Quota Management**

One way to slow the growth of storage on a network is to limit the amount of disk space each user can utilize on a server. There are two ways of doing this in Windows Server 2003 R2—disk quotas and the Quota Management node of the File Server Resource Manager. Disk quotas allow you to create storage limits on each volume for individual users.

The Quota Management node of the File Server Resource Manager allows you to manage storage at a folder or volume level. You can create quota templates and quotas that Windows automatically applies to subfolders and newly created folders. Unlike disk quotas, quotas that you create using Quota Management look at that actual amount of disk space used by a file, enabling users to reduce their quota consumption by using NTFS compression, and they provide powerful notification capabilities.

Note Quotas that you create using Quota Management apply to all users indiscriminately, unlike disk quotas, which you can apply differentially to individual users and groups. Both types of quotas apply only to a single server. To avoid confusion, do not use both types of quotas on the same server. For more information about disk quotas, see the “Using Disk Quotas” section of this chapter.
Quota Concepts
The following list describes the key concepts involved with Quota Management:

- **Quotas**  Sets the total amount of disk space that a folder and all subfolders can consume. For example, if you create a quota that limits the \Users folder to 2 GB, the contents of this folder and all subfolders cannot exceed 2 GB in size, regardless of the user.

To create a quota, choose Create Quota On Path in the Create Quota dialog box, as discussed later in this chapter.

- **Auto Apply Quotas**  Sets the amount of disk space that each subfolder of the specified folder can consume. For example, if you create an auto apply quota for the \Users folder and set the limit at 2 GB, each subfolder (for example, \Users\Jason; \Users\Sharon) and all files and folders within the subfolder is limited to 2 GB in size. An auto apply quota does not set a limit on the contents of the parent folder, only the subfolders (children). This is useful for quickly setting identical quotas on multiple subfolders, such as user folders or project folders.

To create an auto apply quota, choose Auto Apply Template And Create Quotas On Existing And New Subfolders in the Create Quota dialog box, as discussed later in this chapter.

- **Quota Templates**  Standardizes and centralizes quota and auto apply quota settings, making it easy to apply and update multiple quotas. When you change the settings of a quota template, you can automatically apply the changes to all quotas that use the quota template.

- **Hard and Soft Quotas**  Quotas can use either “hard” limits, which prevent users from exceeding their quotas, or “soft” limits, which merely serve as a warning and notification method.

Performance and Scalability
Quotas reduce the Input/Output (IO) per-second performance of the storage subsystem by a small amount (under 10 percent). Evaluate the performance impact in a test lab or pilot deployment before deploying quotas on a production network. Servers that apply quotas to more than 10,000 folders might experience a larger performance penalty.

Note  Quotas work only on fixed NTFS volumes; you cannot use quotas on removable drives or FAT volumes.
Creating Quotas and Auto Apply Quotas

To create a quota or auto apply quotas, use the following steps. To create a quota template, see the “Creating and Editing Quota Templates” section of this chapter.

1. In the File Server Management console, click File Server Resource Management, and then click Quota Management.

2. Right-click Quotas in the console tree and choose Create Quota.

The Create Quota dialog box appears, as shown in Figure 20-3.

![Figure 20-3 The Create Quota dialog box](image)

3. Click Browse, select the folder to which you want to apply a quota, and then click OK.

4. To create a quota that limits the size of a folder, including all subfolders, select the Create Quota On Path option. To create an auto apply quota that limits the size of subfolders individually (which is useful for setting quotas on the \Users folder), select the Auto Apply Template And Create Quotas On Existing And New Subfolders option.

5. Select the quota template you want to apply, or choose Define Custom Quota Properties and click Custom Properties to create a custom quota. (You cannot create custom quotas for auto apply quotas.) Click Create when you are finished.

6. If you chose to create a custom quota, the Save Custom Properties As A Template dialog box appears. Use this dialog box to save the custom quota as a quota template, or choose Save The Custom Quota Without Creating A Template.
7. To create a quota from a command prompt, use the `Dirquota Quota Add` command. For example, open a command prompt window and then type the following command:

```
Dirquota Quota Add /Path:E:\Users /
SourceTemplate:"200 MB Limit Reports To User" /Remote:Srv1
```

**Best Practices**  Use quota templates instead of creating custom quotas. Using a quota template allows you to make changes to the template that apply to all quotas that are derived from the template. For example, to change the administrator e-mail address for all quotas on a server, edit the appropriate quota templates and then apply these changes to all quotas. This eliminates the need to manually update each quota individually.

**Viewing and Managing Quotas**

Click Quotas in the File Server Management console tree (shown in Figure 20-4) to view or manage existing quotas:

- To filter the display by quota type or path, click the Filter hyperlink and then use the Quota Filter dialog box.
- To disable a quota, select the quota or quotas, right-click the quota, and then choose Disable Quotas. To enable a disabled quota, right-click it and choose Enable Quota.
- To reset the peak usage data for a quota, select the quota or quotas, right-click the quota, and choose Reset Peak Usage. Resetting peak usage data resets notifications for a quota so that users receive another notification the next time they cross a threshold.

![Figure 20-4 The Quotas pane of the File Server Resource Manager console](image-url)
Creating and Editing Quota Templates
Quota templates enable you to quickly apply standardized quota settings, as well as simultaneously update all quotas that make use of a template—when you edit a quota template Windows gives you the option to update all quotas based on the template. To create or edit a quota template, use the following steps:

1. In the File Server Resource Manager console, right-click Quota Templates and choose Create Quota Template, or right-click an existing quota template and choose Edit Template Properties.

   To create a quota template based on an existing quota, right-click the quota and choose Create Template From Quota.

2. To base the template on an existing template, in the Create Quota Template dialog box (shown in Figure 20-5) choose a template from the Copy Properties From Quota Template box and then click Copy.

   ![Create Quota Template dialog box](image)

   **Figure 20-5** The Create Quota Template dialog box

3. Type a name and label for the template in the Template Name and Label boxes.

4. In the Limit box, type the maximum amount of disk space each user can use in the specified folder.

5. Choose Hard Quota to prevent users from exceeding the limit you specify, or choose Soft Quota to use the quota only for monitoring.
6. In the Notification Thresholds section of the dialog box, click Add to create a new notification, or select an existing notification and then click Edit. The Add Threshold dialog box appears (as shown in Figure 20-6).

![Figure 20-6 The Add Threshold dialog box](image)

7. In the Generate Notifications When Usage Reaches box, specify when to notify users.

A typical configuration is to use three notification thresholds, which are often set at 85 percent, 95 percent, and 100 percent.

8. Specify which of the following actions to take when a user exceeds the threshold you specify, and click OK when you are finished:

- Use the E-mail Message tab to send an e-mail notification to a user who exceeds the threshold and/or an administrator. Use the E-mail Message section of the tab to customize the message that Windows generates. Click Additional E-mail Headers to change the From or Reply To addresses so that users can easily reply to the appropriate e-mail address.

- Use the Event Log tab to record a log entry on the server when a user exceeds the threshold.
Part III  Network Administration

- Use the Command tab to run a command or script when a user exceeds the threshold.
- Use the Report tab to generate a storage report when a user exceeds the threshold. See the “Scheduling Storage Reports” section earlier in this chapter for more information about storage reports.

**Note** To insert additional variables in an e-mail message or event log entry, select the variable from the list and click Insert Variable.

9. Click OK when you are finished. If you are editing an existing template, the Update Quotas Derived From Template dialog box appears. Choose one of the following options and then click OK:

- **Apply Template Only To Derived Quotas That Match The Original Template**  Updates quotas based on the quota template only if you have not customized them
- **Apply Template To All Derived Quotas**  Updates all quotas based on the quota template
- **Do Not Apply Template To Derived Quotas**  Does not update any quotas based on the template

10. To create a quota template from a command prompt, use the Dirquota Template Add command. For example, open a command prompt window and then type the following command:

   Dirquota Template Add /Template:"500 MB Limit Reports to User" /Limit:500MB /SourceTemplate:"200 MB Limit Reports To User" /Remote:Srv1

   **Note** To import or export quotas from one file server to another, use the Dirquota Template Export and Dirquota Template Import commands. For example, to export all templates, type Dirquota Template Export /File:C:\QuotaTemplates.xml. To import only a template named 1 GB limit, type Dirquota Template Import /Template:"1 GB limit" /File:C:\Templates.xml.

**Screening Files**

Administrators who use storage reporting tools for the first time are often surprised, and occasionally outraged, over how many audio and video files they find on file servers. In addition to the massive amounts of disk space that audio and video files can consume, companies might be legally liable if users obtained these files illegally or share them with coworkers.
To help administrators control what type of files users can save on a file share, Windows Server 2003 R2 includes File Screening Management, which is a component of the File Server Resource Manager MMC snap-in. File Screening Management enables administrators to block users from saving files with certain file extensions to a specific file share, as discussed in the following sections.

**Controlling Audio and Video Files on Company Servers**

If you are serious about blocking users from saving personal audio and video files on public file shares, or you want to protect the organization from any legal liability arising from users’ MP3 collections, you need two things:

- **An acceptable-use policy that clearly states what users may and may not place on file shares.** This policy should state that users may not save illegally obtained files of any type on company file servers, including audio and video files for which the users does not own a license. You might also want to state that users may save only legally obtained audio and video files to their home directory (on which you create a quota, limiting users to a reasonable amount of disk space). Include information about the penalties for transgressions in the policy, such as termination or probation, and enforce it consistently.

- **A file screen that implements this policy.** One way to get people to follow a company policy is to make it hard for them to violate the policy. A file screen makes it difficult for an average user to violate an acceptable-use policy concerning audio and video files, and it reduces legal liability by demonstrating that the organization is taking active steps to prevent its employees from violating its written policy.

**Creating File Screens**

To create a file screen, use the following steps:

1. In the File Server Management console, click File Server Resource Manager and then click File Screening Management.
2. Click the File Screens container, right-click File Screens in the console tree, and choose Create File Screen. The Create File Screen dialog box appears, as shown in Figure 20-7.

![Create FileScreen](image)

**Figure 20-7** The Create File Screen dialog box

3. Click Browse, select the folder to which you want to apply the file screen, and then click OK.

4. Select the file screen template you want to apply, or choose Define Custom File Screen Properties and then click Custom Properties to create a custom file screen. Click Create when you are finished.

5. If you chose to create a custom file screen, the Save Custom Properties As A Template dialog box appears. Use this dialog box to save the custom file screen as a file screen template, or choose Save The Custom File Screen Without Creating A Template.

6. To create a file screen from a command prompt, use the `Filescrn Screen Add` command. For example, open a command prompt window and then type the following command:

   ```command
   Filescrn Screen Add /Path:E:\Projects /SourceTemplate:"Block Audio and Video Files"
   ```

**Creating Exceptions**

To create an exception to a file screen, use the following steps:
1. Click the File Screens container, right-click File Screens in the console tree, and choose Create File Screen Exception. The Create File Screen Exception dialog box appears, as shown in Figure 20-8.

![Figure 20-8 The Create File Screen Exception dialog box](image)

**Note** You cannot create a file screen exception on a path that already has a file screen or exception.

2. Click Browse, select the folder to which you want to apply the file screen, and then click OK. The folder you select cannot already contain a file screen, but it can be a subfolder of a folder that contains a file screen.

3. Select the file groups that you want to allow, excluding them from any file screens applied to parent folders. Click OK when you are finished to return to the File Screening Management snap-in.

4. To create a file screen exception from a command prompt, use the `Filescrn Exception Add` command. For example, open a command prompt window and then type the following command:

```plaintext
Filescrn Exception Add /Path:E:\Projects\Conventions\Powerpoint /Add-Filegroup:"Audio and Video Files"
```
Creating and Editing File Screen Templates

To create or edit a file screen template, use the following steps:

1. In the File Server Resource Manager console, right-click File Screen Templates and choose Create File Screen Template, or right-click an existing quota template and choose Edit Template Properties.

   To create a file screen template based on an existing file screen, right-click the file screen and choose Create A Template From File Screen.

2. To base the template on an existing template, in the Create File Screen Template dialog box (shown in Figure 20-9) choose a template from the Copy Properties From Template box and then click Copy.

   ![Create File Screen Template dialog box](image)

   **Figure 20-9** The Create File Screen Template dialog box

3. Type a name and label for the template in the Template Name box.

4. Choose Active Screening to prevent users from saving files of the type you specify, or choose Passive Screening to use the file screen only for monitoring.

5. Select the file group or groups that you want to block. To create a new file group, click Create; to edit an existing file group, select the group and then click Edit.

6. Specify which of the following actions to take when a user saves a screened file type, and click OK when you are finished:

   - Use the E-mail Message tab to send an e-mail notification to the user who saved a screened file type, and/or an administrator. Use the E-mail Message section of the tab to customize the message that Windows generates.
Use the Event Log to record a log entry on the server when a user saves a screened file type.

Use the Command tab to run a command or script when a user saves a screened file type.

Use the Report tab to generate a storage report when a user saves a screened file type. See the “Scheduling Storage Reports” section earlier in this chapter for more information about storage reports.

Note To insert additional variables in an e-mail message or event log entry, select the variable from the list and click Insert Variable.

7. Click OK when you are finished. If you are editing an existing template, the Update File Screens Derived From Template dialog box appears. Choose one of the following options and then click OK:

- **Apply Template Only To Derived File Screens That Match The Original Template** Updates file screens based on the quota template only if you have not customized them
- **Apply Template To All Derived File Screens** Updates all file screens based on the quota template
- **Do Not Apply Template To Derived File Screens** Does not update any file screens based on the template

8. To create a file screen template from a command prompt, use the Filescren Template Add command. For example, open a command prompt window and then type the following command: **Filescren Template Add/Template:** "Monitor Image Files" /Type:Passive/Add-Filegroup:"Image Files"

Working with File Groups

A file group is a group of similar file types. For example, the Audio And Video file group includes audio files (with the .MP3, .WMA, and .AAC file extensions), as well as video files (with the .WMV, .MPEG, and .MOV file extensions). The storage reports feature uses file groups when reporting on the types of files present on a file share, while file screening uses file groups to control which files to block. To create or edit a file group, use the following steps:

1. In the File Server Management console, click File Server Resource Manager and then click File Screening Management.
2. Click the File Groups container, right-click File Groups in the console tree, and choose Create File Group. The Create File Group dialog box appears, as shown in Figure 20-10.

![Figure 20-10 The Create File Group dialog box](image)

3. Type a name for the file group in the File Group Name box.

4. Type the file name criteria to include in the file group in the Files To Include box, using asterisks (*) as wildcards, and then click Add. For example, type `*.xml` or `financial*.xml`.

5. To exclude files from the file group, type the file name criteria to exclude from the file group in the Files To Exclude box. Click OK when you are finished.

6. To create a file group from a command prompt, use the Filesrnc Filegroup Add command. For example, open a command prompt window and then type the following command:

   ```
   Filesrnc Filegroup Add /Filegroup:"Financial files"
   /Members:"*.qif | *.mny | *.m12 | *.mbf"
   ```

### Using Disk Quotas

Beginning with Windows 2000, Microsoft provides for either advisory or absolute disk quotas by user or group. Disk quotas are useful for setting quotas on entire volumes, but they do not have the granularity, templates, and notification features that quotas created with Quota Management do.
**Note** Local files in the Recycle Bin count toward the limit just as much as regular files (although shadow copies do not), so users must delete files and empty the Recycle Bin to get below the limit when using files on a local drive.

### Enabling Disk Quotas

By default, disk quotas are turned off for all partitions and volumes. Disk quotas are available only for volumes that Windows assigns a drive letter. Follow these steps to enable disk quotas:

1. Right-click the drive letter in Windows Explorer, and choose Properties.
2. Click the Quota tab (shown in Figure 20-11).
3. Select the Enable Quota Management option.
4. Define the limits on disk usage for this drive letter. The available choices are as follows:
   - **Deny Disk Space To Users Exceeding Quota Limit** Select this option to enforce quotas, or clear it to use disk quotas only for auditing.
   - **Limit Disk Space To** Here you can specify the limits of disk space usage for new users on the volume.
   - **Set Warning Level To** This option indicates the limit at which users receive a warning message.
   - **Select the Quota Logging Options for this Volume** You can choose to log an event in the System event log hourly when users exceed either their usage limit or their warning level.
5. You see a confirmation message. If everything is correct, click OK to scan the drive and enable quotas.

6. To enable disk quotas from a command prompt but not set any options, use the Fsutil Quota Enforce command. For example, open a command prompt window and then type `Fsutil Quota Enforce g:\`

The Fsutil Quota command has limited functionality, so to enable disk quotas and set limits, use the Windows Management Instrumentation Command-Line (WMIC). For example, open a command prompt window and then type the following command:

```
WMIC QuotaSetting Set VolumePath=G:, DefaultLimit=1048576, DefaultWarningLimit=524288, State=2, ExceededNotification=True, WarningExceededNotification=True
```

### Setting Quota Entries for Users

To set disk quotas on administrators (who are otherwise excluded from disk quotas), or to tweak the disk quotas for individual users, you need to perform these additional steps:

1. Right-click the drive you want to set quota entries for, and choose Properties. Click the Quota tab to display the dialog box shown previously in Figure 20-7.

2. Click Quota Entries to display the quota entries for the volume. You see the window shown in Figure 20-12. This window contains entries for everyone who has ever stored files on the volume, unless you have explicitly removed the entries for users who no longer store files there. You can sort by any of the columns or use the Find function to locate a specific entry.

![Figure 20-12 The Quota Entries window](image)

3. To change the properties for any entry, double-click the entry, which displays the dialog box shown in Figure 20-13.
4. To view quota entries from a command prompt, use the Fsutil Quota Query command. For example, open a command prompt window and then type `Fsutil Quota Query G:`.

To modify quota entries from the command prompt, use the Fsutil Quota Modify command. For example, type `Fsutil Quota Modify G: 1048576 2097152 EXAMPLE\Wally`.

**Note** To prevent a large administrative headache, make changes to the disk quotas for an individual only when there is a compelling reason to do so, and then keep careful records so that all administrators have ready access to the information. There is no way to assign disk quotas to groups, though you can create a script that emulates this function.

**Exporting and Importing Disk Quotas**

Windows Server 2003 lets you export the disk quotas from one volume to another, simplifying the setup process for complicated disk quota systems. If a user already has a quota entry, Windows asks whether you want to overwrite it with the imported quota entry for that user (as shown in Figure 20-14). Avoid importing disk quota settings onto an existing drive unless you are changing your overall disk quotas across the entire server. Any customizations you made on the current drive could be lost, and having to acknowledge each change that affects an existing user lends itself to mistakes. In addition, any special limits set for specific users on the source volume will be applied to the target volume.
There are two ways to import disk quotas from one volume to another. You can open the Quota Entries window for the source volume, click Quota, choose Export to save the entry to a file, and then open the Quota Entries window for the target volume and choose Import from the Quota menu. Or you can simply open both Quota Entries windows and drag the entries you want to import from the source window to the target one.

Creating Quota Reports

You can use the Quota Entries window to create reports about disk usage. Select the accounts you want to include in the report and drag them into the reporting tool you’ll be using. The supported formats include Rich Text Format, Comma-Separated Values, CF_UNICODETEXT, and CF_TEXT. If you drag the entries into Microsoft Excel, for example, you get not only the entries but also the column headings. This makes whipping out a disk usage report pretty trivial, though not nearly as trivial as creating a storage report, as discussed earlier in this chapter.

Distributed File System

The Distributed File System (DFS) solution in Windows Server 2003 R2 is a combination of two technologies, DFS Namespaces and DFS Replication, that together provide a fault-tolerant, virtual file system composed of file shares on multiple file servers kept in sync by a WAN-friendly replication algorithm that is vastly more efficient and robust than the file replication service (FRS).

DFS Namespaces replaces the Distributed File System component of Windows Server 2003 and Windows 2000 Server. It allows administrators to group shared folders scattered across the network into a virtual tree of folders called a namespace (as shown in Figure 20-15).

DFS Replication is the successor to the FRS. It allows administrators to replicate folders in a bandwidth-efficient manner using the remote differential compression (RDC) algorithm that replicates only the changed blocks within a file, unlike FRS, which can replicate only complete files.
DFS Namespaces and DFS Replication are useful for the following purposes:

- To organize a large number of file shares scattered across multiple servers into a contiguous namespace so that users can find the files they need
- To improve the availability and performance of file shares, especially in network environments with multiple sites, where DFS Namespaces can redirect users to the closest available server
- To “cache” data at a branch office so that users can access files at a local file server, which then efficiently replicates with a central file server across a WAN connection
- To centralize backup from branch offices by replicating all data from the branch office to a central server that is backed up regularly
- To keep two or more file shares in sync over LAN or WAN links

The DFS Namespaces and DFS Replication features of Windows Server 2003 R2 are much more efficient, robust, and easier to use than the Distributed File System and FRS features in previous versions of Windows. This section discusses only the DFS Namespace and DFS Replication tools included in Windows Server 2003 R2.

**Note** You can use DFS to create a loosely coupled collaboration environment where DFS Replication replicates data between multiple servers. However, DFS Replication does not include the ability to “check out” files, or replicate files that are in use, such as multi-user databases. Therefore, use Windows SharePoint Services in environments where users regularly attempt to edit the same file at the same time from different locations.
Real World  Use DFS for Better Performance and Availability

DFS Namespaces offers better availability and performance than normal shared folders. It does this in three ways. First, DFS Namespaces hides the underlying file shares from users. This enables you to replace servers and shares without affecting the users. For example, to take a server offline, simply change the affected folders in DFS Namespaces to point to another server with a copy of the folder share.

Second, DFS Namespaces supports multiple namespace servers and multiple folder targets for each folder in the DFS namespace. When a user attempts to connect to a domain-based namespace, a domain controller refers the user to the nearest namespace server. When the user connects to a folder with multiple folder targets, the namespace server redirects the user to a server in the same site as the user, or if this is not possible, to the server with the lowest WAN costs (performance or financial). If a server fails, the user is automatically connected to another folder target.

Third, DFS Replication in Windows Server 2003 R2 supports the remote differential compression (RDC) replication algorithm for replicating content between folder targets or namespace servers, greatly reducing bandwidth consumption.

What’s New in DFS for Windows Server 2003 R2

There are quite a few changes in DFS for Windows Server 2003 R2; the following list highlights the most noteworthy ones:

- **Terminology changes.** DFS now refers to both DFS Namespaces and DFS Replication. Additionally, a DFS root is now called a namespace (or namespace root); the root server is now called the namespace server; a link is now called a folder; and a link target is now called a folder target.

- **Drag and Drop DFS namespace restructuring.** You can restructure the namespace by using drag and drop, or you can do it at a command-line using the Dfsutil.exe command.

- **Target priorities and client failback.** You can assign priorities to folder targets in DFS Namespaces so that clients preferentially use or avoid certain servers. Client failback enables clients that have failed over to a secondary folder target to automatically switch back to the primary folder target when it comes back online.

- **DFS Replication replaces FRS in DFS.** Windows Server 2003 R2 uses the new DFS Replication tool, instead of FRS, to replicate DFS folders. However, domain controllers still use FRS to replicate the SYSVOL folder, which contains group policy and scripts.
Remote differential compression (RDC) conserves WAN bandwidth. The new remote differential compression (RDC) algorithm replicates only changed blocks in files, yielding large savings in network bandwidth for files larger than 64 KB.

Standalone DFS namespaces support replicating folders. DFS Replication can enable replication on folders in a standalone namespace, as well as on folders that are not part of a namespace, as long as the folder targets are all members of the same Active Directory forest.

Better reliability. DFS Replication is designed to be reliable and self-healing. Unlike FRS, DFS Replication in most cases automatically handles problems such as USN Journal wraps (as described in Microsoft Knowledge Base article 292438), journal loss, database corruption, and file conflicts. DFS Replication also provides new health reports that make it easy to ascertain whether there are any major problems with replication that DFS Replication cannot handle automatically.

Under the Hood  How DFS Replication Recovers from Corruption

If the DFS Replication database becomes corrupts, DFS Replication stops replication, scans the file system, and re-creates the database. DFS Replication then replicates the rebuilt database with an intact database on a replication member. During this replication process, DFS Replication receives metadata for each file, which is approximately twice the length of the file name plus 144 bytes, along with 5 percent overhead from remote procedure call (RPC) and Transmission Control Protocol (TCP) overhead. For example, if the DFS Replication database contains one million files with an average file length of 50 bytes, DFS Replication on the affected server receives roughly 244 MB of metadata from a replication member with an intact database.

Concepts and Terminology

DFS is a distributed file system, and it uses different terminology than the local Windows file system. The following sections talk about namespace roots, folders in DFS Namespaces, and folder targets, as well as DFS replication.

Note  DFS in Windows Server 2003 R2 refers to both DFS Namespaces and DFS Replication, unlike previous versions of Windows, which use the term "DFS" to describe only the namespace component.
Namespace Roots
The structure of a DFS Namespaces tree in Windows Server 2003 R2 begins with a namespace root (called a DFS root in Windows Server 2003 and Windows 2000 Server), similar to the way the Windows file system starts with a drive. The namespace root is the shared folder that serves as the root for a particular namespace. Because DFS is a virtual file system, the namespace root can be any shared folder on an NTFS partition.

The namespace root can contain normal files and subfolders, though you must use folders (as opposed to file system folders) in DFS Namespaces to create the top levels of your namespace structure. So be careful when designing your folder structure. The server that stores the namespace root is called the namespace server (or host server in Windows Server 2003 and Windows 2000 Server).


There are two types of DFS namespaces: standalone and domain based. A standalone namespace (for example, `\srv\public`) stores all namespace information on the registry of the namespace server instead of in Active Directory. Any server running Windows Server 2003 R2, Windows Server 2003, or Windows 2000 Server can host a standalone namespace, regardless of whether the server belongs to a domain or not (though servers running Windows Server 2003 or Windows 2000 Server do not support all features of DFS Namespaces). Standalone namespaces can host more folders (up to 50,000 folders with targets) than domain-based namespaces (which can hold up to 5000 folders with targets), but the only way to provide redundancy for a standalone namespace root is to use a server cluster. You cannot use multiple namespace servers to host a standalone namespace as you can with a domain-based namespace. However, Windows Server 2003 R2 supports replication for folders in a standalone namespace, unlike earlier versions of DFS, as long as all replication members belong to the same Active Directory forest.

Important DFS Replication is not cluster aware. To use DFS Replication with a server cluster, place replicated folders in local storage of each node.

Domain-based namespace roots (for example, `\example.local\public`) differ from standalone namespace roots in a couple of ways. First, you must host domain-based namespace roots on a member server or domain controller of an Active Directory domain. Second, domain-based namespace roots automatically publish the DFS topology in Active Directory. This arrangement provides fault tolerance and network performance optimization by directing clients to the nearest target, as discussed in the next section.
Choose a standalone namespace if the network does not use Active Directory, if the namespace contains more than 5000 folders with targets, or if you want to host the namespace on a server cluster. Otherwise, choose a domain-based namespace to use multiple namespace servers for redundancy and to take advantage of Active Directory for site-aware client referrals. You can also combine the two—for example, you can create a domain-based namespace that includes a standalone root as a folder.

Before creating namespaces, design the namespace hierarchy in a similar manner to the way you designed the domain structure for the organization. (See Chapter 3 for more information.) Create a namespace structure that is logical, easy to use (by end users!), and matches the organization design, and then get the key stakeholders in the project to sign off on the design. Enlist some representative users from the organization to review the namespace design and provide feedback.

**Note** You cannot use DFS Replication to replicate content between forests.

**Folders**

To add content and provide hierarchical structure to a namespace, use DFS folders. A folder in a Windows Server 2003 R2 namespace can contain other DFS folders (adding depth to the folder hierarchy), or it can contain folder targets that map to file shares. Both types of folders appear to users as normal subfolders of the namespace root, even though they can contain files and subfolders from file shares scattered throughout the enterprise. (See Figure 20-16.)

![Figure 20-16](attachment:image.png)
Targets
Unlike normal folders and file shares, DFS folders can link to identical folders on multiple servers called folder targets (or targets or replicas in Windows Server 2003 and Windows 2000 Server). The user sees only a single, ordinary folder.

DFS clients automatically choose a folder target in their site, if available, reducing intersite network utilization. If more than one target is available on the client’s site, each client randomly selects a target, spreading the load evenly across all available servers. If a target goes down, the client automatically picks a different target. (This process is called *client failover.*) When the original target comes back online, the client automatically switches back to the preferred target if the namespace server and the client support client failback. (See the “Requirements” section for more information.) In this way, targets provide fault tolerance, load balancing, and site awareness. You can use DFS Replication to keep folder targets synchronized.

**Note**  When a user opens a new folder in a DFS namespace, he or she is likely connecting to a new server, which entails some delay. Because of this, it is important to minimize the number of “wrong turns” users make by opening folders that do not contain the files they are looking for. To help users find the data they want with as little delay as possible, establish a consistent and intuitive naming structure for DFS folders, and create a site map at key levels of the namespace.

DFS Replication
Windows Server 2003 and Windows 2000 Server use the file replication service (FRS) to replicate content between DFS target folders, as well as to replicate the SYSVOL share for domain controllers. Windows Server 2003 R2 uses the new DFS Replication feature to replicate content between DFS target folders in a replication group but does not replace FRS for domain controller replication.

A replication group is defined as two or more servers that participate in replication. Replication groups define the replication topology used by members for replication. Target folders that Windows synchronizes using DFS Replication are called *replicated folders.*

DFS Replication, like FRS, is a multimaster replication engine that detects changes in a file by monitoring the update sequence number (USN) journal and replicating the changed file once the file is closed. Unlike FRS, DFS Replication uses a version vector exchange protocol to determine what parts of the file are different, and then uses the RDC protocol to replicate only changed blocks of files larger than 64 KB. This makes DFS Replication much more efficient at replication than FRS, which is particularly important when replicating with servers across a WAN link. DFS Replication does not replicate files that make use of EFS encryption.
Note  You can disable RDC on replication groups that consist largely of small files or that do not use a WAN connection, as discussed in the "Managing Replication Groups" section of this chapter. You can also change the minimum file size that RDC will engage from the 64-KB default size by using the Dfsradmin Connection Set command.

Neither DFS Replication nor FRS support file checkout or merging. If two or more users modify the same file simultaneously on different servers, DFS Replication uses a conflict-resolution method that keeps the most recently modified copy of the file (or the earliest creator when dealing with folders). DFS Replication moves the other copies to a conflict folder on the losing server but does not replicate this folder by default, unlike FRS, so the folder remains on the local server. To avoid conflicts, use Windows SharePoint Services when users in multiple locations need to collaborate on the same files at the same time. (Windows SharePoint Services allows users to check out files.)

DFS Replication can make use of several of topologies: hub and spoke, full mesh, and custom. These topologies are familiar to most network administrators, but here is a quick review:

■ Hub and spoke  This topology is also known as a star topology. Each server replicates with a central server, minimizing the use of WAN links. This topology is similar to an Ethernet network, which uses a hub or switch as the center of the network. Choose this topology to reduce network usage when there are more than 10 members of the replication group, or when members of the replication group are in a site connected via a WAN connection.

■ Full mesh  All servers replicate with all other servers. This topology is the default in Windows 2000 Server for DFS replication. (Replication of SYSVOL uses the Active Directory replication topology.) Choose this topology when there are fewer than 10 servers in the replication group and all links have low enough costs (performance or monetary) to allow each server to replicate with every other server. The Full Mesh topology minimizes the time it takes to propagate changes to all members of the replication group and increases reliability by replicating with all members of the replication group, but it also increases network traffic from replication.

■ Custom  This topology allows you to manually specify replication connections.

Requirements

To use the DFS Namespaces and DFS Replication features of Windows Server 2003 R2, clients must have a DFS client, and servers must run Windows Server 2003 R2 or an appropriate version of Windows Server for the DFS features the network requires. If the network does not support NetBIOS over TCP/IP, there are additional requirements.
DFS Clients
To access the DFS folder structure, you need a DFS client. Table 20-1 shows the level of DFS support by operating system. Users can access file shares that are part of a DFS namespace without a DFS client; however, the user does not benefit from any of the DFS features, such as hierarchical namespaces, multiple folder targets, and site-aware client referrals.

Table 20-1 Operating system support for DFS access

<table>
<thead>
<tr>
<th>Operating System</th>
<th>DFS Client Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Microsoft: Apple MacOS, UNIX, IBM OS/2</td>
<td>None. (Thursby Software ADmitMac provides limited support for DFS on Mac OS X clients.)</td>
</tr>
<tr>
<td>MS-DOS</td>
<td>None.</td>
</tr>
<tr>
<td>Windows 3.x</td>
<td>None.</td>
</tr>
<tr>
<td>Windows 95</td>
<td>DFS standalone client is included; DFS domain-based client is installed with Active Directory client.</td>
</tr>
<tr>
<td>Windows 98</td>
<td>Standalone client is included.</td>
</tr>
<tr>
<td>Windows Me</td>
<td>DFS standalone client is included.</td>
</tr>
<tr>
<td>Windows NT 4 with Service Pack 3 or later</td>
<td>DFS standalone client is included; DFS 5 domain-based client is installed with Active Directory client.</td>
</tr>
<tr>
<td>Windows PE 2005</td>
<td>Standalone client is included.</td>
</tr>
</tbody>
</table>

DFS Servers
Any edition of Windows Server 2003 (including Windows Server 2003 Web Edition) or Windows 2000 server can host a namespace root, either in domain-based mode or standalone mode. However, to use all features of DFS Namespaces and DFS Replication, key servers must run Windows Server 2003 with Service Pack 1 or newer, or in some cases Windows Server 2003 R2. (See the sidebar “Upgrading an Existing DFS Infrastructure” for more information.) To use DFS Replication, all replication members must belong to the same Active Directory forest.

Any computer that Windows can resolve using a Uniform Naming Convention (UNC) path can contribute file shares (DFS folders) to a DFS namespace, including Novell NetWare, UNIX, and Mac OS X. Keep in mind that users need adequate permissions on a share to be able to use it. Clients accessing UNIX and NetWare file shares also need client support for Network File System (NFS) and NetWare, respectively.
Important To replicate through firewalls, open port 135 in the firewalls for use by the remote procedure call (RPC) Endpoint Mapper. (This is the same port used by Active Directory and Microsoft Exchange Server replication.) Alternatively, you can use Dfsrdiag.exe on the replication members to specify a static Remote Procedure Call (RPC) port for DFS Replication, and then open that port on the firewalls instead of port 135. Even though DFS Replication encrypts replicated data, do not send replication traffic over a public network such as the Internet without using a virtual private network (VPN) connection or encrypting the traffic using Internet Protocol Security (IPSec).

Upgrading an Existing DFS Infrastructure

To obtain the full functionality of DFS in Windows Server 2003 R2, you must use Windows Server 2003 R2 on all DFS management servers and DFS replication partners by upgrading or replacing the existing servers with servers running Windows Server 2003 R2. Upgrade or replace all domain controllers and namespace servers (DFS root servers) with servers running Windows Server 2003 with Service Pack 1 or Windows Server 2003 R2. See Chapter 6 for information about upgrading a server, and see Chapter 7 for information about using the Configure Your Server Wizard to upgrade the file server role after installing Windows Server 2003 R2.

However, you do not need to replace the entire DFS infrastructure immediately. Use the following list to upgrade a DFS infrastructure selectively to make use of the new functionality included in Windows Server 2003 R2:

- To manage an existing DFS infrastructure using the new DFS Management console, install DFS Management on a server running Windows Server 2003 R2. Note that some features are unavailable until you upgrade other servers.
- To support client referrals with target priority and client failback, upgrade domain controllers and namespace servers (DFS root servers) to Windows Server 2003 with Service Pack 1 or newer. Domain controllers and namespace servers running Windows 2000 Server do not support site-aware client referrals without additional configuration. For more information, see the DFS Management Help system.
- To use DFS Replication, you must update the Active Directory schema to the Windows Server 2003 R2 revision level, and install Windows Server 2003 R2 and DFS Replication on all replication partners.
- Evaluate whether you need to update or upgrade antivirus software to support DFS Replication.
Using DFS Without NetBIOS or WINS

DFS Namespaces relies on NetBIOS to resolve share names. If your network has NetBIOS over TCP/IP disabled or has eliminated WINS, you need to enable fully qualified DFS names in the registry of each DFS namespace server before creating the DFS namespace. (Do not perform this procedure if you use NetBIOS addressing on your network.)

To do so, follow these steps on every server that will host a DFS root:

1. Open the Registry Editor by choosing Run from the Start menu, typing regedit, and then clicking OK.
2. Open the following registry key:
   \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DFS
3. Change the DFSDnsConfig value to have the value data of 1. (A value of 0 disables fully qualified name resolution.) If the value doesn’t exist, create it using the following information:
   Value Name: DFSDnsConfig
   Data Type: REG_DWORD
   Value Data: 1

Installing DFS Management and DFS Replication

Before you can use DFS Management and DFS Replication, you must install them. To do so, use one of the following methods on a server running Windows Server 2003 R2:

- Use the Manage Your Server window and Configure Your Server Wizard to add or upgrade the File Server role.
- Use the Windows Components Wizard to install the Distributed File System component.
- Use the Sysocmgr.exe command-line tool to automate the installation of the DFS management (DFSFRSUI) and DFS Replication (DFSR) components.

**Note**  You do not need to install DFS on servers that act as folder targets unless the folder targets participate in replication, in which case you must install DFS Replication.

DFS Namespaces

DFS namespaces makes it possible to organize file shares scattered throughout an enterprise into a single, contiguous, and hierarchical namespace. This section discusses how to open or create a new namespace, add namespace servers and DFS folders, change advanced settings, and back up the DFS topology.
Note  If you store the files for an intranet Web site on a shared folder instead of on the local Web server itself, create the Web site in a shared folder, create a DFS folder for the shared folder, and configure Internet Information Services (IIS) to use the DFS folder for the Web site. If you need to take down the server that is storing the shared folder, add a DFS folder target that points to a copy of the shared folder on another server and then remove the existing folder target. This method allows you to change the file share without breaking any hyperlinks.

Creating or Opening a Namespace Root

The first step in working with DFS Namespaces is to create a namespace or open an existing namespace root. To do so, follow these steps:

1. Launch the File Server Management console from the Administrative Tools folder, navigate to DFS Management and then to Namespaces.
2. To open an existing namespace root, right-click Namespaces and choose Add Namespace To Display.
3. To create a new namespace root, right-click Namespaces and choose New Namespace. The New Namespace Wizard appears.
4. On the Namespace Server page, type the name of the server that you want to host the namespace root, and then click Next. If the DFS service is disabled, click Yes in the Warning dialog box to start the DFS service and set its startup setting to Automatic.
5. On the Namespace Name And Settings page, type the name to use for the namespace root. This name appears as the share name to users—for example, \example.local\public.

The New Namespace Wizard creates the namespace root in the %SYSTEM-DRIVE%\DFSRoots\name folder and gives all users read-only permissions. To change these settings, click Edit Settings.

6. On the Namespace Type page (shown in Figure 20-17), choose whether to create a domain-based namespace or a standalone namespace:

   - Select Domain-Based Namespace to store the namespace on multiple servers in Active Directory. An example of a domain-based namespace is \example.local\public.
   - Select the Stand-Alone Namespace option to create the namespace on a single server or server cluster. An example of a standalone namespace is \srv1\public.

8. To create a namespace from a command prompt, use the Dfsutil /Addftroot or Dfsutil /Addstdroot commands. For example, to create the same namespace as shown in Figure 20-17, use the following steps:


   b. Open a command prompt window, and then start the DFS service and set the startup type to Automatic if it is not already by typing the following commands:

      Sc Start Dfs
      Sc Config Dfs Start=Auto

   c. Create a folder and file share for the namespace root by typing the following commands:

      Md E:\Public
      Net Share Public=E:\Public

   d. Create the domain-based namespace root by typing the following command:

      Dfsutil /Addftroot /Server:Srv1 /Share:Public
Adding Namespace Servers

The namespace root is the most important part of the namespace. Without it, clients cannot access any DFS folders. Because of this, the first step in creating a more fault-tolerant namespace is to add namespace servers to the namespace root. If possible, add at least one namespace server on each site where users need access to the DFS namespace.

1. In the DFS Management console, navigate to Namespaces, right-click the domain-based namespace root you want to replicate, and then choose Add Namespace Server.

2. In the Add Namespace Server dialog box, type the path to the namespace server, and then click OK.

   Windows creates the namespace root on the target server in the %SYSTEM-DRIVE%:\DFSRoots\name folder and gives all users read-only permissions. To change these settings, click Edit Settings.

3. If the DFS service is disabled, click Yes in the Warning dialog box to start the DFS service and set its startup setting to Automatic.

4. To add a namespace server to a namespace from a command prompt, create the appropriate shared folder, verify that the DFS service is started and the startup type is set to Automatic, and then use the Dfsutil /Addftroot command. For example, open a command prompt window and then type `Dfsutil /Addftroot /Server:Srv2 /Share:Public`

---

**Note** If you assign more than 16 namespace servers to a namespace, change the namespace polling method to Optimize For Scalability. For more information, see the “Changing Namespace Polling Settings” section of this chapter.
Adding DFS Folders
DFS folders allow users to navigate from the namespace root to other file shares on the network without leaving the DFS namespace structure. To create a DFS folder, follow these steps:

1. Right-click the namespace root to which you want to add a folder, and then choose New Folder. This displays the New Folder dialog box, shown in Figure 20-18.

![Figure 20-18 The New Folder dialog box](image)

2. Type a name for the folder in the Name box. To create a folder that contains other DFS folders, click OK without adding any target folders. This creates a layer of structure to the namespace.

3. To add target folders, click Add, and then type the shared folder's UNC or DNS path in the second text box, or click Browse to browse to the shared folder.

4. Add any additional folder targets and then click OK.

5. If you added multiple folder targets, click Yes in the Replication dialog box to create a replication group for the folder targets, or click No to set up a replication group later (or not at all). If you click Yes, the Replicate Folder Wizard appears with some settings already entered. For more information, see the “Creating a Replication Group” section of this chapter.

6. To create a DFS folder from a command prompt, create the appropriate file shares, and then use the Dfscmd /Map command. (You cannot add DFS folders without folder targets from a command prompt.) For example, open a command prompt window and then type the following commands:

```
Dfscmd /Map \Example.local\Public\Software \\Dc1\Software
Dfscmd /Add \Example.local\Public\Software \\Srv2\Software
```
To publish a DFS folder or namespace root in Active Directory so that users can find the folder or namespace when searching Active Directory for shared folders, right-click the appropriate container in the Active Directory Users and Computers console, choose New, choose Shared Folder, and then type the path of the namespace or DFS folder in the Network Path box.

Changing Advanced Settings

The default settings for DFS Management are appropriate for most installations, but if you need to change advanced namespace settings such as the referral order, to change how namespace servers poll domain controllers for DFS metadata, or to delegate DFS management permissions, use the following sections.

Changing Namespace Referral Settings

To change the cache duration, the order in which domain controllers or namespace servers refer clients to namespace servers and folder targets, or the failback settings for an entire namespace, right-click a namespace root or folder, choose Properties, and click the Referrals tab as shown in Figure 20-19:

![Figure 20-19 The Referrals tab of a namespace Properties dialog box](image)

Next, use the following list to complete the process:

- In the Cache Duration box, specify how long clients should cache referrals before polling the domain controller or namespace server for a new referral.
- In the Ordering Method box, choose how domain controllers and namespace servers should refer clients to folder targets and namespace servers.
Select the Clients Fail Back To Preferred Targets option to make a client switch back to using its preferred server when it comes back online.

The preferred server is based on site and any custom referral ordering settings you specify on folder targets. This setting is supported by clients running Windows XP with Service Pack 2 and the post–SP2 Windows XP client failback hotfix, Windows Server 2003 with Service Pack 1 and the Windows Server 2003 client failback hotfix, and Windows Server 2003 R2. See Knowledge Base article 898900 at http://support.microsoft.com/kb/898900/ for information on how to obtain this hotfix.

Overriding Referral Settings on Individual Folders
DFS folders inherit referral settings from the namespace root unless you specifically override them. To override the referral settings for a folder, right-click the appropriate folder, choose Properties, click the Referrals tab, and then specify the settings you want to override.

To explicitly set a single folder target as the preferred target or set the folder target as a target of last resort, right-click the folder target, choose Properties, click the Advanced tab, select the Override Referral Ordering check box, and then specify the priority for the target folder.

Delegating Management Permissions
DFS Management sets the permissions on the namespace object in Active Directory or in the registry of the namespace server (when using a standalone namespace). To change the ability of users to perform common management tasks, use the following list:

- **Create and manage namespaces**  To view, add, or remove groups who can manage namespaces, right-click the Namespaces node, choose Delegate Management Permissions, and then use the Delegate Management Permissions dialog box, shown in Figure 20-20.

- **Manage individual namespaces and replication groups**  To view groups who can manage a namespace or replication group, select the namespace or replication group, and then click the Delegation tab. To remove management permissions for a group, right-click the group and choose Remove. To give management permissions for the namespace to a group, right-click the namespace, choose Delegate Management Permission, type the name of the group in the Select Users Or Groups dialog box, and then click OK.

- **Create and manage replication groups**  To view, add, or remove groups who can manage replication, right-click the Replication node, choose Delegate Management Permissions, and then use the Delegate Management Permissions dialog box.
changing namespace polling settings

To change how namespace servers poll domain controllers for the latest namespace metadata in a domain-based namespace, right-click the appropriate namespace, choose Properties, click the Advanced tab, and then choose one of the following polling methods:

- **Optimize For Consistency**  Polls the primary domain controller (PDC) emulator for new namespace data every hour and after each change to the namespace. Use this setting when the network contains 16 or fewer namespace servers to minimize the time it takes to propagate namespace changes to all namespace servers. This is the default setting.

- **Optimize For Scalability**  Polls the nearest domain controller every hour for changes to the namespace. Use this setting when the network contains more than 16 namespace servers to reduce the load on the PDC emulator. However, choosing this setting increases the amount of time it takes to propagate namespace changes to all namespace servers. Servers running Windows 2000 Server do not support this setting and continue to use the Optimize For Consistency polling method.

To enable the Optimize For Scalability polling method from a command prompt, use the Dfsutil /Rootscalability command. For example, open a command prompt window, change to the directory in which you placed the Dfsutil.exe file, and then type Dfsutil /Root:Example.local\Public /Rootscalability /Enable.

Backing Up and Restoring the DFS Folder Targets

The DFS Namespaces database for domain-based DFS is stored in Active Directory, and you can back it up and restore it using Active Directory–aware backup methods.
To back up the listing of folder targets for a standalone namespace root, type the following text at a command prompt (replacing ServerName and Namespace with the name of the appropriate server name and namespace root):

```cmd
DFScmd /View ServerName\Namespace /Batch >DFS_backup.bat
```

To restore this DFS structure, re-create the DFS namespace and then run the batch file you created.

---

**Note**  In addition to backing up the DFS topology, back up the contents of the actual file shares routinely. Always test the backup before relying on it. You can use the Dfsradmin ReplicationGroup command to export DFS Replication setting such as replication group members and connections.

---

### DFS Replication

An easy-to-use, fault-tolerant, and high-performance file system is not worth much if the data you want to access is unavailable or out of date. To ensure that files are available to users even if a server goes down, create additional folder targets (as described earlier in this chapter) and use DFS Replication to keep the folder targets in sync. You can also use DFS Replication to synchronize folders that are not part of a DFS namespace—for example, to replicate data from a branch office to a server in the main office that you back up regularly and reliably.

To use DFS Replication, select the DFS Replication node in the File Server Management console, right-click Replication, and choose Add Replication Group To Display to open any existing replication groups, and then use the following sections.

#### Creating a Replication Group

There are two ways to create a replication group using DFS Management. You can add a DFS folder to a new replication group, or you can use the New Replication Group Wizard to create a branch office replication group or a multipurpose replication group.

---

**Important**  Do not create replicated folders on volumes managed by Remote Storage. DFS Replication can cause all remote files to be recalled, and it can cause data loss in this configuration.

---

#### Replicating a DFS Folder

To create a replicated folder in a new replication group that replicates a DFS folder, use the following steps (and to add a folder to an existing replication group, see the “Managing Replication Groups” section of this chapter):

1. Right-click the appropriate folder under the Namespaces node of DFS Management, and choose Replicate Folder. The Replicate Folder Wizard appears.
2. On the Replication Group And Replicated Folder Name page, confirm the name for the replication group and for the replicated folder. (The name for the replication group must be unique on the domain. To add to an existing replication group, use the instructions in the following sections.)

3. On the Primary Folder Target page, select the server that holds the data that you want to use as the seed for the initial replication.

---

**Under the Hood  Conflict Resolution During the Initial Replication**

If other members of the replication group have data in the replicated folders, Windows takes the following actions during the initial replication:

- If an identical file already exists on the target server (any server other than the primary member), the primary member does not replicate the file.
- If a file already exists on a target server but the file is not identical to the version on the primary member, Windows moves the file on the target server to the local conflict folder and then replicates the primary member’s version of the file, even if this file is older than the version on the target server.
- If a file exists on a target server that is not present on the primary member, Windows does not replicate it during the initial replication but does replicate it during subsequent replications to other members, including the primary member.

After the initial replication, the primary member role goes away and replication is multiple-master-based. Do not delete, rename, or move files on the primary member or any member that has already replicated until the first replication is complete. (Look for Event 4104 in the DFS Replication log.) Deleting, renaming, or moving files before the first replication is complete can cause the files to reappear if they existed on a target that had not yet replicated.

---

4. On the Topology Selection page, select one of the following replication topologies:

   - **Hub And Spoke**  Spoke servers replicate with one or two central hub servers. Hub servers replicate with all other hub servers by using the Full Mesh topology, as well as with designated spoke servers. Choose this topology in large network environments and environments with multiple branch offices. This topology requires a minimum of three members.
❏ **Full Mesh** All servers replicate with all other servers. Choose this topology when there are less than 10 servers in the replication group and all links have low enough costs (performance or monetary) to allow each server to replicate with every other server instead of a central hub server.

❏ **No Topology** This option does not specify a topology and postpones replication until you specify a replication topology manually. To specify a replication topology after creating the replication group, right-click the replication group in the DFS Management snap-in and then choose New Topology.

5. On the Hub Members page that appears if you chose the Hub And Spoke topology, specify the hub servers.

6. On the Hub And Spoke Connections page that appears if you chose the Hub And Spoke topology, verify that the wizard lists the proper spoke servers. To change the required hub server with which a spoke member replicates preferentially, or the optional hub member with which a spoke member replicates if the required hub member is unavailable, select the spoke server, click Edit, and then specify the required hub and the optional hub.

7. On the Replication Group Schedule And Bandwidth page, choose when to replicate and the maximum amount of bandwidth you want DFS Replication to use.

   To create a custom schedule, choose Replicate During The Specified Days And Times and then click Edit Schedule. You can create a custom schedule that uses Coordinated Universal Time (UTC) or the local time of the receiving server.

   **Note** Windows uses a hash algorithm to compare files, and it uses the RDC protocol to replicate the differences, unless you disable RDC, as discussed in the “Managing Replication Groups” section of this chapter.

8. On the Review Settings And Create Replication Group page, review the settings, and then click Create. Review any errors and then click Close.

   Windows then replicates topology and replication settings to all domain controllers. A replication group member polls its nearest domain controller regularly. (By default, replication group members perform a lightweight poll every 5 minutes for Subscription objects under the local computer container and a full poll every hour.) It receives the settings after Windows updates the domain controller. To change the replication polling interval, use the Dfsrdiag command.
9. To replicate a DFS folder from a command prompt, use the Dfsradmin command. For example, open a command prompt window and then use the following steps:

a. Create a folder for the DFS Staging folder by typing the following commands on each member of the replication group:

```
Md E:\Documents\DfsrPrivate\Staging
Attrib +H /S /D E:\Documents\DfsrPrivate
```

**Note** Use the Dfsradmin Bulk command or a batch file to perform a list of commands from a text file. See the Companion CD for examples.

b. Create a new replication group by typing the following command:

```
Dfsradmin Replicationgroup New /Rgname:Example.local\Public\Documents
```

c. Add members to the replication group by typing the following commands:

```
Dfsradmin Member New /Rgname:Example.local\Public\Documents
/Memname:Dc1 /Force
Dfsradmin Member New /Rgname:Example.local\Public\Documents
/Memname:Srv1 /Force
```

d. Create a new replicated folder by typing the following command:

```
Dfsradmin Replicatedfolder New /Rgname:Example.local\Public\Documents
/Rfname:Documents
/Replicatedfolderdfspath:\\Example.local\Public\Documents /Force
```

e. Add members to the replicated folder by typing the following commands:

```
Dfsradmin Membership Set /Rgname:Example.local\Public\Documents
/Rfname:Documents
/Memname:Dc1 /Membershiplocalpath:E:\Documents
/Membershipstagingpath:E:\Documents\Dfsrprivate\Staging
/Isprimary:True
/Membershipenabled:True /Force
Dfsradmin Membership Set /Rgname:Example.local\Public\Documents
/Rfname:Documents
/Memname:Srv1 /Membershiplocalpath:E:\Documents\Dfsrprivate\Staging
/Membershipstagingpath:E:\Documents\Dfsrprivate\Staging
/Membershipenabled:True /Force
```

f. Create replication connections by typing the following commands:

```
Dfsradmin Connection New /Rgname:Example.local\Public\Documents
/Connectionsendingmembername:Dc1
/Connectionreceivingmembername:Srv1
/Connectionenabled:True
Dfsradmin Connection New /Rgname:Example.local\Public\Documents
/Connectionsendingmembername:Srv1
/Connectionreceivingmembername:Dc1
/Connectionenabled:True
```
Creating a Branch Office Replication Group

To create a replication group that replicates a single branch server with a single hub server, use the following steps:

1. In the DFS Management snap-in, right-click Replication and choose New Replication Group. The New Replication Group Wizard appears.

   Note Creating replicated folders within an existing replication group is faster than creating a new replication group for each replicated folder because the replication group automatically applies its schedule, topology, and bandwidth throttling settings to the new replicated folder.

2. On the Replication Group Type page, choose Replication Group For Data Collection.

3. On the Name And Domain page, type a name for the replication group that is unique on the domain, specify in which domain to host the replication group, and optionally type a description of the replication group.

4. On the Branch Server page, type the name of the branch server that holds the data that you want to replicate with the hub server.

5. On the Replicated Folders page, click Add, and then use the Add Folder To Replicate dialog box to specify the local folder on the branch server to replicate with the hub server, as shown in Figure 20-21. Click OK when you are finished.

   Figure 20-21 The Add Folder To Replicate dialog box

6. On the Hub Server page that appears if you chose Replication Group For Data Collection on the Replication Group Type page, type the name of the hub server that serves as a replication target for the replicated folders.
7. On the Target Folder On Hub Server page, specify the local folder on the hub server in which you want to place replicated data from the branch server. This folder is usually located in a folder or volume that you back up regularly.

8. On the Replication Group Schedule And Bandwidth page, choose when to replicate and the maximum amount of bandwidth you want to allow DFS Replication to use. To create a custom schedule, choose Replicate During The Specified Days And Times and then click Edit Schedule. You can create a custom schedule that uses Coordinated Universal Time (UTC) or the local time of the receiving server.

9. On the Review Settings And Create Replication Group page, review the settings, and then click Create. Review any errors and then click Close. Windows then replicates topology and replication settings to all domain controllers. A replication group member polls its nearest domain controller regularly. (By default, replication group members perform a lightweight poll every 5 minutes for Subscription objects under the local computer container and a full poll every hour.) It receives the settings after Windows updates the domain controller. To change the replication polling interval, use the Dfsrdiag command.

10. To create a replication group from a command prompt, use the Dfsradmin command. For example, open a command prompt window and then use the following steps:

   a. Create a folder for the DFS Staging folder by typing the following commands on each member of the replication group:

      ```
      Md C:\Data\Utilities\Dfsrprivate\Staging
      Attrib +H /S /D C:\Data\Utilities\Dfsrprivate
      ```

      **Note** Use the Dfsradmin Bulk command or a batch file to perform a list of commands from a text file. See the Companion CD for examples.

   b. Create a new replication group by typing the following command:

      ```
      Dfsradmin Replicationgroup New /Rgname:Utilities
      ```

   c. Add members to the replication group by typing the following commands:

      ```
      Dfsradmin Member New /Rgname:Utilities /Memname:Dc1
      Dfsradmin Member New /Rgname:Utilities /Memname:Srv1
      ```

   d. Create a new replicated folder by typing the following command:

      ```
      Dfsradmin Replicatedfolder New /Rgname:Utilities /Rfname:Utilities
      ```
e. Add members to the replicated folder by typing the following commands:

```
Dfsradmin Membership Set /Rgname:Utilities /Rfname:Utilities
    /Memname:Dc1
    /Membershiplocalpath:C:\Data\Utilities
    /Membershipstagingpath:C:\Data\Utilities\Dfsrprivate\Staging
    /Isprimary:True
    /Membershipenabled:True /Force
Dfsradmin Membership Set /Rgname:Utilities /Rfname:Utilities
    /Memname:Srv1
    /Membershiplocalpath:C:\Data\Utilities
    /Membershipstagingpath:C:\Data\Utilities\Dfsrprivate\Staging
    /Membershipenabled:True /Force
```

f. Create replication connections by typing the following commands:

```
Dfsradmin Connection New /Rgname:Utilities
    /Connectionsendingmembername:Dc1
    /Connectionreceivingmembername:Srv1 /Connectionenabled:True
Dfsradmin Connection New /Rgname:Utilities
    /Connectionsendingmembername:Srv1
    /Connectionreceivingmembername:Dc1 /Connectionenabled:True
```

**Note** You can seed a branch member by backing up the replicated folder on the primary member and then restoring it on a target server before setting up replication. This reduces the amount of data that Windows must send over the WAN connection during the initial replication.

**Creating a Multipurpose Replication Group**

To create a replication group that replicates any number of servers with any number of other servers, use the following steps:

1. In the DFS Management snap-in, right-click Replication and choose New Replication Group. The New Replication Group Wizard appears.
2. On the Replication Group Type page, choose Multipurpose Replication Group.
3. On the Name And Domain page, type a name for the replication group that is unique on the domain, specify in which domain to host the replication group, and optionally type a description of the replication group.
4. On the Replication Group Members page, add the servers on which you want to replicate content.
5. On the Topology Selection page (shown in Figure 20-22), select one of the following replication topologies:

- **Hub And Spoke**  Spoke servers replicate with one or two central hub servers. Hub servers replicate with all other hub servers by using the Full Mesh topology, as well as with designated spoke servers. Choose this topology to reduce network usage when there are more than 10 members of the replication group, or when members of the replication group are in a site connected via a WAN connection. This topology requires a minimum of three members.

- **Full Mesh**  All servers replicate with all other servers. Choose this topology when there are less than 10 servers in the replication group and all links have low enough costs (performance or monetary) to allow each server to replicate with every other server. The Full Mesh topology minimizes the time it takes to propagate changes to all members of the replication group by increasing network usage.

- **No Topology**  This option does not specify a topology, and it postpones replication until you specify a replication topology manually. Use this setting if you want to create a custom topology from scratch instead of modifying an existing topology.

![Figure 20-22 The Topology Selection page of the New Replication Group Wizard](image)

6. On the Hub Members page that appears if you chose the Hub And Spoke topology, specify the hub servers.
7. On the Hub And Spoke Connections page that appears if you chose the Hub And Spoke topology, verify that the wizard lists the proper spoke servers. To change the required hub server with which a spoke member replicates preferentially, or the optional hub member with which a spoke member replicates if the required hub member is unavailable, select the spoke server, click Edit, and then specify the required hub and the optional hub.

8. On the Replication Group Schedule And Bandwidth page, choose when to replicate and the maximum amount of bandwidth you want to allow DFS Replication to use. To create a custom schedule, choose Replicate During The Specified Days And Times and then click Edit Schedule. You can create a custom schedule that uses Coordinated Universal Time (UTC) or the local time of the receiving server.

9. On the Primary Member page, select the server that holds the data that you want to use as the seed for the initial replication. For information about how Windows handles conflict resolution during the initial replication, see the “Replicating a DFS Folder” section of this chapter.

10. On the Folders To Replicate page, click Add, and then use the Add Folder To Replicate dialog box to specify the folder to replicate. Click OK when you are finished.

11. On the Local Path Of Folder On Other Members page, select a replication member that you want to participate in replication of the specified folder, click Edit, and then use the Edit Local Path dialog box to enable replication and specify the local folder on the target server in which to place replicated data from the hub server. Repeat this step for every replicated folder you specify in the Replicated Folders page.

12. On the Review Settings And Create Replication Group page, review the settings and then click Create. Review any errors and then click Close.

Windows then replicates topology and replication settings to all domain controllers. A replication group member polls its nearest domain controller regularly. (By default, replication group members perform a lightweight poll every 5 minutes for Subscription objects under the local computer container and a full poll every hour.) It receives the settings after Windows updates the domain controller. To change the replication polling interval, use the Dfsrdiag command.

More Info To create a multipurpose replication group from the command-line, see the “Creating a Branch Office Replication Group” section of this chapter—the command-line procedure is identical.
Managing Replication Groups

Select a replication group, and then use the Memberships, Connections, Replicated Folders and Delegation tabs of the DFS Management console to manage the replication group, as discussed in the following list:

- Use the following options on the Memberships tab to view and manage the member servers for each replicated folder:
  - To disable a member of the replication group, right-click the member and then choose Disable. Disable members that do not need to replicate a specific replicated folder. Do not disable members temporarily and then enable them—doing so causes roughly one kilobyte of replication traffic per file in the replicated folder, and overwrites all changes on the disabled member. (See the “Conflict Resolution During the Initial Replication” sidebar for more information.)
  - To delete a member of the replication group, right-click it and then choose Delete.
  - To add a member server that participates in replication, right-click the replication group in the DFS Management console, choose New Member, and then use the New Member Wizard to specify the local path of the replicated folders, connections, and schedule.
  - To change the size of the conflict or staging folders or to disable the retention of deleted files, right-click the member, choose Properties, click the Advanced tab, and then use the Quota boxes. The conflict folder stores the “losing” files that Windows deletes when it encounters two versions of the same file during replication as well as the most recently deleted files in the replicated folder, and the staging folder queues replication data.

Note: Click a column heading to change how Windows groups items in the view. To add or remove columns, right-click the column heading and choose Add/Remove Columns.

- Use the following options on the Memberships tab to view and manage the member servers for each replicated folder:
  - To disable a member of the replication group, right-click the member and then choose Disable. Disable members that do not need to replicate a specific replicated folder. Do not disable members temporarily and then enable them—doing so causes roughly one kilobyte of replication traffic per file in the replicated folder, and overwrites all changes on the disabled member. (See the “Conflict Resolution During the Initial Replication” sidebar for more information.)
  - To delete a member of the replication group, right-click it and then choose Delete.
  - To add a member server that participates in replication, right-click the replication group in the DFS Management console, choose New Member, and then use the New Member Wizard to specify the local path of the replicated folders, connections, and schedule.
  - To change the size of the conflict or staging folders or to disable the retention of deleted files, right-click the member, choose Properties, click the Advanced tab, and then use the Quota boxes. The conflict folder stores the “losing” files that Windows deletes when it encounters two versions of the same file during replication as well as the most recently deleted files in the replicated folder, and the staging folder queues replication data.

Note: The default size of the staging folder is 4096 MB, but by increasing the size of the staging folder, you can increase the performance of replication group members that replicate with a large number of replication partners or that contain large files that change often. Look for event ID 4208 in the DFS Replication event log; if this event appears multiple times in an hour, increase the staging folder size 20 percent until the event no longer appears frequently.
To create a report showing the replication health as well as RDC efficiency, right-click the replication group, choose Create Diagnostic Report, and then use the Diagnostic Report Wizard to create the report. (See Figure 20-23 for an example of a health report.)

To verify the replication topology, right-click the replication group and then choose Verify Topology.

---

**Note** RDC increases processor utilization on the server, so you might want to disable it on servers with slow processors or high-speed links, and in environments that replicate only new content or files smaller than 64 KB. To disable RDC on a connection, click the Connections tab, right-click the member, choose Properties, and then clear the Use Remote Differential Compression (RDC) check box. You can also change the minimum file size that RDC engages from the 64-KB default size by using the Dfsradmin Connection Set command. Monitor RDC statistics and CPU utilization before and after disabling RDC to verify that you reduce processor utilization enough to warrant the increased network traffic.

Use the Connections tab to view and manage all replication connections. To add a new replication connection between two members of a replication group, right-click the replication group and choose New Connection. Then use the New Connection dialog box to specify the sending member, the receiving member, the schedule, and whether or not to create a one-way replication connection or two-way connection.
Use the following options on the Replicated Folders tab to view and manage all replicated folders:

- To add a new replicated folder to the replication group, right-click the replication group in the DFS Management console, choose New Replicated Folder, and then use the New Replicated Folder Wizard to specify the primary member and the local folders to replicate.

- To omit certain file types or subfolders from replication, click the Replicated Folders tab, right-click the replicated folder, choose Properties, and then use the File Filter and Subfolder Filter boxes on the General tab.

- To share a replicated folder on the network and optionally add the folder to a DFS namespace, right-click the replicated folder, choose Share And Publish In Namespace, and then use the Share Or Publish Replicated Folder Wizard.

Use the Delegation tab to view and manage administrative permissions. See the DFS Namespaces section of this chapter for information about the Delegation tab.

Note To change the replication polling interval, which controls how often a server checks for updated files, use the Dfsrdiag command.

Overview of Storage Manager For SANs

The Storage Manager For the SANs console in Windows Server 2003 R2 lets small and mid-sized organizations with sophisticated storage needs take advantage of low-cost storage area network (SAN) hardware, without using complicated third-party SAN management software that often requires extensive training and a dedicated SAN administrator. It also enables you to administer SAN subsystems from different vendors from the same management computer while using the same tool (Storage Manager For SANs).

Large enterprises with basic SAN requirements can also benefit from Storage Manager For SANs, however, the tool does not provide the same capabilities as enterprise-level SAN management software. For example, Storage Monitoring For SANs does not provide any built-in notification capabilities, although you can integrate Storage Manager For SANs with Microsoft Operations Manager (MOM) to provide this capability.

More Info SANs are complicated, and their implementation varies greatly from manufacturer to manufacturer. Consult the manufacturer of the SAN subsystem for information about what network topologies and methods of SAN discovery the SAN subsystem supports. For more information about Microsoft support for Internet Small Computer System Interface (iSCSI), or to download the Microsoft iSCSI Initiator or iSNS Server, see the Microsoft Web site at http://www.microsoft.com/WindowsServer2003/technologies/storage/iscsi/default.mspx.
Note To test SAN management tasks in a lab that does not have SAN hardware, use third-party software such as WinTarget from String Bean Software (http://www.stringbeansoftware.com) to create a software-based SAN subsystem on a server running Windows Server 2003.

Advantages and Disadvantages of SANs

SANs offer the following advantages:

- **Better utilization of storage resources** Because a SAN centralizes storage, you reduce the amount of unused disk space scattered across multiple servers in small, unusable chunks. For example, instead of 10 servers with 40 GB of free disk space, a SAN centralizes the storage resources into a single 400-GB chunk of free space, which you can allocate to servers as their needs grow. If a server stops hosting an application and no longer requires the associated disk space, you can allocate it to other servers.

- **Greater reliability** Storage on a SAN subsystem usually is fault tolerant, with redundant hard disks, disk controllers, network or Fibre Channel adapters, and power supplies.

- **Faster performance** SANs use large numbers of high-performance hard disks with various hardware RAID levels, and they often communicate with servers over high-performance connections such as Fibre Channel. Multiple servers use the storage resources, allowing you to scale out to service more requests than a single server or Network-Attached Storage (NAS) device. In addition, SAN subsystems communicate with servers by using low-level data blocks with lower communication overhead than the high-level Server Message Block/Common Internet File System (SMB/CIFS) protocol used by NAS appliances and normal file servers. Centralized storage also makes centralized backup easier and faster because backups use the same high-performance storage network (or sometimes a dedicated network for backups).

However, SANs also have a number of drawbacks when compared to traditional direct-attached storage or NAS devices such as Windows Storage Server appliances. The most relevant drawbacks of SANs are the following ones:

- **Cost and complexity** SAN subsystems are usually more expensive than NAS devices and direct-attached storage. They are also more complex than NAS devices, which are designed to be very simple and easy to use, and direct-attached storage, which has very few settings to configure.
Inability to share a single folder with multiple servers  SANs must allocate storage exclusively to a server or server cluster, unlike NAS devices that can share a folder with any number of clients and servers.

New SAN and NAS devices blur the differences between the technologies, and make it possible to choose hybrid approaches, such as NAS appliances that can connect to iSCSI SAN subsystems, and SAN subsystems that can function either as a SAN subsystem or as direct-attached storage.

Concepts and Terminology

To manage a SAN, it is helpful to understand the basics of how SANs work, as well as the terminology used in Storage Manager For SANs to describe various components of a SAN.

At a basic level, a SAN consists of the following components (as shown in Figure 20-24):

- **SAN subsystem**  This is a specialized server or server appliance that hosts a large number of hot-swappable hard disks for use on the storage network. The hard disks in a SAN subsystem are usually connected using a Fibre Channel, Small Computer System Interface (SCSI), or Serial Advanced Technology Attachment (SATA) connection.

- **Storage network switch**  This is a Fibre Channel or Gigabit Ethernet switch (when using the iSCSI protocol) that connects to the SAN subsystem and any hosts that directly access storage on the SAN subsystem.

- **Hosts**  This refers to servers or server clusters that use storage on the SAN subsystem. Storage assigned to the host appears as a normal hard drive in Windows. Hosts are connected to the storage network switch via a Host Bus Adapter (HBA) or a Gigabit Ethernet network card (when using iSCSI), and to the LAN switch via an Ethernet network card.

- **Management computer**  This refers to the server or servers running Windows Server 2003 R2 that are connected to the SAN subsystem for management purposes. A management computer can be a host server or another server on the storage network.

- **LAN switch**  Connects computers to the organization’s internal network, where other servers and client computers are located.
The SAN subsystem contains numerous hard drives, which Storage Manager For SANs can segment and then allocate to hosts. A portion of a SAN that the SAN subsystem makes available to hosts and management servers is called a logical unit (LU). Hosts cannot directly access an LU. First you must use Storage Manager For SANs (or the SAN subsystem’s management software) to assign an address—the logical unit number (LUN)—to the LU. After you create a LUN, you can use Storage Manager For SANs to assign it to a server, where it appears as a normal hard drive. Like a real hard disk, only one server or server cluster can safely access a LUN at a time. To meet this requirement, you must assign the LUN to a server (when using Fibre Channel to communicate with the SAN subsystem) or to a target (when using iSCSI).

A target is a group of one or more LUNs that you create on an iSCSI subsystem using Storage Manager For SANs or other iSCSI management software. To access a LUN on an iSCSI SAN, the host server or server cluster must log on to the target using an iSCSI initiator (driver). The initiator connects to the target using one or more IP addresses and a port numbers. The combination of an IP address and port number is called a “portal.” See Figure 20-25 for a graphical depiction of an iSCSI SAN.

---

**Note** Windows cannot start from an iSCSI LUN unless you use an iSCSI HBA that supports this functionality.
iSCSI Network Considerations

To maximize the security and performance of an iSCSI SAN subsystem, do the following:

- Use a dedicated network that is physically separate from other networks, and do not bridge it with other networks. Also limit who has physical access to ports on this network, the SAN subsystem, and servers on the storage network.
If you cannot ensure physical security for the storage network, create virtual local area networks (VLANs) with your Ethernet switch, or at the very least, use a separate subnet for the storage network.

Implement mutual Challenge Handshake Authentication Protocol (CHAP) authentication on all storage networks.

Implement Internet Protocol security (IPSec) encryption on any storage network that does not have adequate physical security for the sensitivity of the data on the SAN. When using IPSec, use network interface cards or HBAs with TCP Offload Engines (TOE) on the host servers to reduce processor utilization. Storage Manager for SANs does not currently support IPSec encryption.

Ensure that all devices on the storage network support Gigabit or 10-Gigabit Ethernet connections and Ethernet Jumbo Frames.

Use an Ethernet switch designed for enterprise networks instead of small business or home users.

Configure all NICs to use the highest possible Maximum Transmission Unit (MTU).

Open the correct firewall ports on the SAN subsystem if appropriate—for example, TCP ports 3260, 135, and 1817, and UDP port 67. When using a third-party software SAN subsystem running on Windows Server 2003, enable Security Logging in the Windows Firewall to troubleshoot the appropriate ports. See Microsoft Knowledge Base Article 875357 for more information.

When using iSCSI with a server cluster, use a minimum of three NICs per node. Connect each of the following NICs to a physically separate network:

- **SAN** Connect this NIC to the storage network. To add redundancy, use two NICs or iSCSI HBAs to connect to the storage network.
- **Private/Cluster** Connect this NIC to a switch that connects to the other nodes in the cluster, and nothing else.
- **Corporate** Connect this NIC to the company’s internal network.

### Installing Storage Manager For SANs

Before you can use Storage Manager For SANs, you must perform the following steps:

1. Follow the instructions provided with the SAN subsystem to physically install the hardware and configure it to work on the appropriate network (preferably a dedicated storage network with limited physical access).

2. Setup the host servers. This process includes the following tasks:
   - Installing Multipath IO (MPIO) software on the host if using MPIO with multiple Fibre Channel HBAs or a storage array that uses multiple ports.
Installing iSCSI initiator software on the host if using an iSCSI SAN. The Microsoft iSCSI Initiator is available from the following Web site: http://www.microsoft.com/WindowsServer2003/technologies/storage/iscsi/. To use MPIO with iSCSI, select the Microsoft MPIO Multipathing Support For iSCSI option when installing the Microsoft iSCSI Initiator.

Setting up the clustering service if using the host in a server cluster. (See Chapter 19 for information about clustering.)

Host machines that access the SAN do not need Storage Manager For SANs or Virtual Disk Service (VDS) hardware providers.

Important  You must install MPIO software on a host before you enable MPIO support for that host in Storage Manager For SANs. Failure to do so causes irreversible corruption of the volume.

3. Follow the instructions included with the SAN hardware to install the Virtual Disk Service (VDS) hardware provider (provided by the SAN subsystem hardware manufacturer) on the computer on which you want to manage the SAN.

4. Install Storage Manager For SANs on a management computer running Windows Server 2003 R2 using one of the following methods:

   - Use the Manage Your Server window and Configure Your Server Wizard to add or upgrade the File Server role.
   - Use the Windows Components Wizard to install the Storage Manager For SANs component.
   - Use the Sysocmgr.exe command-line tool to automate the installation of the Storage Manager For SANs component.

Using the Storage Manager For SANs Console

To use the Storage Manager For SANs console, open the File Server Management snap-in, or open the Storage Manager For SANs console (SanMmc.msc) from the Administrative Tools folder. The Storage Manager For SANs console, shown in Figure 20-26, consists of three nodes:

- **LUN Management**  This node is where you can perform all management tasks, such as managing server connections, managing iSCSI targets, creating LUNs, and assigning LUNs to servers.

- **Subsystems**  This node lists all SAN subsystems detected by the Storage Manager For SANs console.

- **Drives**  This node lists all hard disks in all SAN subsystems, and it allows you to blink drive lights or beep drive speakers (if supported by the SAN subsystem hardware).
Managing Server Connections

The first task you must perform before you can create and manage LUNs is to set up SAN Manager with connections to the appropriate SAN host computers, as detailed in the following steps:

1. In the Storage Manager For SANs console on the SAN administration computer, right-click LUN Management and then choose Manage Server Connections. The Manage Server Connections dialog box appears (as shown in Figure 20-27), listing the local server and any servers you add to the management console.
2. To add a server, click Add. In the Configure Server dialog box, type the server name and a description, and then click OK.

3. To add a server cluster, add all servers in the cluster, click Manage Clusters, and then click Add in the Manage Clusters dialog box. In the Add Cluster dialog box, type a name for the cluster, select the servers in the cluster, and then click OK.

**Important** Create the server cluster before adding it to Storage Manager For SANs—Storage Manager For SANs cannot create clusters. If you add servers to a cluster in Storage Manager For SANs that do not have the clustering service properly installed and configured, you will irreversibly corrupt the volume.

4. Select a server and then use the Fibre Channel Ports or iSCSI Initiator tabs, as explained in the following list, to view and enable ports on the server:

   - **Fibre Channel Ports** Windows automatically detects Fibre Channel HBA ports on servers running Windows Server 2003 and lists them on the Fibre Channel Ports tab if the server is on the same physical network as the management computer. To add a Fibre Channel port manually, click Add, type the World Wide Name (WWN) of the port and a description in the Add Port dialog box, and then click OK. Select the check box next to each port to enable communication with a LUN.

   - **iSCSI Initiator** Windows lists any iSCSI initiators it detects on the iSCSI Initiator tab. If the iSCSI initiator name does not appear, click Refresh. If Windows cannot find the iSCSI initiator name, locate the name by running the iSCSI Initiator Control Panel tool on the host computer. Next, type the name in the iSCSI Initiator Name box, and click Refresh.

5. To manage server connections from a command prompt, use the Diskraid command. For example, open a command prompt window and then type the following commands:

   ```
   Diskraid
   List Subsystem
   Select Subsystem 0
   List HbaPort
   Select HBAPort 0
   Detail HBAPort
   ```

**Important** Do not enable multiple Fibre Channel ports for communication with a LUN unless you install and configure MPIO software that is compatible with the HBAs. In addition, do not enable multiple iSCSI initiator adapters unless you also enable MPIO support in the iSCSI initiator. Enabling MPIO before properly configuring the HBAs or iSCSI initiator can cause irreversible corruption of the LUN.
Managing iSCSI Targets

If the SAN subsystem is an iSCSI device, use the following procedure to manage iSCSI targets before creating a LUN:

1. On the Storage Manager For SANs console on the SAN administration computer, right-click LUN Management in the console tree and then choose Manage iSCSI Targets. The Manage iSCSI Targets dialog box (Figure 20-28) appears, listing the storage subsystem and any targets you have already added to the management console.

2. Select a subsystem from the Select A Subsystem To Manage box and then click Add to add a target, or select an existing target and click Edit to change the target’s settings.

3. In the Add Target dialog box, type a descriptive name for the target and then select the portals to enable with this target. Click OK when you are finished.

4. To perform this procedure from a command prompt, use the Diskraid command. For example, open a command prompt window and then type the following commands:

   Diskraid
   Select Subsystem 0
   Create Target Name="SQL Data"
Managing iSCSI Security

Although physically separate storage network provides the best performance and security, it is not always practical. In addition, even a physically separate network is not necessarily secure, and it is a best security practice to enable two-way authentication (where the host authenticates with the SAN hardware and the SAN hardware authenticates with the host). To configure iSCSI authentication, use the following steps:

1. On the Storage Manager For SANs console on the SAN administration computer, right-click LUN Management and then choose Manage iSCSI Security. The Manage iSCSI Security dialog box appears. (See Figure 20-29.)

![Figure 20-29 The Manage iSCSI Security dialog box](image)

2. Use the Targets tab to configure one-way CHAP authentication with the appropriate target or targets.

3. Use the Local Initiator tab to configure CHAP authentication for the iSCSI initiator (which is the second part of mutual CHAP authentication).

4. To manage iSCSI security from a command prompt, use the Diskraid command. For example, open a command prompt window and then type the following commands:

   ```bash
   Diskraid
   Select Subsystem 0
   Select target 0
   CHAP Target Set Secret="password" Initiator
   CHAP Target Remember Secret="password"
   CHAP Initiator Set Secret="password"
   CHAP Initiator Remember Secret="password" Target=0
   ```
Security Alert  Use strong secrets that comply with the password policies of your administrator accounts, and do not leave these passwords in insecure locations such as on sticky notes in the datacenter.

Logging On to iSCSI Targets

Before you can use a LUN on an iSCSI target, the iSCSI initiator must log into the target. You need to do this only once; afterwards, the iSCSI initiator logs in automatically.

1. On the Storage Manager For SANs console on the SAN administration computer, right-click LUN Management in the console tree and then choose Log On To iSCSI Targets. The Log On To iSCSI Target dialog box appears. (See Figure 20-30.)

![Figure 20-30](image)

2. Select the targets that you want to log on to, and then click Log On. To change security or authentication methods, click Manage iSCSI Security.

3. To log on to an iSCSI target from a command prompt, use the Diskraid command. For example, open a command prompt window and then type the following commands:

Diskraid
Select Subsystem 1
Select Target 1
Login Target Iadapter=0
Creating and Deploying Logical Units (LUNs)

To give a server or server cluster storage resources on a SAN, you must first create a LUN and assign it to the server or cluster, as detailed in the following steps. A LUN that you assign to a server or cluster appears on the server just like a normal hard drive.

1. On the Storage Manager For SANs console on the SAN administration computer, click the Subsystems node in the console tree and verify that Storage Manager For SANs lists the storage subsystem on which you want to create a LUN.

2. Right-click LUN Management in the console tree and then choose Create LUN. The Create LUN Wizard appears.

3. On the Subsystem And Type page of the Create LUN Wizard, select the subsystem, and then select the LUN type you want to create: Simple, Spanned, Striped, Mirrored, or Striped With Parity.

   Note
   The LUN types that the Create A LUN Wizard lists correspond roughly to the Redundant Array of Independent Disks (RAID) level used by the SAN subsystem. However, the actual implementation is dependent on the hardware; for example, some SAN subsystems use RAID 1+0 (10) for the Striped With Parity setting, while others use the more standard RAID 5. Consult the hardware manufacturer for details on the RAID levels that the SAN subsystem supports.

4. On the Size And Name page, type a name for the LUN (if the SAN subsystem supports LUN naming), and the size for the LUN.

   Note
   You can extend LUNs by using the extend command, but you cannot shrink LUNs.

5. On the Target Access page that appears for iSCSI subsystems, choose Assign The LUN Now and then choose the target to which you want to assign the LUN. You must assign the LUN to an iSCSI target before you can assign it to a server.

6. On the Server Access page, choose Assign The LUN Now and then choose the server or server cluster to which you want to assign the LUN. You must assign the LUN to a server or cluster before you can create a volume on it or access it from the server or server cluster.

7. On the Create Volume page that appears for Fibre Channel subsystems, optionally create a basic volume on the LUN, assign a drive letter, and format the volume. The Create A LUN Wizard cannot create volumes on remote servers; use the Disk Management snap-in or Diskpart.exe command-line tool to create a volume on a remote server.
8. On the Create New LUN page, click Create LUN. Storage Manager For SANs creates the LUN, assigns it to the server or target you specify, and formats the volume (if you chose to on the Create Volume page). If you cannot access the volume from the host server, open Disk Management, initialize the volume, assign a partition to it, and format it.

9. If you did not assign the LUN to a server in the wizard, do so now by right-clicking the LUN in the Storage Manager For SANs console and choosing Assign LUN. Then use the Assign LUN Wizard to select the server to which you want to assign the LUN. To unassign a LUN, right-click it and choose Unassign LUN.

10. To create a LUN and assign it to a server or an iSCSI target from a command prompt, use the Diskraid command. For example, open a command-prompt window and type the following commands:

```
Diskraid
Select Subsystem 0
Create LUN RAID Size=10GB
Associate Targets 0
Unmask LUN Initiator=iqn.1991-05.com.microsoft:srv4.example.local
```

**Note** It is a best practice to perform a full format of new volumes on LUNs. Although this takes more time than a quick format, it scans the LUN for bad sectors and excludes them from the volume, decreasing the likelihood of volume corruption.

**Extending a LUN**

As long as there is available storage space on the SAN, you can increase (extend) the size of an existing LUN. If the SAN subsystem runs low on available disk space, simply add more hard disks.

To extend a LUN, right-click the LUN you want to extend, Choose Extend LUN, and then use the Extend LUN dialog box to specify a new LUN size. After extending a LUN on a remote server, you must use Disk Manager or the Diskpart.exe command-line tool to extend the file system.

**Removable Storage**

The Removable Storage console is the definitive place to turn if you have major device or media management tasks to do or have problems to address. This section covers its terminology and conventions, and shows how to use it to manage your media and devices.
Concepts and Terminology

Removable Storage has its own language relative to removable devices. In the interest of speaking the same language (and impressing people at cocktail parties), here’s a quick discussion of how Removable Storage handles its tasks, as well as the terminology it uses.

Removable Devices and Libraries

Removable storage collectively refers to removable storage devices and their associated media (tapes or disks) as libraries. Before you purchase a removable storage library to use with Removable Storage, check the Windows Server Catalog Web site at http://www.microsoft.com/windows/catalog/server to make sure Windows Server 2003 fully supports the device. Also check to make sure the program you plan to use the device with supports the class of device.

When you connect a removable storage device to the system, Windows tries to recognize and configure it. When you launch Removable Storage, it performs its own device configuration and attempts to configure all removable storage devices connected to the system.

Important  If you plan to use a robotic media library with Removable Storage and want the library to be automatically configured (trust us, you do), make sure that all drives in the library are connected to the same SCSI (or similar) bus as the drives’ associated media changer and that no other devices reside on this SCSI bus. Also make sure that the library supports drive-element address reporting.

Media Pools

All removable media belong to a media pool, which is a group of media that all have the same properties. Media are available for use by applications only if they belong to the appropriate media pool. Two types of media pools exist: system pools and application pools. All media that are not reserved for use by an application reside in one of the three system media pools. See Table 20-2 for a description of the three system media pools.

Note  The free media pool is where applications look when they need media and no media exists with space available in the application’s pool. Therefore, try to keep some media in the free media pool so that applications can draw from it as necessary.
An application media pool is any media pool that applications create to hold their own media. For example, the Windows Backup program creates its own media pool, as does Remote Storage. Applications can create multiple media pools, or multiple applications can share the same media pool, although most require media to be in their own application pool.

Note Keep the number of media to under 1000 to prevent the Removable Storage database from slowing down.

Removable Storage Media Identification
Removable Storage keeps track of all media that you insert into the removable storage libraries in one of two ways: by using on-media identifiers, or by using barcodes. On-media identifiers are small data stamps that Removable Storage imprints on the media the first time you insert them. The identifier has two parts: a label type and a label ID. The label type identifies the format used on the media, and the label ID uniquely identifies the tape or disk. Removable Storage uses these two identifiers to determine which media pool to place new media in and to keep track of all the media in the system. Table 20-3 shows how Removable Storage deals with recognized and unrecognized labels.

<table>
<thead>
<tr>
<th>Label Type Recognized</th>
<th>Label Type Unrecognized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media placed in import media pool</td>
<td>Media placed in unrecognized media pool</td>
</tr>
</tbody>
</table>

If you have a robotic library that has a barcode reader, you can use it to quickly keep track of all media that goes with the library. Removable Storage can use either the on-media
identifier or the barcode to identify the media, although using the barcode is often much faster than using on-media identifiers because you do not have to mount each piece of media to keep track of it.

Removable Storage handles media with file systems on them (such as CD-ROMs and Zip disks) a little differently than other types of media. The label type for these media is usually the format type (NTFS, FAT, or CDFS), and the label ID is the volume serial number. Additionally, in the case of CD-ROM and DVD media, Removable Storage permits multiple media with the same label ID (such as a CD-ROM tower with multiple copies of the same disc), as the media can function interchangeably.

**Media States**

Removable Storage uses *media states* to figure out the current status of a piece of media, both in terms of the physical state of the media—whether it is being used or sitting idle—and in terms of the media’s availability for additional data (for example, whether the media is full, formatted incorrectly, or reserved by a single program). Removable Storage refers to these two types of media states as physical states and side states.

---

**Note** Libraries and drives also have their own states, but they are self-explanatory and less important than media states.

**Physical States**

Physical states describe the actual physical availability of the media—is the media in the drive, and if so, is it ready to be used? Removable Storage recognizes the following five physical states:

- **Idle** The media is in the library or shelved offline in a changer.
- **In-use** The media is currently in the process of being mounted or dismounted.
- **Loaded** The media is mounted and available for read/write operations.
- **Mounted** The media is mounted but not yet available for read/write operations.
- **Unloaded** The media has been dismounted and can be removed from the drive.

**Side States**

A side is where information is actually stored on a tape or disk, and yes, it does refer to which physical side of the tape or disk on which information is stored. Side states in Removable Storage indicate media use; physical states report media readiness.

Removable Storage uses side states in part to determine which media pool to place the media into. Media pools can hold media only in the same state as the pool—for example, the import pool can contain sides that are currently in only the Imported state, the
unrecognized pool can contain sides only in the Unrecognized state, and so on. The nine side states that Removable Storage uses are as follows:

■ **Allocated**  An application has reserved the side.
■ **Available**  The side is currently available for use by applications.
■ **Completed**  The side is in use but full, so it is unavailable for further write operations.
■ **Decommissioned**  The side is no longer available for use because it has reached its allocation maximum.
■ **Imported**  The side label type is recognized, but the label ID hasn’t yet been cataloged into a media pool by this computer’s Removable Storage tool.
■ **Incompatible**  The formatting of the side is incompatible with the library. Remove the media.
■ **Reserved**  The side is unavailable to all applications except the application that allocated the opposite side. This state applies only to dual-sided media where one side has already been allocated.
■ **Unprepared**  The side has been placed in the free media pool but doesn’t yet have a free media label. This state is temporary and changes to the available side state, barring a problem.
■ **Unrecognized**  Removable Storage cannot recognize the side’s label type and ID.

**Use and Management**

To access Removable Storage (Ntmsmgr.msc) from the Computer Management snap-in, launch the Computer Management snap-in from the Administrative Tools folder on the Start menu, and then expand the storage root in the console tree and select Removable Storage from the tree. Then use this section to manage Removable Storage.

**Managing Libraries**

The tasks involved with managing libraries are all physically oriented: configuring libraries added to the system, enabling and disabling libraries, changing the available media types, working with robotic libraries, and cleaning libraries.

**Inventorying Libraries**

Removable Storage automatically creates an inventory of the media as you insert them into the library (actually, each time a library door is accessed). To change the way Removable Storage updates the media inventory for robotic storage libraries, or to force Removable Storage to recheck the inventory, use the following steps:

1. To inventory the robotic storage library, right-click the library in the Libraries folder of Removable Storage and choose Inventory from the shortcut menu. Removable Storage inventories the library according to the default method specified for the library.
2. To change the default method of inventorying for a library, right-click the library in the Libraries folder of Removable Storage and choose Properties from the shortcut menu. Then choose an option from the Inventory Method drop-down list box, described in Table 20-4.

3. Clear the Perform Full Inventory On Mount Failure check box if you don’t want Removable Storage to conduct a full inventory every time the library fails to mount a tape or disk.

4. To inventory a library from the command-line, use the RSM Inventory command. For example, type RSM Inventory /LF "Archive Python 06408-xxx SCSI Sequential Device" /Afast.

Note Run the RSM View command to obtain the friendly name or GUID to use with other commands. For example, to view the friendly name and GUID for all libraries in the server, type RSM View /TLibrary /GUIDDisplay. Enclose friendly names that contain spaces within quotes when using them in commands, and make sure the quotes are strict ACS1 quotes, not Microsoft Word “smart quotes.”

### Table 20-4  Library inventory methods and their descriptions

<table>
<thead>
<tr>
<th>Inventory Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No automatic inventory is performed.</td>
</tr>
<tr>
<td>Fast</td>
<td>Performs a quick inventory by checking which slots have had media swapped.</td>
</tr>
<tr>
<td>Full</td>
<td>Mounts each media in the library, and reads the media’s on-media identifier. The response can be slow on libraries with a lot of media.</td>
</tr>
</tbody>
</table>

### Setting Door and Inject/Eject Port Timeouts

All libraries have at least one inject/eject port that is used for inserting and removing media from the library, and robotic libraries also often have a door that can be opened to directly access media in a particular drive. To set the amount of time allowed before Removable Storage times out the port or door, thereby preventing further operations with it, follow these steps:

1. Right-click the library you want to configure, and then choose Properties from the shortcut menu.

2. Click the Components tab, and then type a timeout period in minutes for the library door (if available) and inject/eject ports.
To open a library door, right-click the library and then choose Door Access from the shortcut menu. When prompted, you can open the door and access the media. (You have until the door timeout period expires.) However, whenever you open the library door, Removable Storage needs to perform a full inventory unless you use a barcode reader. Therefore, it is preferable to use the inject/eject port in most circumstances.

Enabling and Disabling Individual Drives in a Library
If you have a storage library with multiple drives, you can disable or enable individual drives as needed. To do this, follow these steps:

1. Select the library containing the drive you want to configure, and then double-click Drives.
2. Right-click the drive you want to enable or disable, and then choose Properties from the shortcut menu.
3. Clear the Enable Drive check box in the General tab to disable the drive.

To enable or disable a removable storage library (making the library unavailable for use by applications), right-click the library you want to enable or disable, choose Properties, and then select or clear the Enable Library check box.

Cleaning Libraries
Most removable storage libraries need to be cleaned—maybe once a week or more depending on their use and the type of drive. Because of this ongoing need, Removable Storage makes it easy to clean the drives and keep track of when you last did so.

- To clean a robotic library, right-click the library you want to clean and choose Cleaner Management from the shortcut menu. Then use the Cleaner Management Wizard to clean the drive.
- To clean a standalone library, manually insert the cleaning tape and clean the drive as instructed by the drive manufacturer or the tape manufacturer. When you are finished, right-click the drive you cleaned in the pane on the right and choose Mark As Clean from the shortcut menu.

Managing Media Pools
Handling media pools is the most important task you perform with Removable Storage. Applications draw from either the free media pool or one or more application media pools when they require media.
Note To move a piece of media from one media pool to another, drag the media from its current location to the media pool in which you want to store it.

Creating Media Pools
Most of the time Removable Storage and your applications create all the media pools you need, but there might be times when you want or need additional pools. To create additional media pools, follow these steps:

1. Right-click Media Pools (or a media pool that can contain other media pools to create a child media pool), and then choose Create Media Pool.

2. In the Create A New Media Pool Properties dialog box shown in Figure 20-31, type a name and description for the media pool.

3. Select Contains Media Of Type option, and choose the appropriate media type.

4. Select the Draw Media From Free Media Pool check box to take media from the free media pool when no media are available in this media pool. Select the Return Media To Free Media Pool check box to return media to the free media pool when it is no longer needed.

5. To change the permissions for the media pool, click the Security tab and assign the appropriate access permissions for the media pool.

6. To create a media pool from the command-line, use the RSM CreatePool command. For example, type RSM CreatePool /M"8mm Backup" /TF"8mm AIT" /Anew.
Note You can create a media pool to hold different types of media—perhaps for a backup program that needs access to the tape drive as well as a magneto optical (MO) drive. To do this, create a media pool that stores other media pools, and then open the new media pool and create a child media pool for each media type you want to use.

Deleting Media Pools
When an application media pool is no longer required—either you uninstalled it or you no longer use the application for which you created the media pool—you might want to delete it. To do so, move all media in the media pool you want to delete into another media pool, select the media pool you want to delete, and then click the Delete toolbar button.

Managing Physical Media
Physical media—tapes or disks—are the reason storage libraries and media pools exist. Actually dealing with the physical media is pretty easy, and the kind of tasks involved include inserting and ejecting media, mounting and dismounting media, enabling and disabling media, and moving media between media pools. This is simple stuff, but a quick review might be useful.

Injecting and Ejecting Media
Use Removable Storage to handle injecting and ejecting media into robotic storage libraries instead of using the device’s physical buttons or ports. Injecting (inserting) and ejecting media in standalone drives is simple: to inject, place the media in the drive; to eject, press the eject button.

To inject media from a storage library, right-click the library and choose Inject from the shortcut menu. To eject a tape or disk from the storage library, right-click the media you want to eject, and then choose Eject from the shortcut menu.

Mounting and Dismounting Media
When you insert a piece of media in a library, the media is in the Idle state and cannot be immediately accessed by an application. To use a piece of media, Windows must first mount the media, which puts it in the Loaded state. Most applications automatically mount the media as needed; however, you can also manually mount media. To do so, right-click the media and then choose Mount from the shortcut menu.

To eject a piece of media, the media must be idle. Normally if an application is finished accessing the media, the media returns to the Idle state; however, if the media is currently in the Loaded state and you need to eject the media immediately, you have to manually dismount the media before you eject it. To dismount the media, right-click the media and then choose Dismount from the shortcut menu.
Chapter 20  Managing Storage  685

Note  To make a particular piece of media unavailable for use, eject it and store it somewhere. To keep the media in the library and prevent applications from using it, right-click the media in Removable Storage, choose Properties, and then clear the Enable Media check box.

Using the Work Queue
The work queue is a list of all activities that have been performed in Removable Storage. It acts in much the same way as the Windows event log does, except that the work queue lists actions that need to be performed as well as completed actions. To view the work queue or the operator requests list, select Work Queue from the console tree in the Removable Storage MMC snap-in. At this point, you can perform the following tasks:

■ To view any additional information about an action, such as additional error messages on failed actions, right-click the action and choose Properties from the shortcut menu.

■ To cancel a pending action, right-click the action and choose Cancel Action from the shortcut menu.

■ To adjust the priority of a pending action, right-click the pending action and choose Reorder Mounts. Removable Storage displays the Change Mount Order dialog box.

■ To move the request to the beginning of the queue, select the Move To The Front Of The Queue option.

■ To move the request to the end of the queue, select the Move To The End Of The Queue option.

■ To specify exactly which place in the queue the request should be, select the Make It Number option and select the number in the queue that you want the request to be.

Working with Operator Requests
Operator requests occur when an action requires direct operator intervention, such as the insertion of offline media or the need for a new cleaning cartridge. When an operator request occurs, the system displays a message indicating that a specific action is required. Perform the action, and click OK to resolve the request. The following actions are possible:

■ To refuse the request or manually mark the request as completed, select Operator Requests in the Removable Storage console tree, right-click the pending operation, and choose Refuse from the shortcut menu to cancel the request, or choose Complete after fulfilling the request.
To modify how long Removable Storage keeps old operator requests, right-click Operator Requests in the console tree, choose Properties from the shortcut menu, and then use the Operator Requests Properties dialog box to change these settings.

To change how Removable Storage notifies you when an operator request is due, right-click the Removable Storage root in the console tree, choose Properties, and then set the values for the Display Operator Request Dialogs and Use Status Area Icon For Notifying About Mounts check boxes.

---

**Remote Storage**

Like money and RAM, you can never have too much hard disk space. Because of this universal truth, Windows Server 2003 and Windows 2000 include the ability to extend hard disk capacity using tape and magneto-optical media. Remote Storage does this by transparently migrating infrequently used files to tape while keeping them easily accessible.

Users see migrated files as if they were still stored on the disk instead of on tape, the only noticeable differences are a small dialog box informing them that the file is being recalled from tape and of a longer file load time. Remote Storage performs all migration and recovery from tape automatically (unless the required media is offline, in which case Removable Storage places a request for an operator to retrieve the media).

The following sections examine key concepts and requirements of Remote Storage, its setup and configuration, and its data recovery and protection.

---

**Real World  Disk-Based Solutions vs. Remote Storage**

Tape drives have been hard hit by the shrinking costs and growing capacities of hard-disks, especially as new backup-to-disk and hierarchical storage solutions that use inexpensive Serial ATA (SATA) hard drives come to market. Many companies choose not to use remote storage and simply buy more hard drives or hierarchical storage solutions that migrate infrequently used files to inexpensive disk subsystems that are backed-up less frequently.

You can also use the storage reports feature of the File Server Resource Manager console to create a crude disk-based archival script. To do so, create a Least Recently Accessed Files storage report that outputs the report in a format that your script can parse, and then use a script to read the file listing in the report and move old files to an archival disk array, and optionally create shortcuts to the files on the archival array.

However, if your company needs to archive large quantities of data that users access infrequently, Remote Storage in conjunction with large-capacity robotic tape or magneto-optical libraries remains unmatched.
Concepts and System Requirements

You probably have some questions about the purpose of Remote Storage: How does it interact with other programs such as the backup program and antivirus program? What kind of hardware and software do you need to make it work? Here is some background you can use to answer those nagging questions.

Overview

Remote Storage allows for two tiers of data storage. The first tier, local storage, is the standard hard disk or removable disk drive hosting an NTFS volume. The second tier, remote storage, is the tape drive or robotic tape library. Data is initially stored in local storage, and after the data has settled down (has not been accessed within a specified period), it is copied or migrated to remote storage but also left intact, or cached, in local storage for quick access. When it becomes necessary to free up space in local storage for additional data, Remote Storage removes files from local storage that it has migrated to remote storage and replaces them with placeholders (links to the files in remote storage). These placeholders (shown in Figure 20-32) look and act the same as normal locally stored files, except for a few differences.

Note Remote Storage does not follow DFS folder targets and is incompatible with DFS Replication.

Figure 20-32  Windows Explorer in Icon view displaying remote storage placeholders

The differences between these placeholders and normal locally stored files are as follows:

- Windows uses an icon with a small clock face on it to indicate that the file is in remote storage, and to open the file, a user must wait while Windows retrieves the file.
■ Windows Explorer subtracts remote files from disk space estimates, and it does not count them against quotas created with Quota Management. However, Windows does count files in remote storage against disk quotas, and it displays the size of the file the same regardless of whether the file is in remote storage or local storage.

■ Windows Explorer also adds a Remote Storage tab to the Properties dialog box of managed volumes, allowing administrators to view and change the settings on managed volumes directly from within Windows Explorer.

When a user accesses a file in remote storage, the Recalling From Remote Storage dialog box appears. (See Figure 20-33.) If a user does not want to wait for the file, he or she can click Cancel and leave the file in remote storage. Otherwise, Windows copies the file into local storage and resets its last-accessed-date timestamp, preventing Windows from migrating the file back to remote storage until the file settles down.

![Figure 20-33 The Recalling From Remote Storage dialog box](image)

Windows does not recall placeholders that you rename or move to a different location on the same volume. However, when a user copies the file, Remote Storage recalls the file and then copies it to the new location. Note that the new file is in not linked to the old file in remote storage, just as you would expect from a copied file. When a user moves a placeholder to a different volume, Remote Storage recalls the file, copies it to its new location, and then deletes the original file.

**Program Compatibility**

Some programs might not behave optimally unless they are specifically written to be Remote Storage–aware. Two examples are backup programs and antivirus programs.

Backup programs that are not Remote Storage–aware can back up all locally stored data and data links, but they have no way of backing up data that has been moved to remote storage, except by restoring the remotely stored files, rendering Remote Storage useless. If a backup program is Remote Storage–aware (such as the Windows 2000 and Windows Server 2003 Backup program), you might have the option to retrieve files from remote storage and back them up along with all locally stored data, and then return the files to remote storage when finished.
Many antivirus, backup, search, and indexing programs that are not Remote Storage-aware have a nasty tendency to access every file they check, thereby resetting Remote Storage usage data, as well as pulling files from remote storage to check them for viruses. Remote Storage-aware programs do not have this liability.

**Important**  Microsoft Office 97 causes Windows to recall all Word documents, PowerPoint documents, and HTML files in remote storage at the end of Office 97 installation. You can stop this by terminating the Findfast.exe process. Turn FindFast off by using the FindFast Control Panel tool and by making sure the Findfast.exe shortcut isn’t in the Startup folder on the Start menu.

Fortunately, Remote Storage has a workaround for programs that are not Remote Storage-aware. Remote Storage limits the allowable number of successive recalls from remote storage. If a program recalls a file from remote storage and requests another file from remote storage within 10 seconds of the last file, Remote Storage counts this. When the count reaches a configurable limit (the default is 60), Remote Storage prohibits further recalls during that session. Setting a limit does not usually bother normal users, but doing so can prevent an antivirus program that is not Remote Storage-aware from inadvertently restoring all remote storage files.

**Important**  DFS Replication and FRS are not Remote Storage-aware. Do not enable Remote Storage on a volume that contains folders replicated by DFS Replication or FRS.

**Data Safety**
Most companies perform regular backups of the local storage systems and make copies of Remote Storage’s media. Thus, every time you back up the local storage, you make a copy of the Remote Storage media and keep that with the local storage backup. This ensures that the entire storage system is backed up—both the local storage tier and the remote storage tier.

Another way to protect data is by using a Remote Storage-compatible backup program to back up data in remote storage along with the local storage backup. The recovery process is the same as that for any other type of backup.

To thoroughly protect your data, use a strategy similar to the following one (and for more specific information, see the “Data Recovery and Protection” section later in this chapter):

- Back up the local data regularly.
- Validate local volumes managed by Remote Storage regularly.
Make more than one copy (up to three) of the Remote Storage media master, and regularly synchronize these copies with the media master each time you perform a full backup.

Optionally, take a media copy and add it to the backup set (as described later in this chapter). This allows you to keep the complete data together, and removes the limitation of three media copies.

Back up data in remote storage at the same time as you back up local storage. It might take longer and use more media, but it offers greater data protection and flexibility in case of a disaster.

**Important** Although Remote Storage media is not the easiest type of media from which to extract data, it is not a difficult operation to accomplish for an unsavory individual with a stolen Remote Storage tape. Always store backup media in a physically secure location.

**System Requirements**
Remote Storage supports only SCSI-class magneto-optical disks, 4 mm (DAT), 8 mm, and DLT tape libraries that Removable Storage recognizes. It does not support QIC tape libraries, CD-RW, writeable DVD formats, or any type of removable disk drive (Jaz, Zip, and so on). If you are thinking about any of these unsupported formats, you probably do not need Remote Storage—you need additional hard disks.

**Important** Remote Storage will not fail over on a server cluster.

**Setup and Configuration**
The following sections explain how to set up Remote Storage, how to configure it optimally, and how to protect your data from disaster.

**Note** Remote Storage does not detect devices installed after you install Remote Storage. To add a remote storage-compatible library, recall all files from Remote Storage, uninstall Remote Storage, install the device, and then reinstall Remote Storage.

**Setting Up Remote Storage**
Remote Storage is easy to set up. Install the storage library you want to use with Remote Storage and then follow these steps:

1. Open the Add/Remove Programs tool from Control Panel, and then click Add/Remove Windows Components in the left pane.
2. Select the Remote Storage check box, click Next, and then restart the computer.


4. On the Volume Management page, select the volumes with which you want to use Remote Storage. (Only NTFS volumes appear.)

5. On the Volume Settings page (shown in Figure 20-34), type the minimum amount of free space you want available on the managed volumes, the size of the smallest files you want Remote Storage to migrate to tape, and the number of days that must pass since a file has been accessed before the file is eligible for migration to tape.

![Remote Storage Setup Wizard](image)

Figure 20-34 The Volume Settings page of the Remote Storage Setup Wizard

6. On the Media Type page, select the media you want Remote Storage to use from the Media Types drop-down list. (Only detected, supported media are listed.)

   **Important** You cannot change the media type without reinstalling Remote Storage.

7. On the Schedule For Copying Files page, click Change Schedule to change when Remote Storage copies files to tape, or click Next to accept the default schedule.

8. Review the settings you entered, and then click Finish to complete the Remote Storage setup. To Change volume settings later, right-click the volume you want to configure in the Remote Storage console, and then choose Settings from the shortcut menu.
Setting Up Additional Volumes with Remote Storage
To set up additional storage volumes on the system for use with Remote Storage after you already completed the initial setup, you can use the Add Volume Management Wizard. To do so, follow these steps:

1. Launch the Remote Storage MMC snap-in from the Administrative Tools folder on the Start menu, or type `Rsadmin.msc` in the Run dialog box or at a command prompt.
2. Right-click the Managed Volumes folder in the console tree, choose New, and then choose Managed Volume(s). The Add Volume Management Wizard appears.
3. On the Volume Management page, select the check box next to the NTFS volume on which you want to enable Remote Storage, or choose the Manage All Volumes option to instruct Remote Storage to manage all eligible volumes.
4. On the Volume Settings page (shown in Figure 20-31), type the minimum amount of free space you want available on the managed volumes, the size of the smallest files you want Remote Storage to migrate to tape, and the number of days that must pass since a file has been accessed before the file is eligible for migration to tape.
5. Review the settings on the final wizard page, and then click Finish.
6. To set up additional volumes from the command-line, use the RSS Volume Manage command. For example, type `RSS Volume Manage E:`.

Changing Include/Exclude Rules
Remote Storage uses a set of rules to govern which files are eligible for migration to remote storage. You set these rules initially when you set up a storage volume on the computer for Remote Storage to manage, using either the Remote Storage Setup Wizard or the Add Volume Management Wizard. To change these settings or add exclusions follow these steps:

1. Select the Managed Volumes folder in the Remote Storage console tree, right-click the volume you want to configure, and choose Settings from the shortcut menu.
2. Click the Include/Exclude Rules tab, select a rule that you want to modify (some rules cannot be changed), and then click Edit to modify the rule or click Remove to delete it.
3. To add a new rule, click Add to display the Edit Include/Exclude Rule dialog box, shown in Figure 20-35.
4. Type the folder path you want to apply the rule to in the Path box, or type a backslash (\) to apply the rule to the entire volume.

5. In the File Type box, type the type of file you want to include or exclude from Remote Storage.

6. Select Exclude Matching Files to exclude files matching the criteria, or select Include Matching Files to explicitly allow Remote Storage to manage files matching the criteria.

7. Select the Apply Rule To Subfolders check box if you want Remote Storage to apply the rule to all subfolders of the folder listed in the Path box.

8. To change include and exclude rules from a command prompt, use the RSS Volume Set command. For example, open a command prompt window and type `RSS Volume Set E: /Include:\Programs:* .ico`

Disabling Remote Storage for a Managed Volume

If you plan to uninstall Remote Storage, discontinue managing all the volumes and recall the files in remote storage. If you do not perform this step before uninstalling Remote Storage, you must perform a complicated and risky Remote Storage recovery procedure. See “Data Recovery and Protection” later in this chapter for more information.
To remove a managed volume from Remote Storage, or to prevent Remote Storage from adding additional files to the remote storage tier without turning off Remote Storage, follow these steps:

1. Click Managed Volumes in the console tree, right-click the volume you want to remove from Remote Storage, and then choose Remove from the shortcut menu. The Remove Volume Management Wizard appears.

2. On the Removal Options page, choose whether to recall all files from remote storage or to remove volume management while allowing Remote Storage to continue managing the files currently in remote storage. Note that if you choose to recall files, the managed volume must have enough free disk space to hold all recalled files.

3. Click Yes in the dialog box that opens, review the settings, and then click Finish.

4. To disable Remote Storage for a managed volume from a command prompt, use the RSS Volume Unmanage command. For example, open a command prompt window and then type `RSS Volume Unmanage E: /Full`.

### Performing Tasks Manually

Remote Storage is configured to perform almost all operations automatically, using the Windows Scheduled Tasks folder. To perform scheduled tasks manually, click Managed Volumes in the console tree, right-click the appropriate volume, choose All Tasks from the shortcut menu, and then choose a task from the submenu. See Table 20-5 for a description of the tasks you can perform.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy files to remote storage</td>
<td>Immediately copies all eligible files on the managed volume to remote storage.</td>
</tr>
<tr>
<td>Validate files</td>
<td>Verifies that all placeholders and locally cached files are still linked to valid data in remote storage, and updates volume statistics.</td>
</tr>
<tr>
<td>Create free space</td>
<td>Removes all cached data from files that have already been migrated to remote storage. This creates free space only if there is data cached locally.</td>
</tr>
</tbody>
</table>

**Note** Remote Storage places all tasks in the Scheduled Tasks folder—both tasks that Remote Storage performs automatically and tasks that you perform manually. To change the schedule Remote Storage uses to copy files to remote storage, or to validate placeholders and cached files or create free disk space, right-click the Remote Storage root in the Remote Storage console tree and choose Change Schedule from the shortcut menu.
Setting Recall Limits
When you set a recall limit, also known as a *runaway recall limit* because it limits only recalls that take place within 10 seconds of the last recall, you prevent programs that are not Remote Storage–aware from inadvertently recalling all files from remote storage. This usually does not affect end users because most users are not fast enough to trigger the recall limit unless they are performing a mass copy operation.

To configure the recall limit, right-click the Remote Storage root in the Remote Storage console tree, choose Properties, and then click the Limits tab.

---

**Important** Selecting the Limit Does Not Apply To Members Of The Administrators Group check box allows incompatible applications run by an administrator to recall all files from remote storage if the administrator does not explicitly kill the process recalling the data.

---

Data Recovery and Protection
Because even the best data protection plans cannot always prevent a disaster, you must also know how to recover data if a problem occurs. The following sections teach you how to protect and recover data with Remote Storage.

Understanding Data Protection Strategies
The strategy you use to protect the remotely stored data varies depending on your ability to create copies of the Remote Storage media. (You need two drives of the same media type to do this.)

---

**Note** The entire Remote Storage database is stored in only two places: in the `%SystemRoot%\System32\RemoteStorage` folder, and on each media master tape. If the local folder is deleted, you must restore from your Remote Storage tapes—a complicated procedure described in Microsoft Knowledge Base Article 235469. Always perform full backups of essential servers.

---

Single Drive Strategies
If you are using only a single tape drive with Remote Storage, back up the local files according to your preexisting backup plan (and consider replacing Remote Storage with a larger disk array). For full backups, back up migrated Remote Storage data. Note that this almost certainly means backing up to a different drive from the one holding the Remote Storage media. If you do not have another backup device, purchase one or upgrade to a disk-based solution.

Usually you do not need to include files in remote storage in differential or incremental backup schedules because files in remote storage probably have not changed since the
last full backup. If the files have changed since the last full backup and have been migrated to remote storage and have had their local cache removed (if you have a long backup schedule or a short migration schedule and a full volume), you can restore the files from a recent differential or incremental backup. Keep in mind, of course, that the longer the period between full backups, the more incremental restore operations you must perform to restore from backup (which is a good reason to use differential backups instead) or the more data that is lost if you don’t frequently perform incremental backups. See Chapter 37 for more information about using the Windows backup utility.

In addition to the regular backup schedule, frequently verify the remote storage placeholders and cached files to make sure they are still linked to valid data in remote storage. Note that Remote Storage automatically creates an appropriate validation schedule during installation.

**Multiple Drive Strategies**

Supplement your backup plan by creating copies of the remote storage media and frequently synchronizing the copies. Back up the local files according to your preexisting backup plan. For full backups, you can choose to instruct the backup program to back up migrated Remote Storage data, thus eliminating the need to deal with Remote Storage when recovering.

---

**Important** You cannot restore Remote Storage files to another computer. To restore data to another computer, you must use backups that also backed up migrated remote storage files.

---

In addition to your backup schedule, make one to three copies of the media master (the media that holds the remote storage data), and routinely synchronize them. If the media master fails, you can re-create it from one of the copies. If you do not back up the migrated remote storage files during the full backups, make sure you synchronize a media copy and keep it with your full backup. This ensures that the full backup has all data backed up.

---

**Note** To keep your backup sets complete, either perform a full backup (including data in Remote Storage) or back up only local storage, and then add a synchronized media copy to the backup set (by dragging it to the Backup media pool). The media copy you add to the backup set is removed from the Remote Storage media pool, allowing another media copy to be generated to replace it.

---

In addition to the regular backup schedule, frequently verify the remote storage placeholders and cached files to make sure they are still linked to valid data in remote storage.
Remote Storage automatically creates a validation schedule when you install it, and this is usually fine for most purposes. Just make sure it covers all the volumes Remote Storage manages.

**Working with Media Copies**

Because you cannot create fault-tolerant arrays of remote storage devices, Microsoft provides the ability to create copies of Remote Storage media so that some level of redundancy exists for remotely stored data.

---

**Note** Place new media in the free media pool instead of manually in the Remote Storage pool. Remote Storage automatically takes and appropriately formats media from the free media pool when necessary.

Use the following list to work with media copies:

- **Changing the number of media copies**  
  To specify the number of media copy sets, right-click the Remote Storage root in the Remote Storage console tree, choose Properties, click the Media Copies tab, and then specify the number of media copy sets you want to create for each media master set (up to three maximum). When one copy is finished, Remote Storage creates the next copy, provided enough media is available in the Remote Storage application pool or free media pool. Each group of media copies is called a *media copy set*.

  
  **Note** If you decide that you don’t need as many media copy sets as you originally thought, you can decrease the number of sets that Remote Storage displays and accesses, as just described. However, note that doing so does not deallocate any media. If you want to free up media, you need to delete the media copies, as described in the next section.

- **Deleting and checking the status of media copies**  
  To delete or check the status of a media copy, right-click the media master that is associated with the media copy you want to delete or check, choose Media Copies, view the status information of the media copies, and then click the appropriate Delete Copy button for any media copies you want to delete.

- **Synchronizing media copies**  
  To synchronize media copies, right-click Media in the console tree and then choose Synchronize Media Copies from the shortcut menu. You cannot recall or copy data to remote storage while synchronizing media copies.
Adding media copies to backup sets  To add a media copy to a full backup set, creating a complete backup set of both local and remote storage, use the following steps:

a. In the console tree, select Media Pools, select Remote Storage, and then select the appropriate media type for your system.

b. Right-click the synchronized media copy, and choose Copy from the shortcut menu.

c. Select the Backup media pool, right-click the appropriate Backup media pool, and then choose Paste from the shortcut menu. This adds the media copy to the Backup media pool, so you can then eject it and keep it with the rest of your backup set. Remote Storage automatically regenerates the ejected media copy with media from the Remote Storage or free media pools.

Re-creating a Media Master in Case of Disaster  To re-create a media master from a recently synchronized media copy, right-click the most recently synchronized media copy for the media master that you want to re-create, choose Media Copies, click the Recovery tab, and then click Re-create Master.

Re-creating a media master does not recover data that Windows migrated to remote storage and removed from the local cache since the last time you synchronized the media copy.

Recovering from Disaster
Disasters happen. Servers go down. Drives fail. The cable goes out during the season finale of your favorite TV show. These are facts. However, if you are prepared ahead of time, you can reduce the negative impact of disaster when it strikes. The following list summarizes what actions to take in the event of some common disaster scenarios:

Hard disk failure  If the hard disk fails, restore locally stored files from a backup, but do not perform a Remote Storage validation operation until all incremental or differential backups are restored. As long as the Remote Storage database stored in the %SystemRoot%\System32\RemoteStorage folder is not affected, you do not need to do anything other than perform a validation operation to clean up any invalid placeholders.

Hard disk failure of system drive  If the hard disk storing Windows fails, restore the system from backup if possible. The system should function normally; however, you might see the following error when recalling a file from remote storage:

Path\filename.doc. The file cannot be accessed by the system.

If you experience this error, see Knowledge Base Article 235469 and perform the Restore A Damaged RSS Database procedure.
Clean reinstall of Windows  To perform a clean reinstall of Windows, first recall all data from remote storage. (Refer to the “Disabling Remote Storage for a Managed Volume” section earlier in this chapter.)

If a disaster occurs that precludes you from recalling the data and you cannot restore the system from backup, perform a clean install of Windows into the same drive and folder as it was before, without installing Remote Storage, and then restore the Removable Storage database. Next, install Remote Storage and use the Rstore.exe command-line tool to restore the Remote Storage database. This is tricky business, so refer to Knowledge Base articles 235469 and 235032 for the exact procedures.

Summary

Windows Server 2003 R2 provides a number of new and improved features that help you manage storage, including the storage reports, quotas, and file screens of File Server Resource Manager; the fault-tolerant, site-aware namespaces and replication groups of Distributed File System; and the Storage Manager For SANs console, which makes it far easier to manage simple SANs. It also includes the Removable Storage and Remote Storage features, which are unchanged from Windows Server 2003. The next chapter covers how to plan a secure operating environment with Windows Server 2003.
Part IV
Security

Chapter 21
Planning for Security ........................................... 703

Chapter 22
Implementing Security ........................................... 733

Chapter 23
Patch Management ............................................... 783

Chapter 24
Using Microsoft Certificate Services ......................... 797

Chapter 25
Connection Services ............................................. 829

Chapter 26
Implementing Wireless Security .............................. 865
Security, in definition and practice, has changed tremendously in just the past few years. Stretching technology to increase the scope and latitude of what you’re able to accomplish exposes new and often venomous danger points. Amidst the legions of hackers, spies, terrorists, corporate raiders, professional criminals, and vandals, unprotected networks can fall prey to attack. Today’s system administrator has real security threats to address and needs to implement a solution that is both safe and unobtrusive.

Microsoft Windows Server 2003 includes a bevy of configurable security features and options ranging from an entire public-key infrastructure (PKI) to a protocol that protects individual packets as they cross the network. But before you dive into implementing the security features of Windows Server 2003 in Chapter 22 and Chapter 24, let’s review some basic security considerations.

In this chapter, you learn about cryptographic smart cards, revisit some security components that are integral to earlier Microsoft products, and explore the new security features added to Windows Server 2003. You review the common denominators of security such as authentication, data protection, and access control. You tour the Windows Server 2003 PKI and take a detailed look at some of the security-enabled protocols the server uses. You explore virtual private networks (VPNs). Finally, you learn about the underlying cryptographic application interface in Windows Server 2003, Microsoft Cryptographic Application Programming Interface (Cryptographic API, or CryptoAPI), and CAPICOM.
Security Basics

The term security covers a lot of ground, and Windows Server 2003 uses a wide range of methods and mechanisms to implement security. But before you can evaluate those mechanisms, you need to know what a good security system is designed to accomplish. For all the protocols, passwords, and secret keys, security revolves around three basic concepts:

- **Authentication** Confirming the identity of a person or entity before allowing access to a resource
- **Data protection** Ensuring the privacy and integrity of transmitted or stored data
- **Access control** Restricting the access of data and resources to privileged users

In addition to these three security mainstays, two other security features are discussed in this section: auditing and nonrepudiation.

Authentication

*Authentication* describes the process in which a person or entity identifies itself to a second party. In general terms, this can mean showing a driver’s license to a bank teller or inserting a bank card into an ATM and typing a PIN. In computer language, authentication is a bit more deductive. Unlike the bank teller scenario, which has the luxury of personal contact, nearly all computer-related authentication scenarios are virtual. In a Windows Server 2003 environment, authentication involves two distinct processes: interactive logon and network authentication.

*Interactive logon* means logging on to either a domain account or a local computer. Before Windows 2000, the logon procedure was performed by password only; beginning with Windows 2000 and continuing with Windows Server 2003, the logon process allows smart-card authentication. After the user is logged on to the domain account, *network authentication* is required to identify the user to each network resource he or she requires.

Proof of Identity

Typically, *proof of identity* comes in the form of a shared secret—a password, a PIN, or an encryption key—between the requestor and the authenticator. The principal word here is “secret.” The fulcrum of the entire authentication process is the authenticator’s belief that the requestor—and only the requestor—has that secret. After this fails to be true, the system, to some degree or another, is compromised.

Depending on the protocol being used, the shared secret is communicated to the authenticator, who then either grants or denies access. Secure protocols protect the secret in transit; more elaborate schemes don’t send the secret at all. Public-key technology uses a
pair of encryption keys—a private key that is never exposed, and a public key that can be disseminated. The next section explores the types of protocols Windows Server 2003 uses to prove possession of identification credentials.

**Authentication Protocols**

Clearly, the effectiveness of an authentication process and the safety of your secret depend on the protocol being used. Countless books before this one have guided users through installations that require choosing a unique password and then warned them against the hazards of losing the password. Yet how many passwords leave fingerprints and slip unprotected through a network? Table 21-1 shows the Windows Server 2003 protocols that are designed to thwart would-be attackers and that authenticate both internal and external users. The Active Directory service maintains user accounts that hold security credentials for authentication purposes, such as passwords and public-key certificates, and it can store multiple security credentials for each of these protocols.

---

**Note** Be sure to read about the new security technologies with respect to authentication. You can find this information in the “Using Active Directory Federation Services” section in Chapter 14 and the “UNIX Identity Management Services” section in Chapter 27.

---

**Table 21-1  Authentication protocols**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kerberos version 5</td>
<td>Network authentication. Provides mutual authentication between user and resource.</td>
</tr>
<tr>
<td>Microsoft Windows NT LAN Manager (NTLM)</td>
<td>Network authentication. Used for Microsoft Windows NT 4 compatibility.</td>
</tr>
<tr>
<td>NTLM 2</td>
<td>Authentication supporting older versions of Windows (Windows 95 and newer). LAN Manager (LM) supported older versions of Windows, but it was not interoperable with Windows NT and newer. Because of additional features and improved security, NTLM2 is recommended over NTLM even if your installed base includes no versions of Windows older than NT4 SP4 (which was the first to support NTLM 2).</td>
</tr>
<tr>
<td>Extensible Authentication Protocol (EAP)</td>
<td>Network and dial-up authentication. Provides support for additional authentication schemes, including smart cards.</td>
</tr>
</tbody>
</table>
Hardware-Enabled Authentication

Hardware is used for authentication purposes to make it more difficult for someone to impersonate a requestor. By storing encryption keys on a smart card, a PC card, or any other cryptographic token, the logon process becomes more secure. It requires an extra level of possession that a mere password does not. It requires something you know—a PIN or password to access the smart card—and something you have—the smart card itself. An attacker might somehow obtain your PIN, but without the smart card, the PIN or password is useless. To decrease the vulnerability of secret keys, well-designed cryptographic tokens generate encryption keys directly on the token and prohibit extraction of encryption keys, except possibly in encrypted form.

There’s also a lot of talk about the use of biometrics to facilitate authentication. Biometrics include such things as fingerprint identification, face recognition, and hand-geometry verification. Biometrics extend the logon requirements considerably, from something you know or have, to something you are.

Table 21-1  Authentication protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digest Authentication</td>
<td>Credentials are transmitted as a message digest or MD5 hash.</td>
</tr>
<tr>
<td>Passport Authentication</td>
<td>Authentication mechanism offering a single sign-on capability.</td>
</tr>
</tbody>
</table>

Hardware-Enabled Authentication

Hardware is used for authentication purposes to make it more difficult for someone to impersonate a requestor. By storing encryption keys on a smart card, a PC card, or any other cryptographic token, the logon process becomes more secure. It requires an extra level of possession that a mere password does not. It requires something you know—a PIN or password to access the smart card—and something you have—the smart card itself. An attacker might somehow obtain your PIN, but without the smart card, the PIN or password is useless. To decrease the vulnerability of secret keys, well-designed cryptographic tokens generate encryption keys directly on the token and prohibit extraction of encryption keys, except possibly in encrypted form.

There’s also a lot of talk about the use of biometrics to facilitate authentication. Biometrics include such things as fingerprint identification, face recognition, and hand-geometry verification. Biometrics extend the logon requirements considerably, from something you know or have, to something you are.

More Info  Federal Information Processing Standards Publication number 140-2 (FIPS 140-2) is a standard published by the National Institute of Standards and Technology (NIST) that specifies security requirements for cryptographic modules. The standard identifies four levels of security: Levels 1 through 4, with Level 1 representing the lowest level of security and Level 4 representing the highest. You can find this standard at http://csrc.nist.gov/cryptval/140-2.htm.

Mutual Authentication

Authentication isn’t necessarily a one-way street. Many times a requester wants proof of identity from the authenticating host. For instance, when you are creating a secure link to a restricted directory over which confidential data is to be exchanged, the identity of both the client and the server is important. Protocols such as SSL/TLS allow mutual authentication between client and server.
Single Sign-On
One of the additional Windows Server 2003 security features is the ability to authenticate to any computer or resource on the network by logging on to a single domain account. Through single sign-on, the user can log on to a domain account once, with a single password or smart card. The user’s single-sign-on security credentials are stored in Active Directory, and each time a domain resource is required, a network authentication occurs transparently.

The advantages of single sign-on, as opposed to authenticating to each network resource when it’s needed, are quite obvious. Users have fewer passwords to remember and fewer authentication screens to endure, and administrators find it easier to manage only one account per user.

Data Protection
Protecting passwords is critical to maintaining a secure system. Equally important is protecting the data you send after you’re logged on. Whether it’s a company’s proprietary information or a personal credit card, the concerns are the same: keeping network information from being read by unauthorized persons, and preventing it from being modified.

Of course, sensitive information doesn’t need to be on its way somewhere to be vulnerable. Although tools such as network sniffers can capture and read data packets, attacks can also occur on files on a hard disk. In addition to network security, Windows Server 2003 provides security for your stored data through Encrypting File System (EFS), which is discussed in the next section.

Data Confidentiality
The privacy of data—whether it’s an e-mail message, input to a Web page, or distinct IP packets—is jeopardized after the information is transmitted over nonsecure communication lines, such as the Internet. Using encryption algorithms and keys, data privacy can be protected. Without the appropriate decryption keys, unintended recipients intercepting the transmission receive nothing but encrypted garbage.

Note Cryptographic operations use both an algorithm and a key. The algorithm is the specific mathematical process that performs the operation. The key is the input to the algorithm.

The strength of the encryption also depends on the algorithm used and the length of the key. With enough computing power, any encryption key can be broken. Windows Server 2003 supports a range of key lengths, from 40 to 256 bits. Typically, the bulk of data is encrypted using a cipher block algorithm (also known as a symmetric algorithm) and a key. The strength of this method lies in the cipher block chaining (CBC). Encrypting a block at a time, the output of one block is used as the input of the next. In this way, repeated patterns of data won’t produce the same encrypted data. The input to the first
block is a random number called an initialization vector (IV). The IV ensures that each
time a message is encrypted, a unique result is produced.

For ensuring the integrity and confidentiality of transmitted data at the network level,
Windows Server 2003 employs Internet Protocol security (IPSec). One aspect of IPSec,
IPSec Authentication Header (IPSEC AH), allows you to verify the packet’s integrity.
IPSec Encapsulating Security Payload (IPSEC ESP) encrypts TCP/IP packets before trans-
mission and decrypts them upon receipt.

Confidentiality of stored data is also a concern. Although access to stored files can be
restricted for certain users through file permissions, intruders who gain unauthorized
access to your hard disk can modify those permissions. To combat this problem, Win-
dows Server 2003 uses a transparent encryption scheme called Encrypting File System
(EFS). Files on NTFS volumes can be encrypted and decrypted with users’ EFS public/
private-key information. Users need only select the files to be encrypted. The actual
encryption occurs behind the scenes.

**Data Integrity**

Windows Server 2003 supports digital signing, which guarantees the file’s data integrity—
that is, that the file has not been modified or tampered with. Digital signing of a file, mod-
ule, or other software component is somewhat like signing a contract on paper. The
signer is responsible for what he or she signs. Whoever subsequently views the docu-
ment and signature can tell who signed it.

However, digital signatures offer a great deal of security beyond that. A digital signature is
generated by creating a one-way hash of the document and encrypting the hash with the
signer’s private encryption key. This procedure produces a signature that is cryptograph-
ically tied to both the signer and the content of the document. Changing the content
breaks the signature.

Upon verification, the digital signature is decrypted with the signer’s public key. The result-
ing hash is compared against a newly computed hash of the message. As long as the original
key has not been compromised, this process proves undeniably that the signer signed the
message. His or her key was used to verify the signature. In addition, it verifies that the con-
tents of the document haven’t changed because the encrypted hash matched the newly
hash_and_signature_algorithms.asp) for a description of hash and signature algorithms.)

In Windows Server 2003, digital signing has two meaningful purposes. First, it guaran-
tees the integrity of data stored locally or being passed over a network. Second, it authen-
ticates modules or other software components that are obtained from untrusted sources,
such as the Internet. Validating the signature of a module verifies that the software hasn’t
been tampered with and that it was signed by a trusted software publisher.
MD5 and SHA-1 cryptographic hash values are commonly used to verify file-level integrity. A useful tool for doing just that is the File Checksum Integrity Verifier (FCIV). The two most common digital signature algorithms are RSA and Digital Signature Algorithm (DSA). DSA signatures are 40 bytes (320 bits) long, while the length of RSA signatures depends on the key size. A key pair, consisting of a public key and a private key, with a 128-byte (1024-bit) public key typically produces a 128-byte signature.

**Access Control**

As explained earlier, authentication is the first layer of security in the protection of network objects and resources. The second layer is access control—that is, controlling which resources can be accessed, by whom, and with which permissions. An authenticated user doesn’t necessarily have authorization to access all files, printers, and registry keys. Access control is enforced by the manager for each object type, but it’s up to the object owner to determine which access control restrictions to impose.

Access is controlled by assigning rights to users and by setting permissions for objects. Permissions specify which users can access a specific object and which type of access is allowed. For example, the owner of a quarterly finance spreadsheet might set permissions that allow read/write access to the head of finance, allow read-only access to everyone in finance, and deny access to everyone else.

Groups of users have their own rights, and those can be specified when granting object permissions. In the previous example, establishing read-only permissions for everyone in finance probably means setting a group’s rights, not setting users’ rights individually.

Permissions can be explicitly set for an object, or for ease of administration they can be inherited from parent objects. However, the granularity of access control doesn’t necessarily stop at objects. Permissions can even be set for attributes of an object, allowing access to some fields (such as the e-mail address of a user account), but denying access to other fields (such as the user’s telephone number). Standard object permissions include the following:

- Reading an object
- Modifying an object
- Deleting an object
- Reading an object’s permissions
- Modifying an object’s permissions
- Changing an object’s owner

*Note* You cannot set permissions on a file’s individual attribute, but you can set such permissions on an Active Directory object.
Auditing

Another Windows Server 2003 security feature is auditing, which allows an administrator to keep tabs on events that might possibly compromise the system. (If you're familiar with Windows server platforms tracing back to Windows NT, you're already accustomed to the auditing mechanisms available in the new versions.) Events such as logging on and logging off, access to files, and user-account management can all be audited. The administrator can choose which objects to audit, which events on that object to audit, and which users or groups using that object to audit. Both successful and unsuccessful access attempts can be audited.

**Note** Viruses can leave trails of inappropriate writing of executables and dynamic-link libraries (DLLs). Auditing successful and failed write access to these files and monitoring the security log for unexpected occurrences gives you a head start at detecting viruses on your system.

In addition to auditing users' security-related events, Windows Server 2003 provides a means of tracking security management events because an audit trail reflects any changes in security policies. For instance, if an administrator changes the permissions of a particular object to deny access to a specific group, this change in permissions appears on the audit trail. Chapter 22 shows how to manage the security log that Windows Server 2003 generates.

Nonrepudiation

Finally, let's take a look at nonrepudiation, another Windows Server 2003 security feature. Nonrepudiation is undeniable proof that a correspondence was sent or received and usually refers to security-enhanced e-mail messages. Proof that a message was sent is a property exhibited by digital signatures. For undeniable proof of receipt, the recipient of a signed or encrypted message responds to the sender with a signed receipt.

**Important** Some e-mail packages allow for receipts of signed messages, but this doesn't necessarily demonstrate nonrepudiation. A signed receipt is undeniable proof that a message was received only if it is cryptographically tied to both the recipient and the original message.

