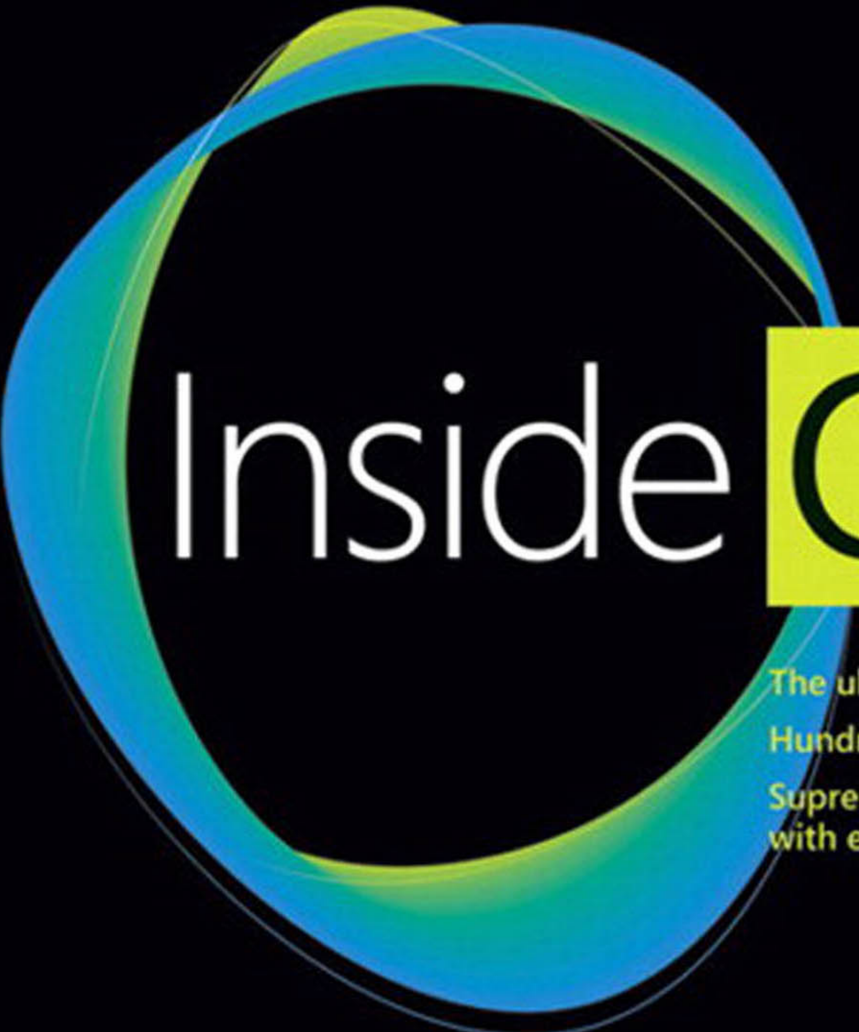
Microsoft



Inside OUT

The ultimate, in-depth reference

Hundreds of timesaving solutions

Supremely organized, packed with expert advice

Windows Server® 2012

William R. Stanek *Windows technologies expert + award-winning author*

Microsoft

Microsoft® Windows Server 2012 Inside Out

William R. Stanek

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

Copyright © 2013 by William R. Stanek

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

Library of Congress Control Number: 2012955900
ISBN: 978-0-7356-6631-3

Printed and bound in the United States of America.

Third Printing

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at http://www.microsoft.com/learning/booksurvey.

Microsoft and the trademarks listed at http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

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

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

Acquisitions Editor: Anne Hamilton
Developmental Editor: Karen Szall
Project Editor: Karen Szall
Editorial Production: Waypoint Press
Technical Reviewer: Mitch Tulloch; Technical Review services provided by Content Master,
a member of CM Group, Ltd.
Copyeditor: Roger LeBlanc
Indexer: Christina Yeager
Cover: Microsoft Press Brand Team

[2013-09-27]

*To my readers—*Windows Server 2012 Inside Out *is my 40th book for Microsoft Press. Thank you for being there with me through many books and many years.*

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.

—William R. Stanek

This page intentionally left blank

Contents at a Glance

Part 1: Windows Server 2012 Overview

Chapter 1
Introducing Windows Server 2012 3

Chapter 2
Deploying Windows Server 2012 61

Chapter 3
Boot configuration 101

Part 2: Managing Windows Server 2012 Systems

Chapter 4
Managing Windows Server 2012 137

Chapter 5
Windows Server 2012 MMC administration 191

Chapter 6
Configuring roles, role services, and features 229

Chapter 7
Managing and troubleshooting hardware 263

Chapter 8
Managing the registry 303

Chapter 9
Software and User Account Control administration 349

Chapter 10
Performance monitoring and tuning 369

Chapter 11
Comprehensive performance analysis and logging. 425

Part 3 Managing Windows Server 2012 Storage and File Systems

Chapter 12
Storage management 479

Chapter 13
TPM and BitLocker Drive Encryption 569

Chapter 14
Managing file systems and storage 621

Chapter 15
File sharing and security. 715

Chapter 16
Managing file screening and storage reporting 797

Chapter 17
Backup and recovery. 821

Part 4: Managing Windows Server 2012 Networking and Domain Services

Chapter 18
Networking with TCP/IP 875

Chapter 19
Managing TCP/IP networking 909

Chapter 20
Managing DHCP. 941

Chapter 21
Architecting DNS infrastructure 1017

Chapter 22
Implementing and managing DNS. 1047

Chapter 23
Implementing and maintaining WINS 1113

Part 5: Managing Active Directory and Security

Chapter 24
Active Directory architecture. 1135

Chapter 25
Designing and managing the domain environment 1161

Chapter 26
Organizing Active Directory 1215

Chapter 27
Configuring Active Directory sites and replication 1233

Chapter 28
Implementing Active Directory Domain Services. 1271

Chapter 29
Deploying read-only domain controllers . . 1315

Chapter 30
Managing users, groups, and computers . . 1345

Chapter 31
Managing Group Policy 1387

Chapter 32
Active Directory site administration. 1443

Table of Contents

Introduction xxvii

Conventions xxviii
How to reach the author xxix
Errata & book support xxix
We want to hear from you xxix
Stay in touch xxix

Part 1: Windows Server 2012 Overview

Chapter 1: **Introducing Windows Server 2012 . . . . 3**

Getting to know Windows Server 2012 4
Windows 8 and Windows Server 2012 8
Planning for Windows Server 2012 10
    Your plan: The big picture 10
    Identifying your organizational teams 12
    Assessing project goals 14
    Analyzing the existing network 18
    Defining objectives and scope 26
    Defining the new network environment. 31
    Final considerations for planning and deployment 35
Thinking about server roles and Active Directory 36
    Planning for server usage 37
    Designing the Active Directory namespace 40
    Managing domain trusts 41
    Identifying the domain and forest functional level 41
    Defining Active Directory server roles 43

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

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

microsoft.com/learning/booksurvey

Planning for availability, scalability, and manageability 45
Planning for software needs 45
Planning for hardware needs 47

Chapter 2: **Deploying Windows Server 2012 . . . . . 61**

Getting a quick start 61
Product licensing 63
Preparing for a Windows Server 2012 installation 64
Understanding installation options 64
Determining which installation type to use 66
Using Windows Update 67
Preinstallation tasks 69
Installing Windows Server 2012 70
Installation on BIOS-based systems 71
Installation on EFI-based systems 72
Planning partitions 72
Naming computers 74
Network and domain membership options 75
Performing a clean installation 77
Performing an upgrade installation 82
Activation sequence 82
Performing additional administration tasks during installations 85
Accessing a command prompt during installation 85
Forcing disk-partition removal during installation 89
Loading mass storage drivers during installation 89
Creating, deleting, and extending disk partitions during installation 90
Troubleshooting installation 91
Start with the potential points of failure 92
Continue past lockups and freezes 93
Postinstallation tasks 96

Chapter 3: **Boot configuration 101**

Boot from hardware and firmware 101
Hardware and firmware power states 102
Diagnosing hardware and firmware startup problems 103
Resolving hardware and firmware startup problems 107
Boot environment essentials 109
Managing startup and boot configuration 111
Managing startup and recovery options 111
Managing System Boot Configuration 113
Working with BCD Editor 117

Managing the Boot Configuration Data store and its entries 119
Viewing BCD entries 119
Creating and identifying the BCD data store 122
Importing and exporting the BCD data store 123
Creating, copying, and deleting BCD entries 123
Setting BCD entry values 125
Changing Data Execution Prevention and physical address extension options 131
Changing the operating system display order 132
Changing the default operating system entry 133
Changing the default timeout 133
Changing the boot sequence temporarily 134

Part 2: Managing Windows Server 2012 Systems

Chapter 4: **Managing Windows Server 2012 . . . . 137**
Working with the administration tools 137
Using Control Panel utilities 140
Using graphical administrative tools 141
Using command-line utilities 145
Working with Server Manager 150
Getting to know Server Manager 150
Adding servers for management 155
Creating server groups 156
Enabling remote management 157
Working with Computer Management 160
Computer Management system tools 160
Computer Management storage tools 161
Computer Management Services And Applications tools 162
Using Control Panel 162
Using the Folder Options utility 163
Using the System console 165
Customizing the desktop and the taskbar 168
Configuring desktop items 168
Configuring the taskbar 169
Optimizing toolbars 175
Displaying custom toolbars 175
Creating personal toolbars 176
Using Remote Desktop 176
Remote Desktop essentials 176
Configuring Remote Desktop 178
Supporting Remote Desktop Connection clients 182
Tracking who’s logged on 189

Chapter 5: **Windows Server 2012 MMC administration 191**
Using the MMC 191
MMC snap-ins 192
MMC modes. 194
MMC window and startup. 196
MMC tool availability 198
MMC and remote computers 201
Building custom MMCs. 203
Step 1: Creating the console 203
Step 2: Adding snap-ins to the console 205
Step 3: Saving the finished console 210
Designing custom taskpads for the MMC. 215
Getting started with taskpads 215
Understanding taskpad view styles 216
Creating and managing taskpads 218
Creating and managing tasks 221
Publishing and distributing your custom tools. 227

Chapter 6: **Configuring roles, role services, and features 229**
Using roles, role services, and features 230
Making supplemental components available. 236
Installing components with Server Manager 237
Viewing configured roles and role services 237
Managing server roles and features 238
Managing server binaries 245
Installing components at the prompt 250
Going to the prompt for Server Management 250
Understanding component names 251
Tracking installed roles, role services, and features. 256
Installing components at the prompt 257
Removing components at the prompt 260

Chapter 7: **Managing and troubleshooting hardware 263**
Understanding hardware installation changes. 263
Choosing internal devices 263
Choosing external devices. 266
Installing devices 269
Understanding device installation 269
Installing new devices 273
Viewing device and driver details 277
Working with device drivers 280
Device driver essentials 280
Understanding and troubleshooting driver signing 281

Viewing driver Information 281
Viewing Advanced, Resources, and other settings 284
Installing and updating device drivers 286
Restricting device installation using Group Policy 289
Rolling back drivers. 290
Removing device drivers for removed devices 291
Uninstalling, reinstalling, and disabling device drivers 292
Managing hardware 292
Adding non–Plug and Play, legacy hardware 293
Enabling and disabling hardware. 294
Troubleshooting hardware 295
Resolving resource conflicts 298

Chapter 8: **Managing the registry. 303**

Introducing the registry 304
Understanding the registry structure. 306
Registry root keys 311
HKEY_LOCAL_MACHINE 312
HKEY_USERS. 318
HKEY_CLASSES_ROOT 319
HKEY_CURRENT_CONFIG. 319
HKEY_CURRENT_USER 320
Registry data: How it is stored and used 320
Where registry data comes from 320
Types of registry data available 322
Registry administration. 324
Searching the registry 324
Modifying the registry. 325
Modifying the registry of a remote machine. 328
Importing and exporting registry data 329
Loading and unloading hive files. 332
Working with the registry from the command line 333
Backing up and restoring the registry 334
Maintaining the registry. 335
Using the Microsoft Fix It Utility. 336
Removing registry settings for active installations that have failed 337
Removing partial or damaged settings for individual applications. 338
Securing the registry. 338
Preventing access to the registry utilities 338
Applying permissions to registry keys. 340
Controlling remote registry access 343
Auditing registry access. 345

Chapter 9: **Software and User Account Control administration. 349**
Software installation essentials 349
Mastering User Account Control. 353
Elevation, prompts, and the secure desktop 353
Configuring UAC and Admin Approval Mode 356
Maintaining application integrity 359
Application access tokens 359
Application run levels. 362
Configuring run levels 364
Controlling application installation and run behavior 366

Chapter 10: **Performance monitoring and tuning 369**
Tuning performance, memory usage, and data throughput. 369
Tuning Windows operating system performance. 369
Tuning processor scheduling 370
Tuning virtual memory. 371
Other important tuning, memory, and data considerations 375
Tracking a system's general health 377
Monitoring essentials. 378
Getting processor and memory usage for troubleshooting 381
Getting information on running applications 388
Monitoring and troubleshooting processes. 391
Monitoring and troubleshooting services 397
Getting network usage information 400
Getting information on user and remote user sessions. 402
Tracking events and troubleshooting by using Event Viewer 405
Understanding the event logs 405
Accessing the event logs and viewing events 408
Viewing event logs on remote systems. 413
Sorting, finding, and filtering events. 414
Archiving event logs. 418
Tracking events using Windows PowerShell. 419
Using subscriptions and forwarded events 422

Chapter 11: **Comprehensive performance analysis and logging 425**
Establishing performance baselines 426
Tracking per-process resource usage 427
Tracking the overall reliability of the server. 436
Comprehensive performance monitoring. 439
Using Performance Monitor 439
Selecting performance objects and counters to monitor 441
Choosing views and controlling the display. 443
Monitoring performance remotely 446

Resolving performance bottlenecks. 448
Resolving memory bottlenecks 448
Resolving processor bottlenecks 451
Resolving disk I/O bottlenecks 452
Resolving network bottlenecks 454
Performance logging 457
Viewing data collector reports 467
Configuring performance counter alerts 470
Monitoring performance from the command line 471
Analyzing trace logs at the command line. 475

Part 3 Managing Windows Server 2012 Storage and File Systems

Chapter 12: **Storage management 479**
Essential storage technologies 479
Using internal and external storage devices 480
Storage-management features and tools. 483
Storage-management role services. 487
Booting from SANs, and using SANs with clusters 492
Working with SMB 3.0 493
Installing and configuring file services. 496
Configuring the File And Storage Services role. 497
Configuring multipath I/O. 500
Meeting performance, capacity, and availability requirements. 505
Configuring Hyper-V 507
Configuring storage 514
Using the Disk Management tools. 514
Adding new disks 519
Using the MBR and GPT partition styles. 521
Using the disk storage types. 525
Creating and managing virtual hard disks for Hyper-V. 529
Converting FAT or FAT32 to NTFS 531
Working with removable disks 533
Managing MBR disk partitions on basic disks 533
Creating partitions and simple volumes 534
Formatting a partition, logical drive, or volume 538
Configuring drive letters 539
Configuring mount points. 541
Extending partitions. 543
Shrinking partitions 546
Deleting a partition, logical drive, or volume 549

Managing GPT disk partitions on basic disks 549
ESP 549
MSR partitions 550
Primary partitions 551
LDM metadata and LDM data partitions 552
OEM or unknown partitions 552
Managing volumes on dynamic disks 552
Creating a simple or spanned volume. 553
Configuring RAID 0: Striping. 555
Recovering a failed simple, spanned, or striped disk 556
Moving dynamic disks 556
Configuring RAID 1: Disk mirroring 558
Mirroring boot and system volumes 559
Configuring RAID 5: Disk striping with parity 564
Breaking or removing a mirrored set 565
Resolving problems with mirrored sets. 565
Repairing a mirrored system volume 567
Resolving problems with RAID-5 sets 568

Chapter 13: **TPM and BitLocker Drive Encryption 569**

Working with trusted platforms 569
Managing TPM. 571
Understanding TPM states and tools 571
Managing TPM owner authorization information 574
Preparing and initializing a TPM for first use. 576
Turning an initialized TPM on or off 580
Clearing the TPM. 580
Changing the TPM owner password 582
Introducing BitLocker Drive Encryption. 583
BitLocker essentials. 583
BitLocker modes 584
BitLocker changes 587
Using hardware encryption, secure boot, and Network Unlock 588
Hardware encrypted drives. 588
Optimizing encryption. 589
Setting permitted encryption types 591
Preparing BitLocker for startup authentication and secure boot. 593
Using Network Unlock 594
Provisioning BitLocker prior to deployment 596
Deploying BitLocker Drive Encryption 596
Setting up and managing BitLocker Drive Encryption 601
Configuring and enabling BitLocker Drive Encryption. 602
Determining whether a computer has BitLocker-encrypted volumes. 605
Enabling BitLocker on fixed data drives 606

Enabling BitLocker on removable data drives 608
Enabling BitLocker on operating-system volumes 611
Managing and troubleshooting BitLocker 615

Chapter 14: **Managing file systems and storage. 621**

Understanding the disk and file-system structure. 621
Using FAT. 625
File allocation table structure 625
FAT features 626
Using NTFS 628
NTFS structures 629
NTFS features. 633
Analyzing the NTFS structure 634
Advanced NTFS features. 637
Hard links 637
Data streams 638
Change journals. 640
Object identifiers. 643
Reparse points. 644
Sparse files 645
Transactional NTFS 647
Using ReFS. 649
ReFS features 649
ReFS structures 651
ReFS advantages 653
ReFS integrity streams, data scrubbing, and salvage 654
Using file-based compression 656
NTFS compression. 656
Compressed (zipped) folders 659
Managing disk quotas. 661
How quota management works. 661
Configuring disk quotas. 663
Customizing quota entries for individual users. 665
Managing disk quotas after configuration. 668
Exporting and importing quota entries 671
Automated disk maintenance 672
Preventing disk-integrity problems 672
Running Check Disk interactively. 675
Analyzing FAT volumes by using ChkDsk 678
Analyzing NTFS volumes by using ChkDsk. 678
Repairing volumes and marking bad sectors by using ChkDsk 679
Automated optimization of disks 680
Preventing fragmentation of disks. 680
Fixing fragmentation by using Optimize Drives 682
Understanding the fragmentation analysis 686

Managing storage spaces. 689
    Storage essentials 689
    Using and configuring offloaded transfers 691
    Working with available storage 694
    Creating storage pools and allocating space. 696
    Creating storage spaces. 697
    Creating a virtual disk in a storage space 700
    Creating a standard volume 702
    Configuring data deduplication 704

Chapter 15: **File sharing and security 715**

File-sharing essentials 716
    Understanding file-sharing models. 716
    Enabling file sharing 717
    Using and finding shares 719
    Hiding and controlling share access 723
    Special and administrative shares 724
    Accessing shares for administration 726
Creating and publishing shared folders. 726
    Creating shares by using File Explorer. 727
    Creating shares by using Computer Management 731
    Creating shared folders in Server Manager 735
    Changing shared folder settings 741
    Publishing shares in Active Directory 741
Managing share permissions. 742
    Understanding share permissions 743
    Configuring share permissions. 744
Managing access permissions 748
    File and folder ownership 749
    Permission inheritance for files and folders. 750
    Configuring access permissions 752
    Troubleshooting permissions 761
Managing file shares after configuration. 763
Managing claims-based access controls 765
    Understanding central access policies. 766
    Enabling dynamic controls and claims-based policy 766
    Defining central access policies 768
Auditing file and folder access 770
    Enabling basic auditing for files and folders 771
    Enabling advanced auditing 773
    Specifying files and folders to audit 775
    Extending access policies to auditing 779
    Monitoring the security logs. 781

Shadow copy essentials. 781
Using shadow copies of shared folders. 781
How shadow copies works 782
Implementing Shadow Copies for Shared Folders 784
Managing shadow copies in Computer Management 786
Configuring shadow copies in Computer Management 786
Maintaining shadow copies after configuration 790
Reverting an entire volume. 791
Configuring shadow copies at the command line 792
Enabling shadow copying from the command line 792
Create manual snapshots from the command line. 793
Viewing shadow copy information 793
Deleting snapshot images from the command line 795
Disabling shadow copies from the command line 796
Reverting volumes from the command line. 796

Chapter 16: **Managing file screening and storage reporting 797**
Understanding file screening and storage reporting 797
Managing file screening and storage reporting. 802
Managing global file-resource settings 802
Managing the file groups to which screens are applied 812
Managing file-screen templates. 813
Creating file screens 816
Defining file-screening exceptions. 817
Scheduling and generating storage reports 817

Chapter 17: **Backup and recovery. 821**
Disaster-planning strategies 821
Developing contingency procedures 822
Implementing problem-escalation and response procedures 823
Creating a problem-resolution policy document 824
Disaster preparedness procedures 826
Performing backups 826
Repairing startup 827
Setting startup and recovery options 828
Developing backup strategies 830
Creating your backup strategy 831
Backup strategy considerations 831
Selecting the optimal backup techniques 833
Understanding backup types 835
Using media rotation and maintaining additional media sets 836

Backing up and recovering your data 837
Using the backup utility. 838
Backing up your data 840
Scheduling backups 841
Performing a one-time backup 846
Tracking scheduled and manual backups. 850
Recovering your data 852
Recovering the system state 857
Restoring the operating system and the full system 858
Backing up and restoring Active Directory. 859
Backup and recovery strategies for Active Directory. 860
Performing a nonauthoritative restore of Active Directory 861
Performing an authoritative restore of Active Directory. 863
Restoring Sysvol data 866
Restoring a failed domain controller by installing a new domain controller. 866
Troubleshooting startup and shutdown 868
Resolving startup issues. 868
Repairing missing or corrupted system files 870
Resolving restart or shutdown issues 871

Part 4: Managing Windows Server 2012 Networking and Domain Services

Chapter 18: **Networking with TCP/IP 875**
Navigating networking in Windows Server 2012. 875
Using TCP/IP 880
Understanding IPv4 addressing 883
Unicast IPv4 addresses. 883
Multicast IPv4 addresses 886
Broadcast IPv4 addresses 887
Special IPv4 addressing rules. 888
Using subnets and subnet masks 890
Subnet masks. 890
Network prefix notation 891
Subnetting 892
Understanding IP data packets. 897
Getting and using IPv4 addresses. 898
Understanding IPv6. 900
Understanding name resolution 903
Domain Name System 903
Windows Internet Naming Service 906
Link-Local Multicast Name Resolution 907

Chapter 19: **Managing TCP/IP networking 909**

Installing TCP/IP networking 909
- Preparing for installation of TCP/IP networking 910
- Installing network adapters. 911
- Installing networking services (TCP/IP). 911

Configuring TCP/IP networking. 912
- Configuring static IP addresses. 913
- Configuring dynamic IP addresses and alternate IP addressing. 917
- Configuring multiple IP addresses and gateways 919
- Configuring DNS resolution 921
- Configuring WINS resolution 924

Managing network connections 926
- Checking the status, speed, and activity for network connections 926
- Viewing network configuration information 928
- Enabling and disabling network connections 930
- Renaming network connections. 930

Troubleshooting and testing network settings. 931
- Diagnosing and resolving network connection problems 931
- Diagnosing and resolving Internet connection problems. 931
- Performing basic network tests 932
- Diagnosing and resolving IP addressing problems. 933
- Diagnosing and resolving routing problems. 935
- Releasing and renewing DHCP settings 936
- Diagnosing and fixing name-resolution issues 938

Chapter 20: **Managing DHCP. 941**

DHCP essentials 941
- DHCPv4 and autoconfiguration 943
- DHCPv6 and autoconfiguration 944

DHCP security considerations 945

DHCP and IPAM 946

Planning DHCPv4 and DHCPv6 implementations 948
- DHCPv4 messages and relay agents 948
- DHCPv6 messages and relay agents 950
- DHCP availability and fault tolerance 952

Setting up DHCP servers 957
- Installing the DHCP Server service. 959
- Authorizing DHCP servers in Active Directory. 962
- Creating and configuring scopes 963
- Activating scopes 973
- Scope exclusions 974
- Scope reservations 976
- Creating and using failover scopes 980

Configuring TCP/IP options 984
Levels of options and their uses 985
Policy-based assignment 986
Options used by Windows clients 987
Using user-specific and vendor-specific TCP/IP options 988
Settings options for all clients. 990
Settings options for RRAS and NAP clients 993
Setting add-on options for directly connected clients 994
Defining classes to get different option sets 995
Advanced DHCP configuration and maintenance 997
Monitoring DHCP audit logging 998
Binding the DHCP Server service to a network interface 1001
Integrating DHCP and DNS. 1002
Integrating DHCP and NAP. 1003
Enabling conflict detection on DHCP servers 1007
Saving and restoring the DHCP configuration. 1008
Managing and maintaining the DHCP database. 1008
Setting up DHCP relay agents 1011
Configuring and enabling Routing And Remote Access 1011
Adding and configuring the DHCP relay agent. 1012

Chapter 21: **Architecting DNS infrastructure 1017**
DNS essentials 1017
Planning DNS implementations 1019
Public and private namespaces 1020
Name resolution using DNS 1021
Understanding DNS devolution 1024
DNS resource records. 1025
DNS zones and zone transfers 1027
Secondary zones, stub zones, and conditional forwarding. 1032
Integration with other technologies 1034
Security considerations. 1036
DNS queries and security 1036
DNS dynamic updates and security. 1037
External DNS name resolution and security. 1038
Architecting a DNS design 1041
Split-brain design: Same internal and external names. 1041
Separate-name design: Different internal and external names 1043
Securing DNS from attacks 1044

Chapter 22: **Implementing and managing DNS 1047**
Installing the DNS Server service 1047
Using DNS with Active Directory 1047
Using DNS without Active Directory 1051
DNS setup. 1052

Configuring DNS using the wizard 1056
Configuring a small network using the Configure A DNS Server Wizard 1056
Configuring a large network using the Configure A DNS Server Wizard 1060
Configuring DNS zones, subdomains, forwarders, and zone transfers 1065
Creating forward lookup zones 1066
Creating reverse lookup zones 1068
Configuring forwarders and conditional forwarding 1068
Configuring subdomains and delegating authority 1071
Configuring zone transfers 1074
Configuring secondary notification 1076
Deploying DNSSEC 1078
DNSSEC essentials 1078
Securing zones with digital signatures 1079
Signing a zone 1080
111Adding resource records 1082
Host Address (A and AAAA) and Pointer (PTR) records 1083
Canonical Name (CNAME) records 1086
Mail Exchanger (MX) records 1087
Name Server (NS) records 1088
Start of Authority (SOA) records 1090
Service Location (SRV) records 1091
Deploying global names 1092
Maintaining and monitoring DNS 1094
Configuring default application directory partitions and replication scope 1094
Setting the aging and scavenging rules 1097
Configuring logging and checking DNS Server logs 1098
Troubleshooting the DNS client service 1099
Try reregistering the client 1099
Check the client's TCP/IP configuration 1099
Check the client's resolver cache 1101
Perform lookups for troubleshooting 1102
Troubleshooting the DNS Server service 1102
Check the server's TCP/IP configuration 1103
Check the server's cache 1103
Check replication to other name servers 1103
Examine the configuration of the DNS server 1104
Examine zones and zone records 1110

Chapter 23: **Implementing and maintaining WINS 1113**

WINS essentials 1113
NetBIOS namespace and scope 1113
NetBIOS node types 1115
WINS name registration and cache 1115

WINS implementation details . . . 1116

Setting up WINS servers . . . 1117

Configuring replication partners . . . 1120

Replication essentials . . . 1120

Configuring automatic replication partners . . . 1120

Using designated replication partners . . . 1122

Configuring and maintaining WINS . . . 1124

Configuring burst handling . . . 1124

Checking server status and configuration . . . 1126

Checking active registrations and scavenging records . . . 1128

Maintaining the WINS database . . . 1129

Enabling WINS lookups through DNS . . . 1132

Part 5: Managing Active Directory and Security

Chapter 24: **Active Directory architecture . . . 1135**

Active Directory physical architecture . . . 1135

Active Directory physical architecture: A top-level view . . . 1135

Active Directory within the Local Security Authority . . . 1137

Directory service architecture . . . 1139

Data store architecture . . . 1147

Active Directory logical architecture . . . 1150

Active Directory objects . . . 1151

Active Directory domains, trees, and forests . . . 1152

Active Directory trusts . . . 1154

Active Directory namespaces and partitions . . . 1157

Active Directory data distribution . . . 1159

Chapter 25: **Designing and managing the domain environment . . . 1161**

Design considerations for Active Directory replication . . . 1162

Design considerations for Active Directory search and global catalogs . . . 1164

Searching the tree . . . 1164

Accessing the global catalog . . . 1165

Designating global catalog servers . . . 1166

Designating replication attributes . . . 1168

Design considerations for compatibility . . . 1171

Understanding domain functional level . . . 1171

Understanding forest functional level . . . 1173

Raising or lowering the domain or forest functional level . . . 1174

Design considerations for Active Directory authentication and trusts . . . 1175

Universal groups and authentication . . . 1175

NTLM and Kerberos authentication . . . 1178

Authentication and trusts across domain boundaries . . . 1183

Authentication and trusts across forest boundaries 1186
Examining domain and forest trusts 1189
Establishing external, shortcut, realm, and cross-forest trusts 1192
Verifying and troubleshooting trusts 1196
Delegating authentication 1196
Delegated authentication essentials 1197
Configuring delegated authentication 1197
Design considerations for Active Directory operations masters 1200
Operations master roles. 1201
Using, locating, and transferring the Schema Master role 1203
Using, locating, and transferring the domain naming master role 1205
Using, locating, and transferring the relative ID master role 1206
Using, locating, and transferring the PDC emulator role. 1209
Using, locating, and transferring the infrastructure master role 1212
Seizing operations master roles 1212

Chapter 26: **Organizing Active Directory. 1215**

Creating an Active Directory implementation or update plan 1216
Developing a forest plan 1216
Forest namespace 1217
A single forest vs. multiple forests 1218
Forest administration 1219
Developing a domain plan. 1221
Domain design considerations 1221
A single domain vs. multiple domains. 1222
Forest root domain design configurations. 1223
Changing domain design 1224
Developing an organizational unit plan 1225
Using organizational units. 1226
Using OUs for delegation 1227
Using OUs for Group Policy 1228
Creating an OU design. 1228

Chapter 27: **Configuring Active Directory sites and replication. 1233**

Working with Active Directory sites 1233
Single site vs. multiple sites 1235
Replication within and between sites 1236
Determining site boundaries. 1237
Understanding Active Directory replication 1238
Tracking Active Directory replication changes over time 1238
Tracking Active Directory system volume changes over time 1240
Replication architecture: An overview. 1246
Intersite replication essentials. 1253

Replication rings and directory partitions 1256
Developing or revising a site design 1260
Mapping network infrastructure 1260
Creating a site design 1262

Chapter 28: **Implementing Active Directory Domain Services 1271**

Preinstallation considerations for Active Directory 1271
Hardware and configuration considerations for domain controllers 1272
Configuring Active Directory for fast recovery with storage area networks 1274
Connecting clients to Active Directory 1276
Installing Active Directory Domain Services 1276
Active Directory installation options and issues 1276
Using the Active Directory Domain Services Configuration Wizard 1280
Performing an Active Directory installation from media 1294
Cloning virtualized domain controllers 1297
Using clones of virtualized domain controllers 1297
Creating a clone virtualized domain controller 1298
Finalizing the clone deployment 1300
Troubleshooting the clone deployment 1301
Uninstalling Active Directory 1302
Creating and managing organizational units 1307
Creating an OU 1307
Setting OU properties 1309
Creating or moving accounts and resources for use with an OU 1310
Delegating the administration of domains and OUs 1311
Understanding delegation of administration 1311
Delegating administration 1312

Chapter 29: **Deploying read-only domain controllers 1315**

Introducing read-only domain controllers 1315
Design considerations for read-only replication 1319
Installing RODCs 1322
Preparing for an RODC installation 1323
Installing an RODC 1324
Installing an RODC from media 1330
Staging an RODC 1332
Managing Password Replication Policy 1336
Working with Password Replication Policy 1336
Allowing or denying accounts in Password Replication Policy 1338
Viewing and managing credentials on an RODC 1340
Determining whether an account is allowed or denied access 1341
Resetting credentials 1342
Delegating administrative permissions 1343

Chapter 30: **Managing users, groups, and computers 1345**
Managing domain user accounts 1345
Configuring user account policies 1345
Creating Password Settings Objects and applying secondary settings. 1350
Understanding user account capabilities, privileges, and rights 1354
Assigning user rights 1355
Creating and configuring domain user accounts 1357
Configuring account options 1361
Configuring profile options. 1364
Troubleshooting user accounts 1366
Maintaining user accounts 1367
Deleting user accounts. 1367
Disabling and enabling user accounts. 1368
Moving user accounts 1368
Renaming user accounts 1369
Resetting a user's domain password 1370
Unlocking user accounts 1371
Creating a user account password backup. 1371
Managing groups. 1373
Understanding groups 1373
Creating a group 1374
Adding members to groups 1377
Deleting a group 1377
Modifying groups 1378
Managing computer accounts. 1379
Creating a computer account in Active Directory. 1379
Joining computers to a domain 1381
Moving a computer account. 1382
Disabling a computer account 1382
Deleting a computer account 1382
Managing a computer account 1382
Resetting a computer account 1383
Troubleshooting computer accounts. 1383
Recovering deleted accounts. 1385
Enabling Active Directory Recycle Bin. 1385
Recovering objects from the recycle bin 1385

Chapter 31: **Managing Group Policy 1387**
Understanding Group Policy 1388
Local and Active Directory Group Policy 1388
Group Policy settings 1389
Group Policy architecture 1390
Administrative templates. 1392

Implementing Group Policy . . . 1393
Working with Local Group Policy . . . 1394
Working with Group Policy Management Console . . . 1397
Working with the default Group Policy Objects . . . 1403
Managing Group Policy through delegation . . . 1406
Managing GPO creation rights . . . 1406
Reviewing Group Policy management privileges . . . 1407
Delegating Group Policy management privileges . . . 1409
Delegating privileges for links and RSoP . . . 1410
Managing Group Policy inheritance and processing . . . 1411
Group Policy inheritance . . . 1411
Changing link order and precedence . . . 1412
Overriding inheritance . . . 1414
Blocking inheritance . . . 1415
Enforcing inheritance . . . 1416
Filtering Group Policy application . . . 1417
Group Policy processing . . . 1418
Modifying Group Policy processing . . . 1420
Modifying user policy preference using loopback processing . . . 1421
Using scripts in Group Policy . . . 1422
Configuring computer startup and shutdown scripts . . . 1422
Configuring user logon and logoff scripts . . . 1423
Applying Group Policy through security templates . . . 1424
Working with security templates . . . 1425
Applying security templates . . . 1426
Maintaining and troubleshooting Group Policy . . . 1427
Group Policy refresh . . . 1427
Modifying Group Policy refresh . . . 1428
Viewing applicable GPOs and the last refresh . . . 1431
Modeling GPOs for planning . . . 1433
Refreshing Group Policy manually . . . 1437
Backing up GPOs . . . 1438
Restoring GPOs . . . 1440
Fixing default Group Policy . . . 1441

Chapter 32: **Active Directory site administration . . . 1443**

Managing sites and subnets . . . 1443
Creating an Active Directory site . . . 1444
Creating a subnet and associating it with a site . . . 1445
Associating domain controllers with a site . . . 1446
Managing site links and intersite replication . . . 1447
Understanding IP and SMTP replication transports . . . 1448
Creating a site link . . . 1449

- Configuring replication schedules for site links . . . 1453
- Configuring site-link bridges . . . 1455
- Determining the ISTG . . . 1457
- Configuring site bridgehead servers . . . 1458
- Configuring advanced site-link options . . . 1461

Monitoring and troubleshooting replication . . . 1462

- Using the Replication Administrator . . . 1463
- Using PowerShell to monitor and troubleshoot replication . . . 1464
- Monitoring replication . . . 1465
- Modifying intersite replication for testing . . . 1466

Index to troubleshooting topics . . . 1469

Index . . . 1471

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

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

microsoft.com/learning/booksurvey

This page intentionally left blank

Introduction

Welcome to *Windows Server 2012 Inside Out*. As the author of many popular technology books, I've been writing professionally about 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 many years. The advantage for you, the reader, is that my solid understanding of these technologies allowed me to dig into the Windows Server 2012 architecture, internals, and configuration to see how things really work under the hood and then pass this information on to you throughout this book.

From top to bottom, Windows Server 2012 is substantially different from earlier versions of Window Server. Not only are there major changes throughout the operating system, but 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 possible previously. 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 generally is 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 generally is the equivalent of a right-click.
- **Swipe to select** Slide an item a short distance in the opposite direction of 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 in or shows less information.
- **Stretch** Touch an item with two or more fingers, and then move those fingers away from each other. Stretching zooms out or shows more information.

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, 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 why you want to use Windows Server. Instead, I focus on configuration, security, auditing, storage management, performance analysis, performance tuning, troubleshooting, and much more.

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 & book support

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed on our Microsoft Press site at oreilly.com:

http://go.microsoft.com/FWLink/?Linkid=275534

If you find an error that is not already listed, you can report it to us through the same page.

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

Please note that product support for Microsoft software is not offered through the addresses above.

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

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

This page intentionally left blank

This page intentionally left blank

CHAPTER 3

Boot configuration

Boot from hardware and firmware 101
Boot environment essentials 109
Managing startup and boot configuration 111
Managing the Boot Configuration Data store and its entries 119

Unlike early releases of server operating systems for Microsoft Windows, Windows Server 2012 doesn't boot from an initialization file. Instead, the operating system uses the Windows Boot Manager to initialize and start the operating system. The boot environment dramatically changes the way the operating system starts, and it is designed to resolve issues related to boot integrity, operating system integrity, and firmware abstraction. The boot environment is loaded prior to the operating system, making it a pre-operating system environment. This ensures that the boot environment can be used to validate the integrity of the startup process and the operating system itself before actually starting the operating system.

