

Microsoft

Windows Server® 2008

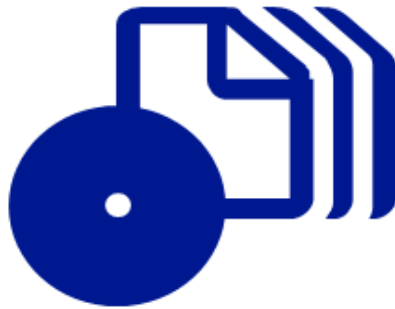


Charlie Russel and
Sharon Crawford

Administrator's Companion



How to access your CD files



The print edition of this book includes a CD. To access the CD files, go to <http://aka.ms/625051/files>, and look for the Downloads tab.

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

Questions? Please contact: mspinput@microsoft.com

Microsoft Press

PUBLISHED BY

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

Copyright © 2008 by Charlie Russel and Sharon Crawford

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: 2008923625

Printed and bound in the United States of America.

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

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

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

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

Microsoft, Microsoft Press, Access, Active Directory, ActiveX, Aero, BitLocker, ESP, Excel, Expression, Hyper-V, IntelliMirror, Internet Explorer, Jscript, MSDN, MS-DOS, OneNote, Outlook, SharePoint, SQL Server, Visual Basic, Win32, Windows, Windows Logo, Windows Media, Windows NT, Windows PowerShell, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

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

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

Acquisitions Editor: Martin DelRe

Developmental Editor: Karen Szall

Project Editor: Melissa von Tschudi-Sutton

Editorial Production: Custom Editorial Productions, Inc.

Technical Reviewer: Randall Galloway; Technical Review services provided by Content Master, a member of CM Group, Ltd.

Cover: Tom Draper Design

Body Part No. X14-65790

Contents at a Glance

Part I

Prepare

1	Introduction to Windows Server 2008	3
2	Introducing Directory Services	13
3	Planning Namespace and Domains	25
4	Planning Deployment	39

Part II

Install and Configure

5	Getting Started	51
6	Upgrading to Windows Server 2008	79
7	Configuring a New Installation	95
8	Installing Server Roles and Features	121
9	Installing and Configuring Server Core	147
10	Managing Printers	165
11	Managing Users and Groups	197
12	Managing File Resources	239
13	Group Policy	281

Part III

Administer the Network

14	Managing Daily Operations	347
15	Using Scripts for Consistent Administration	383
16	Installing and Configuring Directory Services	467
17	Managing Active Directory	535
18	Administering TCP/IP	573
19	Implementing Disk Management	615
20	Managing Storage	651
21	Using Clusters	699

Part IV

Secure the Network

22	Planning Security	745
23	Implementing Security	763
24	Administering Network Access Protection	799
25	Patch Management	833
26	Implementing Remote Access Strategies: SSTP, VPN, and Wireless	847

Part V

Use Support Services and Features

27	Interoperability.	903
28	Managing Software	933
29	Working with Windows Virtualization	961
30	Deploying Terminal Services	1005
31	Internet Information Services	1061

Part VI

Tune, Maintain, and Repair

32	Windows Reliability And Performance Monitor	1107
33	Disaster Planning	1133
34	Using Backup	1147
35	Planning Fault Tolerance and Avoidance	1175
36	Managing the Registry	1193
37	Troubleshooting and Recovery	1223
A	Interface Changes from Windows Server 2003.	1243
B	Optional Components.	1247
C	Understanding TCP/IP v4	1257

Table of Contents

Acknowledgmentsxxxiii
Introduction xxxv

Part I

Prepare

1 Introduction to Windows Server 2008 **3**

 Worth the Wait 4

 Server Virtualization 4

 Server Core..... 4

 PowerShell 5

 Read-Only Domain Controller..... 5

 Active Directory Domain Services..... 5

 Restartable Active Directory Domain Services 6

 Fine-Grained Password Policies..... 6

 Data Mining Tool 6

 Terminal Services..... 7

 Terminal Services Gateway 7

 Terminal Services RemoteApp..... 7

 Terminal Services Web Access 7

 Terminal Services Session Broker..... 8

 Terminal Services Drain Mode..... 8

 Server Manager 8

 Windows Server Backup..... 8

 Clean Service Shutdown..... 9

 More Security Features..... 9

 Address Space Load Randomization 9

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

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

www.microsoft.com/learning/booksurvey/

BitLocker Drive Encryption.....	9
Windows Firewall.....	10
Network Access Protection	10
Versions of Windows Server 2008	10
Summary.....	11
2 Introducing Directory Services	13
Understanding Directory Services	13
Active Directory in Microsoft Windows Server 2008	15
Terminology and Concepts in Active Directory	16
The Active Directory Architecture.....	19
The Directory System Agent	19
Naming Formats	20
The Data Model.....	20
Schema Implementation	20
The Security Model	21
Naming Contexts and Partitions.....	22
The Global Catalog	22
Summary.....	23
3 Planning Namespace and Domains.....	25
Analyzing Naming Convention Needs.....	25
Trees and Forests	26
Defining a Naming Convention	27
Determining Name Resolution	30
Planning a Domain Structure.....	32
Domains vs. Organizational Units.....	33
Designing a Domain Structure	34
Domain Security Guidelines.....	35
Creating Organizational Units.....	36
Planning Multiple Domains.....	36
Planning a Contiguous Namespace	37
Determining the Need for a Multi-Tree Forest.....	37
Creating the Forest	37
Summary.....	38

4 Planning Deployment	39
How Information Technology Functions	40
Identifying Business Needs	41
Getting Specific	41
Seeing into the Future	41
Assessing Current Systems	42
Documenting the Network	42
Making a Roadmap	45
Defining Goals	46
Assessing Risk	47
Summary	48

Part II

Install and Configure

5 Getting Started	51
Reviewing System Requirements	51
Designing a Deployment Environment	53
Choosing an Installation Method	53
Installing Windows Server 2008	53
Automating Server Deployment	61
Installing and Configuring WDS	63
Adding Additional Images	69
Troubleshooting Installations	72
Failure to Boot from a Network Distribution Point	72
Corrupt File During Installation	74
Failure to Find a Hard Disk	75
Stop Errors	76
Summary	77
6 Upgrading to Windows Server 2008	79
Upgrade Matrix	79
Common Threads to Upgrades	80
Pre-Upgrade Steps	81
Architecture	82

Active Directory	83
Hardware Support	85
Software Support	86
Preparing Domains and Computers	87
Upgrading Clients	88
Performing the Upgrade	88
Upgrading To Windows Server 2008	89
Forest and Domain Functional Levels	94
Summary	94
7 Configuring a New Installation	95
Overview of the Tasks	96
Initial Logon	97
Configure Hardware	98
Configuring Basic Computer Information	99
Setting the Time Zone	99
Configuring Networking	101
Setting the Computer Name and Domain	103
Updating and Feedback Settings	106
Enable Updates and Feedback	106
Getting Updates	112
Customizing the Server	112
Adding the Windows PowerShell Feature	113
Enable Remote Desktop	116
Configuring Windows Firewall	117
Closing the Initial Configuration Tasks Wizard	118
Summary	119
8 Installing Server Roles and Features	121
Defining Server Roles	122
Adding and Removing Roles	130
Add a Role	131
Removing a Role	135
Adding and Removing Role Services	139
Adding Role Services	139

Removing Role Services	141
Adding and Removing Features	142
Adding Features	143
Removing Features	144
Summary	145
9 Installing and Configuring Server Core	147
Benefits of a Server Core Installation	148
Security	148
Resources	149
Installing Server Core	149
Configuration	150
Initial Configuration	150
Installing Roles	157
Managing a Server Core Computer	160
Using Windows Remote Shell	162
Using Terminal Server RemoteApp	162
Summary	164
10 Managing Printers	165
Planning Printer Deployment	166
Establishing Printer Naming Conventions	166
Creating a Location-Naming Convention	167
Creating a Print Server	168
Enabling Printer Location Tracking	169
Migrating Print Servers	172
Using the Print Migration Wizard	172
Using the Command Line	174
Installing Printers	174
Deploying Printers with Group Policy	176
Adding PushPrinterConnections Using Group Policy	177
Managing Print Jobs from Windows	179
Temporarily Stopping Print Jobs	179
Canceling Print Jobs	179
Restarting a Print Job	179

Changing a Print Job Priority	180
Moving Print Jobs	180
Managing Printers from the Command Line	181
Setting Security Options.	182
Changing Printer Availability and Group Priorities	182
Specifying a Separator Page	184
Modifying Print Spooling by Printer	185
Spool Print Documents So Program Finishes Printing Faster	186
Print Directly To The Printer	186
Hold Mismatched Documents.	186
Print Spooled Documents First	186
Keep Printed Documents	186
Modifying Spooling on a Print Server	186
Optimizing Print Server Performance	187
Changing the Print Spooling Folder Location.	187
Managing Printer Drivers.	188
Creating Printer Pools.	189
Preparing for Print Server Failure	190
Troubleshooting Printers	191
Starting at the Server	191
Starting at the Client	195
Summary.	195
11 Managing Users and Groups	197
Understanding Groups	197
Assigning Group Scopes.	198
Planning Organizational Units.	200
Creating Organizational Units	201
Moving Organizational Units.	202
Deleting Organizational Units	202
Planning a Group Strategy.	202
Determining Group Names	202
Using Global and Domain Local Groups	203
Using Universal Groups.	203
Implementing the Group Strategy	204

Creating Groups.	204
Deleting Groups.	205
Adding Users to a Group.	205
Managing Default Groups and User Rights.	208
Builtin Local Groups.	208
Builtin Domain Local Groups.	210
Builtin Global Groups.	212
Defining User Rights.	213
Creating User Accounts.	218
Naming User Accounts.	218
Account Options.	218
Passwords.	219
Creating a Domain User Account.	220
Creating a Local User Account.	221
Setting User Account Properties.	222
Testing User Accounts.	223
Managing User Accounts.	223
Finding a User Account.	224
Disabling and Enabling a User Account.	225
Deleting a User Account.	226
Moving a User Account.	226
Renaming a User Account.	226
Resetting a User's Password.	227
Unlocking a User Account.	227
Using Home Folders.	228
Creating Home Folders on a Server.	228
Providing Home Folders to Users.	229
Maintaining User Profiles.	230
Local Profiles.	232
Roaming Profiles.	232
Assigning a Logon Script to a User Profile.	236
Summary.	237

12 Managing File Resources 239

Share Permissions vs. File Permissions.	240
--	-----

Share Permissions	240
File Permissions	241
NTFS Permissions.....	242
How Permissions Work.....	244
Considering Inheritance	245
Configuring Folder Permissions	246
Assigning Permissions to Files.....	247
Configuring Special Permissions.....	248
Ownership and How It Works	250
Shared Folders.....	252
Using Share And Storage Management.....	252
Using the Command Line: Net Share.....	256
Publishing Shares in Active Directory.....	256
Distributed File System (DFS)	257
DFS Terminology	258
Namespace Server Requirements.....	260
Namespace Client Requirements	261
DFS Replication	262
Installing DFS Management.....	263
Creating or Opening a Namespace Root.....	265
Adding Namespace Servers.....	266
Adding DFS Folders.....	267
Changing Advanced Settings	268
Backing Up and Restoring the DFS Folder Targets.....	271
Using DFS Replication.....	271
Summary.....	280
13 Group Policy	281
What's New in Server 2008	282
Components of Group Policy	282
Group Policy Objects.....	282
Order of Implementation.....	283
Order of Inheritance	283
Creating a Group Policy Object.....	284
Editing a Group Policy Object	284

Deleting a Group Policy Object	285
Searching for a Group Policy Object	285
Using Starter GPOs	286
Group Policy Preferences	288
Using Group Policy Preferences for Windows	291
Configuring Common Options	305
Using Group Policy Preferences for Control Panel	306
Delegating Permissions on GPOs	335
Delegating Permission to Create	336
Delegating Permission to Link	336
Delegating Permission to Edit, Delete, or Modify Security	336
Disabling a Branch of a GPO	337
Refreshing Group Policy	337
Backing Up a Group Policy Object	338
Restoring a Group Policy Object	338
Using Group Policy for Folder Redirection	339
Redirecting to One Location	339
Redirecting by Group Membership	340
Removing Redirection	341
Using Resultant Set of Policy (RSOP)	341
Running an RSOP Query	342
A Planning RSOP	342
A Logging RSOP	343
Summary	343

Part III

Administer the Network

14 Managing Daily Operations 347

User Account Control (UAC) for Administration	347
The Admin Approval Mode (AAM)	348
UAC and Registry Virtualization	348
Disabling Aspects of User Account Control	349
Turning Off UAC	352
Using Microsoft Management Console 3.0	353

Setting MMC 3.0 Console Options	353
Creating an MMC Console with Snap-Ins	354
Using the New Taskpad View Wizard.	355
Distributing and Using Consoles.	356
Using MMC for Remote Administration	356
Setting Auditing Policy	357
Auditing Categories	358
Auditing Directory Service Events.	362
Enabling Auditing of AD DS Objects	363
Setting Global Audit Policy	366
Enabling Auditing	367
Using Event Viewer	370
Managing Event Logs	375
Using Task Scheduler.	377
Using the AT Command	378
Delegating Tasks	380
Summary.	381
15 Using Scripts for Consistent Administration	383
Introducing Windows PowerShell.	384
Understanding Windows PowerShell.	385
Basics	386
PowerShell as a Shell.	390
Cmdlets	393
Windows Infrastructure	398
The .NET Framework	398
Windows Management Instrumentation (WMI).	402
Windows Remote Management (WinRM).	404
Component Object Model (COM)	405
Creating Popup and Input Boxes	405
Exploring PowerShell	406
Get-Command	407
Get-Help	408
Get-Member	409
Data Display	410