Smart Cards

New to Microsoft Windows 2000 was the support of cryptographic smart cards. This support is maintained in Windows Server 2003. A smart card is a tamper-resistant, credit card–like hardware token that can be used to implement additional protection
for security-enabled protocols and applications. Unlike credit cards, which have magnetic strips on the back, smart cards use metallic contacts as the hardware interface and require a card reader—Plug and Play (PnP) readers are recommended for use with Windows Server 2003. Manufacturers typically provide a software application interface, such as Crypto Service Provider, for use with Microsoft CryptoAPI, or they use a PKCS #11 module. Support for various smart cards—Gemplus GCR410P and GPR400, Litronic 220P, Rainbow Technologies 3531, and SCM Microsystems SwapSmart (for both the RS-232 and PC Card interface models—is included with the Windows Server 2003 installation.

Smart cards provide the strongest form of user authentication in Windows Server 2003. Either a PIN or password is required to access the card, which protects the user’s credentials from both rogue parties and applications. In addition to storing public-key certificates and private keys, smart cards can also provide on-card functionality, such as digital signing, to ensure that a user’s private key is never exposed.

Smart cards can be moved from computer to computer with ease, providing a high portability level for a user’s credentials. Included in the list of security features is the ability to block a smart card from the system after a certain number of unsuccessful logon attempts, making dictionary attacks impractical. (A dictionary attack is a password attack in which a malicious user sends hundreds or thousands of credentials by using a list of passwords based on common words or phrases.)

**Note** Smart cards aren’t the only way you can have “mobile” credentials. The new Digital Identity Management Service allows credential roaming, enabling secure sharing of user credentials and private keys.

### Public-Key Infrastructures

Now that you have looked at more basic security concepts, let’s examine some security-enabled protocols. In recent years, public-key infrastructures (PKIs) have been used increasingly in both commercial and government sectors. Based on public-key technology, a PKI describes a system of public-key certificate generation and management, including distribution and revocation. The important elements of this infrastructure are certificate authorities (CAs) that issue certificates, clients that use certificates, and directories that store certificates. Many PKIs use a registration authority that ensures user identity and authorization before certificates are granted. Figure 21-1 shows a typical Microsoft Windows Server 2003 PKI.
One of the distinct advantages of using public-key certificates for authentication is that servers no longer need to store and maintain a password list for their individual users. Because identification is based on a trust relationship with the CAs, the servers need to trust only the authority that issued the requester’s certificate. After the chain of trust is determined and the certificate is verified, authentication can be established.

RSA Laboratories maintains a list of public-key cryptography standards (PKCS) that define public-key–related formats. Table 21-2 contains four notable standards.

Table 21-2  Important public-key cryptography standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKCS #7</td>
<td>Cryptographic Message Syntax Standard, the basis for Secure Multipurpose Internet Mail Extensions (S/MIME). Defines the format of signed and encrypted messages. The degenerate case allows the exchange of public-key certificates and certificate revocation lists (CRLs).</td>
</tr>
<tr>
<td>PKCS #10</td>
<td>Certification Requests. Used by clients to request certificates from CAs.</td>
</tr>
<tr>
<td>PKCS #11</td>
<td>Cryptographic Token Interface. Analogous to Microsoft CryptoAPI.</td>
</tr>
<tr>
<td>PKCS #12</td>
<td>Personal Information Exchange (PFX). Enables the encrypted transfer of private keys and associated certificates from one computer to another.</td>
</tr>
</tbody>
</table>
Public-Key Encryption vs. Symmetric-Key Encryption

Although PKIs depend heavily on public-key technology, many functions performed by PKI entities combine public-key encryption and symmetric-key encryption. Symmetric-key encryption has been around for hundreds of years. It involves the use of a single encryption key for both the encryption and decryption of data. Encrypting data this way is analogous to placing a document in a safe and locking it with a key. When the document needs to be retrieved, the same key is used to unlock the safe. Relatively speaking, this method is secure and fast. Unfortunately, this type of encryption doesn’t lend itself well to encrypting data to a person. Because the key must remain private, the difficulty exists in transmitting the key. After all, if there’s a secure means to send the key, why not send the message through that route to begin with?

Public-key encryption, also known as asymmetric encryption, emerged from the necessity to share encrypted data with people, where no secure path existed to pass an encryption key. Public-key encryption uses a pair of keys: a public key that is distributed, and a private key that remains secret. To encrypt a message to someone, the encryption algorithm uses the recipient’s public key. The resulting encrypted message can be decrypted only by the recipient’s private key. This method is analogous to a safe with an entry slot. Anyone can slip a document in, but only the person with the correct private key can retrieve it. This scheme works for self-encryption of files as well. The Windows Server 2003 EFS, for instance, protects data with the user’s public key. To decrypt, the user’s private key is accessed and used.

Unfortunately, public-key encryption algorithms are slow and are rarely used to encrypt large amounts of data. Instead, public keys are used to protect symmetric keys that encrypt large chunks of data. For example, suppose Rosemary wants to encrypt a portfolio to Harold. Rosemary encrypts the portfolio using a symmetric-key algorithm like the Advanced Encryption Standard (AES). She then encrypts the symmetric key with Harold’s public key, producing an asymmetrically encrypted symmetric key. Harold, upon receiving the encrypted portfolio and key, decrypts the encrypted symmetric key with his private key and uses the resulting symmetric key to decrypt the message.

Public-key encryption extends to digital signatures as well. Digital signature algorithms actually reverse the encryption process. Encrypting the hash of a message with a user’s private key generates a digital signature. The signature can be verified later by decrypting the hash with the user’s public key.
Public-Key Certificates and Private Keys

Most public-key infrastructures, including Windows Server 2003 PKI, revolve around the use of X.509 public-key certificates. PKI users have a private key and a circulated public key. A public-key certificate cryptographically binds a public key to the user who holds the corresponding private key. Certificates are issued and digitally signed by a CA. Table 21-3 lists the fields of an X.509 certificate.

Table 21-3 Public-key certificate fields

<table>
<thead>
<tr>
<th>Certificate Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial number</td>
<td>Unique number that the CA assigns to a certificate.</td>
</tr>
<tr>
<td>Signature algorithm</td>
<td>ID of the algorithm that the CA uses to digitally sign the certificate.</td>
</tr>
<tr>
<td>Issuer</td>
<td>Name of the CA that issues the certificate.</td>
</tr>
<tr>
<td>Validity period</td>
<td>A pair of dates indicating when certificate validation begins and when it ends.</td>
</tr>
<tr>
<td>Subject</td>
<td>Name of the certificate user.</td>
</tr>
<tr>
<td>Public key</td>
<td>Public key that, with the corresponding private key, makes up a user’s key pair.</td>
</tr>
<tr>
<td>Extensions</td>
<td>Additional information that a CA can include in the certificate. Examples of extensions are alternate names, such as the user’s e-mail address; key usage, which indicates which operations a public key can be used for; and basic constraints, which show whether the certificate is a CA certificate.</td>
</tr>
<tr>
<td>Signature</td>
<td>Digital signature generated by the issuer.</td>
</tr>
</tbody>
</table>

When a certificate is used, it is validated by verifying the signature with the issuing authority’s public key. As long as the issuing CA is trusted (or is within a trusted path), you can be certain that the user or entity named in the certificate holds the corresponding private key.

Of course, certificates aren’t issued solely to users. CAs have their own certificates. CAs can also issue certificates to services and devices that need to be accessed on the network. A Web server that accepts SSL-encrypted transmissions and a directory that provides two-way authentication are both good examples of entities that use certificates.

Even though certificates belong to users and other entities, that doesn’t mean that a user or entity is limited to one certificate—or, for that matter, that a user can be a member of only one root hierarchy. Certificates are issued for many purposes—server authentication, file encryption, and code signing, to name a few. A user holds any number of certificates and private keys under different CAs or under the same CA; each might differ in usage,
privilege, key size, and algorithm. For example, a security model might need multiple levels of access with separate CAs handling each level. On the other hand, a single user might hold Level 2 and Level 4 certificates; another might hold Level 1 and Level 3 certificates.

Having certificates under different root certificate authorities (root CAs) is common too. Consider the human resources director who has both an enterprise certificate, which allows her to access her company’s human resources server, and a certificate from a commercial CA, which allows her to browse the company’s 401(k) stock portfolio over the Internet.

At the very least, the functions of encryption and digital signatures must be split into separate certificates. Private keys used for encryption can be archived so that encrypted data of a lost key can be recovered. Because the integrity of digital signatures depends on sole possession of the private key, digital signature private keys must not be archived.

Certificate Authorities

Certificate authorities exist to issue certificates for entities—including users, services, devices, subordinate authorities, or the CA itself—which meet the policy set forth for the CA. The CA accepts and fulfills certificate requests and revocation requests and might also manage the policy-directed registration process that a user completes to get his or her certificate. For information about how to install a CA using Microsoft Certificate Services, see Chapter 24.

Root and Subordinate Certificate Authorities

Although CAs can issue and revoke certificates for a host of users, larger companies might be too big to administer with a single CA. In addition, enterprises might want to delegate authority of certain certificate types, or they might have divisions that manage their own resources and need to enforce separate certificate-issuing policies. Production, for instance, might want to issue certificates to anyone whose e-mail address is within the company domain. Engineering might require a picture ID for registration. On the other hand, by using autonomous CAs, users between the two divisions are cryptographically isolated. A digitally signed message sent from a user in production to a user in engineering has no common basis of trust.

To solve this dilemma, CAs can be stacked hierarchically. Root CAs use a certificate they issue to themselves (a self-signed certificate). They also issue certificates to subordinated authorities and in general do not issue user certificates. Subordinate authorities issue certificates to users and other end entities and might also issue certificates to other subordinate CAs. Root CAs are implicitly trusted—subordinate CAs and clients derive trust from the root.
Figure 21-2 shows an example of a CA hierarchy. By stacking CAs hierarchically, an enterprise can manage the certification system from a single authority while delegating control of policy decisions to discrete authorities.

![CA Hierarchy Diagram]

Figure 21-2  A certificate authority hierarchy

Windows Server 2003 also distinguishes between enterprise CAs and standalone CAs. The primary difference is that the enterprise CA uses Active Directory for user information and policy decisions and can publish certificates and CRLs to Active Directory. The standalone CA requires the certificate requestor to supply all user-identifying information.

**Chain Verification and Trust**

Before a received digital signature can be verified, the signer’s certificate must be validated. This is true of any application, whether it’s a service, device, or user performing the verification. Without a hierarchical chain back to a trusted root CA, the identity of the user in the certificate can’t be confirmed.

Chain verification is a two-step process. The first step is to build the certificate chain from the signer’s certificate to a trusted root CA. Consider the CA hierarchy in Figure 21-2. Suppose User 1 in engineering is trying to verify a signature from User 5 in finance. User 1 builds the certificate chain for User 5 back to the root CA, Netsolvers root CA,
which is in User 1’s trusted store. The certificate chain, built from the bottom up, is User 5: Finance CA: Corporate CA: Netsolvers root CA. The verifying entity obtains these certificates from the transmission protocol if they’re included or from an accessible certificate store. The root CA certificate is the pivotal trust component in a certificate chain. It should be published only through a trusted method, such as Active Directory Group Policies.

The second step of chain verification is to verify the certificate chain from the top down. The verifying entity checks each certificate for validity, starting with the trusted root. Validity checking includes verifying the certificate’s digital signature, checking the certificate’s validity period, and ensuring that the certificate hasn’t been revoked. Depending on policy, applications might also check any certificate extensions that the certificate contains.

Note Currently, typical PKI implementations include two-tier or three-tier hierarchies. As the popularity of public-key infrastructure spreads, CA vendors will make more attempts to unite and centralize certificate authorities and root certificate authorities, which will result in longer certificate chains.

Cross-Root Certification
Even with a central root CA and a multitiered CA hierarchy that spans the breadth of a company, users might need to verify digital signatures under different root CAs. This verification is especially important when integrating commercial CAs, such as Verisign, to perform code signing, among other tasks. Using cross-root certification, root CAs can be connected so that validation paths of certificates under different roots extend back to the user’s root CA. By using Active Directory Federated Forests, for example, users in different organizations can authenticate and share information securely.

Certificate Registration
Before being able to use his or her generated public/private key pair for encryption or digital signatures, a user must first obtain a certificate from a CA. A user does this by sending a certificate request—which includes his or her name and public key—to a CA. A number of registration models can exist depending on the registration policy a CA wants to uphold. Many commercial CAs handle PKCS #10 certificate requests and also allow Web-based certificate generation.

For more secure needs, a registration authority can act as a certificate-requesting agent to ensure proper proof-of-identity procedures and to forward certificate requests to the CA. Microsoft Certificate Services includes an enroll-on-behalf-of station where administrators,
using enrollment agent certificates, can program smart cards for users. Figure 21-3 shows two examples of certificate request scenarios.

![Figure 21-3 Two certificate request scenarios](image)

In the first example, a client requests a certificate from an enterprise CA, perhaps using the Certificates snap-in Certificate Request Wizard. User information and certificate rights are obtained from Active Directory. The Certificate Request Wizard generates a public/private key pair for the user. The public key is included in the certificate request and sent to the CA. The private key is saved on the user’s computer. Upon receipt of the certificate request, the CA issues and signs the certificate and pushes it to a directory where other users and entities can retrieve it.

The second example shows an administrator programming a smart card through the enroll-on-behalf-of station. In this case, the private key is written directly to the card. In neither scenario is the private key exposed to the CA or anyone else. Again, after the certificate is issued, it’s written to a directory for public availability. The smart card is returned to the user and is ready for authentication.

**Certificate Directories**

An important piece of the PKI is the directory in which certificates are stored and from which they can be retrieved. To encrypt data to a user, you need the user’s public-key certificate. Similarly, when verifying a digitally signed message, the certificate chain back to the verifier’s root must be established.
In a Windows Server 2003 environment, Active Directory acts as a repository for certificates; any user or computer with appropriate rights can retrieve them. In addition, external users’ certificates can be mapped to Active Directory user accounts.

**Note** Typically, after a client application retrieves a given certificate, it caches the certificate locally to save the overhead of another retrieval. Use the Certificates snap-in to view stored certificates by purpose or by storage category, such as personal or trusted roots.

**Certificate Templates**

A certificate template specifies the structure of a certificate. A template is used when creating certificates to give them a default layout. There are a number of certificate types, and the types accessible by the certificate issuer—in this context, the user of the certificate template—depend on the access rights of the issuer.

Windows 2000 employed what is called a Version 1 template. One notable problem with Version 1 templates is that you cannot control the content of the certificate; Microsoft defined a static layout for each of the Version 1 template types.

Because of the limitations of Version 1 templates, Version 2 templates were developed. Windows Server 2003 Enterprise Edition can use Version 2 templates from the CA. Windows 2000, Windows XP, and Windows Server 2003 can enroll for Version 2 certificates. Version 2 templates enable you to change the contents of the template, allowing you to determine which features all future certificates made from the template will contain.

More information about certificate templates can be found in Chapter 22.

**Certificate Revocation**

In addition to issuing and signing certificates, CAs are responsible for maintaining a list of certificates that are no longer valid. This list, called a certificate revocation list (CRL), is digitally signed by the issuing authority.

Such a list is a necessary requirement for a public-key infrastructure (PKI). Consider a laptop user who dials into his company’s network to access a server that contains finance accounts. He uses his certificate and corresponding private key to authenticate himself to the finance server. Now suppose the laptop is stolen. In the past, a compromised password might have resulted in the administrator changing the user’s password.

In a PKI, however, verification is based on possession of a private key. The finance server has no knowledge of a specific user, only the CAs that it trusts. By using the CRL as a revoking mechanism, the finance server can retrieve a current list of revoked certificates. After the stolen certificate is placed on the CRL and the CRL has been published and retrieved, verification of the certificate results in a failure and access is denied.
Like user certificates, a CRL is digitally signed by the issuing CA and can be verified with the CA’s certificate. Table 21-4 describes the fields of an X.509 CRL.

### Table 21-4 Certificate revocation list fields

<table>
<thead>
<tr>
<th>CRL Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.509 version</td>
<td>X.509 CRLs version. The current CRL version is X.509 version 2.</td>
</tr>
<tr>
<td>Signature algorithm</td>
<td>ID of the algorithm that the CA uses to digitally sign the CRL.</td>
</tr>
<tr>
<td>Issuer</td>
<td>Name of the CA that issues the CRL.</td>
</tr>
<tr>
<td>Last update</td>
<td>Date and time that the current CRL is issued.</td>
</tr>
<tr>
<td>Next update</td>
<td>Date and time that the next CRL will be issued.</td>
</tr>
<tr>
<td>List of revoked certificates</td>
<td>Each entry in the list includes the certificate serial number and the date</td>
</tr>
<tr>
<td></td>
<td>when the certificate was revoked. Optional extensions can be added, such as</td>
</tr>
<tr>
<td></td>
<td>a reason flag.</td>
</tr>
<tr>
<td>Extensions</td>
<td>Optional information that the CA can include in the CRL.</td>
</tr>
<tr>
<td>Signature</td>
<td>Digital signature that the issuer generates.</td>
</tr>
</tbody>
</table>

Just as with the certificate registration and issuing procedures, policies are established for CAs that dictate certificate revocation. These policies should include such procedural decisions as how often CAs refresh their CRLs, which mandatory and discretionary extensions CAs can include in their CRLs, and under what circumstances certificates get revoked. Under one policy, for instance, certificates of employees who leave the company are subject to revocation. Under another, a user merely being denied certain privileges is grounds for revoking his or her certificate.

Because certificates have a validity period, CRLs need to contain only revoked certificates that aren’t yet expired. After a certificate expires (in other words, the Valid To date has passed), verifying entities refuse the certificate and it can be removed from the CRL.

You must also consider CRL dispersal. The rate at which CRLs are issued, or “refreshed,” is a policy decision made by the CA and can be as frequent as once a day. For highly secure domains, the refresh rate can be even more frequent; otherwise, a revoked certificate can continue to be used. To be current, verifying entities need to obtain the latest CRL. Microsoft Certificate Services allows CRLs to be published to Active Directory or to a URL for HTTP access.

### Certificate Renewal

Another set of certificate policy decisions relates to the certificate renewal procedure—specifically, whether certificates are allowed to be renewed, when certificates are renewed, and how certificates are renewed. Renewing certificates with the same key allows a user to extend the life of a public/private-key pair. In contrast, renewing a certificate with a different public key after a user’s certificate expires can make it difficult to read previously encrypted messages.
Full CRLs and Delta CRLs

With Microsoft Windows 2000 Server, certificate authorities could publish CRLs at scheduled times or manually. Each update required the old CRL to be completely replaced by a new full CRL.

With Windows Server 2003, the certificate authorities can use delta CRLs. These represent only the data that has changed since the last CRL update. Delta CRLs provide a number of benefits. Because the delta CRLs are smaller than the full CRLs, the delta CRLs can be updated more often without a large impact on the network or clients. These frequent updates reduce the time it takes for an entry to be published to the CRL. Delta CRLs have to be supported by the client as well; currently, only Windows XP and Windows Server 2003 clients support using delta CRLs.

Security-Enabled Protocols

Security in Windows Server 2003 exists at different levels—from the protection of entire messages at the application level, to secure channels, to the protection of data packets within IP. The security protocols residing at these different layers provide mechanisms not available at other layers.

S/MIME, for example, provides public-key–based encryption, integrity, and authentication of e-mail messages at the application level. SSL resides beneath the application layer, adding security to application protocols. IPSec, on the other hand, provides application-independent data protection at the IP layer. The following sections examine Windows Server 2003 security protocols.

Secure Multipurpose Internet Mail Extensions

S/MIME is included with Microsoft Outlook and Outlook Express. It uses private-key certificates to secure e-mail messages and files in accordance with the PKCS #7 standard. It supports both encryption and digital signatures. When you nest single S/MIME contents, messages can also be signed and then encrypted, or signed multiple times.

Signed Messages

A PKCS #7 digitally signed message includes the message signature, the signature algorithm, and information about the signer. Optionally, the signer’s certificate or certificate chain can be added, as well as any CRLs that the verifier might need. Authenticated attributes, which are protected by the digital signature, and unauthenticated attributes can also be added to the PKCS #7 content. The time at which a message is signed is an example of an authenticated attribute.
The content that is signed might or might not be included in the PKCS #7 message. If the content isn’t included, the verifier needs both the PKCS #7 content and the original file that was signed to complete the verification. If the original file is easily available, this method saves the overhead of having redundant data.

**Encrypted Messages**

The current PKCS #7 standard requires the use of two algorithms for message encryption. Because public-key algorithms are slow, the message is first encrypted with a symmetric-key algorithm, such as DES. The small symmetric key is then encrypted to the recipient, using a public-key algorithm, such as RSA. In this way, a message can be encrypted to multiple recipients while the actual content has to be encrypted only once.

The PKCS #7 message includes the encrypted content and symmetric-key algorithm along with information for each recipient. This information contains the symmetric key encrypted to that specific recipient. Upon receipt, an application searches the list of recipients for one that matches the current user’s certificate. It then decrypts the symmetric key with the user’s private key and subsequently decrypts the message.

**Other Content Types**

The degenerate case of the PKCS #7 message allows for the absence of the content and any signature information. This format provides a transport for certificates and CRLs. Table 21-5 shows the typical file extensions for different PKCS #7 files.

<table>
<thead>
<tr>
<th>Extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.P7M</td>
<td>PKCS #7 encrypted file or signed file with content added</td>
</tr>
<tr>
<td>.P7B</td>
<td>PKCS #7 file extension</td>
</tr>
<tr>
<td>.P7S</td>
<td>PKCS #7 signature file (signed file without the content)</td>
</tr>
<tr>
<td>.P7C</td>
<td>PKCS #7 certificate or CRL-only file</td>
</tr>
</tbody>
</table>

**Note** There are a number of other efforts underway to develop technology to enable secure and authenticated e-mail. The current threats of spamming, phishing, and spoofing are motivating organizations to develop cross-industry standards to combat these threats. See [http://www.emailauthentication.org](http://www.emailauthentication.org) for more information.

**Kerberos Version 5**

Kerberos is another authentication security protocol used by Windows 2000 Server and Windows Server 2003. It is used over a network to mutually identify the requestor (user) and authenticator (network resource). After they are identified, the user and network resource can encrypt transmissions to ensure privacy.
Kerberos works by issuing tickets to users for accessing resources on the network. Before exploring the high-level details of Kerberos, you need to understand some objects and services:

- **Ticket**   A packet of data that allows a client to access a resource. It includes an encrypted piece of client information that, when decrypted, confirms identity.

- **Ticket-granting ticket (TGT)** A special ticket that allows the client to obtain temporary tickets from the ticket-granting service for each authentication.

- **Key distribution center (KDC)** A service that runs as part of Active Directory and administers TGTs. Every domain controller is a KDC.

- **Ticket-granting service (TGS)** A service that is accessed by a client with a TGT and that administers tickets for network resources.

The use of a TGS keeps the user from having to log on for each resource request. Figure 21-4 shows the details of a client using Kerberos to authenticate to a server.

The following steps describe the process a client goes through when using Kerberos to authenticate to a server:

1. A client authenticates once to the key distribution center by using a password or smart card.
2. The KDC issues a TGT to the client, for access to the TGS.
3. When the client wants to access a network resource, such as the corporate finance server, he or she requests a service ticket from the TGS, sending the TGT as proof of identity.

4. The TGS replies with a service ticket for use at the requested network resource server.

5. The client sends the service ticket to the network resource server for access.

6. To mutually authenticate, the network resource server replies with a packet that the client can decrypt.

After a client completes the first two steps, steps 3 through 6 can be repeated each time a user needs to access another resource.

---

**Note**  The advantage of this mechanism is that all Kerberos authentication occurs behind the scenes. The user needs to enter a password only once into the KDC—authentication to all other resources happens transparently.

---

**Windows NT LAN Manager**

Windows NT LAN Manager (NTLM) is the primary authentication mechanism for Windows NT 4. NTLM 2 is an extension that supports backward compatibility for previous versions of Windows. In Windows 2000 Server and later, NTLM and NTLM 2 are superceded by Kerberos as the default authentication protocol. NTLM is included as part of Windows Server 2003 for configurations that involve authentication between Windows NT and Windows Server 2003 machines or where the computers are not in a domain, like workgroups or standalone servers.

**Secure Sockets Layer**

Another Windows Server 2003 security protocol, Secure Sockets Layer (SSL), uses public-key technology to provide a secure channel for applications communicating over a non-secure network. A Web browser and Web server, for instance, can use SSL to communicate securely over the Internet. Before sending encrypted data, the client and server must engage in a security handshake to authenticate the parties involved and establish security levels. The handshake is a multipart process, as described here:

1. The client initiates connection with a request for a secure channel.

2. The server responds with its public-key certificate and can request the client’s certificate for mutual authentication if the client is requesting a resource that requires authentication.

3. The client verifies the server’s certificate. If the server requested the client’s certificate, the client sends it and the server verifies it.
4. The client generates and encrypts a session key with the server’s public key found in its certificate.

5. All communication between the server and client is symmetrically encrypted and decrypted using the session key.

Figure 21-5 illustrates the SSL handshake process. In addition to authentication, the SSL handshake allows the two parties to agree on security parameters. Because of SSL’s positioning, it can add security to application protocols such as HTTP, LDAP, Telnet, FTP, Gopher, and Network News Transfer Protocol (NNTP).

![SSL Handshake Process Diagram](image-url)

**Internet Protocol Security**

Finally, the Windows Server 2003 IPSec security protocol provides end-to-end security of network data using encryption, digital signature, and hashing algorithms. The IPSec driver protects individual packets before they reach the network and unwraps the protection after they’re received. Because the IPSec driver resides at the IP transport layer, individual applications don’t need to handle the specifics of data security during transmission. Data passed though the network from applications without security features can still be protected. Because IPSec protects the packets of data—not the actual link—IPSec can provide security for transmissions on insecure networks, and only the two computers engaging in communications need to know about it. IPSec provides a number of security features:

- **Authentication** Use of a digital signature verifies identity of sender
- **Integrity** Use of hash algorithms ensures that data hasn’t been altered
- **Privacy** Use of encryption protects data from being read
- **Anti-replay**  Prevents packets from being re-sent by an attacker to gain unauthorized access
- **Nonrepudiation**  Use of public-key digital signatures proves message origin
- **Dynamic rekeying**  Ability to generate keys during communication so that parts of transmissions are protected with different keys
- **Key generation**  Diffie-Hellman key agreement algorithm allows two computers to agree on a key without ever exposing it
- **Key lengths**  Provides configurable key lengths for export restrictions or highly sensitive transmissions

**IPSec Policy Management**

An important component of IPSec is the policy agent. The policy agent begins during system startup and is responsible for retrieving IPSec policy information from either Active Directory or the registry and feeding it to the IPSec driver. For domain computers, the domain policy information is acquired from Active Directory at startup and at policy-defined retrieval intervals. For standalone systems or systems that are offline, the policy agent retrieves policies from the registry. When an offline machine reconnects, the retrieved domain policy overrides the local policy.

Figure 21-6 shows how policy information is transferred from Active Directory to the IPSec driver. The IPSec policy agent retrieves security policies and feeds them to the IPSec driver.

![Figure 21-6](image-url)  How policy information is transferred from Active Directory to the IPSec driver
Chapter 22 describes how you can use IPSec Policy Management to define and manage IPSec policies for single computers or entire domains. Windows Server 2003 also provides predefined policies that can be customized to specific needs.

**How IPSec Works**
Before data can be protected and transmitted between two IPSec-enabled machines, a negotiation must take place to agree on which keys, mechanisms, and security policies to use to protect the data. This negotiation produces a security association (SA).

For IPSec communications, an initial SA called Internet Security Association and Key Management Protocol (ISAKMP) is established between the two computers to provide a method of key exchange. Using the ISAKMP for protection, a second negotiation takes place to produce a pair of IPSec SAs and keys, one for inbound and one for outbound communications. Specifically, these SAs include an agreed algorithm for encryption and integrity and the agreed IPSec protocol to use. The two IPSec protocols are:

- **Authentication Header (AH)**  Provides data authentication, integrity, and antireplay to IP packets
- **Encapsulating Security Payload (ESP)**  Provides confidentiality along with data authentication, integrity, and antireplay to IP packets

The IPSec SAs and keys are loaded into the IPSec driver on their respective machines and are used to protect data during transmission.

**Virtual Private Networks**
Before you explore virtual private networks (VPNs), what they mean, and why they’re useful, take a second to consider that acronym, VPN: “virtual,” as in simulated; “private,” as in secret and confidential; “network,” as in a collection of computers.

Logically, a VPN is simply an extension of a private network. In reality, private networks are geographically isolated from remote users and other private networks by nonsecure communication lines such as the Internet. When you use a secure, network-level protocol such as IPSec, a private link can be emulated between two separate networks. Both requestor and authenticator perceive what is actually the wrapping of data before it passes through nonsecure extranets or intranets as a private dedicated line. Because data packets are protected by encryption, any in-transit interception results in unreadable data.

IPSec enables the encryption of communications between peer machines; by design, no server is needed. Compare it with VPNs, which require the use of a dedicated server. That server is tied to the private network. By accepting connections from only VPN-authorized clients, the VPN server allows private traffic within the physical enclave to proceed normally without requiring additional internal security.
Before you can establish a VPN connection, VPN authorization must be confirmed for the client. Authorization is based on the remote access policies set by the network administrator and on the dial-in properties of the client requesting the connection. After a user is determined to be authorized and one-way or mutual authentication occurs, you can establish the VPN. Windows Server 2003 includes two protocols that are used to encapsulate data over the VPN:

- **Point-to-Point Tunneling Protocol (PPTP)**
  Provides data encryption using Microsoft Point-to-Point Encryption (MPPE)

- **Layer Two Tunneling Protocol (L2TP)**
  Provides data encryption, authentication, and integrity using IPSec

### Remote Access VPNs

An authorized but isolated user can access the protected resources of a private or hidden network by authenticating to the network’s VPN server and establishing a VPN connection. The remote user can be at home or on the road needing to connect through an ISP and the Internet, or the remote user can be part of the same intranet but detached from the secure or hidden network.

For example, suppose the engineering division of a company has a hidden enclave within an enterprise-wide network, complete with secret documents and alpha-version software. They want to grant access to the hidden network to the vice president of engineering but don’t want to compromise the confidentiality of the information as it crosses the company’s intranet. By providing a VPN server that blocks unauthorized users but allows the vice president to authenticate and establish a VPN connection, engineering’s secret network is extended to one more user.

---

**Note** Simply having a VPN connection to a private network does not mean you have full access. You still need the correct permissions to access specific resources.

---

After the client establishes a VPN connection with the VPN server, the user appears to be accessing the private network directly. Figure 21-7 shows remote access for an Internet-based VPN.
Router-to-Router VPNs

A VPN connection can also be established for two mutually exclusive private networks; the connection is also known as a VPN Tunnel. In this case, both the VPN client and VPN server are routers. Like remote access VPNs, router-to-router VPNs can involve enclaves that are part of the same intranet, or they can involve private networks that require the Internet infrastructure for communication. Figure 21-8 shows a router-to-router connection for an intranet-based VPN.

![Figure 21-8 A router-to-router VPN connection](image)

Here the VPN client authenticates itself to the VPN server, and a secure VPN connection is negotiated. Again, the logical appearance in both cases is that the private networks are physically connected. You find more on VPNs in Chapter 25.

Windows Rights Management Services

The Windows Rights Management Services (RMS) for Windows Server 2003 is a technology that allows users to protect information, from documents to e-mail. By using RMS, you can specify who else has access to protected content, and what that person can do with the protected content.

RMS consists of three components. The first is a trusted entity that issues a root certificate. The RMS server technologies perform the work required to protect data and authorize its use. RMS client software must be installed to allow users to participate in an RMS environment. Finally, RMS-enabled applications must be developed, using the RMS SDK, to provide the ability to create, distribute, and view protected content.
Security Modules

This chapter would be incomplete without a brief glance at the underlying interface that supports Windows cryptographic-enabled applications, such as Microsoft Certificate Services and Microsoft Internet Explorer.

Cryptographic Application Programming Interface

Microsoft CryptoAPI provides a standardized set of cryptographic functions—such as CryptGenKey, CryptVerifySignature, and CryptEncrypt—that allow applications to offer security without having to maintain their own cache of keys or certificates or know the particulars of the cryptographic device they’re using. Because private keys are handled within the bounds of CryptoAPI, applications don’t need to fumble around with unprotected private-key information.

When used, CryptoAPI passes each of its cryptographic calls off to one of a number of cryptographic service providers (CSPs) that actually perform the operation. Figure 21-9 shows the relationship between the API and the service providers.

![Diagram](image)

Figure 21-9 Cryptographic service providers “plugged in” to CryptoAPI

Cryptographic Service Providers

Cryptographic service providers (CSPs) vary according to the algorithms they use, the key lengths they support, and the cryptographic tokens with which they interface. A vendor introducing a new type of smart card, for instance, writes a CSP for its smart card that “plugs in” to the CryptoAPI. Being able to plug in allows applications to use myriad new
and existing services without having to particularize their cryptographic calls to any one vendor-defined interface.

By displaying a list of available CSPs and allowing the user to choose, applications can take advantage of emerging technologies with little, if any, modification to their source code. Because CSPs provide the specific interface to the cryptographic device, whether it’s software-based or hardware-based, they are responsible for any initialization required, such as PIN or password validation.

**CAPICOM**

CAPICOM is a COM (Component Object Model) client that wraps the details of CryptoAPI in a higher level package. Whereas CryptoAPI requires the developer to have a working knowledge of C/C++, CAPICOM allows users of COM-enabled languages, such as Visual Basic Scripting Edition and C#, to take a more abstract view of the details of CryptoAPI.

**Data Protection API**

The Data Protection API (DPAPI) is a pair of functions that, as part of the CryptoAPI, enable the developer to encrypt and decrypt data. It often uses the logon credentials to perform its encryption and decryption, but can optionally prompt for a password. DPAPI uses the 3DES algorithm and therefore provides strong encryption for end-user applications.

**Summary**

This chapter covered basic security concepts as well as the major security components of Windows Server 2003. The following chapters continue with Windows Server 2003 security. Chapter 22 describes how to implement the concepts and components described in this chapter, Chapter 23 covers patch management, and Chapter 24 explains how to install and configure Certificate Services.
Chapter 22

Implementing Security

The Security Configuration Wizard .............................................. 734
Using Templates to Implement Security Policies ......................... 739
Using Security Configuration and Analysis ............................ 746
Using Windows Firewall ........................................................... 750
Enabling Authentication ......................................................... 751
Implementing Access Control .................................................. 757
Managing Certificates .............................................................. 760
Using Internet Protocol Security Policies ................................ 764
Securing Local Data ............................................................... 773
Auditing .................................................................................. 778
Using Microsoft Baseline Security Analyzer ............................ 781
What to Do When Hacked ....................................................... 782
Summary ................................................................................. 782

In the realm of computer security, one of the most common and critical mistakes administrators make is to confuse the presence of security features with a secure system. It’s not enough to piece together protocols, methods, and algorithms into a collage of security. In such environments, the weakest link usually goes unnoticed until it’s too late. To be effective, system security must be applied as a whole, and it needs to be well designed, complete, and easy to maintain.

This chapter introduces you to a number of tools that allow you to implement and manage security settings for your server. The first tool is the Security Configuration Wizard, which allows you to create, edit, and apply a number of security settings in a single application. We’ll cover the Windows Firewall, a fundamental tool to protect your server from intruders. We also delve into the intricacies of security templates, which are text files that contain all security settings for a system. We cover both authentication and what to do when unauthenticated visitors decide to pay a visit. A thorough understanding of the fundamentals of security is crucial to managing a secure and robust installation.
The Security Configuration Wizard

Well-designed systems are accompanied by policies that dictate how, when, and at what level security is applied. Complete systems provide multilevel security that is both sound and as transparent to the user as possible. Easily maintained systems allow administrators to centrally manage security and keep track of critical events. A flexible but easy-to-use tool for creating, editing, and applying security policies for your server is the Security Configuration Wizard.

Note Before you use the Security Configuration Wizard to harden a particular server, make sure that all roles (such as domain controller or application server) are active and properly configured on that server.

Installing the Wizard

To install the Security Configuration Wizard, start Add/Remove Programs in Control Panel. Select Add/Remove Windows Components. Select it from the list in the Windows Components Wizard (shown in Figure 22-1), and click Next. Have the installation media available, because you might be prompted for it. Click Finish to complete the installation.

Figure 22-1 Installing the Security Configuration Wizard

Verify installation was successful by checking that the Security Configuration Wizard option was added to the Administrative Tools. Note that this is not the only way you can use the Security Configuration Wizard. You can access the same functionality using the Security Configuration Wizard command-line tool, scwcmd.
Using the Wizard

Start the Security Configuration Wizard from the available Administrative Tools. Click Next to close the introductory window.

There are seven parts, or sections, of the Security Configuration Wizard. See Table 22-1 for a description.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting Security Configuration Wizard</td>
<td>Select the action to perform, select the server, and process the security configuration database.</td>
</tr>
<tr>
<td>Role-Based Service Configuration</td>
<td>Select the roles, client features, and administration options. Indicate how to handle unspecified services.</td>
</tr>
<tr>
<td>Network Security</td>
<td>Open and add ports.</td>
</tr>
<tr>
<td>Registry Settings</td>
<td>Specify outbound and inbound authentication methods.</td>
</tr>
<tr>
<td>Audit Policy</td>
<td>Specify the system audit policy.</td>
</tr>
<tr>
<td>Internet Information Services</td>
<td>Enable or disable dynamic content, handle existing virtual directories, and allow or prevent anonymous access.</td>
</tr>
<tr>
<td>Completing Security Configuration Wizard</td>
<td>Save and apply the new or changed security policy.</td>
</tr>
</tbody>
</table>

A security policy, in the most basic terms, is an XML file. The tool to perform operations on a security policy is the Security Configuration Wizard. The Security Configuration Wizard provides you with four options for dealing with security policies. You can create a new security policy, edit an existing policy, apply an existing policy, or roll back the last applied policy. (See Figure 22-2.) Let’s assume you are running the wizard for the first time; we need to create a new configuration by selecting the first option.

![Figure 22-2 Initial options of the Security Configuration Wizard](image-url)
When you create a new configuration, the current server settings are used as a baseline for future edits. By default, the local server is selected as the current server. Select the server whose baseline settings you want to use and click Next. The wizard will detect your settings and use them as the baseline settings. Once the wizard completes this task, you can view the security configuration database. Click Next to continue to the next phase of the wizard, Role-Based Service Configuration. (Click Next to dismiss the initial window of this phase.)

As you see in Figure 22-3, we have a single role for the current server. It’s a file server. Click Next to see the client features installed on the selected server. This might sound odd, but even your server can be a client to other servers, and this window displays the client features your server has installed. Clicking Next again to view the administration and other options that determine which services are enabled and which ports are open. Click Next once you have finished looking through these options.

Figure 22-3  Selecting server roles

The next step of the wizard allows you to specify what you want the server to do if it has a service enabled that is not listed in the configuration database. That is, if the server you’re exporting the Security Configuration Database to has services that aren’t available on the server with which you created the database, what should the new server do? You can either disable the service or leave the service as is.
The final step of the Role-Based Service Configuration portion of the wizard allows you to inspect the changes to the services that you’ve (indirectly) specified in the first steps of the wizard. Click Next to accept those service changes.

The next set of steps allows you to specify port options in Windows Firewall and specify encryption options for port traffic. Once you click Next to dismiss the introductory window, you will see the page that allows you to open ports and allow applications, as shown in Figure 22-4. You can deselect ports you want to close, though that may prevent your server from operating properly. You can also highlight a port and click the Advanced button to specify remote access and local interface restrictions for that port. Click Next once to view the port configuration resulting from the changes you made, and click next again to proceed to the next portion of the Security Configuration Wizard.

**Note** Use netstat to determine port usage. Be careful when you are restricting ports; you can easily lock yourself out of the system!

![Figure 22-4](image)

**Figure 22-4** Opening ports and approving applications

The Registry Settings options allow you to require server message block (SMB) security signatures, require Lightweight Directory Access Protocol (LDAP) signing, select the outbound authentication methods, and select inbound authentication methods. Of course, you’ll have the obligatory summary at the end, so you can go back and make changes if necessary.

The fifth portion of the wizard specifies options for the system audit policy. As you can see in Figure 22-5, you can select the audit objective. You can audit nothing (not recommended), audit successful activities, or audit successful and unsuccessful activities. The summary is displayed when you have finished. Click Next to move to the sixth stage.
Figure 22-5  Selecting an auditing objective

The Internet Information Services (IIS) options allow you to specify the security options with respect to your application server. You can select the Web service extensions the server requires, select the virtual directories to retain, and specify whether or not to deny anonymous write access to files on your Web site. (The last option is valid only if you are running IIS on an NTFS partition.) Click Next when you've selected your options, and click Next again to dismiss the IIS summary.

The final stage of the wizard allows you to save and apply the security policy you've developed in the preceding steps. As shown in Figure 22-6, you use options on this page to save the security policy and give it a meaningful description. You can also view the settings and include security templates at this point. After clicking Next, you will be prompted to apply the security settings now or later. Clicking Next finishes the wizard, with the policy written to a file and, if you opted to apply now, the security policy is applied to the system.

Figure 22-6  Writing the security policy to a file
Deploying the Policy

You can deploy the policy you’ve created in three ways. The first is the Security Configuration Wizard itself. The second is the command-line utility `scwcmd.exe`. The third mechanism available for deploying the policy is Group Policy.

The SCW is the best method to apply a security policy to a single server. On the Configuration Action window, click the Apply An Existing Security Policy button (see Figure 22-2) and follow the instructions. Next, specify the server to which you want to apply the policy and click Next twice. Once the application of your policy is complete, click Next and then click Finish to complete.

`Scwcmd.exe` allows you to easily configure multiple servers. Use the command `scwcmd configure` to view the available application parameters. To apply a security policy, use the command `scwcmd configure /p:filename /i:machine`, where `filename` is the file containing the security policy you want to apply and `machine` is the server you want to apply the policy to.

The `scwcmd.exe` command can also convert the XML-based security policy into a Group Policy object (GPO). Use the command `scwcmd transform /p:filename /g:gponame`, where `filename` is the security policy file and `gponame` is the name of the GPO. The GPO is automatically created in Active Directory and it is applied when you link it to an organizational unit.

Using Templates to Implement Security Policies

Microsoft Windows Server 2003, as you now know or are quickly learning, has a rich and diverse range of security features. With these features, however, comes a multitude of security policies and attribute settings that need to be configured. Configuring a system with policies consistent with your company’s security needs is, in itself, no small task. Multiply that by all the computers at your site or in your organization, and you have quite a chore. And that doesn’t include the maintenance time required whenever company policies need to be reevaluated.

Enter security templates. A security template, quite simply, is a configuration file for all the security attributes of a system. Security templates are powerful and help ease the strain of administration. Using a single interface, an administrator can generate a security template that reflects the security needs of a given server and then apply it to that server or import it into a Group Policy Object in the Active Directory service. When you incorporate the template into a Group Policy Object, all computers affected by that object receive the template settings.
Security templates can be created and modified with the Security Templates snap-in of the Microsoft Management Console (MMC). To add the snap-in to the MMC, do the following:

1. Run Mmc.exe from the Run dialog box, which you access from the Start menu.

2. From the File menu, choose Add/Remove Snap-in. Click Add on the Stand-Alone tab, and select Security Templates from the list of snap-ins provided.

3. Click Add in the Add Stand-Alone Snap-in dialog box to add the Security Templates entry to the Add/Remove Snap-in dialog box and then click Close.

4. Click OK in the Add/Remove Snap-in dialog box, and the Security Templates snap-in is added to Console Root in the console tree.

In the console tree, expand Security Templates and the Security\Templates folder to display an initial list of templates. These are predefined templates that can be tweaked for a company’s specific needs. When a new template is created or an existing one is copied, it’s added to this list. Select any one of these preloaded policies, and the right pane of the console displays all the security areas available for configuration. (See Figure 22-7.)

![Figure 22-7 Predefined security templates](image)

Essentially, each template in the list represents a single readable .INF file. The snap-in is merely an interface for modifying these security template files. The files can be found in the system root folder under %SystemRoot%\Security\Templates. The following is a small excerpt from the securews template (Securews.inf), showing the Account Policies area:

```plaintext
[System Access]
;----------------------------------------------------------------
;Account Policies - Password Policy
;----------------------------------------------------------------
MinimumPasswordAge = 2
MaximumPasswordAge = 42
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 24
RequireLogonToChangePassword = 0
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
EnableGuestAccount = 0
```
Examining Template Policies

Each template contains attribute settings for the seven areas of security configurable in Windows Server 2003. Double-click a security area in the right pane of the console or expand the console tree in the left pane to display the specific sections. Here are the seven configurable areas:

- **Account Policies**  The Account Policies area includes policies pertaining to user accounts. It contains Password Policy, Account Lockout Policy, and Kerberos Policy.

- **Local Policies**  The Local Policies area includes policies pertaining to who has local or network access to the computer and how events are audited. This area contains Audit Policy, User Rights Assignment, and Security Options.

- **Event Log**  The Event Log area contains attributes that determine how the application, security, and system event logs behave. Log attributes include maximum size and access restriction. Event logs can be viewed in Event Viewer.

- **Restricted Groups**  The Restricted Groups security setting is for adding members to built-in user groups, which have predefined capabilities, or to other administrator-defined groups that might be privileged. Built-in user groups include Administrators, Power Users, and Backup Operators.

- **System Services**  The System Services area includes security attributes of all system services on the local computer. System services include file services, print services, network services, and telephone services.

- **Registry**  The Registry area contains security attributes for existing registry keys, including auditing information and the access permissions.

- **File System**  The File System area allows the configuration of access permissions and auditing of specific directories and files on the local system.

Using Predefined Templates

The predefined templates supplied by Windows Server 2003 can be used as is, or they can be customized to conform to a more rigorous security requirement. These templates span a range of security levels and represent typical security scenarios for the different types of computers found in a system—namely workstations, servers, and domain controllers. Table 22-2 shows some of the predefined security templates, categorized by security level.

---

**Note**  These predefined templates intentionally omit user rights assignments so as not to overwrite any assignments made by application setup programs. This omission means that these security templates can be applied to a machine to reset the security configuration of that system.
If you’re familiar with Microsoft Windows 2000 Server, you’ll see that the basicws and basicdc security templates were removed to ensure that Windows Server 2003 is more secure. You must choose from more secure (and hence safer) security templates.

Secure Security Templates
Two secure templates are provided: one for the domain controller, and a combined template for the workstation and server. With stricter password and lockout policies and with audit logs that restrict guest access, the secure templates provide a medium layer of security.

Unsuccessful logon events and privilege use, as well as successful and unsuccessful account management and policy changes, are configured for auditing. In addition, the secure domain controller template provides auditing for object and directory service access. Account and local policies also appear in the secure domain controller template. Because the permissions of files, folders, and registry keys are configured securely by default, these security areas are omitted in this template type.

Real World  Strengthening the Secure Template Without Going Too Far
The secure template is generally a good template to apply to workstations and servers. However, consider the following settings that can improve security without compromising functionality, as some of the high-security templates do. All the following settings are in the Local Policies–Security Options container except the first one, which is in the Local Policies–Audit Policies container:

- **Audit System Events**  Success or Failure
- **Do Not Display Last User Name In Logon Screen**  Enabled
- **LAN Manager Authentication Level**  Send NTLMv2 response only or refuse LM and NTLM (This blocks MS-DOS, Microsoft 9.x, improperly-configured Windows NT 4.0, and OS/2 clients from logging on.)
Highly Secure Security Templates
The highly secure templates are actually quite lean and concentrate on the security of communications in native-mode (Windows XP and Windows Server 2003) environments. In short, security attributes are set for digitally signing client-side and server-side communications and for signing and encrypting secure channel data. Because maximum protocol protection is set, however, systems to which these templates are applied will not be able to communicate with machines running Microsoft Windows 95, Microsoft Windows 98, or Microsoft Windows NT. Aside from there being no Authenticated Users in the Power Users restricted group in the highly secure workstation/server (hisecws) template, the highly secure workstation/server and domain controller templates are essentially the same.

Compatible Security Template
The goal of the compatible security template is to allow most applications to run successfully, while not compromising the security levels of Power Users. The Compatible Security Template settings allow members of the local Users group to run only certified Windows applications, whereas only members of the Power Users group and above can run applications that are not certified. Therefore, if your users need to run uncertified applications, you must promote those users to at least Power User status.

Note
The net effect of promoting all Users to Power Users is lower system security. An alternative method that doesn’t compromise security is to make all users members of the Users group by default. Then adjust security settings to allow the execution of uncertified applications.

To facilitate flexible system usage for members of the Users group, a limited preset list of files, folders, and registry settings are modifiable under the Compatible Security Template.

Out-of-the-Box Security Templates
The setup security template contains security settings appropriate for the installation and initial configuration of workstations and servers. The domain controller security template builds on the setup security template, adding default security settings for domain controllers.
Modifying a Predefined Template
You can use a predefined template as a starting point for your own security scheme. First make a copy of it by right-clicking the template name and choosing Save As. Next specify a filename with the .INF extension. You can modify the attributes in any of the security areas of your new template by fully expanding the template tree to that area. For attributes, right-click an attribute name and choose Security from the shortcut menu to open the Template Security Policy Setting dialog box. For the Restricted Group, Registry, and File System folders, right-click the folder and choose Add Group, Add Key, or Add File, respectively.

Defining New Templates
You can also choose to generate an entirely new security template. In the console tree of the Security Templates snap-in, right-click the parent default template folder (%SystemRoot%\Security\Templates) and choose New Template. In the dialog box that appears, type a template name and a description of the template’s purpose. The new template is saved as an .INF file in the Templates folder and is added to the list of available templates.

At this point, the new template file is empty, except for some version and description info. Viewing any of the policy attributes in the new template lists attributes as Not Defined. The Restricted Groups, Registry, and File System folders contain no entries.

For each security area, you can configure any or all security attributes or you can choose to leave that area untouched. To modify an attribute’s settings, double-click the attribute in the right pane. The Template Security Policy Setting dialog box appears. Select the Define These Policy Settings In The Template check box to enable the settings and set the attribute. Figure 22-8 shows the dialog box for the Audit Account Logon Events attribute. Enabling this option allows you to track successful logon attempts, unsuccessful logon attempts, or both.

Figure 22-8 The dialog box for the Audit Account Logon Events attribute
It’s just as easy to configure security areas that contain a list of items instead of individual attributes. Right-click Restricted Groups, Registry, or File System, and select Add Group, Add Key, or Add File, respectively. You can then browse for the object to add and choose access permissions, ownership, and auditing information in the Access Control dialog box.

After the security template is complete, save it by right-clicking the template name and choosing Save. It’s then ready to be applied to the local computer or to a Group Policy Object.

---

**Planning** When creating new security templates for your system architecture, remember that security can be applied through the layering of templates. The configuration database allows templates to be imported one after another so that the security policies in the different templates have a masking effect. Conflicts of specific attributes are resolved by giving highest priority to the most recently loaded template. This means that templates with varying degrees of security do not need to contain redundant data. Instead, basic security attributes can be applied with a standard security template that you load first. Higher level security templates then need to contain only security differences between the two levels.

---

**Applying Templates**

A security template containing system security settings can be either applied to a local computer or pushed to a group of computers by importing it into a Group Policy object. Applying the template to a local computer is done through the Security Configuration and Analysis snap-in or using the Security Configuration Wizard. See the “Importing and Exporting Templates” section later in this chapter for detailed instructions.

To import the security template into a Group Policy Object, take the following steps:

1. Choose the target Group Policy object in the MMC.
2. Expand the object, and then expand Computer Configuration and Windows Settings to display Security Settings.
3. Right-click Security Settings, and choose Import Policy.
4. From the list of .INF files, choose the desired security templates.

---

**Note** Reduce the administrative hassle of configuring large arrays of security attributes by modifying predefined templates whenever possible.
Using Security Configuration and Analysis

Security Configuration and Analysis is an MMC snap-in that allows an administrator to check the state of a system’s security against one or more security templates and make appropriate modifications. Useful as both a setup tool and a maintenance tool, the snap-in lets you import predefined or modified security templates, analyze every security area against templates with a single command, and view concise results. You can then synchronize system security to the template at once or resolve discrepancies on an attribute-by-attribute basis.

This tool, along with an appropriate security template, is invaluable for setting up the initial security configuration of a machine on which many security attributes—and also file, folder, and registry-key permissions—have to be defined. A company or division’s entire computer security policy can be translated into a single template and imported to quickly configure one or more machines. In addition, the snap-in is useful for maintaining the security level of a system. Invariably, in the course of resolving temporary network or administrative problems, security attributes become disabled and permissions of objects are set to full access. Periodically analyzing a system’s security against its defining template allows you to locate and easily fix security flaws.

Finally, the tool permits you to export security templates that were modified during the configuration of a machine or to reevaluate such templates in the Security Templates snap-in. If more than one template has been imported, you can save a single composite template that is the sum of all the template settings.

Opening a Security Database

Like any other MMC snap-in, Security Configuration and Analysis is added to the MMC by choosing Add/Remove Snap-In from the Console menu. Click Add and select Security Configuration And Analysis from the list of snap-ins provided.

Security templates are imported into a database, which is used to perform the analysis and configuration. Security database files use an .SDB extension. To create a new database or open an existing one, do the following:

1. Right-click Security Configuration And Analysis, and choose Open Database.
2. In the Open Database dialog box, select an .SDB file to open or type a new filename to create a database.
3. When you type a new filename, a second dialog box appears allowing the import of a base security template.
4. Choose a predefined template or a template modified with the Security Templates snap-in.
5. The list of predefined templates is in the %SystemRoot%\Security\Templates folder.
Implementing Security

See the “Using Predefined Templates” section earlier in this chapter for an explanation of these security templates.

Importing and Exporting Templates

After you open a security database, you can import additional security templates into it. To do so, right-click Security Configuration And Analysis and choose Import Template. Select the .INF template file you want to import. This template supplements the current database template or templates; it does not replace them.

In the process of analyzing and configuring a system’s security with a database template, you might find it necessary to define a more precise policy and thereby modify the template. This modification is not saved to the original imported template; instead, it is saved as a database copy. To use the modified template on another machine, you need to export it. You can also combine multiple imported templates into a single composite template that you then export. To export a template, right-click Security Configuration And Analysis and choose Export Template. In the ensuing dialog box, choose a filename for the template, using the .INF extension.

Analyzing Security and Viewing the Results

After you import the necessary templates into the database, you can analyze the system. To analyze system security, right-click Security Configuration And Analysis and choose Analyze System Now. In the Perform Analysis dialog box, select the target path and filename of the analysis results. Click OK, and the Analyzing System Security progress window appears, as shown in Figure 22-9.

![Figure 22-9  The Analyzing System Security progress window](image)

The analysis generates two types of results. First, the success and failure of each analyzed component is written to an error log. Second, the security areas listed under Security Configuration And Analysis in the console tree are populated. Each area gives the analysis results in an attribute-by-attribute comparison. When the analysis is complete, view the error log by right-clicking Security Configuration And Analysis and choosing View Log...
File. The log appears in the right pane with a date and timestamp; it reports on the completion of each analyzed area. The following code is a small excerpt from a typical log file:

```
Log file: C:\My Documents\Security\Logs\NewDB.log

Monday, October 03, 2005 7:27:53 PM
----Analysis engine was initialized successfully.----

----Reading Configuration Info...

----Analyze User Rights... Analyze SeNetworkLogonRight.
Mismatch - SeNetworkLogonRight..

...

Registry values analysis completed successfully.

----Analyze available attachment engines... Attachment engines analysis completed successfully.

----Un-initialize analysis engine...
```

This log file does not show discrepancies in individual attributes but rather integral errors in the analysis. To view the actual analysis results, expand Security Configuration And Analysis in the console tree. The familiar seven areas of system security appear: Account Policies, Local Policies, Event Log, Restricted Groups, System Services, Registry, and File System.

To view analysis results for any of these areas, expand the area and highlight a subcategory. Restricted Groups and System Services are not hierarchical and need only to be highlighted. Figure 22-10 shows sample results for Security Options under Local Policies.

![Figure 22-10  Analysis results for Security Options](image)

In the right pane of the console, each attribute is followed by two settings: the stored template (database) setting, and the analyzed system (computer) setting. The icon for the attribute in which settings agree contains a green check mark. If the database and
computer settings differ, a red “X” punctuates the attribute icon. Attributes that are not configured in the template are not analyzed, and no marking appears in the icon.

Configuring Security

After you successfully analyze the system and find discrepancies between database and computer settings, you have a few alternatives. Depending on your evaluation of the results, you might decide that the current security template is not appropriate for this computer. A more stringent or relaxed template might be required, or perhaps vital attributes were left unconfigured and additional security areas need to be addressed. The solution is to import a template that is better suited to your particular security requirements. Templates can be added in increasing order of importance. New templates that are merged into the database override any conflicting attributes or permissions.

On the other hand, you might decide that the correct template was indeed used but that the specific setting used in the template was incorrect. In this case, you want to change the database template so that further analysis doesn’t show any discrepancies. To do so, right-click the offending attribute and choose Security to display a dialog box in which you can change the database template. For example, right-clicking the attribute that shows a conflict in Figure 22-10 displays the dialog box shown in Figure 22-11. You can change the template setting to match the computer setting, or you can deselect the Define This Policy In The Database check box to specify that the setting should no longer be considered during analysis.

Finally, you might determine that the security template is correct and that the system is in violation of your security policy and needs to be aligned. After you weed out all the template mismatches and only valid discrepancies remain, configure the system by right-clicking Security Configuration And Analysis and choosing Configure Computer Now.
Using Windows Firewall

Windows Firewall protects your system from unsolicited inbound connection attempts. It blocks traffic on unused ports to prevent what’s called an “unsolicited request” from an outside source. Windows Firewall is disabled by default for Windows Server 2003.

Access the Windows Firewall configuration utility from Control Panel. The utility has three tabs: General, Exceptions, and Advanced. The options on the General tab allow you to turn off the firewall completely (which is not recommended unless you’re using another host-based firewall to protect your system) or to disallow exceptions, in which case the Windows Firewall will prevent all incoming activity on any port and, though you won’t be notified by Windows Firewall, discarded traffic is logged. The latter option is useful if your server has been compromised and you are in a discovery and recovery mode. (See the section “What to Do When Hacked” later in this chapter for more information.)

Exceptions are ports or programs you want to leave open for particular programs or protocols that require certain open ports and would not work properly if those ports are blocked. You can specify a port be open—that is, create an exception for your firewall rules—on the Exceptions tab. For example, a Web browser usually accesses content from a server on port 80. (See Chapter 32 and Chapter 33.) Clearly, if your server is an Application Server for your organization or the Web itself, you probably want to leave TCP port 80 open so that the requests will get through. It just so happens that the server whose exception tab is displayed in Figure 22-12 has an exception for TCP traffic through port 80 and therefore accepts incoming request traffic over that port.

Figure 22-12  Firewall exceptions
The Advanced tab allows the administrator to specify which connections are protected by the Windows Firewall. You can also create a log file, which is a useful record of attack attempts on your server, or configure ICMP settings. Finally, you can restore all the Windows Firewall options to a default state by clicking the Restore Defaults button.

You can configure Windows Firewall by using Group Policy. Open the GPO, expand Computer Configuration, Administrative Templates, Network, Network Connections, and then Windows Firewall.

---


---

**Enabling Authentication**

Among its many other tasks, the domain controller authenticates users to a network, using security policies and user authentication information stored in Active Directory. During an *interactive logon* event, a user logs on to a domain account with a password or smart card. The domain controller confirms the user’s identity with the information stored in Active Directory. After an interactive logon event to a domain controller has taken place, *network authentication* is performed for the user without any further effort on the user’s part. The user can access resources on the network without having to reenter a password or smart card personal identification number (PIN). An interactive logon event can also authenticate a user to a local computer rather than a domain account. With a local interactive logon event, network authentication requires the reentry of a password any time the user needs to access a network resource.

The Kerberos version 5 authentication protocol is used for an interactive logon event and is also the default protocol for network authentication. Each domain controller includes Kerberos version 5. Both the key distribution center and the ticket-granting service are components of Kerberos and become integral parts of the domain controller. The key distribution center runs as part of Active Directory, which stores passwords and user account information for authentication. A Kerberos client is installed on all Microsoft Windows XP Professional and Windows Server 2003 machines. See Chapter 21 for more information about Kerberos authentication.

Remote access clients, in addition to logging on to the network, must be authenticated by the remote access server before they can access the network. Smart cards and certificates, as well as password-based protocols, are used for dial-up networking. The next section explains how to obtain and use cryptographic tokens for network authentication, as well as how to configure remote clients and servers.
Obtaining Smart Cards and Certificates

Smart cards combine the security of public-key cryptography with the portability of passwords. Before a smart card can be used for authentication, a logon certificate needs to be programmed onto the card. The administrator can accomplish this by using the Smart Card Enrollment station, which is integrated with Microsoft Certificate Services in Windows Server 2003.


Setting Up an Enrollment Agent

To request smart card certificates from a certificate authority (CA), the administrator needs a special certificate to sign the request. This certificate, known as an Enrollment Agent certificate, must be requested by a logged-on domain administrator from the dedicated machine that will be used to program smart cards. An enrollment agent certificate is a software-based certificate and private key that can be requested through the Certificates MMC snap-in. (See the “Requesting Certificates” section later in this chapter.) Be sure to use the enrollment agent certificate template as the basis for your certificate. Only this template produces certificates that allow the administrator to make smart card certificate requests.

Important  It’s possible, though highly inadvisable, to allow users to program their own smart cards by giving them access rights to the enrollment agent certificate template. Administrative programming and distribution of smart cards provides more accountability.

Programming Smart Cards

After the administrator installs a smart card reader on a system and obtains the enrollment agent certificate, the system is ready to program smart cards. Smart card installation adds a cryptographic service provider (CSP) to the system that is to be selected during the smart card programming process. (See Chapter 21 for more information.)

The Web-based request process first generates a public/private-key pair on your smart card. Using the public key and the user’s name, the CA issues and signs a certificate. Finally the certificate is added to the smart card. To program a smart card, follow these steps:

1. Log on as the enrollment agent.

Note  An enrollment agent is anyone in the domain who has an Enrollment Agent certificate and has security permissions to issue smart card certificates.
2. Open Microsoft Internet Explorer, and specify the URL of the server that houses the certification authority. This URL ends with /Certsrv.


4. Click Request A Certificate For A Smart Card User Using The Smart Card Certificate Enrollment Station. Click Yes if prompted to accept the certificate.

5. The Smart Card Enrollment Station Web page appears. Set the fields to the values shown in Table 22-3.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification Template</td>
<td>Smart Card Logon (if you want to use the smart card for logging on to Windows only)</td>
</tr>
<tr>
<td></td>
<td>Smart Card User (if you want to use the smart card for e-mail as well as logging on to Windows)</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>CA to issue certificate</td>
</tr>
<tr>
<td>Cryptographic Service Provider</td>
<td>The smart card manufacturer’s CSP</td>
</tr>
<tr>
<td>Administrator Signing Certificate</td>
<td>The enrollment agent certificate (discussed in the previous section)</td>
</tr>
</tbody>
</table>

6. In User To Enroll, click the Select User option, and then choose the user account. Finally, click Enroll.

7. Click Submit Certificate Request.

8. Insert the smart card when prompted, and then click OK. Type the PIN when the system prompts you. If the smart card has already been programmed, you are prompted to verify that you want to reprogram it.

9. You can now view the certificate or make a new smart card certificate request.

Note Smart card certificates for users requiring different functionality (such as encryption) can be programmed similarly by specifying a different certification template.

Obtaining Software-Based Certificates
Authentication can also be accomplished with private keys and certificates residing on a local computer. See the “Requesting Certificates” section later in this chapter for information about how to obtain a certificate through the Certificates snap-in.

Logging On with Smart Cards
After a smart card reader is installed on the target system and the user obtains a properly programmed smart card from the administrator, the user can use the smart card to log on
to the computer. To do so, the user inserts the smart card into the reader and types a PIN when prompted to do so. This process takes the place of pressing Ctrl+Alt+Del and typing a user name and password.

**Important** To keep thieves from accessing the system by using a stolen card, the system tracks incorrect logon attempts. After a number of consecutive failures, the card is locked out of the system. The number of allowed failures varies with the hardware; the smart card manufacturer specifies the number of failures, so you have to read the smart card documentation for the specifics.

**Enabling Remote Certificate or Smart Card Authentication**

As was mentioned earlier, a user’s public-key certificate, used for authentication, can be either programmed onto a smart card or stored locally on the computer. Follow the steps in the next two sections to enable dial-in authentication for each scenario.

**Authentication with Certificate on Smart Card**

To enable authentication with a certificate that resides on a smart card, follow these steps:

1. From the Start menu on the remote machine, open Control Panel and double-click Network Connections.

2. Right-click the network or dial-up connection for which you want to enable authentication, and choose Properties. In the Properties window for the connection, click the Security tab (shown in Figure 22-13).
3. Ensure that Typical is selected and that the Validate My Identity As Follows list is set to Use Smart Card, as shown in Figure 22-13. The Require Data Encryption check box can be selected for additional security.

**Authentication with Certificate Stored on Local Computer**

To enable authentication with a certificate that is stored on a local computer, follow these steps:

1. From the Start menu on the remote machine, open Control Panel and double-click Network Connections.

2. Right-click the network or dial-up connection for which you want to enable authentication, and choose Properties. In the Properties window for the connection, click the Security tab (shown in Figure 22-13).

3. Click the Advanced (Custom Settings) button in the connection’s Properties window, and click the Settings button. In the Advanced Security Settings dialog box, shown in Figure 22-14, select Use Extensible Authentication Protocol (EAP) and make sure the list box shows Smart Card Or Other Certificate (Encryption Enabled).

4. Click Properties to display the Smart Card Or Other Certificate Properties dialog box, as shown in Figure 22-15. To configure authentication for certificates residing in the local certificate store, select Use A Certificate On This Computer.
5. Two other certificate-specific options appear in this window. First you can restrict connections to specific servers. To do this, select the Validate Server Certificate option and activate one or both of the validation methods:

- **Connect Only If Server Name Ends With** This option requires servers to be in a certain domain. For instance, type `netsolvers.com` in this box to connect only to servers in the Netsolver domain.

- **Trusted Root Certificate Authority** This option lets you choose which certificate hierarchy the server belongs to. See the “Importing Certificates” section later in this chapter for information about how to add a certificate as a root CA.

The second option, Use A Different User Name For The Connection, keeps the authentication process from automatically using the certificate subject as the user name. This allows you to specify an alternate name.

6. Click OK to accept your changes and close the window.

**Planning** Whether you’re using smart card–based authentication, password-based authentication, or a mix of the two, ensure that your remote access clients and remote access servers support at least one common authentication method.
Configuring Authentication for a Remote Access Server

In addition to configuring the remote access client, you also need to set up the remote access server to allow smart card–based and certificate-based logon events. Follow these steps to do so:

1. Choose Routing And Remote Access from the Administrative Tools folder on the Programs menu.
2. Right-click the name of the remote access server, and choose Properties. On the Security tab, click Authentication Methods, ensure that the Extensible Authentication Protocol (EAP) check box is selected, and then click OK twice.
3. Back in the Routing And Remote Access dialog box, expand the remote access server and click Remote Access Policies. Right-click the policy that is to be used when the smart card clients log on, and choose Properties. Click Edit Profile, and in the Edit Dial-In Profile dialog box, click the Authentication tab. Click EAP Methods. If the Smart Card Or Other Certificate EAP type is not listed, click Add, click Smart Card Or Other Certificate, and then click OK. Click Edit to view the properties of the Smart Card Or Other Certificate EAP type and verify that the correct computer certificate is selected.

**Note**  If your remote access server is configured for RADIUS authentication, you can view and alter the security settings by right-clicking the server’s node, choosing Properties, and then selecting the Security tab on the Properties screen that appears.

**Note**  If clicking Configure returns an error stating that no certificate could be found, a machine certificate needs to be installed. You can do this by ensuring that your enterprise CA is configured for computer certificate auto-enrollment, which automatically allocates computer certificates for members of the domain. With this configured, run `gpupdate` from a command prompt on your remote access server to obtain a computer certificate.

Implementing Access Control

In the real world, authorization is dictated by policy. When it comes to using resources, reading documents, or accessing rooms, different people have different access rights. The implementation of this policy can be locked safes or badge-access
rooms. In the Windows Server 2003 environment, authorization is also based on policy. Different people or groups of people have different access rights. Policy here is implemented through access control. Quite simply, access control determines which users can access which resources. Resources in Windows Server 2003 are described in the following list:

- Files and folders, which can be accessed through Windows Explorer
- Shared volumes, folders, and files
- Active Directory objects, which are managed with the Active Directory Users and Computers snap-in
- Registry keys, which are managed with the Registry Editor
- Services, which are managed with the Security Configuration Tool Set
- Printers, which are configured through Settings on the Start menu

Each resource has a security descriptor associated with it that defines the object’s owner, the object’s access permissions, and the object’s auditing information. Auditing of the object is discussed in the “Auditing” section later in this chapter.

For Active Directory objects, administrative responsibility can be delegated to group administrators. Delegating allows object permissions to be managed in one organizational unit of the domain, without requiring multiple administrators for the entire domain. For more information, see Chapter 9.

**Establishing Ownership**

The owner of an object controls who can access the object by setting object permissions. By default, the object’s owner is its creator. Typically, administrators create most network objects and are responsible for setting the object permissions.

One of the standard permissions associated with all objects is the Take Ownership permission. By granting this permission, the owner allows a user (or member of a group) to assume ownership of the object. Taking ownership can be done through the tool that manages the specific type of object. For example, printers are managed through the interface found under Settings on the Start menu. The Security tab on the Properties window for the printer shows the groups and users for which permissions are set. Clicking Advanced opens the Advanced Security Settings dialog box. With the correct permissions, ownership can be modified on the Owner tab. Administrators can assume control of any object under their administrative jurisdiction, regardless of the setting of the Take Ownership permission for the object.
Assigning Permissions

Object permissions are broken down into specific actions that can be performed on that particular object. For registry keys, this includes the ability to create subkeys and set values. For Active Directory objects, permissions include the ability to create and delete children.

Permissions are set for the specific users or groups who perform actions on a particular object. For a given folder, one group might be granted permissions to create and delete files within that folder. Another group might be allowed only to list the folder’s contents. Figure 22-16 shows printer permissions granted to the Everyone group.

![Access Control Settings dialog box](image)

**Figure 22-16 Printer permissions for the Everyone group**

To display permissions for a user or group, choose an entry in the Advanced Security Settings dialog box, and click Edit. The owner of the object, or a user or group granted Change Permissions permission, can use this dialog box to modify permissions for the user or group. To add a user or group to the access control list (shown in Figure 22-17), click Add and select the user or group to add. Remember to set the appropriate permissions.

**Note** You can ease the burden of administering a domain of user rights and permissions by following a few guidelines. First, delegate administration to local authorities whenever closer management of users and services makes sense. Second, assign permissions on a group basis, rather than on a user basis. Third, set permissions at common node points in Active Directory and let them propagate down the tree to lower nodes.
Managing Certificates

Public-key certificates serve as the security medium for many of the Windows Server 2003 protocols and mechanisms. Network authentication, IPSec, Encrypting File System (EFS), Secure Sockets Layer (SSL), and Secure Multipurpose Internet Mail Extensions (S/MIME) all use certificates. The MMC provides the Certificates snap-in for the single purpose of managing user, computer, and service certificates.

To add the Certificates snap-in to the MMC, run `Mmc.exe` from the Start menu. From the File menu, select Add/Remove Snap-In. Click Add and select Certificates from the list of snap-ins provided. You're given a choice of which account to manage certificates for: My User Account, Service Account, or Computer Account. For the service and computer accounts, you can select which computer the snap-in will manage. For the service account, you also need to specify which service to manage.

**Note** Each account with user-level permissions can administer his or her personal certificate. To administer the certificates for the local computer account or computer service, local administrator permissions are required.

The certificate store is made up of five categories: Personal, Trusted Root Certification Authorities, Enterprise Trust, Intermediate Certification Authorities, and Active Directory User Object. Other categories may also be available based on your server configuration. Trusted Root and Intermediate CA certificates are preloaded. To view the details of any certificate, double-click the certificate. Figure 22-18 shows the public key of a VeriSign root certificate.
Exporting Certificates and Private Keys

The Export command in the Certificates snap-in provides two distinct functions. First, it allows a certificate or certificate chain to be exported for the purpose of sharing it with users or computers that are not privy to a certificate directory. Second, it allows the export of a certificate or certificate chain along with the associated private key for cryptographic use on another machine.

Note  By default, only private keys for basic EFS and EFS recovery agents are marked as available for export. This keeps all other private keys from being unnecessarily exposed. Certificates and keys that are purposely meant to be exported can be marked during certificate request.

You can export any type of certificate, including those in root CAs. Naturally, only certificates with available private keys (that is, personal certificates) that are marked as exported can be exported together. To export a certificate, follow these steps:

1. Find the certificate in the Certificates snap-in, and right-click the entry.
2. Point to All Tasks, and choose Export. You’re welcomed to the Certificate Export Wizard.
3. Make your way through the wizard, choosing whether to export the private key (if available).
4. Choose the format for storing the certificate. DER Encoded Binary and Base 64 Encoded are single-certificate formats. With the PKCS #7 format, you can include the full certificate chain. Private-key combinations are stored in a PKCS #12 file and are password protected; you need to specify a password lor the file.
5. Type a target path and filename for the exported certificate.
Note With a highly populated certificate database, finding a particular certificate for exporting or enabling might be difficult. Use the Find Certificate command, found by right-clicking the Certificates snap-in, to locate certificates by issuer (Issued By), subject (Issued To), fingerprint (SHA1 Hash or MD5 Hash), or serial number.

Importing Certificates

Users can import certificates into any one of the certificate categories found in the certificate store. In the Certificates snap-in, right-click the certificate category to which you want to import the certificate, point to All Tasks, and choose Import. Type the certificate filename, which should have a standard certificate format extension (.PFX, .P12, .CER, .CRT, .P7B, .STL, .SPC, .CRL, or .SST). For PKCS #12 files, which contain private keys as well as certificates, type the password used to protect the file.

Security Alert Root certificates are the basis of trust for certificate verification. Be extremely careful when importing a root certificate. Ensure that the certificate was received from a trusted source and that the certificate thumbprint matches a trusted publication.

Requesting Certificates

Before using any application that relies on the public-key infrastructure, you need a certificate. Chapter 24 covers how to configure and install Microsoft Certificate Services. Certificate servers configured to be enterprise CAs in Active Directory environments can request certificates by using the Certificates snap-in.

Note Using Internet Explorer, you can request certificates from Microsoft Certificate Services, running in either Standalone or Enterprise mode, through the Web interface.

The certificate request process involves first generating a key pair consisting of a public key and a private key. The private key is stored and protected on the local computer. The public key, along with information identifying the user, is sent to the CA as a certificate request. If the CA determines that the user, device, or service is authorized for the certificate being requested, the CA generates and signs the certificate. The certificate can then be retrieved with the Certificates snap-in and placed in the local certificate store.

To request a certificate from an enterprise CA, open a MMC console with the Certificates snap-in installed and right-click the Certificates folder under the Personal certificate store. Point to All Tasks, choose Request New Certificate, and follow the instructions in the Certificate Request Wizard. You need to choose a certificate type (the purpose for which
the certificate is to be used), a friendly name for the certificate, and the CA that is to issue the certificate, if more than one is available. To allow you to download the certificate after the CA issues it, the Certificate Request Wizard provides the Install Certificate option.

**Security Alert** The advanced options of the Certificate Request Wizard allow private keys to be exported. Be extremely judicious when selecting this option. Exported private keys can allow other users to read your encrypted data.

### Enabling Certificates for Specific Purposes

Certificates can be issued for specific types of uses. These uses are programmed directly into the certificate, using a certificate extension field. For example, the Key Usage certificate extension tells whether a certificate can be used for data signing, certificate signing, nonrepudiation, or other functions. The Enhanced Key Usage extension extends this property to other uses, such as time stamping or file recovery.

Certificates can also be enabled for certain purposes on an account basis. That is, a user or administrator can decide which certificates to allow or disallow for specific uses. Although the actual certificate can’t be modified, the attributes in the certificate store can be configured. For example, a certain certificate might have no internal key usage restriction. However, a user might want to enable that certificate only for code signing and secure e-mail.

To set certificate purposes, right-click the certificate and choose Properties. The three choices for enabling certificate purposes, as shown in Figure 22-19, are Enable All Purposes For This Certificate, Disable All Purposes For This Certificate, and Enable Only The Following Purposes. Choose the third option, and select the purposes you want that certificate used for. Remember that only purposes allowed by the actual certificate or certificate path appear in the list.

![Figure 22-19 Options for enabling certificate purposes](image-url)
Using Internet Protocol Security Policies

IPSec provides end-to-end security for network communications—in the form of confidentiality, integrity, and authentication—using public-key technology to protect individual IP packets. Chapter 21 provides a description of this protocol. This section covers the MMC snap-in for IPSec configuration, IP Security Policy Management.

To add the IP Security Policy Management snap-in to the MMC, select Add/Remove Snap-In from the Console menu. Click Add, and select IP Security Policy Management from the list of available snap-ins. The dialog box that appears allows you to select the range of management: the local computer, the local computer’s domain, another domain, or another computer.

Defining IPSec Policies

An IPSec policy is passed from the policy agent to the IPSec driver and defines proper procedures for all facets of the protocol, from when and how to secure data to what security methods to use. Before jumping into the actual configuration, let’s go over some terminology by defining the components of an IPSec policy:

- **IP filter** A subset of network traffic based on IP address, port, and transport protocol. It tells the IPSec driver what outbound and inbound traffic should be secured.

- **IP filter list** The concatenation of one or more IP filters, defining a range of network traffic.

- **Filter action** What the IPSec driver should do with network traffic.

- **Authentication method** How identities are verified for the pair of computers to which an IPSec rule applies.

- **Security method** Security algorithms used for data confidentiality, data integrity, authentication, and key exchange.

- **Tunnel setting** The IP address or DNS name of the tunnel endpoint (if using IPSec tunneling to protect the packet destination).

- **Connection type** The type of connection affected by the IPSec policy: remote access, LAN, or all network connections.

- **Rule** A composite of the components: an IP filter list, a filter action, one or more authentication methods, a tunnel setting, and a connection type. An IPSec policy can have multiple rules to manage each subset of network traffic differently.
Using Predefined IPSec Policies

Three basic predefined policies are available for immediate use or as a starting point for more involved IPSec policies. Figure 22-20 shows the predefined policies.

![Figure 22-20  The three predefined IPSec policies](image)

Use the Client (Respond Only) policy on computers that normally do not send secured data. This policy does not initiate secure communications. If security is requested by a server, the client responds, securing only the requested protocol and port traffic with that server.

The Server (Request Security) policy can be used on any computer—client or server—that needs to initiate secure communications. Unlike the Client policy, the Server policy attempts to protect all outbound transmissions. Unsecured inbound transmissions are accepted but not resolved until IPSec requests security from the sender for all subsequent transmissions.

The strictest of the predefined policies, the Secure Server (Require Security) policy neither sends nor accepts unsecured transmissions. Clients attempting to communicate with a secure server must use at least the Server predefined policy or an equivalent because after this policy is enabled, the server will only accept inbound IPSec-enabled TCP/IP sessions that have been authenticated with Kerberos.

The section that follows demonstrates how to generate an IPSec policy from scratch. Let’s first peruse one of the predefined policies. Notice the Secure Server policy in Figure 22-20. Right-clicking this policy and choosing Properties brings up the Secure Server (Require Security) Properties window, with the Rules tab in the foreground, as shown in Figure 22-21.

![Figure 22-21  Secure Server (Require Security) Properties window](image)

This policy has three rules, all activated, as indicated by the check marks. The first rule has an IP filter of All IP Traffic, a filter action of Require Security, an authentication method of Kerberos, a tunnel setting of None, and a connection type of All. A rule can be added or removed from this list with the appropriate buttons. Clicking Edit brings up an Edit Rule Properties dialog box with five tabs, one for configuring each field of the rule. (See Figure 22-22.)
These configurations are explored in the next section. Back in the Secure Server (Require Security) Properties window (Figure 22-21), you can view the general properties of the policy—including a policy description and minute intervals at which to check for policy change—by clicking the General tab.

Clicking Settings on the General tab displays a Key Exchange Settings dialog box, shown in Figure 22-23. This dialog box allows you to specify the life of a key in minutes or ses-
Implementing Security

Using a short key lifetime makes transmission more secure by increasing the number of keys that an attacker has to break, but it adds overhead to transmission time. Selecting the Master Key Perfect Forward Secrecy check box ensures that existing keys cannot be reused to generate additional keys. Use this option with caution because it adds significant overhead. Clicking Methods allows you to select security methods and preference order. A security method includes an encryption and integrity algorithm, along with a Diffie-Hellman group, which affects key generation.

Figure 22-23  The Key Exchange Settings dialog box

Note  For more information about IPSec, visit http://www.microsoft.com/windowsserver2003/technologies/networking/ipsec/default.mspx.

Creating an IPSec Policy

In addition to using a predefined IPSec policy as a template, an administrator can generate policies from the ground up with the IP Security Policies item in the MMC. A custom policy can be restrictive or permissive, simple or powerful, depending on the function of the machine, the environment in which it operates, and the types of systems with which it communicates.

To add an IPSec policy, right-click the IP Security Policies item in the MMC and select Create IP Security Policy. You're presented with the IP Security Policy Wizard. The following steps guide you through this wizard:

1. Click Next at the Welcome page.
2. Type a meaningful policy name and description, and click Next.
3. Select or clear the Activate The Default Response Rule check box, based on whether the policy should allow negotiation with computers that request IPSec. Clearing this check box adds an inactivated response rule to the policy. Click Next.

4. If you selected the Activate The Default Response Rule check box in the previous step, you see the dialog box shown in Figure 22-24, in which you choose the authentication method. Kerberos version 5 is the Active Directory default protocol but is allowed only on machines that are members of an Active Directory domain. The second choice, Use A Certificate From This Certificate Authority (CA), promotes public-key authentication. You need to choose a CA that is appropriate for the certificate to be used. The third and final option allows you to type a pre-shared key that will be used for key exchange. This string must also be known by the requesting computer for successful exchange. Click Next when you make your choice.

5. Select the Edit Properties check box if you want to display the policy's Properties window. You can also display this window by right-clicking the policy after it's listed and choosing Properties.

**Editing an IPSec Policy**

The previous section showed how to create an IPSec policy, but to add functionality to your policy, you need to edit it. (To do so, right-click the policy and choose Properties.) Figure 22-21 shows the Properties window for an IPSec policy. A newly created policy...
contains only one default response rule, which is activated—or not activated—depending on the choices you made in the wizard during policy creation.

You add functionality to an IPSec policy by creating rules that govern when and how security is to be applied based on the type of TCP/IP traffic being sent/received on the system. Each combination of a filter list, filter action, authentication method, tunnel setting, and connection type is a separate rule.

Rules can be added manually or with the Add Wizard; both accomplish the same thing, but the wizard is a bit friendlier. Turn off the Add Wizard by clearing the Use Add Wizard check box in the lower right corner of the Properties window for the policy. Doing so allows you to explore each aspect of a rule in its native dialog box. Editing rules after they’re created is done through this interface as well.

With the Add Wizard turned off, click Add. You’re presented with the New Rule Properties dialog box, which, except for the title, is the same as the Edit Rule Properties dialog box shown in Figure 22-22. The dialog box has five tabs, one for each element of a rule. Here’s a look at each of the tabs in turn.

**IP Filter List**

The IP filter list is made up of one or more filters that specify which network traffic to act on. As shown in Figure 22-25, the All IP Traffic and the All ICMP Traffic filter lists are added by default but are not activated. In the figure, a third filter list has been added and activated by clicking its option button.

![Figure 22-25 The IP Filter List tab of the New Rule Properties dialog box](image)

Clicking Add brings up the IP Filter List dialog box, which allows you to specify filters to include in a customized filter list. Figure 22-26 shows a filter list under construction.
Here, if you click Add with the Use Add Wizard option selected, the IP Filter Wizard starts, which allows you to construct a new filter based on the following categories:

- **Addressing** Filters the source and destination addresses specified by IP address (My IP Address, Any IP Address, Specific IP Address, Specific IP Subnet, DNS Servers, WINS Servers, DHCP server, or Default Gateway) or a specific DNS name

- **Protocol** Filters by protocol type, such as TCP, and source and destination ports

![The IP Filter List dialog box](image)

**Figure 22-26** The IP Filter List dialog box

**Filter Action**

The filter action determines how the IPSec driver responds to types of traffic represented by entries in the filter list and what security methods to use. You can choose one of the supplied actions shown in Figure 22-27 by selecting it, or you can add your own action.

The Request Security action causes the driver to attempt to establish secure communications with the client, but if this is unsuccessful it communicates without security. The Require Security action requires clients to establish trust and security methods. The Permit action allows unsecured IP packets to pass through. The Block action does exactly that: it causes the driver to block packets.

Adding an action involves choosing a filter name, a description, and general behavior that permits communications, blocks communications, or negotiates security. If you choose to negotiate security, you need to configure two other areas.
In the Communicating With Computers That Do Not Support IPSec step of the Add Filter Action Wizard, you must choose either to disallow communications with those computers or to allow unsecured communication.

In the IP Traffic Security step of the Add Filter Action Wizard, you must select a Security Method: Integrity and Encryption, Integrity Only, or Custom. For the custom security method, you choose encryption and integrity algorithms and specify session key settings such as how often to generate new keys.

### Authentication Methods

The authentication method specifies how trust is to be established with the remote computer. You can specify one or more methods to use when requesting secure communications or when being requested for secure communications. Figure 22-28 shows three allowable authentication methods, listed in order of preference. Change the priority of a method with the Move Up and Move Down buttons. The Add button provides you with the following three choices for a new method:

- **Windows 2000 Default (Kerberos V5 Protocol)** This option uses Kerberos V5, which enables interoperability with Windows 2000 machines in their default configuration.

- **Use A Certificate** This option uses public-key certificates for authentication. You need to specify the CA of users or entities to authenticate. To allow authentication for users under separate CAs, add a separate authentication method for each.

- **Use This String To Protect The Key Exchange** This option uses a preshared key that you specify in the box provided. You can use multiple preshared keys by adding additional authentication methods.
Figure 22-28 The Authentication Methods tab of the Edit Rule Properties dialog box

*Note* If you selected the Permit option in the Filter Action tab, you will not be able to change the settings on the Authentication Methods tab.

**Tunnel Setting**

The Tunnel Setting tab allows you to specify a tunneling endpoint if you choose to invoke IPSec tunneling. The endpoint can be specified as a DNS name if you're running DNS service on your network, or it can be in the form of an IP address.

**Connection Type**

Finally, the Connection Type tab allows you to further refine a rule based on connection type. The All Network Connections option is set as the default; you can instead select either Local Area Network or Remote Access to create a stricter rule.

**Assigning IPSec Policies**

After an IPSec policy is established in the IP Security Policies item in the MMC, it can be applied to a single machine or to a set of computers governed by a Group Policy Object. To assign an IPSec policy to a local machine, right-click the policy name and choose Assign. The active policy's icon includes a green dot. If another policy has already been assigned, this action resets that policy for this computer. Assign IPSec policies to groups by selecting the target Group Policy Object in the MMC. Under this object, expand Computer Configuration, Windows Settings, and then Security Settings. Select IP Security Policies, right-click the desired policy, and choose Assign.

*Note* IPSec policies can be transferred using the Import Policies and Export Policies commands on the Action menu under All Tasks.
Securing Local Data

Encryption of stored files in Windows Server 2003 is accomplished through the use of EFS. Using public-key encryption, EFS allows files and directories stored on NTFS partitions to be encrypted and decrypted transparently. EFS accesses the user's EFS public and private keys to perform self-encryption. In addition, if files encrypted with EFS are saved to another machine, the user's key information must be imported into that machine for decryption to occur.

File encryption keys are automatically encrypted by the recovery agent key. In the event of key loss, the recovery agent can decrypt the files. EFS encrypts the bulk of the file with a single symmetric key. The symmetric key is then encrypted twice: once with the user's EFS public key to allow decryption, and once with the recovery agent's public key to allow data recovery. See Chapter 21 for more information about data encryption.

Creating a Recovery Policy

It's deceptively simple to encrypt and decrypt files in Windows Server 2003. Of course, anything that's sensitive enough to be encrypted should be treated very carefully, so take time to think before implementing file and folder encryption.

First, implement a recovery policy. As mentioned earlier in this chapter, the recovery policy provides a way to recover an encrypted file when its key has been lost. To recover the file, the recovery certificate for the recovery agent (a specially designated user account) is used. On an Active Directory domain, the recovery agent is set automatically to the Administrator account on the first domain controller of the domain.

Security Alert  We suggest that you create a special account just for the recovery agent role, and then assign the recovery agent role to this account. Because the recovery agent is such a sensitive role (specifically, it's capable of decrypting any file on the domain), it's imperative that you take proper precautions with it.

Because the recovery agent is such a sensitive role (specifically, it's capable of decrypting any file on the domain), it's imperative that you take proper precautions with it. The following steps take you through adding extra recovery agents, backing up the recovery certificate to a floppy disk, and deleting the locally stored recovery key for extra security:

1. Launch the Active Directory Users and Computers snap-in.
2. Right-click the appropriate domain or OU, and choose Properties from the shortcut menu.
3. On the Group Policy tab, select the appropriate policy and click Edit.

4. In the console tree, select Computer Configuration, then Windows Settings, Security Settings, and finally Public Key Policies.


6. Right-click the Encrypted Data Recovery Agents folder, and choose Add Data Recovery Agent from the shortcut menu.

7. Use the Add Recovery Agent Wizard to add another recovery agent to the domain or OU. (Microsoft recommends two or more recovery agents per OU.)

---

**Note** Create recovery agent accounts specifically for the recovery agent role, and do not use them for anything else. Replace the default Administrator recovery agent with one of the new, specially created, recovery agent accounts to minimize the impact of the Administrator account getting compromised.

---

8. Right-click a recovery agent, and choose All Tasks and then Export from the shortcut menu.

9. Use the Certificate Export Wizard to export the recovery key to an external storage device, such as a USB key or floppy disk. Store it in a highly secure, preferably off-site, location.

10. Log on using the recovery agent’s account, and then open the Certificates MMC snap-in. (If prompted, select My User Account and click OK.) You might have to open a blank MMC console and add the Certificates snap-in to it.

11. From the console tree, select Personal and then Certificates.

12. Select the certificate corresponding to the recovery key that you exported, and then click the Delete toolbar button. Now the only copy of the recovery key is stored separately in a secured location. Even someone with physical access to the computer does not have access to the recovery key.

---

**Note** You can easily create a recovery agent. For a local computer, add the Group Policy Object Editor snap-in to the MMC console. Select the Local Computer, click Close, and then click OK. Expand Local Computer Policy, Computer Configuration, Windows Settings, Security Settings, and then Public Key Policies. In the rightmost pane, right-click Encrypting File System and click Add Data Recovery Agent from the menu. You can also use the cipher /r command to generate a PFX and a CER file together with a self-signed EFS recovery certificate.
Encrypting Files and Folders

Encrypting files with EFS is as easy as setting any other file attribute, such as Hidden or Read-Only. To encrypt a file in Windows Explorer, follow these steps:

1. Right-click the file and choose Properties.
2. On the General tab, click Advanced.
3. Select the Encrypt Contents To Secure Data check box.

**Important** Encrypt entire folders only. If you encrypt individual files but not their folders, a program might create a temporary file (which won’t be encrypted) and then save the file over the original file, thereby leaving the file decrypted.

**Note** Remember that system files, compressed files, and files on partitions other than NTFS can’t be encrypted using EFS. Further, a drive’s root folder cannot be encrypted using EFS.

Like normal files, encrypted files can be moved and copied with the Edit menu commands Cut, Copy, and Paste. Files moved or copied using drag-and-drop editing do not necessarily retain their encryption. You can also rename encrypted files as you do any other file.

**Important** Encrypted files and directories are not immune from deletion. Any user with appropriate rights can delete an encrypted file.

You can use the same method for encrypting a folder as you use for encrypting a file. When encrypting a folder, you are asked whether you want all files and folders contained in the current folder to be encrypted. If you choose to encrypt them, they are immediately encrypted, but if you choose not to, only the folder is encrypted. No matter which you choose, however, any files or folders subsequently added to the encrypted folder are encrypted as well.

**Note** To ensure the security of temporary files that have been created by applications, mark your system’s Temp folder for encryption.

Decrypting Files and Folders

EFS allows a user to reverse the encryption process. However, describing this as a mere decryption operation is a bit misleading. Indeed, removing data encryption from a file does cause the file to be decrypted, but any encrypted file is also decrypted every time a user or application accesses it. This is permanent decryption.
Real World  Encryption Best Practices

Here are some encryption best practices to consider:

- Encrypt the My Documents folder of sensitive desktops and laptops.
- Encrypt the Temp folders of appropriate user profiles to protect temporary data, or data that was marooned in the Temp folder following a program crash.
- If you use spool files while printing, encrypt the Spool folder.
- Don’t tamper with the EFS keys.

To indicate that a file no longer needs to be encrypted or that a folder no longer needs to encrypt its files, follow these steps:

1. Right-click the file or folder in Windows Explorer and choose Properties.
2. Select the General tab and click Advanced.
3. Clear the Encrypt Contents To Secure Data check box.

Sharing Encrypted Files and Folders

Windows Server 2003 permits the sharing of encrypted files and folders. This mechanism facilitates data recovery and business collaboration by permitting a specified list of users to access encrypted data.

There are a few steps you need to perform to share the encrypted file or folder. Right-click the encrypted file or folder and select the Properties menu item. Select the General tab. Then click Advanced. Click Details in the Advanced Attributes dialog box. Click Add and select the users with whom you want to share the item.

There are a couple of limitations you need to be aware of. You can share the encrypted items with users only; that is, sharing with a group is not permitted. Also, the user you want to share the encrypted file or folder with must have a valid certificate for EFS.

More Info  For a description of the specifics of cryptography, including symmetric-key and public-key methods, visit http://www.microsoft.com/technet/security/topics/cryptographyetc/cryptpki.mspx.

Recovering Files

When you encrypt files to protect them from prying eyes, you run the risk of protecting them from yourself and ultimately losing the data. EFS requires the user’s private key (associated with the user’s EFS public-key certificate) to decrypt a file. As long as this key
is available, EFS-protected files can be accessed. In the event of key loss, a secondary means of retrieving the data is necessary. Consider, too, that a key might be lost because of the voluntary or involuntary departure of a user—for example, a user who encrypts company files might leave the company. Multiuser sharing described in the previous section solves this problem, but consider the situation where sharing isn’t enabled.

The ability to recover files starts when an individual user backs up his or her EFS public-key certificate and associated private key. To back up this information, the user must export the certificate and key through the Certificates snap-in in the MMC. (See the “Exporting Certificates and Private Keys” section earlier in this chapter.) If the private key is ever lost, the user can import the saved EFS private key and certificate and salvage the data. To do so, follow these steps:

1. Launch the Certificates MMC snap-in.
2. Select Personal from the console tree, and then right-click the Certificates folder and choose All Tasks and then Import from the shortcut menu.
3. Use the Certificate Import Wizard to restore the backup key, which allows access to the encrypted file again.

**Note** Exported keys and certificates are stored in a standard PKCS #12 (also known as Personal Information Exchange or PFX) format. This format is understood by a number of security-enhanced applications, allowing exchange of keys between independent computers or applications.

If a user is unable to decrypt lost data, an administrator can salvage the data by using a recovery agent certificate. To do so, follow these steps:

1. Instruct the user with the encrypted files to back up the files using Backup or another Windows Server 2003–compatible backup program, and send the backup file to the recovery agent using e-mail or removable media.
2. Log on using a Recovery Agent account, and restore the recovery key using the previous procedure. (The recovery key is presumably stored in a secure location such as a vault and deleted from the system when not in use.)
3. On the Recovery Agent’s computer, use Backup or another backup program to restore the files to a local folder.
4. In Windows Explorer, right-click the folder and choose Properties from the shortcut menu.
5. In the General tab, click Advanced.
6. Clear the Encrypt Contents To Secure Data check box. This decrypts the files using the recovery agent’s recovery certificate.

7. Back up the decrypted files and e-mail or deliver them to the user, who can then encrypt them using his or her key (which is probably newly issued after the old key was lost). Consider using e-mail encryption when sending the files, if appropriate.

**Real World  Protecting Recovery Agent Certificates**

Store recovery agent certificates in a secured storage facility to prevent possible data compromise. (It’s important to store the old recovery agent certificates because the associated certificate or recovery policy for encrypted files is updated only when the files are opened.) Upon receiving the recovery agent certificate, the recovery agent exports it to a diskette or other device that can be protected and deletes it from the machine. When data needs to be recovered, the certificate and associated private key can be imported. After the data is recovered, delete the certificate again. For information about exporting certificates, see the “Exporting Certificates and Private Keys” section earlier in this chapter.

---

**Auditing**

Both a proactive and reactive security tool, auditing informs administrators of events that might be potentially dangerous and leaves a trail of accountability if a security infraction does occur. Auditing failed logon attempts, for instance, can warn of rogue users attempting to gain unauthorized access to the system. In addition to auditing normal system events, you can audit policy modification to keep a trail of when a specific event audit was disabled and by whom.

The administrator establishes an audit policy by determining which types of security events to audit. Based on the security needs of the organization, the administrator might also choose to audit access to individual objects.

**Establishing an Audit Policy**

The first step in establishing an audit policy is to determine which event categories are to be audited. The following event categories are available for audit:

- Account logon events
- Account management
- Directory service access
To select the event categories to audit, you must first determine whether the computer is a domain controller. If it is not, choose Local Security Policy from the Administrative Tools folder. Expand the Local Policies root node to reach Audit Policy.

If the computer is a domain controller, open the Default Domain Controller policy (Start, All Programs, Administrative Tools, Domain Controller Security Policy). On the Group Policy tab, select the policy and click Edit. Then expand Computer Configuration, Windows Settings, Security Settings, and Local Policies, and then select Audit Policy.

Using either technique, selecting Audit Policy displays the auditable event categories in the right pane. To modify the policy for an event category, right-click that event and choose Properties. Select the check box for auditing successful events, auditing failed attempts, or both.

**Auditing Access to Objects**

After the Audit Object Access category is enabled in the Audit Policy item, members of the Administrators group can specify audit criteria for files, folders, network printers, and other objects. The following list describes some of the audit criteria for an object:

- Who is audited for this object
- Whether accessing this object succeeded or failed
- What type of object access is audited

**Note**  Auditing of local files and folders is limited to NTFS partitions.

Examples of access types include viewing a folder’s permissions, executing a file, and deleting an object. Follow these steps to select an object for auditing:

1. Right-click the object in Windows Explorer and choose Properties.
3. On the Auditing tab, click Add.
4. In the Name box, type the user or group to audit.
5. Click OK to display the Auditing Entry dialog box. Use the Access list to select whether successful access, failed access, or both types of access are audited.
6. For folders, use the Apply Onto drop-down list to indicate where the auditing should take place.
7. Select or clear the Apply These Auditing Entries To Objects And/Or Containers Within This Container Only check box to invoke or prevent inheritance, respectively.

There are more detailed descriptions of auditing in Chapter 12.

Viewing the Security Log

The security log details audit information of events specified in your audit policy. Each time an auditable event occurs, it’s added to the log file where it can filtered, sorted, searched for, or exported. The security log, along with the application and system logs, is located in Event Viewer and can be found in the Computer Management console tree by expanding System Tools, Event Viewer, and Security.

Each entry in the log contains critical information about the audited event, including whether the attempt failed or was successful, the date and time of the event, the event category and ID, and the audited user and computer. Additional information can be obtained for each entry by double-clicking the entry.

Manipulating the Security Log

The security log can be sorted by any of the fields listed in the display, such as user or date of event. Clicking a field header at the top of the pane causes the log events to be arranged in ascending order by that field. Clicking the field header again sorts them in descending order. For even more efficiency, you can filter the log to show only events you’re interested in—for example, failed audits only. On the View menu, click Filter. On the Filter tab of the Security Properties window that appears, select which event criteria to view and click OK.

**Note** Choose Find from the View menu to search through the displayed lists for specific events, such as all events with a certain event ID.

Security Log Maintenance

The security log has a defined maximum size. To set the size, right-click Security in Event Viewer and choose Properties. Edit the Maximum Log Size field specifying the size in
kilobytes. The options beneath this field, which are outlined next, specify how events are overwritten:

- Overwrite as needed. Old events will be discarded if necessary to make room for new events.
- Overwrite events older than X days. Events more than X days old will be discarded to make room for new events. If there is no room and all events older than X days have already been deleted, the new, incoming events will be discarded.
- Do not overwrite events. New events will be discarded if there is no room. A manual cleaning must occur to make room for new events.

**Note** Presumably, all event categories specified in the event policy are relevant. Be careful that automatic event wrapping does not overwrite events more frequently than either log archival or manual log interrogation.

To archive the security log, right-click Security in Event Viewer and choose Save Log File As. Choose the path and filename for the file. If you save it as an event log file (with the extension .EVT), the file can be opened in Event Viewer at a later time.

More information about the settings for the Security Log as well as on other components in Event Viewer can be found in Chapter 12.

### Using Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer is a powerful tool you can use to check the security settings of multiple computers. As such, it’s the first tool to pull out when verifying the security status of computers on your network.

To use the Microsoft Baseline Security Analyzer, take the following steps:

2. Launch the program from the Start menu or the Desktop.
3. Click the Scan A Computer hyperlink to scan a single computer, or click the Scan More Than One Computer link to scan multiple computers.
4. Specify the IP address or address range of the computers, specify what you want to look for, and click Start Scan.
5. Review the results, clicking links as appropriate to view more detailed information.
If you’ve used MBSA before, the second version of the tool adds features you should be aware of. Alongside updated instructions and help files, there is improved 64-bit support, Office XP awareness, and support for Microsoft Update (MU), Windows Server Update Services (WSUS), Systems Management Server (SMS), and Microsoft Operations Manager (MOM). The original version of MBSA is supported only Software Update Services (SUS).

What to Do When Hacked

If your network is hacked, you must take swift action to assess damage, limit further damage, and preserve evidence, which can potentially be used to press charges against the perpetrators. If your system is compromised, you should:

- Immediately remove the system from the network, but do not reboot or shut it down.
- Take a disk image of the server immediately after it was hacked.
- Check with your software and hardware vendors to determine what vulnerability was exploited and how to prevent it from happening again.
- Check log files for evidence.
- Change passwords for any affected systems; social engineering attacks (as popularized by the Iloveyou virus) are startlingly common and effective.
- Document what you learned, and develop an incident response plan. Do this for both internal and external servers.
- Microsoft recommends you reformat and reinstall.

Note  Consider using intrusion-detection software—such as Tripwire or Intrusion’s SecureNet Pro—that can give you notice of attacks.

Summary

As this chapter has shown, security issues extend to nearly every corner of Windows Server 2003. Learning to use the security-related snap-ins in the MMC will help you manage the rich features this operating system has to offer and will help prevent security weaknesses in your system.

Chapter 21 and this chapter cover security in broad terms by discussing planning and implementation. Chapter 24 brings security into sharper focus by covering a particular security feature of Windows Server 2003, Microsoft Certificate Services.
Chapter 23

Patch Management

Patches—everyone hates them, but they are an inescapable part of the everyday computing world. I hated them and complained about them when I was a UNIX system administrator some 20 years ago. And I still hate them now, even though the overall process of obtaining, testing, and applying them has gotten far better than it was back then. I doubt that anything we can say will make you like patches any better than we do, but in this chapter we'll try to cover the basics to make the process as straightforward and manageable as possible.

Real World  Terminology

The first rule of patches is that Microsoft doesn't like that word. It has several different terms it uses, each with a slightly different meaning, but the reality is that to the rest of the world, they’re still called patches. We call them patches, the magazines and newspapers call them patches, even most Microsoft employees call them patches, unless they’re giving a formal presentation. So throughout this chapter, that’s what we’ll call them. But Microsoft does have official terminology, and we should all be clear on what it is:

- **Critical Update** A generally available fix for a critical but non-security-related bug. A critical update has an accompanying Knowledge Base article.
- **Security Update** A generally available fix for a security vulnerability. Security updates have an accompanying Knowledge Base article and Security Bulletin.
- **Software Update** A broad term that covers Service Packs, hotfixes, update rollups, security updates, feature packs, and so on. A software update has an accompanying Knowledge Base article.
- **Service Pack**  A generally available collection of fixes and feature enhancements. Service packs are cumulative and contain all currently available updates, update rollups, security updates, critical updates, and hotfixes, and they might contain fixes for problems that were found internally and have not been otherwise released. Service packs also sometimes add new features (Microsoft Windows XP SP2, for example).

- **Hotfix**  A narrowly available fix for a specific issue. Hotfixes are generally available only through Microsoft Product Support Services and cannot be redistributed. Hotfixes have not had as thorough a test cycle as an update, update rollup, or service pack.

- **Update**  A generally available fix for a specific, nonsecurity and noncritical problem. An update has an accompanying Knowledge Base article.

- **Update rollup**  A generally available, tested collection of hotfixes, security updates, critical updates, and updates that are packaged together. An update rollup has an accompanying Knowledge Base article.

There, you see, all sorts of terms and terminology and not one of them is a patch. For complete, up-to-date details on Microsoft update terminology, see [http://support.microsoft.com/kb/824684/](http://support.microsoft.com/kb/824684/).

---

**Why It’s Important**

In the old days, when your network wasn’t connected to the Internet, when system administrators were the only people who installed software, and when users had only a green screen terminal, deciding when to apply a patch was a fairly straightforward decision. If there was a specific problem you were having and you wanted a bit of overtime on the weekend, you came in and applied a patch. If no one was complaining and you didn’t want to work on the weekend, you threw the tape (patches always came on tapes in those days) in the drawer and waited until you had to come in on the weekend for some other maintenance, or users started complaining about a problem that seemed related. Or you simply never got around to it at all.

Even in the more recent past it was possible to have a more considered and gradual approach to applying patches. When a vulnerability was identified, it often took months before there was any real risk to your network.

Today, that approach simply won’t work, as Code Red, Nimda, Slammer, and others have all too clearly demonstrated. Within hours or at most days of the release of a critical security update, there will almost certainly be sample exploit code posted on the Internet telling anyone and everyone how to exploit the vulnerability. If you ignore critical security updates, you place your entire network, and the data stored on it, at risk.
Applying patches is only one part of a defense-in-depth strategy to protect your network, but it’s a critical part. Don’t neglect it.

Real World  Patch Tuesday

In the old days, patches, especially security updates, were released whenever there was a new vulnerability identified and corrected. When that was happening a few times a year, it wasn’t a big problem, and the system administrator dealt with it as they came out. In most cases, you could just wait till the Service Pack came out, and deal with a whole bunch of them at once. But as more and more security updates and critical updates were released on an almost daily basis, it became increasingly difficult to properly test and identify all the patches that were necessary for your system and the whole process became a serious impediment to productivity.

In direct response to many, many complaints, Microsoft has moved to a monthly update release process. Unless there is a compelling and immediate need for a critical security update to be released off-cycle, all security updates are released once a month on the second Tuesday of the month. This change has greatly simplified the planning and deployment of patches.

The Patching Cycle

There are, or should be, four basic phases in the ongoing cycle of maintaining a well-patched and up-to-date network. The four phases are

- Assess
- Identify
- Evaluate and plan
- Deploy

Each of these phases is essential to the successful management of patches on your network. Depending on the size and complexity of your network, you might combine phases and even bypass them on occasion. However, it’s good to have an understanding of the phases and to think through the steps involved in each one even if you’re combining them.

Assess

The assess phase of patch management is all about understanding what your environment is, where and how it is vulnerable and can be attacked, and what resources and procedures are in place to ameliorate those vulnerabilities.
When a patch is released, you can’t make an informed decision about whether you need to install that patch unless you first know what software is present in your environment and what your critical business assets are that absolutely, positively must be protected. So the first step to an overall patch management process is to figure out what software you’re running in your environment. All of it, hopefully. Whether you build a big spreadsheet, have a fully relational database, or use a full-featured tool such as Microsoft Systems Management Server (SMS), you need to get your software environment audited and documented. One tool that can help with that auditing is Microsoft Baseline Security Analyzer (MBSA).

Identify your critical business assets. Is there confidential data that you couldn’t function without? Are there critical systems that must be available at all times? Are there individuals whose productivity is mission critical? All of these are business assets that you should factor into your overall patch management strategy.

The next part of the assessment phase is to understand what security threats and vulnerabilities you currently have. Do you have legacy Windows NT 4 systems that are no longer supported? Are there Windows 95 or Windows 98 machines on your network? Are you running old versions of software programs that can’t be easily updated or replaced? Do you have public-facing Web servers that are not behind your firewall? What are your security policies and how are they enforced? These and many, many more questions need to be asked, and answered.

Finally, you need to assess your patching infrastructure and resources. How do you deploy software and patches? Who is responsible for identifying, testing, and deploying patches? What resources do they have to help with that? How rapidly can you respond to a critical vulnerability that affects your systems? What steps can you take to improve your response time?

**Identify**

The *identify* phase is about finding out what software updates or patches are available, and how critical it is that they be deployed in your environment.

You need to

- Discover the patch
- Decide whether it’s relevant to your environment
- Download the patch
- Identify the patch’s criticality
There are many ways to discover patches, but for Microsoft products one of the best is to sign up for e-mail alerts. If you do this, Microsoft will send you notifications of security updates before they are actually released. The sign-up page is at: http://www.microsoft.com/technet/security/bulletin/notify.mspx. You can tailor the notification method and detail level to suit your environment.

**Note** The link above provides only alerts for security related patches.

Whatever method you use to discover patches, it’s important that you have a way to trust the source of the patch information. All Microsoft security update alerts are signed with a publicly available PGP key, for example. And it shouldn’t be necessary to say this, but just in case: Microsoft will never send a security update as an attachment to an email! Never.

Once you know about a patch, you need to decide whether it’s relevant to your environment. If all your client machines are running Windows XP Professional SP2 (and they should be!), a patch that applies only to Windows 2000 isn’t really relevant to your environment. However, if the patch is a critical security update for Microsoft Office 2003 and you run that in your environment, you’ll need to apply it.

When you determine that a patch is relevant to your environment, you need to obtain the patch from a known and trusted source. For a Microsoft patch, this generally means downloading it directly from Microsoft. Find the relevant Knowledge Base article for the patch, and then cut and paste the link to the download page directly into your browser. Do not click on the link in an e-mail to get your patch. Even when you have verified that the e-mail is really from Microsoft and is a legitimate e-mail, you shouldn’t click on the links in it. Get into the habit of always using cut and paste. When you use cut and paste to put a link into your browser, you greatly reduce the likelihood a “phishing” attack—that is, of being unknowingly redirected to a site that looks exactly like the site you expected to go to, but is actually a site designed to steal information from you or download unwanted spyware onto your computer.

**Note** Most e-mail clients today have the ability to force all e-mail to display as “plain text.” This is a good thing, because it prevents unscrupulous people from hiding the real destination of a link. The giveaway for detecting a bogus link will usually be that it’s a link to an IP address, not the actual DNS domain name, or if it is a DNS name, it’s not exactly the one you think it is. If you make the change to only reading e-mail in plain text, your e-mail won’t be as pretty, but you’ll give yourself an additional layer of protection from phishing attacks.

To enable plain text e-mail handling in Outlook 2003, select Options from the Tools menu. Click the Preferences tab, and then click on E-Mail Options. Select the Read All Standard Mail In Plain Text and Read All Digitally Signed Mail In Plain Text check boxes. Click OK and restart Outlook.
Once you’ve downloaded the patch and read the associated Knowledge Base article, you are in a position to determine just how critical the patch is in your environment. Is this a patch that needs to be deployed immediately, with limited testing, or even with no testing? Or are there ameliorating factors that allow the patch to be deployed as part of a regular patching schedule after full testing?

**Evaluate and Plan**

The *evaluate and plan* phase of patch management flows naturally out of the identify phase, and in many ways is an extension of it. In this phase, you determine how to respond to the software update you’ve downloaded. Is it critical, or even necessary? How should it be deployed? And to whom? Should interim countermeasures be employed that will minimize your exposure to the vulnerability? What priority does the patch have?

The initial determination of need, suitability and priority is made during the identify phase, but in the evaluate and plan phase, you should take a closer look at the patch. What priority is the patch? If it affects a critical business asset, and there’s no easy or appropriate countermeasure except the patch, it will have a higher priority for testing and deployment than if there’s a simple countermeasure that you can implement until the patch can be deployed. If it targets critical business assets, it’s going to have a higher priority than if the only computers that are affected are several old Windows 98 machines that aren’t running any critical business applications.

Once you’ve identified the priority of the patch, you need to plan the actual deployment. Which machines need to have the patch deployed to them? Are there any constraints or issues that interfere with the deployment? Who needs to be notified, and what steps need to be taken so that the deployment minimizes the disruption to the environment? If this is an emergency release, will it go through a staged deployment, or is every affected machine going to have the patch deployed as soon as possible?

**Deploy**

The *deployment* phase of patch management is in many ways the easiest. You’ve done all your preparatory work, now all you need to do is the actual deployment.

First and foremost, *communicate*. Let everyone who will be affected know that you will be deploying a patch, and what application or area of the operating system it affects. If you know the deployment will cause changes in behavior, tell your users *before* the deployment. You will have far fewer support calls if you’ve warned people that a certain behavior is expected than if you surprise them.

Depending on what the priority of the patch is and how many machines it affects, you should test your deployment on a subset of the machines or on your test network. If no problems are reported, you can extend the deployment to additional users.
Repeat

The four phases of patch management are a circle, and when you’ve finished the last phase—deployment—it’s time to start the first phase—assessment—all over again. You should, at the very least, verify that the patch has been successfully deployed to the affected machines. Update your software map and database so that you know which machines have had the patch applied. Ensure that any nonpatch countermeasures have been successfully deployed as well. Verify that the patch hasn’t caused issues for your end users that were missed during the testing of the patch.

Deployment Testing

Sometimes a patch is so critical and such an emergency that you simply have to deploy it immediately and hope it doesn’t cause too many other problems. We hope that doesn’t happen to you too often, and it shouldn’t if you have a good defense-in-depth approach to protecting your network. But when it does, do the deployment—you might have some issues on some machines, but the risks of serious problems from the vulnerability are a good deal worse.

For all the rest of your patch deployments, however, it’s basic good practice to test the deployment before you roll it out to all the machines on your network. We like to use a three-stage deployment approach, though there are excellent arguments for adding additional stages into the process. The three deployment stages we use are

- Test Network
- Beta Users
- Full

Test Network Deployment

In an ideal IT world, we would have a test network that included all the hardware and software configurations of all our client and server machines. We could then test deploy patches, software updates, and new software applications to this test network before we deployed them in the production network. We’d also have a dedicated team to actually use all our applications and configurations to ensure that there weren’t incompatibilities that only daily use would identify.

Well, in the real world, most of us don’t have the luxury of that kind of setup, unfortunately. But by using virtualization technologies, such as Microsoft Virtual Server 2005 R2 (discussed in Chapter 29) and VMWare Workstation 5.5, we can do a very good job of emulating a full test network on one or two servers.
Copy a Physical Disk to a Virtual Disk

Virtual Server 2005 R2 has the ability to copy a physical disk to a virtual disk, making it possible to create virtual clones of your existing software configurations. This won’t re-create all the physical devices that might be part of your standard hardware configurations, but it will certainly give you the ability to re-create your software configuration. And it has the added advantage of letting you consistently roll back to a known state using the Undo capability of Virtual Server. The process of setting up virtual versions of your existing physical hard disks is documented in the Virtual Server 2005 R2 Administrator’s Guide, which is installed as part of Virtual Server 2005 R2.

The basic procedure requires you to create a linked virtual hard disk, and then convert the linked hard disk to a dynamically expanding hard disk. The process takes a significant amount of time, uses a large amount of processor resources, and requires significant disk space. But the resulting virtual hard disk can be used to create new virtual machines that replicate the configuration of your production network.

VMWare has a similar ability, using a product called P2V Assistant. For more information on P2V Assistant, see http://www.vmware.com/products/p2v.

At this point, you might be asking why we are recommending both Virtual Server 2005 R2 and VMWare Workstation 5.5? Don’t they perform much the same functions? And aren’t they competing products? Well, yes, they perform very similar functions, though with a completely different interface; and yes, they are competing. But each has strengths and weaknesses, and can do some things a good deal better than the other. We like Virtual Server 2005 R2, and it has the distinct advantage of being a Microsoft product, simplifying training, licensing, and support. The one area where we find a need to use VMWare is to test our x64 Edition environments. Virtual Server does not support 64-bit guests. Because x64 is playing an increasingly significant role in our environment, we use VMWare Workstation 5.5 to test x64 patches. VMWare Workstation 5.5 fully supports x64 guests, giving us much more flexibility to test patches on all our environments before we actually deploy them.

Note: VMWare Workstation 5.5 support for x64 guest operating systems is restricted to specific processor revisions. Verify that your processor is supported, or make your processor decisions for new hardware based on the processor versions that are supported.
Beta User Deployment

Once you’ve tested the deployment of a patch or software update on your test network, you should test the deployment in a controlled release to a dedicated group of users before deploying across the entire enterprise. No matter how much testing you do in a test lab, you can never completely replicate what real users will do. It’s much easier to find a problem and address it when you’re dealing with a limited beta deployment than dealing with a full scale, enterprise-wide deployment that has problems.

For your beta-user deployments, you should build a dedicated team of real users from across the company who are your beta team. They should cover as broad a range of user types and configurations as possible, but all need to be willing and able to both identify and deal with problems that the patch or software update might cause, while communicating clearly exactly what the problem is.

Building a beta team is just like building any other team—you need to make them part of the process, give them ownership of the process, and reward them for being on the team. Rewards can, and should, be simple and appropriate. Public recognition of their efforts and their importance to the protection of your network assets is often the most compelling and appropriate reward.

Full Deployment

The final phase of patch deployment is to roll it out to the entire organization. Even though you’ve tested it thoroughly, and your beta testers have also tested it thoroughly, there is still the possibility that there will be problems when the update is deployed across the entire enterprise. Be prepared for an extra support load on the days immediately following a major deployment. And make sure you communicate completely with your user community. They should both know that they’re going to be getting a new software update and be warned about specific problems if they develop.

Obtaining Updates

Microsoft has three basic methods for updating client and server computers: automatic updates from the Windows (or Microsoft) Update site, Windows Server Update Services (WSUS), and Microsoft Systems Manager Server (SMS).

Automatic Updates

Automatic updates, using either Windows Update or Microsoft Update sites, is not really a great option for most enterprise environments. It takes control of which updates are applied, and when, out of the hands of the system administrators and makes it difficult to know who has what patch applied.
For a small business, with less than 20 clients, automatic updates from Windows Update or Microsoft Update is probably an appropriate solution. Even here, though, we’d recommend setting your clients to automatically download updates but not install them. That will allow you to have one or two people test the release before you tell everyone else to go ahead and install it.

Windows Server Update Services

Windows Server Update Services (WSUS) has been through several name changes, along with the accompanying acronym changes, but the name seems to have finally settled down and the software is now officially released—which is a good thing. WSUS is Microsoft’s free software update tool, and it’s quite a useful tool. It doesn’t have the features and capabilities of SMS, but most of us don’t actually need SMS, and the costs of implementing SMS are significant.

Installation


WSUS requires Internet Information Server 6, Background Intelligent Transfer Service 2.0, and .NET Framework 1.1 Service Pack 1 installed prior to installation of WSUS. If SQL Server 2000 is not already installed, the Windows SQL Server 2000 Desktop Engine (WMSDE) will be installed as part of the installation of WSUS.

Note  Windows Server 2003 SP1 and later includes BITS 2.0 and .NET Framework 1.1 SP1, so these do not need to be installed separately.

Prerequisites

You need to download the necessary files before you begin the installation of WSUS. If your server is not already running Windows Server 2003 SP1, you should download the following items:

- .NET Framework 1.1 SP1, which is available at: http://go.microsoft.com/fwlink/?LinkId=47358

In all cases, you must download WSUS itself. This download requires a registration and a Passport account. You can download WSUS at: http://www.microsoft.com/windowsserversystem/updateservices/downloads/wsus.mspx.
Once you have downloaded the necessary software, you can begin installing the prerequisites:

- Install IIS6 on your WSUS server if it isn’t already installed. IIS6 can be installed using Add/Remove Programs, Add/Remove Windows Components.

- Install .NET Framework 1.1 SP1. If you’re already running Windows Server 2003 SP1, you won’t need to install this service pack because it is included in the Windows Service Pack.

- Install BITS 2.0. If you’re already running Windows Server 2003 SP1, you won’t need to install BITS 2.0 because it is included in the Windows Service pack.

If any of the prerequisite steps requires a reboot, you need to do that reboot before starting the WSUS installation.

To install Windows Server Update Services, perform the following steps:

1. Complete the prerequisite installations described previously.

2. Navigate to the location where you downloaded WSUS. Double-click WSUS-Setup.exe to begin the installation and open the Microsoft Windows Server Update Services Setup Wizard.

3. Click Next to open the License Agreement dialog box. As usual, you can either agree to the license or cancel the installation.

4. Click Next to open the Select Update Source dialog box, which is shown in Figure 23-1.

![Figure 23-1](Image)
5. Select Store Updates Locally, and enter a location on an NTFS formatted volume. You can also choose to download updates directly from Microsoft, which will slow down updating clients but save on hard drive space.

6. Click Next to open the Database Options dialog box. By default, WSUS uses WMSDE to store updates. If an existing SQL Server installation is present, you can choose to use the existing database server.

7. Click Next to open the Web Site Selection dialog box, which is shown in Figure 23-2. You can choose to use the IIS Default Web site, or create a special WSUS site.

![Figure 23-2](image)

The Web Site Selection dialog box of the Microsoft Windows Server Update Services Setup Wizard

8. Click Next to open the Mirror Update Settings dialog box. You'll use this dialog box if you're creating a hierarchy of WSUS servers, but for standalone WSUS servers, leave the check box cleared.

9. Click Next and the actual installation will begin.

Basic Configuration
The basic configuration of WSUS requires you to configure and deal with quite a few things right at the beginning, but then the process should be straightforward. The steps to initial configuration are as follows:

- **Configure networking and proxy settings.** WSUS needs to be configured to work with your proxy and firewall server or servers.
- **Synchronize the WSUS server with Microsoft Update.** WSUS downloads the complete list of Critical and Security updates from Microsoft Update for the kinds of client computers on your network.

- **Update and configure automatic updates.** WSUS needs to update Automatic Updates on your client machines to the latest version. Use Group Policy to deploy the latest version.

- **Create computer groups.** WSUS creates two new groups by default (All Computers and Unassigned Computers), but you'll likely want additional groups, such as Test and Beta groups to manage the deployment process.

- **Approve and deploy updates.** WSUS defaults to automatic approval of critical security updates, but you can change the settings and control details of approval. Software isn't actually downloaded and deployed until approved.


---

**Systems Management Server 2003**

Microsoft SMS is not just a patch management application, but an entire network and infrastructure management solution. It has the ability to inventory your network; manage network devices; and deploy applications, operating systems, and patches across a diverse enterprise environment. It also has comprehensive reporting and asset-management features.

The setup and deployment costs for SMS are significant, but the payback for complex environments will be worth it in the long run. If you're managing 50 desktops, don't bother. But if you're managing 500 or more desktops, SMS is worth investigating.

**More Info** For more information about SMS, see http://www.microsoft.com/smservice/default.mspx.

---

**Third-Party Products**

Patch management continues to be a major source of pain for users and system administrators. And where there is pain, there are those who see an opportunity to help reduce the pain while making a profit. The range of products that can help manage patches on your Microsoft network go from the fairly simple, which just deal with Microsoft patches,
to those that are complete infrastructure management and deployment programs, which can handle extremely complex environments.

Of all the products we’ve seen, the one we like the best is unquestionably Shavlik’s HFNetChkPro, which is available at http://www.shavlik.com/hfnetchk-windows.aspx. The original release of Microsoft Baseline Security Analyzer used code written by Shavlik to scan for vulnerabilities. Shavlik HFNetChkPro can scan client computers across the network, with or without an agent on the client, and then automatically deploy patches to each machine. It has the ability to handle both Microsoft products and some common third-party products such as Real Audio, WinZip, Adobe Acrobat, and Firefox/Mozilla.

The biggest strength of HFNetChkPro, in our opinion, is its deployment engine. From a single central console, you can easily deploy patches and even full service packs to targeted groups of machines, setting the time for the actual deployment and scheduling a reboot if appropriate. Click the button, and the patches are downloaded to the client computers and the actual installation will happen automatically without further intervention.

HFNetChkPro scales well from small networks up to quite large ones. You can easily create test networks for beta deployments, and then follow through with the final enterprise deployment with the assurance that the exact same set of parameters and patches will be deployed as on the test network.

**Summary**

In this chapter we’ve looked at some of the concepts of patch management, as well as the Microsoft solutions to help you manage and deploy patches and software updates. We also took a quick look at a third-party solution to patch management, Shavlik’s HFNetChkPro. In the next chapter, we’ll cover using Microsoft Certificate Services to manage and deploy certificates on your network.
In Chapter 21 and Chapter 22, you learned about the security protocols and tools that Microsoft Windows Server 2003 supports. Some of these protocols, such as Kerberos and Internet Protocol security (IPSec), are primarily used to protect network traffic from intrusion; others, such as Secure Multipurpose Internet Mail Extensions (S/MIME) and Encrypting File System (EFS), protect messages and files from being compromised. Even components that don’t have anything to do with security directly, such as the Active Directory Simple Mail Transfer Protocol (SMTP) site connector, can use these services to gain enhanced security.

The Windows Server 2003 public-key infrastructure (PKI) provides a way to issue, revoke, and track digital certificates. Microsoft Certificate Services, included as an optional component in Windows Server 2003, allows you to issue new certificates, certify them as valid, and revoke certificates you no longer want to use. In this chapter, you learn how to install, configure, and manage Certificate Services to provide security for individual computers, domains, and your entire enterprise, both on the Internet and on your intranets. (If you need to know how to manage certificates on a machine, see Chapter 22.)

Note A terminology note: Certificate Services is the actual software; certificate authority (CA) refers to any entity, such as Certificate Services, that issues certificates. This chapter uses the two terms interchangeably.
More Vocabulary

Chapter 21 and Chapter 22 exposed you to most of the security vocabulary you need to work with Certificate Services, but you need to learn some additional terms, as defined in the following sections.

Policy Modules

A policy module is a set of instructions that tells the CA what to do with incoming certificate requests. A policy module can automatically approve or reject a request, based on any criteria coded into the module; it can also mark a request as pending and leave it for a human administrator to handle. Policy modules can also modify the content of a certificate by adding or removing extensions. The standard policy module supplied with Windows Server 2003 does the following:

- Approves incoming requests or marks them as pending, depending on the CA type and the setting you specify
- Adds an optional extension to the certificate that specifies where the issuing CA’s certificate can be obtained
- Adds an optional extension that specifies where certificate revocation lists (CRLs) for the issuing CA can be obtained

Other applications, notably Microsoft Exchange Server, can implement their own policy modules, which can replace or augment the standard policy behavior. Microsoft offers tools that allow you to develop your own policy module if you need to change the policy behavior to match your organization’s security standards.

Exit Modules

An exit module allows the CA to take some action after a certificate is generated. For example, an exit module might publish new certificates by putting them in the Active Directory directory service or publishing them to the file system. The standard Windows Server 2003 exit module performs two tasks: if the requestor specifies a file path, an Active Directory location, or both, the exit module publishes the new certificate to one or both locations; and it publishes CRLs for the CA to the location you specify.

Certificate Publishers

A certificate publisher serves the same function as any other kind of publisher: it makes desirable information available to clients who want it. Specifically, certificate publishers make certificate and CRL information available to clients using whatever mechanism they want. The default certificate publisher in Windows Server 2003 is Active Directory, although you’re free to export certificates or store them in another type of directory or publishing system.
Certificate Templates

A certificate template defines a cookie-cutter set of attributes and extensions that a newly issued certificate has. For example, the Administrator certificate template specifies different attributes from a Domain Controller certificate. The idea behind certificate templates is that the person requesting a certificate can just pick a template that embodies the attributes and extensions he or she needs the new certificate to have, instead of being required to pick and choose from dozens (or even hundreds) of arcane attribute names.

Windows Server 2003 supports 31 certificate templates, listed in Table 24-1. When you request a certificate using a particular template, the CA knows which attributes and extensions to populate the new certificate with. As an administrator, you can control which templates individual users and groups can use when requesting new certificates. (In fact, you can also control whether they can request certificates at all!)

Note The available default templates vary with the Windows Server 2003 edition. For example, Windows Server 2003, Standard Edition includes a subset of those listed in Table 24-1.

Table 24-1 Certificate templates

<table>
<thead>
<tr>
<th>Template</th>
<th>Purpose</th>
<th>Published to Active Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Signs code; signs certificate trust lists (CTLs); secures e-mail and EFS file systems; authenticates clients</td>
<td>Yes</td>
</tr>
<tr>
<td>Authenticated Session</td>
<td>Allows signature-only operations for client authentication</td>
<td>No</td>
</tr>
<tr>
<td>Basic EFS</td>
<td>Encrypts EFS intermediate keys and file volumes</td>
<td>Yes</td>
</tr>
<tr>
<td>CA Exchange</td>
<td>Used for private-key storage</td>
<td>No</td>
</tr>
<tr>
<td>CEP Encryption</td>
<td>Enables holder to act as registration authority when simple certificate enrollment protocol (SCEP) requests are made</td>
<td>No</td>
</tr>
<tr>
<td>Code Signing</td>
<td>Signs executable code, including scripts, to assert its trustworthiness</td>
<td>No</td>
</tr>
<tr>
<td>Computer</td>
<td>Authenticated computers to servers and vice versa</td>
<td>No</td>
</tr>
<tr>
<td>Cross-Certification Authority</td>
<td>Used for qualified subordination and cross-certification</td>
<td>Yes</td>
</tr>
<tr>
<td>Directory e-mail Replication</td>
<td>In an Active Directory, replicates e-mail</td>
<td>Yes</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>Authenticates clients to servers; authenticates servers to clients</td>
<td>Yes</td>
</tr>
<tr>
<td>Template</td>
<td>Purpose</td>
<td>Published to Active Directory</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Domain Controller Authentication</td>
<td>Used to authenticate Active Directory users and computers</td>
<td>Yes</td>
</tr>
<tr>
<td>EFS Recovery Agent</td>
<td>Recovers encrypted files when the original key material is unavailable</td>
<td>No</td>
</tr>
<tr>
<td>Enrollment Agent</td>
<td>Requests certificates for users</td>
<td>No</td>
</tr>
<tr>
<td>Enrollment Agent (Computer)</td>
<td>Requests certificates for computers</td>
<td>No</td>
</tr>
<tr>
<td>Exchange Enrollment Agent (offline request)</td>
<td>Requests certificates for users or computers</td>
<td>No</td>
</tr>
<tr>
<td>Exchange Signature Only</td>
<td>Used to issue certificates to Microsoft Exchange users for signing e-mail</td>
<td>Yes</td>
</tr>
<tr>
<td>Exchange User</td>
<td>Used to issue certificates to Exchange users for encrypting e-mail</td>
<td>No</td>
</tr>
<tr>
<td>IPSec</td>
<td>Allows the use of IPSec encryption and authentication</td>
<td>No</td>
</tr>
<tr>
<td>IPSec (offline request)</td>
<td>Allows computers that are not currently attached to the network to use IPSec when connected</td>
<td>No</td>
</tr>
<tr>
<td>Key Recovery Agent</td>
<td>Recovers private keys stored on the certification authority</td>
<td>No</td>
</tr>
<tr>
<td>RAS and IAS Server</td>
<td>Used to allow IAS and RAS servers to prove their identity to other computers</td>
<td>No</td>
</tr>
<tr>
<td>Root Certification Authority</td>
<td>Used to allow proof of identity of root certification authority</td>
<td>No</td>
</tr>
<tr>
<td>Router (offline request)</td>
<td>Authenticates clients to a server</td>
<td>No</td>
</tr>
<tr>
<td>Smart Card Logon</td>
<td>Authenticates a client to a logon server</td>
<td>No</td>
</tr>
<tr>
<td>Smart Card User</td>
<td>Authenticates a client; provides e-mail security</td>
<td>Yes</td>
</tr>
<tr>
<td>Subordinate Certification Authority</td>
<td>Issues and revokes certificates while acting as a subordinate CA</td>
<td>No</td>
</tr>
<tr>
<td>Trust List Signing</td>
<td>Signs the CTL</td>
<td>No</td>
</tr>
<tr>
<td>User</td>
<td>Authenticates client-to-server messages; signs and encrypts e-mail; encrypts EFS data</td>
<td>Yes</td>
</tr>
<tr>
<td>User Signature Only</td>
<td>Signs e-mail; signs client-to-server authentication messages</td>
<td>No</td>
</tr>
<tr>
<td>Web Server</td>
<td>Authenticates server to clients</td>
<td>No</td>
</tr>
<tr>
<td>Workstation Authentication</td>
<td>Authenticates client computers to servers</td>
<td>No</td>
</tr>
</tbody>
</table>
Each template defines the content of the certificate, using some combination of the tem-
plate features listed in Table 24-2. You can’t control the content of templates, so you must
work with the attribute combinations hard-coded into them by Microsoft.

<table>
<thead>
<tr>
<th>Attribute type</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic constraints</td>
<td>Specifies whether this certificate can be used to sign other certificates and, if so, how many levels of nesting the resulting hierarchy can contain.</td>
</tr>
<tr>
<td>Default CSP list</td>
<td>Provides a list of cryptographic service providers (CSPs) that can be used with this certificate type. For example, EFS requires certificates generated with the Microsoft RSA CSP.</td>
</tr>
<tr>
<td>Display name</td>
<td>Displays the name when someone views the certificate’s information; this is a “friendly” name that’s less complex than the certificate’s distinguished name (DN).</td>
</tr>
<tr>
<td>Extended key usages</td>
<td>Specifies a list of extended functions (including signing a CTL, encrypting e-mail, and establishing secure network connections) for which this certificate can be used. The extended key usage information coexists with, and doesn’t override, the standard key usage fields.</td>
</tr>
<tr>
<td>Include e-mail name</td>
<td>Specifies that the e-mail address associated with the holder of this certificate should be included in the certificate.</td>
</tr>
<tr>
<td>Key usage</td>
<td>Specifies what combination of basic operations (digital signatures, encryption, and key exchange) this certificate can be used for.</td>
</tr>
<tr>
<td>Machine certificate template</td>
<td>Specifies whether certificates that use this template are intended for use by people or by computers.</td>
</tr>
<tr>
<td>Security permission set</td>
<td>Specifies who can request a particular kind of certificate. For example, the default permissions for the Administrator template allow only users with administrative access to request administrator-level certificates.</td>
</tr>
</tbody>
</table>

Certificate Authority Types

Computers running Certificate Services can act as one of two distinct types of CAs: enterprise or standalone. Which type of CA you install determines to whom you can issue a certificate and what it can be used for, so the distinctions between them are important. The only internal difference between the two is which policy module is installed, but the operational differences between them are significant.