Boot from hardware and firmware

At first glance, startup and shutdown seem to be the most basic features of an operating system, but as you get a better understanding of how computers work, you quickly see that there's nothing simple or basic about startup, shutdown, or related processes and procedures. In fact, anyone who's worked with computers probably has had a problem with startup or shutdown at one time or another. Problems with startup and shutdown can be compounded in modern computers because of their extended frameworks for advanced configuration and power management in firmware and hardware.

Note

Many administrators install Windows Server 2012 on desktop-class systems without giving careful consideration to how this could affect the operation of the computer. When you install Windows Server 2012 on a desktop-class system, it is critically important for you to understand how computers designed for desktop operating systems handle advanced configuration and power management in hardware and firmware. This will enable you to modify the hardware and firmware settings so that they work better with Windows Server 2012.

Hardware and firmware power states

Before the boot environment is loaded, computers start up from hardware and firmware. Windows desktop operating systems do things a bit differently from Windows Server operating systems when it comes to power-state management features. In Windows desktops, turning off a computer and shutting down a computer are separate tasks. By default, when you turn off a computer running a Windows desktop operating system, the computer enters standby mode. When entering standby mode, the operating system automatically saves all work, turns off the display, and enters a low power-consumption mode with the computer's fans and hard disks stopped. The state of the computer is maintained in the computer's memory. When the computer wakes from standby mode, its state is exactly as it was when you turned off your computer.

You can turn off a computer running a Windows desktop operating system and enter standby mode by tapping or clicking the Settings charm, tapping or clicking Power, and then tapping or clicking Sleep. To wake the computer from the standby state, you can press the power button on the computer's case or a key on the computer's keyboard. Moving the mouse also wakes the computer.

If you install Windows 8 or Windows Server 2012 on a mobile computer, the computer's power state can be changed by closing the lid. By default with Windows 8, the computer enters the standby state when you close the lid. By default with Windows Server 2012, the computer doesn't change its power state when you close or open the lid, but you can configure the server to shut down when you close the lid.

There are, however, a few "gotchas" with the power button and the standby state in Windows desktop operating systems. The way the power button works depends on the following:

- **System hardware** For the power button to work, the computer hardware must support the standby state. If the computer hardware doesn't support the standby state, the computer can't use the standby state and turning off the computer powers it down completely.

- **System state** For the power button to work, the system must be in a valid state. If the computer has installed updates that require a reboot or you've installed programs that require a reboot, the computer can't enter the standby state and turning off the computer powers it down completely.

- **System configuration** For the power button to work, sleep mode must be enabled. If you reconfigured the power options on the computer and set the power button to the Shut Down action, the computer can't use the standby state and turning off the computer powers it down completely.

You can determine exactly how the power options are configured on a Windows computer by tapping or clicking the Settings charm, tapping or clicking Control Panel, and tapping or clicking Power Options. The options available depend on the type of computing device.

Diagnosing hardware and firmware startup problems

Whether you are working with a Windows desktop operating system or a Windows Server operating system and trying to diagnose and resolve startup problems, be sure to keep in mind that power-state management capabilities are provided by the hardware but are enabled by the operating system. Because of this, to fully diagnose and resolve boot issues, you must look at the computer's hardware and software, including the following items:

- Motherboard/chipset
- Firmware
- Operating system

To better understand the hardware aspects of boot issues, let's dig in and take a look at Advanced Configuration and Power Interface (ACPI). A computer's motherboard/chipset, firmware, and operating system must support ACPI for the advanced power-state features to work. There are many types of motherboards/chipsets. Although older motherboards/chipsets might not be updateable, most of the newer ones have updateable firmware. Chipset firmware is separate from and different from the computer's underlying firmware interface.

Currently, there are three prevalent firmware interfaces:

- Basic Input Output System (BIOS)
- Extensible Firmware Interface (EFI)
- Unified Extensible Firmware Interface (UEFI)

A computer's BIOS, EFI, or UEFI programming provides the hardware-level interface between hardware components and software. Like chipsets themselves, BIOS, EFI, and UEFI can be updated. ACPI-aware components track the power state of the computer. An ACPI-aware operating system can generate a request that the system be switched into a different ACPI mode. BIOS, EFI, or UEFI responds to enable the requested ACPI mode.

ACPI 4.0 was finalized in June 2009 and ACPI 5.0 was finalized in December 2011. Computers manufactured prior to this time will likely not have firmware that is fully compliant, and you will probably need to update the firmware when a compatible revision becomes available. In some cases, and especially with older hardware, you might not be able to update a computer's firmware to make it fully compliant with ACPI 4.0 or ACPI 5.0.

For example, if you are configuring the power options and you don't have minimum and maximum processor-state options, the computer's firmware isn't fully compatible with ACPI 3.0 and likely will not fully support ACPI 4.0 or ACPI 5.0 either. Still, you should check the hardware manufacturer's website for firmware updates.

ACPI defines active and passive cooling modes. These cooling modes are inversely related to each other:

- Passive cooling reduces system performance but is quieter because there's less fan noise. With passive cooling, Windows lessens power consumption to reduce the operating temperature of the computer but at the cost of system performance. Here, Windows reduces the processor speed in an attempt to cool the computer before increasing fan speed, which would increase power consumption.

- Active cooling allows maximum system performance. With active cooling, Windows increases power consumption to reduce the temperature of the machine. Here, Windows increases fan speed to cool the computer before attempting to reduce processor speed.

Power policy includes upper and lower limits for the processor state, referred to as the *maximum processor state* and the *minimum processor state*, respectively. These states are implemented by making use of a feature of ACPI 3.0 and later versions called *processor throttling*, and they determine the range of currently available processor performance states that Windows can use. By setting the maximum and minimum values, you define the bounds for the allowed performance states, or you can use the same value for each to force the system to remain in a specific performance state. Windows reduces power consumption by throttling the processor speed. For example, if the upper bound is 100 percent and the lower bound is 5 percent, Windows can throttle the processor within this range as workloads permit to reduce power consumption. In a computer with a 3-GHz processor, Windows would adjust the operating frequency of the processor between 0.15 GHz and 3.0 GHz.

Processor throttling and related performance states were introduced with Windows XP and Windows Server 2003, but these early implementations were designed for computers with discrete-socketed processors and not for computers with processor cores. As a result, they are not effective in reducing the power consumption of computers with logical processors. Beginning with Windows 7 and Windows Server 2008 R2, Windows reduces power consumption in computers with multicore processors by using a feature of ACPI 4.0 called *logical processor idling* and by updating processor-throttling features to work with processor cores.

Logical processor idling is designed to ensure that Windows uses the fewest number of processor cores for a given workload. Windows accomplishes this by consolidating workloads onto the fewest cores possible and suspending inactive processor cores. As additional processing power is required, Windows activates inactive processor cores. This idling functionality works in conjunction with the management of process performance states at the core level.

ACPI defines processor performance states, referred to as *p-states*, and processor idle sleep states, referred to as *c-states*. Processor performance states include P0 (the processor or core uses its maximum performance capability and can consume maximum power), P1 (the processor or core is limited below its maximum and consumes less than maximum power), and P*n* (where state *n* is a maximum number that is processor dependent, and the processor or core is at its minimal level and consumes minimal power while remaining in an active state).

Processor idle sleep states include C0 (the processor or core can execute instructions), C1 (the processor or core has the lowest latency and is in a nonexecuting power state), C2 (the processor or core has longer latency to improve power savings over the C1 state), and C3 (the processor or core has the longest latency to improve power savings over the C1 and C2 states).

Note

Windows switches processors or cores between any p-state and from the C1 state to the C0 state nearly instantaneously (fractions of milliseconds) and tends not to use the deep sleep states, so you don't need to worry about the performance impact of throttling or waking up processors or cores. The processors or cores are available when they are needed. That said, the easiest way to limit processor power management is to modify the active power plan and set the minimum and maximum processor states to 100 percent.

Windows saves power by putting processor cores in and out of appropriate p-states and c-states. On a computer with four logical processors, Windows might use p-states 0 to 5, where P0 allows 100 percent usage, P1 allows 90 percent usage, P2 allows 80 percent usage, P3 allows 70 percent usage, P4 allows 60 percent usage, and P5 allows 50 percent usage. When the computer is active, logical processor 0 would likely be active with a p-state of 0 to 5, and the other processors would likely be at an appropriate p-state or in a sleep state.

INSIDE OUT Processor Idling

Logical processor idling is used to reduce power consumption by removing a logical processor from the operating system's list of non-processor-affinitized work. However, because processor-affinitized work reduces the effectiveness of this feature, you'll want to plan carefully prior to configuring processing-affinity settings for applications. You can use Windows System Resource Manager to manage processor resources through percent-processor-usage targets and processor-affinity rules. However, both techniques reduce the effectiveness of logical processor idling. Note also that Windows System Resource Manager is deprecated for Windows Server 2012 and will be phased out in future releases of Windows Server.

ACPI 4.0 and ACPI 5.0 define four global power states. In G0, the working state in which software runs, power consumption is at its highest and latency is at its lowest. In G1, the sleeping state (in which software doesn't run), latency varies with the sleep state and power consumption is less than the G0 state. In G2 (also referred to as *S5 sleep state*), the soft off state where the operating system doesn't run, latency is long and power consumption is very near zero. In G3, the mechanical off state (in which the operating system doesn't run), latency is long and power consumption is zero. There's also a special global state, known as *S4 nonvolatile sleep*, in which the operating system writes all system context to a file on nonvolatile storage media, allowing the system context to be saved and restored.

Within the global sleeping state, G1, are the sleep-state variations summarized in Table 3-1. S1 is a sleeping state in which the entire system context is maintained. S2 is a sleeping state similar to S1 except that the CPU and system-cache contexts are lost and control starts from a reset. S3 is a sleeping state in which all CPU, cache, and chipset contexts are lost and hardware maintains the memory context and restores some CPU and L2 cache configuration context. S4 is a sleeping state in which it is assumed that the hardware has powered off all devices to reduce power usage to a minimum and only the platform context is maintained. S5 is a sleeping state in which it is assumed that the hardware is in a soft off state, where no context is maintained and a complete boot is required when the system wakes.

TABLE 3-1 Power states for ACPI in firmware and hardware

State	Type	Description
S0	ON state	The system is completely operational, is fully powered, and completely retains the context (such as the volatile registers, memory caches, and RAM).
S1	Sleep state	The system consumes less power in this state than in the S0 state. All hardware and processor contexts are maintained.

State	Type	Description
S2	Sleep state	The system consumes less power in this state than in the S1 state. The processor loses power, and the processor context and contents of the cache are lost.
S3	Sleep state	The system consumes less power in this state than in the S2 state. The processor and hardware contexts, cache contents, and chipset context are lost. The system memory is retained.
S4	Hibernate state	The system consumes the least power in this state compared to all other sleep states. The system is almost at an OFF state. The context data is written to hard disk, and there is no context retained. The system can restart from the context data stored on the disk.
S5	OFF state	The system is in a shutdown state, and the system retains no context. The system requires a full reboot to start.

Motherboard chipsets support specific power states. For example, a motherboard might support S0, S1, S4, and S5 states, but it might not support the S2 or S3 states. In Windows operating systems, the *sleep power transition* refers to switching off the system to a Sleep or Hibernate mode, and the *wake power transition* refers to switching on the system from a Sleep or Hibernate mode. The Sleep and Hibernate modes allow users to switch off and switch on systems much faster than the regular shutdown and startup processes.

Thus, a computer is waking up when the computer is transitioning from the OFF state (S5) or any sleep state (S1–S4) to the ON state (S0), and the computer is going to sleep when the computer is transitioning from ON state (S0) to OFF state (S5) or sleep state (S1–S4). A computer cannot enter one sleep state directly from another because it must enter the ON state before entering any other sleep state. Sleep and hibernate are disabled in Windows Server.

Resolving hardware and firmware startup problems

On most computers, you can enter BIOS, EFI, or UEFI during boot by pressing F2 or another function key. When you are in firmware, you can go to the Power screen or a similar screen to manage ACPI and related settings.

Power settings you might see include the following:

- **Restore AC Power Loss or AC Recovery** Determines the mode of operation if a power loss occurs and for which you'll see settings such as Stay Off/Off, Last State/Last, Power On/On. Stay Off means the system remains off after power is restored. Last State restores the system to the state it was in before power failed. Power On means the system will turn on after power is restored.

- **Wake On LAN From S4/S5 or Auto Power On** Determines the action taken when the system power is off and a PCI Power Management wake event occurs. You'll see settings such as Stay Off or Power On.
- **ACPI Suspend State or Suspend Mode** Sets the suspend mode. Typically, you'll be able to set S1 state or S3 state as the suspend mode.

> **Note**
> **I provide two standard labels for each setting because your computer hardware might not have these exact labels. The firmware variant you are working with determines the actual labels that are associated with boot, power, and other settings.**

Because Intel and AMD also have other technologies to help reduce startup and resume times, you might also see the following power settings:

- Enhanced Intel SpeedStep Technology (EIST), which can be either Disabled or Enabled
- Intel Quick Resume Technology, which can be either Disabled or Enabled

Enhanced Intel SpeedStep Technology (EIST or SpeedStep) allows the system to dynamically adjust processor voltage and core frequency, which can result in decreased average power consumption and decreased average heat production. When EIST or a similar technology is enabled and in use, you'll see two different processor speeds on the System page in Control Panel. The first speed listed is the specified speed of the processor. The second speed is the current operating speed, which should be less than the first speed. If Enhanced Intel SpeedStep Technology is off, both processor speeds will be equal. Advanced Settings for Power Options under Processor Power Management can also affect how this technology works. Generally speaking, although you might want to use this technology with a Windows desktop operating system, you won't want to use this technology with a Windows Server operating system.

Intel Quick Resume Technology Driver (QRTD) allows an Intel Viiv technology–based computer to behave like a consumer electronic device with instant on/off after an initial boot. Intel QRTD manages this behavior through the Quick Resume mode function of the Intel Viiv chipset. Pressing the power button on the computer or a remote control is what puts the computer in the Quick Sleep state, and the computer can Quick Resume from sleep by moving the mouse, pressing an on/off key on the keyboard (if available), or pressing the sleep button on the remote control. Quick Sleep mode is different from standard sleep mode. In Quick Sleep mode, the computer's video card stops sending data to the display, the sound is muted, and the monitor LED indicates a lowered power state on the monitor, but the power continues to be supplied to vital components on the system, such as the processor, fans, and so on. Because this technology was originally designed for Windows XP Media Center Edition, it does not work in many cases with later Windows desktop operating systems and generally should not be used with Windows Server operating systems. You might need to disable this feature in firmware to allow a Windows desktop operating system to properly sleep and resume.

After you look at the computer's power settings in firmware, you should also review the computer's boot settings in firmware. Typically, you have a list of bootable devices and can select which one to boot. You also might be able to configure the following boot settings:

- **Boot Drive Order** Determines the boot order for fixed disks
- **Boot To Hard Disk Drive** Determines whether the computer can boot to fixed disks, and can be set to Disabled or Enabled
- **Boot To Removable Devices** Determines whether the computer can boot to removable media, and can be set to Disabled or Enabled
- **Boot To Network** Determines whether the computer can perform a network boot, and can be set to Disabled or Enabled
- **USB Boot** Determines whether the computer can boot to USB flash devices, and can be set to Disabled or Enabled

As with power settings, your computer might not have these exact labels, but the labels should be similar. You need to optimize these settings for the way you plan to use the computer. In most cases, with server hardware, you'll only want to enable Boot To Hard Disk Drive. The exception is for when you use BitLocker Drive Encryption. With BitLocker, you'll want to enable Boot To Removable Devices, USB Boot, or both to ensure that the computer can detect the USB flash drive with the encryption key during the boot process.

Boot environment essentials

Windows Server 2012 supports several different processor architectures and several different disk partitioning styles. EFI was originally developed for Itanium-based computers. Computers with EFI use the GUID partition table (GPT) disk type for boot and system volumes. Computers based on x86 use BIOS and the master boot record (MBR) disk type for boot and system volumes. Computers based on x64 use UEFI wrapped around BIOS or EFI.

With the increasing acceptance and use of UEFI and the ability of Windows to use both MBR and GPT disks regardless of firmware type, the underlying chip architecture won't necessarily determine which firmware type and disk type a computer uses for boot and startup. That said, generally, BIOS-based computers use MBR for booting or for data disks and GPT only for data disks. EFI-based computers can have both GPT and MBR disks, but you typically must have at least one GPT disk that contains the EFI system partition (ESP) and a primary partition or simple volume that contains the operating system for booting.

With early releases of the server operating system for Windows, BIOS-based computers use Ntldr and Boot.ini to boot into the operating system. Ntldr handles the task of loading the operating system, while Boot.ini contains the parameters that enable startup, including the identity of the boot partitions. Through Boot.ini parameters, you can add options that control the way the operating system starts, the way computer components are used, and the way operating system features are used.

On the other hand, with early releases of the server operating system for Windows, EFI-based computers use Ia64ldr.efi, Diskpart.efi, and Nvrboot.efi to boot into the operating system. Ia64ldr.efi handles the task of loading the operating system, while Diskpart.efi identifies the boot partitions. Through Nvrboot.efi, you set the parameters that enable startup.

Windows Server 2008 and later don’t use these boot facilities. Instead, they use a pre-operating system boot environment. Figure 3-1 provides a conceptual overview of how the boot environment fits into the overall computer architecture.

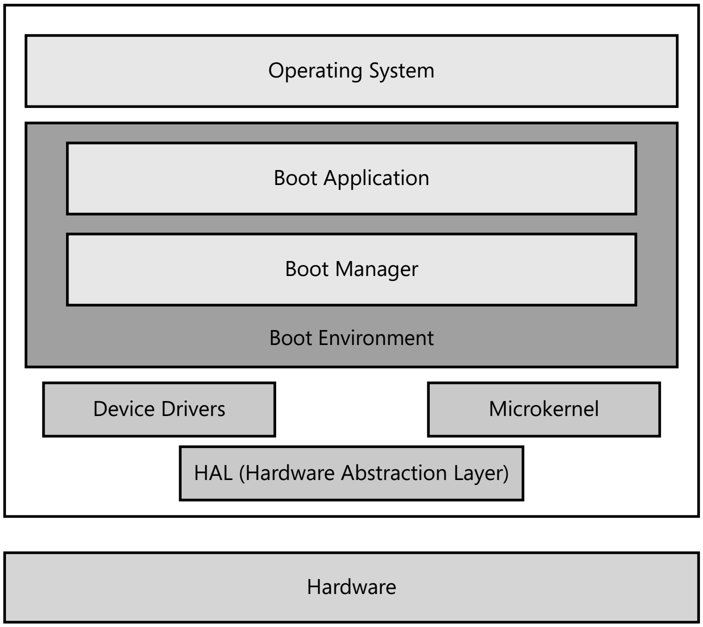


Figure 3-1 A conceptual view of how the boot environment works.

The boot environment is an extensible abstraction layer that allows the operating system to work with multiple types of firmware interfaces without requiring the operating system to be specifically written to work with these firmware interfaces. Within the boot environment, startup is controlled using the parameters in the BCD data store.

The BCD store is contained in a file called the *BCD registry*. The location of this registry depends on the computer's firmware:

- On BIOS-based operating systems, the BCD registry file is stored in the \Boot\Bcd directory of the active partition.
- On EFI-based operating systems, the BCD registry file is stored on the EFI system partition.

Entries in the BCD data store identify the boot manager to use during startup and the specific boot applications available. The default boot manager is the Windows Boot Manager. Windows Boot Manager controls the boot experience, and you can use it to choose which boot application is run. Boot applications load a specific operating system or operating system version. For example, a Windows Boot Loader application loads Windows Server 2012. Because of this, you can boot BIOS-based and EFI-based computers in much the same way.

Managing startup and boot configuration

As discussed in "Troubleshooting startup and shutdown" in Chapter 17, "Backup and recovery," you can press F8 during startup of the operating system to access the Advanced Boot Options menu and then use this menu to select one of several advanced startup modes, including Safe Mode, Enable Boot Logging, and Disable Driver Signature Enforcement. Although these advanced modes temporarily modify the way the operating system starts to help you diagnose and resolve problems, they don't make permanent changes to the boot configuration or to the BCD store. Other tools you can use to modify the boot configuration and manage the BCD store include the Startup And Recovery dialog box, the System Configuration utility, and BCD Editor. The sections that follow discuss how these tools are used.

Managing startup and recovery options

The Startup And Recovery dialog box controls the basic options for the operating system during startup. You can use these options to set the default operating system, the time to display the list of available operating systems, and the time to display recovery options when needed. Whether you start a computer to different operating systems or not, you'll want to optimize these settings to reduce the wait time during startup and, in this way, speed up the startup process.

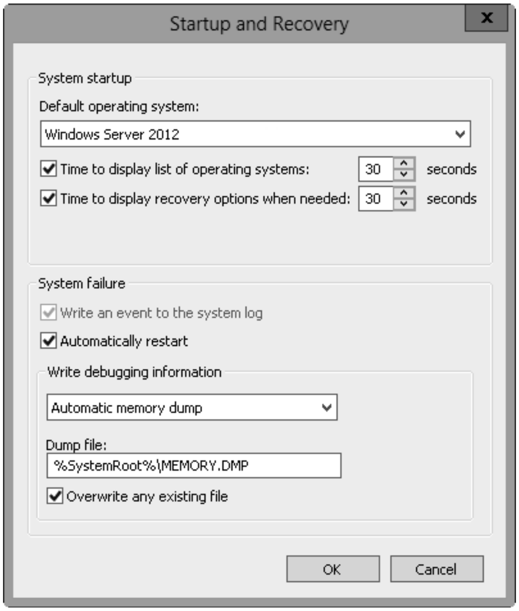
You can access the Startup And Recovery dialog box by completing the following steps:

1. In Control Panel\System and Security, tap or click System to access the System window.

2. In the System window, tap or click Advanced System Settings under Tasks in the left pane. This displays the System Properties dialog box.

3. On the Advanced tab of the System Properties dialog box, tap or click Settings under Startup And Recovery. This displays the Startup And Recovery dialog box, as shown in Figure 3-2.

> **Note**
>
> **Open the Advanced tab of the System Properties dialog box directly by typing SystemPropertiesAdvanced.exe in the Apps Search box and pressing Enter.**



Startup and Recovery

System startup

Default operating system: Windows Server 2012

☑ Time to display list of operating systems: 30 seconds

☑ Time to display recovery options when needed: 30 seconds

System failure

☑ Write an event to the system log

☑ Automatically restart

Write debugging information

Automatic memory dump

Dump file: %SystemRoot%\MEMORY.DMP

☑ Overwrite any existing file

Figure 3-2 Configure system startup options.

4. On a computer with multiple operating systems, use the Default Operating System list to specify the operating system you want to start by default.

5. Set the timeout interval for the operating system list by selecting the Time To Display List Of Operating Systems check box and specifying a timeout in seconds in the field provided. To speed up the startup process, you might want to use a value of five seconds.

6. Set the timeout interval for the recovery options list by selecting the Time To Display Recovery Options When Needed check box and specifying a timeout in seconds in the field provided. Again, to speed up the startup process, you might want to use a value of five seconds.

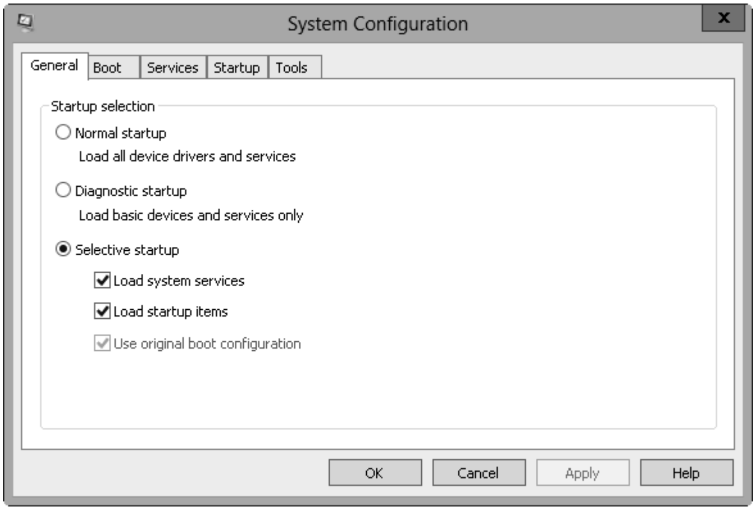
7. Tap or click OK to save your settings.

Managing System Boot Configuration

You can use the System Configuration utility (Msconfig.exe) to fine-tune the way a computer starts. Typically, you use this utility during troubleshooting and diagnostics. For example, as part of troubleshooting, you can configure the computer to use a diagnostic startup where only basic devices and services are loaded.

The System Configuration utility is available on the Tools menu in Server Manager. You can also start the System Configuration utility by pressing the Windows key, typing **msconfig.exe** in the Apps Search box, and pressing Enter. As shown in Figure 3-3, this utility has a series of tabs with options.

Use the General tab options to configure the way startup works. This tab is where you should start your troubleshooting and diagnostics efforts. Using these options, you can choose to perform a normal startup, diagnostic startup, or selective startup. After you restart the computer and resolve any problems, access the System Configuration utility again, select Normal Startup on the General tab, and then tap or click OK.



Startup selection

○ Normal startup
Load all device drivers and services

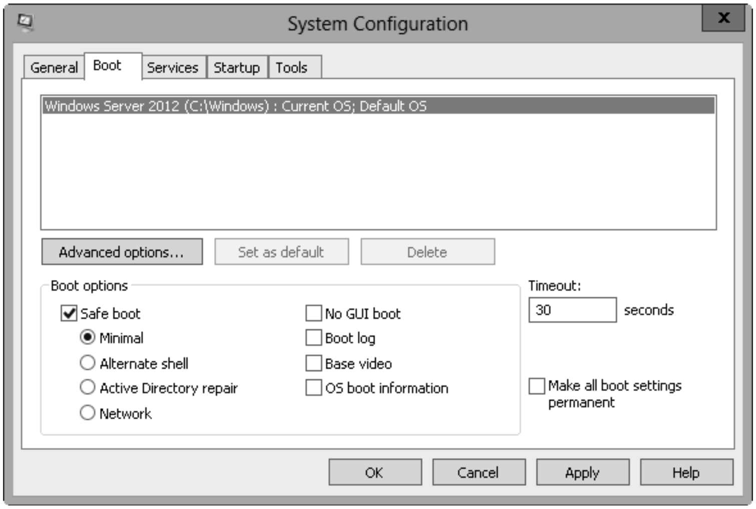
○ Diagnostic startup
Load basic devices and services only

● Selective startup

☑ Load system services
☑ Load startup items
☑ Use original boot configuration

Figure 3-3 Perform a diagnostic or selective startup as part of troubleshooting.

Use the Boot tab options, shown in Figure 3-4, to control the way the individual startup-related processes work. You can configure the computer to start in one of various Safe Boot modes and set additional options, such as No GUI Boot. If after troubleshooting you find that you want to keep these settings, you can select the Make All Boot Settings Permanent check box to save the settings to the boot configuration startup entry.



Windows Server 2012 (C:\Windows) : Current OS; Default OS

Boot options

☑ Safe boot
● Minimal
○ Alternate shell
○ Active Directory repair
○ Network

□ No GUI boot
□ Boot log
□ Base video
□ OS boot information

Timeout: 30 seconds

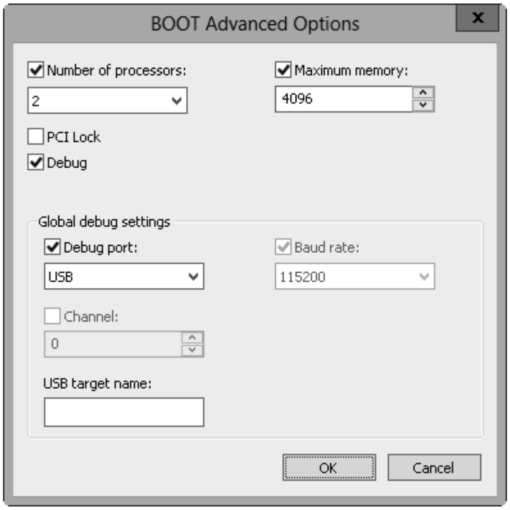
□ Make all boot settings permanent

Figure 3-4 Fine-tune the boot options.

Tapping or clicking the Advanced Options button on the Boot tab displays the BOOT Advanced Options dialog box shown in Figure 3-5. In addition to being able to lock PCI, detect the correct HAL, and enable debugging, you can use the advanced options to do the following:

- Specify the number of processors the operating system should use. You should use this option when you suspect there is a problem with additional processors you installed in a server and you want to pinpoint which processors are possibly causing startup problems. Consider the following scenario: A server shipped with two processors, and you installed two additional processors. Later, you find that you cannot start the server. You could eliminate the new processors as the potential cause by limiting the computer to two processors.

- Specify the maximum amount of memory the operating system should use. You should use this option when you suspect there is a problem with additional memory you installed in a server. Consider the following scenario: A server shipped with 4 GB of RAM, and you installed 4 additional GB of RAM. Later, you find that you cannot start the server. You could eliminate the new RAM as the potential cause by limiting the computer to 4096 MB of memory.



BOOT Advanced Options

☑ Number of processors: 2

☑ Maximum memory: 4096

□ PCI Lock

☑ Debug

Global debug settings

☑ Debug port: USB

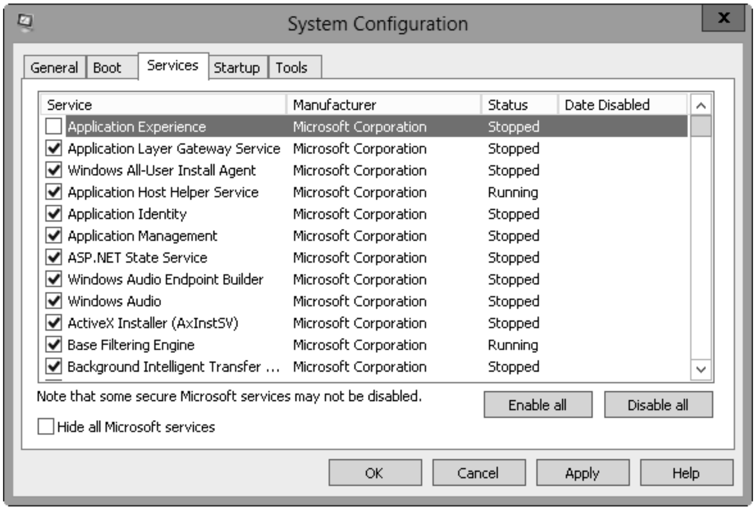
☑ Baud rate: 115200

□ Channel: 0

USB target name:

Figure 3-5 Set advanced boot options as necessary to help troubleshoot specific types of problems.

If you suspect services installed on a computer are causing startup problems, you can quickly determine this by choosing a diagnostic or selective startup on the General tab. After you identify that services are indeed causing startup problems, you can temporarily disable services using the Services tab options and then reboot to see if the problem goes away. If the problem no longer appears, you might have pinpointed it. You can then permanently disable the service or check with the service vendor to see if an updated executable is available for the service. As shown in Figure 3-6, you disable a service by clearing the related check box on the Services tab.



Service	Manufacturer	Status	Date Disabled
☐ Application Experience	Microsoft Corporation	Stopped	
☑ Application Layer Gateway Service	Microsoft Corporation	Stopped	
☑ Windows All-User Install Agent	Microsoft Corporation	Stopped	
☑ Application Host Helper Service	Microsoft Corporation	Running	
☑ Application Identity	Microsoft Corporation	Stopped	
☑ Application Management	Microsoft Corporation	Stopped	
☑ ASP.NET State Service	Microsoft Corporation	Stopped	
☑ Windows Audio Endpoint Builder	Microsoft Corporation	Stopped	
☑ Windows Audio	Microsoft Corporation	Stopped	
☑ ActiveX Installer (AxInstSV)	Microsoft Corporation	Stopped	
☑ Base Filtering Engine	Microsoft Corporation	Running	
☑ Background Intelligent Transfer ...	Microsoft Corporation	Stopped	

Note that some secure Microsoft services may not be disabled.

☐ Hide all Microsoft services

Figure 3-6 Disable services to try to pinpoint the source of a problem.

Similarly, if you suspect applications that run at startup are causing problems, you can quickly determine this using the options on the Startup tab. You disable a startup application by clearing the related check box on the Startup tab. If the problem no longer appears, you might have pinpointed the cause of it. You can then permanently disable the startup application or check with the software vendor to see if an updated version is available.

TROUBLESHOOTING

Remove selective startup after troubleshooting

If you are using the System Configuration utility for troubleshooting and diagnostics, you should later remove your selective startup options. After you restart the computer and resolve any problems, access the System Configuration utility again, restore the original settings, and then tap or click OK.

Working with BCD Editor

The BCD store contains multiple entries. On a BIOS-based computer, you'll see the following entries:

- One Windows Boot Manager entry. There is only one boot manager, so there is only one boot manager entry.
- One or more Windows Boot Loader application entries, with one for each Windows Server 2008 operating system, Windows Vista operating system, or later versions of Windows installed on the computer.
- One legacy operating system entry. The legacy entry is not for a boot application. This entry is used to initiate Ntldr and Boot.ini so that you can boot into Windows XP or an earlier release of Windows. If the computer has more than one Windows XP or earlier operating system, you'll be able to select the operating system to start after selecting the legacy operating system entry.

Windows Boot Manager is itself a boot loader application. There are other boot loader applications, including

- Legacy OS Loader, identified as NTLDR
- Windows Vista or later operating system loader, identified as OSLOADER
- Windows Boot Sector Application, identified as BOOTSECTOR
- Firmware Boot Manager, identified as FWBOOTMGR
- Windows Resume Loader, identified as RESUME

You can directly view and manage the BCD data store using BCD Editor (BCDEdit.exe). BCD Editor is a command-line utility. You can use BCD Editor to view the entries in the BCD store by following these steps:

1. Press and hold or right-click the lower-left corner of the Start screen or the desktop. This displays a shortcut menu.
2. Select the Command Prompt (Admin) to open an elevated command prompt.
3. Enter **bcdedit** at the elevated command prompt.

Table 3-2 summarizes commands you can use when you are working with the BCD data store. These commands allow you to

- Create, import, export, and identify the entire BCD data store.

- Create, delete, and copy individual entries in the BCD data store.
- Set or delete entry option values in the BCD data store.
- Control the boot sequence and the boot manager.
- Configure and control Emergency Management Services (EMS).
- Configure and control boot debugging as well as hypervisor debugging.

TABLE 3-2 Commands for BCD Editor

Commands	Description
/bootdebug	Enables or disables boot debugging for a boot application.
/bootems	Enables or disables Emergency Management Services for a boot application.
/bootsequence	Sets the one-time boot sequence for the boot manager.
/copy	Makes copies of entries in the store.
/create	Creates new entries in the store.
/createstore	Creates a new (empty) boot configuration data store.
/dbgsettings	Sets the global debugger parameters.
/debug	Enables or disables kernel debugging for an operating system entry.
/default	Sets the default entry that the boot manager will use.
/delete	Deletes entries from the store.
/deletevalue	Deletes entry options from the store.
/displayorder	Sets the order in which the boot manager displays the multiboot menu.
/ems	Enables or disables Emergency Management Services for an operating system entry.
/emssettings	Sets the global Emergency Management Services parameters.
/enum	Lists entries in the store.
/export	Exports the contents of the system store to a file. This file can be used later to restore the state of the system store.
/hypervisorsettings	Sets the hypervisor parameters.
/import	Restores the state of the system store using a backup file created with the */export* command.
/mirror	Duplicates a specified entry by mirroring it in the data store.
/set	Sets entry option values in the store.
/store	Sets the BCD store to use. If not specified, the system store is used.

Commands	Description
/sysstore	Sets the system store device. Note that this affects only EFI systems.
/timeout	Sets the boot manager timeout value.
/toolsdisplayorder	Sets the order in which the boot manager displays the tools menu.
/v	Sets output to verbose mode.

Managing the Boot Configuration Data store and its entries

BCD Editor (BCDEdit.exe) is an advanced command-line tool for viewing and manipulating the configuration of the pre-operating system boot environment. Although I discuss tasks related to modifying the BCD data store in the sections that follow, you should attempt to modify the BCD store only if you are an experienced IT pro. As a safeguard, you should make a full backup of the computer prior to making any changes to the BCD store. Why? If you make a mistake, your computer might end up in a nonbootable state and you would then need to initiate recovery.

Viewing BCD entries

Computers can have system and nonsystem BCD stores. The system BCD store contains the operating system boot entries and related boot settings. Whenever you work with the BCD Editor, you will be working with the system BCD store.

On a computer with only one operating system, the BCD entries for your computer will look similar to those in Listing 3-1. As the listing shows, the BCD store for this computer has two entries: one for the Windows Boot Manager and one for the Windows Boot Loader. Here, the Windows Boot Manager calls the boot loader and the boot loader uses Winload.exe to boot Windows Server 2012.

Listing 3-1 Entries in the BCD store on a single boot computer

```
Windows Boot Manager
--------------------
identifier              {bootmgr}
device                  partition=F:
description             Windows Boot Manager
locale                  en-US
inherit                 {globalsettings}
bootshutdowndisabled    Yes
default                 {current}
resumeobject            {5824ba7d-acee-11e1-ba52-cfa3fef36259}
displayorder            {current}
```

```
toolsdisplayorder       {memdiag}
timeout                 30

Windows Boot Loader
-------------------
device                  partition=C:identifier              {current}
path                    \Windows\system32\winload.exe
description             Windows Server 2012
locale                  en-US
inherit                 {bootloadersettings}
recoverysequence        {5824ba7f-acee-11e1-ba52-cfa3fef36259}
recoveryenabled         Yes
allowedinmemorysettings 0x15000075
osdevice                partition=C:
systemroot              \Windows
resumeobject            {5824ba7d-acee-11e1-ba52-cfa3fef36259}
nx                      OptOut
```

BCD entries for Windows Boot Manager and Windows Boot Loader have similar properties. These properties include those summarized in Table 3-3.

