Conquer Mailbox administration—from the inside out!

Focusing on the Mailbox server role, dive into Exchange Server 2013—and really put your enterprise messaging to work! This supremely organized reference packs hundreds of timesaving solutions, troubleshooting tips, and workarounds for managing mailboxes and high availability. Discover how the experts tackle core operations and support tasks—and challenge yourself to new levels of mastery.

- Prepare for installation or upgrade
- Master role-based access control (RBAC) fundamentals
- Create, manage, move, and archive mailboxes
- Implement email address policies
- Configure and manage distribution groups
- Understand Store components and functionality
- Deliver high availability through database availability groups (DAG)
- Manage compliance, retention, mailbox search, and data loss prevention
- Use the Exchange Management Shell and cmdlets
- Administer public folder architecture

Also look for
Microsoft Exchange Server 2013 Inside Out: Connectivity, Clients, and UM
9780735678378

Microsoft Exchange Server 2013: Mailbox and High Availability

For experienced Exchange Server administrators

Foreword by Rajesh Jha
Corporate Vice President, Exchange Server Group, Microsoft Corporation

About the Author
Tony Redmond is a Microsoft Most Valuable Professional (MVP) and one of the leading voices in the Exchange Server community. He has two decades of experience with enterprise mail, focusing on Exchange Server since version 4.0. As an industry consultant, he guides customers through Exchange Server deployment and management issues, and he’s written 10 books.

Microsoft Press
Celebrating 30 years!

Windows Server 2012 R2: Services, Security, & Infrastructure

William R. Stanek: Windows technologies expert + award-winning author
Windows Server 2012 R2 Inside Out: Services, Security, & Infrastructure

William R. Stanek
To my readers—Windows Server 2012 R2 Inside Out: Services, Security, & Infrastructure is my 49th book for Microsoft Press. Thank you for being there with me through many books and many years. It’s been an honor and a privilege.

To my wife—for many years, through many books, many millions of words, and many thousands of pages she’s been there, providing support and encouragement and making every place we’ve lived a home.

To my kids—for helping me see the world in new ways, for having exceptional patience and boundless love, and for making every day an adventure.

To Anne, Karen, Martin, Lucinda, Juliana, and many others who’ve helped out in ways both large and small.

Special thanks to my son Will for not only installing and managing my extensive dev lab for all my books since Windows 8 Pocket Consultant but for also performing check reads of all those books as well.

—William R. Stanek
## Contents at a glance

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Using Remote Desktop for Management</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Networking with TCP/IP</td>
<td>19</td>
</tr>
<tr>
<td>3</td>
<td>Managing TCP/IP networking</td>
<td>55</td>
</tr>
<tr>
<td>4</td>
<td>Deploying DHCP Services</td>
<td>87</td>
</tr>
<tr>
<td>5</td>
<td>Configuring DHCP Services</td>
<td>137</td>
</tr>
<tr>
<td>6</td>
<td>Architecting DNS infrastructure</td>
<td>171</td>
</tr>
<tr>
<td>7</td>
<td>Implementing and managing DNS</td>
<td>201</td>
</tr>
<tr>
<td>8</td>
<td>Maintaining and troubleshooting DNS</td>
<td>251</td>
</tr>
<tr>
<td>9</td>
<td>Implementing and maintaining WINS</td>
<td>273</td>
</tr>
<tr>
<td>10</td>
<td>Active Directory architecture</td>
<td>295</td>
</tr>
<tr>
<td>11</td>
<td>Designing and managing the domain environment</td>
<td>321</td>
</tr>
<tr>
<td>12</td>
<td>Organizing Active Directory</td>
<td>379</td>
</tr>
<tr>
<td>13</td>
<td>Configuring Active Directory sites and replication</td>
<td>397</td>
</tr>
<tr>
<td>14</td>
<td>Implementing Active Directory Domain Services</td>
<td>435</td>
</tr>
<tr>
<td>15</td>
<td>Deploying read-only domain controllers</td>
<td>481</td>
</tr>
<tr>
<td>16</td>
<td>Managing users, groups, and computers</td>
<td>513</td>
</tr>
<tr>
<td>17</td>
<td>Managing Group Policy</td>
<td>565</td>
</tr>
<tr>
<td>18</td>
<td>Active Directory site administration</td>
<td>623</td>
</tr>
<tr>
<td>19</td>
<td>Deploying print services</td>
<td>653</td>
</tr>
<tr>
<td>20</td>
<td>Managing and maintaining print services</td>
<td>701</td>
</tr>
<tr>
<td>21</td>
<td>Backup and recovery</td>
<td>747</td>
</tr>
</tbody>
</table>
# Table of contents

**Introduction** ................................. xvii
Conventions ..................................... xx
How to reach the author ........................... xxi
Errata and book support ......................... xxi
We want to hear from you ....................... xxi
Stay in touch .................................... xxi

**Chapter 1**

**Using Remote Desktop for Management** .............. 1
Remote Desktop essentials ........................ 2
Configuring Remote Desktop ....................... 4
  - Enabling Remote Desktop on servers .......... 4
  - Permitting and restricting remote logon ....... 6
  - Configuring Remote Desktop through Group Policy . 7
  - Tracking who's logged on ..................... 8
Supporting Remote Desktop Connection clients ....... 9
  - Remote Desktop Connection client .......... 9
  - Running the Remote Desktop Connection client ... 12
  - Connecting to a virtual machine in Windows Azure ... 16

**Chapter 2**

**Networking with TCP/IP** ............................ 19
Navigating networking in Windows Server 2012 R2 ..... 19
Using TCP/IP .................................. 24
Understanding IPv4 addressing ..................... 27
  - Unicast IPv4 addresses ...................... 28
  - Multicast IPv4 addresses .................. 31
  - Broadcast IPv4 addresses .................. 31
Special IPv4 addressing rules ...................... 33
Using subnets and subnet masks ................. 34
  - Subnet masks ................................ 35
  - Network prefix notation .................. 36

---

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

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

[http://aka.ms/tellpress](http://aka.ms/tellpress)
Subnetting ................................................................. 36
Understanding IP data packets ................................. 41
Getting and using IPv4 addresses ............................... 42
Understanding IPv6 ...................................................... 45
Understanding name resolution. ................................. 47
Domain Name System ................................................. 48
Windows Internet Naming Service .............................. 50
Link-Local Multicast Name Resolution ......................... 51

Chapter 3  Managing TCP/IP networking .......................... 55
Installing TCP/IP networking ....................................... 55
  Preparing for installation of TCP/IP networking .......... 55
  Installing network adapters .................................... 56
  Installing networking services (TCP/IP) .................... 57
Configuring TCP/IP networking ................................... 58
  Configuring static IP addresses ............................... 59
  Configuring dynamic IP addresses and alternate IP addressing 63
  Configuring multiple IP addresses and gateways .......... 65
  Configuring DNS resolution ................................... 67
  Configuring WINS resolution ................................. 69
Managing network connections ................................... 71
  Checking the status, speed, and activity for network connections 71
  Viewing network configuration information ................ 73
  Enabling and disabling network connections ............... 75
  Renaming network connections ................................ 76
Troubleshooting and testing network settings ............... 76
  Diagnosing and resolving network connection problems .... 76
  Diagnosing and resolving Internet connection problems .... 76
  Performing basic network tests ............................... 77
  Diagnosing and resolving IP addressing problems ........ 78
  Diagnosing and resolving routing problems ................ 80
  Releasing and renewing DHCP settings ...................... 81
  Diagnosing and fixing name-resolution issues ............... 83

Chapter 4  Deploying DHCP Services ............................. 87
DHCP essentials ....................................................... 87
  DHCPv4 and autoconfiguration .................................. 89
  DHCPv6 and autoconfiguration .................................. 89
DHCP security considerations ................................... 91
DHCP and IPAM ....................................................... 92
Planning DHCPv4 and DHCPv6 implementations .......... 94
  DHCPv4 messages and relay agents .......................... 94
  DHCPv6 messages and relay agents .......................... 96
  DHCP availability and fault tolerance ...................... 98
Setting up DHCP servers ............................................ 103
  Installing the DHCP Server service ......................... 104
  Authorizing DHCP servers in Active Directory ........... 109
## Table of contents

Creating and configuring scopes ...................................................... 110  
Activating scopes ........................................................................ 124  
Scope exclusions ........................................................................... 126  
Scope reservations ......................................................................... 127  
Creating and using failover scopes ............................................... 131

### Chapter 5 Configuring DHCP Services ........................................... 137

- Configuring TCP/IP options ......................................................... 137  
- Levels of options and their uses ................................................ 137  
- Policy-based assignment ............................................................ 138  
- Options used by Windows clients ............................................... 140  
- Using user-specific and vendor-specific TCP/IP options .......... 141  
- Setting options for all clients ..................................................... 143  
- Setting options for RRAS and NAP clients ............................... 146  
- Setting add-on options for directly connected clients ........... 147  
- Defining classes to get different option sets ......................... 148

- Advanced DHCP configuration and maintenance ................... 150  
  - Monitoring DHCP audit logging ............................................. 151  
  - Binding the DHCP Server service to a network interface .... 155  
  - Integrating DHCP and DNS .................................................. 156  
  - Integrating DHCP and NAP ................................................... 157  
  - Enabling conflict detection on DHCP servers .................... 161  
  - Saving and restoring the DHCP configuration ................. 162  
  - Managing and maintaining the DHCP database ............ 163

- Setting up DHCP relay agents ...................................................... 165  
  - Configuring and enabling Routing And Remote Access .... 166  
  - Adding and configuring the DHCP relay agent .......... 167

### Chapter 6 Architecting DNS infrastructure .................................. 171

- DNS essentials ........................................................................... 171  
- Planning DNS implementations ............................................... 173  
  - Public and private namespaces .............................................. 174  
  - Name resolution using DNS ................................................. 176  
  - Understanding DNS devolution ......................................... 178  
  - DNS resource records .......................................................... 179  
  - DNS zones and zone transfers ............................................ 180  
  - Secondary zones, stub zones, and conditional forwarding .... 186  
  - Integration with other technologies .................................... 187

- Security considerations ............................................................... 189  
  - DNS queries and security ...................................................... 189  
  - DNS dynamic updates and security .................................... 190  
  - External DNS name resolution and security .................... 192

- Architecting a DNS design .......................................................... 194  
  - Split-brain design: Same internal and external names ..... 195  
  - Separate-name design: Different internal and external names 196  
  - Securing DNS from attacks .................................................. 198
# Chapter 7 Implementing and managing DNS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing the DNS Server service</td>
<td>201</td>
</tr>
<tr>
<td>Using DNS with Active Directory</td>
<td>201</td>
</tr>
<tr>
<td>Using DNS without Active Directory</td>
<td>205</td>
</tr>
<tr>
<td>DNS setup</td>
<td>206</td>
</tr>
<tr>
<td>Configuring DNS using the wizard</td>
<td>211</td>
</tr>
<tr>
<td>Configuring a small network using the Configure A DNS Server Wizard</td>
<td>211</td>
</tr>
<tr>
<td>Configuring a large network using the Configure A DNS Server Wizard</td>
<td>215</td>
</tr>
<tr>
<td>Configuring DNS zones, subdomains, forwarders, and zone transfers</td>
<td>221</td>
</tr>
<tr>
<td>Creating forward lookup zones</td>
<td>221</td>
</tr>
<tr>
<td>Creating reverse lookup zones</td>
<td>223</td>
</tr>
<tr>
<td>Configuring forwarders and conditional forwarding</td>
<td>224</td>
</tr>
<tr>
<td>Configuring subdomains and delegating authority</td>
<td>227</td>
</tr>
<tr>
<td>Configuring zone transfers</td>
<td>229</td>
</tr>
<tr>
<td>Configuring secondary notification</td>
<td>232</td>
</tr>
<tr>
<td>Deploying DNSSEC</td>
<td>233</td>
</tr>
<tr>
<td>DNSSEC essentials</td>
<td>234</td>
</tr>
<tr>
<td>Securing zones with digital signatures</td>
<td>235</td>
</tr>
<tr>
<td>Signing a zone</td>
<td>236</td>
</tr>
<tr>
<td>Adding resource records</td>
<td>238</td>
</tr>
<tr>
<td>Host Address (A and AAAA) and Pointer (PTR) records</td>
<td>239</td>
</tr>
<tr>
<td>Canonical Name (CNAME) records</td>
<td>243</td>
</tr>
<tr>
<td>Mail Exchanger (MX) records</td>
<td>243</td>
</tr>
<tr>
<td>Name Server (NS) records</td>
<td>245</td>
</tr>
<tr>
<td>Start of Authority (SOA) records</td>
<td>246</td>
</tr>
<tr>
<td>Service Location (SRV) records</td>
<td>247</td>
</tr>
<tr>
<td>Deploying global names</td>
<td>248</td>
</tr>
<tr>
<td>Creating reverse lookup zones</td>
<td>223</td>
</tr>
<tr>
<td>Creating forward lookup zones</td>
<td>221</td>
</tr>
<tr>
<td>Configuring forwarders and conditional forwarding</td>
<td>224</td>
</tr>
<tr>
<td>Configuring subdomains and delegating authority</td>
<td>227</td>
</tr>
<tr>
<td>Configuring zone transfers</td>
<td>229</td>
</tr>
<tr>
<td>Configuring secondary notification</td>
<td>232</td>
</tr>
<tr>
<td>Deploying DNSSEC</td>
<td>233</td>
</tr>
<tr>
<td>DNSSEC essentials</td>
<td>234</td>
</tr>
<tr>
<td>Securing zones with digital signatures</td>
<td>235</td>
</tr>
<tr>
<td>Signing a zone</td>
<td>236</td>
</tr>
<tr>
<td>Adding resource records</td>
<td>238</td>
</tr>
<tr>
<td>Host Address (A and AAAA) and Pointer (PTR) records</td>
<td>239</td>
</tr>
<tr>
<td>Canonical Name (CNAME) records</td>
<td>243</td>
</tr>
<tr>
<td>Mail Exchanger (MX) records</td>
<td>243</td>
</tr>
<tr>
<td>Name Server (NS) records</td>
<td>245</td>
</tr>
<tr>
<td>Start of Authority (SOA) records</td>
<td>246</td>
</tr>
<tr>
<td>Service Location (SRV) records</td>
<td>247</td>
</tr>
<tr>
<td>Deploying global names</td>
<td>248</td>
</tr>
<tr>
<td>Creating reverse lookup zones</td>
<td>223</td>
</tr>
<tr>
<td>Creating forward lookup zones</td>
<td>221</td>
</tr>
<tr>
<td>Configuring forwarders and conditional forwarding</td>
<td>224</td>
</tr>
<tr>
<td>Configuring subdomains and delegating authority</td>
<td>227</td>
</tr>
<tr>
<td>Configuring zone transfers</td>
<td>229</td>
</tr>
<tr>
<td>Configuring secondary notification</td>
<td>232</td>
</tr>
<tr>
<td>Deploying DNSSEC</td>
<td>233</td>
</tr>
<tr>
<td>DNSSEC essentials</td>
<td>234</td>
</tr>
<tr>
<td>Securing zones with digital signatures</td>
<td>235</td>
</tr>
<tr>
<td>Signing a zone</td>
<td>236</td>
</tr>
<tr>
<td>Adding resource records</td>
<td>238</td>
</tr>
<tr>
<td>Host Address (A and AAAA) and Pointer (PTR) records</td>
<td>239</td>
</tr>
<tr>
<td>Canonical Name (CNAME) records</td>
<td>243</td>
</tr>
<tr>
<td>Mail Exchanger (MX) records</td>
<td>243</td>
</tr>
<tr>
<td>Name Server (NS) records</td>
<td>245</td>
</tr>
<tr>
<td>Start of Authority (SOA) records</td>
<td>246</td>
</tr>
<tr>
<td>Service Location (SRV) records</td>
<td>247</td>
</tr>
<tr>
<td>Deploying global names</td>
<td>248</td>
</tr>
</tbody>
</table>

# Chapter 8 Maintaining and troubleshooting DNS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintaining and monitoring DNS</td>
<td>251</td>
</tr>
<tr>
<td>Configuring default partitions and replication scope</td>
<td>251</td>
</tr>
<tr>
<td>Setting the aging and scavenging rules</td>
<td>254</td>
</tr>
<tr>
<td>Configuring logging and checking DNS Server logs</td>
<td>256</td>
</tr>
<tr>
<td>Troubleshooting the DNS client service</td>
<td>257</td>
</tr>
<tr>
<td>Try reregistering the client</td>
<td>257</td>
</tr>
<tr>
<td>Check the client’s TCP/IP configuration</td>
<td>257</td>
</tr>
<tr>
<td>Check the client’s resolver cache</td>
<td>259</td>
</tr>
<tr>
<td>Perform lookups for troubleshooting</td>
<td>260</td>
</tr>
<tr>
<td>Troubleshooting the DNS Server service</td>
<td>261</td>
</tr>
<tr>
<td>Check the server’s TCP/IP configuration</td>
<td>261</td>
</tr>
<tr>
<td>Check the server’s cache</td>
<td>261</td>
</tr>
<tr>
<td>Check replication to other name servers</td>
<td>262</td>
</tr>
<tr>
<td>Examine the configuration of the DNS server</td>
<td>263</td>
</tr>
<tr>
<td>Examine zones and zone records</td>
<td>269</td>
</tr>
<tr>
<td>Getting DNS server statistics</td>
<td>271</td>
</tr>
<tr>
<td>Chapter 9</td>
<td>Implementing and maintaining WINS</td>
</tr>
<tr>
<td>WINS essentials</td>
<td>273</td>
</tr>
<tr>
<td>NetBIOS namespace and scope</td>
<td>273</td>
</tr>
<tr>
<td>NetBIOS node types</td>
<td>275</td>
</tr>
<tr>
<td>WINS name registration and cache</td>
<td>275</td>
</tr>
<tr>
<td>WINS implementation details</td>
<td>276</td>
</tr>
<tr>
<td>Setting up WINS servers</td>
<td>277</td>
</tr>
<tr>
<td>Configuring replication partners</td>
<td>279</td>
</tr>
<tr>
<td>Replication essentials</td>
<td>280</td>
</tr>
<tr>
<td>Configuring automatic replication partners</td>
<td>280</td>
</tr>
<tr>
<td>Using designated replication partners</td>
<td>282</td>
</tr>
<tr>
<td>Configuring and maintaining WINS</td>
<td>284</td>
</tr>
<tr>
<td>Configuring burst handling</td>
<td>284</td>
</tr>
<tr>
<td>Checking server status and configuration</td>
<td>286</td>
</tr>
<tr>
<td>Checking active registrations and scavenging records</td>
<td>288</td>
</tr>
<tr>
<td>Maintaining the WINS database</td>
<td>289</td>
</tr>
<tr>
<td>Enabling WINS lookups through DNS</td>
<td>292</td>
</tr>
<tr>
<td>Chapter 10</td>
<td>Active Directory architecture</td>
</tr>
<tr>
<td>Active Directory physical architecture</td>
<td>295</td>
</tr>
<tr>
<td>Active Directory physical architecture: A top-level view</td>
<td>295</td>
</tr>
<tr>
<td>Active Directory within the Local Security Authority</td>
<td>296</td>
</tr>
<tr>
<td>Directory service architecture</td>
<td>299</td>
</tr>
<tr>
<td>Data store architecture</td>
<td>307</td>
</tr>
<tr>
<td>Active Directory logical architecture</td>
<td>310</td>
</tr>
<tr>
<td>Active Directory objects</td>
<td>311</td>
</tr>
<tr>
<td>Active Directory domains, trees, and forests</td>
<td>312</td>
</tr>
<tr>
<td>Active Directory trusts</td>
<td>314</td>
</tr>
<tr>
<td>Active Directory namespaces and partitions</td>
<td>316</td>
</tr>
<tr>
<td>Active Directory data distribution</td>
<td>319</td>
</tr>
<tr>
<td>Chapter 11</td>
<td>Designing and managing the domain environment</td>
</tr>
<tr>
<td>Design considerations for Active Directory replication</td>
<td>322</td>
</tr>
<tr>
<td>Design considerations for Active Directory search and global catalogs</td>
<td>323</td>
</tr>
<tr>
<td>Searching the tree</td>
<td>324</td>
</tr>
<tr>
<td>Accessing the global catalog</td>
<td>325</td>
</tr>
<tr>
<td>Designating global catalog servers</td>
<td>326</td>
</tr>
<tr>
<td>Designating replication attributes</td>
<td>328</td>
</tr>
<tr>
<td>Design considerations for compatibility</td>
<td>330</td>
</tr>
<tr>
<td>Understanding domain functional level</td>
<td>331</td>
</tr>
<tr>
<td>Understanding forest functional level</td>
<td>332</td>
</tr>
<tr>
<td>Raising or lowering the domain or forest functional level</td>
<td>333</td>
</tr>
<tr>
<td>Design considerations for Active Directory authentication and trusts</td>
<td>337</td>
</tr>
<tr>
<td>Universal groups and authentication</td>
<td>337</td>
</tr>
<tr>
<td>NTLM and Kerberos authentication</td>
<td>340</td>
</tr>
<tr>
<td>Authentication and trusts across domain boundaries</td>
<td>344</td>
</tr>
<tr>
<td>Authentication and trusts across forest boundaries</td>
<td>347</td>
</tr>
</tbody>
</table>
Examining domain and forest trusts ........................................ 350
Establishing external, shortcut, realm, and cross-forest trusts .......... 353
Verifying and troubleshooting trusts .................................... 357
Delegating authentication ..................................................... 358
Delegated authentication essentials ....................................... 358
Configuring delegated authentication .................................... 359
Design considerations for Active Directory operations masters .... 362
Operations master roles ...................................................... 362
Using, locating, and transferring the schema master role ............ 366
Using, locating, and transferring the domain naming master role .... 367
Using, locating, and transferring the relative ID master role ......... 368
Using, locating, and transferring the PDC emulator role ............ 372
Using, locating, and transferring the infrastructure master role .... 375
Seizing operations master roles .......................................... 376

Chapter 12 Organizing Active Directory .................................. 379
Creating an Active Directory implementation or update plan ....... 379
Developing a forest plan ..................................................... 380
Forest namespace ............................................................ 380
A single forest vs. multiple forests ....................................... 382
Forest administration ......................................................... 383
Developing a domain plan ................................................... 384
Domain design considerations ............................................. 385
A single domain vs. multiple domains .................................... 386
Forest root domain design configurations ............................... 387
Changing domain design .................................................... 387
Developing an organizational unit plan .................................. 389
Using organizational units .................................................... 389
Using OUs for delegation .................................................... 390
Using OUs for Group Policy ................................................ 391
Creating an OU design ....................................................... 392

Chapter 13 Configuring Active Directory sites and replication ...... 397
Working with Active Directory sites ....................................... 397
Single site vs. multiple sites ................................................ 399
Replication within and between sites ..................................... 400
Determining site boundaries ............................................... 401
Understanding Active Directory replication ............................ 402
Tracking Active Directory replication changes over time .......... 402
Tracking Active Directory system volume changes over time ...... 404
Replication architecture: An overview ................................... 409
Intersite replication essentials .............................................. 416
Replication rings and directory partitions ................................. 419
Developing or revising a site design ....................................... 424
Mapping network infrastructure .......................................... 424
Creating a site design ......................................................... 426
Chapter 14  **Implementing Active Directory Domain Services.**  435