Parameter Sets and Positional Parameters	412
Loading a Snap-in	414
Powershell Scripting Basics	414
Creating a .ps1 Script	415
Comments	417
Variables	418
Scope	418
Strings	419
Here Strings	420
Wildcards and Regular Expressions	421
Arrays	422
Hashtables	424
Operators	424
Functions	425
Conditional Statements	426
Looping Statements	429
Importing and Exporting From and To Files	430
Flow Control	431
Formatting Cmdlets	432
Exiting from Scripts, Functions, and Loops	434
Dot-Sourcing	434
Passing Arguments	435
Param Statement	436
\$_ and \$input	438
Error Handling	439
Redirection Operators	441
Type Accelerators	442
Escaping Characters	442
Windows PowerShell Examples	442
Typical File System Tasks	442
Testing Whether a File or Directory Exists	443
Windows Server Backup Cmdlets	444
Examples of Managing Server Core	444
XML Support	445

Using the File Transfer Protocol (FTP)	445
Downloading a File Using HTTP	446
Sending E-mail via SMTP	446
Compressing Files	447
Dealing with Dates	447
Timer/Countdown	449
Taking Input from the Console	450
Storing Secure Information	451
Checking Services and Processes	451
Checking the Windows Event Log	453
Getting Memory and CPU Information	455
Accessing Performance Counters	456
Checking Disk Space Usage	458
Working with the Registry	459
Copying Files to Another Directory Recursively	459
Rotating Logs	460
Renaming Files	460
Scheduling Tasks	461
Running Against Multiple Targets	462
Creating XML-Formatted Data	463
Checking Open Ports	464
Head, Tail, Touch, and Tee	464
Summary	466
16 Installing and Configuring Directory Services	467
Active Directory in Windows Server 2008	467
Active Directory Domain Services	468
Active Directory Lightweight Directory Services	468
Active Directory Rights Management Services	470
Active Directory Federation Services	472
Active Directory Certificate Services	473
Installing Active Directory Domain Services	473
Prerequisites for Installing AD DS	474
Installing AD DS Using the Active Directory Domain Services Installation Wizard	476

Operating System Compatibility	477
Deployment Configuration	478
Naming the Domain	479
Setting the Windows Server 2008 Functional Levels	480
File Locations	482
Completing the Installation	483
Adding a Domain Controller to an Existing Domain	484
Verifying the Installation of AD DS	484
Advanced Options	485
Install from Media	486
Unattended Installation	487
Uninstalling AD DS	489
Installing and Configuring Read-Only Domain Controllers	492
What Are Read-Only Domain Controllers?	492
Why Use RODCs?	493
Delegating RODC Installations and Administration	493
Configuring Password Replication Policies	496
Managing AD DS with Active Directory Users and Computers	498
Viewing AD DS Objects	499
Creating a Computer Object	503
Configuring Computer Objects	503
Using Remote Computer Management	504
Publishing a Shared Folder	504
Publishing a Printer	504
Moving, Renaming, and Deleting Objects	505
Managing AD DS with Active Directory Domains and Trusts	506
Launching Active Directory Domains And Trusts	506
Managing Domain Trust Relationships	507
Specifying the Domain Manager	509
Configuring User Principal Name Suffixes for a Forest	509
Using Active Directory Sites And Services	510
AD DS Sites Overview	512
Understanding AD DS Replication	513
Launching Active Directory Sites And Services	515

Installing and Configuring Active Directory Lightweight Directory Service	521
AD LDS Overview.....	522
AD LDS Features	522
Configuring Instances and Application Partitions	523
Managing AD LDS.....	526
Configuring Replication	530
Configuring AD DS and AD LDS Synchronization	531
Summary.....	533
17 Managing Active Directory	535
Maintaining the AD DS Database	535
AD DS Data Storage	535
Garbage Collection	537
Online Defragmentation.....	537
Restartable Active Directory Domain Services	538
Offline Defragmentation of the AD DS Database.....	540
Moving Database and Transaction Log Locations	541
Backing Up AD DS.....	541
The Need for Backups.....	543
Backup Frequency	544
Performing an AD DS Backup with Windows Server Backup.....	545
Restoring AD DS	546
Removing Domain Controllers from AD DS with Ntdsutil	546
Performing a Nonauthoritative Restore of AD DS	548
Performing an Authoritative Restore of AD DS	550
Managing the AD DS Schema.....	552
Requirements for Modifying the AD DS Schema	553
Launching Active Directory Schema.....	554
Modifying the Schema	555
Managing Operations Master Roles.....	561
Transferring Operations Master Roles	564
Seizing Operations Master Roles.....	566
Auditing AD DS	567
Configuring the Audit Policy.....	567

Enabling Auditing of AD DS Changes	570
Summary.....	572
18 Administering TCP/IP	573
Using DHCP	574
Designing DHCP Networks	574
Adding the DHCP Server Role.....	576
Creating a New Scope.....	582
Authorizing the DHCP Server and Activating Scopes	589
Adding Address Reservations	590
Using Multiple DHCP Servers for Redundancy.....	592
Setting Up a DHCP Relay Agent.....	593
DHCP Command-Line Administration.....	595
Using DNS Server	595
Setting Up a DNS Server	596
Creating Subdomains and Delegating Authority	603
Adding Resource Records.....	605
Configuring Zone Transfers	608
Interoperating with Other DNS Servers.....	609
Setting Up a Forwarder	610
Setting Up a WINS Server	613
Summary.....	614
19 Implementing Disk Management	615
Understanding Disk Terminology	616
Overview of Disk Management.....	619
Remote Management.....	622
Dynamic Disks	622
Command Line.....	623
Adding a New Disk	623
Partitions and Volumes.....	625
Creating a Volume or Partition	626
Creating Extended Partitions and Logical Drives	631
Converting a Disk to a Dynamic Disk.....	631
Converting a Disk to a GPT Disk.....	632

Changing the Size of a Volume	633
Adding a Mirror to a Volume	637
Setting Disk Quotas	641
Enabling Quotas on a Disk	642
Setting Per-User Quotas	643
Importing and Exporting Quotas	645
Enabling File Encryption	647
Summary	649
20 Managing Storage	651
Using File Server Resource Manager	651
Installation and Initial Configuration of FSRM	652
Scheduling Storage Reports	654
Using Directory Quotas	657
Screening Files	663
Overview of SAN Manager	670
Concepts and Terminology	672
Installing Storage Manager For SANs	674
Using the Storage Manager For SANs Console	675
Managing Server Connections	676
Managing iSCSI Targets	678
Managing iSCSI Security	679
Logging In to iSCSI Targets	680
Creating and Deploying Logical Units (LUNs)	681
Extending a LUN	687
Removable Storage	689
Concepts and Terminology	689
Use and Management	693
Summary	697
21 Using Clusters	699
What Is a Cluster?	699
Network Load Balancing Clusters	700
Failover Clusters	700
New Failover Cluster Features	701

Windows Server 2008 Core	702
Cluster Scenarios	703
Web Server	703
Terminal Services	703
Mission-Critical Applications and Services	703
Requirements and Planning	704
Identifying and Addressing Goals	704
Identifying a Solution	705
Identifying and Addressing Risks	705
Making Checklists	706
Network Load Balancing Clusters	706
NLB Concepts	706
Choosing an NLB Cluster Model	707
Creating an NLB Cluster	709
Planning the Capacity of an NLB Cluster	716
Providing Fault Tolerance	717
Optimizing an NLB Cluster	717
Failover Clusters	718
Failover Cluster Concepts	718
Types of Resources	720
Defining Failover and Failback	723
Configuring a Failover Cluster	724
Planning the Capacity of a Failover Cluster	726
Creating a Failover Cluster	727
HPC Clusters	740
Summary	742

Part IV

Secure the Network

22 Planning Security	745
The Fundamental Principles of Security	745
Confidentiality	746
Integrity	747
Availability	748

The Eight Rules of Security	748
Rule of Least Privilege	749
Rule of Change Management	749
Rule of Trust	749
Rule of the Weakest Link	750
Rule of Separation	750
Rule of the Three-Fold Process	750
Rule of Preventative Action	750
Rule of Immediate and Proper Response	751
The Higher Security Mindset	751
Think in Terms of Zones	753
Create Chokepoints	754
Layer Your Security	755
Understand Relational Security	756
Divide Responsibility	759
Summary	761

23 Implementing Security 763

Introduction	763
Secure at Installation	764
Server Core	767
Roles and Features Wizards	770
Securing the Startup: BitLocker	773
Setting Up BitLocker	773
Securing the Accounts	779
Disabling the Administrator Account	780
Password Policies on Standalone Servers	781
Password Policies in Domains	781
Windows Server 2008 Firewall	785
Setting Firewall Policies Using Group Policy	786
Firewall Rule Basics	788
Rule Definitions	789
Creating a Firewall Policy	791
Windows Firewall Via Command Line	793
Additional Security Changes	795

New Groups	796
Auditing	796
LanMan Hashes and Authentication Level	797
SMBv2	797
Read Only Domain Controllers	798
Summary.....	798
24 Administering Network Access Protection	799
Why the Need for NAP?.....	799
Planning the Deployment	801
NAP Shopping List.....	801
Servers Needed for NAP.....	802
Benefits of NAP	804
Determining the Health Policy	804
Policies Checked	804
Enforcement Levels	806
Determining Exemptions	807
Testing IPsec NAP Enforcement	808
Setting Up a Certificate Server	809
Configuring the NAP Health Policy Server	818
Client Settings for NAP.....	819
IEEE 802.1x Enforcement in NAP	827
Configuring IEEE 802xz Enforcement.....	828
Configuring 802.1X Enforcement	828
The Politics of Deployment	830
Summary.....	832
25 Patch Management	833
Why It's Important.....	834
The Patching Cycle	835
Assess	836
Identify	836
Evaluate and Plan	838
Deploy	838
Repeat	839

Deployment Testing	839
Test Network Deployment	839
Beta User Deployment	840
Full Deployment	840
Obtaining Updates	841
Automatic Updates	841
Windows Server Update Services	841
Systems Center Configuration Manager	845
Third-Party Products	845
Summary	846

26 Implementing Remote Access Strategies: SSTP, VPN, and Wireless 847

Introduction	847
Network Policy Server	848
Planning for NPS	848
Start with the Policies	849
Define the Support	850
Secure Sockets Tunneling Protocol	850
The SSTP Process	851
Configuring SSTP	852
Installing the Server Authentication Certificate	858
Installing Routing And Remote Access	868
Configuring SSTP-based Connection Clients	877
Making the SSTP Connection	881
Troubleshooting Connections	883
Using NPS in Windows Server 2008	887
Configuring Remote Access Per User	887
Configuring Remote Access in the NPS Network Policy	887
Wireless Deployment	889
Prerequisites	890
Adding RADIUS Clients to the Network	892
Configuring the Access Points	893
Configuring Clients to Use Secure Wireless	894
Summary	899

Part V

Use Support Services and Features

27 Interoperability	903
General UNIX Interoperability	903
Permissions and Security Concepts	904
A UNIX File Listing	904
Symbolic Links	906
Privilege Levels	907
Basic Connectivity	908
File Transfer Protocol	908
Telnet	909
File Systems	910
Printing	912
Network File System	912
Legacy User Name Mapping	914
Server For NFS	916
Microsoft Identity Management for UNIX	923
Installing Microsoft Identity Management for UNIX	924
Subsystem for UNIX-based Applications	928
Macintosh Interoperability	932
Summary	932
28 Managing Software	933
Using the Group Policy Software Installation Extension	933
Finding the Right Mix of Services	935
Windows Installer Packages	936
Zap Files	936
Setting Up the Group Policy Software Installation Extension	939
Creating a Software Distribution Point	939
Creating a GPO for Application Deployment	940
Configuring the Group Policy Software Installation Extension	943
Working with Packages	947
Adding a Package to a Group Policy	947
Changing Application Properties	950

Applying Package Upgrades	952
Applying Package Modifications	953
Removing and Redeploying Packages	955
Using Software Restriction Policies	955
How Software Restriction Policies Work	956
Creating Software Restriction Policies	957
Windows Deployment Services	959
Summary	959
29 Working with Windows Virtualization	961
Hyper-V Overview	962
Scenarios	963
Requirements	964
Installation	965
Installing On Windows Server Core	965
Installing on Windows Server 2008	965
Initial Configuration	968
Configuring Networks	969
Server Settings	972
Creating A Virtual Machine	974
Creating a Basic VM	975
Machine Settings	978
Management Settings	994
Working With A Virtual Machine	998
Starting, Stopping, Saving, Snapshotting	998
Clipboard	999
Export/Import	1000
Summary	1003
30 Deploying Terminal Services	1005
Concepts	1007
Remote Access	1008
Central Management	1008
Requirements	1009
RAM	1009

CPU	1009
Network Utilization	1010
Capacity Planning	1010
Installation	1011
Improving the User Experience	1020
Enabling Remote Desktop for Administration Mode	1023
Installing Programs	1024
Administration	1027
Terminal Services Manager	1027
Terminal Services Configuration	1037
Terminal Services Licensing	1042
Installing Terminal Server Licensing	1042
RemoteApps	1044
TS RemoteApp Manager	1045
Adding RemoteApps	1050
Deploying RemoteApps	1052
TS Web Access	1056
Remote Desktop Web Connection	1057
TS Web Access RemoteApp Programs	1058
Summary	1059