TABLE 3-3 BCD entry properties

Property	Description
Description	Shows descriptive information to help identify the type of entry.
Device	Shows the physical device path. For a partition on a physical disk, you'll see an entry such as partition=C:.
FileDevice	Shows the path to a file device, such as partition=C:.
FilePath	Shows the file path to a necessary file, such as \hiberfil.sys.
Identifier	Shows a descriptor for the entry. This can be a boot loader application type, such as BOOTMGR or NTLDR. Or it can be a reference to the current operating system entry or the GUID of a specific object.
Inherit	Shows the list of entries to be inherited.
Locale	Shows the computer's locale setting, such as en-us. The locale setting determines the UI language shown. In the \Boot folder, there are locale subfolders for each locale supported, and each of these subfolders has language-specific UI details for the Windows Boot Manager (BootMgr.exe) and the Memory Diagnostics Utility (MemDiag.exe).
OSDevice	Shows the path to the operating system device, such as partition=C:.
Path	Shows the actual file path to the boot loader application, such as \Windows\System32\winresume.exe.

When you are working with the BCD store and BCD Editor, you'll see references to well-known identifiers, summarized in Table 3-4, as well as globally unique identifiers (GUIDs).

When a GUID is used, the GUID has the following format where each N represents a hexadecimal value:

```
{NNNNNNNN-NNNN-NNNN-NNNN-NNNNNNNNNNNN}
```

Such as:

```
{5824ba7d-acee-11e1-ba52-cfa3fef36259}
```

The dashes that separate the parts of the GUID must be entered in the positions shown.

TABLE 3-4 Well-known identifiers

Identifier	Description
{badmemory}	Contains the global RAM defect list that can be inherited by any boot application entry.
{bootloadersettings}	Contains the collection of global settings that should be inherited by all Windows boot loader application entries.
{bootmgr}	Indicates the Windows boot manager entry.
{current}	Represents a virtual identifier that corresponds to the operating system boot entry for the operating system that is currently running.
{dbgsettings}	Contains the global debugger settings that can be inherited by any boot application entry.
{default}	Represents a virtual identifier that corresponds to the boot manager default application entry.
{emssettings}	Contains the global Emergency Management Services settings that can be inherited by any boot application entry.
{fwbootmgr}	Indicates the firmware boot manager entry. This entry is used on EFI systems.
{globalsettings}	Contains the collection of global settings that should be inherited by all boot application entries.
{hypervisorsettings}	Contains the hypervisor settings that can be inherited by any operating system loader entry.
{legacy}	Indicates the Windows Legacy OS Loader (Ntldr) that can be used to start operating systems earlier than Windows Vista.
{memdiag}	Indicates the memory diagnostic application entry.
{ntldr}	Indicates the Windows Legacy OS Loader (Ntldr) that can be used to start operating systems earlier than Windows Vista.
{ramdiskoptions}	Contains the additional options required by the boot manager for RAM disk devices.
{resumeloadersettings}	Contains the collection of global settings that should be inherited by all Windows resume from hibernation application entries.

When a computer has additional Windows Vista, Windows Server 2008, or later operating systems installed, the BCD store for it has additional entries for each additional operating system. For example, the BCD store might have one entry for the Windows Boot Manager and one Windows Boot Loader for each operating system.

When a computer has a legacy operating system installed, the BCD store has three entries: one for the Windows Boot Manager, one for the Windows Legacy OS Loader, and one for the Windows Boot Loader. Generally, the entry for the Windows Legacy OS Loader will look similar to Listing 3-2.

Listing 3-2 Sample Legacy OS Loader entry

```
Windows Legacy OS Loader
------------------------
identifier:             {ntldr}
device:                 partition=C:
path:                   \ntldr
description:            Earlier version of Windows
```

Although the Windows Boot Manager, Windows Legacy OS Loader, and Windows Boot Loader are the primary types of entries that control startup, the BCD also stores information about boot settings and boot utilities. The Windows Boot Loader entry can have parameters that track the status of boot settings, such as whether No Execute (NX) policy is set for Opt In or Opt Out. The Windows Boot Loader entry also can provide information about available boot utilities, such as the Memory Diagnostics utility.

To view the actual value of the GUIDs needed to manipulate entries in the BCD data store, type **bcdedit /v** at an elevated command prompt.

Creating and identifying the BCD data store

Using BCD Editor, you can create a new, nonsystem BCD data store by using the following command:

```
bcdedit /createstore StorePath
```

Here *StorePath* is the actual folder path to the location where you want to create the nonsystem store, such as:

```
bcdedit /createstore c:\non-sys\bcd
```

On an EFI system, you can temporarily set the system store device using the */sysstore* command. Use the following syntax:

```
bcdedit /sysstore StoreDevice
```

Here *StoreDevice* is the actual device identifier store, such as:

```
bcdedit /sysstore C:
```

Note

The device must be a system partition. Note this setting does not persist across reboots and is used only in cases where the system store device is ambiguous.

Importing and exporting the BCD data store

BCD Editor provides separate commands for importing and exporting the BCD store. You can use the */export* command to export a copy of the system BCD store's contents to a specified folder. Use the following command syntax:

```
bcdedit /export StorePath
```

Here *StorePath* is the actual folder path to which you want to export a copy of the system store, such as:

```
bcdedit /export c:\backup\bcd.dat
```

To restore an exported copy of the system store, you can use the */import* command. Use the following command syntax:

```
bcdedit /import ImportPath
```

Here *ImportPath* is the actual folder path from which you want to import a copy of the system store, such as:

```
bcdedit /import c:\backup\bcd.dat
```

On an EFI system, you can add */clean* to the import to specify that all existing firmware boot entries should be deleted. Here is an example:

```
bcdedit /import c:\backup\bcd.dat /clean
```

Creating, copying, and deleting BCD entries

BCD Editor provides separate commands for creating, copying, and deleting entries in the BCD store. You can use the */create* command to create identifier, application, and inherit entries in the BCD store.

As shown previously in Table 3-4, BCD Editor recognizes many well-known identifiers, including {dbgsettings} used to create a debugger settings entry, {ntldr} used to create a Windows Legacy OS entry, and {ramdiskoptions} used to create a RAM disk additional options entry. To create identifier entries, you use the following syntax:

```
bcdedit /create Identifier /d "Description"
```

Here *Identifier* is a well-known identifier for the entry you want to create, such as:

```
bcdedit /create {ntldr} /d "Earlier Windows OS Loader"
```

You can create the following entries for specific boot-loader applications as well:

- **Bootsector** A real-mode, boot-sector application, used to set the boot sector for a real-mode application
- **OSLoader** An operating-system loader application, used to load a Windows Vista or later operating system
- **Resume** A Windows Resume Loader application, used to resume the operating system from hibernation
- **Startup** A real-mode application, used to identify a real-mode application

Use the following command syntax:

```
bcdedit /create /application AppType /d "Description"
```

Here *AppType* is one of the previously listed application types, such as:

```
bcdedit /create /application osloader /d "Windows 8"
```

You can delete entries in the system store using the */delete* command and the following syntax:

```
bcdedit /delete Identifier
```

If you are trying to delete a well-known identifier, you must use the */f* command to force deletion, such as:

```
bcdedit /delete {ntldr} /f
```

By default, when using the */delete* command, the */cleanup* option is implied, and this means BCD Editor cleans up any other references to the entry being deleted. This ensures that the data store doesn't have invalid references to the identifier you removed. Because entries are removed from the display order as well, this can result in a different default operating system being set. If you want to delete the entry and clean up all other references except the display order entry, you can use the */nocleanup* command.

Setting BCD entry values

After you create an entry, you then need to set additional entry option values as necessary. Here is the basic syntax for setting values:

```
bcdedit /set Identifier Option Value
```

Here *Identifier* is the identifier of the entry to be modified, *Option* is the option you want to set, and *Value* is the option value, such as:

```
bcdedit /set {current} device partition=d:
```

To delete options and their values, use the */deletevalue* command with the following syntax:

```
bcdedit /deletevalue Identifier Option
```

Here *Identifier* is the identifier of the entry to be modified and *Option* is the option you want to delete, such as:

```
bcdedit /deletevalue {current} badmemorylist
```

Note

When you are working with options, Boolean values can be entered in several different ways. For *true*, you can use 1, ON, YES, or TRUE. For *false*, you can use 0, OFF, NO, or FALSE.

To view the BCD entries for all boot utilities and values for settings, type **bcdedit /enum all /v** at an elevated command prompt. This command enumerates all BCD entries regardless of their current state and lists them in Verbose Mode. The additional entries will look similar to those in Listing 3-3 (shown later in the chapter). Each additional entry has a specific purpose and lists values that you can set, including the following:

- **Resume From Hibernate** The Resume From Hibernate entry shows the current configuration for the resume feature. The pre-operating system boot utility that controls resume is Winresume.exe, which in this example is stored in the C:\Windows\system32 folder. The hibernation data, as specified in the *filepath* parameter, is stored in the Hiberfil.sys file in the root folder on the *osdevice* (c: in this example). Because the resume feature works differently if the computer has Physical Address Extension (PAE) and debugging enabled, these options are tracked by the *PAE* and *Debugoptionenabled* parameters.

- **Windows Memory Tester** The Windows Memory Tester entry shows the current configuration for the Windows Memory Diagnostics utility. The pre-operating system boot utility that controls memory diagnostics is Memtest.exe, which in this example is stored in the C:\Boot folder. Because the Memory Diagnostics utility is designed to detect bad memory by default, the *badmemoryaccess* parameter is set to *yes* by default. You can turn this feature off by entering **bcdedit /set {memdiag} badmemoryaccess NO**. With memory diagnostics, you can configure the number of passes using *Passcount* and configure the test mix as BASIC or EXTENDED using *Testmix*. Here is an example: **bcdedit /set {memdiag} passcount 2**.

- **Windows Legacy OS Loader** The Windows Legacy OS Loader entry shows the current configuration for the loading of earlier versions of Windows. The *Device* parameter sets the default partition to use, such as C:, and the *Path* parameter sets the default path to the loader utility, such as Ntldr.

- **EMS Settings** The EMS Settings entry shows the configuration used when booting with Emergency Management Services. Individual Windows Boot Loader entries control whether EMS is enabled. If EMS is provided by BIOS and you want to use the BIOS settings, you can enter **bcdedit /emssettings bios**. With EMS, you can set an EMS port and an EMS baud rate as well. Here is an example: **bcdedit /emssettings EMSPORT:2 EMSBAUDRATE:115200**. You can enable or disable EMS for a boot application by typing **/bootems** followed by the identity of the boot application with the desired state, such as ON or OFF.

- **Debugger Settings** The Debugger Settings entry shows the configuration used when booting with the debugger turned on. Individual Windows Boot Loader entries control whether the debugger is enabled. You can view the hypervisor debug settings by entering **bcdedit /dbgsettings**. When debug booting is turned on, *DebugType* sets the type of debugger as SERIAL, 1394, or USB. With SERIAL debugging, *DebugPort* specifies the serial port being used as the debugger port and *BaudRate* specifies the baud rate to be used for debugging. With 1394 debugging, you can use *Channel* to set the debugging channel. With Universal Serial Bus (USB) debugging, you can use *TargetName* to set the USB target name to be used for debugging. With any debug type, you can use the */Noumex* flag to specify that user-mode exceptions should be ignored. Here are examples of setting the debugging mode: **bcdedit /dbgsettings SERIAL DEBUGPORT:1 BAUDRATE:115200, bcdedit /dbgsettings 1394 CHANNEL:23**, and **bcdedit /dbgsettings USB TARGETNAME:DEBUGGING**.

- **Hypervisor Settings** The Hypervisor Settings entry shows the configuration used when working with the Hypervisor with the debugger turned on. Individual Windows Boot Loader entries control whether the debugger is enabled. You can view the hypervisor debug settings by entering **bcdedit /hypervisorsettings**. When hypervisor debug booting is turned on, *HypervisorDebugType* sets the type of debugger, *HypervisorDebugPort* specifies the serial port being used as the debugger port, and *HypervisorBaudRate* specifies the baud rate to be used for debugging.

These parameters work the same as with Debugger Settings. Here is an example: **bcdedit /hypervisorsettings SERIAL DEBUGPORT:1 BAUDRATE:115200**. You can also use FireWire for hypervisor debugging. When you do, you must set the debug channel, such as shown in this example: **bcdedit /hypervisorsettings 1394 CHANNEL:23**.

Listing 3-3 Additional entries in the BCD data store on a single boot computer

```
Resume from Hibernate
---------------------
identifier              {5824ba7d-acee-11e1-ba52-cfa3fef36259}
device                  partition=C:
path                    \Windows\system32\winresume.exe
description             Windows Resume Application
locale                  en-US
inherit                 {1afa9c49-16ab-4a5c-901b-212802da9460}
recoverysequence        {5824ba7f-acee-11e1-ba52-cfa3fef36259}
recoveryenabled         Yes
allowedinmemorysettings 0x15000075
filedevice              partition=C:
filepath                \hiberfil.sys
debugoptionenabled      No

Windows Memory Tester
---------------------
identifier              {b2721d73-1db4-4c62-bf78-c548a880142d}
device                  partition=F:
path                    \boot\memtest.exe
description             Windows Memory Diagnostic
locale                  en-US
inherit                 {7ea2e1ac-2e61-4728-aaa3-896d9d0a9f0e}
badmemoryaccess         Yes

EMS Settings
------------
identifier              {0ce4991b-e6b3-4b16-b23c-5e0d9250e5d9}
bootems                 Yes

Debugger Settings
-----------------
identifier              {4636856e-540f-4170-a130-a84776f4c654}
debugtype               Serial
debugport               1
baudrate                115200

RAM Defects
-----------
identifier              {5189b25c-5558-4bf2-bca4-289b11bd29e2}
```

```
Global Settings
---------------
identifier              {7ea2e1ac-2e61-4728-aaa3-896d9d0a9f0e}
inherit                 {4636856e-540f-4170-a130-a84776f4c654}
                        {0ce4991b-e6b3-4b16-b23c-5e0d9250e5d9}
                        {5189b25c-5558-4bf2-bca4-289b11bd29e2}

Boot Loader Settings
--------------------
identifier              {6efb52bf-1766-41db-a6b3-0ee5eff72bd7}
inherit                 {7ea2e1ac-2e61-4728-aaa3-896d9d0a9f0e}
                        {7ff607e0-4395-11db-b0de-0800200c9a66}

Hypervisor Settings
-------------------
identifier              {7ff607e0-4395-11db-b0de-0800200c9a66}
hypervisordebugtype     Serial
hypervisordebugport     1
hypervisorbaudrate      115200

Resume Loader Settings
----------------------
identifier              {1afa9c49-16ab-4a5c-901b-212802da9460}
inherit                 {7ea2e1ac-2e61-4728-aaa3-896d9d0a9f0e}

Device options
--------------
identifier              {5824ba7c-acee-11e1-ba52-cfa3fef36259}
description             Windows Recovery
ramdisksdidevice        partition=C:
ramdisksdipath          \Recovery\5824ba7b-acee-11e1-ba52-cfa3fef36259\boot.sdi
```

Table 3-5 summarizes key options that apply to entries for boot applications (BOOTAPP). Because Windows Boot Manager, Windows Memory Diagnostics, Windows OS Loader, and Windows Resume Loader are boot applications, these options apply to them as well.

TABLE 3-5 Key options for boot application entries

Option	Value Description
BadMemoryAccess	When *true*, allows an application to use the memory on the bad memory list. When *false*, applications are prevented from using memory on the bad memory list.
BadMemoryList	An integer list that defines the list of Page Frame Numbers of faulty memory in the system.
BaudRate	Sets an integer value that defines the baud rate for the serial debugger.
BootDebug	Sets a Boolean value that enables or disables the boot debugger.

Option	Value Description
BootEMS	Sets a Boolean value that enables or disables Emergency Management Services.
Channel	Sets an integer value that defines the channel for the 1394 debugger.
DebugAddress	Sets an integer value that defines the address of a serial port for the debugger.
DebugPort	Sets an integer value that defines the serial port number for the serial debugger.
DebugStart	Can be set to ACTIVE, AUTOENABLE, or DISABLE.
DebugType	Can be set to SERIAL, 1394, or USB.
EMSBaudRate	Defines the baud rate for Emergency Management Services.
EMSPort	Defines the serial port number for Emergency Management Services.
GraphicsModeDisabled	Sets a Boolean value that enables or disables graphics mode.
GraphicsResolution	Defines the graphics resolution, such as 1024 by 768 or 800 by 600.
Locale	Sets the locale of the boot application.
Noumex	When set to TRUE, user-mode exceptions are ignored. When set to FALSE, user-mode exceptions are not ignored.
NoVESA	Sets a Boolean value that enables or disables the use of Video Electronics Standards Association (VESA) display modes.
RelocatePhysical	Sets the physical address to which an automatically selected Non-Uniform Memory Access (NUMA) node's physical memory should be relocated.
TargetName	Defines the target name for the USB debugger as a string.
TruncateMemory	Sets a physical memory address at or above which all memory is disregarded.

Table 3-6 summarizes key options that apply to entries for Windows OS Loader (OSLOADER) applications.

TABLE 3-6 Key options for Windows OS Loader applications

Option	Value Description
AdvancedOptions	Sets a Boolean value that enables or disables advanced options.
BootLog	Sets a Boolean value that enables or disables the boot initialization log.
BootStatusPolicy	Sets the boot status policy. It can be *DisplayAllFailures*, *IgnoreAllFailures*, *IgnoreShutdownFailures*, or *IgnoreBootFailures*.

Option	Value Description
ClusterModeAddressing	Sets the maximum number of processors to include in a single Advanced Programmable Interrupt Controller (APIC) cluster.
ConfigFlags	Sets processor-specific configuration flags.
DbgTransport	Sets the file name for a private debugger transport.
Debug	Sets a Boolean value that enables or disables kernel debugging.
DetectHal	Sets a Boolean value that enables or disables hardware abstraction layer (HAL) and kernel detection.
DriverLoadFailurePolicy	Sets the driver load failure policy. It can be *Fatal* or *UseErrorControl*.
Ems	Sets a Boolean value that enables or disables kernel Emergency Management Services.
Hal	Sets the file name for a private HAL.
HalBreakPoint	Sets a Boolean value that enables or disables the special HAL breakpoint.
HypervisorLaunchType	Configures the hypervisor launch type. It can be *Off* or *Auto*.
IncreaseUserVA	Sets an integer value that increases the amount of virtual address space that the user-mode processes can use.
Kernel	Sets the file name for a private kernel.
LastKnownGood	Sets a Boolean value that enables or disables boot to last known good configuration.
MaxProc	Sets a Boolean value that enables or disables the display of the maximum number of processors in the system.
Msi	Sets the MSI to use. It can be *Default* or *ForceDisable*.
NoCrashAutoReboot	Sets a Boolean value that enables or disables automatic restart on crash.
NoLowMem	Sets a Boolean value that enables or disables the use of low memory.
NumProc	Sets the number of processors to use on startup.
Nx	Controls No Execute protection. It can be *OptIn*, *OptOut*, *AlwaysOn*, or *AlwaysOff*.
OneCPU	Sets a Boolean value that forces only the boot CPU to be used.
OptionsEdit	Sets a Boolean value that enables or disables the options editor.
OSDdevice	Defines the device that contains the system root.
Pae	Controls PAE. It can be *Default*, *ForceEnable*, or *ForceDisable*.
PerfMem	Sets the size (in megabytes) of the buffer to allocate for performance data logging.

Option	Value Description
RemoveMemory	Sets an integer value that removes memory from the total available memory that the operating system can use.
RestrictAPICCluster	Sets the largest APIC cluster number to be used by the system.
SafeBoot	Sets the computer to use a Safe boot mode. It can be *Minimal*, *Network*, or *DsRepair*.
SafeBootAlternateShell	Sets a Boolean value that enables or disables the use of the alternate shell when booted into Safe mode.
Sos	Sets a Boolean value that enables or disables the display of additional boot information.
SystemRoot	Defines the path to the system root.
UseFirmwarePCISettings	Sets a Boolean value that enables or disables the use of BIOS-configured Peripheral Component Interconnect (PCI) resources.
UsePhysicalDestination	Sets a Boolean value that forces the use of the physical APIC.
Vga	Sets a Boolean value that forces the use of the VGA display driver.
WinPE	Sets a Boolean value that enables or disables boot to Windows Preinstallation Environment (Windows PE).

Changing Data Execution Prevention and physical address extension options

Data Execution Prevention (DEP) is a memory-protection technology. With DEP enabled, the computer's processor marks all memory locations in an application as nonexecutable unless the location explicitly contains executable code. If code is executed from a memory page marked as nonexecutable, the processor can raise an exception and prevent the code from executing. This behavior prevents malicious application code, such as virus code, from inserting itself into most areas of memory.

For computers with processors that support the nonexecute page protection (NX) feature, you can configure the operating system to opt in to NX protection by setting the *nx* parameter to *OptIn* or opt out of NX protection by setting the *nx* parameter to *OptOut*. Here is an example:

```
bcdedit /set {current} nx optout
```

When you configure NX protection to *OptIn*, DEP is turned on only for essential Windows programs and services. This is the default. When you configure NX protection to *OptOut*, all programs and services—not just standard Windows programs and services—use DEP.

Programs that shouldn't use DEP must be specifically opted out. You can also configure NX protection to be always on or always off using *AlwaysOn* or *AlwaysOff*, such as:

```
bcdedit /set {current} nx alwayson
```

Processors that support and opt in to NX protection must be running in PAE mode. You can configure PAE by setting the *PAE* parameter to *Default*, *ForceEnable*, or *ForceDisable*. When you set *paeState* to *Default*, the operating system will use the default configuration for PAE. When you set *paeState* to *ForceEnable*, the operating system will use PAE. When you set *paeState* to *ForceDisable*, the operating system will not use PAE. You can set *DebugOptionEnabled* to *true* or *false*. Here is an example:

```
bcdedit /set {current} pae default
```

Changing the operating system display order

You can change the display order of boot managers associated with a particular Windows Vista, Windows Server 2008, or later operating system using the */Displayorder* command. The syntax is

```
bcdedit /displayorder id1 id2 … idn
```

Here *id1* is the operating system identifier of the first operating system in the display order, *id2* is the identifier of the second, and so on. Thus, you could change the display order of the operating systems identified in these BCD entries:

```
Windows Boot Loader
-------------------
identifier              {5824ba7f-acee-11e1-ba52-cfa3fef36259}

Windows Boot Loader
-------------------
identifier              {16b857b4-9e02-11e0-9c17-b7d085eb0682}
```

You can do this by using the following command:

```
bcdedit /displayorder {16b857b4-9e02-11e0-9c17-b7d085eb0682}
{5824ba7f-acee-11e1-ba52-cfa3fef36259}
```

You can set a particular operating system as the first entry using */addfirst* with */displayorder*, such as:

```
bcdedit /displayorder {5824ba7f-acee-11e1-ba52-cfa3fef36259} /addfirst
```

You can set a particular operating system as the last entry using */addlast* with */displayorder*, such as:

```
bcdedit /displayorder {5824ba7f-acee-11e1-ba52-cfa3fef36259} /addlast
```

Changing the default operating system entry

You can change the default operating system entry using the */Default* command. The syntax for this command is

```
bcdedit /default id
```

Here *id* is the operating system ID in the boot loader entry. Thus, you could set the operating system identified in this BCD entry as the default:

```
Windows Boot Loader
-------------------
identifier            {5824ba7f-acee-11e1-ba52-cfa3fef36259}
```

You can do this using the following command:

```
bcdedit /default {5824ba7f-acee-11e1-ba52-cfa3fef36259}
```

If you want to use a pre–Windows Server 2008 operating system as the default, you'd use the identifier for the Windows Legacy OS Loader. The related BCD entry looks like this:

```
Windows Legacy OS Loader
------------------------
identifier              {466f5a88-0af2-4f76-9038-095b170dc21c}
device                  partition=C:
path                    \ntldr
description             Earlier Microsoft Windows Operating System
```

Following this, you could set Ntldr as the default by entering the following:

```
bcdedit /default {466f5a88-0af2-4f76-9038-095b170dc21c}
```

Changing the default timeout

You can change the timeout value associated with the default operating system using the */timeout* command. Set the */timeout* command to the desired wait time in seconds, such as:

```
bcdedit /timeout 30
```

To boot automatically to the default operating system, set the timeout to zero seconds.

Changing the boot sequence temporarily

Occasionally, you might want to boot to a particular operating system one time and then revert to the default boot order. To do this, you can use the */bootsequence* command. Follow the command with the identifier of the operating system to which you want to boot after restarting the computer, such as:

```
bcdedit /bootsequence {14504de-e96b-11cd-a51b-89ace9305d5e}
```

When you restart the computer, the computer will set the specified operating system as the default for that restart only. Then, when you restart the computer again, the computer will use the original default boot order.

Index

Symbols

32-bit processing, 4
/32 command parameter, 197–198
64-bit processing, 4–5, 61
  IPv6 addressing and, 900
  registry, 312
/64 command parameter, 197–198
512b disks, 519
512b drives, 264
512e disks, 519
512e drives, 264
1394 debugging, 126
%SystemRoot% folder
  ADMIN$ share, 724–725
%SystemRoot%\System32 directory, 198

A

access control
  auditing and, 779–780
  central access policies, 768–770
  claims-based, 765–770
  DSA functions, 1142
  mechanisms for, 1138
  through SAM, 1139
access permissions. *See also* **permissions**
  basic permissions, 753–757
  on shares, 748–763
access policies
  central, 766, 768–770
  global object access policy, 778–779
access tokens
  for administrator users, 360
  application, 359–362
  for legacy applications, 361
  logon IDs, 360
account policies
  Account Lockout Policy, 1346, 1348–1349, 1353
  configuring, 1346
  Kerberos Policy, 1346–1347, 1349–1350
  local policies, 1346, 1355
  Password Policy, 1346–1348
  password settings policy, 1350
  secondary account policy settings, 1346
  user account policies, 1345–1350
  user rights, assigning, 1355–1357
accounts. *See also* **computer accounts; groups; user accounts**
  Account Lockout Policy, 1404
  allowing or denying in Password Replication Policy, 1338–1340
  capabilities, built-in and assigned, 1354
  credentials, resetting, 1342–1343
  deleted, recovering, 1385–1386
  placing in OUs, 1310–1311
  prepopulating, 1340–1341
  renaming, 1404–1405
  Resultant Set of Policy, 1341–1342
ACEs (access control entries), 1360
ACLs (access control lists), 1136
ACPI 4.0 and ACPI 5.0, 103–104
  global power states, 106–107
ACPI (Advanced Configuration and Power Interface), 103, 314
  cooling modes, 104
  managing settings, 107
  power states, 106–107
  processor idle sleep states, 105
  processor performance states, 105
  Suspend State setting, 108
ACPI BIOS, 286, 298
AC Recovery setting, 107
Action Center
  automated maintenance, managing, 673
  checking for solutions, 295
  device installation failure solutions, 272
  opening, 295
  Reliability Monitor, 438
  View Reliability History link, 295
Active/Active controller model, 500
Active/Active devices, 500
active cooling, 104

Active Directory
accounts. *See* accounts
administrative access, 1220–1221, 1226
applications with write access, 1317
architecture, 1135–1160
authentication, 1175–1196
authoritative restores, 863–865
automated trust anchor distribution and rollover, 1036
backing up and restoring, 859–868
BitLocker recovery information, 600–601
built-in accounts, 1375
central access rules, 766
clients, connecting, 1276
configuration information in, 304
critical-volume backups, 862
database and log file storage, 1273, 1286
database layer, 1141
data distribution, 1159–1160
data store, 1142–1150
data table, 1149
delegation records, 1047
designing, 1216
DHCP server authorization, 960, 962–963, 999
DHCP services, managing, 945
diagnostics data, 459
directory service component, 1139–1147
directory service polling interval, 1103
Directory System Agent, 1141–1142
directory tree, 1152–1153. *See also* directory tree
Distributed File System use, 1243–1244
DNS information, replicating, 1030
DNS, interdependence with, 40–41
DNS server support, 1047
DNS with, 1017, 1047–1051
domain and forest functional levels, 41–43
domain architecture, designing, 31
domain environment, 1161–1214
domains, 1152. *See also* domains
domain trusts, 41
Exchange Server, integration, 1168
existing infrastructure, assessing, 1221
extending, 1278
Extensible Storage Engine, 1142–1147
federated forest design, 1188
File Replication Service use, 1241–1243
forest root zones, 1050
forests, 1153–1154. *See also* forests
functional levels, 1171–1175
global catalog data replication, 1166
Global Resource Properties, refreshing, 770
Group Policy and, 1228
implementation planning, 1216–1221
inheritance of permissions, 1312
installing from media, 1294–1297
Kerberos authentication, 1179–1180
LDAP, 1140, 1164
legacy hooks to NetBIOS over TCP/IP interface, 1114
link table, 1149
log files, 1149
logical layer, 1150–1160
in LSA, 1137–1139
MAPI support, 1141
metadata, cleaning up, 1304
Microsoft DNS, 38
namespace, designing, 40–41
namespaces, 1157–1159
network management, 33
network traffic related to, 1233
nonauthoritative restores, 861–863
object life cycles, 1145–1147
objects, 1136, 1141, 1151–1152. *See also* objects
operations masters, 1200–1214
organizing, 1215–1232
partitions, 1157–1159
physical layer, 1135–1150
planning, 36–44, 1161–1162
postinstallation tasks, 1287–1288
primary data file, 1148–1150
reason codes for in-progress replication, 1398–1399
recovering, 1274–1275
Remote Desktop User group, 179
remote servers, connecting to, 202–203
replication. *See* replication
replication latency, 1213
REPL interface, 1140
root domain, 1153
SAM interface, 1141
schema, 43, 1142, 1143, 1286
security descriptor table, 1149
security infrastructure, 1136
server roles, 43–45
shares, publishing in, 721, 741–742
sites, 44, 1219
SRV records, 1091
Sysvol, 1240–1246
tombstone lifetime, 861
top-level overview, 1136
TPM and BitLocker recovery extensions, 600
transactions, 1143
trees, 40
trust relationships, 907
trusts, 1154–1156, 1175–1196

Active Directory (*continued*)
uninstalling, 1302–1307
user management, 43
zone replication, 1074
zones. *See* zones, DNS
Active Directory Administrative Center, 141
Active Directory Recycle Bin, enabling, 1385
central access policies, preparing for, 768
computer accounts, disabling, 1382
deleted objects, recovering, 1385–1386
domain functional level, raising, 1174
Dynamic Access Controls node, 767
forest functional level, raising, 1174–1175
groups, creating, 1374–1375
groups, deleting, 1377
groups, finding, 1378
OUs, creating, 1309
password settings policies, creating, 1350–1354
passwords, resetting, 1370
user accounts, deleting, 1368
user accounts, moving, 1368
Active Directory Domains And Trusts, 141
domain functional level, raising, 1175
domain naming master, locating, 1205
domain naming master role, transferring, 1205
forest functional level, raising, 1175
trusts, establishing, 1193–1195
trusts, examining, 1189–1192
trusts, validating, 1196
UPN suffix, changing, 1176–1177
Active Directory Domain Services Configuration Wizard, 1048–1050, 1280–1293
Active Directory, removing, 1303–1307
Adprep.exe, 1279–1280
DNS delegation, 1292–1293
domain controllers, demoting, 1303–1307
domain controllers in existing domain, creating, 1281–1289
domains in new forest, creating, 1289–1291
exporting configuration settings, 1286
installation from media, 1294–1297
new domains and domain trees, creating, 1291–1293
prerequisite checks, 1326
RODCs, installing, 1325–1329
testing, 1274
verification errors, 1282
Active Directory Domain Services Installation Wizard, 1332–1335
Active Directory Group Policy, 1388–1389. *See also* **Group Policy**
Active Directory–integrated zones, 1047. *See also* **zones, DNS**
Active Directory zone replication, 1074
Allow Any Authenticated User To Update DNS Records With The Same Owner Name option, 1084
GlobalNames zone, 1093
NS records, 1088
replication scope, 1062–1063, 1066–1067, 1096
secure dynamic updates, 1078–1079
signed zones, 1079
Active Directory Recycle Bin, 1385–1386
enabling, 1385
forest functional level and, 1173, 1174
object deletion with, 1145
objects, recovering from, 1385–1386
Active Directory Rights Management Services, 141
Active Directory Schema snap-in
custom console, adding to, 1169
installing, 1169
object schemas, editing, 1169–1170
schema, changing, 1203–1204
schema master, locating, 1204
schema master role, transferring, 1204
Active Directory Sites And Services, 141
bridgehead servers, configuring, 1460–1461
domain controllers, moving to sites, 1447
global catalog servers, designating, 1166–1168
global replication, configuring, 1453
intersite replication, modifying, 1466–1468
ISTG, determining, 1458
site-link bridging, configuring, 1455–1456
site-link object Options attribute, configuring, 1461–1462
site-link replication schedule, configuring, 1454
site links, creating, 1450–1451
sites, creating, 1444–1445
subnets, creating and associating with sites, 1445–1446
universal group membership caching, configuring, 1177–1178
Active Directory Users And Computers, 141, 1366
account options, setting, 1361–1364
Advanced Features view, 1360
capabilities, 192
computer account passwords, resetting, 1383
computer accounts, creating, 1379–1380
computer accounts, disabling, 1382
computer accounts, moving, 1382
computer account status, checking, 1384
delegating administration of domains and OUs, 1312–1314
groups, adding members, 1377

Active Directory Users And Computers (*continued*)
groups, creating, 1374–1375
groups, deleting, 1377
groups, finding, 1378
infrastructure master role, transferring, 1212
OU properties, setting, 1309–1310
OUs, creating, 1307–1308
Password Replication Policy, editing, 1338–1340
password settings policies, creating, 1350
passwords, resetting, 1342–1343, 1370
PDC emulator role, transferring, 1211–1212
queries, saving and reusing, 1378
RID master role, transferring, 1209
shared resources, finding, 721
user account profile options, setting, 1364–1366
user accounts, creating, 1357–1361
user accounts, deleting, 1368
user accounts, enabling and disabling, 1368
user accounts, moving, 1368
user accounts, renaming, 1369–1370
user accounts, unlocking, 1367, 1371
active partitions, 71, 525
AD CS (Active Directory Certificate Services) role, 230
Add-ADDSReadOnlyDomainControllerAccount cmdlet, 1335
Add Hardware Wizard, 292–294
Add Or Remove Snap-Ins dialog box, 206, 208
address space size limits, 374
Add Roles And Features Wizard, 199, 238–241, 497
Before You Begin page, 239
BitLocker, installing, 602
DHCP Server service, installing, 959–961
DNS Server service, installing, 1052–1053
Group Policy Management Console, installing, 1397
IP Address Management (IPAM) Server feature, adding, 946
notifications, 242–243
Routing And Remote Access, installing, 1011
server management tools, installing, 144–145
WINS Server, installing, 1117
AD DS (Active Directory Domain Services), 230, 303, 1276
Active Directory Domain Services Configuration Wizard, 1280–1293
administrator privileges and installation requirements, 1278
binaries, installing, 1276
configuring, 1277
DNS zones, 1027, 1039–1040
domain controllers, hardware and configuration, 1272–1274
domain controllers, installing from media, 1294–1297
implementing, 1271–1314
installing, 1276–1297
log file properties, examining, 1150
monitoring performance, 440
postinstallation tasks, 1287–1288
preinstallation considerations, 1271–1276
SANs, volumes on, 1274–1275
uninstalling, 1302–1307
AD FS (Active Directory Federation Services) role, 230
AD LDS (Active Directory Lightweight Directory Services) role, 230
Admin Approval Mode, 355–359
security settings, 356–357
administration
of domains and OUs, delegating, 1311–1314
fine-tuning approach, 33
interface for, 191–192. *See also* MMC (Microsoft Management Console)
personal information, protecting, 34
standards for, 34
administration tools, 137–150. *See also* **console tools**
administrative wizards, 138
alternate credentials for, 143
availability, 198–201
command-line utilities, 138, 145–150
Computer Management, 160–162
Control Panel, 138, 140–141, 162–165
custom, building, 203–214
desktop, 168–169
graphical tools, 138, 141–145
installing, 199
opening, 198
opening in author mode, 195
Remote Desktop, 176–189
Remote Desktop Services Manager, 189–190
running, 137, 197
Server Manager, 150–159. *See also* Server Manager
Settings charm, 139
System console, 165–167
taskbar, 169–174
toolbars, 175–176
Windows PowerShell cmdlets, 139. *See also* Windows PowerShell
Administrative Templates, 1390
ADMX files, 1392–1393
Administrator account
renaming, 1404
strong passwords, 81
administrator applications, 361
administrators
account use policies, 1221
administrative rights, delegating, 1226–1228

administrators (*continued*)
- auditing actions of, 1221
- delegated administrator users, 1319
- directory structure changes, 1220
- domain administrators, 1155
- enterprise administrators, 1155
- Enterprise Admins, 1218. *See also* Enterprise Admins group
- file ownership, 662
- GPO creation rights, 1406
- inheritance, blocking, 1415
- inheritance, enforcing, 1416–1417
- permissions for Group Policy, delegating, 1406–1411
- permissions for registry changes, 324
- Schema Admins, 1218. *See also* Schema Admins group
- security tokens, 305
- users, groups, and computers, managing, 1345–1386