- Preinstallation considerations for Active Directory .......................... 435
- Hardware and configuration considerations for domain controllers .......... 436
- Configuring Active Directory for fast recovery with storage area networks ... 438
- Connecting clients to Active Directory ........................................... 439
- Installing Active Directory Domain Services ...................................... 440
- Active Directory installation options and issues ................................. 440
- Using the Active Directory Domain Services Configuration Wizard .......... 443
- Performing an Active Directory installation from media ....................... 457
- Cloning virtualized domain controllers ............................................ 461
- Using clones of virtualized domain controllers .................................. 461
- Creating a clone virtualized domain controller .................................. 462
- Finalizing the clone deployment ..................................................... 464
- Troubleshooting the clone deployment .............................................. 464
- Uninstalling Active Directory ....................................................... 466
- Creating and managing organizational units ...................................... 471
- Creating an OU .............................................................................. 471
- Setting OU properties ..................................................................... 474
- Creating or moving accounts and resources for use with an OU ............... 475
- Delegating the administration of domains and OUs ............................. 475
- Understanding delegation of administration ....................................... 475
- Delegating administration ................................................................ 476

Chapter 15  **Deploying read-only domain controllers.**  481

- Introducing read-only domain controllers ......................................... 481
- Design considerations for read-only replication .................................. 485
- Installing RODCs ............................................................................ 488
- Preparing for an RODC installation .................................................. 488
- Installing an RODC ........................................................................ 490
- Installing an RODC from media ....................................................... 496
- Staging an RODC ........................................................................... 498
- Managing Password Replication Policy ............................................ 502
- Working with Password Replication Policy ....................................... 503
- Allowing or denying accounts in Password Replication Policy ............... 505
- Viewing and managing credentials on an RODC ............................... 508
- Determining whether an account is allowed or denied access ............... 509
- Resetting credentials ..................................................................... 510
- Delegating administrative permissions ............................................. 511

Chapter 16  **Managing users, groups, and computers.**  513

- Managing domain user accounts ....................................................... 513
- Configuring user account policies ..................................................... 513
- Creating Password Settings Objects and applying secondary settings ....... 519
- Understanding user account capabilities, privileges, and rights .............. 524
- Assigning user rights ...................................................................... 524
- Creating and configuring domain user accounts ................................ 527
Chapter 17  Managing Group Policy  ......................................................... 565

Understanding Group Policy ................................................................. 566
   Local and Active Directory Group Policy ........................................... 566
   Group Policy settings ................................................................. 567
   Group Policy architecture .......................................................... 568
   Administrative templates ............................................................ 569
Implementing Group Policy ............................................................... 570
   Working with Local Group Policy .................................................... 571
   Working with Group Policy Management Console............................. 575
   Working with the default Group Policy Objects .................................. 582

Maintaining user accounts ............................................................... 537
   Deleting user accounts ............................................................. 538
   Disabling and enabling user accounts ............................................ 538
   Moving user accounts ............................................................. 539
   Renaming user accounts .......................................................... 539
   Resetting a user’s domain password ............................................. 540
   Unlocking user accounts ........................................................... 541
   Creating a user account password backup ...................................... 542

Managing groups ............................................................................... 543
   Understanding groups ............................................................... 543
   Creating a group ........................................................................ 545
   Adding members to groups ........................................................ 547
   Deleting a group ....................................................................... 548
   Modifying groups ..................................................................... 548

Managing computer accounts ......................................................... 549
   Creating a computer account in Active Directory............................ 549
   Joining computers to a domain .................................................... 551
   Moving a computer account ....................................................... 552
   Disabling a computer account .................................................... 552
   Deleting a computer account ...................................................... 553
   Managing a computer account .................................................... 553
   Resetting a computer account .................................................... 553
   Troubleshooting computer accounts ........................................... 554

Recovering deleted accounts ........................................................... 555
   Enabling Active Directory Recycle Bin ......................................... 556
   Recovering objects from the Recycle Bin ....................................... 556

Working with managed service accounts ....................................... 557
   Creating managed service accounts ............................................ 559
   Configuring managed service accounts for use ............................. 561
   Deleting managed service accounts ............................................ 561
   Moving managed service accounts ............................................. 562
   Using virtual accounts ............................................................. 563

Configuring account options .......................................................... 531
Configuring profile options ............................................................ 534
Troubleshooting user accounts ........................................................ 536
## Table of contents

Managing Group Policy through delegation .................................................. 584  
Managing GPO creation rights ................................................................. 584  
Reviewing Group Policy management privileges ...................................... 585  
Delegating Group Policy management privileges ..................................... 587  
Delegating privileges for links and RSoP ................................................. 588  

Managing Group Policy inheritance and processing .................................. 589  
Group Policy inheritance ............................................................... 589  
Changing link order and precedence ....................................................... 591  
Overriding inheritance ..................................................................... 592  
Blocking inheritance ....................................................................... 593  
Enforcing inheritance ..................................................................... 594  
Filtering Group Policy application ......................................................... 595  
Group Policy processing .................................................................. 597  
Modifying Group Policy processing ....................................................... 599  
Modifying user policy preference using loopback processing ................. 600  

Using scripts in Group Policy ................................................................. 601  
Configuring computer startup and shutdown scripts .............................. 601  
Configuring user logon and logoff scripts .............................................. 602  

Applying Group Policy through security templates .................................. 603  
Working with security templates ........................................................... 604  
Applying security templates ............................................................... 605  

Maintaining and troubleshooting Group Policy ........................................ 606  
Group Policy refresh .................................................................. 606  
Modifying Group Policy refresh ......................................................... 607  
Viewing applicable GPOs and the last refresh ....................................... 610  
Modeling GPOs for planning ............................................................. 612  
Refreshing Group Policy manually ......................................................... 616  
Backing up GPOs .......................................................................... 617  
Restoring GPOs ....................................................................... 619  
Fixing default Group Policy ............................................................... 621  

**Chapter 18**  
**Active Directory site administration** .................................................. 623  

Managing sites and subnets ............................................................... 623  
Creating an Active Directory site ......................................................... 623  
Creating a subnet and associating it with a site .................................... 626  
Associating domain controllers with a site ......................................... 627  

Managing site links and inter-site replication ....................................... 628  
Understanding IP and SMTP replication transports ............................. 629  
Creating a site link ..................................................................... 630  
Configuring replication schedules for site links ...................................... 635  
Configuring site-link bridges ............................................................... 637  
Determining the ISTG ................................................................... 641  
Configuring site bridgehead servers ....................................................... 642  
Configuring advanced site-link options ................................................. 645  

Monitoring and troubleshooting replication ........................................... 646  
Using the Replication Administrator ....................................................... 647
<table>
<thead>
<tr>
<th>Chapter 19</th>
<th>Deploying print services</th>
<th>653</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploying print services</td>
<td>Understanding print services</td>
<td>653</td>
</tr>
<tr>
<td>Planning for printer deployments and consolidation</td>
<td>Sizing print server hardware and optimizing configuration</td>
<td>659</td>
</tr>
<tr>
<td>Setting up print servers</td>
<td>Installing a print server</td>
<td>665</td>
</tr>
<tr>
<td>Adding physically attached print devices</td>
<td>Adding network-attached printers</td>
<td>671</td>
</tr>
<tr>
<td>Changing standard TCP/IP port monitor settings</td>
<td>Connecting users to shared printers</td>
<td>683</td>
</tr>
<tr>
<td>Deploying printer connections</td>
<td>Configuring point and print restrictions</td>
<td>689</td>
</tr>
<tr>
<td>Managing printers throughout the organization</td>
<td>Managing your printers</td>
<td>692</td>
</tr>
<tr>
<td>Migrating printers and print queues</td>
<td>Monitoring printers and printer queues automatically</td>
<td>697</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 20</th>
<th>Managing and maintaining print services</th>
<th>701</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing printer permissions</td>
<td>Understanding printer permissions</td>
<td>701</td>
</tr>
<tr>
<td>Configuring printer permissions</td>
<td>Assigning printer ownership</td>
<td>703</td>
</tr>
<tr>
<td>Auditing printer access</td>
<td></td>
<td>705</td>
</tr>
<tr>
<td>Managing print server properties</td>
<td>Viewing and creating printer forms</td>
<td>708</td>
</tr>
<tr>
<td>Viewing and configuring printer ports</td>
<td>Viewing and configuring print drivers</td>
<td>710</td>
</tr>
<tr>
<td>Configuring print spool, logging, and notification settings</td>
<td></td>
<td>712</td>
</tr>
<tr>
<td>Managing printer properties</td>
<td>Setting general properties, printing preferences, and document defaults</td>
<td>714</td>
</tr>
<tr>
<td>Setting overlays and watermarks for documents</td>
<td>Installing and updating print drivers on clients</td>
<td>717</td>
</tr>
<tr>
<td>Configuring printer sharing and publishing</td>
<td>Optimizing printing through queues and pooling</td>
<td>719</td>
</tr>
<tr>
<td>Configuring print spooling</td>
<td>Viewing the print processor and default data type</td>
<td>725</td>
</tr>
<tr>
<td>Configuring separator pages</td>
<td>Configuring color profiles</td>
<td>727</td>
</tr>
<tr>
<td>Managing print jobs</td>
<td></td>
<td>732</td>
</tr>
<tr>
<td>Pausing, starting, and canceling all printing</td>
<td>Viewing print jobs</td>
<td>733</td>
</tr>
</tbody>
</table>
Managing a print job and its properties ........................................ 734
Printer maintenance and troubleshooting ........................................ 735
Monitoring print server performance ............................................. 735
Preparing for print server failure ................................................... 739
Solving printing problems ............................................................ 740

Chapter 21 Backup and recovery ..................................................... 747
Disaster-planning strategies ......................................................... 747
   Developing contingency procedures ......................................... 748
   Implementing problem-escalation and response procedures .......... 749
   Creating a problem-resolution policy document ....................... 750
Disaster preparedness procedures .................................................. 752
   Performing backups ............................................................. 752
   Repairing startup ............................................................... 753
   Setting startup and recovery options .................................... 754
Developing backup strategies ......................................................... 756
   Creating your backup strategy .............................................. 756
   Backup strategy considerations ........................................... 757
   Selecting the optimal backup techniques ............................... 758
   Understanding backup types ............................................... 760
   Using media rotation and maintaining additional media sets ...... 761
Backing up and recovering your data ............................................. 762
   Using the backup utility ....................................................... 763
   Backing up your data .......................................................... 765
   Scheduling backups ............................................................ 766
   Performing a one-time backup ............................................. 771
   Tracking scheduled and manual backups ............................... 776
   Recovering your data .......................................................... 778
   Recovering the system state ............................................... 784
   Restoring the operating system and the full system ............... 785
Backing up and restoring Active Directory .................................... 787
   Backup and recovery strategies for Active Directory ............... 787
   Performing a nonauthoritative restore of Active Directory ...... 789
   Performing an authoritative restore of Active Directory .......... 790
   Restoring Sysvol data ......................................................... 793
   Restoring a failed domain controller by installing a new domain controller ....... 793
Troubleshooting startup and shutdown .......................................... 795
   Resolving startup issues .................................................... 795
   Repairing missing or corrupted system files ......................... 797
   Resolving restart or shutdown issues ................................. 798

Index ................................................................................................. 799
What do you think of this book? We want to hear from you!
Microsoft is interested in hearing your feedback so we can improve our books and learning resources for you. To participate in a brief survey, please visit:

http://aka.ms/tellpress
Introduction

Welcome to Windows Server 2012 R2 Inside Out: Services, Security, & Infrastructure. As the author of many popular technology books, I’ve been writing professionally about Microsoft Windows and Windows Server since 1994. Over the years I’ve gained a unique perspective—the kind of perspective you can gain only after working with technologies for a long time. The advantage for you, the reader, is that my solid understanding of these technologies allowed me to dig into Windows Server 2012 R2 architecture, internals, and configuration to see how things really work under the hood and then pass this information on to you throughout this book.

Anyone transitioning to Windows Server 2012 R2 from Windows Server 2012 might be surprised at just how much has been updated as changes both subtle and substantial have been made throughout the operating system. For anyone transitioning to Windows Server 2012 R2 from Windows Server 2008 R2 or an earlier release of Windows Server, I’ll let you know right up front that Windows Server 2012 and Windows Server 2012 R2 are substantially different from earlier versions of Windows Server. Not only are there major changes throughout the operating system, but also this just might be the first version of Windows Server that you manage using a touch-based user interface. If you do end up managing it this way, mastering the touch-based UI and the revised interface options will be essential for your success. For this reason, I discuss both the touch UI and the traditional mouse and keyboard techniques throughout this book.

When you are working with touch UI–enabled computers, you can manipulate onscreen elements in ways that weren’t previously possible. You can enter text using the onscreen keyboard and manipulate onscreen elements in the following ways:

- **Tap.** Tap an item by touching it with your finger. A tap or double-tap of elements on the screen is generally the equivalent of a mouse click or double-click.

- **Press and hold.** Press your finger down and leave it there for a few seconds. Pressing and holding elements on the screen is generally the equivalent of a right-click.

- **Swipe to select.** Slide an item a short distance in the opposite direction from how the page scrolls. This selects the items and also might bring up related commands. If pressing and holding doesn’t display commands and options for an item, try swiping to select instead.

- **Swipe from edge (slide in from edge).** Starting from the edge of the screen, swipe or slide in. Sliding in from the right edge opens the Charms panel. Sliding in from the left edge shows open apps and allows you to easily switch between
them. Sliding in from the top or bottom edge shows commands for the active element.

- **Pinch.** Touch an item with two or more fingers and then move those fingers toward each other. Pinching zooms out.

- **Stretch.** Touch an item with two or more fingers and then move those fingers away from each other. Stretching zooms in.

In this book I teach you how server roles, role services, and features work; why they work the way they do; and how to customize them to meet your needs. Regardless of your job title, if you’re deploying, configuring, managing, or maintaining Windows Server 2012 R2, this book is for you. To pack in as much information as possible, I had to assume that you have basic networking skills and a basic understanding of Windows Server and that you are familiar with Windows commands and procedures. With this in mind, I don’t devote entire chapters to basic skills or to why you want to use Windows Server. Instead, I focus on essential services, infrastructure servers, and security.

**Conventions**

The following conventions are used in this book:

- **Abbreviated menu commands.** For your convenience, this book uses abbreviated menu commands. For example, “Tap or click Tools, Track Changes, Highlight Changes” means that you should tap or click the Tools menu, select Track Changes, and then tap or click the Highlight Changes command.

- **Boldface type.** **Boldface** type is used to indicate text that you enter or type.

- **Initial Capital Letters.** The first letters of the names of menus, dialog boxes, dialog box elements, and commands are capitalized. Example: the Save As dialog box.

- **Italicized type.** **Italicized** type is used to indicate new terms.

- **Plus sign (+) in text.** Keyboard shortcuts are indicated by a plus sign (+) separating two key names. For example, Ctrl+Alt+Delete means that you press the Ctrl, Alt, and Delete keys at the same time.
How to reach the author

Email: williamstanek@aol.com
Web: http://www.williamrstanek.com/
Facebook: https://www.facebook.com/William.Stanek.Author
Twitter: http://twitter.com/williamstanek

Errata and book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

http://aka.ms/WSIO_R2_SSI

If you discover an error that is not already listed, please submit it to us at the same page.

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

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to http://support.microsoft.com.

We want to hear from you

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

http://aka.ms/tellpress

We know you're busy, so we've kept it short with just a few questions. Your answers go directly to the editors at Microsoft Press. (No personal information will be requested.) Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: http://twitter.com/MicrosoftPress.
Active Directory is an extensible directory service that enables you to manage network resources efficiently. A directory service does this by storing detailed information about each network resource, which makes it easier to provide basic lookup and authentication. Being able to store large amounts of information is a key objective of a directory service, but the information must also be organized so that it’s easily searched and retrieved.

Active Directory provides for authenticated search and retrieval of information by dividing the physical and logical structures of the directory into separate layers. Understanding the physical structure of Active Directory is important for understanding how a directory service works. Understanding the logical structure of Active Directory is important for implementing and managing a directory service.

Active Directory physical architecture

The physical layer of Active Directory controls the following features:

- How directory information is accessed
- How directory information is stored on the hard disk of a server

Active Directory physical architecture: A top-level view

From a physical or machine perspective, Active Directory is part of the security subsystem. (See Figure 10-1.) The security subsystem runs in user mode. User-mode applications do not have direct access to the operating system or hardware. This means that requests from user-mode applications have to pass through the executive services layer and must be validated before being executed.
Chapter 10  Active Directory architecture

Figure 10-1  Top-level overview of the Active Directory architecture.

NOTE
Being part of the security subsystem makes Active Directory an integrated part of the access-control and authentication mechanism built into Microsoft Windows Server. Access control and authentication protect the resources in the directory.

Each resource in Active Directory is represented as an object. Anyone who tries to gain access to an object must be granted permission. Lists of permissions that describe who or what can access an object are referred to as access control lists (ACLs). Each object in the directory has an associated ACL.

You can restrict permissions across a broader scope by using Group Policy. The security infrastructure of Active Directory uses policy to enforce security models on several objects that are grouped logically. You can also set up trust relationships between groups of objects to allow for an even broader scope for security controls between trusted groups of objects that need to interact. From a top-level perspective, that’s how Active Directory works, but to really understand Active Directory, you need to delve into the security subsystem.

Active Directory within the Local Security Authority

Within the security subsystem, Active Directory is a subcomponent of the Local Security Authority (LSA). As shown in Figure 10-2, the LSA consists of many components that provide the security features of Windows Server and ensure that access control and authentication
function as they should. Not only does the LSA manage local security policy but it also performs the following functions:

- Generates security identifiers (SIDs)
- Provides the interactive process for logon
- Manages auditing

Figure 10-2  Windows Server security subsystem using Active Directory.

When you work through the security subsystem as it is used with Active Directory, you'll find the three following key areas:

- Authentication mechanisms
  - **NTLM (Msv1_0.dll).** Used for Windows NT LAN Manager (NTLM) authentication
  - **Kerberos (Kerberos.dll) and Key Distribution Center (Kdcsvc.dll).** Used for Kerberos VS authentication
  - **SSL (Schannel.dll).** Used for Secure Sockets Layer (SSL) authentication
  - **Authentication provider (Secur32.dll).** Used to manage authentication
Logon/access-control mechanisms

- **NET LOGON (Netlogon.dll).** Used for interactive logon through NTLM. For NTLM authentication, NET LOGON passes logon credentials to the directory service module and returns the SIDs for objects to clients making requests.

- **LSA Server (Lsasrv.dll).** Used to enforce security policies for Kerberos and SSL. For Kerberos and SSL authentication, LSA Server passes logon credentials to the directory service module and returns the SIDs for objects to clients making requests.

- **Security Accounts Manager (Samsrv.dll).** Used to enforce security policies for NTLM.

- **Directory service component: Directory service (Ntdsa.dll).** Used to provide directory services for Windows Server. This is the actual module that allows you to perform authenticated searches and retrieval of information.

As you can see, users are authenticated before they can work with the directory service component. Authentication is handled by passing a user’s security credentials to a domain controller. After the user is authenticated on the network, the user can work with resources and perform actions according to the permissions and rights the user has been granted in the directory. At least, this is how the Windows Server security subsystem works with Active Directory.

When you are on a network that doesn’t use Active Directory, or when you log on locally to a machine other than a domain controller, the security subsystem works as shown in Figure 10-3. Here, the directory service is not used. Instead, authentication and access control are handled through the Security Accounts Manager (SAM). Here, information about resources is stored in the SAM, which itself is stored in the registry.
Active Directory physical architecture

Figure 10-3  Windows Server security subsystem without Active Directory.

Directory service architecture

As you’ve seen, incoming requests are passed through the security subsystem to the directory service component. The directory service component is designed to accept requests from many kinds of clients. As shown in Figure 10-4, these clients use specific protocols to interact with Active Directory.
Protocols and client interfaces

The primary protocol for Active Directory access is Lightweight Directory Access Protocol (LDAP). LDAP is an industry standard protocol for directory access that runs over Transmission Control Protocol/Internet Protocol (TCP/IP). Active Directory supports LDAP versions 2 and 3. Clients can use LDAP to query and manage directory information—depending on the level of permissions they have been granted—by establishing a TCP connection to a domain controller. The default TCP port used by LDAP clients is 389 for standard communications and 636 for SSL.

Active Directory supports intersite and intrasite replication through the REPL interface, which uses either remote procedure calls (RPCs) or Simple Mail Transfer Protocol over Internet Protocol (SMTP over IP), depending on how replication is configured. Each domain controller is responsible for replicating changes to the directory to other domain controllers, using a multimaster approach. The multimaster approach used in Active Directory allows updates to be made to the directory by any domain controller and then replicated to other domain controllers.

For older messaging clients, Active Directory supports the Messaging Application Programming Interface (MAPI). MAPI allows messaging clients to access Active Directory
(which Microsoft Exchange uses for storing information), primarily for address book lookups. Messaging clients use RPCs to establish a connection with the directory service. The RPC Endpoint Mapper uses UDP port 135 and TCP port 135. Current messaging clients use LDAP instead of RPC.

For legacy clients, Active Directory supports the SAM interface, which also uses RPCs. This allows legacy clients to access the Active Directory data store the same way they would access the SAM database. The SAM interface is also used during certain replication activities.

**Directory System Agent and database layer**

Clients and other servers use the LDAP, REPL, MAPI, and SAM interfaces to communicate with the directory service component (Ntdsa.dll) on a domain controller. From an abstract perspective, the directory service component consists of the following:

- **Directory System Agent (DSA),** which provides the interfaces through which clients and other servers connect
- **Database layer,** which provides an application programming interface (API) for working with the Active Directory data store

From a physical perspective, the DSA is really the directory service component and the database layer resides within it. The reason for separating the two is that the database layer performs a vital abstraction. Without this abstraction, the physical database on the disk would not be protected from the applications the DSA interacts with. Furthermore, the object-based hierarchy used by Active Directory would not be possible. Why? Because the data store is in a single data file using a flat (record-based) structure, whereas the database layer is used to represent the flat file records as objects within a hierarchy of containers. Like a folder that can contain files and other folders, a container is simply a type of object that can contain other objects and other containers.

Each object in the data store has a name relative to the container in which it’s stored. This name is aptly called the object’s *relative distinguished name (RDN).* An object’s full name, also referred to as an object’s *distinguished name (DN),* describes the series of containers, from the highest to the lowest, of which the object is a part.

To make sure every object stored in Active Directory is truly unique, each object also has a globally unique identifier (GUID), which is generated when the object is created. Unlike an object’s RDN or DN, which can be changed by renaming an object or moving it to another container, the GUID can never be changed. The DSA assigns it to an object, and it never changes.

The DSA is responsible for ensuring that the type of information associated with an object adheres to a specific set of rules. This set of rules is referred to as the *schema.* The schema is
stored in the directory and contains the definitions of all object classes and describes their attributes. In Active Directory the schema is the set of rules that determine the kind of data that can be stored in the database, the type of information that can be associated with a particular object, the naming conventions for objects, and so on.

Inside OUT

*The schema saves space and helps validate attributes*

The schema serves to separate an object’s definition from its actual values. Thanks to the schema, Active Directory doesn’t have to write information about all of an object’s possible attributes when it creates the object. When you create an object, only the defined attributes are stored in the object’s record. This saves a lot of space in the database. Furthermore, because the schema specifies not only the valid attributes but also the valid values for those attributes, Active Directory uses the schema both to validate the attributes that have been set on an object and to keep track of what other possible attributes are available.

The DSA is also responsible for enforcing security limitations. It does this by reading the SIDs on a client’s access token and comparing them to the SIDs for an object. If a client has appropriate access permissions, it is granted access to an object. If a client doesn’t have appropriate access permissions, it’s denied access.

Finally, the DSA is used to initiate replication. Replication is the essential functionality that ensures that the information stored on domain controllers is accurate and consistent with changes that have been made. Without proper replication, the data on servers would become stale and outdated.

**Extensible Storage Engine**

Active Directory uses the Extensible Storage Engine (ESE) to retrieve information from, and write information to, the data store. The ESE uses indexed and sequential storage with transactional processing, as follows:

- **Indexed storage.** Indexing the data store allows the ESE to access data quickly without having to search the entire database. In this way, the ESE can rapidly retrieve, write, and update data.