31 Internet Information Services1061

Architecture	1062
Components	1062
Modules	1063
Installing IIS	1065
Installing Using the Server Roles Wizard	1065
Installing Using Windows Package Manager	1066
Administration Tools	1068
Internet Information Server (IIS) Manager	1068
AppCmd.exe	1071
Windows Management Instrumentation (WMI)	1073
Administrative Tasks	1073
Managing Servers	1073
Managing Sites	1084

Managing Web Applications	1093
Managing Virtual Directories	1094
Understanding Delegation and Permissions	1094
Delegating Site and Application Management	1095
Configuring Permissions to View and Manage Content	1097
Understanding the Configuration Store	1098
Using Shared Configuration	1099
Remote Administration	1099
Installing and Managing the FTP Publishing Service	1100
FTP Current Sessions	1102
FTP Directory Browsing	1102
FTP Firewall Support	1102
FTP Messages	1102
FTP SSL Settings	1102
FTP User Isolation	1102
Active Directory Federation Services (AD FS)	1103
Summary	1104

Part VI

Tune, Maintain, and Repair

32 Windows Reliability And Performance Monitor 1107

Using Resource View	1107
CPU Details	1109
Disk Details	1110
Network Details	1110
Memory Details	1110
Using Performance Monitor	1111
Adding Counters in Performance Monitor	1112
Changing the Performance Monitor Display	1114
Saving the Performance Monitor Display	1114
Connecting to a Remote Computer Using Performance Monitor	1115
Using Reliability Monitor	1115
Viewing Reliability Monitor on a Remote Computer	1116
Interpreting the System Stability Index	1117

Creating a Data Collector Set	1119
Building a Data Collector Set from a Template.....	1120
Creating a Data Collector Set from Performance Monitor	1123
Constructing a Data Collector Set Manually	1123
Creating a Data Collector Set to Monitor Performance Counters.....	1125
Scheduling Data Collection	1126
Managing Collected Data	1128
Working with Data Log Files	1129
Viewing Reports	1131
Summary.....	1132
33 Disaster Planning	1133
Planning for Disaster.....	1133
Identifying the Risks	1134
Identifying the Resources.....	1135
Developing the Responses.....	1136
Testing the Responses.....	1139
Iterating.....	1140
Preparing for a Disaster	1141
Setting Up a Fault-Tolerant System.....	1141
Backing Up the System.....	1142
System Repair.....	1142
Specifying Recovery Options.....	1144
Summary.....	1145
34 Using Backup	1147
Installing the Backup Service.....	1147
Scheduling a Backup.....	1149
Choosing Volumes to Back Up	1149
Designating a Storage Location	1149
Creating the Backup Schedule.....	1150
Implementing a Rotating Backup Set.....	1154
Modifying a Backup Schedule.....	1155
Stop Running Scheduled Backups.....	1156

Using the Backup Once Wizard	1157
Using the Wbadmin Command	1159
Wbadmin enable backup	1160
Wbadmin disable backup	1160
Wbadmin start backup	1160
Wbadmin stop job	1161
Wbadmin start recovery	1161
Wbadmin start systemstatebackup	1161
Wbadmin start sysstaterecovery	1161
Wbadmin start sysrecovery	1162
Windows Recovery Environment	1162
Wbadmin get versions	1162
Wbadmin get status	1163
Recovering Your Server	1165
Recovering Volumes	1166
Recovering Files and Folders from the Local Server	1167
Recovering Files and Folders from Another Server	1168
Recovering Applications and Data	1169
Recovering the Operating System	1171
Restoring a Backup Catalog	1173
Summary	1174
35 Planning Fault Tolerance and Avoidance	1175
Mean Time to Failure and Mean Time to Recover	1176
Protecting the Power Supply	1177
Local Power Supply Failure	1178
Voltage Variations	1179
Short-Term Power Outages	1182
Long-Term Power Outages	1182
Disk Arrays	1183
Hardware vs. Software	1183
RAID Levels for Fault Tolerance	1183
Hot-Swap and Hot-Spare Disk Systems	1189
Distributed File System	1190
Clustering	1190

Network Load Balancing	1190
Failover Clustering	1190
Summary	1191
36 Managing the Registry	1193
Introducing the Registry	1193
The Origins of the Registry	1194
How Registry Data Is Used	1195
Functional Changes in Windows Server 2008	1196
Understanding the Registry's Structure	1198
The Root Keys	1201
Major Subkeys	1203
How Data Is Stored	1206
Creating Registry Items with the Registry Wizard	1209
Using the Registry Editors	1211
A Whirlwind Tour of the Registry Editor	1211
A Whirlwind Tour of Reg	1220
Backing Up and Restoring the Registry	1221
Choosing a Backup Method	1221
System Recovery	1222
Summary	1222
37 Troubleshooting and Recovery	1223
Determining Priorities	1223
Recovering a System	1225
Identifying Possible Causes	1225
Rolling Back a Device Driver	1226
Recovering Your Server	1227
Recovering Volumes	1227
Recovering Files and Folders from the Local Server	1229
Recovering Files and Folders from Another Server	1229
Recovering Applications and Data	1231
Recovering the Operating System	1233
Recovering the System State	1234
Using System Information	1236

Verifying the Status of Services1236

Using the System Configuration Utility1239

Using the System File Checker1240

Using the Shutdown Event Tracker.....1241

Summary.....1242

A Interface Changes from Windows Server 2003.....1243

B Optional Components.....1247

C Understanding TCP/IP v41257

About the Authors1281

Index.....1283



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

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

www.microsoft.com/learning/booksurvey/

Acknowledgments

No book of this size or scope ever comes only from the authors' hands. We are indebted to many people for their efforts to help us succeed.

From Microsoft Canada, Roger Benes played a crucial and very much appreciated role in helping to make critical connections for us. Plus he's a good and valued friend.

Also from Microsoft Canada, we're indebted to Mark Dickinson, who took that connection to the next step, and to Sasha Krsmanovic, Charlie's super MVP Lead, for always being there when we really needed an answer.

Building and running the kind of hardware it takes to do a book like this is a challenge, even with the ability to virtualize. Hewlett-Packard Canada was extremely generous in lending us a wonderful, fully loaded ML350G5 server to use for this book. It's a great server and we love it. We're indebted to Gordon Pellose and Alan Rogers at HP Canada; SanSan Strozier of HP in the United States; Sharon Fernandez of Hill & Knowlton, HP's public relations firm in Canada; and especially David Chin, also of Hill & Knowlton, for making the loan possible and being generous with their time and expertise.

We also had the use of another excellent Hewlett-Packard server, a DL380G5, thanks to Greg Rankich of Xtreme Consulting Group, Inc. and Dan Cox of Hewlett-Packard USA. A great help to us and much appreciated.

Creating and testing Storage Area Networks is hard to do without a SAN, and we are indebted to Dylan Locsin and Chris Carrier of EqualLogic for generously allowing us to borrow an amazing PS3800XV SAN array. A very well-built and powerful SAN, it served us well and we're grateful for the help.

All the screen captures in this book were made using HyperSnap from Hyperionics. Capturing screens in Server Core was a special challenge, but Greg Kochiniak of Hyperionics created a special build of HyperSnap just for Server Core. Now that's customer support!

We also had help from several other experts to create the content in this book. For three of the security chapters, Susan Bradley, a Microsoft MVP and forensic accountant, was invaluable, jumping in to help and meeting tight deadlines. A fourth security chapter came from Dana Epp, a Security MVP and developer of AuthAnvil, our preferred authentication solution. The clustering chapter was primarily the work of Mark Cooper, of Microsoft, who did an excellent job. For the Active Directory chapters, we couldn't have had a better author than Stan Reimer, who agreed to a ridiculous schedule and then met it with quality. Marco Shaw, a fellow Microsoft MVP for AdminFrameworks, knows way

more about PowerShell than we ever will and contributed the scripting chapter. Finally, Kurt Dillard did an excellent and much appreciated job on the IIS chapter.

We very much appreciate the great people who make working with Microsoft Learning a real pleasure. It starts with Martin DelRe, whom we've known for many years now, and who really pulled out all the stops when we needed a hand at the end. Thank you, Martin; you're a true professional. Our project editor was Melissa von Tschudi-Sutton, who has been a pleasure to work with throughout this long process. This is our second book with Melissa and we hope it won't be the last. We deeply appreciate her enthusiasm, feedback, editorial insights, and patience. Especially her patience, which we sorely tried at times.

Randall Galloway was our technical editor, and we much valued his efforts and comments throughout the process. Our indexer at Hyde Park Publishing Services and desktop publisher at Custom Editorial Productions, Inc. did an excellent and much-appreciated job. The editorial team of Megan Smith-Creed and Becka McKay performed a meticulous and sensitive edit, for which we're very grateful. And last but absolutely not the least, the production and support people at Microsoft Learning, without whom this book would not exist. It is a pleasure to work with a team of professionals of this caliber. Thank you.

As always, we thank the people from past collaborations whose contributions to everything we write can't be overstated: Rudolph S. Langer and David J. Clark.

Introduction

To improve is to change; to be perfect is to change often. –Winston Churchill

Change is inevitable, constant, and inescapable. You can brood about it or you can take the optimist’s view—and Churchill was nothing if not an optimist—and accept that improvement isn’t possible without change. And even though upgrading servers and clients can be a significant challenge for an administrator, it also represents an opportunity to improve how your network functions. And you can be sure that Windows Server 2008 contains many tools to help you move in the direction of change for the better.

Meet the Family

Windows Server is available in five primary versions. Three of those are available without Windows Server Hyper-V, bringing the total number of editions to eight:

- Windows Server 2008 Standard
- Windows Server 2008 Enterprise
- Windows Server 2008 Datacenter
- Windows Server 2008 for Itanium-Based Systems
- Windows Web Server 2008
- Windows Server 2008 Standard without Hyper-V
- Windows Server 2008 Enterprise without Hyper-V
- Windows Server 2008 Datacenter without Hyper-V

For the five primary editions, the table below shows the features available in each one.

Edition	Server Core	Windows Deployment Services	Server Manager	Terminal Services Gateway and RemoteApp	Active Directory Rights Management	Network Access Protection	Hyper-V	Internet Information Services 7.0	Internet Information Services 7.0
Standard	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enterprise	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Datacenter	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Web	Yes	No	Yes	No	No	No	No	Yes	
Itanium	No	No	Yes	No	No	No	No	Yes	

The next table provides some general guidance on hardware requirements. The actual requirements will vary depending on your system and particularly on the applications and features that you use. Processor performance is dependent upon not only the clock frequency of the processor, but also the number of cores and the size of the processor cache. Disk space requirements for the system partition are approximate. Itanium-based and x64-based operating systems will vary from these disk size estimates. Additional available hard disk space may be required if you are installing over a network.

Component	Requirement
Processor	Minimum: 1 GHz (x86 processor) or 1.4 GHz (x64 processor) Recommended: 2 GHz or faster.
Memory	Minimum: 512 MB RAM Recommended: 2 GB RAM or more Optimal: 2 GB RAM for full installation or 1 GB RAM for Server Core installation Maximum for 32-bit systems: 4 GB (Standard) or 64 GB (Enterprise and Datacenter) Maximum for 64-bit systems: 32 GB (Standard) or 2 TB (Enterprise, Datacenter, and Itanium-based Systems)
Available Disk Space	Minimum: 10 GB Recommended: 40 GB or more Computers with RAM in excess of 16 GB will require more disk space for paging, hibernation, and dump files.
Drive	DVD-ROM drive
Display	Super VGA (800 x 600) or higher resolution monitor
Other	Keyboard Mouse or other pointing device

Note An Intel Itanium 2 processor is required for Windows Server 2008 for Itanium-Based Systems.

New in Windows Server 2008

Of course, there are lots of new features in Windows Server 2008, though many of them are not obvious at first glance. Some of the highlights include:

- Server Manager, the expanded Microsoft Management Console (MMC), provides a one-stop interface for server configuration and monitoring with wizards to streamline common server management tasks.

- Windows PowerShell, a new optional command-line shell and scripting language, enables administrators to automate routine system administration tasks across multiple servers.
- Group Policy preference extensions allow the configuration of settings that are simpler to deploy and manage than logon scripts.
- Windows Reliability and Performance Monitor provides diagnostic tools to give you ongoing visibility into your server environment, both physical and virtual, to pinpoint and resolve issues quickly.
- Optimized server administration and data replication increase control over servers in remote locations, such as a branch office.
- Server Core allows minimal installations where only the server roles and features you need are installed, reducing maintenance needs and decreasing the available attack surface of the server.
- Failover clustering wizards make it easy for even IT generalists to implement high-availability solutions. Internet Protocol version 6 (IPv6) is now fully integrated.
- The new Windows Server Backup incorporates faster backup technology and simplifies data or operating system restoration.
- Windows Server 2008 Hyper-V allows you to virtualize server roles as separate virtual machines (VMs) running on a single physical machine, without the need to buy third-party software.
- Multiple operating systems—Windows, Linux, and others—can be deployed in parallel on a single server using Hyper-V.
- Terminal Services (TS) RemoteApp and TS Web Access allow programs that are accessed remotely to be opened with just one click and appear as if they are running seamlessly on the end user's local computer.
- Microsoft Web publishing platform unifies IIS 7.0, ASP.NET, Windows Communication Foundation, and Windows SharePoint Services.
- Network Access Protection helps ensure your network and systems aren't compromised by unhealthy computers, isolating and/or remediating those computers that don't comply with the security policies you set.
- User Account Control provides new authentication architecture for protection against malicious software.
- Read Only Domain Controller (RODC) allows a more secure method for local authentication of users in remote and branch office locations using a read-only replica of your primary AD database.