Administrators group
- Active Directory schema, viewing, 1171
- disk quotas and, 665
- domainwide privileges, 1220
- privileges, 137
- remote logon capabilities, 179

administrator user accounts, 349
- access tokens, 360
- Admin Approval Mode settings, 356–357
- UAC prompts, 354–355

ADMT (Active Directory Migration Tool), 1219, 1224

Adprep.exe, 1279–1280
- /gpprep, 1281
- for RODC installation preparation, 1323, 1324

AD RMS (Active Directory Rights Management Services) role, 230

ADSI Edit
- DSHeuristics attribute, modifying, 1144
- RID pool ceiling, removing, 1208
- schema updates, initiating, 1145

Advanced Boot Options menu, 111

Advanced Format hard drives, 263–264, 519

Advanced Sharing Settings, 717–718

advanced startup modes, 111

alerts
- performance alerts, 154
- performance counter alerts, 425, 470–471
- security alerts, 32

Allowed RODC Password Replication Group, 1337

alternate IP addresses, 913, 917–919

AMD-V (AMD Virtualization), 508

anti-malware, disabling at startup, 869

antivirus software, updating, 32

APIPA (Automatic Private IP Addressing), disabling, 919

Appcmd, 146

application data
- backing up, 841
- recovering, 852–857

Application Information service, 360

Application log, 405
- shadow copy events, 855

application logs, 405

application manifests, 362–363

application partitions, 38

applications
- abnormal process statuses, 390
- access tokens, 359–362
- administrator applications, 361
- application objects, 313
- application types, 313–314
- backing up, 484
- cluster aware, 46
- compatibility testing, 22, 46
- compliant vs. legacy, 359
- events associated with, 417
- exiting, 390
- installation detection, 362
- installation security settings, 366–367
- integration testing, 46
- integrity, 359–368
- machine-wide settings in registry, 315–316
- managing, 162
- monitoring, 388–390
- network applications, 22
- notifications for, 172
- vs. processes, 378
- processes, tracking, 389–390
- processing-affinity settings, 106
- processor-scheduling optimization, 370–371
- publisher verified and not verified, 363
- registry settings, removing, 336–338
- repairing, 337
- RODC compatibility, 1317
- rollback data, 337
- run behavior settings, 366–367
- run levels, 305, 359, 362–366
- running always as administrator, 365–366
- running once as administrator, 364–365
- security context, 360
- security tokens, 305, 359
- in Startup folder, 172–173
- uninstalling, 335–336
- uninstall utilities, 335–336
- user applications, 361
- user-mode, 1135

Application Server role, 231

application servers, planning usage, 39

apps, 349
architecture team, 12
Arp, 146
ARP (Address Resolution Protocol), 943
asymmetric logical unit access controller model, 500
auditing
administrator and user actions, 1221
advanced, 773–775
audit failure events, 410–411
audit success events, 410
basic, 771–773
claims-based access controls and, 779–780
configuring, 771
DHCP events, 998–1001
domain controllers, default policies for, 1405
file and folder access, 770–781
file screening, 806–807
global object access policy, 771, 778–779
logon failures, 1367
registry, 778
registry access, 345–347
Security log, monitoring, 781
targeting, 780
auditing policies, 57
authentication, 1138
across domain boundaries, 1183–1186
across forest boundaries, 1186–1189
against RODCs, 1318
computer clock synchronization tolerance, 1366
constrained delegation, 1197
delegated service or computer account, 1198–1200
delegated user account, 1197–1198
delegating, 1196–1200
design considerations, 1175–1196
of DNS information, 1036
domains, within and between, 1236
domainwide, 1218
failures, troubleshooting, 259
forwarding tickets, 1197
Kerberos, 23, 1178–1181
mechanisms for, 1138
mutual, 1179–1180
NTLM, 1178–1179, 1187
proxy tickets, 1197
of remote computers, 179
requests, trust path, 1156
through SAM, 1139
security tokens, 1175–1177
selective, 1218
shared-secret model, 1180–1181
startup, 593–595, 613–614
TPM modes, 584–585
trust relationships, 41
universal group membership caching, 1176–1177
universal groups, 1175–1178
authentication keys, 588
authorization
cross-forest authorization, 1187
author mode (MMC), 194–196
automated maintenance, 672–680
fragmentation analysis and disk optimization, 680–682
Automatic Black Hole Router Detection, 880
Automatic Dead Gateway Retry, 880
Automatic Updates, 8
Auto Power On setting, 108
availability
99 percent uptime, 45
99.9 percent uptime, 45
99.99 percent uptime, 54
compatibility testing and, 46
DHCP servers, 952–957
disaster planning for, 821
hardware, 47–60
high availability defined, 45
online backups, 46
operational support for, 53–58
planning for, 45–60
predeployment planning, 58–60
software, 45–47
split scopes and, 957
structures and facilities for, 49–52
availability technologies, 505–506

B

background processes, monitoring, 388–390
background programs, 173
background services, processor scheduling, 371
Backup Operators group, 1220
backups
Active Directory, 859–868
application data backups, 841
archive attribute, 834
backup servers, 826–827
considerations for, 831–833
copy backups, 835
critical-volume backups, 862
daily backups, 835
data considerations, 840–841
data file backups, 832
DHCP database, 1010–1011
differential backups, 835–836
disaster planning, 821–826

backups (*continued*)
disaster preparedness procedures, 826–830
of domain controllers, 1274
exclusions, 842
full server backups, 862
of GPOs, 1438–1439
incremental backups, 835–836
media backups, 1294
media rotation and media sets, 836–837
normal backups, 835–836
one-time backups, 846–850
online backups, 46
performing, 826–827
per-server backups, 826–827
planning, 24–25, 55
planning questions, 831
registry, 334–335
scheduling, 841–846
snapshots, 483
status, viewing, 851
stopping, 845–846
storage location, 822, 840–841, 844–845, 847–848
strategies for, 830–837
system file backups, 832
system state, 335, 1274–1275, 1294, 1296–1297
techniques, selecting, 833–834
timing, 833
tracking, 850–851
types, 835–836, 843
for virtual machines, 513
volumes, specifying, 841–842
Wbadmin, 837, 840
Windows Server Backup, 837–851
of WINS database, 1131
Backup Schedule Wizard, 841–846
basic disks, 525. *See also* **dynamic disks**
converting to dynamic, 526–527
GPT partitions on, 549–552
managing, 514–519, 526–527
MBR partitions, managing, 533–549
volumes, extending, 543–546
working with, 525–526
BCD (Boot Configuration Data)
application types, 313–314
objects, 313
registry settings, 313
stores, 313
BCD Editor (BCDEdit.exe), 111, 117–119, 146
BCD store entries, creating, copying, deleting, 123–124
BCD store, importing and exporting, 123
cleaning up references, 124
commands for, 118–119
nonsystem data store, creating, 122
BCDEdit tool, 313
BCD registry, 111
BCD store, 111
additional operating systems entries, 122
boot application entries, 128–129
boot-loader application entries, 124
boot sequence values, 133–134
commands for, 117–119
creating, 122
default operating system entry, 133
default timeout value, 133
DEP options, 131–132
entries, 117
entries, creating, copying, and deleting, 123–124
entries, viewing, 119–122
entry option values, setting, 125–131
entry properties, 120
GUIDs, 120–121
identifier entries, 124
importing and exporting, 123
legacy operating system entries, 122
managing, 119–134
nonsystem, 119
operating system display order, 132
physical address options, 131–132
system, 119
viewing, 117–119
well-known identifiers, 121
Best Practices Analyzer, 154
binary source files
accessing, 241
for DHCP Server role, 959–960
managing, 245–250
removing, 144, 497
restoring, 247–248
retrieving, 499
BIND (Berkeley Internet Name Domain) version 8.1.2, 1047
BIOS-based computers
BCD registry, 111
BCD store entries, 117
boot facilities, 110
disk-partitioning styles, 109–110
installation of operating system on, 71–72
TPM validation-profile settings, 593
BIOS (Basic Input Output System), 103
BitLocker Drive Encryption, 8, 233, 583–587
AES with 128-bit encryption, 587
BitLocker Drive Encryption console, 603
BitLocker Drive Encryption service, 615
boot settings for, 109

BitLocker Drive Encryption (*continued*)
changes from earlier versions, 587
configuring, 601–619
data-recovery agents, 587
deploying, 596–601
disk configuration, 597–600
duplicate keys and PINs, 615
enabling, 602–605
encrypted volumes, viewing, 605–606
on fixed data drives, 606–608
Group Policy settings, 598–600
installing, 602
integrity checks, 612–613
locked computers, 617
management options, 616–617
Microsoft BitLocker Administration and Monitoring, 617
modes, 584–586
without Network Unlock, 834
on operating-system volumes, 611–615
provisioning, 596
recovering data, 617–618
recovery information, 600–601
recovery keys, 613
recovery passwords, 605
on removable data drives, 608–611
secure boot, 593–594
setting up, 602
Smart Card Certificate Only mode, 586
with smart cards, 615
startup authentication, 593–594
Startup Key Only mode, 586
startup keys, 613
startup PINs, 615
status on volumes, 605–606, 615
TPM modes, 584–585
TPM use, 584
troubleshooting, 615–618
turning off, 618–619
unlocking computer, 617–618
unlock passwords, 586
versions, 597
BitLocker Network Unlock, 233
BitLocker To Go, 583
BITS (Background Intelligent Transfer Service), 232
BitsTransfer cmdlet, 486
blocked files, 797. *See also* **file screening**
exception paths, 799
block storage devices, 490
Boolean values, alternate entries, 125
BOOT Advanced Options dialog box, 115
boot applications, 111
key BCD store entry options, 128–129
boot configuration, 101–134
managing, 111–119
boot debugging, 126
configuring, 118
Boot Drive Order setting, 109
boot environment
boot loader applications, 117
conceptual view, 110
configuring, 101–134
failures, registry information, 320
logging at startup, 869
sequence, controlling, 118
services issues, 115–116
troubleshooting, 103–107
boot files, validating, 584. *See also* **BitLocker Drive Encryption**
booting. *See* **startup**
Boot.ini, 110
boot manager, 111
boot failures, 858
controlling, 118
display order, 132
mirrored volumes in, 560, 563
sealing, 570–571
boot partition, 71, 525
BOOTP (Bootstrap Protocol), 941
boot sector, 522
boot sector applications, 117, 124, 314
boot settings
advanced, 115
in firmware, 109
for startup-related processes, 114
Boot To Hard Disk Drive setting, 109
Boot To Network setting, 109
Boot To Removable Devices setting, 109
boot volumes
drive letter, changing, 540
mirroring, 559–563
bottlenecks
defined, 448
disk I/O, 452–454
memory, 448–451
network, 454–457
processor, 451–452
BranchCache, 233
data deduplication interoperability, 707
enabling, 731, 733
BranchCache cmdlet, 486
BranchCache For Network Files role service, 488–489, 731
data deduplication techniques, 489
branch caching, 488–489

bridgehead servers, 44, 1234
automatic compression, 1219
configuring, 1460–1461
designating, 1255, 1447, 1459
inbound replication load, 1321
intersite replication, 1253–1260
Inter-Site Topology Generator, 1253
listing, 1459
load balancing, 1239–1240
multiple, 1258–1259, 1459
processing load, 1458
server object Options attribute, editing, 1466–1468
bridges, 890
broadcasts, 887–888
browsing, testing, 933
Builtin container, 1288, 1375
business systems, predeployment planning, 58–60

C

Cache.dns file, 1039, 1040
CacheLockingPercent registry key, 1019
Cache Manager, 309
caching
branch caching, 488–489
credentials, 1318–1319
disk write caching, 520
resource records, 1018, 1025
shares, 739
universal group membership, 1176–1177
CALs (client access licenses), 63–64
CEIP (Customer Experience Improvement Program), 152
centralized network administration, 24
central logging servers, 422–424
Certification Authority, 141
change journals
NTFS, 640–643
records, 642
summary statistics, 640–641
change management, 35, 54
charms, 139
Check Disk, 871
data integrity errors, scanning for, 673–675
enhanced and legacy scan and repair, 674
running interactively, 675–677
self-healing and, 648
chipset firmware, 103
ChkDsk (Chkdsk.exe)
analysis mode, 676
bad sectors, marking, 679–680
FAT volumes, analyzing, 678
NTFS volumes, analyzing, 678–679
parameters, 677
repairing volumes, 679–680
syntax, 676
CIDR (classless inter-domain routing), 887
notation, 891–892
CIFS (Common Internet File System), 1245
Cipher, 587
claims-based access controls, 765–770
auditing, extending to, 780
claims-based policy, 766–767
Class A networks
IPv4 addressing, 884, 898
subnetting, 893–894
Class B networks
IPv4 addressing, 884–885, 898
subnetting, 895–896
Class C networks
IPv4 addressing, 885, 898
subnetting, 896–897
classful networks, 887. *See also* **networking**
host IDs, 889
network number, 889
network prefixes, 892
subnet masks, 891
classification, file, 807–808
classless networks, 887
class registrations, 319
client computers. *See also* **DHCP clients; DNS clients**
licensing, 63–64
Client for Microsoft Networks, 76
Client for NFS, 233
Cloneable Domain Controllers group, 1298
cloning
applications, evaluating for, 1298
configuration file, generating, 1298
deployment, finalizing, 1300
import-and-rename process, 1298–1300
troubleshooting, 1301–1302
virtualized domain controllers, 1297–1302
clustering, 48, 506
DHCP services, 952
SANs with, 492–493
volume shadow copies on, 788
command line
ChkDsk, running, 676–680
consoles, opening, 199
data, compressing and decompressing, 659
disk quotas, checking, 669
focus, setting, 202
Optimize Drives, running, 683
performance monitoring from, 471–474
registry, backing up, 334

command line (*continued*)
registry, managing, 333–334
shadow copies, configuring, 792–796
tasks, specifying, 223–224
trace logs, analyzing, 475
WINS database, compacting, 1130–1131
command-line utilities, 145–150, 191–192
in Windows PE, 85–88
command prompt
accessing during installation, 85–88
components, installing, 250–260
components, removing, 260–261
elevated, 247
Safe Mode With Command Prompt startup mode, 869
command sources, specifying, 222
commit limit, 373, 385
tracking, 375
virtual memory and, 374
Compact (Compact.exe), 659
compatibility
checking, 350
issues with, 351
compatibility databases, 362
compatibility mode, 361
compliant applications, 359
application manifests, 362–363
UAC functions, 360
component manifest (component.man) files, 280
components
component names, 251–256
installing, 248–249
installing at command prompt, 250–260
machine-wide settings in registry, 315
removing at command prompt, 260–261
repairing, 248–249
status, tracking, 256–257
uninstalling, 335–336
compound identities, 765
Compound TCP, 880
compressed (zipped) folders, 659–661
compression
chunk compression, 705, 706
compressed (zipped) folders, 659–661
file-based, 656–661
IPv6 address block notation, 901
NTFS compression, 656–659
computer accounts
creating, 1379–1380
deleting, 1382
disabling, 1382
domains, joining to, 1381
group memberships, 1384
managed, 1379, 1380
managing, 1379–1384
moving, 1382
password, resetting, 1383
password/trust problems, 1383–1384
pre–Windows 2000 computers, 1379
remote, managing, 1382–1383
standard, 1379
troubleshooting, 1383–1384
Computer icon, 168
Computer Management, 141, 160–162, 193
Computer Management Services And Applications tools, 162
connecting to another computer, 731
defragmentation, configuring, 681–682
Event Viewer add-in, 409
Optimize Drives, running, 683
remote computer settings, accessing, 279
Routing And Remote Access Services, 1011–1012
shadow copies, configuring, 786–789
shadow copies, managing, 786–791
share permissions, configuring, 744–748
shares, accessing, 726
shares, creating, 726, 731–735
shares, publishing, 741
storage tools, 161
system tools, 160–161
Computer Management Services And Applications tools, 162
computers. *See also* **remote computers; system;** *See also* **servers**
central management, 1387
delegated authentication, authorizing, 1198–1200
desktop-class, 101, 264
Directory Services Restore Mode password, 1284
effective access, determining, 1360–1361
events associated with, 417
Group Policy Refresh Interval For Computers policy, 1427
Group Policy settings, 1389
Local Group Policy, 1388–1389
locked, 834
managing, 191. *See also* MMC (Microsoft Management Console)
network speed, determining, 1428
passwords reset disks, 1371–1373
physical access, securing, 569. *See also* BitLocker Drive Encryption; TPM (Trusted Platform Module) Services
reliability history, 295
renaming, 1225
security templates, 1424–1426
software settings, 1389

computers (*continued*)
specifying which to manage, 207–208
time synchronization, 1210–1211
user rights, assigning on, 1356–1357
Windows settings, 1389–1390
Configure A DNS Server Wizard
large networks, configuring, 1060–1065
small networks, configuring, 1056–1060
starting, 1056
console root, 196
default, 203–204
folders, adding, 206
renaming, 204
consoles
author mode options, 194
availability, 198–201
command line, opening from, 199
creating, 203–205
customized views, allowing, 212
customizing, 197
defined, 192
directory for, 198
existing, basing custom design on, 204
folders in, 206–207
initial view, setting, 210–211
mode, changing, 195, 211–212
nodes, 193
opening in author mode, 195
restricting authoring, 195
saving, 195
snap-ins, adding, 205–210
starting, 197
vs. tools, 193
user changes, preventing, 212
user-mode levels, 194
views, saving to Favorites, 224–225
window, renaming, 204
console tools
building, 203–214
icon for, setting, 212–213
.msc file names, 200–201
naming, 214
publishing and distributing, 227
save options, 214
saving, 210–214
taskpads, 215–227
user options, limiting, 218
windows, multiple, 204–205
containers
Builtin, 1288, 1375
Computers, 1289
Configuration, 1157
Domain Controllers, 1289
ForeignSecurityPrincipals, 1289
Forest Root Domain, 1157
GPOs, linking, 1402, 1411
Password Settings Container, 1345–1346
Schema, 1158
Users, 1289
content, classifying, 807
Control Panel, 138, 162–165
accessing, 140, 162
Advanced Sharing Settings page, 718
BitLocker Drive Encryption console, 603, 615–617
Category Control Panel view, 162–163
Folder Options utility, 163–165
Network And Sharing Center, 878
Notification Area Icons page, 173–174
opening, single-click/tap and double-click/tap, 164
searching, 163
Standard Control Panel, 162
System console, 165–168
taskpad view, 215
Uninstall Or Change A Program utility, 335–336
utilities, 140–141, 191, 215
control sets at last successful boot, 317
Convert command, 531–532
cooling modes, 104
copy backups, 835
copying and moving items to desktop, 168
counters, performance, 436–437, 439
adding, 441–442
alerts on, 425, 470–471
data, collecting from, 462–464
Memory\Available Bytes, 449
Memory\Commit Limit, 449
Memory\Committed Bytes, 449
Memory\Page Faults/Sec, 449
Memory\Pages Input/Sec, 450
Memory\Pages Output/Sec, 450
Memory\Pages/Sec, 449
Memory\Pool Nonpaged Bytes, 450
Memory\Pool Paged Bytes, 450
Network Interface\Bytes Received/Sec, 455
Network Interface\Bytes Sent/Sec, 455
Network Interface\Bytes Total/Sec, 455
Network Interface\Current Bandwidth, 455
Paging File\%Usage, 450
Paging File\%Usage Peak, 450
Physical Disk\Avg Disk Queue Length, 450
PhysicalDisk\Avg. Disk Read Queue Length, 454
Physical Disk\Avg Disk Sec/Transfer, 451
PhysicalDisk\Avg. Disk Write Queue Length, 454
PhysicalDisk\Current Disk Queue Length, 453

counters, performance (*continued*)
PhysicalDisk\Disk Reads/Sec, 454
Physical Disk\%Disk Time, 450
PhysicalDisk\%Disk Time, 453
PhysicalDisk\Disk Writes/Sec, 454
Processor\Interrupts/Sec, 452
Processor\%Privileged Time, 452
Processor\%Processor Time, 452
Processor\%User Time, 452
System\Processor Queue Length, 452
CPUs
of domain controllers, 1272
per-process usage, 429–431
problems with, 94–95
process usage, 390, 393
throttling, 383, 384
usage statistics, 383–385, 387
crash dump partition, 71, 526
Create A Shared Folder Wizard, 731
Create Custom View dialog box, 415
Create New Data Collector Set Wizard, 460–462
Create Shadow command, 793
credentials. *See also* **permissions; privileges**
cached, 1366
caching on RODCs, 1318–1319. *See also* Password Replication Policy
for component management, 259–260
stored, 260
critical events, 410
cryptographic keys, wrapping and binding, 570
c-states (processor idle sleep states), 105
Ctrl+Alt+Delete key combination, 94, 871
current commit charge, 373, 385
tracking, 375

D
daily backups, 835
DAS (direct-attached storage), 480
data
backup strategies for, 832. *See also* backups; recovery and restores
compressing. *See* compression
routing over network, 876
tokens, 693
transferring within or between data-storage devices, 691–694
database management system, monitoring performance, 440
Data Center Bridging, 233, 483, 485, 691
data collector reports, 457
cleaning up with Data Manager, 469
details, modifying, 469
viewing, 467–469
data collector sets, 425
Active Directory Diagnostics template, 459
Basic template, 459
creating, 458–462
deleting, 459
on domain controllers, 460
logging directory, 461
managing, 460–462
most recent report, opening, 468
performance counter data, collecting, 462–464
performance trace data, collecting, 464–466
privileges and permissions for, 461
registry configuration changes, recording, 466–467
saving as template, 459, 468
on servers, 460
stopping logging, 468
system defined, 457–460
System Diagnostics templates, 459
System Performance template, 459
templates, 459–462
types, 458
user defined, 457–458
uses of, 457
data deduplication, 489, 704–714
BranchCache interoperability, 707
checksum validation, 705
configuring, 694
data, selecting, 706–707
DFS replication interoperability, 707
exceptions to, 708, 711
failover cluster interoperability, 707
file optimization, 704–705
free space for, 707
for primary data volumes, 705
scheduling, 709–710
Single Instance Storage and, 707
space savings, determining, 706
volumes, 708–711
Windows PowerShell cmdlets, 711–714
Data Deduplication role service, 489, 691
data drives. *See also* **hard drives**
BitLocker, enabling, 606–608
encrypting, 601–602
hardware-based encryption, 589–590
data-encryption keys, 588
datagrams, 875

data integrity, 650, 654, 656
- of deduplicated data, 705
- disk integrity, 672–675
- integrity streams, 654–655
- metadata integrity, 650, 652

Data Manager data collector report cleanup, 469

data prioritization, 183

data-recovery agents, 587, 605

data storage. *See* **storage**

data streams
- NTFS, 638–640
- ReFS, 654–655

day-to-day system operations, 53–58

Dcdiag, 1207

Dcgpofix, 1441–1442

DCList, 1463

Dcpromo log, cloning-related entries, 1301

debug booting, 118, 126

Debugger Settings BCD store entry, 126

debugging mode at startup, 869

decentralized network administration, 24

Deduplication Evaluation tool (DDPEval.exe), 706

Default Domain Controllers Policy GPO, 1389, 1403–1406
- restoring, 1441–1442

Default Domain Policy
- Account Lockout Policy, 1349
- Password Policy, managing, 1347
- password settings policies, 1350

Default Domain Policy GPO, 1345, 1389, 1403–1406
- restoring, 1441–1442

default operating system
- , 133

Defrag (Defrag.exe), 683–686
- options and parameters, 685–686
- summary of fragmentation, 686–688
- syntaxes, 683–684
- virtual disks, optimizing, 685

defragmenting
- automated, configuring, 681–682
- cyclic pickup, 681
- shadow copies and, 786

Delete Shadows command, 795–796

Delete ShadowStorage command, 796

Denied RODC Password Replication Group, 1337–1338

DEP (Data Execution Prevention), 131

deployment of Windows Server 2012
- business reasons, 15–16
- change management, 35, 54
- installation, 11
- IT goals, 16
- outsourcing tasks, 14
- planning, 10–36
- process of, 10–11
- quick start, 12
- success, gauging, 27
- teams for, 12–14

desktop, 168–169
- consoles as icons, 214
- Control Panel, accessing, 140, 162
- customizing, 168–169
- hidden button, 140
- hidden menu, 139–140
- opening from Start, 140
- searching from, 140
- shortcuts, accessing, 175
- taskbar, 169–174
- Windows PowerShell, opening, 148

desktop apps, 349

desktop-class computers
- server operating systems on, 264
- Windows Server 2012 on, 101

Desktop Experience, 9

desktop operating systems, standby mode, 102

development team, 13

device drivers, 269, 280–292
- for backup devices, 859
- choosing, 276
- disabling, 291, 292
- driver signing, troubleshooting, 281
- driver store, 280
- information about, viewing, 283
- installing, 286–289
- installing automatically, 288
- installing manually, 275–276, 288–289
- inventory of, 286
- in Windows Server 2012 standard installation, 273
- loading during installation of operating system, 89–90
- manifest files, 280
- mappings to devices, 315
- reinstalling, 292
- on remote computers, 279
- removing, 291–292
- rolling back, 272, 290–291
- searching for, 275, 287
- Setup Information files, 280
- Setup program, 287
- signed, 281
- software bugs, 263
- source files, 280
- testing, 274, 275, 277
- uninstalling, 291–292

device drivers (*continued*)
updating, 270–271, 288–289
version information, 287
viewing and configuring, 277–279
Device Installation Settings, 270
Device Manager, 161, 274
Conflicting Device list, 299
devices, checking, 96
devices, viewing and configuring, 277–280
dynamic disks, moving, 557–558
opening, 277–278
resource settings, managing, 301
shortcut menu options, 278
warning icons, 278, 296
device resources, 285–286
devices. *See also* **hardware**
automatic detection and installation, 273
availability, 274
device info, 270
Device Installation Settings, 167
disabling, 283, 294
driver associations, 294
enumeration of, 318
error codes, 296–298
error events, 295
installation, allowing or preventing, 289–290
installation failures, 274
installation techniques, 273
installation timeout value, specifying, 277
installing, 269–279
I/O and memory ranges, 286
legacy devices, installing, 293–294
managing, 161
mappings to device drivers, 315
new devices, 273–277
non–Plug and Play devices, installing, 293–294
properties, viewing, 281–287
recovering, 291
on remote computers, 279
restricting with Group Policy, 289–290
slot configuration, 299
status, 282
uninstalling, 294
viewing and configuring, 277–279
Devices And Printers
device availability, 274
devices, installing, 274–275
device software, 270
Dfsdiag, 486
DFS (Distributed File System), 480, 490
client/server architecture, 1245
closest-site selection, 491
DFS Namespaces, 490
DFS Replication, 490
DFS roots, 491
in-memory cache, 1245
metadata, 1244
replication architecture, 1245–1246
storage techniques, 1243–1245
Sysvol replication, 1240–1241, 1465
DFS Management, 141
DFSN cmdlet, 486
Dfsradmin, 486
DFS-R (DFS Replication), 1241
connections, monitoring performance, 440
folders, monitoring performance, 440
log, 406
Dfsutil, 486
DHCID (Dynamic Host Configuration Identifier), 1038
DHCP clients, 941–942
classes, configuring use of, 996–997
classes, defining, 995–998
configuration settings, 961
connection requests, 1000
directly connected clients, settings for, 994–995
DNS Dynamic Update protocol, 1002–1003
identifiers, setting, 991
name protection, 1003
NAP clients, settings for, 993–994
policy-based options, 991
RRAS clients, settings for, 993–994
scope of, 986
standard options, setting, 990
TCP/IP options, 988
user classes, 988–989
vendor classes, 989–990
DHCP console, 961–962
conflict detection, configuring, 1007
database, backing up, 1010
DHCP Server service and networking interface, binding, 1001
DHCP Server service, managing, 997
exclusion ranges, defining, 975
exclusions, displaying, 975
failover scopes, creating, 980–984
NAP settings, configuring, 1005
NAP settings, viewing, 1006–1007
normal scopes for IPv4, creating, 964–969
normal scopes for IPv6 addresses, creating, 970
predefined options, configuring, 985
reservations, creating, 978–979
reservations, displaying, 976

DHCP console (*continued*)
scopes, activating, 973–974
servers, authorizing, 962–963, 999
user classes, creating, 995–996
DHCP (Dynamic Host Configuration Protocol), 941–1016
Active Directory, managing with, 945
address leases, 941–942, 966–967
address leases, releasing and renewing, 936–938
address leases, renewing, 948–949, 966
address leases, terminating, 974
address ranges, planning, 958, 964
audit logging, 998–1001
Automatic Private IP Addressing and, 919
availability, 952–957
backing up, 833
clients, 941–942. *See also* DHCP clients
for clients, 918
configuration settings, saving and storing, 1008
conflict detection, enabling, 1007
default gateways, 967
DHCP Acknowledgment messages, 948
DHCP Administrators group, 960–961
DHCP database, 941, 1008–1011
DHCP Discover messages, 948–949
DHCP Offer messages, 948
DHCP Request messages, 948
DHCP Server service, 959–962. *See also* DHCP Server service
DHCP Users group, 960–961
DHCPv4 client options, 993–994
DHCPv4 messages and relay agents, 948–950
DHCPv6 clients, 944
DHCPv6 messages and relay agents, 950–952
DHCPv6 stateful mode, 951
DHCPv6 stateless mode, 951
DNS dynamic updates, 1037–1038
DNS, integration, 943, 1002–1003, 1034–1035
DNS servers, specifying, 968
in domains, 958
exclusion ranges, 958, 966, 974–976
fault tolerance, 952–957
implementation, planning, 948–957
IPAM and, 946–948
IPv4 autoconfiguration, 943
IPv6 autoconfiguration, 944–945
limited broadcasts, 888
NAP, integration, 1003–1007
NetBIOS scope, setting, 1114
parent domain for DNS resolution, 968
relay agents, 950, 951, 964, 1011–1016
reservations, 942, 964, 966, 976–980
Router Advertisement messages, 950
RRAS, integration, 943
scopes, 942. *See also* scopes, DHCP
scopes, failover, 952–956, 980–984
scopes, split, 955–957
security considerations, 945–946
server discovery, 946
servers, 941–942. *See also* DHCP servers
Solicit messages, 952
TCP/IP options, configuring, 966, 984–997
user classes, 988–989, 995–996
vendor classes, 989–990
WINS servers, specifying, 969
in workgroups, 959
DHCP Policy Configuration Wizard, 992–995
DHCP Post-Install Configuration Wizard, 960–961
DHCP Relay Agent Service, 964
DHCP Server role, 231
binary source files, obtaining, 959–960
DHCP servers
authorizing, 960, 962–963, 999
client scope, determining, 986
configuration settings, saving and restoring, 1008
conflict detection, 1007
database, 1008
database, backing up, 1010–1011
database, moving, 1011
database properties, setting, 1009–1010
DHCP Server service, installing, 959–962
failover scopes, 980–984
FQDNs, 961
name protection, 1038
network interface bindings, 961
as Network Policy Servers, 1003–1006
number of, 952, 958
placement of, 1270
planning usage, 38
policies, processing, 987
post-install configuration, 960–961
remote servers, connecting to, 962
server load, 958
setting up, 957–984
standby servers, 958
starting and stopping, 998
static IP address, assigning, 959
DHCP Server service, 941
audit logging, 998–1001
binding to network interface, 1001
cleanup operations, 999–1000, 1009
database maintenance, 1009
failover on clusters, 952
fault-tolerance implementations, 952

DHCP Server service (*continued*)
installing, 959–962
network interface, binding to, 1001
server hardware, selecting, 946, 957–958
server management, 997
starting, stopping, pausing, and resuming, 997, 1011
unauthorized server detection, 945
DHCP tool, 141
DHCPv6 activities, monitoring performance, 440
DHCPv6-Capable DHCP client, 881
diagnostic startups, 113
differential backups, 835–836
digital signatures
for device drivers, 281
on DNS zone files, 1036, 1079–1080
directory partitions, 1159
bridgehead servers for, 1459
Directory Replicator service, 344
Directory Service logs, 406
directory services, 1135. *See also* **Active Directory**
Directory Services Management Tool, 1295–1296
DirectoryServices object, 1465–1466
Directory Services Recovery mode, 869, 1300–1301
Directory Services Restore mode, 861–865
password, 1284, 1290
directory tree, 1152–1153, 1215
administrative access, 1220–1221
domain controllers, creating in, 1278
domains, moving, 1224
empty roots, 1223
forest root domain, 1217, 1225
searching, 1164–1165
DirQuota command-line utility, 663
disaster planning, 821–826. *See also* **backups; recovery and restores**
contingency procedures, 822–823
problem-escalation procedures, 823–824
problem-resolution policy document, 824–826
response procedures, 823–824
disaster preparedness, 826–830. *See also* **backups; recovery and restores**
backups, performing, 826–827
backup strategies, developing, 830–837
startup and recovery options, configuring, 828–831
startup, repairing, 827–828
disaster recovery. *See* **recovery and restores**
disk duplexing, 558
disk I/O
bottlenecks, 452–454
counters for, 453–454
per-process, 434–435
Disk Management, 161
Check Disk, running, 675–676
Disk List view, 516
disk load-balancing policy, configuring, 505
disk quota entries, customizing, 665–668
disk quota entries, exporting and importing, 671
disk quotas, configuring, 664–665
disk quota violations, checking for, 668–669
disks, initializing, 520
Graphical View, 516
mirrored sets, breaking, 565
mirrored sets, creating, 558–559
mirrors, removing, 565
mount points, configuring, 542–543
partitions, creating, 534–538, 551–552
partitions, logical drives, volumes, deleting, 549
partitions, logical drives, volumes, formatting, 538–539
partition table style, changing, 524
RAID-5 sets, creating, 564–565
remote systems, managing, 515
starting, 515
storage, managing, 514–519
storage types, changing, 527–528
virtual hard disks, working with, 530–531
Volume List view, 516
volumes, creating, 534–538, 554–555
volumes, extending, 544
volumes, shrinking, 546–547
disk mirroring, 506–507, 558–563
configuring, 558–559
DiskPart, 146, 485
disks, converting to dynamic, 562–563
disks, partitions, volumes, listing, 517
disks, partitions, volumes, selecting, 517
ESP and MSR partitions, creating, 561–562
invoking, 517
partitions, deleting, 561
partition table style, changing, 524–525
storage, managing, 516–519
storage types, changing, 527–528
volumes, extending, 545–546
volumes, shrinking, 547–548
Diskpart.efi, 110, 524
disk partitioning styles, 109
disk quotas, 661–671
configuring, 663–665
data deduplication and, 707
for individual users, 665–668
logging violations, 670
managing, 661–663, 668–671
notification interval, 671
quota entries, importing and exporting, 671

DiskRAID utility, 1274–1275
disks, 621. *See also* **hard disks; volumes**
access time, 505
automated maintenance, 672–680
for backup and recovery, 836–837
bad sectors, marking, 679
BitLocker configuration, 597
boot sector, 522
clusters, 623–624
cylinders, 622
disk quotas, 661–671
disk signatures, 520
drive sections, 525–526
fixed, 525
fragmentation, analyzing, 686–689
fragmentation, fixing, 682–686
fragmentation, preventing, 680–682
free-space consolidation, 684
hot swapping, 520
initialization, 520
integrity, 672–675
listing, 517
load-balancing policy, configuring, 505
logical drives, 522
logical structure, 624. *See also* basic disks; dynamic disks
management options, 696
Master Boot Record, 522
nonfixed, 525
optimizing, 680–689
parity error checking, 564
physical structure, 621
platters, 621
primordial pools, 697–698
recovering, 556
remote management, 158
scaling, 516
sealing, 570–571. *See also* BitLocker Drive Encryption; TPM (Trusted Platform Module) Services
sectors, 622
sector size, 623
seek time, 505
solid-state drives, 622. *See also* SSDs (solid-state drives)
solid-state hybrid drives, 623
storage pools, 690. *See also* storage pools
storage types, 525–528
thin provisioning, 684
three-layered architecture, 689–690
tracks, 621–622
transfer rate, 505
disk striping, 506–507
with parity, 506–507, 564–565
disk write caching, 520
configuring, 521
distribution media
booting from, 70, 77–78
Windows\WinSXS folder, 247
DLT (Distributed Link Tracking) Client service, 643
DNS clients, 1017
binding order preference, 1035
DNSSEC, configuring, 1078
dynamic updates, 1037–1038
IPv4 information, 1100
IPv6 information, 1100–1101
LLMNR and NetBios queries, 1035
primary and secondary DNS servers, configuring address, 1042, 1044
records, reregistering, 1097
reregistering, forcing, 1099
resolver cache, 1101–1102
single-label names, resolving, 1024
TCP/IP configuration, checking, 1099–1100
troubleshooting, 1099–1102
Dnscmd, 146, 1053–1054, 1094, 1103
directory service polling interval, setting, 1103
DNS server configuration information, viewing, 1104–1105
DNS servers, configuring, 1105–1109
DNS server statistics, viewing, 1109–1110
zone records, printing, 1111–1112
zones, listing, 1110–1111
DNS (Domain Name System), 903–907
with Active Directory, 1047–1051
without Active Directory, 1051–1052
Active Directory–integrated zones, 1027, 1030–1032, 1039–1040
Active Directory, interdependence with, 40–41
aging and scavenging activities, 1097–1098
application partitions, 1031
authoritative servers, 1022, 1027, 1031, 1041
backing up, 833–834
cache locking, 1018–1019
caching information, 1018
Canonical Name (CNAME) records, 1086–1087
child domains, 904
cleaning references to failed domain controllers, 866–867
clients, 1017. *See also* DNS clients
conditional forwarding, 1023, 1032, 1034, 1068–1071
configuration, assessing, 21
configuring, 921–924
database, 1022
database, clearing, 1097