- **Sequential storage.** Sequentially storing data means that the ESE writes data as a stream of bits and bytes. This allows data to be read from and written to specific locations.
- **Transactional processing.** Transactional processing ensures that changes to the database are applied as discrete operations that can be rolled back if necessary.

Any data that is modified in a transaction is copied to a temporary database file. This gives two views of the data that’s being changed: one view for the process changing the data and one view of the original data that’s available to other processes until the transaction is finalized. A transaction remains open as long as changes are being processed. If an error occurs during processing, the transaction can be rolled back to return the object being modified to its original state. If Active Directory finishes processing changes without errors occurring, the transaction can be committed.

As with most databases that use transactional processing, Active Directory maintains a transaction log. A record of the transaction is written first to an in-memory copy of an object, then to the transaction log, and finally to the database. The in-memory copy of an object is stored in the version store. The version store is an area of physical memory (RAM) used for processing changes. Typically, the version store is 25 percent of the physical RAM.

The transaction log serves as a record of all changes that have yet to be committed to the database file. The transaction is written first to the transaction log to ensure that even if the database shuts down immediately afterward, the change is not lost and can take effect. To ensure this, Active Directory uses a checkpoint file to track the point up to which transactions in the log file have been committed to the database file. After a transaction is committed to the database file, it can be cleared out of the transaction log.

The actual update of the database is written from the in-memory copy of the object in the version store and not from the transaction log. This reduces the number of disk I/O operations and helps ensure that updates can keep pace with changes. When many updates are made, however, the version store can reach a point at which it’s overwhelmed. This happens when the version store reaches 90 percent of its maximum size. When this happens, the ESE temporarily stops processing cleanup operations that are used to return space after an object is modified or deleted from the database.

Although in earlier releases of Windows Server index creation could affect domain controller performance, Windows Server 2012 and Windows Server 2012 R2 allow you to defer index creation to a time when it’s more convenient. By deferring index creation to a designated point in time, rather than creating indexes as needed, you can ensure that domain controllers can perform related tasks during off-peak hours, thereby reducing the impact of index creation. Any attribute that is in a deferred index state will be logged in the event log every 24 hours. Look for event IDs 2944 and 2945. When indexes are created, event ID 1137 is logged.

In large Active Directory environments, deferring index creation is useful to prevent domain controllers from becoming unavailable due to building indexes after schema updates. Before
you can use deferred index creation, you must enable the feature in the forest root domain. You do this using the \textit{DSHeuristics} attribute of the Directory Services object for the domain. Set the eighteenth bit of this attribute to 1. Because the tenth bit of this attribute typically also is set to 1 (if the attribute is set to a value), the attribute normally is set to the following: 000000000100000001. You can modify the \textit{DSHeuristics} attribute using ADSI Edit or Ldp.exe.

ADSI Edit is a snap-in you can add to any Microsoft Management Console (MMC). Open a new MMC by entering \textbf{MMC} at a prompt and then use the Add/Remove Snap-in option on the File menu to add the ADSI Edit snap-in to the MMC. You can then use ADSI Edit to modify the \textit{DSHeuristics} attribute by completing the following steps:

1. Press and hold or right-click the root node and then select Connect To. In the Connection Settings dialog box, choose the Select A Well Known Naming Context option. On the related selection list, select Configuration (because you want to connect to the Configuration naming context for the domain) and then tap or click OK.

2. In ADSI Edit, work your way down to the CN=Directory Service container by expanding the Configuration naming context, the CN=Configuration container, the CN=Services container, and the CN=Windows NT container.

3. Next, press and hold or right-click CN=Directory Service and then select Properties. In the Properties dialog box, select the dsHeuristics properties and then tap or click Edit.

4. In the String Attribute Editor dialog box, type the desired value, such as 000000000100000001, and then tap or click OK twice.

Ldp is a graphical utility. Open Ldp by typing \textbf{ldp} in the Apps Search box or at a prompt. You can then use Ldp to modify the \textit{DSHeuristics} attribute by completing the following steps:

1. Choose Connect on the Connection menu and then connect to a domain controller in the forest root domain. After you connect to a domain controller, choose Bind on the Connection menu to bind to the forest root domain using an account with enterprise administrator privileges.

2. Next, choose Tree on the View menu to open the Tree View dialog box. In the Tree View dialog box, choose CN=Configuration container as the base distinguished name to work with.

3. In the CN=Configuration container, expand the CN=Services container, expand the CN=Windows NT container, and then select the CN=Directory Service container. Next, press and hold or right-click CN=Directory Service and then select Modify.

4. In the Modify dialog box, type the attribute name as \texttt{dsHeuristics} and the value as 000000000100000001.
5. If the attribute already exists, set the Operation as Replace. Otherwise, set the Operation as Add.

6. Tap or click Enter to create an LDAP transaction for this update, and then tap or click Run to apply the change.

**NOTE**
The value 000000000100000001 is nine zeros with a 1 in the tenth position followed by seven zeros with a 1 in the eighteenth position.

Once the change is replicated to all domain controllers in the forest, they will defer index creation automatically. You must then trigger index creation manually by either restarting domain controllers, which rebuilds the schema cache and deferred indexes, or by triggering a schema update for the RootDSE. In ADSI Edit, you can initiate an update by connecting to the RootDSE. To do this, press and hold or right-click the root node and then select Connect To. In the Connection Settings dialog box, choose the Select A Well Known Naming Context option. On the related selection list, select RootDSE and then tap or click OK. In ADSI Edit, press and hold or right-click the RootDSE node and then select Update Schema Now.

To allow for object recovery and for the replication of object deletions, an object that is deleted from the database is logically removed rather than physically deleted. The way deletion works depends on whether Active Directory Recycle Bin is enabled or disabled.

**Deletion without Recycle Bin** When Active Directory Recycle Bin is disabled, as with standard deployments prior to Windows Server 2008 R2, most of the object’s attributes are removed and the object’s **Deleted** attribute is set to TRUE to indicate that it has been deleted. The object is then moved to a hidden Deleted Objects container where its deletion can be replicated to other domain controllers. (See Figure 10-5.) In this state, the object is said to be **tombstoned**. To allow the tombstoned state to be replicated to all domain controllers, and thus removed from all copies of the database, an attribute called **tombstoneLifetime** is also set on the object. The **tombstoneLifetime** attribute specifies how long the tombstoned object should remain in the Deleted Objects container. The default lifetime is 180 days.

![Figure 10-5: Active Directory object life cycle without Recycle Bin.](image-url)
Inside OUT

The tombstone process

When an object is tombstoned, Active Directory changes the distinguished name so that the object name can’t be recognized. Next, Active Directory deletes all of the object’s link-valued attributes, and most of the object’s non-link-valued attributes are cleared. Finally, the object is moved to the Deleted Objects container.

You can recover tombstoned objects using tombstone reanimation. However, attribute values that were removed are not recovered. This means the link-valued attributes, which include group memberships of user accounts, and the non-link-valued attributes are not recovered.

The ESE uses a garbage-collection process to clear out tombstoned objects after the tombstone lifetime has expired, and it performs automatic online defragmentation of the database after garbage collection. The interval at which garbage collection occurs is a factor of the value set for the garbageCollPeriod attribute and the tombstone lifetime. By default, garbage collection occurs every 12 hours. When there are more than 5,000 tombstoned objects to be garbage-collected, the ESE removes the first 5,000 tombstoned objects and then uses the CPU availability to determine if garbage collection can continue. If no other process is waiting for the CPU, garbage collection continues for up to the next 5,000 tombstoned objects whose tombstone lifetime has expired, and the CPU availability is again checked to determine if garbage collection can continue. This process continues until all the tombstoned objects whose tombstone lifetime has expired are deleted or another process needs access to the CPU.

Deletion with Recycle Bin

When Active Directory Recycle Bin is enabled as an option with Windows Server 2008 R2 and later, objects aren’t tombstoned when they are initially deleted and their attributes aren’t removed. Instead, the deletion process occurs in stages.

In the first stage of the deletion, the object is said to be logically deleted. Here, the object’s Deleted attribute is set to TRUE to indicate that it has been deleted. The object is then moved, with its attributes and name preserved, to a hidden Deleted Objects container where its deletion can be replicated to other domain controllers. (See Figure 10-6.) To allow the logically deleted state to be replicated to all domain controllers, and thus removed from all copies of the database, an attribute called ms-DeletedObjectLifetime is also set on the object. The ms-DeletedObjectLifetime attribute specifies how long the logically deleted object should remain in the Deleted Objects container. The default deleted object lifetime is 180 days.
When the deleted object lifetime expires, Active Directory removes most of the object's attributes, changes the distinguished name so that the object name can't be recognized, and sets the object's `tombstoneLifetime` attribute. This effectively tombstones the object (and the process is the same as the legacy tombstone process).

The recycled object remains in the Deleted Objects container until the recycled object lifetime expires, and it's said to be in the `recycled` state. The default tombstone lifetime is 180 days.

As with deletion without the Recycle Bin, the ESE uses a garbage-collection process to clear out tombstoned objects after the tombstone lifetime has expired. This garbage-collection process is the same as discussed previously.

**Data store architecture**

After you examine the operating system components that support Active Directory, the next step is to see how directory data is stored on a domain controller's hard disks. As Figure 10-7 shows, the data store has a primary data file and several other types of related files, including working files and transaction logs.
These files are used as follows:

- **Primary data file (Ntds.dit).** Physical database file that holds the contents of the Active Directory data store

- **Checkpoint file (Edb.chk).** Checkpoint file that tracks the point up to which the transactions in the log file have been committed to the database file

- **Temporary data (Tmp.edb).** Temporary workspace for processing transactions

- **Primary log file (Edb.log).** Primary log file that contains a record of all changes that have yet to be committed to the database file

- **Secondary log files (Edb00001.log, Edb00002.log, ...).** Additional logs files that are used as needed

- **Reserve log files (EdbRes00001.jrs, EdbRes00002.jrs, ...).** Files that are used to reserve space for additional log files if the primary log file becomes full
The primary data file contains three indexed tables:

- **Active Directory data table.** The data table contains a record for each object in the data store, which can include object containers, the objects themselves, and any other type of data that is stored in Active Directory.

- **Active Directory link table.** The link table is used to represent linked attributes. A linked attribute is an attribute that refers to other objects in Active Directory. For example, if an object contains other objects (that is, it is a container), attribute links are used to point to the objects in the container.

- **Active Directory security descriptor table.** The security descriptor table contains the inherited security descriptors for each object in the data store. Windows Server uses this table so that inherited security descriptors no longer have to be duplicated on each object. Instead, inherited security descriptors are stored in this table and linked to the appropriate objects. This makes Active Directory authentication and control mechanisms very efficient.

Think of the data table as having rows and columns; the intersection of a row and a column is a field. The table’s rows correspond to individual instances of an object. The table’s columns correspond to attributes defined in the schema. The table’s fields are populated only if an attribute contains a value. Fields can be a fixed or a variable length. If you create an object and define only 10 attributes, only these 10 attributes will contain values. Although some of those values might be fixed length, others might be variable length.

Records in the data table are stored in data pages that have a fixed size of 8 kilobytes (KBs, or 8,192 bytes). Each data page has a page header, data rows, and free space that can contain row offsets. The page header uses the first 96 bytes of each page, leaving 8,096 bytes for data and row offsets.

Row offsets indicate the logical order of rows on a page, which means that offset 0 refers to the first row in the index, offset 1 refers to the second row, and so on. If a row contains long, variable-length data, the data might not be stored with the rest of the data for that row. Instead, Active Directory can store an 8-byte pointer to the actual data, which is stored in a collection of 8 KB pages that aren’t necessarily written contiguously. In this way, an object and all its attribute values can be much larger than 8 KBs.

The primary log file has a fixed size of 10 megabytes (MBs). When this log fills up, Active Directory creates additional (secondary) log files as necessary. The secondary log files are also limited to a fixed size of 10 MBs. Active Directory uses the reserve log files to reserve space on disk for log files that might need to be created. Because several reserve files are already created, this speeds up the transactional logging process when additional logs are needed.
By default, the primary data file, the working files, and the transaction logs are all stored in the same location. On a domain controller’s system volume, you’ll find these files in the %SystemRoot%\NTDS folder. Although these are the only files used for the data store, Active Directory uses other files. For example, policy files and other files, such as startup and shutdown scripts used by the DSA, are stored in the %SystemRoot%\Sysvol folder.

NOTE

A distribution copy of Ntds.dit is also placed in the %SystemRoot%\System32 folder. This is used to create a domain controller when you install Active Directory on a server running Windows Server. If the file doesn’t exist, the Active Directory Installation Wizard will need the installation media to promote a member server to be a domain controller.

Inside OUT

The log files have attributes you can examine

When you stop Active Directory Domain Services, you can use the Extensible Storage Engine Utility (esentutl.exe) to examine log file properties. At an elevated command prompt, type esentutl.exe –ml LogName, where LogName is the name of the log file to examine, such as edb.log, to obtain detailed information on the log file, including the base name, creation time, format version, log sector sizes, and logging parameters. While Active Directory Domain Services is offline, you can also use esentutl.exe to perform defragmentation, integrity checks, and copy, repair, and recovery operations. To learn more about this utility, type esentutl.exe at an elevated command prompt. Following the prompts, you can then type the letter corresponding to the operation you want to learn more about. For example, type esentutl.exe and then press the D key to learn the defragmentation options.

Active Directory logical architecture

The logical layer of Active Directory determines how you see the information contained in the data store and also controls access to that information. The logical layer does this by defining the namespaces and naming schemes used to access resources stored in the directory. This provides a consistent way to access directory-stored information regardless of type. For example, you can obtain information about a printer resource stored in the directory in much the same way that you can obtain information about a user resource.
To better understand the logical architecture of Active Directory, you need to understand the following topics:

- Active Directory objects
- Active Directory domains, trees, and forests
- Active Directory trusts
- Active Directory namespaces and partitions
- Active Directory data distribution

**Active Directory objects**

Because so many types of resources can be stored in the directory, a standard storage mechanism was needed and Microsoft developers decided to use the LDAP model for organizing data. In this model, each resource that you want to represent in the directory is created as an object with attributes that define information you want to store about the resource. For example, the user object in Active Directory has attributes for a user’s first name, middle initial, last name, and logon name.

An object that holds other objects is referred to as a *container object* or simply a *container*. The data store itself is a container that contains other containers and objects. An object that can’t contain other objects is a *leaf object*. Each object created within the directory is of a particular type or class. The object classes are defined in the schema. Some of the object types include:

- User
- Group
- Computer
- Printer

When you create an object in the directory, you must comply with the schema rules for that object class. Not only do the schema rules dictate the available attributes for an object class, they also dictate which attributes are mandatory and which attributes are optional. When you create an object, mandatory attributes must be defined. For example, you can’t create a user object without specifying the user’s full name and logon name. The reason is that these attributes are mandatory.

Some rules for attributes also are defined in policy. For example, the default security policy for Windows Server specifies that a user account must have a password and that the password must meet certain complexity requirements. If you try to create a user account without
a password or with a password that doesn’t meet these complexity requirements, the account creation will fail because of the security policy.

The schema also can be extended or changed. This allows administrators to define new object classes, add attributes to existing objects, and change the way attributes are used. However, you need special access permissions and privileges to work directly with the schema. Specifically, you must be a member of the Schema Admins group.

**Active Directory domains, trees, and forests**

Within the directory, objects are organized using a hierarchical tree structure called a directory tree. The structure of the hierarchy is derived from the schema and is used to define the parent–child relationships of objects stored in the directory.

A logical grouping of objects that allows central management of those objects is called a domain. In the directory tree, a domain is itself represented as an object. In fact, it’s the parent object of all the objects it contains. An Active Directory domain can contain millions of objects. You can create a single domain that contains all the resources you want to manage centrally. In Figure 10-8, a domain object is represented by a large triangle and the objects it contains are as shown.

![Figure 10-8 An Active Directory domain.](image-url)
Domains are only one of several building blocks for implementing Active Directory structures. Other building blocks include the following:

- Active Directory trees, which are logical groupings of domains
- Active Directory forests, which are logical groupings of domain trees

As described, a directory tree is used to represent a hierarchy of objects, showing the parent–child relationships between those objects. Thus, when we’re talking about a domain tree, we’re looking at the relationship between parent and child domains. The domain at the top of the domain tree is referred to as the root domain (think of this as an upside-down tree). More specifically, the root domain is the first domain created in a new tree within Active Directory. When talking about forests and domains, there is an important distinction made between the first domain created in a new forest—a forest root domain—and the first domain created in each additional tree within a forest—a root domain.

In the example shown in Figure 10-9, cohovineyard.com is the root domain in an Active Directory forest with a single tree—that is, it’s the forest root domain. As such, cohovineyard.com is the parent of the sales.cohovineyard.com domain and the mf.cohovineyard.com domain. The mf.cohovineyard.com domain itself has a related subdomain: bottling.mf.cohovineyard.com. This makes mf.cohovineyard.com the parent of the child domain bottling.mf.cohovineyard.com.

![Figure 10-9 An Active Directory forest with a single tree.](image)

The most important thing to note about this and all domain trees is that the namespace is contiguous. Here, all the domains are part of the cohovineyard.com namespace. If a domain is a part of a different namespace, it can be added as part of a new tree in the forest. In the example shown in Figure 10-10, a second tree is added to the forest. The root domain of the second tree is cohowinery.com, and this domain has cs.cohowinery.com as a child domain.
You create a forest root domain by installing Active Directory on a stand-alone server and establishing the server as the first domain controller in a new forest. To add a tree to an existing forest, you install Active Directory on a stand-alone server and configure the server as a member of the forest, but with a domain name that is not part of the current namespace being used. You make the new domain part of the same forest to allow associations called **trusts** to be made between domains that belong to different namespaces.

### Active Directory trusts

In Active Directory, two-way transitive trusts are established automatically between domains that are members of the same forest. Trusts join parent and child domains in the same domain tree and join the roots of domain trees. Trusts are transitive, which means that if domain A trusts domain B and domain B trusts domain C, domain A trusts domain C. Because all trusts in Active Directory are two-way and transitive, by default every domain in a forest implicitly trusts every other domain. It also means that resources in any domain are available to users in every domain in the forest. For example, with the trust relationships in place, a user in the sales.cohovineyard.com domain could access a printer or other resources in the cohovineyard.com domain—or even the cs.cohowinery.com domain.

However, the creation of a trust doesn’t imply any specific permission. Instead, it implies only the ability to grant permissions. No privileges are automatically implied or inherited by the establishment of a trust relationship. The trust doesn’t grant or deny any permission. It exists only to allow administrators to grant permissions.
Several key terms are used to describe trusts, including the following:

- **Trusting domain.** A domain that establishes a trust is referred to as a *trusting domain*. Trusting domains allow access by users from another domain (the trusted domain).

- **Trusted domain.** A domain that trusts another domain is referred to as a *trusted domain*. Users in trusted domains have access to another domain (the trusting domain).

To make it easier for administrators to grant access throughout a forest, Active Directory allows you to designate two types of administrators:

- **Enterprise administrators.** These are the designated administrators of the enterprise. Enterprise administrators can manage and grant access to resources in any domain in the Active Directory forest.

- **Domain administrators.** These are the designated administrators of a particular domain. Domain administrators in a trusting domain can access user accounts in a trusted domain and set permissions that grant access to resources in the trusting domain.

Going back to the example, Tom, an enterprise administrator in this forest, could grant access to resources in any domain in the forest. If Jim, in the sales.cohovineyard.com domain, needed access to a printer in the cs.cohowinery.com domain, Tom could grant this access. Because in this example cs.cohowinery.com is the trusting domain and sales.cohovineyard.com is the trusted domain, Sarah, a domain administrator in the cs.cohowinery.com domain, also could grant permission to use the printer. Bob, a domain administrator for sales.cohovineyard.com, could not grant such permissions, however, because the printer resource exists in a domain other than the one he controls.

To continue working with Figure 10-10, take a look at the arrows that designate the trust relationships. For a user in the sales.cohovineyard.com domain to access a printer in the cs.cohowinery.com domain, the request must pass through the following series of trust relationships:

1. The trust between sales.cohovineyard.com and cohoverineyard.com

2. The trust between cohovineyard.com and cohowinery.com

3. The trust between cohowinery.com and cs.cohowinery.com

The *trust path* defines the path that an authentication request must take between the two domains. Here, a domain controller in the user’s local domain (sales.cohovineyard.com) would pass the request to a domain controller in the cohovineyard.com domain. This domain controller, in turn, would pass the request to a domain controller in the cohowinery.com domain.
Finally, the request would be passed to a domain controller in the cs.cohowinery.com domain, which would ultimately grant or deny access.

In all, the user’s request has to pass through four domain controllers—one for each domain between the user and the resource. Because the domain structure is separate from the network’s physical structure, the printer could actually be located right beside the user’s desk and the user would still have to go through this process. If you expand this scenario to include all the users in the sales.cohovineyard.com domain, you could potentially have hundreds of users whose requests have to go through a similar process to access resources in the cs.cohowinery.com domain.

Omitting the fact that the domain design in this scenario is very poor—because if many users are working with resources, those resources are ideally in their own domain or in a domain closer in the tree—one solution for this problem would be to establish a *shortcut trust* between the user’s domain and the resource’s domain. With a shortcut trust, you could specify that cs.cohowinery.com explicitly trusts sales.cohovineyard.com. Now when a user in the sales.cohovineyard.com domain requests a resource in the cs.cohowinery.com domain, the local domain controller knows about cs.cohowinery.com and can directly submit the request for authentication. This means that the sales.cohovineyard.com domain controller sends the request directly to a cs.cohowinery.com domain controller.

Shortcut trusts are designed to help make more efficient use of resources on a busy network. On a network with a lot of activity, the explicit trust can reduce the overhead on servers and on the network as a whole. You shouldn’t implement shortcut trusts without careful planning. You should use them only when resources in one domain will be regularly accessed by users in another domain. They don’t need to be used between two domains that have a parent–child relationship because a default trust already exists explicitly between a parent domain and a child domain.

With Active Directory, you can also make use of *external trusts*. External trusts are manually configured and are always nontransitive. External trusts can be either one-way or two-way trusts. When you establish a trust between a domain in one forest and a domain in another forest, security principals from the external domain can access resources in the internal domain. In the internal domain, Active Directory creates a foreign security principal to represent each security principal in the external domain. Foreign security principals can be added to domain local groups in the internal domain.

**Active Directory namespaces and partitions**

Any data stored in the Active Directory database is represented logically as an object. Every object in the directory has a relative distinguished name (RDN). That is, every object has a name relative to the parent container in which it’s stored. The relative name is the name of the object itself, and it’s also referred to as an object’s *common name* (CN). This relative name is
stored as an attribute of the object and must be unique for the container in which it’s located. Following this, no two objects in a container can have the same common name, but two objects in different containers could have the same name.

In addition to an RDN, objects have a distinguished name (DN). An object’s DN describes the object’s place in the directory tree and is logically the series of containers from the highest to the lowest of which the object is a part. It’s called a distinguished name because it serves to distinguish like-named objects and, as such, must be unique in the directory. No two objects in the directory will have the same distinguished name.

Every object in the directory has a parent, except the root of the directory tree, which is referred to as the rootDSE. The rootDSE represents the top of the logical namespace for a directory. It has no name per se. Although there is only one rootDSE, the information stored in the rootDSE specifically relates to the domain controller on which the directory is stored. In a domain with multiple domain controllers, the rootDSE will have a slightly different representation on each domain controller. The representation relates to the capability and configuration of the domain controller in question. In this way, Active Directory clients can determine the capabilities and configuration of a particular domain controller.