Enterprise CA

An enterprise CA is designed to act as part of an enterprise security infrastructure. In that job, it can issue and revoke certificates for end users and subordinate CAs, according to
the active policy modules and security settings you apply to the CA. As befits anything saddled with the “enterprise” label, enterprise CAs require Active Directory access. Several key features distinguish an enterprise CA from a standalone CA.

■ An enterprise CA is always trusted by all users and computers in its domain because the CA certificate appears in the Trusted Root Certification Authorities trust list in Active Directory.

■ Certificates issued by an enterprise CA can be used to log on to Windows Server 2003 domains with smart cards (as discussed in Chapter 21 and Chapter 22).

■ An enterprise CA publishes certificates and CRL information to Active Directory.

Another important difference between enterprise CAs and standalone CAs is that enterprise CAs use certificate types and templates to construct the content of newly issued certificates. This capability leads to some useful features. First, because they use templates, enterprise CAs can stuff the newly formed certificate with the proper set of attributes. In addition, enterprise CAs automatically fill in the subject name for newly issued certificates. Enterprise CAs have the unique property that they always either reject or approve a certificate request—they never mark one as pending. Enterprise CAs make this go/no-go decision based on the security permissions set on the requested template type, as well as on the account’s permissions and group memberships in Active Directory.

**Standalone CA**

A standalone CA doesn’t require Active Directory—it’s designed to be a separate box that can issue certificates for extranet or Internet use. As such, its purpose is to issue certificates for people to use who aren’t part of your core organization and who don’t have Active Directory access. The basic mechanics of certificate issuance for a standalone CA are similar to those for an enterprise CA, with a few exceptions:

■ Requests sent to a standalone CA are automatically marked as pending because the CA has no way to use templates and Active Directory information to verify them. This lack of directory information also means that requestors must completely fill out all the information in their request, because the CA has no way to look it up.

■ Certificates issued by a standalone CA can’t be used for smart card–based logons, although you can store such certificates on a smart card.

■ Certificates and CRLs generated by the standalone CA aren’t published anywhere—you must manually distribute them.

You can install a standalone CA on a server that participates in an Active Directory organization. If you do, the CA is able to publish certificate information if its server is a member of the Certificate Publishers group.
Preinstallation
Before you can successfully and securely install the CA, you must understand some concepts and be able to answer some questions that you’ll be asked during the installation and setup process.

Understanding Certificate Authority Roles
In general, a CA can function in four separate roles. These roles determine what the CA’s certificates are used for, which in turn determines what your users and computers will be able to do.

Enterprise Root CA
A root CA is at the top of a certificate chain, as described in Chapter 21. An enterprise root CA, then, serves as the root CA for an entire enterprise—it occupies the topmost position in the certificate trust chain for all certificates issued by any component of the organization. The enterprise root CA can issue certificates for subordinate CAs, users, and computers, but as a practical matter, it normally issues only subordinate CA certificates. Those subordinates are then responsible for issuing certificates to users and computers in the organization. Splitting certificate issuance that way allows you to delegate authority to issue certificates to the lowest possible level in your organization, while still maintaining robust control over the content, format, and use of those certificates. The enterprise root CA self-signs its certificate, asserting that it is the root by that signature. This allows it to issue certificates for individual users, computers, and subordinate CAs. After the enterprise root CA is installed, it functions as an enterprise CA (as discussed earlier in the chapter).

Enterprise Subordinate CA
The enterprise subordinate CA requires a CA certificate issued by a root CA, so it forms a link in the certificate hierarchy. It acts as an enterprise CA, so it requires Active Directory access. It can issue certificates to subordinate CAs or directly to end users and computers.

Standalone Root CA
The standalone root CA behaves as a standalone server—it doesn’t have to participate in Active Directory but uses it if it is available. The independence from Active Directory is an advantage. You can easily disconnect a standalone CA from your network so that it remains secure from network-borne attacks. Many organizations use standalone root CAs for issuing their most valuable certificates, including subordinate CA certificates, because of the extra security gained by keeping the CA computer network-free.

Standalone Subordinate CA
Like its root counterpart, a standalone subordinate CA can use Active Directory but isn’t required to. It issues certificates only to end users (typically people, because without Active Directory there’s no reason to issue certificates to computers).
Real World  Protecting the Jewels

Because CAs can issue certificates and because certificates form the backbone of the Windows Server 2003 access control and security features, you need to take special measures to protect your CAs from being compromised or lost. It’s tempting to think of a CA as just another server, but remember that it’s more valuable than the average server. At a minimum, Microsoft recommends that you complete the following tasks to secure your CAs:

■ Protect them against physical damage or tampering. Lock your CAs in a secure area with good physical access control and fire suppression. Keep tight control over who has access to the machines, and make sure you take advantage of whatever security features your server vendor has included.

■ Protect them against data loss. You need to diligently back up your CAs, because losing the CA’s private key prevents you from recovering user certificates and forces you to reissue every certificate the CA has issued in the past.

■ Protect your server against hardware failures and viruses. If you lose access to the CA’s database, you aren’t be able to recover certificates.

■ Protect your CAs’ private keys. It’s easy to store the CA keys in an encrypted file. In fact, Microsoft makes this the default. However, the big standalone CA providers such as Thawte, GTE CyberTrust, and VeriSign all use special-purpose hardware devices to store the keys. These devices let you store your keys in a tamper-proof hardware enclosure that makes the keys available only to authorized applications.

To get the most bang for your security dollar, you need to apply these three measures appropriately to each CA, along with the Windows Server 2003 access control and auditing features. Depending on how your certificate hierarchy is organized, you might need to do more to protect a higher-value asset (such as your enterprise root CA) than a lower-value one, but that doesn’t mean you should ignore subordinate CAs.

Preparing for Installation

You need to perform several tasks before you can install Certificate Services. As part of the installation process, your CA either issues and signs its own root CA certificate or requests a certificate from another CA; to avoid having to repeat this process, it’s best to have all the needed information available before you start the installation.
First determine what kind of CA you want. If you want to use an enterprise CA, you need to have Active Directory installed; you can install standalone CAs with or without Active Directory. Also consider whether you want to use advanced options. Certificate Services uses a set of programming interfaces that Microsoft calls CryptoAPI. Each set of cryptographic routines on a Windows Server 2003 system has to be packaged as a CryptoAPI CSP. By installing and removing CSPs, you can customize the set of cryptographic algorithms that your servers use. Normally, a Certificate Services installation uses whatever CSPs it finds on your server. However, you can instruct it to use, or not use, specific CSPs if you want to.

**Installation and Configuration**

After you make the decisions necessary to set up a new CA, you’re ready to install the software and configure it to meet your needs. You install Certificate Services using the Windows Components Wizard. You can install the CA, the Web enrollment component, or both from the wizard. To complete the installation, follow these steps:

1. Launch the Windows Components Wizard by opening Add/Remove Programs in Control Panel. Then select the Add/Remove Windows Components option offered on the left side of the dialog box.

2. When the wizard opens, select Certificate Services from the component list. The installer warns you that after the CA software is installed, you can’t change the name of the server or move it into or out of an Active Directory domain. If you have a server you want to use as an enterprise CA, make sure it is a member of the domain before you start. If the server will also be a domain controller, run `dcpromo` to promote it to domain controller status before installing Certificate Services.

3. If you want to install only one of the components (for example, if you want to set up a CA with no Web-enrollment capacity), click Details and clear any component you don’t want installed. If Internet Information Services (IIS) with Active Server Pages isn’t installed, Web-enrollment support will not install and you’ll be notified of the failure.

4. The CA Type page appears (shown in Figure 24-1). Select the option that corresponds to the CA type you want: enterprise root, enterprise subordinate, stand-alone root, or stand-alone subordinate. (If you’re working on a machine that isn’t in a domain, your available selections are limited.) If you want to change the CSP list for this CA, make sure to select the Use Custom Settings To Generate The Key Pair And CA Certificate check box. (See the “CAs Linked into a Hierarchy” section later in the chapter for more details.)
5. If you selected the Use Custom Settings To Generate The Key Pair And CA Certificate check box, you see the Public And Private Key Pair page shown in Figure 24-2. Use this page to select the CSP you want your CA to use (bearing in mind that some CSPs might not be supported for generating certificates from some templates). The Microsoft Strong Cryptographic Provider CSP is the default choice; other CSPs are available, depending on the software you have installed and whether you have any smart cards or special-purpose cryptographic tokens available.

Figure 24-1  The CA Type page of the Windows Components Wizard

Figure 24-2  The Public And Private Key Pair page of the Windows Components Wizard
6. On the Public And Private Key Pair Selection page, choose among the various options to configure Certificate Services the way you want it and click Next.

- The Hash Algorithm box allows you to choose the hash algorithm you want to use for signatures. Don’t use MD4. If possible, don’t use MD5 either. Both algorithms have known (albeit mostly theoretical) weaknesses. Instead, leave the default setting of SHA-1 alone.

- The Key Length drop-down list lets you select a key length if you’re generating a key pair. You can leave the default value of 2048 bits, or you can go all the way up to 4096 bits if you need to. Non-Microsoft PKI components might have their own requirements and limitations regarding key length, so be sure to make a selection accordingly.

- The Use An Existing Key check box allows you to recycle an existing key pair, provided it was generated with algorithms compatible with your selected CSP. As you choose different CSPs, you see that this check box (and the contents of the list below it) changes to reflect whether any keys exist that you can potentially use.

- The Import button lets you import certificates from a PKCS #12 file, and the View Certificate button shows you the properties for the selected certificate.

- The Use The Certificate Associated With This Key check box lets you use an existing certificate if the key pair you select has one associated with it and if it’s compatible with your chosen CSP.

7. The CA Identifying Information page appears, shown in Figure 24-3. Type a common name for the CA. By default, newly generated CA certificates are valid for five years; you can adjust that period in the Validity Period drop-down list. Click Next.
Important If you type an organization name that includes special characters (such as &, *, [ ], and so on), the CA has to encode them in Unicode to remain compliant with the X.509 standard. This might prevent some applications from decoding and verifying your CA certificate, so the installer warns you and gives you a chance to remove the special characters before proceeding.

Note On the Certificate Database Settings page (shown in Figure 24-4), specify where the CA’s certificate database and log files will be stored. Note that the location you specify isn’t where issued certificates and CRLs are stored; it’s actually where the CA’s own certificates are stored. Make sure you specify a location that is regularly backed up!

![Figure 24-4](image)

Figure 24-4 The Certificate Database Settings page of the Windows Components Wizard

8. As you ponder the storage configuration, also consider these options:

- If you’re going to be interoperating with clients that aren’t using Active Directory, or if you’re not using it, you can specify that you want the CA to maintain a shared folder to store newly created certificates in. To do this, select the Store Configuration Information In A Shared Folder check box, and then supply the name of an existing folder. Because you’re using Active Directory in
the figure, you can see that option is available. If you were not using Active Directory, it would be selected by default and you would not be able to clear the check box.

- If you're reinstalling Certificate Services on a machine that's already been acting as a CA, selecting Preserve Existing Certificate Database forces the installer not to overwrite the existing certificates, meaning that you are still able to use old certificates after the installation finishes.

9. If you're installing a subordinate CA, you have to request a certificate for this subordinate CA from whatever root CA you're using. The “CAs Linked into a Hierarchy” section later in the chapter details how this process works and covers the specifics. If you're installing a subordinate CA now, refer to that section before proceeding with the wizard. Otherwise, click Next.

10. If you're running the IIS WWW service, the installer tells you it must stop the service to complete the installation.

11. When the wizard finishes the installation, Certificate Services is available.

Once Certificate Services is installed, you can launch the Certification Authority snap-in from the Administrative Tools folder.

The Certification Authority Snap-In

After you open the Certification Authority snap-in, notice that it includes one subordinate item for each CA on the target server. Each CA, in turn, has five folders shown below it. Each folder displays some sort of list, so you can customize the list columns and fields using the View menu. Right-click the folder, and then use the Choose Columns and Customize commands until you configure the list the way you want it. The five folders you can view under each CA are as follows:

- **Revoked Certificates**  Lists all the certificates that have currently been revoked. Right-clicking this folder, pointing to All Tasks, and choosing Publish allows you to publish a new CRL (although you get a warning message if your existing CRL is still valid).

- **Issued Certificates**  Lists the certificates that this CA has issued. You can right-click individual certificates and use the Revoke command.

- **Pending Requests**  Shows the requests that are stuck at the CA waiting for you to approve or reject them. Remember, for enterprise CAs, this list is always empty; for standalone CAs, it might contain zero or more requests at any given time.
■ **Failed Requests**  Lists requests that failed or were rejected, including the common name, e-mail address, and submission date of the failed request.

■ **Certificate Templates**  Lists templates currently available for your use (Enterprise CAs only).

### Managing the Certification Authority Service

The Certificate Services service actually runs as a standard service, so you can manage it in two ways. First, you can use the Services item in the Computer Management snap-in to start and stop the service, set recovery options, change the security context it runs in, and so on. (See Chapter 12 for more about using the Services item.) More interestingly, right-clicking the Certification Authority item, or one of the CAs beneath it, gives you access to some useful commands.

First is the Retarget Certification Authority command, which appears when you right-click the Certification Authority item. You use this command to change the CA server you’re managing. By default, the snap-in attaches to the local server unless you specified another one when you installed it. This command lets you pick another CA server in your domain and administer it instead. The remaining commands appear when you right-click an individual CA and choose the All Tasks submenu. They’re discussed in the following sections.

### Starting and Stopping the CA

You can stop and restart the CA with the Start Service and Stop Service commands. When you stop the CA, it simply stops—you don’t get a chance to confirm your command or change your mind. The same is true for starting the service. Note that you have to stop the service before restoring the CA database, although the snap-in offers to do that for you before you start the restore process.

### Backing Up the CA

Backing up and restoring the CA data is critical because if you lose the CA, you lose the ability to issue, revoke, or renew certificates for the CA’s assigned domain. You can (and should) use the Windows backup utility to back up the certificate database. You can also use the Certification Authority Backup Wizard, which is slightly easier to use for the task at hand. All the wizard does is copy the current state of the CA’s data to a folder you specify. You can back up or archive those files easily without stopping the CA.

Selecting the Backup CA command starts the wizard, the first page of which is just an introduction telling you what the wizard does. If the CA service isn’t running, you’re prompted to start it because it must be active for the wizard to work. The second page of the wizard, shown in Figure 24-5, is where you specify what you want to back up.
Figure 24-5  The Items To Back Up page of the Certification Authority Backup Wizard

This wizard page provides the following options:

- The Private Key And CA Certificate check box forces the Certification Authority Backup Wizard to back up the private key and associated certificate that the CA uses. If you choose this option, the wizard asks you for a password that it uses to encrypt the private key and certificate data.

- The Certificate Database And Certificate Database Log check box causes the Certification Authority Backup Wizard to copy the certificate database and the log file, which shows issued certificates and pending requests.

- The Perform Incremental Backup check box allows you to avoid the overhead of backing up the entire log and queue each time. When this box is selected, the Certification Authority Backup Wizard backs up only the entries that have been changed since the last backup. However, you must perform at least one full backup (with this check box cleared) before you perform your first incremental backup. When you restore from incremental backups, you have to perform a restore from the initial backup, and then restore the incremental backups in order.

- Use the Back Up To This Location drop-down list to specify which directory you want the backup material stored in. The backup folder is supposed to be empty; the wizard warns you if it isn’t. You have to put each backup in a different location. For example, if you do one full and two incremental backups each week, you need three separate folders to store the backed-up files.

After you complete the Certification Authority Backup Wizard process, you have a set of files in the specified folder. The file `<caName>.p12` contains the private key material for
the CA, while the Database folder contains the log files. Use your preferred backup tool to make a good copy of these files and you’ll be able to restore the CA when you need to.

---

**Note**  Use the Windows Server 2003 Backup program to back up both the CA and the server. This provides a richer set of utilities for maintaining the necessary operational data for your server.

---

**Restoring the CA**

The Restore CA command runs the Certification Authority Restore Wizard, which in every way is the mirror image of the Certification Authority Backup Wizard. It requires that the CA service be stopped, and it lets you restore the data you backed up using the Certification Authority Backup Wizard. You can selectively restore any combination of the private key and CA certificate, the configuration data, and the issued certificate log and pending request queue. Select the appropriate check boxes, tell the wizard where your backup files are, confirm that you want the data restored, and restart the CA when you’re done.

One caveat: if you want to restore a series of incremental backups, you must first restore the corresponding full backup and then repeat the process for each incremental backup—in the right order! This argues in favor of giving your backup folders descriptive names like `Certserver backup\2005-0815`, or better yet, just do full backups.

---

**Renewing the CA Certificate**

Occasionally, you might need to renew your CA certificate. How often you do this depends on the lifetime you set for your CA certificate when you generate it, as well as on whether the CA’s key has been compromised and how big your current CRL is. The Microsoft CA allows you to reissue a CA certificate with the existing key material or to generate a new key pair and use it in the new certificate. The former option is useful when you just want a new certificate (for example, because your current certificate is about to expire), while the latter is what you use when you need new key material (as in the case of a compromise).

When you right-click the CA and choose the Renew CA Certificate command, the snap-in first warns you that the CA service must be stopped to generate the renewal. If you choose to proceed, a dialog box explains why you might need a new certificate and asks you whether you want to generate a new key pair. Whichever option you choose, the snap-in does its work quietly, issues the new certificate, and restarts the CA service.

---

**Configuring the CA’s Properties**

Each CA has a set of properties you can define, including properties for its policy and exit modules. You change these properties in the CA Properties window, which appears when you right-click a CA object and choose Properties from the shortcut menu.
The General tab of the Properties window shows you the name and description for the CA; it also identifies the CSP and hash algorithm that the CA is using. You’re stuck with all these values—you can’t modify them after the CA is created. You can also use the View Certificate button to see a certificate’s details.

**Note** You can change some certificate options by selecting a certificate from the Properties dialog box of the CA. Select one of the certificates in the CA Certificates list, and click View Certificate. Change to the Details tab on the Certificate dialog box. You see a list of fields and their corresponding values. If the list item has a pencil icon, you can edit that property.

**The Policy Module Tab**

The Policy Module tab shows you which policy module is currently active on your CA. In almost all cases, this is the Enterprise And Stand-Alone Policy module that Microsoft provides with Windows Server 2003. If you want to use an alternate module, you can use the Select button on the tab to select another one.

The Properties button opens the policy module Properties window (shown in Figure 24-6). The Request Handling tab lets you control what happens to incoming requests. The Follow The Settings In The Certificate Template option is selected by default for Enterprise CAs; it acts in accordance with rules included with the template. You can also use the Set The Certificate Request Status To Pending option, which is the default for standalone CAs. This selection requires administrator intervention.

![Figure 24-6](image)

*Figure 24-6  The Request Handling tab of the Properties window*
The Exit Module Tab
The Exit Module tab looks and works much like the Policy Module tab—it shows which exit modules your CA is configured to use. You can have more than one exit module in use at once, unlike policy modules, which are strictly one to a customer. Each exit module is executed in sequence. Because Microsoft provides only one exit module, though, this point is moot unless you’re using a third-party module. The Properties button on the Exit Module tab opens the exit module Properties dialog box, which has only one tab: Certificate Publication.

The Microsoft exit module automatically publishes certificates into Active Directory (if present) or to the location that the certificate request specified. By using the Certificate Publication tab of the exit module’s Properties window (which you access by clicking Properties on the Exit Module tab), you can turn publication on and off in two ways:

- Select the Allow Certificates To Be Published In The Active Directory check box to allow the exit module to load certificates into Active Directory, when present.
- Select the Allow Certificates To Be Published To The File System check box to allow publication to the shared folder you defined at CA setup time.

By default, the CA always publishes CRLs to the %Systemroot%\System32\Certsrv\Certenroll folder, and each CRL is given a name starting with the name of the CA and (when necessary) ending with a number in parentheses that reflects the renewal history of that CA. You can take these files and publish them via HTTP, FTP, or other means, including manually or automatically loading them onto smart cards.

The Storage Tab
The Storage tab, shown in Figure 24-7, shows you where configuration and certificate data are stored. You can't change any of these values after the CA is set up, but having a way to double-check the file locations in case you need them can be useful.

![Figure 24-7  The Storage tab of the Properties window](image-url)
The Security Tab
The Security tab gives you control over which users and groups can do what with your CA. By default, four groups have access control lists (ACLs) that give them predetermined permissions. The Administrators, Domain Administrators, and Enterprise Administrators have both the Issue And Manage Certificates permission and the Manage CA permission allowed. The Authenticated Users group is given only the Request Certificates permission.

Note If you are using a standalone CA, only two groups have ACLs: Administrators and Everyone.

Working with Certificate Templates
Certificate templates give you an easy way to stamp out cookie-cutter certificates you can use for well-defined purposes. Microsoft Windows 2000 Server provided Version 1 templates. These could not be customized for a particular use; you could use them only as designed.

Both the Windows Server 2003 Enterprise Edition and Datacenter Edition provide Version 2 templates as well, which can be edited to suit your needs. If you copy a Version 1 template, it is automatically promoted to a Version 2 template. If you don’t find that an existing template provides what you need, Windows Server 2003 gives you the ability to create new templates.

Note The Certificate Templates snap-in, new in Windows Server 2003, is used to clone and edit the certificate templates.

When someone requests a certificate using your CA’s Web enrollment pages (as described in Chapter 22), he or she can choose any of the templates that are available. You determine which templates the requestor can use by adjusting the security permissions on the templates.

Setting Security Permissions and Delegate Access
Before you can adjust security permissions on a template, you must open the Active Directory Sites And Services snap-in. Open the View menu, and choose Show Services Node. When the Services node appears, expand it and then expand the Public Key Services node and beneath it the Certificate Templates node.

At that point, you can right-click an individual template from the list in the MMC window, and then choose Properties to see that template’s individual properties. When the Properties window appears, switch to the Security tab (shown in Figure 24-8). Adjust the
properties to reflect the access you want individual users or domain groups to have. For example, if you don’t want anyone to issue enrollment agent certificates, just deny full control to all users, and that’s that.

Figure 24-8  The Security tab of the Properties window

Enabling Autoenrollment

You can use a Group Policy setting to allow automatic issuance of certificates for computers. This allows you to automatically generate, issue, and store a new certificate for each computer that joins your domain. As long as you have administrative privileges on the Group Policy Object (GPO) for your domain, you can make this change by using the Automatic Certificate Request Setup Wizard. Here’s what to do:

1. Open the GPO you want to edit by using the Group Policy snap-in. (See Chapter 9 if you need a refresher on GPOs.)

2. Expand the GPO’s Computer Configuration node, and then expand the Windows Settings, Security Settings, and Public Key Policies nodes.

   Note  You can also set autoenrollment for users by selecting the User Configuration node instead of the Computer Configuration node, and then continuing with the steps as described.

3. Double-click the Autoenrollment Settings node. The Autoenrollment Settings Properties dialog box appears (as shown in Figure 24-9).
4. In the dialog box, you can enable or disable autoenrollment for subjects of the Group Policy object.

5. Click OK to save your changes, or click Cancel to discard them.

Managing Revocation and Trust

Certificates provide you with a way to securely verify the identity of principles on your network. However, just having a big bag of certificates doesn’t help you with security—you must also make decisions about which certificates you trust, and you need a mechanism to “untrust” certificates if they’re compromised or if, for some reason, the holder no longer needs (or must no longer have) them.

In the Windows Server 2003 public-key infrastructure (PKI), you codify decisions about trust by specifying which root CAs go on your CTL. You can specify CTLs for individual users and groups; you can also specify as part of a GPO a default CTL that new users, computers, and groups inherit. Likewise, you render certificates untrusted either by removing their issuing CA’s certificate from the CTL or by revoking the certificate itself, depending on whether you issued it. (You can revoke only certificates that your CA issued in the first place.)

Revoking certificates is simple: open the CA snap-in, switch to the Issued Certificates node, right-click the target certificate, point to All Tasks, and choose Revoke Certificate. The command lets you choose a revocation reason. (The default is Unspecified, but you can also mark a certificate revoked for a particular reason, such as a key being compromised or a change in the user’s affiliation.) As soon as you choose a reason, the certificate is revoked. There’s no appeal; you can’t “unrevoke” a certificate, but clients might not notice that the certificate has been revoked until they get the next CRL update.
Publishing CRLs

When you revoke a certificate, Windows Server 2003 adds it to the CRL immediately, but the CRL isn’t published right then—the server automatically updates the CRL and publishes it at the interval you specify. You can manually publish the CRL at any time by right-clicking the Revoked Certificates item in the CA snap-in, pointing to All Tasks, and choosing Publish. After asking you to confirm that you want to supersede the existing CRL, the snap-in forces the CA to publish the current CRL to the CRL distribution points you previously specified.

There is an easy way to reference past revocations. You can view the current CRLs for the server by switching to the View CRLs tab on the Revoked Certificates Properties dialog box.

Windows Server 2003 can also publish CRLs on a schedule you set. The Properties window for the Revoked Certificates item in the CA snap-in, as shown in Figure 24-10, lets you control the interval at which CRLs are published. By default, CRLs are updated weekly, but you can specify an interval ranging from one hour to 9999 years. You can also turn off scheduled CRL publication completely. You might want to do this if you want to control the circumstances and timing under which new CRLs are issued.

Delta CRLs

In Figure 24-10, you can see the delta CRL options. This is a powerful new option for Windows Server 2003, and you should be aware of its purpose. In Windows 2000 Server, the certificate revocation information was published in what RFC 2459 calls a complete CRL. Windows Server 2003 permits a CA to publish delta CRLs, which contain only the
information that changed since the last full CRL was published. The delta CRLs are easier to manage, have less impact on the performance of the network, and enable you to distribute revocation information quickly.

**Note** To use delta CRLs, you need to have a Microsoft Windows XP Professional client and a Windows Server 2003 CA. Clients that don’t use delta CRLs simply retrieve the complete CRL.

**Changing CRL Distribution Points**
The CA honors any certificate publication information it finds in the incoming certificate request. However, it depends on you to specify where CRLs must be published and where the certificates must point for users who want a copy of the CA’s certificate. You supply these locations on the Extensions tab of the CA node’s Properties window. By default, CRLs and root certificates are distributed via HTTP, LDAP, and a shared folder, but you can turn off these distribution points and add your own at any time.

**Controlling Which Trusted Certificates Are Distributed**
You can change the set of trusted root certificates that is distributed as part of a GPO. This enables you to build and deliver a certificate set containing only the CAs you want users in particular groups to be able to trust. Let’s say you use a third-party root CA (such as VeriSign) with your own enterprise subordinate CA. You can set up one GPO for each department and then tweak the list of CAs for that department so that the legal department, for example, doesn’t trust any of your internal CAs.

You can make three basic changes to the root list in a GPO: you can import root certificates and add them to the list, you can remove an existing root certificate from the list, or you can change the root certificate’s allowed roles. All these possibilities require that you open the GPO whose trusted certificate list you want to modify and then expand it so that you can see the Trusted Root Certification Authorities item. (You need to expand the Computer Configuration, Windows Settings, Security Settings, and Public Key Policies nodes.) At that point, you can do the following:

- To import a new certificate and begin trusting it, right-click the Trusted Root Certification Authorities item, point to All Tasks, and choose Import. Tell the Import Wizard where the certificate you want to import is. The wizard then loads the certificate into the list of trusted roots and displays it.

- To remove a root certificate from the list, right-click it and choose the Delete command. You see a confirmation dialog box that warns you of the consequences of removing the certificate.

- To edit the list of approved uses for a root certificate, right-click the root certificate name and choose Properties. A dialog box like the one shown in Figure 24-11
appears. Use the options in the Certificate Purposes group to specify what you trust this certificate to do. When the Enable Only The Following Purposes check box is selected, you can enable or disable specific purposes by selecting or clearing them in the list.

This list of root certificates is distributed as part of the group policy; that means it is available to all users and computer accounts linked to the GPO. Don’t confuse this list with the CTL—more on that in a minute.

![Figure 24-11 The General tab of the properties sheet of a root certificate](image)

Managing Certificate Trust Lists for a Group Policy Object

The CA list you manage in the Trusted Root Certification Authorities item is nothing more than a bag of CA certificates—there’s no implication that your enterprise trusts them (or not). To use certificates issued by other CAs, you have to put them on the CTL. Your CA signs the CTL and distributes it to indicate that you designated the CAs on the CTL as trusted. You can import a CTL that you generated on another Windows Server 2003 machine, or you can create a new one. Both actions occur in the Enterprise Trust node under the Public-Key Policies component of a GPO, and both are available as commands when you right-click the Enterprise Trust folder.

To create a new CTL, point to New on the Enterprise Trust item’s shortcut menu and choose Certificate Trust List to open the Certificate Trust List Wizard. After the wizard opens, you have to complete several steps to successfully create a new CTL:

1. On the Certificate Trust List Purpose page of the wizard (shown in Figure 24-12), specify the prefix used to name the CTL, how long you want the CTL to remain valid, and for what purposes you trust CAs on the CTL. Click Next.
2. On the Certificates In The CTL page of the wizard, add CA certificates to the CTL. (See Figure 24-13.) You can add CA certificates from the certificate store or from a file by using the corresponding buttons. Click Next.

3. Designate a certificate to use for the CTL signature. The certificate you select here is used to sign the CTL, so be sure to choose a certificate that you have good control over. (That way, no one can steal it and spoof your CTL.)
4. After you choose a signer for the CTL, you can choose to add a secure timestamp, which guarantees the date and time recorded in the CTL. However, you must have access to a secure timestamp service.

5. Provide a name and description for the CTL; these items are displayed in the MMC whenever the CTL is shown in a list.

6. Click Finish and the CTL is created. After it is available, you can remove it or edit it (using the wizard interface) by right-clicking it and using the appropriate commands.

Managing Standalone CAs

You already understand the structural differences between an enterprise CA and a standalone CA, but some subtle functional differences exist, too—two management tasks are unnecessary for enterprise CAs but mandatory for standalone CAs.

Setting the Default Action for New Requests

By default, a standalone CA is set to mark all incoming certificate requests as pending. This forces the requests into a queue of pending requests (shown in the Pending Requests item under the CA node), where they remain until a human operator either approves or rejects them. You can change this setting by opening the CA Properties window, clicking the Policy Module tab, clicking Properties, and using the two options on the Default Action tab to change the default action from Set As Pending to Always Issue (or vice versa). After this action takes effect, all incoming requests are treated as you specify, but this change doesn’t affect any pending requests.

Security Alert  
Standalone CAs do not use Active Directory to ensure that the requesting user or computer is authorized to be issued a certificate automatically. Therefore, you should set the default action to Set As Pending for standalone CAs.

Changing Certificate Request Status

Let’s say you have some pending requests in your queue. How can you approve or reject them? The answer lies in the same place as it does for most other “How do I...?” questions involving the Microsoft Management Console (MMC): the right mouse button. Right-clicking a request in the Pending Requests list allows you to approve or reject it.

The Certificates Snap-In

The Certification Authority snap-in is for managing CAs, not the certificates they issue. A corresponding snap-in is intended just for managing certificates—the Certificates snap-in. Clients on your network can manage their own certificates by using the Certificates button on the Content tab of Microsoft Internet Explorer’s Internet Options dialog box; it
does most of what the snap-in can do without requiring that you give your users access to the snap-in.

The basic functions of the Certificates snap-in (along with its installation requirements) are discussed in Chapter 22. However, the behavior and functionality of the Certificates snap-in change slightly when you use it in a domain that has an enterprise or standalone CA. You’ll notice a new item in the Certificates store: REQUEST. The REQUEST store holds certificate requests that are awaiting your approval decision.

**CAs Linked into a Hierarchy**

Your network design might call for connecting several CAs so that you have separate root and subordinate CAs. Splitting up CAs like this is considered good security by most experts because it allows you to have a root CA that issues certificates only to subordinate CAs, so it can be better protected than the subordinate CA servers. To accomplish this with Certificate Services, first install and configure a root CA as described earlier in this chapter. In particular, you must indicate that you want the newly installed CA to be an enterprise root or standalone root server.

After you install and configure the root CA, your next task is to install and configure each subordinate CA. The installation process is largely identical to the process required to install a root CA, except that you must perform an additional step after you specify the storage location you want to use for your certificates: you must request a certificate for the new CA. You do this with the CA Certificate Request page, shown in Figure 24-14. What you do with this screen depends on whether the root CA that “owns” this subordinate CA is available on your network. The next two sections describe each scenario.
Requesting a Certificate if Your Root CA Is Online

If you’re using an all-Windows Server 2003 PKI, and if your root (or parent) CA is available on the network, you’re in luck. All you have to do is select Send The Request Directly To A CA Already On The Network, specify the computer name of the parent CA server, and then choose the parent CA instance on that computer from the Parent CA list. (Remember, a single CA server computer can host multiple CAs.)

Requesting a Certificate if Your Root CA Is Offline

If your root CA isn’t available on your network, you need to select Save The Request To A File. That forces the wizard to generate a PKCS #10 format certificate request and store it in a disk file. You can then e-mail that file to the root CA, put it on a floppy disk or smart card, paste it into a Web page, or do whatever else your root CA requires. If you want to submit a certificate request to a Certificate Services server, you can do so with the following steps:

1. Open Internet Explorer, and connect to http://caServerName/certsrv, where caServerName is the DNS name of your root CA.

   **Note** This procedure works only if the /certsrv virtual root has been created on the CA server. This doesn’t happen if you install IIS after installing Certificate Services. In this instance, you must install the virtual root by typing certutil –vroot at a command line.


3. Click the Submit A Certificate Request Using A Base-64-Encoded PKCS#10 File Or Submit A Renewal Request Using a Base-64-Encoded PKCS#7 File link.

   **Note** Submit the actual subordinate CA request by opening it in Note-pad, copying its text, and pasting it into the Saved Request text box. As an alternative, you can use the Browse button to locate the .REQ file on disk and upload it, but this might require that you modify your Internet Explorer settings so that your root CA is a trusted site.

4. Click Submit. Depending on how you have configured your root CA, you get either a message saying that the certificate request is pending or one indicating that it was approved. If it was approved, use the Download Certificate button to retrieve the certificate and store it on your local disk.

   **Note** If you’re not using a Windows Server 2003 CA, the exact procedure you use to send the request to your CA will vary; consult your CA vendor or documentation for details.
Chapter 24  Using Microsoft Certificate Services

A subtlety is involved in using a third-party CA: The Windows Server 2003 CA Service expects to be able to build a full certificate path when it starts. If your root CA includes CA certificates for all CAs in the certificate path (and the Windows Server 2003 CA does), you don’t have to do anything extra. If not, you have to manually add the CA certificates of any parent CAs to the Intermediate Certification Authorities certificate store, as well as adding the root CA certificate to the Trusted Root Certification Authorities store. You can do these in any order; the key is to make sure you add certificates for the root CA and all subordinate CAs that are parents of the CA you’re installing before you try to install the new subordinate CA’s certificate and start the CA service.

After you load any needed certificates from the certificate path and have requested and received a certificate for your new subordinate CA, you still have to load it into the certificate store. You do this from the Certification Authority snap-in. Select the newly installed subordinate CA, and then click Action, point to All Tasks, and choose Install CA Certificate. Until you do so, your new subordinate CA isn’t able to process any requests.

Command-Line Utilities

Certificate Services includes three command-line tools you can use for various administrative tasks. Although none of these tools are necessary for ordinary operation of your CAs, sometimes they come in handy.

The Certsrv Tool

Certsrv.exe is the actual executable that implements the Certificate Services code. Normally, you start and stop the server using the Services snap-in; however, you can manually start it from the command line. This allows you to start the server only when you need to issue a new certificate. Many sites choose to run their root CAs in this on-demand mode because it helps reduce the risk of an accidental or malicious issuance of an unwanted certificate.

As an extra bonus, if you run Certsrv.exe with the -z command switch, it displays a log of its activities in the console window you used to start it. This is invaluable for debugging or just for gaining a better understanding of how the server accomplishes its tasks.

The Certreq Tool

Most of the time you request certificates through the Web interface (which is discussed in Chapter 22) or through a program that’s been written to take advantage of Certificate Services. However, sometimes manually requesting a certificate is useful. For example, you typically need to manually request certificates for subordinate standalone CAs, and requesting test certificates from a new server is often useful so that you can verify that it’s
working properly. The Certreq tool (Certreq.exe) allows you to request a new certificate from a CA in your domain or retrieve any certificate previously issued by that CA—you can even retrieve revoked or expired certificates.

The Certreq tool has two slightly different forms. The one you use to request certificates looks like this:

[-attrib attribString] [-requestFile [certFile | chainFile]]

- The `-submit` switch submits a request to a CA.
- The `-rpc` switch forces the Certreq tool to contact the CA with a standard Windows remote procedure call (RPC) request instead of a Distributed COM request.
- The `-binary` flag specifies that you want the certificate or CRL to be stored as a binary file instead of in base-64 encoding. You normally use this option when you want to take the object returned from the server and import it into a program that uses certificates directly.
- The `-crl` switch includes the CRLs in the base-64 or PKCS #7 output file.
- Use the `-config` switch to specify which CA you want to send your request to. You have to specify both the server and CA names. For example, to request a certificate from a CA named Netsolvers Purchasing on a server named HQ4, you write

  certreq -config HQ4"Netsolvers Purchasing"

  You can also use a single hyphen in place of a server/CA name if you want to request a certificate from the default CA for your domain.

- If you want to specify additional attributes in the certificate request, use the `-attrib` switch, along with the attribute names and values you want to use. Each name-value pair must be separated with a newline character, “\n”, like this:

  attrib "Hair color:blond\nEye color:blue"

- If you want to submit a request generated by another program, you can do so by specifying the request’s file name. That’s what the `requestFile` parameter is for. The Certreq tool can forward requests in three formats: PKCS #10 (used to request new certificates), PKCS #7 (used to request renewal of an existing certificate), or CMC, short for the Certificate Management protocol using Cryptographic Message Syntax (CMS). CMC is used to request a new certificate. The request file can be either raw binary or base-64 encoded, as long as it’s in one of the supported formats.

- If you’re using Active Directory, the CA publishes newly generated certificates for you. If not, or if you need to get the certificate back as a file so that you can do something with it, specify a filename in place of the `certFile` parameter and Certreq puts
a copy of the new certificate in the specified file—provided that the CA approves the request, of course. In the same vein, supplying a filename in place of the `chainFile` parameter causes Certreq to provide you with a copy of the entire certificate chain for the new certificate, starting at the root CA and including all subordinate CA certificates.

**The Certutil Tool**

The Certutil tool is practically a Swiss Army knife—you know, like the really big ones you see at camping supply stores. It has 40 modes, which perform tasks ranging from stopping the CA service to creating a backup of the CA’s private keys to scanning a certificate file for particular ASCII characters that can confuse older certificate service implementations. For help with the Certutil commands, type `certutil /?` or perform a search in Help for `certutil`.

**Summary**

This chapter explained the fundamentals of planning for and deploying the public-key infrastructure services that Microsoft includes with Windows Server 2003. You learned how to install and manage Microsoft Certificate Services and how to set policies that govern what users can do with it. The next chapter covers the routing and remote access services.
Routing and remote access services have been around in one form or another—under the names Remote Access Service (RAS), Routing and Remote Access Service (RRAS), and Dial-Up Networking—in every version of Microsoft Windows NT. In Microsoft Windows Server 2003, this service is called Routing and Remote Access, although you might still see the acronym RRAS used.

A computer running Microsoft Server 2003 and Routing and Remote Access acts as a remote access server. This server authenticates users and enables the use of services typically available to a LAN-connected user (file and print sharing, applications, messaging, and so forth). The remote access server can connect remote users to the network using...
both virtual private network (VPN) and dial-up technology. Windows Server 2003 also supports Remote Authentication Dial-In User Service (RADIUS), the well-known authentication method used by many Internet service providers (ISPs). The user signs in with a name and password, which is then passed on to a server that authenticates the user and authorizes access.

As in many areas of network administration, the complexities of Routing and Remote Access are more apparent than real. However, it is possible to plunge in and create an amazing amount of confusion if you don’t first understand the concepts underlying the options.

How Dial-Up Remote Access Works

Dial-up remote access, also called Dial-Up Networking, allows an off-site computer to tap into an office computer’s resources using a modem. Figure 25-1 shows typical dial-up connections made to a network.

![Figure 25-1  Dial-up connections to a network](image)

Remote or mobile users using a dial-up communications link can access network resources as if they were directly connected. Windows Server 2003 remote access servers
can connect to clients running Microsoft Windows XP Professional, Windows Server 2003, Windows NT, Windows 95, Windows 98, Windows for Workgroups, MS-DOS, or Apple Macintosh. Typically, the client connects through a standard telephone Integrated Services Digital Network (ISDN), digital subscriber line (DSL), cable, X.25 or Asynchronous Transfer Mode (ATM) link.

### Understanding Virtual Private Networks

A VPN is an extension of a private network across a public network such as the Internet. Using a VPN, connections across the public network can transfer data in an encrypted form that creates a tunnel between the client and the target network. VPNs use the routing infrastructure of the Internet, but to the user it appears as though the data were being sent over a dedicated private link.

The appeal of a VPN is the Internet and its global presence. Communication links can be made quickly, cheaply, and safely across the world. Dedicated private lines aren’t required, and security can be configured at very high levels.

#### Real World  When a VPN Isn’t Appropriate

Although VPNs are great methods of connectivity for branch offices and remote users of every stripe, there are conditions under which a VPN isn’t appropriate:

- When performance at any price is the primary concern
- When most traffic is synchronous, as in voice and video transmissions
- When using an application with unusual protocols that are not compatible with TCP/IP

In these situations, a dedicated private line is almost always the best choice.

#### How VPNs Work

In a VPN, both ends of the connection make a link to the Internet. (Technically, they can link to any public network, but it’s almost always the Internet.) The link can take the usual forms—a regular telephone line, a DSL or cable connection, a wireless connection at your local coffee shop, or a dedicated line of some sort. Instead of sending a packet as the originating node produces it, the VPN, using a tunneling protocol, encapsulates the packet in an additional header. The header provides routing information so that the encapsulated data can traverse the intermediate internetwork. For privacy, the data is
encrypted and, if packets are intercepted, they cannot be unencrypted without the encryption keys.

This technology allows a remote user in Connecticut, for example, to establish a dial-up connection with any ISP and, through that connection, make a direct connection to a server on the company network in British Columbia. It’s quick, it’s cheap, and it’s easy to set up. Figure 25-2 shows a VPN set up so that traveling employees, telecommuters in home offices, and employees in branch offices can all connect to the main network at a company’s headquarters. Each component is connecting to the ISP through a different type of communications channel, but all are part of the same VPN. Figure 25-3 shows a more typical VPN, in which the connection is made from one router to another.
Components of a VPN

A VPN connection in Windows Server 2003 consists of a VPN server, a VPN client, a VPN connection (the portion of the connection in which the data is encrypted), and the tunnel (the portion of the connection in which the data is encapsulated). The tunneling is done through one of the tunneling protocols included with Windows Server 2003, both of which are installed with Routing and Remote Access:

- **Point-to-Point Tunneling Protocol (PPTP)**  An extension of the Point-to-Point Protocol (PPP) in use for many years, PPTP was first used in Windows NT 4.

- **Layer Two Tunneling Protocol (L2TP)**  A combination of PPTP and Layer Two Forwarding (L2F), a tunneling protocol developed by Cisco Systems. L2TP employs Internet Protocol Security (IPSec) for encryption, so the VPN client and server must support both L2TP and IPSec.

**More Info**  For more information about the VPN protocols, see RFC 2637, “Point-to-Point Tunneling Protocol,” and RFC 2661, “Layer Two Tunneling Protocol.” Both can be found at (among other places) [http://www.rfc-editor.org/rfcsearch.html](http://www.rfc-editor.org/rfcsearch.html) on the Internet.

**Common Configurations for Remote Access Servers**

When you run the Routing and Remote Access Server Setup Wizard, you’re asked to choose from a list of configuration options, as shown in Figure 25-4. If none of the defined options describe your aim, select Custom Configuration. However, if you use Custom Configuration, you have to configure all the details manually.
Remote Access (Dial-Up Or VPN)  Select this option for either a dial-up connection (which is discussed in the “Configuring a Server for Dial-up Clients” section) or a secure VPN (which is discussed in the “Configuring a Virtual Private Network” section).

Network Address Translation (NAT)  This option sets up the server to allow internal clients to connect to the Internet using a single IP address (which is discussed in the “Configuring a NAT Server” section).

Virtual Private Network (VPN) Access And NAT  With this option, the server provides a NAT for the internal network and also accepts VPN connections.

Secure Connection Between Two Private Networks  Select this option to set up and connect a router-to-router VPN (which is discussed in the “Elements of a Router-to-Router VPN Connection” section).

Custom Configuration  Select this option to manually select a combination of features from those available.

Configuring a Server for Dial-Up Clients
To allow the connection of multiple, simultaneous dial-up clients, you must have modem-pooling equipment (hereafter referred to as the modem bank) with the appropriate connections to the local telecommunications provider. A typical modem bank for
Windows Server 2003 includes an adapter that is installed on the computer running Windows Server 2003. Make sure that the equipment is in the Windows Catalog (http://testedproducts.windowsmarketplace.com), and that all the protocols needed for the dial-up connections are installed on this server. Then follow these steps:

1. Launch Routing And Remote Access from the Administrative Tools folder on the Programs menu.

2. By default, the local computer is shown as a server. Right-click the computer in the console tree, and choose Configure And Enable Routing And Remote Access from the shortcut menu.


4. In the Configuration dialog box, select Remote Access (Dial-Up Or VPN) and click Next.

5. Choose Dial-Up and then click Next.

6. Select your choice for IP address assignment. Automatic assignment is strongly recommended. Click Next.

7. In the Managing Multiple Remote Access Servers dialog box, select the option of not using a RADIUS server. (If you will have multiple remote access servers, see the “Using RADIUS for Multiple Remote Access Servers” section later in this chapter.)

8. Click Next, and then click Finish. The Routing and Remote Access service starts and initializes automatically.

---

**Configuring a NAT Server**

You can allow the wizard to prompt you for all the steps to set up a NAT server and configure the firewall, or you can use a custom configuration in the initial steps of the wizard and then manually add an interface, static filters, and so on. For most configurations, just take the default settings that the wizard will create. You can always adjust them later.

To configure a NAT server, follow these steps:

1. Launch the Configure Your Server Wizard, and click Next twice.

2. Select the Remote Access/VPN Server role from the Server Role list. Click Next two more times.

3. The Routing And Remote Access Server Setup Wizard starts. To continue, select the Network Address Translation (NAT) option and click Next.
4. Select the interface that will connect to the Internet, as shown in Figure 25-5.

Figure 25-5  NAT Internet Connection page

5. Select the Enable Security box.

6. Click Next, and when you've confirmed that your selections are correct, click Finished.

---

Setting Remote Access Policies

In Windows NT 4, remote access is granted based solely on whether the user's account has dial-in permission. The permission is configured in User Manager or the Remote Access Administration utility.

In Windows Server 2003 and Windows 2000, remote access is somewhat more complicated. Authorization is determined by a combination of the dial-in properties for the user account and the remote access policies. With remote access policies, connections can be authorized or denied based on the time of day, the Windows Server 2003 group to which the user belongs, the type of connection being requested, and many other variables. By default, only one policy is in place when you install Routing and Remote Access: Allow Access If Dial-In Permission Is Enabled. However, this policy operates quite differently, depending on which administration model you use.
Real World  Authorization and Authentication

The similarity between the words *authorization* and *authentication* can cause confusion, and it’s important to understand the differences. *Authorization* is the process of giving a user access to system objects based on his or her identity. *Authentication* is the process of identifying a user. In remote access connections, this is done when the client sends the user’s credentials (user name and password) to the server using an authentication protocol. Authentication ensures that the individual is who he or she claims to be, but it says nothing about the access rights of the individual.

Understanding the Default Policy

When you launch Routing and Remote Access from the Administrative Tools folder and click Remote Access Policies in the console tree, the details pane lists two policies. The first policy is called Connections To Microsoft Routing And Remote Access Server. Double-click the policy to open the Settings dialog box. One policy condition is shown: MS-RAS-Vendor Matches “^311$” (as shown in Figure 25-6). The condition means that the policy applies only when the version of the RADIUS client is ^311$, so subsequent settings in this policy apply only to RRAS machines. Every other RADIUS client (wireless access points and third-party network access servers, for example) will fail to meet this requirement and so move on to the second policy called Connections To Other Access Servers. The first policy, Connections To Microsoft Routing And Remote Access Server, is the default RRAS policy and the one you’ll be modifying to match your needs.

![Figure 25-6 Properties for the default Remote Access policy](image)
The area labeled If A Connection Request Matches The Specified Conditions contains two options: Deny Remote Access Permission and Grant Remote Access Permission. You might think that the default setting of Deny Remote Access Permission would prevent anyone from dialing in to this remote server, but you would be mistaken. Whether these options actually allow or prevent a connection depends on the dial-in permission of the user account.

The confusion arises because people tend to use the terms “permission” and “policy” as if they were interchangeable. Permission is set on the user account, and it is denied by default. The dial-in permission set on the user account overrides the permission option in this Properties dialog box except in the case of the native-mode administration model (described in the next section), in which all user accounts are set to Control Access Through Remote Access Policy.

Read carefully the sections on administrative policies that follow, and study the logic diagrams. The administrative approach you choose should be as simple as possible while still meeting your needs.

### Choosing an Administrative Model for Remote Access Policies

In Windows Server 2003, you can choose from among three models for administering remote access permissions and connection settings:

- Access by user
- Access by policy in a Windows 2000 mixed or Windows Server 2003 interim domain
- Access by policy in a Windows 2000 native or Windows Server 2003 domain

An essential part of planning for remote access is determining which models you can use and deciding on an appropriate one. There is enough variation among the models that attempting to mix them is a recipe for confusion. No matter which model you choose, plan on thoroughly testing your chosen access policies to make sure that you’re getting the results you intend.

### Administering Access by User

In the access-by-user administrative model, remote access permissions are determined by the remote access permissions in the Dial-In tab of the Properties dialog box for the user account. To enable or disable remote access permission for individual users, set Remote Access Permission to either Allow Access or Deny Access. This administrative model is by far the simplest, and it works very well when the number of remote users is small and the access issue is uncomplicated.
If remote access permission for the user account is set to either Allow Access or Deny Access, the remote access permission setting on the remote access policy is effectively overridden. Access by user can be administered with multiple policies, but doing so can be complicated because a connection attempt might be rejected even when the remote access permission on the user account is set to Allow Access. If a connection attempt matches the conditions of a policy but does not match the profile settings or does not match any of the remote access policies, the connection attempt is rejected, as shown in Figure 25-7.

In the access-by-user administrative model, you can control access in three ways:

- **Explicit allow** The remote access permission for the user account is set to Allow Access, and the connection attempt doesn’t conflict with a policy or the settings of the profile and the dial-in properties of the user account.

- **Explicit deny** The remote access permission for the user account is set to Deny Access.

- **Implicit deny** The connection attempt doesn’t match the conditions set in any remote access policies.
The access-by-user model can be used on a standalone remote access server, or a remote access server on any of the four domain functional levels.

More Info  Detailed information on the four domain functional levels can be found in Chapter 14.

Granting Access by User

The access-by-user model resembles the administrative model of Windows NT 4. Individual user accounts are set to Allow Access or Deny Access. Open Routing and Remote Access from the Administrative Tools menu. Double-click the policy Connections To Microsoft Routing And Remote Access Server. The profile should be set to the default settings, and the Deny Remote Access Permission option should be selected.

But wait! If Deny Remote Access Permission is selected, isn’t remote access permission denied? No; it means basically nothing in this scenario. Access is determined solely by the settings in the Properties dialog box for the individual user account. Figure 25-7 shows the progression of a connection under the access-by-user administrative model.

Administering Access by Policy for a Mixed-Mode Domain

In the access-by-policy administrative model for a Windows 2000 mixed or Windows 2003 interim functional level domain, the remote access permission on every user account is set to Allow Access, the default remote access policies are deleted or demoted, and separate remote access policies are created to define the types of connections that are allowed. On a remote access server running Windows Server 2003 that is a member of a mixed or interim functional level domain, the Control Access Through Remote Access Policy option is not available for remote access permission on the user account. If a connection attempt corresponds to the conditions of a policy (subject to the profile and user account dial-in settings), the connection is accepted.

In the access-by-policy administrative model for a mixed or interim functional level domain, you can control access in three ways:

- **Explicit allow**  The connection attempt matches the conditions of a policy, subject to the settings of the profile and the dial-in properties of the user account.

- **Explicit deny**  The connection attempt matches the conditions of a policy but not the settings of the profile. You can do an explicit deny in this model by editing the profile and enabling the Restrict Dial-In To This Number Only option in the Dial-In Constraints tab and then typing a number that does not correspond to any dial-in number being used by the remote access server.

- **Implicit deny**  The connection attempt does not match the conditions of any remote access policies.
Note: The access-by-policy administrative model for mixed or interim domains can be used with Windows NT servers running Routing and Remote Access if the Windows NT servers are configured as RADIUS clients to a Windows 2000 or Windows Server 2003 Internet Authentication Service (IAS) server. A Windows NT server running RAS cannot use access by policy. You must upgrade the server to Windows NT RRAS (or to Windows Server 2003) to employ the remote access policy authorization.

Granting or Denying Access by Group Membership for a Mixed Domain

To allow connections for users by group membership, all user accounts have Remote Access Permission in the Dial-In tab set to Allow Access. To set up the access by groups, the administrator makes the following settings:

- In Routing and Remote Access, double-click the default policy and click Add. Add the Windows-Groups attribute to the policy. Select the group or groups to be granted access.

- On the policy, select the Grant Remote Access Permission option.

In this case, the Grant Remote Access Permission option means what it says. Figure 25-8 shows the progression of a connection attempt when a remote user dials in and access is controlled by group membership.

![Diagram](image)
With these settings, only the members of the specified group are granted access. Perhaps you have a situation in which it’s easier to specify who isn’t allowed access than to specify who is. For example, employees in production might have user accounts on the network but have no need for dial-in access. In this case, you need to make the following settings:

- Double-click the default RRAS policy. Click Add and select Windows-Groups.
- Add the group you want to deny access to.
- Click Edit Profile and, in the Dial-In Constraints tab, select Allow Access Only To This Number and type in any number that is not a dial-in number of the remote access server, as shown in Figure 25-9.

In this case, once again, it doesn’t matter whether Deny Remote Access or Grant Remote Access is selected in the Settings tab for the policy.

Figure 25-9   Configuring the dial-in constraints to deny access to a group

Figure 25-10 shows the logic of the connection attempt when access is denied by group membership.
Administering Access by Policy for a Native Domain

In a domain using the Windows 2000 native or Windows Server 2003 functional levels, you can use the access-by-policy administrative model, which has the following settings:

- The remote access permission on every user account is set to Control Access Through Remote Access Policy.
- Remote access permissions are determined by the remote access permission setting on the remote access policy.

These settings mean that the Remote Access Permission setting on the remote access policy determines whether remote access permission is allowed or denied. Figure 25-11 shows the progression of a connection attempt in a native-mode domain.
In the access-by-policy administrative model for a Windows 2000 native-mode domain, you can control access in three ways:

- **Explicit allow** The remote access permission on the remote access policy is set to Grant Remote Access Permission, and the connection attempt matches the conditions of the policy, subject to the settings of the profile and the dial-in properties of the user account.

- **Explicit deny** The remote access permission on the remote access policy is set to Deny Remote Access Permission, and the connection attempt matches the conditions of the policy.
■ **Implicit deny**  The connection attempt does not match the conditions of any remote access policies.

---

**Note**  If you use the access-by-policy administrative model for a native-mode domain, don’t add remote access policies and don’t change the default remote access policy—that way, no users are allowed remote access. By default, the remote access permission on the default remote access policy is set to Deny Remote Access Permission. If you change the setting to Grant Remote Access Permission, all users are allowed remote access.

The access-by-policy administrative model for a Windows 2000 native or Windows Server 2003 domain also applies to standalone remote access servers that are not members of a domain. You can’t use this access-by-policy administrative model if you have Windows NT 4 RAS or RRAS or IAS servers because a domain with Windows NT servers is either a Windows 2000 mixed or Windows Server 2003 interim domain.

---

**Security Alert**  If you use the access-by-policy administrative model for a Windows Server 2003 or Windows 2000 native domain and you do not use groups to specify which users get access, verify that the Guest account is disabled and that its remote access permission is set to Deny Access.

---

**Granting or Denying Access by Group Membership for a Native Domain**

In a domain using the Windows 2000 native or Windows Server 2003 functional level, setting access by policy requires that all user accounts have the Control Access Through Remote Access Policy option selected in the Dial-In tab of the user account’s Properties dialog box. To allow access by specified groups, the administrator must do the following:

■ Add the Windows-Groups attribute to the default Remote Access policy.
■ Select the group or groups to be granted access.
■ On the policy, select the Grant Remote Access Permission option.

Figure 25-12 shows the progression of a connection attempt with this policy setting.
In a native-mode domain, you can easily reverse the criteria just described and deny access based on group membership. This also requires that all user accounts have the Control Access Through Remote Access Policy option selected in the Dial-In tab of the user account’s Properties dialog box. As in a mixed domain, two policies are needed: one to reject members of a specified group, and another to allow a connection made by anyone else. Follow this procedure to deny access based on group membership:

1. On the default policy, select the Grant Remote Access Permission option.
3. The New Remote Access Policy Wizard starts. Select the option to let the wizard set up a typical policy and give the policy a descriptive name.
4. Choose the access method. In the User Or Group dialog box, select Group and then add the groups to be denied remote access.
5. Accept the default authentication method and default encryption settings unless you have other protocols on your network.

6. Double-click the new policy in the details pane, and select the Deny Remote Access Permission option.

Figure 25-13 shows the logical progression when a connection attempt is made with these settings in effect.

Figure 25-13  Progression of a connection attempt when access is controlled by groups in a native-mode domain
Real World  Windows NT 4 Remote Access in a Windows Server 2003 Domain

A server running Windows NT 4 and either RAS or RRAS can’t authenticate the credentials of domain accounts unless it (the Windows NT server) is also a domain controller. A Windows NT server that is not a domain controller does not have permission to read Active Directory and therefore can validate only local accounts. This same restriction applies when you have a remote access server (running Windows NT, Windows 2000, or Windows Server 2003) in a Windows NT domain that needs to validate user accounts in a trusted Windows 2000 or Windows Server 2003 domain.

The recommended solution is to upgrade the Windows NT 4 server to Windows 2000 or Windows Server 2003. This provides the best functionality and maintains an acceptable level of security.

One alternative is to upgrade the Windows NT server to a domain controller. This exposes the Security Accounts Manager to external attack, and we can no longer recommend this—it’s just too big a security hole. A second solution is to loosen the normal Active Directory security so that the remote access server can read the user account properties. Open a command prompt window on a domain controller and type the following:

```
```

This adds the special identity Everyone to the Pre-Windows 2000 Compatible Access group so that the remote access server can use NT LAN Manager security to read the domain user accounts. This is also an unacceptable weakening of network security, in our opinion. The only viable and secure solution is to upgrade your RRAS servers to Windows Server 2003.

---

Configuring a Remote Access Policy

A remote access policy consists of three elements that make up a rule for analyzing remote connections: the conditions, the profile, and the remote access permission for the policy. The remote access permission was discussed earlier, in the “Understanding the Default Policy” section. Recall that the remote access permission for the policy applies only when an administration-by-policy model is being employed.

Specifying Conditions of Remote Access Policies

When granting or denying access by group membership in the previous sections, you added the Windows-Groups attribute as a condition that users making connection
attempts had to match. (See Figure 25-14.) Table 25-1 describes this and other attributes that can be included in a remote access policy.

![Select Attribute](image)

**Figure 25-14** The remote access attributes that can be added to policies

**Table 25-1** Attributes for remote access policies

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication-Type</td>
<td>Types of authentication for remote access such as Challenge Handshake</td>
</tr>
<tr>
<td></td>
<td>Authentication Protocol (CHAP) and Extensible Authentication Protocol (EAP).</td>
</tr>
<tr>
<td>Called-Station-Id</td>
<td>Phone number of the remote access server. To receive this information, the</td>
</tr>
<tr>
<td></td>
<td>phone line, hardware, and hardware drivers must support the passing of the</td>
</tr>
<tr>
<td></td>
<td>information. Otherwise, the called station ID is set manually for each port.</td>
</tr>
<tr>
<td>Calling-Station-Id</td>
<td>Phone number used by the caller. If you configure a caller ID number for a</td>
</tr>
<tr>
<td></td>
<td>user, the phone system, remote server, and all connecting hardware must</td>
</tr>
<tr>
<td></td>
<td>support the passing of caller ID information. If any link in the connection</td>
</tr>
<tr>
<td></td>
<td>does not support caller ID, the connection attempt is denied.</td>
</tr>
<tr>
<td>Client-Friendly-Name</td>
<td>(IAS server only) Name of the RADIUS client computer that is seeking</td>
</tr>
<tr>
<td></td>
<td>authentication.</td>
</tr>
<tr>
<td>Client-IP-Address</td>
<td>(IAS server only) IP address of the RADIUS client.</td>
</tr>
<tr>
<td>Client-Vendor</td>
<td>(IAS server only) Vendor of the network access server that is a RADIUS</td>
</tr>
<tr>
<td></td>
<td>client. Used to configure different policies for different manufacturers.</td>
</tr>
<tr>
<td>Day-And-Time-Restriction</td>
<td>Days and times allowed for connection attempts.</td>
</tr>
</tbody>
</table>
Configuring Profiles in Remote Access Policies

The profile in a remote access policy is a set of conditions that applies when a connection is authorized. The profile applies whether the condition has been authorized by permission in the user account or by permission in the policy. To see the profile that applies to a policy, double-click the policy in the Routing and Remote Access details pane and click Edit Profile. The Edit Dial-In Profile dialog box has six tabs that can be configured (as shown in Figure 25-15). Each tab is discussed in the sections that follow.

![Figure 25-15 Settings in the remote access policy profile](image)

### Table 25-1 Attributes for remote access policies

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Framed-Protocol</td>
<td>Protocol such as PPP, SLIP, Frame Relay, or X.25 to be used for framing incoming packets.</td>
</tr>
<tr>
<td>NAS-Identifier</td>
<td>(IAS server only) String to identify the originating network access server (NAS).</td>
</tr>
<tr>
<td>NAS-IP-Address</td>
<td>(IAS server only) IP address of the originating NAS.</td>
</tr>
<tr>
<td>NAS-Port-Type</td>
<td>Medium used by the originating caller. Examples are analog telephone and ISDN lines.</td>
</tr>
<tr>
<td>Service-Type</td>
<td>Type of service the caller requests. Examples are framed (PPP) and login (Telnet).</td>
</tr>
<tr>
<td>Tunnel-Type</td>
<td>Tunneling protocols to be used. Examples are PPTP and L2TP.</td>
</tr>
<tr>
<td>Windows-Groups</td>
<td>Groups that the caller is a member of.</td>
</tr>
</tbody>
</table>
Specifying Dial-In Constraints
In the Dial-In Constraints tab, you can set the following limitations on the dial-in connection:

- **Minutes Server Can Remain Idle**  The time after which an idle connection is terminated. By default, no connection is automatically terminated when idle.

- **Minutes Client Can Be Connected**  The time after which a connection is disconnected. By default, there is no time limit on connections.

- **Allow Access Only On These Days And At These Times**  The days and hours when a connection is allowed. This check box is cleared by default. The remote access server will not disconnect a connection that is active at a time when connection attempts aren’t allowed.

- **Allow Access Only To This Number**  The specific number that a user must call for a connection to be allowed.

- **Allow Access Only Through These Media**  The type of connection the caller must be using, such as ISDN, T1, or ADSL. If the medium specified doesn’t match the medium being used, the call is rejected.

Specifying IP Address Policies
The IP tab defines the IP address policies for the profile:

- **IP Address Assignment**  By default, the server supplies an IP address for the connection, but you can specify that the server must supply an address or that the client can request an IP address.

- **IP Filters**  This policy specifies the types of packets that are allowed (or not allowed) in the traffic to the client, from the client, or both. Packet filtering can be based on such things as the source and destination IP addresses, protocol type, source or destination port, and so forth.

Enabling Multilink and the Bandwidth Allocation Protocol
In the Multilink tab, you can choose settings to enable Multilink and the Bandwidth Allocation Protocol (BAP). The server must have Multilink and BAP enabled for these settings to be enforced in the profile. Enabling Multilink allows clients to combine multiple physical connections into a single logical connection. If you enable Multilink, you should also enable BAP so that links can be dynamically added or dropped as needed. (Multilink has no mechanism for adapting to changing bandwidth needs.) In the Multilink tab, choose from the following options:

- **Multilink Settings**  Disable Multilink completely, or set the maximum number of ports that a connection can use. The default is the server’s setting.
Bandwidth Allocation Protocol Settings. These settings cause a Multilink connection to be reduced automatically if the lines fall below a specified capacity for a specified length of time.

Specifying Authentication Methods
In the Authentication tab, you set the authentication methods that are allowed for the connection. The same authentication methods must be enabled on the remote access server for the properties of the profile to be enforced.

Specifying an Encryption Method
The Encryption tab lets you set the encryption properties for this profile. The settings are as follows:

- **No Encryption**  Allows a nonencrypted connection. To require encryption, clear this check box.
- **Basic**  Uses Microsoft Point-to-Point Encryption (MPPE) with a 40-bit key for dial-up and PPTP connections. For L2TP over an IPSec-based VPN, uses 56-bit Data Encryption Standard (DES) encryption.
- **Strong**  Uses MPPE with a 56-bit key for dial-up and PPTP connections. For L2TP over an IPSec-based VPN, uses 56-bit DES encryption.
- **Strongest**  Uses MPPE with a 128-bit key for dial-up and PPTP connections.

Setting Advanced Attributes
In the Advanced tab, you can set RADIUS attributes that are sent to the RADIUS client by the IAS server. These attributes are specific to RADIUS authentication and are ignored by the remote access server.

Configuring a Remote Access Server
Some profile settings described in the previous section must have corresponding entries on the remote access server. This section covers those settings as well as other specific configurations that can be performed on a server. To make configuration changes to a remote access server, open Routing And Remote Access, right-click the server name in the console tree, and choose Properties from the shortcut menu. The various settings available in the Properties dialog box are as follows:

- **Router or Remote Access Server**  The General tab has options for adding the role of router to the remote access server, or to completely change the role of the computer from remote access server to router.
- **Authentication Settings**  To access the authentication settings, click the Security tab in the server's Properties dialog box, and then click Authentication Methods.
default, the Extensible Authentication Protocol (EAP) and Microsoft Challenge Handshake Authentication Protocols (MS-CHAP and MS-CHAP v2) are selected.

- **IP Routing And Assignment** The IP tab of the server’s Properties dialog box gives access to the IP parameters. By default, the profiles in remote access policies use the server’s settings for IP addresses. In turn, the server defaults to allowing IP routing and to assignment of IP addresses using DHCP. If you need to use a static address pool, choose that option and provide a range of addresses to be assigned to connections.

- **Multilink And The BAP** Click the PPP tab to access the options for enabling Multilink and the BAP. See the section “Enabling Multilink and the Bandwidth Allocation Protocol,” earlier in this chapter, for more information.

- **Other Protocols** In the PPP tab, click Software Compression to enable (or remove) support for the Microsoft Point-to-Point Compression (MPPC) protocol. You can also select the Link Control Protocol (LCP) Extensions to PPP.

- **Logging** Click the Logging tab to define the kind of logging you want. The default is to log errors and warnings, which is ideal, especially in the early days after setting up RRAS.

More Info For more information about the MPPC protocol, see RFC 2118, “Microsoft Point-to-Point Compression Protocol.” See RFC 1570, “PPP LCP Extensions,” for more about the LCP extensions.

---

### Configuring a Virtual Private Network

The uses and types of VPNs were described earlier in this chapter and in some detail in Chapter 21. This section outlines the steps involved in configuring and using a VPN for PPTP connections across the Internet.

### Configuring the Internet Connection

Your connection to the Internet will be over a dedicated line of some sort—most typically T1, Fractional T1, or DSL. You’ll need to be sure that the WAN adapter is in the Windows Catalog. The WAN adapter includes drivers that are installed in the operating system, allowing the WAN adapter to appear as a network adapter. The WAN adapter is configured with the IP address and subnet mask assigned for your domain or supplied by an ISP, as well as with the default gateway of the ISP router.

Another configuration that is commonly used has a router that does the actual WAN connection, and your server’s connection is a simple NIC that connects to the router. Configuration of WAN details is then managed on the router, and will vary by router manufacturer. At the RRAS server, you need to set an IP address that is on the same
subnet as the LAN side of the router, and set your default gateway to the IP address of the LAN port on the router.

**Configuring the Remote Access Server as a Router**

For the remote access server to forward traffic properly inside your network, you must configure it as a router with either static routes or routing protocols, so that all the locations of the intranet are reachable from the remote access server.

To configure the server as a router, open Routing And Remote Access, right-click the server name, and choose Properties from the shortcut menu. In the General tab, select the Router option. Then indicate whether you want the router to handle LAN routing only or LAN and demand-dial routing. Click OK to close the Properties dialog box.

**Configuring PPTP Ports**

You must confirm that you have the number of PPTP ports you need. To verify the number of ports or to add more, follow these steps:

1. Launch Routing And Remote Access from the Administrative Tools folder.
2. In the console tree, click the appropriate server, and then right-click Ports and choose Properties from the shortcut menu.
3. In the Ports Properties dialog box (shown in Figure 25-16), select WAN Miniport (PPTP), and click Configure.

![Figure 25-16 Configuring PPTP ports for routing](image)
4. In the Configure Device dialog box, you can set a maximum number of ports for the device and specify whether the device is to be used for incoming connections only or for both incoming and outgoing connections.

5. Click OK when you’re finished.

**Configuring PPTP Filters**

Most networks need to filter packets based on their incoming or outgoing addresses. To set the PPTP filters, follow these steps:

1. Launch Routing and Remote Access from the Administrative Tools folder.
2. In the console tree, expand the appropriate server, then IP Routing, and then General.
3. In the details pane, right-click the interface to be filtered, and choose Properties from the shortcut menu.
4. Click either Input Filters or Output Filters, and supply the source, destination, and/or protocol to be filtered. (The last step in configuring a VPN is to set up remote access policies, as described earlier in this chapter.)

---

**Important** Filtering can be a tricky business, so proceed with caution. It’s all too easy to filter too much or too little. Consult the online Help files of Windows Server 2003 for additional information, or consider installing a stateful firewall such as Microsoft ISA Server 2004.

---

**Elements of a Router-to-Router VPN Connection**

A router-to-router VPN is typically used to connect remote offices over a permanent link such as a dedicated T1 line. However, a router-to-router VPN can also be configured to be available on demand, which means that the connection is made only when needed. This section describes the components of a Windows Server 2003 router-to-router VPN connection.

**VPN Clients**

The client is the calling router that initiates the VPN connection. For router-to-router connections, you can use computers running Windows Server 2003, Windows 2000 Server, or Windows NT Server 4 with RRAS as VPN clients.

**VPN Servers**

The VPN server is the answering router that accepts the connection from the calling router. Computers running Windows Server 2003, Windows 2000 Server, or Windows NT Server 4 with RRAS can be set up as VPN servers.
LAN and Remote Access Protocols
LAN protocols such as TCP/IP and IPX are used to transport information. Windows Server 2003 supports the routing of LAN protocol packets by using the PPP remote access protocol in a router-to-router VPN connection.

Tunneling Protocols
Tunneling protocols encapsulate one network protocol inside another. VPN clients and VPN servers use tunneling protocols to manage tunnels and send tunneled data. PPTP and L2TP are supported by Windows Server 2003, Windows XP Professional, and Windows 2000. Windows NT 4, Windows Me, and Windows 98 support only PPTP. However, with the Microsoft L2TP/IPSec VPN client installed, Windows Me, Windows 98, Windows NT 4 Workstation, and Windows 95 will all support L2TP.

Note
The Microsoft L2TP/IPSec VPN client can be downloaded from the Microsoft Download Center at http://www.microsoft.com/downloads.

Demand-Dial Interfaces
Before configuring the demand-dial interface, decide whether both ends of the connection will be able to initiate calls. For two-way connections (either router can initiate calls), both routers have to be configured with authentication credentials (such as a user account). Both must also have a PPTP port (for a PPTP-based VPN connection) or an L2TP port (for an L2TP-based connection).

If one router always initiates the connection, the setup of the calling router is the same as for a two-way connection. On the receiving router, it’s necessary to create a user account that the calling router uses when calling, and configure static routes on that user account. To set up a demand-dial interface, see the “Adding a Demand-Dial Interface” section later in this chapter.

User Accounts
The calling router needs a user account with dial-in permissions either through the user account or through remote access policies.

Static Routes or Routing Protocols
To be able to forward packets across the router-to-router VPN connection, each router has to have the appropriate routes in the routing tables. Routes are added to the routing tables of both routers either as static routes or by enabling a routing protocol to operate across a persistent router-to-router VPN connection. Static routing is best for a small, single-path internetwork. The “Setting Up Static Routes and Routing Protocols” section later in this chapter, describes how to add routes to the routing tables.
Security Options
Because a Windows Server 2003 remote access router validates the router-to-router VPN connection, you can use all the security features of Windows Server 2003 remote access, including data encryption, RADIUS, smart cards, and callback. See Chapter 21 for more on security considerations.

Adding a Demand-Dial Interface
To add a demand-dial interface to a router, follow these steps:

1. Launch Routing and Remote Access from the Administrative Tools folder.
2. In the console tree, click the appropriate router.
3. Right-click Network Interfaces. Choose New Demand-Dial Interface from the shortcut menu to start the Demand Dial Interface Wizard. Click Next.
4. Enter a name for the demand-dial interface. Use a name that will help you recall the connection being made, such as the name of the branch office or network to which you’re connecting. Click Next.
5. Choose a connection type:
   - If you’re not using VPN on this interface, select the Connect Using A Modem, ISDN Adapter, Or Other Physical Device option, and click Next.
   - Specify the modem and then enter the phone number to be called. In addition to the primary number, you can click Alternates and specify additional numbers to be tried automatically if the primary number can’t be reached.
   - If you select Connect Using Virtual Private Networking (VPN), click Next to open the VPN Type page. Choose the tunneling protocol appropriate for your needs. Click Next.
   - In the Destination Address page, provide either the host name or the IP address for the remote router. Click Next.
6. Under Protocols And Security, select all the conditions that apply to the connection. If you select either the Add A User Account So A Remote Router Can Dial In option or the Use Scripting To Complete The Connection With The Remote Router option (this second option is not a valid option for the VPN interface type) or if you select both options, the wizard presents a page to configure each of the items.
7. Supply the IP address of the network or networks that you want to access.
8. Supply the Dial Out Credentials requested, including the user account name and password.
9. When you're finished, the new interface is added to the routing interfaces in Routing and Remote Access. Right-click the name of the interface, and choose Properties to change or add to the configuration.

**Setting Up Static Routes and Routing Protocols**

As mentioned earlier, for routers to be able to forward packets across the router-to-router VPN connection, each router has to have the appropriate routes in the routing table. Routes can be added as static routes to the routing tables of both routers. To add a static route to the routing table, follow these steps:

1. Launch Routing And Remote Access from the Administrative Tools folder.
2. Click the appropriate router, and then click IP Routing.
3. Right-click Static Routes, and choose New Static Route from the shortcut menu. (You can also view the existing IP routing table from this menu.)
4. In the Static Route dialog box, select the interface and supply the IP address for the destination router.

The route must also be configured on the corresponding router at the other end of the VPN. For a persistent connection, you can add a routing protocol instead of a static route. To do so, right-click General under IP Routing and choose New Routing Protocol from the shortcut menu.

**Using the Internet Authentication Service**

The IAS is the central component in Windows Server 2003 for authenticating, authorizing, and auditing users who connect to a network through a VPN or dial-up access. The IAS server is Microsoft’s implementation of a RADIUS server and proxy. RADIUS is the authentication protocol most commonly used by ISPs. IAS uses data stored on a domain controller to verify the authentication requests received through the RADIUS protocol. When the RADIUS server is part of an Active Directory domain, the server uses the directory service as its user account database. With access to user accounts, the RADIUS server authenticates and authorizes connections.

---

**Note** IAS can be configured for wireless, dial-up, VPN, Internet, or extranet access.

IAS uses the authentication protocols within PPP to authenticate users. These include Challenge Handshake Authentication Protocol (CHAP) and its Windows-specific variant, Microsoft-Challenge Handshake Authentication Protocol (MS-CHAP, and MS-CHAP v2).
Other methods of authentication include Extensible Authentication Protocol (EAP) for smart cards, certificates, and one-time passwords. Other methods are also supported, based on the telephone number that the user calls or calls from, although these methods are inherently less secure.

**Best Practices** Always install and test your remote access servers using local authentication methods before configuring them to use IAS for authentication. This will ensure that RRAS is working correctly and simplify troubleshooting any connection issues.

---

### Installing and Configuring IAS

To use IAS for dial-up or VPN connections, you must perform several tasks, including installing IAS, configuring clients and servers, and setting remote access policy. This section describes each of these tasks in turn.

#### Installing IAS

The first step is to install IAS on the primary and backup remote servers. You might need the Windows Server 2003 installation CD-ROM. To install IAS, follow these steps:

1. On the remote server, open Control Panel.
2. Open Add/Remov e Programs, and click Add/Remove Windows Components.
3. In the Windows Components Wizard, select Networking Services and click Details.
4. Select Internet Authentication Service. Click OK to close the Details dialog box.
5. Click Next, and IAS is installed.

#### Configuring IAS

The default IAS configuration is correct in most cases. If your remote access scenario is very complex, you might need to change the configuration. To check the configuration, follow these steps:

1. Launch Internet Authentication Service from the Administrative Tools folder.
2. In the console tree, right-click Internet Authentication Service and choose Properties from the shortcut menu.
3. In the Service tab, you can change the description or the event logging options.
4. Click the Ports tab to view the default User Datagram Protocol (UDP) ports. If your RADIUS authentication and accounting ports differ, make the changes here.
Note  Port 1812 for authentication and port 1813 for accounting are standard RADIUS ports. However, many access servers use 1645 for authentication and 1646 for accounting. It’s not important which ones you use, but you must be sure that IAS and your access server are using the same ports.

5. Click OK when you’re finished.

**Configuring Clients for IAS**

The next step is to add the network access servers (NASs) and, if you’re using a VPN, the PPTP servers as clients on the primary IAS server. To add clients, follow these steps:

1. Launch Internet Authentication Service from the Administrative Tools folder.
2. In the console tree, right-click RADIUS Clients and choose New RADIUS Client from the shortcut menu.
3. Supply a friendly name for the client and the client address. Click Next.
4. Specify the vendor of the RADIUS client, if necessary, and type a shared secret. At this point, you can add to security by selecting the Request Must Contain Message Authenticator Attribute option. (See the “Under the Hood: How RADIUS Works” sidebar.)
5. Click Finish when you’re done.

A shared secret is a password used between an IAS server and other servers connected to it. The shared secret must be the same on both machines and must follow general password rules—it’s case sensitive, can contain alphanumeric and special characters, and can be up to 255 characters long. Because shared secrets are embedded in the software and you don’t have to type them in all the time as you do passwords, you can easily make them quite long. Longer shared secrets are more secure than short ones.

---

**Under the Hood  How RADIUS Works**

RADIUS authenticates users through a series of communications between the client and the server. Once a user is authenticated, the client provides that user with access to the appropriate network services.

Using a modem, the user dials in to a modem connected to an IAS server. The message must originate from one of the IP addresses you configured for clients or the message is discarded. To prevent unauthorized access from a spoofed IP address, select the Request Must Contain Message Authenticator Attribute option when configuring the client. This will cause encryption of the message using the shared secret as the key.
Next, the server prompts the user for a name and password. The server creates a data packet—the authentication request—from this information. The packet includes information identifying the specific server sending the authentication request, the port that is being used for the modem connection, and the user name and password.

The authentication request is sent over the network from the RADIUS client to the RADIUS server. If the RADIUS server cannot be reached, the RADIUS client can route the request to an alternate server. When an authentication request is received, the authentication server validates the request and then decrypts the data packet to access the user name and password information. This information is passed to the appropriate security system (Kerberos version 5 in Windows Server 2003).

If the user name and password are correct, the server sends an authentication acknowledgment that includes information regarding the user’s network system and service requirements. If at any point in this logon process conditions are not met, the RADIUS server sends an Authentication Reject to the server and the user is denied access to the network.

---

**Using RADIUS for Multiple Remote Access Servers**

When you have more than one remote access server, the administration of remote access policies can become cumbersome very quickly. Instead, you can configure a single computer running Windows Server 2003 and IAS as a RADIUS server and configure the remote access servers as RADIUS clients. The IAS server provides centralized remote access authentication, authorization, accounting, and auditing. Assuming that you’ve already configured the remote access servers to provide access for dial-up or VPN clients, you can accomplish this by performing the procedures listed next. Each of these procedures is described in the sections that follow:

- Configure the remote access servers for RADIUS authentication.
- Configure the remote access servers for RADIUS accounting.
- Configure the IAS server.

**Note** To provide redundancy and fault tolerance, configure a primary and secondary IAS server, and copy the remote access policies from the primary server to the secondary one. Then configure each remote access server with two RADIUS servers that correspond to the two IAS servers. If the primary IAS server becomes unavailable, the remote access servers will automatically fail over to the secondary IAS server.
Configuring a Remote Server for RADIUS Authentication

When you configure the properties of a remote access server running Windows Server 2003, you need to select RADIUS as the authentication provider. To change a server to RADIUS authentication, follow these steps:

1. Right-click the server name in Routing and Remote Access, and choose Properties from the shortcut menu.
2. Click the Security tab. Under Authentication Provider, select RADIUS Authentication, and then click Configure.
3. Click Add. Provide the server name—the host name or IP address of the IAS server. If you already have IAS installed, you do not need to change the shared secret. Otherwise, you need to change it. The remote access server running Windows Server 2003 and the IAS server share a secret that is used to encrypt messages sent between them. The two servers must share the same secret.
4. Click OK when you’re finished.

Note The remote access server sends its authentication requests to the UDP port on which the IAS server listens. The default value of 1812 is based on RFC 2138, “Remote Authentication Dial-in User Service (RADIUS),” and does not need to be changed when you’re using an IAS server.

Configuring the Remote Server for RADIUS Accounting

When you configure the properties of a remote access server running Windows Server 2003, you need to select RADIUS accounting as the accounting provider.

To change a server to RADIUS accounting, follow these steps:

1. Right-click the server name in Routing and Remote Access, and choose Properties from the shortcut menu.
2. Click the Security tab. Under Accounting Provider, select RADIUS Accounting, and then click Configure.
3. Provide the server name—the host name or IP address of the IAS server.
4. If you already have IAS installed, you do not need to change the shared secret. Otherwise, you need to change it. Note that the remote access server running Windows Server 2003 and the IAS server share a secret that is used to encrypt messages sent between them. Both the remote access server and the IAS server must share the same secret. Click OK.
Configuring the IAS Server for RADIUS

You need to register each of the remote access servers as clients on the IAS server. Once the remote access servers are configured to use RADIUS authentication, only the remote access policies stored on the IAS server are used. Therefore, if one of the remote access servers contains the remote access policies that are applied to all the remote access servers, you need to copy the remote access policies to the IAS server. To copy the policies from a remote server to the IAS server, open a command window and type netsh aaaa show config <path\file>.txt. The path can be a relative path, an absolute path, or a Universal Naming Convention (UNC) path. This command creates a text file that includes all the configuration settings.

Copy the text file to the destination IAS server, and open a command prompt on the destination machine. Type netsh exec <path\file>.txt. A message appears telling you whether the update was successful. This procedure does not work unless both the source and destination computers are running the same version of Windows Server 2003.

Using the RADIUS Proxy

New in IAS for Windows Server 2003 is the ability of IAS to act as a RADIUS proxy. A RADIUS proxy server passes messages between two different account databases. You would use IAS as a RADIUS proxy if you wanted to provide authentication and authorization for user accounts that are not members of the same domain as the IAS server or members of a trusted domain. Use the RADIUS proxy if you need to authenticate using a non-Windows database such as a SQL Server or Novell Directory Services database.

To authenticate and authorize messages between two databases, you need a primary and secondary IAS server for each database. After IAS is installed and configured on domain controllers, add the RADIUS clients.

The next step is to create a connection request policy, which is easily done by following these steps:

1. Launch Internet Authentication Service.
2. Double-click Connection Request Processing, right-click Connection Request Policies, and select New Connection Request Policy from the shortcut menu to launch the wizard. Click Next.
3. In the Policy Configuration dialog box, provide a descriptive name for the policy. Click Next.
4. Select Forward Connection Requests To A Remote RADIUS Server For Authentication.
5. Supply a realm name. Click New Group to define the destination for connection requests.

6. The New Remote RADIUS Server Group Wizard starts. Provide the group name and then the names of the servers and the shared secret.

7. Click Next and then click Finish to complete the policy.

**Note** A *realm* is a security authentication device used by Kerberos version 5. The uses of realms are spelled out in RFC 1510, “The Kerberos Network Authentication Service (V5).”

Next you need to configure the secondary IAS proxy. First, install IAS on another domain controller. Then copy the primary IAS proxy configuration into a text file using the methods described in the earlier section, “Configuring the IAS Server for RADIUS.”

As a final step, configure RADIUS authentication and accounting on the access servers, a procedure described in the previous sections “Configuring a Remote Server for RADIUS Authentication” and “Configuring the Remote Server for RADIUS Accounting.”

**More Info** For the many permutations of IAS as a RADIUS proxy, see the Windows Server 2003 Help and Support Center.

---

**Summary**

Consistent and reliable remote access is a necessity for many, if not most, organizations today. Windows Server 2003 includes tools for setting up access ranging from a simple dial-in connection to multiple remote access servers running virtual private networks. In the next chapter, we move on to a new section of the book, which deals with implementing wireless security.
Chapter 26
Implementing Wireless Security

Understanding 802.11 Protocols ........................................ 867
Encryption and Authentication ........................................... 868
Deployment Scenarios .................................................... 872
Summary ........................................................................... 875

Many IT professionals approach wireless devices and wireless security with a good deal of fear and loathing, primarily because they’ve “heard” that wireless is inherently insecure and unsafe. Well, it isn’t. Yes, wireless security requires attention and understanding, and careful implementation. But it isn’t something you need to fear.

For those who doubt that wireless networks can be secure, consider Microsoft Corporation. Microsoft is one of the most visible targets for those who would like to prove something by compromising the security of a wireless network. And everywhere on the Microsoft campus wireless networking is available. Clearly secure wireless is possible. In this chapter, we’ll try to provide you with the basics for setting up a wireless network that meets your security requirements.


Real World  Security Is Relative

Security is a relative term. If your wireless access point is not turned on and is stored in a bank vault with no connection to the outside world, it’s fairly secure but hardly useful for day-to-day operations. As soon as you power it up and connect it to anything else, your level of security goes down.
How secure you need to be depends on two factors:

- **Your risk assessment** You must determine how much your network is at risk.
- **Your risk tolerance** You must determine how much you care if someone is listening to your network.

By carefully assessing these two factors on your wireless network, you can gauge how much effort and expense you need to put into security.

**Risk Assessment**

To properly assess risks on your wireless network, you should examine three factors:

- **Density** How many potential intruders are in the immediate area of your wireless network?
- **Isolation** How far beyond the perimeter of the area you control does your wireless signal reach?
- **Profile** How attractive a target is your wireless network?

Density is fairly straightforward. A wireless network in downtown Toronto, Canada, is in an area of greater density than one in the Denali National Park in Alaska, United States. This doesn’t mean that you shouldn’t pay attention to security if your wireless network is in a small town—after all, it takes only one intruder with ill intent and access to your network to cause problems.

Isolation does not refer to isolation from potential intruders. Instead, it is an estimate of the likelihood of someone getting within range of your signal without you being aware of it. If you’re in a city of high-rise buildings and your signal could be detected from the next building over (highly likely), you need to be more concerned than if your access point is inside your campus where access to the grounds is limited by a secured gate.

Finally your profile matters. Microsoft is a much more interesting target than a local business with a dozen employees and no sensitive information or significant assets (for example, defense contracts, credit card information, and so forth).

**Risk Tolerance**

Risk tolerance is your assessment of how much it matters if someone does, accidentally or intentionally, gain access to your wireless network. If you are using your wireless network to carry sensitive and critical information, your risk tolerance is lower than if you use your wireless network to provide convenient access to publicly available information or resources.
Understanding 802.11 Protocols

Wireless networking is based on a set of standards and protocols known as the Institute of Electrical and Electronics Engineers (IEEE) 802.11 protocols. The original Wireless Local Area Network (WLAN) specification is 802.11, with subsidiary specifications that describe particular implementations or features that can be part of the overall 802.11 solution. The specifications in general use at this point include: 802.11a, 802.11b, and 802.11g, each of which describes an overall speed and frequency of connection; 802.11i, which describes security specifications for WLAN networking; and 802.11h, which extends the 802.11a specification to allow its use in Europe.

802.11

IEEE 802.11 was the initial shared WLAN standard. It used the carrier sense multiple access with collision avoidance (CSMA/CA) media access control (MAC) method. The standard allows either direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) transmissions at the physical layer. The specification defines data rates of 1 Mbps and 2 Mbps at a radio frequency of 2.45 gigahertz (GHz). While technically still in effect, this standard has been supplanted by later specifications.

802.11a

802.11a, adopted in 1999, defines a data transmission rate as high as 54 Mbps at a radio frequency of 5.8 GHz. Instead of DSSS and Complementary Code Keying (CCK), which the earlier 802.11b uses, 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM). OFDM allows data to be transmitted by subfrequencies in parallel, providing greater resistance to interference and improved throughput. 802.11a operates on a different frequency from microwave ovens, most wireless home phones, and Bluetooth, thus enabling both a higher data rate and a cleaner signal.

802.11b

The 802.11b specification, adopted in 1999, was the first major enhancement to the original 802.11 specification. It standardizes the physical layer to DSSS to support higher bandwidth than the original 802.11, enabling additional speeds of 5.5 Mbps and 11 Mbps. The frequency range is the same, at 2.4 to 2.5 GHz, with a different modulation scheme, CCK, at the higher data rates of 5 Mbps and 11 Mbps.

802.11g

The 802.11g standard, adopted in 2003, uses the same radio frequency range as 802.11b, 2.4 to 2.5 GHz, with a maximum data transmission rate of 54 Mbps. The 802.11g standard uses Orthogonal Frequency Division Multiplexing (OFDM) and Packet Binary
Convolution Coding (PBCC) for the higher speeds, but the standard requires backward compatibility with the 802.11b standard. Mixed networks with both 802.11b and 802.11g will run at the slower 802.11b speed.

802.11h

The 802.11h standard, adopted in 2004, operates at the same frequency as the 802.11a standard, but it extends 802.11a to prevent interference with existing devices in Europe.

802.11i

The 802.11i standard, adopted in 2004, extends and defines the security parameters for wireless devices. The original wireless standards used Wired Equivalent Privacy (WEP) for encryption. WEP has, however, proven inadequate and flawed. An interim standard, Wi-Fi Protected Access (WPA), was developed that provided increased security. WPA is incorporated as a subset of 802.11i. The IEEE 802.1X Authentication Protocol is also an element of 802.11i. Older hardware will probably not be able to fully conform to 802.11i because of the use of the Advanced Encryption Standard (AES), but many existing devices can support WPA.

802.11e

The IEEE 802.11e standard, finalized in July of 2005, defines Quality of Service (QoS) standards for wireless networks, enabling high-bandwidth and low-latency applications such as Voice over IP (VoIP) and multimedia streaming on a wireless network.

802.11n

The IEEE 802.11n standard, still in its early stages, will define the protocols to be used for wireless speeds greater than 100 Mbps. There are still several different technologies that are competing for inclusion in the final specification.

Encryption and Authentication

Because the radio signal that a wireless network uses is freely available to anyone within range of the signal, it is necessary to encrypt the signal to prevent unauthorized viewing of the contents of the packets being transmitted. Further, it is important to authenticate that the packets are coming from a known source to prevent “man in the middle” attacks against the encryption.

The use of WPA or full 802.11i, also referred to as WPA2, provides sufficient encryption and, when combined with 802.1X, authentication can provide the basis for a highly secure wireless network. Additional steps, such as two-factor authentication and VLAN segmentation
can be incorporated to increase the level of security. The use of 802.1X requires a Remote Authentication Dial-In User Service (RADIUS) server, such as the Internet Authentication Service (IAS) running on Windows Server 2003. IAS was covered in Chapter 25.

Under the Hood  Why WEP Isn’t Good Enough

The original encryption technology that was intended to provide security for wireless transmissions was Wired Equivalent Privacy (WEP). WEP has two levels of encryption: 40 bit (sometimes referred to as 64 bit), and 104 bit (sometimes referred to as 128 bit). As the name implies, the intent of WEP was to provide a level of wireless network security that was equivalent to a typical wired Ethernet network. Unfortunately, the encryption algorithm for WEP has been proven to be flawed and subject to a number of different attack vectors. The weakness of WEP is described well in the paper “Weaknesses in the Key Scheduling Algorithm of RC4” by Fluher, Mantin and Shamir. (The paper is available at http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf.)

Since the presentation of the paper in 2001, a number of freely available software programs have been developed that will crack a WEP-protected network in a very short amount of time if additional security measures aren’t taken to supplement WEP, such as 802.1X and two-factor authentication. A network protected by WEP alone should be assumed to be freely available to anyone who wants to read every packet that travels on it.

WPA and WPA2

Because of the problems with the original WEP encryption algorithm and the time it takes to get a full IEEE standard adopted and agreed on, the Wi-Fi Alliance adopted an interim standard called Wi-Fi Protected Access (WPA). WPA increases security on three fronts: data encryption, data integrity, and user authentication.

The WPA standard has been absorbed into the 802.11i standard, but at the time of this writing, the products generally available on the market are a mix of those that implement the full 802.11i standard and those that only meet WPA certification.

Note Products that are certified to support 802.11i are designated “WPA2” by the Wi-Fi Alliance.

Data Encryption

WPA replaces the flawed encryption algorithm of WEP with either Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES). TKIP changes the encryption
key for each frame, but it can still run on existing hardware, while AES will likely require a
new generation of hardware from wireless vendors.

Data Integrity
The original WEP standard had only a weak check for packet integrity—that is, there was
no assurance that the packet you received was actually the packet that was sent, making
WEP vulnerable to “Man in the Middle” attacks. WPA adds a Message Integrity Check
(MIC), using the method known as “Michael.” This MIC ensures that the packet received
is the same as the packet sent. Additionally, Michael helps prevent replay attacks.

More Info
For more on MIC and other features of WPA, you can find a useful

User Authentication
WPA supports the use of a RADIUS server for user authentication. In environments with-
out a RADIUS server, WPA uses a pre-shared key for initial authentication of clients.

WPA2
The WPA2 is a product certification signifying that a specific product meets the 802.11i
standard. It replaces the encryption scheme (RC4) that was the basis of the WEP prob-
lems with a new and much more secure encryption scheme: Advanced Encryption Stan-
dard (AES). The AES used in WPA2 and 802.11i is the Counter Mode Cipher Block
Chaining-Message Authentication Code (CBC-MAC) protocol (CCMP).

More Info
For more information on WPA2, 802.11i, and AES an excellent starting
point is the Cable Guy article on Microsoft’s TechNet site: http://www.microsoft.com/
 technet/community/columns/cableguy/cg0805.mspx.

Real World  Wireless Security Strategies
A variety of security strategies for wireless networking have been suggested and
used over the years—some useful, and some not. Here’s our evaluation of several of
them:

MAC Address Filtering  Only a statically managed list of MAC addresses is
allowed access to the wireless network. It’s a nice idea, but this strategy can be
easily defeated with a sniffer—MAC addresses can be easily spoofed. Plus, a
static list of “allowed” MAC addresses is a hopeless mess to manually main-
tain. All in all, it’s a complete waste of time.
• **SSID Hiding**  This strategy requires that the client know the name of the wireless network to be able to connect to it. Even if the network is known and configured into the Windows client, that client must continually probe to make sure that the network is present. This requirement causes all sorts of problems and limits the ability of Microsoft Windows to manage connections. And the strategy is totally useless because anyone with access to the packets in the air can read the SSID from the commonly sent 802.11 management frames in a matter of seconds. Whereas broadcasting the SSID, when combined with appropriate security, makes the network easier to manage, and easier for users as well. Hiding the SSID is another complete waste of time.

• **WEP Encryption**  The original encryption standard for wireless, this standard uses either a 40-bit or 104-bit key (along with a fixed 24-bit initialization vector). It is easily hacked by anyone with ill intent and will keep only the most casually curious out of your network. WEP keys are static keys and must be manually maintained. Every time a user who had wireless access leaves the organization, the WEP keys need to be changed. A network protected with WEP alone should be considered completely unsecured.

• **WPA**  The WPA encryption standard is based on RC4, which can be compromised. However, because it changes keys with sufficient frequency and derives the new keys in an improved way as compared to WEP, it is generally considered secure. With 802.1X authentication and the appropriate authentication method, the initial encryption keys are automatically generated. Pre-shared key authentication generates new initial encryption keys for each authentication. Configuration of WPA preshared keys is simplified in Windows XP SP2 with the Wireless Network Setup Wizard. If your wireless hardware doesn’t support at least WPA, don’t let it inside your network.

• **WPA2**  The WPA2 encryption is based on AES and is much more secure than RC4, while the WPA2 standard incorporates additional security measures beyond just encryption. Both preshared key and RADIUS authentication scenarios are supported. All new wireless hardware you buy should support WPA2.

• **IEEE 802.11i**  This is the underlying standard for WPA2, which is described in the preceding bullet point.

• **VPNs**  One solution to setting up secure wireless networks is to place the network outside your main network and use a virtual private network (VPN) connection to the main network. This approach has the advantage of getting around the insecurities of older equipment, but has inherent problems. If the external access point is open and unsecured, it leaves the client exposed to
any other computer in range. It also imposes a performance hit and requires a VPN connection for every client. Machine group policies are not applied, and the overall reliability of the connection and the administrative overhead are significant issues as well. However, even with its problems, this can be a viable temporary solution where new equipment isn’t in the budget and a limited number of clients need to be supported.

- **IEEE 802.1X** Using 802.1X as the authentication mechanism for WPA or WPA2 encryption is an excellent solution for large organizations with RADIUS servers.

## Deployment Scenarios

The choice of how you deploy and secure wireless networking depends on a combination of factors, including your overall risk assessment, risk tolerance, and infrastructure. If you’re already using RADIUS servers and 802.1X, the choice of how to set up your wireless network is straightforward and simple—use the existing RADIUS servers to provide 802.1X authentication, and use the highest encryption that your hardware will support. In environments that don’t have an in-place RADIUS infrastructure, the choice of deployment will depend on whether your infrastructure can support the addition of RADIUS to the environment.

### Enterprise Deployment with 802.1X

To deploy wireless devices in the enterprise, you need to address three areas: external or guest clients, internal or managed clients, and rogue or unauthorized wireless networks.

#### Guest Access

Many organizations find it necessary and desirable to provide connectivity to clients, customers, and visitors who are not part of their managed network—for example, a visiting consultant who needs access to e-mail, or business partners or customers who need to access their own network. With the pervasiveness of wireless technology in mobile devices and laptop computers, one of the easiest ways to provide this connectivity is with a wireless network that sits outside the company’s firewall. It need not, and should not, have any connection to the internal network that isn’t through that firewall. To the internal network, it appears as any other Internet connection.

When setting up a guest access wireless environment, you should keep it focused in “public” areas of the company. You do not want the public wireless connection to become a bypass point that allows internal users to bypass the corporate firewall and corporate policies on acceptable use.
**Important** Be careful with providing external wireless networks for guest access—malicious users might leverage such a network to launch a DoS attack against another company’s network and you might be legally liable as a result!

### Managed Clients

Your internal wireless clients should use both authentication via 802.1X and a minimum of WPA encryption. Using 802.1X will ensure that only known wireless clients have access to your internal network. In environments where there is already a public-key infrastructure (PKI) in place, or where the resources exist to deploy one, the use of Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) for authentication is recommended.

Use Windows Server 2003 Active Directory to simplify management of wireless clients by putting all wireless clients in a single universal or global group and implementing security filtering on this group with Group Policy. You can then use the Wireless Network (IEEE 802.11) Policies Group Policy extension on a Windows Server 2003 SP1 (or later) domain controller to configure WPA encryption and authentication options for wireless clients running Windows XP or Windows Server 2003.

**Note** At the time of this writing, WPA2 authentication options cannot be directly set by Group Policy.

### Unauthorized Wireless Access Points

Unauthorized or rogue access points can be a significant problem for the security of your network. They are almost always set up as a convenience by people who don’t realize the security implications of what they’re doing, and they are rarely intended for malicious use. But it matters little whether they are intended for malicious use—because they are unmanaged and rarely set up with proper security, they pose a real and often unknown hazard to the security of your network and can cause interference with managed and authorized access points as well.

Dealing with rogue access points is first and foremost a management issue, not a technological one. Within the organization, there needs to be a clear and well-publicized policy that explicitly prohibits the use of any unauthorized wireless device that connects to the network. Beyond the simple publication of the policy, however, you need to educate users and management about the reasons behind the policy, the very real danger such devices present to the network and the organization, and the consequences for violating the policy. The other side of the equation, however, is that you need to make sure that users can get the authorized wireless resources they need to get their jobs done effectively.
From a technological defensive standpoint, there are some versions of managed network switches that can detect a downstream wireless access point from most of the common wireless vendors. And there are wireless scanners you can use to detect wireless networks. But all the technological solutions are secondary to a clear, unambiguous, and well-publicized policy on wireless networking.

**Small and Medium Business Deployment with WPA**

Deploying a wireless network in a small to medium sized business creates the same challenges as deploying one in a large enterprise, but usually with fewer resources to call on. Fortunately, it’s possible to configure and set up wireless networking without having to use RADIUS servers and have a full PKI infrastructure.

**Guest Access**

The requirements and needs for guest access in a small to medium size business are no different than those for a large business in many cases, and the issues and set up are the same as discussed in the previous sections, with one additional concern. With small to medium size businesses being in a physically smaller location, almost certainly without dedicated “public” buildings, the issue of an external wireless access point spilling over and being visible to internal users is at least as much of a problem as it is with a large organization. Address it in much the same ways as you address a rogue access point—that is, implement a clear, unambiguous, and well-publicized company policy and careful education of users and administrators. In addition, make sure that internal resources are available and that they address the needs of your users.

**Managed Clients**

Your internal wireless clients should all use a minimum of WPA encryption, with WPA2 preferred if your hardware supports it. If you’re subject to stringent, externally imposed, requirements, such as the Health Insurance Privacy and Portability Act (HIPPA), then you have stronger requirements that might require WPA2. If you’re using a pre-shared key (WPA-PSK), the initial key should be as complex and lengthy as you can stand. We find that a 20 to 30 character pass-phrase has the advantage of being both possible to remember and of reasonable complexity. Where your clients are all running Windows XP SP2 or later, you can use the Wireless Network Setup Wizard included with Windows XP SP2 and a USB key to automatically configure your clients.

**More Info** For more information, see the “Wireless Deployment Recommendations and Best Practices” article at http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/wideprec.mspx.
Unauthorized Wireless Access Points
The issues created by rogue access points are the same in small and medium sized businesses as in large businesses. Ensure that you have a clear and well-publicized policy about acceptable use of wireless networking.

Summary
In this chapter, we’ve covered the implementation of secure wireless networking, including the support for IEEE 802.11i and WPA2. In the next chapter, we’ll look at the support services and features of Windows Server 2003, starting with the interoperability features and services of Windows Server 2003. These features and services include the greatly expanded support for UNIX and Linux interoperability that ships as part of Windows Server 2003 R2.
Part V
Support Services and Features

Chapter 27
Interoperability .......................................................... 879

Chapter 28
Managing Software ...................................................... 901

Chapter 29
Application Compatibility and Virtual Server ..................... 955

Chapter 30
Deploying Terminal Services ......................................... 981

Chapter 31
Using the Indexing Service ........................................... 1009
Enterprise computing inevitably means interacting with other environments and operating systems. That can mean interoperating with, and integrating with, existing UNIX networks; connecting to and working with Novell networks; or supporting Macintosh clients that need full access to the resources of the Microsoft Windows network.

In this chapter, we'll cover the basics of interoperability across these platforms, paying particular attention to the new features that are part of Windows Server 2003 R2 that provide greatly enhanced interoperability with UNIX and Linux networks and even the ability to compile and run UNIX applications natively on Windows Server 2003. We'll also pay attention to the challenges that supporting 64-bit computers adds to providing full interoperability.

**UNIX Interoperability**

Frequently, Microsoft Windows Server 2003 networks need to connect to and work with UNIX in one or another of its various incarnations. On its own, Windows Server 2003 SP1 has basic connectivity tools that enable it to function on the same network with UNIX servers. The additions that are part of Windows Server 2003 R2 allow UNIX and Windows Server 2003 to work nearly seamlessly together, so the system administrators of both environments can provide users with full access to the resources of the other environment almost transparently.

This chapter assumes you have at least a passing familiarity with UNIX or Linux, and that's why you're trying to interoperate. We start by examining permissions and security issues because they are related to many of the other subjects in this chapter. Next comes basic connectivity and file systems, followed by a look at the changes and improvements introduced with Window Server 2003 R2. Finally, we cover the differences between the Windows Server 2003 cmd.exe shell, and the new Subsystem for UNIX Applications (SUA) shells.
Permissions and Security Concepts

One of the most important and pervasive differences between Windows Server 2003 and UNIX is the manner in which they handle permissions and security. These differences are subtle and frequently lead the unwary to make false assumptions. Because Chapter 21 and Chapter 22 have already explained in great detail how Windows Server 2003 handles security, we’ll spare you those details here, but if you’re going to coexist with UNIX servers, you need to understand how UNIX handles security to avoid problems. Let’s look at a UNIX file listing first, and then examine symbolic links, privilege levels, and permissions.

A UNIX File Listing

A UNIX file listing might look something like this:

```
-rwxr-x--x 2 charlie dba 2579 Aug 30 15:49 resize
```

This listing tells you virtually all you need to know about the security and permissions of the file you’re looking at. Start at the left of the line and work your way across to see what’s here and what it means—and how it compares to Windows Server 2003.

The first dash (-) tells you this listing is not a directory. If it were a directory, a “d” would be in that place instead. UNIX treats a directory as simply another file, although a special one, and the permissions have a slightly different meaning when referring to a directory as opposed to a file. Directory permissions are covered in a bit, but let’s stay with regular files for now.

The next three characters correspond to the permissions of the file owner—who can be someone other than the original creator because UNIX allows a user to “give” a file to another user. The “r” indicates that the owner has the right to read the file; the “w” means she or he can write to it, delete it, or otherwise modify it; and the “x” allows the owner to execute the program.

Real World  UNIX-Executable Programs

In Windows Server 2003, the operating system decides whether a program is executable based on the filename. If the filename has an extension of .COM, .EXE, .BAT, or .CMD, it can be executed, assuming the user has the appropriate permissions. In UNIX, no association exists between the extension and whether the file is executable. In fact, most UNIX files have no extension at all. The only determinant of whether a file is executable is the permission of the file. So, although it might be the convention on a particular system to always name shell scripts (the UNIX equivalent of a batch file) with a name that ends in .sh or .ksh, this has no actual meaning. The file must be given the execute permission before it can be executed directly.
The fifth, sixth, and seventh characters correspond to the permissions of members of the same group as the owner of the file. The “r” indicates that members of the group can read the file (or perform actions that leave it unchanged, such as copying it); the dash indicates that they do not have permission to write to it, delete it, or otherwise modify it; and the “x” gives them the ability to execute the program.

Finally, the last three characters of the first group correspond to the permissions of the rest of the world. The initial dash indicates that these users don’t have the right to read the file, or in any way look at the contents, nor do they have permission to copy the file. The second dash indicates that they don’t have permission to change, modify, or delete the file, and finally, the last “x” indicates that they can execute the file if executing doesn’t actually require a read.

**Real World Permissions**

UNIX has only three basic permissions: Read, Write, and Execute.

- **Read** The right to read a file or list its contents. The right to make a copy of the file. For directories, the right to list the contents of the directory.

- **Write** The right to alter the contents of a file. For a directory, the right to create files and subdirectories. If you have Write permission on a directory, you have the right to delete files in the directory even if you don’t have Write permission on the file—if you also have either Read or Execute permission on the directory.

- **Execute** The right to execute the file. Even the owner of a file needs this permission to execute it. For a directory, the right to change into the directory or to execute files within the directory. Having this right on a directory does not, however, give you permission to list the contents of the directory, so you might be able to execute a file without being able to see that it is there.

The next character, the number 2, indicates that there are two hard links to the file. A hard link gives the exact same file another name. There is still only a single actual file stored on the hard disk, but there are two directory entries pointing to the file. There are no practical limits to the number of hard links that can exist to a single file, but all links to the file must exist on the same file system. Windows Server 2003 supports hard links on the NTFS file system.

The next two groups in the listing are the owner of the file, “charlie,” and the group for the file, “dba.” These are normally user and group names, but they could also be a number if either the owner or group of the file doesn’t actually have an account on the system.

Next is the size of the file (2579 bytes in this case), the date and time when the file was created or last updated, and the name of the file—actually, the directory entry for the file.
that corresponds to this hard link to the file. Note that no link has any preference over any other. There is nothing significant about which name comes first; all are treated equally. Deleting one link does not delete the file—just that reference to it. Any other versions of the file remain.

**Symbolic Links**

UNIX supports both hard links and symbolic links. *Symbolic links* are vaguely analogous to Windows Server 2003 shortcuts but with several important differences. The most important difference is that in UNIX when you access the symbolic link, you actually access the file it points to, not the link itself. For example, if you edit a symbolic link to a text file, you're actually editing the original text file. With a Windows Server 2003 shortcut, you can use the shortcut only to start an executable file or to open a folder. Windows Server 2003 does not directly support symbolic links, but the SUA subsystem does support symbolic links.

A symbolic link differs from a hard link in that the actual file has precedence over any of the symbolic links to it. In fact, the listing for a symbolic link to the earlier resize file makes it immediately clear that this is a symbolic link, not a hard link:

```
lrwxrwxrwx 1 charlie dba 2579 Aug 30 15:49 resize -> /u/cpr/resize
```

As you can see, the listing not only begins with the letter “l” in the first position, but it also actually shows where the link is pointing. You’ll notice that the two filenames are identical. Although this isn’t a requirement, it is the most common use of symbolic links—to make a file appear as if it were in one place when it actually resides elsewhere.

Another feature of a symbolic link that distinguishes it from a hard link is that it can point across to a different file system or even a different machine. You can have a symbolic link that points to a file that resides on a completely different computer.

---

**Important** If you copy a file on top of a symbolic link, the link is broken. Your new file actually replaces the link with the file. The original file still exists, however, making the duplication of files confusing at best.

**Privilege Levels**

Traditionally, UNIX divides the world into only three types of users: the owner of a file, a member of the same group as the owner, and all the rest of the world. These three privilege levels are called owner, group, and other. So far, so good. This sounds a lot like Windows Server 2003, right? A big difference is in the second privilege level: group.

On UNIX systems with traditional security, a user is active only in a single group at a time. When that user creates a file, the file has permissions for the group based strictly on the
current group of the file creator. This situation can have interesting and subtle complications when compared to the Windows Server 2003 methodology. If a user’s primary logon is to one of the standard groups, things generally behave as you expect. However, when a user belongs to a specialized group with limited membership and creates files while that group is the active group, the ability of users outside the group to access the file could be constrained.

A user who isn’t an active member of the group that owns a file and who isn’t the actual owner of the file is in the other privilege level. This arrangement is essentially the same as the Windows Server 2003 Everyone group. A user in the other category has no permission to access the file except what every other user has. It’s important to understand that UNIX lacks the equivalent of “Authenticated User” in the Windows Server 2003 world—so the other group aligns with the Windows Everyone group, not the Authenticated User.

**Real World  The UNIX Super User**

In discussions of UNIX security, keep in mind one overriding principle: the root user (sometimes called the super user) has access to everything. In the Windows Server 2003 world, you can easily set a file or directory so that even users with administrative privileges don’t have access without changing the ownership of the file, but in the UNIX world that restriction doesn’t exist. Not only that, but the super user can even change identities to have the same identity as you without knowing your password.

**Basic Connectivity**

Now that you understand the differences between the security models of Windows Server 2003 and UNIX, let’s look at how they are compatible. For one thing, with no additional add-ons, Windows Server 2003 coexists reasonably well with UNIX servers. The default networking protocol for both operating systems is the same—TCP/IP. They can easily share DNS, DHCP, and other services. Simple connectivity between Windows Server 2003 and UNIX can be handled by FTP and Telnet.

**File Transfer Protocol**

All versions of Windows Server 2003 include a simple FTP command-line client and can handle FTP from within Microsoft Windows Explorer to a limited extent. The character-mode client provides no frills but should feel quite comfortable to the UNIX user—and it works without quirks, though it lacks some of the sophistication that a UNIX user would expect. Those who want a more graphical, friendly FTP client have a variety to choose from, including shareware and some that are pure freeware. A personal favorite is
WS_FTP Pro from Ipswitch (http://www.ipswitch.com). Windows Server 2003 also includes full-featured FTP server capability as part of its optional Internet Information Services (IIS) component. With both an FTP server and a client natively available, you can easily copy files between the UNIX and Windows Server 2003 machines on your network.

**Telnet**

All versions of Windows Server 2003 come with the character-mode Telnet client that debuted in Services for UNIX (SFU). The semi-graphical Telnet client that had been around since Microsoft Windows 3 is finally gone. The new client is faster, has better terminal emulations, and is actually quite decent for most uses. It supports American National Standards Institute (ANSI) features—including color, VT52, VT100, and VTNT (a special emulation that can be useful when running character-mode Windows Server 2003 applications such as Edit). If your need for terminal emulation isn’t met by one of these modes, there are excellent third-party commercial Telnet clients available.

---

**Real World   Secure Shell (SSH)**

Telnet and FTP, although great and useful protocols, have an inherent security risk, as they transmit information, including passwords, across the network in plain text without encryption. This can be acceptable in many situations where the internal network is thoroughly protected from outside intrusion and internal users are all trusted, but it poses unacceptable risks in other situations. One solution to this, and the de facto standard in the UNIX world, is the SSH protocol, a secure, encrypted protocol that supports a Telnet-like character mode logon feature, an FTP-like file transfer protocol, and additional features.

There are both commercial and open-source versions of SSH available. Of the commercial versions, Reflection for Secure IT is one that is FIPS certified, and it supports virtually all UNIX operating systems, as well as Windows Server 2003. OpenSSH is an excellent Open Source implementation of the SSH protocol and is widely available in both compiled forms and as source code.

Windows Server 2003 Server even has two built-in Telnet daemons, or servers. The first, which operates as a Windows service and is part of the Win32 subsystem, uses the Windows character mode shell (Cmd.exe) for client sessions. The second is the telnetd daemon of the SUA subsystem. It must be enabled by editing the /etc/inetd.conf file. Only one telnet server can be running at any given time, so do not enable telnetd unless you first disable the Win32 telnet service.
File Systems

Windows Server 2003 R2 network file sharing supports both Server Message Block (SMB), the native Microsoft networking mechanism, and the UNIX-originated Network File System (NFS). To allow Windows Server 2003 and UNIX to share a common file system, you need to add SMB to your UNIX systems or NFS to your Windows systems.

Until the original release of SFU, only third-party NFS solutions were available for Windows systems that needed to be able to share file resources with UNIX systems, and most of these solutions were expensive and problematic. The biggest issue was their inability to keep up with Microsoft Windows NT service packs, which seemed to break these NFS solutions more often than not. In addition, these solutions often had significant performance problems. The Client for NFS, Server for NFS, and Gateway for NFS included with SFU were the first Microsoft shipped solutions, and now, in Windows Server 2003 R2, Microsoft Services for NFS provides full NFS client and server functionality.

There are several powerful SMB-based UNIX and Linux solutions that address the problem of sharing file resources between Windows and UNIX by adding support for SMB to UNIX, rather than NFS to Windows. These SMB solutions vary in cost from free to expensive, and they support native Windows networking at either the workgroup or domain level. With the release of Windows Server 2003, only time will tell how well these solutions will keep up with the changes in the Windows Server 2003 security model as compared to the Windows NT model; currently only Samba appears to be making any strides toward supporting the Active Directory service.

The Network File System

Originally, NFS was designed to run as a broadcast protocol using User Datagram Protocol (UDP). This protocol created substantial performance and network traffic issues for those intending to implement large amounts of NFS networking and made it difficult to share file systems across routed boundaries. Eventually, the NFS standard changed to support TCP for NFS networking, and virtually all modern clients and servers support this mechanism. However, some older NFS implementations still in use don’t support TCP, so Windows Server 2003 Client for NFS supports UDP, TCP, or both. The default is TCP only.

Server Message Block

The biggest issue that the SMB-on-UNIX crowd has to deal with is the changing Windows Server 2003 security model. Two mechanisms are used for handling security with the SMB-on-UNIX solutions—workgroup-level security and limited Active Directory authentication.
Workgroup security suffers from all the same problems as workgroups in the enterprise environment: it becomes more difficult to manage as the number of users and machines increases, and it has limited options for actually managing security. However, workgroup security has a definite place in the smaller environment, where it’s easy to understand and simple to set up. Plus, there’s a nice cost advantage—a widely available and well-implemented freeware SMB server called Samba is available on virtually all UNIX and Linux platforms. Samba can also run as a Windows NT 4 primary domain controller and can authenticate users against a Windows Server 2003 domain as long as the Windows Server 2003 domain is running in Windows 2000 mixed functionality mode. Version 3 of SAMBA supports direct authentication against Active Directory, eliminating the need to run in mixed mode. Other commercial, workgroup SMB servers are also available that run on a variety of platforms. They tend to be more Windows-like and easier to set up and administer than Samba, which shows its open-source heritage.

Windows NT 4 domain SMB servers are also available from a number of UNIX vendors. All of these (except Samba) are based on AT&T’s initial port to UNIX of Microsoft Advanced Server technology. Each is limited to running on the platform for which it was designed, and each has slight differences because the port from AT&T required tweaking in most cases. All of these UNIX SMB servers can be either primary domain controllers or backup domain controllers in a Windows NT domain, and some can even be a simple member server, but all have problems dealing with the new security model in Windows Server 2003. Because these servers are based on the Windows NT 4 security model, you’ll be forced to stay in mixed mode.

The UNIX SMB domain servers do have one important advantage over the Samba and SMB workgroup servers: to the users and administrators of the Windows network, they all look and feel exactly like a native Windows NT 4 server. The familiar Windows NT Server administration tools are used to manage them, and servers and shares look exactly like a Windows NT server to users, eliminating training and user interface issues.

**Printing**

Microsoft Windows Server 2003 includes native support for TCP/IP printing protocols. When installing or configuring a printer, you can add a TCP/IP printer port as described in Chapter 8. In addition, you can add support for the UNIX lpr/lpd protocol, allowing Windows Server 2003 to function as a remote print server for UNIX clients.

To add print services for UNIX, complete the following steps:

1. Open Add/Remove Programs in Control Panel.
2. Select Add/Remove Windows Components.
3. Highlight Other Network File And Print Services, and click Details to open the Other Network File And Print Services dialog box shown in Figure 27-1.

![Figure 27-1 The Other Network File And Print Services dialog box](image)

4. Select the Print Services For UNIX check box, and click OK.

5. Click Next to add the service, and click Finish when the wizard completes.

**Microsoft Services for NFS**

Microsoft Services for NFS includes an NFS client and an NFS server, along with the necessary authentication components. Which authentication components you need will depend on your network configuration and what clients you need to support on your network. In general, you must install the following items:

- **Server for NFS** to support sharing Windows file systems with UNIX clients.
- **Client for NFS** to access filesystems on UNIX servers.
- **User Name Mapping** on one or more servers on the network to align Windows users with UNIX users.
- **Server for NFS Authentication** on all domain controllers if you are installing Server for NFS.
- **Microsoft Services for NFS Administration** to administer the service.
- **RPC External Data Representation** to provide remote procedure call (RPC) data services to Client for NFS and Server for NFS.
■ **RPC Port Mapper** to provide port mapping services to Server for NFS and User Name Mapping.

You need to install only one User Name Mapping server on the local subnet. Microsoft Services for NFS also supports the use of a Microsoft Services for UNIX v3.5 (SFU) User Name Mapping server. Ideally, User Name Mapping should be installed on a domain controller to limit network traffic.

If your Active Directory is not at the Windows Server 2003 domain functional level, you must install Server for NFS Authentication on every domain controller in the domain, and on every domain controller of any domain whose accounts might need access to NFS resources on this domain.

To install Microsoft Services for NFS, complete the following steps:

1. Open Add/Remove Programs in Control Panel.
2. Select Add/Remove Windows Components.
3. Highlight Other Network File And Print Services, and click Details to open the Other Network File And Print Services dialog box shown in Figure 27-1.
4. Highlight Microsoft Services For NFS, and click Details to open the Microsoft Services For NFS dialog box shown in Figure 27-2.

![Figure 27-2](image)

5. Select the services required, click OK, and then click Next to install Services for NFS on your server.
**Real World  Microsoft Services for NFS vs. Microsoft Services for UNIX**

How is Microsoft Services for NFS different from the NFS included in Microsoft Services for UNIX? Good question. The first and most obvious answer is that Microsoft Services for NFS is supported on both 32-bit and 64-bit servers. This is a major advancement over SFU, which supports only 32-bit Windows.

There are also significant performance and usability enhancements in Services for NFS when compared with earlier versions of NFS from Microsoft. The new NFS Management console is a definite improvement, for one. And the ability to use Active Directory lookups directly, instead of User Name Mapping, is a definite plus. The overall speed of NFS is improved somewhat in Microsoft Services for NFS, though NFS is still slower than SMB in almost all cases.

**Configuring User Name Mapping**

Even when a user has exactly the same logon name in UNIX and Windows Server 2003, they aren’t actually the same user. The UNIX system uses a combination of user identity (UID) and group identity (GID) to identify a user. This UID/GID pair could be repeated across multiple systems—nothing about it is unique. Windows Server 2003 uses a Security Identifier (SID) to identify the user that is globally unique—even if a user is deleted from the system and then re-created, with exactly the same name, it will be a different SID. The User Name Mapping (UNM) service was originally introduced by Services for UNIX to handle mapping between the UNIX UID/GID and the Windows Server 2003 SID.

When a UNIX user requests access to a Windows resource, or when a Windows user requests access to a UNIX resource, UNM is called to map the UNIX user to the Windows user or vice-versa. Note, however, that UNM doesn’t actually do the authentication—that is performed by Active Directory in the case of Windows Server 2003, or the UNIX authentication mechanism on a UNIX system, as appropriate. Microsoft Services for NFS includes its own User Name Mapping service, or it can leverage an existing User Name Mapping already up and running on your network.

To configure User Name Mapping, complete the following steps:

1. Start the Microsoft Services for NFS console on the computer that has UNM installed. This can be any computer on the network, but if you have large numbers of mapped users, you should choose a domain controller to host UNM to improve performance and reduce network traffic.
2. Right-click User Name Mapping in the left pane, and select Properties to open the dialog box shown in Figure 27-3.

![Figure 27-3 The User Name Mapping properties dialog box](image)

3. Choose the UNIX authentication method that will be used, either Use Network Information Services (NIS) or Use Password And Group Files. If you select Use Password And Group Files, you'll need to set the path to the files. Click Apply to apply any changes before changing screens.

   **Note** The default files for password and group files are: %windir%\system32\drivers\etc\passwd and %windir%\system32\drivers\etc\group. You should use these filenames and locations unless there is a compelling reason not to in your environment. These files can be copied from an existing UNIX server or manually created. The encrypted password field in the files is not used, though the field is still present.

4. Select the Simple Mapping tab. If your user names are identical in both UNIX and Windows, except for case, you can use simple maps by selecting the check box and selecting the domain from the drop-down list. If some user names are different, you'll need to use Advanced Maps to handle those users.

5. To create advanced user maps, right-click User Maps and select Create Map from the Action menu to open the Create Advanced User Mapping dialog box shown in Figure 27-4.
6. Select the correct Windows domain from the drop-down list, and click the List Windows Users button to populate the Windows User list box. Click the List UNIX Users button to populate the UNIX User list box.

7. Highlight a Windows User and a UNIX user, and click Add. Repeat this to add additional advanced maps.

8. Click Close when you have created all the maps you need.

**Note** You can map multiple Windows users to a single UNIX user, but you cannot map multiple UNIX users to a single Windows user.

**Note** You can also use the command line tool mapadmin.exe to manage User Name Mapping. Type `mapadmin /?` for syntax details, or `man mapadmin` from the SUA shell for additional help.

To enable other computers to connect to the User Name Mapping service on a server, you must edit the `.maphosts` file. This file is in the `%SFUDIR%\Mapper` directory on SFU servers and in `%windir%\msnfs` in Windows Server 2003 R2 servers. If the file is not present, no computers can connect to the User Name Mapping server. If the file is present, but empty, only the local computer can connect to the User Name Mapping server. Entries in `.maphosts` explicitly allow or disallow connection by remote computers. Table 27-1 gives the syntax and meaning of entries in the `.maphosts` file.
Support Services and Features

Additional instructions for the syntax required are included as comments in the file as shipped with both SFU and Windows Server 2003 R2. You should initially enable all computers to access UNM until you have confirmed that everything is working as desired, and then restrict access to only those computers that need access, including the UNIX computers that will need to connect to UNM.

Connecting to an NFS Share

Microsoft Services for NFS includes an NFS client that enables Windows Server 2003 R2 computers to connect to a shared (exported) NFS filesystem on a remote UNIX computer. To use the command line to connect to an NFS export on a remote server, use the following:

1. Open a command window or SUA shell.
2. Type the following command:
   
   net use drive: servername:/export
   
   where drive is the drive letter to use, servername is the name of the NFS server, and export is the NFS share name on the NFS server.
3. You can also use the UNIX mount command, which provides additional options for how the NFS export is mounted. Type `mount -?` for full syntax, or `man mount` from an SUA shell for additional help details on the mount command.

You can use any of the following commands to connect to an NFS export. They will all have the same result.

```
net use * servername:/export
net use * \servername\export
mount servername:/export *
mount \servername\export *
```
You can also use Windows Explorer to locate and connect to a remote NFS resource. To use Windows Explorer to locate and connect to NFS shares, do the following:


2. Right-click NFS Network, and choose Add/Remove NFS LANs from the Action menu to open the dialog box shown in Figure 27-5.

3. Click Add to open the Add Broadcast LAN dialog box shown in Figure 27-6.

4. Type in a name for the LAN, the IP address of an NFS server on the LAN, and the subnet mask for the LAN, as shown in Figure 27-6.
5. Browse the LAN to see available NFS exports, as shown in Figure 27-7.

![Figure 27-7](image)

**Figure 27-7** Browsing with Windows Explorer to find NFS exports on the network

6. Select an NFS export, and then, from the Tools menu, select Map Network Drive to map the NFS export to a drive letter.

**Note** When specifying an NFS resource, use the `server:/export` syntax, instead of `\server\export`, for faster setup of the connection.

### Configuring Client for NFS

There are several options that you can configure in Client for NFS. These include the protocols to use, the default mount type, buffer size, and default file permissions. Any of these options can be manually set for a specific mount by using the mount command with the appropriate options. The options available and what they mean are described in Table 27-2. To set these options, open the Microsoft Services for NFS Management console, right-click Client for NFS, and select Properties from the Action menu.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Page</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Protocol</td>
<td>Client Settings</td>
<td>TCP, UDP, TCP+UDP</td>
</tr>
<tr>
<td>Use Soft Mounts</td>
<td>Client Settings</td>
<td>Number of times to retry a connection. Default is 1 attempt.</td>
</tr>
<tr>
<td>Use Hard Mounts</td>
<td>Client Settings</td>
<td>Default is 0.8 seconds, and applies to both hard and soft mounts.</td>
</tr>
<tr>
<td>Interval between retries</td>
<td>Client Settings</td>
<td></td>
</tr>
<tr>
<td>Read buffer size</td>
<td>Client Settings</td>
<td>1-64 KB. Default is 32 KB.</td>
</tr>
<tr>
<td>Write buffer size</td>
<td>Client Settings</td>
<td>1-64 KB. Default is 32 KB.</td>
</tr>
</tbody>
</table>
Table 27-2  Client for NFS Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Page</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>File Permissions</td>
<td>Default file permissions for new files. Read(r), Write(w), and Execute(x) are true by default.</td>
</tr>
<tr>
<td>Group</td>
<td>File Permissions</td>
<td>Default file permissions for new files. Read(r) and Execute(x) are true by default.</td>
</tr>
<tr>
<td>Others</td>
<td>File Permissions</td>
<td>Default file permissions for new files. Read(r) and Execute(x) are true by default.</td>
</tr>
</tbody>
</table>

Creating an NFS Share

Server for NFS enables you to share (or export, to use the UNIX terminology) a folder or file system. Sharing is simple from either the command line or from Windows Explorer.

Real World  NFS Doesn’t Support Multilevel Exports

The NFS protocol doesn’t support sharing the subdirectory of an already shared resource, so you need to ensure that you share from as far up the tree as necessary, because you won’t be able to then share another folder within that directory structure. The one exception to this is that each drive letter is shared as the top of a file system.

To share a directory with NFS, complete the following steps:

1. Highlight the directory you want to share in Windows Explorer.
2. Right-click and select Sharing and Security from the Action menu.
3. Click the NFS Sharing tab to open the NFS Sharing dialog box shown in Figure 27-8.
4. Select Share Name, and enter the name for the export. Set additional options as described in Table 27-3.

5. Click OK to exit and make the share available to NFS clients on the network.

6. The command line to share the same backup directory shown in Figure 27-8 with default options would be

```
nfsshare backup=G:\backup
```

Table 27-3 Properties of NFS Sharing

<table>
<thead>
<tr>
<th>Property</th>
<th>Default</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share name</td>
<td>The shortest name of the directory</td>
<td></td>
</tr>
<tr>
<td>Allow anonymous access</td>
<td>No</td>
<td>When true, you can also set the default UID and GID for an anonymous user.</td>
</tr>
<tr>
<td>Permissions</td>
<td>All Machines</td>
<td>Read-only, ANSI, Root Access Denied. Click Add to add additional machines with specific permissions levels.</td>
</tr>
<tr>
<td>Type of Access</td>
<td>Read-only</td>
<td>No access, Read-only, Read/Write.</td>
</tr>
<tr>
<td>Allow root access</td>
<td>No root access</td>
<td>Allow or deny root access.</td>
</tr>
</tbody>
</table>

Configuring Server for NFS

There are several options that you can configure in Server for NFS. These include the protocols and NFS version to use, filename handling, locking options, and auditing. The options available and what they mean are described in Table 27-4. To set these options, open the Microsoft Services for NFS Management console, right click Server for NFS, and select Properties from the action menu.

Table 27-4 Server for NFS Properties

<table>
<thead>
<tr>
<th>Setting</th>
<th>Page</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols</td>
<td>Server Settings</td>
<td>TCP, UDP, TCP+UDP. Default is TCP+UDP.</td>
</tr>
<tr>
<td>Enable NFS v3 Support</td>
<td>Server Settings</td>
<td>Enabled by default. When not selected, only NFSv2 support is available.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Server Settings</td>
<td>Renewal period set in seconds or don't renew at all.</td>
</tr>
<tr>
<td>Translate File Names</td>
<td>Filename Handling</td>
<td>Disabled by default. You can specify a character translation table.</td>
</tr>
</tbody>
</table>
### UNIX Identity Management Services

Windows Server 2003 R2 adds integrated UNIX identity management directly to Windows Server, with support for Server for NIS, password synchronization, and Active Directory UNIX UID and GID lookup. The UNIX identity management components extend the identity management components that have been part of Services for UNIX and bring them into Windows as a part of the operating system. Server for NIS acts as a master NIS server for your existing UNIX NIS domain, integrating into and extending the Active Directory schema to support both standard and nonstandard mappings.

### Windows Subsystem for UNIX-Based Applications

First introduced as part of Services for UNIX v3.0, the Interix subsystem provided a full UNIX application execution environment on Windows running as a native Windows subsystem. The Windows Subsystem for UNIX-Based Applications extends the Interix...
subsystem to support 64-bit processors and brings it into the core operating system beginning with the release of Windows Server 2003 R2.

SUA is a full-featured, POSIX-compliant, UNIX application environment with more than 2000 UNIX APIs. The SUA shells and applications run as a full subsystem on the Windows kernel and support standard UNIX shell programs and applications.

SUA gives the UNIX programmer or user a familiar environment, with a single-rooted file system that supports typical file locations such as `/etc`, `/usr/bin`, and `/usr/local/bin`. SUA supports symbolic and hard links that are transparent to the UNIX user. SUA can also support full-case sensitivity and SUID behavior if required.

The SUA architecture, shown in Figure 27-9, provides a highly compatible environment for UNIX applications. SUA supports both multiprocess and multithreaded applications. Applications can use `fork` to spawn new processes, but note that fork is not supported across the SUA/Win32 boundary. SUA also supports POSIX threads that use the pthread APIs.

![Figure 27-9 The Subsystem for UNIX-Based Applications Architecture](image-url)
Note While SUA ships on the Windows Server 2003 R2 CD, the SUA SDK, applications, and shells are available only as a separate download from http://www.microsoft.com/windowsserver2003/R2/unixcomponents/webinstall.mspx.

Macintosh Interoperability

Despite periodic predictions of its demise, the Apple Macintosh remains popular in some environments, and the increased capabilities and interoperability of the latest versions of Mac OS X have made it easier to support mixed environments. If your Mac clients are running Mac OS X 10.1 or later, there is little or no need for the File Server for Macintosh (FSM) or the Print Server for Macintosh (PSM). If your Macintosh clients are running a version of Mac OS earlier than Mac OS X, you need to use FSM and PSM for full interoperability. FSM and PSM are not supported on 64-bit versions of Windows Server 2003.

On the CD For complete details on integrating Mac clients, including older versions of the Mac OS, see Chapter 25 from the first edition of this book, which is included on the CD for your convenience.