DNS (Domain Name System) (*continued*)
default application directory partitions, 1094–1096
design architecture, 1041–1046
destination cache, 940
devolution, 1024–1025
DHCID resource record, 1038
DHCP, integration, 1002–1003, 1034–1035
directory service polling interval, 1103
Dnscmd, 1053–1054. *See also* Dnscmd
DNS Manager, 1053. *See also* DNS Manager
domain controllers, installation on, 1048–1050
domain names, 904–905
domain namespace, 1020–1021
domain structure, 1071
dynamic port range, 1055
dynamic updates, 923, 1032, 1037–1038
external name resolution, 1038–1040
external root servers, 1040
forwarders, 1068–1071
forward lookup zones, 1027, 1066–1067. *See also* forward lookup zones
fully qualified domain names, 905
GlobalNames zone, 1092–1093
glue records, 1034
Host Address (A and AAAA) records, 1083–1086
host names, 904
host names, pinging, 933
implementation, planning, 1019–1035, 1041–1042
infrastructure, 1017–1046
internal and external domain names, 1043
IP spoofing, 1044–1045
large networks, configuring, 1060–1065
LLMNR and, 907, 1034–1035
logging, 1098–1099
Mail Exchanger (MX) records, 1087–1088
monitoring performance, 440
name-resolution process, 905–906, 1022–1023
Name Server (NS) records, 1088–1089
namespaces, public and private, 1020–1021
name squatting, 1038
neighbor cache, 940
operations, 1022
parent domains, 904
Pointer (PTR) records, 1083–1086
primary zones, 1027
public domain names, 904
public Internet resources, IP address of, 1041
queries, 1017. *See also* DNS queries and replies
replication scope, 1066–1067, 1070–1071, 1096
requests, forwarding, 1023
resolver cache, 939–940, 1101–1102
resolvers, 1022
resource records, 1022, 1025–1026, 1082–1092
resource records, DNSSEC, 1037
reverse lookups, 905–906
reverse lookup zones, 1027, 1068. *See also* reverse lookup zones
root hints, modifying, 1039
secondary notification, 1076–1077
secondary zones, 1027, 1032–1033
security, 1036–1040
security configurations, 1045–1046
security threats, mitigating, 1044–1046
separate-name design, 1043–1044
server discovery, 946
Server log, 1098–1099
servers, 1017, 1022. *See also* DNS servers
Service Location (SRV) records, 1091–1092
small networks, configuring, 1056–1060
split-brain design, 1041–1042
split-brain syndrome, 1032
Start of Authority (SOA) records, 1090
storage of information, 38
stub zones, 1027, 1033–1034
subdomains, 1021, 1071–1074
Time to Live values, 1018
top-level domains, 904, 905, 1020–1021
trusts, role in, 1192
WINS, integration, 1132
WINS lookups, enabling, 1132
zones, 1022, 1027–1032. *See also* zones, DNS
zone transfers, 1028, 1074–1076
DNS Dynamic Update protocol, 1002–1003
DNS Manager, 1053
automatic notification of secondary servers, configuring, 1076–1077
CNAMEs, creating, 1086–1087
conditional forwarding, configuring, 1070–1071
Configure A DNS Server Wizard, starting, 1056
default application partitions, creating, 1095–1096
DNS-related events, viewing, 1099
DNSSEC, enabling and disabling, 1078
forwarding, configuring, 1069–1071
forward lookup zones, creating, 1066–1067
GlobalNames zone, deploying, 1093
host entries, creating, 1083–1084
MX records, creating, 1087–1088
NS records, creating, 1089
PTR records, creating, 1084–1085
recursion, disabling, 1071
replication scope, configuring, 1096
serial numbers, incrementing, 1090, 1103
server cache, clearing, 1103
SOA records, viewing, 1090

DNS Manager (*continued*)
stale resource records, scavenging, 1098
zone delegation, 1293
zones, signing, 1080–1082
zone transfers, enabling, 1075–1076
DNS queries and replies
forward lookups, 1017
LLMNR and NetBIOS queries, 1035
LLMNR query timeout, 1035
parallel, 1035
query timeout, 1070, 1071
redirection attacks, 1045
requests, forwarding, 1023
reverse lookups, 1018
security, 1036–1037
DNSSEC (DNS Security), 1036–1037, 1077–1082
resource records, 1037
zones, securing, 1079–1080
zones, signing, 1078, 1080–1082
DNS Server log, 406
DNS Server role, 231
DNS servers, 1017
Active Directory interoperability, verifying, 1273–1274
aging/scavenging properties, 1097
BIND version 8.1.2 or later, 1047
cache, 1103
conditional forwarding, 1069–1071
configuration parameters, 1105–1109
configuration settings, viewing, 1094, 1104–1110
configuring, 1056
delegation for, 1284
delegation of authority, 1072–1074
directory partitions replication, 1162
DNSSEC-aware, 1079
flooding, 1045
forwarders, designating, 1068–1070
forwarding on ISP name servers, configuring, 1042, 1044
forwarding with or without recursion, 1060
forward lookup zones, creating, 1066–1067
global names, 1093
host names, 1042
internal resource records on ISP name servers, 1042, 1044
key masters, 1079
management tools, 1053–1054
placement of, 1270
planning usage, 37–38
preferred DNS server IP address, 1054
primary, 1028, 1051
public Internet resource records, 1042
querying, 1102
recursion, 1069
remote, connecting to, 1053
replication issues, 1103
resource records, 1025–1026
resource records, caching, 1018, 1025
resource records, list of, 1026
reverse lookup zones, creating, 1068
root hints file, 1039–1040, 1060, 1065
root name servers, 1069
root servers, connecting with, 1038–1040
round robin for load balancing, 1085–1086
secondary, 1028, 1051, 1052
single-label names, 1092–1093
site-local addresses, 1034
startup tasks, 1032
statistics, viewing, 1109–1110
TCP/IP settings, 1054, 1103
troubleshooting on, 1102–1112
zone data, 1031
zone data, background loading, 1032
zones, 1022
zone transfers, 1074–1076
DNS Server service, 1017, 1047–1065
configuring, 1042–1044
default application directory partitions, creating, 1094–1095
DNSSEC and, 1036
events, logging, 1098–1099
installing, 1042–1044, 1052–1055
replication scope, 1062–1063
on RODCs, 1317
round robin for load balancing, 1085–1086
signings, keys, and trust anchors, 1079–1082
source port randomization, 1055
stopping and starting, 1039
troubleshooting, 1102–1112
DNS tool, 141
documentation
of network, 15
project worksheets, 18
documents. *See also* **files**
shadow copies, 483
Domain Admins group
domainwide privileges, 1220
forest ownership, 1216
Password Replication Policy management, 1338
RODC account, attaching server to, 1332, 1335
Domain Controller Diagnostic Utility (Dcdiag.exe), 1273
domain controllers
Active Directory information, restoring, 860
Active Directory server roles, 43–45
application data replication, 1159

domain controllers (*continued*)
auditing policies, 1405
authentication duties, 1236
authoritative DNS servers, 1031
backing up, 1274
backup files in registry, 322
bridgehead servers, 44. *See also* bridgehead servers
claims-based policy, 766–767
cloning, 1297–1302
configuration considerations, 1272–1274
configuration directory partition, shared, 1217
connecting with, 203
CPU, 1272
creating additional in existing domain, 1278–1289
creating in new domain or new tree, 1278, 1291–1293
creating in new forest, 1278, 1289–1291
critical volumes for backup, 862
data protection, 1273
data storage capacity, 1272–1273
DCList, 1463
DC Security template, 1425
dedicated, 860–861
demoting, 1302–1307
DHCP on, 946
directory data store, 1147–1150
Directory Services Restore Mode password, 1284
DNS delegation, 1284, 1292–1293
DNS installation, 1048–1050
DNS services, 1284
domain, changing, 167
Domain Controllers OU, 1405
domain directory partitions, 1159
domainwide data replication, 1159, 1162–1163
encrypted files and folders, decrypting, 1279, 1285
exporting configuration settings, 1286
failures, 860, 866–868
first, installing, 1048–1050
forestwide data partitions, 1159
forestwide data replication, 1159, 1162–1163
global catalog servers, 44, 1160, 1165–1166
global catalog services, 1284
Group Policy refresh interval, 1427
hardware considerations, 1272–1274
index creation, 1143–1145
installation media, creating, 1332
installing, 242, 866–868
installing additional, 1277
installing from media, 1278, 1285, 1294–1297
Inter-Site Topology Generators, 1255
member computers, viewing, 876
memory, 1272
moving out of Domain Controllers OU, 1405
moving to sites, 1443, 1446–1447
multiprocessing, 1272
name, changing, 167
NETLOGON share, 725
network services and applications, inventorying, 21–22
Network Unlock servers, 595
nondedicated, 861
number of, 1202
operating systems supported for, 1171
operations masters, 43–44, 1200–1214
Password Replication Policy, 1336–1344
physical security of, 1220
placement, 1237
planning usage, 37
primary name servers, 1027
promoting, 1276, 1280
read-only, 1162
read-only domain controllers, 1315–1344
references to, cleaning, 866–868
removal, forcing, 1304
removing, 1303–1307
rename changes, 1225
replication, 1142, 1162–1164, 1246–1247. *See also* replication
replication partners, 860, 1256–1258, 1285
restoring, 866–868, 1294
restoring vs. replacing, 833
RID pool, 1206
rootDSE representation, 1157
roots and links on, 1245–1246
RPC-over-IP connections, 1448
schema, shared, 1217
secure communications, 1275–1276
security settings, 1405
shutting down, 1299
site-link bridges, 1266–1269
site location, 1284
site location, determining, 1446–1447
sites, associating with, 1446–1447
SRV records, 1091
static IP addresses, 1273, 1278
store-and-forward replication, 1237. *See also* replication
synchronization, 1287
system data collector sets, 460
TCP/IP settings, 1279
time synchronization, 1211
update sequence numbers (USNs), 1251–1252
up-to-dateness vector, 1252
virtualized, 1297–1302
writable, 1162
DomainDnsZones application partition, 38

domain environment, 1161–1214. *See also* **Active Directory**
- administrative access, 1220–1221
- authentication, delegation of, 1196–1200
- authentication design considerations, 1175–1196
- compatibility design considerations, 1171–1175
- domain planning, 1221–1225
- federated forest design, 1188
- forest planning, 1216–1221
- forest root domain, 1223–1224
- global catalogs design considerations, 1164–1171
- operations masters design considerations, 1200–1214
- organizational unit planning, 1225–1232
- organizing, 1215–1232
- replication design considerations, 1162–1163
- search design considerations, 1164–1171
- security configuration, 357, 368
- trusts design considerations, 1175–1196

domain local groups, 1374

domain name resolution, 1047. *See also* **DNS (Domain Name System); name resolution**

domain naming masters, 44, 1205
- locating, 1205
- placement of, 1203
- role, transferring, 1205

Domain Rename (Rendom.exe), 1224–1225

domains, 1215. *See also* **DNS (Domain Name System)**
- accessing in Group Policy Management Console, 1400
- adding and removing, 1205. *See also* domain naming masters
- administration, delegating, 1311–1314
- administrative rights, delegating, 1226–1228
- administrators, 1155
- application directory partitions in, 1094
- authentication within and between, 1236
- authoritative servers, 1049, 1088
- Builtin container, 1288
- changing membership, 166
- child domains, 1217, 1291–1292
- Computers container, 1289
- computers, joining to, 1381
- creating, 1291–1293
- data-recovery agents, 587
- Default Domain Policy, 1228
- default GPOs, 1389
- delegation of authority, 1072–1074
- design, changing, 1224–1225
- design considerations, 1221–1222
- DHCP services, setting up, 958
- domain controllers, adding, 1281–1289
- Domain Controllers container, 1289
- domain controllers, creating in, 1278
- domain functional level, 1171–1173
- domain structure, 1071
- DSHeuristics attribute, 1144
- enterprise administrators, 1218
- external trusts, 1156
- ForeignSecurityPrincipals container, 1289
- forest groupings, 1153
- forest root domain, 1153–1154
- functional levels, 41–43
- for geographically separated sites, 1219
- global catalog data, 1165–1166, 1218
- global catalog servers, 1160
- GPOs linked to, 1389
- grouping objects in, 1226
- group policy inheritance, 1416
- Group Policy permissions, 1407–1409
- group-to-user references, 1212
- installing, 1277
- languages used in, 1222
- legacy hooks to NetBIOS over TCP/IP interface, 1114
- logical partitioning, 1159
- mail exchange servers, 1087–1088
- membership, listing, 152
- multiple-domain design, 1223
- namespaces, 1153–1154
- in new forest, creating, 1289–1291
- number of objects in, 1223
- numbers of, 1222–1223
- object groupings in, 1152–1153
- operations masters, 44, 1201
- organizational units, 41, 1215. *See also* OUs (organizational units)
- planning, 1221–1225
- preparing for new domain controllers, 1279–1281
- preparing for RODCs, 1281
- renaming, 1224–1225
- replicas, distribution of, 1159–1160
- as replication boundary, 1221
- RODCs in, 1323
- root domains, 1153, 1157, 1223–1224
- rootDSE, 1157
- schema administrators, 1218
- security policies, 1222
- servers, adding, 76
- shortcut trusts, 1156
- single-domain design, 1222–1223
- subdomains in same zone as parent, 1071–1072
- subdomains in separate zone from parent, 1071–1074
- tree groupings, 1153
- trusted domains, 1155

domains (*continued*)
trusting domains, 1155
trust relationships, 41, 1154–1156, 1183–1186, 1190–1191, 1218. *See also* trusts
user access, 1181–1183
user rights, assigning, 1355–1356
Users container, 1289
zone transfers, enabling, 1074–1076
domains, Internet
subdomains, 1021, 1029
top-level, 1020–1021
domain trees, creating, 1292
double-colon notation, 901
drag-and-drop functionality
of snap-ins, 192
drive letters
assigning, 535, 555
availability, 534, 558
configuring, 539–541
ESP, assigning to, 562
Driverquery utility, 279, 286
drivers. *See* **device drivers**
driver signature enforcement, disabling at startup, 869
DriverStore folder, 280
DSADD
computer accounts, creating, 1380
groups, creating, 1375–1376
DSA (Directory System Agent), 1141–1142
DSHeuristics attribute, 1144
Dsmgmt, 1343–1344
DSMs (Device Specific Modules), 500
installing, 504
dump files
creating, 390
generating, 475
kernel memory dumps, 830
location, 830
duplex settings, 284
Duplicate Files report, 800
dynamic disks, 525. *See also* **basic disks**
converting to, 562–563
converting to basic, 526–527
deprecated status, 74
managing, 514–519, 526–527
moving, 556–558
RAID-5 volumes, 526
upgrading to, 73
volumes, extending, 543–546
volumes, managing, 552–568
working with, 525–526
dynamic IP addresses, 75–76, 913, 917–919
dynamic virtual machine storage, 508–509

E

Edb.chk, 1148
Edb.log, 1148
Effective Access tool, 1360
Effective Permissions tool, 1382
EFI-based computers
BCD registry, 111
boot facilities, 110
disk-partitioning styles, 109–110
installation of operating system on, 72
EFI (Extensible Firmware Interface), 103, 523
required partitions, 523
EFS (Encrypting File System), 569
EFSInfo utility, 1279
EIDE (enhanced integrated drive electronics), 264–265
EIST (Enhanced Intel SpeedStep Technology), 108
elevation, 349, 355. *See also* **UAC (User Account Control)**
elevation prompts
behavior settings, 356–359
color-coding, 363–364
settings, 353, 367
spoofing prevention, 364
emergency response planning, 56
emergency response teams, 56, 823–824
EMS (Emergency Management Services)
BIOS settings, 126
booting with, 126
controlling, 118
EMS Settings BCD store entry, 126
Enable-ADAccount cmdlet, 1359
Enable-ServerManagerStandardUserRemoting cmdlet, 138
encrypted hard drives, 588–589
encryption. *See also* **BitLocker Drive Encryption**
encrypted files, finding, 1279
of files, 569
FIPS-compliant, 601
hardware-based, 588–591
private key, 1036–1037
of shares, 739
SMB encryption, 494, 496
software-based, 589–591
type, restricting, 591–592
engineering staff responsibilities, delineating, 824
Enhanced Storage, 233, 588
enhanced storage devices, 485
enterprise administrators, 1155
Enterprise Admins group
enterprisewide privileges, 1220

forest-level privileges, 1218
forest ownership, 1216
Enterprise Read-Only Domain Controllers group, 1337
enterprise solid-state drives, 372
EPTs (extended page tables), 508
error codes, device, 296–298
error events, 410
eSATA, 268
escalation of problems, 825
ESE (Extensible Storage Engine), 1142–1147
garbage collection, 1146–1147
ESP (EFI system partition), 72, 110, 523, 549–550
creating, 561–562
drive letter, assigning, 562
event IDs, 417
Event Log format (.evtx), 418
event logs, 154, 405–408
accessing, 408
applications and services logs, 405–407
archiving, 407, 418–419
backup events, 850–851
checking for errors, 97
configuration, 408
event levels, 410
filtered views, 414–417
find and filter options, 417
overwriting of events, 407
remote management, 159
searching, 414
sizing, 407
sorting, 414
viewing, 409–412
Windows logs, 405–406
Event Log service, 405
events
computer causing, 412
defined, 405
details about, 411
device errors, 295
DHCP events, 998–1001
displaying, 154
filtering, 414–417
forwarding, 422–424
Help And Support Center links, 412
properties, 412
on remote systems, viewing, 413
searching for, 414
sorting, 414
tracking with Windows PowerShell, 419–422
types, 410
users associated with, 412
viewing, 409–412
Event Trace Providers dialog box, 465
event traces
data, collecting from, 464–466
starting and stopping, 458
Startup Event Traces, 458
Event Viewer, 141, 143, 160, 409–410
event information, 411–412
filtered views, 414–416
remote computers, viewing events on, 413
saved logs, opening, 418–419
subscriptions, creating, 422–423
Exchange Server
Active Directory, integration, 1168
domain renames and, 1224
exFAT file system, 533
Expand (Expand.exe), 659
extended authorization platform, 765
Extended Selective Acknowledgments, 880
extended taskpad views, 216–218
Extend Volume Wizard, 544
Extensible Storage Engine Utility (esentutl.exe), 1150
Extensions For dialog box, 208–209
extensions, snap-in, 193–194, 208
options for, 194
external hardware devices, 266–269
external storage devices, 480–483
paths to, 484
Extract Compressed (Zipped) Folders dialog box, 351

F

failback policies, 500
Failover Clustering, 233
Failover Cluster Manager, 142
failover clusters, and data deduplication, 707
failover policies, 500
failover protection, and NIC teaming, 456–457
failover scopes, 952–956, 964. *See also* **scopes, DHCP**
active relationships, identifying, 984
client lead time, setting, 982
creating, 980–984
deconfiguring and reconfiguring, 984
failover configuration, reusing, 982
failover mode, specifying, 982–983
failover relationships, naming, 982
fault tolerance, 954–955, 982
identifying, 983–984
load sharing, 953–954, 982
managing, 984
partner server, specifying, 981
shared secret for partners, 983
switchover interval, 983

FAT (file allocation table) file systems, 524, 536, 621, 625–628
analyzing volumes with ChkDsk, 678
Check Disk legacy scans, 676
cluster sizes, 623–624, 627–628
converting to NTFS, 531–532
data streams and, 640
disk integrity, 672–675
FAT12, FAT16, FAT32, and exFAT (FAT64), 623
FAT16, FAT32, and exFAT, comparison of, 627
features, 626–628
mounting volumes, 628
for removable storage devices, 533
share permissions, 748
structure, 625–626
volume size and, 627
fault tolerance
building in, 822
DHCP, 952–957
disk striping with parity, 564
failover scopes for, 954–955
hardware, 48
multiple default gateways, 919
RAID configurations, 506–507
site-link bridging, 1455
split scopes for, 956–957
storage availability and, 505–506
Fax Server role, 231
Fax Service Manager, 142
FC-AL (Fibre Channel–Arbitrated Loop), 492
FCoE (Fibre Channel over Ethernet), 483
FCP (Fibre Channel Protocol), 481–482
features
adding, 238–241, 246
binary source files, 241
binary source files, removing, 144
component names, 254–256
configuring, 229–262
defined, 229
installing at command prompt, 257–260
IP Address Management (IPAM) Server, 946
list of, 232–236
managing at command prompt, 250–251
managing with Server Manager, 237–249
removing, 243–246
removing at command prompt, 260–261
server performance and, 230
supplemental, 236
tracking, 256–262
viewing, 246
federated forest design, 1188
Fibre Channel, 481–482
cabling, 482
layers, 483
network topology, 482–483
priority-based flow controls, 483
File and Printer Sharing for Microsoft Networks, 76
File And Storage Services role, 231, 487
configuring, 497–500
planning usage, 39
file associations, 316
storage in registry, 319
user-specific, 318, 320
file-based compression, 656–661
compressed (zipped) folders, 659–661
NTFS compression, 656–659
File Explorer
Advanced Sharing dialog box, 730–731
auditing, configuring, 776–778
basic permissions, setting, 754–755
Check Disk, running, 675–676
console tools, starting, 197
Control Panel, accessing, 140
drives, compressing, 657–658
file and folder attributes, viewing, 748
file or folder ownership, taking, 749
files and folders, compressing, 658–659
File Sharing dialog box, 728
folder views, configuring, 163–165
network drives, mapping, 719
Network Explorer, opening, 721
Optimize Drives, running, 683
shares, creating, 726–731
special permissions, viewing, 757–758
file extensions, hiding, 164
File Replication Service log, 407
FileRepository folder, 280
files
auditing access, 770–781
backing up, 832, 835
basic attributes, 748
basic permissions, 754
classifying, 807–808
compressing, 657–661
data streams, 638–640
disk fragmentation and, 680
dragging to desktop, 168
encrypting, 569
file deltas, 1241
finding, 140
hard links, 637–638
locked, shadow copying, 715
object identifiers, 643–644
open, shadow copying, 715

files (*continued*)
optimizing, 704–705
ownership, 662, 749–750
permission inheritance, 750–752
properties and personal information, 640
public, 716–717
recovering, 484, 781, 832, 852–857
reparse points, 644–645
screening. *See* file screening
sharing. *See* file sharing; shares
short file names, 643
sparse files, 645–647
special permissions, 759
file screening, 491, 797–801
Access-Denied Assistance policies, 809–812
email notifications, 802–804, 814–815
event logging, 815
exception paths, 799, 817
file classification rules and properties, 807–809
file groups, 798–799
file groups, managing, 812–813
Files By File Group report, 800
Files By Owner report, 800
Files By Property report, 800
File Screen Auditing Report, 806–807
File Screening Audit report, 800
file-screen paths, 797
file screens, creating, 816
file-screen templates, 798
file-screen templates, managing, 813–815
Folders By Property report, 800
global options, 802–812
Large Files report, 800
Least Recently Accessed Files report, 800
modes, 797
Most Recently Accessed Files report, 800
notification limits, 804–805
Quota Usage report, 801
storage reports, 799–801
storage reports, scheduling and generating, 817–820
File Server Resource Manager, 142, 801
Access-Denied Assistance, configuring, 809–812
email notifications, configuring, 802–804
file classification, scheduling, 808
file groups, configuring, 812–813
file-screen auditing, configuring, 806–807
file-screen exceptions, creating, 817
file screens, creating, 816
file-screen templates, configuring, 813–815
file-screen templates, defining, 797
notification limits, configuring, 805
storage report location, configuring, 806
storage reports, configuring, 805
storage reports, scheduling, 817–819
FileServerResourceManager cmdlet, 486
File Server Resource Manager role service, 797
file servers
backing up, 484, 834
clustering, 494
configuring, 487
failover, 494
File And Storage Services role, configuring, 497–500
hash publication, enabling, 489
NFS support, 481
role services and features, adding, 497–500
services, configuring, 496–513
shares on, 737
storage-management features and tools, 483–487
Windows Standards-Based Storage Management feature, 691
File Server service, 487
File Server VSS Agent Service, 484, 489
File Server VSS provider, 484
file sharing, 715–796. *See also* **shares**
auditing access, 770–781
claims-based access controls, 717, 765–770
DFS, 490
enabling, 717–718
encryption, enabling, 496
folder path, 719
in-place, 716
maximum transmission units, 494
NFS, 490, 736
password-protected, 718
public folder sharing, 716–717
on removable disks, 533
Server service, 716
shadow copies and, 781–786
share name, 719
shares, locating, 21
SMB 3.0, 493–497
standard, 716–717
file storage. *See also* **storage**
assessing, 20
file system cache, 440
file systems
auditing, 774
changing types, 538
checking type, 628
cluster size, 537
encrypting, 587, 606
FAT, 625–628. *See also* FAT (file allocation table) file systems
file-based compression, 656–661

file systems (*continued*)
formatting disks with, 623
function of, 621
NTFS, 628–649
ReFS, 649–656
self-healing, 648
types, 536
virtualization, 305, 361
Filter Current Log dialog box, 415–416
FIPS (Federal Information Processing Standard) compliance, 601
firewalls
profile and status on servers, 154
remote management and, 202
replication through, 1448–1449
Windows Firewall, 9. *See also* Windows Firewall
FireWire, 268, 269
FireWire controller cards, 269
firmware
booting from, 101–109
boot settings, 109
chipset firmware, 103
cooling modes, 104
power settings, managing, 107–108
TCG-compliant, 571
troubleshooting, 92–93
updating, 103–104
upgrading, 95–96
virtualization support, 507
firmware boot manager application, 314
fixed-disk provisioning, 488
fixed disks, 525
booting to, 109
FAT, 625
mount points, 541
fixed drives
BitLocker, enabling, 606–608
Group Policy BitLocker settings, 599
fixed provisioning, 701
Fix It Portable, 336–338
focus, setting, 202
folder icons, consoles as, 214
Folder Options utility, 163–165
folders
adding to console root, 206
auditing access, 770–781
backing up, 835
basic attributes, 748
basic permissions, 754
central access policies, applying, 770
classifying files by, 807
compressing, 656–659
dragging to desktop, 168
home folders for users, 1365–1366
ownership, 662, 749–750
permission inheritance, 750–752
personal toolbars for, 176
recovering, 781, 852–857
renaming, 206–207
reparse points, 644–645
sharing. *See* file sharing; shares
special permissions, 759
synchronizing across LANs and WANs, 490
zipping, 660
foreground processes, 389
ForestDnsZones application partition, 38
forest root zones
creation of, 1050
primary DNS servers for, 1091
forests, 40, 1153, 1215
accessing in Group Policy Management Console, 1399
adding, 1220
administration, 1219–1221
authentication across, 1186–1187
Configuration container, 1157–1158
connecting to, 216, 1444
creating, 1289
cross-forest authorization, 1187
cross-forest trusts, 1218
default application directory partitions in, 1094
domain controllers, creating in, 1278
domain naming masters, 1201
domains, creating in, 1291–1293
domains, removing, 1303
empty roots, 1223
enterprise administrators, 1155
federated forest design, 1188
forest functional levels, 1173–1175
forest root, 40
forest root domain, 1153–1154, 1157–1158, 1217, 1223–1225
Forest Root Domain container, 1157–1158
forest root domain, installing, 1277
forestwide changes, authority over, 1217
functional levels, 41–43
for geographically separated sites, 1219
global catalog, 1218
global catalog servers in, 1165–1166
legacy hooks to NetBIOS over TCP/IP interface, 1114
merging, 1219
multiple, 1218
multiple domains in, 1219
multiple namespaces in, 1219
namespace, 1217–1218

forests (*continued*)
number of, 1218–1219
operations masters, 44
owners, 1216–1217
planning, 1216–1221
preparing for new domain controllers, 1279–1280
replication in, 1236
root domains, 1157
Schema container, 1158
schema masters, 1201, 1217
sites in, 1239
size of organization and, 1219
time synchronization, 1210–1211
trusts, 1186–1189, 1218. *See also* trusts
Forgotten Password Wizard, 1372
Format-Table cmdlet, 395
Forwarded Events log, 405, 423
forward lookup zones, 1051. *See also* **zones, DNS**
creating, 1049, 1057, 1061–1062
dynamic updates, 1059, 1063–1064, 1067
forwarding, 1059–1060
GlobalNames zone, 1092–1093
maintaining by ISP, 1057
maintaining with DNS server, 1057
master name servers, identifying, 1058, 1063, 1067
name, 1058, 1067
resource records, 1082
SRV records, 1091
types, 1066
zone files, 1063, 1067
zone transfers, 1074
FQDNs (fully qualified domain names), 905
of nodes in DNS namespace, 1020
fragmentation, 680–689
manually checking, 682–683
FRS (File Replication Service)
replication architecture, 1242–1243
storage techniques, 1241–1242
Sysvol replication, 866, 1240–1241, 1465
FSRM (File Server Resource Manager), 491
Fsutil, 486
FSUtil Behavior command, 632
FSUtil FSinfo command, 634–635
FSUtil Hardlink command, 638
FSUtil Objectid command, 644
FSUtil Quota command, 669
FSUtil Quota Violations command, 670
FSUtil ReparsePoint command, 645
FSUtil Sparse command, 647
FSUtil Transaction command, 648
FSUtil Usn Queryjournal command, 640
FSUtil Usn Readdata command, 642
FSUtil Volumeinfo command, 628
Ftp, 146
Full Server installations, 66–67
converting to Server Core, 98
FWBOOTMGR, 117

G

gateways, 890, 919–921
DHCP, 967
Get-ADDCCloningExcludedApplicationList cmdlet, 1298
Get-ADReplicationFailure cmdlet, 1464
Get-ADReplicationPartnerMetadata cmdlet, 1464
Get-AdReplicationUpToDatenessVectorTable cmdlet, 1213
Get-Counter cmdlet, 474
Get-Credential cmdlet, 260
Get-DedupMetadata cmdlet, 713
Get-DedupSchedule cmdlet, 714
Get-DedupStatus cmdlet, 711
Get-DedupVolume cmdlet, 712
Get-Eventlog cmdlet, 419–422
grouping events, 420–421
–logname parameter, 420
–newest parameter, 420
searching for events, 421–422
sorting events, 421
Get-MSDSMGlobalDefaultLoadBalancePolicy cmdlet, 502
Get-MSDSMSupportedHw cmdlet, 504
Get-Netroute cmdlet, 935
Get-Process cmdlet, 379–380, 391, 395–397
properties for, 396–397
resource usage, 380
Get-Service cmdlet, 379–381, 397, 399–400
Get-SmbSession cmdlet, 495
Get-Smbshare cmdlet, 723, 763
Get-WindowsFeature cmdlet, 246, 250, 256–258
Get-WindowsOptionalFeatures cmdlet, 596
global catalog servers, 44, 1160, 1165–1166
accessing, 1165–1166
designating, 1166–1168
listing, 1305
Options attribute, 1467
placement of, 1203, 1270
removing, 1305
replication among, 1236
replication attributes, 1168–1171
in replication topology, 1259
in sites, 1445
SRV records, 1091
global groups, 1374

global sleeping state, 106–107
GPMC (Group Policy Management Console), 1228, 1393, 1397–1403
applied GPOs, viewing, 1431–1432
domains, accessing, 1400
forests, accessing, 1399
GPO creation rights, delegating, 1406–1407
GPOs, backing up, 1438–1439
GPOs, creating and linking, 1400–1401
GPOs, deleting, 1403
GPOs, editing, 1401–1403
GPOs, listing, 1397–1398
GPOs, restoring, 1440–1441
GPOs, selectively applying, 1418
infrastructure status, 1398
link order, changing, 1414
links to GPOs, removing, 1403
logon and logoff scripts, configuring, 1424
loopback processing, configuring, 1421–1422
management privileges, determining, 1407–1409
management privileges, granting, 1409–1410
OUs, listing, 1397–1398
policies, enabling and disabling, 1420
policy editors, 1346
policy inheritance, blocking, 1415
policy inheritance, enforcing, 1416–1417
policy scope, viewing, 1416
reason codes for in-progress replication, 1398–1399
remote updates, 1438
sites, accessing, 1400
slow-link detection, configuring, 1428–1429
starter GPOs, creating, 1403
startup and shutdown scripts, configuring, 1423
status details, 1398
user rights, assigning, 1355–1356
GPOs (Group Policy Objects), 1389
backing up, 1438–1439
core policies, 1392
creating and linking, 1400–1401
creation rights, managing, 1406–1407
Default Domain Controllers Policy GPO, 1403–1406
Default Domain Policy GPO, 1403–1406
deleting, 1403
editing, 1392, 1401–1403
editing permissions, 1417
linking, 1402, 1410
modeling, 1433–1437
preference order, 1401
processing, 1427–1428
restoring, 1440–1441
security templates, 1425–1426
selectively applying, 1417–1418
sites, domains, and OUs, linking to, 1389
starter GPOs, 1402–1403
WMI filters, linking, 1436
GPPREP, 1281
GPT disks, 521–525
boot and system volumes, mirroring, 560–563
checksum fields, 522–523
converting to MBR, 524–525
drive letter assignment, 534
ESP, 549–550
FAT/FAT32, converting to NTFS, 531–532
formatting, 524
GPT headers, 523
LDM Metadata and LDM Data partitions, 552
managing, 549–552
mirrored system volumes, rebuilding, 567–568
MSR partitions, 550–551
OEM partitions, 552
partition size, 523
partitions on, 72
partition types, 549
primary and backup partition tables, 523
primary partitions, 551–552
storage type, changing, 527
unknown partitions, 552
GPT (GUID partition table), 109
Gpupdate, 1437–1438
graphical administration tools, 141–145
alternate credentials for, 143
group membership
computer accounts, 1384
examining, 1341–1342
recovery and, 863–864
simulating changes, 1435–1436
updating, 1212
Group Policy, 1387–1442
Access-Denied Assistance policies, 809–812
Account Lockout Policy, 1404
Account Policies, 1404
Accounts: Rename Administrator Account policy, 1404
Accounts: Rename Guest Account policy, 1404–1405
Active Directory Group Policy, 1388–1389
Admin Approval Mode settings, 356–357
Administrative Templates, 1390, 1392–1393
advanced auditing, configuring, 773–775
Allow Log On Through Remote Desktop Services user right, 180
Allow Network Unlock At Startup policy, 595
application installation and run behavior settings, 366–367
Apply Group Policy permission, 1417
architecture, 1390–1392

Group Policy (*continued*)
- backing up, 834
- basic auditing, configuring, 771–773
- central management of folders, configuring, 782
- client-side extensions, 1390, 1391
- component installation and repair, configuring, 248–249
- Computer Configuration settings, 1418–1421
- Configure Device Installation Time-out policy, 277
- Configure The Level Of TPM Owner Authorization Information Available To The Operating System policy, 575
- Configure Use Of Hardware-Based Encryption For Fixed Data Drives policy, 589–590
- Configure Use Of Hardware-Based Encryption For Operating System Drives policy, 590–591
- Configure Use Of Hardware-Based Encryption For Removable Data Drives policy, 590
- Configure Use Of Passwords For Operating System Drives policy, 586
- console authoring, restricting, 195
- Default Domain Policy, 1228
- default GPOs, 1403–1405, 1441–1442
- Deny Log On Through Remote Desktop Services user right, 181
- device installation policies, 289–290
- Disallow Standard Users From Changing The PIN Or Password policy, 586
- DNS client settings, 1035
- DNS devolution, controlling, 1025
- domain security policies, 1222
- Edit Settings, Delete, Modify Security permission, 1408–1410
- Edit Settings permission, 1408–1410
- encryption policies, 589–591
- Enforce Drive Encryption Type policy, 591
- event log configuration, 408
- filtering application of, 1417–1418
- FIPS compliance settings, 601
- Fixed Data Drive policies and settings, 606
- global access policy, configuring, 778–779
- GPOs, viewing, 1431–1433. *See also* GPOs (Group Policy Objects)
- Group Policy Management Console, 1397–1403. *See also* GPMC (Group Policy Management Console)
- Group Policy Refresh Interval For Computers policy, 1427
- Hash Publication For BranchCache policy, 489
- implementing, 1393–1405
- inheritance, 1411–1417
- IPAM provisioning, 947
- KDC Support For Claims, Compound Authentication Dynamic Access Control And Kerberos Arming policy, 767
- Kerberos Policy, 1404
- Link GPOs permission, 1407, 1410
- link management, delegating, 1410–1411
- link order, changing, 1412–1414
- Local Group Policy, 1388–1389, 1394–1397
- local settings, managing, 1396
- logon and logoff scripts, 1423–1424
- loopback processing policy, 1421–1422
- Management Console restrictions, 573
- management privileges, delegating, 1409–1410
- management privileges, reviewing, 1407–1409
- managing through delegation, 1406–1411
- modeling GPOs, 1433–1437
- Network Access: Allow Anonymous SID/Name Translation policy, 1346, 1405
- Network Security: Force Logoff When Logon Hours Expire policy, 1346, 1405
- OU settings, 1228
- Password Policy, 1404
- Perform Group Policy Modeling Analyses permission, 1407, 1410
- policies, disabling and enabling, 1414–1415
- Policies node, 1388
- policy precedence, 1411–1414
- policy processing order, 1412–1414
- policy processing policies, 1429
- Preferences node, 1388
- processing, 1418–1421, 1427–1428
- Read Group Policy Results Data permission, 1407, 1410
- Read permission, 1408–1410
- refresh, 1411, 1420, 1427–1428
- refresh, forcing, 770
- refresh, manual, 1433–1437
- refresh, modifying, 1428–1430
- registry-based policy settings, 1392–1393
- registry, managing with preferences, 329
- Remote Desktop Services settings, 181–182
- Removable Data Drives policies and settings, 608
- Require Additional Authentication At Startup policy, 593
- resetting to default, 196
- Restrict The User From Entering Author Mode policy, 195
- Restrict Users To The Explicitly Permitted List Of Snap-Ins policy, 195
- RSoP, delegating, 1410–1411
- security settings, 1396
- security templates, 1424–1426