- BitLocker Drive Encryption provides enhanced protection against data theft and exposure of server hardware if lost or stolen, and it provides more secure data deletion when your servers are eventually decommissioned.

And, as the saying goes, there's more—much more.

What's In This Book

Windows Server 2008 Administrator's Companion consists of thirty-seven chapters arranged in an order roughly corresponding to each stage in the development of a Windows Server 2008 network.

Chapters 1 through 4 are all about planning. Perhaps you've heard Edison's famous quote, "Genius is one percent inspiration and ninety-nine percent perspiration." Modify that slightly and you have a good motto for network building: A good network is one percent implementation and ninety-nine percent preparation. The first chapter is an overview of Windows Server 2008, its components, and its features. This is followed by chapters on directory services and namespace planning. The last chapter in this section covers specific issues that need to be addressed when planning your deployment.

Chapters 5 through 9 cover installation and initial configuration. These chapters take you through the process of installing Windows Server 2008 and configuring hardware. Also included are chapters on installing server roles and installing Server Core.

Chapters 11 through 21 cover day-to-day tasks, including managing file resources and using scripts for administration.

Chapters 22 through 26 are all about security—how make a plan and how to implement a security plan.

Chapters 27 through 31 cover additional features including virtualization and terminal services—both of which add exciting new capabilities to Windows Server 2008.

The final chapters on tuning, maintenance, and repair cover important material on network health. There's a chapter on the Windows Server Backup and another on performance monitoring. There are also chapters on the important topics of disaster planning and prevention. If, despite your best efforts, the network falters, here's where you'll find information on troubleshooting and recovery. In addition, we include a chapter on the registry—the brains of Windows Server 2008—and some advice if you're contemplating brain surgery.

At the end of the book, you'll find supplemental material about interface changes and support tools.

Within the chapters themselves, we've tried to make the material as accessible as possible. You'll find descriptive and theoretical information, as well as many step-by-step

examples for how to implement or configure a particular feature. These are supplemented with graphics that make it easy to follow the written instructions.

In addition, we've made extensive use of the reader aids common to all books in the Administrator's Companion series.

Note Notes generally represent alternate ways to perform a task or some information that needs to be highlighted. Notes may also include tips on performing tasks more quickly or in a not-so-obvious manner.

Important Text highlighted as Important should always be read carefully. This is information that can save time or prevent a problem or both.



Real World

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

Under the Hood

When wizards perform their magic or other procedures are done offstage, Under The Hood sidebars describe what is going on that can't be seen.

We encourage you to take advantage of additional books offered by Microsoft Learning. Other Windows Server 2008 titles that allow in-depth studies of specific areas include *Windows Server 2008 Active Directory Resource Kit*, *Windows Server 2008 Security Resource Kit*, and *Windows Group Policy Resource Kit: Windows Server 2008 and Windows Vista*.

System Requirements

The following are the minimum system requirements to run the companion CD provided with this book:

- Microsoft Windows XP, with at least Service Pack 2 installed and the latest updates installed from Microsoft Update Service
- CD-ROM drive
- Internet connection

- Display monitor capable of 1024 x 768 resolution
- Microsoft Mouse or compatible pointing device
- Adobe Reader for viewing the eBook (Adobe Reader is available as a download at <http://www.adobe.com>)

About the Companion CD

The companion CD contains the fully searchable electronic version of this book and additional sample chapters from other titles that you might find useful. We've also included scripts from Chapter 9 and Chapter 15.

Digital Content for Digital Book Readers: If you bought a digital-only edition of this book, you can enjoy select content from the print edition's companion CD. Visit <http://www.microsoftpressstore.com/title/9780735625051> to get your downloadable content. This content is always up-to-date and available to all readers.

Support

Every effort has been made to the accuracy of this book and companion CD content. Microsoft Press provides corrections to this book through the Web at <http://www.microsoft.com/mspress/support/search.aspx>

If you have comments, questions, or ideas regarding the book or companion CD content, please send them to Microsoft Press using either of the following methods:

E-mail: mspinput@microsoft.com

Postal mail:

Microsoft Press
Attn: Windows Server 2008 Administrator's Companion Editor
One Microsoft Way
Redmond, WA 98052-6399

Please note that product support is not offered through the preceding mail addresses. For support information, please visit the Microsoft Help and Support Web site at <http://support.microsoft.com>.

Chapter 9

Installing and Configuring Server Core

Benefits of a Server Core Installation	148
Installing Server Core.....	149
Configuration	150
Initial Configuration.....	150
Managing a Server Core Computer.....	160
Summary	164

The usual progression for an operating system (or an application, for that matter) is to grow and add features, sometimes well beyond what any of us want or need. Windows Server 2008 reverses that trend with a completely new installation option—Server Core. When you install Windows Server 2008, regardless of which edition you're installing, you have the option of choosing a full installation, with everything, or just the Server Core portion.

Server Core is just the essentials, with little or no graphical interface. The logon provider has the same graphical look, but then, when you've logged in, all you see is a single command-shell window, as shown in Figure 9-1.

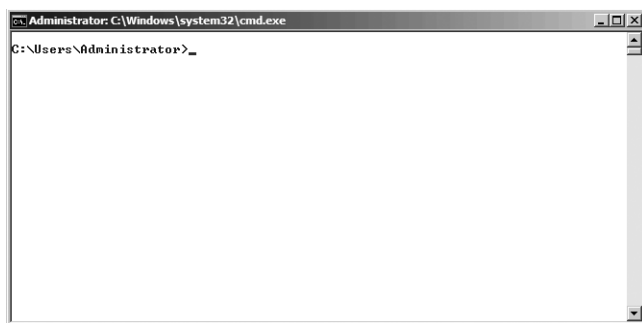


Figure 9-1 The Windows Server 2008 Core desktop.

Note For improved readability in screen shots used here and in the rest of the book, we've changed the default color scheme for Command Prompt windows to dark blue text on a white background.

Benefits of a Server Core Installation

All Windows Server 2008 editions support Server Core, with the exception of Compute Cluster Edition. And installing Server Core doesn't give you a break on the cost of the license—it's exactly the same license and media as the full Windows Server 2008 installation. At install time, you simply choose which edition you are installing. So, if you don't save any money, and you don't have special media, and you have reduced functionality, why in the world would you choose Server Core over the full product? It's simple, really: security and resources. Let's take a look at those two in a bit more depth before we go on to the details of how to actually install and configure Server Core.

Security

In the old days, whenever you installed Windows Server, it automatically installed just about everything that was available, and turned on all the services that you were likely to need. The goal was to make installation as simple as possible, and this seemed like a good idea at the time. Sadly, the world is not a friendly place for computers any more, and that approach is no longer safe or wise. The more services that exist, and the more services that are enabled, the more attack vectors the bad guys have to work with. To improve security, limiting the available attack surfaces is just good common sense.

In Server Core, Microsoft has completely removed all managed code, and the entire .NET Framework. This leaves a whole lot fewer places for possible attack. This does, obviously, impose some severe limits on what you can and can't do with a Server Core installation. And it also means that there isn't any PowerShell possible, which in our opinion is easily the biggest limitation of Server Core—but one that we hope will be resolved in a later version of Windows Server.

The default installation of Server Core has only less than 40 services running. A typical full Windows Server 2008 installation, with one or two roles enabled, is likely to have 60 or even 70 or more services running. Not only does the reduced number of services limit the potential attack surface that must be protected, but it also limits the number of patches that are likely to be required over the life of the server, making it easier to maintain.

Resources

The second major benefit to running Server Core is the reduced resources required for the base operating system. While the official requirements for installing Windows Server 2008 are the same for Core as for a full installation, the effective numbers are significantly less, in our experience—with the exception of the disk space required (only 2 to 3 GB of HD space for a running Core installation). Plus with the limited subset of tasks that you can perform, we think Server Core is ideal for running those infrastructure tasks that everyone runs, and that don't require much interaction over time. Tasks such as DHCP, DNS, and, increasingly, virtualization. Now if it just had PowerShell...

Installing Server Core

Installing Windows Server 2008 Server Core is ultimately the same as installing the full graphical version of Windows Server 2008. The installation engine is the same, and the only difference occurs during the install, when you have to choose which version of Windows Server 2008 to install, as shown in Figure 9-2.

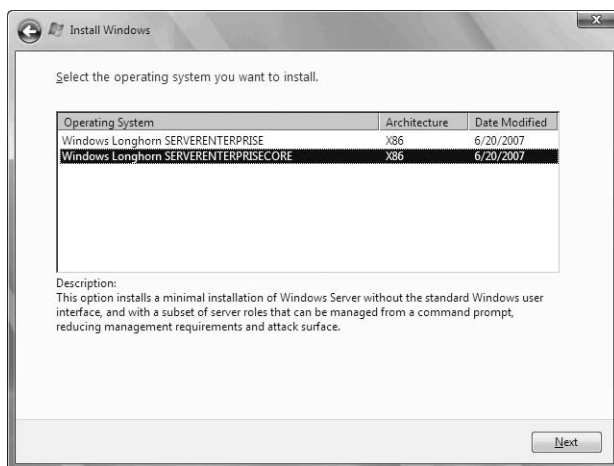


Figure 9-2 During initial installation, you make an irrevocable choice between Server and Server Core.

Once installation completes, you're presented with the initial logon screen. Log on as Administrator, with no password, and you'll be immediately prompted to change the password and then logged on to the desktop, as shown earlier in Figure 9-1. All initial configuration takes place from the command line, though once you've configured the basics, you'll be able to use familiar management consoles remotely.

You can use an unattend.xml file to automate the initial install and configuration of your Server Core installation. For details on the settings and syntax of unattend.xml, see <http://go.microsoft.com/fwlink/?LinkId=81030>.

Configuration

You can do all configuration tasks for Server Core at the command line, and all the initial tasks must be done at either the command line or as part of the installation process by using an unattend.xml script. Once you're performed these initial configuration tasks, you can then use regular Windows management consoles to manage the additional settings. Unfortunately, there isn't a single command shell for the tasks, but a collection of old favorites, each with a different behavior and syntax.

Initial Configuration

The initial steps you'll need to perform on a Server Core installation will depend somewhat on your intended use of the installation, but we think that the following ones are the most obvious:

- Set a fixed IP address.
- Change the server name to match your internal standards.
- Join the server to a domain.
- Change the default resolution of the console.
- Enable remote management through Windows Firewall.
- Enable remote desktop.
- Activate the server.

We'll walk through these steps for you, and leave you with a couple of basic scripts that you can modify to automate these tasks for your environment. Table 9-1 contains the settings we'll be using during this install scenario.

Table 9-1 Settings for Initial Server Core Configuration (Example)

Setting	Value
IP Address	192.168.51.4
Gateway	192.168.51.1
DNS Server	192.168.51.2
Server Name	Hp350-core-04

Table 9-1 Settings for Initial Server Core Configuration (Example)

Setting	Value
Domain To Join	example.local
Default Desktop Resolution	1024x768
Remote Management	Enable for Domain Profile
Windows Activation	Activate

Set IP Address

To set the IP address for the server, you need to use the **netsh** command-line tool. Follow these steps to configure TCP/IP:

1. From the command window, use **netsh** to get the “name” (index number) of the network card.

```
netsh interface ipv4 show interfaces
```

2. The result will be something like the following:

```
C:\Users\administrator>netsh interface ipv4 show interfaces
```

Idx	Met	MTU	State	Name
2	10	1500	connected	Local Area Connection
1	50	4294967295	connected	Loopback Pseudo-Interface 1

The Idx value for your real network card (2, in this case) will be used as the name value in future commands for **netsh**.

3. Now, using the Idx value from step 2, run the following **netsh** command:

```
netsh interface ipv4 set address name=<Idx> source=static
address=<IP Address> mask=<netmask>
gateway=<IP Address of default gateway>
```

Note The **netsh** lines above, and in examples below, are actually one long command line, but we had to break them (and indent subsequent lines) because of the limitations of the printed page. And it's not just **netsh** that is a problem—most of the commands you end up having to use with Server Core are long and will be artificially broken in this chapter.

4. Next, specify the DNS server for the adapter, using **netsh** again:

```
netsh interface ipv4 add dnsserver name="<Idx>"
address=<IP Address of DNS Server> index=1
```

5. For secondary DNS servers, repeat the command in step 4, increasing the index value by one each time.

Renaming the Server and Joining to a Domain

The next step in initial configuration is assigning the name of the server and joining it to a domain. During initial installation of Windows Server 2008, an automatically generated name is assigned to the server and the server is placed in the WORKGROUP workgroup. You'll want to change this to align the computer name with your corporate naming policy and join the server to the correct domain and Organizational Unit. Our naming policy here has three parts: the model of server, the functional role, and a number reflecting its IP address. Thus the Server Core computer we're building in this chapter is named hp350-core-04: it's a Hewlett Packard ML 350 G5 server, it is running Server Core, and the final octet of its IP address is four. Your server naming convention will undoubtedly be different, but the important thing is to be consistent. Our domain for this book is example.local.