Novell Netware Interoperability

Both Novell and Microsoft provide a number of ways for clients to access NetWare and Windows Server 2003 resources. Novell provides client software for MS-DOS, Microsoft Windows 3.1x, Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows NT 4 Workstation, Microsoft Windows 2000 Professional, and Microsoft Windows XP Professional. Microsoft has NetWare client software for Windows 95, Windows 98, Windows NT 4 Workstation, Windows 2000 Professional, and Windows XP Professional. With the installation of any of these clients, a computer can be a client of Windows Server 2003 and NetWare simultaneously.

Summary

The original release of Windows Server 2003 provided comprehensive interoperability with legacy operating systems. The R2 release of Windows Server 2003 extends that interoperability substantially by providing a full suite of UNIX interoperability tools and protocols as a part of the operating system. This includes the new Subsystem for UNIX-Based Applications that gives UNIX and Linux application developers a highly compatible and high-performance subsystem to compile and run UNIX applications on Windows natively. Also included are full Microsoft Services for NFS to provide file system compatibility across platforms, and an integrated suite of UNIX identity management components.

In the next chapter, we’ll look at the ways to manage software on your Windows Server 2003 network.
Managing software on client computers can be a tedious task. Fortunately, Microsoft Windows Server 2003 integrates several technologies that can make managing computers more efficient. You can use Group Policy to deploy applications automatically. You can use Software Restriction Policies to block unauthorized programs and scripts. Finally, you can use Remote Installation Services (RIS) to boot client and server computers from a network connection and easily install Microsoft Windows. Although these features are not as powerful as those provided by dedicated management programs such as Microsoft Systems Management Server (SMS), they are easy to use and provide a basic set of management capabilities.

Note Because the Group Policy Software Installation extension, Software Restriction Policies, and Remote Installation Services all use Group Policy, it is important to understand Group Policy before using these tools. See Chapter 11 for more information about Group Policy.

Using the Group Policy Software Installation Extension

The Group Policy Software Installation extension enables you to deploy applications to computers in the domain or forest using Group Policy and includes the capability to do the following:

- Publish applications so that users can view and install programs from the network
- Assign applications to users or computers so that the applications are installed automatically when users need them or on the next restart or logon
Target applications to different groups using Group Policy

View installation status using Group Policy Results

To deploy an application, create or edit the appropriate Group Policy Object (GPO) and add the application’s Windows Installer package to either the user or computer policy, depending on whether you want it to apply to users or computers. The next time the user logs on or the computer restarts, Windows applies the relevant policy to the user or computer depending on the package settings you specify in the GPO. (See Table 28-1.)

Windows Installer handles the automatic installation or removal of all programs, as well as any upgrades or repairs.

Table 28-1  GPO settings needed for specific actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Setting Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically install the application</td>
<td>Install This Application At Logon</td>
</tr>
<tr>
<td>Add the application to a list of installable programs in Add/Remove Programs</td>
<td>Publish</td>
</tr>
<tr>
<td>Add a shortcut to the application in the Start menu and install it on first use</td>
<td>Assign The Application (Note: Do not use the Install This Application At Logon setting.)</td>
</tr>
</tbody>
</table>

Microsoft IntelliMirror Technologies

IntelliMirror is a set of technologies that allows users’ data, settings, and applications to follow them to other computers running Windows 2000, Windows XP, or Windows Server 2003 on the network—or even off the network, in the case of laptops. The components of IntelliMirror are as follows:

- **User Data Management**  Allows users to access their documents and data from any computer on or off the network (in the case of synchronized laptops). This is done by redirecting the My Documents folder to a network share and then using the offline folders feature to ensure the ability to access the data when offline. For information about folder redirection, see Chapter 11; for information about offline folders, consult the Windows Help system, and remember that Microsoft SharePoint files are not available offline.

- **User Settings Management**  More simply known as *roaming profiles*, this feature allows users to log on to any computer on the network as if it were their own computer, with all their application and Windows settings intact.

- **Software Installation and Maintenance**  Allows administrators to deploy applications automatically to users using Group Policy.

- **Remote Installation Services (RIS)**  Allows users to start a computer with no functioning operating system from the network, logon, and then select an approved operating system that Windows installs automatically.
Finding the Right Mix of Services

Look at the following details of the technologies (and Table 28-2) to determine the best mix of services for your type of network:

■ RIS (Remote Installation Services) permits a user to start a computer (with or without an operating system) from a RIS server over the network and then automatically install Windows 2000 Professional, Windows XP Professional, or Windows Server 2003. RIS works much like using unattended answer files and disk imaging, but with greater ease of use.

■ Group Policy allows users to access their data, settings, and applications from any computer on the network running Windows 2000, Windows XP Professional, or Windows Server 2003. Group Policy distributes data, software, and settings using a pull approach, meaning that the client requests data from Active Directory as needed. This approach works best when connectivity between the client and the nearest domain controller or software distribution server is at LAN speeds.

■ SMS manages the deployment of software and operating systems on complex networks and networks with sophisticated software management requirements. SMS controls the deployment schedule, and it provides software inventorying and license tracking, as well as planning and diagnostic tools. SMS can push software to clients using almost any version of Windows. It can also push software to distribution points from which Group Policy either installs the software or allows users to do so. SMS includes rich reporting and inventory capabilities so that you can determine which installations were successful. SMS requires a significant investment of resources to install and configure on a complex network, so it is appropriate only for networks with sophisticated software deployment and management needs.

■ Microsoft Operations Manager (MOM) provides an overarching management layer to Microsoft servers (including SMS), allowing you to monitor the network and determine what tasks need to be done. MOM is a powerful tool to use when the network gets so large that you need a way to manage your management tools.

Note Although most documentation insists that only SMS can perform managed Windows upgrades, you can also use Group Policy to perform them, as discussed in Chapter 23.
For users with a persistent network connection and without processor-intensive or highly graphical applications, deploy Terminal Services to centralize application maintenance and make it easier to provide a reliable and secure desktop environment. For more information about Terminal Services, see Chapter 30.

Natively Authored Windows Installer Packages

A native Windows Installer package created by the software manufacturer for use with Group Policy is usually the best option for deploying software. Deployment is relatively simple and requires no user intervention, and natively authored Windows Installer packages can repair themselves if a key file is inadvertently deleted or corrupted. You can also create transform files for some packages. For example, you can create a transform file to customize a Microsoft Office installation so that only Microsoft Word and Microsoft Outlook are installed rather than the entire suite.

More Info To customize a Microsoft Office installation, pick up a copy of the Microsoft Office 2003 Resource Kit (Microsoft Press, 2003), which includes an Installation Customization tool.

Zap Files

The easiest way to deploy applications that are not natively authored for Windows Installer is to create a .zap file. A .zap file is a text file that points to the 32-bit or 64-bit setup program for the application and can optionally run automated setup scripts. (Microsoft Windows Small Business Server 2003 uses a similar approach to application deployment.)

Although .zap files are simple and easy to create, .zap files cannot do the following:

- Assign applications to particular users or computers, though you can use a .zap file to publish applications.
■ Install applications with elevated permissions (Windows Installer gives higher permissions to installation programs so that a local administrator account isn’t needed to install software.)

■ Install applications automatically on first use

■ Perform partial installations of applications, with advanced features installed when needed

■ Perform a complete rollback of an unsuccessful installation or enable applications to repair themselves

Despite these limitations, most users find that using .zap files to deploy earlier applications is more reliable than repackaging applications, because .zap files make use of the original installation program. (It’s unlikely that you can write a better setup routine than the original, especially without access to more in-depth information about the program.)

Note Windows hides published applications that use 32-bit .zap files from 64-bit clients by default because 32-bit .zap files fail more often on 64-bit versions of Windows.

Repackaged Applications

If an application does not use Windows Installer to install itself, you can automate setup using an installation script and a .zap file, as discussed earlier, or repackage it into a Windows Installer package. When you repackage an application, you take "snapshots" of a computer before the application is installed using a commercial authoring package and then again after installing the application. The authoring package compares the two snapshots to determine what changes the application made during setup and then bundles the changes into a new Windows Installer package.

More Info To repackage an application, use a commercial authoring package such as one from Macrovision (which acquired InstallShield) or WISE Solutions; or you can use the light version of the Veritas Software WinInstall program, which is included with Windows 2000 Server (but unfortunately not with Windows Server 2003). WinInstall LE is discussed in the Microsoft Windows 2000 Server Administrator’s Companion.

Repackaged applications convey many of the advantages inherent in natively authored Windows Installer packages; however, a number of hazards are involved as well. If the client system differs from the reference system used to repackage the application, problems can occur because the repackaged application has only very limited means of resolving differences. Repackaged applications occasionally copy .DLL files to the wrong locations or they break shortcuts. Additionally, the All Users folder can potentially be deleted after
uninstalling a repackaged application. Technically speaking, poorly tested repackaged applications can trash the system. Also, repackaged applications aren’t easily upgraded—uninstall the existing version to install the new version.

Although there are potential problems, repackaging applications is a powerful way to deploy software if the repackaged application is thoroughly tested in a lab and pilot roll-out before widespread deployment.

**More Info**  For more on the support boundaries and technical difficulties inherent in repackaging applications, see Microsoft Knowledge Base Articles 264478, 320539, and 305955.

### Deciding Whether to Publish or Assign Applications

An application published in Active Directory becomes available from Add/Remove Programs for the users to whom the Group Policy Object (GPO) applies. (As described earlier, applications are published to users, not computers.) An assigned application, on the other hand, can be assigned to either users or computers and is installed without any action on the user’s part. Assigned applications appear on the Start menu and are installed on first use, unless you specify that they should be fully installed at the next logon.

Assign essential applications to users or computers so that these applications are always available, and publish optional programs to make it easy for users to find applications when they need them. Do not assign or publish an application to both computers and users. Table 28-3 summarizes the differences between publishing and assigning applications.

**Table 28-3 Differences between publishing and assigning deployed applications**

<table>
<thead>
<tr>
<th>Published Applications</th>
<th>Applications Assigned to Users</th>
<th>Applications Assigned to Computers</th>
</tr>
</thead>
<tbody>
<tr>
<td>When after deployment is the software available for installation?</td>
<td>Immediately, or after replication to the nearest DC</td>
<td>After the next logon*</td>
</tr>
<tr>
<td>How is the software installed?</td>
<td>Through Add/Remove Programs in Control Panel</td>
<td>Automatically on first use, or after the next logon event (Icons are present on the Start menu or the desktop.)</td>
</tr>
<tr>
<td>Is the software installed when a file associated with the application is opened?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Chapter 28  Managing Software

Updating Applications Deployed via Group Policy

The Group Policy Software Installation extension does not explicitly support updating applications. To update Microsoft applications, use Windows Server Update Services (WSUS). To update applications that WSUS does not support, use a third-party patch management application that supports the necessary applications, deploy the patches via login scripts, or instruct users to install the software updates from a network share (assuming the users are local administrators).

There are two other noteworthy methods of updating applications using Group Policy. The simplest method is to update the administrative installation or setup files in the software distribution point, and then redeploy the application (as discussed later in this chapter). However, this method can cause the client computers to become out of sync if users use the Install On Demand or Detect And Repair features before reinstalling the application. When using this method, promptly update Group Policy for all affected users and computers so that the application is reinstalled before it can get out of sync. Be prepared for a surge in network traffic as the computers reinstall the application from the network. When a client computer is out of sync with the software distribution point, Windows might prompt users for an installation CD and refuse to install the updated version. To resolve this condition, try logging off or restarting the computer, or use a local administrator account to uninstall the application and then reinstall it using Group Policy. You can also use the Install This Application At Logon setting when assigning applications to users.

Another way to update applications using Group Policy is to make a copy of the administrative install or folder in the software distribution point containing the setup files. Update this copy and then add the updated application to the GPO as an upgrade to the existing application. This enables existing clients to continue to access the original installation files.

<table>
<thead>
<tr>
<th>Can the user remove the software?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Published Applications</td>
</tr>
<tr>
<td>Yes, by using Add/Remove Programs (Reinstallation is also supported.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What package types are supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Published Applications Assigned to Computers</td>
</tr>
<tr>
<td>Windows Installer packages and .zap files</td>
</tr>
</tbody>
</table>

* By default, Windows XP clients process Group Policy asynchronously as a background refresh during startup and logon, which shortens startup times but requires two restarts to install assigned software to computers, or two logons to install software to users. For more information, see the “Windows XP Takes Two Restarts or Logons to Install Assigned Applications” sidebar in the “Setting Software Installation Options” section of this chapter.

### Table 28-3 Differences between publishing and assigning deployed applications

<table>
<thead>
<tr>
<th>Published Applications</th>
<th>Applications Assigned to Users</th>
<th>Applications Assigned to Computers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can the user remove the software?</td>
<td>Yes, by using Add/Remove Programs (Reinstallation is also supported.)</td>
<td>Yes, although the software becomes available again after the next logon event</td>
</tr>
<tr>
<td>What package types are supported?</td>
<td>Windows Installer packages and .zap files</td>
<td>Windows Installer packages</td>
</tr>
</tbody>
</table>

* By default, Windows XP clients process Group Policy asynchronously as a background refresh during startup and logon, which shortens startup times but requires two restarts to install assigned software to computers, or two logons to install software to users. For more information, see the “Windows XP Takes Two Restarts or Logons to Install Assigned Applications” sidebar in the “Setting Software Installation Options” section of this chapter.
until Windows applies the GPO and upgrades the application. When using this method, copy the original GPO and use the copy for testing and pilot deployment. (Make sure that the copy has a lower link order than the original so that Windows applies it instead of the original.) Once you verify that the upgrade works properly, disable the original GPO (and eventually delete it).

Whichever method is used to update applications, test the method thoroughly in a lab before implementing it on a production network, and perform pilot deployments of updates or staged rollouts to mitigate risk.

Setting Up the Group Policy Software Installation Extension

Before deploying software using Group Policy, create a shared folder or DFS folder to store the setup files, and create a GPO for application deployment, as discussed in this section.

Creating a Software Distribution Point

To deploy applications using Group Policy, first create a software distribution point on the network that contains the setup files for the applications. (Make sure you have volume licenses for the applications.) The best way to do this is to create a folder structure in DFS. This allows you to alter the location of the software distribution point without breaking application deployment, add multiple folder targets for load balancing, and set up WAN-friendly replication, as discussed in Chapter 20.

To create a software distribution point, use the following steps:

1. Design and create a DFS or shared folder structure for software.

   Create a DFS folder that contains other DFS folders that categorize software. The second (or third) level of DFS folders usually contains DFS folders with folder targets that store the actual installation files. For example, the DFS folder that contains the Microsoft Office 2003 setup files might be `\example.local\Software\Productivity\Microsoft Office 2003`, with the `\Srv2\Software\Productivity\Microsoft Office 2003` folder target.

2. Set the following NTFS permissions on the software distribution folder. (Set the share permissions to Everyone = Full Control to prevent conflicting file and share permissions.)

   - Authenticated Users = Read
   - Domain Computers = Read
   - Administrators = Full Control
Important Permissions that are incorrectly set are among the most common causes of problems when deploying software via Group Policy, so verify that file and share permissions are set properly on the software distribution folder.

3. Copy the application setup files to the software distribution point, or use an administrative setup command to install the setup files to the software distribution point. Consult the software manufacturer for specific instructions and recommendations.

   For example, to install Microsoft Office 2003 to a software distribution point, type D:\Setup.exe /A Pro11.msi, substituting D:\ with the drive letter of the Office CD and Pro11.msi with the .MSI package appropriate for your version of Office. Do not simply copy the setup files.

   Note To publish the software distribution folder in Active Directory so that users can find the folder when searching Active Directory for shared folders, right-click the appropriate container in the Active Directory Users and Computers console, choose New, select Shared Folder, and then type the path of the DFS folder or shared folder in the Network Path box.

Creating a GPO for Application Deployment

Before adding or administering deployed applications, create a new GPO for the applications. To do so, follow these steps:

More Info For more information about Group Policy, the Group Policy Object Editor, and the Group Policy Management Console, see Chapter 11.

1. Install the Group Policy Management Console, if necessary, and then open the Group Policy Management Console from the Administrative Tools folder on the Start menu.

2. Create a new GPO, and then link it to the appropriate site, domain, or organizational unit (OU).

3. Use the Security Filtering section to apply the GPO to the appropriate groups of users or computers, as shown in Figure 28-1.
Figure 28-1  The Group Policy Management Console

**Note**  Do not unlink or delete a GPO immediately after using it to uninstall applications; Windows applies the policy when users log on or restart their computers, so if you unlink or delete the GPO before these events occur, Windows does not uninstall the applications.

**Real World  Planning Ahead**

Use the following list to help plan software deployment via Group Policy:

- To deploy applications to certain groups, create multiple GPOs and use the Security tab to apply each GPO only to the appropriate group. Or change the security settings for individual programs within a GPO so that only the appropriate groups have access to the applications (as discussed later in this chapter).

- Assign GPOs as high up in the Active Directory tree as possible. If all users in a domain need Microsoft Word and Microsoft Excel, put those applications in a GPO that applies to that domain, not in a separate policy for each OU.

- Test software deployment in a lab, and use OUs to pilot software deployment in a production network. For example, create a GPO and test it in a single OU. If the GPO functions properly, unlink it from the OU and link it to the appropriate domain. (Do not assign or publish the same applications to the same users or computers in multiple GPOs.)
■ Modify quotas to allow users enough disk space to install applications, and leave room for the temporary files created during software installations.

■ Enable Group Policy Results, formerly known as Resultant Set Of Policies (RSoP), on Windows XP Service Pack 2 clients by enabling the Windows Firewall: Allow Remote Administration Exception Group Policy setting. This enables you to remotely check which GPOs Windows has processed on clients. For more information, see Chapter 11.

Configuring the Group Policy Software Installation Extension

A number of options control how Group Policy deploys and manages software packages. These options determine how packages are added to the GPO, the amount of control users have over an installation, and the default application for a given file extension, as well as which categories you can use for grouping applications. The following sections cover these options in detail.

Note Software Installation settings for applications deployed to users are not shared with applications that are deployed to computers. Each type of deployment maintains its own set of applications and settings.

Setting Software Installation Options

To change the default settings for the Group Policy Software Installation extension, first open the Software Installation Properties dialog box by performing the following steps:

1. Open the appropriate GPO, select either User Configuration or Computer Configuration, Software Settings, and then Software Installation.

2. Right-click the Software Installation container, and then choose Properties. The Software Installation Properties dialog box appears.

After completing these steps, use the Software Installation Properties dialog box to perform the following tasks:

■ To specify the default location for application packages, type the UNC path of the software distribution folder in the Default Package Location box of the General tab. This path must be a Uniform Naming Convention (UNC) name; it cannot be a direct reference to a local drive. To reduce the potential for name resolution problems, use a fully qualified Domain Name System (DNS) name—for example, \srv1.example.local\software.

■ To change the default action to perform on new packages, use the New Packages area of the General tab, as discussed in Table 28-4.
To uninstall applications automatically when the GPO no longer applies to the user or computer, select the Uninstall The Applications When They Fall Out Of The Scope Of Management check box on the Advanced tab (which is shown in Figure 28-2).

Important Choosing the Uninstall The Applications When They Fall Out Of The Scope Of Management check box can lead to a user inappropriately losing an important application. For example, if a GPO is applied by site and a laptop user travels to a branch office, the user might lose software if the branch office’s GPOs do not include the same software applications. To avoid this, be careful when choosing this option and, if possible, do not deploy software by site.
To allow 64-bit Windows clients to install 32-bit Windows Installer applications, select the Make 32-Bit X86 Windows Installer Applications Available To Win64 Machines check box. To allow 64-bit clients to install applications published using a .zap file (as discussed in the “Finding the Right Mix of Services” section earlier in this chapter), select the Make 32-Bit X86 Down-Level (ZAP) Applications Available To Win64 Machines check box. Note that you cannot deploy applications written for x64 editions of Windows on Itanium-based versions of Windows, and vice versa.

To change which application Windows installs to open files of a given format, click the File Extensions tab, select a file extension from the Select File Extension list, select the default application for the extension, and then click Up to move it to the top of the list. Windows lists only the file extensions associated with packages already present in the GPO.

To set up a list of software categories, making it easier for users to find the application they want, click the Categories tab, click Add, and type the category name. Categories apply to the entire domain, not just the Group Policy object with which you are working.

### Real World  Windows XP Takes Two Restarts or Logons to Install Assigned Applications

By default, Windows XP clients use the Fast Logon Optimization feature to process Group Policy asynchronously during startup and logon, which shortens startup times. However, because this means that Windows processes Group Policy in the same way as a background refresh, Windows requires two restarts to install assigned software to computers, or two logons to fully install or remove assigned packages assigned to users.

To apply a Group Policy to a computer or user without two restarts or logons, open a command prompt window, type Gpupdate, and then log off or restart the computer. To force Windows XP clients to always process Group Policy synchronously like Windows 2000 clients, open the appropriate GPO; select Computer Configuration, Administrative Templates, System; and then select Logon. Then enable the Always Wait For The Network At Computer Startup And Logon policy. For more information, see Microsoft Knowledge Base Article 305293.
Changing Software Installation Behavior over Slow Links

Group Policy by default considers all connections slower than 500 Kbps (kilobits per second) to be slow links. When Windows detects a slow link, it disables logon and startup scripts, software installation, folder redirection, and disk quotas. To change the connection speed Windows considers slow, use the following procedure:

1. Open the appropriate GPO, select Computer Configuration or User Configuration, and then Administrative Templates, followed by System, and finally Group Policy.

2. In the details pane, double-click the Group Policy Slow Link Detection policy setting (shown in Figure 28-3). The Group Policy Slow Link Detection Properties dialog box appears.

3. Choose the Enabled option and then type the connection speed to define as slow. Enter 0 to disable slow link detection, forcing Group Policy to consider every connection a LAN connection.

Besides changing what speed Group Policy considers slow, you can enable or disable the processing of the following policy items over a slow network link:

- Internet Explorer Maintenance Policy Processing
- Software Installation Policy Processing
- Folder Redirection Policy Processing
- Scripts Policy Processing
Working with Packages

After creating the GPO and the general software installation options, you can start working with software packages—the setup files for a software application. The following sections help you add packages to the GPO, change their properties, upgrade and modify packages, and remove obsolete packages.

Adding a Package to a Group Policy

Before Group Policy can assign or publish applications that you copy to the software distribution point discussed earlier in this chapter, you must add the installation packages to the GPO. To add a package to a GPO, follow these steps:

1. Install the application to the software distribution point using an administrative setup command or by manually copying the setup files, as discussed in “Creating a Software Distribution Point” earlier in this chapter.

2. Open the appropriate GPO, select either User Configuration or Computer Configuration, and then Software Settings.

3. Right-click Software Installation, choose New and then Package.

4. Select either Windows Installer Package or ZAW Down-Level Application Packages (zap) from the Files Of Type list, depending on the type of application you want to deploy. (Note that you can deploy .zap files only to users, not computers.)

Real World Not All Windows Installer Packages Work with Group Policy

Not all Windows Installer packages work properly with Group Policy. However, many companies provide Windows Installer Packages designed for use with Group Policy to licensed customers upon request. For example, Adobe and Macromedia both provide instructions on how to extract or obtain the appropriate files to deploy Adobe Reader and Macromedia Flash Player using Group Policy.
5. Type the path to the DFS folder or shared folder that stores the package you want to deploy, click Open, select the package, and then click Open again. Do not use a local file path.

**Note** You can use Group Policy to assign Windows operating system upgrades to computers or publish a Windows upgrade to users. To do so, first verify that each computer in the GPO has sufficient disk space and is compatible with the version of Windows you want to deploy. Then copy the entire Windows CD-ROM to the software distribution point and add the Winnt32.msi package to the appropriate GPO, just like any other piece of software. After adding the package, modify the package or GPO security settings so that the upgrade applies only to the appropriate computers or users.

6. In the Deploy Software dialog box (shown in Figure 28-4), choose from the following options how to deploy the package and then click OK:

- Select Published to publish the application in Active Directory with the default settings (available only with User Configuration).
- Select Assigned to assign the application with the default properties.
- Select Advanced to modify how Windows deploys the application. (The next section describes the deployment options.)

**Figure 28-4** The Deploy Software dialog box

**Note** Windows deploys packages after the second logon or restart for Windows XP clients, after the first logon or restart for Windows 2000 clients, and after the first logon or restart if you enable the Always Wait For The Network At Computer Startup And Logon policy. For more information, see the “Windows XP Takes Two Restarts or Logons to Install Assigned Applications” sidebar earlier in this chapter.
Creating .Zap Files for Earlier Applications

To publish an application that does not provide a Windows Installer package (a setup file containing the .MSI file extension), you can repackage the application as described later in this chapter or you can create a .zap file.

A .zap file is a text file that points to the setup program for an earlier application. To create a .zap file, type the following text, replacing the file and computer names as necessary:

```
[Application]
FriendlyName="Your Application's Name"
SetupCommand="\servername\sharename\foldername\setup.exe"
```

Many installers permit the recording or creation of installation scripts, which can then be used to automatically install the program after setup is launched by the zap file. To do this for a program that uses InstallShield to install, use the following procedure:

1. Run the program’s setup followed by the \r parameter (for example, Setup.exe /r).
2. Walk through the setup, keeping mindful of the fact that each choice is recorded in the installation script.
3. Locate the Setup.iss file that is created in the \Winnt or \Windows folder, and copy it to the subfolder of the distribution folder where the application is stored.
4. Use the following setup command in the .zap file to launch the installation file using the newly created setup script: Setup /R /F1:“C:\Temp\Setup.iss”, replacing Setup.iss with the filename for the setup script.

For more information about using .zap files, see Microsoft Knowledge Base Article 231747. For more information about scripting program installations, go to the support Web site for the installer program (InstallShield, Wyse, and so on), and perform a search for “silent install.”

Changing Application Properties

After you add a software package to a GPO, you might want to change the package’s application category, deployment type (assign or publish), or security settings.
To do so, double-click the software package in the Software Installation node of the Group Policy Object Editor console. The Properties dialog box appears, as described in the following list:

- To change the name of the package and support information, use the General tab.
- To assign the application or publish it, use the Deployment Type area of the Deployment tab (shown in Figure 28-5).

![Figure 28-5](image_url)  
*Figure 28-5  The Deployment tab of a software package's Properties dialog box*

- To automatically install the application when a user opens a file associated with the program, select the Auto-Install This Application By File Extension Activation check box on the Deployment tab.
- To prevent users from installing or uninstalling the application from Add/Remove Programs, select the Do Not Display This Package In The Add/Remove Programs Control Panel check box on the Deployment tab.
- To completely install the application the first time users log on after the application is assigned to them, select the Install This Application At Logon check box on the Deployment tab. This option allows clients with intermittent network connectivity (such as laptop users) to get the whole application when they log on rather than the first time they launch the program, which might occur when they’re offline.
To show users a limited amount of information about the installation progress, select Basic in the Installation User Interface Options section of the Deployment tab. To display all screens and messages to the user, select Maximum.

To make a 32-bit application available on 64-bit versions of Windows, uninstall previous installations of the product, or force Group Policy to ignore language settings when deploying the package, click Advanced on the Deployment tab.

To assign the application to a category, click the Categories tab, select a category, and click Select. You can assign an application to more than one category.

To allow only certain groups or users access to the program, use the Security tab.

Applying Package Upgrades

You can use Group Policy to automatically upgrade software packages. For example, when you get a new version of an application, publish it as both an upgrade and a full installation (for those without an earlier version of the application) so that users can upgrade to it if they want. Later, assign the application to users, and require them to either upgrade or install the new version in parallel with the old version (if you make that option available). You can also prevent new installations of the old version. After all users are accustomed to the new version, remove the old software package and uninstall it from users’ systems to complete the transition.

Use the following procedure to install upgrades. See the “Removing and Redeploying Packages” section later in this chapter for information about how to complete the process and remove obsolete packages.

Note You can apply a transform to the upgrade package—for example, to allow Microsoft Outlook 2000 users to upgrade to Microsoft Outlook 2003 without installing the rest of Office 2003. To do this, see the next section, “Applying Package Modifications.”

1. In the console tree of the appropriate GPO, select either User Configuration or Computer Configuration and then Software Installation.

2. After adding the upgrade package (if necessary), right-click the upgrade package (not the older version), and choose Properties from the shortcut menu.

3. Click the Upgrades tab and then click Add (unless the older application was automatically detected and listed here). Windows automatically detects older packages located in the same GPO.
4. In the Add Upgrade Package dialog box (shown in Figure 28-6) select the package to upgrade from the list of packages provided, and choose whether to uninstall the existing package before installing the new package (which might discard user’s settings). Click OK when you are finished.

![Add Upgrade Package dialog box](image)

Figure 28-6  The Add Upgrade Package dialog box

**Note**  Select the Uninstall The Existing Package, Then Install The Upgrade Package option when a real upgrade is not possible (in the case of upgrading to a different application) or desirable (when the upgrade process works poorly). Also select this option when upgrading a repackaged application.

5. Select the Required Upgrade For Existing Packages check box to require users to upgrade to the new package. (Otherwise, users have a choice to not upgrade.)

6. Click OK. Windows applies the upgrade package after the second logon or restart for Windows XP clients, or after the first logon or restart if you enable the Always Wait For The Network At Computer Startup And Logon policy or for Windows 2000 clients. (For more information, see the “Windows XP Takes Two Restarts or Logons to Install Assigned Applications” sidebar earlier in this chapter.)

**Applying Package Modifications**

Package modifications, also called *transforms*, customize an installation package without completely re-authoring it. For example, instead of offering Microsoft Office only in its complete configuration, you can deploy a package with only Microsoft Word and Microsoft Outlook.
Because transforms are merely a way to modify a package for deployment, not a mechanism for allowing a single package to present multiple options to users and administrators, you still need to add the package multiple times—once for each transform configuration available to users. For example, to deploy Office in its entirety, first deploy the standard Office .MSI package. Then deploy transforms of this installation to allow users to quickly select a customized installation of Office.

To create a customized installation of Office, use the Custom Installation Wizard (Ork.exe) included in the Microsoft Office 2003 Editions Resource Kit tools and available for download at http://www.microsoft.com/office/orkarchive/2003ddl.htm. To add a transform, first create the transform (this process varies by program), and then follow these steps:

1. Open the appropriate GPO, select either User Configuration or Computer Configuration, and then Software Settings.
2. Right-click Software Installation, choose New and then Package.
3. Type the path to DFS folder or shared folder that stores the package you want to deploy, click Open, select the package, and then click Open again. Do not use a local file path.
4. Choose the Advanced option in the Deploy Software dialog box, and then click OK.

**Note** If the Deploy Software dialog box does not appear, select the Display The Deploy Software Dialog Box option in the Software Installation Properties window, as described in the "Setting Software Installation Options" section of this chapter.

5. Click the Modifications tab and then click Add.
6. Use the Open dialog box to select the Windows Installer transform package to add.

**Important** As soon as you click OK, Windows immediately deploys the package, potentially affecting a lot of users. If you realize you made a mistake after clicking OK, you can fix it either by upgrading the incorrectly configured package with a correct one or by removing the package from Active Directory and all users.

7. On the Modifications tab, add or remove any additional transforms and place them in the proper order, using the Move Up and Move Down buttons, as shown in Figure 28-7. Windows applies the transform at the bottom of the list last, and therefore this transform takes precedence over earlier transforms because it can overwrite files written by earlier transforms.
Review all tabs of the Properties dialog box to ensure that the settings are correct, and then click OK when you are finished.

**Removing and Redeploying Packages**

When an application outlives its usefulness in your company, it is time to remove it from all systems—or at least to stop deploying it on new systems. There are also times when you might want to reinstall an application on all clients, such as after adding a software update. Use the following steps to perform these tasks:

1. Open the appropriate GPO, select either User Configuration or Computer Configuration, and then Software Settings.

2. Right-click Software Installation, choose New and then Package.

3. Right-click the application you want to remove or redeploy, and choose All Tasks from the shortcut menu.

4. To redeploy the application, reinstalling it on all systems that already installed it, choose Redeploy Application. To remove the application, choose Remove from the submenu.

5. In the Remove Software dialog box, shown in Figure 28-8, choose the first option to remove the software immediately from all computers. Or choose the second option to prevent new installations of the software while allowing existing users to continue using it and to perform repairs.
Chapter 28  Managing Software  923

Using Software Restriction Policies

Software restriction policies can be used in two ways:

- To prevent users from running specific applications. This corresponds to the default policy of Unrestricted and is useful for typical users and computers.
- To lock down systems so that users can run only applications that you specifically allow. This corresponds to the default policy of Disallowed and is useful for low-security user accounts, Terminal Servers, and public kiosks.

Software restriction policies are not a substitute for antivirus programs or firewalls. Imprudentially used, they can add significantly to the workload of administrators and Help desk personnel and seriously irritate end users. So employ software restriction policies only when the increased security or reliability benefit outweighs the added administrative burden, and when extensive testing indicates that the policies do not adversely affect users.

How Software Restriction Policies Work

Software restriction policies provide two security levels for programs—unrestricted, which allows programs to run, and disallowed, which blocks programs from executing. Use the following types of rules to control which programs to allow or disallow:

- **Hash rules**  Identify software by the unique characteristics of files, translated into an algorithmic hash. This is useful for identifying a specific version of a program because each version has a unique hash, even if a user renames or moves it.
Certificate rules  Identify software by its digital signature. This is useful for scripts you digitally sign. (You can block all scripts that do not contain an approved digital signature.)

Path rules  Identify software by file path or registry location. This is useful for controlling programs, scripts, and viruses that are always located in a specific location or named a certain name.

Internet zone rules  Identify Windows Installer (.MSI) packages downloaded from various locations. This is useful for controlling from which Internet Explorer zones (Trusted Sites, Intranet, and so on) users can download and install programs.

Default rule  Applies to all software not identified by a rule. Usually this is set to Unrestricted, but you can set it to Disallowed to block all unidentified software from running (though this can partially cripple a system if you don’t create rules for every program needed by users and Windows itself).

Because there are usually multiple rules within a software restriction policy, Windows processes rules in the order listed above. (When conflicting rules apply to the same program, the more specific rule wins.) Windows downloads software restriction policies with other Group Policy Objects during Windows startup or user logon, and it checks software restriction policies each time a user starts a program.

Note  Software restriction policies do not apply to programs that use the common language runtime (the .NET Framework) because they are controlled separately using the Code Access Security Policy. Software restriction policies also do not apply to drivers, programs run by the SYSTEM account, and Microsoft Office macros. You must update Windows XP to Service Pack 1 or newer for software restriction policies to work with 16-bit applications.

Creating Software Restriction Policies

To create a software restriction policy, use the following steps:

1. Create and open a new GPO for the software restriction policy. (This makes it easy to disable.) To apply the policy to only a single computer, open the computer’s Local Security Policy instead.

Note  Do not modify the default domain policy—leave it unchanged so that you have a pristine GPO to fall back to. Also, avoid linking a GPO containing software restriction policies to a different domain from which it resides—doing so can lead to poor program start times.
2. In the console tree, select User Configuration or Computer Configuration, and then Windows Settings, followed by Security Settings, and finally Software Restriction Policies (shown in Figure 28-9).

![Figure 28-9 The Software Restriction Policies container](image)


4. Specify the default rule by selecting the Security Levels container, right-clicking the appropriate security level, and then choosing Set As Default from the shortcut menu.

   **Important** If you set the default security level to Disallowed, create path rules to allow all locations from which Windows runs login scripts, and do not delete the default path rules or change them to Disallowed. Doing so can inadvertently prevent users from logging on by blocking the execution of key Windows programs. When using the Disallowed security level, set the Apply Group Policy permission of the GPO to Deny for the Domain Admins group, pay attention to any application dependencies, and test the policy extensively in a lab. The Disallowed setting increases your workload, because every new program and many updates require changes to the software restriction policy. If you inadvertently lock yourself out, restart the computer in Safe Mode, log on as a local Administrator and then change or disable the software restriction policy.

5. Create rules to identify software. To do so, right-click the Additional Rules container and then choose one of the following options:

   - **New Certificate Rule** Select the certificate to require or block.
   - **New Hash Rule** Select the file to allow or block.
New Internet Zone Rule  Select the Internet Zone from which you want to permit or block program installation.

New Path Rule  Select or type the path to allow or block. Use the existing registry path rules as a guide for creating path rules that reference registry keys.

6. Double-click the Enforcement item in the Software Restriction Policies container to specify how to enforce the policies. Select the All Software Files Except Libraries option to reduce the risk of inadvertently blocking key files and to reduce the performance impact of the policy. Select the All Users Except Local Administrators option to allow local administrators to get around software restriction policies. (Local administrators can defeat software restriction policies anyway with a small amount of effort.)

7. Double-click the Designated File Types item to control which file types are included in the software restriction policies. Most of the essential types are listed, though you can add Perl (.PL) or another file type to the list, depending on what is in use on the network.

8. Double-click the Trusted Publishers item to control whether End Users, Local Computer Administrators, or Enterprise Administrators are allowed to determine which certificates are trusted when opening ActiveX controls or other digitally signed programs.

Note  When blocking access to system utilities, make sure to create a path rule that blocks the System File Protection cache folder (%SystemRoot%\System32\DLLCache), where Windows stores backup copies of system utilities.

Remote Installation Services
Remote Installation Services (RIS) is a Windows Server 2003 service that enables users to boot a bare-metal, functioning or nonfunctioning computer from the network and install Windows in a small number of simple steps. You can use RIS with the IntelliMirror technologies (User Settings Management, User Data Management, and Software Installation) to install Windows and then automatically add a user’s personalized work environment—complete with the user’s computer settings, software applications, and data.

This capability can come in handy. For example, you might want to purchase a new computer and give it to an existing user, or recycle an old server as a desktop. Using RIS and IntelliMirror, simply boot the computer from the network, log on and select the appropriate operating system image, which is then installed automatically. When a user logs on
for the first time, Windows downloads settings and applications from the network, minimizing setup time and effort.

The sections that follow describe how RIS works, how to determine whether the network meets the requirements for RIS, and how to install and use RIS to set up client systems.

More Info  RIS is not the optimal Windows deployment technology for all scenarios. For information about choosing the best deployment methods for a network, see Chapter 5. For more in-depth information about RIS, see the Windows Server 2003 Deployment Kit, available on the Microsoft Web site at http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx.

How RIS Works

The following steps occur when installing an operating system using RIS:

1. The user or administrator turns the client computer on.

2. The client computer performs its power on self-test (POST) sequence and then uses a network card with Preboot Execution Environment (PXE) support (or the Remote Boot Disk) to obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server on the local subnet.

3. All RIS servers on the local subnet that receive the client computer’s DHCP request broadcast examine the globally unique identifier (GUID) of the client (also known as the universally unique identifier UUID), and then search Active Directory for a prestaged computer account with this GUID.

More Info  See the “Prestaging a Client” section of this chapter for information about prestaged computer accounts.

- If the RIS servers find a computer account with the client computer’s GUID, or if the RIS servers are configured to respond to unknown client computers, the RIS servers query Active Directory to determine whether a particular RIS server is assigned to the client. If so, that server handles the request; if not, the first RIS server to respond handles the request.

- If the RIS servers do not find a computer account with the client computer’s GUID and the RIS servers are configured to reply only to known client computers, the client computer request fails.

4. After the client computer receives a response from the RIS server, it uses the Trivial File Transfer Protocol (TFTP) to download Startrom.com.
5. Startrom.com prompts the user to press F12 to start the computer from the network. After pressing F12, the client computer uses TFTP to download the Client Installation Wizard pages from the RIS server.

   **Note** To start client computers from the network automatically without pressing F12, rename Startrom.com to Startrom.bak, and rename Startrom.n12 to Startrom.com. However, do not do this if the network adapter is listed first in the BIOS boot order of the client computers. Instead, list the hard drive first so that when the drive is blank the computer starts from the network adapter, but subsequently starts from the hard drive.

6. After the user authenticates with Active Directory by logging in, RIS uses Group Policy to determine which pages to display.

7. After the user selects an operating system image, RIS restarts the computer in text-mode Windows Setup, repartitions and formats the hard drive, and then proceeds with Setup using the RIS server as the installation source.

---

**Under the Hood  Single Instance Storage**

RIS servers install the Single Instance Store (SIS) service, which monitors the volume or partition on which the Remote Installation folder is located for duplicate files. If SIS detects a duplicate file, it creates an NTFS reparse point for the duplicate file and then deletes the file, greatly reducing the storage requirements for storing multiple operating system images, without affecting functionality (which is similar to the way Remote Storage works).

---

**Supported Versions of Windows**

RIS servers running Windows Server 2003 can deploy the following versions of Windows:

- Windows Server 2003 R2, Standard Edition (32 bit and 64 bit)
- Windows Server 2003 R2, Enterprise Edition (32 bit and 64 bit)
- Windows Server 2003 R2, Datacenter Edition (32 bit and 64 bit)
- Windows Server 2003 R2, Web Edition (32 bit and 64 bit)
- Windows Server 2003, Standard Edition (32 bit and 64 bit)
RIS Requirements and System Recommendations

You can install RIS on any server running Windows Server 2003 or Windows 2000 server that is a member of a properly functioning Active Directory forest. Use the following guidelines to ensure adequate RIS server performance:

- Place one or more RIS servers on each network segment that has RIS clients. RIS is not slow-link aware and relies on DHCP broadcasts that routers might not forward, so avoid deploying Windows over a WAN connection using RIS. If you have multiple sites, deploy one or more RIS servers to each site.

- In environments where administrators centrally install large numbers of systems using RIS, create a build lab with an appropriate level of physical security and a dedicated high-speed network to maximize performance and security and to minimize impact on the production network.

- Use one RIS server for every 75 simultaneous RIS clients at most. RIS ignores additional PXE client requests in most circumstances.

- Use dedicated RIS servers in high-volume environments. If a RIS server becomes overloaded, it might affect any other services running on the server, such as DHCP. See Chapter 5 for information about sizing a server.


- Create a separate NTFS partition or use a separate physical disk or RAID subsystem with a minimum of 2 GB of free disk space (and 10 GB is better) for operating system images.
Do not use Encrypting File System (EFS), mount points, or DFS folder targets in the Remote Installation folder.

Do not use multiple network interface cards (NICs) on the RIS server.

**Note** You can use DFS Replication to replicate images and answer files from one RIS server to another, though you must manually specify RIS settings on each server. To replicate images, create a replication group for the Images folder (for example E:\Reminst\Setup\English\Images). See the “Creating a Multipurpose Replication Group” section of Chapter 20 for more information.

RIS clients also need to meet or preferably exceed the minimum system requirements for the operating system. In addition, the systems require a 10-Mbps or preferably 100-Mbps wired NIC that supports PXE remote boot or is explicitly supported by the remote boot disk. (See the “Creating a Remote Boot Disk” section later in this chapter for more information.)

**Note** 3Com 3C905 series network cards might generate unnecessary broadcast traffic in Windows if the BOOTP ROM chip is installed (which is necessary for PXE support). If you use these cards with the BOOTP ROM chip installed and see a decrease in network performance, use Network Monitor to determine whether the cards are generating unnecessary BOOTP/DHCP broadcasts. If they are, replace the affected network cards or pull the BOOTP ROM chips after installing Windows.

**Installing RIS**

After choosing the RIS server, use the following procedure to install the service and run the initial setup wizard:

1. Open Add/Remove Programs from Control Panel, and then click Add/Remove Windows Components in the left pane to launch the Windows Components Wizard.

2. Select the Remote Installation Services check box, and then click Next to install it. Restart the server when prompted.

3. Launch Remote Installation Services Setup from the Administrative Tools folder using a user account that is a member of the Enterprise Admins group or has delegated permissions.

4. On the Remote Installation Folder Location page, type the folder path to use as the root for the RIS operating systems. The path cannot be on the system partition, and it must be an NTFS 5–formatted unencrypted partition or volume with enough free
disk space for all the installations. You cannot use a DFS folder target either, although you can use DFS Replication to replicate the Remote Installation folder.

5. On the Initial Settings page, select the Respond To Client Computers Requesting Service check box to enable RIS immediately and optionally select the Do Not Respond To Unknown Client Computers check box to prevent computers that do not already have a computer account in Active Directory from receiving an operating system installation.

This limits the amount of information that rogue clients can obtain about the RIS server, and it can help mitigate the risk of rogue servers when combined with pre-staged accounts that specify the RIS server. See the “Prestaging a Client” section later in this chapter for more information.

6. On the Installation Source Files Location page, type the path to the Windows installation files.

7. On the Windows Installation Image Folder Name page, type a name for the folder that stores this operating system image. The name cannot contain any special characters or spaces and must contain 39 characters or fewer. The total path cannot exceed 130 characters.

8. On the Friendly Description And Help Text page, type a user-friendly name and description for the operating system image. This is the description users see listed as an operating system choice when they boot from the network.

9. Review the settings on the next page, and then click Finish to set up the server. RIS configures a number of settings and copies the necessary files, and then the service starts, if you chose to enable it, allowing the server to begin serving client requests.


10. To install and configure RIS from a command prompt, you can use the **Risetup** command. For example use the following steps:

    a. Create an answer file for the Windows Components Wizard by creating a text file named `C:\Sysocmgr.ini` (for example) that includes the following text:

        `[Components]
        Reminst = On`

    b. Insert the Windows Server 2003 CD-ROM or connect to the Windows installation share, open a command prompt window, and then type the following command: `Sysocmgr /i:%WINDIR%\Inf\Sysoc.inf /u:C:\Sysocmgr.ini`
c. Create an answer file for the Remote Installation Services Setup Wizard by creating a text file named `C:\Risetup.ini` that includes the following text:

```
[Version]
Signature = "$Windows NT$"

[Risetup]
RootDir = "E:\RemoteInstall"
Source = "D:\"
Directory = "Windows_XP_Pro"
Description = "Windows XP Professional"
Screens = "Overwrite"
Architecture = "x86"
Language = "English"
```

d. Open a command prompt window and then type the following command:

```
Risetup /auto C:\Risetup.ini.
```

**Note** To use RIS to deploy Windows Server 2003 R2, you must perform some additional steps, as discussed in the “Adding a Windows Server 2003 R2 Image” section of this chapter.

### Administering RIS

The Remote Installation Services Setup Wizard sets basic options and installs a single operating system image. To deploy additional operating systems or to change settings, use the following sections.

**Note** You can use DFS Replication to replicate images and answer files from one RIS server to another, though you must manually change RIS settings on each server. To do so, use the “Creating a Multipurpose Replication Group” section of Chapter 20 to create a replication group for the Images folder (for example, `E:\Reminst\Setup\English\Images`).

### Changing RIS Settings

To change RIS settings, view RIS clients, or verify the functionality of a RIS server, open the Active Directory Users and Computers console, right-click the server hosting RIS, choose Properties, and then click the Remote Install tab. Then use the following list to decide which options you should use:

- **Verifying Server Functionality** To quickly check the status of a RIS server and attempt to fix any problems, click Verify Server or type `Risetup /check` in a command prompt window to start the Check Server Wizard. Click Finish on the last page of the wizard to start or unpause the Remote Installation service if it is stopped or paused, or click Cancel to leave the service in its current state.
Note: The Check Server Wizard checks only that the RIS server is installed properly. It does not check the integrity of any operating system images on the server or the ability of clients to reach the server across the network. If you experience any problems, check the server’s event log and check the functionality of the DHCP, DNS, and Active Directory services.

- **Enabling or Disabling RIS** To enable the RIS server to respond to client requests, select the Respond To Client Computers Requesting Service check box. To prevent the RIS server from responding, clear the check box.

- **Ignoring Unknown Client Computers** To prevent computers that do not already have a computer account in Active Directory from installing an operating system using RIS, select the Do Not Respond To Unknown Client Computers check box. This limits the amount of information that rogue clients can obtain about the RIS server, and it can help mitigate the risk of rogue servers when combined with pre-staged accounts that specify the RIS server. See the “Prestaging a Client” section later in this chapter for more information.

  Ignoring unknown clients is also necessary if there is another remote boot/installation program on the network.

- **Viewing Clients** To view a list of clients that have used the server to install Windows or that are prestaged to install Windows from the server, click Show Clients.

- **Changing How RIS Names Computer Accounts** To change how RIS creates computer names (perhaps to match your computer naming convention), click Advanced Settings, and then use the Generate Client Computer Names Using box in the Remote-Installation-Services Properties dialog box, as shown in Figure 28-10, or click Customize to create your own computer name format, as shown in Figure 28-11.

  By default, RIS creates a computer name by appending a number to the user name of the account used to log on to Active Directory during the client installation. The user account used to log on during client installation must have sufficient permissions to create a computer account in the appropriate Active Directory container unless the system is prestaged, as described in “Prestaging a Client” later in this chapter.

Note: You can combine several fields when defining a computer-naming format. For example, the string %1First%10Last%# yields computer names using the first letter of a user’s first name and then 10 characters from the user’s last name, followed by a number—for example, JSMITH11. This yields a NetBIOS-compliant computer name that is easily readable by legacy clients such as Windows NT and Windows 98.
Changing Where RIS Creates Computer Accounts  To change where RIS creates computer accounts, click Advanced Settings on the Remote Install tab, and then use the Client Account Location section of the Remote-Installation-Services Properties dialog box to specify where to create the clients' computer accounts:

- To create the clients' computer accounts in the default Active Directory location (the Computers container in the RIS server's domain), select the Default Directory Service Location option on the New Clients tab.
To create the computer accounts in the same place in Active Directory as the user’s user account (probably the Users container), select the Same Location As That Of The User Setting Up The Client Computer option.

To manually specify a location in Active Directory for the computer accounts, select The Following Directory Service Location, and then click Browse and locate the appropriate container. Click OK when finished.

Changing Client Group Policy Settings

You can regulate the level of control users have over RIS installations by using Group Policy. To do so, use the following procedure. (Note that you can also apply permissions to individual operating system images, as discussed in the “Managing Operating System Images” section later in this chapter.)

1. Create and link a new GPO to the appropriate domain or OU that contains the RIS users. Make sure that the link order for the GPO takes precedence (is lower) than the Default Domain Policy.

2. In the Group Policy Object Editor, select User Configuration, and then Windows Settings, followed by Remote Installation Services, and finally double-click Choice Options.

3. Enable, disable, or leave unconfigured the following client installation choices, which appear during client setup after the user logs on:

   - **Automatic Setup**  The easiest installation option, this option checks the GUID of the computer to see whether it has been prestaged, and if so, it keeps the previously created computer account. Otherwise, it creates a computer name based on the naming convention specified by the RIS server (as described earlier in this chapter) without prompting the user.

   - **Custom Setup** This option provides users the ability to specify the computer name and the location within Active Directory used to store the computer account. When this option is enabled, administrators can prestage a client computer by using the Client Setup Wizard and canceling on the last page before beginning Windows Setup, after RIS creates the managed computer account.

   - **Restart Setup** This option allows RIS to restart a failed setup attempt using the information already provided by the user (if applicable), without attempting to fix setup problems. For example, if the user typed her full name during the failed setup attempt, RIS would not prompt the user again, if possible.

   - **Tools** This option displays any maintenance tools installed for network boot clients.
Important  Do not enable Custom Setup in a GPO that applies to end users when you are going to prestage the computers, because it presents the possibility of the users creating duplicate computer accounts if the GUID, computer name, and Active Directory location they choose do not exactly match those created when prestaging the computers.

Managing Operating System Images
Managing the operating systems available for install using RIS involves a few different tasks, such as adding operating system images, customizing existing images with answer files, and changing permissions and settings for existing images, as discussed in the following sections.

More Info  For information about adding device drivers, service packs, or software updates to the Remote Installation folder, see the “Creating and Modifying a Distribution Share” section of Chapter 5.

Adding CD-Based Images
To use a Windows CD-ROM or installation source to add a Setup-based operating system “image” to a RIS server (not to be confused with a disk image solution such as that used by RIPrep), use the following procedure:

1. Open the Active Directory Users and Computers console.
2. In the applicable domain and OU, right-click the server hosting RIS, choose Properties, and then click the Remote Install tab.
3. Click Advanced Settings, and then click the Images tab (as shown in Figure 28-12).
4. Click Add, select Add A New Installation Image on the New Answer File Or Installation Image page of the Add Wizard, and then click Next. The Remote Installation Services Setup Wizard appears.

Note  You install RIPrep images from the computer you create the image on, and you do so at the time you create the image. For more information, see the “Using Remote Installation Preparation” section later in this chapter.
5. On the Installation Source Files Location page, type the path to the \i386 or \amd64 folder.

6. On the Windows Installation Image Folder Name page, type a name for the folder to store this operating system image. The name cannot contain any special characters or spaces and must contain 39 characters or fewer. The total path cannot exceed 130 characters.

7. On the Friendly Description And Help Text page, type a user-friendly name and description for the operating system image. This is the description users see listed as an operating system choice when they boot from the network.

---

**Note** To enable clients to install support for multiple languages, copy the contents of the \i386\Lang folder (and all subfolders) from the Windows CD-ROM to the \RISServerName\RemoteInstall\Setup\clientlanguage\Images\imagename\i386\Lang folder. (Use the \amd64\Lang folder for x64-based images.) To enable multiple languages during client setup, replace the Welcome.osc file on the RIS server with an appropriately modified and renamed Multilng.osc, and create Client Installation Wizard pages for any additional languages. For more information, see the Windows Server 2003 Deployment Kit, available on the Microsoft Web site at [http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx](http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx).
8. If the Previous Client Installation Screens Found page appears, choose whether to keep the existing client installation screens or overwrite them with the client installation screens provided by the operating system you are adding (even if they are older than the existing screens).

Keep the screens associated with the newest version of Windows you deploy, unless you make customizations to the client installation screens, in which case select Use The New Client Installation Screens, And Rename The Old Ones With A .bak Extension to make backup copies of the existing screens that you can later integrate with the newer screens.

Real World  Client Installation Screens for x64 Editions of Windows

Clean installations of Windows Server 2003 R2 and Windows Server 2003 with Service Pack 1 include the X8664.osc screen that enables users with x64-based computers to choose between x64 and x86 versions of an operating system. To enable this screen on a RIS server upgraded to Windows Server 2003 Service Pack 1 or Windows Server 2003 R2, add an x64-based Windows image and choose to overwrite the existing screens. Do not overwrite these newer screens with those of an older version of Windows, such as Windows XP Service Pack 2. Doing so disables or deletes the X8664.osc screen.

To force all new x64 RIS clients to see only x64 images, or only x86 images, use the following registry key: HKLM\System\CurrentControlSet\Services\BINLSVC\Parameters. Set the DefaultPlatformforX8664 value to "amd64" or "i386". For more information, see Microsoft Knowledge Base Article 891128.

1. On the Review Settings page, click Finish to add the image to RIS.

2. To start the Add Installation Wizard from a command prompt, open a command prompt window and then type Risetup /Add. To automate the Add Installation Wizard, use the Risetup /Auto command with an answer file. For example, use the following steps:

   a. Create (or edit) an answer file for the Remote Installation Services Setup Wizard by creating a text file named C:\Risetup.ini (for example) that includes the following text:

      [Version]
      Signature = "$Windows NT$"
b. Open a command prompt window and then type the following command:
   `Risetup /auto C:\Risetup.ini`.

**Note** To use RIS to deploy Windows Server 2003 R2, you must perform some additional steps, as discussed in the “Adding a Windows Server 2003 R2 Image” section of this chapter.

**Adding a Windows Server 2003 R2 Image**

To add a CD-based Windows Server 2003 R2 image to a RIS server, add a Windows Server 2003 with Service Pack 1 CD-Based image to the RIS server, and then modify the image to install Windows Server 2003 R2 automatically. No special steps are needed to create a Windows Server 2003 R2 RIPrep image.

To add a CD-based Windows Server 2003 R2 image to a RIS server, follow these steps:

1. Add a Windows Server 2003 with Service Pack 1 CD-Based image to the RIS server, as described in the previous section. This image must be of the same platform, edition, and language as the Windows Server 2003 R2 image you want to add.

2. Copy the `\Cmpnents` folder from Windows Server 2003 R2 Disc 2 into the existing Windows Server 2003 with Service Pack 1 RIS image at the same level as the `\i386` or `\amd64` folder—for example, `E:\RemoteInstall\Setup\English\Images\WindowsServer2003R2Enterprise\Cmpnents`.

3. Create a copy of the RIS answer file (Ristndrd.sif by default), and add the following lines:
   ```
   [GUIRunOnce]
   "Cmd /C \%SERVERNAME%\Reminst\%INSTALLPATH%\Cmpnents\R2\Setup2.exe /Q /A"
   ```

4. Associate the new RIS answer file with the image (as described in the next section).
Forcing RIS to Log On Automatically

When installing a CD-based Windows Server 2003 R2 image using RIS, Windows installs Windows Server 2003 with Service Pack 1, disables the local Administrator account, and then stops. Disabling the local Administrator account is more secure than setting a shared Administrator password for all computers that use the plaintext RIS answer file. You cannot encrypt the Administrator password and use the Autologon feature.

After an administrator logs on using an account that is a member of the Domain Admins group, Windows Server 2003 R2 Setup runs automatically from the [GUIRunOnce] section of the answer file.

To force RIS to logon automatically using the local Administrator account, install Windows Server 2003 R2, disable the local Administrator account for proper security, and then restart, use the following steps:

1. Open the answer file and type a semicolon in front of the following line so that RIS does not disable the local Administrator account during Setup:
   
   DisableAdminAccountOnDomainJoin=1

2. Add the following lines to the [GuiUnattended] section so that RIS logs on automatically without prompting for a password:
   
   AdminPassword = "Password"
   AutoLogon = Yes
   AutoLogonCount = 1

3. Add the following [GuiRunOnce] section, where Install@example.local is the name of a limited security domain account with Read And Execute permissions to the Remote Installation share, Password is the password for the user account, and EXAMPLE is the name of the domain. This section authenticates with the Remote Installation share, runs Windows Server 2003 R2 Setup, disables the local Administrator account, and then restarts the computer.

   [GUIRunOnce]
   "Cmd /C Net Use \%SERVERNAME%\Reminst /User:Install@example.local Password"
   "Cmd /C \%SERVERNAME%\Reminst\%INSTALLPATH%\Components\R2\Setup2.exe /Q /A"
   "Cmd /C WMIUserAccount Where 'Name='Administrator' And Domain!=EXAMPLE' Set Disabled=True" "Cmd /C Shutdown -R -T 0"

Adding Unattended Answer Files to Existing Images

Answer files are small text files that provide answers to the questions asked by a program such as Windows Setup. Answer files can completely automate the Windows setup process, partially automate the process, or merely provide default settings.
Create additional answer files for RIS images by making copies of the existing answer files and then modifying the copies using the same techniques as for a standard Unattend.txt answer file (which are discussed at length in Chapter 5). After customizing an answer file, associate it with an operating system image in RIS. The answer file then appears as a new operating system image, both on the RIS server and to RIS clients, although very little additional disk space is consumed (just a couple of kilobytes for the answer file). The answer file simply modifies how clients use an existing image.

**Under the Hood  The Default Ristndrd.sif and RIPrep.sif Answer Files**

When adding an operating system image to a RIS server, RIS creates an answer file called Ristndrd.sif (or Riprep.sif in the case of RIPrep images) located in the `\RISServerName\RemoteInstall\Setup\Clientlanguage\Images\Image-name\i386\Templates` folder. Ristndr.sif automates the setup process after the Client Installation Wizard completes, except for prompting the user for the Product Key. To eliminate this prompt, add the following line to the `[UserData]` section of the answer file, replacing the Xs with the appropriate volume license product key:

```
ProductKey = "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
```

To use individual product keys automatically, you must use the Windows Management Instrumentation (WMI) Windows Product Activation (WPA) provider. See the Microsoft Developer Network (MSDN) Web site at [http://msdn.microsoft.com](http://msdn.microsoft.com) for more information.

If the user account used to authenticate with the RIS server during the Client Installation Wizard does not have a first and last name (as is typical for the Administrator account), another prompt appears during Setup asking for the user’s first and last name. To avoid this, prestage the computer account and instruct the end-user to perform the installation, add a first and last name to the appropriate administrator account, or hard code the first and last name into the answer file using the `FullName` parameter of the `[UserData]` section.

RIS also includes the Rinorprt.sif answer file, which is identical to the Ristndr.sif answer file except for the `Repartition = No` line in the `[RemoteInstall]` section, which instructs Setup not to repartition the hard drive.

To associate an answer file with an existing image on a RIS server, use the following procedure:

1. On the Images tab of the Remote-Installation-Services Properties dialog box (shown in Figure 28-12), click Add. The Add Wizard appears.
2. On the New Answer File Or Installation Image page, select Associate A New Answer File To An Existing Image.

3. On the Unattended Setup Answer File Source page, choose whether to use a sample answer file provided by Windows (Ristndr.sif or Rinorprt.sif), an answer file from another RIS server, or an answer file in another location.

4. On the Select An Installation Image, select the operating system image to which you want to apply the answer file.

5. On the Select A Sample Answer File page that appears when you choose to use a sample answer file, choose the default answer file (Ristndr.sif) or the “no repartition” answer file (Rinorprt.sif).

6. On the Select A Remote Installation Server page that appears when you choose to use an answer file from another RIS server, specify the RIS server that contains the answer file.

7. On the Select An Answer File To Copy page that appears when you choose to use an answer file from another RIS server, select the appropriate answer file.

8. On the Friendly Description And Help Text page, type a user-friendly name and description for the operating system image. This is the description users see listed as an operating system choice when they boot from the network.

9. On the Review Settings page, click Finish to associate the answer file to the appropriate operating system image.

10. To add an answer file to an existing image from a command prompt, copy the answer file to the \i386\Templates and/or \amd64\Templates folder of the operating system image. For example, type the following command:

    Copy E:\R2ris.sif \Srv4\Reminst\Setup\English\Images\WindowsServer2003R2Enterprise\i386\Templates\English\Images\WindowsServer2003R2Enterprise\i386\Templates\English\Images\WindowsServer2003R2Enterprise\i386\Templates\

**Setting Permissions for Images**

To control which groups of users can install an operating system image using RIS, use the following procedure to modify the security settings for the answer file associated with an operating system image:

**Note** The default permissions for the Remote Installation folder (usually \Reminst) allow members of the Authenticated Users group to perform installations, and members of the Administrators group to administer operating system images and answer files. The \Reminst share permissions grant Everyone Full Control, but the folder permissions supersede the share permissions.
1. Right-click the Remote Installation folder (usually \Reminst) in Windows Explorer, choose Properties, and then use the Security tab to set the appropriate general permissions for RIS:
   - Set the Read & Execute, List Folder Contents, and Read permissions to Allow for a group to enable members of the group to use RIS. Remove a group to prevent members of the group from using RIS.
   - Set the Full Control permission to Allow for a group to enable members of the group to administer RIS. Do not remove the System group.

2. On the Images tab of the Remote-Installation-Services Properties dialog box, select an operating system image from the list and then click Properties.

3. Click Permissions and then click the Security tab, as shown in Figure 28-13.

4. Set the Read permission and the Read & Execute permission to Allow for a particular group to enable members of the group to see this answer file in the Client Installation Wizard. Remove a group to prevent members of the group from seeing this answer file.

![Figure 28-13  The Security tab](image)

**Note** To delegate the ability to manage operating system images (such as adding answer files and controlling access to the images) to a group, grant the group Full Control permissions for the \Images folder or appropriate subfolder.
Changing Image Properties
To rename operating system images, change their descriptions, or remove operating system images from a RIS server, on the Images tab of the Remote-Installation-Services Properties dialog box, select an operating system image from the list, click Properties and then use the following list:

- To view or change the friendly description and help text associated with an image, select the image and click Properties. You can also see whether the image is CD-based (flat) or RIPrep-based here.
- To remove an unattended answer file associated with an operating system image, select the image to remove and click Remove. (Make a copy of the answer file first so you don’t lose it.)

**Note**  When removing an operating system from the list, RIS deletes the answer file for the image but leaves the actual installation files intact. To delete the installation files, open Windows Explorer and delete the physical folder containing the operating system image.

Adding RIS Tools
RIS provides the ability to add tools to a RIS server that client computers can download and execute over the network. One invaluable tool to add to a RIS server is Microsoft Windows PE. Start Windows PE from a RIS server and then use it to prepare the hard disk, perform hardware diagnostics, and run utilities. To obtain Windows PE, see the Microsoft Volume Licensing Web site at [http://www.microsoft.com/licensing/programs/ sa/support/winpe.mspx](http://www.microsoft.com/licensing/programs/sa/support/winpe.mspx).

**Note**  To maximize RIS server scalability when using Windows PE, use a Windows Server 2003 RIS server and add a Windows PE 2005 or newer RAM disk image instead of a CD-based image. When using a RAM disk image, the client computer downloads the RAM disk image and then releases its connection with the RIS server, allowing the server to service more clients.

In addition to Windows PE, there are RIS “menu editors” that allow adding your own tools in the form of a boot image that downloads from the RIS server. This is useful for adding disk imaging programs to the Maintenance And Troubleshooting Tools page of the Client Installation Wizard, for example. Two companies that make RIS menu editors are Argon Technology ([http://www.argontechnology.com](http://www.argontechnology.com)) and emBoot Inc. ([http://www.emboot.com](http://www.emboot.com)).
Using Remote Installation Preparation

The Remote Installation Preparation (RIPrep) Wizard allows you to create a Windows installation complete with applications and settings, image it, and then deploy it using RIS. This technique is similar to using the System Preparation (Sysprep) tool in combination with a third-party disk-imaging program. However, using RIPrep has a couple of advantages, such as built-in imaging and distribution software and greater tolerance for different hardware; and it has a couple disadvantages, such as slower performance and reliance on network adapters with PXE boot capabilities. For more information about the relative merits of RIPrep images, see Chapter 5.

**Important** Install the operating system and all applications and files in a single boot partition on the C drive of the reference computer. RIPrep does not support multiple partitions.

**Real World  RIPrep Cautions**

Make sure the BIOS on both the reference system and the RIS clients have up-to-date Advanced Configuration Power Interface (ACPI) support. RIPrep does not support mixing systems with different hardware abstraction layers (HALs), such as ACPI, Standard PC, uniprocessor, and multiprocessor. You cannot include encrypted files in a RIPrep image.

Additionally, certain desktop shortcuts might not work properly on RIS clients made from RIPrep images. For example, the Microsoft Outlook 2000 desktop shortcut does not work after a RIPrep RIS installation unless you disable 8.3 name creation on the reference computer before running RIPrep. To do this, change the \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystems\NtfsDisable8dot3NameCreation registry key from 0 to 1. For more information, see Microsoft Knowledge Base Article 250642.

To create an operating system image using RIPrep, follow these steps:

1. Add a CD-based image of the operating system to the RIS server. The CD-based image must be of the same language, version, and SKU as the operating system you want to image using RIPrep, but it does not need to be the same service pack level.

2. Install Windows on the reference system, preferably using RIS. Create a single disk partition and make it only large enough to accommodate the operating system and any applications you install. During client setup, RIS uses the size of the reference system’s C partition to determine the required disk space for the Windows installation, and later expands the disk partition to fill the entire disk.

3. Install any applications that do not use Windows Installer.
4. Install any Windows Installer applications by using Group Policy, as described earlier in this chapter. This permits you to manage these applications through Group Policy after the RIS setup process installs Windows on client systems. (Make sure to apply the same GPOs to both the reference computer and the computers that eventually install Windows using the RIS image; otherwise, the software you install might be immediately uninstalled.)

Note: Install applications from a permanently accessible location such as a DFS folder so that if an application needs to use the setup files again, it can do so without prompting the user for a CD-ROM.

5. Change the system settings as appropriate—for example, by changing the color scheme or desktop settings. To save the profile settings, copy the profile into the Default User profile. (See the sidebar “Copying User Profiles” for more information.)

6. Delete any local user accounts that you do not want to copy to RIS client computers, and delete any extra user profiles.

Copying User Profiles

To configure the default settings for users of computers deployed using a RIPrep image, use the following steps to copy the user profile you modified to the Default Users profile:

1. Log on with an administrator account (probably an account that is a member of the Domain Admins group), and change the system settings as appropriate.

2. Create a local administrator account.

3. Log on using the new local administrator account.

4. Open the System tool in Control Panel, click the Advanced tab, and then click Settings in the User Profiles section.

5. Select the account with the settings to copy and then click Copy To.

6. In the Copy To dialog box, type the path of the Default User profile and then click Change.

7. In the Select User Or Group dialog box, select the local computer, and then specify the Everyone group.

8. Log off, log back on using the original administrator account, and then continue creating the RIPrep image.

To test the user profile, log on using a different user account (such as another domain account). The settings specified should propagate to the new profile automatically.
7. Close all applications, and stop all nonessential services running on the system.

8. Run Riprep.exe from the RIS server’s \RemoteInstall\Admin\i386 folder. The Remote Installation Preparation Wizard appears.

9. On the Server Name page, type the name of the RIS server on which to store the image.

10. On the Folder Name page, type a name for the folder that will store this operating system image.

11. On the Friendly Description And Help Text page, type a user-friendly name and description for the operating system image. This is the description users see listed as an operating system choice when they boot from the network.


13. On the Stop Services page, review the list of services that must be stopped before the Remote Installation Preparation Wizard can image the system. When you click Next, the Remote Installation Preparation Wizard attempts to stop these services automatically.

14. On the Programs Or Services Are Running page, review the list of programs or services that the Remote Installation Preparation Wizard cannot stop, and then close these applications or stop these services manually using the Services MMC snap-in and Task Manager, if necessary.

15. Review the information presented after the image is created, and then click Next to copy the image to the RIS server. When this process is complete, the system shuts down.

After installing the RIPrep image on a new computer, Mini-Setup runs, prompting the user for a Product Key and his name before preparing the computer for use. To eliminate these prompts, see the “The Default Ristndrd.sif and Riprep.sif Answer Files” sidebar, earlier in this chapter.

---

**Note** When installing clients from a RIPrep image, RIS partitions the hard disk into one large partition on the first disk. If you prefer, RIS can create a partition on the first disk that is exactly the same size as the image partition and leave the rest of the disk unpartitioned. To do this, change the setting of the UseWholeDisk key in the Riprep.sif file from Yes to No. This file is located in the \RISServerName\RemoteInstall\Setup\clientlanguage\Images\imagename\i386\Templates folder.
Performing User Installations

After setting up the RIS servers, you can start deploying Windows to computers that meet the requirements for RIS (as discussed in the “RIS Requirements and System Recommendations” section of this chapter). This section describes how to prestage a client computer, create a remote boot disk, and perform a client installation using RIS.

Prestaging a Client

Prestage a client by creating a managed computer account in Active Directory. A managed computer account is simply an account associated with the client system’s globally unique identifier (GUID) or universally unique identifier (UUID), which are unique to every network card and not as susceptible to theft by rogue clients as Media Access Control (MAC) Layer addresses are.

Prestaging client computers has the following benefits:

- Helps protect a RIS server against rogue clients when combined with the Do Not Respond To Unknown Clients setting.
- Helps protect RIS clients against rogue servers when combined with specifying in the managed computer account the RIS server to which the client computer can connect.
- Enables users who do not have permissions to create computer accounts to use the Client Setup Wizard (when you grant the appropriate group permission to join the computer account to the domain, as discussed below).
- Ensures that the computer name complies with the organization’s computer naming conventions.

Note Many original equipment manufacturers (OEMs) will provide a spreadsheet containing a list of GUIDs for the computers you purchase. Use this list in conjunction with the sample scripts included in the Microsoft Windows Server 2003 Deployment Kit (available on the Microsoft Download Web site at http://www.microsoft.com/downloads) to prestage a large number of computers simultaneously.

There are two ways to prestage a client computer. The easiest way to prestage a computer is to boot the client computer into the Client Installation Wizard (as discussed later in this chapter), logon using an Administrator account, select an operating system image, and then power off the computer when the Installation Information page appears that displays the computer account name and GUID. This creates a managed computer account for the computer and joins it to the domain, but it does not install Windows. A user can use RIS later to install an operating system on the computer without requiring permissions to create a computer account or join the account to the domain, because these tasks are already complete.
You can also prestage a client from a server, which eliminates the need to touch the client computer. To do so, follow these steps:

1. Open the Active Directory Users and Computers console.
2. Open the domain or OU in which you want to create the new computer account.
3. Right-click the container in which you want to store the computer account, choose New, and then Computer.
4. On the New Object – Computer page (shown in Figure 28-14), type the name for the computer and, if necessary, a 15-character or shorter version of the name so that Pre-Windows 2000 clients can access the computer.

![Figure 28-14 Assigning a name to a new computer account](image)

5. Click Change and then use the Select User Or Group dialog box to specify who can use this computer account during the Client Installation Wizard to install Windows and join the domain. This does not grant the specified user or group permissions to create or add other computer accounts.

**Important** Prestaging a client computer does not automatically enable users to perform the RIS installation—you must explicitly grant the appropriate group permission to join the computer to the domain when creating the computer account. Otherwise, users receive an Access Denied message during the Client Installation Wizard.

6. On the Managed page, select the This Is A Managed Computer check box, and then type the GUID for the computer in the Computer's Unique ID box, as shown in Figure 28-15.
7. On the Host Server page, choose whether you want the client to use the first RIS server to respond to the client request or a specific server. Specifying a server helps reduce the risk of the client computer connecting to a rogue RIS server created by an attacker on the internal network.

8. On the New Object—Computer page, review the settings and then click Finish to create the computer account.

Figure 28-15 Typing a GUID for a managed computer account

Real World Working with GUIDs

RIS uses a computer’s GUID to keep track of client computers. The GUID comes from the PXE ROM on PXE-enabled network cards or from the network card’s MAC address when you boot with the Remote Boot Disk. (In this instance, it is the MAC address with 20 zeros appended to the beginning of the address.) The computer manufacturer often writes the GUID on a sticker located on or inside the computer’s case. It can also be located inside the system BIOS.

If you have trouble finding the GUID, there are a number of ways to locate it. The first way is to make a WMI query for the UUID property of the Win32_ComputerSystemProduct class. You can do this from a command prompt by typing Wmic /Node: “Computername” CProduct Get UUID, where Computername is the name of the appropriate computer.

You can also set up a RIS server configured to answer all RIS client requests on a private subnet. Then connect any clients to prestage and have them perform a network boot, log on, and select an OS image. Just before the client performs the Windows installation, the Client Installation Wizard displays a summary page with the computer account name and GUID. At this point, the client is prestaged in Active Directory as long as the RIS server used is part of the Active Directory. Write down the GUID for reference.
Creating a Remote Boot Disk
If a client computer does not have a NIC that is PXE remote-boot compatible, you need to create a remote boot disk to use RIS. To do so, follow these steps:

1. Place a blank, 1.44-MB floppy disk in the computer's floppy drive.
2. Connect to the RIS server, and launch Rbfg.exe from the server's \RemoteInstall\Admin\i386 folder.
3. In the Microsoft Windows Remote Boot Disk Generator dialog box, select the floppy drive.
4. To view a list of network cards supported by the remote boot disk, click Adapter List.
5. Click Create Disk to create the disk.

Performing a Remote Operating System Installation
The actual process of installing an operating system remotely is easy, and you might choose to have users perform it themselves. To perform a remote OS installation, go to the client system and follow these steps:

1. If using a boot disk, place it in the floppy drive.
2. Turn on or restart the computer, and then set the appropriate boot order in the system BIOS, as described here:
   - If the hard disk is blank, set the BIOS to boot from the hard disk first and the Network second. This enables you to automatically boot into the Client Installation Wizard by renaming the Startrom.n12 file on the RIS server to Startrom.com, eliminating the press F12 prompt.
   - If the hard disk has an existing operating system that you want to overwrite, set the BIOS to boot from the Network first and the hard disk second (or third), or disable the boot partition on the client computer by typing the following commands from within Windows PE, Windows Server 2003, or Windows XP Professional Service Pack 1 or later:
     ```
     Diskpart
     Select Disk 0
     Select Partition 1
     Inactive
     Exit
     ```
3. Press F12 when prompted to boot from the network. The Client Installation Wizard appears.
4. On the Logon page of the Client Installation Wizard, type a valid user name and password for the domain.
If you did not prestage the computer, use an account with sufficient privileges to create a new computer account. If you prestaged the account from a server but did not delegate permission to join the computer account to the domain, use an account with sufficient privileges to join the computer account to the domain.

**Security Alert** An attacker that succeeds in creating a rogue RIS server on the network could use the Client Installation Wizard to harvest user names and passwords. To mitigate this risk, prestage computer accounts and specify a known RIS server for each account, take appropriate steps to physically secure the network, and check the server name on the Logon page to verify that you connect to a valid RIS server.

5. On the Main Menu page, choose Automatic Setup, Custom Setup, Restart A Previous Setup Attempt, or Maintenance And Troubleshooting Tools, and then press Enter.

   Some or all of these options might not be available depending on the Group Policy settings that apply to the user. For more information about these settings, see the “Changing Client Group Policy Settings” section of this chapter.

6. If you choose to perform a custom setup, on the Custom Setup page type the computer name and directory service path to use for the computer account.

7. On the OS Choices page, choose the image to install.


9. On the Installation Information page, optionally write down the computer’s account name and GUID and then press Enter, or turn off the computer to complete Setup later. At this point, the computer is staged (or prestaged if you complete Setup later).

   Windows then installs automatically, pausing only for a user name and CD-key (unless you added this information to the answer file, as described earlier in this chapter). If installing Windows Server 2003 R2, the final step of Setup (Windows Server 2003 R2 Setup) takes place after you logon to the server for the first time and Windows executes Setup2.exe from the [GUIRunOnce] section of the answer file.
Summary

Windows Server 2003 provides several useful tools for managing software. You can use the Software Installation component of Group Policy to deploy applications to computers on the network. The Software Restriction Policies component of Group Policy makes it possible to control which applications and scripts users can execute. Finally, RIS makes it easy to perform automated clean installations of Windows over the network, reducing the time it takes to set up new computers for employees or reuse old computers.
Chapter 29

Application Compatibility and Virtual Server

Virtual Server Overview ................................................................. 955
Installing Virtual Server .............................................................. 956
Configuring Virtual Server .......................................................... 961
Creating Virtual Machines ......................................................... 967
Administering Virtual Server ....................................................... 978
Alternatives to Virtual Server ...................................................... 979
Summary ...................................................................................... 980

Many IT professionals need to support legacy or specialized applications in their environment that require an older operating system, such as Windows NT4, or one that is not generally used by the rest of the company, such as a version of UNIX. Many of these specialized or dedicated applications run on older servers that could not be easily replaced in the event of a hardware failure. By consolidating them onto a newer server but running them in a virtual machine environment, the overall maintenance and supportability is improved.

Another critical application compatibility need is the testing of new applications or patches to existing applications before they are deployed across the company. Few IT professionals have the luxury of a completely segregated and isolated test environment with all the possible configurations and environments that they need to support and test against.

Virtual Server Overview

Microsoft Virtual Server is a virtualization application that creates a virtual hardware environment that can support multiple virtual machines running multiple operating systems on the same physical hardware. The physical server is called the “host” and each virtual operating system is called a “guest.” Guest operating systems can be any operating system that runs on standard x86 hardware, including UNIX, Linux, MS-DOS, Microsoft Windows 3.1, Windows 9x, Windows NT, or any of the currently shipping and supported 32-bit Windows operating systems.
Virtual Server presents each guest operating system with an entirely segregated and isolated virtual environment that simulates the necessary hardware for the guest operating system to run. The guest has no awareness of being in a virtual environment and is fully supported running under Virtual Server.

Virtual Server is an ideal environment for testing new applications and patches to existing applications. You can create multiple guest virtual machines on a single server, and test the new application under carefully controlled and isolated conditions that accurately reflect your real network conditions, without having to have many dedicated machines to support.

Virtual Server is also a great tool for testing new technologies, such as clustering, in a controlled environment and without having to actually buy expensive clustering hardware until you’re sure everything will work as you expect.

### Installing Virtual Server

Virtual Server 2005 R2 can be installed on any 32-bit version of Windows Server 2003, and on x64 versions of Windows Server 2003. It can also be installed on Windows XP Professional Service Pack 2 and Windows XP Professional x64 Edition. It is not, however, supported for production use when installed on Windows XP.

**Note** The screen shots and steps used in this chapter were taken using a beta version of Microsoft Virtual Server R2.

### Installing Internet Information Services for Virtual Server

To install Virtual Server, you need to first install Internet Information Services 6.0 (IIS6) on either the host computer (the default) or on another computer with access to the machine that will host Virtual Server. This is because all configuration and maintenance of Virtual Server is done on the Virtual Server Administration Website. This Web site is created on the host machine by default, but if you need to configure Virtual Server to be administered from a separate computer you should follow the instructions in the Release Notes for Virtual Server. If you won’t be using IIS for any other Web functionality, you should just install the minimum components of IIS that are required for Virtual Server. These are: Common Files, Internet Information Services Manager, and World Wide Web Service. Installing these components will reduce the number of unnecessary services and attack surfaces on your server. If you already have IIS running somewhere on your network, do the installation of Virtual Server as a split installation.
To install IIS for Virtual Server, follow these steps:

1. Open Add/Remove Components, and select Add/Remove Windows Components to open the Windows Components Wizard, shown in Figure 29-1.

2. Highlight Application Server, and click Details.

3. Highlight Internet Information Services, and click Details.

4. Select Common Files and Internet Information Server Management.

5. Select World Wide Web Service, and click Details to open the World Wide Web Service page shown in Figure 29-2.
6. Select only World Wide Web Service and then click OK twice to return to the Application Server page. You should have Enable Network COM+ Access selected and Internet Information Services (IIS) partially selected, as shown in Figure 29-3.

![Figure 29-3](image)

Figure 29-3 The Application Server page, with the necessary selections for Virtual Server

7. Click OK one more time, and then click through the rest of the wizard to finish installing IIS.

If your intention is to only use IIS for management and configuration of Virtual Server, you should configure the Windows Firewall accordingly to block access to the default Web site, especially from any externally facing IP address.

**Performing the Installation**

To install Virtual Server, follow these steps:

1. Ensure that IIS is installed and started.

2. Start the Virtual Server 2005 installation program, setup.exe, from the CD or other installation point to bring up the Microsoft Virtual Server 2005 Setup Wizard shown in Figure 29-4.
3. Click Install Microsoft Virtual Server 2005, and then Accept the license agreement and click Next again.

4. Fill in the Customer Information dialog box, and click Next to bring up the Setup Type dialog box shown in Figure 29-5.

5. Choose Complete if you are installing Virtual Server on a computer that has IIS already installed.
6. If you are doing a split installation, choose Custom, and then change Virtual Server Web Application to This Feature Will Not Be Available, as shown in Figure 29-6.

![The Virtual Server Custom Setup dialog box](image)

**Figure 29-6** The Virtual Server Custom Setup dialog box

7. Click Next to bring up the Configure Components dialog box shown in Figure 29-7 (available with a complete install only).

![Configure the Administration Website components](image)

**Figure 29-7** Configure the Administration Website components

8. Click Next, and select Enable Virtual Server exceptions in Windows Firewall.

9. Click Next and then click Install to perform the actual installation.
10. When the installation completes, the Installation Summary page will be displayed, as shown in Figure 29-8. The exact contents of this page will vary, depending on exactly what components were installed.

![Installation Summary page](image)

Figure 29-8 The Installation Summary page

11. Note the location of the Installation Summary page for future reference, or add it to your Favorites. Finally, click Finish to close the installation program. No reboot is required.

### Configuring Virtual Server

Virtual Server is entirely configured from the Administration Website shown in Figure 29-9. When you first log on to this Web site, you’ll be prompted by the Windows Server 2003 Internet Explorer Enhanced Security Configuration. For simplicity, if you’ll be configuring Virtual Server from the server’s console, you should add the Web site to your Trusted Sites. You can also connect from your personal workstation by pointing Internet Explorer at `http://machinename:1024`, assuming you used the default port for the Virtual Server Web site.

By default, only members of the local Administrators group on the Virtual Server host machine have access to the Administration Website, and you’ll be prompted for credentials when you attempt to log on.
You can create virtual networks, virtual disks, and virtual machines from within the Web site. All the settings for individual machines and their virtual hardware are controlled from this Web interface. We’ll start by configuring our networks, and then setting some useful defaults before we actually create a virtual machine. While you can also preconfigure and create Virtual Disks, we prefer to create the disks when we are creating the virtual machine.

**Configuring Virtual Networks**

Virtual Server will create a virtual network card for each enabled physical network card it sees on the computer during initial installation, plus another virtual network card that is only for connecting to other virtual machines on the same physical computer. To see the list of available virtual network cards, log on to the Administration Website if you aren’t already logged on, and click Configure- and then View All in the Virtual Networks section of the leftmost frame of the Web site. This will display all the virtual network cards that are currently configured, as shown in Figure 29-10.
Figure 29-10  Viewing all the virtual networks

This is a nice feature because it lets you see what virtual networks you have. But you can’t actually change anything from this page. On the server xmpl-srv4, we see that there are three virtual networks defined—two external networks and the Internal Network. The Internal Network is not connected to any physical network card on the host server; rather, it is connected to a private, virtual network on the host that only other virtual machines can connect to.

Configuring the Internal Network
To configure the Internal Network, perform the following steps:

1. Click Configure, Internal Network under the Virtual Networks section of the left-most frame of the Administration Website to open the “Internal Network” Virtual Network Properties shown in Figure 29-11.
2. Click Network Settings to change the settings for this adapter. They’re not terribly interesting for the Internal Network.

3. Click DHCP Server to change the settings for the built-in Dynamic Host Configuration Protocol (DHCP) server, as shown in Figure 29-12. By default, the DHCP server is enabled for this network and uses a 10.237.0.0 network address.

![Configure the Internal Network DHCP Server](image)

4. Make any changes to the default DHCP settings and then click OK to save them. If you’ll be creating and assigning a DHCP role to one of your virtual machines on this network, you should disable this virtual DHCP server to avoid issues. Otherwise, it would be good to enter in the IP addresses of the DNS server or servers that will be created on the network, along with WINS servers, and a gateway if you will be configuring this network to connect to an outside network.

**Configuring External Networks**

To configure the external networks, follow these steps:

1. Click Configure, External Network under the Virtual Networks section of the leftmost frame of the Administration Website to open the External Network Virtual Network. If you have multiple physical network cards on the host computer, you’ll actually be choosing from multiple external networks, each with a very long name that describes the hardware.
2. Click Network Settings to open the Network Properties page shown in Figure 29-13.

![Image of Network Properties page]

**Figure 29-13** The Network Properties page

3. Give the virtual network a useful name that identifies it clearly, but that also is a bit easier to work with. You can also change the physical network card that this network is connected (bridged) to if you need to change the default. Add any administrative notes, and click OK to save the settings.

**Important** Always click OK to save your changes on any page in the Administration Website. If you navigate off the page without clicking OK, your changes will not be saved. There is no way to do several sets of changes together and then save them all at once.

**Configuring Server Properties**

There are two server properties that you can set for the host server to simplify management and creation of virtual machines. There are other settings for the server and Web
site we can set, but we’ll address them in the “Administering Virtual Server” section later in the chapter. The two settings we’ll worry about now are these:

- **Virtual Machine Remote Control**  A feature of Virtual Server that allows a remote connection directly to the virtual machine

- **Search Paths**  The path that Virtual Server will use to find resources and components it needs

**Enabling Virtual Machine Remote Control**

To enable Virtual Machine Remote Control, follow these steps:

1. Log on to the Virtual Server Administration Website if you aren’t already logged on.
2. Click Server Properties in the Virtual Server section of the leftmost frame.
3. Click Virtual Machine Remote Control (VMRC).
4. Select Enable to allow the VMRC client to be able to connect to virtual machines on this host.
5. Set the TCP/IP address. The default is All Assigned. If you have externally facing adapters on the host, you should specify only the internal adapter IP address to limit access to the virtual machines.
6. Set the Idle timeout. The default is enabled, and it times out after 15 minutes of inactivity. We find that a bit short for how we use Virtual Server, so we set it to 30 minutes.
7. Configure any other settings here you want to change, and then click OK to actually enable the changes.

**Setting Search Paths**

To set search paths, perform the following steps:

1. Log on to the Virtual Server Administration Website if you aren’t already logged on.
2. Click Server Properties in the Virtual Server section of the leftmost frame.
3. Click Search paths.
4. The default search path is in a bad place and would put all your virtual machines on the system drive by default. We suggest creating a SharedVirtualMachines folder on a different volume where you have plenty of space. Enter that folder path into the Default virtual machine configuration folder box.
5. You can also specify additional search paths that Virtual Server will use when it looks for CD, floppy, and hard drive images. When you’ve entered any additional paths you want to add, click OK to save the changes.
Creating Virtual Machines

Once you’ve got your Virtual Server environment set up and ready, it’s time to actually create a virtual machine (VM). The wizard will walk you through creating the virtual machine and let you make some basic choices. You can then adjust them as appropriate for your particular environment.

To create a basic Windows XP Virtual Machine, follow these steps:

1. Log on to the Virtual Server Administration Website if you aren’t already logged on.

2. Click Create in the Virtual Machines section of the leftmost frame to open the Create Virtual Machine page, shown in Figure 29-14.

3. Enter a name for the virtual machine. The name should be as descriptive as possible, especially if you’ll be running several different but similar virtual machines on the same host. The machine will be created in its own subfolder of the default shared virtual machine folder you specified previously. If you want this machine to be in a different location, specify a fully qualified path name to the location for the machine.

4. Enter the amount of RAM to make available to the virtual machine.

5. Specify the maximum size of the first hard disk for this virtual machine and the type of virtual hard disk to create (IDE or SCSI). If you already have a virtual hard disk you want to reuse, you can specify that instead of a new hard drive.

6. Specify the initial network adapter to connect to. You can add more network adapters later.
7. Click Create, the virtual machine will be created and added to the Master Status panel of the Administration Website, and you’ll see the status page for the virtual machine as shown in Figure 29-15.

![Figure 29-15 The status page for a newly created virtual machine](image)

### Initial Configuration of a Virtual Machine

When you first create a virtual machine, you’ll see the status page for that machine as shown in Figure 29-15. From here, you can start the virtual machine immediately or set additional configuration details for the machine before starting it. Some configuration details can be set only on virtual machines that are shut down, so now is a good time to take care of those items. The default settings are listed in Table 29-1.

<table>
<thead>
<tr>
<th>Property</th>
<th>Initial Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Properties</td>
<td>Don’t start automatically.</td>
</tr>
<tr>
<td></td>
<td>Save state when the virtual machine stops.</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Not installed by default.</td>
</tr>
<tr>
<td>Additions</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>Depends on the guest operating system.</td>
</tr>
<tr>
<td>Hard Disks</td>
<td>1 virtual IDE hard disk.</td>
</tr>
<tr>
<td></td>
<td>Automatically expands to 16 GB maximum size.</td>
</tr>
<tr>
<td>CD/DVD</td>
<td>1 virtual CD/DVD drive. Attached to the first physical CD/DVD drive in the host computer.</td>
</tr>
</tbody>
</table>
Capturing a Physical Device

Virtual machines use a combination of the existing physical hardware on the host machine and virtual hardware that is generated by Virtual Server. The default hard disks are examples of virtual hardware—they are created on the host’s hard disks as a simple file, but they appear to the virtual machine as a hard disk, with partitions, files, and folders on it. Using the physical devices of the host computer, however, requires that the device first be “captured” by the virtual machine. Once a device is captured by a virtual machine, it isn’t available for any other virtual machine until it is released from the first virtual machine.

Captures can be changed while a virtual machine is running, but you can’t add or remove devices. So you can capture the physical CD/DVD drive, for example, while the virtual machine is running, or change to capture an .ISO file, without having to stop and start the virtual machine. When a physical CD/DVD drive is captured, you can insert or remove CDs and DVDs and they will behave as you would expect on the virtual machine where the drive is captured.

Devices that can be captured include a CD/DVD drive, a floppy drive, COM ports, and LPT ports.

Table 29-1  Default Virtual Machine Settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Initial Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCSI Adapters</td>
<td>None, unless you specified a SCSI virtual hard disk.</td>
</tr>
<tr>
<td>Network Adapters</td>
<td>1 virtual network adapter, with a dynamic MAC address.</td>
</tr>
<tr>
<td>Scripts</td>
<td>Initially disabled.</td>
</tr>
<tr>
<td>Floppy Drive</td>
<td>1 virtual floppy drive, but not connected to any device</td>
</tr>
<tr>
<td>COM Ports</td>
<td>2 initial virtual COM ports. Not connected by default.</td>
</tr>
<tr>
<td>LPT Ports</td>
<td>1 initial virtual LPT port. Not connected by default.</td>
</tr>
</tbody>
</table>

Configuring CD/DVD

The default configuration for a virtual machine has a single CD/DVD drive attached to the master position on the second virtual IDE channel. This virtual CD/DVD drive is set to capture the first physical CD/DVD drive on the host machine. You can change this to capture a different physical CD/DVD if you have more than one CD/DVD drive on the host computer, or you can capture a CD or DVD image file. An image file, usually with the extension of .ISO, is an actual image of what the CD or DVD contains. It can be captured and used by Virtual Server just as if it were a physical CD or DVD drive. This is extremely useful for rapid access to operating system CDs, for example, where you have multiple VMs running different operating systems on the same host. You don’t need to have
physical access to the host computer to swap out CDs; just capture the appropriate .ISO file for the operating system used by that virtual machine.

To configure a Virtual CD/DVD Drive, perform the following steps:

1. Log on to the Virtual Server Administration Website if you aren’t already logged on.
2. Click Master Status in the Navigation section of the leftmost frame.
3. Highlight the virtual machine you want to configure the CD/DVD drive for, and select Edit Configuration, as shown in Figure 29-16.

![Figure 29-16 The action menu for a virtual machine](image)

4. The status page for the virtual machine will open. Click CD/DVD in the configuration section to open the CD/DVD Properties page for the virtual machine, as shown in Figure 29-17.

![Figure 29-17 The CD/DVD Properties page for a virtual machine](image)

5. Select No Media to release any existing captures. Select Physical CD/DVD Drive, and specify which physical drive to capture. Or select Known Image Files to specify the path to an .ISO file to capture.
6. If you’re capturing an .ISO image and it is on your search path (as described in the steps for setting search paths earlier in the chapter), you can select it from the drop-down list under Known image files, or you can enter the exact, fully qualified path name for the .ISO file you want to capture.

7. Click OK to capture the file.

Starting the Virtual Machine for the First Time

OK, you’ve got everything configured and ready to go, and you really want to create that first virtual machine. There are two ways to start the machine and install the operating system:

- Click the image of the virtual machine in the Master Status window.
- Connect directly to it with the Virtual Machine Remote Control (VMRC) client.

Personally, we like the second option that allows us to do it directly from our main desktop, but there are significant security implications if you’re not certain of who might be listening to your network. Definitely don’t use that method over a wireless connection from a remote machine, for example. The more usual method is to open the Virtual Server Administration Website and click the image of the target virtual machine. This will start the virtual machine and leave it as a thumbnail on the Master Status page. Choose Remote Control from the action menu to open the remote control page for a particular virtual machine—you’ll see your virtual machine running directly in the Web page, as shown in Figure 29-18.

![Figure 29-18 The Remote Control page for a virtual machine](image.png)
To connect to a Virtual Machine with VMRC, follow these steps:

1. Open the VMRC from the Start, All Programs, Microsoft Virtual Server menu to open the VMRC as shown in Figure 29-19.

![Figure 29-19 The Virtual Machine Remote Control client](image)

2. Enter the information for the virtual machine to connect to. You need to use the fully qualified host name, the port number (5900 by default) and the virtual machine name, as shown in Figure 29-19—for example: `vmrc://xmpl-srv4.example.local:5900/xmpl-xp-vm1`.

3. You'll be warned about the security implications with two separate messages, as shown in Figure 29-20, and Figure 29-21. Click Yes in each message box to proceed.
4. Finally, you’ll be prompted for credentials to connect to the remote host machine. Enter your credentials, and click OK to open the VMRC and connect to the virtual machine.

**Installing an Operating System**

Once your virtual machine starts, it behaves exactly like any other physical machine. You will see the standard power-on self test (POST) messages from the BIOS, the enumeration of your hard drives—including any SCSI devices—and the machine will boot from the available media. Follow the standard operating system installation instructions for your guest operating system.

---

**Note** To configure the BIOS settings on your virtual machine, including the boot priority, press the Delete key as soon as the virtual machine starts to open the AMI BIOS for the virtual machine. The default boot priority is Floppy, CD/DVD drive, PXE, and then the first hard drive.

---

**Installing SCSI Shunt Driver**

If you’re installing Windows Server 2003, Windows XP Professional, or Windows 2000 and you want to use a virtual SCSI hard disk, it can be installed without extra drivers, but it will be faster with the Virtual Machine SCSI Shunt drivers installed. To load these during the setup process, use the standard Windows technique of pressing the F6 key when the first blue installation screen is displayed. When prompted to specify additional drivers, go to the configuration screen for the VM, click Floppy drive, and select Known Floppy Disks, and then select the SCSI Shunt Driver from the drop-down list, as shown in Figure 29-22. Click OK to capture the floppy image.
Using Virtual Machine Remote Control

VMRC is an application you’ll love to hate. It is an essential tool for managing and configuring your virtual machines, but its behavior is not always as you’d expect or wish. Once you know its quirks, though, you’ll find it a useful tool. The basic keystrokes are the same whether you use the standalone VMRC or the ActiveX control in the Administration Website. The default key bindings are shown in Table 29-2.

<table>
<thead>
<tr>
<th>Function</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect to Server</td>
<td>Host+C</td>
</tr>
<tr>
<td>Connect to the Administrative Display</td>
<td>Host+A</td>
</tr>
<tr>
<td>Full Screen (Toggle)</td>
<td>Host+Enter</td>
</tr>
<tr>
<td>View Connection Properties</td>
<td>Host+I</td>
</tr>
<tr>
<td>View Only</td>
<td>Host+V</td>
</tr>
<tr>
<td>Change Host Key</td>
<td>Host+H</td>
</tr>
<tr>
<td>Switch to Next VM</td>
<td>Host+RightArrow</td>
</tr>
<tr>
<td>Switch to Previous VM</td>
<td>Host+LeftArrow</td>
</tr>
<tr>
<td>Release Mouse/Keyboard</td>
<td>Host</td>
</tr>
<tr>
<td>Send Ctrl+Alt+Del</td>
<td>Host+Delete</td>
</tr>
</tbody>
</table>
Probably the two most important keys in Table 29-2 are the Host key itself, which will release your keyboard and mouse when they’ve been captured by the virtual machine, and the Host+Delete combination that sends the Ctrl+Alt+Delete secure attention sequence (SAS) to the guest operating system. The need for the Host key to release your mouse and keyboard will go away once you actually get the operating system installed and can add the Virtual Machine Additions to it. Assuming, of course, that it is an operating system that has a set of Virtual Machine Additions to support it.

**Configuring Virtual Machines**

Once your virtual machine has been created and the operating system has been installed, there are several changes you can make to improve the functionality of Virtual Server and a particular VM. Some changes can be accomplished while the machine is running, and some can be accomplished or changed only while the machine is completely shut down.

**Configuring Running Virtual Machines**

Some features of a virtual machine can be modified while the virtual machine is running. Here are your options:

- Change the devices that are captured.
- Pause the virtual machine.
- Save the state of the virtual machine.
- Turn off the virtual machine.

The final option listed, turning off the virtual machine, is a lot like pulling the power cord on the virtual machine. This is usually not what you intended to do. We’ve already talked about capturing devices, so we won’t cover that option again here. Pausing the virtual machine is just like it sounds. When you pause a virtual machine, it stops using any of the available processing power of the host machine. It’s a lot like putting a laptop into standby mode. You don’t release any of the memory being used by the virtual machine, but it doesn’t actually do anything while it’s paused, nor does it require any processor cycles.

Save state is the virtual machine equivalent of hibernate on your laptop. It saves the current state of the virtual machine to your hard drive, and then frees up the memory it was using. When you restore your virtual machine from the saved state, it returns to exactly where it was when you saved the state.

**Important** Do not use save state on a domain controller. It can cause problems with replication in the domain.

If you have Undo Disks enabled, you have some additional options. For a full list of possible options for a running virtual machine, see Table 29-3.
Configuring Stopped Virtual Machines

All changes to the hardware configuration of a virtual machine have to be done while the machine is completely shut down. Hardware changes can be made even if undo information exists. But hardware changes can not be made when the virtual machine is paused or in a saved state.

The configuration options that you can change while a machine is stopped include the following:

- Add or remove a hard drive
- Add or remove a CD/DVD drive

### Table 29-3 Options for Running Virtual Machines

<table>
<thead>
<tr>
<th>Option</th>
<th>What the Option Does</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turn On</td>
<td>Starts the virtual machine (Power On).</td>
</tr>
<tr>
<td>Pause</td>
<td>Standby mode.</td>
</tr>
<tr>
<td>Resume</td>
<td>Resumes from Pause.</td>
</tr>
<tr>
<td>Save State</td>
<td>Hibernates the virtual machine.</td>
</tr>
<tr>
<td>Save and Commit Undo Disks</td>
<td>Hibernates the virtual machine, and merges the undo disk back into the main disk.</td>
</tr>
<tr>
<td>Save State and Keep Undo Disks</td>
<td>Hibernates the virtual machine, but maintains the undo status so that the virtual machine can be rolled back to its prior saved state.</td>
</tr>
<tr>
<td>Shut Down Guest OS</td>
<td>Tells the operating system to shut down.</td>
</tr>
<tr>
<td>Shut Down Guest OS and Keep Undo Disks</td>
<td>Tells the operating system to shut down, and does not merge the undo disks.</td>
</tr>
<tr>
<td>Shut Down Guest OS and Commit Undo Disks</td>
<td>Tells the operating system to shut down, and merges the undo disk, resulting in a complete shutdown.</td>
</tr>
<tr>
<td>Turn Off</td>
<td>Essentially pulls the plug on the virtual machine.</td>
</tr>
<tr>
<td>Turn Off Virtual Machine and Commit Undo Disks</td>
<td>Turns off the virtual machine immediately, and merges any undo information back into the parent.</td>
</tr>
<tr>
<td>Turn Off Virtual Machine and Discard Undo Disks</td>
<td>Turns off the virtual machine immediately, and discards any undo information. When the virtual machine restarts, it will be back at its previous saved state.</td>
</tr>
<tr>
<td>Reset</td>
<td>Resets the virtual machine, which is slightly politer than Turn Off.</td>
</tr>
<tr>
<td>Restore From Saved State</td>
<td>Resumes from hibernate.</td>
</tr>
<tr>
<td>Discard Saved State</td>
<td>Discards any saved state information. Does not restart the machine.</td>
</tr>
</tbody>
</table>
Add or remove a floppy drive
Add or remove a SCSI adapter
Change a hard disk type (IDE or SCSI)
Add or remove a network adapter
Enable or disable scripts
Enable or disable undo disks

We haven’t talked about the last option in the list. You can enable a “snapshot” capability with Virtual Server that allows you to make changes to a virtual machine and then simply abandon those changes and return to a known state. To enable this, you need to turn on Undo Disks for the particular virtual machine. Then, when you shut down or save the state of a virtual machine, you have the option to commit the undo disks (move the fallback position to the current state), discard the undo disks (rollback to the fallback position), or simply save the current state without changing the undo status. This is a powerful capability that lets you repeatedly test a configuration change on your test network to see whether it’s a good idea to make the change. Once you’ve tried it, you can roll back to the original condition and try it a different way.

Installing Virtual Machine Additions

A useful add-on to Virtual Server is Virtual Machine Additions. These improve the integration of the guest operating system in the host computer and the overall performance and manageability of the virtual machine. Among other things, they get rid of the trapped mouse problem. Virtual Machine Additions are available for the following versions of Windows:

- Microsoft Windows Server 2003 (all versions)
- Microsoft Windows 2000 Server
- Microsoft Windows NT Server 4.0 with Service Pack 6a (SP6a)
- Microsoft Windows XP (all versions)
- Microsoft Windows 2000 Professional
- Microsoft Windows Millennium Edition
- Microsoft Windows 98
- Microsoft Windows 95

To install Virtual Machine Additions, perform the following steps:

1. Log on to the Virtual Server Administration Website if you aren’t already logged on.
2. Click Master Status in the Navigation section of the leftmost frame.
3. Highlight the virtual machine you want to install the additions to, and select Edit Configuration from the action menu.

4. Click Install Virtual Machine Additions in the Status window.

5. Select the Install Virtual Machine Additions box in the Virtual Machine Additions Properties page, as shown in Figure 29-23, and click OK.

6. In the virtual machine, the installation will start automatically if the virtual machine is running. When the installation completes, reboot the guest operating system.

**Administering Virtual Server**

In addition to the areas of Virtual Server we’ve already discussed, there are additional administrative capabilities you can take advantage of. The administrative options you can change for Virtual Server are listed in Table 29-4.

**Table 29-4 Administrative Settings for Virtual Server**

<table>
<thead>
<tr>
<th>Setting</th>
<th>What the Setting Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Server security</td>
<td>Allows you to assign permissions to users and groups. The default is a single entry for local administrators to have full control.</td>
</tr>
<tr>
<td>Virtual Machine Remote Control</td>
<td>Enable or Disable VMRC and sets the IP address and port for VMRC connections.</td>
</tr>
<tr>
<td>Virtual Server scripts</td>
<td>Enable or disable scripts, and specifies scripts for various conditions.</td>
</tr>
<tr>
<td>Search Paths</td>
<td>Specifies the search paths that Virtual Server will use to locate resources.</td>
</tr>
</tbody>
</table>
Alternatives to Virtual Server

There are two well-known alternatives to Virtual Server that run on Windows Server 2003: Microsoft Virtual PC and VMWare’s suite of virtualization products, including VMWare Workstation.

Virtual PC

Microsoft Virtual PC (VPC) is designed for running personal virtual machines. VPC is not really a server-class product, and it will not install on x64 Editions of Windows, including Windows XP Professional x64 Edition. Virtual machines running under VPC do support a virtual audio card however, something that is not supported in Virtual Server.

Virtual PC doesn’t require a running Web server and generally has a more user-friendly interface compared to Virtual Server. In our experience, virtual machines running under Virtual PC don’t seem to run quite as fast as those running under Virtual Server, even on identical single-processor hardware. And VPC doesn’t take advantage of multiple processors or hyperthreading.

VMWare

VMWare’s VMWare Workstation is an interesting and powerful competitor to Virtual Server. It supports both x64 hosts and guests, giving it a real advantage in environments that are testing x64 compatibility.

VMWare Workstation also has a broader range of supported virtual hardware, including audio support and USB support. VMWare Workstation also supports multiple snapshots, giving you additional options for recovering to a known good point or testing multiple scenarios.

Another interesting VMWare Workstation capability is virtual teams. A virtual team is a group of virtual machines that can share a private network and can be started and stopped together.

<table>
<thead>
<tr>
<th>Setting</th>
<th>What the Setting Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website Properties</td>
<td>Controls various settings for the Administration Website, including refresh rate, number of events displayed, number of virtual machines displayed, and so forth.</td>
</tr>
<tr>
<td>Resource Allocation</td>
<td>Controls the resources assigned to virtual machines, including percentage of CPU reserved for the machine.</td>
</tr>
</tbody>
</table>
Summary

In this chapter, we’ve covered the setup and configuration of Microsoft Virtual Server 2005 R2, an important tool for the IT professional who needs to provide application compatibility for legacy applications, consolidate resources onto fewer servers, and provide a robust testing environment for new applications and patches. In the next chapter, we’ll cover another key tool for the IT professional—terminal services.
Microsoft Windows Terminal Services (WTS) was introduced for Microsoft Windows NT 4 Server with the separate Terminal Server Edition. However, starting with Microsoft Windows 2000, and continuing in Microsoft Windows Server 2003, it is a fully integrated part of all Windows servers, at least in the Remote Desktop for Administration mode (equivalent to what was called Remote Administration Mode in Windows 2000 Server)—simply another service. It’s also a part of Microsoft Windows XP Professional in a single user mode where it is called Remote Desktop. You can use WTS as a mechanism to manage and control your servers from anywhere in the enterprise, or you can take advantage of its application server ability to vastly simplify deployment and maintenance of a wide range of applications to a diverse user population.

**Note** Although both the client and server portion of Windows Terminal Services are sometimes referred to as Remote Desktop, in this chapter we’ll use Windows Terminal Services (WTS) whenever we’re referring to the server portion, or the combination of the server portion and the client portion. We’ll stick to referring to the client alone as Remote Desktop to help keep everything straight.

This chapter covers Windows Terminal Services concepts, requirements, and installation procedures. It also covers three main applications that are used to administer Terminal Services servers and clients: Terminal Services Manager, Terminal Services Configuration, and Terminal Services Client Creator.

**Concepts**

Windows Terminal Services is a new concept for many system administrators who expect systems to be essentially single user. It brings true multiuser capability to Windows.
UNIX systems have traditionally been primarily multiuser, with a single large server that serves many terminals.

Each user who connects to a Windows Server 2003 server using Remote Desktop is actually using the resources of the server itself, not the particular workstation at which he or she is seated. The user’s experience doesn’t depend on the speed of the workstation; rather the user’s workstation is actually sharing the processor, RAM, and hard disks of the server itself.

Each user gets his or her own WTS session, and each session is completely isolated from other sessions on the same server. An errant program in one session can cause that session’s user to have a problem, but other users are unaffected.

Each user who connects to a Windows Server 2003 server using Remote Desktop is actually functioning as a terminal on that server. Windows Terminal Services supports a wide variety of machines as terminals—from diskless display stations running Microsoft Windows CE entirely in memory to Microsoft Windows 95 and Microsoft Windows 98 workstations to Windows Server 2003 servers. The terminal is responsible solely for the console functions—that is, the keyboard, mouse, and actual display. All else resides on and is part of the server, although the disks, printers and serial ports of your local workstation can be connected to the remote session.

**Remote Access**

Terminal Services provides an ideal solution for the mobile user who needs to be able to run network-intensive or processor-intensive applications even over a dial-up connection. Because the local machine is responsible only for the actual console, the responsiveness and bandwidth requirements are substantially better compared to trying to run applications across a dial-up line. The actual bandwidth used for Windows Terminal Services can be tuned by enabling or disabling certain graphics features to improve responsiveness over a slow connection.

**Central Management**

Because all applications in a WTS session are running on the server, management of sessions and applications is greatly simplified. Any changes to applications or settings need only be made once, on the server, and these changes are seen by all future Windows Terminal Services sessions.

In addition, Windows Terminal Services allows an administrator to view what is happening in a user’s session, or even to directly control it. Help desk personnel can actually see exactly what the user is seeing without leaving their desks. If the user is configured accordingly, the Help desk person can share control of the session, walking the user through a difficult problem.
When configured in the default Remote Desktop for Administration mode, WTS gives the system administrators a powerful management tool. In this mode, administrators can log on directly to the machine from their desktops to perform normal system maintenance without having to sit at the server console. They can even take over the actual server console, rerouting it to their own desktop. This is a powerful addition to the administrator’s repertoire, enabling direct control of all servers without administrators leaving their desktop. Every system administrator will probably enable the Remote Desktop for Administration mode of all their servers. The overhead on the server is minimal compared to the benefits.

**Requirements**

Windows Terminal Services is installed on all Windows Server 2003 computers. It requires approximately 14 MB of additional hard disk space to host the client installation files, but it needs no additional space for the operating system. However, the real requirements are substantially higher for a machine that will be used with WTS in application server mode. Because each user will be executing his or her programs on the server itself, you need to determine exactly how your users work and what their real requirements are. Each installation will be different, but what follows are some guidelines to help you size your server appropriately.

**RAM**

Each session on the Windows Terminal Services server uses a minimum of approximately 20 MB of RAM just to log on. Add to this any RAM required to run the programs that each session launches. A typical user running Microsoft Office Outlook, Word, and Excel while connecting to the Internet uses approximately 40 MB of RAM, or approximately 20 MB beyond what the session itself requires. However, a power user can easily use twice that amount, and developers or other extreme users can go even farther.

**CPU**

Predicting exactly how much CPU power will be required per user is difficult, because each user has a different mix of applications and expectations. A dual processor server running 32-bit Windows Server 2003 SP1, with sufficient RAM present to avoid swapping can realistically host somewhere between 50 and 100 users. The limiting factor is usually not the CPU, or even the RAM, but the actual virtual memory address space available to the operating system. Most 32-bit Windows Terminal Services servers run out of system page table entries (PTEs) before they become processor bound.

Windows Terminal Services is one area where the release of Microsoft Windows Server 2003 x64 Editions has provided a dramatic gain. An x64 architecture server, with 4
processors and a well-designed I/O subsystem, can support 400 concurrent users. The limiting factor for most real-world x64 Edition servers is usually the I/O subsystem. Supporting hundreds of concurrent users requires a very well thought out disk array.

These numbers are our best estimates for reasonable expectations at this time; however, they are contingent on many factors. As with all estimates of this sort, they should be tested and verified against your mix of users and applications with the most up-to-date tools available from the Microsoft Web site.

**Network Utilization**

Typical network utilization depends on the type of client and level of graphics being transmitted (for example, an 800 × 600 connection takes a lot less bandwidth to support than a 1600 × 1200 connection), but the average bandwidth per user should work out to somewhere between 2 and 6 Kbps. The Remote Desktop client allows the end user to tailor the session to match the bandwidth available, significantly improving the end-user experience over limited-bandwidth connections.

**Capacity Planning**

The figures just mentioned should give you some starting points to plan the Terminal Services implementation, but the ultimate capacity the implementation will require depends on your situation and scenario. Use these figures only as a starting point for your own planning. Create a test environment that mimics the ultimate implementation on a smaller scale with real users and real applications to gather your own data.

---


Some the factors that play a major role in the requirements of the Terminal Services implementation are as follows:

- Which applications do your users run? Do they use a single dedicated application or a wide variety of essentially standard applications?

- Are your users primarily performing a single, routine task, or are they knowledge workers using the computer as their primary tool?

- Are your users all connected using a LAN, or are they a mix of WAN, LAN, and mobile users?
Planning for Maximum Capacity

Microsoft Windows Server 2003 is available in three different architectures: 32-bit x86, 64-bit x64, and 64-bit ia64 (Itanium). Both the traditional 32-bit x86 architecture and the new 64-bit x64 architecture are useful servers for supporting Windows Terminal Services clients. For smaller workloads of less than 50 concurrent users, either architecture will do a good job supporting the users. For any deployment that is projected to go beyond 50 users, we strongly suggest using x64 architecture processors and one of the Microsoft Windows Server 2003 x64 Editions.

The limiting factor in supporting large numbers of concurrent Windows Terminal Services users is usually the I/O subsystem on Windows Server 2003 x64 Edition. On 32-bit Windows Server 2003, the limiting factor is often the virtual memory address space available to Windows, which is limited to 2 GB in 32-bit versions of Windows. For x64 versions of Windows, the virtual memory address space for the operating system itself is 8 Terabytes (TB).

A well-designed redundant array of independent disks (RAID) for Windows Terminal Services should be composed of as many disks as possible. More, but smaller, disks are far better than a few larger disks because they distribute the I/O load across the whole array. Fiber channel will usually support greater total I/O than Small Computer System Interface (SCSI), though a well-designed SCSI array is also a good choice, and the new Serial Attached SCSI (SAS), combined with 2.5-inch drives provides a high-density array in a significantly smaller footprint.

Another important consideration is the total RAM available. You should test your deployment under as close to real workload conditions as possible to determine the RAM used per user. To maximize the number of users that a server can support, allocate somewhat more RAM per user than the minimum required—additional RAM will allow Windows to allocate additional memory to cache, which will improve the overall I/O throughput.

Installation

If you’re going to use WTS for Remote Administration only, you don’t need to install it at all—it’s already there. All you need to do is enable remote connections, and that’s covered next. If you’re going to be using WTS as an application and terminal server for multiple clients, however, you need to install Windows Terminal Services to the server. The easiest way is to add the role to the server, using the Manage Your Server Wizard, or if you prefer,
you can use the Windows Components Wizard, accessible via the Add Or Remove Programs tool in Control Panel.

To add the Terminal Server role to your Windows Server 2003 computer, using the Manage or Configure Your Server Wizard, take the following steps:

1. Click Add Or Remove A Role from the main Configure Your Server page.
2. Make sure all the relevant peripherals are both plugged in and enabled, and then click Next to bring up the Server Role page shown in Figure 30-1.

![Figure 30-1 The Server Role page of the Configure Your Server Wizard](image)

3. Highlight Terminal Server and click Next.
4. Click Next again to confirm the selection.
5. You get a warning that this installation requires a reboot as shown in Figure 30-2.

![Figure 30-2 The Windows Terminal Server role requires a reboot](image)

6. Click OK. If you don’t have the Installation CD-ROM in your CD-ROM drive or connectivity to your original installation media, you might get prompted for it. When all the files are found, the installation process proceeds automatically and the server reboots without further warning.
7. After the server reboots and you log back on, you get a confirmation that the Terminal Server role has been added to the server, and the Windows Help Checklist for Terminal Server opens to help complete the remaining configuration tasks, as shown in Figure 30-3.

![Figure 30-3 The Windows Help system checklist for setting up Terminal Server](image)

**Security Alert** Adding the Terminal Server role to a Domain Controller is a significant and unacceptable risk. As tempting as it might be on a small network, don’t do it.

**Real World Adding and Removing Multiple Components**

The temptation to install more than one application or add multiple components to Windows Server 2003 at a single pass is great, and the Manage Your Server Wizard lets you. Knowing that you might have to reboot the machine for each application, wouldn’t it be easier to simply add everything at once, stacking up reboots and saving time? Unless this is a very familiar software and machine configuration that you’ve done repeatedly, resist the temptation. Yes, you save some time if everything goes right, but it’s much harder to troubleshoot a problem if you change multiple components at once, and it’s a lot tougher to recover to a known stable state.
Enabling Remote Desktop for Administration Mode

Windows Server 2003 automatically installs all that is necessary for WTS Remote Desktop for Administration mode as part of all installations, but before it can be used, it must be enabled. To enable Remote Desktop for Administration mode, do the following:

1. Open the System application in Control Panel, and click the Remote tab to bring up the dialog box shown in Figure 30-4.

2. Select the Allow Users To Connect Remotely To This Computer check box. By default, members of the Domain Administrators group are able to connect remotely, but if you want to add users or groups who should be enabled for remote access, click Select Remote Users.

3. Click OK and you get reminded that only accounts with passwords can connect using Remote Desktop.

![Figure 30-4](image)

Remote Desktop must be enabled before users can connect to the server

The Terminal Services component of Windows Server 2003 requires approximately 14 MB of hard disk space, but this is strictly for the client installation-creator files. Terminal Services itself requires essentially no additional space for the operating system. However, each user who connects using Terminal Services requires a minimum of about 400 KB of disk space for his or her profile (and many users require a lot more space) and whatever storage space he or she uses on the server.

Installing Programs

Installing programs with Remote Desktop for Administration mode enabled is no different from installing on a server without Terminal Services. No special steps are required,
and no changes to the installation process or special compatibility scripts to support applications are required.

Application server mode, however, requires special consideration when installing many programs. When you activate the application server mode, Windows Server 2003 knows it must be prepared to deal with multiple users accessing the same application running simultaneously in separate memory spaces without interference or crossover. Certified for Windows programs handle the situation correctly, but if it is a noncertified program you’re installing, carefully follow the required steps to ensure that the application is installed correctly and that it will function correctly as a multiuser application.

Most applications install without problems in application server mode, though some might require special compatibility scripts. Consult the documentation for the given application. Any application that meets the rigorous “Certified for Windows” Server 2003 logo requirements must run successfully in WTS. VeriTest maintains a useful site at \textit{http://www.veritest.com} that lists applications that have been tested and certified for Windows and the Windows Catalog is also a good resource.

**Install Mode vs. Execute Mode**

Windows Server 2003, when configured as a Terminal Services application server, has two separate and distinct modes of operation—install mode and execute mode. To install an application that doesn’t meet the Certified for Windows logo requirements on a server, you must be in install mode or the application will not be installed correctly.

Windows Server 2003 is usually smart enough to recognize when you are running an installation program and automatically sets the necessary mode. However, if you’re installing an older application that isn’t Certified for Windows, especially if it doesn’t use Setup.exe or Install.exe as its installation program, manually switch the server to install mode before running the installation.

You can change to install mode in either of two ways: by using the Change command on the command line or by using Add/Remove Programs in Control Panel. If you like lots of extra mouse clicks, feel free to use Add/Remove Programs—we use the Change command.

**Using Add/Remove Programs to Install Applications**

While it isn’t absolutely required for most applications, it’s a good idea to run the installation from the server’s console. Wherever you run the installation from, however, make sure all users are logged off the terminal server before beginning installation. To install a program using Add/Remove Programs, follow these steps:

1. Open Add/Remove Programs from Control Panel.
2. Click Add New Programs and then click CD Or Floppy to display the Install Program From Floppy Disk Or CD-ROM dialog box. Click Next.
3. The Run Installation Program dialog box shown in Figure 30-5 opens. If Windows Server 2003 is able to find the setup program, you see it already highlighted in the Open box. However, if you’re installing from a network drive or Windows Server 2003 can’t locate it for some other reason, use the Browse button to locate the installation program for the application you’re installing.

![Figure 30-5 The Run Installation Program dialog box](image)

4. When you select the correct setup program in the box, click Next to begin the installation. While the installation is proceeding, the After Installation dialog box remains open in the background.

5. When the installation is completed, whether successfully or not, do not accept an immediate reboot if you have a choice and the application requires one. Finish the installation and then return to the After Installation dialog box. Click Next to get to the final dialog box and then click Finish. If the application requires a reboot, you can do it now.

The Change Command

The Change command was introduced in Windows NT 4 Terminal Server Edition and is still available in Windows Server 2003. The Change command allows you to change between user modes (install and execute), reassign port mappings for Terminal Services sessions, and enable or disable logon events to Terminal Services. The three basic commands, and their options for the Change command, are as follows:

- **Change User** Initiates change between install or execute mode when running as an application server. Options are the following:
  - **Install** Installs new applications on the server for multiuser access
  - **Execute** Allows programs to be executed in multiuser mode (the default value on startup)
  - **Query** Displays the current user mode
Change Port  Changes the port assignments of COM port mappings for MS-DOS compatibility. Options are the following:

-  \texttt{portx=porty}  Maps port X to port Y
-  \texttt{/D portx}  Deletes the current mapping for port X
-  \texttt{/Query}  Displays the current port mappings

Change Logon  Enables or disables logon sessions. Options are the following:

-  \texttt{/Enable}  Allows users to log on from Terminal Services sessions
-  \texttt{/Disable}  Prohibits users from initiating logon sessions (current sessions aren’t disconnected or terminated)
-  \texttt{/Query}  Displays the current logon status

Using the Change Command to Install an Application

You can also install new applications into Windows Terminal Services using the Change command. This is especially useful for scripting installations that will be installed on multiple terminal servers in an identical configuration. To install a new application using the Change command, follow these steps:

1. Disable new logons to the server by typing \texttt{change logon /disable}.
2. Find out which users are currently logged on to the server and what their session IDs are by typing \texttt{query session}.
3. Warn the users that they need to log off their current session using the \texttt{Msg} command. A broadcast warning to all users would have the form:
   \begin{verbatim}
   msg * "message text"
   \end{verbatim}
4. Reset sessions of users that are currently logged on to the server with the command \texttt{reset session <sessionID>}.
5. Change to install mode with the command \texttt{change user /install}.
6. Run the application’s setup or installation program.
7. Change back to execute mode by typing \texttt{change user /execute}.
8. Re-enable logons to the server with \texttt{change logon /execute}.

As you can see, using the Change command, along with other command-line utilities included with Windows Server 2003, enables you to easily script the installation of a program to WTS. In large organizations where multiple terminal servers are being used, especially where Network Load Balancing is being used with the Session Directory to support large user populations, using command-line utilities allows the administrator to limit the disruption to the network as new applications are installed and made available,
and easily ensures that applications are installed uniformly across the enterprise, simplifying support and training.

Administration

Windows Terminal Services can be centrally administered and configured across a domain from a single console. Three main applications used to administer Terminal Services servers and clients are as follows:

- **Terminal Services Manager**  Monitors and controls the connections to all Terminal Services servers on the network
- **Terminal Services Configuration**  Runs only locally on each terminal server; a Microsoft Management Console (MMC) snap-in that lets you modify the configuration of the local Terminal Services server
- **Terminal Services Licensing**  Manages Client Access Licenses for Terminal Services across the domain or workgroup

**Tip**  If you need to run the Terminal Services Configuration console, but don’t want to get up and go into the server room to do it, you can open a console Remote Desktop session to the server.

Terminal Services Manager

Terminal Services Manager (Tsdadmin.exe) is the main mechanism for managing the various connections to the servers. A typical Terminal Services Manager window is shown in Figure 30-6. From here, you can see not only the available terminal servers on the network, but also who is connected to them, which sessions are active, which protocols are being used, and so on.
Overview
Terminal Services Manager shows all the servers in the domain. By default, it connects to only a single server at a time, although you can opt to connect to all the available servers at once. The icons for the current active connection, server, and domain are shown in a different color (green, by default). With Terminal Services Manager, you can view and manage the users, sessions, and processes by network, domain, server, or connection, giving you a comprehensive look at the critical information for your Terminal Services deployment.

Finding Servers
You can use Terminal Services Manager to identify all the servers in your network that are currently active or all the servers in a particular domain. To find all the servers in a domain, right-click the domain name in the left pane of Terminal Services Manager and select Refresh Servers In Domain. To find all the servers on the network, right-click All Listed Servers and choose Refresh Servers In All Domains.

Note
This will find only the servers running in applications server mode. Those running in remote administration mode will not be listed. You can, however, explicitly connect to them. They will be shown in Terminal Services Manager in a different color.

Important
Using either of the Refresh Servers commands causes a domain-wide or network-wide series of broadcast messages. Use this command with caution.

Making Connections
To manage the processes, sessions, and users connected to a given server, you need to first connect to that server using Terminal Services Manager. To connect to a server, right-click the server's icon in the left pane of Terminal Services Manager and choose Connect. If it's a server you regularly connect to, add it to your Favorite Server by selecting Add To Favorites.

Managing Connections
Terminal Services Manager lets you view and manage each of the connections to the terminal servers, including the console session. From any session that has sufficient permissions, you can forcibly disconnect a session, reset a session entirely, log off a session, view the status of the connection, manage users' sessions, send a message to the display of a connection, use remote control to take control of a session on the connection, and connect to any other session. You can also use Terminal Services Manager to see a variety of information about the processes and status of the connections to a server and even to kill a hung process.
Disconnecting Sessions
When a session is disconnected, all the programs of that session continue to run but the input and output from the session are no longer transmitted to the remote terminal. Disconnecting a session leaves user programs and data in their normal state, protecting them from loss of data. Disconnecting a session doesn't release memory or other resources from the server, and the session continues to be counted as a licensed session.

Any user can disconnect his or her own session, or an administrator with the Full Control privilege can disconnect a session. To disconnect a session using Terminal Services Manager, right-click the session in either pane of Terminal Services Manager and choose Disconnect from the shortcut menu. Click OK to confirm that this is what you really meant to do, and the session is disconnected.

You can disconnect multiple sessions on multiple servers as well. Simply select the sessions in the right pane of Terminal Services Manager and right-click. Choose Disconnect from the menu, click OK in response to the prompt, and the sessions are disconnected. The console where the sessions are being displayed receives a message like that shown in Figure 30-7. When you click OK, the message box disappears.

![Remote Desktop Disconnected message box](image)

Figure 30-7 The Remote Desktop Disconnected message box

Real World Using Disconnect to Manage Your Sessions from Multiple Locations
Disconnecting from a Terminal Services session has many advantages for the mobile user who might need to connect from a different location or who wants to be able to work in relatively short bursts as time permits. When you disconnect from a session, everything continues to run, just as if you were connected. So when you reconnect to the same server, the session is restored exactly as you left it. You can then easily return to a project or document exactly where you left off. However, because the session continues to run it continues to use resources on the server, so reserve disconnect for mobile users. Encourage regular users located on high-quality connections to log off their sessions to free the resources for others.
Resetting Sessions
You can reset a session if the session is your own or if you have the Full Control privilege for sessions. When you reset a session, all work in that session is lost, programs stop running, and memory is freed. To reset a session, right-click the session and choose Reset from the menu. You get a warning message. Click OK and the session is reset.

You can reset multiple sessions by selecting them in the right pane of Terminal Services Manager, right-clicking them, and selecting Reset. You must have the Full Control privilege for each of these sessions, or they must be your own.

You can also use the command line to reset sessions. To find out what sessions are active, type

```
query session
```

This will list all the sessions on the current server, including their session ID. To disconnect a session, type

```
reset session <ID>
```

The reset session command also accepts the session name as an argument instead of session ID, and lets you specify the server as well. The query session can provide more detailed information about the session parameters—type `query session /?` for full syntax.

---

**Important**  Resetting a session can result in data loss for the user of that session. Reset a session only when the session has stopped responding or has otherwise malfunctioned.

Logging Off a Session
You can log off your own session or log off a user's session if you have the Full Control privilege. Right-click the session in the right pane of Terminal Services Manager, and select Log Off from the shortcut menu, shown in Figure 30-8. You'll get a warning that the user’s session will be logged off. If you click OK, the session is logged off. Logging off a session frees up any resources used by that session, returning them for use by other connections.

---

**Important**  Logging off a session can result in data loss for users of that session. Always warn users by sending them a message before logging off their session.
Viewing Processes and Other Information About a Session

You can view the active processes in a session and a variety of other information about the session, including which client the session is coming from, the security level, the session resolution, and so forth. To view the active processes in a session, highlight the session in the left pane of Terminal Services Manager and click the Processes tab in the right pane, as shown in Figure 30-9. To view information about the same session, click the Information tab in the right pane, as shown in Figure 30-10.
Chapter 30  Deploying Terminal Services

You can also use Terminal Services Manager to show all the processes, users, and sessions on a given server, for the whole domain or for the entire network. The Processes tab is shown in Figure 30-11 for the entire Example domain. You can sort the processes by user, session, or server. If you have the Full Control privilege, you can even kill a process from here, although the usual caveats about killing processes apply.

Managing User Sessions

You can use Terminal Services Manager to view and manage the user sessions on a particular server or across the entire domain or network. To view all the users across the entire domain, highlight the domain name in the left pane of Terminal Services Manager.
and click the Users tab in the right pane. In the left pane, you see a list of all the servers in the domain, and the connected users appear in the right pane. You can select any entry in the right pane and send a message to the user's session, disconnect the session, or take control of the user's session for troubleshooting or training.

**Sending a Message to a Session**

You can use Terminal Services Manager to send a message to a particular session. To send a message to all the sessions on a particular server, just highlight all the sessions and send a message to all of them at once. To send a message to one or more sessions or users, follow these steps:

1. Right-click the sessions or users in the right pane of Terminal Services Manager.
2. Choose Send Message to open the dialog box.
3. Type the message you want to send. Press Ctrl+Enter to start a new line.
4. Click OK to send the message.

You can also use the command-line `Msg` command to send a message to a particular session or to all the users on a particular server. The `Msg` command has additional options and functionality over the graphical Terminal Services Manager messaging. The syntax for the `Msg` command is as follows:

```
msg {username|sessionname|sessionid}@filename*[/SERVER:servername] [/TIME:seconds] [/V] [/W] [message text]
```

The options for the `Msg` command are as follows:

- **username** Sends the message to a particular user on the server.
- **sessionname** Sends a message to a particular session, identified by the session name.
- **sessionId** Sends a message to a particular session identified by session ID.
- **@filename** Sends a message to a list of user names, session names, or session IDs contained in the file.
- ***\** Sends a message to all users connected to the server.
- **/SERVER:servername** Specifies the server to which the session or user is connected. The default is the current server.
- **/TIME:seconds** Specifies the number of seconds to wait for the recipients to acknowledge the message. If the message isn’t acknowledged in the time specified, it goes away. The default time is 60 seconds if no /TIME option overrides the default.
Chapter 30  Deploying Terminal Services  999

- /V  Displays information back to the command line about the actions being performed on the server.

- /W  Waits for a response from the user before returning control to the command line. If no response is received before the message times out, control is returned when it times out.

- message text  Specifies the message to send. If none is specified, the text is accepted from STDIN or you are prompted for the text.

Controlling a Session
If you have appropriate permission (Full Control), you can connect to another user’s session and remotely control it. The keyboard, mouse, and display are the same for both your session and the user’s session. This gives you the ability to easily troubleshoot a user’s session or train the user by walking him or her through the steps of a particular task. Input for the session comes equally from your session and the user’s. If the user or protocol settings are set to view only the session, not directly control it, you see only what the user does on his or her screen, but you aren’t able to interact with it using your mouse or keyboard.

By default, when you connect to a user’s session using remote control, the user is notified that you are connecting and is asked to confirm the permission. This notification can be turned off on a per-user basis by modifying the user’s account in Active Directory. (See Chapter 9 for more about user accounts.) You can also configure this notification on a per-protocol basis for a given server using Terminal Services Configuration (explained shortly). To take control of a user’s session, follow these steps:

1. Right-click the session or user in the right pane of Terminal Services Manager.
2. Choose Remote Control to open the dialog box shown in Figure 30-12. Select an appropriate hot key that will terminate the remote session. The default is Ctrl+*, where the asterisk symbol (*) is from the numeric keypad.

![Figure 30-12  The Remote Control dialog box](image)
3. The dialog box shown in Figure 30-13 appears to the user, requesting permission to allow you to connect, while a dialog box opens on your session advising you that your session is waiting to establish control. If permission isn’t required for this protocol or user, the user doesn’t get a message at all. Until the user confirms permission to connect to his or her session, your session appears to freeze.

![Figure 30-13 The Remote Control Request dialog box](image)

You can also use the Shadow command to take control of a user’s session. The Shadow command has the following syntax:

```
shadow {sessionname|sessionid} [/SERVER:servername] [/V]
```

In this syntax, `sessionname` and `sessionid` identify the particular session you want to take control of, and the server defaults to the current server if `/SERVER` isn’t specified. The `/V (verbose)` option gives additional information about the actions being performed.

**Connecting to a Session**

You can connect to another session on the server you are on if you have the appropriate permission and the other session is either in an active or a disconnected state. You can always connect to a session that is logged on with the same user account as your current logon name, or you can connect to another user’s session if you have Full Control or User Access permission. You are prompted for the user’s password.

This ability to connect to another session can be a useful tool for both administrators and users. Get home and realize you forgot to finish off that important memo? Log on remotely and connect to your working session at the office and pick up right where you left off. To connect to a session, follow these steps:

1. Right-click the session or user in the right pane of Terminal Services Manager.
2. Choose Connect to connect to the session. If the session is that of a different user than the current user, you’re prompted for the target session user’s password. If the session is one of your own, you’re switched to that session and your current session is disconnected.

**Terminal Services Configuration**

Use the Terminal Services Configuration MMC to change the settings for all connections to a particular server. (See Figure 30-14.)
Figure 30-14  The Terminal Services Configuration MMC

From here, you can change any of the following settings:

- **Delete Temporary Folders On Exit**  When enabled, automatically deletes any temporary folders created on the server when the user logs off. Default is true (Yes).