Group Policy (*continued*)
Server Manager autostart policy, 150
Set Group Policy Refresh Interval For Domain Controllers policy, 1427
settings, 1389–1390
slow-link detection, 1428
snap-in availability, restricting, 195
Software Settings, 1389
Specify Intranet Microsoft Update Service Location policy, 272
Specify Search Order For Device Driver Source Locations policy, 271
Specify Settings For Optional Component Installation And Component Repair policy, 248
Specify The Search Server For Device Driver Updates policy, 272
startup and shutdown scripts, 1422–1423
TCP/IP networking and, 909
Time (In Seconds) To Force Reboot When Required policy, 290
TPM and BitLocker configuration settings, 598–600, 603–605
TPM-related policies, 576
TPM validation-profile settings, 593
troubleshooting settings, 1419
Turn Off Access To All Windows Update Features policy, 271, 288
Turn Off Local Group Policy Objects Processing policy, 1395
user account policies, 1345–1350
User Configuration settings, 1418–1421
user-specific, 1394
version of Windows operating system, 1388
Windows Settings, 1389
Group Policy Management, 142, 233
central access policies, editing, 768–770
Group Policy Management Editor, 1391, 1393
Group Policy Modeling Wizard, 1433–1437
Group Policy Object Editor
refresh, configuring, 1429
starting, 1395
Group Policy Results Wizard, 1431–1432
Group Policy Starter GPO Editor, 1393
groups
administrative rights, delegating to, 1227–1228
Cloneable Domain Controllers group, 1298
creating, 1374–1376
deleting, 1377–1378
distribution groups, 1373
domain local groups, 1374
effective access, determining, 1360–1361
finding, 1378
global groups, 1374
GPOs, permissions on, 1408–1409
Group Policy, applying or denying, 1417
linking GPOs permission, 1410
managing, 1373–1378
members, adding, 1377
modifying, 1378
password settings policy, 1350
RODC-related, 1337
RSoP permission, 1410
scopes, 1373
security groups, 1373
security identifiers, 1378
universal groups, 1176–1178, 1374
Guest account, renaming, 1404–1405
guest operating systems, virtualizing, 507
GUIDs (globally unique identifiers)
in BCD store entries, 120–121
GUID partition table, 109
of objects, 1141–1142

H

HAL (hardware abstraction layer), 280
handles
of processes, 394
summary statistics, 384
hard disks. *See also* **disks**
backing up to, 844
booting to, 109
conflicts with, 96
I/O activity, 453–454
optimizing performance, 453
partitioning at installation, 72–74
read/write activity, monitoring, 440
solid-state drives, 265, 372
hard drives
Advanced Format, 264, 519
bytes per physical sector, determining, 264
choosing, 263–264
compressing, 657–658
drive shares, 724
EIDE, 264–265
encrypting, 588–592
interrupts, 451
managing, 161
physical structure, 621–622
SATA, 264–266
SCSI, 264
SSDs, 265. *See also* SSDs (solid-state drives)
Standard Format, 519
hard links, 637–638

hard page faults, 449
memory pages read to and from disk, 449–450
hard shutdowns, 871
hardware. *See also* **devices**
access controls, 52
automatic detection and installation, 273
availability, 47–60, 274
booting from, 101–109
change control, 54–55
compatibility, 26, 47, 92
configuration data in registry, 314–315
current configuration at startup, 319
deploying, 49
descriptions, 314–315
detection, 269
device and driver information, viewing, 277–280
device drivers, 280–292
Device Installation Settings, 167
device maps, 315
disabling, 294
earthquake protection, 51
external devices, 266–269
fire protection, 51
firmware updates, checking for, 33
installing, 263–279
internal devices, 263–266
inventory of, 20
managing, 292–302
new devices, installing, 273–277
physical environment, protecting, 50–51
physical security, 822
power protection, 823
power settings, managing, 107–108
power-state management, 103
profiles, 318
redundancy, 48
registry settings, 312–313
reliability problems, 295
searching for, 293–294
selecting for install, 293–294
standardizing, 34, 47–48
standby state support, 102
support structures and facilities, 49–52
temperature and humidity, 50
troubleshooting, 295–298
uninstalling, 294
hardware diagnostics, 295
hardware encryption, 588–592
Hardware Events log, 407
hardware RAID, 73, 506. *See also* **RAID (redundant array of independent disks)**
hashing, FIPS-compliant, 601
hash publication, 489
HDDs (hard disk drives). *See also* **disks; hard drives**
help desk structure, 56
Hiberfil.sys file, 125
Hibernate mode, 107
hidden files, folders, and drives
viewing, 164
.hiv extension, 330, 333
HKCC (HKEY_CURRENT_CONFIG) key, 311, 319
HKCR (HKEY_CLASSES_ROOT) key, 311, 319
HKCU (HKEY_CURRENT_USER) key, 311, 320
HKLM\BCD00000000 key, 313–314
HKLM\HARDWARE key, 314–315
HKLM (HKEY_LOCAL_MACHINE) key, 311–313
CurrentControlSet subkey, 317–318
subkeys, 312–318
HKLM\SAM key, 315
HKLM\SECURITY key, 315
HKLM\SOFTWARE key, 315–316
HKLM\SYSTEM key, 317–318
HKU (HKEY_USERS) key, 311, 318–319
homegroups, 876
data-recovery agents, 587
Hostname, 146
hot swapping, 520
Hyper-V, 6–7
compatibility issues, troubleshooting, 508
configuring, 507–514
installing, 509–511
planning usage, 39
requirements, 507
virtual machines, creating, 511–513
hypervisor debugging, 126
configuring, 118
Hypervisor Settings BCD store entry, 126
Hyper-V Manager, 142, 511
Hyper-V role, 231

I

Ia64ldr.efi, 110
IANA (Internet Assigned Numbers Authority), 887
ICANN (Internet Corporation for Assigned Names and Numbers), 887
top-level domain management, 1020
icons
Computer icon, 168
for consoles, setting, 212–213
Network icon, 169
Notification Area Icons page, 173–174
Permissions icon, 353
shield icon, 353

icons (*continued*)
for tasks, 223
for tasks, setting, 223
warning icons, 278, 296
IDE (Integrated Device Electronics) drives, 96
IEEE 802.1ax, 456
IEEE 1394, 268
IE ESC (Internet Explorer Enhanced Security Configuration), 152–153
iFCP (Internet Fibre Channel Protocol), 483
image names, 378
incident response teams, 57, 823–824
incremental backups, 835–836
inetOrgPerson objects, 1226
.inf extension, 280
Inf folder Setup Information files, 273
information events, 410
infrastructure masters, 44, 1212
placement of, 1203
role, transferring, 1212
inheritance
blocking, 1415
enforcing, 1416–1417
Group Policy, 1411–1412
overriding, 1414–1415
Ink and Handwriting Services, 233
in-place file sharing, 716
Install-ADDSDomain cmdlet, 1277
Install-ADDSDomainController cmdlet, 1277, 1336
Install-ADDSForest cmdlet, 1277
Installation image, mounting, 99, 247–248
installation media, creating, 1294
installation of Windows Server 2012, 70–85
activation, 79, 82–85
additional tasks, 242–243
automated setup, 62
on BIOS-based systems, 71–72
clean installations, 64–65, 77–81
command prompt, accessing, 85–88
device drivers, loading, 89–90
disallowed upgrade paths, 65
distribution media, booting from, 70
driver and system files, updating, 67–69
on EFI-based computers, 72
failure points, 92–93
Installation image, mounting, 99
installation location, 80–81
installation options, 64–65
installation types, 66–67, 98
interactive installations, 61–62, 70
lockups and freezes, continuing past, 93–99
naming computers, 74–75
network and domain membership options, 75–77
partitions, creating, deleting, and extending, 90–91
partitions, planning, 72–74
partitions, removing, 89
postinstallation tasks, 96–99
preinstallation tasks, 69–70
preparing for, 64–70
product IDs, 64
product key, providing, 79, 80
quick start, 61–62
rebooting, preventing, 62
Setup.exe, 62
system requirements, 64, 93
temporary installation files, location, 62
troubleshooting, 65, 91–96
unattended installations, 62
upgrade installations, 82
User Interfaces And Infrastructure features, 67
installer programs, 350
installation failures, 352
InstallShield, 350
Install-WindowsFeature cmdlet, 246–247, 250, 257–260
–Credential parameter, 259–260
–Restart parameter, 260
–Whatif parameter, 260
Install-windowsfeature gpmc cmdlet, 1397
integration testing, 46
integrity
application, 359–368
BitLocker checks, 612
Intel Quick Resume Technology, 108
Intel Quick Resume Technology Driver (QRTD), 108
Intel Virtualization Technology (Intel VT), 508
internal hardware devices, 263–266
internal storage devices, 480–483
Internet
access, 23
connectivity, troubleshooting, 931–932
top-level domains, 1021
Internet Information Services (IIS) 7.0 Administrator's Pocket Consultant, 39
Internet Information Services (IIS) Manager, 142
Internet Printing Client, 233
interrupts
excessive, 451
false, 451
hardware, 452
intrusion detection, 57
I/O (input/output) subsystem, 621, 624
reparse points and, 644

IP addresses, 75–76
100/100 failover technique, 956–957
address ranges, planning, 964
address space, managing, 946–948
alternate, 913
assigning, 941. *See also* DHCP (Dynamic Host Configuration Protocol)
configuration details, viewing, 928–929
configuring, 913
conflicts, preventing, 1007
DHCP leases, 913, 936–937
diagnosing and resolving problems, 933–934
domain names, resolving, 1047. *See also* DNS (Domain Name System); name resolution
dynamic, 913, 917–919
exclusions, 942, 964, 974–976
fixed, 942
multiple, 919–921
pinging, 932
planning assignment, 910–911
public Internet resources, 1041
for remote clients, 943
reservations, 964, 966, 976–980
reserved vs. static, 976
resolving computer names to. *See* name resolution
resolving to NetBIOS names, 1113. *See also* WINS (Windows Internet Naming Service)
scopes of, 942
standard options, setting, 990
static, 913–917, 976
testing, 914–916
IP Address Management Server, 233
IPAM (IP Address Management), 946–948
provisioning, 947
security groups, 946–947
Ipconfig command, 146, 929, 934–935
DNS client information, retrieving, 938
DNS names, registering, 939
DNS resolver cache, flushing, 940
IP address, releasing and renewing, 979–980
lease settings, releasing and renewing, 937
network adapters, specifying, 938
resolver cache, viewing records, 939
user class memberships, viewing, 989
IP datagrams, 875
IP (Internet Protocol). *See also* **TCP/IP (Transmission Control Protocol/Internet Protocol)**
as replication transport protocol, 1448–1449
IPsec (Internet Protocol security)
with IPv6 addressing, 903
network routing and, 936
IP spoofing, 1044–1045
IPv4 addressing, 880, 883–888, 913. *See also* **DHCP (Dynamic Host Configuration Protocol)**
address classes, 884–886
addresses, getting and using, 898–900
addressing plan, 900
address space limitations, 898, 900
autoconfiguration, 943
broadcast addresses, 887–888
Class A networks, 884, 893–894
Class B networks, 884–885, 895–896
Class C networks, 885, 896–897
Class D addresses, 884, 886
Class E addresses, 884
data packets, 897
DHCP relay agent, configuring, 1012–1014
diagnosing and resolving problems, 933–934
failover scopes, 953
host groups, 886
host IDs, 883, 889
loopback addresses, 885, 888
multicast addresses, 886–887
network IDs, 883, 889
normal scopes, creating, 964–969
packet headers, 897
payloads, 897
private addresses, 886, 888, 898, 914
private to public address translation, 886
proxies, 886
public addresses, 885, 891, 898, 900
reserved addresses, 888–889
rules, 888–890
split scopes, 957
static addresses, configuring, 917
subnetting, 890–897
unicast addresses, 883–886
WINS name resolution, 1113. *See also* WINS (Windows Internet Naming Service)
IPv4 communications, monitoring performance, 440
IPv6 addressing, 880, 900–903, 913. *See also* **DHCP (Dynamic Host Configuration Protocol)**
64-bit processors and, 900
autoconfiguration, 944–945
decimal notation, 901
DHCPv6 stateful mode, 944–945
DHCPv6 stateless mode, 944–945, 953
diagnosing and resolving problems, 934
DNS server addressing, 939
double-colon notation, 901
global unicast addresses, 902
hexadecimal notation, 901
IP security, 903

IPv6 addressing (*continued*)
jumbograms, 902–903
link-local unicast addresses, 902
loopback addresses, 902
multicast addresses, 902
normal scopes, configuring, 969–972
packets, 902
private addresses, 914
security, 900
static addresses, configuring, 916
subnet prefix length, 902
TCP/IP enhancements for, 881–882
temporary and nontemporary addresses, 971
unicast addresses, 901
unspecified addresses, 902
IPv6 communications, monitoring performance, 440
IRQ settings, shareability, 298
ISA devices, IRQ settings, 299
ISA interrupts, 299
iSCSI cmdlet, 486
iSCSI Initiator, 142
iSCSI (Internet SCSI), 264, 481
backups of virtual disks, 489
dedicated network, 482
device discovery, 505
initiators, 482
IscsiTarget cmdlet, 486
iSCSI Target Server service, 490, 691
iSCSI Target Storage Provider service, 489, 691
iSNS (Internet Storage Name Service), 482
iSNS Server service, 233, 485
ISTGs (Inter-Site Topology Generators), 1253, 1255
bridgehead server connections, load balancing, 1459
determining, 1457–1458
processing overhead, 1457
processing overhead, reducing, 1455
replication topology, generating, 1256, 1258, 1261
site-link prioritization, 1447
IT staff
deployment planning, 13–14
responsibilities, delineating, 824
security, assigning tasks, 32–33

J

jumper settings, 300

K

KCC (knowledge consistency checker), 1238
CPU utilization, 1272
manually running, 1240
Options attribute, modifying, 1468
replication topology, generating, 1248–1249, 1256, 1258, 1260–1261
running, 1240
unbalanced connections, 1240
KDC (Key Distribution Center), 1180
RODCs as, 1318–1319
Kerberos, 23
armoring, 765
clock synchronization tolerance, 1366, 1384
Kerberos Policy, 1349–1350, 1404
trust establishment, 1183–1189
Kerberos authentication, 1178–1183
components of, 1180
delegated authentication, 1197
Key Distribution Center, 1180
process, 1180–1181
Kerberos Ticket Granting accounts, 1319
kernel memory, 386
kernel memory dumps, 830
KTM (Kernel Transaction Manager), 647

L

L1 cache, 384
L2 cache, 384
LANs (local area networks), DHCP relay agents, 950
Last Known Good Configuration
booting to, 317
Last Known Good Configuration startup mode, 869
LCAP (Link Aggregation Control Protocol), 456
LDAP (Lightweight Directory Access Protocol), 1140, 1151
Active Directory use, 1164
directory store access, 1397
lookups, 1276
LDM Data partitions, 552
LDM Metadata partitions, 552
Ldp.exe
DSHeuristics attribute, modifying, 1144
RID pool ceiling, removing, 1208
legacy applications, 350, 359
access tokens, 361
virtualization of file system and registry, 361
write failures, redirecting, 307
legacy clients
Active Directory access, 1141
NTLM authentication, 1179
legacy devices, 293–294
legacy operating system BCD store entry, 117
Legacy OS Loader (NTLDR), 117

LGPOs (Local Group Policy Objects), 1394–1397
account policy for, 1346
conflicts, resolving, 1394–1395
managing, 1396
multiple, 1394
processing order, 1394
top-level, 1395–1396
user types, 1394
licensing
evaluating, 20
product IDs, 64
for Remote Desktop, 177
Windows Server 2012, 5–6, 63–64
limited broadcasts, 888
Link-Layer Topology Discovery Mapper I/O Driver, 77
Link-Layer Topology Discovery Responder, 77
Link To Web Address snap-in, 208
Link To Web Address Wizard, 208
listening ports, 436
List Shadows command, 793–794
List ShadowStorage command, 794–795
live migrations, 508
enabling, 510
LLMNR (Link-Local Multicast Name Resolution), 881, 907–908, 1034–1035
controlling, 1035
disabling, 908
reverse mapping, 908
LMHOSTS file, 906, 924
load balancing
on bridgehead servers, 1239–1240
dynamic least queue depth, 500
in failover scopes, 952–954
MPIO policies, 502
NIC teaming and, 456–457
round robin for, 500, 1085–1086
split scopes for, 956
weighted path, 500
local accounts, 349
local computers, 201–203
local drives, backing up to, 847
Local Group Policy, 1388–1389, 1394–1397
Local Group Policy Editor, 1396–1397
Local Group Policy Object Editor, 1393
localization, 20
local security policy, 142
advanced auditing, configuring, 773–775
basic auditing, configuring, 771–773
global access policy, configuring, 778–779
registry security settings, 344–345
registry virtualization settings, 307
UAC settings, 357–359, 368
user rights, assigning, 1357
Local Security Policy console, 357–359, 1396
Local Users And Groups, 161
log files
registry hive, 321–322
size of, 462
logging. *See also* **data collector sets**
Active Directory database events, 1143
Active Directory data store transactions, 1148
Active Directory performance, 1466
data collector reports on, 467
default location, 462
DHCP events, 998–1001
disk quota violations, 670
expiration date, 462
performance data, 457–476
scheduling, 461–462
trace logs, 475
logical drives, 522
deleting, 549
drive letters, configuring, 539–541
I/O activity, tracking, 435
logical processors
idling, 104–106
workload graphs, 383
logoff
forcing, 1405, 1437
logoff scripts, 1423–1424
logon
authentication, 1176. *See also* authentication
with cached credentials, 1366
events at, 1419
logon hours, 1405
logon scripts, 1364, 1419, 1423–1424
mechanisms for, 1138
restrictions, 1349
security token assignment, 1176
traffic, isolating, 1235
UPN assignment, 1176
logon sessions
disconnecting vs. logging off, 190
viewing and managing, 189–190
LPR Port Monitor, 233
LSA (Local Security Authority), 360
Active Directory, 1137–1139
functions, 1137
LUNs (logical unit numbers) of virtual disks, 506

M

MAC (Media Access Control) addresses, 942
- of network interfaces, 977

mail exchange servers, 1087–1088

maintenance
- automated, 672–680
- Check Disk, running, 675–677
- fragmentation, preventing, 680–682
- managing, 673
- software maintenance, 349–350

manageability, planning deployment for, 45–60

managed servers, 229
- roles and features, managing, 238–245
- roles and role services, viewing, 237–238

management application interface, 191. *See also* **MMC (Microsoft Management Console)**

Manage The TPM Security Hardware Wizard, 572, 577–583

manifest files, 280

man-in-the-middle attacks, 1275

MAPI (Messaging Application Programming Interface), Active Directory support, 1141

MBAM (Microsoft BitLocker Administration and Monitoring), 617

MBR disks, 521–525
- boot and system volumes, mirroring, 559–560
- configuration, 533
- converting to GPT, 524–525
- drive letter assignments, 534
- dynamic disk database, 526
- extended partitions, 522
- FAT/FAT32, converting to NTFS, 531–532
- formatting, 524
- maximum volume size, 522
- mirrored system volume, rebuilding, 567
- primary partition, 522
- storage type, changing, 526

MBR (master boot record), 109, 522

MBR partitions
- on basic disks, 533–549

media
- for backup and recovery, 836–837, 841
- installation media, 1294–1297

Media Foundation, 234

member servers
- backup files in registry, 322
- viewing, 876

memory. *See also* **physical memory; virtual memory**
- adding, 387, 448
- bottlenecks, 448–451
- composition, 386
- current commit charge, 373
- maximum allowed for operating system, 115
- performance counters for, 449–451
- performance, monitoring, 440
- per-process usage, 432–434
- physical configuration, 387
- process usage, 394
- usage statistics, 375, 381–382, 385–386

memory protection with Data Execution Prevention, 131

Memtest.exe, 126

menu commands, 215
- creating, 222–223
- running, 215

Message Queuing, 234

Microsoft accounts, 349

Microsoft Application Compatibility Toolkit, 362

Microsoft DNS, 38

Microsoft DSM, 500, 504

Microsoft Exchange Server 2010 Administrator's Pocket Consultant, 1168

Microsoft Fix It Portable, 336–338
- Program Install And Uninstall Troubleshooter, 337–338

Microsoft Project, 28

Microsoft Reliability Analysis task (RacTask), 438–439

Microsoft Saved Console file. *See* **.msc files**

Microsoft Software Shadow Copy Provider, 782

Microsoft\Windows log, 407

Microsoft Windows PowerShell 2.0 Administrator's Pocket Consultant (Stanek), 21

Minimal Server Interface installations, 66–67
- converting to Server Core, 98
- converting to Server With A GUI, 98

mirrored sets
- breaking, 565
- configuring, 558–559
- resynchronizing, 565–566
- system volumes, rebuilding, 567–568
- troubleshooting, 565–566

mirrored volumes, 553
- boot volumes, 559–563
- system volumes, 559–563

mirroring the operating system, 74

MLDv2 (Multicast Listener Discovery version 2), 882

MMC 3.0, 192

Mmc.exe, 197
- file associations, 198

MMC (Microsoft Management Console), 191
- 32-bit and 64-bit versions, 197–198
- author mode, 194–196
- console tools, building, 203–214
- console tree, 196
- custom taskpads, designing, 215–227

MMC (Microsoft Management Console) (*continued*)
- main pane, 196–197
- remote computers and, 201–203
- remote computers, connecting to, 413
- /S command parameter, 197
- snap-ins, 191–194
- user mode, 194–196
- window, 196–198

mobile computer power state transitions, 102

Modified Fast Recovery Algorithm, 880

monitoring, 53
- backups, 55
- outside-in, 54
- performance. *See* performance monitoring

motherboards/chipsets, 103
- power states, 107–108

mount points
- configuring, 541–543
- volume, 788

Mountvol, 486

Mpclaim
- multipath I/O, configuring, 503
- multipath I/O, uninstalling, 504

MPIO (Microsoft Multipath I/O), 234, 485, 500–501
- devices, adding, 501, 503
- devices, removing, 504
- iSCSI devices, automatic claiming, 502
- load-balancing policy, 502
- managing, 504–505
- snapshot of, 505
- Windows PowerShell cmdlets for, 501

MPIO tool, 142

.msc files
- command parameters, 197
- for console tools, 200–201
- file path to, 197
- overwriting, 204

_msdcs subdomain, 1050

MSR (Microsoft Reserved) partitions, 72, 523, 550–551
- creating, 561–562

multicasts
- IPv4, 886–887
- IPv6, 902

multipath devices, discovering, 504

multipath I/O, 484
- configuring, 500–505
- installing, 500–501

multiple-item selecting and editing, 192

N

named pipes, 725

name resolution, 40, 903–906, 1047
- broadcast messages for, 1115
- DNS, 903–907. *See also* DNS (Domain Name System)
- LLMNR, 907–908
- NetBIOS, 1114
- for Windows Vista and later, 908
- WINS, 906–907, 1113–1132

name squatting, 1038

NAP (Network Access Protection), integration with DHCP, 1003–1007

NAS (network-attached storage), 480–481
- server-storage communications, 480–481
- Windows Storage Server 2012, 491

NAT (Network Address Translation), 886

navigation components, 215

navigation tasks, creating, 224–227

Nbtstat, 146

Neighbor Unreachability Detection for IPv4, 881

Net, 146

NetBIOS names
- cache of, 1116
- namespace and scope, 1113–1114
- node types, 1115
- registering and resolving, 1113. *See also* WINS (Windows Internet Naming Service)

NetBIOS (Network Basic Input/Output System), 22
- computer names, pinging, 932
- IPv6 and, 907
- name resolution for, 924
- WINS for, 906–907

NetBIOS over TCP/IP, 907

Net command-line tools, 147

.NET Framework 3.5, 232

.NET Framework 4.5, 232

Net Share command, 723, 727, 763–765

Netsh command, 146, 934–935
- DNS client IPv4 and IPv6 information, viewing, 1100–1101
- IPv6 addresses, adding, 939
- IPv6 router M and O flag configuration, 950–951

Netsh DHCP command, 962
- configuration settings, saving and restoring, 1008
- conflict detection, configuring, 1007
- database properties, setting, 1010–1012
- database properties, showing, 1009
- database, starting and stopping, 1010
- exclusion ranges, defining, 975–976
- exclusions, displaying, 975

Netsh DHCP command (*continued*)
leases, terminating, 974
normal scopes, creating, 972–973
reservations, creating, 977–979
reservations, listing, 976
scopes, activating and deactivating, 974
servers, authorizing, 963
server scope commands, 973
Netsh WINS command, 1118–1119
registrations, viewing, 1128–1129
scavenging, initiating, 1129
server configuration details, viewing, 1127–1128
server statistics, viewing, 1126–1127
Netstat, 146
Network Access Policy servers, 1012
network adapters
aggregating, 456–457
balancing load across, 456
bandwidth, 455
configuration, viewing, 928–930
failover between, 456
installing, 911
mixed-state settings, 879
multiple, 455
network category settings, 877
performance, monitoring, 440
Remote Direct Memory Access, 494
selecting by name, 938
send and receive speed, 455
TCP/IP configuration settings, 877, 879
teaming, 436
transmission preference settings, 284–285
types, 880
virtual switches on, 509–510
Network And Sharing Center, 875, 878–879
network broadcasts, 887
network connections, 912
bytes sent and received, 927
connection duration, 927
connection speed, 927
enabling and disabling, 930
IPv4 connection state, 927
IPv6 connection state, 927
managing, 926–931
media state, 927
renaming, 930–931
status, viewing, 926–928
troubleshooting, 931
network devices
mapping, 719–720
power protection, 823
recovery plans, 822–823
Network Diagnostics Framework, 881
Network Discovery, 876–877
Network Explorer, 875, 877–878
browsing network, 721
network category, changing, 877
network fax share, 725
Network icon, 169
networking, 909
addressing, 19
administration, 23–24, 33
bandwidth availability, 454
bandwidth, per-process usage, 435–436
booting from, 109
bottlenecks, 454–457
bridges, 890
browsing, testing, 933
cables, installing, 51
capacity, 454
change control, 54–55
classful networks, 887
components, installing, 76–77
costed networks, 1428
counters for, 455
dependencies in, 22
discovery, 876–878, 933
disk time and processor time and, 455
documentation of, 24
domain networks, 876
essential services and systems, 822
existing infrastructure, analyzing, 18–26
fault tolerance, 822
gateways, 890
infrastructure, planning, 899
internal networks, 1021
IPv4 addressing, 883–888, 898–900
IPv6 addressing, 900–903
latency, 454
link failures, 1267
local IP routing table, 935
management and growth and, 18
management tools, assessing, 25
monitoring, 53
name resolution, 903–906
Network And Sharing Center, 875
Network Discovery, 876–877
Network Explorer, 875
Network Location Awareness, 876
network maps, 19
network operations, changes in, 31–32
network services, identifying, 21–22
network settings, managing, 878–879
network topology, 19. *See also* network topology

networking (*continued*)
new configuration, defining, 31–35
nonclassful networks, 887
physical network configuration, 19
planning, 35–36
private networks, 876
protocols, 75–76
proxies, 886
public networks, 876
responsiveness, 454
routers, 890
Safe Mode With Networking startup mode, 869
security, 22–23, 945–946
subnetting, 890–897
switches, 899
TCP/IP, 909–940
TCP/IP backbone, 875–908
traffic, 19
traffic management, 1233
usage statistics, 381–382, 400–401
Windows Internet Naming Service, 906–908
Windows Network Diagnostics, 875
Windows Server 2012 features, 875–883
network interfaces
device unique identifier, 977
DHCP Server service, binding to, 1001
MAC addresses, 977
multiple IP addresses, 919–921
network numbers, 889
unicast IPv4 address, 883
user class memberships, viewing, 989
Network Level Authentication, 402
Network Load Balancing Manager, 142
Network Location Awareness, 876
network management, 191. *See also* **MMC (Microsoft Management Console)**
Network Policy and Access Services, planning usage, 39
Network Policy console, 1003
Network Policy Servers, 142, 1003–1007
network resource management, 1135. *See also* **Active Directory**
Network Solutions, 898
network topology, 19
hub-and-spoke design, 1267
mapping, 1260–1262
site-link bridging and, 1267–1268
sites in, 1233
subnets in, 1233
Network Unlock, 585–586, 594–595
installing, 602
New-ADDCCloneConfigFile cmdlet, 1298–1299
New-ADFineGrainedPasswordPolicy cmdlet, 1350
New-ADUser cmdlet, 1359
New Delegation Wizard, 1072–1074, 1293
New-MSDSMSupportedHw cmdlet, 504
New RAID-5 Volume Wizard, 564–565
New Scope Wizard
normal scopes for IPv4 addresses, creating, 964–969
normal scopes for IPv6 addresses, creating, 969–972
New Share Wizard, 736
New Simple Volume Wizard, 534–538
New-SmbShare cmdlet, 727
New Taskpad View Wizard, 218–220
New Task Wizard, 221–227
New Virtual Machine Wizard, 512–513
New Volume Wizard, 702–704
data deduplication, configuring, 709
Next Generation TCP/IP stack, 880–882
NFS file shares, 736–737
NFS (Network File System), 481, 490
support, adding, 481–483
NIC (network interface card) teaming, 436, 455–457, 879
status, showing, 153
teaming modes, 456
NLB (Network Load Balancing), 234
nodes, snap-in, 193
in console tree, 196
nonclassful networks, 887
host IDs, 889
network number, 889
nonexecute page protection (NX) feature, 131–132
nonfixed disks, 525
nonpaged pool, 386
monitoring, 448–449
size, 450
non–Plug and Play devices
adding, 293–294
displaying in device list, 279
normal backups, 835–836. *See also* **backups**
notification area, 172–174
notifications
of additional installation tasks, 242–243
of disk quota violations, 671
of emergency and security incidents and outages, 825
NPAS (Network Policy and Access Services) role, 231
NPTs (nested page tables), 508
NRPT (Name Resolution Policy Table), 1078
Nslookup, 146, 1102
starting, 940
Ntdsa.dll, 1138, 1141

Ntds.dit, 1148, 1150, 1161
fields, 1149
indexed tables, 1149
Ntdsutil
domain controllers, creating from backup media, 1295–1296
failed domain controllers, cleaning references to, 867–868
RODCs, installing, 1330–1332
NTFS compression, 656–659
NTFS (NT file system), 536, 621, 628–636
advanced features, 637–649
analyzing volumes with ChkDsk, 678–679
boot sector, 629
change journals, 640–643
Check Disk scans, 674–675
cluster size, 623, 633–634
data streams, 638–640
disk integrity, 672–675
disk quotas, 661–671
extending, 628
FAT/FAT32 partitions, converting, 531–532
features, 633–634
file and folder information, 630
file screening, 797
file size limit, 505
hard links, 637–638
master file table, 629–633
metadata, 629, 649
MFT zone, 632–633
object identifiers, 643–644
on-disk store engine, 651
permissions, 716, 755–757
vs. ReFS, 649–650
reparse points, 644–645
resident and nonresident attributes, 630
restructuring volumes, 628
Self-Healing NTFS, 648
shadow copy support, 715–716
share permissions, 748
sparse files, 645–647
storage reporting, 797
structure, 629–633
structure, analyzing, 634–636
transactional, 647–648
volume size, 505
Ntldr, 110, 117, 314
NTLM (NT LAN Manager)
authentication, 1178–1179, 1187
trusts, 863
Ntuser.dat, 321
Nvrboot.efi, 110

O

object classes, 1168
object identifiers, NTFS, 643–644
objects
access control entries, 1360
access control lists, 1136
Active Directory schema, 1142
attributes, replicating, 1168–1171
changes to, tracking, 1251–1252
classes, 1151
common names, 1157
container objects, 1151
in data store, 1149
deleting, 1145–1146
directory tree, 1152–1154
distinguished names, 1141, 1157, 1164
domains, 1152–1153
full control over, 1311
globally unique identifiers, 1141–1142
grouping for management, 1227, 1228
inetOrgPerson objects, 1226
inheritance of permissions, 1312
leaf objects, 1151
linked attributes, 1149
in organizational units, 1226
parents, 1157
performance, monitoring, 440
policy rules, 1151–1152
recycled, 1147
relative distinguished names, 1141, 1157, 1164
schema rules for, 1151
searching for, 1164–1165
security descriptors, 1149, 1360
tombstoned, 1145–1146
uSNChanged attribute, 1251–1252
version store, 1143
ODBC (Open Database Connectivity), 316
ODX (Offloaded Data Transfer), 691–694
functionality, 692–693
support for, verifying, 693
operating system. *See also* **system; Windows 8; Windows Server 2012**
activating, 165–166
advanced management features, 167
default, 112, 133, 829
display order, 132
in domain functional levels, 1171–1173
dual IP layer architecture, 880
edition and version, 165
in forest functional levels, 1173–1174
identifying and documenting, 20
loader applications, 124

operating system (*continued*)
memory, maximum amount for, 115
mirroring, 74
notifications for, 172
partitions used by, 71
power-state management, 103
processors, number of, 115
recovering, 842, 858–859
timeout interval, 113
tuning, 97
operating system drives
BitLocker, enabling, 611–615
Group Policy BitLocker settings, 599–600
Operational log
backup events in, 850–851
recovery events, 855
operations masters, 43–44
design considerations, 1200–1214
domain naming masters, 1205
flexible single-master operations (FSMO) role, 1201
infrastructure masters, 1212
listing, 1202
PDC emulators, 1209–1212
placement of, 1203
RID masters, 1206–1209
roles, changing, 1202
roles, seizing, 1212–1214
roles, transferring, 1202
schema masters, 1203–1204
operations team, 54
Optimize Drives
command-line version, 683–686
disk optimization, 680–682
fragmentation analysis, 680–682
free space requirements, 683
graphical version, 683
manual disk analysis and optimization, 682–686
OSLOADER applications, 117
BCD store entry options, 129–131
OUs (organizational units), 41, 1215
accounts, placing in, 1310–1311
administration, delegating, 1311–1314
administration model, 1231–1232
canonical name, 1310
COM+ partition, 1310
cost center model, 1231
creating, 1307–1309
delegating with, 1227–1228
deleting, 1308
deletion protection, 1308
descriptive information, 1310
designing, 1228–1232
division or business unit model, 1229
full control over, 1311
geographic model, 1230
GPOs linked to, 1389
group policy inheritance, 1416
Group Policy permissions, 1407–1409
manager of, 1310
multiple levels, 1227, 1228
object attributes, 1310
objects, grouping for management, 1227, 1228
objects in, 1226
planning, 1225–1232
properties, setting, 1309–1310
Remote Desktop Services, 182
resources, placing in, 1310–1311
user rights, assigning, 1355–1356
outages
post-action reporting, 826
prioritizing, 825
responding to, 824

P

packet filtering, 936
PAE (Physical Address Extension), 125
configuring, 132
paged pool, 386, 394
monitoring, 448–449
size, 450
page faults, 394, 449
average number per second, 449
Pagefile.sys, 372
paging file partitions, 71, 526
paging files
address space limits, 374
configuring, 375–377
creation of, 371–372
disk speed and, 453
location and size information, 376
maximum size, 374
moving, 377
multiple, 372
peak size, 450
percentage used, 450
performance and, 448–449
performance, monitoring, 440
RAID configuration and, 373
RAM and, 387
sizing, 372–373, 377
SSDs for, 372
Parallel SCSI (SPI), 264
parity error checking, 564

partitions
- active, 525
- Active Directory, 1158–1159
- on basic disks, 525
- BitLocker partition, 597
- boot, 525
- bridgehead servers for, 1459
- checking and finalizing, 97
- crash dump, 526
- creating, 90–91, 534–538
- default application directory partitions, 1094–1096
- defined, 514
- deleting, 90–91, 549, 561
- drive letters, configuring, 539–541
- EFI system partition, 523
- ESP, 549–550
- extended partitions, 522, 534
- extending, 90–91, 543–546
- file and folder compression, 537
- formatting, 524, 536–537
- formatting without error checking, 537
- GPT style, 521–525
- labels, 537
- listing, 517
- MBR style, 521–525
- Microsoft Reserved partition, 523
- mount points, configuring, 541–543
- MSR partitions, 550–551
- multiple, 72
- for operating system, 71–74
- paging file, 526
- primary partitions, 522, 534, 551–552
- removing during installation, 89
- replication of, 1258
- shrinking, 546–548
- system, 526
- vs. volumes, 71

passive cooling, 104

Password Replication Policy, 1336–1344
- accounts, allowing or denying, 1338–1340
- Advanced Password Replication Policy dialog box, 1340–1341
- Allowed, Denied, Revealed, Authenticated To lists, 1336–1337
- built-in groups, 1337
- configuring, 1323–1324, 1327, 1334
- credentials, viewing and managing, 1340–1341
- managing, 1338
- Resultant Set of Policy, 1341–1342

passwords
- caching on RODCs, 1322–1323, 1336. *See also* Password Replication Policy
- changes, processing, 1209–1210
- changes, replication of, 1250
- complexity requirements, 1348
- for computer accounts, 1383
- maximum age, 1347
- minimum age, 1348
- minimum length, 1348
- password history, 1347
- password policies, 1347–1348, 1350
- Password Policy, 1404
- password reset disk, 1371–1373
- plain text encryption, 1348
- prepopulating, 1340–1341
- recovery and restores and, 863
- resetting, 1227–1228, 1342–1343, 1370–1371

PATA (Parallel ATA), 264

Pathping command, 147, 935

payloads
- alternate source file path, 248, 249
- download issues, troubleshooting, 249
- download restrictions, 248
- managing, 245–250
- restoring, 247–248
- Windows Update as source, 248