To change the name of the server and join it to the example.local domain, follow these steps:

1. From the command prompt, use the **netdom** command to change the name of the server:

```
netdom renamecomputer %COMPUTERNAME% /newname:<newname>
```

2. After you change the name, you must reboot the server.

```
shutdown /t 0 /r
```

3. After the server restarts, log on to the Administrator account.
4. Use the **netdom** command again to join the domain.

```
netdom join %COMPUTERNAME% /DOMAIN:<domainname>
/userd:<domain admin account> /password:*
```

5. You'll be prompted for the password for the domain administrative account you used. Enter the password. When the domain join has succeeded, you'll again need to reboot the server.

```
shutdown /t 0 /r
```

6. After the server restarts, log back on to a domain administrator's account. (You'll need to click Change User because the server will default to the local administrator account.)

Under the Hood Scripting Initial Configuration

If you set up more than one or two Server Core computers, you'll quickly get tired of doing all this interactively from the command prompt. We know we did. You have the choice of either using an unattend.xml file to set options during the install or using simple scripts to automate the process. Both work, and both have their adherents, but we tend to use scripts after the fact. You can modify the following three scripts (which you'll also find on the companion CD) for your environment to automate the initial TCP/IP, server name, and domain join steps.

The first script sets the IP address, sets the DNS server, and changes the server name.

```
echo off
REM filename: initsetup1.cmd
REM
REM initial setup for a Server 2008 Server Core installation.
REM command file 1 of 3
REM
REM Created: 4 September, 2007
REM ModHist: 5/9/07 - switched to variables (cpr)
REM
REM Copyright 2007 Charlie Russel and Sharon Crawford. All rights reserved.
REM You may freely use this script in your own environment, modifying it
REM to meet your needs. But you may not re-publish it without permission.

REM first, set a fixed IP address. You'll need to know the index number
REM of the interface you're setting, but in a default Server Core install,
REM with only a single NIC, the index should be 2. To find the index,
REM you can run:
REM     netsh interface ipv4 show interfaces
REM

SETLOCAL
REM Change the values below to match your needs
SET IPADD=192.168.51.4
SET IPMASK=255.255.255.0
SET IPGW=192.168.51.1
SET DNS1=192.168.51.2
SET NEWNAME=hp350-core-04

netsh interface ipv4 set address name="2" source=static
address=%IPADD% mask=%IPMASK% gateway=%IPGW%

REM Next, set DNS to point to DNS server for example.local.
REM 192.168.51.2 in this case
netsh interface ipv4 add dnsserver name="2" address=%DNS1% index=1
```

```
REM Now, we need to change the computer name. After we're done, the server
REM must be restarted, and we can continue with the next batch of commands.
REM we use the /force command here to avoid prompts
netdom renamecomputer %COMPUTERNAME% /newname:%NEWNAME% /force
```

```
@echo If everything looks OK, the it's time to reboot
pause
REM now, shutdown and reboot. No need to wait.
shutdown /t 0 /r
```

The second script we use is to actually join the server to the domain.

```
@echo off
REM Filename: initsetup2.cmd
REM
REM initial setup for a Server 2008 Server Core installation.
REM command file 2 of 3
REM
REM Created: 4 September, 2007
REM ModHist:
REM
REM Copyright 2007 Charlie Russel and Sharon Crawford. All rights reserved.
REM You may freely use this script in your own environment, modifying it
REM to meet your needs. But you may not re-publish it without permission.
```

```
SETLOCAL
SET DOMAIN=example.local
SET DOMADMIN=Administrator
```

```
REM Join the domain using the netdom join command. Prompts for password
REM of domain administrator account set above
```

```
netdom join %COMPUTERNAME% /DOMAIN:%DOMAIN% /userd:%DOMADMIN% /password:*
```

```
REM now, shutdown and reboot. No need to wait, and that's all we can do
REM at this time
```

```
shutdown /t 0 /r
```

Finally, use the third script to enable remote management and activate the server.

```
echo off
REM initsetup3.cmd
REM
REM initial setup for a Server 2008 Server Core installation.
REM command file 3 of 3
REM
REM Created: 4 September, 2007
REM ModHist:
REM
```



```
REM Copyright 2007 Charlie Russel and Sharon Crawford. All rights reserved.
REM You may freely use this script in your own environment, modifying it
REM to meet your needs. But you may not re-publish it without permission.

REM Use netsh to enable remote management through the firewall for the
REM domain profile. This is the minimum to allow using remote MMCs to work
REM from other computers in the domain.

netsh advfirewall set domainprofile settings remotemanagement enable

REM allow remote administration group
netsh advfirewall firewall set rule group="Remote Administration" new
    enable=yes

REM Allow remote desktop
REM (also works with group="Remote Desktop" instead of name=)
netsh advfirewall firewall set rule name="Remote Desktop (TCP-In)" new
    enable=yes

REM Enable Remote Desktop for Administration, and allow
REM downlevel clients to connect
cscript %windir%\system32\scregedit.wsf /AR 0
cscript %windir%\system32\scregedit.wsf /CS 0

REM Now, run the activation script
REM No output means it worked
Slmgr.vbs -ato
```

Setting Desktop Display Resolution

To set the display resolution for the Server Core desktop, you need to manually edit the registry. We'd give you a script to do it, but it is dependent on correctly identifying the specific GUID for your display adapter. Not something we want to automate. So, to change the resolution on your Server Core desktop, follow these steps:

1. Open **regedit**.
2. Navigate to **HKLM\System\CurrentControlSet\Control\Video**.
3. One or more GUIDs is listed under Video. Select the one that corresponds to your video card. Hint: They each have a device description under the 0000 key that can sometimes help.
4. Under the GUID for your video card select the 0000 key, and add a DWORD **DefaultSettings.XResolution**. Edit the value to the X axis resolution you want. For a width of 1024 pixels, use 400 hexadecimal, as shown in Figure 9-3.

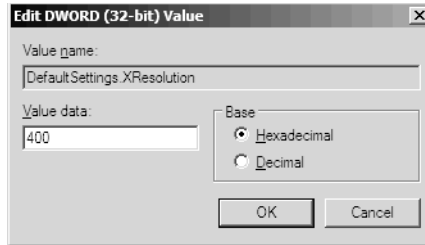


Figure 9-3 Editing the display resolution value for the X axis

5. Add a DWORD DefaultSettings.YResolution. For height of 768 pixels, use 300 hexadecimal.

Note In some cases, these keys will already exist. If they do, you can simply change their value as necessary.

6. Exit the registry editor and log off using the following:

```
shutdown /l
```

7. Once you log back on, the new display settings will take effect.

Enabling Remote Management

To allow access to the familiar graphical administration tools, you need to enable them to work through Windows Firewall. This requires another set of **netsh** commands. Use the following steps to enable remote administration and Remote Desktop:

1. From the command prompt, use the **netsh** command to enable remote management:

```
netsh advfirewall set domainprofile settings remotemanagement enable
```

2. Now, enable the Remote Administration group of firewall rules.

```
netsh advfirewall firewall set rule group="Remote Administration" new  
enable=yes
```

3. Finally, life is easier when you can connect using remote desktop, so let's enable that, too:

```
netsh advfirewall firewall set rule name="Remote Desktop (TCP-In)" new  
enable=yes
```

You should now be able to do additional management using familiar graphical tools from another server but connecting to the Server Core computer.

Activating the Server

The final step in basic configuration of the Server Core computer is to activate it. This requires using a Visual Basic script, which is provided. Use the following command:

```
Slmgr.vbs -ato
```

Note All the basic initial setup commands for Server Core are included in the three scripts described in the Under The Hood sidebar, and are also available on the CD that comes with the book.

Installing Roles

Windows Server 2008 Core doesn't support all the possible roles and features of the full graphical Windows Server, but it does support the most important infrastructure roles. We think one of the most compelling scenarios for Server Core is as a remote site server to enable basic functionality at a remote site where there isn't anyone on site to administer it. By combining the DHCP Server, DNS Server, File Services, and Print Services roles with a read-only Active Directory Domain Services role, you have a "branch office in a box" solution—just add a remote access device such as a VPN router and you're in business.

The File Services role is added by default as part of the base Server Core installation, but you can add additional role services to support additional functionality.

The command used to install a role in Server Core is `Ocsetup.exe`. The exact same command is used to uninstall a role, but with the `/uninstall` command-line parameter. The full syntax for **Ocsetup** is:

```
Ocsetup </?|/h|/help>  
Ocsetup <component> [/uninstall][/passive][/unattendfile:<file>] [/quiet]  
          [/log:<file>][/norestart][/x:<parameters>]
```

The important thing to remember about **Ocsetup** is that it is quite unforgiving. It is case-sensitive, and even a slight mistake in the case of the component name will cause the command to fail.

A script to install the roles for this solution, except the domain controller role, would look like this:

```
@REM filename: SetupBranch.cmd  
@REM  
@REM Setup file to install roles for a branch office server  
@REM  
@REM Created: 5 September, 2007  
@REM ModHist:  
@REM
```

```
@REM Copyright 2007 Charlie Russel and Sharon Crawford. All rights reserved
@REM You may freely use this script in your own environment,
@REM modifying it to meet your needs.
@REM But you may not re-publish it without permission.

@REM Using "start /w" with ocsetup forces ocsetup to wait until it
@REM completes before
going on to the next task.

@REM Install DNS and DHCP
@echo Installing DNS and DHCP roles...
start /w ocsetup DNS-Server-Core-Role
start /w ocsetup DHCP-Server-Core

@REM Now, install File Role Services
@echo Now installing File Role Services...
start /w ocsetup FRS-Infrastructure
start /w ocsetup DFSN-Server
start /w ocsetup DFSR-Infrastructure-ServerEdition

@REM Uncomment these two lines to add NFS support
@REM start /w ocsetup ServerForNFS-Base

@REM start /w ocsetup ClientForNFS-Base

@REM Install Print Server Role

@echo Installing Print Server Role
start /w ocsetup Printing-Server-Core-Role

@REM Uncomment next for LPD support
@REM start /w ocsetup Printing-LPD-PrintService
```

Note You can't include the **DCPromo** command in the script above because installing the Print Server role requires a reboot, which locks out **DCPromo**.

You cannot use **DCPromo** interactively to create a domain controller—you must create an `unattend.txt` file to use with it. The basic minimum `unattend.txt` file is:

```
[DCInstall]
InstallDNS = Yes
ConfirmGC = yes
CriticalReplicationOnly = No
RebootOnCompletion = No
ReplicationSourceDC = hp350-dc-02.example.local
ParentDomainDNSName = example.local
ReplicaOrNewDomain = ReadOnlyReplica
ReplicaDomainDNSName = example.local
```

```

SiteName=Default-First-Site-Name
SafeModeAdminPassword = <passwd> UserDomain = example
UserName = Administrator
Password = <passwd>

```

Important The passwords fields must be correct, and will be automatically stripped from the file for security reasons. For Server Core, you must specify a *ReplicationSourceDC* value. You should set *ReplicaOrNewDomain* to the value shown here—*ReadOnlyReplica*—to create a read-only domain controller.

To install the read-only Domain Controller role, follow these steps:

1. Use Notepad or your favorite ASCII text editor (we use GVim, which works quite well in Server Core) to create an unattend.txt file with the necessary settings for the domain you will be joining. The specific filename of the unattend file is not important because you specify it on the command line.
2. Change to the directory that contains the unattend file. If the server has any pending restarts, you *must* complete them before promoting the server to domain controller.
3. Run DCPromo with the following syntax:
`Dcpromo /unattend:<unattendfilename>`
4. If there are no errors in the unattend file, DCPromo will proceed and promote the server to be a read-only domain controller, as shown in Figure 9-4.

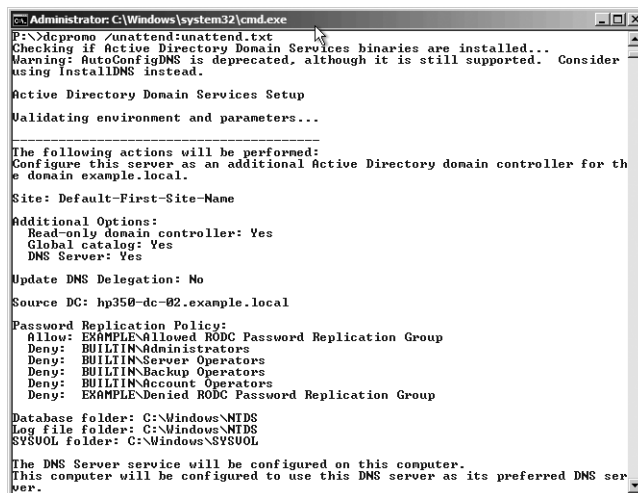


Figure 9-4 Use DCPromo to create a read-only domain controller with an unattend file.

Listing Roles

The `Oclist.exe` command provides a complete list of the available Server Core roles, role services, and features, as well as their current state. Use `Oclist` to get the exact, case-sensitive list of the features and roles you want to install.

Managing a Server Core Computer

Managing a Server Core computer is a different experience for most system administrators. None of the graphical tools you're used to using is available *on the server*. But once you've configured the Server Core computer for remote management, as described under "Initial Configuration" earlier in the chapter, you can create management consoles that point to the Server Core computer, which allow you to do all your tasks from a graphical console.

More Info For details on how to create custom MMCs, see Chapter 14, "Managing Daily Operations."

There are four basic ways to manage a Server Core installation. They are:

1. Locally using a command prompt.
2. Remotely using Remote Desktop. The shell in Remote Desktop will have only the same functionality (a command prompt) as being logged on locally.
3. Remotely using Windows Remote Shell.
4. Remotely using an MMC snap-in from a computer running Windows Vista or Windows Server 2008.