- **Use Temporary Folders Per Session**  When enabled, each session gets its own set of temporary folders. Default is true (Yes).

- **Licensing**  Choose between Per Device and Per User.

- **Active Desktop**  When enabled, user connections are permitted to use Active Desktop. Disable this option to reduce the amount of resources and bandwidth required for Terminal Services sessions.

- **Permission Capability**  Choose between Full Security (the default) and Relaxed Security. Relaxed security might be necessary for earlier applications, but it will allow all users to have full access to critical registry and file system locations.

- **Restrict Each User To One Session**  When enabled, the default users are limited to a single session on the terminal server to conserve resources.

- **Session Directory**  Disabled by default. When enabled, it allows Session Directory to manage the sessions in a cluster. (Present only on Windows Server 2003 Enterprise Edition or Datacenter Edition.)

- **License Server Discovery Mode**  Automatic by default. You can specify a list of servers to use.

**Connection Properties**

You can change the properties of the connections from Terminal Services Configuration. By default, the only connection protocol installed is Microsoft Remote Data Protocol.
(RDP) 5.2. Other protocols are available from third parties, including the Independent Computing Architecture (ICA) protocol used by Citrix MetaFrame. All protocols can be configured from this point.

RDP allows you to configure a wide variety of settings for each server (listed in Table 30-1). Most of these settings are normally controlled by the client, or you can set the server to override the client settings. To set properties for the RDP connections, double-click the RDP-Tcp entry under Connection to open the dialog box shown in Figure 30-15.

![Figure 30-15  The RDP-Tcp Properties dialog box](image)

### Table 30-1 Terminal Services Configuration settings for RDP

<table>
<thead>
<tr>
<th>Tab</th>
<th>Property</th>
<th>Setting</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Encryption Level</td>
<td>Low</td>
<td>Data from client to server is encrypted using the standard encryption key.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Client Compatible</td>
<td>Data is encrypted using the maximum key strength supported by the client in both directions (default setting).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High</td>
<td>Data is encrypted in both directions using the maximum key length supported. Clients that do not support this level of encryption are not allowed to connect.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FIPS Compliant</td>
<td>Encrypts data in both directions using Federal Information Processing Standard (FIPS) encryption algorithms. This encryption is designed to provide compliance with FIPS 140-1 (1994) and FIPS 140-2 (2001) for Security Requirements for Cryptographic Modules.</td>
</tr>
</tbody>
</table>
### Table 30-1  Terminal Services Configuration settings for RDP

<table>
<thead>
<tr>
<th>Tab</th>
<th>Property</th>
<th>Setting</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon Settings</td>
<td>Use Standard Windows Logon Interface</td>
<td>True</td>
<td>Do not use alternate authentication package even if installed.</td>
</tr>
<tr>
<td></td>
<td>Use Client-Provided Logon Information</td>
<td>True</td>
<td>Client determines the logon security user.</td>
</tr>
<tr>
<td></td>
<td>Always Use The Following Logon Information</td>
<td>False</td>
<td>Logon information for all clients uses this same logon information.</td>
</tr>
<tr>
<td></td>
<td>Always Prompt For Password</td>
<td>False</td>
<td>Client can use embedded password.</td>
</tr>
<tr>
<td></td>
<td>Security Tip: Domain Controllers should have this box selected to always force a remote session to enter a password.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sessions</td>
<td>Override User Settings: (disconnected, active, and idle sessions)</td>
<td>False</td>
<td>User settings control termination of disconnected sessions, active session limit, and idle session limit.</td>
</tr>
<tr>
<td></td>
<td>Override User Settings: (session limit action)</td>
<td>True</td>
<td>The server controls session limits.</td>
</tr>
<tr>
<td></td>
<td>Override User Settings (reconnection)</td>
<td>False</td>
<td>User settings control session limit behavior.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>True</td>
<td>Server settings control session limit behavior—disconnect or end the session.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>False</td>
<td>User settings control reconnection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>True</td>
<td>Server settings control reconnection.</td>
</tr>
<tr>
<td>Environment</td>
<td>Initial Program</td>
<td>False</td>
<td>Forces clients to connect to the desktop.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>True</td>
<td>Client specifies initial program. (This is the default.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled</td>
<td>All clients are forced to run the program specified.</td>
</tr>
<tr>
<td>Remote Control</td>
<td>Use remote control with default user settings</td>
<td>True</td>
<td>Settings for remote control are set as part of the user’s account data.</td>
</tr>
<tr>
<td></td>
<td>Do not allow remote control</td>
<td>False</td>
<td>When true, all remote control to sessions on the server is disabled.</td>
</tr>
<tr>
<td></td>
<td>Use remote control with the following settings</td>
<td>False</td>
<td>When true, you override remote control settings for all users connecting to the server.</td>
</tr>
</tbody>
</table>
Support Services and Features

Terminal Services Licensing

Windows Server 2003 requires that at least one Windows Terminal Services license server be installed and running on any network that uses application server mode. If a license server is not installed within 180 days, all Windows Terminal Services connections will be disabled. Windows Terminal Services requires a separate Terminal Server Client Access License (CAL) for each user or device in addition to any Windows Server CALs you might need. The Terminal Server Licensing server does not track per-user license usage, but it does enable you to install per-user licenses.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Property</th>
<th>Setting</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Settings</td>
<td>Use connection settings from user settings</td>
<td>True</td>
<td>Printer and drive connections are specified as part of the user’s account settings.</td>
</tr>
<tr>
<td></td>
<td>Limit Maximum Color Depth</td>
<td>True</td>
<td>When True, you can choose the maximum color depth used by clients. Default value is 16 bit.</td>
</tr>
<tr>
<td></td>
<td>Drive Mapping</td>
<td>True (not selected)</td>
<td>Client drives are mapped to the user session.</td>
</tr>
<tr>
<td></td>
<td>Windows Printer Mapping</td>
<td>True (not selected)</td>
<td>Clients can map Windows printers, and mappings are remembered.</td>
</tr>
<tr>
<td></td>
<td>LPT Port Mapping</td>
<td>True (not selected)</td>
<td>Automatic mapping of client LPT ports is enabled.</td>
</tr>
<tr>
<td></td>
<td>COM Port Mapping</td>
<td>True (not selected)</td>
<td>Clients can map printers to COM ports.</td>
</tr>
<tr>
<td></td>
<td>Clipboard Mapping</td>
<td>True (not selected)</td>
<td>Clients can map clipboard.</td>
</tr>
<tr>
<td></td>
<td>Audio Mapping</td>
<td>False (selected)</td>
<td>Clients can't map audio.</td>
</tr>
<tr>
<td>Network Adapter</td>
<td>Network Adapter</td>
<td>All</td>
<td>All available network adapters can be used to connect to Terminal Services.</td>
</tr>
<tr>
<td></td>
<td>Unlimited Connections</td>
<td>True</td>
<td>There is no limit to the number of connections permitted.</td>
</tr>
<tr>
<td></td>
<td>Maximum Connections</td>
<td>True</td>
<td>The maximum number of connections permitted using this adapter.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Full Control</td>
<td>Administrators/SYSTEM</td>
<td>Administrators and SYSTEM have Full Control privilege.</td>
</tr>
<tr>
<td></td>
<td>User Access</td>
<td>Remote Desktop Users</td>
<td>Query, Logon, and Connect privileges.</td>
</tr>
</tbody>
</table>

Table 30-1 Terminal Services Configuration settings for RDP
Installing Terminal Server Licensing

In small deployments, installing the Terminal Server Licensing service on the same server that is running Terminal Services is a reasonable choice, but in larger deployments, the Terminal Server License Server should be on a different server from Terminal Services.

**To Install Terminal Services**

1. Open Add/Remove Programs, and select Add/Remove Windows Components.
2. Select Terminal Server Licensing from the components list, and click Next.
3. On the Terminal Server Licensing Setup page, shown in Figure 30-16, choose whether this license server will service the entire enterprise, or only the local domain or workgroup, and designate a location for the license database to reside.

![Figure 30-16](image)

**Figure 30-16** The Terminal Server Licensing Setup page

4. Click Next and the installation will proceed.

**To Activate the License Server**

1. Open the Terminal Services Licensing MMC (Licmgr.exe).
2. If this is the first server in your enterprise, no license server will be found, as shown in Figure 30-17. Click OK.

![Figure 30-17](image)

**Figure 30-17** Terminal Server Licensing—No Server Found
3. Right-click All Servers in the leftmost pane, and select Connect.

4. Type the name of the new Terminal Server Licensing Server and click OK, as shown in Figure 30-18.

![Figure 30-18 The Connect To License Server dialog box](image)

5. Right-click the server in the rightmost pane, and select Activate Server.

6. The Terminal Server License Server Activation Wizard opens. Click Next to open the Connection Method page shown in Figure 30-19.

![Figure 30-19 The Connection Method page](image)

7. Select a connection method from the drop-down list. The choices are Automatic Connection, Web Browser, or Telephone. Automatic Connection requires an Internet connection from the server you are activating. Web Browser also requires an Internet connection, but it can be run from any workstation. Click Next.

8. If you've chosen Automatic, the connection will be made, and then the first Company Information page (shown in Figure 30-20) is displayed. Fill in all the fields on this page because they are required. Click Next.
9. The second page of company information is displayed. All information on this page is optional—fill it in only if you want to. Click Next, and if your connection is good, your server will activate and you’ll be presented with the completion page. You can continue to add Client Access Licenses by selecting the Start Terminal Server Licensing Wizard Now box. Click Next or Finish.

To Install Windows Terminal Server Client Access Licenses
1. Open the Terminal Server Licensing Wizard if it isn’t already open.
2. Right-click the server you want to add licenses to.
3. Select Install Licenses to open the Terminal Server CAL Installation Wizard.
4. Click Next and fill in the license code. Click Next again, and the activation will complete.

Note Additional steps are required for either Web browser or telephone methods. If you need to reactivate your server and re-install licenses, you will be required to use the telephone method.

Remote Desktop Client
The %windir%\system32\clients\tsclient\win32 directory of Windows Server 2003 contains an installable version of the Remote Desktop Client program. You can use this to install the Remote Desktop Client on earlier versions of Windows, including Windows 95, Windows 98, Windows Me, Windows NT 4, and Windows 2000.
You can install the Remote Desktop Client on any earlier client system either by making the \%windir\%\system32\clients\tsclient\win32 directory available as a network share, or by using the Windows Server 2003 installation CD-ROM. To install the Remote Desktop Client from the installation CD-ROM, do the following:

1. Insert the CD-ROM into the CD-ROM drive on the client computer. If the setup page doesn't automatically appear, run the Setup.exe program in the root directory of the CD.

2. Select Perform Additional Tasks.

3. On the next page, select Set Up Remote Desktop Connection, which launches the Remote Desktop Connection Install Shield Wizard. This is a standard Install Shield wizard—go through the pages to install the Remote Desktop Client on the local computer.

You can install and run Remote Desktop Client on any computer running Windows Server 2003, Windows XP, Windows 2000 (all editions), Windows NT 4, Windows 95, or Windows 98. A version is also available for hardware vendors to include in their versions of Windows CE, and a version for Mac OS X computers is available on the Microsoft Web site. Other operating systems can use clients from third-party vendors; however, these might require the use of the Citrix MetaFrame ICA protocol. Special Windows CE-based thin clients are available from a number of manufacturers that allow you to connect to a Windows Server 2003 Terminal Services server with no hard disk at all—the base operating system and Remote Desktop Client are loaded in ROM.

### Summary

Windows Server 2003 Terminal Services is an important addition to all versions of Windows Server 2003 Server. It provides a way to centralize management and application deployment across the entire enterprise. Terminal Services Manager lets you control the connections to servers across the entire enterprise. All Windows Server 2003 servers include the Remote Desktop for Administration mode to give the system administrator the ability to easily connect to all the servers in his or her network. The next chapter covers the Indexing Service.
Chapter 31

Using the Indexing Service

Understanding the Indexing Service ........................................ 1009
Planning Your Indexing Service ............................................. 1012
Creating and Configuring Catalogs ........................................ 1015
Registry Entries for the Indexing Service ............................... 1021
Querying the Index .............................................................. 1023
Examining Performance ......................................................... 1028
Troubleshooting the Indexing Service .................................... 1030
Summary ............................................................................ 1033

One of the lesser known services in Microsoft Windows Server 2003 is the Indexing Service. The Indexing Service provides Web-type indexing and querying to corporate intranets, Internet sites, and more conventional networks without reformatting documents. With the click of a button, users can index and query the contents of intranet or Internet sites on Windows Server 2003 with Internet Information Services (IIS). The Indexing Service does more than just index documents, however. It provides a system for publishing information on your intranet or on the Web. Because the Indexing Service indexes both the content and properties of formatted documents, you don’t need to convert existing documents to HTML to make them available to your users. Instead, documents in a variety of formats, such as Microsoft Office Word or Excel, are directly available.

Even though its primary function is the indexing of Web servers, the Indexing Service is useful on any network where searches for documents are common, and it is essential on any network with frequent searches through large numbers of files.

Understanding the Indexing Service

The Indexing Service functions much as one would expect—it catalogs a set of documents, enabling dynamic full-text searches using the search function, a query form, or Microsoft Internet Explorer. Just as an index in a book maps an important word to a page inside the
book, content indexing on a computer takes a word within a document and maps it back to that document. Documents to be indexed can be specified in catalogs and can include document properties as well as the actual text in the document. After the Indexing Service is set up, no ongoing maintenance is needed, and administration is required only when you need to change a basic configuration. If you didn't include the Indexing Service in your original installation of Windows Server 2003, you can add it through Add/Remove Programs in Control Panel.

Note By default, the Indexing Service is disabled in Windows Server 2003.

Defining Terms
When administering the Indexing Service, you'll encounter a number of terms that have a special meaning when used in the Indexing Service context. Here are some of the most common ones, with their definitions:

- **Catalog** A directory where all temporary (word lists) and persistent (shadow and master) indexes and cached properties are stored for a particular scope.

- **CiDaemon** A child process created by the Indexing Service (cisvc.exe). CiDaemon works in the background, filtering documents for the Indexing Service.

- **Corpus** The entire collection of HTML pages and other documents indexed by the Indexing Service.

- **Filter** Part of a dynamic-link library (DLL) of filters, each designed to extract textual information and properties from a specific type of formatted document.

- **Master index** A persistent index that contains the indexed data for a large number of documents. This is usually the largest persistent data structure. In an ideal state, this is the only index present because all the indexed data is stored in the master index and there are no shadow indexes or word lists. A master index is created through a master merge.

- **Master merge** The process by which shadow indexes are combined with the current master index into a single master index. Unlike shadow merges, this is usually a fairly long process.

- **Persistent index** Data for an index that is stored on disk. Unlike word lists, which exist only in memory, a persistent index survives shutdowns and restarts. Persistent-index data is stored in a highly compressed format. There are two types of persistent indexes: shadow indexes (also referred to as saved indexes and temporary indexes) and master indexes.

- **Query** A request to search files for specific data.
- **Scan**  The process by which files and directories are checked for modifications. Scanning is performed against virtual roots that have been selected for indexing.

- **Scope**  The range of documents to be searched when executing a query. Physical paths or virtual roots can specify scopes.

- **Shadow index (also known as saved index)**  A persistent index created by merging word lists and occasionally other shadow indexes into a single index. A catalog can have multiple shadow indexes.

- **Shadow merge**  The process by which word lists and shadow indexes are combined into a single shadow index. A shadow merge is performed to free up memory used by word lists and also to make the filtered data persistent.

- **Virtual root**  An alias to a physical location on disk. Index Server can index any directory defined as a virtual root. Index Server can be set up to work with a central index but point to files on other servers.

- **Word list**  When a document is indexed, the index information goes first to a small temporary index, called a word list. Word lists are maintained in memory until the Indexing Service combines them into the existing indexes.

### How Indexing Works

The Indexing Service uses filters that can read certain types of documents, extract the text and properties, and send that information to the indexing engine. The filters included with Windows Server 2003 index the following kinds of documents: text, HTML, Microsoft Office 95 and later, and Internet Mail and News (provided that IIS is installed). The Indexing Service can use other filters made available by software vendors. The vendor that supplies the filter also supplies installation instructions.

After extracting the text and properties, the Indexing Service determines the language the document is written in and removes words that are on the language’s exception list. The exception list contains prepositions, pronouns, articles, and so forth, and is appropriately named Noise.xxx, where xxx represents the language. Noise.xxx is in the System32 directory. Figure 31-1 shows a portion of the Noise.eng file, which contains the exception list for American English. You can add words to or remove words from the exception list using any text editor, such as Notepad.

After words from the exception list are removed, the remaining words are stored first in a word list in memory. At least once a day, the word lists are combined to form temporary saved indexes, and later the Indexing Service consolidates the temporary indexes into a single master index. All this is done automatically, although under certain circumstances you might need to intervene by initiating a merge manually, as described later in this chapter.
Planning Your Indexing Service

When designing an indexing site, the first question that arises is how much storage space will be needed. The minimum disk space allocated should be at least 30 percent of the size of your corpus, and 40 percent is better. During a master merge, the Indexing Service can temporarily need up to 45 percent of the corpus size.

Depending on the filters used to index a group of documents, the actual size of the indexes might be less than the standard 30 percent. For example, if you write a filter for indexing large documents (such as large image files), you can limit indexing to the first few hundred bytes (about all you need to get the header information), thus reducing the amount of space needed for the index.

Note Because most Indexing Service operations are read requests (searching the indexes, returning the results, and then accessing the actual documents), disk striping (RAID-0) or a RAID-5 array is a good way to reduce disk-bound I/O operations. Disk striping and RAID arrays are covered in detail in Chapter 19.

Planning for future site growth is essential. Moving documents to larger disks to overcome space limitations can cause query errors until you are able to run a complete reindex, which can take many hours. Another critical part of planning an Indexing Service site is to make sure that plenty of memory is available on the indexing machine. Table 31-1 shows the minimum memory required versus the recommended minimum amount for different quantities of documents. As usual, the more memory you have available, the better (and with the price of memory as low as it is, consider 512 MB a minimum for any type of Windows Server 2003). With large numbers of documents, a faster CPU also speeds up indexing and searching.
Merging Indexes

The Indexing Service automatically combines memory-resident word lists into disk-resident temporary lists and, once a day, merges all temporary indexes into a master index. Depending on the number of temporary lists, merging can be a long process that uses much of the CPU's resources. Queries are slower during a merge, and other processes on the computer are slower still.

By default, merges are done at midnight local time. If this is unsuitable for your system, you can change the default when the master merge is performed. You can also initiate a merge manually when a large number of documents in a catalog are changed. This section describes how to perform these two tasks.

Setting the Time to Start a Master Merge

To change the operation’s schedule from the default time, follow these steps:

1. Run Regedit.exe.
2. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex.
3. In the rightmost pane of the Registry Editor window, double-click the MasterMergeTime value.
4. The DWORD Editor dialog box opens. In the Data box, type the number of minutes after midnight when a master merge should be initiated. Be sure to select Decimal from the Base options.
5. Click OK and close the Registry Editor.

Note MasterMergeTime has a valid range of values from 0 to 1439 minutes, though no error is reported if you enter a larger value. The default is 0. When the specified number of minutes after midnight has passed, the Indexing Service initiates a master merge.

<table>
<thead>
<tr>
<th>Number of Documents</th>
<th>Minimum Memory</th>
<th>Recommended Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fewer than 100,000</td>
<td>128 MB</td>
<td>128 MB</td>
</tr>
<tr>
<td>100,000 to 250,000</td>
<td>128 MB</td>
<td>128 MB to 256 MB</td>
</tr>
<tr>
<td>250,000 to 500,000</td>
<td>128 MB</td>
<td>256 MB to 512 MB</td>
</tr>
<tr>
<td>500,000 or more</td>
<td>256 MB</td>
<td>512 MB or more</td>
</tr>
</tbody>
</table>
Manually Merging Indexes
If a large number of documents change in a short period, you might want to perform a merge of the temporary indexes without waiting for the scheduled master merge. To initiate a merge, follow these steps:

1. Open Computer Management, and select Indexing Service in the console tree.
2. Right-click the appropriate catalog, point to All Tasks on the shortcut menu, and choose Merge. (See Figure 31-2.)
3. You’re asked to confirm that you want to merge the catalog. Click Yes.

Setting Up an Indexing Console
For easy and frequent access, ideally you should set up a Microsoft Management Console (MMC) with Indexing Service. To do so, follow these steps:

1. Choose Run from the Start menu. Type `mmc`, and press Enter.
2. Choose Add/Remove Snap-in from the File menu. Click Add.
3. In the Add Standalone Snap-In box, select Indexing Service and click Add. Select Local Computer.
4. Click Close and then OK, and you see an Indexing Service MMC like the one shown in Figure 31-3.
The illustrations and examples in the following sections use the Indexing Service MMC, but you can also perform these tasks just as well through Computer Management.

Creating and Configuring Catalogs

A catalog contains all the index information for a particular set of file directories. During installation, the Indexing Service creates a default catalog called System. This catalog lists the contents of all permanently attached disk drives and, by default, all the directories and subdirectories on the drives. If IIS is installed, the Indexing Service also creates a Web catalog that contains all the IIS files.

You can create catalogs, adding and removing them as needed. You can also configure catalogs, setting which directories are to be included or excluded and specifying which properties are to be stored.

Creating a Catalog

To create a catalog for the Indexing Service, open the MMC with the Indexing Service snap-in and follow these steps:

1. Highlight Indexing Service in the console tree.
2. From the Action menu, choose New, and then choose Catalog.
3. In the Add Catalog dialog box, supply a name for the catalog and a path to the folder in which you want the catalog placed. (See Figure 31-4.) Click OK.
4. You must stop and restart the Indexing Service before the new catalog can be found and indexed. Right-click Indexing Service, and choose Stop from the shortcut menu. To restart the Indexing Service, right-click Indexing Service again and choose Start from the shortcut menu.

**Note**  Catalogs can’t be added to a remote computer if the default administrative shares have been removed.

### Configuring a Catalog

After you create a catalog, you need to configure it so that it works as you expect. To do so, open the Indexing Service console and locate the catalog. Right-click the catalog, and choose Properties to do the following:

- **Index a Web server**  Click the Tracking tab and, in the WWW Server box, select the Web server you want to index. If IIS isn’t installed, this option isn’t available.

- **Index files with unknown extensions**  Click the Generation tab. Ordinarily, this setting is inherited from the overall Indexing Service properties and is inactive by default. If you want all the files in this catalog to be indexed, including those without installed filters, clear the Inherit Above Settings From Service check box. Select the Index Files With Unknown Extensions check box.

- **Generate abstracts**  Click the Generation tab. The Generate Abstracts setting is inherited from the overall Indexing Service properties and is inactive by default. To select this option, you must first clear the Inherit Settings From Service check box. If Generate Abstracts is selected, the Indexing Service produces abstracts in the list of query results. This slows the query process, so it’s best not to increase the default size of abstracts.
Add a network share alias automatically  
Click the Tracking tab. By default, this setting is inherited from the Indexing Service, where it is enabled.

With the exception of Generate Abstracts, all these changes take effect only after you stop and restart the catalog. To do so, right-click the catalog, point to All Tasks on the shortcut menu, and choose Stop. Then right-click again, point to All Tasks, and choose Start. If you change the Generate Abstracts setting, you need to stop and restart the Indexing Service for the change to be recognized.

Including or Excluding a Directory

By default, the System catalog includes everything on the local drives, excluding temporary Internet files and history files. When you create a new catalog, you have to add the directories that are to be included as well as specifically exclude directories that are not to be part of the index. To add a directory to a catalog, follow these steps:

1. Open the Indexing Service console. Right-click the new catalog, and select new and then Directory from the shortcut menu.
2. In the Add Directory dialog box, supply the path to the directory and the Uniform Naming Convention (UNC) path, if necessary.
3. If the directory is on another computer, supply a name and password for a user with permission to access the remote share, as shown in Figure 31-5. Click OK and the directory becomes part of the catalog.

To change settings for a directory, double-click the directory in the details pane of the Indexing Service console to open the Add Directory dialog box.

To exclude a particular directory, you must specify it. For example, the Bettiman Archives catalog shown being created in Figure 31-4 includes a directory called Book Files. In that directory is a subdirectory called Correspondence that you want to exclude from indexing.
To exclude a directory, follow these steps:

1. Open the Indexing Service console. Right-click the catalog, and select New and then Directory.

2. In the Add Directory dialog box, supply the path to the directory you want to exclude and the UNC path, if necessary. Again, if the directory is on another computer, supply a name and password for a user with permission to access the remote share.

3. In the Include In Index area, select No. Click OK.

The directory appears in the directory list, but under Include In Catalog, the entry is No.

**Note** Although you can include a directory and then specifically exclude a portion of it, this process does not work in reverse. If you exclude a directory, you cannot then include some portion of it, even if you specify the directory and set it to be included in the index. If you attempt to do this, the directory is in the catalog’s directories and is listed as being included in the catalog, but it is not indexed.

**Indexing and Security**

The Indexing Service is fully compatible with NTFS security. If the catalog is on an NTFS volume, users don’t see documents in the results list unless they have permission to do so. However, if you index a UNC share, the results list shows the documents on that share whether or not the user has permission to access the documents.

Users are also able to see a catalog on a FAT drive whether they have permissions or not. If the remote FAT volume isn’t hosted by Microsoft Windows NT, Windows 2000, or Windows Server 2003, the system is forced to scan the volume periodically for changes.

Remote Novell NetWare and UNIX shares can be indexed; however, there is no security checking. Novell NetWare volumes must be periodically rescanned to detect changes.

Encrypted documents are not indexed. If a document in the index is later encrypted, it is removed from the index.
Configuring the Property Cache

The Indexing Service saves certain file properties in a two-level cache in each catalog. The primary level contains a small number of values that are accessed frequently. The secondary level contains values that are used less often. Table 31-2 shows the properties that are stored in each catalog by default, though many more are available.

Table 31-2 Property values stored in a catalog by default

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Function</th>
<th>Value</th>
<th>Storage Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>DocTitle</td>
<td>Document title</td>
<td>0x2</td>
<td>Secondary</td>
</tr>
<tr>
<td></td>
<td>Unique identifier for NTFS volumes</td>
<td>0x5</td>
<td>Primary</td>
</tr>
<tr>
<td></td>
<td>Work ID of the parent directory</td>
<td>0x6</td>
<td>Primary</td>
</tr>
<tr>
<td></td>
<td>Secondary storage ID, used internally by the Indexing Service</td>
<td>0x7</td>
<td>Primary</td>
</tr>
<tr>
<td>File Index</td>
<td>Unique identifier of a document in an NTFS partition</td>
<td>0x8</td>
<td>Primary</td>
</tr>
<tr>
<td>Path</td>
<td>Document path</td>
<td>0xb</td>
<td>Secondary</td>
</tr>
<tr>
<td>Size</td>
<td>Document size</td>
<td>0xc</td>
<td>Secondary</td>
</tr>
<tr>
<td>Attrib</td>
<td>Document attributes</td>
<td>0xda</td>
<td>Primary</td>
</tr>
<tr>
<td>Write</td>
<td>Date and time the document was last written to</td>
<td>0xe</td>
<td>Secondary</td>
</tr>
</tbody>
</table>

In general, approach changing these properties with caution, always bearing in mind the following facts:

- Adding property values to either level—but particularly to the primary level—has a negative effect on the performance of the Indexing Service.
- Adding variable-length properties to the primary level increases the size of the cache exponentially.
- After you add a property value to either level and then restart indexing, you can’t change the level for that property.

But don’t assume that changing the property cache is always a poor idea. For example, information such as when files were created or when they were last accessed can be important, depending on your needs.

Adding a Property

To add a property to the properties saved in the property cache, follow these steps:

1. Open the Indexing Service console. Under the appropriate catalog, click Properties.
2. In the details pane, select the property you want to add.
3. From the Action menu, choose Properties to open the property’s Properties dialog box.
4. To include this property in the property cache, select the Cached check box. (See Figure 31-6.) You can see and change the datatype and the size of the property. (Only properties with variable sizes can be adjusted.) The storage level can also be assigned. Click OK when you’re done.

![Figure 31-6 Adding a property to be cached](image)

Changes take effect after the Indexing Service is stopped and restarted, but these newly added properties are included in the property cache only for new documents. To update the entire index with the newly included properties, perform a full scan of the index, as described in the next section. If you later decide to remove a property or alter its settings, you can do so by clearing the Cached check box in the property’s Properties dialog box. Again, a full scan is required to update the entire index.

**Running a Scan of the Index**

A full scan of the index consists of a complete inventory of all the documents in the catalog. The Indexing Service automatically performs a full scan when it is first installed, when a directory is added to a catalog, and as a part of recovery if an error occurs. Incremental scans are done automatically when the Indexing Service restarts to detect documents that were changed while it was inactive. You can perform a full or incremental scan at any time by following these steps:

1. Open the Indexing Service console. In the console tree, click the appropriate catalog and then click Directories.
2. In the details pane, select the directory to be scanned.

3. From the Action menu, point to All Tasks and then choose Rescan (Full) or Rescan (Incremental), depending on the type of scan you want to perform. You’re asked to confirm your choice. Click Yes and the scan proceeds.

---

**Registry Entries for the Indexing Service**

The Indexing Service is controlled by entries in the registry. These entries can be edited using Regedit.exe, although the usual caveats apply because a misstep in the registry can cause problems in not only the Indexing Service but elsewhere in Windows Server 2003 as well. Edit only those entries that you must. If the Indexing Service console has a method for making changes, use that instead. Always back up the registry before editing it.

Entries for the Indexing Service can be found in the registry at `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex`. Figure 31-7 shows some of the registry entries for the Indexing Service. (Remember, the values displayed by Regedit are in hexadecimal. An entry of 0x7530 is actually 30,000 in decimal.) Table 31-3 lists some of the critical operational parameters for the Indexing Service that are accessible through the registry.

![Registry Editor](image)

**Figure 31-7** Entries for the Indexing Service in the Registry
Table 31-3  Selected registry entries for the Indexing Service

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventLogFlags</td>
<td>Controls the generation of event log messages.</td>
</tr>
<tr>
<td>FilterContents</td>
<td>Indicates whether the contents of a file will be filtered or whether only the properties of the file will be filtered. A value of 0 specifies that the contents will not be filtered. With any other value, the file will be filtered.</td>
</tr>
<tr>
<td>FilterDirectories</td>
<td>When set to a value of 0, directories will not be filtered for system properties or displayed in query results. With any other value, the directories will be filtered.</td>
</tr>
<tr>
<td>FilterFilesWithUnknown-Extensions</td>
<td>Indicates whether files with nonregistered extensions will be filtered. When set to a value of 0, only registered file types will be filtered.</td>
</tr>
<tr>
<td>FilterRetries</td>
<td>Indicates the maximum number of times a file will be retried for filtering after a failure.</td>
</tr>
<tr>
<td>GenerateCharacterization</td>
<td>Controls the automatic generation of file abstracts.</td>
</tr>
<tr>
<td>IsapiMaxEntriesInQueryCache</td>
<td>Shows the maximum number of cached queries.</td>
</tr>
<tr>
<td>IsapiMaxRecordsInResultSet</td>
<td>Indicates the maximum number of rows to return for a single query.</td>
</tr>
<tr>
<td>IsapiMaxRecordsPerGetRows</td>
<td>Indicates the maximum number of rows to fetch when getting data to display on an HTML page.</td>
</tr>
<tr>
<td>IsapiRequestQueueSize</td>
<td>Controls the maximum number of Web query requests to queue when the server is busy with other requests.</td>
</tr>
<tr>
<td>MasterMergeTime</td>
<td>Indicates the time at which a master merge will occur. This value is stored as the number of minutes after midnight. (The default is 60 minutes after midnight.)</td>
</tr>
<tr>
<td>MaxCharacterization</td>
<td>Shows the maximum number of characters in abstracts generated automatically.</td>
</tr>
<tr>
<td>MaxFileSizeFiltered</td>
<td>Controls the maximum size in kilobytes of a single file to be filtered using the default filter. If the size of a file exceeds this value, only file properties will be filtered. This limit does not apply for registered file types. The default is 256.</td>
</tr>
<tr>
<td>MaxFreshCount</td>
<td>Specifies the maximum number of files whose latest indexed data is not in the master index. (The default is 100,000.) If this number is exceeded, a master merge is performed.</td>
</tr>
<tr>
<td>MaxIndexes</td>
<td>Sets the maximum number of saved indexes in the catalog. If this number is exceeded (25 is the default), a shadow merge is performed.</td>
</tr>
</tbody>
</table>
Querying the Index

The simplest way to query the index is to use the Search operation on the Start menu. Point to Search, choose For Files And Folders, and type a filename or a single word from the text or some other known property. Depending on the number of documents to be searched, the use of the Indexing Service can make a remarkable difference in search times. Even in small-sized to medium-sized databases, a search that takes 10 seconds without indexing appears instantaneous with indexing.

Queries can also be performed using the Indexing Service query form, which enables wide-range searches. Clicking the Query The Catalog directory in the Indexing Service console opens the query form. (See Figure 31-8.)

<table>
<thead>
<tr>
<th>Registry Entry</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxPendingDocuments</td>
<td>Sets the maximum number of pending documents to be filtered before considering the content index out of date for property queries.</td>
</tr>
<tr>
<td>MaxQueryExecutionTime</td>
<td>Identifies the maximum execution time (in seconds) for a query. If the CPU time for a query takes longer than this value, processing stops and an error message is returned.</td>
</tr>
<tr>
<td>MaxShadowFreeForceMerge</td>
<td>A master merge is forced when free space on the catalog hard disk has fallen below the MinDiskFreeForceMerge value and the disk space occupied by the shadow indexes exceeds this value.</td>
</tr>
<tr>
<td>MaxShadowIndexSize</td>
<td>A master merge is started when the disk space occupied by the shadow indexes exceeds this percentage of the catalog drive.</td>
</tr>
<tr>
<td>MaxWordLists</td>
<td>Sets the maximum number of word lists that can exist at a time. The default is 20.</td>
</tr>
<tr>
<td>MinDiskFreeForceMerge</td>
<td>A master merge is forced when the free space on the catalog drive has fallen below the amount set here (the default is 15 MB) and the disk space occupied by the shadow indexes exceeds the value of MaxShadowFreeForceMerge.</td>
</tr>
<tr>
<td>MinSizeMergeWordLists</td>
<td>Sets the minimum combined size of word lists that will force a shadow merge.</td>
</tr>
</tbody>
</table>
With the query form, you can do the following:

- Search for words and phrases.
- Search for words or phrases that are in proximity to other words or phrases.
- Search for words or phrases within textual properties. For example, you can search for a word that appears in a document’s abstract or summary.
- Search for words or phrases in specific document formats, such as within a Microsoft Excel spreadsheet or a Microsoft PowerPoint presentation.
- Use the relational operators $<$, $<=$, $=$, $=>$, $>$, and $!=$ against a constant, such as a date or file size.
- Use the Boolean operators AND, OR, AND NOT, and NEAR. (Note that the Boolean operators are available only in the English language.)
- Use wildcard characters such as * and ? and regular expressions for “fuzzy” queries.
- Rank results by the quality of the match.

The Indexing Service uses three types of files—very similar to those implemented by IIS—to allow the development of custom query forms, formatted results pages, and administrative scripts. These file types are as follows:

- Internet data query files
Creating Query Forms

With a query form, you can conveniently search for a word or phrase anywhere in a set of documents. The user simply types a word or phrase, and all documents containing the word or phrase are returned in a list.

With the Indexing Service, the administrator of a Web server can create customized forms to help employees and other clients find specific information from a set of documents. For example, a form can be tailored to search for a word or phrase (such as “systems management”) or for properties (such as the author or subject). You create a query form in standard HTML format, just as you create any Web page. If you know how to create pages in HTML format, you can quickly put together a simple query form such as the following:

```html
<Form Action="/scripts/querydemo.idq?" Method="POST">
So what's your question?:
<Input Type="TEXT" Name="CiRestriction" Size="60" MaxLength="100" Value="">
<Input Type="SUBMIT" Value="Start Search">
<Input Type="RESET" Value="Clear">
</Form>
```

More Info For assistance in creating a query using ASP.NET, go to http://support.microsoft.com and search for Knowledge Base Article 311521.

The `<FORM ACTION>` line shows the location of the .IDQ (Internet data query) file, which defines query parameters such as the scope of your search, any restrictions, and query result sets. A basic .IDQ file looks something like this:

```
[Query]
CiColumns=filename,size,rank,characterization,vpath,DocTitle,write
CiFlags=DEEP
CiRestriction=%CiRestriction%
CiMaxRecordsInResultSet=100
CiMaxRecordsPerPage=25
CiScope=/
CiTemplate=/scripts/bdq.htx
CiSort=rank[d]
CiCatalog=d:\
```

The following list explains each line of the sample .IDQ file:

```
[Query]
Identifies the information that follows as a query specification.
CiColumns=filename,size,rank,characterization,vpath,DocTitle,write
```

- HTML extension files
- Index data administration files
Indicates the kind of information to return in the result set.

CiFlags=DEEP

Tells the query to search all subdirectories within the scope.

CiRestriction=%CiRestriction%

Indicates the query terms to search for.

CiMaxRecordsInResultSet=100

Sets the maximum number of results to be returned, 100 in this example.

CiMaxRecordsPerPage=25

Determines how many results are shown on each Web page returned, 25 in this example.

CiScope=/

Tells where to start the query. In this example, the query starts at the root of the storage space.

CiTemplate=/scripts/bdq.htx

Indicates what file to use to format the results; in this case, it's Bdq.htx.

---

“File Not Found” Errors

When you issue a query in the Indexing Service, the result set might include links to documents that were recently deleted from the server. Clicking on these links returns “file not found” errors. This problem occurs when you index and then delete files that contain long filenames. When these files are created, Windows Server 2003 creates an 8.3 short filename so that older applications can access the document. When the Indexing Service catalogs these files, it stores the information for both the long and short filenames. However, when the file is deleted, the Indexing Service removes only the information on the short filename from the catalog. Queries that match the document still return hits to the entry for the long filename.

This long filename entry is usually removed when a master merge occurs, but it might not happen soon enough to prevent users from becoming annoyed. If this becomes a problem, you can edit the registry to prevent Windows Server 2003 from creating short filenames for older applications. To do this, open the Registry Editor (Regedit.exe), and navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem. Set the NtfsDisable8dot3NameCreation value to 1.

The usual warnings apply regarding backing up the registry before altering it.
CiSort=rank[d]

Tells how to sort the results. In this example, the results will be listed by rank—by how well the document matches the query—and [d] indicates that the results will be listed in descending order.

CiCatalog=d:"

Points to the index to use. In this example, the index stored on d: is to be used.

The combination of the sample HTML file and the sample .IDQ file produces the query form shown in Figure 31-9.

![Figure 31-9 A simple query form](image)

**Indexing a New Site**

When you create a new Web site, it isn’t automatically marked as indexed when you create a catalog for it. To correctly index a new Web site, follow these steps:

1. Open the Indexing Service console, and create a new catalog.
2. Right-click the new catalog, and choose Properties from the shortcut menu.
3. Click the Tracking tab, and select the Web site you want to index. Click OK.
4. Open the Internet Information Services console. Right-click the appropriate Web site, and choose Properties from the shortcut menu.
5. Click the Home Directory tab, select the Index This Resource check box, and click OK.
6. Stop the Indexing Service and then restart it. The new catalog should come online and begin indexing the new Web site.
Examining Performance

The performance of the Indexing Service depends, obviously, on the number and size of the documents being indexed and the resources available to the Indexing Service. When the number of documents being indexed is fewer than 100,000, no special hardware or tuning is likely to be needed. The Indexing Service works in the background and without attention. As the number of documents grows, however, performance begins to lag unless sufficient memory is available.

Modifying the Indexing Service’s Performance

You can adjust the performance of the Indexing Service based on how you use the service. It’s not always necessary to perform hardware upgrades. Instead, you can reduce the amount of resources needed for indexing by reducing the demand that indexing places on the system. Alternatively, you can give the Indexing Service a high priority on a given system when many documents need to be processed. To adjust the Indexing Service’s performance, follow these steps:

1. Open the Indexing Service console. In the console tree, right-click Indexing Service and choose Stop from the shortcut menu.
2. From the Action menu, point to All Tasks and choose Tune Performance.
3. In the Indexing Service Usage dialog box, you can select the option that best describes how this computer uses indexing:
   - **Dedicated Server** Adjusts performance settings to provide maximum Indexing Service performance. The underlying settings are “Instant” indexing and “High Load” querying.
   - **Used Often, But Not Dedicated To This Service** Adjusts performance settings to provide improved performance. The underlying settings are “Lazy” indexing and “Moderate Load” querying. (This is the default setting.)
   - **Used Occasionally** Adjusts performance settings to provide lowest resource utilization at the expense of some performance loss. The underlying settings are “Lazy” indexing and “Low Load” querying.
   - **Never Used** Turns off Indexing Service.
   - **Customize** Allows the use of custom settings.
4. If you select the Customize option and then click Customize, the dialog box shown in Figure 31-10 opens.
Move the Indexing slider to Instant for immediate indexing of all new and modified documents. Move the slider to Lazy for indexing to take place when the system isn’t busy with other tasks and for indexing that does not affect overall system performance.

Move the Querying slider to High Load for processing many queries at a time. Move the slider to Low Load if few queries are expected at a time.

![Image](image.png)

**Figure 31-10** Customizing indexing performance

5. Click OK twice when you’re finished.

Changes to the Indexing Service’s performance are unlikely to have noticeable results except in an environment where indexing needs are either very high or very low. In most environments, the Indexing Service works unobtrusively in the background without fine-tuning.

**Using Performance Monitor**

Chapter 35 describes how to use the data from Performance Monitor to target processes and components that need to be optimized, monitor the results of tuning and configuration efforts, and understand and observe the trends in workloads and the corresponding effect they have on resource usage. Among the many performance counters available in Windows Server 2003 are several that can assist in monitoring the Indexing Service and the Indexing Service Filter. Table 31-4 lists the relevant counters and what they measure. See Chapter 35 for details about analyzing performance data to determine acceptable values for counters and for information about solving any performance problems that are found.
Troubleshooting the Indexing Service

This section lists common error messages and possible solutions. Some of the most common problems with the Indexing Service can be fixed quite easily. For more complex issues, search the Microsoft Knowledge Base online at http://support.microsoft.com/search for solutions.

No Documents Matched the Query

Instead of receiving a list of matching documents when you perform a query using the Indexing Service, you might receive the error message “No Documents Matched the Query.” This common error means that the catalog is responding correctly but that

<table>
<thead>
<tr>
<th>Performance Object</th>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indexing Service</td>
<td>Number of documents indexed</td>
<td>Number of documents indexed in the current indexing session</td>
</tr>
<tr>
<td></td>
<td>Deferred for indexing</td>
<td>Number of documents in use that need to be indexed</td>
</tr>
<tr>
<td></td>
<td>Documents to be indexed</td>
<td>Smallest number of documents known to need indexing</td>
</tr>
<tr>
<td></td>
<td>Index size (MB)</td>
<td>Total size, in megabytes, of all saved indexes</td>
</tr>
<tr>
<td></td>
<td>Merge progress</td>
<td>Percentage of merge completed</td>
</tr>
<tr>
<td></td>
<td>Running queries</td>
<td>Number of queries currently being processed</td>
</tr>
<tr>
<td></td>
<td>Saved indexes</td>
<td>Number of saved indexes</td>
</tr>
<tr>
<td></td>
<td>Total number of documents</td>
<td>Number of documents known to the Indexing Service</td>
</tr>
<tr>
<td></td>
<td>Total number of queries</td>
<td>Total number of queries that have been conducted in the current indexing session</td>
</tr>
<tr>
<td></td>
<td>Unique keys</td>
<td>Number of unique keys (words, properties) in the index</td>
</tr>
<tr>
<td></td>
<td>Word lists</td>
<td>Total number of word lists</td>
</tr>
<tr>
<td>Indexing Service Filter</td>
<td>Binding time (msec)</td>
<td>Average time in milliseconds to bind to a filter</td>
</tr>
<tr>
<td></td>
<td>Indexing speed (MBph)</td>
<td>Speed of indexing document contents in megabytes per hour</td>
</tr>
<tr>
<td></td>
<td>Total indexing speed (MBph)</td>
<td>Speed of indexing document contents and properties, in megabytes per hour</td>
</tr>
</tbody>
</table>

Table 31-4 Performance Monitor counters related to the Indexing Service
there is an incorrect setting somewhere. To find the incorrect setting, try each of the following procedures in turn, testing after each one:

- In an .IDQ file, you should see a line like the following:

  \texttt{CiCatalog=d:\inetpub\wwwroot\tmjs_index}

  You might need to change the pointer to the catalog if you are not using the default catalog. Make sure the path is pointing to the directory that contains the catalog’s Catalog.wci directory.

- In the code of your page, make sure that the following is true:

  \texttt{CiScope=/}
  \texttt{CiRestriction=%CiRestriction%}
  \texttt{CiCatalog=<path to the directory holding the Catalog.wci directory>}

- Launch Internet Information Services (IIS) Manager from the Administrative Tools folder on the Programs menu. Right-click the root of your Web site and choose Properties. In the Home Directory tab, make sure that the Index This Resource check box is selected. Try your query again.

- The Indexing Service does its indexing as the System account. If the System account does not have at least Read permissions on the files that are to be cataloged, the files are not indexed. Also, make sure that the System account has Full Access permissions on the root of the drive that physically contains the catalog and on the Catalog.wci directory.

- Users are allowed to view only results that they have permissions to see. If you are accessing the query page as an anonymous user, make sure that the anonymous user has at least Read permission on the document you are trying to find.

- Authenticate coming into the query page as an administrator if possible. Try setting the directory that the query page is located in to Basic/Clear Text authentication only, so that you receive a prompt when you attempt to connect to that page. If you get results, you have a permissions issue. If you log on as an administrator and still receive a “No Documents Matched the Query” message, you probably do not have a permissions issue.

- If you are querying on a specific page and it is returning in a \texttt{#filename} query but it is not being filtered (the abstract is not populated), and it is an HTM, HTML, or ASP page, make sure you do not have a ROBOTS=NOINDEX metatag in the header of the document. This does not prevent indexing, but it does prevent filtering.
PDF Files Aren’t Indexed

Adobe makes a free filter called Adobe PDF IFilter v6.0 that enables the indexing of .PDF (Portable Document Format) files. After you install the filter, .PDF files might not be indexed after the Indexing Service is restarted or the computer is restarted.

The problem is caused when the Indexing Service restarts and reregisters all the filter .DLL files. One of these .DLL files has a default association with the .PDF extension and therefore registers itself as the filter for these files. To fix this problem, ensure that the list of filter .DLL files includes the PDF filter by following these steps:

1. Stop the Indexing Service. (Right-click Indexing Service in the console pane, and select Stop.)
2. Start the Registry Editor (Regedit.exe).
3. Locate the following key in the registry:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex
4. Add the path to the Pdffilt.dll to the DLLsToRegister key. The path to the PDF filter should be added as the last entry in this key.
5. Close the Registry Editor. Restart the Indexing Service.


Query Produces Inconsistent Results

When you use the Indexing Service to run a query and you set the sort method to anything other than Rank Descending, you do not receive the top matching records and you might get a different set of files on subsequent queries. Sorting on Rank Descending is the only way to get the top matching records from the catalog when the maximum number of returns is limited. Sorting on anything other than Rank Descending returns a subset of the total set of matching documents.

Catalog Is Reportedly Corrupted

If the Indexing Service reports that the catalog is corrupted after the indexing process is completed, it means that a file can’t be filtered and that Filter Retries is set to a number greater than 4. This can occur as soon as the indexing process has completed or several minutes later.

When this happens, the information that the filter process sends to the Indexing Service causes a report that the catalog information is corrupted even though the data on
the drive is fine. To fix this, start the Registry Editor (Regedit.exe) and navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex\FilterRetries. Change the value of this key to 4 or less, close Registry Editor, and restart the Indexing Service.

**Indexing Is Slow and Some Documents Aren’t Indexed**

On occasion, it might take an extremely long time to index documents, and some documents might appear not to get indexed at all. In addition, the abstract for documents might be blank or contain incorrect information. This is usually caused by third-party software that places a lock on the Web content you are attempting to index. Antivirus software programs and any other software that monitors or scans your Web content for extended periods of time can cause this problem. To work around this problem, disable any software that may be monitoring the Web content.

**More Info** For more about the Indexing Service, visit the public newsgroup microsoft.public.inetserver.indexserver or search for “indexing service” on http://www.microsoft.com. Another good source of information about Index Server is the Index Server FAQ, which can be found at http://www.indexserverfaq.com.

**Summary**

The Indexing Service offers administrators of Web sites or networks with large numbers of documents a way to locate and access documents quickly and easily. Queries can be delimited by document contents and properties. The next chapter begins the portion of the book devoted to Internet servers and services with a discussion of the basics of Internet Information Services.
Part VI
Internet Servers and Services

Chapter 32
Basics of Internet Information Services ......................... 1037

Chapter 33
Advanced Internet Information Services ......................... 1069

Chapter 34
Internet Security and Acceleration Server 2004 ................. 1123
Chapter 32

Basics of Internet Information Services

Protocols Supported .................................................. 1037
Administration Tools .................................................. 1044
The WWW Publishing Service ....................................... 1047
The FTP Publishing Service ........................................... 1058
Basic Administrative Tasks .......................................... 1062
Summary .................................................................... 1068

Microsoft Windows Server 2003 incorporates a set of services that provide server-side support for the most popular application-level Internet protocols, enabling your server to function as a Web server, a File Transfer Protocol (FTP) server, a Simple Mail Transfer Protocol (SMTP) host, or a Network News Transfer Protocol (NNTP) host.

Basic Internet services are fully integrated into all the Windows Server platforms, and are fully integrated with each operating system. This chapter examines the protocols that Internet Information Services (IIS) 6 supports, along with the other tools you can use to manage Internet services on Windows Server platforms. Chapter 33 takes a more detailed look at how to configure the services described in this chapter.


Protocols Supported

In Chapter 16, the discussion of the TCP/IP suite focused mainly on the network-layer protocols (such as IP) and transport-layer protocols (such as TCP and UDP) and how they work. The only application-layer protocols considered were the rather specialized ones called DHCP and DNS, which provide addressing and name resolution functions on TCP/IP internetworks such as the Internet.
In addition, TCP/IP includes a whole series of application-layer protocols whose function is to allow users to interface with client/server applications and distributed applications on an internetwork. Examples of these protocols include Telnet, HTTP, FTP, Gopher, SMTP, NNTP, and so on. Other protocols, such as Simple Network Management Protocol (SNMP) and remote network monitoring, provide network management functions to simplify management of hosts on an internetwork. And because TCP/IP is constantly evolving, protocols are being enhanced and newer ones are emerging as older ones become obsolete.

As outlined in the next four sections, Microsoft chose to implement four of these application-layer protocols within the framework of IIS 6 on Windows Server 2003.

**HTTP**

As you probably already know, HTTP is the application-layer protocol of TCP/IP that makes the Web possible. This protocol handles the publishing of static and dynamic Web content on Windows Server 2003. Publishing a Web page you create is simply a matter of telling your server software (for example, IIS) the Web page is available. You learn how to do this later in this chapter.

HTTP defines a client/server protocol that describes how communications occur between HTTP servers (called Web servers) and HTTP clients (called Web browsers). The following is a typical HTTP session between a Windows Server 2003 machine running IIS 6 (a Web server), and a client machine running Microsoft Internet Explorer 6 (a Web browser). An HTTP session is essentially made up of a connection, a request, and a response:

1. The client machine uses TCP to establish a connection to the server, typically using port 80, which is the default or well-known port number for HTTP connections. You can specify other port numbers on the server if you want, but the client then needs to know the port number to connect to the server. The connection is formed using a standard TCP three-way handshake.

2. After connecting to the server, the client machine requests a Web page or some other file from the server. The user can specify the page by typing its URL in the Address box in Internet Explorer, or by clicking a hyperlink on another page to request the new one. Either way, the client sends a packet to the server containing an HTTP Get Request message. A typical client’s Get Request message might look like the following:

```
GET /html/web.htm HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/msword, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1; .NET CLR 1.0.2817)
Host: 192.168.1.128
Connection: Keep-Alive
```
The various lines of this request are called headers, and these headers allow the client to communicate information such as the following to the server:

- The particular Web page or other file that is being requested (in this example, the Web page `/html/web.htm`)
- The fact that the client supports version 1.1 of HTTP
- The Multipurpose Internet Mail Extensions (MIME) types, languages, and encoding methods that the client understands
- The type of client being used, which in this example is Internet Explorer 6
- The Web server from which the page is requested (in this example, the server at IP address 192.168.1.128)
- Various other information, such as the fact that HTTP Keep-Alives are enabled on the client

The server responds to the request by sending a series of packets containing the Web page or other content requested by the client. The first of these returned packets contains header information, which the server sends to the client. The first few lines returned are headers that tell the client about what HTML version is supported, the type of server, the date and time, and other information.

After the headers comes the beginning of the actual Web page requested by the client, showing the HTML that formats the information for the client so that it can be displayed as a Web page.

3. At this point, if HTTP Keep-Alives are enabled, the TCP connection between the client and server stays open in case the client wants to request additional files from the server. If Keep-Alives are disabled, the TCP connection is terminated after the page is downloaded, and a new TCP connection must be established to download the next file (an embedded image within the page, for example). Establishing this connection can be difficult if, for example, the Web page you are downloading has 33 embedded images, 3 Java applets, 1 ShockWave animation, and other sophisticated content. Without Keep-Alives, the additional overhead of establishing and tearing down TCP connections for each file downloaded slows the process down a bit, so it’s usually smart to leave Keep-Alives enabled (as explained in the Chapter 33).

More Info  Version 1.1 of Hypertext Transfer Protocol is defined in RFC 2616.

That’s basically all there is to HTTP. It’s a simple client/server application-layer protocol based on the underlying TCP transport-layer protocol. HTTP is by far the most important of the four Internet protocols supported by IIS, and it is the basis of the Web.
Real World  Troubleshooting HTTP Sessions

Unless Internet communications are specifically encrypted using the Secure Sockets Layer (SSL) protocol, HTTP sessions are transmitted in clear (unencrypted) text, which allows you to view the header information in HTTP packets using a tool such as Network Monitor. You can optionally install Network Monitor on Windows Server 2003 using Add/Remove Programs in Control Panel and selecting Add/Remove Windows Components. Then select the Management And Monitoring Tools component, and click Details to access the Network Monitor Tools option. Network Monitor is often useful when you are trying to troubleshoot HTTP session problems.

Another useful tool for troubleshooting HTTP session problems is the telnet client program that is started from the command line. By starting telnet and opening a connection to the server using the HTTP port 80 instead of the usual telnet port 20, you can manually enter HTTP Get Request headers and view the results. Note that after typing your headers, you enter a single blank line (CR/LF) to transmit the request to the server. Make sure you have Local Echo enabled on your telnet client and that you have set a large buffer size as well, to receive the response from the server.

FTP

FTP is an earlier TCP/IP application-layer protocol that enables users to transfer files over an internetwork such as the Internet. FTP defines a client/server protocol that describes how communications take place between FTP servers and FTP clients. Specifically, FTP enables clients to upload files to or download files from an FTP server over an internetwork. A typical FTP session is essentially made up of a connection, request, and response, as the following example shows:

1. The client forms a TCP connection with port 21 on the server. Port 21 is the standard TCP port that an FTP server continually “listens” to for FTP clients’ connection attempts. After a connection is formed, a randomly assigned port number above 1023 is given to the client. This initial TCP connection is used for transmission of FTP control information—that is, for commands sent from the client to the server—and for response codes returned from the server to the client.

2. The client then issues an FTP command to port 21 on the server using the first TCP connection established in Step 1. These commands are all issued as clear (unencrypted) text over the Internet connection, which means you can use the same tools (Network Monitor and telnet) to monitor and troubleshoot FTP sessions that you can use for HTTP. Typical FTP commands include Get (download a file), Put (upload a file), Binary (switch to binary mode), Cd (change to a different directory on the server), and so on.
3. If the command issued by the client initiates a data transfer (upload or download) with the server, the server opens a second TCP connection with the client for performing the transfer. This second TCP connection uses port 20 on the server and a randomly assigned port number greater than 1023 on the client. (The first TCP connection—to port 21 on the server—is used only to send control information between the client and server, not for data transfer.)

More Info  The File Transfer Protocol is defined in RFC 959.

4. After the data transfer is complete, the second TCP connection goes into a TIME_WAIT state until either another data transfer takes place or the connection times out.

Note  You can use the Netstat utility from the command line to view information about TCP connections that FTP uses. Just open a command-prompt window on the client or server, and type `Netstat -p tcp` to see the active TCP connections.

**SMTP**

SMTP is a popular TCP/IP application-layer protocol that forms the basis of the Internet’s e-mail system.

SMTP is both a client/server and server/server protocol, and it is used essentially for transferring e-mail from one SMTP host to another over an internetwork. A typical SMTP session begins with a connection followed by a series of commands. For example, consider the following scenario, in which the local (initiating) SMTP host wants to transfer e-mail to the remote (responding) SMTP host:

1. An SMTP client connects to a local SMTP host to send an e-mail message addressed to a user residing in the domain of a remote SMTP host. The local host is responsible for transferring the message to the remote host so that the intended recipient is able to receive it.

2. The local SMTP host forms a TCP connection on port 25 with the remote SMTP host using a standard TCP three-way handshake. After the connection is established, the remote host returns a Ready response to the local host, indicating that it’s ready to initiate an SMTP session.

3. The local host issues a Hello command, to which the remote host responds with OK. An SMTP session is now established.

4. The local host issues a Mail From command indicating the name of the user who sent the e-mail. The remote host responds with OK.
5. The local host issues a Rcpt To command indicating the name of the user to whom the e-mail is directed. The remote host responds with OK.

6. The local host issues a Data command indicating that the body of the message will now be transferred. The remote host responds with OK.

7. The message body is then transferred as a data stream of 7-bit ASCII characters. (8-bit binary data must be encoded into 7-bit ASCII data using the MIME protocol because SMTP understands only ASCII.) The local host indicates the end of the data stream with a period (.), which is on a line by itself.

8. If the intended recipient is running the SMTP client and is connected to the remote host, the recipient then receives the message that the sender addressed to him or her (but see the Real World sidebar “SMTP Limitations”).

9. Further messages are then transferred. The local host terminates the SMTP session by issuing a Quit command, after which the TCP connection between the hosts is terminated.

---

**More Info**  The Simple Mail Transfer Protocol is defined in RFC 2821.

---

**Real World  SMTP Limitations**

SMTP is designed mainly for moving e-mail from one SMTP host to another, and it has no facility to store messages in folders for users so that the messages can be retrieved and read later. SMTP clients must therefore be continually connected to an SMTP host to retrieve and read their e-mail; otherwise, the e-mail is returned to the sender. As a result, other Internet e-mail protocols were developed to enable e-mail to be temporarily stored until users can connect to retrieve their messages.

The most popular of these protocols are Post Office Protocol version 3 (POP3) and Internet Message Access Protocol version 4 (IMAP4). However, IIS 6 in Windows Server 2003 supports neither of these protocols because the SMTP service is primarily intended to provide e-mail–sending capability to Active Server Pages (ASP) applications running on IIS—it’s not designed to function as a corporate e-mail server. If you want the full Internet capabilities of a corporate SMTP/POP3/IMAP4 e-mail server, you can use Microsoft Exchange Server for this purpose. Windows Server 2003 does include a standalone POP3 service, though it’s not part of IIS and hence isn’t covered in detail here. Install it just like other Windows components (that is, go to Control Panel, Add Or Remove Programs, Add/Remove Windows Components, Email Services).
NNTP

NNTP is a TCP/IP application-layer protocol that forms the basis of the USENET system of newsgroups used on the Internet. NNTP is both a client/server protocol and a server/server protocol that provides the following functionality:

- Allows an NNTP client (newsreader) to connect to an NNTP server (host) to download a list of available newsgroups on the server, read individual messages in the newsgroups, and reply to existing messages or post new ones to the server.
- Allows one NNTP host to replicate its list of newsgroups and their messages with another host on an internetwork. This replication between hosts is performed by using newsfeeds (or simply feeds), which can be either pushed or pulled between hosts.

Some of the commands a newsreader can use during a session with a host include the following:

- **List**  Retrieves a list of newsgroups available on the host
- **Group**  Selects a particular newsgroup from which to retrieve messages
- **Article**  Retrieves a specific message from a newsgroup

More Info  The Network News Transfer Protocol is defined in RFC 977.

The commands used for communications between hosts (called **NNTP control messages**) include these:

- **Newgroup**  Indicates that a new newsgroup has been created
- **Rmgroup**  Indicates that a newsgroup should be deleted
- **Cancel**  Indicates that a specific message in a newsgroup should be deleted

More Info  A full discussion of an NNTP session is beyond the scope of this book, but you can learn more about NNTP control messages in RFC 1036.

Other Protocols

Although IIS 6 supports only the four application-layer Internet protocols just described, it does support other complementary Internet protocols that provide enhanced functionality to HTTP, FTP, SMTP, and NNTP. These additional protocols include the following:

- **Secure Sockets Layer (SSL)**  Used to encrypt authentication and data transmission for HTTP and NNTP transmission using public-key cryptography
- **Transport Layer Security (TLS)**  Used for encrypting SMTP transmissions only. A variant of SSL
Lightweight Directory Access Protocol (LDAP)  Used by the SMTP service for accessing information in a directory service

Multipurpose Internet Mail Extensions (MIME)  Used by the HTTP service for communicating acceptable file formats to HTTP clients

More Info  A full discussion of these four Internet protocols is beyond the scope of this book, but you can find various RFCs associated with them by using the RFC Editor Search page at http://www.rfc-editor.org/rfcsearch.html.

Administration Tools

Windows Server 2003 contains a variety of tools for administering the four core IIS 6 services just discussed. The next several sections describe the tools for administering these services.

Adding the Application Server Role

By default, new installations of Windows Server 2003 have no server roles activated. IIS is not installed. This is a security measure; there is no reason to enable it if it will go unused, unconfigured, and possibly unprotected against ever-changing threats. Through the Manage Your Server application, you can install the components necessary for IIS. Start the application by selecting it from the top of the Start Menu. Select Add Or Remove A Role from the list on Manage Your Server’s main window and the Preliminary Steps window describing the process appears. Click Next. Your current settings will be detected, and the Configure Your Server Wizard will start.

The initial wizard display lists the available roles your server can assume. (See Figure 32-1.) Select Application server (IIS, ASP.NET), and click Next.

![Figure 32-1  Adding the Application server role to your server](image-url)
You can remove roles in the same place. Simply select the role you want to remove and click Next. You'll see a confirmation dialog box describing what you're about to remove, in case you change your mind.

In the next step of the wizard, you can add either FrontPage Server Extensions or ASP.NET. Click Next. The next dialog box presents a summary of your choices so far. Click Next to commit the changes to your server's configuration. (You might need the installation media, so be prepared.) After a few moments, you will see a dialog box with the message “This Server is Now an Application server.” Next, you'll need to configure IIS for your specific needs.

You can also install IIS through Control Panel, Add Or Remove Programs, Add/Remove Windows Components, or you can install it through an unattended setup, for which you create an answer file that responds automatically to the setup questions.

**Internet Information Services**

The Internet Information Services (IIS) Manager, shown in Figure 32-2, is the primary tool used for administering IIS 6 on Windows Server 2003–based networks; therefore, it's the primary tool used for IIS 6 administration in this chapter and the next. To access IIS Manager, select Administrative Tools from the Start menu and then select IIS Manager.

The basic installation of IIS includes the common files needed by IIS, documentation, configuration tools, and the World Wide Web service. To modify the settings of the installed components, use IIS Manager. In Figure 32-2, you see that you're able to manage application pools, Web sites, and Web service extensions. You can install the optional IIS services by opening Control Panel, Add/Remove Programs, and selecting the Add/Remove Windows Components option. Select the Internet Information Services component, and click Details to make changes to the IIS configuration. Among the additional services available are the Background Intelligent Transfer Service (BITS), the FTP Service, Internet Printing, the NNTP Service, and the SMTP Service.
Internet Servers and Services

Figure 32-2  The Internet Information Services (IIS) Manager window

**Important**  IIS is initially installed in a secure mode that will serve only static content. Many features will be disabled unless explicitly enabled. Use the IIS Manager’s Web Service Extensions node to change this default behavior.

**Remote Administration**

The three primary methods of administering your IIS installation from another machine are the IIS Manager, the Remote Administration (HTML) Tool, and Remote Desktop.

- **IIS Manager**  You can administer IIS on a remote machine using the IIS Manager. Start IIS Manager, and either select Connect from the Internet Information Services node’s shortcut menu or click Add A Computer To The List in the IIS Manager toolbar.

- **Remote Administration Tool**  You must install the Remote Administration (HTML) Tool to enable the administration options from a remote browser. Go to Control Panel, Add Or Remove Programs, and select Add/Remove Windows Components. Select Internet Information Services and then click Details. Select the World Wide Web Publishing Service and click its Details button. Select the check box for the Remote Administration (HTML) option, and click OK. Acknowledge all choices to dismiss the cascade of dialog boxes and complete the installation. When the Remote Administration Tool is installed, you can use the address `https://hostname:8098` (where `hostname` is the name of the computer name) to remotely administer the IIS Web server.

- **Remote Desktop**  You can also use Remote Desktop to remotely administer IIS installations. Enable the Remote Desktop functionality by opening the System from Control Panel. Go to the Remote tab and select the Enable Remote Desktop On This Computer check box. Then you can configure the users you want to have this access.
Administration Scripts

To run administration scripts on Windows Server 2003, use the IIS Windows Management Instrumentation (WMI) interface or Active Directory Service Interfaces (ADSI). Either interface enables you to perform common administrative tasks such as creating new Web sites, configuring Web site security, creating virtual directories, stopping and starting Web sites, and so on. You can write these scripts in a number of COM-compatible languages, such as Visual Basic Scripting Edition (VBScript), Jscript, or Perl.

WMI is the preferred interface to the programmatic controls of IIS. It offers a number of advantages over ADSI, including query support and object model GUI tools.

Note  You can find more information about WMI in the document “WMI Reference.” It’s available on MSDN (http://msdn.microsoft.com).

It’s always easier to get started if you have some examples. Sample administration scripts can be found in the %SystemRoot%\System32 folder.

The WWW Publishing Service

In this section, you’ll learn about the steps you need to take to create your Web site and serve it to clients using IIS. You begin by examining the Default Web Site that is included as an example when you install Windows Server 2003 on a machine. Then you look at common tasks such as creating new Web sites and virtual directories. You also explore how to use Web sharing.

The Default Web Site

In Figure 32-2, you saw an administrator’s view of the Default Web Site—a series of sample configuration files whose default location on the server’s local file system is \Inetpub\wwwroot, the root directory for your Web site. The \Inetpub directory actually contains several important subdirectories, which are summarized in Table 32-1.

<table>
<thead>
<tr>
<th>Subdirectory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdminScripts</td>
<td>Sample IIS administration scripts.</td>
</tr>
<tr>
<td>ftproot</td>
<td>Root directory of Default FTP Site.</td>
</tr>
<tr>
<td>mailroot</td>
<td>Various folders used by the SMTP service.</td>
</tr>
<tr>
<td>nntpfile</td>
<td>Various folders used by the NNTP service.</td>
</tr>
</tbody>
</table>
Note that some of these subdirectories are present only if their related IIS optional components are installed on the server. You don’t necessarily need to store Web site content in any of these directories—content can be located in any directory on the server, or on a network share located on some other server, as you will soon see.

### Connecting to a Web Site

On the server, you can access the home page of the Default Web Site (Figure 32-3) in various ways by using a Web browser. Try these methods:

- From the local console, click Start, point to Run, type `http://127.0.0.1`, and click OK. This opens Internet Explorer and accesses the home page by using the TCP/IP loopback address.

- From the local console, start Internet Explorer, type `localhost` in the Address bar, and press Enter.

- From IIS Manager, select the Default Web Site node and then do one of the following:
  - Right-click and choose Browse from the shortcut menu
  - Click Action on the toolbar, and select Browse from the drop-down menu

**Table 32-1  IIS-related subdirectories located within the default \Inetpub directory**

<table>
<thead>
<tr>
<th>Subdirectory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scripts</td>
<td>Default location for application scripts used by the Default Web Site. Includes samples and tools.</td>
</tr>
<tr>
<td>wwwroot</td>
<td>Root directory of the Default Web Site.</td>
</tr>
</tbody>
</table>

Figure 32-3  The home page of the Default Web Site
When you attempt access from a remote machine on the connected network, you see an “Under Construction” message, but that message actually tells you that the site is active and accessible. To connect, start Internet Explorer, press Ctrl+O to open the Open dialog box, type any of the items in the following list, and then click OK:

- The IP address of the Web server (for example, 192.168.1.128)
- The NetBIOS name of the Web server (for example, Server)
- The DNS name of the Web server (for example, server.example.com), provided either a name server is accessible or the Hosts file is configured on the client

Other Web Sites

The Default Web Site is only one small example of how you can deploy a Web site using IIS 6. In fact, you can create as many Web sites as you want using IIS 6, and you can host the content (pages, images, and other files) for these sites in a variety of locations. Each Web site acts as a separate entity, or virtual server—that is, it acts as if it were running on its own server and using the full resources available to it on that server. To illustrate this, let’s create a new Web site on the server MyServer, create a simple home page for it, and then test it by connecting to it from another machine on the network.

Using the Web Site Creation Wizard

Before using the Web Site Creation Wizard to create a new Web site, you must decide how to name this site on the network. As you saw previously, when you use a Web browser such as Internet Explorer to connect to a Web site and view its home page, you can specify the URL of the site in a variety of ways, including using the site’s IP address, NetBIOS name, or fully qualified DNS name.

For this example, you bind a second IP address to the network interface card (NIC) on the Windows Server 2003 MyServer and establish a mapping between the new Web site you’ll create and the new IP address you’ll add. (Other ways to distinguish different Web sites on the same server are discussed in Chapter 33.) To add a second IP address, follow these steps:

1. Expand the Network Connections list in Control Panel and select the Local Area Connection icon.
2. On the General tab of the Local Area Connection Status dialog box, click Properties.
3. In the Local Area Connection Properties window, double-click Internet Protocol (TCP/IP).
4. In the Internet Protocol (TCP/IP) Properties window, click Advanced.
5. On the IP Settings tab in the Advanced TCP/IP Settings dialog box (Figure 32-4), click Add in the IP Addresses section. Then specify an additional IP address and subnet mask, and click Add.

6. Click OK until all dialog boxes have been closed.

![Figure 32-4 Adding IP addresses for Web site identities](image)

Two more steps are required prior to creating the site. First, establish a new directory (for example, C:\Company) on the local server, which will store the content for the new site. Then create a simple home page called Default.htm within this site, using basic HTML. If you aren’t familiar with HTML, type the following text into Notepad and save the file in the \Company directory as Default.htm, ensuring that your editor does not add a .TXT extension:

```html
<HTML>
<HEAD><TITLE>The Company Site</TITLE></HEAD>
<BODY>
<H1>Welcome to the Company's Web Site</H1>
This site is under construction!
</BODY>
</HTML>
```

Now create a new Web site called Company by following these steps:

1. Start IIS Manager on the machine acting as your Web server (or start it on a different server or workstation and connect to your Web server by clicking Action on the toolbar and selecting Connect from the drop-down menu), and select the server's name in the console tree.
2. Expand the server's node in the tree view, and right-click the Web Sites node. Point to New, and choose Web on the menu. The first page of the Web Site Creation Wizard appears (as shown in Figure 32-5). Click Next.

![Figure 32-5](image)

**Figure 32-5** The first page of the Web Site Creation Wizard

3. Type Company as the description for the site. This name is displayed in IIS Manager, and identifies the new site for the administrator. Click Next.

4. Specify your second IP address as the one to be mapped to the site, leaving the remaining settings as they are (Figure 32-6). Click Next.

![Figure 32-6](image)

**Figure 32-6** The IP Address And Port Settings page of the Web Site Creation Wizard
5. Specify the path to the home directory for the Web site as C:\Company. (Using the Browse button is the easiest way to do this.) Note that the home directory for your site can be either a local directory or a network share. Leave the check box selected to allow anonymous access to the Web site. (Because this is a public Web site, you want anyone to be able to access it.) Click Next.

6. Leave the access permissions set at their default settings. (These permissions are covered in more detail in Chapter 33.)

7. Click Next, and then click Finish to complete the wizard. The new Company Web site should appear as a node under your server’s node in IIS Manager, showing its single Web page Default.htm (as shown in Figure 32-7).

![Figure 32-7](Image)

The new Web site

**Testing the New Web Site**

To test the IP address mapping (that is, Web site identity) for the new Web site, go to a different machine on the network, start Internet Explorer, and open the URL http://192.168.1.129, which specifies the new Web site using its associated IP address. The page Default.htm should load in the browser window. (See Figure 32-8.) Note that if a name server mapped this IP address to a DNS name such as www.example.com, you can access the Web site by using http://www.example.com instead of by using the IP address.

As a further test, try opening http://192.168.1.128 or http://server instead.

![Figure 32-8](Image)

Testing the new Company Web site from a remote machine
Each of these URLs specifies an identity for the Default Web Site on the server and should open the default page for the site. (Remember, 192.168.1.129 was the IP address for the Company Web site.) Web site identities are covered in more detail in Chapter 33.

Virtual Directories

In the previous example, you created a new Web site called Company whose content was located in the home directory C:\Company on the server machine. To access content in this directory, you can use either of the following URLs:

- http://<IP_Address>, where <IP_Address> represents the IP address bound to the server’s NIC that is mapped to that particular Web site
- http://<DNS_Name>, where <DNS_Name> is the fully qualified DNS name (such as servername.domainname.com) that is associated on the name server with the IP address mapped to that particular Web site

Taking the first URL, you can associate or map a particular URL with the Web content stored in the site’s home directory as represented here:

C:\Company ↔ http://192.168.1.129

But what if you want to locate content for this Web site in a variety of locations and not just in the \Company directory on the server? You can do this by using something called a virtual directory. A virtual directory is a way of mapping an alias (a portion of a URL) to a physical directory containing additional Web site content not located in the home directory for the site.

For example, say you want to store additional content in the directory C:\SalesData on the local server and associate it with the virtual directory /Sales. Note that the virtual directory uses a forward slash (/) instead of a backslash (\). The URL-to-directory mapping is

C:\SalesData ↔ http://192.168.1.129/sales

Note that from the point of view of the client using the Web browser, the /sales content appears as a subdirectory of the home directory for Company. In other words, the content virtually appears as a subdirectory of the home directory http://192.168.1.129. But in fact, the content is physically located in an entirely separate part of the directory tree on the server’s file system (instead of being located in \Company\sales, as you might expect from the URL). Virtual directories thus enable a kind of virtual file system specified by URLs that bears no direct relationship to the actual location of Web content for the site.
Local Virtual Directories vs. Remote Virtual Directories
The content that is mapped to the alias representing a virtual directory can be located in one of two places, resulting in two kinds of virtual directories:

- **Local virtual directory**  The content is located on the local server. This solution might be the simplest because all content for the Web site is on the local server and can be backed up in a single operation. Content for company departments can be located in different directories on the server for security and integrity reasons.

- **Remote virtual directory**  The content is located on a remote file server on the network. This solution is often the best when publishing earlier content that is already stored on network file servers. Security is enhanced because a user account is required to access the remote share, and suitable permissions can be assigned to this account. This remote placement of content also increases security by allowing content developers access only to file servers instead of to the Web servers themselves, and it reduces the processing load on the Web server. The only disadvantage is that the performance is slightly slower for content hosted on remote file servers, but this can be minimized by physically locating file servers close to the Web server on the network.

The Virtual Directory Creation Wizard
Now let’s use the Virtual Directory Creation Wizard to create a virtual directory for the Company site. Here are the steps:

1. Start IIS Manager on your server (or start it on a different server or workstation, and connect to the IIS server by clicking Action on the toolbar and choosing Connect from the drop-down menu).

2. Select the Company entry in the console tree, click Action on the toolbar, point to New, and choose Virtual Directory from the drop-down menu (or right-click the Company node in the console, point to New, and choose Virtual Directory from the shortcut menu). The Virtual Directory Creation Wizard starts. Click Next.

3. Specify *sales* as the alias for the virtual directory. (You don’t include the forward slash here.) Click Next.

4. Specify the path to the folder containing the pages you want access to, as seen in Figure 32-9. (If it’s on another machine, specify the Uniform Naming Convention, or UNC, path.) You can also use the Browse button to navigate to the share folder. Click Next.
5. The Access Permissions dialog box allows you to change the security settings. For this example, they are left as is.

6. Click Next to reach the final dialog box. Click Finish to complete the wizard.

If you now examine the Company node in the Internet Information Services console tree, you notice a new node beneath it representing the new virtual directory. (See Figure 32-10.) Because you created the virtual directory under your Company site, you can access it via the URL http://192.168.1.129/sales. Of course, you must create content, including a Default.htm page, for the browser to render.

Figure 32-9  The Web Site Content Directory page of the Virtual Directory Creation Wizard

Figure 32-10  The /sales virtual directory within the Company site
Web Sharing
Another way to create a new virtual directory is to use what’s called Web sharing. For example, assume you have the directory C:\Testing located on the local Web server and you want to share this directory as a virtual directory of the Company. To do this, complete the following steps:

1. Right-click the \Testing directory in My Computer, and select Sharing And Security from the shortcut menu.
2. In the Testing Properties window, click the Web Sharing tab.
3. Select the Company site from the Share On drop-down box. This creates a new local virtual directory mapped to the \Testing directory for its content.
4. To open the Edit Alias dialog box (shown in Figure 32-11), select the Share This Folder option. You can specify an alias that is different from the name of the folder if you want.

![Figure 32-11 The Edit Alias dialog box](image)

5. Click OK twice, and the virtual directory is created. Try accessing this directory by using the URL http://192.168.1.129/Testing. (Place a Default.htm page in the \Testing directory first.)

Virtual Directories, Physical Directories, and Icons
Virtual directories can be confusing for a couple of reasons. First, there are two icons you can use for nodes representing virtual directories in IIS Manager. Second, physical directories can behave like virtual directories if they’re physically located as subfolders of the home directory or another virtual directory. Take a look at Figure 32-12 as an example.
As you add a virtual directory, you can select among the five access permissions options: read, run scripts, execute, write, and browse. Looking at the various subnodes under the Default Web Site node in the console tree, you can easily see which have the run scripts or execute options set: they have the gear sprocket icon. Each of these—the starting directory for a Web application, typically developed by using ASP—creates dynamic content by running a script on your Web site.

In Figure 32-12, you see various virtual directories whose names start with “VirtualDirectory_.” Each is named with the access permissions. The /VirtualDirectory_ReadBrowse virtual directory has an icon that looks like a folder with a globe attached to it. This is a virtual directory that doesn’t create dynamic content, and therefore has neither the run scripts nor execute permission set. /VirtualDirectory_ReadRunExecute has the read, run scripts, and execute permission set; the sprocket icon is present because of the latter two. (You’ll learn more about dynamic content in Chapter 33.) The /Images directory isn’t a virtual directory at all, but rather a subdirectory of the Default Web Site’s physical directory on the server’s file system. As a result, it appears with an ordinary folder icon in the console tree. However, users can connect to it as if it were a physical directory by using the URL http://192.168.1.128/Images.

Another icon you might see is the Error icon, which resembles a stop sign. This icon is used to indicate an error has occurred. For example, if a network device that contained the folder a node represents gets disconnected, that node will have the Error icon.
The FTP Publishing Service

Now you look at concepts and tasks associated with the File Transfer Protocol Service. You begin by examining the Default FTP Site included as an example when you install the FTP service. Then you look at common tasks such as creating new FTP sites and virtual directories. These tasks are similar to ones you just learned for the World Wide Web service.

The Default FTP Site

As with the WWW service, installing the FTP service on Windows Server 2003 creates a new default site, called the Default FTP Site. Unlike the WWW service, the FTP service is not included in a default IIS installation. You can add it (and remove it later, if necessary) via Add/Remove Programs on Control Panel. Unlike the Default Web Site with its sample pages and numerous directories, however, the Default FTP Site is empty. This is singularly uninteresting, so let’s move on!

Other FTP Sites

As with the WWW service, you can create as many FTP sites as you want using IIS 6 and you can host the content (pages, images, and other files) for these sites in either local directories or network shares. Each FTP site acts as a separate entity, or virtual server, and acts as if it were running on its own Windows Server 2003 using the full resources available to it on that server. To illustrate this, you will now create a new FTP site on the server, place a test file in its home directory, and then download the test file from another machine on the network.

Using the FTP Site Creation Wizard

As with Web sites, you can specify FTP sites on an internetwork in a variety of ways, including using the site’s IP address, NetBIOS name, or fully qualified DNS name. For the present example, use a default private IP address, 192.168.1.128. You must create a home directory for the new FTP site. Start by creating a new folder on the C drive of the local server and naming it C:\ftphome. Then copy a bitmap file such as C:\Windows\Greenstone.bmp to the C:\ftphome directory so that you have something to download from the client. Follow these steps to create the new FTP site:

1. Start IIS Manager. Select the FTP Sites node in the tree.
2. On the toolbar, click Action, point to New, and choose FTP Site (or right-click the server’s FTP Sites node in the console, point to New, and choose FTP Site from the shortcut menu). This starts the FTP Site Creation Wizard. Click Next.
3. Type Company FTP Site as the name for the site. This name is displayed in IIS Manager, and it identifies the new site for the administrator. Click Next.
4. Specify the IP address mentioned previously as the one to be mapped to the site, leaving the port number at its default setting of 21. Click Next.
5. Select the option most suitable for the limitations you want to place on users browsing folders on the server. The three options are to let users have free reign, isolate users to their own folder (and below), or use Active Directory to manage user permissions.

6. Specify the path to the home directory for the new FTP site as \ftphome and click Next. (Using the Browse button is the easiest way to do this.)

   **Note** The home directory for your site can be a local directory or a network share.

7. Make sure that both Read permissions and Write permissions are selected. This allows you to both download files from and upload files to your new FTP site.

8. Click Next, and then click Finish to complete the wizard. The new Company FTP Site should appear as a node under the server’s FTP Sites node in the Internet Information Services console window (shown in Figure 32-13). Note that the Greenstone.bmp file within the home directory doesn’t appear in the right pane of the console window. This is different from Web sites, where files in home directories and virtual directories are displayed in the console window. (You can see it by right-clicking the FTP site’s node and selecting Explore from the menu.)

   ![Figure 32-13](image)

   **Figure 32-13** The new Company FTP Site shown in the Internet Information Services console window

   **Note** In Figure 32-13, you still see the Default FTP Site that was created by default by the FTP Service installation process. You can use it as a starting point for your own FTP site. Because you created an FTP site from scratch, you can delete the Default FTP Site.

**Testing the New FTP Site**

To test the new FTP site, go to a different machine on the network, start Internet Explorer 6, and open the URL `ftp://192.168.1.128`, which specifies the new FTP site using its associated
IP address. The file Greenstone.bmp should be displayed in the browser window, along with the IP address you’re connecting to and the user name Anonymous. (See Figure 32-14.)

Figure 32-14  Connecting to the new Company FTP Site using Internet Explorer 6

After you connect to the FTP site, you can perform various actions in Internet Explorer including the following:

- Download the file to your machine by right-clicking its icon, choosing Copy To Folder, and specifying the destination folder on your machine (or anywhere else accessible on the network).
- Drag files from My Computer on your local machine into the browser window to upload them to the FTP site.
- Right-click the file icon, and choose Properties to display the type, location, size, and date modified of the original copy of the file on the FTP site.
- Log on to the FTP site as a different user (if access is controlled by user names) by choosing the Login As command from the browser’s File menu.
- View the FTP welcome message (if there is one) using the Help menu.

Now isn’t that more fun than using the old text-based FTP command from the command prompt?

Virtual Directories

You can create virtual directories for FTP sites the same as you can for Web sites. Let’s look at this briefly now.

Using the Virtual Directory Creation Wizard

You already saw the Virtual Directory Creation Wizard. It doesn’t matter whether you create the virtual directory within a Web site or within an FTP site—the same wizard creates them. But just for variety, because you created a local virtual directory for the Company Web site last time, this time create a remote virtual directory for the Company FTP Site. (The following steps are compressed because you’re already familiar with the wizard.)

1. Open IIS Manager. Right-click the Company FTP Site node, point to New, and choose Virtual Directory from the shortcut menu. Click Next.
2. Provide a name for the virtual directory. For this example, you're just sharing documents, so name the virtual directory “Documents.” Type **Documents** as the alias for the virtual directory and click Next.

3. Specify the remote path for the location of the content directory that maps to the virtual directory being created. Here, you're connecting to a folder named Documents on the machine named Frog. Type `\Frog\Documents` here and then click Next.

4. You're prompted for a user name and password in the Security Credentials dialog box. Type the information needed to connect to the remote folder and click Next.

5. Change the access permissions to enable write access and disable read access on the directory.

6. Click Next, and then click Finish to complete the wizard.

The new local virtual directory `/Documents` is now visible as the node underneath the Company FTP Site node in the console tree. (See Figure 32-15.) Notice that the icon used to represent FTP virtual directories is different from the icons used to represent Web virtual directories.

![Figure 32-15](image)

Figure 32-15 The `/Documents` virtual directory within the Company FTP Site

**Testing the New Virtual Directory**

Try accessing the new virtual directory from a remote machine by opening the URL `ftp://192.168.1.128/Documents` virtual directory on the Company FTP Site using Internet Explorer. A message should appear in a dialog box saying, “An error occurred opening that folder on the FTP Server. Make sure you have permission to access that folder.” Click OK to close the error message.

Now try dragging a file from My Computer into the browser window. Verify on the server that the file was indeed uploaded to the directory on the server. Now try refreshing the browser window. The same error message appears as before. Click OK to close the error message, and the browser window—which is still open to the `/Documents` virtual directory—should appear empty. This verifies that anonymous users can upload files to the virtual directory, but can’t view or download files from it, per the options you set in Step 5.
Basic Administrative Tasks

This chapter concludes with a look at some basic administrative tasks you can perform on Web sites and FTP sites by using the IIS Manager console. Chapter 33 takes a more detailed look at the settings you can configure for these sites. For now, the focus is on basic tasks such as configuring permissions, stopping and starting services, and enabling FrontPage Extensions on the server.

Configuring Permissions

Understanding permissions, and how they are configured and applied on IIS 6, is a part of the larger picture of understanding IIS security in general. This section covers the levels of security you can use to control access to content in Microsoft Server 2003 Web sites and FTP sites—and looks at the order in which these layers are applied. (More detailed information about configuring individual aspects of IIS 6 security is covered in Chapter 33.)

Understanding IIS 6 Security

Administrators can control access to content on Web sites and FTP sites hosted on IIS 6 in four ways. These methods are applied in order each time a user tries to access a Web or FTP resource (an HTML or other file) on the server. The four-stage access control model is presented next, and only when all four of these rules have been applied and passed is the user granted access to the requested resource.

1. Is the user’s IP address or domain name allowed access to the resource?
   
   If not, access is denied and no further rules are applied. You can configure IP address and domain name restrictions using the Directory Security tab of the Properties window for the Web site, FTP site, or virtual or physical directory, or on the File Security tab of the Properties window for a file. Note that the Properties windows referred to here and in the next two steps apply to those accessed from the Internet Information Services console window. (See Chapter 33 for more information about these Properties windows.)

2. Has the user been properly authenticated for accessing the resource?
   
   If not, access is denied and no further rules are applied. You can configure authentication security settings on the Directory Security tab of the Properties window for a Web site or virtual or physical directory, on the Security tab of the Properties window for a file, or on the Security Accounts tab of the Properties window for an FTP site. Note that you can’t configure this level of security on virtual directories that are located within FTP sites, only on those within Web sites.
3. Are the IIS access and application permissions configured to allow users access to the resource?

If not, access is denied and no further rules are applied. You can configure IIS access and application permissions on the Home Directory tab of the Properties window for a Web site or FTP site, on the Virtual Directory tab of the Properties window for a virtual directory, or on the Security tab of the Properties window for a physical directory or file.

4. Do NTFS permissions on the resource allow the user to access the resource?

If not, access to the resource is denied to the user. NTFS permissions are configured in the usual way by using the Security tab of the Properties window for the resource in My Computer.

Note In the four-stage access control model, Steps 2 and 4 are user-specific while Steps 1 and 3 apply regardless of the user’s identity. In other words, IP address/domain name restrictions and IIS access/application permissions are global settings that apply uniformly for all users.

Setting Permissions

Permissions settings are accessible by selecting Properties on the Action menu in IIS Manager. To change the security settings on the /Sales virtual directory created earlier within the Company Web site, follow these steps:

1. Select the Sales node under the Company Web site node.
2. On the Action menu, select Properties.
3. In the Properties dialog box, click the Directory Security tab, as shown in Figure 32-16.

![Figure 32-16 The Directory Security tab of the Virtual Directory's Properties dialog box](image)
4. In the Authentication And Access Control section, click Edit to alter the authentication methods for /Sales.

5. In the Authentication Methods dialog box, you can enable or disable anonymous access, represented by the account IUSR_<MachineName>. (In Figure 32-17, IUSR_SERVER is the anonymous access account because your machine name is SERVER.) The Authenticated Access section also allows you to specify other authentication methods when anonymous access is not allowed or the NTFS security settings limit access. After making your selections, click OK to return to the Properties page.

![Authentication Methods dialog box](image)

**Figure 32-17** The Authentication Methods dialog box

6. In the IP Address and Domain Name Restrictions section (see Figure 32-16), click Edit. In the IP Address And Domain Name Restrictions dialog box (shown in Figure 32-18), select one of the options to allow or prevent access from specific computers, groups of computers, and whole domains and then click OK to return to the Properties page.

- To grant access to all machines except those in the list you create, select Granted Access.
- To deny access to all machines except those in the list, select Denied Access.
- To create the exception list, click Add. You can add single computers, a range of computers, or domains.
7. In the Secure Communications section (Figure 32-16), click Edit to display the Secure Communications dialog box (Figure 32-19). You can specify that SSL is required, alter certificate acceptance settings, and enable client certificate mapping.

8. Make your selections and click OK.

**Stopping, Starting, and Pausing IIS Services**

Remember that individual Web sites and FTP sites that are created on IIS 6 are actually virtual servers—that is, they act and behave as if they were separate Windows Servers and had access to all the resources on the server. This allows Web sites for many companies to be hosted on a single Windows Server 2003 machine. Sometimes you might need to stop, start, or pause IIS services on these machines, however. For example, when files are...
being modified on a Web site, it's usually smart to pause the site so that no new user connections can be established with the site and to allow users who are currently connected a grace period before they're disconnected.

Another example is when you're testing a Web application developed by using ASP—you might need to stop and then restart the site during the testing process if the application hangs or becomes unresponsive. The trouble is, if you have multiple sites running on your server, you don't want to bring them all down just to deal with the problems of a particular site.

To solve this problem, Windows Server 2003 allows you to use IIS Manager to stop individual Web sites and FTP sites without having to stop the WWW and FTP services for all sites on the server. To pause, stop, or start a site, select the node in the console tree that represents the site and do one of the following:

- Click the appropriate control button on the toolbar.
- Right-click the node, and make the appropriate choice from the shortcut menu.
- Click Action, and select the appropriate choice from the drop-down menu.

Alternately, you can restart all Web and FTP sites on your server by selecting the node representing the server (the parent node of all the sites you've configured) in the console tree of IIS Manager. Then click Action on the toolbar, and select Restart IIS from the All Tasks menu. You might expect that you can stop all Web sites running on a machine by stopping the WWW service using the Services node under System Tools in Computer Management. Don't do it this way. IIS is implemented differently from other Windows Server 2003 services and should not be stopped or started in this fashion. Finally, if you want to control IIS from the command line, type `iisreset<Computer_Name> /option`.

Table 32-2 lists the available control options. This command is useful in a batch file.

<table>
<thead>
<tr>
<th>Command</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>/restart</td>
<td>Stops and restarts all IIS services.</td>
</tr>
<tr>
<td>/start</td>
<td>Starts all IIS services.</td>
</tr>
<tr>
<td>/stop</td>
<td>Stops all IIS services.</td>
</tr>
<tr>
<td>/reboot</td>
<td>Reboots the server.</td>
</tr>
<tr>
<td>/rebootonerror</td>
<td>If starting, stopping, or restarting IIS services results in an error, reboots the server.</td>
</tr>
</tbody>
</table>
Using FrontPage Server Extensions

IIS 6 uses a set of proprietary server-side DLLs called FrontPage Extensions to support many of the advanced FrontPage features, such as its ability to create navigation bars, search tools, discussion Webs, and so on. Finally, let’s look at installing FrontPage server extensions. In IIS 6, this is a basic Web server administration task for networks where developers use the popular Web content creation tool, Microsoft FrontPage. Content development isn't covered here, but you do examine how to enable the server to operate with FrontPage.

FrontPage Extensions are an optional component of IIS. Before you can enable FrontPage Extensions, you have to install them. Then you need to enable these extensions on the specific Web sites that your FrontPage content developers will be using. To see how this works, use the Company Web site and follow these steps:

1. Right-click the Company Web site node in the Internet Service Manager console tree, point to All Tasks, and choose Configure Server Extensions 2002 from the shortcut menu and enter your credentials when requested. This generates and opens the Extend Virtual Server With FrontPage Server Extensions 2002 page.

2. Click Submit to enable FrontPage Server Extensions 2002. This opens to the Server Administration Web page, shown in Figure 32-20. The three options allow you to alter rights, set installation defaults, and reset user passwords. Below them are the virtual servers that you can administer.

<table>
<thead>
<tr>
<th>Command</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>/noforce</td>
<td>If the service doesn't respond to a stop command, don't forcefully terminate it.</td>
</tr>
<tr>
<td>/timeout:val</td>
<td>Specifies the number of seconds (represented by val) to wait for a service to respond to a stop command. If /rebootonerror is also specified, the system restarts.</td>
</tr>
<tr>
<td>/status</td>
<td>Displays the current status of all running IIS services.</td>
</tr>
<tr>
<td>/enable</td>
<td>Enables the restarting of IIS services on the local server.</td>
</tr>
<tr>
<td>/disable</td>
<td>Disables the restarting of IIS services on the local server.</td>
</tr>
</tbody>
</table>
3. Click the Set List Of Available Rights link to proceed to the Rights page. View the rights listed, and select the check boxes to enable those rights on the server. Navigate back to the previous page to examine the next option.

4. Click the Set Installation Defaults link to edit the mail and security settings. Mail Settings allows you to specify the SMTP server, From address, and Reply-To address for use in e-mail features of FrontPage Server Extensions. Security Settings allows you to log authoring activities, require SSL, and permit uploading executables by authors. Navigate to the previous page again to move to the last option.

5. Click the Reset User Password link. The Reset User Password page appears. You can specify the user name and new password you want to assign.

After the FrontPage Extensions are installed, you'll find that a number of new files and directories are created and added to your site. Don’t delete any of these FrontPage files or directories, or the server extensions might fail to work properly!

Summary

IIS 6 is an integral part of Windows Server 2003. No additional software is needed to manage multiple Web sites—even on the same server. Wizards are supplied to guide the administrator through all the basic configuration processes, including creating Web sites and virtual directories and setting permissions. With the comprehensive tool IIS Manager, setting up an Internet server has never been simpler. Keeping it running reliably and safely can be a more difficult process. Chapter 33 covers the more complex administrative tasks of Web site and FTP site management.
Chapter 33

Advanced Internet Information Services

Server-Level Administration ............................................. 1071
Site-Level Administration ............................................... 1075
Directory-Level Administration ......................................... 1076
File-Level Administration ............................................... 1077
Managing WWW Sites .................................................... 1078
Managing FTP Sites ...................................................... 1095
Managing NNTP Virtual Servers ........................................... 1102
Managing SMTP Virtual Servers ......................................... 1110
Web Service Extensions .................................................. 1117
Remote Administration ................................................... 1119
Summary .......................................................................... 1121

The previous chapter examined some basic administration tasks associated with Internet Information Services (IIS) on Microsoft Windows Server 2003. This chapter explains how to configure the basic WWW Publishing Service and the FTP Publishing Service in more detail. It also examines Network News Transfer Protocol (NNTP) and Simple Mail Transfer Protocol (SMTP) and how to configure them. Then it briefly covers the lock-down features of IIS. Finally, it briefly discusses remote administration of IIS using the optional Remote Administration (HTML) component.

IIS settings can be configured and its servers, directories, and files administered at four levels. The four levels of administration apply to the four services discussed later in this chapter. Those levels are as follows:

- **Server-level administration** The configuration of settings that apply globally to all virtual servers on a Windows server with IIS installed. Server-level settings are inherited by all virtual servers and their virtual and physical directories and files.
Site-level administration  The configuration of settings that apply to a particular virtual server on the IIS machine—that is, to a particular Web, File Transfer Protocol (FTP), SMTP, or NNTP site on the machine. Although server-level settings apply globally to virtual servers that support Web sites and FTP sites on the machine, each of these virtual servers can also have its settings separately configured at the site level.

Directory-level administration  The configuration of settings that apply to a particular virtual (or physical) directory located within a virtual server. Although site-level settings apply globally to all virtual (or physical) directories located within a particular Web, FTP, SMTP, or NNTP site, each directory can also have its settings separately configured at the directory level.

File-level administration  The configuration of settings that apply to a particular file located within a virtual (or physical) directory. Although directory-level settings apply globally to all files located within a particular directory, each file can also have its settings separately configured at the file level. These file-level settings override settings configured at the directory level and are a subset of the directory-level settings.

Rudimentary configuration tasks can be performed by the various wizards examined in the previous chapter, such as the Web Site Creation Wizard and the Virtual Directory Creation Wizard. To fully configure the various aspects of IIS on a Windows server, you need to use the Properties windows for IIS objects. These objects include physical and virtual servers, physical and virtual directories, and files. Each of these types of objects is represented by a node in the console tree of IIS Manager, the main tool for managing and configuring these objects.

Figure 33-1 illustrates the four levels of IIS administration and how settings on Properties windows are inherited and overridden between these levels. We’ll look at these settings later in the chapter, but first let’s take a look at the four administration levels in more detail. For all four levels, this chapter focuses specifically on the WWW Publishing Service because it has the broadest range of configuration options.

Figure 33-1  The four levels of IIS administration
Real World  Inheritance of Settings

Settings configured for an object (physical or virtual server, physical or virtual directory, or file) are automatically inherited by objects at lower levels. For example, if you configure an IIS setting at the server level, this setting will be inherited (if applicable) by all virtual servers, virtual directories, physical directories, and files relating to IIS. You can override these inherited settings at any particular level, however. For example, you can override the settings for a particular virtual server (Web or FTP site) and all its directories and files, for a particular virtual or physical directory and the files it contains, or for a particular file. Note that after you manually modify an inherited setting at some level, subsequently changing the setting at a higher level doesn’t cause your modification to be automatically overwritten. Instead, you are prompted to decide whether you want to override the modified setting.

Server-Level Administration

Server-level administration involves the following tasks:

- Connecting to a machine running IIS to administer that machine
- Backing up and restoring the configuration of the machine
- Enabling global bandwidth throttling for all Web and FTP sites on the machine
- Configuring various master properties that apply globally to all Web and FTP sites created on the machine
- Compressing files by using HTTP compression
- Configuring the global Multipurpose Internet Mail Extensions (MIME) map
- Setting server extensions (if you have Microsoft FrontPage server extensions installed)

Let’s begin with the general administration tasks and global settings you can configure for IIS on a Windows server. You can perform some common server-level administration tasks using the IIS Manager introduced in Chapter 32.

Connecting to an IIS Server

You can administer multiple servers running Windows Server 2003 and IIS from a single IIS console window. To administer a server, you need to connect to it first. To do so, follow these steps:

1. Start the Manage Your Server application from the Start Menu.
2. Select Manage this application server from the options available under the Application Server heading.

3. The Application Server console window will appear. Select the root node (called Internet Information Services) in the IIS console tree.

4. Click Action on the toolbar and choose Connect from the drop-down menu, or right-click the root node and choose Connect from the shortcut menu. (Remember that in a console window, the drop-down Action menu provides the same options as the shortcut menu that is displayed when you right-click any selected node.)

5. In the Connect To Computer dialog box, type the name of the IIS machine to which you want to connect in the text box, and click OK. You can specify the name of the machine as any of the following:
   - Network Basic Input/Output System (NetBIOS) name (for instance, the name “server”)
   - Internet Protocol (IP) address (for instance, 192.168.1.128)
   - Fully qualified DNS name (for instance, server.example.com)

6. To disconnect from a server, select the node in the console tree that represents the server, click Action, and choose Disconnect.

Creating Configuration Backups

You can save the configuration settings for an IIS machine and all of its Web and FTP sites to a configuration backup file. Each backup file is stamped with a version number and its time and date of creation. You can create any number of backup files and restore these files if you want to restore your previous settings. This feature is quite useful—it allows you to take a snapshot of your IIS configuration before you start modifying permissions and other settings for the virtual servers, directories, and files on your machine.

Note Configuration backup files restore only the IIS settings on your machine’s Web and FTP sites and their virtual and physical directories and files. They don’t back up the actual content files themselves—that is, the HTML, images, and scripts within a Web site. Use the utilities provided by Windows, such as the Backup or Restore Wizard, to back up the content files for your sites.

Backing Up a Server Configuration

To back up the configuration of your IIS machine, follow these steps:

1. Select the node in the console tree that represents your server.

2. Click Action, point to the All Tasks menu item, and when it is revealed, choose the Backup/Restore Configuration menu item.
3. As Figure 33-2 shows, the Configuration Backup/Restore dialog box that appears displays the various backup files you created, their version numbers, and date/time of creation. Version numbers start with zero and increase sequentially.

![Figure 33-2](image)

**Figure 33-2** The Configuration Backup/Restore dialog box

4. To create a new backup file, click Create Backup and give the file a friendly name. The backup file is saved in the System32\inetsrv\MetaBack directory. The information is stored in binary format and is specific to the machine on which it has been created. If you reinstall Windows Server 2003 on the machine, you'll be unable to use previously created backup files to re-create your IIS configuration.

You can provide a password to encrypt the backup. You can read the backup information because only the secure properties are encrypted. Without the correct password, however, you are not able to restore the system with the backup files.

**Restoring a Server Configuration**

To restore the configuration of your server to a previous version, open the Configuration Backup/Restore dialog box, select the backup file you want to restore to, and click Restore. Note that IIS must stop its services to perform a restore, so a restore takes longer than a backup.

**Note** You can export the contents of the rightmost pane of the console window by selecting a particular node in the leftmost pane, clicking Action, and choosing Export List. You can save the information as an ASCII or Unicode text file in either tab-delimited format or comma-delimited format. This is a great way to document home directories for the various virtual directories you create within a Web site.

**Configuring Server Properties**

Server-level properties for the WWW service are configured using the properties of the Web Sites node in IIS Manager. Since these properties are pretty much the same as those for individual Web sites, we'll discuss them in more detail later in this chapter.
The configuration of IIS is stored in what's called the metabase. The metabase is a plain text file in XML (Extensible Markup Language) format named Metabase.xml. This file is in your system32\inetsrv directory. Metabase.xml is tied to a file called MBschema.xml that defines the schema of the metabase. It defines properties and specifies what properties can be written to what keys in the metabase configuration.

**Note**  An excellent source for information about XML is [http://www.w3.org/XML/](http://www.w3.org/XML/).

### Editing the Metabase

Making the metabase a plain text file enables easy editing and viewing of your settings. You can edit the file in a text editor such as Notepad. You can view the file in a program that can render XML, such as Microsoft Internet Explorer.

You can change the configuration of your server without having to stop IIS. If you right-click the server node and select the Properties menu item, you can select the Enable Direct Metabase Edit option, which is shown in Figure 33-3.

![Figure 33-3 Enabling metabase changes without stopping IIS](image)

The metabase schema consists of containers called collections. Each collection exists at the same hierarchical level; no collection can be contained in another collection.

Properties represent a configurable facet of IIS. The IISConfigObject collection contains all properties in the metabase. Each property consists of ID, Type, UserType, Attributes, and DefaultValue. Some properties have other attributes; these include MetaFlags, MetaFlagsEx, StartingNumber, and EndingNumber.
Metabase History
If you have a basic grasp of the layout of the metabase file and a working knowledge of XML, you can begin to change the contents of the metabase. As you edit the metabase, the metabase history feature provides a level of safety. Changes are saved to disk in the system32\inetsrv\history directory.

By default, 10 metabase pairs (Metabase.xml and MBSchema.xml) are maintained in the history folder. If a new pair is being written and the history folder already contains 10 pairs, the oldest pair is deleted. The default number of versioned history pairs can be changed by editing the MaxHistoryFiles property.

Site-Level Administration
Site-level administration of IIS differs considerably in its tasks depending on which of the four IIS services you are dealing with: WWW, FTP, SMTP, or NNTP. As a result, there is a detailed discussion of the various tasks involved in administering different kinds of sites (virtual servers) later in this chapter. (In other words, to learn how to administer WWW sites, go to the “Managing WWW Sites” section.)

Site-level settings for a newly created Web or FTP site are inherited from the server-level (Web Sites or FTP Sites node) properties. You can, however, modify settings at the site level and have those settings override the settings configured at the server level. Another important point to consider is that site-level settings are inherited by all virtual and physical directories and files within the site (that is, within the virtual server). This is true whether you are considering WWW, FTP, SMTP, or NNTP sites.

A sample site-level settings dialog box is shown in Figure 33-4.

![Figure 33-4 Editing site-level settings](image)
Directory-Level Administration

Directory-level settings are inherited by all files within the directory. They also override those configured at the site and server levels. Directory-level settings apply to both virtual and physical directories within a particular Web or FTP site.

Directory-level properties are simply a subset of site-level properties. In fact, the WWW service master properties for a particular IIS machine are configured through a Master Properties page that has nine tabs: Web Site, Performance, ISAPI Filters, Home Directory, Documents, Directory Security, HTTP Headers, Custom Errors, and Service. Also, the Properties window for a particular Web site, such as the Default Web Site, has a set of tabs comparable to the set in the server’s Master Properties window, replacing the Service tab with a Server Extensions 2002 tab.

Similarly, as Figure 33-5 shows, the Properties window for a particular virtual (or physical) directory within a Web site has a subset of the tabs in the Web site’s Properties window: Directory (versus Home Directory), Documents, Directory Security, HTTP Headers, and Custom Errors. The following list summarizes the kinds of settings you can configure at the directory level:

■ Location of content for the directory (local directory, network share, or redirection to a URL)
■ Application settings (application name, starting point, execute permissions, and so on)
■ Default documents and document footers
■ Anonymous access and authentication control
■ IP address and domain name restrictions
■ Secure communications using SSL
■ Content expiration
■ Custom HTTP headers
■ Content rating
■ MIME mappings
■ Custom HTTP errors
Figure 33-5  The Properties window of a directory within the Default Web Site

Note  Remember that directory-level settings for a newly created Web site are inherited from the site-level settings previously specified. Modifying the settings at the directory level overrides similar settings configured at higher levels.

File-Level Administration

File-level administration is the last of the four levels of IIS administration. At this level, you configure the properties of individual files within a Web or FTP site’s home directory or other directories. For example, although a WWW service directory-level Properties window has five tabs, the Properties window for an individual Web page or other file has only four tabs: File, File Security, HTTP Headers, and Custom Errors, as you can see in Figure 33-6.

Configuring file-level properties is basically the same as configuring directory-level properties, except that a single file can’t have a default document specified for it as a directory can, and you can’t configure the following options at the file level: Directory Browsing, Index This Resource, and Enable Document Footer. Also, the location of the file can be either specified or redirected to a URL.
Managing WWW Sites

Let’s now look in detail at the various site-level administrative tasks you can perform on IIS. How to manage Web sites or virtual servers created using the WWW service is covered first, followed by sections about FTP sites and SMTP and NNTP virtual servers.

You’ve already briefly examined the configuration items used at the site level for administering individual Web sites, and you’ll now see the various tabs and their settings in detail. The Default Web Site is the one configured in this section.

**Note**  A Server Extensions 2002 tab is also present if FrontPage extensions are configured on the Web site, as discussed earlier in this chapter.

Web Site Tab

The Web Site tab of the Properties page, shown in Figure 33-7, allows you to specify Web site identities, configure a connection timeout, enable or disable HTTP Keep-Alives, and enable IIS logging on your server. Let’s examine how to assign identities to Web sites first.
Web Site Identification
Each Web site hosted on an IIS machine must have a unique identity so that browser clients can connect to it to download its content. Web sites are defined using three parameters: IP address, TCP port number, and host header name.

The identity for a Web site is specified on the Web Site tab of the Properties window for the particular Web site under consideration. For Web sites on the same machine to have unique identities, they must differ from each other in at least one of the three parameters just mentioned. Let’s look at some different ways of specifying Web site identities by considering how to host several different Web sites on the same server.

Configuring Multiple IP Addresses on the Server’s Network Card
You can configure multiple IP addresses on the server’s network card or install multiple network cards, each with a different IP address. Select a different IP address for each Web site. Leave each site’s Transmission Control Protocol (TCP) port set to 80 (the default TCP port for HTTP), and don’t configure host header names. The advantage here is that clients can connect easily to each site by using the site’s IP address in the URL they request (or by using a fully qualified DNS name if a unique host name has been configured on the DNS server for each of the IIS machine’s IP addresses).

Configuring Only One IP Address for the Server’s Network Card
The disadvantage is that if many sites must be hosted on the machine, many IP addresses must be obtained and assigned to it. This isn’t a problem on a private internetwork when using one of the private IP address blocks such as 10.y.z.w, 172.16-31.z.w, or 192.168.z.w.
On servers directly connected to the Internet, however, you must obtain a sufficient number of IP addresses from your Internet service provider. Nevertheless, this method of specifying Web site identities is the preferred and commonly used one.

Specify a different TCP port (above 1023) for each Web site hosted on the machine. The main disadvantage here is that clients must know the port number of the Web site to which they want to connect. For example, if the DNS name of the server is server.example.com and a Web site on the server is assigned port 8023, the client has to use the URL `http://server.example.com:8023` to access the site.

**Configuring One IP Address and Leaving the TCP Port Set to Default**

Configure only one IP address for the server's network card, and leave the TCP port set to the default value of 80 for each site. Configure a unique host header name for each site, using the Advanced button. Host header names are a feature of HTTP 1.1, which is supported by IIS 6. The host header name associated with each site is typically the fully qualified DNS name that is assigned to the site in the database of an available DNS server (or in the local Hosts file on the clients).

---

**Note** When you open the Properties window for the Default Web Site and select the Web Site tab, the IP address is specified as (All Unassigned). This means that this Web site responds to any IP addresses that aren't specifically assigned to other Web sites on the machine. That's actually what makes this site the Default one, and only one Web site on an IIS machine can have its IP address specified this way.

When the client requests a URL such as `http://sales.example.com`, the client passes the host header name sales.example.com in the HTTP request headers that it sends to the server. (See Chapter 32 for more information about HTTP headers.) The server parses the host header name, identifies which Web site the client is requesting, and returns the appropriate files. One disadvantage is that the client must also support host header names—that is, the ability to pass the DNS name of the site in its HTTP request headers. Host header names are supported by Microsoft Internet Explorer 3 or later and by Netscape Navigator 2 or later. Another disadvantage is that host header names don't work with Secure Sockets Layer (SSL) connections because the HTTP session is encrypted.

If you're working with older browsers that don’t support host header names, you can implement a cookie-based mechanism to enable the browsers to distinguish between Web sites having the same IP address and TCP port number. See the online documentation for more information about how to do this.
Connections
The Web Site tab also allows you to enable or disable HTTP Keep-Alives and specify a connection timeout value. HTTP Keep-Alives are a feature of HTTP 1.1 that enables a client to keep open a TCP connection with a server after downloading a file, in case other files need to be immediately downloaded from the server. If clients start complaining about the server being sluggish or that they’re frequently receiving HTTP 500: Busy errors, try decreasing the connection timeout value so that unused TCP connections time out more quickly.

Note  Connection timeouts specified on the Web Site tab are for active TCP sessions. TCP has its own settings for automatically terminating half-open TCP connections, such as those created during a Denial of Service (DoS) attack that tries to bring down a Web server by flooding its network connection with TCP SYN packets.

IIS Logging
The Web Site tab also allows you to enable IIS logging on your server. This feature is enabled by default and allows administrators to monitor access to the site by client browsers. Logging information can be saved in a variety of formats, including the following:

■ Microsoft IIS Log Format  This option creates a fixed-format ASCII file.

■ NCSA Common Log File Format  The National Center for Supercomputing Applications (NCSA) common log file format option creates a space-delimited ASCII file with a predetermined set of fields.

■ ODBC Logging  This option logs IIS traffic to any Open Database Connectivity (ODBC)-compliant database using the specified data source name (DSN) for the database.

■ W3C Extended Log File Format  The World Wide Web Consortium (W3C) extended log file format option is the default value. It creates a space-delimited ASCII file with a group of fields that the administrator can specify.

New IIS logs can be created hourly, daily, weekly, or monthly, or when the existing log file grows to a specified size. Logs are stored by default in the \%WinDir%\System32\LogFiles folder, but you can use the Properties button to modify this setting. Note that the older Microsoft IIS Log File Format (supported under IIS 4, but not under IIS 5) has made a triumphant return.
Enabling IIS logging on the Web Site tab doesn’t actually mean that visits to all parts of your site are logged. In the Web site’s dialog box, you can select the Log Visits check box on the Home Directory tab to enable or disable the logging of access to content located in the site’s home directory. On other tabs, you can similarly track visits to other directories or even individual files.

Performance Tab
You can tune performance for individual Web sites using the Performance tab of the site’s Properties page, shown in Figure 33-8. On this tab you can configure the following settings:

- **Bandwidth throttling** You can turn on and specify a limit if you want to limit a Web site’s bandwidth to a certain range. This is useful in a situation in which certain sites have lower priority than others, such as when you want employee personal pages to have lower priority than the online catalog for your company.

- **Web site connections** You can limit the active connections count to a specific number or leave it as Unlimited.

![Figure 33-8 The Performance tab for the Default Web Site](image)

ISAPI Filters Tab
Internet Server Application Programming Interface (ISAPI) filters are optional dynamic-link libraries (DLLs) that perform specific actions when IIS processes an HTTP request from a client. You can use the ISAPI Filters tab to install a series of these filters and specify the order in which IIS processes them. Filters installed here at the site level are used only by the selected site; filters installed at the server level apply to all sites on the server.
ISAPI filters perform their action before the server actually responds to the HTTP request itself. For example, you can design an ISAPI filter to perform custom authentication, encrypt data, write traffic information to a custom log file, or perform some other action. Implementing ISAPI filters is beyond the scope of this book.

**Home Directory Tab**

The Home Directory tab, shown in Figure 33-9, allows you to specify the location of the content that is mapped to a Web site’s home directory, to specify various access permissions and other settings for the directory, and to specify application settings relating to any Web application you implemented in this directory.

![Figure 33-9 The Home Directory tab for the Default Web Site](image)

**Home Directory**

The home directory for a site determines the location of any content that is accessed using a URL such as http://Site_Name/File_Name, where Site_Name represents the NetBIOS name, IP address, or DNS name of the site, and File_Name represents the name of any particular HTML page, image file, script, or other file in the site’s home directory. You can specify the home directory for a site in three ways:

- As a directory located on a local drive of the machine.
- As a Uniform Naming Convention (UNC) path to a network share located on a file server. (You need to specify credentials for connecting to the share.)
- As a redirection to a URL that instructs the client to connect to a different Web server (not even necessarily an IIS one) to access the content mapped to the home directory. This redirection can be either temporary or permanent.
Real World Redirecting Access

Being able to redirect the home directory (or any virtual directory) to a URL is useful when Web sites are being developed or are down for maintenance or upgrade. IIS gives you the option of redirecting a request for any file in the home directory to the same URL (such as a We're Down For Maintenance page) or to a similar file in the remote directory (for example, to a temporary mirror site). You can also redirect access to a subdirectory of the current home directory if your maintenance page or mirror content is located on the same server.

Specify a permanent redirection only if you plan to move the site’s content to another server, because some browsers that receive an HTTP 301 Permanent Redirect message might automatically modify a favorite or bookmark linked to the site. The result is that when redirection is turned off, the client continues to access the alternate site instead of the original one.

Access Permissions

If you specify the location of the home directory as either a local directory or a network share, you have the option on the Home Directory tab of specifying various access permissions and other settings for the directory, as shown in Figure 33-9. (These settings aren’t available if you specify redirection to a URL for the home directory location.) You can specify the following settings:

- **Script Source Access** Select this check box if you want users to be able to access the actual source code of scripts, such as Active Server Pages (ASP) files. Note that this setting does nothing unless you also select either Read or Write. (Selecting Read then lets users read the source file for the script, while selecting Write allows them to modify the script.) This option is used primarily on development servers where content is created. It is disabled by default.

- **Read** Selecting this check box allows users to view the contents of a directory or file and its associated properties, such as creation time and file size. This setting is enabled by default.

- **Write** Selecting this check box allows users to modify the contents of a directory or file. Only browsers that support the PUT feature of HTTP 1.1—such as Internet Explorer 4 or later—can write files to the server. This setting is disabled by default.

- **Directory Browsing** Selecting this check box allows users to view the contents of the home directory when no default home page is present in the directory. This setting should generally be disabled (and is by default) to hide the directory structure of your content directories from accidental viewing by users who might use this to snoop in places you don’t want them to go.
Log Visits   Selecting this check box causes an entry to be added to the IIS log files whenever any file in the home directory is accessed by a client. Note that Enable Logging must first be selected on the Web Site tab before this feature works. Logging of the home directory is enabled by default.

Index This Resource   Select this check box if you want the Indexing Service to add the contents of the home directory to its master index. By default, the Indexing Service is installed when you install Windows Server 2003.

Note   Although Read access is enabled by default on the Default Web Site, whether you can access a particular Web site and its contents depends on a number of conditions. See Chapter 32 for more information about securing access to IIS Web sites.

Application Settings
If you selected a local directory or network share for your home directory, you also have the option on the Home Directory tab to specify application settings relating to any Web application you implemented in this directory. An example of a Web application might be a collection of ASPs working together to provide some programmatic functionality to the user who visits the site. Developing Web applications is not the subject of this book, but the settings you can configure here include these:

- **Application Name**   Use this field to give your application a unique friendly name.
- **Starting Point**   Applications can consist of a tree of directories and their contents. The top of this tree is the application starting point.
- **Execute Permissions**   This option allows you to specify which types of applications are allowed to run in the home directory. Choices include None, Scripts Only, or Scripts And Executables.
- **Application Pool**   This option allows you to select the application pool associated with this home directory.

Important   If you specify Write access for the directory along with Scripts And Executables, your security might be threatened. An untrusted user might be allowed to upload a hostile executable program file to the server and cause damage.

Documents Tab
The Documents tab of the Properties window for a Web site allows you to specify possible file names for default documents for the home directory and specify the order in which a browser attempts to access them. The five types specified by default are (in order) Default.htm, Default.asp, Index.htm, Iisstart.asp, and Default.aspx.
For example, if a browser tries to connect to the Default Web Site on the server server.example.com by using the URL \texttt{http://server.example.com}, the server first checks to see whether a file named Default.htm resides in the home directory. If such a file is there, it is returned to the client. If not, the server checks for a file named Default.asp. The process continues until either a file is returned or the list of default documents is exhausted. You can specify additional default document names or delete existing ones if you like. You can also disable default documents entirely, in which case clients must know and type the actual name of the file they want to access on the server—for example, by using the URL \texttt{http://server.example.com/default.htm}.

This tab also lets you specify the name of a footer file (written in HTML) that is appended to the bottom of every file retrieved from the site by a client. You can use this, for example, to add a copyright statement or disclaimer to the bottom of each page. If you’re using FrontPage to develop your content, you can create complex footers that display information such as the date when the file was last modified, a hit counter, and so on.

**Directory Security Tab**

The Directory Security tab allows you to specify whether anonymous users are allowed to access content in your site, to restrict access to a Web site, and to enable secure HTTP communication. Let’s take a look.

**Anonymous Access and Authentication Control**

To specify whether anonymous users are allowed to access content in your site or whether some form of authentication will be required, open the Authentication Methods dialog box, shown in Figure 33-10, by clicking Edit within the Anonymous Access And Authentication Control field on the Directory Security tab. Use the dialog box to configure these settings:

- **Enable Anonymous Access** This option specifies whether anonymous access is allowed and which Windows user account is used to provide this kind of access. The default anonymous user account, created during installation of IIS on the server, is named \texttt{IUSR_servername}, where \texttt{servername} is the NetBIOS name of the server. Anonymous access means users can access content in the site using their Web browsers without needing to have their credentials authenticated in any way, and it’s the typical authentication method used for public Web sites on the Internet. The other forms of authentication discussed next authenticate the user’s credentials in some fashion and are used primarily for intranets, extranets, and secure Internet sites.

- **Integrated Windows Authentication** Here, a cryptographic exchange is used to securely authenticate the user without actually passing credentials across the connection. The user isn’t prompted for credentials; instead, his or her currently logged-on credentials are used. Integrated Windows authentication can also use Kerberos authentication if the server has Active Directory installed on it and if the client browser supports it.

- **Digest Authentication For Windows Domain Servers** This authentication method works only with Active Directory accounts. It can work across firewalls and proxy
servers. A hash or message digest is passed across the connection instead of the user’s actual credentials. The information is transmitted in clear text but is hashed, so it’s essentially undecodable and secure. The domain controller for which the authentication request is made requires a plain-text copy of the user’s password, however, so special precautions must be taken to secure the domain controller. Note that a Realm must be defined if you are using digest authentication.

- **Basic Authentication** This option specifies whether basic authentication is allowed. If used, the client is presented with a dialog box requesting credentials and those credentials are then passed over the network connection in unencrypted form. Basic authentication is defined in the original HTTP 1 specification and is supported by virtually all types of Web browsers, including the oldest ones. If users accessing your site are using older browsers that can’t be authenticated using other forms of authenticated access, you might need to enable basic authentication on your site, but be aware that it is intrinsically insecure.

- **.NET Passport Authentication** This uses Microsoft Passport technology to perform authentication. A default domain must be defined before you can enable this authentication method.

**Note** Integrated Windows authentication is designed to be used primarily on intranets and other internal networks because it won’t work through an HTTP proxy connection. It will, however, work over a Point-to-Point Tunneling Protocol (PPTP) connection.

Figure 33-10  The Authentication Methods dialog box
Real World  Combining Different Authentication Methods

Consider the consequences of selecting more than one method in the Authentication Methods dialog box. If you select Anonymous Access together with some form of authenticated access such as basic authentication, anonymous access is attempted first. If this fails, authenticated access is tried. Enabling Anonymous Access can fail if the NTFS permissions on the resource explicitly deny access to the anonymous user account, for example.

If you select two or more forms of authenticated access, the most secure forms are attempted first. For example, integrated Windows authentication is tried before attempting basic authentication. For information about how authentication fits into the general scheme of IIS security, see Chapter 32.

IP Address and Domain Name Restrictions

The Directory Security tab also allows you to restrict access to a Web site by giving clients a particular IP address or DNS domain name. Figure 33-11 shows the IP Address And Domain Name Restrictions dialog box that you can access from this tab.

![IP Address and Domain Name Restrictions](image)

**Figure 33-11**  The IP Address And Domain Name Restrictions dialog box

Use this dialog box either to allow access to the site for all clients except for those whose IP addresses or domain names are specified here, or to deny all clients access to the site except for those whose IP addresses or domain names are specified here. You can place restrictions on clients in three ways:

- Specify the IP address of a particular client.
- Specify a network ID and subnet mask representing a range of IP addresses.
- Specify the DNS name of a particular domain.
Note that selecting the last option can significantly affect server performance because reverse DNS lookups must be performed on all clients prior to granting them access. For information about how IP address and domain name restrictions fit into the general scheme of IIS security, see Chapter 32.

Secure Communications

The Directory Security tab also allows you to enable secure HTTP communications by implementing the SSL 3 protocol, which you can use to encrypt Web traffic between client and server. SSL is essential if you plan to use your server for running Web applications that involve financial transactions or hosting sensitive information. Web browsers access a secure server using SSL by using URLs that are prefixed by `https://` instead of the usual `http://` prefix.

SSL is based on public-key cryptography, in which digital certificates are used to establish the identity and trustworthiness of servers (and of clients), while a public/private key pair is used for encrypting and decrypting transmissions to ensure that the information being transmitted is secure and has integrity (in other words, that it’s from who it says it’s from). Public-key cryptography and its associated concepts are covered in Chapter 21.

Before attempting to implement secure communications, you must establish access to a certificate authority (CA) that can grant the IIS server the necessary server certificate and public/private key pair. For this purpose, you have the following choices:

- Use a trusted public CA—such as VeriSign, Inc.—to obtain the certificate and key pair. This solution is good if you want to enable secure communications for a public Internet site you are hosting on your server.

- Install Certificate Services on one or more Windows servers in your enterprise and be your own CA. This solution is best if you want to enable secure communications to a private intranet site you are hosting on your server. See Chapter 24 for information about how to install and configure Certificate Services.

To enable SSL, you first need to generate a certificate request file and submit this to a CA in order to receive a server certificate from the CA. The server certificate contains the associated public key and is used for verifying the identity of the server and establishing secure connections.

To obtain a server certificate, follow the steps outlined next. For this example, the server certificate is being requested for the Default Web Site on server server.example.com; this server is also running Certificate Services. The (clever) name of the CA is Company Root CA.

1. Click Server Certificate on the Directory Security tab of the Default Web Site Properties window. This starts the Web Server Certificate Wizard. Click Next to dismiss the welcome message and display the available options. (See Figure 33-12.)

2. Select Create A New Certificate. Click Next.
3. Select Prepare The Request Now But Send It Later if you plan to submit a security request file to a public CA. (Later, you'll need to install or bind the certificate you receive from the CA to your server.) Or select Send The Request Immediately To An Online Certification Authority if you want to request, obtain, and bind the certificate in one shot by submitting your request directly to a certificate server in your enterprise. Click Next.

4. Specify a friendly name for the certificate (the name Default Web Site is suggested here by default) and a bit length to indicate the strength of the encryption key (which can be powers of 2 between 512 and 16384 bits, inclusive). Click Next.

5. Specify organization and organizational unit names for your certificate. Click Next.

6. Specify a common name for your site. Use the fully qualified DNS name for the site if your site is a public one on the Internet. In this example, server.example.com is the common name for the Default Web Site. Click Next.

7. Specify the city, state, and country. Use official names and not abbreviations (except for two-letter country codes). Click Next.

8. Type a file name for the certificate request. Click Next.

9. A summary page is displayed showing you what just happened. You're using your own CA here, however, and you don't need to find another one.

10. In this example, you generate a file that encapsulates the request. Because you're handling the CA on your own server, you have to finish the process. Open the Certification Authority, submit the new request, and then issue the certificate. You can then install the certificate.
After a server certificate is installed on your Web site, you can view the certificate information by clicking View Certificate on the Directory Security tab. Figure 33-13 shows a certificate installed on the server.

![Server certificate for server.example.com](image)

**Figure 33-13  Server certificate for server.example.com**

Now finish enabling SSL for the Default Web Site on server.example.com by following these steps:

1. Switch to the Web Site tab of the Default Web Site Properties window, and verify that the SSL port is specified as 443, the default SSL port. (You can use the Advanced button to configure other SSL identities for the site if you want.)

2. Switch back to the Directory Security tab, and click Edit in the Secure Communications section of the tab. The Secure Communications dialog box opens. (See Figure 33-14.)

3. Select the check box Require Secure Channel (SSL), and click OK to finish configuring SSL for the Default Web Site. (The other options in this dialog box are discussed in the sidebar “Secure Communications Options.”) Click OK again to apply the changes to your site and implement the new settings.

4. Now test secure communications by using Internet Explorer to open the URL `http://server.example.com`. Select the Default Web Site node in the console tree of IIS, click Action, and select Browse from the drop-down menu.

5. Internet Explorer starts and tries to access the default home page of `http://server.example.com`. The result should be a message displayed that says, “This page must be viewed over a secure channel.” Choose Open from the File menu and type the revised URL `https://server.example.com`. 

6. A dialog box might appear indicating that you are about to view pages over a secure connection; if it does, click OK. The home page Default.htm should be displayed.

**Real World  Secure Communications Options**

Besides enabling SSL using the server certificate installed on the IIS system, you can also use the Secure Communications dialog box in Figure 33-14 for the following purposes:

- To specify that SSL connections will use strong 128-bit encryption.
- To specify how to handle client certificates. Client certificates verify the identity of clients and are typically used when remote users need to securely access a corporate intranet over a nonsecure Internet connection. You can specify either to ignore, accept, or require client certificates during SSL communications.
- To enable client certificate mapping. This feature enables administrators to create mappings between Windows Server user accounts and client certificates so that users who have the appropriate client certificate can automatically be authenticated and logged on to the network.
- To enable a certificate trust list (CTL). A CTL is a list of approved CAs for the Web site that are considered trusted by the Web site. CTLs are created using the CTL Wizard by clicking New at the bottom of the Secure Communications dialog box.
HTTP Headers Tab
You can use the HTTP Headers tab of the Properties window for a Web site to enable content expiration on the site, to specify custom HTTP headers that are returned by the server to requesting HTTP clients, to enable and specify Internet Content Rating Association (ICRA) content ratings on the server, and to specify additional MIME mappings for a particular Web site.

Content Expiration
When you enable content expiration on the site and a client browser requests a file from the site, the HTTP headers returned by the server include information regarding the expiration date of the site’s contents. The client can then decide whether it needs to download a newer version of the file or use an existing copy in the client browser cache.

Note  If your site contains information that changes frequently (such as sports scores), you can force clients to always retrieve fresh copies of files from the server (and never use cached versions of these files) by selecting the Expire Immediately option.

Custom HTTP Headers
This rather esoteric feature allows you to specify custom HTTP headers that are returned by the server to requesting HTTP clients. You might use this option in certain situations involving firewalls or proxy servers to enable or disable specific features during HTTP sessions. You can see the dialog box in Figure 33-15.

Content Rating
This option is used to enable and specify Internet Content Rating Association (ICRA) content ratings on the server. These settings rate the site’s violence, sex, nudity, and language content and are typically enabled on sites hosting content unsuitable for viewing by minors.
More Info  For more information about the ICRA, see http://www.icra.org.

MIME Types
The MIME type option allows you to specify Web site–specific MIME mappings. Click MIME Types and add, edit, or delete the mappings for the current site.

Custom Errors Tab
The Custom Errors tab allows you to specify how your server will generate HTTP error messages when users attempt to access the selected Web site. (See Figure 33-16.)

Figure 33-16  Specifying custom HTTP error messages

The HTTP specification defines that the first header line returned by a Web server in response to a request by a client will contain a number and associated message indicating the status of the request. These three-digit numbers are called HTTP status codes, and they fall within various ranges:

- **200 through 299**  A successful HTTP transaction has occurred. (The most common status code is 200 OK.)
- **300 through 399**  Redirection to another URL has occurred.
- **400 through 499**  An error has occurred. Examples include the following:
  - **400 Bad Request**  The server can’t understand the syntax of the request.
  - **401 Unauthorized**  The user’s credentials don’t allow him or her to log on to the server.
❑ **403 Forbidden**  Access is denied for some reason other than user credentials, such as the client having a restricted IP address or needing to use SSL to access the server.

❑ **404 File Not Found**  The file you’re trying to access doesn’t exist (or is misplaced or misnamed) on the server.

■ **500 through 599**  A server error has occurred or the requested feature isn’t implemented.

Instead of returning bare HTTP status codes and their brief messages for the error codes (400 through 499), however, IIS is configured by default to use predefined HTML pages that contain somewhat more information than the status codes and messages. These “error files” are located in the `\%WinDir%\help\ishelp\common` folder on the server, and you can modify them if you want.

Alternatively, by selecting one of these error files on the Custom Errors tab and clicking Edit Properties, you can specify that the default HTTP status codes and messages will be returned by the server when that error occurs, or that any specified file located in either a local folder or a network share will be returned when that error occurs. Companies commonly use this feature to create error pages that contain elements such as the company logo, the e-mail address of customer support, or even a search tool for finding the page the client is trying to access.

---

**Note**  IIS uses more detailed error messages than are included in the original HTTP specification. For example, the HTTP error code 401—which in HTTP simply means unauthorized—is represented in IIS by a group of codes spanning from 401.1 through 401.7, representing various reasons a server might deny a user’s credentials.

---

**Managing FTP Sites**

The four levels of IIS administration that apply to the World Wide Web Publishing Service also apply to the second core service of IIS, the FTP Service. Because administering servers, sites, directories, and files is similar between the two services, this section is condensed to avoid repetition.

By default, the FTP service is not installed. Use Control Panel to install the FTP service. This process creates a default FTP site, which you can access in the IIS Manager.
Server-Wide FTP Properties

In addition to the general server-level tasks of connecting to an IIS server to administer its services, backing up and restoring a server configuration, and throttling total bandwidth used by all IIS operations on the machine, IIS also lets you globally configure the master properties for all existing FTP sites on your server and for all new ones you might create.

To configure the FTP server-level properties for a particular IIS server, select the FTP Sites node in the IIS console tree that represents the server, click Action on the toolbar, and choose Properties from the drop-down menu to open the Properties window for the server. (See Figure 33-17.)

![Figure 33-17  The FTP Sites Properties window](image)

This Properties window has five tabs used for configuring the default global settings for existing FTP sites. All new FTP sites you create on the machine inherit these settings. Note that some of the settings at this level are unavailable because they can’t be applied to all FTP sites but only to specific FTP sites. For example, the IP Address field on the FTP Site tab can’t be globally configured because it is specific to each FTP site.

Configuring Individual FTP Site Properties

The site-level properties for a particular FTP site are identical to those at the FTP Sites level shown in Figure 33-17. This section covers the various settings you can configure using the Properties window for a particular FTP site. Remember that site-level settings for a newly created FTP site are inherited from the FTP Sites properties previously specified, while
modifying settings at the site level overrides similar settings configured at the FTP Sites level. The properties of the Default FTP Site are used for this discussion.

**FTP Site Tab**

Like the Web site properties used in site-level administration, the FTP site properties allow you to specify FTP site identities, configure connections, and enable logging. The connections and logging settings work the same way as those for Web site properties, so they aren’t covered here. But identification and current sessions are.

**Identification**

Like Web sites, each FTP site hosted on an IIS machine must have a unique identity so that FTP clients can connect to it to upload or download files. Unlike Web sites, however, FTP uses two (not three) parameters to define an FTP site: IP address and TCP port number.