Below the rootDSE, every directory tree has a root domain. The root domain is the first domain created in an Active Directory forest and is also referred to as the forest root domain. After it’s established, the forest root domain never changes, even if you add new trees to the forest. The LDAP distinguished name of the forest root domain is DC=ForestRootDomainName, where DC is an LDAP identifier for a domain component and ForestRootDomainName is the actual name of the forest root domain. Each level within the domain tree is broken out as a separate domain component. For example, if the forest root domain is cohovineyard.com, the domain’s distinguished name is DC=cohovineyard,DC=com.

When Active Directory is installed on the first domain controller in a new forest, three containers are created below the rootDSE:

- The Forest Root Domain container, which is the container for the objects in the forest root domain
- The Configuration container, which is the container for the default configuration and all policy information
- The Schema container, which is the container for all objects, classes, attributes, and syntaxes

From a logical perspective, these containers are organized as shown in Figure 10-11. The LDAP identifier for an object’s common name is CN. The DN for the Configuration container is CN=configuration,DC=ForestRootDomainName, and the DN for the Schema container is CN=schema,CN=configuration,DC=ForestRootDomainName. In the cohovineyard.com
domain, the DNs for the Configuration and Schema containers are CN=configuration,DC=cohovineyard,DC=com and CN=schema,CN=configuration,DC=cohovineyard,DC=com, respectively. As you can see, the distinguished name allows you to walk the directory tree from the relative name of the object you are working with to the forest root.

![Diagram of the directory tree in a new forest.](image)

**Figure 10-11** The directory tree in a new forest.

As shown in the figure, the Forest Root Domain container and the Configuration and Schema containers exist within their own individual partitions. Active Directory uses partitions to logically apportion the directory so that each domain controller does not have to store a complete copy of the entire directory. To do this, object names are used to group objects into logical categories so that the objects can be managed and replicated as appropriate. The largest logical category is a directory partition. All directory partitions are created as instances of the domainDNS object class.

As far as Active Directory is concerned, a domain is a container of objects that is logically partitioned from other container objects. When you create a new domain in Active Directory, you create a new container object in the directory tree, and that container, in turn, is contained by a domain directory partition for the purposes of management and replication.
Active Directory data distribution

Active Directory uses partitions to help distribute three general types of data:

- Domainwide data, which is data replicated to every domain controller in a domain
- Forestwide data, which is data replicated to every domain controller in a forest
- Application data, which is data replicated to an arbitrary set of domain controllers

Every domain controller stores at least one domain directory partition and two forestwide data partitions: the schema partition and the configuration partition. Data in a domain directory partition is replicated to every domain controller in the domain as a writeable replica.

Forestwide data partitions are replicated to every domain controller in the forest. The configuration partition is replicated as a writeable replica. The schema partition is replicated as a read-only replica, and the only writeable replica is stored on a domain controller that is designated as having the schema operations master role. Other operations master roles also are defined.

Active Directory can replicate application-specific data that is stored in an application partition, such as the default application partitions used with zones in Domain Name System (DNS) that are integrated with Active Directory. Application partition data is replicated on a forestwide, domainwide, or other basis to domain controllers that have a particular application partition. If a domain controller doesn’t have an application partition, it doesn’t receive a replica of the application partition.

In addition to full replicas that are distributed for domains, Active Directory distributes partial replicas of every domain in the forest to special domain controllers designated as global catalog servers. The partial replicas stored on global catalog servers contain information on every object in the forest and are used to facilitate searches and queries for objects in the forest. Because only a subset of an object’s attributes is stored, the amount of data replicated to and maintained by a global catalog server is significantly smaller than the total size of all object data stored in all the domains in the forest.

Every domain must have at least one global catalog server. By default, the first domain controller installed in a domain is set as that domain's global catalog server. You can change the global catalog server, and you can designate additional servers as global catalog servers as necessary.
### Numbers and Symbols

- *** (asterisk)**, 647
- **@ (at symbol)**, 338, 731
- **$_ automatic variable**, 108
- **$ (dollar sign)**, 561, 563, 731
- **\ (backslash)**, 108, 279, 731

### A

#### A (Host Address) records
- about, 179, 238–239
- adding, 239–242
- DNS delegation and, 456
- dynamic updates and, 156, 190
- forward lookup zones and, 203
- root servers and, 194
- stub zones and, 186

#### AAAA (IPv6 Host Address) records
- about, 179, 239
- adding, 239–242
- DNS delegation and, 456
- dynamic updates and, 191

#### AB performance counters, 649

#### access control entries (ACEs), 444, 530

#### access control lists (ACLs), 296, 502, 596

#### Account Is Disabled policy setting, 528

#### Account Lockout Duration policy setting, 517, 520

#### Account Lockout Policy
- about, 515, 582
- policy settings, 517, 523
- troubleshooting, 537

#### Account Lockout Threshold policy setting, 517, 520

#### Account Operators group
- Builtin container and, 546
- computer accounts and, 550
- domain user accounts and, 527
- editing Password Replication Policy, 505
- managing groups, 545

#### Account Will Be Locked Out policy setting, 523

#### Accounts: Rename Administrator Account policy setting, 583

#### Accounts: Rename Guest Account policy setting, 583

#### Acknowledgment message (DHCP), 94–95

#### ACLs (access control lists), 296, 502, 596

#### Active Directory
- authorizing DHCP servers in, 109
- backing up and restoring, 787–795
- compatibility considerations, 330–337
- connecting clients to, 439
- creating computer accounts in, 549–551
- creating implementation/update plan, 379–384
- data distribution, 319
- data store architecture, 301–302, 307–310, 326
- database layer, 301–302
- developing domain plan, 384–389
- developing organizational unit plan, 389–396
- directory service component, 298–300
- directory service polling interval, 262
- Directory System Agent, 301–302
- DNS support, 181, 183–185, 201–205, 212, 217–219, 222–223
- domains, trees, and forests, 312–314
- Extensible Storage Engine, 302–307
- global catalogs, 325–330
- GlobalName zone and, 249
- indexed tables, 309
- Local Security Authority and, 296–299
- logical architecture, 310–319
- namespace considerations, 316–318
- operations masters, 362–377
- partition considerations, 316–318, 419–423
- performing authoritative restores, 790–793
- performing installation from media, 457–461
- performing nonauthoritative restores, 789–790
- physical architecture, 295–310
- protocols and client interfaces, 300–301
- search considerations, 323–325
- site considerations, 397–401, 424–433, 623–661
- top-level architectural view, 295–296
- trust relationships, 51, 314–316, 344–358

---

**Index**

---
Active Directory Administrative Center
configuring domain account options, 531
configuring profile options, 534
creating clone virtualized domain controller, 462–464
creating/moving accounts/resources for use with OUs, 475
creating OUs, 471, 473
domain user accounts, 527, 537–541
enabling Active Directory Recycle Bin, 556
managing computer accounts, 549–554
managing groups, 545–548
obtaining effective access, 530–531
OU deletion protection, 472–473
password settings policies, 520, 522–523
PSO precedence, 521
raising/lowering domain/forest functional levels, 333–334
Active Directory Domain Services (AD DS)
Active Directory-integrated zones, 181
cloning virtualized domain controllers, 461–466
creating and managing organizational units, 471–475
creating/moving accounts/resources for use with OUs, 475–479
DHCP support, 91
installing, 440–461
managing Group Policy, 565
preinstallation considerations, 435–439
Scan Operators security group, 668
uninstalling, 466–471
Active Directory Domain Services Configuration Wizard
adding AD DS role, 440
Adprep.exe support, 443
creating domain controllers in domains, 445–453
creating domains in forests, 453–457
installing DNS Server service, 202–204
installing RODCs, 490–495
performing installation from media, 457–461
promoting servers to domain controllers, 443–445
removing global catalogs, 469
uninstalling Active Directory, 466–471
Active Directory Domain Services Installation Wizard, 499–501
Active Directory Domains And Trusts
establishing trusts, 354–357
examining trusts, 350–353
manipulating UPN suffixes, 338
operations master roles, 367–368
raising/lowering domain/forest functional levels, 333–335
verifying and troubleshooting trusts, 357–358
Active Directory Group Policy, 566–567, 570
Active Directory Migration Tool (ADMT), 383, 387
Active Directory objects, 311–312, 316–318
Active Directory Recycle Bin
domain functional level support, 332
enabling, 556
recovering deleted accounts, 555–557
recovering deleted objects, 305–307
Active Directory Sites And Services (Dssite.msc)
associating domain controllers with sites, 627–628
configuring advanced site-link options, 646
configuring bridgehead servers, 644–645
configuring site-link bridges, 638–639
creating site links, 631–633
creating sites, 624–625
creating subnets, 626–627
designating global catalog servers, 326–327
enabling universal group membership caching, 338–340
replication schedules for site links, 635–636
Active Directory Users And Computers
checking for updates, 452
configuring delegated user accounts, 359
configuring domain account options, 531
configuring profile options, 534
creating/moving accounts/resources for use with OUs, 475
creating OUs, 471
delegating administration of OUs, 476
deleting OUs, 473
domain user accounts, 527–528, 537–541
editing Password Replication Policy, 505
Effective Access tool, 530
managing computer accounts, 549–554
managing groups, 545–548
managing RODCs, 499, 505–506, 508–511
managing service accounts, 559
password settings policies, 520
PSO precedence, 521
saving queries, 549
setting OU properties, 474–475
transferring infrastructure master roles, 375
AD DS (Active Directory Domain Services)
Active Directory-integrated zones, 181
cloning virtualized domain controllers, 461–466
creating and managing organizational units, 471–475
creating/moving accounts/resources for use with OUs, 475–479
DHCP support, 91
installing, 440–461
managing Group Policy, 565
preinstallation considerations, 435–439
Scan Operators security group, 668
uninstalling, 466–471
adaptive query timeout, 26
Add A Script dialog box, 601–603
Add-ADComputerServiceAccount cmdlet, 560
Add-ADGroupMember cmdlet, 559
Add Counters dialog box, 736–738
Add-DhcpServerInDC cmdlet, 109
Add-DhcpServerv4ExclusionRange cmdlet, 123, 127
Add-DhcpServerv4Scope cmdlet, 122
Add-DhcpServerv6ExclusionRange cmdlet, 124
Add-DhcpServerv6Scope cmdlet, 123
Add/Edit Condition dialog box, 146–147
add exclude range command, 121
Add Features Wizard, 571
Add Forest dialog box, 577–578
Add Group Or User dialog box, 588–589
add ip range command, 121
Add Navigation Nodes dialog box, 334, 556
Add Or Remove Scanners dialog box, 667
Add Or Remove Snap-ins dialog box, 329, 574, 604
Add-Printer cmdlet, 686
Add Printer Driver Wizard, 711–712
Add Printer Wizard, 683–686
Add RADIUS Client dialog box, 158
Add/Remove Servers dialog box, 693–694
Add Roles And Features Wizard
adding AD DS role, 443–444
adding IPAM Server feature, 92
installing AD DS, 440–443
installing DHCP Server service, 104–105
installing DNS Server service, 205–210
installing printer servers, 665–667
installing RODCs, 490
installing Windows Server Backup, 763
integrating DHCP and NAP, 157
LPR Port Monitor feature, 676
setting up WINS servers, 277–279
Add Server dialog box, 132, 282
Add Services dialog box, 361–362
Add User Or Group dialog box, 525–526
Additional Drivers dialog box, 718–719
Additional Navigation Nodes dialog box, 473, 520
AddressUtilizationCollectionTask, 93
ADM file format, 569–570
admin mode, 3, 12–16
administration OU design model, 395–396
administrative templates, 567–570, 607, 689
Administrators group
Active Directory supported, 315
adding print devices, 671
backup and recovery operations, 763
Builtin container and, 546
changing Group Policies, 515
computer accounts and, 550
creating OUs, 471
domain user accounts and, 527
forest plans and, 382, 384
managing printers, 693
printer permissions, 702–703
remote logon, 6–7
RODC Denied Accounts list and, 505
schemas and, 330
trustworthy printer drivers and, 690
Administrators Local Group Policy, 571
.adml file extension, 570
ADMT (Active Directory Migration Tool), 383, 387
ADMX file format, 569–570
Adprep.exe program, 443–444, 489–490
ADSI Edit snap-in, 304–305, 370–371
Advanced Encryption Standard (AES), 332
Advanced Password Replication Policy dialog box, 508–510
Advanced Security Settings dialog box, 705–707
Advanced Settings dialog box, 767
Advanced TCP/IP Settings dialog box, 66–71
.aero top-level domain name, 175
AES (Advanced Encryption Standard), 332
aging records, 254–256
All Application Packages group, 702
all-subnets-directed broadcasts, 32
Allow Logon Locally right, 584
Allow Logon Through Remote Desktop Services right, 524
Allow Processing Across A Slow Network Connection policy setting, 609
Allowed RODC Password Replication Group, 504–505
American Standard Code for Information Interchange (ASCII), 727
APIPA (Automatic Private IPv4 Addressing)
configuring remote clients, 89
disabling, 65
IP addressing problems, 78
reserved IPv4 addresses, 33
APOs (Authentication Policy objects), 519
Application event log, 466, 776, 782
application partitions
data distribution, 319
default, 251–254, 319
replication partners, 421
RODC considerations, 487
Applications Policy Processing policy, 608
Apply Group Policy permission, 595–596
archive attribute, 760
ASCII (American Standard Code for Information Interchange), 727
.asia top-level domain name, 175
asterisk (*), 647
at symbol (@), 338, 731
ATQ performance counters, 649
auditing
Active Directory support, 297
authentication policies, 519
Group Policy support, 584
logging support, 151–155
logon failure, 537
printer access, 706–708
Auditing Entry For dialog box, 705–706
AuditTask, 93
authentication. See also Kerberos authentication
across domain boundaries, 344–347
across forest boundaries, 347–350
Active Directory support, 296–299, 337–350
delagating, 358–362
NTLM, 297–298, 340–341
remote computers, 5
RODC support, 484
security tokens, 337–338
trusts and, 315, 357
universal group membership caching, 337–340
Authentication Mechanism Assurance, 332
authentication policies, 518–519
Authentication Policies container, 518–519
Authentication Policy object, 518
Authentication Policy objects (APOs), 519
Authentication Policy Silo object, 518
Authentication Policy Silos container, 518
Authoritative Restore Confirmation dialog box, 792
authorizing DHCP servers, 109
Automatic Private IPv4 Addressing (APIPA)
configuring remote clients, 89
disabling, 65
IP addressing problems, 78
reserved IPv4 addresses, 33
automatic replication partners, 280–282
AVHD files, 462
B
B-Node (Broadcast Node), 275
Back Up Group Policy Object dialog box, 617–618
Background Priority policy setting, 609
backslash (\), 108, 279, 731
backup and recovery processes
about, 762–766
backing up and restoring Active Directory, 787–795
configuring Active Directory for fast recovery with SANs, 438–439
creating problem-resolution policy documents, 750–752
developing backup strategies, 756–762
developing contingency procedures, 748–749
DHCP databases, 165
disaster-planning strategies, 747–752
disaster preparedness procedures, 752–756
GPOs, 617–621
implementing problem-escalation and response procedures, 749–750
installing Active Directory from, 457–461
media rotation and maintaining media sets, 761–762
one-time backups, 771–776
printer failures, 740
recovering data, 778–784
restoring operating system, 785–787
scheduling backups, 766–771
System State backup, 460, 784–785
tracking backups, 776–777
troubleshooting startup and shutdown, 795–798
WINS database, 291–292
Backup dialog box, 618–619
Backup-GPO cmdlet, 617
Backup Once Wizard, 771–776
Backup Operators group
backup and recovery operations, 763
Builtin container and, 546
editing Password Replication Policy, 505
forestwide administration, 384
Backup Progress dialog box, 776
Backup Schedule Wizard, 766–771
Backup utility (Windows Server)
about, 752, 760, 762–763
Back Up Once feature, 763
backing up data, 765–766
Backup Schedule feature, 763
getting started with, 763–764
installing, 763
new enhancements, 765
performing one-time backups, 771–776
recovering data, 778–784
restoring operating system, 785–787
scheduling backups, 766–771
tracking scheduled and manual backups, 776–777
Berkeley Internet Name Domain (BIND), 201, 457
binary source files, 667
BIND (Berkeley Internet Name Domain), 201, 457
BitLocker Driver Encryption, 442, 759
.biz top-level domain name, 175
Boolean Attribute Editor dialog box, 371
BOOTP (Bootstrap Protocol), 87, 141
Bootstrap Protocol (BOOTP), 87, 141
Branch Office Direct Printing option, 671–672, 681
bridgehead servers
  configuring, 642–645
determining, 643
intersite replication and, 416–419, 422
load balancing and, 403
bridges, 34, 430–432
BRIDGES_REQUIRED flag, 640
broadcast IPv4 addresses, 31–33
Broadcast Node (B-Node), 275
Browse For A Group Policy Object dialog box, 574
Browse For Domain dialog box, 471
Browse For Folder dialog box, 165, 291, 605, 620
Browse For Virtual Hard Disks dialog box, 105, 206, 665
BuiltIn container, 546
burst handling of registrations (WINS), 284–285
business unit OU design model, 392–393
Bytes Printed/Sec performance counter, 738
C
CA (certificate authority), 630
CacheLockingPercent registry key, 173
caches and caching
  cache locking, 173
  cache poisoning attacks, 173, 210
  credentials, 536
  DNS, 172–173, 199, 259–262
  flushing, 83, 85
  LDAP, 409
  persistent caches, 26–27
universal group membership caching, 337–340, 433
WINS, 275–276
CAD (computer-aided design), 661, 716
CAL (Client Access License), 3
canceling print jobs, 733
Canonical Name (CNAME) records, 171, 180, 243
CCNA (Cisco Certified Network Associate), 35
certificate authority (CA), 630
challenge, NTLM authentication, 340–341
Change Directory Server dialog box, 367–368, 375, 506
Change Domain dialog box, 471
Change Forest dialog box, 624, 631
Change Operations Master dialog box, 368
Change Schema Master dialog box, 366–367
Change Zone Replication Scope dialog box, 254
child domains, 49
Choose Computer Container dialog box, 614
Choose User Container dialog box, 614
CIDR (classless inter-domain routing), 32, 36
CIFS (Common Internet File System), 408
Cisco Certified Network Associate (CCNA), 35
Class A networks
  about, 29, 42
  addressing rules, 33–34
  network prefix notation, 36
  subnets and subnet masks, 35–39
Class B networks
  about, 29, 42
  addressing rules, 33–34
  network prefix notation, 36
  subnets and subnet masks, 35, 39–40
Class C networks
  about, 29–30, 42
  addressing rules, 33–34
  network prefix notation, 36
  subnets and subnet masks, 35, 40–41
Class D networks, 31
class IDs, 150
classful networks, 31, 33–36
classless inter-domain routing (CIDR), 32, 36
classless networks, 32
Clear-DnsClientCache cmdlet, 260
Clear-DnsServerCache cmdlet, 262
ClearType fonts, 10
Client Access License (CAL), 3
client classes
  about, 138, 148
  configuring clients to use classes, 149–150
configuring DHCP options, 138, 141–143
creating, 148–149
Client Site Cache, 409
Cloneable Domain Controllers group, 462, 465
cloning virtualized domain controllers, 461–466
cmdlets, defined, 2. See also specific cmdlets
CNAME (Canonical Name) records, 171, 180, 243
color profiles (printers), 663, 732–733
.com top-level domain name, 175
Common Internet File System (CIFS), 408
compacting WINS database, 290–291
computer accounts
about, 549
creating at command line, 551
creating in Active Directory, 549–551
delegated authentication and, 359–362
deleting, 553
disabling, 552–553
Group Policy settings, 567–568, 597–598, 600–601
joining to domains, 550–552, 554
managing, 553
managing Password Replication Policy, 502–512
moving, 552
resetting, 553–554
troubleshooting, 552, 554–555
computer-aided design (CAD), 661, 716
Computer Management
configuring managed service accounts, 561
configuring virtual accounts, 563
managing computer accounts, 553
Computer object, 328
computer startup and shutdown processes
repairing, 753–754
resolving, 798
scripts automating, 601–602
setting options, 754–756
troubleshooting, 795–798
ComputerName environment variable, 572
Computers container, 332
Computers object, 389
conditional forwarding, 186–187, 224–227
Configuration container, 317–318
ConfigurationTask, 93
Configure A DNS Server Wizard
about, 203
configuring large networks, 215–221
configuring small networks, 211–215
Configure Failover Wizard, 132–135
Configure Group Policy Slow Link Detection policy, 607–608, 685
Configure NAP Wizard, 158–159
Configure Standard TCP/IP Port Monitor dialog box, 682–683
Configuring Logon Computer computer option, 533
conflict detection (DHCP), 161–162
Connect-PSSession cmdlet, 109
Connection Settings dialog box, 304–305, 370–371
constrained delegation, 358
Contact object, 328
Contacts object, 389
container objects (containers), 311
contingency procedures, 748–749
Control Panel, 1. See also specific utilities
cross-forest trusts, 348–350, 382
 .csv file extension, 625
D
DACLs (discretionary access control lists), 544
daily backups, 761
data packets (IP), 19, 41–42
data prioritization settings, 10–11
Data Sources Policy Processing policy, 608
data table (Active Directory), 309
database layer (Active Directory), 301–302
datagrams, 19, 47
DCCloneConfig.xml file, 461
Dcdiag.exe (Domain Controller Diagnostic Utility), 370, 437–438
Dcpopfix utility, 621–622
Dcpromo log, 464–465
default application partitions, 251–254, 319
Default BOOTP Class, 141–142, 147–148
Default Domain Controllers Policy GPO, 566, 582–584, 621–622
Default Domain Policy, 391, 513–515, 520
Default Domain Policy GPO, 513–514, 566, 582–584, 621–622
Default-First-Site-Name site, 623
Default Network Access Protection Class, 141
Default Routing And Remote Access Class, 141–142
Default User Class, 141
DEFAULTIPSITELINK site link, 625
delegation
  authentication, 358–362
  managing Group Policy through, 584–601
  organizational units, 390–391, 475–479
  RODC, 501
  RODC administrative permissions, 511–512
Delegation Of Control Wizard, 476–479
delete excluderange command, 121
delete iprange command, 121
delete permission, 587
deleted accounts, recovering, 555–557
Deleted Objects container, 306–307, 556–557
deleting
  computer accounts, 553
  GPOs, 582
  groups, 548
  managed service accounts, 561–562
  organizational units, 472–473
  snapshot of domain controllers, 463
  user accounts, 538
denial of service (DoS) attacks, 91
Denied RODC Password Replication Group, 504–505
device unique identifier (DUID), 128–129
Devices Policy Processing policy, 608
devolution (DNS), 178–179
DFS (Distributed File System), 399, 404–409, 649–650
DFS-R (DFS Replication), 405, 461
DFS Replication (DFS-R), 405, 461
DFS Replication event log, 466
DHCID (Dynamic Host Configuration Identifier), 192
DHCP clients, 87, 94–98, 139–140
DHCP console, 107, 150
DHCP (Dynamic Host Configuration Protocol)
  about, 87–91, 137
  availability and fault tolerance, 98–103
  backup and recovery strategies, 759
  binding service to network interface, 155–156
  configuring DNS resolution, 67, 69–71
  configuring IP addressing, 59, 63, 65
  configuring TCP/IP options, 137–150
  diagnosing and resolving problems, 79
  domain considerations, 389
  dynamic IP addresses, 87, 433
  enabling conflict detection, 161–162
  integrating with DNS, 156–157, 188
  integrating with NAP, 157–161
  IPAM and, 92–94
  limited broadcasts, 32
  managing, 150–151
  managing and maintaining DHCP database, 163–165
  monitoring audit logging, 151–155
  NetBIOS scope, 274
  planning implementations, 94–103
  releasing and renewing settings, 81–82
  saving and restoring configuration, 162–163
  security considerations, 91–92
  setting up relay agents, 165–169
  setting up servers, 103–136
  troubleshooting printers, 743
DHCP Policy Configuration Wizard, 145–148
DHCP Post-Install Configuration Wizard, 105–106
DHCP servers
  activating scopes, 124–126
  authorizing in Active Directory, 109
  binding service to network interface, 155–156
  configuring TCP/IP options, 138
  copying configuration script to, 162
  creating and configuring scopes, 110–124
  creating and using failover scopes, 98–101, 110, 131–136
  enabling conflict detection, 161–162
  installing DHCP Server service, 104–109
  IP address lease, 59, 87–88
  moving DHCP databases to, 165
  policy-based assignments, 138–140
  recommendations, 88
  scope exclusions, 88, 123–124, 126–127
  scope reservations, 127–131
  security considerations, 91–92
  setting up, 103–104
  site considerations, 399
  starting and stopping, 150
DHCP User Classes dialog box, 148
DhcpClientIdentiﬁer registry key, 144
DHCP Server module (PowerShell), 108–109
DHCPv4
  autoconﬁguration, 89
  messages and relay agents, 94–96
  scope reservations, 129–130
  setting options for clients, 146–147
<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6, 89–90, 96–98</td>
<td></td>
</tr>
<tr>
<td>differential backups, 760–761</td>
<td></td>
</tr>
<tr>
<td>digital signatures (DNSSEC), 190, 234–238</td>
<td></td>
</tr>
<tr>
<td>directory partitions, 419–423, 487, 644</td>
<td></td>
</tr>
<tr>
<td>directory service component (Ntdsa.dll), 298–302</td>
<td></td>
</tr>
<tr>
<td>Directory Service event log, 464, 466</td>
<td></td>
</tr>
<tr>
<td>directory service polling interval, 262–263</td>
<td></td>
</tr>
<tr>
<td>Directory Services Recovery mode, 464</td>
<td></td>
</tr>
<tr>
<td>Directory Services Restore mode, 454</td>
<td></td>
</tr>
<tr>
<td>Directory System Agent (DSA), 301–302</td>
<td></td>
</tr>
<tr>
<td>directory trees, 312–313, 317</td>
<td></td>
</tr>
<tr>
<td>Disable-NetAdapter cmdlet, 21, 24, 75</td>
<td></td>
</tr>
<tr>
<td>disaster recovery</td>
<td>about, 762–766</td>
</tr>
<tr>
<td>backing up and restoring Active Directory, 787–795</td>
<td></td>
</tr>
<tr>
<td>configuring Active Directory for fast recovery with SANs, 438–439</td>
<td></td>
</tr>
<tr>
<td>creating problem-resolution policy documents, 750–752</td>
<td></td>
</tr>
<tr>
<td>developing backup strategies, 756–762</td>
<td></td>
</tr>
<tr>
<td>developing contingency procedures, 748–749</td>
<td></td>
</tr>
<tr>
<td>DHCP databases, 165</td>
<td></td>
</tr>
<tr>
<td>disaster-planning strategies, 747–752</td>
<td></td>
</tr>
<tr>
<td>disaster preparedness procedures, 752–756</td>
<td></td>
</tr>
<tr>
<td>GPOs, 617–621</td>
<td></td>
</tr>
<tr>
<td>implementing problem-escalation and response procedures, 749–750</td>
<td></td>
</tr>
<tr>
<td>installing Active Directory from, 457–461</td>
<td></td>
</tr>
<tr>
<td>media rotation and maintaining media sets, 761–762</td>
<td></td>
</tr>
<tr>
<td>one-time backups, 771–776</td>
<td></td>
</tr>
<tr>
<td>printer failures, 740</td>
<td></td>
</tr>
<tr>
<td>recovering data, 778–784</td>
<td></td>
</tr>
<tr>
<td>restoring operating system, 785–787</td>
<td></td>
</tr>
<tr>
<td>scheduling backups, 766–771</td>
<td></td>
</tr>
<tr>
<td>System State backup, 460, 784–785</td>
<td></td>
</tr>
<tr>
<td>tracking backups, 776–777</td>
<td></td>
</tr>
<tr>
<td>troubleshooting startup and shutdown, 795–798</td>
<td></td>
</tr>
<tr>
<td>WINS database, 291–292</td>
<td></td>
</tr>
<tr>
<td>Disconnect-PSSession cmdlet, 109</td>
<td></td>
</tr>
<tr>
<td>disconnecting sessions, 9, 16</td>
<td></td>
</tr>
<tr>
<td>Discover message (DHCP), 94–95, 98–99</td>
<td></td>
</tr>
<tr>
<td>DiscoveryTask, 93</td>
<td></td>
</tr>
<tr>
<td>discretionary access control lists (DACLs), 544</td>
<td></td>
</tr>
<tr>
<td>Disk Quota Policy Processing policy, 608</td>
<td></td>
</tr>
<tr>
<td>disk storage considerations, 436–437, 660–662</td>
<td></td>
</tr>
<tr>
<td>DiskRAID utility, 438–439</td>
<td></td>
</tr>
<tr>
<td>DISM command, 207, 667</td>
<td></td>
</tr>
<tr>
<td>Display Records dialog box, 288</td>
<td></td>
</tr>
<tr>
<td>display resolution, RDC client, 9</td>
<td></td>
</tr>
<tr>
<td>distinguished name (DN), 301, 316–318, 324</td>
<td></td>
</tr>
<tr>
<td>Distributed File System (DFS), 399, 404–409, 649–650</td>
<td></td>
</tr>
<tr>
<td>Distributed Scan Server, 666, 668</td>
<td></td>
</tr>
<tr>
<td>distribution groups, 544, 546</td>
<td></td>
</tr>
<tr>
<td>division OU design model, 392–393</td>
<td></td>
</tr>
<tr>
<td>DLL (dynamic-link library), 329, 406, 568</td>
<td></td>
</tr>
<tr>
<td>DN (distinguished name), 301, 316–318, 324</td>
<td></td>
</tr>
<tr>
<td>DNS Admins group, 445</td>
<td></td>
</tr>
<tr>
<td>DNS clients</td>
<td></td>
</tr>
<tr>
<td>checking resolver cache, 259–260</td>
<td></td>
</tr>
<tr>
<td>checking TCP/IP configuration, 257–259</td>
<td></td>
</tr>
<tr>
<td>diagnosing and fixing name-resolution issues, 83–85</td>
<td></td>
</tr>
<tr>
<td>integration with other technologies, 187–189</td>
<td></td>
</tr>
<tr>
<td>name resolution enhancements, 26–27</td>
<td></td>
</tr>
<tr>
<td>reregistering, 257</td>
<td></td>
</tr>
<tr>
<td>troubleshooting, 257–261</td>
<td></td>
</tr>
<tr>
<td>DNS (Domain Name System). See also name resolution; resource records (DNS); zones (DNS)</td>
<td></td>
</tr>
<tr>
<td>about, 48, 171–173</td>
<td></td>
</tr>
<tr>
<td>aging and scavenging rules, 254–256</td>
<td></td>
</tr>
<tr>
<td>application partitions, 319</td>
<td></td>
</tr>
<tr>
<td>architecting designs, 194–199</td>
<td></td>
</tr>
<tr>
<td>backup and recovery strategies, 759</td>
<td></td>
</tr>
<tr>
<td>checking DNS Server logs, 256–257</td>
<td></td>
</tr>
<tr>
<td>conditional forwarding, 186–187, 224–227</td>
<td></td>
</tr>
<tr>
<td>default partitions, 251–254</td>
<td></td>
</tr>
<tr>
<td>delegating authority, 227–229</td>
<td></td>
</tr>
<tr>
<td>DHCP integration, 156–157, 188</td>
<td></td>
</tr>
<tr>
<td>DNS devolution, 178–179</td>
<td></td>
</tr>
<tr>
<td>DNSSEC support, 189–190, 233–238</td>
<td></td>
</tr>
<tr>
<td>domain controller guidelines, 437</td>
<td></td>
</tr>
<tr>
<td>domain names, 48–49, 55, 174–175</td>
<td></td>
</tr>
<tr>
<td>dynamic updates, 88, 156, 190–192, 199, 201, 214–215, 223, 239</td>
<td></td>
</tr>
<tr>
<td>enabling WINS lookups, 292–293</td>
<td></td>
</tr>
<tr>
<td>global names, 248–249</td>
<td></td>
</tr>
<tr>
<td>host names, 48, 51, 78</td>
<td></td>
</tr>
<tr>
<td>installing DNS Server service, 201–221</td>
<td></td>
</tr>
<tr>
<td>LLMNR support, 51–52</td>
<td></td>
</tr>
<tr>
<td>logging, 256–257</td>
<td></td>
</tr>
<tr>
<td>planning implementations, 173–189</td>
<td></td>
</tr>
<tr>
<td>public and private namespaces, 174–175</td>
<td></td>
</tr>
<tr>
<td>replication considerations, 251–254, 411–412, 423</td>
<td></td>
</tr>
<tr>
<td>RODC considerations, 487</td>
<td></td>
</tr>
<tr>
<td>secondary notification, 232–233</td>
<td></td>
</tr>
<tr>
<td>security considerations, 189–194, 198–199</td>
<td></td>
</tr>
<tr>
<td>subdomains, 227–229</td>
<td></td>
</tr>
<tr>
<td>TCP/IP options, 140</td>
<td></td>
</tr>
</tbody>
</table>
testing network connections, 78
troubleshooting DNS clients, 257–261
troubleshooting DNS servers, 261–272
zone transfers, 182, 229–232, 457