Some tasks are a bit tricky in Server Core—we're used to usually doing them exclusively from the GUI. An obvious task is changing the password on your account. For that, use the `net user <username> *` command. Some of the tasks that can be a problem, and their solutions, are shown in Table 9-2.

Table 9-2 Common Task Workarounds in Server Core

Task	Solution/Workaround
Enable automatic updates	Cscript %windir%\system32\scregedit.wsf /AU [value] Where values are: 1 – disable automatic updates 4 – enable automatic updates /v – view current setting

Table 9-2 Common Task Workarounds in Server Core

Task	Solution/Workaround
Enable Remote Desktop for Administrators	Cscript %windir%\system32\scregedit.wsf /AR [value] Where values are: 0 – enable Remote Desktop 1 – disable Remote Desktop /v – view current setting
Enable Terminal Server clients from Windows versions prior to Windows Vista	Cscript %windir%\system32\scregedit.wsf /CS [value] Where values are: 0 – enable prior versions 1 – disable prior versions /v – view current setting
Allow IPSec Monitor remote management	Cscript %windir%\system32\scregedit.wsf /IM [value] Where values are: 0 – disable remote management 1 – enable remote management /v – view current setting
Configure DNS SRV record weight and priority	Cscript %windir%\system32\scregedit.wsf /DP [value] Where DNS SRV priority values are: 0-65535. (Recommended value = 200) /v – view current setting Cscript %windir%\system32\scregedit.wsf /DW [value] Where DNS SRV weight values are: 0-65535. (Recommended value = 50) /v – view current setting
Update User passwords	Net user <username> [/domain] *
Installing .msi files	Use the /q or /qb switches from the command line with the full .msi filename. /q is quiet; /qb is quiet but with a basic user interface
Changing the time zone, date, or time	timedate.cpl
Change internationalization settings	intl.cpl
Using Disk Management console	From the command line of the Server Core installation: Net start VDS Then run Disk Management remotely.
Get Windows version information	Winver is not available. Use systeminfo.exe instead.
Get Help (regular Windows Help and Support files are not viewable in Server Core)	Cscript %windir%\system32\scregedit.wsf /cli

Using Windows Remote Shell

You can use Windows Remote Shell to remotely execute commands on a Server Core computer. But before you can run Windows Remote Shell, you need to first enable it on the target Server Core computer. To enable Windows Remote Shell, use the following command:

```
winrm quickconfig
```

To run a command remotely, use the `WinRS` command from another computer using the following command:

```
winrs -r:<ServerName> <command string to execute>
```

Using Terminal Server RemoteApp

One neat trick that we like is to use the new TS RemoteApp functionality of Windows Server 2008 to publish a Command Prompt window for the Server Core computer directly onto our desktop. This is simpler and more direct, and saves screen real estate, which is always a benefit. To create an RDP package that you can put on your desktop, follow these steps:

1. On a Windows Server 2008 server that has the Terminal Services role enabled, open the TS RemoteApp Manager, as shown in Figure 9-5.

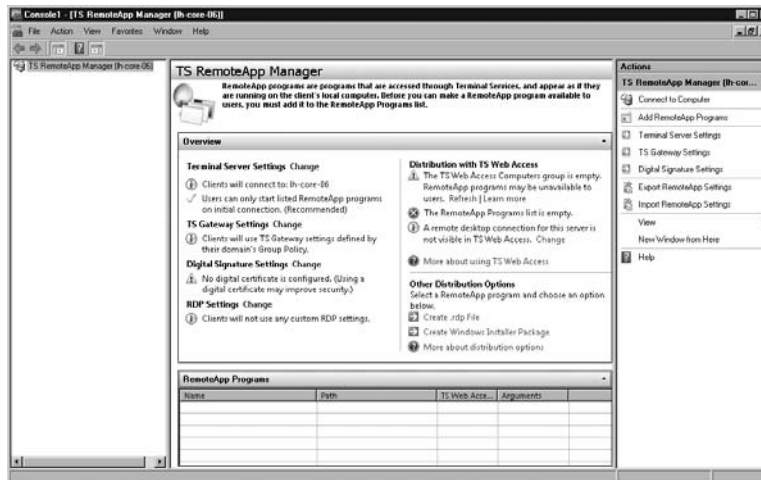


Figure 9-5 Use the TS RemoteApp Manager to create a remote cmd.exe window.

2. Connect to the Server Core computer you want to build an RDP package for.

3. Click Add RemoteApp Programs in the actions pane to open the RemoteApp Wizard.
4. Click Next to open the Choose Programs To Add To The RemoteApp Programs List page, shown in Figure 9-6.

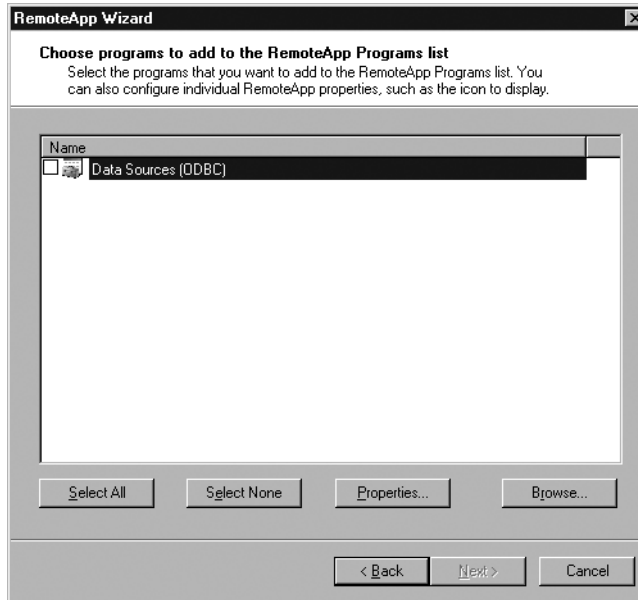


Figure 9-6 The Choose Programs To Add To The RemoteApp Programs List page of the RemoteApp Wizard

5. Click Browse, and navigate to \\<ServerName>\c\$\windows\system32\cmd.exe. Click Open.
6. Click Next and then click Finish to add the remote program and return to the TS RemoteApp Manager.
7. Select cmd.exe in the RemoteApp programs pane and click Create .rdp File in the actions pane.
8. Click Next, and specify any additional package settings for the RDP package. Note the location where the package will be saved.
9. Click Next twice and then click Finish to create the RDP package.
10. Copy the package to the computer where you will use it.

Now you can open a Command Prompt window directly onto the Server Core computer simply by double-clicking the RDP package you created and saved.

Summary

In this chapter we've covered some basic steps for setting up and configuring the new Server Core installation option of Windows Server 2008. We think this is an exciting new way to get the power of Windows Server while maintaining very high levels of security and ease of management. And yes, we know that sounds a bit like marketing hype, but we actually think that Server Core is an important step forward.

In the next chapter, we'll cover managing and configuring your printers using the Printer Management console.

Chapter 19

Implementing Disk Management

Understanding Disk Terminology	616
Overview of Disk Management	619
Partitions and Volumes	625
Setting Disk Quotas	641
Enabling File Encryption	647
Summary	649

Servers are used for many functions and have many reasons for existence, but the single most pervasive function of most servers is storage. And you can't store anything if you don't have something to store it on. For servers, that something is primarily hard disks. Rather than cover all topics related to storage in a single chapter, we've split it up a bit. Both for reasons of length (our editors have this irrational fear of 100+ pages chapters) and also to group topics together rationally.

In this chapter, we'll start by defining some terms that we'll use throughout our discussions of storage. Once we've got that basic ground covered, we'll move on to the physical aspects of storage—the disk subsystem and how you manage and administer it. This includes disks, partitions, and volumes, along with logical drives. And we'll cover special features of the NTFS file system, including encryption and quotas. Throughout this chapter, we'll cover both the graphical way to do things and the command-line way.

In Chapter 20, “Managing Storage,” we'll shift gears and talk about storage from a logical perspective, with full coverage of the Storage Resource Manager, and we'll also cover Storage Area Networks (SANs)—a way to centralize and abstract storage for a group of servers.

The hard disk management functions of Windows Server 2008 build on earlier versions of Windows Server to make hard disk management flexible and easy for administrators while hiding the complexities from end users. One important—and long overdue—new feature is the ability to grow or shrink partitions dynamically without losing data.

Understanding Disk Terminology

Before going into the details of managing disks and storage, let's review some definitions:

- **Physical drive** The actual hard disk itself, including the case, electronics, platters, and all that stuff. This is not terribly important to the disk administrator.
- **Partition** A portion of the hard disk. In many cases, this is the entire hard disk space, but it needn't be.
- **Allocation unit** The smallest unit of managed disk space on a hard disk or logical volume. It's also called a *cluster*.
- **Primary partition** A portion of the hard disk that's been marked as a potentially bootable logical drive by an operating system. MS-DOS can support only a single primary partition, but Windows Server 2008 can support multiple ones. There can be only four primary partitions on any hard disk.
- **Extended partition** A nonbootable portion of the hard disk that can be subdivided into logical drives. There can be only a single extended partition per hard disk, but it can be divided into multiple logical drives.
- **Extended volume** Similar to, and sometimes synonymous with, a spanned volume. This is any dynamic volume that has been extended to make it larger than its original size. When an extended volume uses portions of more than one physical disk, it is more properly referred to as a *spanned volume*.
- **Logical drive** A section or partition of a hard disk that acts as a single unit. An extended partition can be divided, for example, into multiple logical drives.
- **Logical volume** Another name for a logical drive.
- **Basic disk** A traditional disk drive that is divided into one or more partitions, with a logical drive in the primary partition, if present, and one or more logical drives in any extended partitions. Basic disks do not support the more advanced functions of Disk Management, but they can be converted to dynamic disks in many cases.
- **Dynamic disk** A managed hard disk that can be used to create various volumes.
- **Volume** A unit of disk space composed of one or more sections of one or more disks. Prior versions of Windows Server used volume only when referring to dynamic disks, but Windows Server 2008 uses it to mean partitions as well.
- **Simple volume** Used interchangeably with partition in Windows Server 2008, earlier versions of Windows used simple volume only when referring to a dynamic disk. A portion of a single disk, a simple volume can be assigned either a single drive letter or no drive letter and can be attached (mounted) on zero or more mount points.

- **RAID (redundant array of independent [formerly “inexpensive”] disks)** The use of multiple hard disks in an array to provide for larger volume size, fault tolerance, and increased performance. RAID comes in different levels, such as RAID-0, RAID-1, RAID-5, and so forth. Higher numbers don’t necessarily indicate greater performance or fault tolerance, just different methods of doing the job.
- **Spanned volume** A collection of portions of hard disks combined into a single addressable unit. A spanned volume is formatted like a single drive and can have a drive letter assigned to it, but it will span multiple physical drives. A spanned volume—occasionally referred to as an *extended volume*—provides no fault tolerance and increases your exposure to failure, but does permit you to make more efficient use of the available hard disk space.
- **Striped volume** Like a spanned volume, a striped volume combines multiple hard disk portions into a single entity. A striped volume uses special formatting to write to each of the portions equally in a stripe to increase performance. A striped volume provides no fault tolerance and actually increases your exposure to failure, but it is faster than either a spanned volume or a single drive. A stripe set is often referred to as *RAID-0*, although this is a misnomer because plain striping includes no redundancy.
- **Mirror volume** A pair of dynamic volumes that contain identical data and appear to the world as a single entity. Disk mirroring can use two drives on the same hard disk controller or use separate controllers, in which case it is sometimes referred to as *duplexing*. In case of failure on the part of either drive, the other hard disk can be split off so that it continues to provide complete access to the data stored on the drive, providing a high degree of fault tolerance. This technique is called *RAID-1*.
- **RAID-5 volume** Like a striped volume, a RAID-5 volume combines portions of multiple hard disks into a single entity with data written across all portions equally. However, it also writes parity information for each stripe onto a different portion, providing the ability to recover in the case of a single drive failure. A RAID-5 volume provides excellent throughput for read operations, but it is substantially slower than all other available options for write operations.
- **SLED (single large expensive disk)** Now rarely used, this strategy is the opposite of the RAID strategy. Rather than using several inexpensive hard disks and providing fault tolerance through redundancy, you buy the best hard disk you can and bet your entire network on it. If this doesn’t sound like a good idea to you, you’re right. It’s not.
- **JBOD** Just a bunch of disks. The hardware equivalent of a spanned volume, this has all the failings of any spanning scheme. The failure of any one disk will result in catastrophic data failure.

More Info Additional RAID levels are supported by many hardware manufacturers of RAID controllers. These include RAID 0+1, RAID 10, RAID 6, and RAID 50. For more details on various RAID levels, see the manufacturer of your RAID controller or http://en.wikipedia.org/wiki/RAID#Standard_RAID_levels.



Real World Disk Technologies for the Server

The first time we wrote a chapter about disk management, basically three possible technologies were available: Modified Field Modification (MFM), Pulse Frequency Modulation (PFM), and Small Computer System (or Serial) Interface (SCSI). Unless you were a total geek (and had oodles of money), your systems used either MFM or PFM, and RAID wasn't even an option. Over time, SCSI became the only real choice for the vast majority of servers and even became mainstream on high-end workstations. Servers at the high end might use fiber, but SCSI had the vast majority of the server disk market. SCSI has changed over the years to support faster speeds, more disks, and greater ease of configuration and use, but is finally reaching its limits as a parallel interface.

Integrated Device Electronics (IDE), later called Advanced Technology Attachment (ATA), became the standard on the personal computer. However, IDE never made a serious inroad into the server market because, while fast for single tasks, it lacked the inherent multitasking support and bus mastering that a server disk interface technology required, and no real hardware RAID solutions supported it.