The identity for an FTP site is specified on the FTP Site tab of the Properties window for the particular FTP site under consideration. For FTP sites on the same machine to have unique identities, they must differ from each other in at least one of the two parameters. In other words, to host several FTP sites on the same server, you can use one of the following methods:

- Configure multiple IP addresses on the server’s network card, and select a different IP address for each FTP site, leaving each site’s TCP port set to 21 (the default TCP port for FTP). Clients can then connect to a specific site by using either the site’s IP address or its associated fully qualified DNS name (if either a DNS server is available on the network or a local hosts file is configured on the client). This method is preferred for public FTP sites because it is the easiest way for users to connect.

- Configure only one IP address for the server’s network card, and use this IP address for every FTP site while assigning a different TCP port (above 1023) to each FTP site hosted on the machine. In this case, the user must know the TCP port of each site to connect to it. This method is sometimes used to hide private FTP sites from view (although FTP is inherently nonsecure anyway, as you shall soon see).

**Current Sessions**

The Current Sessions button on the FTP Site tab opens the FTP User Sessions dialog box for that site, which displays all users who are currently connected to the site, the IP addresses of their clients (or of your proxy server if they’re behind your firewall), and the time elapsed since they connected. (See Figure 33-18.) You can select any user to disconnect him or her from your site, or you can click Disconnect All to terminate all sessions on your site.
Note  Figure 33-18 displays two anonymous users who are connected to the Default FTP Site, which is configured to allow anonymous access. The user IEUser@ accessed the site by opening the URL ftp://ftp.example.com in Internet Explorer 6, while the user someone@example.com used the Windows command-line FTP utility and logged on with user name anonymous together with the optional password equal to the user’s e-mail address, someone@example.com. On the other hand, if users log on using basic authentication (described next), the FTP User Sessions dialog box shows their user names in the Connected Users column.

Security Accounts Tab
The Security Accounts tab of an FTP site’s Properties window functions similarly to the Directory Security tab of a Web site’s Properties window. FTP site operators have limited administration rights on the site, similar to those granted to Web site operators discussed previously. However, authentication control is much simpler for the FTP service. (See Figure 33-19.) Although the WWW service supports four levels of authentication (anonymous, basic, digest, and integrated) plus the option of enabling SSL for encrypted transmission, FTP supports only the anonymous access and basic authentication methods.

Because you already know about anonymous access and basic authentication, now you just need to learn how to configure FTP authentication settings using the Security Accounts tab, which at first glance appears a bit confusing. Two check boxes account for this confusion:

- Allow Anonymous Connections
- Allow Only Anonymous Connections
Table 33-1 shows how combinations of selecting and deselecting these two check boxes produce different combinations of anonymous access and basic authentication. If you enable anonymous access, IIS needs a user account to make this work. By default, the IUSR_servername account is specified, but you can select another one if you like. (Make sure it has the right to log on locally to the server console, because this is necessary for basic authentication to work.) You can then either specify the password manually or allow IIS to synchronize the password with those set in Windows.

Table 33-1 Combinations of anonymous and basic authentication for FTP

<table>
<thead>
<tr>
<th>Allow Anonymous Connections</th>
<th>Allow Only Anonymous Connections</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Only anonymous access is enabled</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Both anonymous access and basic authentication are enabled, with anonymous access being attempted first</td>
</tr>
<tr>
<td>No</td>
<td>N/A</td>
<td>Only basic authentication is enabled</td>
</tr>
</tbody>
</table>

**Note** If you must enable basic authentication on your FTP site, only users who have the right to log on locally to the IIS server hosting the FTP site are able to be authenticated and connect to the site. Make sure you physically secure the server from misuse by these users if they are working in your organization.
Real World  FTP Security

FTP is viewed as less secure than HTTP because FTP supports only anonymous access and basic authentication. For instance, if you're running an internal FTP site within a company and are using basic authentication, any person with a network sniffer can potentially obtain a trace of an FTP session and determine a user's password. Furthermore, if you connect to an FTP site using Internet Explorer and are authenticated using basic authentication (after entering your credentials into the Login As box), your user name appears in the URL as something similar to ftp://someone@ftp.example.com. So if you leave your machine, lock your console or people will know who logged on to the FTP site.

Messages Tab

FTP sites typically have a banner, welcome, exit, and maximum connections message that the server provides for users as appropriate. Specify the text of these messages on the Messages tab of an FTP site's Properties window.

Home Directory Tab

FTP has two possible choices for the location of the home directory mapped to the virtual root of the site. One is a local directory on one of the server's disks; the other is a UNC path to a network share located on a file server somewhere else on the network. (Credentials must be supplied to access this share.) Specify either of these on the Home Directory tab shown in Figure 33-20. Note that FTP sites can't be redirected to a URL like Web sites can (as was shown in Figure 33-9).

Figure 33-20  The Home Directory tab for the Default FTP Site
Access Permissions

FTP permissions are simpler than WWW permissions:

- **Read**  Selecting this check box allows users to read or download files stored in the home directory and allows users to list the contents of the directory.

- **Write**  Selecting this check box allows users to upload files to the home directory.

- **Log Visits**  Selecting this check box causes an entry to be added to the IIS log files whenever any file is downloaded from or uploaded to the home directory by a client. Note that Enable Logging must first be selected on the FTP Site tab before this feature works. Logging of the home directory is enabled by default.

*Note*  If you're hosting a public FTP site on the Internet, select UNIX style for maximum compatibility with users running older FTP client software. Some clients might be unable to interpret MS-DOS style correctly.

Directory Listing Style

When a Web browser such as Microsoft Internet Explorer accesses an FTP site, provided that Read access is enabled for the home directory, the user is presented with a directory listing showing the contents of the directory. This directory listing can be presented in either the original FTP style (UNIX style) or in standard Windows style (MS-DOS style). The same information is presented either way; it’s just displayed differently.

Directory Security Tab

Like Web sites, you can also control access to FTP sites according to the IP address or a range of IP addresses (discussed for Web sites earlier in the chapter).

Configuring FTP Directory Properties

In FTP directory-level administration (that is, in the administration of FTP virtual directories), Properties windows of virtual directories created within FTP sites have only the following two tabs:

- **Virtual Directory**  You can configure the location of the content for the virtual directory and specify the access permissions.

- **Directory Security**  You can specify IP address and domain name restrictions for the virtual directory.
Unlike Web sites, physical directories within an FTP site aren’t displayed within the IIS console window. The FTP service in IIS requires no file-level administration because individual files within an FTP site aren’t displayed in the console window either.

**Managing NNTP Virtual Servers**

The third core IIS facility on Windows Server 2003 is the Network News Transfer Protocol (NNTP) service. NNTP is the application-layer protocol that underlies the worldwide USENET system of news servers on the Internet. IIS includes an NNTP service that can be used to create news sites, which are also implemented as virtual servers in the same way as Web and FTP sites. Use Add/Remove Programs in Control Panel to install the NNTP service subcomponent of IIS if you need to.

**What NNTP Service Does**

The NNTP service on IIS fully supports both the client/server and server/server portions of NNTP and can be administered either through the IIS snap-in for the MMC or by a Web browser using NNTP Service Manager (HTML). Like other core IIS facilities, the NNTP service is fully integrated with Windows Server 2003 event and performance monitoring, and it integrates with the Indexing Service for full-text indexing of newsgroup content.

You can use the NNTP service to implement private news servers for hosting departmental discussion groups within your company or to implement public news servers that provide customer support resources to Internet users. It isn’t designed to pull feeds from USENET hosts on the Internet, however. For that purpose, obtain Microsoft Exchange Server and implement the Internet News Service on it to give it NNTP capability. You can use Microsoft Outlook Express to connect to NNTP service on an IIS machine to download a list of newsgroups, read existing messages, reply to messages, and post new messages.

When you install the NNTP service on IIS, it automatically creates the Default NNTP Virtual Server, shown in Figure 33-21. You configure this virtual server in a moment, but first know that you can host multiple NNTP virtual servers on a single machine. In this way, several departments in your company can run separate news servers on a single IIS machine, just as they can run separate Web or FTP servers. How to do this is covered next, and then other aspects of managing NNTP virtual servers are discussed. Notice that the NNTP service is managed with a combination of Properties windows and wizards, just like the other IIS core services.
NNTP Service Wizards

You can run the following wizards from the IIS console to configure and manage various aspects of NNTP virtual servers:

- New NNTP Virtual Server Wizard
- New Virtual Directory Wizard
- New Expiration Policy Wizard
- New Newsgroup Wizard

New NNTP Virtual Server Wizard

To create a new NNTP virtual server, select the server’s node in the IIS console tree, click Action, point to New, and choose NNTP Virtual Server from the drop-down menu. This starts the New NNTP Virtual Server Wizard, which takes you through the following steps:

1. Specify a display name for the new NNTP virtual server that will be used in the IIS console tree.
2. Specify an IP address and port number for the server. (The standard TCP port for NNTP is 119.) The identity of the virtual server you are creating must be different from that of any existing virtual servers on the machine.
3. Specify locations for the internal server files and news content files. These can be local directories or network shares.
4. Click Finish, and a new NNTP virtual server is created on your IIS machine.
New Virtual Directory Wizard
The NNTP service allows you to create virtual directories within your NNTP virtual server. You can use these virtual directories to store portions of the news server’s content. To see how this works, follow this procedure to create a new virtual directory within the Default NNTP Virtual Server:

1. To start the wizard, select the Virtual Directories node under Default NNTP Virtual Server in the console tree, click the Action menu, point to New, and choose Virtual Directory from the drop-down menu.

2. On the opening page of the wizard (Figure 33-22), specify the newsgroup subtree whose content you want to store in the directory. For example, if you want to store messages for the newsgroups example.support.pc, example.support.mac, and example.support.unix, you can specify example.support in this text box. You actually do this now and create the three newsgroups later. Click Next.

3. Choose File System or Remote Share, and then click Next to specify a path to the local directory or network share where the content will be located. (If you choose a network share, you must enter appropriate credentials.) Choose File System, and specify C:support as your path. Click Finish.

4. The Virtual Directories node under the Default NNTP Virtual Server node in the console tree now shows the new virtual directory listed there, along with its associated newsgroup subtree. You can double-click the new virtual directory to open a Properties window where you can adjust its settings.
New Expiration Policy Wizard
In the New Expiration Policy Wizard, you can create an expiration policy that specifies how long articles remain in newsgroups before they expire (are deleted). Articles can expire if they surpass a specified age. Follow these steps to create an expiration policy for the example.support.* newsgroups:

1. Start the New Expiration Policy Wizard by selecting the Expiration Policies node under the NNTP virtual server, opening the Action menu, and then selecting Expiration Policy from the New menu.

2. Specify a descriptive name for the expiration policy, such as Expiration Policy for example.support.* groups. Click Next.

3. In the Newsgroups list, you see a list of the groups the expiration policy applies to. Remove the default (*) from the list because you don’t want it to apply to all the groups present on the NNTP server.

4. Click Add, type example.support as the pattern that groups need to match to have this expiration policy, and then click OK. You can add several patterns if you want to apply your expiration policy to several disjointed newsgroup subtrees. Click Next.

5. Specify the time in hours that articles are allowed to remain in the group before expiring. (The default is 168 hours, or 7 days.) Click Finish.

6. Select the Expiration Policies node under the Default NNTP Virtual Server node in the console tree to see the new expiration policy displayed. You can double-click the expiration policy to open its Properties window and reconfigure it manually if you want.

New Newsgroup Wizard
To add a new newsgroup, select the Newsgroup node in the console tree, click Action, point to New, and choose Newsgroup from the drop-down menu. Specify a display name for the new newsgroup and click Next. Alternatively, you can provide a description and pretty name. Click Finish. It’s just that simple.

Configuring the Default NNTP Virtual Server
To configure an NNTP virtual server, use the various tabs in its Properties window. For simplicity, the Default NNTP Virtual Server continues as your example. You’ll notice some similarities between configuring NNTP virtual servers and Web/FTP sites discussed previously. Along the way, you also create the three company.support.* newsgroups mentioned earlier.
The General Tab
Figure 33-23 shows the General tab of the Default NNTP Virtual Server Properties window on the Windows Server 2003 called server.example.com. On this tab, you can specify the following options:

■ **Path Header**  Whatever you type here appears in the Path line of the NNTP headers attached to messages posted to this virtual server. Typically, you might type the fully qualified DNS name of the virtual server here, but this is optional.

■ **IP Address**  Like FTP sites discussed earlier in this chapter, NNTP virtual servers are uniquely identified by a combination of IP address and TCP port, and each NNTP virtual server hosted on the same IIS machine must differ in at least one of these parameters. Although you already know the advantages and disadvantages of the different ways of configuring this, note that the Advanced button allows you to configure additional identities (combinations of IP address, TCP port number, and SSL port number) for an NNTP virtual server, if you want to.

![Figure 33-23](image)

**Figure 33-23**  The General tab of the Properties window for the Default NNTP Virtual Server

Connections and logging on this tab are similar to that for Web and FTP sites discussed earlier in this chapter. You can enable logging here, but you can also enable or disable it on a directory-by-directory basis, just as you can with Web and FTP sites.
Access Tab
The Access tab allows you to specify which authentication methods can be used when users try to connect to the virtual server. Do this by clicking Authentication under Access Control, which opens the Authentication Methods dialog box. These methods are similar to those for Web sites as discussed earlier in this chapter, although the way this dialog box presents them is slightly different.

Connection Control is the same as IP Address And Domain Name Restrictions for Web and FTP sites, which were discussed earlier. Secure Communication is also similar. Click Certificate to start the somewhat misnamed Web Server Certificate Wizard described earlier in this chapter.

Settings Tab
The Settings tab contains a variety of settings related to how NNTP functions for the selected virtual server. Specifically, you can set the following options:

■ Enable or disable posting to the virtual server by NNTP clients. For example, you might disable posting when you are performing maintenance on the server.
■ Limit the maximum size of a message that can be posted. This is usually a good idea.
■ Limit the maximum amount of data that can be posted by a user during a single connection. This is also a good idea.
■ Allow other NNTP servers to pull newsfeeds from this virtual server. This option does not enable pulling from other IIS servers because the NNTP service on IIS doesn’t support this—rather, this option applies to USENET hosts and Exchange Servers running the Internet News Service.
■ Allow control messages. This allows clients and servers to issue special commands to the virtual server for performing tasks such as creating new newsgroups or deleting existing ones.
■ Specify the DNS name of an SMTP mail server to be used for moderated newsgroups hosted on the virtual server.
■ Specify the fully qualified DNS name to which the moderator belongs.
■ Specify the e-mail address for the administrator of the virtual server so that this person can receive any error messages generated by the NNTP service when messages posted to a moderated newsgroup can’t be delivered to the specified SMTP mail server.

Security Tab
On the Security tab, you can specify an NNTP operator who can perform limited administrative tasks on the virtual server, just as with Web and FTP sites discussed earlier.
Managing Newsgroups

To view the list of existing newsgroups on the virtual server, to modify the properties of a group, to create new groups, or to delete existing ones, use the Newsgroups node of the NNTP server. Note that a number of default newsgroups already exist within the Default NNTP Virtual Server. Let’s create the three newsgroups described earlier. Follow these steps to create the group company.support.pc:

1. Select the Newsgroups node, click Action, select New, and then select Newsgroup on the drop-down menu. This opens the New Newsgroup Wizard, shown in Figure 33-24.

2. Type `example.support.pc` for the name of the newsgroup. Click Next.
3. Type a description, if you want.
4. Type a newsgroup pretty name. (Some clients, such as Outlook Express, support this feature.)
5. Click Finish, and the new newsgroup should appear in the right pane of the console.

Repeat these steps to create the `example.support.mac` and `example.support.unix` groups. You test these groups in a moment.

Note If you have hundreds (or thousands) of newsgroups defined on your virtual server, you can use the Limit Enumeration option on the Newsgroups shortcut menu to locate newsgroups whose properties you want to modify. In the Find Newsgroups dialog box, just specify a portion of the newsgroup name and the maximum number of results you want returned.
Connecting to the Default NNTP Virtual Server

After you configure your NNTP virtual server properties, you can test it by trying to access your newsgroups using an NNTP client such as Outlook Express. Follow these steps:

1. Start Outlook Express. If this is the first time you have used Outlook Express, cancel out of the wizard that tries to help you configure an SMTP mail account. (After you configure an account, it doesn't appear again.)

2. Choose Accounts from the Tools menu to open the Internet Accounts dialog box.

3. Click Add and choose News to create a new NNTP account. Specify your name, e-mail address, and the fully qualified DNS name of the news server (or its IP address if you prefer). If the NNTP virtual server doesn't have anonymous access enabled, select the check box My News Server Requires Me To Log On and specify your credentials accordingly.

4. Click Next and then click Finish.

5. Close the Internet Accounts dialog box. You're prompted to download newsgroups from the news account you just added. Click Yes.

6. The Newsgroup Subscriptions dialog box appears, showing you all the newsgroups available on the NNTP virtual server you connected to and allowing you to subscribe to groups of your choice. Double-click a group to subscribe to it.

7. Click OK to return to the main Outlook Express window.

8. To test the newsgroups, simply browse through them on your virtual server, post messages, read messages, and so on. (See Figure 33-25.)

![Figure 33-25 Testing the new newsgroups using Outlook Express](image-url)
Displaying NNTP Sessions

After you make some test postings, switch to the IIS console on your IIS server and select the Current Sessions node under the Default NNTP Virtual Server node in the console tree. This displays information regarding the users who are currently logged on to the virtual server. You can select any user, click Action, and choose either to terminate that user’s connection or terminate all connections to the NNTP virtual server.

Rebuilding an NNTP Virtual Server

You can perform one important maintenance task on an NNTP virtual server: rebuilding the indexes and hash tables that the virtual server employs to keep track of the articles that have been posted to it. Circumstances that warrant rebuilding the server include manually deleting files from the NNTP directories where newsgroup content is stored, experiencing a disk failure and losing some newsgroup content, or having trouble accessing articles.

To rebuild the Default NNTP Virtual Server, for example, follow these steps:

1. To stop the Default NNTP Virtual Server, select the Virtual Server in the console tree and then click Stop on the console toolbar (or click Action or right-click the Virtual Server node and then choose the Stop command).

2. With the Default NNTP Virtual Server node still selected, click Action, point to All Tasks, and choose Rebuild Server from the drop-down menu.

3. Select a standard or thorough rebuild (thorough is slower), and click Start.

Managing SMTP Virtual Servers

The fourth and last core service that is included as part of IIS on Windows Server is the Simple Mail Transport Protocol (SMTP) service. SMTP is the application-layer protocol that underlies the worldwide system of SMTP hosts (mail servers) on the Internet. If it’s not already installed on IIS, use the Add/Remove Programs utility in Control Panel.

What SMTP Service Does

Administer the SMTP service on IIS 6 as you have for the other services: by using the IIS Manager. Like other core IIS facilities, it is fully integrated with Windows Server 2003 event and performance monitoring. IIS includes the SMTP service primarily for use by mail-enabled Web applications. A simple example is an HTML form that a user fills out and submits, upon which the form handler (the script or program that takes the information entered by the client and actually does something with it) composes an e-mail message and sends it using the SMTP service.
Chapter 33  Advanced Internet Information Services

Note that the SMTP service included with IIS isn’t intended to replace a company mail server—IIS has no facility for creating individual user mailboxes, and even the POP3 e-mail server of Windows Server 2003 doesn’t really substitute for a full company mail server. For that, we recommend Microsoft Exchange 2003. The SMTP service is intended mainly for mail forwarding by mail-enabled Web applications, although it can both send and receive mail and relay mail from other SMTP hosts. If you need a full-featured mail server for your company, try Exchange Server and implement the Internet Mail Service on it to give it SMTP capability.

Note  Another alternative is to add the mail server role in Manage Your Server. This provides both SMTP and POP3 (for receiving) services.

When you install the SMTP service on IIS, it automatically creates a Default SMTP Virtual Server, as shown in Figure 33-26. You can host multiple SMTP virtual servers on a single machine, but this is rarely needed because the Default SMTP Virtual Server can be configured to forward mail for multiple SMTP domains. Like other IIS core services, the SMTP service is managed by a combination of Properties windows and wizards.

Figure 33-26  The Default SMTP Virtual Server shown in the IIS console window

SMTP Directories

Important to the operation of an SMTP virtual server is a series of directories that are used for processing mail. For the Default SMTP Virtual Server, these directories are all located within the \inetpub\mailroot directory on the server. Some of the more important directories include the following:

- **Drop**  If the SMTP service receives incoming messages that are addressed to recipients belonging to SMTP domains managed by the SMTP virtual server, they are dropped here. Web applications can then be written to collect incoming mail delivered to this directory and process it accordingly.
Pickup  If the SMTP service picks up outgoing messages, they are placed in the Pickup folder and delivered to their destination SMTP host when a connection is made with that host (or with an intermediate host that can relay mail).

Queue  If a message that a Web application places in the Pickup folder can’t be delivered immediately (for example, if the remote SMTP host is temporarily down), it is moved to the Queue folder to await further attempts at delivery.

Badmail  If message delivery repeatedly fails, outgoing mail is classed as undeliverable, and if it can’t be returned to sender, it winds up here.

Configuring the Default SMTP Virtual Server

To configure an SMTP virtual server, use the various tabs in its Properties window. For this example, the Default SMTP Virtual Server is used for simplicity. Configuring an SMTP virtual server is similar to configuring Web and FTP sites and NNTP virtual servers (all of which were discussed previously).

General Tab

The virtual server identity is configured on the General tab of the Properties window for the virtual server, shown in Figure 33-27. The options are similar to those offered by the services discussed so far. IIS logging is implemented in the same way as for the other IIS core services. Note, however, that logging is disabled by default.
Identification
An SMTP virtual server has a two-part identity similar to that of an NNTP virtual server. The two parameters that uniquely specify an SMTP virtual server are IP address and TCP port number. (The default TCP port number is 25.) By clicking Advanced on this tab, you can assign multiple identities (IP address and TCP port number) to your server, but each identity must differ by at least one of these parameters. The usual procedure is to leave the TCP port set to 25 and use one IP address for the virtual server, with a mapping from this address to a fully qualified DNS name in a DNS server or Hosts file.

Connections
You also configure connection limits on the General tab. You can either specify the number of connections allowed numerically or set them as unlimited by clearing the check boxes. Also, you can set a timeout value for outgoing connection attempts.

IIS Logging
IIS logging is implemented in the same way as for the other IIS core services. Again, logging is disabled by default.

Access Tab
On the Access tab, you can choose the type of access and control you want.

Access Control
The SMTP service supports anonymous access, basic authentication, and integrated Windows authentication for inbound connection attempts. Basic authentication security uses a user name and password, while integrated Windows authentication includes the Windows Server 2003 domain name as well. Clicking Authentication on the Access tab opens the Authentication dialog box, where you can configure these settings. Note that only the anonymous access option is selected by default.

The Transport Layer Security (TLS) option is essentially a variant of SSL encryption, and you can enable it here for inbound connection attempts. You must first obtain a server certificate from a CA and install it on the SMTP virtual server before TLS can be properly enabled. (See the next section.) For more information about IIS authentication methods, see the earlier coverage of virtual server security in this chapter.

Note The settings configured here specify how your SMTP virtual server authenticates remote SMTP hosts that are trying to connect to it to deliver mail—that is, for inbound connection attempts. To specify authentication methods for outbound connection attempts, select Outbound Security on the Delivery tab.

Secure Communication
As expected, if you click Certificate, the Web Server Certificate Wizard (still a misnomer) starts. Click Communication to require that access take place on a secure channel, after
the certificate is installed on the virtual server. Requesting, obtaining, and installing server certificates is discussed earlier in this chapter.

Connection Control
IP address and domain name restrictions function in the same way for the SMTP service as they do for the other three IIS core services.

Relay Restrictions
Click Relay in the Relay Restrictions field on the Access tab to open the Relay Restrictions dialog box, shown in Figure 33-28. This setting is important because allowing untrusted SMTP hosts to relay mail through your SMTP virtual server is an invitation for sending spam. Generally deny relay privileges to all hosts and grant them to only known hosts you trust or those that can properly authenticate with your server.

![Relay Restrictions dialog box](image)

Figure 33-28  Configuring relay restrictions for the Default SMTP Virtual Server

Messages Tab
You can use the Messages tab to limit messages in three ways:

- Limit the maximum message and session sizes in kilobytes for this virtual server. (Session size refers to all the messages delivered by a single SMTP connection.)
- Limit the maximum number of outbound messages that can be sent in one connection. If more messages need to be sent, additional connections are opened between the hosts.
- Limit the maximum number of recipients for a message.

In addition, you can change the directory where bad mail is placed, and you can specify the e-mail address to which copies of nondelivery reports (NDRs) will be sent.
Note Make sure the maximum session size is greater than the maximum message size. Don’t choose a maximum session size that’s too low, or a remote SMTP host might continually resubmit a message for delivery. On the other hand, if you regularly send a lot of messages to a few domains, set the maximum number of outbound messages per connection low enough so that the SMTP service opens multiple connections to the remote host, resulting in faster and more efficient transfer of messages.

Delivery Tab
The Delivery tab allows you to specify the following settings related to mail delivery:

- **Outbound** Allows you to specify how your virtual server responds when it tries to connect to a remote SMTP host to deliver mail but can’t connect. For outbound mail, you can specify a series of retry intervals, a delay notification value, and an expiration timeout value.

- **Local** For local delivery, you can specify only delay notification and expiration timeout values.

- **Outbound Security** Allows you to specify the authentication method (anonymous access, basic authentication, or integrated Windows authentication, any of which can run with or without TLS) when attempting an outbound connection with a remote SMTP host. If you specify either form of authenticated access, you need to specify credentials as well. Note that you can configure only one outbound authentication method for an SMTP virtual server, and anonymous access is selected by default because this is most commonly used on the Internet.

- **Outbound Connections** Allows you to limit the number of connections and specify the timeout value for terminating inactive connections. You can also limit the number of connections per domain and specify the TCP port used for outgoing transmissions.

- **Advanced** Clicking this button opens the Advanced Delivery dialog box, on which you can configure the following options:
  - **Maximum Hop Count** Allows you to specify the maximum number of hops between SMTP hosts that are allowed before the message is determined to be undeliverable. The value you specify here is included in the header fields of each message sent. Be sure to specify a value here to prevent messages from endlessly looping when they can’t be delivered directly to the remote host.
  - **Masquerade Domain** Allows you to specify the DNS domain name, which replaces the local domain name in the Mail From header field of each message sent. This feature is optional.
− **Fully Qualified Domain Name** Allows you to specify the full DNS name of the SMTP virtual server. The value displayed here is the one found on the Network Identification tab of the System Properties window in Control Panel, but you can change this if your server has multiple roles and DNS names.

− **Smart Host** Allows you to route all outgoing messages to a specific SMTP host instead of trying to connect to the host responsible for the recipient’s DNS domain. You can type either a fully qualified domain name or an IP address. (Place square brackets around the IP address if you use one.) This feature is optional.

− **Attempt Direct Delivery Before Sending To Smart Host** This option can be enabled only when a smart host has been specified. Its use is self-explanatory.

− **Perform Reverse DNS Lookup On Incoming Messages** Should be left disabled because it causes a significant hit on server performance.

**LDAP Routing Tab**

If you want your SMTP virtual server to be able to access a Lightweight Directory Access Protocol (LDAP)–compliant directory service to obtain information such as the addresses of senders and recipients, you can enable this feature and specify the name, schema type, binding type, account, password, and naming context for connecting to the directory server. If you enable LDAP Routing, the default entries in the fields allow the SMTP virtual server to connect to and use the Windows Server 2003 Active Directory. Supported directory services include the following:

− Microsoft Exchange Server directory

− Microsoft Windows Active Directory

− Microsoft Commercial Internet System 2.0 Mail with Microsoft LDAP Service

**Security Tab**

SMTP operators have limited administration privileges for the virtual server, similar to the way operators function in Web sites, FTP sites, and NNTP virtual servers.

**SMTP Domains**

Each SMTP virtual server that is created manages at least one SMTP domain. This domain is specified automatically as the default local domain, and you can view it by selecting the Domains node under the SMTP virtual server node in the console tree. This is the DNS domain that is being serviced by the virtual server, and any incoming messages addressed to recipients within this domain are either dropped in the Drop folder or returned to sender with an NDR.

You can have only one default local domain on the virtual server, and this domain is stamped on the message headers of all outgoing messages. However, you can create
additional alias domains so that your virtual server can manage more than one SMTP domain. Alias domains use the same settings as the default domain and deliver incoming messages to the same Drop folder.

You can also create remote domains and specify delivery requirements for each one differently, which is useful if some remote SMTP hosts that you need to connect to use TLS but others don’t. Global TLS configuration isn’t enough in this case. In addition, for remote domains you can specify a predefined delivery route and even use wildcards to include subdomains. Use remote domains for connecting to remote SMTP hosts to which you frequently need to send mail.

**Note**  
Like the NNTP service, an SMTP virtual server node has a Current Sessions node under it in the console tree that you can use to view current connections to the server and terminate any or all of those connections.

### The New Domain Wizard

Use the New Domain Wizard to create either alias domains or remote domains. Creating alias domains is covered here. (See the online documentation for information about creating remote domains.) To create an alias domain for the Default SMTP Virtual Server, follow these steps:

1. Select the domain node in the console tree, click Action, point to New, and choose Domain from the drop-down menu. This starts the New SMTP Domain Wizard.
2. Click the Alias domain type button, which creates an alias domain for the default local domain. Click Next.
3. Specify the DNS name for the new alias domain. Click Finish.
4. View the domains for the Default SMTP Virtual Server by selecting the Domains node in the console tree. Any incoming messages that are addressed to recipients in the alias domain are dropped in the Drop folder and stamped with the default domain name.

**Note**  
By opening the Properties window for the default local domain, you can change the location of the folder where mail is dropped from Mail-root\Drop to some other local folder on your server. Alias domains always use the same Drop folder as the default local domain, however.

### Web Service Extensions

IIS is in a secure state when installed, unless you’re upgrading. This means that no dynamic content is served, only static content. If you’re doing an upgrade, however, the settings that were in effect at the time of the upgrade are maintained. You can specify
what Common Gateway Interfaces (CGIs) and ISAPIs can run on your server, as well as list those that are forbidden, and enable ASP and ASP.NET applications. To view and edit the current settings, click the Web Service Extensions node under the server. You see the currently configured settings, as Figure 33-29 shows.

![Web Service Extensions settings](image)

**Figure 33-29**  Web Service Extensions settings

Usually, you visit the Web Service Extensions solely to enable and disable extensions. Do this by highlighting the extension name and selecting Allow or Prohibit. There are a number of additional tasks you can perform on the Web Service Extensions page, however. Among them are the following:

- Add new Web service extensions, as seen in Figure 33-30. Provide a name, provide the path to the file (by using a DLL for an ISAPI extension and an EXE for a CGI extension), and finally set the status to Allowed.

![New Web Service Extension dialog box](image)

**Figure 33-30**  The New Web Service Extension dialog box
Allow all Web service extensions for a specific application. Start this task, and then open the application drop-down box to select an application. You see the extensions that applications can use in the Extensions To Be Allowed list box.

Prohibit all Web service extensions. This will likely break much of the functionality of your server, so carefully consider using this option.

Remote Administration

The final topic for the chapter is using a standard Web browser such as Internet Explorer for remote administration of IIS sites, servers, and services. Until now, only the IIS console has been used for IIS administration. IIS console administration is intended primarily for administration on the internal network of a company. By using Remote Administration (HTML), however, administrators can manage most (but not all) aspects of IIS from remote locations, even over a nonsecure connection on the Internet and through a proxy server or firewall (if configured properly). This section looks briefly at Remote Administration (HTML) and how to use it.

Administration Web Site

Remote Administration (HTML) is an optional component of IIS that is not installed by default when you install Windows Server 2003. When this component is installed, a new Web site appears in the console tree of the IIS console window. This new Web site is called the Administration Web Site and is basically an ASP application that allows administrators to manage IIS using any Web browser that supports JavaScript.

Enabling Remote Administration

To be able to use Remote Administration (HTML), administrators need only to be able to connect to the Administration Web Site. To make this possible, you need to perform this procedure first:

1. Open the Properties window for the Administration Web Site in the IIS console.
2. On the Web Site tab, find the TCP port number assigned to this site and write it down. By default, the TCP port is 8099. If you want secure access, set the SSL port to something appropriate. By default, the TCP port is 8098.
3. Switch to the Directory Security tab, and open the IP Address And Domain Name Restrictions dialog box. By default, all IP addresses are granted access; you’ll probably want to limit this to a set of IP addresses you know are safe, such as 127.0.0.1. (Remote clients need to have static IP addresses.)
4. Apply the changes by closing the Properties window for the Administration Web Site. You’re ready to go.
Testing Remote Administration

To test your configuration of the Administration Web Site, start Internet Explorer on the machine whose IP address you have granted access and open the URL \textit{https://Server\_Name:Admin\_Port}, where \textit{Server\_Name} is the IP address or DNS name of the IIS server, and \textit{Admin\_Port} is the SSL port number you noted for remote administration. The default is port 8098.

A dialog box appears requesting your credentials (user name, password, and Windows domain), after which you’re informed that you are using a nonsecure connection for performing remote administration. (You can configure SSL on the Administration Web Site just as on any other Web site if you prefer more security.)

At this point (if you’ve done everything correctly), Remote Administration (HTML) should be functional and you should be connected to the Administration Web Site with your browser. (See Figure 33-31.) You can perform most administration tasks using Remote Administration (HTML), but not all. For example, you can’t configure certificate mapping using Remote Administration (HTML) because to do so requires coordination with other Windows Server services that aren’t accessible from a Web browser.

![Figure 33-31](image)

Figure 33-31  The opening page of Remote Administration (HTML) as seen in Internet Explorer 6

\textbf{Note}  Another, and in many ways easier, method of remote administration of an IIS server is to enable Remote Desktop on the server. This lets you use the regular IIS Manager, which we find easier to use and navigate.
Summary

This chapter demonstrated the common administration tasks of configuring the settings of the four IIS core services: WWW, FTP, NNTP, and SMTP. You can configure these services at up to four levels: server, site, directory, and file. You configure them by using a combination of Properties windows and wizards and by working with the XML metabase. The next chapter addresses Microsoft Internet Security and Acceleration Server 2004.
Microsoft Internet Security and Acceleration Server 2004 (ISA 2004) is the latest and most secure version of the outstanding software firewall from Microsoft. What started many years ago as Microsoft Proxy Server has come a long way.

This chapter introduces you to important concepts related to ISA 2004, covers some planning considerations, and then shows you how to set up and manage ISA 2004 on the network.

Concepts

The main goals of ISA 2004 are to protect a network from hackers, improve Internet performance for clients on the network, provide secure access to internal resources for remote users and offices, and control client access to the Internet.

ISA 2004 maintains control of connectivity and isolates the internal network by having two (or more) completely separate physical connections—one to the Internet and one to the internal network. Each network is connected to a different network card, and all packets must pass through the ISA 2004 software to get from one connection to the other.

The mechanisms that ISA 2004 uses to achieve these aims are fairly straightforward. The following three basic techniques are used:

- Network address translation
- Packet filtering and application layer filtering
- Caching
The following sections discuss each of these techniques, as well as the different methods available to support clients, how ISA 2004 works in a large enterprise environment, and how to plan your ISA 2004 deployment.


---

**Real World  Methods of Sharing Internet Connections**

There are two basic methods of providing Internet connectivity to clients on the network: using standalone devices such as a router or firewall device, and using software-based solutions running on a PC.

Microsoft offers a number of software-based solutions: Internet Connection Sharing (a simple method of sharing an Internet connection in a workgroup that is built into all versions of Windows newer than Microsoft Windows 98), Routing and Remote Access (a somewhat more sophisticated solution that comes integrated into Windows Server 2003 and Windows 2000 Server), and ISA 2004.

Although Routing and Remote Access is capable of sharing an Internet connection with multiple clients and providing limited security to the internal network using network address translation (NAT), ISA 2004 provides better security and user control, in addition to accelerating Internet access for users.

---

**Network Address Translation**

Network address translation (NAT) hides your actual IP address from machines beyond the device doing the translation. Only the device doing NAT needs to have a valid Internet IP address; all clients and servers on the internal network can be given addresses from the address ranges reserved for private networks. (See the “IP Addresses for Internal Networks” sidebar.)

To provide NAT, you can use a standalone router or firewall device, a proxy server or firewall software package such as ISA 2004, or the built-in NAT functionality of Windows Server 2003 (provided by either the Routing and Remote Access service or the Internet Connection Sharing service).

Although NAT is the backbone of any Internet connection-sharing technique, the security it provides is minimal. ISA 2004 uses stateful packet and application layer inspection to provide a robust firewall solution.
Real World  IP Addresses for Internal Networks

Back when folks were deciding how to parcel out IP addresses (and long before anyone figured out how to perform NAT), the need for addresses that could be used for test networks was recognized. A special set of IP addresses called private network addresses was defined in RFC 1918 for test or other networks not physically connected to the Internet.

These private network addresses allow a much larger address space than would be possible with officially assigned addresses, while protecting the integrity of the Internet. If a machine with one of these addresses were to connect to the Internet, it wouldn’t cause a conflict with another machine because routers automatically filter out these addresses.

The following addresses are designated for private networks that won’t be directly connected to the Internet. They can, of course, be connected to the Internet through ISA 2004 or another method that performs NAT:

- 10.0.0.0 through 10.255.255.255 (a single “Class A” network)
- 172.16.0.0 through 172.31.255.255 (16 contiguous “Class B” networks)
- 192.168.0.0 through 192.168.255.255 (256 contiguous “Class C” networks)

ISA 2004 automatically includes these addresses in its local address table (LAT) when you initially install the program.

Another byproduct of using ISA 2004 for address translation is that all the machines on a network appear to have the same single address to the outside world—the external address of ISA 2004 itself. This allows an entire organization to connect to the Internet with as little as a single public IP address, and even that one address doesn’t need to be a fixed IP address—ISA 2004 can handle a variable public IP address.

Packet Filtering and Application Layer Filtering

Because every packet that passes to or from the Internet must first pass through ISA 2004, ISA 2004 is in a perfect position to act as a gatekeeper. Besides performing simple NAT, ISA 2004 can inspect each packet and permit only packets that use approved protocols and ports to enter or leave the internal network. (This process is called packet filtering.) When packet filtering is enabled, you can also restrict access to specific external sites or enable only certain external sites to be seen. In addition, third-party ISA 2004 plug-ins can add other controls and functionality.
In addition to basic packet filtering, ISA provides Stateful Packet Inspection (SPI), which analyzes the origin of every packet and allows only unaltered packets from approved hosts or networks to pass through the firewall. This prevents hackers from tampering with packets, and it provides the ability to block incoming packets that aren’t specifically requested by network clients.

Stateful packet filtering is filtering that happens on layer 3 (the IP layer) of the OSI stack. As such, it is useful, but it can no longer be considered sufficient for all security needs because it must open ports based on a presumption that a packet is authorized, without being able to verify that the content isn’t malicious. ISA 2004 adds intelligent application filtering—stateful application-layer inspection—that inspects the actual application frames to determine the content and can filter based on that content. ISA 2004 ships with a number of intelligent application-layer filters, including HTTP, RPC, and SMTP.

**Caching**

Every organization has certain Web sites that users visit regularly. ISA 2004 can cache information from these frequently accessed sites so that when users connect to the site, much of the information is actually delivered by ISA 2004, not the remote site. Caching significantly improves the apparent speed of the connection to the Internet and leaves more Internet bandwidth available.

ISA 2004 can use off hours, when few users are connected to the Internet, to check frequently accessed sites to make sure the information it has stored for that site is current. This monitoring, called *active caching*, helps to balance and smooth out demand, providing improved throughput during busier times because fewer pages and images need to be downloaded.

ISA 2004 also performs fancy tricks such as splitting audio or video streams and sharing them with multiple users on the network, and performing reverse caching, which accelerates the perceived performance of Web servers to Internet clients.

**Client Types**

Clients can connect to ISA 2004 using the Firewall client, SecureNAT client, or Web Proxy client.

For Microsoft Windows clients, install the Firewall client software. This lets you manage clients by user group. For Macintosh and UNIX clients and network devices, set up TCP/IP properties to use ISA 2004 as the default gateway. (This configuration is what a SecureNAT client is, a client that uses ISA 2004 as a gateway.) Set up all systems to use the Web proxy service for Web browsing. This is done automatically when installing the Firewall client software, but it needs to be done manually for SecureNAT clients. Table 34-1 describes each method.
Chapter 34  Internet Security and Acceleration Server 2004

In this section, we’ll cover the basic installation and initial configuration of ISA Server 2004 Standard Edition in a single perimeter configuration—the most basic firewall and caching configuration. This is certainly not the only installation or even the most common installation in an enterprise setting, but it demonstrates the basic concepts of installation, which can be extended to more complex requirements.


System Requirements

The system requirements for ISA 2004 are pretty basic, as shown in Table 34-2. Note the operating system requirement, however, for Enterprise Edition. It is supported only in Windows Server 2003.

Table 34-1  ISA 2004 client modes

<table>
<thead>
<tr>
<th>Feature</th>
<th>Firewall Client</th>
<th>SecureNAT Client</th>
<th>Web Proxy Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Windows clients</td>
<td>All TCP/IP systems</td>
<td>All HTTP 1.1–compliant Web browsers</td>
</tr>
<tr>
<td>support</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software configuration</td>
<td>Firewall client software</td>
<td>TCP/IP default gateway</td>
<td>Web browser proxy configuration</td>
</tr>
</tbody>
</table>

Table 34-2  ISA Server 2004 system requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Pentium III, 550 MHz or equivalent.</td>
</tr>
<tr>
<td>RAM</td>
<td>256 MB, minimum.</td>
</tr>
<tr>
<td>Hard disk</td>
<td>150 MB minimum on an NTFS partition. More for caching.</td>
</tr>
<tr>
<td>Other</td>
<td>One network adapter for the internal network. One additional network adapter, modem, or ISDN adapter for each additional network connected to the ISA server. One additional network adapter for interarray communications when using a network load balancing (NLB) array of Enterprise Edition ISA servers. The usual operating system requirements of a CD/DVD, video monitor, keyboard, and mouse.</td>
</tr>
</tbody>
</table>
Installation

Installation of ISA 2004 is typical of many Microsoft installations. There’s an autostart menu program, as shown in Figure 34-1. Click Install ISA Server 2004 to start the actual installation.

Figure 34-1 The ISA Server 2004 installation menu

The Installation Wizard opens, and you can click through the usual steps, including agreeing to the licensing agreement, entering your name and the serial number, choosing a typical, full, or custom installation. As always, you should choose the custom installation option to give yourself the most flexibility and control over what is installed and where. The default for a custom installation is shown in Figure 34-2.

Figure 34-2 The default settings for a custom installation
You’ll probably want to add at least the Firewall Client Installation Share if this is a simple perimeter ISA 2004 installation. The Message Screener can be installed only if the SMTP Virtual Server is installed.

Next, you can specify the network addresses that are to be treated as being on the local network. Click Add here to specify the addresses, as shown in Figure 34-3.

![Figure 34-3  Specifying the local network addresses during the ISA Server 2004 installation](image)

You can manually enter the address range here, or choose the network adapter that is connected to your internal network by clicking Select Network Adapter, which will open the dialog box shown in Figure 34-4.

![Figure 34-4  The Select Network Adapter dialog box](image)
If your ISA 2004 server is connected to a device that also does network address translation such as a router or gateway, as ours is, you should deselect the box to automatically add private address ranges to your internal network. You'll need to manually add the private address ranges that are not used by the router to your internal network.

Once you've entered the internal address range, you'll get a chance to confirm it or make changes. As you click through the steps of the wizard, you'll find it's even smart enough to know whether you're running the installation from a Remote Desktop session, and it will offer to set up a system policy to allow remote management from your current workstation. You can also allow earlier versions of the Firewall Client to connect.

**Note** There is no publicly available 64-bit Firewall Client at the time of this writing, though one is expected “soon”. If your network has to support x64 Edition clients, you’ll need to configure them as NAT clients. This may mean creating special rules for these computers.

The wizard will also disable several services if it finds them present, for security reasons. While you could go back and re-enable them, it’s a bad idea. Your ISA server should run nothing but ISA 2004. Really. Nothing else. Just ISA 2004.

If the ISA 2004 installation detects that you’re currently using the server as a Routing and Remote Access server, it will offer to migrate the existing rules or let you choose to start from scratch. If your existing Routing and Remote Access Service (RRAS) and virtual private network (VPN) connections are working right, by all means migrate them.

Finally, click Install to begin the actual installation. Once the installation completes, you'll have a choice of exiting or starting the ISA Server Management console to continue the configuration, as shown in Figure 34-5.

![Figure 34-5 The ISA 2004 Installation Wizard Completed dialog box](image)
Chapter 34  Internet Security and Acceleration Server 2004

Note  If you’re running the installation from a Remote Desktop session, even if it’s a console session, you will lose connectivity during the installation. Be patient. When the installation is finished, you can reconnect if the session has timed out, or your session will automatically come back to life.

Securing Your ISA 2004 Server

ISA 2004 is a critical layer in the overall defense of your network. You need to take concrete steps to ensure that it is itself secure and protected against attack. If your firewall is compromised, it’s certain your network won’t be far behind.

The following are the key steps to securing your ISA 2004 server:

- Ensure that the ISA 2004 server is in a physically secure location. If untrusted people have physical access to your firewall, you no longer have a secure network.
- Use the Microsoft Baseline Security Analyzer 2.0 (MBSA2) to analyze your system security. This step should be regularly repeated to ensure that all appropriate updates have been applied.
- Determine who should have the ability to logon to the ISA 2004 server, and restrict logon rights accordingly.
- Disable any services that are not absolutely required, and do not add more applications or roles to the ISA 2004 server that aren’t absolutely required for ISA 2004 to function.
- Require strong passwords on the network as a whole, but especially on all accounts that can log on to the ISA 2004 server.

Initial Configuration of ISA Server 2004

The installation of ISA 2004 creates an environment that does not allow any computers on your network to connect to the Internet—users attempting to browse will see the error message shown in Figure 34-6 if they have the Microsoft Firewall Client installed or have an explicit proxy setting in Internet Explorer. Otherwise, they’ll see an unhelpful 404 message. In either case, you’re going to get some calls to the help desk if you haven’t warned people or provided an alternative!
Before computers on your network can connect to the Internet, you need to do some initial configuration. You need to complete the following tasks:

- Define your network topology
- Create firewall policy rules
- Define caching rules

As you can see from the Getting Started page of ISA 2004, shown in Figure 34-7, you can also define VPN rules and set up monitoring, but neither of those tasks is necessary to get your network back online, so we'll hold off on those for a bit.
Defining Your ISA 2004 Network Topology
The first step in getting your network back online and using ISA 2004 as its firewall and caching server is to define the network configuration that ISA 2004 should use. To do this, open the ISA management console, if it isn’t already open, and connect to the ISA 2004 server you want to manage. Then follow these steps:

1. Click the server name in the leftmost pane to open the Getting Started page shown in Figure 34-7.

2. Select Define Your ISA Server Network Configuration to open the Networks page shown in Figure 34-8. The default Edge Network that we’re setting up is shown, but if your network topology is different, you’ll need to define it accordingly. Start by clicking on the Templates tab in the rightmost pane to see a list of typical network topologies, and pick the one that matches your network. If none of them is a good match, you can define your own network topology.

Figure 34-8 The Networks page of the ISA Server 2004 management console
3. ISA 2004 creates definitions for several networks based on the answers you gave during initial installation. If you need to add more networks, network sets, or network rules, you can do that here, and you can come back to this page at any time to add or change the settings here.

4. If you want to enable automatic discovery of your ISA 2004 server by Firewall clients and Web proxy clients, now’s a good time to do it. Double-click the Internal network, and then click the Auto Discovery tab, shown in Figure 34-9.

![Figure 34-9 The Auto Discovery tab for the Internal network](image)

5. Select the Publish Automatic Discovery Information box.

6. Modify the DNS records for your internal DNS domain to create an alias called WPAD that points to the fully qualified domain name (FQDN) of your ISA 2004 server, as shown in Figure 34-10.

   More Info  For details on creating DNS aliases, see Chapter 17.

7. Close the Properties dialog box, and click the Apply button at the top of the center pane of the ISA management console, as shown in Figure 34-11.
Figure 34-10  Create a DNS alias called WPAD that points to your ISA 2004 server

Figure 34-11  Any changes in ISA configuration must be applied before they take effect

8. Click Back to Getting Started at the bottom of the rightmost pane to return to the Getting Started page.
Create Firewall Policy Rules

Next we need to define Firewall Policies that will allow clients from our internal network to connect to the outside world. By default, the only policy created during initial installation is the generic Deny policy that should always appear as the last policy in your rule list.

To allow basic Web browsing from computers in our network, we need to define an Allow policy to allow computers on the Internal network to use standard Web protocols to access computers on the External network. We’ll create just a simple “Allow All” rule that allows all computers on the Internal network to browse Web sites on the External network.

To create an Allow All Browsing Rule, follow these steps:

1. Open the ISA management console, and connect to the ISA 2004 server you want to manage, if you haven’t already done so.
2. Click the server name in the leftmost pane to open the Getting Started page shown in Figure 34-7.
3. Select View And Create Firewall Policy Rules, to open the Firewall Policy page shown in Figure 34-12. As you can see, there is only a single policy defined—a Deny policy.
4. Click the Tasks tab in the rightmost pane, and then click Create New Access Rule to open the New Access Rule Wizard.
5. Type a name for the new Rule, such as Allow All Browsing, and click Next to open the Rule Action dialog box.
6. Select Allow, and click Next to open the Protocols page shown in Figure 34-13. Select Selected Protocols from the drop-down list.

![Figure 34-13](image)

**Figure 34-13** The Protocols page of the New Access Rule Wizard

7. Click Add to open the Add Protocols dialog box shown in Figure 34-14. Select the protocols you want to allow from the various categories. For our basic Web access rule, we'll select the two browsing protocols, HTTP and HTTPS, the Ping protocol, POP3 so that our users can get mail, and MSN Messenger to allow instant messaging. Your choices might be different, of course.

![Figure 34-14](image)

**Figure 34-14** The Add Protocols dialog box
8. Click Close to close the Add Protocols dialog box, and then click Next to open the Access Rule Sources page.

9. Click Add to open the Add Network Entities dialog box. Here you'll select All Protected Networks from Network Sets and click Add to add this network set to the Access Rule Sources page, shown in Figure 34-15. Close the Add Network Entities dialog box.

![Figure 34-15 The Access Rule Sources page of the New Access Rule Wizard](image)

**Note** The All Protected Networks set is predefined by ISA 2004, and it includes all networks except the predefined External network set.

10. Click Next to open the Access Rule Destinations page. Click Add to open the Add Network Entities dialog box again, and this time add the External network from the Networks section. Close the Add Network Entities dialog box.

11. Click Next to open the User Sets page. It will show All Users already added, and you'll leave that alone. Click Next and then Finish to complete the New Access Rule Wizard.

12. Click Apply to actually enable the changes. The new firewall policy isn't actually enabled until you click the Apply button on the main ISA 2004 management page, as shown in Figure 34-11.

13. If you now try to connect to the Web from a machine on your internal network, instead of getting the Access Denied message shown earlier in Figure 34-6, you'll be connected.
Define Caching Rules
ISA 2004 is also a caching server that can save your organization significant time and money by caching frequently accessed Web sites locally. When a user browses to the site, they’re actually receiving the pages from the hard drive of the ISA 2004 server. Meanwhile, the server can be configured to proactively update pages during hours of low bandwidth usage, distributing the Internet bandwidth usage more evenly and reducing the need for additional bandwidth to provide acceptable speed during busy times.

To enable caching, follow these steps:
1. Open the ISA 2004 management console, and navigate to the Getting Started page.
2. Click Define How ISA Server Caches Web Content.
3. Click the Tasks tab of the rightmost pane, as shown in Figure 34-16.

![Figure 34-16 The initial Cache Rules Tasks page](image)

4. Click Define Cache Drives (Enable Caching) to open the Define Cache Drives dialog box shown in Figure 34-17. ISA 2004 uses only NTFS drives for caching.
5. Select a drive, and enter the amount of space to use for caching on that drive in the Maximum Cache Size (MB) field and click Set. For optimum caching, you should choose a drive on a physically separate disk from the system drive, and ideally you should distribute the caching load across multiple physical disks if possible.

Note Always define the maximum cache size your system can support. If your cache runs out of space, it will drop older items in the cache. If a user then needs that item, it will have to be retrieved from the Internet and will in turn force another item out of the cache.
6. Once you’ve defined all your caching drives, click OK to close the Define Cache Drives dialog box.

7. Click Apply on the main ISA 2004 management console page to actually apply the changes. You’ll be warned that enabling caching will require restarting the Firewall service, as shown in Figure 34-18. If you choose to restart the service now, any current connections to or from the Internet will be dropped. You can, however, choose to save the changes but not actually apply them until you restart the service manually.

8. Restarting the service enables the caching and allocates the space on the cache drives.
Additional Configuration Tasks

The steps completed to this point will perform a basic installation and configuration to get ISA 2004 up and running as a perimeter firewall and caching server, with internal clients having basic Web access. For most installations, that is only the starting point. Most installations will need to have additional tasks completed, including setting up VPN access, configuring monitoring, and configuring additional Firewall policies to expand and fine-tune the rules that control access. And, finally, many installations will need to have reverse proxy set up or have internal servers published that need to be securely reachable from the Internet.

Define VPN Access

One of the common tasks for ISA 2004 is setting up VPNs. And it’s something that ISA 2004 does really well. Frankly, as an old time network administrator, I was dreading having to write the VPN section because I remember what a colossal pain it was in the old days.

To define VPN access, follow these steps:

1. Open the ISA 2004 management console, and navigate to the Getting Started page.
2. Click Configure VPN Access to open the VPN Clients tab of the Virtual Private Networks (VPN) page, shown in Figure 34-19.
3. Click Verify That VPN Client Access Is Enabled to open the VPN Clients Properties dialog box shown in Figure 34-20.
4. Select the Enable VPN Client Access check box. Specify the maximum number of VPN clients that this ISA server will allow. The default is 100.

5. Click the Groups tab and then click Add to add the accounts you will allow to VPN in your network. Avoid specifying individual accounts; rather, create a specific security group that is allowed access, as shown in Figure 34-21.
6. Click the Protocols tab, and specify the VPN protocols you will support. The default is PPTP, but you can also use L2TP/IPSec for more secure access.

7. Click the User Mapping tab. If you will be using RADIUS to authenticate requests, you can simplify the configuration by setting a default Windows domain to use. For simple, Windows-managed VPN access that includes only Windows clients, you can leave User Mapping disabled.

8. Click OK to close the dialog box. Nothing has yet been actually enabled—we need to Apply the settings before they can take effect, and we're not ready yet.

9. Click Remote Access Configuration to open the Virtual Private Networks (VPN) Properties dialog box shown in Figure 34-22.

![Figure 34-22 The Virtual Private Networks properties dialog box of Remote Access Configuration](image)

10. The defaults are for only External networks to use VPN access, DHCP on the Internal network for IP address assignment, MS-CHAPv2 authentication, and no RADIUS server. Click the appropriate tabs to make any changes necessary, and then click OK to close the dialog box.

11. Optional: Click View Firewall Policy For The VPN Clients Network to configure the Firewall Policy rules for VPN clients if you want to create special policies that apply only to your VPN clients.

12. Optional: Click View Network Rules to verify the network rules for incoming VPN clients and to set up any special network rules that only apply to VPN clients.
13. When you’ve configured all the settings, click Apply in the main ISA 2004 VPN Clients page, and the new configuration will be applied and VPN access will be enabled.

Setup Monitoring
ISA 2004 provides a diverse set of monitoring tools. The main front end to the monitoring is the Dashboard, shown in Figure 34-23, which has a capsule summary of connectivity, services, reports, alerts, sessions, and the overall system performance all on a single page. The biggest weakness of the dashboard is that it’s read only. If you want more information or detail about a particular report, alert, and so on, you need to drill down to the tab related to the type of element it is. No double-clicking or right-clicking to get more information.

![Figure 34-23 The Dashboard page](image)

The default installation provides a good starting point to add any additional reports or monitoring you need for your environment. To add a new alert or report, change the filtering of sessions, or make other monitoring changes, click the tab in the center pane for the kind of monitoring you want to modify, and then click the Tasks tab in the rightmost pane. You’ll have context-sensitive choices that are appropriate to the kind of monitoring you’re configuring.

Publishing Servers (Reverse Proxy)
In addition to firewall and caching features, ISA 2004 also supports “reverse proxy.” Reverse proxy lets you keep your key network services inside your firewall perimeter but still be available from the Web, thus protecting the servers. The two most common
examples of doing this are an extranet Web server and your e-mail server. ISA 2004 makes it easy to publish the servers and services you need to make available while protecting the servers from attack.

To publish a mail server, follow these steps:

1. Open the ISA 2004 management console, and navigate to the Firewall Policy page.
2. On the tasks pane, click Publish A Mail Server to open the New Mail Server Publishing Rule Wizard.
3. Enter a name for the rule, and click Next to open the Select Access Type dialog box, shown in Figure 34-24.

![Figure 34-24: The Select Access Type dialog box of the New Mail Server Publishing Rule Wizard](image)

4. Select the type of access you'll be providing to the mail server, and then click Next.

   **Note** If you'll be providing both direct POP3/IMAP4 access and OWA access, you need to run the wizard twice.

5. Select the services your e-mail server uses, and then click Next.
6. Specify the IP address of the server. This IP address will be on your internal network segment.
7. Click Next to open the IP Addresses dialog box shown in Figure 34-25.
8. Specify the IP addresses that should have access to the server, and click Next.

9. Click Finish to close the wizard, and then click Apply on the main Firewall Policy page to actually implement the changes.

Additional Configuration

The initial setup and configuration of ISA 2004 is fairly straightforward, as we’ve seen, in a basic configuration. Adding more features and specific rules and filters adds complexity, but doing this follows the same logic and steps as the basic configuration. We can’t begin to cover all the possibilities in a single chapter, but we want to highlight some typical configuration and management tasks. ISA 2004 has a logical consistency in the way it’s configured, and if you understand how to do one set of tasks in it, you’ll find it easy to extend that knowledge to additional tasks.

The Toolbox

The Toolbox is where you create, modify, and delete all the various elements that make up the policies of ISA 2004. You can find the Toolbox tab in the rightmost pane of the Firewall Policy section. The elements you can add, delete, or edit here include:

- Protocols
- Users
- Content Types
- Schedules
- Network objects
By combining these elements, you can create the rules and policies that you need for your network.

**Defining Network Entities**

ISA 2004 has several predefined network entities, as we've seen in setting up our original access rule. But there might well be reasons you need to define additional entities. These might take the form of individual computers or specific subnets, and they can refer to either internal or external computers and networks.

---

**Note**  
Because there is no 64-bit firewall client, you can define special rules for your 64-bit computers, allowing you to provide special access rules that apply only to them. Once a 64-bit client is available, you should remove special rules for 64-bit computers and apply consistent policies across your client network.

---

To define a new network entity, follow these steps:

1. Open the ISA 2004 management console if it isn’t already open.
2. Click Firewall Policy in the leftmost pane.
3. Click the Toolbox tab, and expand the Network Objects panel, as shown in Figure 34-26.

---

**Figure 34-26**  
The Toolbox tab, with the Network Objects panel expanded
4. Select the kind of object you want to create from the New menu as shown in Figure 34-27. The kinds of network objects you can create are listed in Table 34-3.

![Figure 34-27 Selecting a new computer object]

Table 34-3 Network object types in ISA 2004

<table>
<thead>
<tr>
<th>Object</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>One or more contiguous ranges of IP addresses.</td>
</tr>
<tr>
<td>Network Set</td>
<td>One or more defined networks. Allows you to combine noncontiguous ranges of IP addresses into a logical grouping.</td>
</tr>
<tr>
<td>Computer</td>
<td>A single IP address. (Note: A computer object is defined by an IP address only and is not directly correlated to a computer name. If you’re using DHCP to distribute IP addresses, you should use a DHCP reservation if you need a specific computer to be defined for ISA purposes.)</td>
</tr>
<tr>
<td>Address Range</td>
<td>A single contiguous range of IP addresses.</td>
</tr>
<tr>
<td>Subnet</td>
<td>A single IP subnet (network ID and subnet mask).</td>
</tr>
<tr>
<td>Computer Set</td>
<td>One or more computers, address ranges, or subnets. Predefined computer sets in ISA 2004 are Anywhere, IPSec Remote Gateways, and Remote Management Computers.</td>
</tr>
<tr>
<td>Web Listeners</td>
<td>The addresses and ports on a network that will listen for Web requests.</td>
</tr>
<tr>
<td>URL Set</td>
<td>One or more URLs that can be used to define specific access rules.</td>
</tr>
<tr>
<td>Domain Name Set</td>
<td>Groups DNS domain names into a set. Specific firewall policies can then be applied to the set.</td>
</tr>
</tbody>
</table>

5. Fill in the wizard or dialog box necessary for the object type you’re creating. Figure 34-28 shows the dialog box for creating a computer object.

6. Once the new network entity has been added, you can use it in rules to either permit or deny specific access to the entity.
Defining Users

If your clients are running the ISA Firewall Client, you can manage access to and from the Internet by user and group, giving you much more flexibility and simplifying the maintenance of policies and access rules. Plus the user will have the correct level of access regardless of what computer she or he is logged on to.

To define a new set of users, follow these steps:

1. Open the ISA 2004 management console, and navigate to the Firewall Policy page.
2. Click the Toolbox tab in the leftmost pane, and expand the Users section. There are three sets of predefined users—All Authenticated Users, All Users, and System and Network Service.
3. Click New, and the New User Sets Wizard opens, as shown in Figure 34-29. Type a name for this set of users in the User Set Name field, and click Next.
4. Click Add, and the choice of types of users to add opens, as shown in Figure 34-30.

![Add](Windows users and groups...)  
RAOD...  
Security...

**Figure 34-30** ISA 2004 supports users of three very different types

5. Select the user type, and the users or groups of users you want to add. You can choose from multiple source types here. When you have added all the users you want, click Next.

6. Click Finish to close the wizard, and then Apply in the main Firewall Policy pane to implement the change.

---

**ISA Firewall Client**

The ISA Firewall Client software provides a uniform Winsock service provider that Winsock applications can use. When an application makes a request, the Firewall Client software intercepts the request and determines whether the request needs to be routed to the ISA 2004 server. If the request is not considered local, it is routed to the ISA 2004 server for processing and further routing. Windows user information can be included in the request, allowing the ISA 2004 server to process rules and firewall policies that are user-specific.

The ISA Firewall Client is usually distributed directly from the ISA 2004 server. During initial installation, you can choose to create a distribution share for the Firewall Client. If you didn’t create the client distribution share during initial installation, just re-run the setup program to add the Firewall Client distribution share. The default share location is `\isaservername\MSPClnt`.

You can run the setup interactively, or you can perform an unattended setup to have it run without intervention. The unattended setup command line would be

`\isaservername\MSPClnt\setup /v "SERVER_NAME_OR_IP=isaservername /qn"`

By installing the ISA Firewall Client on the computers on your network, you enable advanced firewall policies that make decisions based on the Windows user or group credentials. Without the Firewall Client, you won’t have the Windows user credentials available to make firewall policy decisions.

---

**Note** There is currently no Firewall Client available for 64-bit clients. If you have policies that use Windows user credentials, you’ll need to make special exceptions for clients that are 64-bit.
Import, Export, Backup, and Restore

ISA 2004 provides both export/import capability, and full backup and restore capability. Both have their place in the defense and protection of your ISA 2004 server and should be performed regularly and on an as-appropriate basis.

Export and import can include the entire ISA 2004 configuration, but it’s most appropriate to save the partial configuration information after you’ve made a change or where you want to be able to propagate that configuration information to another server. You can choose during the export process whether to include confidential information, and apply an encryption password to the resulting .xml file that contains the configuration information.

Backup and restore are used when you want to save a complete backup of the server configuration. It includes user permissions and all confidential information, and an encrypting password is required. Use backup and restore when you want to clone the configuration of an ISA 2004 server.

To backup the configuration of an ISA 2004 server, follow these steps:

1. Open the ISA 2004 management console, and navigate to the Getting Started page.

2. Click Backup The ISA Server Configuration in the rightmost pane to open the Backup Configuration dialog box shown in Figure 34-31. Enter a descriptive file name for the backup, and click Backup.

![Figure 34-31 The Backup Configuration file dialog box](image-url)
3. The Set Password dialog box will open. Enter a password to encrypt the backup file. Passwords must be at least 8 characters and should follow strong password rules. Click OK, and the backup will start. When completed, click OK again.

To restore the configuration of an ISA 2004 server, follow these steps:

1. Open the ISA 2004 management console, and navigate to the Getting Started page.
2. Click Restore The ISA Server Configuration in the rightmost pane to open the Restore Configuration dialog box. Navigate to the saved configuration file, and click Restore.
3. Enter the encrypting password, and click OK. If you type the wrong password, you’ll see the dialog box shown in Figure 34-32, and the restore operation will terminate. If the restore operation is successful, you’ll still need to click the Apply button on the main Getting Started page before the restored configuration will be implemented.

![Figure 34-32 The ISA Server Error dialog box](image)

To export the configuration of an ISA 2004 server, follow these steps:

1. Open the ISA 2004 management console, and navigate to the main page of the portion of ISA 2004 configuration you want to export. To export the entire configuration, navigate to the Getting Started page. As an example of a partial export, navigate to the Firewall Policy page.
2. Click Export System Policy on the Tasks tab in the rightmost pane to open the Export Configuration dialog box shown in Figure 34-33. Enter a descriptive file name for the export. Select the Export Confidential Information box. If available, in this section, select the Export User Permission Settings box.
3. Click Export to open the Set Password dialog box, if you’ve chosen to export confidential information. Enter and confirm the password to encrypt the information.
4. Click OK to begin the export. Click OK again when the export completes.
To import the configuration of an ISA 2004 server, follow these steps:

1. Open the ISA 2004 management console, and navigate to the main page of the portion of ISA 2004 configuration you want to import. To import the entire configuration, navigate to the Getting Started page. As an example of a partial import, navigate to the Firewall Policy page.

2. Click Import System Policy in the rightmost pane to open the Import Configuration dialog box. Highlight the policy you want to import. Select Import Cache Drive Settings and SSL Certificates if you want.

3. Click Import. If the export was encrypted, you’ll be prompted to enter the password for the file. Enter the password and click OK.

4. Once the import completes, click OK to close the dialog box. The actual changes to the ISA 2004 server configuration won’t be implemented until you click the Apply button on the main System Policy page.

**Summary**

Every network that connects to the outside world needs a strong and flexible firewall to protect the network. Microsoft Internet Security and Acceleration Server 2004 provides a full-featured, highly configurable, and secure firewall and caching server that can be the cornerstone of the in-depth protection of your Windows network. In this chapter, we’ve covered some basic firewall and caching proxy concepts, along with the basic configuration to set up ISA 2004 on your Windows network. In the next section, we move on to tuning, maintenance, and repair. The first chapter in that section covers performance monitoring and tuning.
Part VII
Tuning, Maintenance, and Repair

Chapter 35
Performance Monitoring and Tuning ...........................................1157

Chapter 36
Disaster Planning .................................................................1203

Chapter 37
Using Backup .................................................................1221

Chapter 38
Planning Fault Tolerance and Avoidance .................................1249

Chapter 39
Using the Registry ..........................................................1265

Chapter 40
Troubleshooting and Recovery .............................................1293
Chapter 35
Performance Monitoring and Tuning

Documenting the Network, Policies, and Procedures ..................1158
Selecting a Monitoring Method .............................................1160
Using Event Viewer .........................................................1166
Using the Microsoft Windows Server 2003 Performance Advisor .....1171
Using System Monitor .......................................................1175
Performance Logs and Alerts ................................................1180
Using Network Monitor ....................................................1186
Memory and Network Tuning ..............................................1199
Summary ...........................................................................1202

Performance monitoring and tuning are two tasks that administrators often overlook, but they play an important role in server operations. Many scenarios call for monitoring a server, including the following:

- Establishing a baseline of a server's performance to serve as a reference for future comparison
- Monitoring servers to determine load and whether to upgrade the servers or reallocate workloads
- Regularly checking for program or operating system errors that can indicate a problem or potential problem
- Using a packet sniffer to perform in-depth network troubleshooting when authentication or other communications fail

This chapter discusses how to perform these tasks and others using the tools that come with Microsoft Windows Server 2003 or are available for download. For more in-depth information about performance monitoring and tuning, see the Microsoft Windows Server 2003 Performance Guide book in the Microsoft Windows Server 2003 Resource Kit (Microsoft Press, 2005).
**What Is a Bottleneck?**

Simply put, a bottleneck is a condition in which one resource is preventing another resource from functioning optimally. For example, when one application monopolizes the system processor to the exclusion of all other operations, there is a bottleneck at the processor.

Bottlenecks can occur in virtually any Windows subsystem or on any element of the network, for a number of reasons, including the following:

- The system does not have sufficient resources.
- A program or client is monopolizing a particular resource.
- A program, device, or service is failing.
- The system has incorrectly installed or configured software.
- The system is incorrectly configured for the workload.

The role of performance monitoring is to identify bottlenecks. To maximize the performance of a Windows system, you must recognize bottlenecks and take action to eliminate them.

---

**Documenting the Network, Policies, and Procedures**

Before monitoring and tuning a server, it is important to gain an understanding of the context in which the server operates. To do so, review or create documentation of the network configuration and usage, and any organizational policies or procedures that relate to the performance of the server.

**Documenting the Network**

Accurate and up-to-date documentation of a network helps prioritize performance issues and identify potential bottlenecks in the network. Create or review the following documentation:

- **Performance Priorities** Applications and network services that are business critical, as well as optimal and minimum required levels of performance for noteworthy applications and services. For example, optimal printing performance might be two minutes to print a 10-page document, while the minimum level of performance during busy times might be 20 minutes to print the same document.

- **Usage Patterns** Estimates of when users use applications and services. Document daily usage patterns such as the morning logon and e-mail rush, weekly patterns
such as end-of-the week report printing, and monthly and yearly patterns such as project deadlines and tax-preparation activities. The following list contains typical user tasks and the network components stressed by the tasks:

- Logon and Logoff events (domain controllers, DHCP, and DNS servers)
- Software updates (LAN and WAN bandwidth, software update servers)
- Accessing documents (file servers, LAN bandwidth)
- Database usage (database server)
- Internet usage (proxy and firewall servers, routers, and Internet connection)
- E-mail usage (e-mail servers)
- Wireless usage (access points, RADIUS servers, certificate servers, and domain controllers)

### Network Design
The network topology and structure and location of each device. At a minimum, record the following items:

- Internet and WAN link speeds
- Firewall locations
- Router and switch locations and speeds
- Physical network topology map
- Subnets and Virtual LANs (VLANs)
- Domains and sites
- Location of client computers, servers, Network Attached Storage (NAS), printers, and other network devices

**Note** Include with the network documentation a series of performance-monitoring logs or traces that establish a performance baseline for important servers (as discussed later in this chapter). You can also include simple network benchmarks by timing typical user tasks such as file copy operations, printing, database queries, and Intranet page loads.

### Evaluating Policies and Procedures
Another important factor in performance monitoring is reviewing the organization’s acceptable-use policy and network administrator procedures. Acceptable-use policies for employees might include provisions prohibiting or limiting the use of applications that consume large quantities of network bandwidth, such as Peer-to-Peer (P2P) applications, streaming radio or video, Voice Over Internet Protocol (VOIP) applications, and multiplayer network games.
Examine and update administration procedures as necessary to minimize the performance impact of regularly scheduled tasks such as backup, downloading and installing software updates, and software deployment.

**Selecting a Monitoring Method**

There are numerous methods of monitoring servers running Microsoft Windows. To choose the most suitable method, use the following list.

- To quickly check the real-time processor and memory usage on a server, use the Windows Task Manager.
- To monitor a large number of servers, use Microsoft Operations Manager (MOM). For more information, see the Microsoft Web site at [http://www.microsoft.com/mom](http://www.microsoft.com/mom).
- To check for functionality or security-related problems, use Event Viewer.
- To observe performance in real-time, use a graph in System Monitor. Graphs are helpful for short-term monitoring of a remote or local computer.
- To perform long-term monitoring and record keeping, use the Microsoft Windows Server 2003 Performance Advisor, Performance Logs And Alerts, or both. Server Performance Advisor provides a simple way to collect counter data, trace data, and system settings and view reports for one or more servers. Performance Logs And Alerts provides a more granular way to collect the counter and trace data, and it enables you to create alerts when specific counters go over or under the specified values.
- To monitor data sent over the network to and from a server, usually to troubleshoot network communication, use Network Monitor.

To determine how often to monitor servers or what counters to use when monitoring specific performance aspects such as memory usage, use the following sections.
Real World  Monitoring and Tuning Strategies

When monitoring or tuning a system, use the following strategies:

- Make one change at a time. Bottlenecks can be the fault of several components. Do not confuse the issue by making too many changes at once, which can make it impossible to assess the impact each change has on the system.

- Keep a record of each change, and repeat the monitoring process after every change. Tuning one resource can affect another and potentially necessitate additional changes.

- Retain logs for an extended period, and store the data in a database for trend analysis, performance assessment, and capacity planning.

- Pay attention to event logs. Operating system and application errors can have a huge impact on performance. (A failed server does not usually perform well.)

- Turn off any screen-saver programs, and stop any services that are not relevant or essential to monitoring the system.

Determining How Often to Monitor

The appropriate sampling interval depends on the duration and goals of the monitoring session. For example, use an interval of 3 to 15 seconds for short monitoring sessions and when searching for brief performance impacts. Use a longer sampling interval for routine, long-term logging or to look for a slow memory leak—5 to 15 minutes usually provides enough detail in this situation while minimizing log file size and the load on the server. Decreasing the sampling interval causes the data rate to increase, producing larger log files and placing a heavier load on the system.

Reducing the Performance Impact of Monitoring

To reduce the performance impact of monitoring a server, use the following list:

- Limit the number of objects and counters you monitor—each object and counter increases overhead.

- Do not run System Monitor in graph view for long periods on the server you are monitoring. This view incurs the highest overhead. Use Performance Logs And Alerts instead.

- Increase the sampling interval to reduce overhead. Specify sampling intervals of three seconds or more for intense scrutiny, or 10 to 15 minutes for routine logging.

- Record logs to a disk subsystem not used for performance-critical applications or services.
Monitoring Memory Usage

Lack of sufficient memory is one of the most frequent performance issues on a server. To determine whether this is the case, verify that the system has the required amount of memory to run the operating system and all applications and services, and then use Server Performance Advisor, Performance Logs And Alerts, or System Monitor to monitor the counters in the following list. See the “Memory and Network Tuning” section of this chapter for information about optimizing page files and memory usage.

- **Memory\ Available MBytes** Displays the amount of currently unused physical memory (RAM). Windows uses available memory to satisfy the memory requirements of programs. When available memory falls into short supply, Windows takes memory from the working sets of less active programs, which can result in more paging and reduced performance as Windows transfers data to and from the hard disk subsystem. Adding RAM when less than 10 to 15 percent of the total physical memory is available usually improves the performance of a server.

- **Memory\ Pages/Sec** Displays the number of pages written to or read from disk to resolve hard page faults. A *hard page fault* occurs when a process requires code or data that Windows has paged to disk and removed from physical memory. A high value for this counter does not always indicate lack of memory, but if this value is consistently above 20 per page file and the Available MBytes is below 10 to 15 percent of the physical memory in the system, the system probably would perform better with more RAM.

- **Memory\ Cache Bytes** Displays the physical memory used by the file system cache and device drivers, as well as operating system and program code that Windows can page to disk when not in use.

To check for a memory leak, look for a steady increase in the following counters regardless of the load on the server:

- **Memory\ Committed Bytes** Displays the number of committed bytes of virtual memory. Monitor this counter in conjunction with Memory\ Available Bytes.

- **Process\ Working Set, Process\ Virtual Bytes, and Process\ Handle Count** The Process\ Working Set and Virtual Bytes counters display the amount of physical memory and total memory allocated to all threads in the process you suspect might have a memory leak. The Process\ Handle Count counter displays the number of handles used by the process.

- **Memory\ Pool Nonpaged Bytes** Displays the number of bytes allocated to the nonpaged pool for objects that Windows must keep in physical memory as long as they are allocated. Use this counter in conjunction with Memory\ Pool Nonpaged
Allocs if you suspect that a kernel-mode process (such as a device driver) is the cause of a memory leak.

- **Memory\ Pool Nonpaged Allocs** Displays the number of calls to allocated space in the nonpaged pool.

To monitor paging, use these counters:

- **Paging File\ % Usage (all instances)** Displays the current percentage of used space in all page files on the system. If you suspect that paging is to blame for a bottleneck, review this value along with Memory\ Available Bytes and Memory\ Pages/Sec. Enlarge the page file(s) if the Paging File\ % Usage counter exceeds 70 percent.

- **Physical Disk\ Avg. Disk Sec/Transfer and Memory\ Pages/Sec** The Physical Disk\ Avg. Disk Sec/Transfer counter displays the average duration of each disk-transfer operation in seconds. The Memory\ Pages/Sec counter displays the number of pages written to or read from the disk when a process requires information that is no longer in its working set and must be retrieved from disk. To determine whether the system is paging excessively, multiply the values of these two counters. If the result exceeds 0.1, paging is taking up more than 10 percent of disk access time. If this condition persists over a long period, add RAM to reduce paging.

---

**Important** When the paging file reaches the maximum limit assigned to it, Windows displays a warning and increases the limit. Programs can become unstable during this time, and the system might crash if there is not enough disk space for additional virtual memory.

---

**Monitoring Processor Activity**

Two common causes of processor bottlenecks are excess demand placed on the processor by CPU-bound programs and excess interrupts generated by drivers or subsystem components, such as disk or network components. When a bottleneck occurs because a process’s threads need more processor cycles than are available, processor queues build up, causing the system response to suffer.

To monitor processor activity, examine the server roles and applications in use on the server and then use Server Performance Advisor, Performance Logs And Alerts, or System Monitor to monitor the following counters:

- **Processor\ % Processor Time (all instances)** Displays the percentage of time all processors in the system are busy. If the counter consistently exceeds 85 percent, evaluate whether the server meets the performance priorities of the organization during periods of heavy load. If it does not, install additional processors, upgrade the processors, or transfer server roles to another server to reduce load.
- **Processor\% User Time**  Displays the percentage of nonidle processor time that the server spends in user mode, where most applications and services run. To resolve a high rate, move workloads to another server, or upgrade or install additional processors. Use this counter in conjunction with Processor\% Processor Time (all instances).

- **System\ Processor Queue Length (all instances)**  Displays the number of threads waiting to execute. A sustained queue length of more than two to five items per processor or processor core indicates that the processors cannot keep up with the load.

- **Server Work Queues\ Queue Length**  Displays the number of Server service threads waiting to execute. A queue length of greater than four over a sustained period indicates possible processor congestion from the Server service.

- **Processor\ Interrupts/Sec**  Displays the number of hardware interrupts received and processed by the processor per second. Use this counter to determine whether interrupt activity is causing a bottleneck. A dramatic increase in this counter value without a corresponding increase in system activity indicates a possible hardware problem. To resolve this problem, find the network adapter or other device that is causing the interrupts. Refer to the manufacturer’s specifications for the acceptable processor threshold; use 1000 interrupts per second as a starting point.

- **Processor\% Interrupt Time**  Displays the percentage of time the processor spends receiving and servicing hardware interrupts during the sampling interval. This value gives you an indirect indication of the activities of devices that generate interrupts, such as disk drives, network adapters, and other peripheral devices. These devices interrupt the processor when they require attention or complete a task.

- **Processor\% Privileged Time**  Displays the percentage of nonidle processor time designated for hardware-manipulating drivers and operating system components. A high rate indicates a failing device or device driver. Use this counter in conjunction with Processor\% Processor Time (all instances).

---

**Note**  Setting processor affinity on multiprocessor servers can prevent other program threads from migrating to the least-busy processor and can hurt overall system performance. In general, let Windows assign threads to processors.

---

### Monitoring Disk Activity

Monitor disk activity using the Server Performance Advisor, Performance Logs And Alerts, or System Monitor to determine whether the disk subsystem of a server is performing acceptably. When used in combination with the Storage Reports feature of File
Server Resource Manager (discussed in Chapter 20), the following counters present a good summary of the health of a server’s storage subsystem:

**Note** Windows Server 2003 and Windows XP enable disk counters permanently. To enable disk counters for Windows 2000 or Windows NT, use the Diskperf command. (Type `Diskperf -?` at a command prompt for additional information.)

- **Physical Disk\ Current Disk Queue Length (all instances)** Displays the number of requests waiting for disk access. This number should remain steady at no more than 1.5 to 2 times the number of spindles that make up the disk subsystem. Most disks have one spindle; redundant array of independent disks (RAID) devices have two or more spindles.

- **Physical Disk\ % Disk Time** Displays the percentage of time that a drive is active. If the value of this counter rises to more than 90 percent, check the Physical Disk\ Current Disk Queue Length (all instances) counter to see how many disk requests are queued for disk access. RAID devices can cause the Physical Disk\ % Disk Time value to exceed 100 percent and thus give an incorrect reading.

- **Physical Disk\ Avg. Disk Sec/Transfer** Displays the amount of time a disk takes to fulfill a request. A high value might indicate that the disk controller is continually trying to access the disk because of failures. For most systems, a value of 0.3 seconds or higher indicates a high average time for disk transfers.

- **Physical Disk\ Avg. Disk Bytes/Transfer** Displays the average number of bytes transferred from or to a disk during read or write operations. A value less than 15 KB under load might indicate that an application is accessing the disk drive inefficiently or that the drive is fragmented.

- **Physical Disk\ Disk Transfers/Sec** Displays the number of bytes transferred to and from the storage subsystem. If these counters indicate that actual usage is near the minimum sustained transfer rate of the physical disks, reduce the server’s workload or upgrade to a RAID subsystem.

**Monitoring Network Activity**

There are two primary reasons to monitor network activity: to troubleshoot network issues such as authentication, or to observe network performance. To troubleshoot network issues, use Network Monitor, as discussed in the “Using Network Monitor” section of this chapter. To observe basic network performance, monitor the following counters using Server Performance Advisor, Performance Logs And Alerts, or System Monitor. Abnormal network counter values usually indicate a problem or shortcoming of the
server’s processor, memory, or storage subsystems, though they can occasionally be due to a saturated network segment or interface, a broadcast storm or a failed network card.

- **Server\ Bytes Total/Sec**  Displays the number of bytes the Server service has sent to and received from the network. This value is helpful in providing an indication of how busy the server is. Segment the network if the sum of the Bytes Total/Sec for all servers is close to the maximum transfer rate of the network.

- **Server\ Work Item Shortages**  Displays the number of times no work items are available to service incoming requests. Consider tuning `InitWorkItems` or `MaxWorkItems` in the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer` if the value of the Server\ Work Item Shortages counter reaches or exceeds the threshold of 3.

- **Server\ Server Sessions and Server\ Logon/sec**  Displays the number of connections to the Server service and the number of logons per second. A high number of sessions or logons can indicate a busy (and perhaps overloaded) server. Use Network Monitor to pinpoint traffic from individual computers.

### Using Event Viewer

Event Viewer is both a service and a Microsoft Management Console (MMC) snap-in that tracks and displays events recorded in the application, security, and system logs. It gathers information about software, hardware, and system problems and tracks security events. When you launch Event Viewer (`Eventvwr.msc`) from the Administrative Tools folder on the Programs menu, the Event Viewer console appears. (See Figure 35-1.)

![Event Viewer Console](image)
Event Log Files
By default, Windows Server 2003 creates three event logs. As you assign additional roles to the server, these roles might create additional logs. The default logs are:

- **Application log** Contains events logged by programs or applications. For example, a database program might log a file error in the program log. Application and program developers determine the events that programs log. All users can view this log, which is stored in the `%WINDIR%\System32\Config\AppEvent.evt` file by default.

- **Security log** Records security events such as invalid and valid logon attempts and events related to resource use, such as creating, opening, or deleting files. Only administrators can view this log, which is stored in the `%WINDIR%\System32\Config\SecEvent.evt` file by default. You can also set an auditing policy in the registry to halt the system when the security log becomes full. See Chapter 11 for information about creating an auditing policy using Group Policy.

- **System log** Contains events logged by the Windows Server 2003 system components. For example, services that fail during startup generate errors in the System log. All users can view this log, which is stored in the `%WINDIR%\System32\Config\` file by default.

Components of an Event
The two key components in the interpretation of an event are the event header and the event description. The event description is the most useful piece of information because it indicates the significance of the event.

The Event Header
Windows displays event headers in columns in the Event Viewer console, as shown in Figure 35-2 and described in the following list:

- **Type** Lists the severity of the event. Event Viewer classifies events in the application, system, and security logs using the following classifications, which are represented by symbols in the normal view:
  - **Information** Describes the successful operation of a service, driver, or application. For example, when the Event Log service starts successfully, it records an Information event.
  - **Warning** Indicates events that pose a possible future problem. For example, when Windows cannot renew its IP address, it generates a Warning event.
Error Indicates that a significant problem has occurred, such as loss of functionality or loss of data. For example, if a service such as Net Logon fails to load, it generates an Error event.

Failure Audit Lists a failed attempt to perform an audited security event. For example, if a user fails a logon attempt, Windows generates a Failure Audit event.

Success Audit Lists a successful attempt to perform an audited security event. For example, when a user logs on successfully, Windows generates a Success Audit event.

Date Indicates the date the event occurred.

Time Indicates the (local) time the event occurred.

Source Lists the software that logged the event. The software can be a program name, a component of the system, or a component of a large program, such as a driver name.

Category Shows the way the event source classifies the event; primarily used in the security log. Security audits are one type of event that Windows classifies here.

Event Lists the event number that identifies the particular event type. The name of the event type is usually contained in the first line of its associated description.

User Indicates the user name of the user for whom the event occurred. If a server process caused the event, the user name is the client ID. If impersonation is not taking place, Windows displays the primary ID. Impersonation occurs when one process takes on the security attributes of another process, and is normal. The security log entry lists both the primary and the impersonation IDs when applicable.

Computer Specifies the name of the computer on which the event took place.
The Event Description

Double-clicking a specific event in Event Viewer displays the Event Properties dialog box shown in Figure 35-3. This dialog box describes the event and usually includes a link to more information about the event on the Microsoft Help and Support Center Web site. If the description is not helpful, select noteworthy text or the Event ID, press Ctrl+C to copy the text, and then perform a Web search for more information using the text you copied.

![Figure 35-3 The Event Properties dialog box](image)

Viewing an Event Log on Another Computer

Event Viewer can display the event log for remote machines running Windows Server 2003, Windows XP, Windows 2000, or Windows NT. To view the event log for another computer, right-click Event Viewer (Local) at the top of the tree and choose Connect To Another Computer. In the Select Computer dialog box, type the name of the other computer, or click Browse to search for the desired computer.

To tune Event Viewer for a low-speed connection to the remote machine, right-click the log, choose Properties, and then select Low Speed Connection in the Properties dialog box.

**Note** For more sophisticated monitoring and analysis of a large network of computers, use Microsoft Systems Management Server (SMS), Microsoft Operations Manager (MOM), or both. Information about these products is available at [http://www.microsoft.com/smsserver](http://www.microsoft.com/smsserver) and [http://www.microsoft.com/mom](http://www.microsoft.com/mom).
Changing Event Log Settings

To change Event Log settings, right-click the log in Event Viewer, choose Properties, and then use the following list:

- To change the size of the event log, use the Maximum Log Size box to specify a new log size 4 GB in size or smaller. Before decreasing the size of the log file, clear the log of events by right-clicking the log and choosing Clear All Events.

  By default, the application, security, and system logs each have a maximum size of 16 MB in Windows Server 2003 (8 MB for Microsoft Windows XP Service Pack 1, and 512 KB for Windows XP and Windows 2000).

- To change the action Windows performs when a log file is full, choose one of the following options: Overwrite Events As Needed, Overwrite Events Older Than, or Do Not Overwrite Events. Windows overwrites events as needed by default. Logging stops if the log file is full and cannot overwrite itself.

  Note You can use Group Policy to specify log file settings. To do so, in the Group Policy Object Editor, click Computer Configuration, Windows Settings, Security Settings, and then Event Log. See Chapter 11 for coverage of Group Policy.

Archiving an Event Log

To save an event log to a file, right-click the log in Event Viewer and then choose Save Log File As. You can archive event logs in one of the following three formats:

- **Event Log** Allows you to view the log in Event Viewer. Its extension is .EVT.

- **Text (Tab delimited)** Enables you to view the data easily in any text editor or word processor. Its extension is .TXT.

- **CSV (Comma-delimited text)** Enables you to use the data in a spreadsheet or flat-file database. Its extension is .CSV.

To open an archived log file saved in the Event Log (.evt) format, right-click a log in Event Viewer, choose Open Log File, and then search for the log file in the Open dialog box.

  Note Archived logs save the event description in the following order: date, time, source, type, category, event, user, computer, description. Windows saves the entire log file sequentially by date, ignoring filtering options and sort order.
Using the Microsoft Windows Server 2003 Performance Advisor

The easiest way to monitor the performance of a single server running Windows Server 2003 is to use the Microsoft Windows Server 2003 Performance Advisor tool (Server Performance Advisor), which is available from the Microsoft Download center at [http://www.microsoft.com/downloads](http://www.microsoft.com/downloads). This program creates customizable reports that provide a summary of the overall performance of one or more servers running Windows Server 2003, with supplemental detail that simplifies further analysis and troubleshooting.

Although Server Performance Advisor can monitor multiple servers, the setup process is complex (as discussed later in this section), making it a less suitable solution for casual monitoring.

### Note

### Overview
The Server Performance Advisor uses three types of data sources to collect data: performance counters (which are also used by System Monitor), trace providers (data from Event Tracing for Windows, or ETW), and configuration settings (registry settings). The Server Performance Advisor groups these data sources into one or more “data collector groups” that gather data and prepare reports. Server Performance Advisor creates one data collector group by default, the System Overview, but you can easily add other data collector groups by server role, or create your own.

### Note
Because reports use a large amount of disk space (approximately 20 MB per 100 seconds for the System Overview), the default data collector groups monitor for short periods of 100 to 300 seconds. Schedule or run data collector groups manually during periods that represent normal, heavy, and low usage to obtain a better overall understanding of a server’s performance.

The first time you open the Server Performance Advisor, the Start Page appears. Click Quick Tour to analyze the overall system performance of the server during the next 100-second period, or click Add/Repair Data Collector Groups to add data collector groups. Choose Add/Repair Data Collector Groups from the File menu to add other data collector groups.
Click the icon on the left of the Start Page to display the Scope Tree (console tree), which is shown in Figure 35-4. The console three has the following three nodes:

- **Data Collectors And Reports**  Lists data collection groups, the data collectors for each group, and the reports generated by each group. Use this node to view reports generated by the System Overview data collection group or other data collection groups.

- **Trace Providers**  Lists trace providers that you can drag into data collection groups to add them to the data sources included in reports.

- **Performance Counters**  Lists performance counters that you can drag into data collection groups to add them to the data sources included in reports.

**Note**  You can create and view customized groups of performance counters using Server Performance Advisor. To do so, first right-click Performance Counters in the console tree (also known as the Scope Tree), choose New, and then select Counter Group. Then drag counters from the All Counters group into the counter group you created. After adding the appropriate counters, drag the counter group into the main window to display System Monitor with the selected counters.
Recording and Viewing Data

To start recording data, select the appropriate data collection group, and then click the Start System Overview button (for example) on the toolbar. Server Performance Advisor collects data for the specified period and then generates a report from the data, as shown in Figure 35-4.

To view recorded data in System Monitor, click the Show System Monitor toolbar button. Even though the data in a report is static, you can add or remove counters from the System Monitor view, or use the System Monitor view to change the timeframe and then regenerate the report by clicking the Window Report toolbar button.

To schedule a data collection group, right-click the data collection group (for example, System Overview), choose Properties, and then click the Schedule tab, shown in Figure 35-5. Use the Duration box to change how long the data collection group gathers data, and click Change to schedule the data collection.

![Figure 35-5 The Schedule tab of the System Overview Properties dialog box](image)

Monitoring Multiple Servers

Server Performance Advisor can monitor multiple servers (data servers) from a single report server running Server Performance Advisor, thereby centralizing monitoring and reporting. Unfortunately, setup is complex. This is because the System Service account under which Server Performance Advisor runs does not have sufficient permissions to run the appropriate tasks and transfer data across the network. Running the Server Performance Advisor with an account that belongs to the Domain Admins group fixes this problem, but it poses a large security risk!
The best workaround is to run Server Performance Advisor on the data servers using an account that belongs to the local Performance Log Users group. To do this and set up a central report server to monitor multiple data servers, use the following steps:

1. Install Server Performance Advisor on the report server and all data servers. To deploy Server Performance Advisor to a large number of servers, use Group Policy as described in Chapter 28.

2. Create a Global group called Server Performance Advisor Users (or another descriptive name).

3. Create a user account with a nonexpiring password, and add it to the Server Performance Advisor Users group. Limit the permissions given to the account, and deny the account dial-in rights by right-clicking the account in Active Directory Users And Computers, clicking Properties, clicking the Dial-In tab, and then selecting the Deny Access check box.

4. Add the Server Performance Advisor Users group to the Performance Log Users local group (or built-in group on domain controllers) on all data servers and the report server that generates reports.

5. Share the \PerfLogs\Transfer folder on the report server, or create a suitable DFS folder. (See Chapter 20 for information about the Distributed File System.)

6. Set the Share permissions on the \Transfer share to give the Everyone group Full Control permissions, and set the NTFS permissions on the folder to give Write permissions to the group or groups to which all data server computers belong, as well as the Server Performance Advisor Users group or the built-in Performance Log Users group.

7. Schedule the appropriate data collection group on each data server as described in the “Recording and Viewing Data” section of this chapter.

8. Open the Readme.txt file in the \Program Files\Server Performance Advisor\Data folder, and use the sample code at the end of the file to create a batch file that sets the proper permissions for the Scheduled Tasks folder and Server Performance Advisor jobs.

9. Run the batch file on each data server. For example, open a command prompt window and then type PerfLogUsersUseSPA.bat All /G to enable members of the Performance Log Users group to run all report jobs, where PerfLogUsersUseSPA.bat is the name of the batch file.

10. On the report server and each data server, right-click Local Computer in the System Performance Advisor console tree, choose Properties, and then use the Local
Computer Properties dialog box to change the Transfer folder location to the \Transfer share or DFS folder.

11. On each data server, choose Data from the Role box in the Local Computer Properties dialog box.

12. On the report server, choose either Report from the Role box in the Local Computer Properties dialog box or Both to collect data from the report server as well as the data servers.

13. Right-click the appropriate data collection group on the report server, choose Properties, and then change the Generate property to Every 10 Minutes to force System Performance Advisor to check for new data from the data servers every 10 minutes.

14. Right-click the appropriate data collection group on each data server, choose Properties, and then under Run As type the username and password of the dedicated user account you created.

**Note**: When testing this functionality, set the schedule to a couple minutes from the current time, but remember to check the starting date. If you have trouble getting it to work, try adding the user temporarily to the Domain Admins group to ascertain whether there is a problem with permissions. Refer to the Readme.txt file in the \Program Files\Server Performance Advisor\Data folder for more troubleshooting information.

---

**Using System Monitor**

System Monitor is a utility designed to track various processes on a Windows Server 2003 system in real time, using a graphical display. Use the data from System Monitor to quickly evaluate a server’s current performance. Use the Server Performance Advisor and/or Performance Logs And Alerts tools as described elsewhere in this chapter to perform long-term monitoring or create performance baselines.

When you launch the Performance (Perfmon.msc) MMC snap-in from the Administrative Tools folder, the main console (shown in Figure 35-6) appears, displaying the Pages/sec, Avg. Disk Queue Length, and % Processor Time counters.

**Note**: Save changes to the Performance console using a filename other than Perfmon.msc to avoid changing the default configuration of the performance tools on the computer.
Objects, Counters, and Instances

System Monitor uses three types of items to monitor the system: objects, counters, and instances:

- **Object** A collection of counters associated with a resource or service that generates data. Each time an object performs a function, System Monitor updates its counters. Windows comes with a range of objects corresponding to major hardware and software components; programs add other components and their corresponding objects. Here is a listing of commonly used objects:

  - **Browser** Monitors the Browser service for a domain or workgroup
  - **Cache** Monitors disk cache usage
  - **Memory** Monitors memory performance for physical and virtual memory
  - **Objects** Monitors the number of events, mutexes, processes, sections, semaphores, and threads on the computer at the time of data collection
  - **Paging File** Monitors page file usage
  - **Physical Disk** Monitors hard disks with one or more partitions
  - **Process** Monitors all processes running on a machine
  - **Processor** Monitors each processor on the system
Chapter 35  Performance Monitoring and Tuning

❑ **Server**  Monitors bytes, sessions, certain system errors, pool nonpaged usage, and pool paged usage

❑ **System**  Monitors the counters that affect all the hardware and software running on the system

❑ **Thread**  Monitors all threads running in the system

■ **Counter**  A component within an object that represents data for a specific aspect of the system or service.

■ **Instance**  A single occurrence of multiple performance objects of the same type on a machine. If a particular object has multiple instances, you can track the statistics for each instance by adding a counter for each. You can also add a counter to track all instances at once. An instance can also be an average of the last two values for a process over the period between samples.

**Adding Counters**

System Monitor can display dozens of counters at a time. To add counters, use the following steps:

1. Click Add Counters to display the Add Counters dialog box. (See Figure 35-7.)

![Figure 35-7  The Add Counters dialog box](image)

2. Select the Select Counters From Computer option, and then type the name of the server to monitor.
3. Choose an object to monitor from the Performance Object list.

4. Select the Select Counters From List option, and then choose a counter. Click Explain to obtain a description of the counter.

   If you select a counter that has multiple instances, choose All Instances to monitor all instances of the selected counter, or choose Select Instances From List to specify the instances to monitor. Be aware that the instance index number assigned to a particular instance might change over time because whenever Windows starts or stops an instance, it might give the instance a different instance number.

   

   **Note** To stop monitoring specific counters, select the name of a counter in the legend in the System Monitor details pane, and click Delete on the toolbar. To stop monitoring all counters, click New Counter Set on the toolbar.

**Matching Counters to Graph Lines**

There are two ways to determine which counter matches a line on the graph:

- Compare the color and bar thickness of each counter within the legend to the lines in the System Monitor graph.

- Double-click a line in the graph to select the corresponding counter in the legend located under the graph. If chart lines are close together, locate a position in the graph where they diverge.

   

   **Note** You can highlight a chart line by clicking the counter to highlight and then clicking the Highlight toolbar button. A black line replaces the colored data line if the background color of the chart is white or a light color; for all other background colors, the line is white. To highlight a different line double-click it. System Monitor highlights whatever line you click as long as the Highlight button is depressed.

**Modifying the Display**

You can change the way System Monitor displays information by using the System Monitor Properties dialog box. (See Figure 35-8.) To access this dialog box, click Properties on the toolbar or right-click in the details pane and choose Properties from the shortcut menu.
Figure 35-8  The System Monitor Properties dialog box

On the General tab the System Monitor Properties dialog box, you can choose to view the data in the form of a graph, histogram, or report:

- **Graph view**  Presents information in a traditional line-graph format. System Monitor displays each of the counters and instances with a different color and line thickness, as shown in Figure 35-6. This view is the default, and it offers the greatest variety of options.

- **Histogram view**  Presents information in a bar-graph format. As in graph view, System Monitor displays each of the counters and instances in a different color. You can easily track up to 100 counters using this view because System Monitor adjusts the bars to fit the display.

- **Report view**  Presents the counter data in a report list format. System Monitor lists objects in alphabetical order, as is the case for each of the chosen counters. System Monitor displays the data itself numerically. Each object displays the total percentage of processor time in use for the chosen counters. This view works well for tracking a large number of counters.

Choose which display elements to view, as described in the following list:

- **Legend**  Displays a legend at the bottom of the details pane that shows the data scale for each counter, the counter name, the instance, the parent object (if applicable), the object the counter belongs to, the computer being monitored, and the color used to draw the line for the counter. Display the legend to see the counter name associated with a data line.
Value Bar Displays a value bar at the bottom of the details pane that provides a way to display the last, average, minimum, and maximum values recorded for the selected counter. System Monitor calculates the values from the number of samples and period displayed in the graph. The value bar also displays the total elapsed time displayed in the graph, which System Monitor derives from the sampling interval.

Toolbar Displays the toolbar functions across the top of the details pane. The toolbar is the only way to do some tasks in System Monitor.

Choosing the Sampling Interval
System Monitor displays 100 samples onscreen at a time and uses a default sampling interval of one second, yielding 100 seconds (one minute and 40 seconds) of samples by default. To change how frequently System Monitor samples data, use the Sample Automatically Every \( n \) Seconds box on the General tab of the System Monitor Properties dialog box. To view longer periods and decrease the load placed on the server by System Monitor, increase the sampling interval.

Changing Grid Lines and Graph Scales
To enable vertical or horizontal grid lines or adjust the scale of the graph or histogram, use the following list:

- To add vertical and horizontal grid lines to the graph and histogram views, click the Graph tab of the System Monitor Properties dialog box, and then select the Vertical Grid and/or Horizontal Grid checkboxes.

- To change the maximum and minimum vertical scale values of the graph, use the Maximum and Minimum boxes on the Graph tab. The defaults are 100 for the maximum value and 0 for the minimum value. The highest value you can specify is 999999999, and the lowest value is 0. Both of these values must be a positive integer. To determine the vertical scale range, look at the range of values generated by the counters you are monitoring.

- To adjust the counter scale settings for a specific counter, click the Data tab, select the counter, and then use the Scale box. Counter scale values can range exponentially from 0.0000001 to 1000000.0. Adjusting the scale does not affect the statistics displayed in the value bar.

Performance Logs and Alerts
Performance Logs And Alerts is a useful tool for monitoring one or more servers over a long period. It can record counter logs and trace logs, as well as generate alerts when counters go over or under the values you specify. You can import the log files into spreadsheets or
databases for analysis and report generation or into System Monitor for viewing. Performance Logs and Alerts runs as a service, obviating the need for a logged-on user.

There are two types of data that Performance Logs And Alerts can collect: counter logs and trace logs, as discussed in the following list:

- **Counter logs** Collects data from the specified object at a predefined interval. Counter logs are helpful for recording data about system services activities and hardware usage. You can log data on demand or schedule logging to start and stop automatically. The system can also perform continuous logging, depending on the file size and duration limits. You can view logged data through the System Monitor display or export it to spreadsheets or databases.

  
  **Note** To view data from a counter log in real-time, save the log settings as an HTML page, as discussed in the “Saving Log and Alert File Settings” section of this chapter. The resulting page hosts the System Monitor ActiveX control that displays the counter data in real-time.

- **Trace Logs** Monitors data continuously and waits for specific events, such as page faults, to occur. Trace logs record data into a trace log file. To interpret a trace log file, use a parsing tool.

  **Note** A parsing tool is software that reads the raw data and puts it into a form you can understand. Developers can create parsing tools by using the APIs provided at Microsoft’s MSDN Online Library site at [http://msdn.microsoft.com/library/default.asp](http://msdn.microsoft.com/library/default.asp) or by using Log Parser 2.2, which is available from the Microsoft Download Center at [http://www.microsoft.com/downloads](http://www.microsoft.com/downloads).

### Creating Counter and Trace Logs

To create a counter log or a trace log, perform the following steps:

1. Open the Performance (Perfmon.msc) MMC snap-in from the Administrative Tools folder, and then double-click Performance Logs And Alerts.

   Performance Logs And Alerts lists existing logs in the details pane. A green icon indicates a log that is running; a red icon indicates a log that is not.

   **Note** You cannot run multiple trace logs concurrently that include the same provider—attempting to run more than one generates an error message.

2. Right-click either Counter Logs or Trace Logs, and then choose New Log Settings.
3. In the New Log Settings dialog box, type a name for the log settings and then click OK.

4. Choose the objects and counters or trace log providers to monitor, as described in this list:

   - When creating a counter log, click Add Objects or Add Counters to collect data from entire objects or specific counters. (See Figure 35-9.) See the “Adding Counters” section earlier in this chapter for more information.

   - When creating a trace log, select Events Logged By System Provider and then select the appropriate system providers, or select Nonsystem Providers and then click Add to monitor trace providers not associated with the core operating system.

   **Important** Always set a maximum log file size when creating trace log files that monitor page faults or file details—these providers generate a huge amount of data.

5. When creating a counter log, use the Interval box to specify the sampling interval. For guidelines about setting sampling intervals, see “Determining How Often to Monitor” earlier in this chapter.
6. Click the Log Files tab, choose a log file type (as described in the “Understanding Log File Parameters” sidebar), and specify the ending to use for log file names. (See Figure 35-10.)

**Important** To store the log file in a folder other than the PerfLogs folder on the system partition, or to limit the size of a log file, click Configure on the Log Files tab. Use the When The Log File Is Full option on the Schedule tab to run a command when the log file reaches its limit.

![File Services dialog box](image)

Figure 35-10 The Log Files tab of a counter log’s Properties dialog box

7. Click the Schedule tab, and set the appropriate schedule for the log file.

**Understanding Log File Parameters**

The Log Files tab (shown in Figure 35-10) of a counter or trace log allows you to set a number of file parameters, such as the file type and whether to end the filename with a set of sequential numbers or a date.

For a counter log, choose from the following five file types:

- **Text File—Comma Delimited** Stores data in a comma-delimited text file that uses the file extension .CSV. Use this format to export data to a spreadsheet program.
Text File—Tab Delimited Stores data in a tab-delimited text file that uses the file extension .TSV. Use this format to export data to a spreadsheet program or to view the data in a text editor.

Binary File Stores data in a sequential binary file that uses the file extension .BLG. Use this format, which is the default format for counter logs, for intermittent instances (instances that stop and start after the log) and for later viewing in System Monitor.

Binary Circular File Stores data in a binary file that overwrites the oldest records with the newest and that uses the file extension .BLG. Use this format to record data continuously to the same log file for later viewing in System Monitor.

SQL Database Stores data in a SQL database. Use this format with networks that maintain a centralized SQL database for logs.

For a trace log, choose from the following two file types:

Circular Trace File Stores data in a binary file that overwrites the oldest records with the newest and that uses the file extension .ETL. Use this format to record data continuously to the same log file.

Sequential Trace File Stores data in a sequential binary file that uses the file extension .ETL. Use this format, which is the default format for trace logs, to collect data until the trace file reaches the user-defined limit. When the file reaches the limit, Performance Logs And Alerts closes the current file and starts a new one.

Saving Log and Alert File Settings
To save the settings for a log or an alert file, right-click the name of the log or alert file in the details pane, and then choose Save Settings As. Use the Save As dialog box to save the settings as an HTML file.

To use the saved settings for a new log or alert, right-click Counter Logs, Trace Logs or Alerts in the details pane, choose New Log Settings From, and then select the HTML that file contains the settings to use.

Note You can open settings files for counter logs or alerts in Internet Explorer to view the counter data in a System Monitor ActiveX control.

Using Alerts
Use the alerts feature of Performance Logs and Alerts to log entries in the application event log, start performance logs, send network messages, or run custom commands when counters fall below or rise above values you specify.
To create an alert, follow these steps:

1. Open the Performance (Perfmon.msc) MMC snap-in from the Administrative Tools folder and then double-click Performance Logs And Alerts.
   
   Performance Logs And Alerts lists existing alerts in the details pane. A green icon indicates an alert that is running; a red icon indicates an alert that is not.

2. Right-click Alerts and choose New Alert Settings.

3. In the New Log Settings dialog box, type a name for the log settings and then click OK.

4. Click Add and then use the Add Counters dialog box to select a counter to monitor. See the “Adding Counters” section earlier in this chapter for more information.

5. Use the Alert When The Value Is and Limit boxes shown in Figure 35-11 to specify when to trigger an alert. Use System Monitor, Performance Logs And Alerts, or the Server Performance Advisor to determine an appropriate value.

![Figure 35-11 The Properties dialog box for an alert](image)

**Note** To create or modify a log or alert, you must have Full Control permission for the registry entry KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SysmonLog\LogQueries. Members of the local Administrators group have this permission by default.
6. Use the Interval box to specify the sampling interval. For guidelines about setting sampling intervals, see the “Determining How Often to Monitor” section earlier in this chapter.

7. Click the Action tab and then specify what actions to perform when the counter exceeds the specified threshold, as described in the following list:

   - **Log An Entry In The Application Event Log**  Logs an entry in the application event log of Event Viewer
   - **Send A Network Message To**  Sends an alert message to the specified computer using the Messenger service (if the service is not disabled on the target computer)
   - **Start Performance Data Log**  Runs an existing counter or trace log
   - **Run This Program**  Specifies a command file and command-line arguments to run when an alert occurs

8. Click the Schedule tab, and specify when to make the alert active.

---

**Note**  The Send A Network Message To option on the Action tab relies on the Messenger service, which is disabled by default on Windows Server 2003 and Windows Server XP Service Pack 2 to improve security by reducing the attack surface.

---

**Using Network Monitor**

Network Monitor is a packet-sniffer included with Microsoft Windows Server 2003 that captures and displays frames received from the network. It provides a way to examine at a low-level data traversing the network, and it’s invaluable for troubleshooting network issues such as authentication or connection problems.

Network Monitor consists of two components that you must install using the Windows Components Wizard or Sysocmgr.exe: Network Monitor, and the Network Monitor driver. The Network Monitor driver enables Network Monitor to receive frames from the network adapter and is compatible with Windows Server 2003, Windows XP, or Windows 2000.

---

**Note**  The Systems Management Server (SMS) version of Network Monitor adds a number of features, including the ability to put the network adapter in promiscuous mode. Promiscuous mode allows the adapter to read all the frames (packets) it receives over the network, instead of only packets addressed to the server. This mode does not work unless the network uses a hub or a switch with port mirroring activated.
About Network Frames

A frame is a portion of information from the network data stream that networking software has divided into smaller pieces and sent onto the network. Network Monitor makes it possible to capture these frames and display, filter, save, or print the captured frames to help identify network traffic patterns and network problems.

A frame contains the following data:

- The source MAC address of the machine that sent the frame
- The destination MAC address of the machine that received the frame
- The header information for the protocol that sent the frame
- The actual data sent to the destination computer

To isolate a specific subset of frames, design a capture filter or create a capture trigger that starts a capture when Network Monitor locates a frame that matches the criteria you specify, as discussed later in this section.

Capturing Frames

To capture frames from the network, use the following steps:

1. Open Network Monitor from the Administrative Tools folder using an account with local Administrator permissions.
2. Click OK and then select the network to monitor in the Select A Network dialog box, as shown in Figure 35-12, and then click OK again. If this dialog box does not appear, choose Networks from the Capture menu to open it.
3. Click Start Capture on the toolbar of the Capture window to begin capturing frames.
For more information about the Capture window, see the “Viewing the Capture Window” section of this chapter.

4. To halt the data capture temporarily, choose Pause from the Capture menu. To stop capturing data, click Stop And View Capture on the toolbar.

**Note**  Network Monitor displays network statistics while capturing all network packets to a temporary 1 MB capture file with the .CAP extension located in a subfolder of the \Documents and Settings\User\Local Settings\Temp folder. To change the amount of data Network Monitor captures, see the “Modifying the Capture Buffer” section of this chapter.

**Viewing the Capture Window**

Network Monitor displays the Capture window when you open Network Monitor and during a capture. After a capture, use the Window menu to switch between the Capture window and the Frame Viewer window.

The Capture window has four panes that display frame statistics, as discussed in the following list and shown in Figure 35-13:

- The graph pane (the upper leftmost pane in Figure 35-13) graphically displays the total capture statistics of current network activity.
- The session statistics pane (the middle left pane in the figure) displays statistics for current individual network sessions. Network Monitor identifies both participants
in a session and the amount of information passed between them in either direction. Network Monitor displays only the first 128 unique addresses, so use a capture filter to identify a specific workstation on a busy network segment.

- The station statistics pane (the bottom pane in the figure) displays statistics about activities that occur from or to the local machine running Network Monitor. As with the session statistics pane, Network Monitor displays only the first 128 unique addresses.

- The total statistics pane (the rightmost pane in the figure) summarizes statistics about overall network activity detected by Network Monitor from the time the current capture process began. The total statistics pane consists of five panels:

  - **Network Statistics** displays statistics about the total amount of traffic that has occurred since the current capture on Network Monitor began. The status is always Normal on an Ethernet network and reflects the status of the ring on a token ring network.

  - **Captured Statistics** displays statistics regarding the current capture that is running.

  - **Per Second Statistics** displays averages of current activity. All frames, even those excluded by a filter, are included in these statistics.

  - **Network Card (MAC) Statistics** reflects the average activity detected by the network adapter from the time the current capture session began.

  - **Network Card (MAC) Error Statistics** displays network adapter card errors that have occurred from the time the current capture session began.

**Note** Not all network adapter cards support all statistics—if the network adapter card does not support a statistic, Network Monitor replaces the label for a statistic with the word “Unsupported”.

Note Network Monitor displays the session statistics for only the first 100 unique network sessions. To view information for the next 100 unique network sessions, you must choose Clear Statistics from the Capture menu.

**Viewing the Frame Viewer Window**

Network Monitor displays captured frames in the Frame Viewer window (shown in Figure 35-14), which appears after you click Stop And View Capture. To return to the Capture window, select the appropriate capture from the Window menu.
The Frame Viewer window has three panes, which you can toggle using the toolbar buttons:

- **The Summary pane** displays general information about the captured frames in the order in which Network Monitor captured them.
- **The Detail pane** displays the frames’ contents, including the protocols used to send them.
- **The Hex pane** displays the ASCII and hexadecimal representation of the captured data.

Double-click a frame to display the Detail and Hex panes for that frame; double-click the frame again to hide the detail and hex panes. If double-clicking a frame does not display a pane, select Zoom Pane and all windows from the Window menu.

**Note** To change the Time column to display the actual time instead of the time elapsed, choose Options from the Display menu and then choose Time Of Day in the Display Options dialog box.

### Configuring and Customizing Network Monitor

This section describes how to expand the capture buffer to capture more data, edit the address database, add comments to a capture, or print captured frames.

#### Modifying the Capture Buffer

By default, Network Monitor captures a maximum of 1 MB of data in its capture buffer (a binary file with the .CAP extension saved in the Windows Temp folder). When the buffer is full, Network Monitor overwrites the oldest data with the newest.
To adjust the size of the capture buffer in Network Monitor, choose Buffer Settings from the Capture menu and then use the Capture Buffer Settings dialog box to adjust the Buffer Size (MB) or Frame Size (Bytes) options. Network Monitor supports capturing and displaying up to 1 GB of data at a time.

**Editing the Address Database**

To make the Frame Viewer window easier to understand, you can replace IP addresses with computer names. To do so, choose Find All Names from the Display menu in the Frame Viewer window. Alternatively, you can right-click an IP address in the Frame Viewer window, choose Edit Address, and then use the Nslookup command at a command prompt to resolve the computer name for the appropriate IP address (provided that the network has a reverse lookup zone and that the host in question has a PTR record in the zone), and then type the host name in the Address Information dialog box. To save this name in Network Monitor's local address database, select the Permanent Name checkbox.

To display the address database (shown in Figure 35-15), choose Addresses from the Display menu of the Frame Viewer window. Click Save to export the database to a file, or click Load to import a previously saved address database.

![Figure 35-15  The Address Database dialog box](image)

**Adding a Comment Frame to a Capture**

A comment frame is a helpful tool you can use to add comments or other information to a capture file within the Frame Viewer. For example, use comment frames to mark the beginning and ending points for a group of authentication frames.

To add a comment frame, choose Insert Comment Frame from the Tools menu or right-click the Frame column at the point to insert the comment frame and choose Insert
Comment from the shortcut menu. The Insert Comment Frame dialog box appears. (See Figure 35-16.) The options in this dialog box are as follows:

- **Frame Number** The frame position where Network Monitor places the comment frame within the capture. Network Monitor lists the selected frame by default.

- **Type Of Frame To Insert** The Comment or Bookmark protocol parser used to process the comment frame. The default parser is Comment.

- **No Statistics** Disables statistical generation for the comment frame.

- **Apply Current Filter To Statistics** Calculates statistics using the current display filter.

- **Enter In A Comment For This New Frame** Specifies the comment text to attach to the frame.

![The Insert Comment Frame dialog box](image)

**Figure 35-16** The Insert Comment Frame dialog box

**Printing Captured Frames**

To print captured frames, choose Print from the File menu in the Frame Viewer window. Select the desired output options on the Netmon tab in the Print dialog box. The Output Detail area enables you to specify the amount of detail to print for each of the frames. You can also set filters and add page breaks to the output.

**Designing a Capture Filter**

Network Monitor uses a capture filter to determine what frames to capture, and it ignores frames that do not match the filter. This can reduce the amount of captured data and make it easier to locate relevant frames.

To design a capture filter, stop any captures, choose Filter from the Capture menu of the Capture window, and then use the Capture Filter dialog box shown in Figure 35-17 to design the capture filter, as described in this section.
Specifying Capture Filter Protocols
Filter protocols capture frames sent using a specific protocol. To design filter protocols, double-click the default line SAP/ETYPE = Any SAP Or Any ETYPE in the decision tree of the Capture Filter dialog box shown in Figure 35-17. In the Capture Filter SAPs And ETYPES dialog box (shown in Figure 35-18), select the protocols to omit from the capture and then click Disable. The default is to enable all the protocols.

![Figure 35-17 The Capture Filter dialog box](image)

![Figure 35-18 The Capture Filter SAPs And ETYPES dialog box](image)
Specifying Address Pairs

Address pairs capture or exclude traffic between the computer running Network Monitor and up to three other computers.

To designate address pairs, double-click the AND (Address Pairs) line in the decision tree shown in Figure 35-17, and then specify address pair properties in the Address Expression dialog box shown in Figure 35-19 and described in the following list:

1. Choose Include or Exclude to include or exclude data that travels between the members of the address pair.

2. Choose the first address from the Station 1 list and the second address from the Station 2 list.

3. Choose one of the three arrows from the Direction list to indicate the direction of the traffic to filter between the two addresses:
   - <>: This arrow specifies frames that travel in either direction between the Station 1 and Station 2 computers. This arrow is the default.
   - -->: This arrow specifies frames that travel from Station 1 to Station 2.
   - <--: This arrow specifies frames that travel from Station 2 to Station 1.

4. Optionally, modify the existing address database by clicking Edit Addresses and then adding, editing, or deleting information.

Note Broadcast and Multicast are always destination addresses.
Defining Pattern Matches

To capture frames that consist of a specific pattern at a specified offset, create pattern matches. You can create up to four pattern matches by double-clicking the AND (Pattern Matches) line in the decision tree, and then using the Pattern Match dialog box.

Type the hexadecimal or ASCII data pattern present in the frames to capture. Then, in the Offset box, type the hexadecimal number that specifies the byte where the pattern begins. Network Monitor interprets the offset number depending on whether you specify the From Start Of Frame option or the From End Of Topology Header option.

To find a pattern to use in a pattern match filter, use the following steps:

1. Perform a capture, and open the capture in the Frame Viewer.
2. Double-click a frame to display the Details And Hex pane.
3. Select a portion of the frame in the Detail pane to obtain its pattern and offset. For example, select the SMB: NT status code = 0x0 text, as shown in Figure 35-20.

![Figure 35-20 The Frame Viewer window](image)

4. Write down the highlighted text in the left part of the Hex pane (this is the pattern) and the text in parentheses listed in the Off: section of the Status bar. (This is the offset from the beginning of the frame.) For example, Figure 35-20 shows the pattern 00 00 00 00 with an offset of x3F.
5. Remove any spaces from the pattern, type it in the Pattern box, and then select Hex, as shown in Figure 35-21.
6. Remove the leading “x” from the offset, type it in the Offset box and then select From Start Of Frame.
Designing a Display Filter

By default, Network Monitor displays all captured frames in the Frame Viewer, which can make it difficult to locate specific frames. To make it easier to locate frames of interest, create a display filter that tells Network Monitor to display only the frames that are of interest to you.

To create a display filter, perform a capture, choose Filter from the Capture menu of the Capture window, and then use the Capture Filter dialog box shown in Figure 35-22 to design the capture filter, as described in this section.
There are two default branches on the decision tree, each with a single expression: the Protocol branch, which lists the protocols to display, and the Address Pairs branch, which lists the computer address pairs to display.

To add operators, use the AND, OR, and NOT buttons; to change an existing operator, select it and then click Change Operator. To create a new expression or edit an existing expression, click Expression or select an existing expression and then click Edit Expression. Use the Expression dialog box that appears to create or edit an expression.

The Expression dialog box contains three tabs, as discussed below and shown in Figure 35-23.

![Figure 35-23  The Expression dialog box](image)

- **Address tab** Specifies address pairs to display. Refer to “Specifying Address Pairs” earlier in this chapter for information about how to design address pairs.

  **Note** Broadcast and multicast frames come from a single system and are never a source; choosing either of these for Station 1 filters out all frames.

- **Protocol tab** Specifies protocols to display in the Frame Viewer. Choose protocols by selecting protocols and then clicking the Disable, Enable, Disable All, or Enable All buttons. Network Monitor enables all protocols by default.

- **Property tab** Specifies protocol properties to find. Follow these steps to design protocol properties:

  - Choose the properties from the Protocol:Property list. If a plus sign appears next to a protocol name, you can expand the protocol to choose a property from its list.
Choose a relational operator from the Relation list. Use a relational operator to specify the connection between the protocol property and its possible values.

Type the value to use as a comparison to the selected property in the Value (Address) box.

**Setting a Capture Trigger**

Use a capture trigger to set conditions that initiate an action such as stopping data capture and executing a program or command. To set a capture trigger, follow these steps:

1. Choose Trigger from the Capture menu of the Capture window. The Capture Trigger dialog box appears, as shown in Figure 35-24.

2. Choose from the options in the Trigger On area:
   - **Pattern Match** Performs the trigger action when the specified hexadecimal or ASCII pattern match occurs.
   - **Buffer Space** Performs the trigger action when the capture fills the specified percentage of the capture buffer.
   - **Pattern Match Then Buffer Space** Monitors the capture for the specified data pattern, and then performs the trigger action when the capture fills the specified percentage of the capture buffer.
Buffer Space Then Pattern Match  Monitors the capture buffer until the capture fills the specified percentage of the capture buffer, after which point Network Monitor monitors for the specified pattern. When the pattern match occurs, Network Monitor performs the trigger action.

Note  If you choose the Pattern Match Then Buffer Space option and set Buffer Space to 100 percent, Network Monitor overwrites the frame that has the data pattern match because Network Monitor does not start counting the buffer space until after it finds the pattern match.

3. In the Trigger Action area, choose the action to perform when the trigger criteria are met:
   - Audible Signal Only  Beeps and continues to capture frames. This is the default option.
   - Stop Capture  Ends the capture process.
   - Execute Command Line  Executes a command line or opens a file. The command can be up to 259 characters.

Memory and Network Tuning
Windows Server 2003 is configured optimally for most workloads by default. If the default behavior is not appropriate for your environment, you can improve performance by choosing the appropriate file system cache settings, optimizing the page file, and tuning network performance, as described in this section.

Changing File System Cache Settings
Windows Server 2003 favors the file system cache over running programs and processes by default, which is appropriate for file servers. However, the default settings can reduce the performance of database servers or other network applications. To change the way Windows Server 2003 allocates memory, use the following steps:

1. Click Start, choose Control Panel and then Network Connections, and then right-click the internal network connection and choose Properties.
2. Select File And Printer Sharing For Microsoft Networks and then click Properties.
3. Select the memory optimization method for the server to use and then click OK, as described here and shown in Figure 35-25:
   - Minimize Memory Used  This setting uses the least amount of RAM for caching. Use it only when the server has a small amount of RAM.
❑ **Balance**  Balances the available RAM between the system cache and applications, and is inappropriate for servers with an adequate amount of RAM.

❑ **Maximize Data Throughput For File Sharing**  This is the default setting and is appropriate for most servers, especially those that act as file or print servers or have a large amount of memory. Also use this setting if the server is running a network application and memory is not a bottleneck, and the application does not have its own memory manager. The Maximize Data Throughput For File Sharing setting allocates the largest amount of RAM for the system cache (up to 960 MB), maximizing file-sharing performance but reducing the amount of available RAM for other programs.

❑ **Maximize Data Throughput For Network Applications**  Allocates a smaller amount of RAM for the system cache (up to 512 MB), making as much RAM available for server-based applications as possible while still ensuring good performance for clients. Use this setting for servers that run network applications that include their own memory managers, such as Microsoft SQL Server or Microsoft Exchange Server, and for servers that run network applications that require large amounts of free memory such as Internet Information Services (IIS).

---

**Figure 35-25** Optimizing memory usage for File and Printer Sharing

---

**Note**  File and Printer Sharing optimization settings are not available on Windows Server 2003, Web Edition.
Under the Hood  The LargeSystemCache Registry Value

The memory optimization settings for File and Printer Sharing control two registry keys—the LargeSystemCache value of the HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management key and the Size value of the HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters key. The LargeSystemCache value controls the maximum size of the file-system cache (512 MB when set to 0, or 960 MB when set to 1). Table 35-1 shows the values of these keys.

<table>
<thead>
<tr>
<th>Setting</th>
<th>LargeSystemCache Value</th>
<th>Size Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimize Memory Used</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Balance</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Maximize Data Throughput For File Sharing</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Maximize Data Throughput For Network Applications</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

Optimizing the Page File

There are a number of ways to optimize the Windows page file, and even more opinions about the best way to do so. Use the Advanced tab of the System tool in Control Panel and the following guidelines to optimize the Windows page file without a lot of debate:

- Remove any current page files on the partition, and defragment the partition before creating the page file to ensure that Windows allocates the page a contiguous area on the hard drive.

- Create a page file on the system (most likely C:\) partition with the initial size and maximum size set to slightly larger than the size of the crash dump file. To change the type of crash dump file the system creates in the event of a Stop Error (blue screen), click Settings in the Startup And Recovery section of the Advanced tab in the System Properties dialog box.

- In addition to the page file on the system partition, create a page file on a dedicated disk, RAID-0, RAID 0+1, or RAID-1 array. If this is impractical, allocate space for the page file on the fastest drive or drives in the system. Placing it on multiple physical drives improves performance, unless the drives are slow or heavily used (avoid these). Placing page files on multiple partitions on the same drive does not improve performance.
Avoid RAID-5 volumes when possible because the data redundancy can reduce performance. Choose a simple volume, stripe set, mirror, or RAID 0+1 volume (a mirrored stripe set) for the page file.

If you must place the page file on the same physical disk as the operating system, place it on the same partition as the operating system to minimize disk seek time and maximize disk performance.

Use the Committed Bytes counter in Performance Monitor to determine how much virtual memory Windows consumes under the heaviest usage conditions. Set the initial size of the page file to a value significantly larger than the peak usage to allow for future growth or unusual conditions. This reduces page file fragmentation by reserving a block on the hard drive for the page file and eliminating the need to dynamically increase the file size.

Set the maximum size to the maximum size you can imagine ever needing. This provides Windows the ability to increase the size of the page file in an emergency rather than deny memory requests.

**Tuning Network Performance**

To optimize network performance, use the following list:

- Unbind infrequently used protocols.
- Set the order in which the workstation and NetBIOS software bind to each protocol when using more than one protocol. Average connection time decreases when you list the most frequently used protocol first.
- Ensure that users and resources are located on the same subnet when possible.
- Install multiple network adapters to increase file-sharing throughput.
- Upgrade network adapters on heavily loaded servers to high-performance adapters designed for server loads.

**Summary**

Windows Server 2003 is equipped with tools for monitoring servers and the network, finding problems, and fine-tuning performance. Although some of the processes might appear daunting, you can approach performance monitoring gradually and increase monitoring as you become comfortable with the tools and methods. The next chapter discusses how to prepare and implement a plan for recovering from the inevitable failure of hardware.
Chapter 36

Disaster Planning

Planning for Disaster ................................................................. 1203
Preparing for a Disaster............................................................. 1211
Summary .................................................................................. 1220

Smart bicycle riders wear helmets even though they ride carefully and certainly don’t plan a headfirst landing. Schools and businesses have fire drills even though the vast majority of buildings never burn down. Similarly, system administrators sincerely hope they will never need their verified backups and Automated System Recovery disks. Nevertheless, we keep them because there are only two types of networks: those that have experienced disaster and those that haven’t. Yet.

Disaster can take many forms, from the self-inflicted pain of a user or administrator doing something really, really unwise to the uncontrollable, unpreventable results of a natural disaster such as a flood or earthquake. In any case, your competence as a system administrator will be judged by how well you were prepared for the disaster and how well you and your team responded to it and recovered from it.

This chapter covers emergency preparedness. It discusses creating a disaster recovery plan, with standardized procedures to follow in the event of a catastrophe. It also describes how to prepare for a disaster, including how to make an Automated System Recovery disk, how to make a boot disk, how to install the Recovery Console, how to specify recovery options in Windows Server 2003, and how to create an external recovery drive.

Planning for Disaster

Some people seem to operate on the assumption that if they don’t think about a disaster, one won’t happen. This is similar to the idea that if you don’t write a will, you’ll never die—and just about as realistic. No system administrators should feel comfortable about their network’s degree of preparedness without a clear disaster recovery plan that has been thoroughly tested. That plan should only be your starting point, however. A good disaster recovery plan is one you are constantly examining, improving, updating, and
testing. But understand your disaster plan’s limitations: it isn’t perfect, and even the best disaster recovery plan needs to be constantly examined and adjusted or it quickly gets out of date.

Planning for disaster or emergencies is not a single step, but an iterative, ongoing process. Systems are not mountains, but rivers, constantly moving and changing, and your disaster recovery plan needs to change as your environment changes. To put together a good disaster recovery plan, one you can bet your business on, you need to follow these steps:

1. Identify the risks.
2. Identify the resources.
3. Develop the responses.
4. Test the responses.
5. Iterate.

**Identifying the Risks**

The first step in creating a disaster recovery plan is to identify the risks to your business and the costs associated with those risks. The risks vary from the simple deletion of a critical file to the total destruction of your place of business and its computers. To properly prepare for a disaster, you need to perform a realistic assessment of the risks, the potential costs and consequences of each disaster scenario, the likelihood of any given disaster scenario, and the resources available to address the risks. Risks that seemed vanishingly remote a few years ago are now part of our everyday life.

Identifying risks is not a job for a single person. As with all the tasks associated with a disaster recovery plan, all concerned parties must participate. There are two important reasons for this: you want to make sure that you have commitment and buy-in from the parties concerned, and you also want to make sure you don’t miss anything important.

No matter how carefully and thoroughly you try to identify the risks, you’ll miss at least one. You should always account for that missing risk by including an “unknown risk” item in your list. Treat it just like any other risk: identify the resources available to address it, and develop countermeasures to take should it occur. The difference with this risk, of course, is that your resources and countermeasures are somewhat more generic, and you can’t really test your response to the risk, because you don’t yet know what it is.

Start by trying to list all the possible ways your system could fail. If you have a team of people responsible for supporting the network, solicit everyone’s help in the process. The more people involved in the brainstorming, the more ideas you’ll get and the more prevention and recovery procedures you can develop and practice.
Next, look at all the ways some external event could affect your system. The team of people responsible for identifying possible external problems is probably similar to a team looking at internal failures, but with some important differences. In a large industrial plant, for example, when you start to look at external failures and disasters, you’ll want to involve the security and facilities groups, because they will need to understand your needs as well as provide input on how well the plant is protected from these disasters.

The risk identification phase is really made up of two parts—identification and assessment. They are different tasks. During the identify portion of the phase, you need to identify every possible risk, no matter how remote or unlikely. No risk suggested should be regarded as silly—don’t limit the suggestions in any way. You want to identify every possible risk that anyone can think of. Then, when you have as complete a list as you can create, move on to the assessment task. In the risk assessment task, you will try to understand and quantify just how likely a particular risk is. If you’re located on a flood plain, for example, you’re much more likely to think flood insurance is a good investment.

**Identifying the Resources**

Once you’ve identified the risks to your network, you need to identify what the resources are to address those risks. These resources can be internal or external, people or systems, hardware or software.

When you’re identifying the resources available to deal with a specific risk, be as complete as you can, but also be specific. Identifying everyone in the IT group as a resource to solve a crashed server might look good, but realistically only one or two key people are likely to actually rebuild the server. Make sure you identify those key people for each risk, as well as the more general secondary resources they have to call on. So, for example, the primary resources available to recover a crashed Microsoft Exchange server might consist of one or two staff members who can recover the failed hardware and another one or two staff members who can restore the software and database. General secondary resources would include everyone in the IT group as well as the hardware vendor and Microsoft Premier Support.

An important step in identifying resources in your disaster recovery plan is to specify both the first-line responsibility and the back-end or supervisory responsibility. Make sure everyone knows who to go to when the problem is more than they can handle or when they need additional resources. Also, clearly define when they should do that. The best disaster recovery plans include clear, unambiguous escalation policies. This takes the burden off individuals to decide when and who to notify and makes it simply part of the procedure.
Developing the Responses

An old but relevant adage comes to mind when discussing disaster recovery scenarios: when you’re up to your elbows in alligators, it’s difficult to remember that your original objective was to drain the swamp. This is another way of saying that people lose track of what’s important when they are overloaded by too many problems that require immediate attention. To ensure that your swamp is drained and your network gets back online, you need to take those carefully researched risks and resources and develop a disaster recovery plan. There are two important parts of any good disaster recovery plan:

- Standard operating procedures (SOPs)
- Standard escalation procedures (SEPs)

Making sure these procedures are in place and clearly understood by all before a disaster strikes puts you in a far better position to recover gracefully and with a minimum of lost productivity and data.

Standard Operating Procedures

Emergencies bring out both the best and worst in people. If you’re prepared for the emergency, you can be one of those who come out smelling like a rose, but if you’re not prepared and let yourself get flustered or lose track of what you’re trying to accomplish, you can make the whole situation worse than it needs to be.

Although no one is ever as prepared for a system emergency as they’d like to be, careful planning and preparation can give you an edge in recovering expeditiously and with a minimal loss of data. It is much easier to deal with the situation calmly when you know you’ve prepared for this problem and you have a well-organized, tested standard operating procedure (SOP) to follow.

Because the very nature of emergencies is that you can’t predict exactly which one is going to strike, you need to plan and prepare for as many possibilities as you can. The time to decide how to recover from a disaster is before the disaster happens, not in the middle of it when users are screaming and bosses are standing around looking serious and concerned.