**DNS Manager (Dnscmd tool)**
about, 208
adding resource records, 240–242
checking event logs, 257
checking for DNS updates, 451–452
checking replication to other name servers, 262
checking server cache, 261
configuring cache locking, 173
configuring large networks, 216
configuring small networks, 211
creating zone delegation, 457
DNS setup, 207–208
examining server configuration, 263–269
examining zones and zone records, 269–271
troubleshooting DNS server, 261–262

**DNS Security (DNSSEC) protocol**
about, 233–235
deploying, 233–238
digital signatures, 190, 234–238
security considerations, 189–190, 235–238

**DNS servers**
Active Directory support, 201–205, 222
aging and scavenging rules, 255–256
checking cache, 261–262
checking logs, 256–257
checking TCP/IP configuration, 261
configuring IP addresses, 63, 188
configuring resolution, 67–69
default application partitions, 251–254
delegating authority, 228–229
domain controllers as, 322, 442
examining configuration, 263–269
getting statistics, 271–272
installing, 455
installing TCP/IP networking, 56
normal scope setup options, 116
primary, 181, 205–206, 239, 437
RODC support, 483–484, 489
secondary, 181, 232–233, 437
security considerations, 189–190
site considerations, 399, 433
TCP/IP options, 140
troubleshooting, 261–272

**Dnscmd tool (DNS Manager)**
about, 208
adding resource records, 240–242
checking event logs, 257
checking for DNS updates, 451–452
checking replication to other name servers, 262
checking server cache, 261
configuring cache locking, 173
configuring large networks, 216
configuring small networks, 211
creating zone delegation, 457
DNS setup, 207–208
examining server configuration, 263–269
examining zones and zone records, 269–271
troubleshooting DNS server, 261–262

**DNSKEY (Domain Name System Key) records**, 234

**DNSSEC (DNS Security) protocol**
about, 233–235
deploying, 233–238
digital signatures, 190, 234–238
security considerations, 189–190, 235–238

**DnsServer module (PowerShell)**, 209

**DnsUpdateProxy group**, 92

**Do Not Apply During Periodic Background Processing policy setting**, 609

**documents**
overlays for, 717–718
problem-resolution policy, 750–752
viewing print jobs, 733–734
watermarks for, 717–718

**dollar sign ($)**, 561, 563, 731

**Domain Admins group**
about, 315
backing up GPOs, 618
changing Group Policies, 515
calendar accounts and, 550
domain user accounts and, 527
establishing trusts, 353
forestwide administration, 384, 443
managing groups, 545
restoring GPOs, 620
RODC considerations, 498, 502, 504–505
Users container and, 546

**Domain-Based Root Referral Cache**, 409

**Domain Controller Diagnostic Utility (Dcdiag.exe)**, 370, 437–438

**Domain Controller Referral Cache**, 409

**Domain Controllers container**, 471, 501

**Domain Controllers OU**
default GPO, 566, 582, 584
verifying installation, 452, 495–496
domain environment. See also replication; sites
about, 312–314, 321–322, 379
accessing in GPMC, 577–578
Active Directory group policies, 566–567
administrator support, 315
assigning user rights, 525–526
associating domain controllers with sites, 627–628
authentication in, 337–350, 358–362
bridgehead servers and, 644–645
changing designs, 387–389
creating domain controllers in domains, 442, 445–453
creating domain controllers in forests, 441
creating domains in forests, 453–457
data distribution, 319
developing plans, 384–389
directory partitions, 421
disaster recovery strategies, 787–788
DNS and, 204, 217
domain controllers as DNS servers, 322, 442
domain functional levels, 330–337
domain user accounts, 513–537
forcing removal of domain controllers, 468
forest functional levels, 330–337
global catalog servers and, 319, 325–330, 625
Group Policy considerations, 391, 590, 594–595
hardware and configuration considerations, 436–438
installing domain controllers, 201–202
joining computer accounts to, 550–552, 554
manipulating UPN suffixes, 338
moving domain controllers, 584, 628
namespaces, 317–318
operations master roles, 362–377
partitions, 317–319
read-only domain controllers, 322, 444–445, 481–512
reliable time sources, 373–374
restoring failed domain controllers, 793–795
searching the tree, 324–325
secure communications, 439
single versus multiple, 386–387
troubleshooting, 465
trust relationships, 315–316, 344–347, 350–357
universal groups and, 337–340
virtualized domain controllers, 461–466
zones and, 181, 184
domain functional levels
about, 330–332
choosing desired, 454
forest functional levels and, 454
listed, 331–332
raising or lowering, 331, 333–337
RODCs and, 488
domain local groups, 544
Domain Name Referral Cache, 409
Domain Name System (DNS). See also name resolution;
resource records (DNS); zones (DNS)
about, 48, 171–173
aging and scavenging rules, 254–256
application partitions, 319
architecting designs, 194–199
backup and recovery strategies, 759
checking DNS Server logs, 256–257
conditional forwarding, 186–187, 224–227
default partitions, 251–254
delegating authority, 227–229
DHCP integration, 156–157, 188
DNS devolution, 178–179
DNSSEC support, 189–190, 233–238
domain controller guidelines, 437
domain names, 48–49, 55, 174–175
dynamic updates, 88, 156, 190–192, 199, 201, 214–215, 223, 239
enabling WINS lookups, 292–293
global names, 248–249
host names, 48, 51, 78
installing DNS Server service, 201–221
LLMNR support, 51–52
logging, 256–257
planning implementations, 173–189
public and private namespaces, 174–175
replication considerations, 251–254, 411–412, 423
RODC considerations, 487
secondary notification, 232–233
security considerations, 189–194, 198–199
subdomains, 227–229
TCP/IP options, 140
testing network connections, 78
troubleshooting DNS clients, 257–261
troubleshooting DNS servers, 261–272
zone transfers, 182, 229–232, 457
Domain Name System Key (DNSKEY) records, 234
domain names (DNS)
about, 48–49
fully qualified domain name, 49, 85, 174
namespaces and, 174–175
specifying, 202
TCP/IP networking option, 55
domain naming master role, 362–363, 365, 367–368
domain networks, 20–21, 24
Domain object, 328
Domain registry key, 407
Domain Rename utility, 388
Domain Services (DS) records, 234
domain trees
about, 312–314, 379
creating domain controllers in, 442
creating in forests, 455–457
domain user accounts
applying secondary settings, 519–523
assigning capabilities, 524
assigning user rights, 524–527
built-in capabilities, 524
configuring account options, 531–534
configuring account policies, 513–519
configuring profile options, 534–536
creating and configuring, 527–531
creating Password Settings Objects, 519–523
disabling, 534
obtaining effective access, 530–531
reset disks, 542–543
setting permissions, 524
troubleshooting, 536–537
DomainDnsZones partition
about, 322, 421
removing DNS data in, 470
RODC support, 483
DoS (denial of service) attacks, 91
dot (period), 27, 35, 48
double-colon notation, 45–46
DRA performance counters, 649
Drive Maps Policy Processing policy, 608
DS (Domain Services) records, 234
DS performance counters, 649
DSA (Directory System Agent), 301–302
DSADD command, 546, 551
DSGET GROUP command, 546
DSHeuristics attribute, 304
Dsmgmt utility, 511
DSMOD command, 537, 547, 551
DSMOVE command, 551
DSQUERY command, 469, 537, 627
DSRM command, 551
Dssite.msc (Active Directory Sites And Services)
associating domain controllers with sites, 627–628
configuring advanced site-link options, 646
configuring bridgehead servers, 644–645
configuring site-link bridges, 638–639
creating site links, 631–633
creating sites, 624–625
creating subnets, 626–627
designating global catalog servers, 326–327
enabling universal group membership caching, 338–340
replication schedules for site links, 635–636
DUID (device unique identifier), 128–129
duplex printers, 662
Dynamic Host Configuration Identifier (DHCID), 192
Dynamic Host Configuration Protocol (DHCP)
about, 87–91, 137
availability and fault tolerance, 98–103
backup and recovery strategies, 759
binding service to network interface, 155–156
configuring DNS resolution, 67, 69–71
configuring IP addressing, 59, 63, 65
configuring TCP/IP options, 137–150
diagnosing and resolving problems, 79
domain considerations, 389
dynamic IP addresses, 87, 433
enabling conflict detection, 161–162
integrating with DNS, 156–157, 188
integrating with NAP, 157–161
IPAM and, 92–94
limited broadcasts, 32
managing, 150–151
managing and maintaining DHCP database, 163–165
monitoring audit logging, 151–155
NetBIOS scope, 274
planning implementations, 94–103
releasing and renewing settings, 81–82
saving and restoring configuration, 162–163
security considerations, 91–92
setting up relay agents, 165–169
setting up servers, 103–136
troubleshooting printers, 743
dynamic IP addresses
autoconfiguration, 90
configuring, 63–65
defined, 59
DHCP and, 87, 433
diagnosing and resolving problems, 79
RODC considerations, 500
dynamic-link library (DLL), 329, 406, 568
dynamic port mapping, 629
dynamic port ranges, 210
dynamic updates (DNS)
about, 199
Active Directory and, 201
configuring, 214–215, 223
DHCP and, 88
resource records and, 156, 190–192, 239

E
Edb.chk (checkpoint) file, 308
Edb.log (primary log) file, 308
Edit permission, 620
Edit Settings permission, 587
.edu top-level domain name, 175
Effective Access tool, 530–531
EFS (Encrypting File System), 442, 448, 467
EFS Recovery Policy Processing policy, 608
EFSInfo utility, 443
emergency response teams, 750
EMF data type
about, 654, 656
document processing, 659
troubleshooting printers, 744, 746
empty root, 387
Enable-ADAccount cmdlet, 529
Enable-NetAdapter cmdlet, 21, 24
Enable-WindowsOptionalFeature cmdlet, 667
EnableMulticast registry key, 52–53
Encrypting File System (EFS), 442, 448, 467
encryption
Active Directory installation and, 442–443
authentication and, 340–344
DHCP support, 91
DNSSEC digital signatures, 190, 235–238
password policies, 516, 520
RDP support, 10
RPC considerations, 630
Enforce Maximum Password Age policy setting, 523
Enforce Minimum Password Age policy setting, 523
Enforce Minimum Password Length policy setting, 522
Enforce Password History policy setting, 515, 520, 523
Enforce User Logon Restrictions policy setting, 517
Enterprise Admins group
about, 315
advanced site-link options, 645
backing up GPOs, 618
changing Group Policies, 515
computer accounts and, 550
Denied RODC Password Replication Group and, 504
domain user accounts and, 527
forestwide administration, 381, 384, 443
managing groups, 545
restoring GPOs, 620
Users container and, 546
Environment Policy Processing policy, 608
ESE (Extensible Storage Engine), 302–305, 310
event IDs
calendar accounts, 553, 555
DHCP servers, 91, 151–152
event logs
Backup utility, 776–777, 782–783
DHCP servers, 91
DNS servers, 257
FRS, 406
troubleshooting clone deployment, 464–466
Event Viewer, 695, 697
Everyone group, 702
Exchange Server, 328
exclusions (IP addresses)
defined, 88, 126
displaying, 126–127
setting ranges, 113, 123–124, 127
Exit-PSSession cmdlet, 109
Export-DhcpServer cmdlet, 163
Export-DhcpServer–File cmdlet, 163
Export-VM cmdlet, 463
Extensible Storage Engine (ESE), 302–305, 310
external trusts, 316