Recently, the introduction of Serial ATA (SATA) technology has made serious inroads into the lower end of the server marketplace. With SATA RAID controllers built into many motherboards, and stand-alone SATA RAID boards that support 8 or more SATA drives and have substantial battery-backed RAM cache onboard, many low- to mid-range servers are finding that SATA RAID solutions provide a cost-effective alternative to SCSI. While most SATA RAID controllers lack the ability to hot-swap a failed drive, and don't have the performance potential of SCSI or Serially Attached SCSI (SAS), they are still quite attractive alternatives where cost is a primary factor. SATA also makes sense as secondary or "near-line" storage for a server.

The new kid on the block, however, is SAS. This is the most interesting addition to the server storage equation in quite a while. Using the same thin cables and connectors as SATA, with none of the configuration nuisance of traditional SCSI, SAS is definitely the way to go. When combined with new 2.5-inch drives, the ability to put a really large amount of very fast storage in a small space has taken a significant

step forward. SAS drives interoperate with SATA drives to combine the two technologies on the same controller. SAS disk controllers can control SATA drives as well, though the reverse is not true.

With the main bottleneck for servers continuing to be I/O in general, and especially disk I/O, there will continue to be pressure to find new and faster methods to access disk-based storage. SAS, combined with 2.5-inch drives, enables fast and flexible storage arrays in remarkably smaller spaces. Because 64-bit servers are the only real option, and because of the enormous datasets supported on 64-bit Windows Server 2008, the need for fast and easily expandable disk storage keeps increasing. Windows virtualization technology and the move to greater virtualization in the data center also drive the need for faster disk and I/O subsystems.

Overview of Disk Management

While solid state and hybrid disks are starting to find their way into laptops and even some desktops, conventional hard disk storage continues to be the long-term storage method of choice for modern computers, from the mainframe to the desktop. In Windows Server 2008, you must first initialize this conventional hard disk storage and organize it into volumes, drives, and partitions before you can use it.

Under the Hood RAID

RAID (redundant array of independent disks) is a term used to describe a technique that has gone from an esoteric high-end solution to a normal procedure on most servers. Fifteen years ago, RAID was mostly unheard of, although the original paper defining RAID was written in 1988. In the past, most server systems relied on expensive, higher-quality hard disks—backed up frequently. Backups are still crucial, but now you can use one form or another of RAID to provide substantial protection from hard disk failure. Moreover, this protection costs much less than those big server drives did.

You can implement RAID at a software or hardware level. When implemented at the hardware level, the hardware vendor provides an interface to administer the arrays and the drivers to support the various operating systems it might need to work with. Processing for the RAID array is handled by a separate processor built into the RAID controller, offloading the work from the computer's CPU. Additionally, many hardware RAID controllers include a substantial dedicated RAM cache, often with

a battery backup. The combination of a separate, dedicated processor and a separate, dedicated cache provides a substantial performance advantage over software RAID. Additionally, most server-class hardware RAID controllers offer additional RAID levels when compared to software RAID, providing redundancy advantages such as multiple disk failure protection. Hardware RAID is generally substantially more expensive than the software RAID built into Windows Server 2008, though many manufacturers today include basic hardware RAID capabilities on the motherboard.

Windows Server 2008 includes an excellent and flexible implementation of RAID levels 0, 1, and 5 in software. It doesn't cover all the possibilities by any means, but it is certainly sufficient for some purposes. However, most serious servers should be using hardware RAID.

The primary GUI for managing disks in Windows Server 2008 is the Disk Management console, Diskmgmt.msc, shown in Figure 19-1, which can be run stand-alone or as part of Server Manager. The primary command-line tool for managing disks is DiskPart.exe.

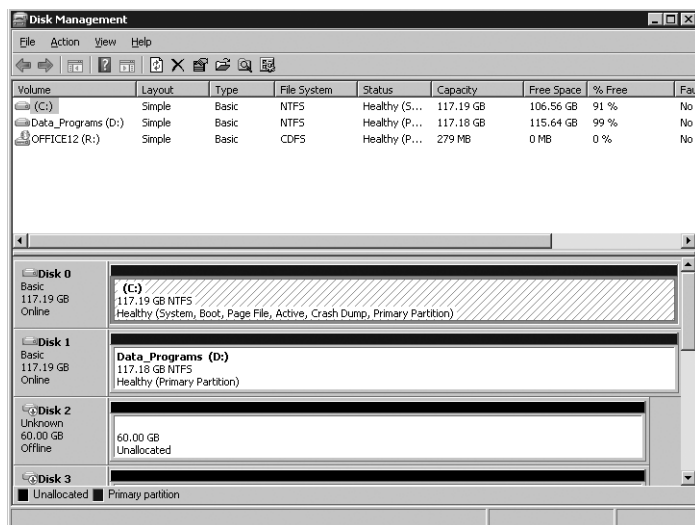


Figure 19-1 The Disk Management console

To open Disk Management, you can start it stand-alone by running Diskmgmt.msc from a command line, or by typing it into the Run dialog box on the Start menu. Disk Management is also part of the Server Manager console, in the Storage section, as shown in Figure 19-2.

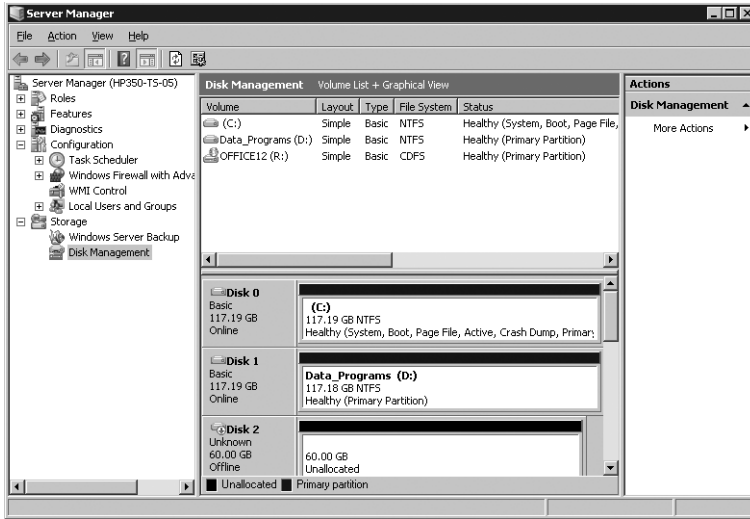


Figure 19-2 The Server Manager console



Real World Hardware RAID

Although Disk Management provides an adequate software RAID solution, hardware RAID is widely available, from either the original server vendor or from third parties, and it provides substantial advantages over software RAID. Hardware RAID solutions range from a simple, motherboard-integrated RAID controller to fully integrated, stand-alone subsystems. Features and cost vary, but all claim to provide superior performance and reliability over a simple software RAID solution such as that included in Windows Server 2008. In general, they do, with the notable exception of some basic motherboard-integrated solutions offered on consumer-level motherboards for SATA drives. Even if circumstances force you to use what is an essentially desktop system, avoid using the built-in RAID on the motherboard, except as a simple SATA controller. Acceptable, uncached, stand-alone RAID controllers are reasonably priced and will provide far better performance and reliability. If your budget is so limited that even that is too much, use Windows Server 2008's built-in software RAID.

Some advantages that a good hardware RAID controller offers can include the following:

- Hot-swap and hot-spare drives, allowing for virtually instantaneous replacement of failed drives
- Integrated disk caching for improved disk performance

- A separate, dedicated system that handles all processing, for improved overall performance
- Increased flexibility and additional RAID levels, such as RAID 1+0 or RAID 0+1, combinations of striping (RAID-0) and mirroring (RAID-1) that provide for fast read and write disk access with full redundancy

Not all stand-alone hardware RAID systems provide all these features, but all have the potential to improve the overall reliability and performance of your hard disk subsystem. They belong on any server that isn't completely fungible.

Remote Management

The Disk Management console in Windows Server 2008 lets you manage not only the local hard disks but also drives on other computers running any version of Windows 2000, Windows XP, Windows Server 2003, Windows Vista, or Windows Server 2008, allowing an administrator to manage disk tasks and space allocations from a workstation without having to sit at the computer that is being administered. This capability is a boon for remote site management and also simplifies management of Windows Server 2008 Core.

For details on how to create custom management consoles that connect to remote computers, see Chapter 14, “Managing Daily Operations.”

Dynamic Disks

Dynamic disks were introduced in Windows 2000 Server. By converting a disk to a dynamic disk, you give Disk Management the ability to manage it in new ways, *without requiring a reboot* in most cases. You can extend a disk volume, span a volume across multiple physical disks, stripe the volume for improved performance, mirror it, or add it to a RAID-5 array—all from the Disk Management console and all without a reboot, after the disk is converted to a dynamic disk. When combined with the new remote management functionality, dynamic disks give the system administrator powerful tools for managing the type and configuration of hard disk storage across the enterprise.



Real World Dynamic versus Basic Disks

We used to be big fans of dynamic disks. They provided increased flexibility and functionality in a way that was pretty transparent. And they were a huge step forward when they were introduced in Windows 2000. At the time, RAID controllers were both more expensive and less functional, and many servers didn't have hardware RAID on them. That's simply not the case anymore.

If using dynamic disks increases your options, isn't that a good thing? Well, yes. But. And it's a big but. A dynamic disk complicates the disaster recovery process, and we dislike anything that creates potential issues in a disaster recovery scenario. We definitely don't think dynamic disks are appropriate for a system disk. And we just have a hard time seeing where the upside is given the functionality that your RAID controller or SAN array management application provides.

If you do find a need that can't be solved any other way, then by all means use dynamic disks. There's no apparent performance cost, and you use the same tools to manage both dynamic disks in Windows Server 2008 and basic disks. But avoid converting your system disk to dynamic. And make sure your disaster recovery procedures are updated appropriately.

Command Line

Windows Server 2008 includes a full command-line interface for disks. The primary command-line tool is DiskPart.exe. This command-line utility is scriptable or it can be used interactively. Additional functionality is available using Fsutil.exe and Mountvol.exe. As we go through the steps to manage disks in this chapter, we'll provide the equivalent command lines and a few basic scripts that you can use as the starting point for building your own command-line tools.

The one task that doesn't appear to have a command-line solution is initializing a new disk. As far as we've been able to tell, you need to use Disk Management to initialize new disks before they can be used.

Adding a New Disk

Adding a new disk to a Windows Server 2008 server is straightforward. First, obviously, you need to physically install and connect the drive. If you have a hot-swappable backplane and array, you don't even have to shut the system down to accomplish this task. If you're using conventional drives, however, you need to shut down and power off the system.

After you install the drive and power up the system again, Windows Server 2008 automatically recognizes the new hardware and makes it available. If the disk is a basic disk that is already partitioned and formatted, you can use it without initializing, but it will initially appear "offline" in Disk Management. If it's a brand-new disk that has never been partitioned or formatted, you need to initialize it first. And if it's a dynamic disk or disks, but from another computer, you need to import it before it's available. If the disk has never been used before, you're prompted by the Initialize And Convert Disk Wizard.

Note If you're adding a drive to your server that uses a different technology than existing drives, or simply a different controller, it might require a new driver before the system recognizes the disk.

Setting a Disk Online

To set an offline disk to online, follow these steps:

- 1. Open Disk Management.
- 2. Right-click the disk you want to bring online, and select Online from the Action menu, as shown in Figure 9-3.

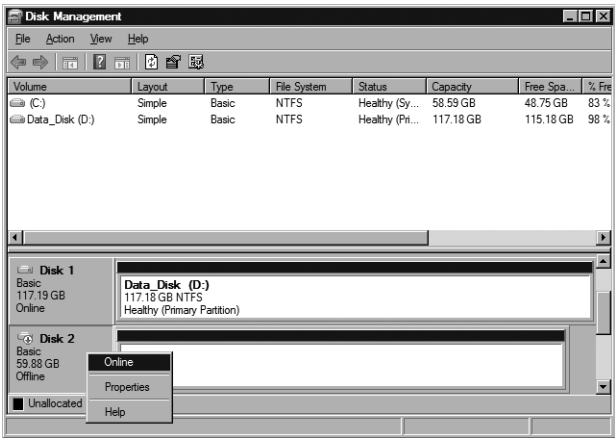


Figure 19-3 Bringing a disk online using Disk Management
The command-line equivalent is shown in Figure 19-4.

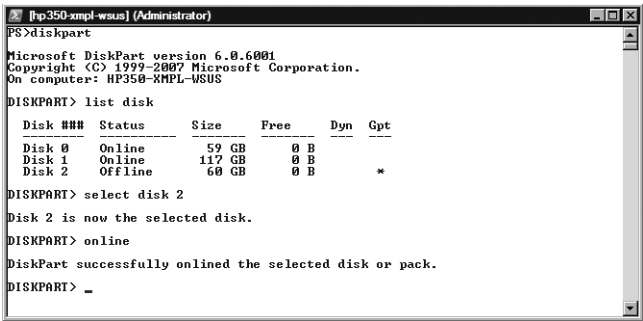


Figure 19-4 Bringing a disk online using the command line

Initializing a New Disk

When you install a brand-new disk that has never been formatted or used by Windows, you need to initialize it. It might initially be shown as offline. If so, you need to first set the disk online, and then initialize it. If the new disk is online, the Initialize Disk dialog box will automatically display when you start Disk Management, as shown in Figure 19-5.