Your risk assessment phase involved identifying as many possible disaster scenarios as you could, and in your resource assessment phase you identified the resources that are available and responsible for each of those risks. Now you need to write up SOPs for recovering the system from each of the scenarios. Even the most level-headed system administrator can get flustered when the system has crashed, users are calling every 10 seconds to see what the problem is, the boss is asking every five minutes when you’ll have it fixed, and your server won’t boot. And that’s the easy case compared to the mess that can be caused by an external disaster.
Reduce your stress and prevent mistakes by planning for disasters before they occur. Practice recovering from each of your disaster scenarios. Write down each of the steps, and work through questionable or unclear areas until you can identify exactly what it takes to recover from the problem. This is like a fire drill, and you should do it for the same reasons—not because a fire is inevitable, but because fires do happen, and the statistics demonstrate irrefutably that those who have prepared for a fire and practiced what to do in a fire are far more likely to survive it.

Your job as a system administrator is to prepare for disasters and practice what to do in those disasters—not because you expect the disaster, but because if you do have one, you want to be the hero, not the goat. After all, it isn’t often that the system administrator gets to be a hero, so be ready when your time comes.

The first step in developing any SOP is to outline the overall steps you want to accomplish. Keep it general at this point—you’re looking for the big picture here. Again, you want everyone to be involved in the process. What you’re really trying to do is make sure you don’t forget any critical steps, and that’s much easier when you get the overall plan down first. There will be plenty of opportunity later to cover the specific details.

Once you have a broad, high-level outline for a given procedure, the people you identified as the actual resources during the resource assessment phase should start to flesh in the outline. You don’t need every detail at this point, but you should get down to at least a level below the original outline. This will help you identify missing resources that are important to a timely resolution of the problem. Again, don’t get too bogged down in the details at this point. You’re not actually writing the SOP, just trying to make sure that you’ve identified all its pieces.

When you feel confident that the outline is ready, get the larger group back together again. Go over the procedure and smooth out the rough edges, refining the outline and listening to make sure you haven’t missed anything critical. When everyone agrees that the outline is complete, you’re ready to add the final details to it.

The people who are responsible for each procedure should now work through all the details of the disaster recovery plan and document the steps thoroughly. They should keep in mind that the people who actually perform the recovery might not be who they expect. It’s great to have an SOP for recovering from a failed router, but if the only person who understands the procedure is the network engineer, and she’s on vacation in Bora Bora that week, your disaster recovery plan has a big hole in it.

When you create the documentation, write down everything. What seems obvious to you now, while you’re devising the procedure, will not seem at all obvious in six months or a year when you suddenly have to use it under stress.
Real World  Multiple Copies, Multiple Locations

It’s tempting to centralize your SOPs into a single, easily accessible database. You should do that, making sure everyone understands how to use it. But you’ll also want to have alternative locations and formats for your procedures. Not only do you not want to keep the only copy in a single database, you also don’t want to have only an electronic version. Always maintain hard-copy versions as well. The one thing you don’t want to do is create a single point of failure in your disaster recovery plan!

Every good server room should have a large binder, prominently visible and clearly identified, that contains all the SOPs. Each responsible person should also have one or more copies of at least the procedures he or she is either a resource for or likely to become a resource for. We like to keep copies of all our procedures in several places so that we can get at them no matter what the source of the emergency or where we happen to be when one of our pagers goes off.

Once you have created the SOPs, your job has only begun. You need to keep them up to date and make sure that they don’t become stale. It’s no good having an SOP to recover your ISDN connection to a branch office when you ripped the ISDN line out a year ago and put in a DSL line with three times the bandwidth at half the cost.

You also need to make sure that all your copies of an SOP are updated. Electronic ones should probably be stored in a replicated database. However, hard-copy documents are notoriously tricky to maintain. A good method is to make yet another SOP that details who updates what SOPs and who gets fresh copies whenever a change is made. Then put a version control system into place and make sure everyone understands his or her role in the process. Build rewards into the system for timely and consistent updating of SOPs—if 10 or 20 percent of your staff’s bonus is dependent on keeping those SOPs up to date and distributed, you can be sure they’ll be done at least as often as the review process.

Standard Escalation Procedures

No matter how carefully you’ve identified potential risks, and how detailed your procedures to recover from them, you’re still likely to have situations you didn’t anticipate. An important part of any disaster recovery plan is a standardized escalation procedure. Not only should each individual SOP have its own procedure-specific SEP, but you should also have an overall escalation procedure that covers everything you haven’t thought of—because it’s certain that you haven’t thought of everything.

An escalation procedure has two functions—resource escalation and notification escalation. Both have the same purpose: to make sure that everyone who needs to know about the problem is up to date and involved as appropriate, and to keep the overall noise level
down so that the work of resolving the problem can go forward as quickly as possible. The resource escalation procedure details the resources that are available to the people who are trying to recover from the current disaster, so that they don’t have to try to guess who (or what) the appropriate resource might be when they run into something they can’t handle or something doesn’t go as planned. This helps them stay calm and focused. They know that if they run into a problem, they aren’t on their own, and they know exactly who to call when they do need help.

The notification escalation procedure details who is to be notified of serious problems. Even more importantly, it should provide specifics regarding when notification is to be made. If your print server crashes but comes right back up, you might want to send a general message only to the users of that particular server letting them know what happened. However, if your mail server has been down for more than half an hour, a lot of folks are going to be concerned. The SEP for that mail server should detail who needs to be notified if the server is unavailable for longer than some specified time, and it should probably detail what happens and who gets notified when it’s still down some significant amount of time after that.

This notification has two purposes: to make sure that the necessary resources are made available as required, and to keep everyone informed and aware of the situation. If you let people know that you’ve had a server hardware failure and that the vendor has been called and will be on site within an hour, you’ll reduce the number of phone calls exponentially, freeing you to take the necessary steps to ensure that you’re ready when the vendor arrives.

**Testing the Responses**

A disaster recovery plan is nice to have, but it really isn’t worth a whole lot until it has actually been tested. Needless to say, the time to test the plan is at your convenience and under controlled conditions, rather than in the midst of an actual disaster. It’s a nuisance to discover that your detailed disaster recovery plan has a fatal flaw in it when you’re testing it under controlled conditions. It’s a bit more than a nuisance to discover it in a situation where every second counts.

You won’t be able to test all aspects of all disaster recovery plans. Few organizations have the resources to create fully realistic simulated natural disasters and test their response to each of them under controlled conditions. Nevertheless, there are things you can do to test your response plans. The details of how you test them depend on your environment, but they should include as realistic a test as feasible and should, as much as possible, cover all aspects of the response plan. The other reason to test the disaster recovery plan is that it provides a valuable training ground. If you’ve identified primary and backup resources, as you should, chances are that the people you’ve identified as backup resources are not as skilled or knowledgeable in a particular area as the primary resource. Testing the procedures gives you a chance to train the backup resources at the same time.
You should also consider using the testing to cross-train people who are not necessarily in the primary response group. Not only will they get valuable training, but you’ll also create a knowledgeable pool of people who might not be directly needed when the procedure has to be used for real, but who can act as key communicators with the rest of the community.

**Iterating**

When you finish a particular disaster recovery plan, you might think your job is done, but in fact your work is just beginning. Standardizing a process is actually just the first step. You also need to improve it.

You should make a regular, scheduled practice of pulling out your disaster recovery plan with your group and making sure it’s up to date. Use the occasion to evaluate how you can improve on it. Take the opportunity to examine your environment. What’s changed since you last looked at the plan? What servers have been retired, and what new ones have been added? What software is different? Are all the people on your notification and escalation lists still working at the company in the same roles? Are the phone numbers up to date?

---

**Real World  Understand and Practice Kaizen**

*Kaizen* is a Japanese word and concept that means “small, continuous, improvement.” Its literal translation is “Change (kai) to become good (zen).”

So, why bring a Japanese word and concept into a discussion about disaster recovery? Because a good disaster recovery plan is one that you are constantly Kaizening. When you really understand Kaizen, it becomes a way of life that you can use in many ways.

The first thing to understand about Kaizen is that you are *not* striving for major change or improvement. Small improvements are the goal. Don’t try to fix or change everything all at once. Instead, focus on one area, and try to make it just a little bit better.

The second part of Kaizen is that it is continuous. You must constantly look for ways to improve and implement those improvements. Because each improvement is small and incremental, you can easily implement it and move on to the next one.

Kaizen is very much about teamwork. Good Kaizen balances the load on a team and finds ways to build the strengths of the team as a whole. If you practice Kaizen and continually look for small, incremental ways to improve your work, you will soon have a better and more enjoyable place to work. As a manager, if you find ways to encourage and reward those who practice Kaizen, your team and you will grow and prosper.
Another way to iterate your disaster recovery plan is to use every disaster as a learning experience. Once the disaster or emergency is over, get everyone together as soon as possible to talk about what happened. Find out what they think worked and what didn’t in the plan. Actively solicit suggestions for how the process could be improved. Then make the changes and test them. You’ll not only improve your responsiveness to this particular type of disaster, but you’ll improve your overall responsiveness by getting people involved in the process and enabling them to be part of the solution.

Preparing for a Disaster

As Ben Franklin was known to say, “Failure to prepare is preparing to fail.” This is truer than ever with modern operating systems, and although Windows Server 2003 includes a number of exceptionally useful recovery modes and tools, you still need to prepare for potential problems. Some of these techniques are covered in detail in other chapters and are discussed here only briefly, whereas others are covered here at length.

Setting Up a Fault-Tolerant System

A fault-tolerant system is one that is prepared to continue operating in the event of key component failures. This technique is very useful for servers running critical applications. Here are a few of the many ways to ensure fault tolerance in a system:

- Use one or more RAID arrays for system and data storage, protecting you from hard disk failure. If a hard disk in the array fails, only that disk needs to be replaced—and no data is lost. See Chapter 18 for information about using Windows Server 2003 to implement software RAID.

- Use multiple SCSI adapters to provide redundancy if a SCSI controller fails.

- Use an uninterruptible power supply (UPS) to allow the server to shut down gracefully in the event of a power failure.

- Use multiple network cards to provide redundancy in case a network card fails.

- Use multiples of everything that is likely to fail, including power supplies and so on.

- Use clusters to provide redundancy and failover in the event of a server failure. See Chapter 19 for information about implementing clusters in Windows Server 2003.

More Info  For more on fault tolerance, see Chapter 38.
Back up the system and system state regularly using a good Windows Server 2003 backup program. If a hard disk fails and must be replaced and you're not using some sort of RAID array, the data and system can be restored from backup. (If you lose the system entirely, you'll need to install Windows Server 2003 on it before restoring the original system.) See Chapter 37 for details on using the Windows Server 2003 backup program.

Creating Automated System Recovery Disks

Whereas Microsoft Windows NT and Microsoft Windows 2000 created an emergency repair disk (ERD) to help rescue the system in the event of a disaster, the Windows Server 2003 family creates an Automated System Recovery (ASR) disk. The ASR disk contains important information that can be used to fix system files, the boot sector, and the startup environment. The ASR disk is easy to make, and it is very useful in the event of a disaster.

Note In Windows Server 2003, you might have noticed that you didn't get prompted to create an ERD during installation, as you do during Windows NT setup. In fact, the entire procedure has changed. Now, instead of an ERD, you run the Backup program in Windows Server 2003 to create an ASR disk and backup. To make a fresh ASR disk, you need a floppy disk that you don't mind being formatted and a fresh tape for your tape drive (or fresh Zip disk, Jaz disk, hard drive, or other supported media, for your target backup device). Always use a freshly formatted floppy disk to create an ASR disk. It's also a good idea to have a backup of your ASR disk, so always keep at least one generation back. We also like to keep an original ASR disk created immediately after the installation process as a kind of ultimate fallback position.

To make an ASR disk, follow these steps:

1. Open the Windows Server 2003 Backup program from the Start menu by pointing to Programs, Accessories, and System Tools and then choosing Backup.
2. Switch to the Advanced Mode if you get a wizard prompt.
3. Click Automated System Recovery Wizard, as shown in Figure 36-1 to open the Automated System Recovery Preparation Wizard, shown in Figure 36-2. Click Next.
4. In the Backup Destination page shown in Figure 36-3, select the backup type and destination you'll be using. Windows Server 2003 doesn’t support directly writing to CD or DVD, but you can write to any device that is supported by the Windows Backup program. Click Next.
5. Click Finish to complete the wizard. The backup starts automatically when you exit the wizard, as shown in Figure 36-4.

6. Once the backup has completed, you’ll be prompted to insert a blank floppy disk to create the ASR disk, as shown in Figure 36-5.
Chapter 36  Disaster Planning  1215

Figure 36-5  Insert a formatted, blank floppy disk for ASR to use

7. Insert a blank floppy disk in drive A, and click OK.

8. Backup writes the necessary files to the floppy disk and confirms that the process has been successful, as shown in Figure 36-6. Label the disk and the backup media used as requested, and store them in a safe place.

Figure 36-6  The Windows Backup Utility confirms the successful creation of the ASR disk

Note  The ASR disk is not bootable; it must be used in conjunction with the Windows Server 2003 installation media.

Under the Hood  Using the ASR Set Effectively

What, exactly, is on the ASR disk? Well, certainly not all the stuff that used to be there in Windows NT. Instead of trying to fit all the files necessary to recover your system onto a single floppy disk, a task that had become more than a little problematic, Windows Server 2003 now copies only the following three files to the floppy:

- **Setup.log**  Points to the location of system files on your server
- **Asr.sif**  Contains information on disk, partitions and volumes on the system, and the location of the backup media used
- **Asrnpn.sif**  Contains information on the various plug and play devices on the system
With this change, it’s easy to maintain multiple generations of repair information because each ASR disk points to a specific system backup. You should always keep the ASR disk with the specific backup that it was made with.

Whenever you make a major change to your system, it’s a good idea to make a fresh ASR set before you make the change. This gives you a fallback position if something goes wrong. If something doesn’t work right, you can quickly restore the previous configuration. Once you’ve confirmed that the new configuration is stable and working, then and only then should you update your ASR set for that server.

What constitutes a major change? Adding, removing, or otherwise modifying the hard disks or their partitions, formats, configurations, and so on is one category of major changes. Any time you make a change to the hard disk configuration, you’ll definitely want to make a fresh ASR set just before you make the change. Another major change would be the addition of a new component to the server, such as adding Microsoft Exchange Server or Microsoft SQL Server. Any changes made from Control Panel are candidates for redoing the ASR set as well.

Creating a Boot Disk

With Windows Server 2003, you can still create a useful boot disk that can help with recovery in the event something corrupts a critical file on your hard disk. Although this is less important these days—because you can add the recovery console to your boot menu or run it from the Windows Server 2003 installation CD-ROM—we’re the cautious type; we like to have every possible way to recover available. Although a Windows Server 2003 boot disk doesn’t get you to a command prompt, as a Microsoft Windows 95 or Microsoft Windows 98 boot disk does, it does permit you to boot the system under the following circumstances (provided that your actual Windows Server 2003 installation isn’t damaged in any other way):

■ Corrupted boot sector
■ Corrupted master boot record (MBR)
■ Virus infections of the MBR
■ Missing or corrupt Ntldr or Ntdetect.com files

The boot disk can also be used to boot from the shadow drive of a broken mirror set, although you might need to edit the Boot.ini file on the boot disk.
Why MS-DOS Boot Disks Won’t Help

More than one person new to Windows Server 2003 has accidentally deleted or corrupted a key file required to boot the system and tried to recover by digging out an old MS-DOS or Windows boot floppy disk. Alas, it doesn’t work.

The files you need to get your hard disk back to booting condition aren’t even on an MS-DOS floppy disk. When you install Windows Server 2003, it modifies the system’s boot sector to look for and run a file called Ntldr. When you format a floppy disk under MS-DOS, even when you make it a system disk, this file doesn’t get created, because MS-DOS doesn’t know anything about Windows Server 2003.

As such, a boot disk is occasionally useful, and because it’s easy to make and floppy disks grow on trees (although these trees are rarely seen outside of the Microsoft campus), you might as well make one. The boot disk is not generic for every Windows Server 2003 machine. However, if you have a standard configuration across several machines, this disk will work for all the machines that use the same partition and disk controller as their Windows Server 2003 boot partition. Follow these steps to create a boot disk:

1. Insert a blank floppy disk into your floppy drive.
2. At a command prompt, type the command `format a: /u`.
3. Copy the Ntdetect.com and Ntldr files from the \i386 folder on the Windows Server 2003 CD-ROM to the floppy disk.
4. Create a Boot.ini file, or copy the file from the boot drive to the floppy disk.

Real World  ARC Naming Conventions

Understanding how the hard disks and partitions are named on your system is not a trivial task, unfortunately. To provide a uniform naming convention across multiple platforms, Microsoft uses a fairly arcane designation for all the disks and partitions on your computer. Called ARC—short for Advanced RISC Computing—this is a generic naming convention that can be used in the same way for both Intel-based and RISC-based computers.

The convention describes the adapter type and number, the disk number, the rdisk number, and finally the partition number. The format is as follows:

```
<adapertype>(x)disk(y)rdisk(z)partition(n)
```
where `<adaptertype>` can be either SCSI, multi, or signature. Use multi for all non-SCSI adapters and for SCSI adapters that use a BIOS—as most adapters used with Intel-based processors do. The `(x)` is the adapter number, starting at zero. If `<adaptertype>` is signature, `(x)` is an 8-character drive signature.

The value for `(y)` is the SCSI ID of the disk for SCSI adapters. For multi this is always zero. The number for `(z)` is zero for SCSI, and is the ordinal number of the disk for multi, starting with zero. Finally, the partition number `(n)` is the number of the partition on the target disk. Here the partitions start at one, with zero reserved for unused space.

### Installing the Recovery Console

One of the most useful recovery features in Windows Server 2003 is the Recovery Console. This is basically an enhanced, NTFS-enabled, secure command prompt that can be used to copy files, start and stop services, and perform other recovery actions if you can’t boot the system using Windows Server 2003’s safe mode. The Recovery Console is always available for use through the Windows Server 2003 CD-ROM; however, you can also install it as an option on the Boot menu for use in those instances when you can’t boot using Windows Server 2003 safe mode. You’ll still need to use the boot disk if you can’t get to the Boot menu or if the Recovery Console is damaged. To install the Recovery Console, follow these steps:

2. Close the Autorun dialog box.
3. At a command prompt or in the Run dialog box, type the command `d:\i386\winnt32\cmdcons`, replacing `d` with the drive letter of the Windows Server 2003 CD-ROM or network share.
4. Click Yes to install the Recovery Console, as shown in Figure 36-7.

![Figure 36-7 The Windows Server 2003 Setup window](image)
Specifying Recovery Options

You can specify how you want Windows Server 2003 to deal with system crashes by changing a few options in the System tool in Control Panel. To do so, follow these steps:

1. Open the System tool from Control Panel, and click the Advanced tab.

2. Click Settings in the Startup And Recovery box to display the Startup And Recovery dialog box, shown in Figure 36-8.

3. If you have multiple operating systems on the machine, select the operating system you want to have boot by default from the Default Operating System list box.

4. If you want to boot the default operating system automatically, without waiting, clear the Time To Display List Of Operating Systems check box. Otherwise, specify how long you want to display a list of options in the box provided.

5. If you want recovery options automatically displayed in the event of problems, select the Time To Display Recovery Options When Needed check box, and set the time for it.

6. Select the Write An Event To The System Log check box, if available, to record an entry in the event log when the system experiences a crash.

7. Select the Send An Administrative Alert check box to send an alert to administrators over the network when the system crashes.

8. Select the Automatically Restart option to instruct Windows Server 2003 to reboot the system in the event of a crash. Otherwise, the system remains at a blue screen until an administrator manually reboots it.
9. Select how much debugging information you want to record from the Write Debugging Information list box. Note that if you have a large amount of RAM you need the same amount of free disk space if you want to use the Complete Memory Dump option.

10. Enter the filename for the dump file in the Dump File text box, and select the Overwrite Any Existing File check box to maintain only a single dump file.

Creating and Using a Recovery Drive

An excellent way to recycle an old, small drive that’s not good for much else is to use it as an external recovery drive. This drive needs to be only about 2 GB or so, smaller than you could even buy today. The recovery drive can even be used for several servers if you set it up as a portable device. Using a recovery drive in this way offers a somewhat cheaper alternative to mirroring the drive.

To create the recovery drive, perform a minimal install of Windows Server 2003 on the drive, configuring your paging file to be on that drive. Make sure that the installation includes the tape driver you will be using for tape backup. Create a bootable Windows Server 2003 floppy disk, following the procedure outlined earlier in the “Creating a Boot Disk” section, and edit the Boot.ini file on it to point to the SCSI address of the recovery drive.

When a system failure occurs, simply cable the recovery drive to the server and boot from the boot disk that points to the recovery drive. If the recovery drive has sufficient user accounts and software to keep your system running, you can run off the recovery drive until you can schedule a full-scale repair or replacement of the failed drive. When you are able to take the system down and replace the failed drive, all you need to do is restore your backup tape to it and restart the server. You can even do the restore in the background while you continue to run off the recovery drive if necessary.

Note Using a recovery drive in this way presents some interesting licensing and activation issues. If you have one dedicated drive for each machine, you’d need to install, license, and activate a copy for each machine. And if you have only one that you can attach to multiple servers, you’re going to run up against activation if you plug it into a different machine. Consult your Microsoft Account Manager or other licensing resource for information about how to do this most effectively.

Summary

Assume that a disaster will eventually occur, and plan accordingly. Create standardized recovery procedures and keep them up to date. When there’s a lot of turmoil, as always happens in the case of a major failure, people forget important steps and can make poor decisions. Standardized procedures provide a course of action without the need for on-the-spot decisions. The next chapter describes how to use the Windows Server 2003 Backup utility.
Chapter 37

Using Backup

Selecting a Backup Medium ........................................... 1221
Developing a Backup Strategy ........................................ 1224
Backing Up Data ......................................................... 1227
Restoring Data .......................................................... 1239
Planning for Failure ...................................................... 1242
Handling Backup and Restore Problems ......................... 1243
Third-Party Backup Utilities ............................................ 1246
Summary ........................................................................ 1248

Backing up the data on your network is frequently more complicated than it has to be, and Microsoft Windows Server 2003 has an additional complication in the form of the Active Directory service. Fortunately, the operating system includes the Windows Server 2003 Backup utility licensed from Veritas Software that, although it doesn’t include all the bells and whistles of the major third-party network backup products, at least gets the job done in a reasonably efficient manner. You can use Windows Server 2003 Backup to protect the Windows Server 2003 system on which it runs and to back up other systems accessible by way of the network. This chapter examines the capabilities and limitations of Windows Server 2003 Backup, and it describes some basic strategies you can use to protect your network against data loss related to hardware failure, virus attack, or accidental file deletion.

Selecting a Backup Medium

The first decision you must make when planning a backup strategy is where you intend to store your data. Windows Server 2003 Backup supports magnetic tape, the traditional backup medium, but it can also archive your data to a backup file you can store on any device addressable by the Windows Server 2003 file systems, including cartridge drives (such as Iomega Zip and Jaz drives), floppy disks, and even recordable CD-ROMs. For more extensive archiving, Windows Server 2003 Backup also supports the use of media pools—that is, libraries of disks or tapes that you access through a jukebox or autochanger.
Choose your medium based on your budget, the amount of data you have to back up, and how much time you have available for creating the backup.

Estimating the cost of a backup storage medium isn’t simply a matter of pricing tape drives and disk drives. The cost of the recording medium is also an important consideration. Also look at the ongoing costs, especially if you’re using offsite, long-term storage where you’ll need more media on an ongoing basis.

**Using Removable Storage**

When you install a tape, CD-ROM, cartridge drive, or autochanger in Windows Server 2003 using the Add New Hardware Wizard, the drive falls under the control of the Removable Storage service. The Windows Server 2003 Backup utility relies on this service to provide basic media-handling functions. When you mount, dismount, or eject a disk or tape, the Removable Storage service, not Windows Server 2003 Backup, manages the device.

The Removable Storage service has its own user interface, separate from Windows Server 2003 Backup, in the Removable Storage snap-in for the Microsoft Management Console (MMC), as shown in Figure 37-1. You use this tool when you need to send commands directly to a tape drive or other device, such as when you want to eject, format, or re-tension a tape.

![Figure 37-1  The Removable Storage service snap-in](image)

**Note** Don’t use removable storage very often? It’s available in the Computer Management snap-in as well.
Backing Up to Files

As an alternative to backing up using a device registered in the Removable Storage service, you can also back up system data to a file. Windows Server 2003 Backup can create the file on any writable storage device addressable by using a standard drive letter, such as a hard disk, cartridge, floppy disk drive, or even a CD/DVD drive if you have software that makes it look like a regular drive. By default, the backup file has a .BKF extension, but you can name the file anything you want and store it on any supported device.

Using CD-ROMs

Because of their extremely low media cost, recordable CD-ROMs can be an excellent storage medium for system backups. Two types of writable CD-ROMs are commonly used: CD-Rs, which are WORM (write once, read many) devices, and CD-RWs, which you can write to many times. Using CD-Rs for backups might seem wasteful because you can fill them only once, but blank disks are cheap enough to make this feasible. As an added benefit, you get a permanent archive of your system, eliminating the need to develop a media rotation system and keep track of how many times you have used a particular tape or cartridge.

Real World  Backups vs. Archiving

Normal business backups have a limited lifespan. Their purpose is disaster recovery and business continuity. Normal backups that are older than a few weeks have limited usefulness for disaster recovery because the data loss becomes unacceptable for normal business recovery and continuity.

Archival backups, however, are not used for business continuity, but are done for historical purposes or because of a specific legal requirement to retain data for a specified time period. These kinds of backups should be done on a backup media that will have a long shelf life, and should be stored in special locations that will subject them to the minimum amount of deterioration.

CD-R and CD-RW media have a limited lifespan and should not be considered archival media. They deteriorate over time and are subject to environmental deterioration as well. Here are some suggestions for extending the lifespan of your CDs:

- Do not use adhesive labels of any sort.
- Store them in a cool, dry, dark place.
- Keep them away from solvents and airborne pollutants.
Note  Windows Server 2003 Backup doesn’t provide direct support for WORM devices such as recordable CD-ROMs. You must use third-party backup software to use CD-R devices. CD-RW devices can be used like a standard removable disk drive if you have the appropriate packet-writing software installed (such as Roxio’s DirectCD).

Developing a Backup Strategy

To effectively back up a network, you must plan your approach to this complex task. Network backups are more complicated than simply putting a tape in the drive and starting up the software. Your backup strategy should address all the following questions:

- How much data do you have to back up?
- How much time do you have to perform backups?
- How often should you back up the data?
- Who is going to be responsible for seeing that backups are completed?
- How many tapes (or other media) do you plan to use?
- How often do you overwrite your tapes?

Note  For maximum security, assign the Backup and Restore permissions to different users. Only trusted administrators should be allowed to restore from backup to guard against data corruption or theft.

The Backup Window

The backup window is the amount of time you have available to perform backups of your data. The length of your backup window is a major factor in determining which devices you purchase for backing up your network and which types of backups you perform. Compare the length of your backup window with the amount of data you have to back up to determine the optimum backup rate for your network. If, for example, your organization works overlapping shifts, leaving only a few hours of network time during which to perform backups, you might have to purchase faster equipment or run several devices in parallel to back up all your data in the time allotted. Or you might consider using a two-stage backup—backing up to fast hard disk space during your backup window, and then backing from the hard disk to tape or other removable media after the first stage of the backup completes. With the price of hard drives coming down, the wide availability of relatively inexpensive Network Attached Storage (NAS), the speed of tape not keeping
up, and the huge volumes of data that need to be backed up, this option is becoming more attractive.

**Backup Types**

Part of creating a strategy to fit your available backup window involves selecting the type of backups you'll perform. Windows Server 2003 Backup supports five types of backup jobs that specify how much of your data is backed up during each job. By selecting the appropriate job type, you can minimize the number of tapes (or other media) and the amount of time required to perform your backups without compromising the safety of your data.

Most of these backup types depend on the archive attribute to determine when the files on a given disk have changed and must be backed up again. The archive attribute in Windows Server 2003 is the same as it was back in the days of MS-DOS, no matter which file system you're using. The attribute is a single bit included in the directory entry for each file, which the backup software can set or clear as needed.

Typically, a backup program clears the archive attributes for all the files it backs up during a particular job. When you modify a file later, the system automatically sets the attribute as it writes to the disk. This enables the backup software to examine the archive attributes during the next job and back up only the files for which the attribute is set—that is, the files that have changed since the last backup. The backup types described in the following sections are variations on this technique.

**Normal Backup**

A normal backup, in Windows Server 2003 parlance, is a full backup of all the files and directories you select in the Windows Server 2003 Backup software. As part of the job, the program clears the archive attribute on each file. This type of job is the baseline for future jobs that back up only the modified files.

**Incremental Backup**

During an incremental backup, the program examines the archive attributes and backs up only the files that have changed since the last normal or incremental backup. As with a normal backup, this type of job also clears the archive attribute on each file it copies. Incremental backups use the minimum amount of tape and also save time by not copying all the files that remain unchanged during every job. However, performing a restore is inconvenient.

For example, if you perform a normal backup on Monday and incremental backups on Tuesday through Friday, you must restore from all five of these tapes in the order in which they were written to ensure that you have the most current version of every file. If
a particular file is updated daily, Windows Server 2003 Backup overwrites it with a newer version during the restoration of each tape. However, if you restore only the Monday and Friday tapes, because they represent the last normal backup and the most recent incremental backup, you lose the most current versions of files that were modified on Tuesday through Thursday, but not on Friday.

### Differential Backup

A differential backup is identical to an incremental backup except that the program doesn’t clear the archive attributes for the files that it copies to tape. This means that during each differential backup you are copying every file that has changed since the last normal or incremental backup. Thus, after a normal backup on Monday, a differential backup on Tuesday copies all the files that have changed (just like an incremental job). However, the differential backups performed on Wednesday through Friday copy all the files changed since Monday’s normal backup. In other words, some redundancy of data is likely during this kind of job because a file modified only once on Tuesday is copied during each day’s differential backups.

This type of job requires more tape than using incremental jobs, and more time as well, but the advantage is that when you perform a restore, you need only the tapes containing the last normal backup and the most recent differential. Thus, if you have to rebuild a system on Saturday, you need restore only the normal backup from the previous Monday and the most recent differential backup from Friday.

A network backup strategy typically uses incremental or differential backups in addition to normal jobs, but not both. If you’re faced with a lot of data to back up and a limited backup window, incremental backups are faster and more economical. However, if you have to perform frequent restores, differential backups make the process far easier.

### Daily Backup

A daily backup copies only the files that have changed on the day that the backup job is performed, disregarding the current state of the archive attribute. This type of job also doesn’t clear the archive attributes of the files it copies as it runs. Daily jobs are useful when you want to perform an extra backup on a given day without disturbing an established backup strategy by modifying the archive attributes.

### Copy Backup

A copy backup job is the equivalent of a normal backup, except that the program doesn’t clear the archive attributes of the files it writes to the tape or other backup medium. You can use a copy backup job to perform an extra full backup without disturbing the archive attributes used by an established backup strategy.
Media Rotation

A media rotation scheme dictates how many tapes (or other media) you use for your backups. In most cases, you’ll want to keep copies of your backups for a while in case you need to perform a restore from them, but eventually, they become obsolete and you can reuse the tapes. For example, a small network might use a total of five tapes to perform a full backup each weekday and reuse the same tapes each week. In contrast, a large, security-conscious organization might use new tapes for every backup and permanently archive all the used ones. Most media rotation schemes fall somewhere between these two extremes.

One popular rotation scheme is known as the grandfather-father-son method because it uses three “generations” of tapes representing monthly, weekly, and daily backups, respectively. In this rotation scheme, you perform a full backup every month and retain the tape for a year (preferably off-site); this is the “grandfather.” You also perform a full backup every week and retain the tape for a month; this is the “father.” The “son” backups are performed daily and retained for a week. The daily jobs can be either full, incremental, or differential backups.

The point of a media rotation scheme is to ensure that you always have a current copy of your data on tape and to reuse the tapes in an even and organized manner. Be sure to label your tapes carefully and store them in a safe place, away from magnetic fields and other adverse environments. It is also strongly recommended that you store a copy of your backups off-site, such as in a safety deposit box or other fireproof vault, or with a service that provides pickup, secure storage, and retrieval, so that in the event of a true disaster, such as a fire, your data is protected.

Note Some third-party network backup products can automatically implement a customizable rotation scheme by tracking the tapes, the number of times they’re used, and the names to put on the labels. These programs also tell you which tape to put in the drive each day and let you know which tapes you must use to restore particular files. Unfortunately, Windows Server 2003 Backup lacks this feature.

Backing Up Data

The Windows Server 2003 Backup program provides several methods you can use to create and execute backup jobs. When you launch Windows Server 2003 Backup for the first time—by clicking Start, pointing to Programs, choosing Accessories, choosing System Tools, and then choosing Backup—you see the Welcome page for the Backup Or
Restore Wizard. This wizard provides a straightforward way to back up the local computer, but for more flexibility, clear the check box for Always Start In Wizard mode and click the Advanced Mode link.

Backup jobs can also be run from the command line using the executable program Ntbackup.exe with the appropriate parameters. See “Executing Jobs from the Command Line” later in this chapter for more information.

The following sections examine the various methods for creating a backup job. Regardless of the particular method you use, creating any backup job involves the following basic steps:

- Select the drives, directories, and files you want to back up.
- Specify the storage medium that is the destination for the backup.
- Configure backup options such as backup type, logging, and file exclusions.
- Specify when the backup is to occur.

Real World  **NTBackup Cannot Back Up Case-Sensitive File Systems**

The NTBackup program has serious limitations when dealing with some advanced features introduced in Windows Server 2003 R2. Specifically, it cannot correctly back up and restore files and folders on an NFS volume, nor does it know how to handle the case-sensitive files that can be created by Windows Subsystem for UNIX-Based Applications (SUA), even when those files are stored locally on an NTFS volume. The backup portion of NTBackup will report that it has successfully backed up case-sensitive files, but if there are multiple files with the same name except for case, only one version of the file will be available to restore—and which version of the file that is cannot be predicted. This means that C:\MyFiles\ImportantFile.txt and C:\MyFiles\importantfile.TXT will be reported as backed up, but only one of them will be restorable.

The only workaround that will successfully back up case-sensitive files is to use a UNIX or SUA tar program to backup the file system and then use NTBackup to back the tar file to your backup media.

**Using Windows Server 2003 Backup**

The Backup tab of the Windows 2000 Backup program (shown in Figure 37-2) is where you select the files and directories to be backed up and choose their destination. You use a Microsoft Windows Explorer–like hierarchical display to browse local and network
drives and make selections with the check boxes. You can select entire drives or individual files and directories for backup. The System State item backs up the registry and the Active Directory database on the local machine, as well as other system elements required in a disaster recovery situation. See “Backing Up the System State,” later in this chapter, for more information about the system state and disaster recovery.

Figure 37-2  Choosing files and folders to back up

Creating Selection Scripts
After you select the files and directories to back up, you can create a selection script that contains the job configuration you created. After choosing Save Selections from the Job menu, you specify a filename with a .BKS extension for the selection script and the directory where the program should create it. You can use selection scripts to create an identical backup job during a subsequent session by loading the selection script from the Job menu. When you do this, the same system elements you selected before creating the script are selected again. You can then run the job as is or make additional selections. You can also use the script to execute the job from the Ntbackup.exe command line.

Accessing Files and Folders for Backup
To back up any files and folders, the account used to run the job must have the appropriate permissions granting access to those files and folders. A user who is a member of the local Backup Operators group or Administrators group is automatically granted permission to back up any and all files and folders on the local machine. Members of the domain Backup Operators group and Administrators group can back up all files and folders on any computer in the domain, as well as any computer in a domain with which a two-way trust relationship exists.
A user who isn’t a member of any of these groups must either be the owner or have the Read, Read and Execute, Modify, or Full Control permission for each of the files and folders to be backed up. Disk quota restrictions can also limit a user’s ability to back up systems.

**Selecting the Storage Medium**

After you specify what you want to back up, you must tell the program where to write the data. By default, Windows Server 2003 Backup provides the File option only in the Backup Destination field. If you installed a tape drive or other device so that it is managed by the Removable Storage service, that device is also provided as a destination option. After you make a selection, use the Backup Media field or the File Name field to specify a tape or disk name or the path and filename the program should use to create a backup file.

When you select a tape or other removable storage drive, the Backup Media field enables you to select it by the name you already created with Windows Server 2003 Backup or to select New Media, which enables you to specify a name for a new blank device.

**Configuring Backup Options**

At this point, you can click Start Backup to trigger the backup job using the parameters specified on the Backup tab of the Backup window, or you can further configure the job by choosing Options from the Tools menu. On the General tab of the Options dialog box, you can specify whether the program should use certain media-handling features and, most importantly, select whether the program should verify the data on the tape after completing the backup job. A verification pass compares the data that has been written to the tape or other medium with the original copy on the hard disks to ensure that the data has been written properly. Although the verification process considerably lengthens the time required to run the job, it’s a good precaution to take, especially when you’re working with a newly installed drive.

---

**Important** Although verifying the backup data written to any tape is a wise precaution to take, it isn’t foolproof. Many times a backup job seems to complete successfully and is even verified, but the data can’t be restored for one reason or another. The only absolutely reliable method for ensuring that the data you backed up has actually been written to the tape is to perform test restores.

On the Backup Type tab of the Options dialog box, you select the type of job you want to run (either normal, incremental, differential, copy, or daily, as described in the “Backup Types” section earlier in this chapter). The default is to run a normal backup, which might be undesirable if you’re in the midst of a backup sequence that relies on the archive attributes to determine which files the program should copy to the tape.
Note You’re prompted to specify values for the Backup options when you run a backup job using either the Start Backup button or the Windows Server 2003 Backup Wizard. The settings you specify for these options now are the default values in the prompts generated later.

Logging Backups
On the Backup Log tab of the Options dialog box (shown in Figure 37-3), you can specify whether the program should keep a log of the activities that occur during the job and the level of detail in the log. Because a detailed log lists every file and directory copied during the job, the file can be quite long. If you want to review the job only to see that all the procedures completed successfully, select the Summary option.

![Figure 37-3 The Backup Log tab of the Options dialog box](image)

The backup logs are stored as ASCII files with a .LOG extension in a subfolder named Local Settings\Application Data\Microsoft\Windows NT\NTBackup\Data. This path is located in the Documents And Settings folder named for the user scheduling the job. You can view the logs with any text editor, but unfortunately, Windows Server 2003 Backup gives the files incremental names like Backup01.log and Backup02.log, making it difficult to locate the log for a particular job. To view a log by the job name, choose Report from the Backup program’s Tools menu, select a particular job, and click View or Print. This displays the log file using Notepad.
Excluding Files
On the Exclude Files tab (shown in Figure 37-4), you can list specific files and directories that the program should skip during the backup process. By default, the list already contains the files that never need to be backed up, such as the Windows Server 2003 memory paging file (Pagefile.sys). You can add other items to the list as needed. The advantage of using the Files Excluded For All Users list instead of simply clearing specific files on the Backup tab is that you can use wildcards to skip files located anywhere in the job. For example, you can add the file mask Backup*.wbk to the list to exclude all the automatically created Microsoft Word document backup files, wherever they occur in the selected drives and directories.

![Figure 37-4 The Exclude Files tab of the Options dialog box](image)

The Exclude Files tab contains two lists: one to exclude files owned by all users on the system, and one to exclude only files owned by the user currently logged on. With the latter option, you can add the Backup*.wbk file mask to the current-user-only list and safely skip your Word document backups without disturbing anyone else’s.

To add files to either list, click the appropriate Add New button and either select a registered file type or specify a custom file mask in the Add Excluded Files dialog box. (See Figure 37-5.) You can also specify a particular path in which the files—selected either by file type or by file mask—are to be excluded. By default, the program excludes the files in the chosen folder and all its subfolders, but you can limit the exclusion to the selected folder only by clearing the Applies To All Subfolders check box.
Running a Job

After you configure the options for the job, click Start Backup on the Backup tab and the Backup Job Information dialog box opens. (See Figure 37-6.) You’re prompted to specify a descriptive name for the backup set and to decide whether the job should be appended to the selected tape (or other medium) or whether to overwrite any existing data. If you intend to overwrite the tape, you must specify a new name for it. If you choose to overwrite the tape, you can also control access to the data written to the tape by selecting a check box that permits only the owner of the job and members of the Administrators group to restore its files.
When you click Advanced in the Backup Job Information dialog box, the program prompts you for a backup type (with the value selected on the Backup Type tab of the Options dialog box as the default), and you can choose to enable the following options:

- **Back Up Data That Is In Remote Storage**  When selected, this causes the program to back up data that has been migrated to remote storage. (The data must be temporarily recalled to be backed up.)

- **Verify Data After Backup**  When selected, this causes the program to compare the data written to the tape with the original data. The default value is taken from the equivalent item on the General tab of the Options dialog box.

- **If Possible, Compress The Backup Data To Save Space**  When selected, this activates the data compression capabilities built into the selected tape drive or other device. Windows Server 2003 Backup doesn’t include any software-based compression capabilities; it facilitates only the use of your storage device’s hardware-based compression. This option is enabled by default if the selected device has hardware-based compression capabilities, and it’s disabled if the device doesn’t.

- **Automatically Back Up System Protected Files With The System State**  This option is enabled only if the System State object has been selected for backup. When this option is selected, all the system files in the %SystemRoot% folder and any subfolders are backed up in addition to the files normally backed up for a system state backup.

- **Disable Volume Shadow Copy**  When selected, this option allows the backup of in-use documents. See Chapter 18 and 20 for details on configuring and using shadow copies.

### Scheduling a Job

At this point, you can start the backup job immediately by clicking Start Backup in the Backup Job Information dialog box, but to establish an organized backup strategy, you’ll want to schedule your jobs to execute at specific intervals. When you click Schedule in the Backup Job Information dialog box, if the backup selections have not been saved, you are instructed to do so before you can schedule a backup. Otherwise, the program prompts you to specify the user name and password for the account that the system should use when running the job. The program then calls for you to specify a name for the job and displays the current date and time for the start date. To execute the job later, click Properties to display the Schedule Job dialog box shown in Figure 37-7.
Here you can specify whether the job is to be executed once at a certain time or repeated at regular intervals. The options available in the Schedule Task drop-down list are as follows:

- **Once**  Executes the job once at a specific time on a specific date.
- **Daily**  Executes the job at the specified time each day or, if you modify the value of the Schedule Task Daily selector, each specified number of days.
- **Weekly** Executes the job at the specified time on each of the specified days of the week or, if you modify the value of the Schedule Task Weekly selector, each specified number of weeks.
- **Monthly** Executes the job at the specified time once a month, based on either a selected date (such as the first of every month) or a day of the week (such as the first Monday of every month). By clicking Select Months, you can specify the months in which the job should run.
- **At System Startup** Executes the job the next time the system is started.
- **At Logon**  Executes the job the next time the job owner logs on.
- **When Idle**  Executes the job when the system has been idle for a specified number of minutes.
Note  The scheduling capabilities of Windows Server 2003 Backup are quite comprehensive but not always intuitive. For example, you must select Weekly to run a daily job only on weekdays, and then select all the days except Saturday and Sunday.

If you select the Show Multiple Schedules check box, the heading on the Schedule tab changes to a selector in which you can create and manage separate schedules for the same job. You can, for example, schedule a normal backup job to execute every weekday and create a separate event to execute the same job on the last Sunday of each month, to create an extra copy for off-site storage.

If you select Once, Daily, Weekly, or Monthly from the Schedule Task list, the Advanced button becomes available. Clicking this button opens the Advanced Schedule Options dialog box. In this dialog box, you can specify a date at which a repeating job should no longer be rescheduled and you can also configure a job to repeat continually after a specified interval has elapsed. You can use this feature to copy important and volatile data to a backup file every few minutes, as an extra precaution against data loss.

On the Settings tab of the Schedule Job dialog box, you can specify conditions under which the system is instructed not to run the job, such as when the computer has not been idle for a specified length of time or when it’s running on battery power. You can also configure the job to terminate if it doesn’t finish within a specified length of time.

After you schedule a job for later execution, you see an icon representing it in the backup program’s Schedule Jobs tab. Rest the pointer on any icon for the name of the job to appear. (See Figure 37-8.) You can modify the parameters for any scheduled job by clicking its icon to access its Scheduled Job Options dialog box.

![Figure 37-8 The Schedule Jobs tab of Windows Server 2003 Backup](image)
Using the Windows Server 2003 Backup Wizard

Windows Server 2003 Backup includes still another wizard to guide you through the process of configuring and creating a backup job. You can launch the wizard either from the Windows Server 2003 Backup program's Welcome tab, by double-clicking a particular calendar date on the Schedule Jobs tab, or by clicking Add Job on the Schedule Jobs tab. If you already selected drives, folders, or files to back up on the Backup tab, the program offers to use those selections in the wizard when you select a date.

The prompts presented by the wizard correspond to the options available in the program's regular GUI dialog boxes, reminding users of the program's capabilities and preventing them from inadvertently omitting an important option.

Executing Jobs from the Command Line

In addition to the wizards and the GUI, you can also execute jobs from the command line. In fact, when you schedule a job for later execution using the GUI or the Backup Wizard, the program actually uses the Windows Server 2003 Task Scheduler to launch the job with the command-line equivalents to the options you chose. Select Task Scheduler from the Control Panel menu, and select your backup job. On the Task tab, you can see the command line for your job in the Run field. (See Figure 37-9.)

The executable file for the Windows Server 2003 Backup program is still called Ntbackup.exe and is located in the %SystemRoot%\System32 folder. The best application for this command-line capability is to execute selection scripts that you previously
created in the backup program’s GUI interface from batch files or other scripts. The syntax for running Ntbackup.exe from the command line is as follows:

```
Ntbackup backup [systemstate] "@filename.bks" /J "jobname"
[/P "poolname"] [/G "guidname"] [/T "tapename"] [/N "medianame"]
[/F "backupfilename"] [/D "setdescription"] [/DS "servername"
[/IS "servername"] [/A] [/V:{yes|no}] [/R:{yes|no}] [/L:{f|s|n}]
[/M "backuptype"] [/RS:{yes|no}] [/HC:{on|off}] [/SNAP:{on|off}]
```

- **backup**: Specifies that the program perform a backup operation (even though `restore` is not a valid parameter on the command line).
- **systemstate**: Specifies that the program should back up the system state in addition to the files and folders specified on the local computer’s command line or in a selection script.
- **bksfilename|foldername**: Specifies the name of a selection script file or the name of a folder for the program to back up (along with its subfolders). The `@` character must precede the name of the .bks Backup selection file.
- **/J "jobname"**: Specifies a name for the backup job that the program uses to identify it in the log file.
- **/P "poolname"**: Specifies the name of the media pool from which the program should take the tape (or other medium) to perform the backup. This option must not be used with the `/A`, `/G`, `/F`, or `/T` switch.
- **/G "guidname"**: Specifies that the program perform the backup to a tape or other medium identified by the `guidname` variable. This option cannot be used with the `/P` switch.
- **/T "tapename"**: Specifies that the program perform the backup to a tape or other medium identified by the `tapename` variable. This option cannot be used with the `/P` switch.
- **/N "medianame"**: Specifies the new name for a tape or other medium that is being overwritten by the backup job. This option cannot be used with the `/A` switch.
- **/F "backupfilename"**: Specifies the name of the .BKF file to which the program should back up the selected files and folders. This option cannot be used with the `/P`, `/G`, or `/T` switch.
- **/D "setdescription"**: Specifies a descriptive label to be assigned to the backup set.
- **/DS "servername"**: Causes the program to back up the directory service file for a specified Microsoft Exchange server.
- **/IS "servername"**: Causes the program to back up the information store file for a specified Microsoft Exchange server.
Chapter 37  Using Backup

- **/A**  Causes the program to append the backup job to the tape or other medium specified by the /G or /T switch. This option cannot be used with the /P switch.

- **/V:**{yes|no}  Specifies whether the program should verify the data after the backup is completed.

- **/R:**{yes|no}  Specifies whether access to data on the tape or other medium should be restricted to the owner of the job and members of the Administrators group.

- **/L:**{f|s|n}  Specifies the type of log that the program should keep while executing the backup job, where f = full, s = summary, and n = none.

- **/M backuptype**  Specifies the type of backup to be performed, where backuptype is replaced by one of the following values: normal, incremental, differential, copy, or daily.

- **/RS:**{yes|no}  Specifies whether the program should back up migrated Removable Storage data. (The Remote Storage database is backed up automatically when you back up the %SystemRoot% folder.)

- **/HC:**{on|off}  Specifies whether the program should activate the hardware-compression capabilities of the tape drive.

- **/SNAP:**{on|off}  Specifies whether the backup should use a volume shadow copy.

The default states of the /V, /R, /L, /M, /RS, and /HC switches correspond to the current settings of the corresponding options in the backup program’s GUI dialog boxes.

---

Restoring Data

Windows Server 2003 Backup allows you to select individual files and directories for restoration or simply to restore the entire backup set to its original location. As with the program’s backup function, you can create restore jobs using GUI screens or a wizard. There is no command-line restore function in NTBackup, a serious omission in our opinion.

Selecting Files to Be Restored

When you display the Restore And Manage Media tab in the Windows Server 2003 Backup program, you see a list of the media in the backup media pool and the backup files you created. As part of each backup operation, Windows Server 2003 Backup creates a catalog of the backup set and stores it on the tape or other medium. (If a backup job spans two or more tapes, the backup set catalog is stored on the last tape.) The program accesses this catalog whenever you select a tape from the list for restoration.
After you insert the proper tape into the drive, the program reads the catalog and shows the contents of the tape in a hierarchical display just like that of the Backup tab. (See Figure 37-10.) You can select drives, folders, and files to restore just as you selected them to be backed up.

**Figure 37-10**  The Restore And Manage Media tab

### Selecting Destinations for Restored Files

In a disaster-recovery situation, you probably want to restore an entire backup set to its original location, but in many cases, network administrators perform restores to retrieve a copy of a file or folder that a user has accidentally deleted or that has become corrupted somehow. When this is the case, you might not want to restore the files to their original location, and Windows Server 2003 Backup provides options that enable you to specify another location. The Restore Files To drop-down list on the Restore And Manage Media tab provides the following options:

- **Original Location**  Restores all the selected files and folders to their original locations on local or network drives, preserving the original directory structure
- **Alternate Location**  Restores all the selected files and folders to a specified folder, preserving the directory structure of the restored material
- **Single Folder**  Restores all the selected files to a single specified folder, disregarding the original directory structure
Important If you elect to use the Single Folder option when performing a restore and you have files with identical names in the selected directories, the program uses the settings from the Restore tab in the Options dialog box to determine whether to overwrite the first files with subsequent, identically named files.

Setting Restore Options
On the Restore tab of the Options dialog box (Options from the Tools menu), you specify how the backup program should behave when it encounters existing files with the same names during a restore operation. The following options are available:

- **Do Not Replace File On My Computer**  Restores only the files that don’t already exist on the destination disk
- **Replace The File On Disk Only If The File On Disk Is Older**  Compares the dates of the identically named files, and overwrites existing files on the destination disk only if the backed-up version is newer
- **Always Replace The File On My Computer**  Restores all the selected files to the destination disk, overwriting any existing files with identical names

When you click Start Restore, the Confirm Restore dialog box gives you the opportunity to click Advanced to configure the following advanced restore options before beginning the restore process:

- **Restore Security**  Specifies whether the program should restore all the security settings for each file and folder, including ownership, permissions, and audit entries. To restore the security settings, the destination for the restore job must be an NTFS drive (and the files and folders must have been backed up from an NTFS drive).
- **Restore Removable Storage Database**  Specifies whether the program should restore the Removable Storage database to the `\%SystemRoot%\System32\Ntmsdata` folder, overwriting any existing Removable Storage database at that location.
- **Restore Junction Points, And Restore File And Folder Data Under Junction Points To The Original Location**  Specifies whether the program should restore the junction points created with mounted drives as well as the data that the junction points reference. When this feature is disabled, Windows Server 2003 Backup restores the junction points themselves but doesn’t necessarily restore the referenced data.
When Restoring Replicated Data Sets, Mark The Restored Data As The Primary Data For All Replicas  Specifies whether the program should restore file replication service (FRS) data so that it is replicated to other servers. When this feature is disabled, Windows Server 2003 Backup restores the FRS data, but because of its age, it is likely to be overwritten later by data from the replicas on other servers.

Note  Windows Server 2003 Backup can only execute restore jobs immediately. The program can’t schedule restores for later execution.

Planning for Failure
A catastrophic hard-disk failure on a server is every network administrator’s ultimate challenge, and other misfortunes can end in the destruction of disks or even entire systems. Making sure you have current backups of your disks is an essential part of any disaster recovery plan, as described in Chapter 36, but other Windows Server 2003 system elements should also be protected. Windows Server 2003 Backup includes additional features that allow you to protect the entire system configuration and simplify the process of restoring the computer to its former state.

Backing Up the System State
A separate entry called System State appears with the local drive letters under the My Computer heading on the Backup tab of Windows Server 2003 Backup. Selecting the System State entry causes the program to back up the components of the local system configuration that aren’t directly accessible through the file system. These components include the following:

- Registry (on both servers and workstations)
- Class Registration database (on both servers and workstations)
- System boot files (on both servers and workstations)
- Certificate Services database (on certificate servers only)
- Active Directory (on domain controllers only)
- SYSVOL folder (on domain controllers only)

Backing up these components makes it possible for you to completely restore a system to a new disk without losing any of the domain and local user accounts or the rights and permissions associated with them. You can back up the system state only for the local machine, meaning that if you have multiple Windows Server 2003 systems on your network, you have to run the backup program on each computer to fully protect them. In
most cases, however, only Windows Server 2003 domain controllers contain system state information that is irreplaceable.

Because of dependencies between the system state elements, you can’t back them up or restore them individually; you must treat them as a unified system element. However, you can restore the system state to another location, in which case on domain controllers the program restores only the registry, SYSVOL, and system boot files.

Note Even if you can’t back up the system state on remote systems, you can back up disks from those systems over the network. You can effectively protect all your systems by first running a backup of the system state on each computer, saving it to a network share. Schedule the same backup to run at regular intervals. Then schedule a backup of the files on the share in addition to the regular remote backup to run after the backup of the local system states. Should you need to reconstruct a machine, the data files can be restored from the network backup and the system state can be restored locally.

Handling Backup and Restore Problems

Backing up and restoring data in a network environment is a process that has always been subject to special problems and considerations. Windows Server 2003 Backup addresses some of these problems, as discussed in the following sections.

Backing Up Exchange Servers

Because they can be constantly in use, mail servers such as Microsoft Exchange have unique backup problems. The backup program includes a feature specifically designed to back up Exchange servers, which is available only when the program detects an Exchange module called Edbbcli.dll on the local system. When this module is present, a Microsoft Exchange item appears in the backup program’s Tools menu, enabling you to specify the Uniform Naming Convention (UNC) name of the Exchange server you want the program to access. Also, the expandable display in the Backup tab includes a Microsoft Exchange icon you select to back up the mail server.

Note The shadow copy feature can’t be used to back up versions of Exchange Server up to and including Exchange Server 2000.

Backing Up Encrypted Files

Encrypted files aren’t stored any differently from unencrypted files by the Windows Server 2003 file systems; only their data format is different. Therefore, backing up encrypted files doesn’t in any way compromise their security status. The files are copied
to the tape or other medium in their encrypted form and restored the same way. The personnel responsible for backing up the files don’t need to have access to the encryption codes, nor does access to the tape itself present a risk.

Restoring the System State

Back up the system state is as simple as selecting the appropriate box on the Backup tab, but restoring it is a bit trickier. The restoration process must not only overwrite vital system data that is currently in use, such as the registry, but it must also (in the case of a domain controller) restore the Active Directory database. This problem is particularly difficult because in a domain with multiple domain controllers, the replication system can overwrite the newly restored data because of its outdated update sequence numbers.

Therefore, to effectively restore the system state on a domain controller, you must perform two special procedures during the restoration process: start the computer in directory services restore mode, and perform an authoritative restore of the Active Directory database.

---

**Note** You can restore the system state only on the local system. The Windows Server 2003 Backup program automatically determines the correct destination for the restored data, based on the location of the system root directory (typically C:\Windows), and it overwrites the existing system state data on the computer.

Directory Services Restore Mode

To restore Active Directory and the SYSVOL volume on a Windows Server 2003 domain controller, you must first reboot the system in directory services restore mode, a form of safe mode that ensures that the system is ready to have its Active Directory database overwritten. To do this, restart the system and press the F8 key when you see the Please Select The Operating System To Start message. From the Boot menu, choose Directory Services Restore Mode. After checking the system’s local drives to ensure their integrity, Windows Server 2003 loads the operating system in a standalone server configuration with a set of generic drivers that permit safe-mode access to the operating system.

Because your domain controller system isn’t functioning as a domain controller at this time, you might see error messages stating that Active Directory–dependent services have failed to load. This is to be expected. Because the machine isn’t functioning as a domain controller, it isn’t using the user and group objects associated with the domain. Instead, the system is using a small set of user and group accounts stored in the registry rather than in Active Directory. At this point, you can run Windows Server 2003 Backup and restore the system state.
Authoritative Restore
When you restore the system state on a domain controller, the restored Active Directory objects have the same update sequence numbers as when they were backed up. These numbers are necessarily older than those currently in use in Active Directory and, as a result, they are considered to be outdated and are overwritten during the next replication pass. To prevent this from happening, you must perform an authoritative restore of the Active Directory data stored as part of the system state on the backup medium. An authoritative restore is one that flags the restored Active Directory objects as authoritative, meaning that during the next replication event they overwrite the equivalent objects on the domain controllers containing the replicas.

To perform an authoritative restore, you must run the Windows Server 2003 Ntdsutil.exe program after you restore the system state and before you reboot the computer. Ntdsutil.exe modifies the update sequence numbers of the restored objects so that they appear to the replicas to contain the newest data available. During the next replication pass, the system uses the restored Active Directory database objects to overwrite the data on the domain’s other controllers.

---

**Note**  Windows Server 2003 will not allow a restoration of domain controller backup older than the tombstone lifetime configured for the enterprise. The default tombstone lifetime is 60 days except on Windows Server 2003 SP1 or later where the default is 180 days when creating a new forest, as described in Microsoft Knowledge Base Article 216993. See [http://support.microsoft.com/default.aspx?scid=216993](http://support.microsoft.com/default.aspx?scid=216993) for more information.

Ntdsutil
The Ntdsutil.exe program is an interactive command-line utility copied to the \%SystemRoot%\System32 folder by default during the operating system installation. You see a prompt labeled ntdsutil: when you run the executable file from the command line. The program uses a series of menus to navigate its various functions. Type a question mark (?) or help at any prompt to list the available commands and submenus for that prompt. To perform an authoritative restore, type **authoritative restore** at the ntdsutil prompt and then type help to display the available commands, which are as follows:

- **Restore Database**  Modifies the update sequence numbers of all Active Directory objects, making them authoritative for the entire domain
- **Restore Database Verinc %d**  Authoritatively restores the entire database specified by the variable %d, and overrides version increase
- **Restore Subtree %s** Modifies the update sequence numbers of Active Directory objects in the subtree specified by the %s variable, making them authoritative for the entire domain.

- **Restore Subtree %s Verinc %d** Authoritatively restores the subtree specified by the variable %s, and overrides version increase.

Thus, to use the entire Active Directory database restored with the system state as authoritative information, you use the Restore Database command at the Ntdsutil.exe authoritative restore: prompt. The program opens the database and increases the version number of all the Active Directory objects by 100,000. When the process is complete, you can exit the program by typing `quit` twice, and restart the system in normal mode. When the computer is functioning as a domain controller again, it replicates its Active Directory database to all the other controllers in the domain, and because the version numbers of its objects are substantially higher than those of the other replicas, the system copies the restored data to all the replicas in the domain.

**Preserving NTFS Permissions**

File system permissions are an essential element of any network storage policy, and for a backup program to function in a network environment, it must be able to save the permissions along with the files and restore them either to the same or a different location. However, the various file systems supported by Windows Server 2003 complicate this process considerably. The FAT file systems don’t support permissions, the NFS file system has a completely different set of permissions, and if you restore a backup of an NTFS drive to a FAT or NFS drive, those permissions are lost or, in the case of NFS, simplified.

**Third-Party Backup Utilities**

The Windows NT backup utilities suffer from serious deficiencies in their tape-drive support, scheduling capabilities, and other features. For some networks, NTBackup will be sufficient, but in many enterprise environments, it just isn’t a sufficient tool.

One of the shortcomings of the Windows Server 2003 Backup program is that because the backup set catalogs are stored on the backup media themselves, you can’t tell whether a particular file is on a tape without loading it so that the program can read the catalog. This can be more than a little time consuming and annoying if you have several days’ worth of tapes to go through to find a particular version of the file. Some third-party backup products store the catalog information in a database on the local drive,
enabling you to search for particular files (and even particular versions of files) to discover which tape you must use to restore them. This feature uses a substantial amount of disk space, but disk space is much less expensive than an administrator’s time in most environments.

Although Windows Server 2003 Backup supports backing up to CD-RW media (if you have packet-writing software such as Roxio’s DirectCD installed), it doesn’t support disk spanning (the ability to save the backup to multiple disks), and it doesn’t support DVD at all. This, combined with the lack of CD-R support (because CD-R disks are much cheaper than CD-RW disks), makes the Windows Server 2003 Backup program less than useful when paired with CD-ROM burners. Fortunately, most third-party backup programs support both CD-R media and disk spanning, allowing you to back up to multiple CD-ROM media (although your patience might be taxed if backing up more than a couple of gigabytes).

Most third-party programs also simplify the process of creating a media rotation scheme by enabling you to specify the types of jobs you want to run each day and indicating when to run them. The program takes charge of the tape labeling by telling you which tape to insert each day and assigning it a new name. After overwriting each tape a specified number of times, the program advises you to retire it and add a new tape to the rotation. This also makes restoring to a specified file easier because the program can tell you by name exactly which tape you need to restore from.

Some network backup solutions also provide additional capabilities such as modules that enable you to back up certain types of files while they’re in use or that allow you to back up workstations running non-Windows operating systems. Although third-party network backup solutions aren’t absolutely necessary, they can provide simplified backup administration and expanded capabilities.

While not a third-party solution, the Microsoft System Center Data Protection Manager 2006 (DPM) is a new, and interesting, addition to the system administrator’s backup toolset. Unlike NTBackup, which is primarily a tape-based backup and recovery tool, DPM is designed around disk-based backup and recovery. It provides nearly continuous backups of files and file modifications, and enables rapid restoration of file versions from multiple points in time. This initial release only supports file system backups, but future versions will support additional Microsoft products such as Exchange and SQL Server. DPM is not a complete substitute for NTBackup or another tape-based backup utility, but should be actively considered as a supplement to a tape solution.
Summary

After you develop an adequate backup strategy and configure the software to implement it, it’s up to the administrator to see that the plan is carried out. Frequently, backups require no more attention than the insertion of a new tape into a drive, and yet even this simple task is often overlooked. Too many administrators learn about the importance of keeping current backups the hard way, through the irretrievable loss of important data. Those who find suitable employment afterward have usually learned their lesson, but it’s always better if you can learn painful lessons without the pain. The next chapter focuses on the tools for building a Windows Server 2003 environment that is both fault tolerant and available.
Chapter 38
Planning Fault Tolerance and Avoidance

Mean Time to Failure and Mean Time to Recover ..................... 1250
Protecting the Power Supply ............................................. 1251
Disk Arrays ................................................................. 1256
Distributed File System ..................................................... 1262
Clustering ................................................................. 1263
Summary ................................................................. 1264

Even the most optimistic system administrator knows that sooner or later he will be faced with a major problem. In Chapter 36, we covered disaster recovery planning in depth, and you should refer to that chapter for information on how to prepare for major problems and build a disaster recovery plan to respond quickly and efficiently to major trouble. But as exhilarating as it might be to work through a major problem and successfully recover from it, it’s far better to avoid major as much as possible.

This chapter focuses on the hardware and software tools that help you to build a highly available and fault-tolerant Microsoft Windows Server 2003 environment. Remember, however, that hardware and software are only a small part of the equation—building and deploying for high availability and fault tolerance requires time, a clear understanding of the trade-offs required, and—most important—discipline.

Building highly available and fault-tolerant systems involves hard work and can be expensive. You should have a clear understanding of the business needs you’re trying to resolve and a realistic assessment of the resources available to meet those requirements in order to make informed decisions. When planning for a highly available and fault-tolerant deployment, you should consider all points of failure and work to eliminate any single point of failure. Redundant power supplies, dual disk controllers, multiple network interface cards (multihoming), and fault-tolerant disk arrays (RAID) are all strategies that you can and should employ.
Mean Time to Failure and Mean Time to Recover

The two most common metrics used to measure fault tolerance and avoidance are the following:

- **Mean time to failure (MTTF)**  The mean time until the device will fail
- **Mean time to recover (MTTR)**  The mean time it takes to recover once a failure has occurred

Although a great deal of time and energy is often spent trying to lower the MTTF, you should keep in mind that even if you have a finite failure rate, if your MTTR is zero or near zero, this may be indistinguishable from a system that hasn’t failed. Downtime is generally measured as MTTR/MTTF, so increasing the MTTF will reduce the downtime. But it can be prohibitively expensive to increase MTTF beyond a certain point, so you should spend both time and resources on managing and reducing the MTTR for your most likely and costly points of failure.

Most modern electronic components have a distinctive “bathtub” curve that represents their failure characteristics, as shown in Figure 38-1. During the early life of the component (referred to as the “burn-in phase”), it’s more likely to fail; once this initial phase is over, a component’s overall failure rate remains quite low until it reaches the end of its useful life, when the failure rate increases again.

![Bathtub Curve](image)

**Figure 38-1**  The normal statistical failure rates for mechanical and electronic components: a characteristic “bathtub” curve

The typical commodity hard disk of 10 years ago had an MTTF on the order of three years. Today, a typical MTTF for a commodity hard disk is more likely to be 35 to 50 years, with MTTF ratings of server-oriented hard drives hitting 134 years! At least part of that
difference is a direct result of counting only the portion of the curve in the normal aging section while taking externally caused failure out of the equation. Therefore, a hard disk that fails because of a power spike that wasn’t properly filtered doesn’t count against the MTTF of the disk, nor does a disk that fails in its first week or two. This might be nice for the disk manufacturer’s statistics, but it doesn’t do much for the system administrator whose system has crashed because of a disk failure. As you can see, it’s important to look at the total picture and carefully evaluate all the factors and failure points on your system. Only by looking at the whole system, including the recovery procedures and methodology, can you build a truly fault-tolerant system.

### Protecting the Power Supply

The single biggest failure point for any network is its power supply. If you don’t have power, you can’t run your computers. It seems pretty obvious, and most of us slap an uninterruptible power supply (UPS) on the order when we’re buying a new server, or we at least make sure that the current UPS can handle the extra load. However, this barely scratches the surface of what you can and should do to protect your network from power problems. You need to protect your network from four basic types of power problems:

- **Local power supply failure**  Failure of the internal power supply on a server, router, or other network component
- **Voltage variations**  Spikes, surges, sags, and longer term brownouts
- **Short-term power outages**  External power failures lasting from fractions of a second to several minutes
- **Long-term power outages**  External power failures lasting from several minutes to several hours or even days

Each type of power problem poses different risks to your network and requires somewhat different protection mechanisms. The level of threat that each poses to your environment varies depending on the area in which you are located, the quality of power available to you, and the potential loss to your business if your computers are down.

### Local Power Supply Failure

Computer power supplies have made substantial gains in the last 10 years, but they are still one of the greatest risk points. All the power conditioning, uninterruptible power supplies, and external generators in the world won’t help much if your server’s power supply fails. Most servers these days either come with a redundant power supply or have the option of including one. Take the option! The extra cost associated with adding a redundant power supply to a server or critical piece of network hardware is far less than the cost of downtime should the power supply fail.
If your server, router, or other piece of network hardware doesn’t have the option of a redundant power supply, order a spare power supply for it when you order the original hardware. Don’t count on the hardware manufacturer’s “4-hour response” time, especially when you consider the cost to your business even if they actually repair the equipment in 4 hours. If you have a spare power supply in a well-marked cabinet where you can find it, you can quickly, and with minimal disruption, replace the failed power supply and return the equipment to full functionality. Then you can afford to wait patiently for the manufacturer’s service response.

**Real World  It’s Only Useful if You Can Find It!**

Having a good supply of critical spares is a great idea, but sometimes reality intrudes. Storage can be the weak link here. Most server rooms are not nearly as spacious as administrators would like them to be, and all too often the spare parts end up jammed into a bin with inadequate identification. If your network is down and you need a power supply to get it back up, you don’t want to be pawing through a jumble of spare parts looking for the right power supply.

Make every effort to develop a single, central, secure location for all spare parts. Then make sure the manufacturer’s part number is visible, and clearly label the machine or machines each part is for. Finally, keep a master list of the spare parts you have and where they are located. It does you no good to have a spare power supply if you can’t find it or don’t know you have it.

Finally, practice! If you’ve never replaced a power supply before, and you don’t have clear and detailed instructions, it will take you orders of magnitude longer to replace it when your mail server is down and everyone is yelling and the phone keeps ringing. By practicing the replacement of the power supplies in your critical hardware, you’ll save time and reduce the stress involved. Document the steps you need to perform and include well-illustrated and detailed instructions on how to replace the power supplies of your critical hardware as part of your disaster recovery standard operating procedures. If you can change the power supply in a very short time, the cost of having it fail diminishes significantly. If you have to wait for your original equipment supplier to get a replacement to you, even if you’re on a 4-hour response service contract, the cost can be much higher than the cost of keeping a spare around.

**Voltage Variations**

Even in areas with exceptionally clean power that is always available, the power that is supplied to your network inevitably fluctuates. Minor, short-term variations merely stress your electronic components, but major variations can literally fry them. You should
never, ever simply plug your computer into an ordinary wall socket without providing some sort of protection against voltage variations. The following sections describe the types of variations and the best way to protect your equipment against them.

**Spikes**

Spikes are large but short-lived increases in voltage. They can occur because of external factors, such as lightning striking a power line, or because of internal factors, such as a large motor starting. The most common causes of severe voltage spikes, however, are external and outside your control. The effects can be devastating. A nearby lightning strike can easily cause a spike of 1000 volts or more to be sent into equipment designed to run on 110 to 120 volts. Few, if any, electronic components are designed to withstand large voltage spikes of several thousand volts, and almost all will suffer damage if they’re not protected from them.

Protection from spikes comes in many forms, from the $19.99 (U.S.) power strip with built-in surge protection that you can buy at your local hardware store to complicated arrays of transformers and specialized sacrificial transistors that are designed to die so that others may live. Unfortunately, those $19.95 power strips just aren’t good enough. They are better than nothing, but barely, because they have a limited ability to withstand really large spikes.

More specialized (and more expensive, of course) surge protectors that are specifically designed to protect computer networks are available from various companies. They differ in their ability to protect against really large spikes and in their cost. There’s a fairly direct correlation between the cost of these products and their rated capacity and speed of action within any company’s range of products, but the cost for a given level of protection can differ significantly from company to company. As always, if the price sounds too good to be true, it is.

In general, these surge protectors are designed to work by sensing a large increase in voltage and creating an alternate electrical path for that excessive voltage that doesn’t allow it to get through to your server. In the most severe spikes, the surge protectors should destroy themselves before allowing the voltage to get through to your server. The effectiveness of these stand-alone surge protectors depends on the speed of response to a large voltage increase and the mechanism of failure when their capacity is exceeded. If the surge protector doesn’t respond quickly enough to a spike, bad things will happen.

Many newer UPSs also provide protection from spikes. They have built-in surge protectors, plus isolation circuitry that tends to buffer the effects of spikes. The effectiveness of the spike protection in a UPS is not directly related to its cost, however—the overall cost of the UPS is more a factor of its effectiveness as an alternative power source. Your responsibility is to read the fine print and understand the limitations of the surge protection a given UPS offers. Also remember that just as with simple surge protectors, large voltage
spikes can cause the surge protection to self-destruct rather than allow the voltage through to your server. That’s the good news; the bad news is that instead of having to replace just a surge protector, you’re likely to have to repair or replace the UPS.

Finally, one other spike protection mechanism can be helpful—the constant voltage transformer. You’re not likely to see one unless you’re in a large industrial setting, but they are often considered to be a sufficient replacement for other forms of surge protection. Unfortunately, they’re not really optimal for surge protection. They do filter some excess voltage, but a large spike is likely to find its way through. However, in combination with either a fully protected UPS or a good stand-alone surge protector, a constant voltage transformer can be quite effective. They also provide additional protection against other forms of voltage variation that surge protectors alone can’t begin to manage.

**Surges**

Voltage surges and spikes are often discussed interchangeably, but we’d like to make a distinction here. For our purposes, a surge lasts longer than most spikes and isn’t nearly as large. Most surges last a few hundred milliseconds and are rarely over 1000 volts. They can be caused by many of the same factors that cause voltage spikes.

Providing protection against surges is somewhat easier than protecting against large spikes. Most of the protection mechanisms just discussed also adequately handle surges. In addition, most constant voltage transformers are sufficient to handle surges and might even handle them better if the surge is so prolonged that it threatens to overheat and burn out a simple surge protector.

**Sags**

Voltage sags are short-term reductions in the voltage delivered. They aren’t complete voltage failures or power outages and are shorter than a full-scale brownout. Voltage sags can drop the voltage well below 100 volts on a 110- to 120-volt normal line and cause most servers to reboot if protection isn’t provided.

Stand-alone surge protectors provide no defense against sags. You need a UPS or a very good constant voltage transformer to prevent damage from a voltage sag. Severe sags can overcome the rating of all but the best constant voltage transformers, so you generally shouldn’t use constant voltage transformers as the sole protection against sags. A UPS, with its battery power supply, is an essential part of your protection from problems caused by voltage sag.

**Brownouts**

A brownout is a planned, deliberate reduction in voltage from your electric utility company. Brownouts most often occur in the heat of the summer and are designed to protect the utility company from overloading. They are not designed to protect the consumer, however.
In general, a brownout reduces the available voltage by 5 to 20 percent from the normal value. A constant voltage transformer or a UPS provides excellent protection against brownouts, within limits. Prolonged brownouts might exceed your UPS’s ability to maintain a charge at the same time that it is providing power at the correct voltage to your equipment. Monitor the health of your UPS carefully during a brownout, especially because the risk of a complete power outage increases if the power company’s voltage reduction strategy proves insufficient.

The best protection against extended brownouts is a constant voltage transformer of sufficient rating to fully support your critical network devices and servers. This transformer takes the reduced voltage provided by your power company and increases it to the rated output voltage. A good constant voltage transformer can handle most brownouts for an extended time without problems, but you should still supplement the constant voltage transformer with a quality UPS and surge protection between the transformer and the server or network device. This extra protection is especially important while the power company is attempting to restore power to full voltage because during this period you run a higher risk of experiencing power and voltage fluctuations.

**Short-Term Power Outages**

Short-term power outages last from a few milliseconds to a few minutes. They can be caused by either internal or external events, but you can rarely plan for them even if they are internal. A server that is unprotected from a short-term power outage will, at the minimum, reboot or, at the worst, fail catastrophically.

You can best protect against a short-term power outage by using a UPS in combination with high-quality spike protection. Be aware that many momentary interruptions of power are accompanied by large spikes when the power is restored. Further, a series of short-term power outages often occur consecutively, causing additional stress to electronic components.

**Long-Term Power Outages**

Long-term power outages, lasting from an hour or so to several days, are usually accompanied by other, more serious problems. Long-term power outages can be caused by storms, earthquakes, fires, and the incompetence of electric power utilities, among other things. As such, plans for dealing with long-term power outages should be part of an overall disaster recovery plan. (See Chapter 36 for more on disaster planning.)

Protection against long-term power outages really becomes a decision about how long you want or need to function if all power is out. If you need to function long enough to be able to gracefully shut down your network, a simple UPS or a collection of them will be sufficient, assuming that you’ve sized the UPS correctly. However, if you need to be sure that you can maintain the full functionality of your Windows Server 2003 network
during an extended power outage, you're going to need a combination of one or more UPSs and an auxiliary generator.

If your situation requires an auxiliary generator to supplement your UPSs, you should carefully plan your power strategy to ensure that you provide power to all the equipment that the network will require in the event of a long-term power outage. Test your solution to make sure you didn't miss anything! Further, you should regularly test the effectiveness of your disaster recovery plans and make sure that all key personnel know how to start the auxiliary generator manually in the event it doesn’t start automatically.

Finally, you should have a regular preventive maintenance program in place that services and tests the generator and ensures that it is ready and functioning when you need it. This preventative maintenance program should include both static tests and full load tests on a regular basis, and it should also call for periodically replacing the fuel to the generator. One of the best ways to do all this is to plan and execute a “disaster day,” where your entire disaster recovery plan is tested in as close to real-world conditions as possible, including running your entire operation from the backup generator.

### Disk Arrays

The most common hardware malfunction is probably a hard disk failure. Even though hard disks have become more reliable over time, they are still subject to failure, especially during their first month or so of use. They are also vulnerable to both catastrophic and degenerative failures caused by power problems. Fortunately, disk arrays have become the norm for most servers, and good fault-tolerant RAID systems are available in Windows Server 2003 and RAID-specific hardware supported by Windows Server 2003. The choice of software or hardware RAID, and the particulars of how you configure your RAID system, can significantly affect the cost of your servers. To make an informed choice for your environment and needs, you must understand the trade-offs and the differences in fault tolerance, speed, configurability, and so on.

### Hardware vs. Software

RAID can be implemented at the hardware level, using RAID controllers, or at the software level, either by the operating system or by a third-party add-on. Windows Server 2003 supports both hardware RAID and its own software RAID.

Hardware RAID implementations require specialized controllers and cost significantly more than an equal level of software RAID. However, for that extra price, you get a faster, more flexible, and more fault-tolerant RAID. When compared to the software RAID provided in Windows Server 2003, a good hardware RAID controller supports more levels of
RAID, on-the-fly reconfiguration of the arrays, hot-swap and hot-spare drives (discussed later in this chapter), and dedicated caching of both reads and writes.

Implementing software RAID in Windows Server 2003 requires that you first convert your disks to dynamic disks. That means your disks will no longer be locally available to other operating systems, although this really shouldn’t be a problem in a production environment since dual-boot is rarely used there. However, you should consider carefully whether you want to convert your boot disk to a dynamic disk. Dynamic disks can be more difficult to access if a problem occurs, and the Windows Server 2003 setup and installation program provides only limited support. For maximum fault tolerance, we recommend using hardware mirroring (RAID 1) on your boot drive; if you do use software mirroring, make sure that you create the required fault-tolerant boot floppy disk and test it thoroughly before you need it. (See Chapter 36.)

**RAID Levels for Fault Tolerance**

Except for level 0, RAID is a mechanism for storing sufficient information on a group of hard disks such that even if one hard disk in the group fails, no information is lost. Some RAID arrangements go even further, providing protection in the event of multiple hard disk failures. The more common levels of RAID and their appropriateness in a fault-tolerant environment are shown in Table 38-1.

<table>
<thead>
<tr>
<th>Level</th>
<th>Number of Disks*</th>
<th>Speed</th>
<th>Fault Tolerance</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$N$</td>
<td>+++</td>
<td>- - -</td>
<td>Stripping alone. Not fault-tolerant—it actually increases your risk of failure—but does provide for the fastest read and write performance.</td>
</tr>
<tr>
<td>1</td>
<td>$2N$</td>
<td>+</td>
<td>++</td>
<td>Mirror or duplex. Slightly faster read than single disk, but no gain during write operations. Failure of any single disk causes no loss in data and minimal performance hit.</td>
</tr>
<tr>
<td>3</td>
<td>$N+1$</td>
<td>++</td>
<td>+</td>
<td>Byte-level parity. Data is striped across multiple drives at the byte level with the parity information written to a single dedicated drive. Reads are much faster than with a single disk, but writes operate slightly slower than a single disk because parity information must be generated and written to a single disk. Failure of any single disk causes no loss of data but can cause a significant loss of performance.</td>
</tr>
</tbody>
</table>
When choosing the RAID level to use for a given application or server, consider the following factors:

- **Intended use**  Will this application be primarily read intensive, such as file serving, or will it be predominantly write intensive, such as a transactional database?
- **Fault tolerance**  How critical is this data, and how much can you afford to lose?
- **Availability**  Does this server or application need to be available at all times, or can you afford to be able to reboot it or otherwise take it offline for brief periods?
- **Performance**  Is this application or server heavily used, with large amounts of data being transferred to and from it, or is this server or application less I/O intensive?
- **Cost**  Are you on a tight budget for this server or application, or is the cost of data loss or unavailability the primary driving factor?

You need to evaluate each of these factors when you decide which type of RAID to use for a server or portion of a server. No single answer fits all cases, but the final answer requires you to carefully weigh each of these factors and balance them against your situation and

---

### Table 38-1  RAID levels and their fault tolerance

<table>
<thead>
<tr>
<th>Level</th>
<th>Number of Disks*</th>
<th>Speed</th>
<th>Fault Tolerance</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>( N+1 )</td>
<td>++</td>
<td>+</td>
<td>Block-level parity with a dedicated parity disk. Similar to RAID-3 except that data is striped at the block level.</td>
</tr>
<tr>
<td>5</td>
<td>( N+1 )</td>
<td>+</td>
<td>++</td>
<td>Interleaved block-level parity. Parity information is distributed across all drives. Reads are much faster than a single disk but writes are significantly slower. Failure of any single disk provides no loss of data but results in a major reduction in performance.</td>
</tr>
<tr>
<td>0+1 and 10</td>
<td>( 2N )</td>
<td>+++</td>
<td>++</td>
<td>Striped mirrored disks or mirrored striped disks. Data is striped across multiple mirrored disks or multiple striped disks are mirrored. Failure of any one disk causes no data loss and no speed loss. Failure of a second disk could result in data loss. Faster than a single disk for both reads and writes.</td>
</tr>
<tr>
<td>Other</td>
<td>Varies</td>
<td>+++</td>
<td>+++</td>
<td>Array of RAID arrays. Different hardware vendors have different proprietary names for this RAID concept. Excellent read and write performance. Failure of any one disk results in no loss of performance and continued redundancy.</td>
</tr>
</tbody>
</table>

*In the Number of Disks column, \( N \) refers to the number of hard disks required to hold the original copy of the data. The plus and minus symbols show relative improvement or deterioration compared to a system using no version of RAID. The scale peaks at three symbols.*
your needs. The following sections take a closer look at each factor and how it weighs in the overall decision-making process.

**Intended Use**

The intended use, and the kind of disk access associated with that use, plays an important role in determining the best RAID level for your application. Think about how write intensive the application is and whether the manner in which the application uses the data is more sequential or random. Is your application a three-square-meals-a-day kind of application, with relatively large chunks of data being read or written at the same time, or is it more of a grazer or nibbler, reading and writing little bits of data from all sorts of different places?

If your application is relatively write intensive, you’ll want to avoid software RAID if possible and avoid RAID-5 if other considerations don’t force you to use it. With RAID-5, any application that requires more than 50 percent writes to reads is likely to be at least somewhat slower, if not much slower, than it would be on a single disk. You can mitigate this to some extent by using more but smaller drives in your array and by using a hardware controller with a large cache to offload the parity processing as much as possible. RAID-1, in either a mirror or duplex configuration, provides a high degree of fault tolerance with no significant penalty during write operations—a good choice for the Windows Server 2003 system disk.

**Note**  Mirroring won’t protect you from data corruption caused by a catastrophic power interruption to a write cached system disk. Disabling write caching on boot and system volumes can is highly recommended if your system isn’t protected by a UPS. And no UPS can protect you from tripping over the power cord. A good, battery-backed cache, however, will protect you even then.

If your application is primarily read intensive, and the data is stored and referenced sequentially, RAID-3 or RAID-4 might be a good choice. Because the data is striped across many drives, you have parallel access to it, improving your throughput. And because the parity information is stored on a single drive rather than dispersed across the array, sequential read operations don’t have to skip over the parity information and are therefore faster. However, write operations are substantially slower, and the single parity drive can become an I/O bottleneck during write operations.

If your application is primarily read-intensive and not necessarily sequential, RAID-5 is an obvious choice. It provides a good balance of speed and fault tolerance, and the cost is substantially lower than the cost of RAID-1. Disk accesses are evenly distributed across multiple drives, and no one drive has the potential to be an I/O bottleneck. However, writes require calculation of the parity information and the extra write of that parity, slowing write operations down significantly.

If your application provides other mechanisms for data recovery or uses large amounts of temporary storage, which doesn’t require fault tolerance, a simple RAID-0, with no fault tolerance but fast reads and writes, is a possibility.
Fault Tolerance

Carefully examine the fault tolerance of each of the possible RAID choices for your intended use. All RAID levels except RAID-0 provide some degree of fault tolerance, but the effect of a failure and the ability to recover from subsequent failures can be different.

If a drive in a RAID-1 mirror or duplex array fails, a full, complete, exact copy of the data remains. Access to your data or application is unimpeded, and performance degradation is minimal, although you do lose the benefit gained on read operations of being able to read from either disk. Until the failed disk is replaced, however, you have no fault tolerance on the remaining disk. Once you replace the failed disk, overall performance is significantly reduced while the new disk is initialized and the mirror is rebuilt.

In a RAID-3 or RAID-4 array, if one of the data disks fails, a significant performance degradation occurs because the missing data needs to be reconstructed from the parity information. Also, you'll have no fault tolerance until the failed disk is replaced. If it is the parity disk that fails, you'll have no fault tolerance until it is replaced, but also no performance degradation. Once you replace the failed disk, overall performance is significantly reduced while the new disk is initialized and the parity information or data is rebuilt.

In a RAID-5 array, the loss of any disk results in a significant performance degradation, and your fault tolerance will be gone until you replace the failed disk. Once you replace the disk, you won't return to fault tolerance until the entire array has a chance to rebuild itself, and performance is seriously degraded during the rebuild process.

RAID systems that are arrays of arrays can provide for multiple failure tolerance. These arrays provide for multiple levels of redundancy and are appropriate for mission-critical applications that must be able to withstand the failure of more than one drive in an array.

Real World  Multiple Disk Controllers Provide Increased Fault Tolerance

Spending the money for a hardware RAID system increases your overall fault tolerance, but it can still leave a single point of failure in your disk subsystem: the disk controller itself. Although failures of the disk controller are certainly less common, they do happen. Many hardware RAID systems are based on a single multiple-channel controller—certainly a better choice than those based on a single-channel controller—but an even better solution is a RAID system based on multiple identical controllers. In these systems, the failure of a single disk controller is not catastrophic but simply an annoyance. In RAID-1, this technique is known as duplexing, but it is also common with many of the proprietary arrays of arrays that are available from server vendors and in the third-party market.
Availability
All levels of RAID, except RAID-0, provide higher availability than a single drive. However, if availability is expanded to also include the overall performance level during failure mode, some RAID levels provide definite advantages over others. Specifically, RAID-1, mirroring/duplexing, provides enhanced availability when compared to RAID levels 3, 4, and 5 during failure mode. There is minimal performance degradation when compared to a single disk if one half of a mirror fails, whereas a RAID-5 array has substantially compromised performance until the failed disk is replaced and the array is rebuilt.

In addition, RAID systems that are based on an array of arrays can provide higher availability than RAID levels 1 through 5. Running on multiple controllers, these arrays are able to tolerate the failure of more than one disk and the failure of one of the controllers, providing protection against the single point of failure inherent in any single-controller arrangement. RAID-1 that uses duplexed disks running on different controllers—as opposed to RAID-1 that uses mirroring on the same controller—also provides this additional protection and improved availability.

Hot-swap drives and hot-spare drives (discussed later in this chapter) can further improve availability in critical environments; this is especially true for hot-spare drives. By providing for automatic failover and rebuilding, they can reduce your exposure to catastrophic failure and provide for maximum availability.

Performance
The relative performance of each RAID level depends on the intended use. The best compromise for many situations is arguably RAID-5, but you should be suspicious of that compromise if your application is fairly write intensive. Especially for relational database data and index files where the database is moderately or highly write intensive, the performance hit of using RAID-5 can be substantial. A better alternative is to use RAID-0+1 or RAID10.

Whatever level of RAID you choose for your particular application, it will benefit from using more small disks rather than a few large disks. The more drives contributing to the stripe of the array, the greater the benefit of parallel reading and writing you'll be able to realize—and your array's overall speed will improve.

Cost
The delta in cost between RAID configurations is primarily the cost of drives, potentially including the cost of additional array enclosures because more drives are required for a particular level of RAID. RAID-1, either duplexing or mirroring, is the most expensive of the conventional RAID levels, because it requires at least 33 percent more raw disk space for a given amount of net storage space than other RAID levels.
Another consideration is that RAID levels that include mirroring or duplexing must use drives in pairs. Therefore, it’s more difficult (and more expensive) to add on to an array if you need additional space on the array. A net 36-GB RAID-0+1 array, comprising four 18-GB drives, requires four more 18-GB drives to double in size, a somewhat daunting prospect if your array cabinet has bays for only six drives, for example. A net 36-GB RAID-5 array of three 18-GB drives, however, can be doubled in size simply by adding two more 18-GB drives, for a total of five drives.

**Hot-Swap and Hot-Spare Disk Systems**

Hardware RAID systems can provide for both hot-swap and hot-spare capabilities. A hot-swap disk system allows failed hard disks to be removed and a replacement disk inserted into the array without powering down the system or rebooting the server. When the new disk is inserted, it is automatically recognized and either will be automatically configured into the array or can be manually configured into it. Additionally, many hot-swap RAID systems allow you to add hard disks into empty slots dynamically, automatically or manually increasing the size of the RAID volume on the fly without a reboot.

A *hot-spare* RAID configuration uses an additional, preconfigured disk or disks to automatically replace a failed disk. These systems usually don’t support hot-swapped hard disks so that the failed disk can’t be removed until the system can be powered down, but full fault tolerance is maintained by having the hot spare available.

**Distributed File System**

The Distributed File System (DFS) is primarily a method of simplifying the view that users have of the available storage on a network—but it is also, when configured appropriately, a highly fault-tolerant storage mechanism. By configuring your DFS root on a Windows Server 2003 domain controller, you can create a fault-tolerant, replicated, distributed file system that gives you great flexibility while presenting your user community with a cohesive and easy-to-navigate network file system.

When you create a fault-tolerant DFS root on a domain controller and replicate it and the links below it across multiple servers, you create a highly fault-tolerant file system that has the added benefit of distributing the load evenly across the replicated shares, giving you a substantial scalability improvement as well. See Chapter 20 for more on setting up your DFS and ensuring that replication works correctly.
Clustering

Windows Server 2003 supports two different kinds of high availability clustering, either of which can greatly improve your fault tolerance:

- For many TCP/IP-based applications, the Network Load Balancing service provides a simple, “shared nothing,” fault-tolerant application server.
- Server clusters provide a highly available fault-tolerant environment that can run applications, provide network services, and distribute loads. Server clusters are available only with Windows Server 2003, Enterprise Edition, and Windows Server 2003, Datacenter Edition.

Network Load Balancing

The Network Load Balancing service allows TCP/IP-based applications to be spread dynamically across up to 32 servers. If a particular server fails, the load and connections to that server are dynamically balanced to the remaining servers, providing a highly fault-tolerant environment without the need for specialized, shared hardware. Individual servers within the cluster can have different hardware and capabilities, and the overall job of load balancing and failover happens automatically, with each server in the cluster running its own copy of Wlbs.exe, the Network Load Balancing control program.

Server Clusters

Server clusters generally use a shared resource between nodes of the cluster. This resource is generally a shared SCSI or Fibre Channel–attached disk array. Each server in the cluster is connected to the shared resource, and the common database that manages the clustering is stored on this shared disk resource. Nodes in the cluster generally have identical hardware and identical capabilities, although it is technically possible to create a server cluster with dissimilar nodes. Windows Server 2003 supports up to eight node server clusters.

Server clusters provide a highly fault-tolerant and configurable environment for mission-critical services and applications. Applications don’t need to be specially written to be able to take advantage of the fault tolerance of a server cluster, although if the application is written to be clustering aware, it can take advantage of additional controls and features in a failover and fallback scenario.
Summary

Building a highly available and fault-tolerant system requires you to carefully evaluate both your requirements and your resources to eliminate single points of failure within the system. You should evaluate each of the hardware subsystems within the overall system for fault tolerance, and ensure that recovery procedures are clearly understood and practiced to reduce recovery time in the event of a failure. Uninterruptible power supplies, RAID systems, distributed file systems, and clustering are all methods for improving fault tolerance. In the next chapter, we discuss the registry: what it is, how it’s structured, and how to back it up and restore it.
Chapter 39

Using the Registry

Introducing the Registry .......................................................... 1265
The Origins of the Registry ......................................................... 1265
What Registry Data Is Used For .................................................. 1267
Understanding the Registry’s Structure ................................. 1268
Using the Registry Editors ......................................................... 1279
Backing Up and Restoring the Registry ................................. 1290
Summary .................................................................................. 1292

The registry is a source of fear for many system administrators because it’s the central repository of system configuration settings. Making mistakes while editing the registry can have undesirable consequences, but it’s not so different from using a power saw—or an automobile, for that matter. All-powerful tools cause negative consequences if misused. If you know what you’re doing and take a few simple safety precautions, you can take advantage of a powerful tool—like the registry—without grief.

Introducing the Registry

The registry is a binary database that organizes all of a system’s configuration settings into a hierarchy. Applications, system components, device drivers, and the Microsoft Windows kernel all use the registry to store their own preferences, read them back again, and obtain information about the system’s hardware configuration, current user’s preferences, and default settings that should be used when no predefined settings exist (such as when a new user logs on to the machine for the first time).

The Origins of the Registry

Back in the days of Microsoft Windows 3.1, applications and Windows stored configuration information in .INI files. These files were simple to edit, which was both a blessing and a curse—users could easily make changes when needed, but they could also easily
make changes when they weren’t needed. The proliferation of Windows applications soon meant that machines were littered with dozens of .INI files, each with its own combination of settings—not all of which were documented or even understood by anyone other than the application programmers.

Microsoft Windows NT 3.1 largely eliminated .INI files, replacing them with the registry. Indeed, the Windows NT 3.1 registry has some important features that survived more or less unchanged to Windows Server 2003:

- Registry data is organized by category, so settings that pertain to a single user (like your choice of default wallpaper) are kept separate from settings for other users or the system’s own internal parameters. Each setting is stored as an independent piece of data.

- Registry data is stored in binary database files on disk; the only way to view or edit these files is to use special-purpose tools that call the registry access routines of the Win32 API.

- Each data item in the registry has a data type, like REG_DWORD (a long integer) or REG_SZ (an ASCII string). The system’s registry editors enforce these data types, so you can’t put a string where a number belongs. This restriction helps weed out one class of mistakes—well-intentioned but misinformed attempts to put a round peg into a square hole.

- Like every other object in the system, each registry item has an owner, and it can have its own independent set of security access control lists (ACLs) and auditing controls.

- With appropriate permissions, administrators or programs on one computer can connect to, read, and modify the registries of remote computers.

Some of these features made it into Microsoft Windows 95, Windows 98, and Windows Me, which share the organizing principles of the Windows Server 2003 registry without its security or remote access features. The two operating system families use different internal formats for their registry databases even though their registries look similar to registry-editing tools; their files aren’t interchangeable or interoperable.

Perhaps the most remarkable aspect of the Windows Server 2003 registry is how little it has changed from the Windows NT 4 version. The binary structures used to store the data remain the same, as do the structural underpinnings discussed later in this chapter.
Real World  Being on Your Best Behavior

Microsoft continually warns us that editing the registry is dangerous— is it really, or are they just covering themselves? The answer is somewhere between the two extremes. Because the registry is used by virtually every part of Windows, and because most programmers are lazy when it comes time to write code to check the validity of values that come from the registry, making an improper or ill-advised registry change can certainly harm your machine. Having said that, however, if you’re careful and attentive, you don’t need to be afraid of the registry. A few simple rules will keep you out of trouble:

■ Don’t edit a part of the registry for fun. If you don’t know how a certain change will affect your system, don’t make it unless you can live with the consequences.

■ Be careful about adding new values or keys. Software pays attention only to keys that have names it understands. Adding a new key or value in the hope that some component will recognize it and change its behavior is like adding a new switch labeled “Jet Boost” to your car’s dashboard and expecting it to increase your car’s speed. The exception to this rule is that Microsoft often uses code that can recognize a hidden (or at least under-documented) key and change its behavior accordingly.

■ Maintain a current backup of your system state. Regedit.exe provides import and export functionality particularly suitable for maintaining backups and restoring them when needed. These two features are discussed in the “Importing and Exporting Registry Data” section later in the chapter.

What Registry Data Is Used For

Now that you have a general understanding of what the registry’s data is used for, it’s time to get more specific. Registry data is used in six areas:

■ Registry data is used during setup, installation, configuration, and removal of the operating system itself, of operating system components such as Internet Information Services (IIS) or Certificate Services, and of hardware devices. Any time you see an “Add/Remove Something-or-Other Wizard,” you can bet that registry data is being used.
At boot time, the Windows Server 2003 recognizer (Ntdetect.com) and some associated code in the Windows Server 2003 kernel search for hardware devices and store their findings in a memory-based portion of the registry.

The Windows Server 2003 kernel uses the information gathered at boot time to figure out which device drivers to load and in what order; it also stores information needed by those drivers in the registry.

Device drivers use the data written by the recognizer and the kernel to configure themselves to work with the physical hardware in the machine.

System tools and applications, such as control panels and some MMC snap-ins, read and write configuration data in the registry.

Applications can store their own settings in the registry; in addition, they can read (and possibly write) the data gathered by other software that uses the registry.

Note that during the boot, kernel, and device-driver phases, the system can’t use the disk—until the device drivers are loaded, the system can’t “talk” to the disk. We’ll cover how the system works around this seemingly severe limitation in the “Volatile Keys” section later in the chapter.

### Understanding the Registry’s Structure

In a file system, the root objects are disks, which contain folders and files. A single folder can contain an arbitrary number of other folders and files; each folder or file has a name. By combining the names of the folders that enclose a file, you can construct a path that unambiguously names only one file on the disk, so that `C:\Windows\system32\Mapi32.dll` and `C:\Windows\SysWOW64\Mapi32.dll` are completely separate files, for example.

The registry is organized much like a file system, except that the vocabulary needed to describe it is somewhat different. At the root of the registry structure are the root keys (which can be likened to a disk in a file system). Each root key contains several subkeys (folders); in turn, these subkeys contain other subkeys and values (the registry equivalent of files). Like files, each value has a name that must be unique in the subkey or folder that encloses it; each value also has an associated data type that governs what kind of data it can hold.

Any registry value can be identified by specifying its full path, starting at the root. For example, the path `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange\Security\ObscureWireDataFormat` specifies a particular value in the Security subkey that belongs to Microsoft Exchange Server. Figure 39-1 shows an annotated section of the Windows Server 2003 registry so that you can identify the root keys, subkeys, and values in it.
Under the Hood  64-Bit and 32-Bit Side by Side

A 32-bit version of Windows Server 2003 has the five root keys described here. A 64-bit version of Windows Server 2003 has the same five root keys, but it has a special feature called Registry Redirector. The Registry Redirector presents 32-bit applications with a different view of the registry than a 64-bit application. This enables both 32-bit and 64-bit COM registration and application states to be supported side by side. The following keys are redirected for 32-bit applications:

- HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT \SYSTEMCERTIFICATES
- HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY \SERVICES
- HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES\HCP
- HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT \ENTERPRISECERTIFICATES
- HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\MSMQ
- HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT \CURRENTVERSION\NETWORKCARDS
- HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT \CURRENTVERSION\PROFILELIST
- HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT \CURRENTVERSION\PERFLIB
- HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT \CURRENTVERSION\PRINT
- HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT \CURRENTVERSION\PORTS
- HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS \CURRENTVERSION\CONTROL PANEL\CURSORS\SCHEMES
- HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS \CURRENTVERSION\TELEPHONY\LOCATIONS
- HKEY_LOCAL_MACHINE\SOFTWARE\POLICIES
- HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS \CURRENTVERSION\GROUP POLICY
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS \CURRENTVERSION\POLICIES
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS \CURRENTVERSION\SETUP\OC MANAGER
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\SOFTWARE \MICROSOFT\SHARED TOOLS\MSINFO
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS \CURRENTVERSION\SETUP
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\CTF\TIP
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\CTF \SYSTEMSHARED
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT \CURRENTVERSION\FONTS
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT \CURRENTVERSION\FONTSUBSTITUTES
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT \CURRENTVERSION\FONTDPI
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT \CURRENTVERSION\FONTMAPPER
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\RAS
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\DRIVER SIGNING
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\NON-DRIVER SIGNING
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY \CALAIS\CURRENT
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY \CALAIS\READERS
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT \CURRENTVERSION\TIME ZONE
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\TRANSACTION SERVER
■ HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\DFS
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT \TERMSERVLICENSING

When a 32-bit application accesses one of these keys, it sees a special 32-bit version of it, allowing both 32-bit and 64-bit versions of an application to exist side by side.

Further, for those 32-bit applications that write REG_EXPAND_SZ keys containing %ProgramFiles% to the registry, WOW64 intercepts the write and substitutes “%ProgramFilesx86%”. Thus, if the Program Files directory is on the C drive, “%ProgramFilesx86%” expands to “C:\Program Files (x86)”.


Figure 39-1  The three separate components of a registry value

The Root Keys

When you open the My Computer icon on your desktop, you always see certain items, such as icons that represent the logical disk volumes on your computer. The same is true
of the registry. When you open it with Registry Editor, you always see the same set of root keys. Each root key has a distinct purpose:

- **HKEY_LOCAL_MACHINE (HKLM)** stores all settings that pertain to the local machine. For example, the HARDWARE subkey of HKLM is where the system and its device drivers record and share information about the hardware devices that the system finds at boot time (as well as other Plug-and-Play devices you can add after the system is booted). Applications are supposed to store data here only if it pertains to everyone who uses a machine; for example, a printer driver might store a set of default print settings here and copy them to each new user’s profile when he or she logs on.

- **HKEY_USERS (HKU)** contains one entry for each user who has previously logged on to your computer. Each user’s entry is owned by that user’s account, and it contains the profile settings that were in effect for that user. When you use Group Policy (discussed in Chapter 11), the policy settings you specify are applied to an individual user’s profile here.

- **HKEY_CURRENT_CONFIG (HKCC)** stores information about the system’s current boot configuration. In particular, it contains information about the current set of system services and which devices were present at boot time. This root key is actually a pointer to sections inside HKLM.

- **HKEY_CURRENT_USER (HKCU)** points to the currently logged-on user’s profile inside HKU. Microsoft requires that Windows applications store any user-specific preferences in subkeys under HKCU; for example, HKCU\SOFTWARE\Binary Research\GhostSrv\Settings holds a user’s personal preferences for Symantec’s Ghost product. Another user’s settings for the same product are available in the same key only when that user is logged on.

- **HKEY_CLASSES_ROOT (HKCR)** ties file extensions and OLE class identifiers together; it actually points to HKLM\SOFTWARE\Classes. System components such as Windows Explorer (and Microsoft Internet Explorer, for that matter) use these associations to determine which applications or components to use when opening or creating a particular type of file or data object. Because Windows Server 2003 relies heavily on the Component Object Model (COM), which in turn relies on the object identifiers stored in HKCR, this key and its subkeys are more important than you might think at first.

**Note** In the Windows documentation, Microsoft identifies only two registry root keys: HKLM and HKU. Because HKCU, HKCC, and HKCR are actually pointers to subkeys of HKLM and HKU, this is technically correct, but you might be confused if you’re used to the idea of five separate root keys. To avoid that confusion, the old-style notation is used here.
Real World  HKCR in Windows Server 2003

If you’re upgrading from Windows NT 4, you’ll see a difference in the way Windows Server 2003 uses the HKCR tree. In Windows NT 4 and earlier, the data in HKCR is the same for all users. In some ways, this was a reasonable design decision for Microsoft to make—all users on the machine have access to the same set of installed OLE components and file mappings.

However, one common complaint from administrators whose users have to share machines is that two users’ preferred associations might differ. If one user chooses Firefox as the preferred Web browser, that modifies HKCR; if another user later sets Internet Explorer as the preferred browser at the same machine, that undermines the original choice. More importantly, the ability for users to change these values reduces system security in two ways: it allows users to change associations for other users (increasing the risk of introducing malicious code), and it forces administrators to remove permissions from HKLM\SOFTWARE\Classes, because all users need access to it.

In subsequent server releases, Microsoft changed this. HKCR actually contains data from two sources: the user’s profile (where user-specific customizations are stored) and HKLM\SOFTWARE\Classes, where systemwide settings live. Users can register and unregister COM components, change file associations, and so on without affecting other users. Administrators can adjust permissions on HKLM\SOFTWARE\Classes so that users can’t tamper with the systemwide settings you want them to have. Each user’s unique settings are stored in the Usrclass.dat file, which is treated like its own registry hive. (See the “Where Data Goes on Disk” section later in the chapter for more details about hive files.)

Major Subkeys

Within these root keys, several subkeys are noteworthy. Because each root key has so much information under it, you usually hear these individual subkeys referred to—after all, HKLM\HARDWARE and HKLM\SOFTWARE don’t have much in common except their root key.

HKLM\HARDWARE
The HKLM\HARDWARE subkey stores information about the hardware found in the system. All the values stored here are held only in RAM, not on disk, because of the device-driver ordering problem mentioned earlier. When the hardware recognizer starts,
it enumerates every device it can find, both by walking the system buses and by searching for specific classes of devices such as parallel ports or keyboards. Three major subkeys live under HKLM\HARDWARE:

- The DESCRIPTION subkey contains descriptions of the CPUs, floating-point processors, and multifunction devices in the system. If you are moving directly from Windows NT 4 to Windows Server 2003, you'll see big changes; for example, the CentralProcessor subkey now tracks a number of settings that aren’t present in Windows NT 4. For computers that use multipurpose chipsets such as Intel’s BX series, one of the multifunction devices listed in this key reflects the chipset’s integrated controllers, with separate entries for disk, keyboard, and serial controllers.

- The DEVICEMAP subkey links a specific device to a specific driver. For example, DEVICEMAP\Video has a value named \Device\Video1 that contains a string, which is a pointer to the place where the driver for that video controller stores its parameters.

- The RESOURCEMAP subkey contains three primary subkeys: one for the hardware abstraction layer (HAL) to use when keeping track of the devices it finds, one for the Plug-and-Play Manager to record devices it knows how to handle, and one that reflects the amount of system resources (which is Microsoft-speak for memory and related resources) available on the machine.

Additional subkeys can exist, depending on the configuration of your machine. For example, systems that support the Advanced Configuration Power Interface (ACPI) have an ACPI subkey that contains information about the specific ACPI subfeatures that the computer supports.

HKLM\SAM
Just because Windows Server 2003 includes the Active Directory directory service, don’t assume that no vestiges of the Security Accounts Manager (SAM) have survived. When you create local accounts or groups on a Windows Server 2003 machine, they are stored in HKLM\SAM, just as they were in Windows NT. However, you can’t normally view or change data in this subkey, and it is mostly useful for compatibility with earlier Windows NT code that expects SAM to exist. The programming routines that access SAM data have all been revamped to use Active Directory data when it exists, or SAM when no Active Directory server is present.
Real World  Look, But Don’t Touch!

If you’re feeling adventurous and want to see what’s in HKLM\SAM and HKLM\SECURITY, you can open these keys by running Regedit in the LocalSystem security context. The easiest way to do this is to use the At command to schedule Regedt32 to run in an interactive session. Just schedule it to run a minute or so into the future, like this:

\texttt{at 12:34 /interactive regedt32.exe}

That command tells the system to schedule Regedit to run one minute from now (this being written at 12:33); when it runs, the system scheduler service launches the application, so it runs in the LocalSystem context instead of the context you’re logged on as. Although this is an interesting way to see what’s in these subkeys, be warned of two things. First, you aren’t able to make much sense out of the values in these keys, because they’re intentionally obfuscated. Second, and more importantly, remember that changing any of these values will provoke unintended and probably undesirable consequences. In other words, look, but don’t touch.

HKLM\SECURITY

HKLM\SECURITY contains a lot of security information, as you might expect. Its format is hidden and undocumented, and you can’t do anything in the subkey. However, the system caches logon credentials, policy settings, and shared server secrets in this subkey. The SECURITY\SAM subkey contains a copy of most of the data from HKLM\SAM.

HKLM\SOFTWARE

The HKLM\SOFTWARE subkey serves as the root location for applications and system components to store their machine-wide settings. For example, HKLM\SOFTWARE\Microsoft\EnterpriseCertificates contains keys that hold the certificate trust lists (CTLs) and trusted CA certificates for this machine—individual users’ CTLs and trusted CAs are stored elsewhere. Individual programs, control panels, and the like can create their own subkeys under HKLM\SOFTWARE; the de facto standard is for each vendor to create its own top-level key (for example, HKLM\SOFTWARE\Intel) and then create subentries beneath that key.

The most interesting parts of this subkey are HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion (which stores much of the GUI preference data and is named the same as the corresponding key under Windows 95, Windows 98, and Windows Me) and HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion. This latter subkey was significantly expanded in Windows 2000, adding new keys for automated system recovery
handling, the Encrypting File System, the Security Configuration Editor, Terminal Services, and other goodies. Windows Server 2003, as you’d expect, maintains the Windows 2000 structure.

**HKLM\Software\Wow6432Node**
The HKLM\Software\Wow6432Node is present only on 64-bit versions of Windows. Its function is to provide a separate, 32-bit HKLM\Software subkey that is seen by 32-bit applications. When the registry is accessed by a 32-bit application, the application is redirected to this subkey when it looks for a key or value in HKLM\Software. This enables both 32-bit and 64-bit versions of the same application to co-exist and have different settings and locations.

**HKLM\SYSTEM\CurrentControlSet**
When you boot your server, the last action in the boot phase is to update the registry to reflect which set of controls and services was last used for a successful boot. CurrentControlSet always points to the set of controls actually in use on the system. If you look under HKLM\SYSTEM, you usually see several ControlSetXXX keys. Each ControlSetXXX subkey represents a control set that existed at one time, whether or not it was successfully used to boot. CurrentControlSet is just a pointer to the most recent successful boot set, but because it isn’t easy to determine which set that was, the OS and applications use CurrentControlSet instead.

CurrentControlSet has four subkeys:

- **Control** Contains control information for services and system tools. For example, Control\BackupRestore\KeysNotToRestore contains a list of keys that the Backup Utility shouldn’t restore (including the contents of the Plug-and-Play subkey) when it restores the registry.

- **Enum** Contains one entry for every physical device or pseudo-device that the system can find. For example, Enum\IDE\DiskMaxtor_94098U8 contains information about the system’s IDE disk drive. Because it was present at boot time, it is included in the enumeration list.

- **Hardware Profiles** Contains one entry for each hardware profile defined on a machine. Comparable with the numbering system seen in the HKLM\SYSTEM tree, each profile has a serial number, starting with 0001. HKLM\SYSTEM\Hardware Profiles\Current always points to the profile selected at boot time.

- **Service** Contains one subkey for each installed service. These subkeys, in turn, hold all the configuration information that the service needs. The exact set of subkeys on two machines are different if they have different services loaded on them.
Windows Server 2003 dynamic disk volumes (discussed in Chapter 18) are a neat technical achievement and a boon to administrators, but they depend on having information about the current configuration of the logical volumes on disk. Applications (and snap-ins, such as the Disk Management snap-in) get this information from the Logical Volume Manager service; in turn, this service stores its list of mounted and available devices in the MountedDevices subkey.

**How Data Is Stored**

Although programs and services that use the registry don’t have to understand how registry data is stored, administrators do—that way you know where data is stored, how the registry handles different types of data, and which files need to be safeguarded as part of your backups. You don’t need to understand the internal format that the registry tools use, but do understand the basic data types and storage locations.

Each value in the registry (Microsoft calls them *value entries*) has three parts: a name, data type, and actual value. For example, if you see a Microsoft Knowledge Base article that talks about some key—REG_SZ: HKLM\SYSTEM\CurrentControlSet\Services\Replicator\Parameters\GuardTime, for example—you’re seeing a complete definition of a value entry (although it’s always nice to see a full path for values so that you know where to add or remove them).

**Useful Data Types**

Seven data types can be used to store data in the registry. Actually, only two of these types are used for most registry data: REG_DWORD and REG_SZ. The seven types are as follows:

- REG_BINARY stores arbitrary binary data in raw form, without any reformatting or parsing. You can view binary data in binary or hex forms by using one of the Windows Server 2003 registry editors (described later in the chapter).

- REG_DWORD stores a 4-byte integer (or double word) value. This data type is usually used when a value indicates a count or interval, but it’s also common to see REG_DWORD flags—0 means the flag is off, and 1 means it’s on.

- REG_SZ is an ordinary Unicode string. These strings can be of any length. This data type is usually used to store paths, human-readable messages or device names, and so on.

- REG_EXPAND_SZ is a REG_SZ with a twist—applications can embed a special token in the string and then expand the token when they read the value from the registry. The token is a variable name framed by the % character. For example, Something is a REG_EXPAND_SZ whose normal value is %SystemRoot%\System32\Something. When Windows Server 2003 reads the string, it expands %SystemRoot% to the full path where the operating system is installed.
■ REG_MULTI_SZ is a collection of an arbitrary number of REG_SZ values. For example, the list of DNS servers you specify in the TCP/IP Properties dialog box is stored in a REG_MULTI_SZ value. Applications must know how to pick apart a single REG_MULTI_SZ into its component parts.

■ REG_FULL_RESOURCE_DESCRIPTOR is a rare bird; it is used to encode information about the system resources required by a particular device. We’ve never seen it appear outside the subkeys of HKLM\HARDWARE.

■ REG_NONE is just a placeholder. It is used to indicate that a registry value exists but doesn’t contain any actual data. Some components look for the presence or absence of a specified key or value to control their behavior at run time; it’s common for those components to look for an item of type REG_NONE—because this type doesn’t hold any data, users can’t mess these values up.

In day-to-day administration, what you need to know about these data types is mostly restricted to understanding the difference between REG_DWORD and REG_SZ values. A REG_DWORD value whose contents are 0 (the numeric value for zero) is different from a REG_SZ whose contents are “0” (the character “0”). If you need to add a new registry value (perhaps because a Microsoft Knowledge Base article recommends doing so), you have to ensure you get the type right, or you might have problems with the components that use the value.

Volatile Keys
Some registry keys and values are volatile, in the original sense of the word—they aren’t persistent and can evaporate at any moment. As an example, none of the data in HKLM\HARDWARE exists anywhere on disk; that entire subkey and all its contents reside entirely in memory. Every time you boot a Windows Server 2003 machine, that subkey is created anew, and when you shut it down, its contents disappear.

Disk-Based Keys
Volatile keys are useful for data that doesn’t need to stay around between reboots, but most of the data stored in the registry would be pretty useless if it weren’t persistent. Imagine having to reconfigure all your preferences and settings after every reboot of your desktop machine—that would get old fast. The majority of registry keys are disk-based, meaning that their contents are held in structures on disk. When a key’s contents are updated, the version on disk is updated too.

Even though disk-based keys are eventually stored on disk, Windows Server 2003 maps them into the paged memory pool (an area of memory whose contents can be written to the pagefile when not being used) to provide more efficient access. The registry size limit, discussed later in this chapter, regulates how much registry data can be stored in the paged pool.
Where Data Goes on Disk
Microsoft uses the term “hive” to refer to a group of keys and values that belong together. A hive can be a root key, or it can be a subkey; for example, HKCC is a hive (even though it’s just a pointer to part of HKLM), and so is HKLM\SAM. The important concept to remember about hives is that a hive is a self-contained unit that can be loaded and unloaded independently of other hives.

Windows Server 2003 uses seven hives: DEFAULT (corresponding to HKU\.DEFAULT), SAM (HKLM\SAM), SECURITY (HKLM\SECURITY), SOFTWARE (HKLM\SOFTWARE), and SYSTEM (HKLM\SYSTEM). The sixth hive, which corresponds to the contents of HKCU, is better known as a user profile—a user profile is just a hive that is loaded into the registry when the user logs on and unloaded at logout. The final hive is HKEY_CURRENT_CONFIG, which was discussed previously.

Each hive exists in its own set of files on disk (with the files having the same names as the hives), along with a separate log file that acts as a journal of all changes made to that hive. (The only exception to this is HKEY_CURRENT_CONFIG, whose data is held with the HKLM\SYSTEM data in the files System and System.log. Hive files don’t have extensions, and the system keeps them open all the time—that’s why you have to use a special-purpose backup tool such as the Backup Utility to back them up.

So, where do these hive files live? As with so many other Windows Server 2003–related questions, the answer is a hearty “It depends.” In this case, the answer depends on which hives you’re talking about. The big five (DEFAULT, SAM, SECURITY, SOFTWARE, and SYSTEM), along with their .LOG files, are stored in the System32\Config subfolder of the %windir%.

The location of the user profile files (Ntuser.dat and Ntuser.dat.log for the logged-on user, Default and Default.log for the default user) depends on which operating system was on the machine before Windows Server 2003. Machines that were originally upgraded from Windows NT 4 keep these profiles in the Profiles\Username subfolder of the system root folder. (Each user has his or her own subfolder.) For machines with a fresh installation or that were upgraded from Windows 95 or Windows 98, profiles are stored in a folder named for the user in the systemdrive\Documents and Settings\username folder.

Using the Registry Editors
On occasions when you need to change values in the registry, you have to use some kind of registry editor. Many of the settings you can change with Control Panel items, Group Policy objects, or MMC snap-ins are actually stored in the registry, so you can think of
these utilities as a kind of registry editor. Another kind is the custom-written script you use to make a specific change, perhaps as part of a logon script or a file you distribute to your users. However, most of the time when you need to make a change directly to the registry, you use one of the provided Windows registry editing utilities.

There are two primary tools you can use to edit your registry. You can always configure items in the MMC snap-ins, but for most changes you make, you’ll probably choose the Registry Editor (Regedit.exe) or the command-line utility Reg.

**Real World  What Happened to Regedt32?**

If you are moving from a previous Microsoft server operating system, you probably noticed that when you run Regedt32.exe in Windows Server 2003, it starts Regedit.exe. Now, it’s just a placeholder; the old Regedt32.exe has been removed.

Regedt32.exe was developed early in the life of Windows NT, and it reflected the Microsoft design standards of the day. Since Windows 95 was released, development of multiple document interface (MDI) applications has been frowned upon, and Microsoft has finally removed one of the last remaining applications—Regedt32.exe—of that type.

When Regedt32 was still a part of Windows, there were some things you couldn’t do in Regedit.exe. It was clear both tools were needed. The missing functionality available in Regedt32 only (such as key security settings) has been rolled into Regedit. Now all your editing needs are satisfied in a single application.

**A Whirlwind Tour of the Registry Editor**

As a user of Windows Explorer (or any version of Windows), you already know about 85 percent of what you need to use the Registry Editor. This familiarity is entirely by design—Microsoft has tried to make it an easy-to-use tool by copying the user interface that you’re already familiar with.

The Registry Editor’s main window is shown in Figure 39-2. The important parts of the interface are fairly simple to understand. Notice the following features:

- The tree in the left pane of the Registry Editor window shows all the root keys and subkeys. What you see here depends on which keys and subkeys you expanded.

- The right pane shows the values associated with the selected key in the left pane. Each value is shown with three items: the value name (the name (Default) is used for the unnamed default value every key has), the value’s type, and the value’s contents or data.
The status bar at the bottom of the window shows the full path to the currently selected key. (The Registry Editor can also copy this key’s path to the clipboard for you, thanks to the Copy Key Name command on the Edit menu. This feature is handy when you’re writing a book or otherwise documenting your work.)

Figure 39-2  The Registry Editor user interface

Because these interface features are written with the standard Windows controls, all the keyboard navigation and control shortcuts you’re accustomed to using with Windows Explorer work here. For example, you can jump to a particular key by clicking anywhere in the left pane and typing the first few letters of the key’s name. And you can use the arrow keys to move around in either half of the Registry Editor window.

Note 64-bit versions of Windows Server 2003 include both a 32-bit and 64-bit versions of Regedit.exe. The 32-bit version sees the redirected view of the registry, while the 64-bit version sees the 32-bit sections of the registry as the HKLM\Software\WOW6432node. The default version of regedit is the 64-bit version. You can start the 32-bit version by explicitly running %windir%\Syswow64\regedit.exe.

Searching for Keys and Values
The Find command on the Edit menu in the Registry Editor is worth its weight in gold when you need to find which key, or value, has a specific name or contents. The interface to this function is uncomplicated—as Figure 39-3 shows. Even with the simple interface,
the tool is extremely valuable because it searches the entire registry for a specific value. Here’s how to use the Find dialog box to get what you’re looking for:

- Type the pattern you’re looking for in the Find What box. You can search only for plain ASCII text—no wildcards are allowed. And no expansion of variables are allowed either—so if you search for “%ProgramFiles(x86)\”, it searches for that exact string, not what that variable would expand to. If you’re searching for values, the Registry Editor searches only string values (REG_SZ, REG_EXPAND_SZ, and REG_MULTI_SZ) for the pattern you give.

- Use the options in the Look At box to control where the Registry Editor looks for the specified value. By default, it searches for key names (the Keys check box), value names (the Values check box), and value contents (the Data check box), but you can fine-tune it.

- The Match Whole String Only check box tells the Registry Editor to find the entire search string, not just a portion of it. For example, if you search for “Windows” with this check box selected, the search ignores HKLM\SOFTWARE\Microsoft\Windows NT.

![Figure 39-3  The Registry Editor’s Find dialog box](image)

When you make your selections in the Find dialog box, click Find Next and the Registry Editor begins searching. Eventually, one of two things happens: the Registry Editor either hits the end of the registry (in which case, it tells you it didn’t find any matches), or it finds a match. In the latter case, the match is highlighted. If the match isn’t what you were looking for, the Find Next command on the Edit menu (or F3, its shortcut key) continues the search.

**Editing Value Contents**

The Modify command on the Edit menu lets you change the contents of the selected value entry. (You can also edit a value by selecting it and pressing Enter.) What you see next depends on the type of value you’re editing; separate editor dialog boxes exist for string values, DWORD values, and binary values. The Registry Editor lets you edit data types it doesn’t support, such as REG_FULL_RESOURCE_DESCRIPTOR or REG_MULTI_SZ. For those types, it opens the binary editor dialog box. The editor dialog boxes themselves are straightforward—each presents the current value and lets you edit it. The keyboard shortcuts for the Cut, Copy, and Paste commands work in the editor dialog boxes, too.
Adding and Removing Keys and Values

The Registry Editor also allows you to add and remove keys, subkeys, and individual values. Now is a good time to reiterate the frequent warning from Microsoft: making unnecessary changes to the registry will likely damage your Windows installation. Be careful when you add data, and be doubly careful when you remove it. (See the “Being on Your Best Behavior” sidebar earlier in this chapter for more details about why this is a good idea.) To add a new key as a child of the selected key, open the Edit menu, point to New, and choose Key. The Registry Editor creates a new key and selects its name so that you can set it correctly. (It defaults to New Key #1.)

The new key automatically has an unnamed value attached to it. You can add more values using the five remaining commands on the New submenu: String Value, Binary Value, DWORD Value, Multi-String Value, and Expandable String Value. Note that the Registry Editor can’t create any other data types, and if you create a binary value, components interpret it as raw REG_BINARY data. Creating a new value adds it as a child of the selected key and gives it a default name (New Value #1, New Value #2, and so on), which you can immediately change. When you’re done adding and naming the new values, you can use the standard editor dialog boxes to change their contents to the appropriate values.

Removing values and keys is simple. Select the item you want to zap, and either choose Delete from the Edit menu or just press the Delete key. The Registry Editor asks you to confirm your command; after you confirm it, the value or key is immediately removed. (It’s permanent, unlike most file commands—there’s no undo!)

Importing and Exporting Registry Data

You can import and export registry data from the Registry Editor. The resulting text files are easy to read, and you can safely move them from machine to machine. In fact, the default association for .REG files automatically launches the Registry Editor and loads the contents of the file when you double-click it. The Export Registry File command on the Registry menu lets you save the selected key to a file, and the Import Registry File command does the reverse. Note that importing a registry file from within the Registry Editor happens immediately—a confirmation dialog box appears that tells you whether the import succeeded or not, but you don’t get a chance to stop it. (If you launch a .REG file by clicking it, however, you do get a confirmation dialog box.)

---

Important If you create these .REG files, they appear in the My Recent Documents menu. Inexperienced users on an exploring expedition might run across the files and try to open them. This can cause serious problems that are nearly impossible to correct. Fortunately, this item doesn’t exist on a Windows Server 2003 machine, although it does on client machines such as Windows XP.
Creating Your Own .REG Files

If you need to distribute registry changes to your users, one way to do it is with the policy mechanisms discussed in Chapter 9. However, sometimes using a .REG file makes more sense. For example, sites that don’t have direct access to Active Directory resources can’t receive Group Policy updates. You can easily mail out .REG files and have your users double-click them. (Of course, that creates a potential security problem because anyone can send your users the same kinds of files—make sure to educate them about proper and safe e-mail use.)