F
failover scope (IP addresses), 98–101, 110, 131–136
fault tolerance
data protection and, 437
developing contingency procedures, 748
DHCP failover scope, 98–101
DHCP split scope, 101–103
printer pooling, 724
federated forest design, 349
fields, defined, 309
file deltas, 405
File Explorer, 689
File Replication Service (FRS), 332, 404–407, 649–650
File Transfer Protocol (FTP), 180
filters and filtering
Group Policy support, 595–597
packet support, 81
printers, 698–699
WMI support, 615
Find dialog box, 550
Find Users, Contacts, And Groups dialog box, 548
firewalls
  blocked pings, 60–61
  configuring replication through, 629–630
diagnosing and resolving routing problems, 81
GPO considerations, 612, 617
Remote Desktop and, 5
shared printers and, 686
FireWire (IEEE 1394) interface, 662
font smoothing, 10
forest functional levels
  about, 330–333
domain functional levels and, 454
  listed, 333
  raising or lowering, 332–337
RODCs and, 488
Forest Root Domain container, 317–318
forest root domains
  about, 313–314, 317–318, 379–381
design configurations, 387
  PDC emulator role and, 333, 373
forest root zones, 204
forest trusts, 348
ForestDnsZones partition
  about, 322, 421
  removing DNS data in, 470
RODC support, 483
forests
  accessing in GPMC, 577–578
  Active Directory data distribution, 319
  administering, 383–384
  configuring point and print restrictions, 691
  creating domain controllers in, 441
  creating domains in, 453–457
defined, 313–314, 379
developing plans, 380–383
  geographically separated sites and, 383
global catalog servers, 326
  Group Policy inheritance, 594
  manipulating UPN suffixes, 338
  namespace considerations, 380–382
  operations master roles, 362–366
  single versus multiple, 382–383
  trust relationships, 345, 347–357, 381
  viewing, 624
Forgotten Password Wizard, 542
Form To Tray Assignment print option, 716
forward lookups
  creating zones, 203, 211–212, 215–216, 221–223
  resource records, 238–242
  WINS support, 50, 292
forwarders
  about, 186–187
  configuring, 214–215, 220, 224–227
FQDN (fully qualified domain name), 49, 85, 174
FRS (File Replication Service), 332, 404–407, 649–650
FSMO role, 362, 377
FTP (File Transfer Protocol), 180
fully qualified domain name (FQDN), 49, 85, 174
G
  garbage collection, 305–307
  garbageCollPeriod attribute, 306
gateways
  configuring multiple, 65–67
defined, 34
diagnosing and resolving problems, 79
  installing TCP/IP networking, 56
GDI (Graphics Device Interface), 656
global catalog servers, 326
group policies
  domain functional levels and, 454
  listed, 333
  raising or lowering, 332–337
RODCs and, 488
Get-Acl cmdlet, 713
Get-ADDCCloningExcludedApplicationList cmdlet, 462
Get-ADDomain cmdlet, 335, 364, 371, 374–375
Get-ADDomainController cmdlet, 627–628, 649
Get-ADForest cmdlet, 335, 364, 366–367
Get-ADReplicationFailure cmdlet, 648
Get-ADReplicationPartnerMetadata cmdlet, 648
Get-ADReplicationSite cmdlet, 641
Get-ADReplicationSiteLinkBridge cmdlet, 643
Get-ADReplicationSiteLinkBridgeIdentity cmdlet, 643
Get-ADReplicationUpToDatenessVectorTable cmdlet, 377
Get-ADServiceAccount cmdlet, 560
Get-Command –Module DnsServer cmdlet, 209
Get-Command –Module NetTCPIP cmdlet, 27
Get-Credential cmdlet, 560
Get-DhcpServerAuditLog cmdlet, 154
Get-DhcpServerDatabase cmdlet, 163–164
Get-DhcpServerv4ExclusionRange cmdlet, 124, 126
Get-DhcpServerv4Reservation cmdlet, 128
Get-DhcpServerv4Scope cmdlet, 122
Get-DhcpServerv4Scope cmdlet, 108
Get-DhcpServerv6ExclusionRange cmdlet, 124, 126
Get-DhcpServerv6Scope cmdlet, 123
Get-DnsClientCache cmdlet, 260
Get-DnsClientServerAddress cmdlet, 258–259
Get-DnsServer cmdlet, 269
Get-DnsServerCache cmdlet, 173, 262
Get-DnsServerDsSetting cmdlet, 262–263
Get-DnsServerSetting cmdlet, 242
Get-DnsServerStatistics cmdlet, 262, 269, 271–272
Get-DnsServerZone cmdlet, 261, 270
Get-DnsServerZoneAging cmdlet, 256, 262
Get-NetAdapter cmdlet, 24
Get-NetConnectionProfile cmdlet, 21
Get-Net IPAddress cmdlet, 27, 75
Get-NetIPv4Protocol cmdlet, 27
Get-NetIPv6Protocol cmdlet, 27
Get-NetNeighbor cmdlet, 27
Get-NetOffloadGlobalSetting cmdlet, 27
Get-NetRoute cmdlet, 27, 80
Get-NetTCPConnection cmdlet, 27
Get-NetTCPSetting cmdlet, 27
Get-Service cmdlet, 108
Get-VMSnapshot cmdlet, 463
Get-WMIObject Win32_PingStatus cmdlet, 60, 77

global catalog and global catalog servers
about, 319, 325–326
accessing, 325–326
designating, 326–328
directive, 423
directory partitions, 421
domain controllers and, 319, 325–330, 625
in forest plans, 381
operations master roles and, 365–366
removing, 469
replication and, 328–330, 411
RODC considerations, 487, 492
site considerations, 433
universal groups and, 545
global groups, 544
global unicast IPv6 addresses, 46–47
globally unique identifier (GUID)
Active Directory objects, 301
CNAME records and, 247
network adapters, 65
operations master roles, 367
PSO precedence and, 521
GlobalNames zone, 248–249

glue records, 186
.gov top-level domain name, 175
Gpedit.msc (Group Policy Object Editor)
configuring scripts, 602–603
configuring security settings, 574
editing GPOs, 580
Group Policy refresh, 607–609
modifying Group Policy settings, 7, 600
starting, 572

GPMC (Group Policy Management Console)
about, 571, 575–577
accessing forests, domains, sites, 577–578
assigning user rights, 525
backing up GPOs, 617
blocking inheritance, 594
changing link order and precedence, 591–592
configuring account policies, 514–515
configuring point and print restrictions, 690
configuring scripts, 602–603
creating and linking GPOs, 579–580
deleting GPOs, 582
deploying printer connections, 688
editing GPOs, 580
enforcing inheritance, 595
filtering Group Policy application, 596–597
Group Policy refresh, 607–612
linked GPOs, 580–581
managing Group Policy, 391
managing Group Policy through delegation, 584–589
modeling GPOs for planning purposes, 612–616
modifying Group Policy processing, 599–601
refreshing Group Policy manually, 617
restoring GPOs, 619
starter GPOs, 581
viewing applicable GPOs, 610–611

GPOs (Group Policy Objects)
about, 566–567
administrative templates, 569–570, 607
backing up, 617–619
backup and recovery strategies, 759
creating and linking in GPMC, 579–580
delegating privileges, 585–588
deleting in GPMC, 582
deploying printer connections, 687
depending, 571
depending in GPMC, 580
filtering Group Policy, 595–597
linked, 579–581, 588–589
managing creation rights, 584–585
modeling for planning purposes, 612–616
restoring, 619–621
script support, 601–603
security templates, 604–605
starter, 581
top-level account policy, 513, 572
viewing applicable, 610–612
viewing inherited, 591–592
Graphics Device Interface (GDI), 656
Group object, 328, 415
Group Policy
about, 565–566
Active Directory support, 296, 566–567
administrative templates, 569–570, 607
applying through security templates, 603–606
architectural overview, 568–569
assigning user rights, 525
backup and recovery strategies, 759
binary source files, 667
configuring point and print restrictions, 689–691
configuring Remote Desktop through, 7–8
creating domain user accounts, 528
default GPOs, 582–584
DNS devolution, 179
domains and, 391
filtering application of, 595–597
groups permitted to change, 515
implementing, 571–584
inheritance support, 589–595
Local Group Policy, 566–567, 571–575
maintaining, 606–622
management privileges, 585–588
managing LLMNR, 53
managing NRPT, 234
managing through delegation, 584–601
OU usage for, 391–392
overriding, 590
permitting and restricting remote logon, 6–7
Plug and Play device redirection, 12
processing overview, 597–601, 606–612
refreshing, 599, 606–612, 616–617
script usage in, 601–603
settings for, 567–568
troubleshooting, 606–622
Group Policy Creator Owners group, 515
Group Policy Management Console (GPMC)
about, 571, 575–577
accessing forests, domains, sites, 577–578
assigning user rights, 525
backing up GPOs, 617
blocking inheritance, 594
changing link order and precedence, 591–592
configuring account policies, 514–515
configuring point and print restrictions, 690
configuring scripts, 602–603
creating and linking GPOs, 579–580
deleting GPOs, 582
deploying printer connections, 688
editing GPOs, 580
enforcing inheritance, 595
filtering Group Policy application, 596–597
Group Policy refresh, 607–612
linked GPOs, 580–581
managing Group Policy, 391
managing Group Policy through delegation, 584–589
modeling GPOs for planning purposes, 612–616
modifying Group Policy processing, 599–601
refreshing Group Policy manually, 617
restoring GPOs, 619
starter GPOs, 581
viewing applicable GPOs, 610–611
Group Policy Management Editor, 568, 689
Group Policy Modeling Wizard, 612–615
Group Policy Object Editor (Gpedit.msc)
configuring scripts, 602–603
configuring security settings, 574
editing GPOs, 580
Group Policy refresh, 607–609
modifying Group Policy settings, 7, 600
starting, 572
Group Policy Objects (GPOs)
about, 566–567
administrative templates, 569–570, 607
backing up, 617–619
backup and recovery strategies, 759
creating and linking in GPMC, 579–580
deleating privileges, 585–588
deleting in GPMC, 582
deploying printer connections, 687
editing, 571
editing in GPMC, 580
filtering Group Policy, 595–597
linked, 579–581, 588–589
managing creation rights, 584–585
modeling for planning purposes, 612–616
restoring, 619–621
script support, 601–603
security templates, 604–605
starter, 581
top-level account policy, 513, 572
viewing applicable, 610–612
viewing inherited, 591–592
Group Policy Results Wizard, 610–611
Group Policy Starter GPO Editor, 571
groups
about, 543–545
adding members, 547
creating, 545–547
deleting, 548
distribution, 544, 546
domain local, 544
finding, 548
global, 544
host, 31
managing, 543–549
modifying, 548
printer permissions, 705
security, 544, 546, 668
universal, 337–340, 433, 544–545
Groups object, 389
GUID (globally unique identifier)
Active Directory objects, 301
CNAME records and, 247
network adapters, 65
operations master roles, 367
PSO precedence and, 521
H
H-Node (Hybrid Node), 275
Handle Count performance counter, 737
high availability
  developing contingency procedures, 748
  DHCP considerations, 98–103
  printer pooling, 724
Home Folder option, 535–536, 540
hop counts, DHCP messages, 97
Host Address (A) records
about, 179, 238–239
adding, 239–242
DNS delegation and, 456
dynamic updates and, 156, 190
forward lookup zones and, 203
root servers and, 194
stub zones and, 186
host groups, defined, 31
host IDs
  address classes and, 29, 33–34
  broadcast types and, 32
defined, 28
IPv6 addressing and, 47
network prefix notation, 36
subnets and subnet masks, 35–41
host names (DNS)
defined, 48
host-name resolution, 67–69
LLMNR support, 52
pinging, 78
troubleshooting. 465
HTTP (Hypertext Transfer Protocol), 741
hub-and-spoke design, 430–432
Hybrid Node (H-Node), 275
Hypertext Transfer Protocol (HTTP), 741
I
IAID (identity association identifier), 88
IANA (Internet Assigned Numbers Authority), 31, 42–43
ICANN (Internet Corporation for Assigned Names and Numbers)
about, 174
IANA and, 31, 42–43
top-level domains, 49, 174–175
ICM (Integrated Color Management), 663
identity association identifier (IAID), 88
IEEE 1394 (FireWire) interface, 662
IETF (Internet Engineering Task Force), 87
IGNORE_SCHEDULES flag, 640
IIS (Internet Information Services), 435, 559
Import-CSV cmdlet, 529, 625
Import-DhcpServer cmdlet, 163
Import Template dialog box, 605
Import-VM cmdlet, 463
incident response teams, 749–750
incremental backups, 760–761
incremental zone transfers, 230
indexed storage, 302–305
inetOrgPerson object, 328, 389–390
.inf file extension, 680
.info top-level domain name, 175
infrastructure master role, 362–363, 365, 375
inheritance (Group Policy)
about, 589–590
blocking, 593–594
changing link order and precedence, 591–592
enforcing, 594–595
overriding, 592–593
inkjet printers, 660–663
Install-ADDSDomain cmdlet, 441
Install-ADDSDomainController cmdlet, 441
Install-ADDSForest cmdlet, 440–441
Install-ADServiceAccount cmdlet, 560–562
Install From Disk dialog box, 675, 680
Install Profile dialog box, 732
Install-Windowsfeature ad-domain-services cmdlet, 440
Install-Windowsfeature gpmc cmdlet, 575
Installed Memory print option, 716
.int top-level domain name, 175
Integer Attribute Editor dialog box, 646, 651
Integrated Color Management (ICM), 663
Inter-Site Topology Generator (ISTG) about, 416
bridgehead servers and, 642–645
determining, 641–642
intersite replication and, 419
KCC and, 418
mapping network infrastructure, 424
monitoring for changes, 638
site links and, 629
Inter-Site Transports container, 635–636, 638–639
International Organization for Standardization (ISO), 174
Internet Assigned Numbers Authority (IANA), 31, 42–43
Internet Corporation for Assigned Names and Numbers (ICANN) about, 174
IANA and, 31, 42–43
top-level domains, 49, 174–175
Internet Engineering Task Force (IETF), 87
Internet Information Services (IIS), 435, 559
Internet Printing Protocol (IPP), 666
Internet Printing role service, 666
Internet Protocol (IP), 19. See also TCP/IP
Internet service providers (ISPs), 30, 42–43, 213
InterNIC, 42
intersite replication about, 398, 400–402
designing topology, 428–429
ISTG and, 419
managing, 628–630, 641–646
modifying for testing, 650–651
REPL interface and, 300
replication rings, 416–419
RPC over IP, 629
transport options, 640
intrasite replication about, 398, 400–402, 412–413
REPL interface and, 300
Invoke-Command cmdlet, 108
Invoke-GPUpdate cmdlet, 616–617
IP address leases assigning permanently, 88
defined, 59, 87
DHCP audit logging, 152–153
setting lease renewal time, 123
terminating, 124
IP Address Management (IPAM), 92–94
IP addresses. See also IPv4 addresses; IPv6 addresses; scopes (IP addresses)
associating domain controllers with sites, 627–628
associating subnets with sites, 626–627
configuring, 59, 188
configuring multiple, 65–67
diagnosing and resolving problems, 78–79
exclusions, 88, 123–124, 126–127
forward lookups, 50
installing TCP/IP networking, 56
name resolution and, 26–27, 47–53
reverse lookups, 50
running RDC client, 12
security considerations, 198
subnets and subnet masks, 34–42
testing, 60–62, 77–78
troubleshooting, 465
IP data packets, 19, 41–42
IP header, 19, 41–42, 47
IP (Internet Protocol), 19. See also TCP/IP
IP payload, 19, 41–42, 47
IP spoofing, 198
IPAM Administrators group, 92
IPAM ASM Administrators group, 92
IPAM (IP Address Management), 92–94
IPAM IP Audit Administrators group, 92
IPAM MSM Administrators group, 92
IPAM Users group, 92
IPCONFIG command checking DNS client, 258–260
configuring clients to use classes, 149–150
configuring DNS servers, 209
diagnosing name resolution issues, 83–85
diagnosing routing problems, 80
renewing and releasing settings, 82
reregistering clients, 257
scope reservations, 129–131
static IP addressing settings, 79
viewing configuration settings, 74–75
viewing user class memberships, 141–142
IPP (Internet Printing Protocol), 666
IPsec (IP security), 47, 81, 630
IPv4 addresses
about, 24, 27–28
activating scopes, 124–126
address classes, 28–30, 33–34
addressing plans, 44
broadcast, 31–32
checking DNS client configuration, 257–258
configuring, 59–60, 62–63
creating normal scopes, 111–117, 120–122
DHCP relay agents, 167–169
diagnosing and resolving problems, 78–79
DNS clients, 187–188
DNS resource records, 179
dynamic port ranges, 210
going and using, 42–44
limitations, 43–44
multicast, 31
scope exclusions, 88, 123–124, 126–127
scope reservations, 127–131
special addressing rules, 33–34
split scope, 103
subnets and subnet masks, 34–42
testing, 60–62
unicast, 28–30
IPv6 addresses
about, 24, 45–47
activating scopes, 124–126
broadcast addresses, 97
checking DNS client configuration, 258–259
configuring, 59–60, 62–63
creating normal scopes, 117–123
DHCP relay agents, 167–169
diagnosing and resolving problems, 79
DNS clients, 187–188
DNS resource records, 179
dynamic port ranges, 210
scope exclusions, 88, 123–124, 126–127
scope reservations, 129
subnets and subnet masks, 47
TCP/IP enhancements, 26
testing, 60–62
IPv6 Host Address (AAAA) records
about, 179, 239
adding, 239–242
DNS delegation and, 456
dynamic updates and, 191
ISO (International Organization for Standardization), 174
ISPs (Internet service providers), 30, 42–43, 213
ISTG (Inter-Site Topology Generator)
about, 416
bridgehead servers and, 642–645
determining, 641–642
intersite replication and, 419
KCC and, 418
mapping network infrastructure, 424
monitoring for changes, 638
site links and, 629
J
Job Errors performance counter, 738
Job Timeout print option, 716
Jobs performance counter, 738
Jobs Spooling performance counter, 738
jumbograms, 47
junction points (reparse points), 407
K
KCC (knowledge consistency checker)
about, 402–403
domain controller guidelines, 436
intrasite replication and, 412
ISTG support, 418
load balancing and, 404
mapping network infrastructure, 424
replication rings and, 412, 414, 419–422
KDC (Key Distribution Center)
about, 297
delegated authentication, 358
establishing initial authentication, 341–344
RODC support, 484
Kerberos authentication
about, 297–298, 340–341
accessing resources after authentication, 343–344
changing shared passwords, 413
establishing, 341–343
policy settings, 515, 517–518
replication process overview, 411–412
SPN support, 558–559
troubleshooting, 555
trust relationships and, 353
Kerberos Policy, 515, 517–518, 536, 582
Kerberos Ticket Granting accounts, 484–485, 504
Key Distribution Center (KDC)
about, 297
delegated authentication, 358
establishing initial authentication, 341–344
RODC support, 484
Key Master (DNSSEC), 190
KEY (public key) records, 190
key signing key (KSK), 235–237
knowledge consistency checker (KCC) about, 402–403
domain controller guidelines, 436
intrasite replication and, 412
ISTG support, 418
load balancing and, 404
mapping network infrastructure, 424
replication rings and, 412, 414, 419–422
KSK (key signing key), 235–237

LAN (local area network). See also sites
checking network connection status, 71–73
enabling and disabling connections, 75–76
network adapters connecting to, 62
relay agents and, 96
renaming connections, 75–76
viewing configuration information, 73–75
laser printers, 661–664
Last Known Good Configuration option, 796–797
LDAP (Lightweight Directory Access Protocol)
DFS support, 409
forest root domains, 317
FRS support, 405–406
Group Policy Management Console and, 575
managing directory information, 323–324
performing lookups, 439
port numbers, 300, 411
replication process overview, 410–411
resource records and, 180, 204
limited broadcasts, 32
Line Printer Daemon (LPD) service, 660, 666
Line Printer Remote (LPR) service, 660, 676, 682
link costs, 428–432, 631
Link GPOs permission, 588
Link-Local Multicast Name Resolution (LLMNR), 51–53, 188–189
link-local unicast IPv6 addresses, 46–47, 60, 90
link table (Active Directory), 309
linked GPOs, 579–581, 588–589
LIR (local Internet registry), 30
List Folder Contents permission, 703
LLMNR (Link-Local Multicast Name Resolution), 51–53, 188–189
LMHOSTS file, 51, 70–71
load balancing (load sharing)
bridgehead servers and, 403
DHCP failover scope, 98–100
DHCP split scope, 101–103
manually forcing, 404
local area network (LAN). See also sites
checking network connection status, 71–73
enabling and disabling connections, 75–76
network adapters connecting to, 62
relay agents and, 96
renaming connections, 75–76
viewing configuration information, 73–75
Local Group Policy, 566–567, 570–575, 589
Local Group Policy Editor, 574–575
Local Group Policy Object Editor, 571
Local Group Policy Objects (LGPOs), 514, 571–575
local Internet registry (LIR), 30
local links, 52
Local Security Authority (LSA), 296–299, 413
Local Security Policy console, 526–527, 574
Local Service account, 557
Local System account, 557
local user accounts, 514–516, 542–543
Locate File dialog box, 675
log files
Active Directory, 308, 310
Backup utility, 776–777, 782–783
checking for DNS servers, 256–257
DHCP audit logging, 151–155
FRS, 406
printer, 712–714
recording logon failure, 537
RODC support, 494
transaction, 303
troubleshooting clone deployment, 464–466

**Log On As A Service right**, 584
logging off
configuring scripts for, 602–603
sessions, 9, 16

**logon mechanisms**
Active Directory support, 298
configuring scripts, 602–603
last interactive logon information, 332
recording logon failure, 537
Logon Script Name option, 540
Logon Script option, 535

**loopback addresses**
IPv4, 30, 33
IPv6, 46
loopback processing, 600–601
LPD (Line Printer Daemon) service, 660, 666
LPR (Line Printer Remote) service, 660, 676, 682
LSA (Local Security Authority), 296–299, 413
LSA Server, 298

**M**

M-Node (Mixed Node), 275
MAC addresses, 88, 128–129, 465
Mail Exchanger (MX) records, 180, 243–244
Manage Backups dialog box, 619–620
Manage Documents permission, 702

**managed service accounts**
about, 557–559
configuring, 561
creating, 559–561
deleting, 561–562
moving, 562–563
virtual accounts and, 563