PCI devices
- IRQ settings, 299
- resource conflicts, 300–301

PCI interrupts, 299

PDC emulators, 44, 1209–1212
- clones, verifying, 1297
- GPO creation and editing changes, 1393
- locating, 1211
- password change replication, 1250
- placement of, 1203
- RODCs, communication paths to, 1319
- role, transferring, 1211–1212
- SRV records, 1091
- time synchronization, 1210–1211

performance
- of Active Directory, 1466
- baselines, establishing, 426–439
- BitLocker Drive Encryption and, 584
- bottlenecks, 448–457
- counter data, collecting, 462–464
- CPU utilization and, 384–385, 429–431
- disk I/O bottlenecks, 452–454
- disk-related, 434–435
- graphical depiction, 437
- hard page faults and, 449
- logging, 457–476
- memory bottlenecks, 448
- memory-related, 432–433

performance (*continued*)
monitoring, 161. *See also* performance monitoring
multiple systems, comparing, 447
network bottlenecks, 454–467
of network connections, 436
paging file size and, 373
paging file use and, 448–449
performance counter alerts, 470–471
postinstallation baselines, 426
processor affinity and, 451
processor bottlenecks, 451–452
roles, role services, and features and, 230
of services, 397–400
of storage, 505
test baselines, 426
trace data, collecting, 464–466
troubleshooting, 382
tuning. *See* performance tuning
typical usage baselines, 426
performance alerts, configuring, 154
Performance Monitor, 425, 439–447
counter list, copying and pasting, 444
counters, 436–437, 439. *See also* counters, performance
data collector reports, viewing, 467–468
data collector sets, creating and managing, 458–462
Data Collector Sets node, 457
data collector sets, using, 459–462
data collector templates, 459–460
display, 443–446
graphs, 443
Histogram Bar view, 445
Legend, 443, 447
performance counter alerts, configuring, 470–471
performance object instances, 439
performance objects, 439–442
remote monitoring, 446–447
replication, monitoring, 1465–1466
Reports node, 457
Report view, 446
sampling interval, 443
Toolbar, 444
Value Bar, 443
views, 443–446
performance monitoring
from command line, 471–474
essentials, 378–381
event traces, 458
network usage, 400–401
with Performance Monitor, 439–447
per-process resource usage, 427–436
processes, 391–397
processor and memory usage, 381–388
remote, 446–447
running applications, 388–390
services, 397–400
user sessions, 402–405
Windows PowerShell cmdlets, 474
Performance Monitor Users group, 446
performance state, managing, 104
Performance tool, 161
performance tuning
operating system performance, 369–370
processor scheduling, 370–371
virtual memory, 371–375
permissions. *See also* **credentials; privileges**
access control lists, 1136
access permissions, 748–763
Apply Onto options, 757
basic permissions, 753–757
changing, 751–752
cumulative, 761
delegating, 1311–1314
denying, 744–748
determining, 1360–1361
effective, 761–763
Effective Access tool, 1360
Effective Permissions tool, 1382
granting, 745–748
on groups, 743
inheritance, 750–752, 1312
inheritance, stopping, 751–752
NTFS, 716, 755–757
on public folders, 716
on REG command, 339–340
on Registry Editor, 338–339
on registry keys, 340–343
resetting, 752
on shares, 716, 729, 734–735, 742–748
for snap-ins and tasks, 227
special permissions, 757–761
Take Ownership permission, 749
tracking, 763
troubleshooting, 761–763
user and device claims, 762
Permissions icon, 353
physical access to network, 945
physical attacks, protecting against, 569–570. *See also* **BitLocker Drive Encryption; TPM (Trusted Platform Module) Services**
physical disks. *See also* **disks**
512b disks, 519
512e disks, 519
adding, 519–521
disk queue length, 450

physical disks (*continued*)
disk transfer time, 451
I/O activity, tracking, 435
layout, management of, 690
performance, monitoring, 440
read and write request servicing statistics, 450
slabs, 685
standard volumes, creating, 702–704
storage pools, adding to, 699
three-layered architecture, 689–690
physical drives. *See also* **hard drives**
partitions, 514
physical memory, 448
available, 385
available limit, 449
bytes available, 449
currently allocated, 385
for processes, 390
process usage, 432–433
troubleshooting problems, 388
physical security of hardware, 822
PING command, 147, 914–916, 932–933
IP addresses, testing, 914–916
planning deployment of Windows Server 2012, 10–36
Active Directory namespace, 40–41
Active Directory server roles, 43–44
administration methods, 33
availability, 45–60
big picture, 10–12
budget, 29
compatibility issues, 26
contingencies, 29–30
day-to-day operations, 53–58
documentation, 15, 18
domain and forest functional levels, 41–43
domain trusts, 41
estimates of deployment process, 30
existing network infrastructure, analyzing, 10, 18–26
goals, 10, 14–18
highly available servers, 58–60
interaction of IT staff and business units, 16–17
manageability, 45–60
management approval, 31
mission-critical systems, predeployment planning, 58–60
network, 35–36
network change, predicting, 17–18
new installations, 35–36
new network environment, 11, 31–35
organizational objectives, 26
personal information, protecting, 34
scalability, 45–60
scheduling, 28
scope creep, 26
scope, defining, 11, 26–31
server usage, planning, 37–40
teams, identifying, 10, 12–14
testing, 11
Plug and Play, 273, 292
ACPI and, 298
device redirection, 184
interrupt reservations, 92–93
Plug and Play Manager resource mappings, 315
PNRP (Peer Name Resolution Protocol), 234
power button, power state transitions, 102
power consumption, reducing, 104–106
power policy, 104
power protection, 823
power-state management, 102–103, 107–109
Windows desktop vs. Windows Server operating systems, 102
power supplies, redundant, 51
Power Users group, 362
PPPv6 (IPv6 over Point-to-Point Protocol), 881
preferences
in registry, 304
user-specific, in registry, 320
pre-operating system boot environment, 101, 110
managing, 119–134
Print And Document Services role, 231
planning usage, 39
printer sharing, 725
Print Management, 142
print queue performance, monitoring, 440
print services, assessing, 22
private key encryption, 1036–1037
privileges. *See also* **credentials; permissions**
for administrator applications, 361
administrator vs. standard user access tokens, 360
run-level designations, 362–363
for user applications, 361
problem-escalation procedures, 823–824
Problem Reporting balloons, 295
problem-resolution policy document, 824–826. *See also* **backups; disaster planning; recovery and restores**
problem-resolution procedures, 826. *See also* **disaster planning; disaster preparedness**
problem situations. *See also* **recovery and restores; troubleshooting**
help desk structure, 56
response planning, 56

processes
32-bit and 64-bit, isolating, 392
vs. applications, 378
CPU usage, 429–431
disk activity, 434–435
grouping by type, 389
handles, 431
information about, 390–391
listening ports, 436
memory usage, 432–434
modules, 431
monitoring, 391
network bandwidth usage, 435–436
performance, monitoring, 440
resource usage, monitoring, 427–436
service running, 431
statistics on, 393–395
stopping, 396
summary statistics, 384
TCP connections, 436
terminating, 353
processing power, conserving, 369
processor affinity, 106, 451
processors. *See also* **CPUs**
architecture, 109
bottlenecks, 451–452
counters for, 452
hardware interrupts, 452
idle sleep states (c-states), 105
nonidle thread execution, 452
number to use, specifying, 115
performance, monitoring, 440
performance states (p-states), 105
performance statistics, 381
performance, troubleshooting, 431
Privileged mode, 452
problems with, 94–95
resources, managing, 106
scheduling, tuning, 370–371
state, maximum and minimum, 104
throttling, 104–105
User mode, 452
Process Resource Monitor, 377
product management team, 12
Program Compatibility Assistant, 351
program management team, 12–13
programs. *See also* **applications; software**
vs. apps, 349
processor scheduling for, 370–371
Programs And Features page, 352
Provision IPAM Wizard, 947
PSC (Password Settings Container), 1345–1346
PSOs (Password Settings Objects), 1345–1346
creating, 1350
linking to groups, 1354
precedence, 1351
public folder sharing, 716–717
configuring, 718
password protection, 717

Q
QoS Packet Scheduler, 77
Quality Windows Audio Video Experience, 234
Quick Resume mode, 108
Quick Sleep state, 108
quotas on shares, 740
QUSER command, 189

R
RAID devices
hard disk busy time, 453
read and write performance, 454
RAID (redundant array of independent disks)
availability, 506
hardware, 506
paging file location and, 373
planning, 73
RAID 0, 506–507, 555–556
RAID 0+1, 506–507
RAID 1, 506–507, 558–559
RAID 5, 74, 506–507, 553, 564–565, 568
RAID 5+1, 506–507
software, 506
RAM
paging file size and, 387
problems with, 94
problems with RAM modules, 388
Random Interface IDs, 882
RAS Connection Manager Administration Kit, 234
RDC (Remote Differential Compression), 490, 1241
RDMA (Remote Direct Memory Access), 494
Read-Only Domain Controllers group, 1337
read operations
disk reads counter, 454
performance, 680
Receive Window Auto Tuning, 881
recovery and restores, 852–857
Active Directory, 859–868, 1274
on another server, 856–857
application data, 854
authoritative, of Active Directory, 860, 863–865

recovery and restores (*continued*)
automated recovery disks, 97
backup date and time, 853
contingency plans for, 822
current server, 852–856
Directory Services Restore mode, 861–863
disaster planning, 821–826
disaster preparedness procedures, 826–830
domain controllers, 860–861, 866–868, 1294
files and folders, 853
full system, 858–859
GPOs, 1440–1441
group memberships and, 863–864
from incremental and differential backups, 835–836
from installation disc, 827–828
list of files restored, 855–856
managing, 111–113
nonauthoritative, of Active Directory, 861–863
NTLM (NT LAN Manager) trusts, 863
operating system, 828, 858–859
passwords and, 863
planning, 24–25, 55
planning questions, 831
practicing, 56
to previous version of Windows, 78
recovery password, 834
registry, 334–335
restore location, 854–855
server, 828, 841
spare parts, maintaining, 56
startup issues, 868–870
after stop errors, configuring, 828–831
system-state files, 857
Sysvol, 866
testing, 831
update sequence number incrementation, 864–865
virtual machines, 853
volumes, 853–854
with Windows Server Backup, 838
WINS database, 1131–1132
recovery keys, 613
recovery passwords, 605
Recovery Wizard, 852–857
redundancy, disk mirroring and, 558
ReFS (Resilient File System), 491, 524, 531, 536, 543, 546, 621, 649–656
advantages, 653–654
B+ trees, 651–652
checksums, 652, 654
cluster size, 623, 653
data integrity, 652
data scrubbing, 655
data streams, 654–655
features, 649–651
file identifiers, 653
file sizes, 653
hierarchical allocators, 653
vs. NTFS, 649–650
on-disk store engine, 651
salvage, 655
shadow paging, 654
share permissions, 748
Storage Spaces integration, 650–651, 656
structures, 651–653
volume sizes, 653
REG_BINARY data type, 322
REG command, 324
permissions on, 339
subcommands, 333–334
REG_DWORD data type, 322
modifying, 326–327
Regedit.exe, 310
permissions on, 338
Regedt32.exe, 310
Reg.exe permissions, 338–340
REG_EXPAND_SZ data type, 323
.reg files, 329–330
REG_FULL_RESOURCE_DESCRIPTOR data type, 323
registry, 303–347
32-bit and 64-bit keys, 312
access, auditing, 345–347
access, preventing, 338–340
Administrative Templates, 1390
administrator permissions for changes, 324
application settings, 305, 338
backing up, 324, 334–335
CacheLockingPercent key, 1019
changes, distributing, 331
changes, tracking, 331
command-line administration, 333–334
components, uninstalling, 335–336
configuration changes, recording, 466–467
configuration information in, 303
data, dynamically created, 320–322
data, importing and exporting, 329–331
data prioritization settings, 183
data stored on disk, 320–322
data types of value entries, 322–323
domain-based root server entries, 1244
domain controller backup files, 322
Fix It Portable, 336–338
hierarchical structure, 304, 306–311
hive files, copying, 332
hive files, loading and unloading, 332

registry (*continued*)
hives, 308
hives written to disk, 321
HKEY_CLASSES_ROOT key, 319
HKEY_CURRENT_CONFIG key, 319
HKEY_CURRENT_USER key, 320
HKEY_LOCAL_MACHINE, 311–313
HKEY_USERS key, 311, 318–319
HKLM\BCD00000000 key, 313–314
HKLM\HARDWARE key, 314–315
HKLM\SAM key, 315
HKLM\SECURITY key, 315
HKLM\SOFTWARE key, 315–316
HKLM\SYSTEM key, 317–318
InProgress key, 337
installation failures, removing settings, 337
keys, 310
keys, access permissions on, 340–343
keys, adding, 327–328
keys, redirected, 312
keys, removing, 328
keys, shared, 312
LocalAccountTokenFilterPolicy key, 158
managing with preferences, 329
managing with Windows PowerShell, 334
memory usage, 309
operating system settings, 304
optimizing, 335–338
physical and logical structure, 307–308
reading, 309
recovering, 336
redundancies and fail-safe processes, 321
REG command, 324, 333–334
REG SAVE command, 334–335
remote access, restricting, 343–345
on remote computers, modifying, 328–329
Remote Registry service, 345
RID Block Size value, 1206
root keys, 309, 311–320
root keys, backing up, 334–335
searching, 324–325
securing, 338–347
settings, 303
settings, cleaning out, 336
storage in memory, 309
subkeys, 309
subtrees, 310, 311
system state information, 304
tools for, 306
TPM authorization information, 574–576
Transactional Registry, 306
updating, 321
user-profile directories, 321
value entries, 309, 322–323
values, 309, 310
values, adding, 327–328
values, modifying, 325–327
values, path to, 307
values, removing, 328
virtualization, 305, 307, 361
Registry Editor, 309
auditing, configuring, 346–347
hive files, loading and unloading, 332
keys, adding, 327–328
keys, removing, 328
keys, setting permissions on, 340–341
permissions on, 338–339
registry data, importing and exporting, 329–331
remote computers, modifying registry settings, 328–329
searching registry, 324–325
starting, 324
values, adding, 327–328
values, modifying, 325–327
values, removing, 328
versions of, 310
Windows Clipboard and, 327
REG_LINK data type, 322
REG_MULTI_SZ data type, 323
modifying, 326
REG_NONE data type, 322
REG_QWORD data type, 322
REG_RESOURCE_LIST data type, 323
REG_RESOURCE_REQUIREMENTS_LIST data type, 323
REG SAVE command, 334–335
REG_SZ data type, 323
modifying, 325–326
relay agents, 950, 951, 1011–1015
IPv4, 1012–1014
IPv6, 1014–1015
release management team, 13
reliability
monitoring, 161
multiple DHCP servers, 952
Reliability Monitor, 295, 425, 437–439
reports, 438
Save Reliability History option, 438
remote access
console sessions, multiple, 403
enabling, 402
user connection information, 403–404
Remote Access Management, 142
Remote Access role, 231
Remote Assistance, 8, 234

remote computers
- authentication, 179
- with BitLocker, 596
- connecting in DNS Manager, 1053
- device and driver information, viewing, 279
- DHCP servers, connecting to, 962
- encryption, enabling, 496
- events, viewing, 413
- focus, setting on, 202
- Group Policy, refreshing, 1437–1438
- LGPOs, accessing, 1395
- managing, 143–144, 176–189, 1382–1383
- managing with Disk Management, 515
- performance, monitoring, 446–447
- registry hives, loading and unloading, 329
- registry, modifying, 328–329
- remote management, enabling, 157–160
- shares, managing, 726
- snap-ins on, 201–203

Remote Desktop, 9, 176–189
- admin mode, 177
- configuring, 178–182
- disconnecting vs. logging off sessions, 190
- enabling, 159
- licensing, 177
- permitting and restricting logon, 179–181
- Remote Desktop Connection client, 182–189
- Remote Desktop Server mode, 178–179
- System utility settings, 167
- virtual sessions, 177

Remote Desktop Connection, 402–405

Remote Desktop Connection client, 182–189
- admin mode, 185
- client settings, 186–188
- data prioritization, 183
- disconnecting session, 188
- features, 182–183
- flow control, 183–184
- logging off, 189
- Plug and Play device redirection, 184
- resource redirection, 184
- running, 185–188
- virtual session mode, 185

Remote Desktop Services, 176–177, 232, 402–405
- configuring in Group Policy, 181–182
- logon sessions, viewing and managing, 189–190
- OU for, 182
- planning usage, 40

Remote Desktop Services Manager, 189–190

Remote Desktop User group, 179–180

Remote Differential Compression, 234

Remote Event Log Management, 405

remote locations, 19

remote management
- enabling, 157–159, 158
- firewall rules, 202
- Storage Spaces, 158
- Windows PowerShell for, 159

Remote Procedure Call (RPC) over HTTP Proxy, 234

Remote Registry service, 345

remote users
- processes run by, 389
- sessions, tracking and managing, 402–405

removable media, 533
- BitLocker, enabling, 608–611
- BitLocker To Go for, 583
- booting to, 109
- FAT, 625
- file system formatting, 533
- Group Policy BitLocker settings, 600
- write access, 587

Remove-MSDSMSupportedHw cmdlet, 504

Remove Roles And Features Wizard, 243–245

Repadmin, 1213

reparse points, NTFS, 644–645

replication, 43, 44, 1030, 1140, 1142, 1159–1160, 1162–1163, 1233, 1238–1270
- boundary for, 1221–1222
- changes over operating system versions, 1238–1240
- in complex environments, 1259–1260
- compression of traffic, 1219, 1239, 1253, 1462
- directory partitions and, 1257–1260
- disabling, 1467
- of DNS record updates, 1317–1318
- of domain directory partition, 1221–1222
- through firewalls, 1448–1449
- forcing, 864
- granular replication, 1241
- in hub-and-spoke topology, 1268–1269
- intersite, 1234, 1236–1239, 1253–1255, 1447–1462
- intersite replication topology, 1264–1266
- intrasite, 1234, 1236–1238, 1248–1249
- key services, 1247–1248
- managing, 1447–1462
- maximum replication latency, 1256
- monitoring, 1462–1468
- multimaster approach, 1140
- notification of changes, 1253, 1462
- of object attributes, 1238
- partition replication, 1258
- of password changes, 1250
- of priority changes, 1250
- process of, 1246–1247

replication (*continued*)
- push and pull replication partners, 1249
- of read-only Active Directory data, 1316
- replication partner connections, preventing, 1467
- replication partners, 1256–1258
- replication schedule, 1264–1265
- replication traffic, controlling, 1235
- ring topology, 1249–1251, 1256–1260
- on RODCs, 1321
- RPC over IP transport, 1448
- scheduled intervals, 1239, 1253
- schedule for, 1453–1454
- of schema changes, 1252
- security checks, lack of, 1220
- site-link configuration and, 1255
- site-link costs, 1261
- SMTP transport, 1448–1449
- store-and-forward model, 1237
- synchronization, 1462
- of Sysvol, 1240–1241
- TCP and UDP ports, 1248
- testing, 1466–1468
- transport protocols, 1448–1449
- troubleshooting, 1462–1468
- unidirectional replication, 1316
- update delay, 1249
- update sequence numbers (USNs), 1251–1252
- up-to-dateness vector, 1252
- Windows PowerShell cmdlets, 1464–1465

Replication Administrator (RepAdmin), 1463–1464

Reset Password Wizard, 1372

resource conflicts, 298–301

Resource Manager Disk Quotas, 491

Resource Monitor, 425
- columns, adding to panels, 430
- CPU tab, 429–431
- Disk Activity panel, 434–435
- Disk tab, 434–435
- general categories, 427
- global selections, 431
- Memory tab, 432–433
- Network tab, 435–436
- Overview tab, 428
- process resource utilization, 427–428
- Storage panel, 435

resource records, 1022, 1025–1026
- adding, 1082–1092
- DHCID RR, 1038
- DNSSEC, 1037
- listing, 1111–1112
- for new domains, 1293

resources
- access permissions, 1222
- access rules, 766
- Active Directory objects, 1151. *See also* objects
- authenticating access to, 1181–1183
- mappings, 315
- placing in OUs, 1310–1311
- sharing across domains, 1218
- virtualized views of, 305

resource utilization
- baseline, 426
- overview, 428–429
- per-process, 427
- tracking, 378–381

restarts
- automatic, 830
- automatic, disabling, 869
- forcing, 290
- in safe mode, 281
- troubleshooting, 871

Restart-Service cmdlet, 400

Restore AC Power Loss setting, 107

RESUME applications, 117

resume feature, 125

Resume From Hibernate BCD store entry, 125

Resume-Service cmdlet, 400

reverse lookup zones, 1056. *See also* **zones, DNS**
- creating, 1049, 1056, 1064–1065
- dynamic updates, 1068
- forwarding, 1065
- IPv4, 1064, 1068
- IPv6, 1064, 1068
- replication scope, 1068
- resource records, 1082
- types, 1068
- zone files, 1065, 1068
- zone transfers, 1074

Revert Shadow command, 796

RID masters, 44, 1206–1209
- locating, 1209
- placement of, 1203
- role, transferring, 1209
- SID compatibility, 1207–1208

RIDs (relative identifiers), 44
- exhaustion of, 1206
- RID consumption warnings, 1207
- RID pool ceiling, removing, 1208
- RID Reuse pool, 1207

RODCs (read-only domain controllers), 1315–1344
- account, attaching server to, 1335
- account, pre-creating, 1332–1335

RODCs (read-only domain controllers) (*continued*)
administrative permissions, delegating, 1324, 1343–1344
Allowed, Denied, Revealed, Authenticated To lists, 1336–1338
authentication against, 1318
configuration settings, exporting, 1329
credentials, caching, 1318–1319, 1322–1323
credentials, resetting, 1342–1343
credentials, viewing and managing, 1340–1341
database and log folders storage, 1328
delegated administrator users, 1319
design considerations, 1319–1322
directory partitions, replicating, 1321
Directory Services Restore Mode password, 1327
DNS Server service on, 1317, 1323, 1326
domains, preparing for, 1281
inbound replication, 1321, 1322
installation, preparing for, 1323–1324
installing, 1322–1336
installing from media, 1324, 1327, 1330–1332
Kerberos Ticket Granting accounts, 1319
as Key Distribution Center, 1318–1319
Password Replication Policy, 1318, 1327, 1334, 1336–1344
placement, 1319–1322, 1326
post-installation tasks, 1329
referrals to writeable domain controllers, 1322
replication of data, 1316
staging deployment, 1324, 1332–1336
synchronization process, 1329
role services
adding, 246
binary source files, 241
binary source files path, 499
binary source files, removing, 144, 497
component names, 250–255
configuring, 229–262
defined, 229
File Server VSS Agent Service, 484
installing at command prompt, 257–260
managing at command prompt, 250–251
managing with Server Manager, 237–249
removing, 246
removing at command prompt, 260–261
of roles, 230–232
server performance and, 230
supplemental, 236
tracking, 256–262
viewing, 237–238, 246
roles, server
Active Directory Domain Services role, 1271. *See also* AD DS (Active Directory Domain Services)
Active Directory server roles, 43–45
adding, 238–241, 246
binary source files, 241
binary source files, removing, 144, 497
component names, 250–255
configuring, 229–262
defined, 229
installing at command prompt, 257–260
list of, 230–232
managing at command prompt, 250–251
managing with Server Manager, 237–249
multiple on server, 40
removing, 243–245, 246
removing at command prompt, 260–261
roles services related to, 230–232
server performance and, 230
supplemental, 236
tracking, 256–262
viewing, 237–238, 246
Rollback Wizard, 78
Route, 147
routers, 890
DHCPv6 support, 944
M and O flags, configuring, 950–951
pinging, 935
Router Advertisement messages, 950
Routing and Remote Access, 142
Routing And Remote Access Setup Wizard, 1012
Routing Compartments, 881
RPC over IP, 1448–1449
RPCs (remote procedure calls), for replication, 1140
RRAS (Routing and Remote Access Service)
configuring, 1011–1012
DHCP, integration, 943
RSAT (Remote Server Administration Tools), 144, 157, 234
RSoP (Resultant Set of Policy), 1341–1342
permissions on, granting, 1410–1411
Run As Administrator, 364–366
troubleshooting with, 362
RunAsAdmin privilege, 363
RunAsHighest privilege, 363
RunAsInvoker privilege, 362
runaway processes, 385
run levels, application, 362–364
configuring, 364–366

running processes. *See also* **processes**
statistics on, 390
tracking, 379–380
viewing, 391
RVI (Rapid Virtualization Indexing), 508
RWDCs (read/writeable domain controllers), 1315. *See also* **domain controllers**
binding calls to, 1317

S

S4 nonvolatile sleep state, 106
S5 sleep state, 106
SACK-Based Loss Recovery, 881
Safe Boot modes, 114
safe mode
restarting in, 281
starting in, 868–870
SAM (Security Accounts Manager)
access control, 1139
authentication, 1139
database, 315
SANs (storage area networks), 480
Active Directory volumes, 1274–1275
booting from, 492–493, 1274
with clusters, 492–493
configuration problems, troubleshooting, 493
connectivity, 484–485
Device Specific Module, 500
exclusive access, configuring, 492
server-to-storage communications, 481–482
SAS (Serial Attached SCSI), 264
device discovery, 505
SATA (Serial ATA), 264–266
scalability
64-bit versions of Windows, 4–5
planning for, 45–60
SCCM (System Center Configuration Manager) hardware and software inventories, 21
scheduled tasks, remote management, 159
schema
changes, replication of, 1252
Password Settings Container, 1345–1346
Password Settings Object, 1345–1346
Schema Admins group
forest ownership, 1216
object class attributes, managing, 1169–1171
schema modification privileges, 1218
schema masters, 44, 1203–1204, 1217
connecting to, 1169
locating, 1204
placement of, 1203
role, transferring, 1204
schema container, 1203
Schtasks, 147
scopes, DHCP, 942
activating, 961, 969, 972–974
creating, 961, 963–973
description, 964, 970
exclusions, 942, 966, 970, 974–976
failover configuration, reusing, 982
failover scopes, 952–956, 964, 980–984
forcing clients to switch to, 973–974
IP address range, configuring, 965, 970
lease duration, configuring, 966–967, 971–972
lease, terminating, 974
multicast scopes, 963
name, 964, 970
NAP settings, 1006–1007
normal scopes, 963
normal scopes, creating with Netsh, 972–973
normal scopes for IPv4 addresses, 964–969
normal scopes for IPv6 addresses, 969–972
policies, creating, 992
preference values, 969
reservations, 976–980
reservations, forcing client to use, 979–980
split, 955–957
standard options, setting, 990
superscopes, 957, 963, 965, 980
screening. *See* **file screening**
scripts
logon and logoff scripts, 1423–1424
registry files, 329
startup and shutdown scripts, 1422–1423
SCSI (Small Computer System Interface), 264
Search box, 140
console tools, starting, 197
Search charm, 140
searching
in Control Panel, 163
registry, 324–325
secure boot, 593–594
secure desktop, 355, 367
access to, 364
security
Admin Approval Mode settings, 356–357
application installation and run behavior settings, 366–367
architecture, 349
auditing file and folder access, 770–781
binary source files, removing, 144, 245

security (*continued*)
BitLocker Drive Encryption, 569. *See also* BitLocker Drive Encryption
cache-poisoning attacks, 1055
central access policies, 766, 768–770
claims-based access controls, 765–770
computer naming scheme and, 75
for conversion to NTFS, 532
default access permissions, 744
of DHCP, 945–946
DNS, 1036–1040, 1044–1046
of DNS zones, 1079–1080
dynamic controls, 766–767
file screening, 797–801
of file sharing, 715–796
infrastructure, assessing, 22–23
Internet access, 23
IPv6 addressing, 900
man-in-the-middle attacks, 1275
network connection rules, 936
network discovery settings, 876
Password Replication Policy settings, 1336
per-computer settings, 357–358, 368
private networks, 1041
registry, 338–347
reviewing, 32–33
RODCs and, 1315
roles, role services, and features binaries, removing, 497
secure communications, 1275–1276
security information in registry, 315
security templates, 1424–1426
security tokens, 305
subsystem. *See also* security subsystem
Trusted Platform Module Services, 569. *See also* TPMS (Trusted Platform Module Services)
User Account Control, 353–359
security alerts, 32
Security Configuration And Analysis snap-in, 1425–1426
Security Configuration Wizard, 142
security incidents
post-action reporting, 826
prioritizing, 825
responding to, 824
Security log, 406
event levels, 410
monitoring, 781
security principals, creating, 1206. *See also* **RID masters**
security subsystem
Active Directory in, 1135–1139
authentication mechanisms, 1138
directory service component, 1138–1147. *See also* Active Directory
logon/access-control mechanisms, 1138
Security Templates snap-in, 1425–1426
security tokens, 359
selective startups, 113
removing, 116
self-extracting files, installing software from, 351–352
Self-Healing NTFS, 648
SERIAL debugging, 126
Server Configuration, 159
Server Core installations, 66–67
limited roles and role services, 66
UAC and, 353
Server For NFS service, 490
server groups
creating, 156–157
details, viewing, 237–238
management options, 155
Server Manager, 137–138, 150–159, 485
Add Other Servers To Manage option, 151
Add Roles And Features option, 150
AD DS, installing and configuring, 1280
AD DS, uninstalling, 1302–1303
administration tools, 141–143, 199
administrative wizards, 138
alternate credentials, connecting with, 151
auditing, configuring, 776
Check Disk, running, 675
command-line version, 245, 250–256
components, installing, 237–249
console tools, starting, 197
console tree, 151
Create A Server Group option, 151
Dashboard, 150–151
data deduplication, configuring, 710–711
device list, customizing, 279
DHCP console, 961–962
DHCP servers, starting and stopping, 998
disk management options, 690, 696
DNS Server service, starting, 1053
domain controllers, promoting, 1276
Events panel, 408
Event Viewer console, 409
features, adding, 150, 238–241, 497–498
features, configuring, 229–262
features, removing, 243–245
File And Storage Services node, 694–695
file or folder ownership, taking, 749
Group Policy Management Console, 1397
Hyper-V, installing, 509–511

Server Manager (*continued*)
- inheritance settings, changing, 752
- IPAM node, 947–948
- Local Security Policy console, 1396
- managed servers, 229
- new components, installing, 236
- NIC teaming, configuring, 436, 455
- NTFS permissions, setting, 755–757
- remote access, configuring, 402
- remote management, 413, 515
- remote management, enabling, 157–159
- RODCs, installing, 1324
- roles, adding, 150, 238–241, 497–498
- roles, configuring, 229–262
- role services, adding, 150
- role services, configuring, 229–262
- role services, viewing, 237–238
- roles, removing, 243–245
- roles, viewing, 237–238
- server configuration properties, 152–154
- server groups, creating, 151, 156–157
- server management tools, installing, 144–145
- servers, adding for management, 151, 155–156
- share permissions, configuring, 746–748
- shares, creating, 727, 735–740
- special permissions, viewing, 757–758
- standard users, granting permissions, 138
- starting, 237
- starting at logon, 150
- storage pools, creating, 696–700
- Tools menu options, consoles as, 214
- virtual disks, creating, 701–702
- volume management options, 694–695
- Windows backup and recovery tools, installing, 838
- WINS console, 1118

ServerManager.exe, 138

ServerManager module, 245
- components, installing, 250–256

Server Operators group domainwide privileges, 1220

server room
- access controls, 52
- support structures and facilities, 49–52

servers. *See also* **DNS servers; domain controllers; file servers; global catalog servers; WINS servers**
- adding for management, 155–156
- administration tools on, 144
- automated recovery disks, 97
- background optimization, 708
- backup servers, 826–827
- CEIP participation settings, 152
- clean installations on, 65
- computer name, 152, 166
- configuration properties, 152–154
- connecting with alternate credentials, 151
- data collector sets, 460
- DHCP, 957–984
- domain, changing, 166
- domain membership, 152
- domains, joining to, 76, 1381
- driver update process, 272, 277
- dynamic address leases, 936–937
- dynamic controls, 766–767
- encryption, enabling, 496
- Ethernet connections, 152
- event forwarding, 422–424
- fault tolerance, planning, 822
- features, configuring, 497–498
- features, listing, 154
- fixed IP addresses, 942
- highly available, planning deployment, 58–60
- IE ESC status, 152–153
- importing, 156–157
- inventorying, 20
- licensing, 63–64
- load balancing, 431, 433, 435, 451
- mail exchange servers, 1087–1088
- management options, 155
- management panels, 154
- management tools, installing, 144–145
- memory, adding, 387
- memory requirements, 448
- memory usage for registry, 309
- multichannel communications, 494
- multiple roles on, 40
- network services and applications, inventorying, 21–22
- network types, 876
- NIC teaming status, 153
- performance alerts, configuring, 154
- performance baselines, 369
- performance, monitoring, 440
- per-server backups, 826–827
- physical access, 569
- physical environment, 49–52
- physical security, 338, 822
- power protection, 823
- power supply, 51
- properties, 154
- recovering, 822–823, 841, 852–857
- reliability, tracking, 436–439
- Remote Desktop Server mode, 178–179
- remote management, enabling, 157–159
- remote management status, 153

servers (*continued*)
remote settings, 153
roles, 37–40. *See also* roles, server
role services, configuring, 497–500
roles, listing, 154
server groups, 156–157
services, listing, 155
shadow copies, 782. *See also* shadow copies
single-label names, 1092–1093
sites, placement in, 1269–1270
standardizing, 34
throughput optimization, 708
time, synchronizing, 953
time zone, 153
updating, 97
upgrading, 65
WER status, 154
Windows Firewall status, 154
Windows Update configuration, 154
WINS service and client on, 1113
workload, planning, 36–44
work queue performance, monitoring, 441
Server service, 716, 1113
services
backup functions, 833
delegated authentication, authorizing, 1198–1200
details about, 399
disabling, 115–116
events associated with, 417
listing, 155
monitoring, 397–400
points of contacts for, 824–825
process ID, 398
registry subkeys for, 318
related identities, 398
remote management, 159
remote registry access, 344
service host contexts, 398
service tickets, 1349
startup problems with, 115–116
tracking, 379–381
uninstalling, 335–336
Services dialog box, 207
Services for Network File System (NFS), 142
services logs, 405
Services tool, 142
session IDs, 404
sessions
admin sessions, 177
console sessions, 403
disconnecting, 190
logging off, 190
logon sessions, 189–190
remote sessions, 177
service tickets, 1349
user sessions, 402–405
virtual sessions, 177
Set-ADAccountControl cmdlet, 1359
Set-ADAccountPassword cmdlet, 1359
Set-ADUser cmdlet, 1359
Set-Location cmdlet, 334
Set-MPIOSetting cmdlet, 502
–PathVerificationPeriod parameter, 502
–PathVerifyEnabled parameter, 502
–PDORemovePeriod parameter, 502–503
–RetryCount parameter, 503
–RetryInterval parameter, 503
Set-SmbServerConfiguration cmdlet, 495, 496
settings
finding, 140
storage in registry, 303
Settings charm, 139
Setup, 62
advanced drive setup options, 64
debug mode, 92
files, alternate location for, 62
media errors, 93
potential points of failure, 92–93
Rollback Wizard, 78
running and re-running, 352
starting, 77
Setup Information files
device driver, 280
identification tags, 273
Setup log, 406
Set-VmNetworkAdapter cmdlet, 456
shadow copies, 483
accessing, 786
on clustered file servers, 788
configuring at command line, 792–796
configuring in Computer Management, 786–789
defragmenting and, 786
deleting, 790
differential copy procedure, 783
disabling, 790–791, 796
disk space requirements, 784
enabling, 792
of files in shared folders, 715
implementing, 784–786
listing, 793–794
of locked files, 715
maintaining, 790–791
managing in Computer Management, 786–791

shadow copies (*continued*)
- of open files, 715
- run schedule, 783, 785
- as scheduled tasks, 789
- Shadow Copies for Shared Folders, 782–786
- shadow storage, 784, 792–795
- of shared files, 781–786
- snapshots, creating manually, 790, 793
- snapshots, deleting, 795–796
- viewing information, 793–795
- volume mount points and, 788
- volume shadow copy service writers, 782–783
- volumes, reverting, 791, 796

Shadow Copies for Shared Folders, 784–786

Shadow Copy API, 833

Share and Storage Management, 142

shared folders. *See also* **file sharing; folders; shares**
- backing up to, 844–845, 848
- grouping in namespaces, 490
- managing, 161

Shared Folders, 161

shares
- access-based enumeration, 739
- access permissions, 720, 740, 743, 748–763
- Active Directory, publishing in, 721, 741–742
- ADMIN$ share, 724
- administrative view, 723, 726, 735–736
- auditing access, 774
- caching, 739
- Change permission, 743
- configuration details, 764
- configuring, 741
- connecting to, 720
- creating, 726–742
- creating in Computer Management, 731–735
- creating in File Explorer, 727–731
- creating in Server Manager, 735–740
- default, 724
- description, 733, 738
- drive shares, 724
- encrypting, 739
- FAX$ share, 725
- file-share profiles, 736
- finding, 719–723
- folder management properties, 740
- folder path, 719, 731–732, 737
- Full Control permissions, 729, 734, 740, 743
- hidden, creating, 723–724
- IPC$ share, 725
- keywords associated with, 723, 742
- local access permissions, 723
- managing, 763–765
- name, 719, 732, 738
- NETLOGON share, 725
- network drives, mapping, 719–720
- NTFS (access) permissions, 716, 755–757
- offline use, 731, 733, 739
- ownership, 749
- permissions, 716, 723, 729–730, 734–735, 742–748
- permissions on groups, 743
- PRINT$ share, 725
- quotas, 740
- Read access, 723, 734, 743
- Read & Execute permissions, 729
- settings, reviewing, 741
- shadow copies, 715, 781–782
- share permissions, 723, 742–748
- special permissions, 757–761
- special shares, 724–725
- SYSVOL share, 725
- viewing list of, 763–765