The first, and easiest, way to create your own .REG file for distribution is to use the Registry Editor to export the keys and values you want to pass around. As an alternative, you can create your own files using NotePad or any other text editor. Here’s an example:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug]
"Auto"="1"
"Debugger"="drwtsn32 -p %ld -e %ld -g"
"UserDebuggerHotKey"=dword:00000000
```

The first line tells the Registry Editor it’s looking at a .REG file. (The blank line that follows is required, too.) After that, the format is easy to understand: define a key by putting its full path in square brackets, and then follow it with each value you want to import, one per line. Enclose value names and string value contents in straight double quotes. (It is important that you use straight double quotes instead of the “smart quotes” that are inserted by many word-processing systems including Microsoft Office Word.) REG_DWORD values are specified using the DWORD: prefix; they don’t have to be enclosed in quotes. You can bundle multiple keys into the same file, as long as you add a blank line before each key name. Each key can contain any number of values.

One tip: while you’re becoming proficient with .REG files, practice by using a harmless destination path. Create your own key (for example, HKLM\SOFTWARE\Testing123), and import your .REG files under it until you’re sure they make only the changes you want made.
Loading and Unloading Hives
You can load and unload hives for HKEY_USERS and HKEY_LOCAL_MACHINE. On
the File menu, these options are enabled only when one of the two keys is selected. To
either load or unload a hive, you must be a member of the Administrators group or you
must have been given the authority to do so.

To load a hive, click Load Hive on the File menu and navigate to the folder that contains
the hive you want to load. Select it and click Open. Provide a key name and click OK to
save it. To unload a hive, select a hive in the Registry Editor and from the File menu, select
Unload Hive.

Note Loading and unloading hives is done while trying to recover from registry
corruption. Do not do it on a production system that is running and not having
problems.

Connecting to a Remote Machine’s Registry
If you’re logged on with sufficient permissions, you can use the Registry Editor to con-
nect to another computer’s registry and inspect or edit it. To accomplish this voodoo,
your account must have administrative privileges on both the machine on which you’re
running the Registry Editor and the other machine whose registry you want to inspect or
edit, and the remote registry service must be running on the target machine. In addition,
Group Policy settings or Windows Firewall settings might prevent you from gaining
access.

Assuming your credentials are in order, you actually connect to the remote machine by
choosing Connect Network Registry from the File menu. This command lets you browse
your network to find the machine you want to connect to. After you successfully connect,
the computer’s name appears in the left pane on the same level as My Computer. You can
expand its root keys, poke around in the subkeys, search, and modify data to your heart’s
content. When you’re done, choose Disconnect Network Registry from the File menu
and select the computer to disconnect.

Renaming Keys and Values
You can change the name of a key or a value by choosing Rename from the Edit menu. In
most cases, you won’t want or need to do this. Because software looks for specific named
values in the registry, changing the name of one of them is a bad idea. However, when you
add keys or values based on advice from Microsoft Knowledge Base articles, it’s possible
to misspell the name (or, worse yet, to type it correctly but find out that the name in the
Knowledge Base article is wrong!), and the Rename command is your only alternative to
deleting and re-creating the key.
Managing Security on Registry Keys
Regedit allows you to adjust registry key security by selecting a key and choosing the Permissions command from the Edit menu. Everything you learned about setting permissions on files (discussed in Chapter 9) is still true here, and the basic operations work exactly the same way: you select an object and then grant or deny specific privileges to specific users and groups. Figure 39-4 shows an example on a domain controller. Note that five security principles are shown in the Permissions dialog box: Administrators, CREATOR OWNER, Server Operators, SYSTEM, and Authenticated Users. The exact contents you see on your computer varies according to the security template you applied; more restrictive templates might change these permissions significantly.

![Figure 39-4 The standard Permissions dialog box for a registry key](image)

On the Permissions dialog box, you can grant and deny the Full Control, Read, and Special Permissions options on keys. However, in general, don't do so on keys owned by the system—that's why Microsoft includes the security templates. You can easily set permissions accidentally that are so restrictive that software that needs registry access can't get it, or you can easily err in the opposite direction and set permissions that are unnecessarily loose.

Advanced control can be exercised by clicking Advanced, which brings up the Advanced Security Settings dialog box for the key you selected. There are four tabs labeled Permissions, Auditing, Owner, and Effective Permissions.
When you set permissions using the Permissions tab on the Advanced Security Settings dialog box, be sure to note whether you select the Allow Inheritable Permissions From Parent To Propagate To This Object check box. If this check box is selected and you apply new permissions, those permissions are automatically propagated to all subkeys of the selected key. Depending on the level at which you apply these permissions, inheritance might have unintended consequences—if you loosen permissions on a key, you might accidentally loosen permissions on a subkey that should remain secure. Before you change permissions on any keys, be sure to make a good backup of your registry and make a note of the changes you made so that you can reverse them later.

Settings that belong to applications, of course, are another matter altogether. The only way to determine appropriate permissions for most applications’ keys is to tighten them as much as possible, and then gradually relax controls until the application starts working properly. It might not be easy, but it’s effective. The control this method provides is absolute.

Here’s a summary of what the various tab dialog-box items allow you to do:

- The Permissions tab’s View/Edit button allows you to assign more granular permissions to individual users. For example, you can fine-tune who can create new values in a key by adjusting the setting for the Set Value permission. Table 39-1 shows the permissions you can grant or deny. Because most registry keys gain their permissions from inheritance, be aware that you might not be able to make changes here without turning inheritance off.

- The Auditing tab lets you set auditing permissions for the selected key. First, you specify the users or groups whose actions you want to audit; next, you specify which particular actions you want recorded. (See Figure 39-5.) Note that the actions you can audit are the same as the permissions shown in Table 39-1. You can audit successful or failed attempts to exercise these permissions.

- The Owner tab lets you reassign ownership of the selected key, either with or without propagating that change to all subitems beneath it. Note that depending on your security settings, a change in ownership might result in an audit trail being generated.

- The Effective Permissions tab lets you see what permissions would be given to a particular user or group given the current settings.
A Whirlwind Tour of Reg

Reg (Reg.exe) is a utility that allows you to view, edit, or add registry entries from the command line. It’s script-friendly and just as powerful as the Registry Editor, but it doesn’t have the pretty interface. You can use it in batch files, for example, to repeatedly apply changes to your registry.
Using Reg takes a little getting used to if you’re not familiar with the command line. There are a number of options available, and you pass them as parameters to the executable. The format of Reg usage is:

```
reg action [options]
```

where `reg` is the Reg executable, `action` is the Reg command you want to perform, and `options` is the list of command-specific parameters.

The primary commands of Reg are listed in Table 39-2. The return status of the commands is 0 if the command succeeded or 1 if a failure occurred, except where noted.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Adds a new subkey or entry to the registry.</td>
</tr>
</tbody>
</table>
| Compare | Looks at the values for the two specified subkeys or entries, and returns the following:  
0 if the comparison succeeds and there are no differences  
1 if the comparison failed  
2 if the comparison was successful and differences existed |
| Copy    | Copies registry information to a new location in the local or network registry. |
| Delete  | Removes registry information. |
| Export  | Pulls information out of the registry, and writes it to a file. This file can be used to transfer the registry data to other machines using the Import command. |
| Import  | Imports a registry file, and creates and modifies keys specified in the file into the local registry. |
| Load    | Allows you to move registry data to a new position within the registry, enabling you to troubleshoot changes without the threat of doing permanent damage. |
| Query   | Prints all the registry information beneath the specified key. |
| Restore | Restores registry information from a file created by the Save command. |
| Save    | Saves specified registry information in a file. This is useful if you’re planning to edit a key and want to make a backup of it first. |
| Unload  | Removes the registry data that was added with the Load command. |
Backing Up and Restoring the Registry

In Chapter 37 you learned how to use the Backup Utility to back up and restore the overall state of your system. This is somewhat different from Windows NT, where you could easily back up the registry by making an emergency repair disk (ERD) or running Ntbackup and selecting the Include Local Registry check box.

The reason for these differences revolves around Active Directory. In Windows NT, a registry backup contained a copy of the SAM database for the local machine (as well as the domain SAM, when you back up a domain controller). In a network using Active Directory, the directory contains most of the information that was formerly in the SAM, which is why you have to perform a two-step recovery process for domain controllers. (See Chapter 37 for more details about how the process works.) First you restore the local machine’s SAM registry hive so that you can log on, and then you restore the Active Directory store.

Important As a side effect of the way these changes are implemented, the emergency repair disk is no longer called the ERD but the system recovery disk, and contains no registry information—the only backup copy on the computer itself is in the %SystemRoot%\Repair folder. With no ERD to fall back on, it’s especially important to make regular and usable backups.

Choosing a Backup Method

Because the registry is more than an ordinary file, it makes sense that you have to give your backup and restore procedures more than the ordinary amount of thought. You can back up and restore your registry in other ways besides making a complete backup of the entire system state. Of course, still perform regular backups of your data and the system state for each computer you administer. It is still useful to back up the registry by itself, because the registry is where most applications and system components store their preferences and settings.

Backup Utility

When you use the Backup Utility to back up the system state, it includes a complete copy of that machine’s registry. It also includes copies of the system volume (on domain controllers), certificate data, COM+ class registration information, and other information that is unrelated to what is in the registry. On the other hand, the Backup Utility automates the process of backing up the registry, so it’s easy to use and understand. In addition, keeping your registry data with the rest of your server data ensures that you’re able to recover everything without having to hunt for third-party CD-ROMs, drivers, and the like.
Third-Party Products
Many Windows server sites use third-party backup tools. In general, these tools provide more sophisticated backup capabilities than the tools Microsoft ships. If you’re using a third-party backup product, you might want it to back up your registry too. Be sure you have everything on hand that you need to restore data backed up with a third-party tool, and double-check to make sure your vendor’s software is fully compatible with the version of Windows Server 2003 that you’re running.

Do-It-Yourself Backups
Because Regedit allows you to export and import .REG files, you might think you can approximate what the Backup Utility does by manually saving to a hive file the keys you’re most interested in, copying the resulting files someplace safe, and reloading them if you need them. This approach works fine and is most useful when you want to make changes to the registry while preserving a fall-back position, but it’s labor-intensive because there’s no way to automate the process of telling the Registry Editor which keys to save.

Backing Up the Registry
When you’re ready to make a backup, you’ll be happy to see how simple the process is—Microsoft has worked hard to streamline the process.

Using the Backup Utility
Chapter 37 covered the mechanics of backing up and restoring your system state, of which the registry is a small but critical part. If you’re comfortable with the process of making and restoring a system state backup with the Backup Utility, you’re in good shape. However, a quick review might be helpful:

1. Launch the Backup Utility application; when it appears, click Advanced Mode on the Backup Utility Wizard.
2. On the Backup Utility dialog box, click the Backup tab.
3. Specify the backup device or location you want to use with the Backup Destination and Backup Media Or File Name options.
4. If necessary, expand the My Computer icon.
5. Select the System State check box. (Remember, the system state items are interrelated and can’t be backed up individually.)
6. Click Start Backup. When the system backs up the system state information, the registry files are included, so you can restore them later.
Automated System Recovery
Automated System Recovery (ASR) is an indispensable tool when you want to recover from a system failure. Among other things, ASR saves the information required to start your machine, including the registry.

Be sure to use it to back up the system files whenever the operating system changes. When you apply a service pack or change a driver, for example, run the backup portion of the ASR procedure. When a problem happens, you can run the ASR restore and your system startup files are restored.

The ASR backup stores the backup copy of your data on the backup media of your choice and creates a floppy disk used to restore it. To start the backup procedure, click the ASR Wizard item on the Tools menu of the Backup Utility application. Back up your data to the media you want and you’re prompted to create the floppy disk to contain information needed for the restore.

The ASR restoration procedure requires your backup media, the created floppy, and your installation media. Boot off the installation CD-ROM, press the F2 key when prompted, and the ASR process guides you through the restore.

**Note**  Remember, ASR does not back up and restore your data. Refer to Chapter 37 for all the information you need to perform appropriate backups. A good backup routine of both your system data and your system startup information ensures that your recovery from a severe failure will be simple and the downtime resulting from the failure will be minimized.

**Summary**
Windows Server 2003 depends on the registry for storing and retrieving vital configuration data. Knowing what’s in it, how and when to edit the registry, and how to back it up and restore it is vital for system administrators. In particular, knowing how registry-editing utilities work and what they can do is a key skill you need to keep your Windows Server 2003 machines up and running. The next chapter addresses troubleshooting.
Troubleshooting and recovering from problems is one of the most important jobs of an administrator, and one of the most difficult. Chapter 36, Chapter 37, and Chapter 38 can help you prepare for disasters; this chapter can help you triage problems and implement a troubleshooting and recovery plan.

**More Info**  To troubleshoot Windows Setup, see Chapter 5; for problems with hardware devices, see Chapter 7; for printing problems, refer to Chapter 8. Additional help is available at the Microsoft Help and Support center (http://support.microsoft.com), or from Microsoft Product Support Services.

---

**Triaging the Situation**

The first thing to do when a major problem occurs is triage the situation. Use the following list to evaluate the problem and determine what actions to take:

- **Identify priorities**  Identify the most important priorities. If you are in the middle of a hurricane, fire, or other physical danger, safety is the first priority. Protecting the organization’s data is probably the second priority, followed by maintaining the minimum required level of service for the organization and customers.

- **Take steps to prevent further damage**  Disable backup software to avoid overwriting good backups. If the problem involves an attacker or a virus, remove the server from the network immediately.
Set deadlines  Create deadlines to accomplish the goals you identify. If there is physical danger, people could die if you miss a deadline. Missing a deadline in more benign situations can result in lost data or revenue. Revise these deadlines as you gather additional information.

Review relevant procedures  Review any disaster recovery or troubleshooting procedures. (See Chapter 36.) If there are no existing procedures, create simple procedures to help guide troubleshooting.

Identify fallback plans  Part of a disaster recovery procedure is a complete restore or replacement scenario, along with a time estimate for how long this takes and possible effects it will have. Do not spend hours troubleshooting a critical server that you can restore from backup quickly and with minimal repercussions. Also, identify the fallback plan in case all recovery plans fail.

Identify available personnel  Identify who is available to perform troubleshooting or recovery. Use two people when possible for important tasks to reduce the potential for errors, especially during emergencies when it is easier to make mistakes. If the available personnel do not have enough experience performing the task, get outside help.

Identify available physical resources  Identify physical resources such as food, water, bathroom facilities, power, medical supplies, shelter, and security. This is important during physical emergencies but is also relevant during normal conditions—spare computers need power, and personnel need food and access to a restroom without being locked out of the server room.

Identify available hardware and software  Identify what hardware and software resources are available. Use the following list as a guide:

- Servers to take over roles from the affected systems
- Spare servers and parts
- External USB hard drives or spare internal drives
- USB flash drives
- Backup tapes
- Installation CDs, including old versions
- Software licenses and keys

Take stock of available backups  Identify available backups, including disk images, full system backups, data backups, Previous Versions (using the Shadow Copy service), and online backups.
■ **Prepare for changes**  With major disasters, priorities usually change before you are finished recovering. Organization priorities might change, and your own personal priorities might change.

■ **Document relevant actions**  Document the actions you perform so that another administrator can take over if necessary. Taking notes also makes it easier to update procedures with anything you learn from the troubleshooting or recovery process.

■ **Implement the plan**  Do not spend an excessive amount of time triaging—when the triage deadline expires, implement the plan.

---

**Note**  When troubleshooting or recovering from a problem, try to increase the number of recovery options. If a server is failing, create a new backup before troubleshooting it. Do not overwrite an old backup—it might come in handy later, especially for computer forensics. If there is a single backup of important data, write-protect it and make a copy before restoring.

---

**Performing a System Recovery**

This section discusses how to troubleshoot and recover a system that does not start. If the organization has a relevant disaster recovery plan (as described in Chapter 36), follow those procedures. Use this section to supplement the plan as necessary, and take notes about how you can update the plan.

The recovery steps outlined in this section proceed from least drastic to most drastic. In any recovery procedure, always adopt a minimalist approach. To minimize information loss and the impact on the network, start with the least invasive steps.

**Note**  Recovering a domain controller is no different from recovering a normal server, except if you want to restore the Active Directory and the SYSVOL volume from a backup. To do this, start the server using the Directory Services Restore Mode, as described in Chapter 37.

---

**Identifying Possible Causes**

Computers rarely “just fail.” Usually something happens to cause a system to fail. Therefore, the first thing to do is ask what changed between the last time the system started and now.

The following list describes possible causes and the appropriate troubleshooting steps to take for each. Detailed procedures are located later in this chapter.
- **Installing or uninstalling a device or driver** Start Microsoft Windows using the Last Known Good startup option, or start Windows in safe mode and use the Device Driver Rollback Wizard to revert to an older driver.

- **Installing or uninstalling a program or software update** Start Windows using the Last Known Good startup option, or start Windows in safe mode and then uninstall the program.

- **Editing the Registry or changing system settings** Start Windows using safe mode, and edit the relevant system settings. If Windows does not start in safe mode, perform a repair installation or use the Automated System Recovery (ASR) process to restore Windows from a backup. If none of these methods work and you are troubleshooting a computer running Windows XP, see Microsoft Knowledge Base Article 307545 for information about how to recover a corrupted registry using the Recovery Console.

- **Failing hardware** If the computer sounds different or experiences a power outage or other environmental problem, closely check the functioning of all moving devices in the system. Look, listen, or feel for air movement from case fans, power supply fans, and processor fans.

  Boot the system, and verify that the power-on self test (POST) proceeds properly. If the POST fails or does not appear, there is probably a hardware failure with the power supply, RAM, motherboard, display card, or CPU. If the POST succeeds, use a hardware-monitoring tool in the BIOS, Extensible Firmware Interface (EFI), or vendor-provided troubleshooting program to determine whether any devices are failing.

- **Failing hard drive** If the hard drives make unusual clicking sounds (or no sound), or a server with a hardware RAID controller starts beeping loudly, one of the hard drives might be failing. Open the RAID controller software and check the status of the drive, check the Event Viewer for disk-related errors, and use the Chkdsk command to scan the drive.

  **Note** Press F8 when the computer displays the Starting Windows text, and then choose the Enable VGA Mode option to resolve display malfunctions temporarily. After Windows starts, select a more conservative display setting (lower the resolution, refresh rate, or both) or choose a different display driver.

---

**Using the Last Known Good Configuration**

If you suspect a problem with a device driver or hardware-related system setting, start the computer using the Last Known Good Configuration startup option. This option rolls back any new device drivers or changes made to the HKLM\SYSTEM\CurrentControlSet...
subkey since the last time Windows started and a user logged on successfully. If the sys-
tem starts properly but produces an error message, skip to the “Fixing the Underlying
Problem” section of this chapter.

If you know which device driver is causing the problem, start Windows using safe mode
and use the Device Driver Roll Back feature instead of the Last Known Good Configura-
tion to minimize changes. If this does not resolve the problem, try the Last Known Good
Configuration—Windows does not update the Last Known Good Configuration in safe
mode.

To start a computer using the Last Known Good Configuration startup option, follow
these steps:

1. Restart or turn on the computer.
2. If the computer displays a choice of operating systems, select the appropriate Win-
dows installation and then press F8. Otherwise, press F8 when the computer
displays the Starting Windows text (but before any color images are displayed).
3. Choose Last Known Good Configuration, and then press Enter. Windows attempts
to start using the Last Known Good Configuration. If it succeeds, evaluate what
cause the trouble in the first place (probably a new device driver) and then plan
future maintenance of the system accordingly. (Do not use the same driver again.)
If this fails, use the information in the next section to start the computer using safe
mode.

Using Safe Mode

Windows safe mode is a special diagnostic mode that disables all unnecessary services
and drivers, maximizing the chances of starting successfully. Safe mode provides full
access to the system, making it easier to fix the underlying condition.

To boot using the Safe Mode option, use the following procedure:

1. Restart or turn on the computer.
2. If the computer displays a choice of operating systems, select the appropriate Win-
dows installation and then press F8. Otherwise, press F8 when the computer
displays the Starting Windows text (but before any color images are displayed).
3. Choose Safe Mode and then press Enter. Windows attempts to start using safe
mode.

Choose Safe Mode With Networking if the fault does not lie in the networking
subsystem, or Safe Mode With Command Prompt to bypass the Explorer shell and
use a command prompt interface, further increasing the chances of successfully
starting.
4. If Windows starts safe mode successfully, use normal Windows troubleshooting techniques and tools to resolve the underlying problem, as discussed in the “Fixing the Underlying Problem” section of this chapter.

5. If Windows does not start successfully in safe mode, perform the following tasks:
   
a. Use the Last Known Good Configuration startup option.
   
b. Use an antivirus program to rule out viruses.
   
c. Use the Recovery Console to view the boot log file, Ntbtlog.txt (located in the %WINDIR% folder). Scroll to the end of the file to see what driver or service Windows was loading when it failed, and then disable the service or replace the driver files.
   
d. Use the recovery techniques discussed in the rest of this section.

---

**Note** To create a boot log (Ntbtlog.txt), start the computer, press F8 when the computer displays the Starting Windows text, and then choose the Enable Boot Logging option from the Windows Advanced Options menu. Doing so creates a log file with all the drivers and services loaded or failed during the boot process.

---

**Using a Boot Disk to Recover the System**

Using a boot disk is simple—insert the disk and then start the computer. (You might have to change the boot order in the system BIOS as well.) This bypasses the master boot record (MBR), boot sector, and startup environment on the hard drive, and then executes Ntoskrnl.exe from the hard drive, which starts Windows. To create a Windows Server 2003 boot disk, see Chapter 36.

If the system starts properly only when using a boot disk, there is a problem with the Boot.ini file, MBR, boot sector, or Windows startup environment. To correct this, start Windows using the boot disk, edit the Boot.ini file, and replace missing or corrupt Windows files such as Ntldr or Ntdetect.com, as discussed later in this chapter. To fix the MBR or boot sector, use the Recovery Console, as discussed in Appendix D.

If the system does not start when using a boot disk, the operating system or hard disk is probably damaged. Use the Recovery Console to check the hard disk and repair files, or use the procedures discussed in the rest of this section to repair or restore Windows from a backup.
Editing the Boot.ini File

Windows NT, Windows 2000, Windows XP, and Windows Server 2003 all use the Boot.ini text file to control startup options and operating systems. You can manually edit the hidden Boot.ini file using any text editor (by typing `Attrib -R -S -H C:\Boot.ini` first), but the easiest way to edit it is by using the System Configuration Utility (discussed later in this chapter) or the BootC fg command.

To specify a particular boot mode for troubleshooting, append the appropriate options listed in Table 40-1 to the operating system line in the Boot.ini file.

<table>
<thead>
<tr>
<th>Boot Option</th>
<th>Switch to Use in Boot.ini</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe Mode</td>
<td>/Safeboot:Minimal /Sos /Bootlog /Noguiboot</td>
</tr>
<tr>
<td>Safe Mode With Networking</td>
<td>/Safeboot:Network /Sos /Bootlog /Noguiboot</td>
</tr>
<tr>
<td>Safe Mode With Command Prompt</td>
<td>/Safeboot:Minimal(Alternateshell) /SOS /Bootlog /Noguiboot</td>
</tr>
<tr>
<td>Enable Boot Logging</td>
<td>/Bootlog</td>
</tr>
<tr>
<td>Enable VGA Mode</td>
<td>/Basevideo</td>
</tr>
<tr>
<td>Directory Service Restore Mode (domain controllers only)</td>
<td>/Safeboot:Dsrepair /Sos</td>
</tr>
<tr>
<td>Debugging Mode</td>
<td>/Debug</td>
</tr>
</tbody>
</table>

Booting from Mirrored Boot Partitions

If the primary boot drive fails on a system with mirrored boot partitions using software mirroring, the system continues to operate normally until the next restart, at which point the system fails unless the drives and controllers involved in the mirror set are exactly the same (down to the firmware revisions and partitioning schemes).

If a system with a failed mirror set does not boot, create a boot floppy disk using the procedure outlined in Chapter 36, with one additional step. Edit the Boot.ini file on the floppy disk to change the Advanced RISC Computing (ARC) name of the boot partition to point to the secondary mirror drive rather than the primary one. For example, if the system uses a pair of SCSI adapters with duplexed boot drives that use the SCSI BIOS to boot from the primary partition on the first hard disk, the Boot.ini file might include the following line:

```
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows Server 2003" /fastdetect
```
To boot from the secondary drive, change the line to

```
multi(1)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows Server 2003"
/fastdetect
```

After starting the system and replacing the failed drive, re-create the mirror as described in Chapter 18.

---

**More Info**  See Microsoft Knowledge Base Article 167045 for more information about how Windows Server 2003 handles failed mirror sets.

---

### Performing an In-Place Upgrade

Windows Server 2003 includes the ability to perform an in-place upgrade (also called a repair installation), which preserves system and application settings but is otherwise similar to a clean install and takes roughly the same amount of time. This is a good solution for problems that otherwise require a clean install or restoring from an old ASR backup set.

---

**Important**  Performing an in-place upgrade deletes all restore points (for systems running Windows XP) and registry backups in the `%SYSTEMROOT%\Repair` folder. To maximize recovery options on an important server, start the computer using the Recovery Console, Windows PE, or a copy of Windows on a recovery drive, and then back up or copy the system partition to another location before performing an in-place upgrade.

To perform an in-place upgrade, check recovery deadlines to ensure there is sufficient time, and then follow these steps:

1. Boot from the Windows CD-ROM. (If necessary, switch the boot order to boot from the CD-ROM first.)

   When possible, use a Windows CD-ROM of the same service pack revision as the operating system installation you want to repair. This reduces the likelihood of file version conflicts.

2. To load mass storage drivers not included with Windows—such as drivers for a Small Computer System Interface (SCSI) or RAID controller—press F6 when Windows Setup starts. To specify a different hardware abstraction layer (HAL) manually, press F5.

3. After Windows Setup loads, press Enter. (Do not choose the Recovery Console option.)

4. Press F8 to accept the Windows licensing agreement.
5. Select the Windows installation to reinstall, and then type R. Windows installs files and then prompts for regional settings and the Windows CD-ROM key.

6. Reinstall all Windows software updates.

If performing an in-place upgrade does not fix the problem, use the ASR process discussed in the next section.

Using the Automated System Recovery Process
The Windows Server 2003 ASR process allows you to automatically format the system partition, restore disk and partition information, reinstall a minimal version of Windows, and restore the system partition from backup. It is the fastest way to recover from a system failure that requires a complete reinstall, such as a failed hard drive subsystem, as long as you create the ASR backup before the problem occurs. (See Chapter 36 for more information.)

Important The ASR process formats the system partition, erasing any changes made since the last ASR backup. To maximize recovery options, before performing the ASR procedure start the computer using the Recovery Console, Windows PE, or a copy of Windows on a recovery drive, and then back up or copy the system partition to another location. Also, write-protect the ASR backup media before using it to restore files. If there is only a single copy of the media, create a copy of the backup media before using it.

To recover a system using the ASR procedure, use the following steps:

1. Locate the ASR backup tape or tapes and floppy disk, the original Windows Server 2003 CD-ROM, and any third-party mass-storage drivers or network drivers that Windows requires to complete Setup. Windows restores updated drivers later in the ASR process.

2. Insert the Windows Server 2003 CD-ROM, and boot the system from the CD-ROM.

3. At the beginning of the boot process, press F6 when prompted to install a separate mass-storage driver if necessary.

4. Press F2 shortly after being prompted to press F6 to begin the ASR process.

5. Insert the ASR floppy disk and press Enter. Windows formats the system drive, restores the disk configuration, copies files in text mode Setup, restarts, and proceeds with graphical mode Setup. If graphical mode Setup does not start properly, restart the ASR process.

After installing Windows, the Backup utility launches, automatically restores the system from the ASR backup set, and then restarts.
6. Verify that the ASR process resolved the problem and that the server is running properly, reinstall any software updates that you installed since you created the ASR backup, and restore any other backups.

If you cannot resolve the problem using the ASR process or by consulting the Microsoft Knowledge Base, Microsoft Technical Communities (http://www.microsoft.com/communities), or Microsoft Product Support Services, perform a parallel installation of Windows to continue troubleshooting the problem or to resolve permissions issues. If you cannot resolve the problem using the parallel installation, perform a clean reinstall of Windows and all applications, or transfer all workloads and data to another server. For information about installing Windows, see Chapter 5.

**Note** To restore a server cluster in which all nodes have failed and you cannot restore the quorum disk, perform ASR on each node. See Chapter 19 for more information about working with server clusters.

---

**Real World  Using ASR to Restore to Different Hardware**

Microsoft does not support using the ASR process to restore a system configuration onto a different server. Nonetheless, if the original hardware is inoperable and identical hardware is unavailable, the ASR process might be the only reasonable option to get the organization back online. When using the ASR process to restore to different hardware, obtain the most similar hardware possible and perform an in-place upgrade if Windows does not start after restoring from the ASR set. When the crisis is over, transfer all workloads and data to another server to ensure the best stability and reliability.

---

**Fixing the Underlying Problem**

If the system can start Windows or Windows safe mode but still does not function properly, perform additional troubleshooting steps to locate the underlying problem. Begin by performing the tasks in the following list. Then use the tools and methods described in this section to further define the problem.

**Important** Disable backup tasks until the server is operating properly, or insert new media so that you do not overwrite potentially critical backups.

- **Restart Windows** If Windows starts successfully in safe mode, try restarting in normal mode. If Windows starts successfully, check the system closely for possible causes, such as a slowly failing boot device.
Check the Microsoft Knowledge Base  If Windows displays any specific error messages, go to the Microsoft online Help and Support center (http://support.microsoft.com) and search under the Windows Server 2003 category for a few keywords from the error message. This can help you quickly determine the cause.

Undo changes  Undo any changes that you recently made to the system if possible. Start the computer using the Last Known Good Configuration or by using the Device Driver Rollback feature in safe mode, as discussed in the next section. Uninstall recently added drivers or programs, and remove or disable any recently added devices. See the “Check Device Manager” section later in this chapter for information about checking for hardware problems.

Check Event Viewer  Event Viewer often reveals clues as to the cause of the problem and sometimes provides instructions to fix the problem. For more information about using Event Viewer, see Chapter 35.

Note  When troubleshooting, act like a scientist running an experiment. Change one thing at a time to minimize the likelihood of confounding variables, and closely scrutinize the results. If the system hangs on a certain service, check to make sure the service is not dependent on another service that is the underlying problem. Start with the least painful steps first—save formatting the hard disk and reinstalling Windows for last.

Check Device Manager  Examine the system for devices with conflicts or errors, and disable these devices or remove them from the system. Removing them from Device Manager usually just causes Windows to redetect them the next time the system starts.

When troubleshooting difficult resource conflicts, disable or remove every device in the system that Windows can start without, such as sound cards, network cards, and modems. If the problem goes away, add the devices back one by one until the problem reappears, and then troubleshoot the device in question. Chapter 7 includes more information about troubleshooting hardware.

Note  Advanced Configuration Power Interface (ACPI) systems automatically configure all PCI devices, preventing you from changing a device’s resource settings to resolve a conflict. To resolve resource conflicts, remove the devices in question from Device Manager and allow it to rescan them, or plug cards into different slots.

Rolling Back Recently Installed Drivers  Device drivers are one of the most common causes of system instabilities, so if the system becomes unstable after updating a device driver, revert to the previous driver. Windows
Server 2003, like Windows XP, makes this easy by providing a simple Roll Back Driver button. To use this feature, follow these steps:

1. Launch Computer Management from the Administrative Tools folder on the Programs menu.
2. Select Device Manager from the Computer Management console tree, right-click the suspect device (which might show a yellow exclamation point next to it), and choose Properties.
3. Click the Driver tab, and then click Roll Back Driver (as shown in Figure 40-1).
4. Click Yes to roll back the driver to the previous version.

![Figure 40-1  The Driver tab of a device's Properties dialog box]

Note The Last Known Good Configuration also rolls back drivers, but only drivers installed since the last time the computer started Windows successfully and a user logged on.

Using Help And Support to Gather Basic Information

The Windows Server 2003 Help And Support Center includes tools that gather basic information about the system. To use these tools, follow these steps:

1. Launch Help And Support Center from the Start menu.
2. Click Tools under the Support Tasks heading, and then click Help And Support Center Tools.

3. Click the My Computer Information link. The following links provide useful (but basic) information about the system:

- **View General System Information About This Computer**  Displays basic information about the operating system, processor, and other settings, including the system model and BIOS version.

- **View the Status of My System Hardware and Software**  Displays a list of obsolete drivers, a summary of installed hardware and whether the device drivers are approved by Microsoft, as well as the amount of hard disk space available on local hard drives.

- **Find Information About The Hardware Installed On This Computer**  Displays a summary of hardware in the system, driver versions, and whether Microsoft certifies the drivers. (See Figure 40-2.)

- **View A List Of Microsoft Software Installed On This Computer**  Information about installed software, including Product Identification (PID) numbers, and any crash information that Windows Watson records.

![Figure 40-2  My Computer Information – Hardware report](image-url)
4. Click the Advanced System Information link. The following links provide useful information about the system:

- **View Detailed System Information (Msinfo32.exe)** Launches the System Information tool
- **View Running Services** Displays a summary of all services
- **View Group Policy Settings Applied** Displays a summary of Group Policy settings that are applied to the computer
- **View The Error Log** Displays noteworthy events from Event Viewer

**More Info** For information about working with Group Policy, see Chapter 11; for information about software restriction policies, see Chapter 28.

**Using System Information to Gather Advanced Information**

The System Information utility (Msinfo32.exe) provides detailed information about the software and hardware environment of a system. To open the System Information utility, click Start, choose All Programs, Accessories, System Tools, and finally System Information. Then use the following list of tasks:

- To look for device problems, select Components and then Problem Devices. Make a note of any devices listed here, and then use Device Manager to disable or troubleshoot them.
- To view a list of hardware conflicts and shared resources, select Hardware Resources and then Conflicts/Sharing. Most shared resources do not cause problems on a modern system, but some devices do not like to share.
- To view a list of programs that start with Windows, select Software Environment and then Startup Programs. Disable any programs you suspect might be causing problems, and then restart the computer. (See the “Using the System Configuration Utility” section later in this chapter.)
- To view a list of Windows errors the system has reported to Microsoft, select Software Environment and then Windows Error Reporting, as shown in Figure 40-3.
- To view a list of Microsoft Office application errors (on a client system), select Office 2003 Applications and then Office Event/Application Fault.
To scan for unsigned system files, choose File Signature Verification Utility (Sigverif.exe) from the Tools menu and then click Start.

To scan for other unsigned files, click Advanced. For example, to scan for unsigned device drivers, search the %WINDIR%\System32\Drivers folder and subfolders. Make a note of any unsigned drivers (or refer to the Sigverif.txt log file saved in the %WINDIR% folder), and disable them by disabling the associated device (or updating the driver) in Device Manager, uninstalling the driver using Add/Remove Programs, or renaming the driver in the %WINDIR%\System32\Drivers folder.

### Checking Services

Important services that fail or do not start can cause major problems on a server. To avoid this, set all important services to start automatically, disable any services that you suspect might be causing problems, and specify what actions to take if a service fails.

To view the status of a service or change its options, launch Services (Services.msc) from the Administrative Tools folder on the Programs menu and then use the following list:

- To view the status of a service or to make changes to its status, select the service in the Services window, shown in Figure 40-4, and then use the Start Service, Stop Service, Pause Service, and Restart Service toolbar buttons.
To change advanced settings for a service, double-click the service to open its Properties dialog box, shown in Figure 40-5 and described in the following list:

- To change when the service starts, use the Startup Type list on the General tab.
- To specify which account the service uses to log on, use the Log On tab.
- To specify what actions to take when the service fails, use the Recovery tab.
- To view the services on which the service is dependent, click the Dependencies tab.
Using the System Configuration Utility

The System Configuration Utility (Msconfig.exe) is a handy troubleshooting tool that provides central access to virtually every relevant startup parameter. To troubleshoot startup problems using the System Configuration Utility, follow these steps:

1. Start Windows in safe mode or normal mode, type **Msconfig** in the Run dialog box or in a command prompt window and then click OK.

2. If you started Windows normally, select the Diagnostic Startup option and then click OK. When prompted to restart, click Restart.

   **Note**  
   You cannot create an ASR backup set unless all settings in the System Configuration Utility are set to Normal Startup.

3. If the problem no longer occurs, skip to Step 4; otherwise, review the following possible causes and solutions:

   - **Missing or damaged system files.** Look for an error message during startup or in the boot log, or use the File Signature Verification Tool or the System File Checker to determine whether all Windows files are intact and digitally signed. If a file is missing, damaged, or is the wrong version, extract a fresh copy from the Windows CD-ROM, use the In-place Upgrade procedure to reinstall Windows, or use the Automated System Recovery procedure to restore from a recent backup.

   - **Damaged registry.** Use the Last Known Good Configuration to restore the HKLM\SYSTEM\CurrentControlSet subkey, perform an in-place upgrade, or use the Automated System Recovery (ASR) process to restore Windows from a backup. If none of these methods work and you are troubleshooting a computer running Windows XP, see Microsoft Knowledge Base Article 307545 for information about how to recover a corrupt registry using the Recovery Console.

   - **The computer has a virus.** Use a virus checker with recent virus definition updates to scan for viruses and remove any it finds.

   - **A Windows upgrade failed.** If you suspect this is the case, reinstall Windows using the in-place upgrade procedure discussed earlier in this chapter.

4. If the system starts properly using the Diagnostic Startup option or with safe mode, open the System Configuration Utility, choose the Selective Startup option, and then clear all but the last option (Load Startup Items), as shown in Figure 40-6.
5. Click OK, and then restart the system. If the problem reappears, the problem lies with the selected option. If it does not come back, open the System Configuration Utility again, choose the Selective Startup option, and then clear all but the next option and try again.

6. When you identify generally where the problem lies, click the appropriate tab and troubleshoot the services, startup items, or lines in the file one by one, until you locate the specific problem.

7. After you locate the problem, note the offending line or program, return the settings in the System Configuration Utility to normal startup, and then permanently disable the offending line or program. (Use the System Configuration Utility only to troubleshoot problems, not to fix them.) To disable the program or line, use the appropriate action based on the location of the problem:

- For problems with services, use the Services MMC snap-in to change the service startup type to Disabled (as described in the previous section).

- For problems with startup items, make a note of the item’s location, and then remove the program from the Startup Items folder on the Start menu (if the location of the item is Common Startup), or use Registry Editor to export the key and then delete it from the registry.
For problems in the System.ini or Win.ini files, type `Sysedit` in the Run dialog box or at a command prompt and then remove or comment out the offending line in the appropriate file. (Use a semicolon before the line to disable it.)

### Using the System File Checker

The System File Checker is a command-line tool that verifies that the system has the correct versions of protected system files. If the System File Checker finds an incorrect version of a protected system file, it retrieves the correct version from the `%SYSTEMROOT%\System32\Dllcache` folder (or the Windows CD-ROM) and uses it to replace the incorrect version.

To use the System File Checker, log on locally as an administrator, open a command prompt window, and then type `Sfc` followed by the appropriate parameter. See Table 40-2 for a list of parameters.

**Note** If the `%SYSTEMROOT%\System32\Dllcache` folder is corrupt, use one of the following commands to repair the folder: `Sfc /Scannow`, `Sfc /Scanonce`, or `Sfc /Scanboot`.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/Scannow</code></td>
<td>Scans all protected system files.</td>
</tr>
<tr>
<td><code>/Scanonce</code></td>
<td>Scans all protected files a single time.</td>
</tr>
<tr>
<td><code>/Scanboot</code></td>
<td>Scans all protected files every time the computer is booted.</td>
</tr>
<tr>
<td><code>/Revert</code></td>
<td>Resets the scan to its default configuration.</td>
</tr>
<tr>
<td><code>/Purgecache</code></td>
<td>Deletes all files in the <code>%SYSTEMROOT%\System32\Dllcache</code> folder (the Windows File Protection cache), and immediately scans the protected system files.</td>
</tr>
<tr>
<td><code>/Cachesize=x</code></td>
<td>Specifies the size (in megabytes) of the <code>%SYSTEMROOT%\System32\Dllcache</code> folder (the Windows File Protection file cache). The default size is 50 MB. After using this command, restart the computer and then use the <code>/Purgecache</code> command.</td>
</tr>
</tbody>
</table>

### Restoring from a Backup

Choosing to restore Windows from a backup can be a difficult decision, especially when the system is partially functional. Before restoring from a backup, ask the following questions:

- How recent is the backup, and what data and settings would you lose?
- How confident are you that the problem is not also present on the backup?
Can you back up the current state of the server before restoring the server?

Does restoring from a backup help or hinder recovery deadlines?

Can Microsoft Product Support Services (PSS) help resolve the problem without restoring from a backup?

To restore Windows from a backup, use the ASR process as described earlier in this chapter, or start Windows and then use the Windows Backup program (or a third-party program), as described in Chapter 37.

Reinstalling Windows

If you cannot resolve the problem through troubleshooting, restoring from a backup, or consulting the Microsoft Knowledge Base, Microsoft Technical Communities (http://www.microsoft.com/communities), or Microsoft Product Support Services, the situation is dire indeed. An in-place upgrade might resolve the problem, but if the problem lies with system settings (which are largely preserved during an in-place upgrade), a clean install is the last option.

To perform a clean install, uninstall Windows using the method described in the “Uninstalling Windows” section later in this chapter (or by formatting the disk), or perform a parallel installation to replace or troubleshoot the failed installation. See Chapter 5 for information about performing a clean installation of Windows.

Emergency Management Services and Headless Servers

Emergency Management Services (EMS) is a service that permits Windows administrators to do what UNIX administrators have long been able to do—remotely manage servers under virtually all circumstances, and even run “headless servers” that do not have locally attached keyboards, mice, or monitors.

The following sections provide an overview of EMS and so-called out-of-band management, discuss the requirements for EMS, and discuss how to use it to manage unresponsive servers.

EMS Overview

EMS is the out-of-band management solution for the Microsoft Windows Server 2003 family. Administrators can use EMS to perform the following actions via a remote management port, without being physically present at the server:

- Restart or shut down a partially unresponsive server.
- View STOP error messages.
- View a list of processes, and kill hung or problematic processes.
- View and change the IP address of the server.
- Start and access command prompts, and securely run text-based utilities such as BootC fg.
- View setup logs during Windows Setup when upgrading Windows.
- Install Windows.
- Select which operating system to boot.
- Turn on a server*.
- Change BIOS or EFI settings*.
- Troubleshoot problems using the Recovery Console*.

Items marked with an asterisk (*) require firmware or service processor support for console redirection, as described later in this chapter. Figure 40-7 shows during which operational states EMS is available and how it relates to Windows Server 2003’s various in-band remote management tools.

![Remote system management overview](image)

**Figure 40-7** Remote system management overview

**Note** EMS is text-only with no capacity for using GUI-based tools or services over an out-of-band connection.
In-Band and Out-of-Band Management

There are two categories of remote management tools: in-band and out-of-band. In-band-management tools—such as Remote Desktop, MMCs, and scripts—provide powerful network-based administration capabilities when the operating system is running properly. As such, these are the tools administrators use everyday, and they are the primary means of administering a server. However, they do not provide a complete remote administration solution.

Out-of-band management tools provide access to a server over a serial port connection or dedicated Ethernet management port when in-band-management tools fail to respond, such as when the operating system is frozen or starting. As such, they exist primarily to return a server to an in-band state where more administrators can use more powerful in-band management tools.

Hardware and Software Requirements

Although EMS is compatible with virtually all modern servers, EMS works best with the following hardware and software:

- A BIOS or EFI that supports firmware-based console redirection, or an add-on service processor
- A 16550 or 16450 UART (Universal Asynchronous Receiver/Transmitter) serial port that is fully described in the Serial Port Console Redirection (SPCR) table or EFI console device path, or an Ethernet management port with support for sharing the management port with EMS
- VT-UTF8 support in the firmware or service processor as well as the terminal software (VT100+ or VT100 support at a minimum)
- Smart power switches and UPS devices that do not interrupt communications and that support escape sequences, VT100+, and powering on or resetting the server remotely
- Terminal concentrators (also called console servers or terminal servers) that have the appropriate number of serial ports for the number of servers

**Note** After enabling EMS, the serial port that EMS uses for out-of-band administration disappears from Device Manager. This is normal; you cannot use the serial port for anything else.
Real World  Security and Terminal Concentrators

A terminal concentrator or console server is a device that connects to the serial port of multiple servers, and in turn connects to the network. Administrators can access the terminal concentrator from across the network and perform out-of-band administration of the servers.

As useful as terminal concentrators are, they can also be large security risks. Anybody with access to the management port of a server that has out-of-band management enabled can easily restart, shut down, or kill processes on the server, all without needing a password. The following list describes how to enhance the security of servers that use EMS:

- Place servers in a secure location—if an attacker can gain physical access to the server, it is not secure enough.
- Use the concentrator’s built-in security features. Many concentrators can create an access list, and some permit server-based authentication, authorization, and accounting (AAA) using RADIUS, packet filtering, and encryption using Advanced Encryption Standard (AES) encryption.
- Place the concentrator on a secure network. Many networks make use of a dedicated and highly secure management network that is separated by a firewall from the standard corporate network—this is an excellent location for the terminal concentrator. To access a server via EMS, administrators can tunnel into the management network and then connect to the terminal concentrator.

Setting Up EMS

Windows does not enable EMS by default, so unless the server came with Windows Server 2003 preinstalled and EMS enabled, you must configure the hardware and Windows to work with EMS. To do this, first configure the server’s hardware and firmware and then enable EMS, either during Windows installation or afterward.

To determine whether EMS is enabled, open a command prompt and type `Bootcfg /Query`. If you see redirect settings, EMS is enabled.

**Note**  Enable the server to restart automatically following a blue screen. (This is the default behavior.) Doing so permits the system to resume normal operation quickly and minimizes downtime. To enable this setting, in Control Panel, double-click System, click the Advanced tab, click Settings in the Startup And Recovery section, and then select the Automatically Restart check box.
Configuring the Firmware for EMS

Before enabling EMS, enable firmware-based console redirection. If the system does not support firmware-based console redirection, the system must have a display card and keyboard (though you do not need to use them).

To prepare a server for out-of-band management using EMS, perform the following steps:

1. Enable console redirection in the system BIOS or in the service processor’s firmware.
2. Verify that the firmware’s console redirection is set up to use the Serial Port Console Redirection (SPCR) table.
3. Configure and test the management port. EMS uses COM1 at 3F8 by default.
4. Specify the appropriate terminal definition. Use VT-UTF8 if possible—it supports colors, standardized escape sequences, and non-English characters. Otherwise, use VT100+ or VT100, in that order. Use the same terminal definition for the terminal software and terminal concentrator.
5. Check the server or service processor’s documentation to see whether there are any further configuration steps to perform.

Manually Installing Windows on a Headless Server

Most administrators enable EMS during Windows Setup, especially if the server is a headless server. Most new servers built in the last several years support firmware (BIOS or EFI) based console redirection, or they have a service processor that provides out-of-band management capabilities to the server. As long as the firmware or service processor supports the Serial Port Console Redirection (SPCR) table, setting up a server with EMS is easier than finding a Starbucks in Seattle because Setup automatically checks with the SPCR and directs all output accordingly.

To install Windows Server 2003 on a headless server using the Windows Server 2003 CD-ROM, take the following steps (setting up EMS during a Windows upgrade or after Setup completes is discussed later in this chapter):

1. Start the system, turn on console redirection and SPCR table support in the firmware, and set the server to boot from the CD-ROM first.

   **Note** If the system does not support firmware-based console redirection, perform the installation using a locally attached keyboard and display, or perform a headless installation using Remote Installation Services (RIS) or an answer file, as discussed later in this chapter.

2. On the management computer, open a terminal program such as Telnet or HyperTerminal.
3. If the server connects to a terminal concentrator, open a TCP/IP connection to the
terminal concentrator, log on, and establish a connection with the desired server.
Otherwise, connect to the appropriate serial port.

**Note**  By default, EMS uses COM1 at 9600 baud with 1 stop bit, no parity,
8 data bits, and hardware flow control.

4. Insert the Windows Server 2003 CD-ROM, and start the computer using the appro-
riate command for the server’s firmware or service processor, or by pressing the
power switch.

5. Press a key when prompted to boot from the CD-ROM. Text mode setup or the Cli-
ent Installation Wizard (for RIS installati ons) appears, as discussed in Chapter 5
and Chapter 28.

6. At the end of text-mode setup, click OK to install Windows without user input.

7. After Setup completes, use in-band administration tools such as Remote Desktop.

**Note**  The Special Administration Console or SAC is available during GUI-
based Setup, but you cannot use it to monitor or control Setup.

### Installing Windows Using RIS on a Headless Server

By default, RIS-based installations require local input during the Client Installation Wiz-
ard. Because local input is impossible for some headless servers, RIS provides a way to
redirect console output over the serial or management port and use EMS to control the
Client Installation Wizard.

To install Windows Server 2003 using RIS on a headless server, use the following
procedure:

1. Make a backup copy of the StartROM.com file in the `\Server_Name\Reminst\Oschooser\Platform` folder (where `Server_Name` is the name of the RIS server and `Platform` is either i386 or amd64).

2. Rename the appropriate file described in the following list (located in the same
folder as Startrom.com) to **Startrom.com**:

   - **Hdlscom1.com, Hdlscom2.com**  For systems that do not support console
     redirection. Specifies that RIS enables EMS on COM1 (Hdlscom1.com) or
     COM2 (Hdlscom2.com), and redirects the Press F12 For Network Boot
     prompt to the appropriate serial port.
Hdlscom1.n12, Hdlscom2.n12  For systems that support firmware-based console redirection. Specifies that EMS enables EMS on COM1 (Hdlscom1.com) or COM2 (Hdlscom2.com), and boots directly into the Client Installation Wizard without displaying the Press F12 For Network Boot prompt.

Note  Clients with an EFI instead of a BIOS do not use the Startrum.com file.

3. On the management computer, open a terminal program such as Telnet or HyperTerminal.

4. If the server connects to a terminal concentrator, connect to the terminal concentrator, log on, and establish a connection with the desired server. Otherwise, connect to the appropriate serial port.

5. Start the computer using the appropriate command for the server’s firmware or service processor, or simply turn the system on when performing the installation locally.

6. Press F12 to boot from the network and start RIS setup. (Change the boot order in the system BIOS or EFI if necessary.)

7. At the end of text-mode setup, click OK to install Windows without user input.

8. After Setup completes, use in-band administration tools such as Remote Desktop.

Note  The Special Administration Console or SAC is available during GUI-based Setup, but you cannot use it to monitor or control Setup.

Installing Windows Using an Answer File on a Headless Server
To install Windows remotely on a server that does not support firmware-based console redirection and the SPCR table, use RIS (as described in the previous section), or add the following lines to the [Data] section of the Unattend.txt or Winnt.sif answer file (which is discussed in Chapter 5):

- **Emsport={Com1 | Com2 | Usebiossettings | off}**  Specifies which serial port EMS uses for out-of-band administration (COM1 is the default). The Usebiossettings parameter specifies that EMS uses the SPCR table to configure EMS; if SPCR support is not available, Windows disables EMS.

- **Emsbaudrate={9600 | 19200 | 57600 | 115200}**  Specifies what baud rate EMS uses for the serial port. The default is 9600, but a higher rate increases the redraw speed of the console. If you have trouble communicating with a server using EMS, try lowering the baud rate.
Autopartition={1}  Specifies whether Setup chooses the partition on which to install Windows. The value 1 enables automatic selection; if you omit this line, text-mode Setup stops to prompt the user for input. Do not disable automatic selection unless the server supports firmware-based console redirection.

Msdosinitiated={0}  Specifies that Setup runs directly from the Windows CD-ROM. Always set this value to 0 to prevent Setup from failing at the beginning of GUI mode Setup. (This setting does not affect unattended installations from a distribution folder.)

Unattendedinstall={No | Yes}  Tells Setup to run in unattended mode. Set this to Yes.

To install from a CD-ROM, rename the Unattend.txt file to Winnt.sif and copy it to a floppy disk. Insert the floppy disk immediately after the system boots from the CD-ROM.

Enabling EMS during Windows Upgrades

To enable EMS support during a version upgrade or in-place Windows upgrade, use the following steps:

1. Connect to the desired server using a Remote Desktop connection.
2. Close all programs, and disable all virus protection programs.
3. Insert the Windows CD-ROM, or connect to the appropriate network share for the Windows install files.
4. Open a command prompt window, and launch Winnt32.exe from the CD-ROM (in the \i386 or \amd64 folder) or network share using the following parameters (for example, Winnt32.exe /Emsport=COM1 /Emsbaudrate=115200 /Unattend):

   - /Emsport={Com1 | Com2 | Usebiossettings | off}  Specifies which serial port (COM1 or COM2) EMS uses for out-of-band administration. The Usebiosettings parameter specifies that EMS uses the SPCR table to configure EMS; if SPCR support is not available, Windows disables EMS.

   - /EmsbaudRate={9600 | 19200 | 57600 | 115200}  Specifies what baud rate EMS uses for the serial port. The default is 9600. If you have trouble communicating with a server using EMS, try lowering the baud rate.

   - /Unattend  Runs Setup in unattended mode, taking all settings from the previous version or installation. This setting is optional; if you omit it, Setup prompts you to answer a few questions at the beginning of Setup.
5. Windows Setup copies files to the hard drive and restarts into text-mode Setup. This is followed by GUI-based Setup, and then a fully installed Windows operating system. If necessary, use EMS to navigate text-mode Setup.

6. After Setup completes, use in-band administration tools such as Remote Desktop.

---

**Note** The Special Administration Console or SAC is available during GUI-based Setup, but you cannot use it to monitor or control Setup.

**Enabling EMS after Setup**

To enable EMS support after installing Windows, use the following procedure:

1. Connect to the desired server using Remote Desktop or telnet, and open a command prompt.

2. Type `Bootcfg /Ems` followed by the appropriate parameters (for example `Bootcfg /Ems On /Port Com1 /Baud 115200 /Id 1`):

   - **On** Enables EMS for the operating system specified by the `/Id` parameter.
   - **Off** Disables EMS for the operating system specified by the `/Id` parameter.
   - **Edit** Edits the COM port settings for the operating system specified by the `/Id` parameter.
   - **/Port {Com1 | Com2 | Com3 | Com4 | Biosset}** Specifies which serial port (COM1 through COM4) EMS uses for out-of-band administration. The **Biosset** parameter specifies that EMS uses the SPCR table to configure EMS; if SPCR support is not available, Windows disables EMS.
   - **/Baud {9600 | 19200 | 57600 | 115200]** Specifies what baud rate EMS uses for the serial port. The default is 9600. If you have trouble communicating with a server using EMS, lower the baud rate.
   - **/Id** Specifies the operating system entry in the Boot.ini file for which to enable EMS. This is usually 1, but it can be another number if the server has multiple operating systems.

3. Restart the server to enable EMS.

---

**Note** To enable EMS support for the Recovery Console on a server that does not support firmware-based console redirection, install the Recovery Console on the hard drive and then edit the Winnt.sif file located in the Cmdcons folder of the hard drive as described in the "Installing Windows Using an Answer File on a Headless Server" section of this chapter.
Using EMS for Out-of-Band Administration

After you enable EMS, the Special Administration Console (SAC) becomes available. The SAC is a special command-line tool that is largely independent of Windows and remains available at most times when Windows is not. Use the SAC and its sister, the !SAC, to perform out-of-band administration via the server’s management port during most phases of server operation, including operating system startup and shutdown, normal operation, stop errors, and most instances when the server becomes unresponsive.

Although you can accomplish many administration tasks out-of-band using the SAC, the point of the SAC is to return the server to a state where you can administer it using in-band management tools such as Remote Desktop.

The !SAC is available only when the system generates a STOP error, and it provides a subset of the SAC commands—just enough to view information about the computer and the STOP error and then restart the computer.

To use the SAC and !SAC, follow these steps:

1. On the management computer, open a terminal program such as Telnet or HyperTerminal.
2. If the server connects to a terminal concentrator, open a TCP/IP connection to the terminal concentrator, log on, and establish a connection with the desired server. Otherwise, connect to the appropriate serial port.
3. Press Enter to display the SAC> command prompt.
4. Use the commands in Table 40-3 and Table 40-4 to administer the server from the SAC> command prompt. If the server produces a STOP error, press Enter to display the !SAC> command prompt, which contains only the restart, D, Id, and Q commands.

Table 40-3  SAC commands and their functions

<table>
<thead>
<tr>
<th>SAC Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ch</td>
<td>Displays a listing of any open command prompt channels.</td>
</tr>
<tr>
<td>Cmd</td>
<td>Opens a new command prompt channel that you can use to run text mode programs and commands, as long as Windows is sufficiently functional. Log on to each command prompt channel using an account with appropriate credentials.</td>
</tr>
<tr>
<td>Crashdump</td>
<td>Artificially generates a STOP error, and saves the current contents of the server’s memory to a crashdump file in the root directory of the system partition.</td>
</tr>
<tr>
<td>D</td>
<td>Creates a dump file of the current operating system kernel log.</td>
</tr>
</tbody>
</table>
Table 40-3  SAC commands and their functions

<table>
<thead>
<tr>
<th>SAC Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>Toggles whether the T command displays only processes, or processes and threads.</td>
</tr>
<tr>
<td>I</td>
<td>Displays and sets the server’s IP addresses, similar to the IPCfg command. To change the TCP/IP configuration of the server, type I followed by the network interface number, the new IP address, subnet mask, and gateway (for example, I 2 192.168.1.101 255.255.255.0 192.168.1.1).</td>
</tr>
<tr>
<td>Id</td>
<td>Displays information about the server’s identity (for example, the server name).</td>
</tr>
<tr>
<td>K&lt;PID&gt;</td>
<td>Kills (forcibly ends) the process whose Process ID (PID) you specify.</td>
</tr>
<tr>
<td>L&lt;PID&gt;</td>
<td>Lowers the priority of the specified process and all child processes to the lowest priority level.</td>
</tr>
<tr>
<td>Lock</td>
<td>Locks all channels that are lock-enabled. To unlock a locked channel, log on with an appropriate user account.</td>
</tr>
<tr>
<td>M&lt;PID&gt;&lt;megabytes_allowed&gt;</td>
<td>Limits the amount of memory the specified process can use. (Specify the amount of memory in megabytes.)</td>
</tr>
<tr>
<td>P</td>
<td>Pauses the output of the T command after each full screen. (Use with the T-list command.)</td>
</tr>
<tr>
<td>R&lt;PID&gt;</td>
<td>Raises the priority of the desired process and all child processes up one priority level.</td>
</tr>
<tr>
<td>Restart</td>
<td>Restarts the server.</td>
</tr>
<tr>
<td>S</td>
<td>Displays the current date using a 24-hour clock format. To change the time, type the correct time in the mm/dd/yyyy hh:mm format—for example, 03/02/2006 13:42.</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Shuts down and powers off the computer. To turn the server on again, use the proper escape sequence on the UPS (if the UPS supports remote power on capabilities).</td>
</tr>
<tr>
<td>T</td>
<td>Displays a list of processes and threads currently running. Use the F and P commands to modify the output.</td>
</tr>
<tr>
<td>? or Help</td>
<td>Provides a list of commands. Type a command name followed by a question mark for help.</td>
</tr>
</tbody>
</table>

Table 40-4  SAC channel control commands and their functions

<table>
<thead>
<tr>
<th>SAC Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ch</td>
<td>Displays a listing of open command prompt channels.</td>
</tr>
<tr>
<td>Ch –Si &lt;n&gt;</td>
<td>Switches control to the specified channel number. SAC does not support overlapping windows.</td>
</tr>
<tr>
<td>Ch –Sn &lt;name&gt;</td>
<td>Switches control to the specified channel name.</td>
</tr>
</tbody>
</table>
Chapter 40  Troubleshooting and Recovery

Miscellaneous Challenges

This section covers some tasks (we like to call them “challenges”) you might need to perform. If you do not find a task or problem here, check the Microsoft Knowledge Base at http://support.microsoft.com or the Microsoft Technical Communities (newsgroups) at http://www.microsoft.com/communities, or contact Microsoft Product Support Services.

Using the Shutdown Event Tracker

Uptime is of paramount importance to servers. A server that is off or restarting is not available to service clients. To help administrators keep track of why a server restarts, Windows Server 2003 provides the Shutdown Event Tracker tool.

The Shutdown Event Tracker is a simple tool that gathers information about why a server shuts down and records it in Event Viewer. If the server shuts down voluntarily (for example, a user chooses the Start menu’s Shut Down command), a dialog box prompts the user to explain the reason for the shutdown. If the server shuts down unexpectedly (for example, due to a hardware failure), Windows prompts the next user with shutdown privileges who logs on to describe why the server shut down. Besides this user-provided information, any time a user shuts down the system and specifies in the Shutdown Event Tracker that the shutdown was unplanned, Windows records the system state data for later analysis.

Administrators can then use the information about when and why the server shuts down to improve uptime. To view shutdown events, open Event Viewer and then follow these steps:

1. Display the System log in Event Viewer.
2. Choose the View menu’s Filter command.
3. Choose USER32 from the Event Source drop-down list.
4. Click OK to display the System log in Event Viewer filtered to display only shutdown events and other USER32 events.

Table 40-4  SAC channel control commands and their functions

<table>
<thead>
<tr>
<th>SAC Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ch –Ci &lt;n&gt;</td>
<td>Closes the specified channel number.</td>
</tr>
<tr>
<td>Ch –Cn &lt;name&gt;</td>
<td>Closes the specified channel name.</td>
</tr>
<tr>
<td>&lt;Esc&gt;&lt;Tab&gt;</td>
<td>Switches between channels (just like &lt;Alt&gt;&lt;Tab&gt;).</td>
</tr>
<tr>
<td>&lt;Esc&gt;&lt;Tab&gt;0</td>
<td>Switches to the SAC channel.</td>
</tr>
</tbody>
</table>

Ch –Ci <n> Closes the specified channel number.
Ch –Cn <name> Closes the specified channel name.
<Esc><Tab> Switches between channels (just like <Alt><Tab>).
<Esc><Tab>0 Switches to the SAC channel.
5. Double-click an event to view the description of the shutdown event, as shown in Figure 40-8.

![Figure 40-8 Viewing a shutdown event](image)

**Note** To change Shutdown Event Tracker settings, use the Group Policy editor to change the Display Shutdown Event Tracker and Activate Shutdown Event Tracker System State Data Feature settings (located in the Computer Configuration-Administrative Templates-System container). Windows enables the Shutdown Event Tracker by default on systems running Windows Server 2003, and disables it by default on Windows XP Professional systems.

### Adding a Processor to the System

Adding a processor to a modern server is easy: simply turn the computer off and then add the additional processor. (The processor must be the same model, speed, and stepping as the current processor.) Windows Plug and Play automatically installs the additional processor, and if necessary, changes the kernel from a uniprocessor kernel to a multiprocessor kernel. In some cases, Windows also changes the hardware abstraction layers (HAL).

Installing an additional processor in older servers that use one of the following types of processors is sometimes more complex:

- A single Intel processor without Hyper-Threading Technology or multiple cores
- A single AMD 32-bit processor
If Windows does not automatically detect the new processor when adding one of the above processor types, use the following procedure to change the HALs that Windows uses:

**Important**  If you choose an incompatible HAL, you must perform an in-place upgrade of Windows to recover, or you must restore from a previous backup.

1. Start Windows, open Task Manager, and then click the Performance tab to confirm that Windows displays the proper number of logical and/or physical processors in the CPU Usage field.

2. If Task Manager does not show the new processor, update the ASR backup set and then launch the Computer Management snap-in from the Administrative Tools folder on the Programs menu.

3. Click Device Manager in the console tree.

4. In the details pane, expand the Computer branch of the Device Manager tree, right-click the computer item (most likely ACPI Uniprocessor PC), and choose Update Driver.

5. Click Next to let the Hardware Update Wizard locate the appropriate HAL for the multiprocessor system.

6. If Windows does not automatically find a different HAL, upgrade from the ACPI Uniprocessor PC HAL to the ACPI Multiprocessor PC HAL by manually choosing the new HAL in the Hardware Update Wizard.

7. If Windows fails to start after changing the HAL, use the ASR process to recover the system or launch Windows Setup from the Windows CD-ROM. Then press F5 when prompted to press F6, choose the appropriate HAL, and then perform an in-place upgrade.

**Troubleshooting Shutdown Problems**

Although Windows Server 2003 usually shuts down reliably, it can occasionally hang during shutdown. Here are some suggestions for solving the problem (for more in-depth information, use the Help system's Startup and Shutdown Troubleshooter or search the Microsoft Knowledge Base):

- Use the System Configuration Utility (Msconfig) to troubleshoot the startup files and pinpoint which file contains the issue that causes Windows to hang during shutdown.

- Disable or uninstall antivirus programs that might scan drives during Windows shutdown.
■ Roll back display drivers.
■ Disable sound cards.
■ Disable network cards and modems.
■ Check to see whether the Exit Windows sound file is corrupt (for computers with a sound card). If it is, change the Exit Windows sound to none, extract a new copy of the file from the Windows CD-ROM, or copy it from another computer.

**Uninstalling Windows**

To remove Windows Server 2003, use the recovery console to format the system drive, or use the following steps to remove Windows without formatting the drive:

1. Verify the location of Windows Server 2003 and the partition layout on the hard disk. The Disk Management snap-in located in the Computer Management console shows the partition information.
2. Back up or copy any valuable files located in the %SYSTEMROOT% or Program Files folders.
3. To remove Windows Server 2003 completely from the system, replace the Windows Server 2003 boot sector with that of the operating system you want to use. Windows NT users can use the emergency recovery process to do this.

   **Note** Instead of replacing the Windows boot sector, you can edit the Boot.ini file to remove the Windows installation and change the default operating system.

4. Delete the %SYSTEMROOT% folder in which the Windows installation was located (which is C:\Windows by default).
5. Delete the following files in the root directory of the boot partition:
   - Pagefile.sys
   - Ntdetect.com
   - Ntbootdd.sys
   - Cmldr
   - Cdldr
   - Arcldr.exe
   - Arcsetup.exe
❑ Boot.ini (Do not delete this if you want to keep using the Windows Boot menu.)

❑ Ntldr (Do not delete this if you want to keep using the Windows Boot menu.)

6. To increase the free disk space on the drive, move any important files out of the Program Files, Documents and Settings, Recycler, and System Volume Information folders, and then delete the folders.

---

**Summary**

When troubleshooting a problem or recovering from a failure, start by triaging the situation to determine priorities and what actions to take. Then use the steps outlined in your recovery procedures or this chapter to recover basic functionality. Once the computer can successfully start Windows or Windows safe mode, use the utilities provided with Windows to find and fix the underlying problem.

This chapter also discussed how to use the Emergency Management Service (EMS) for out-of-band administration of unresponsive servers, and how to perform other troubleshooting tasks such as using the Shutdown Event Tracker.
Part VIII
Appendixes

Appendix A
Interface Changes from Windows 2000 Server .........................1331

Appendix B
Interface Changes from Windows NT 4 ..............................1337

Appendix C
Optional Components ..................................................1345

Appendix D
Using the Microsoft Windows Server 2003 Recovery Console ....1353

Appendix E
Using the Microsoft Windows Server 2003 Support Tools ........1357
Appendix A

Interface Changes from Windows 2000 Server

The interface for Microsoft Windows Server 2003 R2 and Windows Server 2003 is similar to the Windows 2000 Server interface, though there are some significant changes and additions. Table A-1 lists some of the components that Microsoft renamed, changed, or introduced in the first release of Windows Server 2003, while Table A-2 summarizes the changes since the first release of Windows Server 2003.

Table A-1  Changes in Windows Server 2003

<table>
<thead>
<tr>
<th>Windows 2000 Server Name</th>
<th>Windows Server 2003 Name</th>
<th>Operating System Support</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency Repair Process</td>
<td>Automated System Recovery (ASR)</td>
<td>Windows Server 2003, Windows XP</td>
<td>Formats the system partition, restores disk and partition information from the ASR floppy disk, reinstalls a minimal version of Windows, and restores the system partition from backup.</td>
</tr>
<tr>
<td>Group Policy tab of the Properties dialog box in Active Directory Users or Active Directory Sites And Services</td>
<td>Group Policy Management Console (GPMC)</td>
<td>Windows Server 2003 (with download), Windows XP (with download)</td>
<td>Provides a central location to manage and create Group Policy Objects.</td>
</tr>
<tr>
<td>Internet Information Services (IIS) 5</td>
<td>IIS 6</td>
<td>Windows Server 2003</td>
<td>Hosts Web sites and applications with improved security, performance and reliability, including the ability to isolate processes and applications.</td>
</tr>
<tr>
<td>(Classic) Start Menu</td>
<td>Start Menu</td>
<td>Windows Server 2003, Windows XP</td>
<td>Provides quick access to frequently used programs. To use the Classic Start Menu, right-click the Start button, choose Properties, and then select Classic Start Menu.</td>
</tr>
</tbody>
</table>
Table A-1  Changes in Windows Server 2003

<table>
<thead>
<tr>
<th>Windows 2000 Server Name</th>
<th>Windows Server 2003 Name</th>
<th>Operating System Support</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Services in Application Mode</td>
<td>Terminal Services</td>
<td>Windows Server 2003</td>
<td>Provides clients remote access to applications and the Windows desktop running on a Windows Terminal Services server.</td>
</tr>
<tr>
<td>(None) Compressed Folders</td>
<td>Windows Server 2003, Windows XP</td>
<td></td>
<td>Creates views and extracts files from compressed archive files using the .zip file format.</td>
</tr>
<tr>
<td>(None) Emergency Management Services (EMS)</td>
<td>Windows Server 2003</td>
<td></td>
<td>Administers servers remotely when in-band management tools are unavailable.</td>
</tr>
<tr>
<td>(None) Enterprise Universal Description, Discovery, and Integration (UDDI) Services</td>
<td>Windows Server 2003</td>
<td></td>
<td>Provides a UDDI directory for organizing and categorizing Web services.</td>
</tr>
<tr>
<td>(None) Fax Services</td>
<td>Windows Server 2003</td>
<td></td>
<td>Provides basic fax server functionality.</td>
</tr>
</tbody>
</table>
### Table A-1  Changes in Windows Server 2003

<table>
<thead>
<tr>
<th>Windows 2000 Server Name</th>
<th>Windows Server 2003 Name</th>
<th>Operating System Support</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>(None) Previous Versions client</td>
<td>Windows Server 2003, Windows XP Service Pack 2; other versions available for download</td>
<td>Allows users to access Shadow Copies in a Windows Server 2003 file share.</td>
<td></td>
</tr>
<tr>
<td>(None) Shadow Copies</td>
<td>Windows Server 2003, Windows XP, Windows 2000</td>
<td>Creates point-in-time copies of file shares that users can access and restore using the Previous Versions client.</td>
<td></td>
</tr>
<tr>
<td>(None) Software Restriction Policies</td>
<td>Windows Server 2003</td>
<td>Uses Group Policy to control which applications and scripts users can run.</td>
<td></td>
</tr>
</tbody>
</table>

### Table A-2  Changes since Windows Server 2003

<table>
<thead>
<tr>
<th>Windows Server 2003 Name</th>
<th>New Name</th>
<th>Operating System Support</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed File System</td>
<td>DFS Namespaces</td>
<td>Windows Server 2003 R2</td>
<td>Provides an enhanced interface for grouping shared folders scattered across the network into a virtual tree of folders called a namespace.</td>
</tr>
<tr>
<td>Internet Connection Firewall (ICF)</td>
<td>Windows Firewall</td>
<td>Windows Server 2003 Service Pack 1 or later, Windows XP Service Pack 2 or later</td>
<td>Provides a host firewall that works during Windows startup and has additional configuration options. Does not replace the Basic Firewall feature of the Routing and Remote Access (RRAS) service.</td>
</tr>
</tbody>
</table>
Table A-2  Changes since Windows Server 2003

<table>
<thead>
<tr>
<th>Windows Server 2003 Name</th>
<th>New Name</th>
<th>Operating System Support</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Services for UNIX (download)</td>
<td>Microsoft Services for Network File System; Identity Management for UNIX; Subsystem for UNIX-based Applications</td>
<td>Windows Server 2003 R2</td>
<td>Provides support for Network File System (NFS), Network Information Service (NIS) servers, and custom UNIX-based applications. Previous versions of these tools are available for download as a part of Windows Services for UNIX.</td>
</tr>
<tr>
<td>Printers and Faxes folder</td>
<td>Print Management console</td>
<td>Windows Server 2003 R2</td>
<td>Provides a central management interface for managing print servers and pushing printer connections to clients using Group Policy.</td>
</tr>
<tr>
<td>Microsoft Management Console 2.0</td>
<td>MMC 3.0</td>
<td>Windows Server 2003 R2; Windows Server 2003 and Windows XP Service Pack 2 versions available for download</td>
<td>Hosts MMC 3.0 and earlier snap-ins, and provides a new Action pane with frequently used tasks.</td>
</tr>
<tr>
<td>Microsoft .NET Framework 1.1</td>
<td>Microsoft .NET Framework 2.0</td>
<td>Windows Server 2003 R2; other versions available for download</td>
<td>Provides support for applications written for Microsoft .NET Framework 2.0.</td>
</tr>
<tr>
<td>(None) Active Directory Application Mode (ADAM)</td>
<td></td>
<td>Windows Server 2003 R2; Windows Server 2003 (with download), Windows XP (with download)</td>
<td>Provides the ability to use Active Directory for applications independent of any existing Active Directory forests.</td>
</tr>
<tr>
<td>(None) Active Directory Federation Services</td>
<td></td>
<td>Windows Server 2003 R2</td>
<td>Provides single user sign-on capabilities to related Web applications during an online session.</td>
</tr>
<tr>
<td>(None) Common Log File System (CLFS)</td>
<td></td>
<td>Windows Server 2003 R2</td>
<td>Provides applications with enhanced log file support.</td>
</tr>
<tr>
<td>(None) File Server Resource Manager</td>
<td></td>
<td>Windows Server 2003 R2</td>
<td>Tracks storage usage on the local server, and creates hard or soft policies limiting the amount and type of files that users can save in specific folders.</td>
</tr>
</tbody>
</table>
### Table A-2  Changes since Windows Server 2003

<table>
<thead>
<tr>
<th>Windows Server 2003 Name</th>
<th>New Name</th>
<th>Operating System Support</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>(None)</td>
<td>Hardware Management</td>
<td>Windows Server 2003 R2</td>
<td>Allows administrators to write scripts that manage and monitor server hardware remotely using Windows Remote Management (WinRM).</td>
</tr>
<tr>
<td>(None)</td>
<td>Remote Access Quarantine Service</td>
<td>Windows Server 2003 Service Pack 1</td>
<td>Limits network access for remote access connections until a script verifies that the clients comply with network policies.</td>
</tr>
<tr>
<td>(None)</td>
<td>Security Configuration Wizard</td>
<td>Windows Server 2003 Service Pack 1 or later</td>
<td>Creates, applies, and edits role-based security policies that reduce the attack surface of a server.</td>
</tr>
<tr>
<td>(None)</td>
<td>Storage Management for SANs</td>
<td>Windows Server 2003 R2</td>
<td>Provides a simple MMC console and command-line interface for managing Storage Area Networks (SANs).</td>
</tr>
<tr>
<td>(None)</td>
<td>Windows SharePoint Services</td>
<td>Windows Server 2003 R2; other versions available for download</td>
<td>Provides an integrated intranet Web site solution for file storage and team collaboration.</td>
</tr>
</tbody>
</table>

Appendix B

Interface Changes from Windows NT 4

Initially, the Microsoft Server 2003 interface looks much like the Microsoft Windows NT 4 interface, but enough differences exist that you might find yourself periodically stymied by a “missing” function. This appendix lists some of the components...
that were renamed, moved, or introduced since the first release of Windows NT 4. These components are listed by their Windows NT name if they have a new name in Windows Server 2003.

---

**Clipboard Viewer**

Clipboard Viewer was renamed ClipBook Viewer. ClipBook Viewer shows any information you copied to the clipboard. This information can be stored permanently in your Local ClipBook and shared with other users. The Local ClipBook opens when you start ClipBook Viewer.

The ClipBook service is not started by default. To set up the service, follow these steps:

1. Launch Services from the Administrative tools menu, and double-click the ClipBook service.
2. Click the Dependencies tab. The ClipBook service is dependent on two other services, Network DDE and Network DDE DSDM. Check both of these services to make sure they are set to start automatically and that they have, in fact, started.
3. Return to the ClipBook service, and set it to start automatically. Click Apply and then Start.
4. Then, to start ClipBook Viewer, select Run from the Start menu, type `clipbrd`, and then press Enter.

---

**Compression Agent**

Windows Server 2003 doesn’t include Compression Agent. You can compress NTFS drives by following these steps:

1. Open My Computer.
2. Right-click the drive you want to compress, and choose Properties from the shortcut menu.
3. On the General tab, select Compress Drive To Save Disk Space. Click OK.

To compress a single file or folder, follow these steps:

1. Open Microsoft Windows Explorer. Right-click the file or folder to be compressed, and choose Properties from the shortcut menu.
2. Click Advanced. Select the Compress Contents To Save Disk Space check box. Click OK twice.
3. If you’re compressing a folder, you’re asked whether you want changes to apply to only the folder or to subfolders and files as well. Select the option you want. Click OK again.

The compression option is available only on disks formatted with NTFS. When you add or copy a file into a compressed folder, it is compressed automatically. If you move a file from a different NTFS drive into a compressed folder, it is also compressed. However, if you move a file from the same NTFS drive into a compressed folder, the file retains its original state, whether it is compressed or uncompressed. Compressed files can’t be encrypted, and encrypted files can’t be compressed unless you first decrypt the files.

---

**Computers Near Me**

When Microsoft Windows 2000 Professional clients are members of a workgroup, Computers Near Me appears inside My Network Places. Computers Near Me shows the computers and other resources that are accessible by members of the workgroup. Computers Near Me isn’t created when Windows Server 2003 is installed on a machine that is a member of a domain.

---

**Devices**

Devices has been renamed Device Manager and is located in Computer Management. On Windows Server 2003, right-click My Computer on the Start menu and choose Manage from the shortcut menu. In the console, expand System Tools if necessary and click Device Manager.

From a Windows Server 2003, an administrator can view Device Manager on a remote computer by following these steps:

1. Launch Active Directory Users and Computers.
2. In the console pane under the appropriate domain, click Computers.
3. In the details pane, right-click the computer name and select Manage.
4. In the new Computer Management window, click System Tools and then Device Manager.

---

**Dial-Up Networking**

You can find Dial-Up Networking in Network Connections in Control Panel. Unless you’re logged on as an administrator or a member of the Administrators group, some features of Network and Dial-Up Connections aren’t available.
Disk Administrator

Disk Administrator has been renamed Disk Management. Disk Management is a graphical tool for managing disks and volumes. It supports partitions, logical drives, new dynamic volumes, and remote disk management. To open Disk Management, right-click My Computer on the Start menu and choose Manage from the shortcut menu. In the console pane, expand Storage, if necessary, and then click Disk Management.

Find

In Windows Server 2003, Find has been renamed Search and it is located on the Start menu.

MS-DOS Prompt

The MS-DOS prompt was renamed the Command Prompt and is now located on the Accessories menu. (Actually, Microsoft Windows NT 4, Windows 2000, and Windows XP also call it a command prompt, but Microsoft Windows 95 and Microsoft Windows 98 do not.) The Command Prompt comes with a number of useful functions, including file and folder autocompletion.

You set Command Prompt options such as color and font by right-clicking the Command Prompt title bar and selecting Properties; in the Apply Properties To Shortcut dialog box, select the Modify Shortcut That Modified This Window option. To set these options for a single session, right-click the Command Prompt title bar and choose Properties; in the Apply Properties To Shortcut dialog box, select the Apply Properties To Current Window Only option.

My Briefcase

You can now access the Briefcase, a default presence on the Windows NT 4 desktop, by right-clicking the desktop and selecting New and then Briefcase. A briefcase is created and placed on the desktop.

My Documents

My Documents is a new folder on every Windows Server 2003 that acts as the default location for saved files. Inside My Documents is the subfolder My Pictures, the default location for graphics files. These folders are, by default, located in %SystemDrive%\Documents and
Settings\username on the system drive. My Documents is one of the special folders that can be redirected to a location on the network. See Chapter 11 for information about using Group Policy for folder redirection.

**Network Neighborhood**

Network Neighborhood was replaced by My Network Places, which shows the shared computers, files and folders, printers, and other resources on the network to which your computer is connected. Network Connections (Control Panel) displays your Internet, LAN, and dial-up connections.

My Network Places is not on the desktop any longer. To see it, start Windows Explorer and click My Network Places in the console pane.

**Personalized Menus**

By default, Windows Server 2003 uses personalized menus for the Start menu and its offshoots, but only if you are using the Classic Start menu. This means that the system keeps track of how often you access items on each menu and places the most frequently used items at the top.

To return to menus where all items are shown, right-click Start and choose Properties. On the Start Menu tab, click Customize next to the Classic Start menu. (If you are using the default Start menu, personalized menus can’t be turned off.) In the Customize Classic Start Menu dialog box, clear the check mark next to Use Personalized Menus. Click OK twice.

**Start Menu**

The Start menu isn’t new, but it has changed somewhat from Windows NT 4. To customize the Start menu, right-click Start and select Properties. Click the Start Menu tab and then Customize for the menu style you have.

**System Information**

System Information displays your system configuration data. To see System Information, select Help and Support from the Start menu. Under Support Tasks, find the Tools entry and click System Information. In the details pane, select the type of system specifics you’re looking for.
If you want to cut to the chase, select Run from the startup menu and type `msinfo32` for detailed system information.

From a machine running Windows Server 2003, you can view System Information on a remote computer by following these steps:

1. Launch Active Directory Users and Computers.
2. In the console pane under the appropriate domain, click Computers.
3. In the details pane, right-click the computer name and select Manage.
4. In the new Computer Management window, click System Tools and then System Information.

**TCP/IP**

To install, remove, or configure TCP/IP in Windows Server 2003, click the Start menu and then select Programs. Then select Accessories, followed by Communications, and finally Network Connections. Right-click the connection and select Properties.

**User Manager**

In Windows Server 2003, what was User Manager is now Local Users and Groups and is located in Computer Management. Right-click My Computer, and choose Manage from the shortcut menu. A domain controller does not have this option. Domain accounts are managed with Active Directory Users and Computers.

**User Manager for Domains**

Most of the functions of User Manager for Domains were replaced by Active Directory Users and Computers. In Windows Server 2003, Active Directory Users and Computers is on the Administrative Tools menu. Active Directory Domains and Trusts is used for creating and managing trust relationships.

**View Options**

In Windows Server 2003, View Options is called Folder Options and is on the Tools menu in many places, including My Computer, My Documents, My Network Places, and Control Panel. Use Folder Options to change the appearance of your desktop and folder.
content and to specify how folders open. You can also specify whether folders open with a single click or a double click, and you can set how folders display.

**Windows NT Explorer**

Windows NT Explorer has been renamed Windows Explorer and is located on the Accessories menu.
Appendix C

Optional Components

Accessories and Utilities .................................................. 1346
Certificate Services ....................................................... 1348
Distributed File System (DFS) ............................................. 1348
E-mail Services .............................................................. 1348
Fax Services ................................................................. 1348
Indexing Service ........................................................... 1348
Internet Explorer Enhanced Security Configuration ................. 1349
Management and Monitoring Tools ..................................... 1349
Microsoft .NET Framework 2.0 .......................................... 1349
Networking Services ....................................................... 1350
Other Network File and Print Services ................................. 1350
Remote Installation Services ............................................. 1351
Remote Storage ............................................................. 1351
Security Configuration Wizard .......................................... 1351
Subsystem for UNIX-Based Applications ............................. 1351
Terminal Server ............................................................. 1351
Terminal Server Licensing ................................................ 1351
UDDI Services .............................................................. 1351
Update Root Certificates .................................................. 1352
Windows Media Services ................................................ 1352
Windows SharePoint Services ............................................ 1352

The Microsoft Windows Server 2003 platforms have a number of optional components you can install or remove to configure your system the way you want it. The availability
of some components depends on the version of Windows Server 2003 you have and
which release of Windows Server 2003 you have.

To add or remove one of these optional components, open Control Panel, click Add Or
Remove Programs, and then click the Add/Remove Windows Components icon on the
left side of the window. The various components are grouped by type, with the currently
installed components selected.

To remove a component, clear its check box; to add a component, select its check box.
After you make your selections, click Next. Click Next again, and your Windows compo-
nents are updated. You might be prompted to insert your Windows installation CD-ROM.
After the update completes, click Finish. Depending on the changes you're making, you
might be prompted to reboot the server, so it's best to add or remove components when
you can afford to have the server offline long enough to reboot.

---

**Accessories and Utilities**

Within the Accessories And Utilities grouping, there are additional component groups.
To see the specifics of any component grouping, highlight the grouping and click Details.
If the Details button is unavailable, you are highlighting an individual component and
not a group of components.

**Accessibility Wizard**

The Accessibility Wizard allows you to configure your system to make it more accessible
to those with special vision, hearing, and mobility needs. Installed with the wizard are
additional accessibility tools, including Narrator, Magnifier, and On-Screen Keyboard, as
well as the Utility Manager to manage the configuration of these utilities.

**Accessories**

*Accessories* is a grouping of applications and features designed for a single use or purpose.
These include the following:

- **Calculator**  Provides a simple, onscreen graphical calculator
- **Character Map**  Displays all the characters in any installed font, and allows you to
insert special characters and symbols into your current document
- **Clipboard Viewer**  Enables you to view and save the contents of the clipboard
- **Desktop Wallpaper**  Provides additional background images and pictures for
enhancing your Windows desktop
■ **Document Templates**  Allows opening of new documents using the right mouse button

■ **Mouse Pointers**  Provides additional mouse pointers, including larger pointers and animated pointers

■ **Paint**  Provides a basic bitmap painting program

■ **WordPad**  Provides a simple word processor that can read Microsoft Word documents and handle ASCII text documents

**Communications**

Communications is a grouping of two simple programs, as described next, that enhance the communications capabilities of your server:

■ **Chat**  Installs a useful chat application, but doesn’t create an icon for it on your Start menu. To use Chat, open the Start menu, choose Run, and type `Winchat.exe`.

■ **HyperTerminal**  Uses a modem (or null modem cable) to connect to other computers or online services that still require terminal emulation.

**Active Directory Services**

New to Windows Server 2003 R2 are the following three optional Active Directory Services:

■ **Active Directory Application Mode (ADAM)**  A special version of Active Directory that can be used by applications to store data specific to the application

■ **Active Directory Federation Service (ADFS)**  Used for providing single sign-on to federated Web services

■ **Identity Management for UNIX**  Installs Server for NIS, password synchronization, and administrative components to support Active Directory running as the master NIS server.

**Application Server**

Application server installs the necessary components to enable Web applications, including the following ones:

■ **Internet Information Services (IIS)**  Installs various components, including Web server, NNTP, FTP, SMTP, Internet Printing, and the Background Intelligent Transfer Service (BITS)
- **COM+ access**  Allows the server to host COM+ distributed application components
- **DTC access**  Allows DTC applications for network transactions
- **Message Queuing**  Installs MSMQ for routing, security, and transactional support of messages

**Certificate Services**
Microsoft Certificate Services includes a certificate authority (CA) server that can issue public-key security certificates. It also includes support for adding Web pages to your Web server that allow you to submit and issue certificates. Refer to Chapter 21, Chapter 22, and Chapter 24 for a detailed discussion of the security and cryptographic capabilities of Windows Server 2003.

**Distributed File System (DFS)**
DFS installs the DFS Replication Service, DFS management tools, and DFS diagnostic and configuration tools. For more information about DFS, see Chapter 20.

**E-mail Services**
E-mail services installs the POP3 service and POP3 service Web administration tool to provide e-mail retrieval and sending abilities.

**Fax Services**
This component allows you to send and receive faxes with your Windows server. This component is not available on 64-bit versions of Windows Server 2003.

**Indexing Service**
This component indexes your existing documents to allow for fast, full-text searches across those documents. Chapter 31 includes an in-depth discussion of the Indexing Service.
Internet Explorer Enhanced Security Configuration

This component lets you restrict which Internet and intranet Web sites can be accessed by administrators and non-administrators using Internet Explorer. It’s a good idea never to browse the Web from a server, so this component should generally be enabled.

Management and Monitoring Tools

Management And Monitoring Tools is a group of several management and monitoring applications or protocols, as described here:

- **Connection Manager Administration Kit**  Adds the Connection Manager Administration Kit for creating customized remote access connections
- **Connection Point Services**  Adds the Phone Book Service
- **File Server Management**  Adds the File Server Management Console (FSMC), as described in Chapter 20
- **File Server Resource Management**  Adds the ability to manage directory quotas, file screening, and storage reports
- **Hardware Management**  Adds tools for managing hardware
- **Network Monitor Tools**  Allows you to capture and analyze network traffic at the packet level
- **Print Management Component**  Adds the new Printer Management console
- **Simple Network Management Protocol**  Provides SNMP support, allowing monitoring and reporting of the activity of a variety of network devices
- **Storage Manager for SANs**  Adds the new Storage Manager for SANs snap-in
- **WMI SNMP Provider**  Provides access to SNMP information via Windows Management Instrumentation
- **WMI Windows Installer Provider**  Enables client applications to use WMI to get Windows Installer information

Microsoft .NET Framework 2.0

This installs version 2.0 of the .NET Framework. Note that the installation of several other optional components will automatically install the .NET Framework.
Networking Services

Networking Services is a group of optional networking components you can add. The components in the Networking Services group include the following:

- **Domain Name System (DNS)**  Adds the Microsoft dynamic DNS server
- **Dynamic Host Configuration Protocol (DHCP)**  Adds a DHCP server to automatically assign IP addresses and configuration information to network client computers
- **Internet Authentication Service**  Adds support for the RADIUS protocol for dial-up and VPN users
- **Remote Access Quarantine Service**  Adds the ability for quarantined remote clients to be removed from the segregated network
- **RPC over HTTP Proxy**  Enables RPC/DCOM over HTTP by way of IIS
- **Simple TCP/IP Services**  Provides support for a variety of minor TCP/IP services, including Echo and Quote of the Day
- **Windows Internet Name Service (WINS)**  Adds a WINS server for supporting NetBIOS names in mixed-mode networks

Other Network File and Print Services

Other Network File and Print Services is a group of five file and print services that provide support for clients on other operating systems. Components include the following:

- **Common Log File System**  A new common logging file system introduced in Server 2003 R2
- **File Services for Macintosh**  Supports Apple Macintosh computers in both storing files and accessing files on Windows Server 2003 machines
- **Microsoft Services for NFS**  Installs Server for NFS, Client for NFS, and the necessary authentication services (See Chapter 27 for more on Services for NFS.)
- **Print Services for Macintosh**  Supports Macintosh computers printing to Windows Server 2003 printers
- **Print Services for UNIX**  Supports UNIX and Linux users printing to Windows Server 2003 printers using line printer remote (LPR)
Remote Installation Services
RIS adds support for remote installation of Windows onto client computers with appropriate remote boot-enabled network cards.

Remote Storage
Remote Storage provides services and tools to allow you to store less frequently accessed files and data on tape or magneto-optical disks, freeing up hard disk space.

Security Configuration Wizard
This component installs the new Security Configuration Wizard introduced in Windows Server 2003 SP1, which is covered in Chapter 22.

Subsystem for UNIX-Based Applications
New to Windows Server 2003 R2, this component installs a complete UNIX application execution environment. See Chapter 27 for details.

Terminal Server
This configures the server to support multiple user sessions, delivering Windows-based applications and the Windows desktop to almost any computing device, including devices that cannot run Windows. See Chapter 30 for more information about Windows Terminal Server.

Terminal Server Licensing
Terminal Server Licensing provides Terminal Server clients with licenses for accessing Terminal Servers on your network. The Terminal Server license server must run on a domain controller.

UDDI Services
Universal Description, Discovery and Integration (UDDI) is used to store and retrieve information about Web services.
**Update Root Certificates**
Microsoft Windows products come with a set of certificate authorities (CAs) that Microsoft deems trustworthy. If a certificate originated from an untrusted CA, the user is prompted with the option to establish trust with that CA. Often, users aren’t knowledgeable about the subject matter. Update Root Certificates lessens the burden by updating the system’s lists of trusted CAs by contacting the Windows Update Web site. This option is automatically selected in default installations.

**Windows Media Services**
Installs the necessary components to support streaming of digital media across networks using Windows Media Services.

**Windows SharePoint Services**
Windows SharePoint Services 2.0 provides for Web-based collaboration and document sharing.
Appendix D

Using the Microsoft Windows Server 2003 Recovery Console

Recovery Console Limitations..............................................1353
Starting the Recovery Console.............................................1354
Using Recovery Console Commands...................................1355

The Recovery Console is a powerful tool that enables you to start a computer from the Windows CD-ROM (or a hard drive) and use a command prompt interface to recover a Windows system that does not start. Use the Recovery Console to perform recovery tasks such as the following:

- Fixing disk errors
- Fixing the Master Boot Record (MBR) and boot sector
- Starting and stopping services
- Extracting and copying files

Security Alert  Third-party products such as Winternals ERD Commander (http://www.winternals.com) can boot Windows Server 2003 systems from a CD-ROM, access NTFS partitions, and even reset the local Administrator password. This functionality is useful for administrators, but it also serves as a stern reminder to keep servers physically secure.

Recovery Console Limitations

Although the Recovery Console can log on to a Windows Server 2003 installation and access any NTFS, FAT, or FAT32 drives, by default it can access only the root folder of each drive, the %SYSTEMROOT% folder and subfolders, the Cmdcons folder (if present), and any removable media drives attached to the system. The Recovery Console also cannot copy files from the hard disk to a floppy disk by default, although it can copy files from a floppy disk to the hard disk, or from one hard disk to another.
To enable full access to hard drives and removable media from the Recovery Console, change the Recovery Console settings in the relevant Group Policy object, as discussed in Microsoft Knowledge Base article 310497. Although this makes it easier for an attacker to use the Recovery Console as an attack tool, the attacker must gain physical access to the server or gain remote access by using Emergency Management Services (EMS) and a local administrator password. An attacker with this level of access can obtain complete control of the server regardless of Group Policy settings and without using the Recovery Console.

**Starting the Recovery Console**

To start the Recovery Console, follow these steps:

1. Start up the system from the Windows CD-ROM disc, or select Microsoft Windows Recovery Console from the Windows Boot Menu if you installed Recovery Console on the system as discussed in Chapter 36.

2. To load mass storage drivers not included with Windows—such as drivers for a Small Computer System Interface (SCSI) or RAID controller—press F6 when Windows Setup starts.

3. Press F10 while Windows Setup is loading (when it says “Press F6”), or type R after Setup loads, to repair an existing Windows Server 2003 installation.

4. Type the number corresponding to the appropriate Windows Server 2003 installation and then press Enter.

5. Type the password for the local Administrator account.

You can use the Recovery Console even if you disabled the local Administrator account. For more information, see Microsoft Knowledge Base article 814777.

---

**Note** To log on to a domain controller, use the directory services restore mode password. To change the password, restart the domain controller in directory service restore mode and then type `Net User Administrator Password` at a command prompt, replacing `Password` with the new password (or use the Local User and Groups snap-in). See Microsoft Knowledge Base articles 239803 and 888301 for more information.
Using Recovery Console Commands

After logging on to the Recovery Console, use the following commands to administer the system:

- **Attrib**  Changes the attributes of a file or folder.
- **Batch**   Executes commands specified in a text file, and outputs them to screen, or another text file.
- **Bootcfg** Displays and modifies the Boot.ini file (as discussed in Chapter 40).
- **Cd (Chdir)** Changes the current folder. Enclose folder names that contain spaces with quotation marks.
- **Chkdsk**  Checks, repairs, or recovers a drive. Also marks bad sectors and recovers readable information.
- **Cls**    Clears the screen.
- **Copy**   Copies a single file. Does not work with folders or wildcard (*) characters.
- **Delete (Del)** Deletes a single file. Does not work with wildcard (*) characters.
- **Dir**    Displays a list of files and subfolders in a folder.
- **Disable** Disables a system service or driver.
- **Diskpart** Manages disk partitions and volumes.
- **Enable** Enables a system service or driver.
- **Exit**   Quits the Recovery Console and restarts the computer.
- **Expand** Expands a compressed .CAB file.
- **Fixboot** Writes new Windows Server 2003 boot sector code on the boot partition.
- **Fixmbr** Repairs the master boot record (MBR) of the boot partition.

**Important** The Fixmbr command has the potential to damage partition tables if a virus is present or a hardware problem exists. This command might lead to inaccessible partitions. Check the system with an up-to-date antivirus program before using the Fixmbr command.

- **Format** Formats the specified drive.
- **Help**  Displays help for the Recovery Console.
- **Listsvc**  Lists all available services, drivers, and their startup types.

**Note**  Listsvc uses the %SYSTEMROOT%\System32\Config\System hive. If the System hive is damaged or missing, Listsvc might not operate properly.

- **Logon**  Lists all detected installations of Windows Server 2003, Microsoft Windows XP, Windows 2000, and Windows NT, and then requests the local administrator password for the installation you chose. If three attempts to log on fail, the console quits and the computer restarts.

- **Map**  Lists drive letters, file system types, partition sizes, and mappings to physical devices.

- **Md (Mkdir)**  Creates folders. Does not work with wildcard (*) characters.

- **More**  Displays the contents of a text file.

- **Rd (Rmdir)**  Deletes the specified folder. The folder must be empty.

- **Ren (Rename)**  Renames a file.

- **Set**  Displays or modifies four recovery console environment options:
  - **Allowwildcards**  Enables wildcards in the Recovery Console
  - **Allowallpaths**  Allows access to all folders
  - **Allowremovablemedia**  Enables copying files to removable media devices
  - **Nocopyprompt**  Enables the copy command to overwrite files without prompting

**Note**  The Set command is disabled by default. To enable it, enable the Recovery Console: Allow Floppy Copy And Access To All Drives And Folders policy in Group Policy or the Local Security Policy.

- **Systemroot**  Sets the current working folder to the %SYSTEMROOT% folder.

- **Type**  Displays the contents of a text file.

**More Info**  For more information about a Recovery Console command, type the command followed by /? at the Recovery Console command prompt, or see Microsoft Knowledge Base articles 326215 and 314058.
Appendix E

Using the Microsoft Windows Server 2003 Support Tools


To use the Support Tools, install them from the \Support\Tools folder of the Windows Server 2003 CD-ROM, from a service pack CD-ROM, or from the Microsoft Download Center at http://www.microsoft.com/downloads/. Then open a command-prompt window, switch to the \Program Files\Support Tools folder, and type the appropriate commands, as listed in the following table:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Filename</th>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL Diagnostics</td>
<td>Acldiag.exe</td>
<td>Cmd</td>
<td>Diagnoses and troubleshoots permissions problems with Active Directory objects; reapplies security delegation templates.</td>
</tr>
<tr>
<td>Active Directory Replication Monitor</td>
<td>Replmon.exe</td>
<td>GUI</td>
<td>Displays and controls Active Directory replication information.</td>
</tr>
<tr>
<td>Active Directory Search Tool</td>
<td>Search.vbs</td>
<td>Cmd</td>
<td>Searches a Lightweight Directory Access Protocol (LDAP) directory such as Active Directory.</td>
</tr>
<tr>
<td>ADSI Edit</td>
<td>Adsiedit.msc</td>
<td>GUI</td>
<td>Adds, moves, and deletes objects and object attributes within Active Directory.</td>
</tr>
<tr>
<td>Advanced Power Management Status</td>
<td>Apmstat.exe</td>
<td>Cmd</td>
<td>Provides information about Advanced Power Management (APM) features in older computers.</td>
</tr>
<tr>
<td>Application Deployment Diagnosis</td>
<td>Adddiag.exe</td>
<td>Cmd</td>
<td>Displays the status of software deployed to the local computer using Group Policy.</td>
</tr>
<tr>
<td>Binary File Difference Finder</td>
<td>Bindiff.exe</td>
<td>Cmd</td>
<td>Compares two binary files, and displays the differences.</td>
</tr>
<tr>
<td>Tool</td>
<td>Filename</td>
<td>Format</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>BITS Administration Utility</td>
<td>Bitsadmin.exe</td>
<td>Cmd</td>
<td>Administers the Background Intelligent Transfer Service (BITS), which manages background file-transfers for Internet Information Services (IIS).</td>
</tr>
<tr>
<td>Browser Status</td>
<td>Browstat.exe</td>
<td>Cmd</td>
<td>Displays network Browser status.</td>
</tr>
<tr>
<td>Cabinet Tool</td>
<td>Cabarc.exe</td>
<td>Cmd</td>
<td>Creates, views, and extracts compressed .CAB files.</td>
</tr>
<tr>
<td>Clone Principal</td>
<td>Clonepr.dll</td>
<td>Cmd</td>
<td>Creates clones of Windows NT 4 users and groups so that they can be migrated to a Windows Server 2003 forest.</td>
</tr>
<tr>
<td>Dependency Walker</td>
<td>Depends.exe</td>
<td>GUI</td>
<td>Scans a Windows module, and reports all dependencies. Also displays the minimum set of files the application requires to load, and what functions the module uses or exports.</td>
</tr>
<tr>
<td>Device Console Utility</td>
<td>Devcon.exe</td>
<td>Cmd</td>
<td>Provides Device Manager functionality at a command prompt.</td>
</tr>
<tr>
<td>DFS and SYSVOL Replication Topology Analysis Tool</td>
<td>Topchk.cmd</td>
<td>Cmd</td>
<td>Displays the file replication service (FRS) replication topology and replication partners. Use in conjunction with the Ntfrsutl Ds command.</td>
</tr>
<tr>
<td>DHCP Server Locator Utility</td>
<td>Dhcploc.exe</td>
<td>Cmd</td>
<td>Displays and monitors Dynamic Host Configuration Protocol (DHCP) servers on the subnet, as well as any unauthorized DHCP servers.</td>
</tr>
<tr>
<td>Directory Disk Usage</td>
<td>Diruse.exe</td>
<td>Cmd</td>
<td>Displays and monitors directory sizes and compression info.</td>
</tr>
<tr>
<td>Directory Services ACL Editor</td>
<td>Dsacls.exe</td>
<td>Cmd</td>
<td>Manages access control lists (ACLs) for Active Directory objects.</td>
</tr>
<tr>
<td>Directory Services Utility</td>
<td>Dsastat.exe</td>
<td>Cmd</td>
<td>Compares two directory trees within a domain, or across different domains (when comparing copies of the global catalog).</td>
</tr>
<tr>
<td>Diskprobe</td>
<td>Dskprobe.exe</td>
<td>Gui</td>
<td>Directly edits disk sector information (including the master boot record, or MBR).</td>
</tr>
<tr>
<td>Disk Manager Diagnostics</td>
<td>Dmdiag.exe</td>
<td>Cmd</td>
<td>Displays detailed diagnostic information about local hard disk drives.</td>
</tr>
<tr>
<td>Distributed File System Utility</td>
<td>Dfsutil.exe</td>
<td>Cmd</td>
<td>Manages Distributed File System (DFS), as discussed in Chapter 20.</td>
</tr>
<tr>
<td>DNS Lint</td>
<td>Dnslint.exe</td>
<td>Cmd</td>
<td>Tests Domain Name System (DNS) records for delegation problems or other errors.</td>
</tr>
<tr>
<td>Tool</td>
<td>Filename</td>
<td>Format</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DNS Server Troubleshooting Tool</td>
<td>Dnscmd.exe</td>
<td>Cmd</td>
<td>Allows administrators to view and modify DNS servers, zones, and resource records.</td>
</tr>
<tr>
<td>Domain Controller Diagnostic Tool</td>
<td>Dcdiag.exe</td>
<td>Cmd</td>
<td>Analyzes and creates reports about the state of domain controllers.</td>
</tr>
<tr>
<td>Extensible Performance Counter List</td>
<td>Exctrlst.exe</td>
<td>Gui</td>
<td>Displays and manages performance counters registered in the Registry.</td>
</tr>
<tr>
<td>Fault Tolerant Disk Mounter</td>
<td>Ftonline.exe</td>
<td>Cmd</td>
<td>Mounts Windows NT 4 fault-tolerant disk sets.</td>
</tr>
<tr>
<td>File and Directory Comparison</td>
<td>Windiff.exe</td>
<td>Cmd, GUI</td>
<td>Compares ASCII text files or folders.</td>
</tr>
<tr>
<td>File Replication Utility</td>
<td>Ntfrsutil.exe</td>
<td>Cmd</td>
<td>Displays the status of the FRS.</td>
</tr>
<tr>
<td>File Version</td>
<td>Filever.exe</td>
<td>Cmd</td>
<td>Reports version information for a file or folder.</td>
</tr>
<tr>
<td>FRS Connection Status Report</td>
<td>Connstat.cmd</td>
<td>Cmd</td>
<td>Creates a report summarizing FRS replication status by processing the output generated by the Ntfrsutil.exe Sets command.</td>
</tr>
<tr>
<td>FRS Health Check</td>
<td>Health_chk.cmd</td>
<td>Cmd</td>
<td>Displays the FRS status and health of the specified domain controller.</td>
</tr>
<tr>
<td>FRS Inbound and Outbound Logs</td>
<td>Iologsum.cmd</td>
<td>Cmd</td>
<td>Displays information about FRS replication. Must be used with the Ntfrsutil Inlog, Ntfrsutil Outlog, or Ntfrsutil Idtable commands.</td>
</tr>
<tr>
<td>Get Security ID</td>
<td>Getsid.exe</td>
<td>Cmd</td>
<td>Verifies whether the user account database is corrupt by comparing the security identifiers (SIDs) of the same account on two domain controllers.</td>
</tr>
<tr>
<td>Global Flags Editor</td>
<td>Gflags.exe</td>
<td>GUI</td>
<td>Edits global registry settings or flags in use by the kernel.</td>
</tr>
<tr>
<td>HTTP Configuration Utility</td>
<td>Httpcfg.exe</td>
<td>Cmd</td>
<td>Manages the HTTP application programming interface (API) so that applications can receive data using HTTP without using IIS.</td>
</tr>
<tr>
<td>Tool</td>
<td>Filename</td>
<td>Format</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IAS Parse Tool</td>
<td>Iaspars.exe</td>
<td>Cmd</td>
<td>Parses Internet Authentication Service (IAS) and Remote Access Service (RAS) log files, and outputs the results to the screen or to an IAS or Open Database Connectivity (ODBC) format file.</td>
</tr>
<tr>
<td>Kerberos Keytab Setup</td>
<td>Ktpass.exe</td>
<td>Cmd</td>
<td>Enables a non–Windows Server 2003 Kerberos service (such as a UNIX-based service) to be a security principal in Active Directory.</td>
</tr>
<tr>
<td>Kerberos Setup</td>
<td>Ksetup.exe</td>
<td>Cmd</td>
<td>Configures Windows Server 2003 clients to use a Kerberos V5 realm.</td>
</tr>
<tr>
<td>LDP Tool</td>
<td>Ldp.exe</td>
<td>GUI</td>
<td>Performs LDAP operations.</td>
</tr>
<tr>
<td>Manipulate Service Principal Names For Accounts</td>
<td>Setspn.exe</td>
<td>Cmd</td>
<td>Manipulates Service Principal Names (SPNs) for Active Directory service accounts.</td>
</tr>
<tr>
<td>Memory Pool Monitor</td>
<td>Poolmon.exe</td>
<td>Cmd</td>
<td>Displays information about the system's memory pool and general memory usage.</td>
</tr>
<tr>
<td>Memory Profiling Tool</td>
<td>Memsnap.exe</td>
<td>Cmd</td>
<td>Writes a snapshot of the memory resources used by all processes to a log file.</td>
</tr>
<tr>
<td>Move Users</td>
<td>Movetree.exe</td>
<td>Cmd</td>
<td>Moves objects (such as users) between domains in a forest, leaving all linked group policies intact.</td>
</tr>
<tr>
<td>Network Connectivity Tester</td>
<td>Netdiag.exe</td>
<td>Cmd</td>
<td>Troubleshoots network connectivity.</td>
</tr>
<tr>
<td>Network Monitor Capture Utility</td>
<td>Netcap.exe</td>
<td>Cmd</td>
<td>Uses the Network Monitor driver to capture frames to a log file.</td>
</tr>
<tr>
<td>Nltest</td>
<td>Nltest.exe</td>
<td>Cmd</td>
<td>Queries the status of trusts, lists domain controllers, forces a shutdown, or forces a user database into sync on a Windows NT domain.</td>
</tr>
<tr>
<td>Port Query</td>
<td>Portqry.exe</td>
<td>Cmd</td>
<td>Displays detailed Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port status information.</td>
</tr>
<tr>
<td>Process Viewer</td>
<td>Pviewer.exe</td>
<td>GUI</td>
<td>Displays processes, changes process priorities, and kills processes.</td>
</tr>
<tr>
<td>Remote Command Line</td>
<td>Remote.exe</td>
<td>Cmd</td>
<td>Allows users to connect to the computer remotely using named pipes (with no authentication) and run commands.</td>
</tr>
<tr>
<td>Remote Storage Diagnostic Utility</td>
<td>Rsdiag.exe</td>
<td>Cmd</td>
<td>Queries and reports on remote storage databases.</td>
</tr>
<tr>
<td>Tool</td>
<td>Filename</td>
<td>Format</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Remote Storage File Analysis Utility</td>
<td>Rsdir.exe</td>
<td>Cmd</td>
<td>Displays information about files in remote storage.</td>
</tr>
<tr>
<td>Security Administration Tools</td>
<td>Sidwalk.exe, Showaccs.exe, Sidwalk.msc</td>
<td>Cmd, Cmd, GUI</td>
<td>Manages ACLs.</td>
</tr>
<tr>
<td>Security Descriptor Check Utility</td>
<td>Sdcheck.exe</td>
<td>Cmd</td>
<td>Displays the effective access controls on an object in Active Directory.</td>
</tr>
<tr>
<td>Service Pack Check</td>
<td>Spcheck.exe</td>
<td>Cmd</td>
<td>Creates a file listing the service pack version of key system files.</td>
</tr>
<tr>
<td>Windows Domain Manager</td>
<td>Netdom.exe</td>
<td>Cmd</td>
<td>Administers domains and trust relationships.</td>
</tr>
<tr>
<td>Windows Installer Cleanup Utility</td>
<td>Msicuu.exe</td>
<td>GUI</td>
<td>Removes registry entries from a faulty installation.</td>
</tr>
<tr>
<td>Windows Installer Zapper</td>
<td>Msizap.exe</td>
<td>Cmd</td>
<td>Removes registry entries from a faulty installation. Use only as a last resort.</td>
</tr>
<tr>
<td>Xcacls.exe</td>
<td>Xcacls.exe</td>
<td>Cmd</td>
<td>Sets and displays file ACLs.</td>
</tr>
</tbody>
</table>
Glossary

Special Characters

802.11 Refers to a family of specifications for wireless networking.

802.11a An extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band.

802.11b (also called Wi-Fi) An extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b is a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.

802.11g An extension to 802.11 that applies to wireless LANS and provides 54 Mbps transmission in the 2.4 GHz band. 802.11g is backward compatible with 802.11b allowing the two to work together.

A

Access control entry (ACE) An entry in an access control list (ACL) that defines the level of access for a user or group.

Access control list (ACL) A set of data associated with a file, directory, or other resource that defines the permissions users or groups have for accessing it. In Active Directory, the ACL is a list of access control entries (ACEs) stored with the object it protects. In Microsoft Windows NT, an ACL is stored as a binary value called a security descriptor.

Account lockout A security feature that disables a user account if failed logons exceed a specified number in a specified period of time. Locked accounts can’t log on and must be unlocked by an administrator.


Active Directory-integrated zone A DNS (Domain Name System) zone stored in Active Directory so it has Active Directory security features and can be used for multimaster replication.

ActiveX A loosely defined set of technologies that allows software components to interact with each other in a networked environment.

ActiveX component Reusable software component that adheres to the ActiveX specification and can operate in an ActiveX-compliant environment.
Address  A precise location where a piece of information is stored in memory or on disk. Also, the unique identifier for a node on a network. On the Internet, the code by which an individual user is identified. The format is username@hostname, where username is your user name, logon name, or account number, and hostname is the name of the computer or Internet provider you use. The host name might be a few words strung together with periods.

Address Resolution Protocol (ARP)  A TCP/IP and AppleTalk protocol that provides IP-address-to-MAC (media access control) address resolution for IP packets.

Administrative credentials  Logon information used to verify the identity of a member of the administrators group.

Advanced Configuration Power Interface (ACPI)  An industry specification, defining power management on a range of computer devices. ACPI compliance is necessary for devices to take advantage of Plug and Play and power management capabilities.

Allocation unit  The smallest unit of managed space on a hard disk or logical volume. Also called a cluster.

Anonymous FTP  A way to use the FTP program to log on to another computer to copy files when you don’t have an account on that computer. When you log on, enter anonymous as the user name and your address as the password. This gives you access to publicly available files. See File Transfer Protocol (FTP).

AppleTalk  Local area network architecture built into Macintosh computers to connect them with printers. A network with a Windows Server 2003 server and Macintosh clients can function as an AppleTalk network with the use of AppleTalk network integration (formerly Services for Macintosh).

Associate  To connect files having a particular extension to a specific program. When you double-click a file with the extension, the associated program is launched and the file you clicked is opened. In Windows, associated file extensions are usually called registered file types.

Asynchronous Transfer Mode (ATM)  A network technology based on sending data in cells or packets of a fixed size. It is asynchronous in that the transmission of cells containing information from a particular user isn’t necessarily periodic.

Attribute  A characteristic. In Windows file management, it is information that shows whether a file is read-only, hidden, compressed, encrypted, ready to be backed up (archived), or should be indexed.

Audit policy  Defines the type of security events to be logged. It can be defined on a server or an individual computer.

Authentication  Verification of the identity of a user or computer process.
In Windows Server 2003, Windows 2000, and Windows NT, authentication involves comparing the user’s security identifier (SID) and password to a list of authorized users on a domain controller.

**B**

**Backup domain controller (BDC)** In a Windows NT domain, a computer that stores a backup of the database that contains all the security and account information from the primary domain controller (PDC). The database is regularly and automatically synchronized with the copy on the PDC. A BDC also authenticates logons and can be promoted to a PDC when necessary. In a Windows Server 2003 or Windows 2000 domain, backup domain controllers aren’t required; all domain controllers are peers, and all can perform maintenance on the directory.

**Backup media pool** A logical set of backup storage media used by Windows Server 2003 Backup.

**Bandwidth** On a network, the transmission capacity of a communications channel stated in megabits per second (Mbps). For example, Ethernet has a bandwidth of 10 Mbps. Fast Ethernet has a bandwidth of 100 Mbps.

**Binding** A software connection between a network card and a network transport protocol (such as TCP/IP).

**BOOTP** Boot Protocol. Used on TCP/IP networks to enable a diskless workstation to learn its own IP address, the location of a BOOTP server on the network, and the location of a file to be loaded into memory to boot the machine. This allows a computer to boot without a hard disk or a floppy disk.

**Broadcasting** To simultaneously send a message to everyone on a network. See *multicasting*.

**Browser service** The service that maintains a current list of computers and provides the list to applications when needed. When a user attempts to connect to a resource in the domain, the Browser service is contacted to provide a list of available resources. The lists displayed in My Network Places and Active Directory Users and Computers (among others) are provided by the Browser service. Also called the Computer Browser service.

**C**

**Certificate** A credential used to prove the origin, authenticity, and purpose of a public key to the entity that holds the corresponding private key.

**Certificate authority (CA)** The service that accepts and fulfills certificate requests and revocation requests and that can also manage the policy-directed registration process a user completes to get a certificate.
Certificate revocation list (CRL)  A digitally signed list (published by a certificate authority) of certificates that are no longer valid.

Child domain  Domains located directly beneath another domain name (parent domain). For example, Engineering.scribes.com is a child domain of scribes.com, the parent domain. Also called a subdomain.

Child object  An object inside another object. For example, a file is a child object inside a folder, which is the parent object.

Cluster  A set of computers joined together in such a way that they behave as a single system. Clustering is used for network load balancing as well as fault tolerance. In data storage, the smallest amount of disk space that can be allocated for a file.

Cluster service  The collection of software on each node that manages all cluster-specific activity.

Codec  Technology that compresses and decompresses data, particularly audio or video. Codecs can be implemented in software, hardware, or a combination of both.

Console tree  The default left pane in Microsoft Management Console (MMC) that shows the items contained in a console.

Container  An Active Directory object that has attributes and is part of the Active Directory namespace. Unlike other objects, it doesn’t usually represent something concrete. It is a package for a group of objects and other containers.

D

Daemon  A background program that runs unattended, gathering information or performing other tasks.

Delegate  Assign administrative rights over a portion of the name-space to another user or group.

Directory service  A means of storing directory data and making it available to network users and administrators. For example, Active Directory stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information.

Disk quota  A limitation set by an administrator on the amount of disk space available to a user.

Distinguished name (DN)  In the context of Active Directory, “distinguished” means the qualities that make the name distinct. The distinguished name identifies the domain that holds the object, as well as the complete path through the container hierarchy used to reach the object.

Distributed file system (DFS)  A file management system in which files can be located on separate computers but are presented to users as a single directory tree.
DNS name servers  Servers that contain information about part of the Domain Name System (DNS) database. These servers make computer names available to queries for name resolution across the Internet. Also called domain name servers.

Domain  A group of computers that share a security policy and a user account database. A Windows Server 2003 domain is not the same as an Internet domain. See domain name.

Domain controller  A server in a domain that accepts account logons and initiates their authentication. In an Active Directory domain, a domain controller controls access to network resources and participates in replication.


Domain local group  A local group used on ACLs only in its own domain. A domain local group can contain users and global groups from any domain in the forest, universal groups, and other domain local groups in its own domain.

Domain name  In Active Directory, the name given to a collection of networked computers that share a common directory. On the Internet, the unique text name that identifies a specific host. A machine can have more than one domain name, but a given domain name points to only one machine. Domain names are resolved to IP addresses by DNS name servers.

Domain Name System (DNS)  A service on TCP/IP networks (the Internet included) that translates domain names into IP addresses. This allows users to employ friendly names like FinanceServer or Ourbusiness.com when querying a remote system, instead of using an IP address such as 198.45.233.59.

Domain naming master  The one domain controller assigned to handle the addition or removal of domains in a forest. See Operations Master.

DWORD  A data type consisting of four bytes in hexadecimal.

Dynamic Data Exchange (DDE)  Communication between processes implemented in the Windows family of operating systems. When programs that support DDE are running at the same time, they can exchange data by means of conversations. Conversations are two-way connections between two applications that transmit data alternately.

Dynamic Host Configuration Protocol (DHCP)  A TCP/IP protocol used to automatically assign IP addresses and configure TCP/IP for network clients.
Dynamic-link library (DLL)  A program module that contains executable code and data that can be used by various programs. A program uses the DLL only when the program is active, and the DLL is unloaded when the program closes.

Enterprise  Term used to encompass all of a business’s operation, including all remote offices and branches.

Environment variable  A string of environment information such as a drive, path, or filename associated with a symbolic name. The System option in Control Panel or the Set command from the command prompt can be used to define environment variables.

Ethernet  A local area network protocol. Ethernet supports data transfer rates of 10 Mbps and uses a bus topology and thick or thin coaxial, fiber-optic, or twisted-pair cabling. A newer version of Ethernet called Fast Ethernet supports data transfer rates of 100 Mbps, and an even newer version, Gigabit Ethernet, supports data transfer rates of 1000 Mbps.

Extended partition  A nonbootable portion of a hard disk that can be subdivided into logical drives. There can be only a single extended partition per hard disk.

Extensible Authentication Protocol (EAP)  An extension to the Point-to-Point Protocol (PPP) that allows the use of arbitrary authentication methods for validating a PPP Connection.

Extensible Markup Language (XML)  An abbreviated version of the Standard General Markup Language (SGML), it allows the flexible development of user-defined document types and provides a non-proprietary, persistent, and verifiable file format for the storage and transmission of text and data both on and off the Web.

External trust  A one-way or two-way transitive trust for providing access to a Windows NT 4 domain or a domain located in another forest that is not joined by a forest trust.

Failover  An operation that automatically switches to a standby database, server, or network if the primary system fails or is temporarily shut down for servicing. In server clusters, the process of taking resources off one node in a prescribed order and restoring them on another node.

Fault tolerance  The ability of a system to ensure data integrity when an unexpected hardware or software failure occurs. Many fault-tolerant computer systems mirror all operations—that is, all operations are done on two or more duplicate systems, so if one fails the other can take over.

File Transfer Protocol (FTP)  A method of transferring one or more files from one computer to another over a network
or telephone line. Because FTP has been implemented on a variety of systems, it’s a simple way to transfer information between usually incongruent systems such as a PC and a minicomputer.

**Firewall** A protective filter for messages and logons. An organization connected directly to the Internet uses a firewall to prevent unauthorized access to its network. See *proxy server*.

**Folder redirection** An option in Group Policy to place users’ special folders, such as My Documents, on a network server.

**Forest** A group of one or more Active Directory trees that trust each other through two-way transitive trusts. All trees in a forest share a common schema, configuration, and Global Catalog (GC). When a forest contains multiple trees, the trees don’t form a contiguous namespace. Unlike trees, a forest doesn’t need a distinct name.

**Forest trust** A transitive trust used to share resources between forests. It can be one-way or two-way.

**Fully qualified domain name (FQDN)** A domain name that includes the names of all network domains leading back to the root to clearly indicate a location in the domain namespace tree. An example of an FQDN is Accts.finance.dataflointl.com or Sales.europe.microsoft.com.

---

**G**

**Gateway** A device used to connect networks using dissimilar protocols so that information can be passed from one to another.

**Global catalog (GC)** Contains a full replica of all directory objects in its host domain plus a partial replica of all directory objects in every domain in the forest. A GC contains information about all objects in all domains in the forest, so finding information in the directory doesn’t require unnecessary queries across domains. A single query to the GC produces the information about where the object can be found.

**Global group** A group that can be used in its own domain and in trusting domains. However, it can contain user accounts and other global groups only from its own domain.

**Globally unique identifier (GUID)** Part of the identifying mechanism generated by Active Directory for each object in the directory. If a user or computer object is renamed or moved to a different name, the security identifier (SID), relative distinguished name (RDN), and distinguished name (DN) will change, but the GUID will remain the same.

**Group Policy** Setting of rules for computers and users in Windows Server 2003. Group Policy is able to store policies for file deployment, application deployment, logon/logoff
scripts, startup/shutdown scripts, domain security, Internet Protocol security (IPSec), and so on.

**Group Policy object (GPO)** A collection of policies stored in two locations: a Group Policy container (GPC) and a Group Policy template (GPT). The GPC is an Active Directory object that stores version information, status information, and other policy information (for example, application objects). The GPT is used for file-based data and stores software policy, script, and deployment information. The GPT is located in the system volume folder of the domain controller.

**Headless server** A server without a monitor, keyboard, mouse, or video card, which is administered remotely.

**Hive** One of five sections of the registry. Each hive is a discrete body of keys, subkeys, and values that record configuration information for the computer. Each hive is a file that can be moved from one system to another but can be edited only by using the Registry Editor.

**Host** Any device on the network that uses TCP/IP. A host is also a computer on the Internet you might be able to log on to. You can use FTP to get files from a host computer and use other protocols (such as Telnet) to make use of the host computer.

**Hosts file** A local ASCII text file that maps host names to IP addresses. Each line represents one host, starting with the IP address, one or more spaces, and then the host's name.

**Hypertext** A system of writing and displaying text that enables the text to be linked in multiple ways, available at several levels of detail. Hypertext documents can also contain links to related documents, such as those referred to in footnotes.

**Hypertext Markup Language (HTML)** A system used for writing pages for the World Wide Web. HTML allows text to include codes that define fonts, layout, embedded graphics, and hypertext links.

**Hypertext Transfer Protocol (HTTP)** The method by which Web pages are transferred over the network.

**IntelliMirror** A suite of technologies that allows a complete operating environment to follow the user to other computers, as well as offline. Components include the user’s profiles, data, and applications.

**Internet Authentication Service (IAS)** The Microsoft implementation of Remote Authentication Dial-In User Service (RADIUS), an authentication and accounting system used by many Internet Service Providers (ISPs). When a user connects to an ISP using a username and password, the
Internet Control Message Protocol (ICMP)  
A protocol used to report problems encountered with the delivery of data, such as unreachable hosts or unavailable ports. ICMP is also used to send a request packet to determine whether a host is available. The receiving host sends back a packet if it is available and functioning. See ping.

Internet Protocol (IP)  
The inter-network layer protocol used as a basis of the Internet. IP enables information to be routed from one network to another in packets and then reassembled when they reach their destination.

Internet Protocol version 6 (IPv6)  
The newest version of Internet Protocol, which is supported in Windows Server 2003. The earlier version of IP is version 4, also known as IPv4. IPng is an evolutionary upgrade and will coexist with version 4 for some time.

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)  
Transport protocols used in Novell NetWare networks.

IP number or IP address  
In IPv4, a four-part number separated by periods (for example, 165.113.245.2) that uniquely identifies a machine on the Internet. Every machine on the Internet has a unique IP number. In IPv6, this is a six-part hexadecimal number, separated by colons.

Internet Protocol security (IPSec)  
An Internet Engineering Task Force (IETF) standard for creating virtual private networks (VPNs).

Kerberos  
An identity-based security system that authenticates users at logon. It works by assigning a unique key, called a ticket, to each user who logs on to the network. The ticket is then embedded in messages to identify the sender of the message. The Kerberos security protocol is the primary authentication mechanism in Windows Server 2003 and Windows 2000 Server.

Kernel  
The part of the executive (or operating system) that manages the processor. The kernel performs thread scheduling and dispatching, interrupt and exception handling, and multiprocessor synchronization.

Layer Two Tunneling Protocol (L2TP)  
An extension to the Point-to-Point Protocol (PPP) used in conjunction with IPSec to provide VPN connections.

Lightweight Directory Access Protocol (LDAP)  
A protocol used to access a directory service. LDAP is a simplified version of the Directory Access Protocol (DAP), which is used to gain
access to X.500 directories. LDAP is the primary access protocol for Active Directory.

LISTSERV A family of programs that manage Internet mailing lists by distributing messages posted to the list, and adding and deleting members automatically.

Lmhosts An ASCII text file like Hosts but used to associate IP addresses to host names inside a network. To remember which is which, remember Lmhosts as LAN Manager Hosts.

Local area network (LAN) A group of connected computers, usually located close to one another (such as in the same building or the same floor of the building) so that data can be passed among them.

Log on The act of entering into a computer system; for example, “Log on to the network and read your e-mail.”

Logon The account name used to gain access to a computer system. Unlike a password, the logon name isn’t a secret.

Logon or logoff script Typically a batch file set to run when a user logs on or logs off a system. A logon script is used to configure a user’s initial environment. A logoff script is used to return a system to some predetermined condition. Either script can be assigned to multiple users individually or through Group Policy.

M

Master boot record (MBR) The first sector on a hard disk where the computer gets its startup information. The MBR contains the partition table for the computer and a small program called the master boot code.

Media access control (MAC) address A unique 48-bit number assigned to network interface cards by the manufacturer. MAC addresses are used for mapping in TCP/IP network communication.

Media pool A logical collection of removable media sharing the same management policies.

Member server A server that is part of a domain but is not a domain controller. Member servers can be dedicated to managing files or printer services or other functions. A member server doesn’t verify logons or maintain a security database.

Mirror 1. Two partitions on two hard disks configured so that each will contain identical data to the other. If one disk fails, the other contains the data and processing can continue. 2. An FTP server that provides copies of the same files as another server. Some FTP servers are so popular that other servers have been set up to mirror them and spread the FTP load to more than one site.
**Multicasting**  Simultaneously sending a message to more than one destination on a network. Multicasting is distinguished from broadcasting in that multicasting sends to only selected recipients.

**Multilink dialing**  Combining two or more physical communication links into a single logical link to increase available bandwidth.

**Multimaster replication**  A feature of Active Directory, multimaster replication automatically propagates every object (such as users, groups, computers, domains, organization units, security policies, and so on) created on any domain controller to each of the other participating domain controllers. All domain controllers contain the same directory data, so the domain doesn’t depend on a single source for directory information.

**Multitasking**  Computer legerdemain by which tasks are switched in and out of the processor so quickly that it appears they are all happening at once. The success of a multitasking system depends on how well the various tasks are isolated from one another.

**Multithreading**  The simultaneous processing of several threads inside the same program. Because several threads can be processed in parallel, one thread doesn’t have to finish before another one can start.

---

**N**

**Name resolution**  The process of mapping a name to its corresponding address.

**Namespace**  A name or group of names defined according to a naming convention; any bounded area in which a given name can be resolved. Active Directory is primarily a namespace, as is any directory service. The Internet uses a hierarchical namespace that partitions names into categories known as top-level domains, such as .com, .edu, and .gov.

**Native mode**  In Windows 2000 domains, the condition of a domain when all domain controllers have been upgraded to Windows 2000 and the administrator has enabled native mode operation. In Windows Server 2003 domains, where there are no Windows 2000 or Windows NT 4 domain controllers, native mode is simply called Windows Server 2003 mode or functional level. See domain functional level.

**Net Logon service**  A service that accepts logon requests from any client and provides authentication from the Security Accounts Manager (SAM) database of accounts.

**NetBIOS Enhanced User Interface (NetBEUI)**  A small and fast protocol that requires little memory but can be routed only by using token ring routing. Remote locations linked by routers can’t use NetBEUI to communicate.
Network  Two or more computers connected for the purpose of sharing resources.

Network Access Server (NAS)  A server that accepts Point-to-Point Protocol connections and places them on the network served by NAS.

Network Address Translation (NAT)  Enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

Network News Transfer Protocol (NNTP)  A protocol defined for distribution, inquiry, retrieval, and posting of news articles on the Internet.

Newsgroup  On the Internet, a distributed bulletin board system about a particular topic. USENET News (also known as Netnews) is a system that distributes thousands of newsgroups to all parts of the Internet.

Node  A location on a tree structure with links to one or more items below it. On a LAN, a device that can communicate with other devices on the network. In clustering, a computer that is a member of a cluster.

NTFS file system  The native file system for Windows Server 2003, Windows 2000, and Windows NT. Supports long filenames, a variety of permissions for sharing files, and a transaction log that allows the completion of any incomplete file-related tasks if the operating system is interrupted.

Object  A particular set of attributes that represents something concrete, such as a user, a printer, or an application. The attributes hold data describing the thing that is identified by the object. Attributes of a user might include the user's given name, surname, and e-mail address. The classification of the object defines which types of attributes are used. For example, the objects classified as users might allow the use of attribute types like common name, telephone number, and e-mail address, whereas the object class of organization allows for attribute types like organization name and business category. An attribute can take one or more values, depending on its type.

Object identifier (OID)  A globally unique identifier (GUID), which is assigned by the Directory System Agent (DSA) when the object is created. The GUID is stored in an attribute, the object GUID, which is part of every object. The object GUID attribute can't be modified or deleted. When storing a reference to an Active Directory object in an external store (for example, a database), you should use the object GUID because, unlike a name, it won't change.

Operations Master  A domain controller that has been assigned Active Directory operations that are single master—that is, operations that are
not permitted to occur at different places in the network at the same time. Some single-master operations include schema modification, domain naming, and the relative identifier (RID) allocator.

**Organizational unit (OU)** A container object in Active Directory used to separate computers, users, and other resources into logical units. An organizational unit is the smallest entity to which Group Policy can be linked. It is also the smallest scope to which administration authority can be delegated.

---

**P**

**Packet** The basic unit of information sent over a network. Each packet contains the destination address, the sender’s address, error-control information, and data. The size and format of a packet depend on the protocol being used.

**Page** A document, or collection of information, available over the World Wide Web. A page can contain text, graphics, video, and sound files. Also, a portion of memory that the virtual memory manager can swap to and from a hard disk.

**Paging** A virtual memory operation in which pages are transferred from memory to disk when memory becomes full. When a thread accesses a page that’s not in memory, a page fault occurs and the memory manager uses page tables to find the page on disk and then loads the page into memory.

**PDC Emulator master** The domain controller that services network clients that do not have Active Directory client software installed and replicates changes to any Windows NT backup controllers. The PDC emulator master also handles authentication requests for accounts with recently changed passwords, if the change has not been replicated yet to the entire domain.

**Ping** A network management utility that checks to see whether another computer is available and functioning. It sends a short message to which the other computer automatically responds. If the other computer doesn’t respond to the ping, you usually can’t establish communications.

**Point of presence (POP)** A physical site in a geographic area where a network access provider, such as a telecommunications company, has equipment to which users connect. The local telephone company’s central office in a particular area is also sometimes referred to as their POP for that area.

**Point-to-Point Tunneling Protocol (PPTP)** A protocol that provides router-to-router and host-to-network connections over a telephone line (or a network link that acts like a telephone line). See **Serial Line Internet Protocol (SLIP)**.
Post Office Protocol (POP)  A protocol by which a mail server on the Internet lets you access your mail and download it to a PC or Macintosh. Most people refer to this protocol with its version number (POP2, POP3, and so on) to avoid confusing it with points of presence (POPs).

Primary domain controller (PDC)  In a Windows NT domain, the server that authenticates domain logons and maintains the security policy and master database for a domain. In a Windows 2000 or Windows Server 2003 domain, running in mixed mode, one of the domain controllers in each domain is identified as the PDC emulator master for compatibility with down-level clients and servers.

Primary partition  A portion of the hard disk that’s been marked as a potentially bootable logical drive by an operating system. MS-DOS can support only a single primary partition. Master boot record disks can support four primary partitions. Computers with the Intel Itanium processor use a GUID partition table that supports up to 128 primary partitions.

Profile  Loaded by the system when a user logs on, the profile defines a user’s environment, including network settings, printer connections, desktop settings, and program items.

Proxy server  A server that receives Web requests from clients, retrieves Web pages, and forwards them to clients. Proxy servers can dramatically improve performance for groups of users by caching retrieved pages. Proxy servers also provide security by shielding the IP addresses of internal clients.

Public-key cryptography  A method of secure transmission in which two different keys are used—a public key for encrypting data and a private key for decrypting data.

Quality of Service (QoS)  A set of standards for assuring the quality of data transmission on a network.

Realm trust  Used to connect between a non-Windows Kerberos realm and a Windows Server 2003 domain. Realm trusts can be transitive or non-transitive, one-way, or two-way.

Redundant array of independent disks (RAID)  A range of disk management and striping techniques to implement fault tolerance.

Relative distinguished name (RDN)  Active Directory uses the concept of a relative distinguished name (RDN), which is the part of the distinguished name that is an attribute of the object itself.

Relative identifier (RID)  The part of the security identifier (SID) that is unique to each object.
Remote Access Service (RAS)  Allows users to connect from remote locations and access their networks for file and printer sharing and e-mail. The computer initiating the connection is the RAS client; the answering computer is the RAS host.

Remote Authentication Dial-In User Service (RADIUS)  A security authentication system used by many Internet service providers (ISPs). A user connects to the ISP and enters a user name and password. This information is verified by a RADIUS server, which then authorizes access to the ISP system.

Remote Installation Services (RIS)  Allows clients to boot from a network server and use special preboot diagnostic tools installed on the server or to automatically install client software.

Replication  On network computers, enables the contents of a directory, designated as an export directory, to be copied to other directories, called import directories. Active Directory changes are replicated to all domain controllers on a regular schedule.

Requests for comments (RFCs)  An evolving collection of material that details the functions within the TCP/IP family of protocols. Some RFCs are official documents of the Internet Engineering Task Force (IETF), defining the standards of TCP/IP and the Internet, whereas others are simply proposals trying to become standards, and others fall somewhere in between. Some are tutorial in nature, whereas others are quite technical.

Router  A special-purpose computer (or software package) that handles the connection between two or more networks. Routers look at the destination addresses of the packets passing through them and decide which route to use to send them.

Schema  A set of definitions of the object classes and attributes that can be stored in Active Directory. Like other objects in Active Directory, schema objects have an access control list (ACL) to limit alterations to only authorized users.

Schema master  The single domain controller assigned to track all updates to a schema within a forest.

Scope  In DHCP, the range of IP addresses available to be leased to DHCP clients by the DHCP service. In groups, scope describes where in the network permissions can be assigned to the group.

Security Accounts Manager (SAM)  Manager of user account information including group membership. A service used at logon.

Security Identifier (SID)  A unique number assigned to every computer, group, and user account on a Windows Server 2003, Windows 2000,
or Windows NT network. Internal processes in the operating system refer to an account’s SID, rather than a name. A deleted SID is never reused.

**Serial Line Internet Protocol (SLIP)** A protocol used to run IP over serial lines or telephone lines using modems. Rapidly being replaced by Point-to-Point Tunneling Protocol (PPTP). SLIP is part of Windows remote access for compatibility with other remote access software.

**Server** A computer that provides a service to other computers on a network. A file server, for example, provides files to client machines.

**Shortcut trust** Used to reduce logon times between two domains in a Windows Server 2003 forest. This type of trust is transitive and can be one-way or two-way.

**Simple Object Access Protocol (SOAP)** An XML/HTTP–based protocol that provides a way for applications to communicate with each other over the Internet, independent of platform.

**Site** In Active Directory, an area of one or more well-connected subnets. When users log on to a site, clients use Active Directory servers in the same site. See well connected.

**Smart card** A credit card–sized device that securely stores user credentials such as passwords, certificates, public and private keys, and other types of personal information.

**Snap-in** A tool that can be added to a console supported by the Microsoft Management Console (MMC). You can add a snap-in extension to extend the function of a snap-in.

**Socket** An endpoint to a connection. Two sockets form a complete path for a bidirectional pipe for incoming and outgoing data between networked computers. The Windows Sockets API is a networking API for programmers writing for the Windows family of products.

**Subnet** The portion of a TCP/IP network in which all devices share a common prefix. For example, all devices with an IP address that starts with 198 are on the same subnet. IP networks are divided using a subnet mask.

**Superscope** A collection of scopes grouped into a single administrative whole. Grouping scopes together into a superscope makes it possible to have more than one logical subnet on a physical subnet.

**SystemRoot** The path and folder where the Windows system fileshare is located. The value `%SystemRoot%` can be used in paths to replace the actual location. To identify the SystemRoot folder on a computer, type `%SystemRoot%` at a command prompt.
Telnet  The protocol and program used to log on from one Internet site to another. The Telnet protocol/program gets you to the logon prompt of another host.

Terminal  A device that allows you to send commands to another computer. At a minimum, this usually means a keyboard, a display screen, and some simple circuitry. You will usually use terminal software in a personal computer—the software pretends to be, or emulates, a physical terminal and allows you to type commands to another computer.

Token ring  A type of computer network in which the computers connected in a circle. A token, which is a special bit pattern, travels around the circle. To communicate to another computer, a computer catches the token, attaches a message to it, and the token continues around the network, dropping off the message at the designated location.

Thread  An executable entity that belongs to one (and only one) process. In a multitasking environment, a single program can contain several threads, all running at the same time.

Transitive trust  The standard trust between Windows Server 2003 domains in a domain tree or forest. Transitive trusts are always two-way trusts. When a domain joins a domain tree or forest, a transitive trust relationship is established automatically.

Transmission Control Protocol/Internet Protocol (TCP/IP)  A set of protocols that networks use to communicate with each other on the Internet.

Tree  A tree in Active Directory is just an extension of the idea of a directory tree. It’s a hierarchy of objects and containers that demonstrates how objects are connected, or the path from one object to another. Endpoints on the tree are usually objects.

Trust relationship  A security term meaning that one workstation or server trusts a domain controller to authenticate a user logon on its behalf. It also means a domain controller trusts a domain controller in another domain to authenticate a logon.

Uniform Resource Locator (URL)  The standard way to give the address of any resource on the Internet that is part of the World Wide Web. For example, http://www.capecod.net/~fcollege/index.htm. The most common way to use a URL is to enter it into a Web browser program.

Universal group  A group that can be used anywhere in a domain tree or forest. Members can come from any
domain, and rights and permissions can be assigned at any domain. Universal groups are available only when the domain is in native mode.

**Universal Naming Convention (UNC)** A PC format for indicating the location of resources on a network. UNC uses the following format: `\Server\Shared_resource_path`. To identify the Example.txt file in the Sample folder on the server named Ample, the UNC would be `\Ample\Sample\Example.txt`.

**UNIX** An operating system designed to be used by many computer users at the same time (multiuser) with TCP/IP built in. A common operating system for servers on the Internet.

**User account** A user’s access to a network. Each user account has a unique user name and security ID (SID).

**User profiles** Information about user accounts. See profile.

**Virtual Private Network (VPN)** A network constructed by using public wires to connect nodes. VPNs use encryption and other security mechanisms to make sure only authorized users can access the network and that the data cannot be intercepted.

**Voice over Internet Protocol (VoIP)** A method for using the Internet as a transmission medium for telephone calls.

**Well connected** Sufficiently fast and reliable for the needs of Active Directory clients and servers. The definition of “sufficiently fast and reliable” for a particular network depends on the work being done on the specific network.

**Wide area network (WAN)** Any Internet or network that covers an area larger than a single building or campus.

**Windows Internet Name Service (WINS)** A name resolution service that converts computer names to IP addresses in a routed environment.

**Windows Sockets (Winsock)** Winsock is a standard way for Windows-based programs to work with TCP/IP. You can use Winsock if you use SLIP to connect to the Internet.

**Workstation** In Windows NT, a computer running the Windows NT Workstation operating system. In a wider context, used to describe any powerful computer optimized for graphics or computer-aided design (CAD) or any of a number of other functions requiring high performance.
X

**X.500** A standard for a directory service established by the International Telecommunications Union (ITU). The same standard is also published by the International Standards Organization/International Electrotechnical Commission (ISO/IEC). The X.500 standard defines the information model used in the directory service. All information in the directory is stored in entries, each of which belongs to at least one object class. The actual information in an entry is determined by attributes that are contained in that entry.

Z

**Zone** A part of the DNS namespace that consists of a single domain or a domain and subdomains managed as a single, separate entity.
Charlie Russel and Sharon Crawford are co-authors of numerous books on operating systems. Their titles include Microsoft Windows Small Business 2003 Server Administrator’s Companion; Microsoft Windows Server 2003 Administrator’s Companion; Microsoft Windows XP Resource Kit, Third Edition; and Upgrading to Windows 98.

Charlie Russel is a chemist by education; an electrician by trade; a UNIX sysadmin and Oracle DBA because he raised his hand when he should have known better; an IT Director and consultant by default; and a writer by choice. Charlie is the author of more than two dozen computer books on operating systems and enterprise environments, including Microsoft Windows Small Business Server 2003 Administrator’s Companion; Microsoft Windows XP Resource Kit, Third Edition; and (with Robert Cordingley) the Oracle DBA Quick Reference Series. He has also written numerous white papers and case studies on Microsoft.com and is a regular columnist for the Windows Expert Zone.

Sharon Crawford is a veteran, even grizzled, writer of computer books. In addition to the books with Charlie, Sharon co-authored (with Jason Gerend) Faster Smarter Microsoft Windows 98. Sharon writes a regular column on using Windows XP at home for the Microsoft Windows XP Expert Zone at http://www.microsoft.com/windowsxp/expertzone.

Jason Gerend is a freelance author and network consultant who has contributed to over 30 books. A Microsoft MVP and a Microsoft Certified Systems Engineer (MCSE), Jason was the primary writer at Microsoft for the Windows Server 2003 R2 Corporate Deployment Tools and OEM Preinstallation Kit. He co-authored the Microsoft Windows Small Business Server 2003 Server Administrator’s Companion, the Microsoft Windows 2003 Server Administrator’s Companion, and other books with Sharon and Charlie. Jason enjoys mountain climbing, backcountry snowboarding, and installing operating systems. He’s been fooling around with PCs since the days of MS-DOS 2.0, loved OS/2 2.1 and BeOS, and been a freelance consultant and Webmaster since 1995.
Microsoft Press Support Information

Every effort has been made to ensure the accuracy of this book. Microsoft Press provides corrections for books through the Microsoft Press Technical Support Web site at http://www.microsoft.com/learning/support/books/.

If you have comments, questions, or ideas regarding the book and the CD-ROM, please send them to Microsoft Press via e-mail to:

mspinput@microsoft.com

Or via postal mail to:

Microsoft Press
Attn: Editor, Microsoft Windows Server 2003 Administrator’s Companion, Second Edition
One Microsoft Way
Redmond, WA 98052-6399

Please note that product support is not offered through the above address. For more information about Microsoft software support options, connect to http://www.microsoft.com/support/.