Managed Service Accounts container, 559
managed virtual accounts, 558
Manager This Printer permission, 702
MAPI (Messaging Application Programming Interface), 300–301
Max Jobs Spooling performance counter, 738
Max References performance counter, 738
Maximum Lifetime For Service Ticket policy setting, 517
Maximum Lifetime For User Ticket policy setting, 518
Maximum Lifetime For User Ticket Renewal policy setting, 518
Maximum Password Age policy setting, 515–516, 520
maximum replication latency, 419
Maximum Tolerance For Computer Clock Synchronization policy setting, 518
Maximum Tolerance For Computer Clock Synchronization setting, 536
Media Transfer Protocol (MTP), 11
memory
domain controller guidelines, 436
LDAP caches, 409
printers and, 659, 661, 716
property, 661
version stores, 303
messages
DHCPv4, 94–96
DHCPv6, 96–98
Microsoft Application Programming Interface (MAPI), 300–301
Microsoft Management Consoles (MMCs)
about, 2
ADSI Edit snap-in, 304–305, 370–371
Group Policy Management Editor, 568
Group Policy Object Editor, 572
Security Configuration And Analysis snap-in, 604–605
Security Templates snap-in, 604–605
Microsoft Options vendor class, 142
Microsoft Universal Printer Driver, 658
Microsoft VBScript, 601, 687
Microsoft Windows 2000 Options vendor class, 142
.mil top-level domain name, 175
Minimum Password Age policy setting, 516, 520
Minimum Password Length policy setting, 516, 520
Mixed Node (M-Node), 275
MMCs (Microsoft Management Consoles)
about, 2
ADSI Edit snap-in, 304–305, 370–371
Group Policy Management Editor, 568
Group Policy Object Editor, 572
Security Configuration And Analysis snap-in, 604–605
Security Templates snap-in, 604–605
.mobi top-level domain name, 175
Modify dialog box, 304–305, 371
Modify permission, 587
Modify Security permission, 587
monitor spanning, 10
monitoring
  DHCP audit logging, 151–155
  ISTG, 638
  print server performance, 735–739
  print services, 659
  printers and print queues automatically, 697–699
  replication, 648–650
monthly duty cycle (printers), 663–664
monthly print volume (printers), 663–664
Move-ADDirectoryServer cmdlet, 628
Move dialog box, 539, 552
Move Server dialog box, 628
ms-DeletedObjectLifetime attribute, 306
MSCONFIG command, 465
msDS-AuthenticatedToAccountList attribute, 503
msDS-ManagedServiceAccounts object class, 558
msDS-NeverRevealGroup attribute, 503
msDS-PasswordSettingsPrecedence attribute, 521
msDS-Reveal-OnDemandGroup attribute, 503
msDS-RevealedUsers attribute, 503
msDS-RIDPoolAllocationEnabled attribute, 370–371
MTP (Media Transfer Protocol), 11
multicast addresses
  IPv4, 31
  IPv6, 46
multicast scope (IP addresses), 110
multiprocessing guidelines, 436
.name top-level domain name, 175
Name Resolution Policy Table (NRPT), 234
Name Server (NS) records
  about, 180, 238–239
  adding, 245–246
  DNS delegation and, 456
  forward lookup zones and, 203
  RODC considerations, 483
  root servers and, 194
  stub zones and, 186
NAP (Network Access Protection)
  about, 157
  integrating with DHCP, 157–161
  NPS connection request policy, 166
  TCP/IP options, 141, 146–147
NAS (network-attached storage), 438
NET USE command, 686
NetBIOS (Network Basic Input/Output System)
  configuring logon computer, 533
  DNS considerations, 188–189
  node types, 275
  TCP/IP options, 141, 143
  WINS support, 50–51, 70–71, 273–275
NETDOM command, 358, 363–364, 377
NETLOGON service, 298, 553, 555
NETSH command
  DHCP console alternative, 107–108, 121–122
  DHCP settings, 109, 161–162
  DNS clients, 188, 257–259
  DNS servers, 209
  Dnscmd tool and, 208
  dynamic port ranges, 210
  IP addressing problems, 79–81
  name resolution issues, 83, 85
  normal scopes, 120–122
  scope activation, 124–125
  scope exclusions, 126–127
  scope reservations, 128, 130–131
NETUS command
WINS database, 288
WINS servers, 278–279, 286–288
NetTCPIP module (PowerShell), 27
Network Access: Allow Anonymous SID/Name Translation policy setting, 583
Network Access Protection (NAP)
about, 157
integrating with DHCP, 157–161
NPS connection request policy, 166
TCP/IP options, 141, 146–147
network adapters
configuring networking, 58
correcting network category, 20–21
GUID for, 65
installing, 56–57
LAN connections, 62
PowerShell support, 21, 24
Network Address Translation (NAT), 30, 175
Network And Sharing Center
about, 19, 23
changing adapter settings, 57–58, 62–63
characteristics, 64
network-attached storage (NAS), 438
Network Basic Input/Output System (NetBIOS)
configuring logon computer, 533
DNS considerations, 188–189
TCP/IP options, 141
WINS support, 50–51, 70–71
network broadcasts, 32
network discovery, 19–20, 22
Network Explorer, 19–22
network IDs
address classes and, 29–30, 33
broadcast types and, 32
defined, 28
IPv6 addressing and, 47
network prefix notation, 36
subnets and subnet masks, 35–36, 39–40
network interface card (NIC), 88
Network Location Awareness, 19–20
Network object
AddWindowsPrinterConnection method, 687
SetDefaultPrinter method, 687
Network Policy Server (NPS), 157, 159, 166
network prefix notation, 36
Network Printer Installation Wizard, 669–670, 673–682
network printers, 669–671
Network Security: Force Logoff When Logon Hours Expire policy setting, 583
Network Service account, 557
Network Solutions, 42
Network Time Protocol (NTP), 131, 373
networks and networking. See also specific types of networks
categories supported, 20–22
correcting network category, 20–21
classful, 31, 33–35
classless, 32
configuring, 58–71
configuring alternate IP addressing, 63–65
configuring DNS resolution, 67–69
configuring dynamic IP addresses, 63–65
configuring large networks, 215–221
configuring multiple IP addresses and gateways, 65–67
configuring networking, 58–71
configuring small networks, 211–215
configuring static IP addresses, 59–63
configuring WINS resolution, 69–71
connecting to Internet, 49
diagnosing and fixing name-resolution issues, 83–85
diagnosing and resolving connection problems, 76–77
diagnosing and resolving IP addressing problems, 78–79
diagnosing and resolving routing problems, 80–81
enabling and disabling connections, 75–76
installing, 55–58
installing network adapters, 56–57
installing networking, 55–58
installing networking services, 57–58
managing connections, 71–76
managing network connections, 71–76
mapping network infrastructure, 424–427
multiple subnets on same network, 113
nonclassful, 31–33, 35
performing basic network tests, 77–78
preparing for networking installation, 55–56
print services, 662–663
releasing and renewing DHCP settings, 81–82
renaming connections, 75–76
security considerations, 198–199
solving printer problems, 740
structuring, 43–44
subnets and subnet masks, 34–42
tool suite supporting, 19–24
troubleshooting and testing network settings, 76–85
troubleshooting and testing settings, 76–85
troubleshooting problems, 41
viewing configuration information, 73–75
WINS considerations, 275
New-ADComputer cmdlet, 359
New-ADDCClonetConfigFile cmdlet, 462
New-ADFineGrainedPasswordPolicy cmdlet, 520
New-ADReplicationSite cmdlet, 625
New-ADReplicationSiteLink cmdlet, 635
New-ADReplicationSiteLinkBridge cmdlet, 640
New-ADReplicationSubnet cmdlet, 627
New-ADServiceAccount cmdlet, 359, 560, 562
New-ADUser cmdlet, 359
New Class dialog box, 149
New Delegation Wizard, 228, 457
New GPO dialog box, 579–580
New Host dialog box, 239–240
New Interface For DHCP Relay Agent dialog box, 167, 169
New Name Server Record dialog box, 228–229, 245–246
New Object–Computer Wizard, 549–550
New Object–Group dialog box, 545
New Object–Organizational Unit dialog box, 472
New Object–Site dialog box, 624
New Object–Site Link Bridge dialog box, 639
New Object–Site Link dialog box, 631–632
New Object–Subnet dialog box, 626
New Object–User Wizard, 527–528
New-PSSession cmdlet, 108
New Replication Partner dialog box, 282
New Reservation dialog box, 129–130
New Resource Record dialog box, 240–241, 243–244
New Routing Protocol dialog box, 167–168
New Scope Wizard
creating normal scopes for IPv4 addresses, 111–117
creating normal scopes for IPv6 addresses, 117–120
creating superscope, 112
setting default gateways, 115
setting DNS servers, 116
setting duration of leases, 120
setting exclusion ranges, 113, 119
setting IP address range and subnet information, 112
setting lease duration, 114
setting network prefix and preference value, 118
setting scope name and description, 111
setting WINS servers, 116
New Starter GPO dialog box, 581
New Trust Wizard, 354–357
New Zone Wizard, 214–215, 217–224, 249
Next (NXT) records, 190
NextSECure (NSEC) records, 238
NIC (network interface card), 88
NIR (national Internet registry), 30
NLTEST command, 562
Non-Administrators Local Group Policy, 571
nonclassful networks, 31, 33, 35
normal backups, 760–761
normal queues, 721
normal scope (IP addresses)
creating for IPv4 addresses, 111–117
creating for IPv6 addresses, 117–120
creating with NETSH, 120–122
creating with New Scope Wizard, 111–120
defined, 110
Not Ready Errors performance counter, 738
notifications
printer settings, 712–714
problem-resolution policy documents, 750
secondary, 232–233
Notify dialog box, 232–233
NPS (Network Policy Server), 157, 159, 166
NRPT (Name Resolution Policy Table), 234
NS (Name Server) records
about, 180, 238–239
adding, 245–246
DNS delegation and, 456
forward lookup zones and, 203
RODC considerations, 483
root servers and, 194
stub zones and, 186
NSEC (NextSECure) records, 234, 238
NSEC3 standard, 235
NSLOOKUP command, 85, 260–261
NT File Replication Service (NTFRS), 444
NT LAN Manager (NTLM), 297–298, 340–341, 790
Ntdsa.dll (directory service component), 298
Ntds.dit (primary data) file, 308–310
NTDSUTIL utility
authoritative restores of Active Directory, 792
creating partition snapshots, 459
installing RODC from media, 496
restoring failed domain controllers, 794–795
seizing operations master roles, 377
transferring schema master role, 366
NTFRS (NT File Replication Service), 444
NTFS file system, 406, 409, 437
NTLM (NT LAN Manager), 297–298, 340–341, 790
NTP (Network Time Protocol), 131, 373
Number Of Failed Logon Attempts Allowed policy
setting, 523
NXT (Next) records, 190
octets, defined, 27
Offer message (DHCP), 94–95, 98–99
one-way trusts, 344–350
Open Database dialog box, 605
Operational log, 776, 782
operations master roles. See also PDC emulator role about, 362–363
changing, 365–366
determining current, 363–364
domain naming master role, 362–363, 365, 367–368
infrastructure master role, 362–363, 365, 375
recommended placement of, 365–366
relative ID master role, 362–363, 365, 368–372
schema master role, 362–363, 365–367, 482
seizing, 376–377
Operations Masters dialog box, 368, 371–372, 375
Options attribute, 640, 645–646, 650–651
.org top-level domain name, 175
organizational units (OUs)
assigning user rights, 525–526
creating, 471–473
creating designs, 392–396
creating for Remote Desktop Services, 8
creating groups, 545
creating/moving accounts/resources, 475
defined, 389, 471
delegating administration, 475–479
for delegation, 390–391
deleting, 472–473
developing plans, 389–396
Group Policy support, 390–392
setting properties, 474–475
OUs (organizational units)
assigning user rights, 525–526
creating, 471–473
creating designs, 392–396
creating for Remote Desktop Services, 8
creating groups, 545
creating/moving accounts/resources, 475
defined, 389, 471
delegating administration, 475–479
for delegation, 390–391
deleting, 472–473
developing plans, 389–396
Group Policy support, 390–392
setting properties, 474–475
Out Of Paper Errors performance counter, 739
overlays for documents, 717–718
P
P-Node (Peer-to-Peer Node), 275
packet filtering, 81
Page File Bytes performance counter, 737
pages printed per minute (printers), 663
paging operations, 660
parallel queries, 26
parent domains, 48
partitions
application, 251–254, 319, 421, 487
bridgehead servers and, 643–644
creating snapshots of, 459
directory, 419–423, 487, 644
domain environment, 317–319
in forest plans, 381
LDAP support, 410
removing data in, 470
replication rings and, 419–423
RODC considerations, 487
Partner Down state, 135
passive (standby) servers, 98–99
Password Does Not Expire policy setting, 520–521
Password Must Meet Complexity Requirements policy setting, 516, 520, 523
Password Never Expires policy setting, 528
Password Not Required policy setting, 520–521
Password Policy, 515–516, 559, 582
Password Replication Policy
about, 484–485
allowing or denying accounts, 505–507
configuring, 489, 493, 501, 503–505
managing, 502–512
Password Settings Container (PSC), 514
Password Settings Objects (PSOs), 514–515, 519–523
password settings policies, 519–523
passwords
changing shared, 413
command, 555
computer accounts, 553–554
creating user account password backup, 541–542
Directory Services Restore mode, 454
enforcing policies, 515–516, 519–523
operations master roles, 372–373
reset disks, 542–543
resetting, 391, 540–541
RODC considerations, 484, 503
trust, 356
PATHPING command, 80
pausing print jobs, 733
PCL print devices, 658–659
Pcl.sep separator page, 728

PDC emulator role
about, 362–363, 372–375
DFS metadata and, 407
GPO support, 571
password changes, 541
recommended placement, 365
replicating urgent changes, 413–414
RODC considerations, 485
security principals and, 333
troubleshooting, 465
verifying clones, 461

Peer-to-Peer Node (P-Node), 275

Perform Group Policy Modeling Analyses permission, 588

Performance Monitor
monitoring print server performance, 735–739
monitoring replication, 649–650

period (dot), 27, 35, 48

permissions and privileges
computer accounts, 554
DACL support, 544
delegating for Group Policy, 585–588
delegating for RSoP, 588–589
domain user accounts, 524–527, 538
managing for printers, 701–708, 713, 744
obtaining effective access, 530–531
RODCs, 511–512
SIDs and, 548

persistent caching, 26–27
persistent connections (WINS), 276
phone rosters, 750
photo printing, 662–663, 716

Picture Transfer Protocol (PTP), 11

PING command, 60–62, 77–78, 743–744

Plug and Play devices, 11–12

Point And Print Restrictions policy setting, 689–691
Point And Print Restrictions Properties dialog box, 690–691

Pointer (PTR) records
about, 172, 180, 238–239
adding, 239–242
dynamic updates and, 156, 190

Pool Nonpaged Bytes performance counter, 737
Pool Paged Bytes performance counter, 737
pooling, printer, 722–725

port numbers
global catalog servers, 325
LDAP, 300, 411
remote sessions, 5, 16
replication process overview, 411
RPC endpoint mapper, 629
security considerations, 199
SSL, 300, 411

PortNumber registry key, 5
post-action reporting, 751

PostScript page description language, 654, 658, 728, 731

power protection, 749

PowerShell (Windows). See also specific cmdlets
about, 2
activating scopes, 125–126
changing network categories, 21
configuring scripts, 602–603
creating domain user accounts, 529
creating normal scopes, 122–124
DHCP Server module, 108–109
DnsServer module, 209
getting IP configuration in, 75
manipulating network adapters, 21, 24
monitoring replication, 648–649
NetTcpIp module, 27
opening Group Policy Editor, 573
remote connections to virtual machines, 16
scope exclusions, 126–127
scope reservations, 128
troubleshooting replication, 648–649

primary DNS servers
about, 181, 205–206
creating and changing records on, 239
domain controller guidelines, 437

Print And Document Services role, 665–667, 692
Print Management console
about, 668
adding physically attached print devices, 672–673
auditing printer access, 706–707
changing TCP/IP port monitor settings, 682
configuring printer permissions, 703–705
deploying printer connections, 687–688
installing network printers automatically, 669
installing print servers, 665
managing print jobs, 733
managing print server properties, 708–709
managing printer properties, 714–733
managing printers, 692–694
migrating printers and print queues, 694–695
monitoring printers and print queues automatically, 697–699
viewing and configuring print drivers, 710
Print Operators group, 671, 676
Print Processor dialog box, 727
print services
automatic restart, 658
managing from command line, 668
managing print jobs, 733–735
managing printer permissions, 701–708
managing printers, 692–699
managing properties, 708–733
monitoring, 659
planning for deployment and consolidation, 659–665
printer maintenance, 735–739
process overview, 653–658
setting up print servers, 665–692
troubleshooting, 739–746
Print Spooler service
clearing out stuck documents, 734
configuring, 712–714, 725–726
permissions and, 703
print process and, 657–658
troubleshooting printers, 741, 744
Printbrm.exe tool, 668
Printer Migration Wizard, 694–697
printer pooling, 722–725
.printerExport file extension, 695, 740
printers and print servers
adding network-attached, 676–682
adding physically attached, 671–675
assigning ownership, 705–706
auditing access, 706–708
changing TCP/IP port monitor settings, 682–683
configuring color profiles, 633, 732–733
configuring logging settings, 712–714
configuring notification settings, 712–714
configuring point and print restrictions, 689–691
configuring print spooling, 712–714, 725–726
configuring publishing, 719–720
configuring separator pages, 725, 727–732
default data type, 726–727
deploying connections, 687–689
installing network printers automatically, 669–671
installing print servers, 665–668
managing permissions, 701–708, 713, 744
managing print jobs, 733–735
managing print server properties, 708–714
managing printer properties, 714–733
managing printers, 692–694
migrating printers and print queues, 694–697
monitoring performance, 735–739
monitoring printers and print queues automatically, 697–699
optimizing configuration, 659–664
optimizing printing through queues and pooling, 720–725
preparing for failure, 739–740
printer drivers, 656–658, 675, 690, 710–712, 718–719
printer status values, 698
resolving garbled or incorrect printing, 745–746
setting overlays and watermarks for documents, 717–718
shared printers, 683–689, 719–720
sizing hardware, 659–664
troubleshooting problems, 740–746
UNIX-based, 676
viewing and configuring printer ports, 709–710
viewing print processor, 726–727
Printers folder, 675
Printers object, 389
Printing Preferences dialog box, 716–717
PrintQueue object, 328
priority queues, 721
private IPv4 addresses
addressing rules, 33
defined, 30, 42
diagnosing and resolving problems, 78–79
IPv6 addresses and, 46
recommendations, 42
subnet masks, 35
private keys, 190, 235
private namespaces, 174–175
private networks
about, 20
changing categories, 21, 24
configuring IP addresses, 60
NAT support, 30
PrnCnfg script, 668
PrnDrv script, 668
PrnJobs script, 668
PrnMngr script, 668
PrnPort script, 668
PrntQctl script, 668
.pro top-level domain name, 175
problem-escalation and response procedures, 749–750
problem-resolution policy documents, 750–752
Process Even If The Group Policy Objects Have Not Changed policy setting, 609
processing (Group Policy)
modifying, 599–601
order of, 589–590
refreshing, 599, 606–612, 616–617
% Processor Time performance counter, 737
processors
for domain controllers, 436
for printers, 726
Profile Path option, 534–535
Properties dialog box
computer accounts, 360
DHCP relay agents, 167–169
Directory Service object, 304
DNS servers, 193, 215, 224–225, 234, 245–246
documents, 734–735
domain user accounts, 531–532, 534–535, 540
domains, 230–231, 351–354, 439
groups, 547
IPv4, 153, 155, 157, 160
IPv6, 153, 155
network connections, 57–58, 62–63
NTDS settings, 327–328, 338–339, 641–642, 651
organizational units, 472–475
print servers, 708–714
printer filters, 699
printer permissions, 703
printers, 672, 682, 705–707, 715–720, 724–733, 741
replication attributes, 330
replication partners, 280–281, 283–284
RODC, 506–507
site links, 632–633
subnets, 230–231
system, 4–6, 68, 754
TCP/IP, 278
transport protocol, 635–636, 638, 640
trusts, 352–353
user accounts, 359
user rights, 525–527
WINS, 284–285, 289–290
zone aging/scavenging, 255–256
Protected Users security group, 519
PROXIABLE flag, 358
PSC (Password Settings Container), 514
PScript5.dll, 658
PScript.sep separator page, 728
PSOs (Password Settings Objects), 514–515, 519–523
PTP (Picture Transfer Protocol), 11
PTR (Pointer) records
about, 172, 180, 238–239
adding, 239–242
dynamic updates and, 156, 190
public IPv4 addresses
configuring, 60
defined, 30, 42
IPv6 addresses and, 46
limitations, 43–44
subnet masks, 35
Public Key (KEY) records, 190
public keys, 190, 235
public namespaces, 174–175
public networks, 20–21, 24
Pubprn script, 668
pull replication partners, 280, 282–283, 412–413
push replication partners, 280, 282, 284, 412–413
queries
adaptive query timeout, 26
forwarding, 214–215, 220, 224–227
to global catalog servers, 325
LDAP support, 323–324
parallel, 26
query coalescing, 26
reliable time sources, 373–374
reusing, 549
reverse-lookup, 171–172
saving, 549
security considerations, 189–190, 198
query coalescing, 26
queues, printer, 720–725
QUSER command, 8
RAID (redundant array of independent disks), 437
Raise Domain Functional Level dialog box, 334–335
RAW data type
about, 654–656
document processing, 659
network-attached printers and, 676
as printer default, 727
selecting, 682
troubleshooting printers, 744, 746
RD CAL (Remote Desktop Client Access License), 3
RDC (Remote Desktop Connection), 2, 9–17
RDC (Remote Differential Compression), 405
RDN (relative distinguished name), 301, 316–317, 324
RDP (Remote Desktop Protocol), 5, 10
Read & Execute permission, 703
Read Group Policy Results Data permission, 588
read-only domain controllers (RODCs)
about, 322, 481–485
delegating administrative permissions, 511–512
design considerations, 485–488
installing, 490–496
installing from media, 496–498
managing credentials, 508–509
Password Replication Policy, 484–485, 489, 493, 501–512
preparing domains for, 444–445
preparing for installation, 488–490
staging, 498–502
testing applications prior to deployment, 483
Read permission
about, 587
creating backups, 618
filtering Group Policy application, 595–596
for printers, 702–703, 705
realm trusts, 353
reconnecting sessions, 10
recovery processes
about, 762–766
backing up and restoring Active Directory, 787–795
configuring Active Directory for fast recovery with SANs, 438–439
creating problem-resolution policy documents, 750–752
developing backup strategies, 756–762
developing contingency procedures, 748–749
DHCP databases, 165
disaster-planning strategies, 747–752
disaster preparedness procedures, 752–756
GPOs, 617–621
implementing problem-escalation and response procedures, 749–750
installing Active Directory from, 457–461
media rotation and maintaining media sets, 761–762
one-time backups, 771–776
printer failures, 740
recovering data, 778–784
restoring operating system, 785–787
scheduling backups, 766–771
System State backup, 460, 784–785
tracking backups, 776–777
troubleshooting startup and shutdown, 795–798
WINS database, 291–292
Recovery Wizard, 778–784
Recycle Bin (Active Directory)
domain functional level support, 332
enabling, 556
recovering deleted accounts, 555–557
recovering deleted objects, 305–307
redundant array of independent disks (RAID), 437
References performance counter, 738
regional Internet registry (RIR), 30, 43
registration release (WINS), 287
Registry Policy Processing policy, 608
Regsvr32 command, 329
relative distinguished name (RDN), 301, 316–317, 324
relative ID master role, 362–363, 365, 368–372
relative IDs (RIDs), 362–363, 365, 368–372
relay agents
configuring, 110
DHCPv4, 94–96
DHCPv6, 96–98
setting up, 165–169
remote access servers, 88–89
Remote Desktop
about, 2–3
configuring through Group Policy, 7–8
enabling on servers, 4–5
licensing, 3
permitting and restricting remote logon, 6–7
tracking logged on users, 8–9
Remote Desktop Client Access License (RD CAL), 3
Remote Desktop Connection client
about, 9–12
Advanced tab, 15
connecting to virtual machines in Windows Azure, 16–17
Display tab, 14
Experience tab, 15
General tab, 14
Local Resources tab, 14–15
Programs tab, 15
running, 12–16
Remote Desktop Connection (RDC), 2, 9–17
Remote Desktop mode, 2
Remote Desktop Protocol (RDP), 5, 10
Remote Desktop Server mode, 2
Remote Desktop Services, 2–3, 7–8
Remote Desktop Services Configuration, 7
Remote Desktop Services Configuration tool, 12
Z01682559.indd   826
3/25/2014   4:27:05 PM
Remote Desktop Services Manager, 8–9
Remote Desktop Users dialog box, 6
Remote Desktop Users group, 6–7, 524–525
Remote Differential Compression (RDC), 405
remote procedure calls (RPCs)
  about, 301
  domain naming master role and, 367
  dynamic port mapping, 629
  FRS support, 405–406
  printing process and, 657, 659
  REPL interface and, 300
  replication process overview, 411–413
  troubleshooting, 465
remote sessions
  admin mode, 3
  disconnecting, 9, 16
  logging off, 9, 16
  port numbers, 5, 16
  reconnecting, 10
  virtual session mode, 3
Remove-ADComputerServiceAccount cmdlet, 560
Remove-ADServiceAccount cmdlet, 560
Remove-DhcpServerv4ExclusionRange cmdlet, 124
Remove-DhcpServerv4Lease cmdlet, 125
Remove-DhcpServerv6ExclusionRange cmdlet, 124
Remove-DhcpServerv6Lease cmdlet, 125
Remove Roles and Features Wizard, 466
Rename User dialog box, 539–540
Rename-VM cmdlet, 463
renaming
  network connections, 76
  user accounts, 539–540
REPADMIN command
  determining bridgehead servers, 643
  determining ISTG for sites, 641
  key commands, 647–648
  load balancing manually, 404
  seizing operations master roles, 376
  showing replication status, 451
reparse points (junction points), 407
REPL interface, 300
replica root, 407
replication. See also intersite replication
  Active Directory support, 302, 322–323, 328–330
  architectural overview, 409–416
  designating attributes, 328–330
  designing topology, 428–429
  DNS support, 251–254, 262
domain design considerations, 385
domain functional levels, 332
forest functional levels, 333
intrasite, 300, 398, 400–402, 412–413
monitoring, 648–650
of priority/urgent changes, 413–414
site considerations, 398, 400–401, 629–630
tracking replication changes over time, 402–404
tracking system volume changes over time, 404–409
troubleshooting, 648–649
Replication Administrator, 646–648. See also REPADMIN command
replication interval, 631
replication partners
  application partitions, 421
  automatic, 280–282
  directory partitions, 421
  pull, 280, 282–283, 412–413
  push, 280, 282, 284, 412–413
  RODC considerations, 487
  WINS servers, 276, 279–284
replication schedules, 416, 631, 635–637
reporting, post-action, 751
Request message (DHCP), 94–95
reserved IP addresses, 33, 128–131, 138
Reset Account Lockout Counter After policy setting, 517, 520
Reset-ADServiceAccountPassword cmdlet, 562
reset disks, 542–543
Reset Failed Logon Attempts Count After policy setting, 523
Reset Password dialog box, 540–541
Reset Password Wizard, 543
Resource Record Signature (RRSIG) records, 234
resource records (DNS)
  about, 171–172, 179–180
  adding, 238–248
  DHCP considerations, 91, 156
  DNS delegation and, 456–457
  DNSSEC, 234–238
  dynamic updates and, 156, 190–192, 239
  name resolution and, 176–177
  RODC considerations, 483, 495
resource redirection, 11
response, NTLM authentication, 341
Restart-Service Spooler cmdlet, 734
Restore dialog box, 620–621
Restore To dialog box, 557
Resultant Set of Policy (RSoP)
- access considerations, 444
- delegating privileges for, 588–589
- Group Policy management privileges and, 586
- PSO considerations, 523
reverse lookups
- DNS support, 171–172
- resource records, 238–242
- WINS support, 50, 292
reverse mapping, 52
Reversible Password Encryption Required policy setting, 520–521
RFC 950, 32
RFC 1034, 171
RFC 1035, 171
RFC 1812, 32–33
RFC 2136, 190
RFC 4033, 233
RFC 4034, 233
RFC 4035, 233
RID pool, 368–370
RIDs (relative IDs), 362–363, 365, 368–372
rIDSetReference attribute, 369
ring topology model, 412–415
RIR (regional Internet registry), 30, 43
RODCs (read-only domain controllers)
- about, 322, 481–485
- delegating administrative permissions, 511–512
- design considerations, 485–488
- installing, 490–496
- installing from media, 496–498
- managing credentials, 508–509
- Password Replication Policy, 484–485, 489, 493, 501–512
- preparing domains for, 444–445
- preparing for installation, 488–490
- staging, 498–502
- testing applications prior to deployment, 483
root domains, defined, 379. See also forest root domains
root hints file, 192
root servers, 192–194
rootDSE, 317
Router Advertisement messages, 90, 96
Router Solicitation messages, 90
routers and routing
- configuring as relay agents, 110
- defined, 34
- diagnosing and resolving problems, 80–81
TCP/IP options, 140–141
WINS servers, 282
Routing and Remote Access Server Setup Wizard, 166
Routing and Remote Access Service (RRAS)
- configuring and enabling, 166
- configuring relay agents, 110, 166
- DHCP support, 88–89
- TCP/IP options, 141, 146–147
RPC endpoint mapper, 301, 412, 629
RPC over IP, 629–630
RPCs (remote procedure calls)
- about, 301
  - domain naming master role and, 367
  - dynamic port mapping, 629
  - FRS support, 405–406
  - printing process and, 657, 659
  - REPL interface and, 300
  - replication process overview, 411–413
  - troubleshooting, 465
RRAS (Routing and Remote Access Service)
- configuring and enabling, 166
- configuring relay agents, 110, 166
- DHCP support, 88–89
- TCP/IP options, 141, 146–147
RRSIG (Resource Record Signature) records, 234
RSoP (Resultant Set of Policy)
- access considerations, 444
  - delegating privileges for, 588–589
  - Group Policy management privileges and, 586
  - PSO considerations, 523
S
Safe Mode, 795–797
SAM performance counters, 649
SAM (Security Accounts Manager)
- authentication and access control, 298, 341
- creating local databases, 470–471
- legacy client support, 301
SANs (storage area networks), 438–439
Scan Management snap-in, 666–667
Scan Operators security group, 668
scavenging records, 254–256, 288–289
Schedule For dialog box, 633
Schedule For SiteLink dialog box, 637
scheduling, queue, 721–722
Schema Admins group
- changing schemas, 330
- Denied RODC Password Replication Group and, 504
  - designing replication attributes, 328–329
Security Accounts Manager (SAM)
authentication and access control, 298, 341
creating local databases, 470–471
legacy client support, 301
Security Configuration And Analysis snap-in, 604–605
security considerations. See also authentication; entries
beginning with Active Directory
Default Domain Policy GPO, 514
developing contingency procedures, 748
DHCP, 91–92
DNS, 189–195, 198–199
DNSSEC and, 189–190, 235–238
NTFS volumes, 437
printers, 705–707
zone transfers, 230
security descriptor table (Active Directory), 309
security descriptors, 530
security groups, 544, 546, 668
security identifiers (SIDs)
deleting computer accounts, 553
deleting domain user accounts, 538
deleting groups and, 548
DSA support, 302
Local Security Authority and, 297
Security Templates snap-in, 604–605
security tokens, 337–338
Select Computer dialog box, 610
Select GPO dialog box, 580–581
Select Groups dialog box, 462, 547
Select Items dialog box, 768
Select Items To Exclude dialog box, 767
Select Print Server dialog box, 693
Select The Printer Migration File To Use dialog box, 696
Select Users, Computers, Or Groups dialog box
adding members to groups, 547
assigning printer ownership, 705
assigning user rights, 525, 527
auditing printer access, 705
configuring printer permissions, 704
defining allowed accounts, 507
delegating administration, 476
Group Policy management privileges, 588
managing GPO creation rights, 585
Select Users Or Computers dialog box, 361, 509
Select Users Or Groups dialog box, 6, 523, 550
separate-name design, 194, 196–198
Separator Page dialog box, 729
separator pages (printing)
about, 727–729
customizing, 730–732
printer pooling and, 725
setting up, 729
testing, 729
sequential storage, 302
Server Authentication option, 5
Server Manager
about, 1–2
configuring managed service accounts, 561
configuring virtual accounts, 563
installing network printers, 669
installing printer servers, 665
installing Windows Server Backup, 763
Local Security Policy console, 574
starting and stopping DHCP servers, 150
Server Message Block (SMB)
Active Directory and, 439
CIFS support, 408
print servers and, 660
replication and, 412
Server object, 328
Server Operators group, 384, 505
Server Options dialog box, 144
ServerAvailabilityTask, 93
service accounts, 359–362, 557–563
Service Location (SRV) records
about, 180, 239
adding, 247–248
DNSSEC enhancements, 235
RODC considerations, 495
security considerations, 91
Service Principal Names (SPNs), 558–559
service set identifiers (SSIDs), 91
Services snap-in console, 561–563
sessions (remote)
admin mode, 3
disconnecting, 9, 16
logging off, 9, 16
port numbers, 5, 16
reconnecting, 10
virtual session mode, 3
Set-ADAccountControl cmdlet, 529
Set-ADAccountPassword cmdlet, 529
Set-ADComputer cmdlet, 359
Set-ADDomainMode cmdlet, 335–336
Set-ADForestMode cmdlet, 335–336
Set-ADServiceAccount cmdlet, 359, 560
Set-ADUser cmdlet, 529
Set-DhcpServerAuditLog cmdlet, 154–155
Set-DhcpServerDatabase cmdlet, 164
Set-DhcpServerSetting cmdlet, 162
Set-DhcpServerv4Binding cmdlet, 155
Set-DhcpServerv4Scope cmdlet, 122, 125
Set-DhcpServerv6Binding cmdlet, 156
Set-DhcpServerv6Scope cmdlet, 123, 125
Set-DnsClientServerAddress cmdlet, 188, 209–210
Set-DnsServerCache cmdlet, 173
Set-DnsServerDsSetting cmdlet, 262–263
Set-DnsServerGlobalNameZone cmdlet, 249
Set-DnsServerSetting cmdlet, 242, 262
Set Group Policy Refresh Interval For Domain Controllers policy, 606
Set-NetConnectionProfile cmdlet, 21
Setting Logon Hours computer option, 532
SHA encryption algorithm, 235, 238
Shared Folders object, 389
shared printers, 683–689, 719–720
shortcut trusts, 316, 346–347
show clients command, 122
Show Domains dialog box, 578
show excluderange command, 122
show iprange command, 122
show role administrators command, 511–512
Show Sites dialog box, 578
show state command, 122
Shutdown option, 9, 16
shutdown process, 601–602, 795–798
Shutdown utility, 9
sidCompatibilityVersion property, 370
SIDs (security identifiers)
deleting computer accounts, 553
deleting domain user accounts, 538
deleting groups and, 548
DSA support, 302
Local Security Authority and, 297
SIG (Signature) records, 190
Sign Out option, 9, 16
Signature (SIG) records, 190
Simple Mail Transfer Protocol over Internet Protocol (SMTP over IP), 300
Simple Mail Transfer Protocol (SMTP), 411–412, 629–630
Site Cost Cache, 409
site group policies, 589
site-link bridging, 430–432, 637–640
site links
configuring advanced options, 645–646
creating, 630–635
link costs, 428–432, 631
managing, 628–630
replication schedules, 416, 631, 635–637
selecting, 625
transitive nature of, 634–635
Site object, 328
sites
accessing in GPMC, 577–578
associating domain controllers with, 627–628
associating subnets with, 626–627
creating, 623–625
creating subnets, 626–627
deﬁned, 397
determining boundaries, 401
determining ISTG, 641–642
developing or revising designs, 424–433
managing, 623–628
managing intersite replication, 628–630, 641–646
managing site links, 628–640
monitoring replication, 646–651
namespaces and, 397
replication considerations, 398, 400–401
RODC considerations, 487–488
single versus multiple, 399–400
troubleshooting replication, 648–649
Sites container, 631, 635–636, 638–639
SMB (Server Message Block)
Active Directory and, 439
CIFS support, 408
print servers and, 660
replication and, 412
SMTP over IP (Simple Mail Transfer Protocol over Internet Protocol), 300
SMTP (Simple Mail Transfer Protocol), 411–412, 629–630
snapshots
creating of partitions, 459
deleting of domain controllers, 463
SOA (Start Of Authority) records
about, 180, 238
forward lookup zones and, 203
stub zones and, 186
Solicit message (DHCP), 97
SOM (Scope Of Management), 612
split-brain design, 194–196
split scopes, 101–103
SPNs (Service Principal Names), 558–559
SQL Server, 559
SRV (Service Location) records
about, 180, 239
adding, 247–248
DNSSEC enhancements, 235
RODC considerations, 495
security considerations, 91
SSIDs (service set identifiers), 91
SSL (Secure Sockets Layer)
authentication support, 297–298
port numbers, 300, 411
replication process overview, 411
standard zones, 181
standby (passive) servers, 98–99
Start-DnsServerScavenging cmdlet, 256
Start Of Authority (SOA) records
about, 180, 238
forward lookup zones and, 203
stub zones and, 186
Start-Service cmdlet, 155, 164
Start SystemStateBackup command, 460, 784
Start SystemStateRecovery command, 460, 784–785
Start-VM cmdlet, 464
starter GPOs, 581
starting print jobs, 733
Startup And Recovery dialog box, 754–755
Startup Or Logon Properties dialog box, 689
startup process
repairing, 753–754
resolving, 798
scripts automating, 601–602
setting options, 754–756
troubleshooting, 795–798
Startup Repair Wizard, 754
stateful mode (DHCP), 96
stateless mode (DHCP), 90, 97
static IP addresses
conﬁguring, 59–60, 62–63
deﬁned, 59, 128
diagnosing and resolving problems, 79
domain controller guidelines, 437
RODC considerations, 500
testing, 60–62
Status dialog box, 72–74
Stop-Service cmdlet, 155, 164
Stop-VM cmdlet, 463
storage area networks (SANs), 438–439
Store Password Using Reversible Encryption policy setting, 516, 520, 523