Shell32.dll, 213

shell commands, 215
- creating, 223–224
- running, 215

shortcuts
- desktop, dragging to, 168
- taskbar, pinning to, 172

shutdown
- hard shutdowns, 871
- orderly, 823
- shutdown scripts, 1422–1423
- troubleshooting, 868–872

SIDs (security identifiers)
- anonymous user requests, 1405
- on groups, 1378
- on user accounts, 1367–1368

signing
- FIPS-compliant, 601
- SMB signing, 1276

Simple TCP/IP Services, 235

simple volumes, 552. *See also* **volumes**
- creating, 553–555
- recovering, 556

single boot computers, 119–120, 127–128

SIS (Single Instance Storage), 707

site links
- configuration options, 1461–1462
- costs, 1449, 1451
- creating, 1449–1452
- default configuration, 1447
- DEFAULTIPSITELINK, 1445, 1447
- descriptive name, 1450
- managing, 1447–1462

site links (*continued*)
- Options attribute, configuring, 1461–1462
- replication intervals, 1450, 1451
- replication schedules, 1450, 1453–1454
- replication transport protocols, 1448–1449
- schedules, ignoring, 1457
- site-link bridging, 1455–1457
- transitive nature, 1448, 1452
- transport protocol, 1450

sites, Active Directory, 1219, 1233–1238
- accessing in Group Policy Management Console, 1400
- available bandwidth, 1263
- boundaries, 1233, 1237–1238, 1443
- bridgehead servers, configuring, 1458–1461
- bridging, 1455–1457
- client authentication, 1235
- configuration options, 1461–1462
- creating, 1444–1445
- Default-First-Site-Name, 1443
- defined, 19, 44
- descriptive name, 1445
- designing, 1234, 1260–1270
- domain controllers, adding, 1443
- domain controllers, associating with, 1446–1447
- domain controllers in, 1284
- global catalog servers in, 1445
- GPOs linked to, 1389
- Group Policy permissions, 1407–1409
- intersite replication, 1447–1448
- intersite replication topology, 1264–1266
- ISTG, determining, 1457–1458
- link failure, 1267
- link speed, 1443
- managing, 1443–1447
- name resolution, 1235
- naming, 1264
- network architecture, mapping, 1261–1262
- network segments of, 1445
- number of, 1239
- replication between, 1234, 1236–1237, 1253–1260
- replication schedule, 1264–1265
- replication traffic, controlling, 1235–1236
- replication within, 1234, 1236–1237, 1248–1249
- servers, placement of, 1269–1270
- site-link bridges, 1266–1269
- site-link configuration, 1255
- site-link costs, 1261, 1265
- site-link speed, 1263
- site-to-network mapping, 1263
- subnet associations, identifying, 1264
- subnets, associating with, 1445–1446

SLAT (second-level address translation), 508

sleep mode, 102, 107

sleep power transition, 107

SMB 1.0, checking for and disabling, 495

SMB 3.0, 493–497
- features, 494
- forced downgrade security feature, 495
- small random reads and writes and, 737
- virtual machine storage, 509

SMB (Server Message Block), 480, 493
- dialect negotiation, 495
- shares, 723, 736

SmbShare cmdlet, 486

SMB signing, 1276

SMI-S (Storage Management Initiative Specification), 484, 691

SMTP over IP (Simple Mail Transfer Protocol over Internet Protocol), 1140

SMTP (Simple Mail Transfer Protocol)
- as replication transport protocol, 1448–1449

SMTP (Simple Mail Transfer Protocol) Server, 234

snap-ins, 191. *See also* **MMC (Microsoft Management Console)**
- 32-bit and 64-bit versions, 198
- access permissions, 227
- adding to consoles, 205–210
- availability, restricting with Group Policy, 195
- capabilities, 192
- computers, choosing which to work with, 207
- consoles, 192. *See also* consoles
- extensions, 193–194, 208–209
- folders for organizing, 209
- on local and remote systems, 201–203
- MMC 3.0 support, 192
- nodes, 193, 196
- preconfigured, 192–193
- standalone, 194

snapshots. *See also* **shadow copies**
- creating manually, 790, 793
- deleting, 790, 795–796, 1299
- MPIO configuration, 505
- for RODC media, 1330
- settings and run schedule, 790

SNMP (Simple Network Management Protocol) Services, 235

soft page faults, 449

software. *See also* **applications**
- availability, 45–47
- change control, 54–55
- compatibility checking, 350
- compatibility issues, 26
- compliant vs. legacy, 350, 359
- finding, 140

software (*continued*)
machine-wide settings in registry, 315
maintenance, administrator privileges for, 349–350
notifications for, 172
reconfiguring, 352
repairing, 352
standardizing, 34, 46–47
uninstalling, 352
updating, 32, 350
software-based encryption, 590
software installation, 349–353
backups for, 350
compatibility checking, 350
compatibility issues, 351
credentials, validating, 350
elevation prompts, 349
failures, 350
managing, 352–353
updates, checking for, 350
from .zip and self-extracting files, 351–352
software RAID, 73, 506. *See also* **RAID (redundant array of independent disks)**
spanned volumes, 553
creating, 553–555
recovering, 556
sparse files, 645–647
SpeedStep, 108
SPI (Parallel SCSI), 264
split scopes, 955–957
Spooler service, 344
Spurious Retransmission Timeout Detection, 881
SRK (Storage Root Key), 570
SSDs (solid-state drives), 265, 622
in enterprise, 622
hybrid drives, 623
for paging files, 372
performance, 621
Standard Format hard drives, 263–264, 519
standard taskpad views, 216–218
standard user accounts, 349. *See also* **user accounts**
access tokens, 360
Admin Approval Mode settings, 356–357
UAC prompts, 353–354
standard user security tokens, 305
standard volumes, creating, 702–704
standby hardware systems, 48
standby mode, 102
Stanek, William R., 21
Start screen
Control Panel, accessing, 140, 162
hidden button, 140
hidden menu, 139–140
opening from desktop, 140
searching from, 140
Server Manager button, 137
Settings panel, 139
Windows PowerShell, opening, 148
Start-Service cmdlet, 400
Start-Transaction cmdlet, 306
startup. *See also* **restarts**
advanced modes, 111
authentication at, 593–596, 613–614
boot order, 92
configuration options, 113–114
debugging mode, 92
from distribution media, 77–78
events at, 1419
from firmware and hardware, 101–109
to GPT disks, 560
after installation, 97
from installation disc, 827–828
integrity, 101
Last Known Good Configuration, 317
managing, 111–119
repairing, 827–828
in Safe Mode, 868–870
from SANs, 492, 1274
to secondary drives, 560
speeding, 113
startup modes, 869–870
startup scripts, 1422–1423
after stop errors, 828–831
troubleshooting, 868–872
Startup And Recovery dialog box, 111–113
startup applications, disabling, 116
Startup Event Traces, 458
Startup folder, 172–173
startup keys, 613
Startup Repair tool, 827
Startup Repair Wizard, 828, 871
static IP addresses, 913
configuring, 913–917, 916–917
stop errors, 93–94
debugging information, 830
logging, 830
startup and recovery after, 828–831
Stop errors
paging file, writing to, 377
Stop-Process cmdlet, 397
–confirm parameter, 397
Stop-Service cmdlet, 400
Stop-Transaction cmdlet, 306

Stop-VM cmdlet, 1299
storage, 479–568
automated disk maintenance, 672–680
availability, 505–507
block storage devices, 490
capacity, 505–507
configuring, 514–533
Data Center Bridging, 485
data deduplication, 704–714
data store storage, 1142
data transfer, 691–694
deprecated tools and features, 480
direct-attached, 480
disk quotas, 661–671
disks, 621. *See also* disks
disks, adding, 519–521
disk storage types, 525–528
disk write caching, 520
efficiency techniques, 489
enhanced storage devices, 485
essential technologies, 479–496
external devices, 480–483
file screening, 491
File Server Resource Manager, 491
file services, configuring, 496–513
indexed, 1142
internal devices, 480–483
iSNS Server service, 485
management options, 694–696
managing, 689–714
managing with command-line tools, 485–486
managing with Disk Management, 514–519
managing with Server Manager, 485
managing with Windows PowerShell cmdlets, 486–487
Multipath I/O, 484
network-attached, 480
offloaded transfers, 691–694
performance, 505–507
provisioning, 487
role services, 487–491
sequential, 1142
server solutions, 479
SMB 3.0, 493–497
snapshots, 483
standards-based approaches, 480
standard volumes, 702–704
Windows Server 2012 features and tools, 483–487
Windows Server 2012 management capabilities, 690–691
storage arrays, 73
Storage cmdlet, 486
Storage Management API, 485
storage pools, 487, 690
creating, 696–700
mirror layout, 700
parity layout, 700
physical disk allocations, 698
primordial pools, 697–698
virtual disks, allocating, 700–702
storage providers, 484
storage reports, 799–801
default parameters, changing, 805
delivering, 819, 820
generating, 491, 819–820
incident reports, 799
on-demand reports, 799
scheduled reports, 799
scheduling, 817–819
standard reports, 800–801
storage location, configuring, 806
Storage Services role service, 487, 690
Storage Spaces, 73, 161, 506, 525
mirroring or disk striping with parity and, 654
ReFS integration, 650–651
remote management, 158
thin provisioning, 487–488
storage tools, 161
string values, modifying, 325–326
striped volumes, 553
creating, 555–556
recovering, 556
SUA (Subsystem for UNIX-Based Applications), 235
subnetting, 890–897
address prefix, 1445–1446
Class A networks, 893–894
Class B networks, 895–896
Class C networks, 896–897
DHCP and, 950, 966
managing, 1443–1447
network prefix notation, 891–892
site associations, 1445–1446
sites, Active Directory, 1233
subnet broadcasts, 887
subnet masks, 890–891
subnets, creating, 1445–1446
subnets, documenting, 1261
zone transfers, enabling, 1074–1076
subscriptions, creating, 422–424
Suspend Mode setting, 108
Suspend-Service cmdlet, 400
switches
server-class, 456
switches, network, 899
Symmetric Network Address Translators, 882

Sync-ADObject cmdlet, 1465
.sys extension, 280
system
administration tools, 137–150
auditing, 57
availability, 45–60
change log, 868
day-to-day operations, 53–58
fault tolerance, 822
growth and, 18
information in registry, 317–318
manageability, 45–60
monitoring, 53
orderly shutdown, 823
performance, tuning, 369–370
physical access, 569
points of contacts for, 824–825
power-state management, 102–103
properties, 165
properties, managing, 166–167
restoring, 858–859
scalability, 45–60
stability, 437
system caching, 385
System Configuration utility (Msconfig.exe), 111, 113–116, 142
System console, 165–167
links, 165
support tools links, 165–166
system diagnostics, 459–460
system disks, moving, 557
system drives, hardware-based encryption, 590–591
system files
backing up, 832
hiding and showing, 165
recovering, 832
repairing, 870–871
System Image Recovery, 65
system images, recovering from, 859
System Information utility (Msinfo32.exe), 142
resources conflicts, checking, 299–300
system logs, 406
disk quota violations, 670
hardware events, 295
SAN configuration error events, 493
stop error events, 830
system partitions, 71, 526
System Properties dialog box, 166–167
Remote tab, 153
system resources. *See also* **resources; resource utilization**
per-process usage, 427–436
system state
backing up, 324, 335, 833, 1274–1275, 1296–1297
restoring, 857, 861
standby state and, 102
storage in registry, 304
system store device, setting, 122–123
system tools, 160–161
System utility, 828–831
system volumes
compressing, 658
drive letter, changing, 540
encrypting, 601
mirrored, 559–563, 567–568
repairs, scheduling, 676
Sysvol
Active Directory Group Policy, 1389
changes over operating system versions, 1240–1246
domain folder, 1243
junction (reparse) points, 1243
moving, 1273
reason codes for in-progress replication, 1399
replication of, 1240–1241, 1465
restoring, 866
Staging folder, 1243
SYSVOL share, 725

T

taskbar, 169–174
Address toolbar, 175
configuring, 169–174
items, combining, 171–172
Links toolbar, 175
notification area, 169, 172–174
programs/toolbars area, 169
Server Manager button, 137
shortcuts, pinning, 172
size and position, 170
toolbars, 175–176
Touch Keyboard toolbar, 175
visibility, 170–171
Task Manager
commit charge and commit limit, tracking, 375
Details tab, 378, 391–395
ending tasks, 871
expanded view, 375, 378
graph summary view, 383
Networking tab, 401
opening, 378
Performance tab, 378, 381–382, 400
processes, stopping, 396

Task Manager (*continued*)
- Processes tab, 378, 388–390
- remote user sessions, managing, 189–190
- resource usage, 379
- resource utilization, determining, 427
- running programs, managing, 352–353
- Services tab, 378, 397–398
- summary view, 378, 382
- system health, tracking, 377
- user sessions, viewing, 189
- Users tab, 378, 404

taskpads
- author mode, 221
- console tree, placement in, 220
- creating, 218–220
- custom, designing, 215–227
- horizontal lists, 217
- menu commands, 215
- multiple, 215
- names and descriptions, 220
- navigation components, 215
- no list option, 217, 218
- organization of, 216–218
- properties, editing, 221
- shell commands, 215
- target, specifying, 219–220
- taskpad views, 215–218
- tasks, creating, 221–227
- user options, limiting, 218
- vertical lists, 216, 217

tasks
- access permissions, 227
- arranging, editing, removing, 226–227
- creating, 221–227
- delegating permissions for, 1311–1314
- icons, selecting, 223
- managing, 160, 162
- menu command tasks, 222–223
- name and description, 223
- navigation tasks, 224–227
- running, 215
- shell command tasks, 223–224

Task Scheduler, 9, 143, 160
- automated maintenance tasks, 673
- DiscoveryTask, 947
- IPAM scheduled tasks, 947
- RacTask, 439
- ScheduledDefrag task, 680
- ShadowCopyVolume tasks, 789

TCG (Trusted Computing Group)-compatible firmware, 571

TCP connections, 436

TCP Extended Statistics, 881

TCP/IP networking, 909–940
- command-line tools, 145
- configuring, 912–926
- DHCP leases, releasing and renewing, 936–938
- DHCP options, configuring, 984–997
- DNS resolution, 921–924
- dynamic IP addresses, 917–919
- gateways, 919–921
- installing, 909–912
- multiple IP addresses, 919–921
- name-resolution issues, troubleshooting, 938–940
- network adapters, installing, 911
- network connections, managing, 926–931
- networking services, installing, 911–912
- preparing for installation, 910–911
- routing, 935
- static IP addresses, 913–917
- testing, 932–933
- troubleshooting, 931–940
- WINS resolution, 924–926

TCP/IP (Transmission Control Protocol/Internet Protocol), 875–908
- configuration, checking, 97
- configuring, 911–912
- datagrams, 875
- DNS client installation, 1017
- installing, 75–76, 911–912
- IPv4 addressing, 883–888
- NetBIOS over TCP/IP, 907
- Next Generation TCP/IP stack, 880–882
- Windows PowerShell cmdlets, 882

TCP/IPv4 (Internet Protocol version 4), 76

TCP/IPv6 (Internet Protocol version 6), 77

TCPv4 communications, monitoring performance, 441

TCPv6 communications, monitoring performance, 441

team network adapters, 456

teams for deployment, 12–14

Telnet Client, 235

Telnet Server, 235

Test-Connection cmdlet, 914–916, 932–933

testing
- burn-in, 59–60
- deployment plan, 11
- integration testing, 46
- IP addresses, 914
- load testing, 60
- replication, 1466–1468
- stress testing, 59–60
- TCP/IP networking, 932–933
- wiring and cabling, 50–51

testing team, 13

thin provisioning, 487–488, 684, 701
threads
performance, monitoring, 441
of processes, 395
queue length, 452
summary statistics, 384
timeout for default operating system boot, 133
time servers, 1209–1212
time synchronization, 953, 1210–1211, 1350, 1384
Tmp.edb, 1148
toolbars, 175–176
name labels, 175
personal, 176
tools
administration and support tools, 137–150
Computer Management Services And Applications tools, 162
vs. consoles, 193
console tools. *See* console tools
DNS server management tools, 1053–1054
management tools, 144–145
storage-management tools, 483–487
storage tools, 161
system tools, 160–161
torn writes, 649, 650, 654
TPM (Trusted Platform Module) Services, 570–571. *See also* **BitLocker Drive Encryption**
backup to Active Directory, 576
in firmware, turning on, 571
Group Policy settings, 598
initializing, 571–572, 576–579
managing, 571–583
owner authorization information, 574–576
tools, 571–574
TPM, clearing, 580–582
TPM management on local computer, 573
TPM password, backing up, 579
TPM password, changing, 582–583
TPM password, creating, 576–577
TPMs, 570
TPM states, 571–574
turning on and off, 571, 580
trace analysis reports, 475
trace logs
analyzing, 475
command line, analyzing at, 475
Tracerpt, 475
Tracert, 147
traditional defrag, 684
free-space consolidation, 684
optimization, 684
transactional NTFS, 647–648
Transactional Registry, 306
transactions, 647–649
processing, 1143
registry, managing with, 306
transaction log, 1143
workspace for, 1148
transmission, 284
preference settings, 284–285
troubleshooting
authentication failures, 259
binary download issues, 249
BitLocker Drive Encryption, 615–618
boot issues, 103–106
class ID problems, 997
clone deployment, 1301–1302
compatibility issues with legacy programs, 365
component installation, 258–259
computer accounts, 1383–1384
connecting USB 3.0 to USB 2.0, 268
CPU incompatibility, 95
device driver signing, 281
device error codes, 296
device slot configuration, 299
DHCP lease renewal, 936–938
DHCP server issues, 999
diagnostic and selective startup options, 113–114
DNS clients, 1099–1102
DNS Server service, 1102–1112
driver signing, 281
email notifications, 804
firmware issues, 92–93
Group Policy settings, 1419
hardware problems, 295–298
Hyper-V compatibility issues, 508
installation of Windows Server 2012, 65, 91–96
Internet connection problems, 931–932
IP addressing issues, 933–934
joining computers to a domain, 1381
memory-related performance issues, 433
mirrored sets, 565–566
mirrored system volumes, 567–568
mixed-state network adapter settings, 879
name-resolution issues, 938–940
network connections, 931
network problems, 897
with NSLookup, 1102
performance issues, 382
permissions, 761–763
physical memory problems, 388
pings, blocked, 914
potential points of failure, identifying, 92–93
PowerShell passthrough problems, 150

troubleshooting (*continued*)
processes, 391–392
processor issues, 431
RAID-5 sets, 568
RAM incompatibility, 95
recovering devices, 291
remote monitoring, 447
replication, 1462–1468
resource conflicts, 300
routing problems, 935
SAN configuration problems, 493
selective startup, removing, 116
startup and shutdown, 868–872
storage report generation, 806
TCP/IP networking, 931–940
transmission preference settings, 284–285
trust errors, 1196
update problems, 272
user accounts, 1366–1367
viewing events for, 295
virtualization, 362
WINS registration and replication problems, 1119, 1127
Trusted Platform Module Management, 572
accessing, 573
TPM, clearing, 580–582
TPM, initializing, 577–579
TPM manufacturer, 573–574
TPM owner password, changing, 582–583
TPM status, 573–574
trusts, 1218
across domain boundaries, 1183–1186
across forest boundaries, 1186–1189
authentication levels, 1218
cross-forest trusts, 1218
design considerations, 1175–1196
direction of, 1192, 1194
DNS role in, 1192
domain trusts, 1192
establishing, 1193–1195
examining, 1189–1192
explicit trusts, 1185
external trusts, 1186–1187
forest trusts, 1186–1188, 1192
incoming and outgoing sides, 1192, 1194
one-way, 1183, 1218
outgoing trust authentication level, 1195
parent and child trusts, 1191
passwords for, 1194–1195
realm trusts, 1192
shortcut trusts, 1185–1186
transitivity of, 1192
tree-root trusts, 1191
troubleshooting, 1196
trust tree, 1184
two-way transitive trusts, 1184, 1191, 1218
validating, 1196
Typeperf, 471–474
counters, viewing, 473
input for, 473
output, redirecting, 473
parameters, 472
performance counter path syntax, 472–473
sampling interval, controlling, 474

U

UAC (User Account Control), 353–359
Admin Approval Mode, 355–359
administrator user prompts, 354–355
application run levels, 305
for compliant and legacy applications, 360
domain settings, 357, 368
elevation, 349, 355
elevation prompts, 363–364
Group Policy settings, 356–357
local security policy settings, 357–359, 368
secure desktop, 355, 364, 367
shield icon, 353
standard user prompts, 353–354
UDPv4 communications, monitoring performance, 441
UDPv6 communications, monitoring performance, 441
UEFI (Unified Extensible Firmware Interface), 103
TPM validation-profile settings, 593
unauthorized content, blocking, 797. *See also* **file screening**
Undo-Transaction cmdlet, 306
unicasts
IPv4, 883–886
IPv6, 901
Uninstall Or Change A Program utility, 335–336
Uninstall-ServerManager cmdlet, 260–261
Uninstall-WindowsFeature cmdlet, 250
universal groups, 1374
authentication, 1175–1178
membership caching, 1177–1178
Update Driver Software Wizard, 275, 287–289
updates
checking for, 32–33
device driver, 270–272
searching for, 272
for software, 350
UPNs (User Principal Names), 1176
suffix, changing, 1176–1177
UPS (uninterruptible power supply), 51, 823

uptime summary statistics, 384
USB 2.0, 266–267
connecting to USB 3.0, 268
USB 3.0, 266–267
connecting to USB 2.0, 268
USB Boot setting, 109
USB controllers, 267
USB debugging, 126
used space, encrypting, 591–592
user accounts
account options, configuring, 1361–1364
administrator, 349. *See also* administrator user accounts
capabilities, privileges, and rights, 1354–1355
creating, 1357–1361
deleting, 1367–1368
disabling, 1364, 1366, 1368
enabling, 1364, 1368
expiration options, 1363
home folder, 1365–1366
logon computers, 1363
logon hours, 1362, 1405
logon scripts, 1364
moving, 1368
password reset disk, 1371–1373
passwords, resetting, 1370–1371
renaming, 1369–1370
roaming user profile path, 1364
security descriptors, 1360
security identifiers, 1367–1368
standard, 349. *See also* standard user accounts
troubleshooting, 1366–1367
unlocking, 1363, 1367, 1371
user applications, 361
user data, central management of, 782
Userenv.dll, 1390
user experience team, 13
User Interface Accessibility (UIAccess) application security settings, 366–367
User Interfaces And Infrastructure, 235
User mode—full access level, 194, 211–212
User mode—limited access, multiple window level, 194, 212
User mode—limited access, single window level, 194, 212
user mode (MMC), 194–196
UserName environment variable, 1366
user profiles, registry subkey for, 318–319
users
access to domains, 1181–1183
account lockout, 1348–1349, 1353, 1366
Account Lockout Policy, 1404
account policies, configuring, 1345–1350
adding to groups, 1377
auditing actions of, 1221
authenticating, 1138
BitLocker PIN and password, resetting, 586
component installation rights, 259
delegated authentication support, 1197–1198
disk quotas, 663, 665–668
effective access, determining, 1360–1361
event forwarding, 424
events associated with, 417
file associations for, 318
file recovery with VSS, 484
GPOs, permissions on, 1408–1409
Group Policy settings, 1389
information in registry, 320
linking GPOs permission, 1410
managing, 161, 191, 1345–1373. *See also* MMC (Microsoft Management Console)
processors run by, 389
rights, assigning, 1355–1357
RSoP permission, 1410
security credentials, 1138
security tokens for, 1175–1177
sharing files and folders with, 729. *See also* file sharing
UPNs, 1176–1177
Windows settings, 1389–1390
Users container, 1375
user sessions
connecting to, 405
ending, 404
tracking and managing, 402–405
USNs (update sequence numbers), 1251–1252

V

validation, TPM modes, 584–585
video, low-resolution startup mode, 869
virtual disks
allocating space to, 700–702
creating, 700–702
in disk architecture, 689
iSCSI, 691
layouts, 700
management options, 696
sizing, 702
slab consolidation and retrim, 685, 688–689
slabs, 685
standard volumes, creating, 702–704
virtual hard disks
creating, 529
formatting, 529
initializing, 530

virtual hard disks (*continued*)
managing, 530–531
role services and features, configuring, 497–500
sizing, 529
types, 529–530
volumes, creating, 530
working with, 530–531
virtualization, 7
benefits, 508
dynamic virtual machine storage, 508–509
exceptions to, 362
file system, 305, 361
firmware support, 507
Hyper-V, 507–514
live migration, 508
registry, 305, 307, 361
write failure settings, 367
virtualized domain controllers, cloning, 1297–1302
virtual machines
backing up, 513
creating, 511–513
data storage location, 512
DS Restore Mode boot flag, removing, 1301
memory allocation, 511, 512
network adapter configuration, 512
recovering, 853
SMB 3.0 storage configuration, 509
virtual hard disk location, 513
virtual memory, 448
available limit, 449
bytes committed, 449
commit limit, 373
current commit charge, 373
file-mapping view, 374
page file–backed, 374
private, 374
for processes, 393
reserved, 373, 374
sizing, 372
tuning, 371–375
Windows management, 376
Virtual Network Manager, 509
virtual networks, creating, 509
virtual operating system environments, 6–7
virtual switches, creating, 509–510
visual effects, performance impact, 369–370
VLANs (virtual LANs), network traffic on, 456
Volume Activation Services role, 232
Volume Activation Tools, 143
volumes. *See also* **disks; physical disks**
analyzing with ChkDsk, 678–679
backing up, 840–842
backups, writing to, 844
basic, 525. *See also* basic disks
BitLocker status, 605–606, 615
change journals, 640–643
creating, 534–538
deduplicating, 704, 708–711
deleting, 549
in disk architecture, 689
disk quota entries, importing and exporting, 671
disk quotas, 662, 664–665
dismount, forcing, 679
drive letters, configuring, 539–541
dynamic, 525, 552–553. *See also* dynamic disks
encrypted files, finding, 1279
encrypting, 591–592. *See also* BitLocker Drive Encryption
extending, 543–546, 553
filter-system drivers, 693–694, 709
fixed-disk provisioning, 488
formatting, 524, 555
fragmentation, 680–689
integrity checks, 612–613
labels, 537
listing, 517
managing, 552–568, 694–695
mount points, 541–543, 788
vs. partitions, 71
recovering, 852–857
remote management, 158
repairing, 674–676, 679–680
repairing with ChkDsk, 679–680
reverting, 791, 796
shadow copies, configuring, 786–789, 792
shrinking, 546–548
simple, 553–555
sizing, 534–535
snapshots, 483
spanned, 553–555
standard volumes, 702–704
storage utilization, 488
summary of fragmentation, 686–688
thin-disk provisioning, 488
volume shadow copy service writers, 782–783
VSSAdmin, 486, 792–796
VSS (Volume Shadow Copy Service), 483, 715, 782, 834, 837. *See also* **shadow copies**
file recovery, 484

W

Wake On LAN From S4/S5 setting, 108
wake power transition, 107
warning events, 410
Wbadmin, 147, 837, 840
  system state, backing up, 335
  system state, restoring, 857
WDS (Windows Deployment Services) role, 232
Web Server (IIS) role, 232
web servers, planning usage, 40
WER (Windows Error Reporting), 154
Wevtutil, 147
Where-Object cmdlet, 421–422
WHQL (Windows Hardware Quality Lab), 274, 281
Window PowerShell 2.0 Administrator's Pocket Consultant, 334
windows
  adding to console tools, 204–205
  tiling, 204
Windows 8, 8–9
  Automatic Updates, 8
  BitLocker Drive Encryption, 8
  desktop apps, 349
  Desktop Experience, 9
  Hyper-V, 7
  NT 6.2 kernel, 3, 8
  Remote Assistance, 8
  Remote Desktop, 9
  Task Scheduler, 9
  Windows Firewall, 9
  Windows Time, 9
  Wireless LAN Service, 9
Windows 8 Enterprise, 8
Windows 8 Pro, 8
Windows Biometric Framework, 235
Windows Boot Loader, 314
  BCD store application entries, 117
Windows Boot Manager, 111, 314
  adding to boot order, 62
  BCD store entry, 117
Windows BranchCache, 488
Windows Clipboard, 327
Windows commands at Windows PowerShell prompt, 149–150
Windows Deployment Services, 143, 1379
Windows desktop operating systems
  power-state management, 102–103
Windows domains. *See also* **domains**
  assessing, 20
Windows Error Recovery mode, 870
Windows Filtering Platform, 881
Windows Firewall, 9
  management areas, inbound rules, 143
  network discovery settings and, 876
  pings, blocking, 914
  Remote Desktop Protocol connections exceptions, 179
  remote management rules, 158–159
  Remote Volume Management, 158
  status, listing, 154
Windows Firewall With Advanced Security, 143
  applications, inbound rules for, 157
Windows Installer, 350
Windows Internal Database, 235
Windows Legacy OS Loader, 122, 126
Windows logs, 405
Windows Memory Diagnostics, 143
Windows Memory Diagnostic Tool (Memdiag.exe), 125–126, 388
Windows Memory Test BCD store entry, 125–126
Windows memory tester application, 314
Windows Network Diagnostics, 875, 931–932
Windows OS Loader applications, 129–131
Windows PE (Windows Preinstallation Environment), 85
  BitLocker Drive Encryption, provisioning, 596
  command-line tools, 85–88
Windows PowerShell, 235
  ActiveDirectory module, 1464–1465
  Active Directory replication, working with, 1213
  ADDSDeployment module, 1277
  administration tools, 139
  cmdlets, listing, 148–149, 487
  cmdlet verbs, 148
  components, installing, 250–256
  credentials, stored, 260
  data deduplication cmdlets, 711–714
  Deployment Image Servicing and Management (DISM) module, 596
  DnsServer module, 1054
  elevated prompts, 247
  installing, 148
  IP configuration, retrieving, 930
  modules, importing, 487
  NetTCPIP module, 882
  passthrough problems, 150
  registry, accessing, 334
  registry transactions, 306
  remote access for management, 157, 158
  remote management with, 159
  running, 147–149
  ServerManager module, 245

Windows PowerShell (*continued*)
storage management cmdlets, 486–487
user accounts, creating, 1359
Windows commands, entering, 149
Windows PowerShell 2.0 Administrator's Pocket Consultant, 306
Windows PowerShell Classifier, 808
Windows PowerShell Web Access, 235
Windows Process Activation Service, 235
Windows processes. *See also* **processes**
monitoring, 388–390
Windows resume application, 314
Windows Resume Loader applications, 124
Windows RE (Windows Recovery Environment), 597
Windows Search service, 485
Windows Security screen, 871
Windows Server 2003 domain functional mode, 42
Windows Server 2003 forest functional level, 42
Windows Server 2008 domain functional mode, 42
Windows Server 2008 forest functional level, 42
Windows Server 2008 R2 domain functional mode, 42
Windows Server 2008 R2 forest functional level, 42
Windows Server 2012
64-bit versions, 4–5, 61
activating, 79, 82–85, 165–166
administration tools, 137–150
adopting, 3–4
Automatic Updates, 8
BitLocker Drive Encryption, 8
compatibility issues, 95–96
compatibility testing, 46
deployment planning, 10–36
on desktop-class systems, 101
Desktop Experience, 9
device driver library, 280
dual IP layer architecture, 880
evaluation period, 83
evaluation version, 83
features. *See* features
features list, 232–236
forest and domain functional levels, 23
hardware detection, 272
hardware diagnostics, 295
improvements and additions, 3
installation. *See* installation of Windows Server 2012
installation quick start, 61–62
licensing, 5–6, 63–64
networking features, 875–883. *See also* networking
NIC teaming, 456
NT 6.2 kernel, 3
postinstallation tasks, 96–99
product identifier, 153
Remote Assistance, 8
Remote Desktop, 9
roles and role services list, 230–232
role services. *See* role services
security, 32. *See also* security
security architecture, 349
security subsystem, 1135–1139
server roles, 37–40. *See also* roles, server
startup, configuring, 101–134
storage management, 483–487, 690–691
system requirements, 64, 93
Task Scheduler, 9. *See also* Task Scheduler
virtual memory management, 376
virtual operating system environments, 6–7. *See also* Hyper-V
Windows 8 and, 8–9
Windows Firewall, 9
Windows Time, 9
Wireless LAN Service, 9
Windows Server 2012 Datacenter, 6
Windows Server 2012 domain functional mode, 42
Windows Server 2012 Essentials, 6
Windows Server 2012 forest functional level, 43
Windows Server 2012 Foundation, 5–6
Windows Server 2012 Standard, 6
Windows Server Backup, 143, 161, 235, 485, 837–851. *See also* **backups**
backup disk management, 837
full backups, 839
improvements in, 840
manual backups, 846–850
performance settings, 839
recovery with, 838
Recovery Wizard, 852–857
registry backups, 334–335
scheduling backups, 839, 841–846
starting, 838–839
summary details, 855
tracking backups, 850–851
Windows Server Catalog, 47
Windows settings, 1389
Windows Side-by-Side folder, 245
Windows Software Management Licensing tool, 166
Windows Standards-Based Storage Management, 235, 484, 691
Windows Storage Server 2012, 491
Windows System Resource Manager, 106, 143
Windows TIFF IFilter, 236

Windows Time, 9
Windows Update
binary source files, retrieving, 499
blocking, 288
configuration, viewing, 154
controlling with Group Policy, 271
device drivers, retrieving, 269
hosting on local server, 70
during installation of operating system, 67–69
notifications for, 173
payloads, restoring, 248
sharing files, 68
from Windows Update site, 68
Winload.exe, 119
Winresume.exe, 125
WinRM IIS Extension, 236
WinRM (Windows Remote Management), 157
disabling, 158
WINS console
automatic replication partners, configuring, 1120–1121
burst handling, configuring, 1124–1125
database, backing up, 1131
database consistency checks, configuring, 1129–1130
database, restoring, 1131
registrations, viewing, 1128
replication partners, specifying, 1122–1124
scavenging, initiating, 1128–1129
server status, checking, 1126–1127
WINS Server, 236
WINS servers
automatic replication partners, 1116, 1120–1121
configuration and status, viewing, 1126–1128
multiple servers, 1116
planning usage, 39
primary and secondary servers, 1118
pull replication partners, 1120, 1123
push replication partners, 1120, 1124
registrations, 1115–1116, 1119
replication of database entries, 1116
replication partners, configuring, 1118, 1120–1124
setting up, 1117–1119
TCP/IP configuration, 1118, 1119
WINS service, 1113
installing, 1117–1118
stopping and starting, 1130–1131
WINS tool, 143
WINS (Windows Internet Naming Service), 906–908, 1113–1132
Active Directory trust relationships and, 907
active registrations, 1128–1129
admin-triggered scavenging, 1128–1129
architecture, 1113–1114
automatic replication partners, 1116
backing up, 833
burst handling, 1124–1125
cache, 1115–1116
database, 1115–1116, 1129–1132
decommissioning, 1114
DHCP, specifying servers for, 969
DNS, integration, 1132
forward and reverse lookups, 906
implementation details, 1116–1117
legacy application support, 1114
lookups through DNS, 1132
multicasting, 1121–1122
name registration, 1115–1116, 1119
name registration Time to Live, 1116
name-resolution problems, 1127
NetBIOS namespace and scope, 1113–1114
NetBIOS node types, 1115
NetBIOS support, 906–907
persistent connections, 1116
postinstallation task, 1118
record export feature, 1117
registration release problems, 1127
remote management and configuration, 1118
replication errors, troubleshooting, 1119, 1127
replication partners, 1118, 1120–1124
scavenging, 1128–1129
servers. *See* WINS servers
server setup, 1117–1119
for TCP/IP networking, 924–926
tombstoning, manual, 1117
WINS client, 1113
WINS console, 1118
WINS service, 1113, 1117–1118, 1130–1131
Wireless LAN Service, 9, 236
wiring and cabling, testing and certifying, 50–51
Wise Install, 350
wizards, 191
snap-ins, adding to consoles, 208
WMI (Windows Management Instrumentation), 157
filters, linking to GPOs, 1436
workgroups, 876
changing membership, 166
data-recovery agents, 587
DHCP services, setting up, 959
workstations
data storage on, 479
domains, joining to, 1381
Workstation service, 1113
WOW64 Support, 236

write operations
caching, 520
disk writes counter, 454
performance, 680
torn writes, 649, 650, 654
WSH (Windows Script Host), 1422
WSRM (Windows System Resource Manager), 236
WSUS (Windows Server Update Services), 68–69, 143
for updates, 272
WSUS (Windows Server Update Services) role, 232

X

XPS Viewer, 236

Z

zip compression technology, 659–660
installing software from, 351–352
zones, DNS
Active Directory–integrated zones. *See* Active Directory–integrated zones
aging/scavenging properties, 1097
authoritative servers, 1090
Canonical Name (CNAME) records, 1086–1087
configuration, 1028–1030, 1071
DNSSEC, signed with, 1078
file-backed zones, 1079
forest root zones, 1050
forward lookup zones. *See* forward lookup zones
GlobalNames zone, 1092–1093
Host Address (A and AAAA) records, 1083–1086
listing, 1110–1111
Mail Exchanger (MX) records, 1087–1088
master name servers, identifying, 1063
name, 1063
Pointer (PTR) records, 1083–1086
primary zones, 1061
removing, 1305
resource records, adding, 1082–1092
resource records, listing, 1111–1112
reverse lookup zones. *See* reverse lookup zones
secondary zones, 1050–1051, 1061
securing, 1079–1080
Service Location (SRV) records, 1091–1092
signing, 1079–1082
Start of Authority (SOA) records, 1090
stub zones, 1050–1051, 1061
subdomains in, 1071–1074
WINS name resolution, configuring, 1132
zone delegation, 1293
zone transfer notification, configuring, 1076–1077
zone transfers, configuring, 1074–1076
Zone Signing Wizard, 1080–1082