stub zones
about, 181, 186–187
Active Directory and, 205
creating, 217, 221
subdomains, 227–229, 457
subnet broadcasts, 32
Subnet object, 328
subnets and subnet masks. See also sites
associating subnets with sites, 626–627
creating subnets, 626–627
defined, 34–35
diagnosing and resolving problems, 79
installing TCP/IP networking, 56
IPv6 addressing and, 47
managing subnets, 623–628
mapping network infrastructure, 424–425
multiple subnets on same network, 113
network prefix notation, 36
superscope (IP addresses), 110, 112, 132
Support Policy Security Settings dialog box, 597
Sync-ADObject cmdlet, 377, 648–649
Sysprint.sep separator page, 728
Sysprtj.sep separator page, 728
System event log, 464, 466
system files, repairing, 797
System State backup, 460, 784–785
System utility (Control Panel), 2, 754
Sysvol (system volume)
Active Directory Group Policy, 566, 569
creating backup media for, 459
default file storage in, 437
default folder location, 449–450
in-progress replication reason codes, 576–577
replicating, 649
restoring data, 793
RODC support, 495, 497–498
tracking changes over time, 404–409

T
Target Site Cache, 409
Task Manager, 8–9
Task Manager dialog box, 8
TCP/IP Gateway Address dialog box, 66
TCP/IP networking
about, 19, 24–27
Active Directory support, 300
changing port monitor settings, 682–683
checking DNS client configuration, 257–259
checking DNS server configuration, 261
checking status for network connections, 71–73
configuration options and uses, 137–138
configuring alternate IP addressing, 63–65
configuring DNS resolution, 67–69
configuring dynamic IP addresses, 63–65
configuring multiple IP addresses and gateways, 65–67
configuring networking, 58–71
configuring static IP addresses, 59–63
configuring WINS resolution, 69–71
defining static IP addresses, 59–63
DHCP support, 87
diagnosing and fixing name-resolution issues, 83–85
diagnosing and resolving connection problems, 76–77
diagnosing and resolving IP addressing problems, 78–79
diagnosing and resolving routing problems, 80–81
directly-connected client options, 147–148
dynamic port ranges, 210
enabling and disabling connections, 75–76
installing network adapters, 56–57
installing networking, 55–58
installing networking services, 57–58
IPv4 addressing, 27–34, 42–44
IPv6 addressing, 26, 45–47
key enhancements, 25–26
managing network connections, 71–76
name resolution, 47–53
NAP-specific options, 146–147
NetBIOS support, 50–51, 70–71
performing basic network tests, 77–78
policy-based assignment, 138–140
preparing for networking installation, 55–56
releasing and renewing DHCP settings, 81–82
renaming connections, 75–76
RRAS-specific options, 146–147
setting options for all clients, 143–146
subnets and subnet masks, 34–42
testing network settings, 76–85
troubleshooting, 76–85, 552
user-specific options, 141–143
vendor-specific options, 141–143
viewing configuration information, 73–75
Windows-specific options, 140–141
WINS servers, 278
TCP (Transmission Control Protocol), 19. See also TCP/IP
Tcpip registry key, 144
TermDD registry subkey, 10–11
Test-Connection cmdlet, 60–61, 77

**testing**
- applying prior to RODC deployment, 483
- IP addresses, 60–62
- modifying intersite replication for, 650–651
- network settings, 76–85
- separator pages, 729

**Time to Live (TTL) value**
- DNS, 84, 172
- multicast scope, 110
- WINS, 276, 281–282

**tmp.edb (temporary data) file, 308**

**tombstoned records, 276–277, 288–289, 305–307**

**tombstoneLifetime attribute, 305, 307**

**top-level domains, 48–49, 174–175**

**Total Jobs Printed performance counter, 739**

**Total Pages Printed performance counter, 739**

**TRACERT command, 80**

**transactional processing, 303**

**Transmission Control Protocol (TCP), 19.** See also TCP/IP
- .travel top-level domain name, 175

**Tree View dialog box, 304, 371**

**troubleshooting**
- clone deployment, 464–466
- computer accounts, 552, 554–555
- DNS clients, 257–261
- DNS servers, 261–272
- domain user accounts, 536–537
- Group Policy, 606–622
- hardware devices, 57
- network problems, 41
- network settings, 76–85
- printer permissions, 703
- printers and print servers, 739–746
- replication, 648–649
- sites, 648–649
- startup and shutdown processes, 795–798
- trusts, 357–358

**trust path, 315**

**trust relationships**
- Active Directory, 51, 314–316
- domains and, 315–316, 344–347, 350–357
- forests and, 345, 347–357, 381
- verifying and troubleshooting, 357–358
- WINS, 51

**trust trees, 345**

**trusted domains, 315, 345**

**trusting domains, 315, 345**

**TTL (Time to Live) value**
- DNS, 84, 172
- multicast scope, 110
- WINS, 276, 281–282

**Turn Off Local Group Policy Objects Processing policy setting, 572–573**

**two-way transitive trusts, 345–350**

**UDP (User Datagram Protocol)**
- DHCP support, 97
- dynamic port ranges, 210
- LLMNR support, 52
- port numbers, 301, 412
- replication process overview, 411
- security considerations, 199

**UNC (Universal Naming Path)**
- backup media and, 458
- DHCP servers, 105
- referrals for namespaces, 409
- WINS servers, 279

**unicast IPv4 addresses, 28–30**

**unicast IPv6 addresses, 46–47, 60**

**Unidrv.dll, 658**

**Uninstall-ADServiceAccount cmdlet, 561–562**

**uninterruptible power supply (UPS), 749**

**universal groups**
- caching membership, 337–340, 433
- defined, 337, 544–545

**Universal Naming Path (UNC)**
- backup media and, 458
- DHCP servers, 105
- referrals for namespaces, 409
- WINS servers, 279

**Universal Principal Name (UPN), 337–338**

**universal serial bus (USB), 662**

**UNIX print servers, 676**

**unlocking domain user accounts, 541**

**unspecified IPv6 addresses, 46**

**up-to-dateness vector, 415**

**update sequence numbers (USNs)**
- tracking for domain controllers, 415
- tracking replication changes, 376
- tracking system volume changes over time, 406
- virtualized domain controllers and, 461

**UPN (Universal Principal Name), 337–338**

**UPS (uninterruptible power supply), 749**

**USB (universal serial bus), 662**
user accounts
  built-in, 557
  creating password backup, 541–542
delimited authentication and, 359
deleting, 538
disabling, 538
domain, 513–537
enabling, 538
Group Policy settings, 567–568, 597–598
maintaining, 537–543
moving, 539
renaming, 539–540
resetting domain passwords, 540–541
unlocking, 541
User Cannot Change Password policy setting, 528
User classes, 141–142, 149–150
User Datagram Protocol (UDP)
  DHCP support, 97
dynamic port ranges, 210
LLMNR support, 52
port numbers, 301, 412
replication process overview, 411
security considerations, 199
User Must Change Password At Next Logon policy setting, 528
User object, 328, 520–521
User Profile Path option, 540
userAccountControl attribute, 520–521
UserName environment variable, 536
Users container, 332, 545–546
Users object, 389
uSNChanged attribute, 415
USNs (update sequence numbers)
  tracking for domain controllers, 415
  tracking replication changes, 376
  tracking system volume changes over time, 406
  virtualized domain controllers and, 461
  VSS (Volume Shadow Copy Service), 407, 438, 752, 759

V
Validation Results dialog box, 466
vendor classes, 141–142
version stores, 303
VHDs (virtual hard disks)
  DHCP servers, 105
  DNS servers, 206
  merging AVHD files into, 462
  print servers, 665
  WINS servers, 277
views, defined, 1
virtual accounts, 558, 563
Virtual Bytes Peak performance counter, 737
Virtual Bytes performance counter, 737
virtual hard disks (VHDs)
  DHCP servers, 105
  DNS servers, 206
  merging AVHD files into, 462
  print servers, 665
  WINS servers, 277
virtual machines (VMs)
  connecting to in Windows Azure, 16–17
  performing backups, 752
  VM-Generation ID value, 461
virtual session mode, 3, 12–16
virtualized domain controllers, 461–466
VM-Generation ID, 461
VMs (virtual machines)
  connecting to in Windows Azure, 16–17
  performing backups, 752
  VM-Generation ID value, 461
W
W32TM command, 373
Wait Timeout print option, 716
WAN (wide area network), 183. See also sites
watermarks for documents, 717–718
WBADMIN command
  about, 762, 765
  backing up system state, 460
  recovering system state, 460, 784–785
Web Services on Devices (WSD), 666, 677
Where-Object cmdlet, 108
Wi-Fi Protected Access Version 2 (WPA2), 91
Wi-Fi Protected Access (WPA), 91
wide area network (WAN), 183. See also sites
Windows Azure, connecting to virtual machines, 16–17
Windows Boot Manager, 753–754
Windows Error Recovery mode, 797
Windows Firewall, 5, 60–61, 81
Windows Internet Naming Service (WINS)
  about, 50–51, 273
  active registrations, 288–289
  backup and recovery strategies, 759
  burst handling, 284–285
decommissioning, 274
diagnosing and resolving problems, 79
  enabling lookups through DNS, 292–293
  establishing trust relationships, 51
implementing, 276–277
installing TCP/IP networking, 56
maintaining database, 289–292
name registration and cache, 275–276
name resolution, 50–51, 287, 292
NetBIOS namespace and scope, 273–274
NetBIOS node types, 275
replication partners, 276, 279–284
scavenging records, 288–289
server status and configuration, 286–288
testing network connections, 78
Windows Management Instrumentation (WMI), 615
Windows Network Diagnostics, 19, 76–77
Windows operating systems
configuring point and print restrictions, 691
deploying printer connections, 687–689
DNS support, 83, 188
domain functional levels, 331–332
forest functional levels, 332–333
LLMNR support, 51–52
performing Active Directory installation from media, 457–461
printer considerations, 657, 718, 726
RODC support, 481–482
TCP/IP options, 140–141
Windows PowerShell. See also specific cmdlets
about, 2
activating scopes, 125–126
changing network categories, 21
configuring scripts, 602–603
creating domain user accounts, 529
creating normal scopes, 122–124
DHCPServer module, 108–109
DnsServer module, 209
getting IP configuration in, 75
manipulating network adapters, 21, 24
monitoring replication, 648–649
NetTCPIP module, 27
opening Group Policy Editor, 573
remote connections to virtual machines, 16
scope exclusions, 126–127
scope reservations, 128
troubleshooting replication, 648–649
Windows Process Activation Service, 666
Windows Remote Management (WinRM) service, 109
Windows Script Host (WSH), 601
Windows Security dialog box, 17

Windows Server. See also Backup utility (Windows Server)
Active Directory support, 296, 299
changing network categories, 24
detecting print devices, 672–673
DNS resource records, 179–180
establishing trust relationships, 51
installing network adapters, 57
print process and, 657–658
WSH support, 601
Windows Update, 675
Winprint processor, 726
WinRM (Windows Remote Management) service, 109
WINS database
backing up, 291
backup and recovery strategies, 759
compacting, 290–291
examining records, 288–289
restoring, 292
verifying consistency, 289–290
WINS servers
checking status and configuration, 286–288
configuring resolution, 69–71
installing TCP/IP networking, 56
normal scope setup options, 116
replication partners, 276, 279–284
setting up, 277–279
TCP/IP options, 141
WINS (Windows Internet Naming Service)
about, 50–51, 273
active registrations, 288–289
backup and recovery strategies, 759
burst handling, 284–285
decommissioning, 274
diagnosing and resolving problems, 79
enabling lookups through DNS, 292–293
establishing trust relationships, 51
implementing, 276–277
installing TCP/IP networking, 56
maintaining database, 289–292
name registration and cache, 275–276
name resolution, 50–51, 287, 292
NetBIOS namespace and scope, 273–274
NetBIOS node types, 275
replication partners, 276, 279–284
scavenging records, 288–289
server status and configuration, 286–288
testing network connections, 78
wireless WAN (WWAN), 607–608
WMI (Windows Management Instrumentation), 615
Working Set Peak performance counter, 737
Working Set performance counter, 737
WPA (Wi-Fi Protected Access), 91
WPA2 (Wi-Fi Protected Access Version 2), 91
Write permission, 618
WSD (Web Services on Devices), 666, 677
WSH (Windows Script Host), 601
WWAN (wireless WAN), 607–608

X
x64 user-mode drivers, 718
x86 user-mode drivers, 718

Z
zone delegation, 457
zone signing key (ZSK), 235–237
Zone Signing Wizard, 236–238
zone transfers (DNS)
configuring, 229–232
defined, 182
enabling name resolution, 457
incremental, 230
security considerations, 230
zones (DNS)
about, 180–181, 186
Active Directory-integrated, 181, 183–185, 201, 212,
217–219, 222–223
aging and scavenging rules, 255–256
configuring, 221–224
configuring for large networks, 215–221
configuring for small networks, 211–215
creating subdomains, 227–229
default application partitions, 251–254, 319
derefined, 176
delegating authority, 227–229
examining, 269–271
forward lookup, 203, 211–212, 215–216, 221–223
GlobalNames zone, 248–249
secondary, 186–187, 204–205, 217, 221, 457
security considerations, 199, 235–238
standard, 181–183
ZSK (zone signing key), 235–237