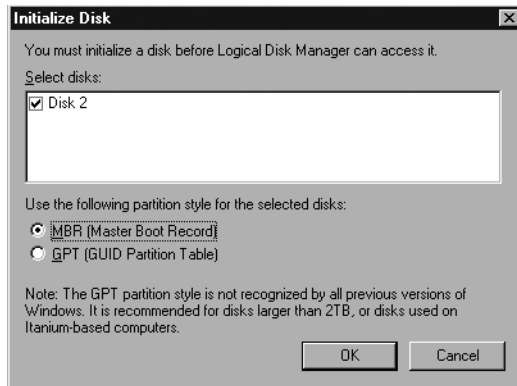


Figure 19-5 The Initialize Disk dialog box

When you initialize the disk, you can choose whether to use Master Boot Record (MBR) or GUID Partition Table (GPT) as the partition style. For any disk larger than 2TB, GPT is recommended. We're still using MBR for all our disks, except for the one huge SAN volume we have, but we're leaning toward changing that for all new disks.

Partitions and Volumes

In Windows Server 2008 the distinction between volumes and partitions is somewhat murky. When using Disk Management, a regular partition on a basic disk is called a *simple volume*, even though technically a simple volume requires that the disk be a dynamic disk.

As long as you use only simple volumes or partitions, you can easily convert between a basic disk (and partition) and a dynamic disk (and a volume). Once you use a feature that is supported only on dynamic disks, however, changing back to a basic disk will mean data loss. Any operation that would require conversion to a dynamic disk will give you fair warning, as shown in Figure 19-6.

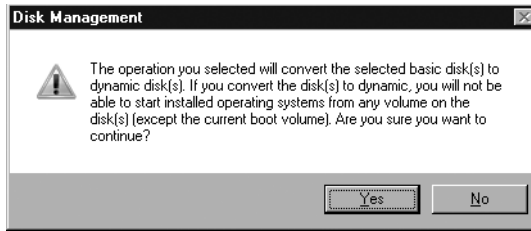


Figure 19-6 Disk Management will warn you before any operation that would cause a conversion to dynamic disks.

When using Disk Management, the conversion to dynamic disks as required happens automatically. When using DiskPart, however, you need to explicitly specify each step of the process.

Creating a Volume or Partition

You can create a new volume or partition on any disk that has empty space. If the disk is dynamic, a volume is created. If the disk is a basic disk, a primary partition is created. If the empty space is part of an extended partition, a new logical drive will be created. All of them called a simple volume, but each one a different structure.

Note You can no longer create an extended partition in Disk Manager. If you need to create an extended partition, you need to use DiskPart.exe. But there's really no longer any need for extended partitions.

To create a new volume or partition, follow these steps:

1. In Disk Management, right-click the unallocated disk and select the type of volume to create, as shown in Figure 19-7. Click Next.



Figure 19-7 Creating a volume

Depending on the number of available unallocated volumes, you see one or more options for the type of volume, including the following:

- ☐ New Simple Volume
- ☐ New Spanned Volume
- ☐ New Striped Volume

- ☐ New Mirrored Volume
 - ☐ New RAID-5 Volume
2. Select the type you want to create. The New Volume Wizard for that specific type of volume will open. Figure 19-8 shows the New RAID-5 Volume Wizard.

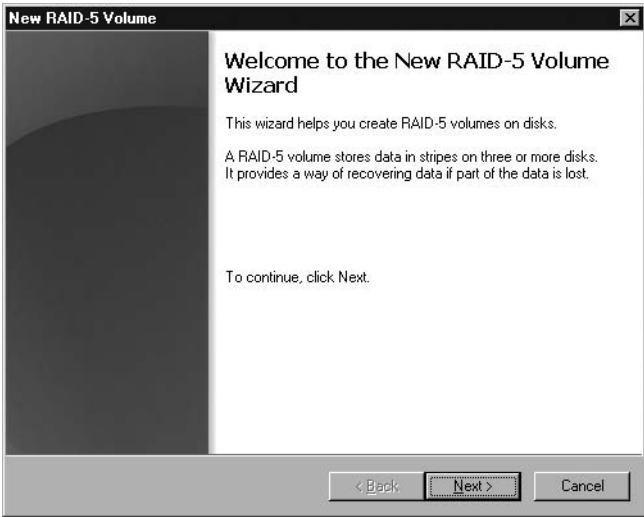


Figure 19-8 The New RAID-5 Volume Wizard

3. Select the disks to use for the new volume. The choices available and the selections you need to make depend on the type of volume you're creating and the number of available unallocated disks. Figure 19-9 shows a RAID-5 volume being created.

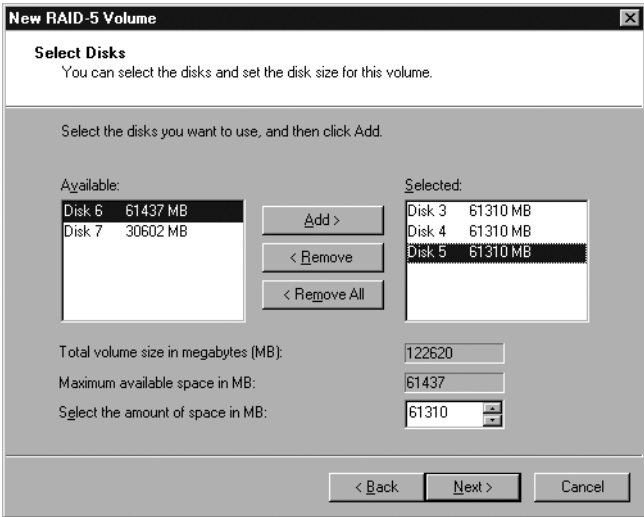


Figure 19-9 Select the disks that will be part of this volume.

4. On the same page, adjust the size of the new volume. By default, the new volume will use the maximum available space from each of the selected disks. For spanned volumes, this will be the sum of the free space on the selected disks; for other types of volumes, it will be the number of disks multiplied by the available space on the smallest of the selected disks. Click Next.
5. Select either a drive letter or a mount point for the new volume, as shown in Figure 19-10, or opt not to assign a drive letter or path at this time. With Windows Server 2008, you can “mount” a volume on an empty subdirectory, minimizing the number of drive letters and reducing the complexity of the storage that is displayed to the user. If you want to take advantage of this feature, click Browse to locate the directory where you will mount the new volume. Click Next. (See the Real World sidebar “Mounted Volumes” for more about this subject.)

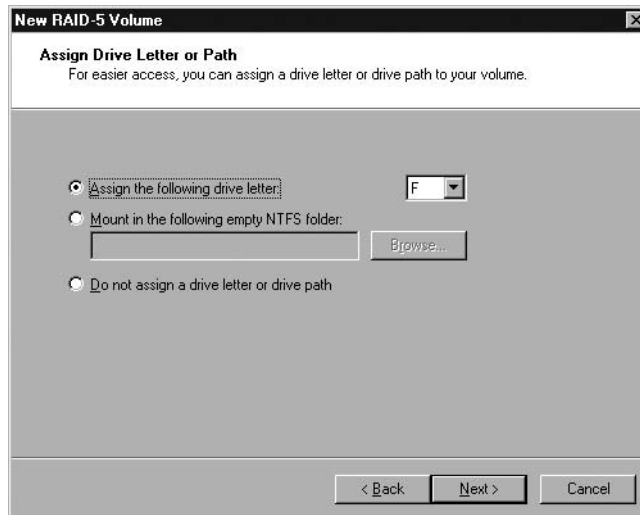


Figure 19-10 Select a drive letter or mount point for the new volume.

6. Select the formatting options you want (shown in Figure 19-11). Even when mounting the volume rather than creating a new drive, you can choose your format type without regard to the underlying format of the mount point. Click Next.

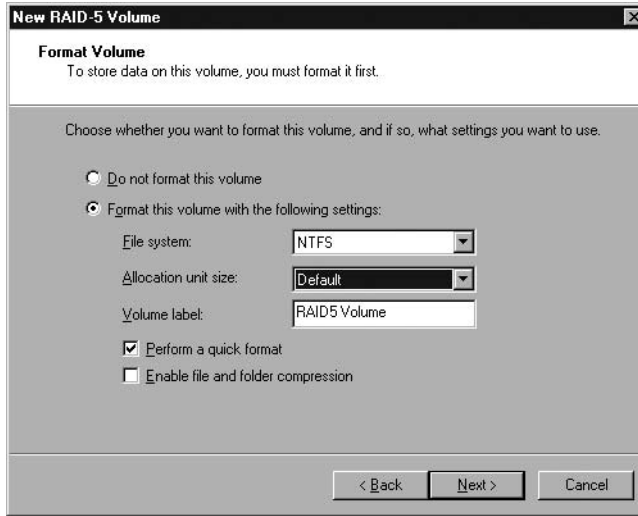


Figure 19-11 Set the formatting options for the new volume.

7. On the confirmation page, if all the options are correct, click Finish to create and format the volume. If the type you've selected requires that the disks be converted to dynamic disks, you'll see a confirmation message from Disk Management, as shown in Figure 19-12.

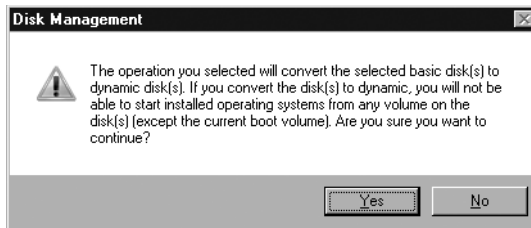


Figure 19-12 Before converting disks to dynamic, you must confirm the change.

8. Once the volume is created, it's displayed in Disk Management, as shown in Figure 19-13.

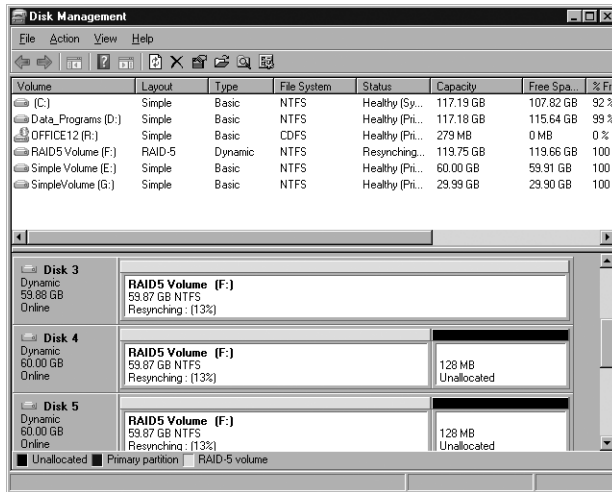


Figure 19-13 The new RAID-5 volume being created

You could use the following script to perform the same RAID-5 volume creation using DiskPart.exe:

```
REM Filename: RAID5Vol.txt
REM
REM This is a DiskPart.exe Script. Run from the command line
REM or from another script, using the syntax:
REM
REM    diskpart /s RAID5Vol.txt > logfile.log
REM
REM to run this script and dump the results out to a log file.
REM
REM This script creates a RAID5 Volume combining disks 3,4 and 5,
REM and then formats it and assigns the next available drive letter to it.

REM First, list out our disks. Not required for scripting, but useful
REM to show the overall environment if we need to troubleshoot problems
list disk

REM Create the volume (No SIZE parameter, so the maximum size for the
REM selected disks will be used.)
create volume RAID disk=3,4,5

REM Format the new volume.
Format fs=NTFS label=ÓRAID 5 VolumeÓ quick

REM Assign without parameters will choose the next available HD letter.
Assign
```



Real World Mounted Volumes

Windows Server 2008 borrows a concept from the UNIX world by adding the ability to mount a volume or partition on a subfolder of an existing drive letter. A mounted volume can also have a drive letter associated with it—although it does not need to—and it can be mounted at more than one point, giving multiple entry points into the same storage.

A volume must be mounted on an empty subfolder of an existing NTFS volume or drive. FAT and FAT32 drives do not support mounted volumes. You can, however, mount a FAT or FAT32 volume at any mount point. (But really, it's time to let go of FAT as a file system for hard disks!) You can mount only a single volume at a given mount point, but you can then mount further volumes on top of an existing mounted volume, with the same rules and restrictions as any other mount. The properties of a drive do not show all the available disk space for that drive, because they do not reflect any volumes mounted on the drive.

You can use mounted volumes to provide a mix of redundant and nonredundant storage in a logical structure that meets the business needs of the enterprise while hiding the complexities of the physical structure from the users. Unfortunately, mounted volumes are not handled correctly by Network File System (NFS) shares and should be avoided in environments where Server for NFS is used.

Creating Extended Partitions and Logical Drives

If you have extended partitions on your disks for some reason, you can create logical drives on the partition using DiskPart.exe. However, you no longer have a graphical way to create an extended partition or a logical drive, nor any real need to do so. With Windows Server 2008 providing full support for GPT disks, the old limit of a maximum of four partitions on a disk is gone—GPT disks in Windows Server 2008 support 128 partitions. If you have any existing MBR disks that include an extended partition, either because you moved a disk from another computer to your Windows Server 2008 computer or because you upgraded to Windows Server 2008 from an earlier version, we suggest you remove the existing extended partition and convert the disk to GPT.

Converting a Disk to a Dynamic Disk

Unlike earlier versions of Windows Server, with Windows Server 2008 you generally have no need to directly convert a disk to a dynamic disk. Operations that require conversion to a dynamic disk will perform the conversion as part of the operation. And delet-

ing a volume that required dynamic disks causes the disks to convert back to basic disks in most cases. There are a few cases where the automatic conversion doesn't happen if you're using DiskPart.exe to manipulate the disk, but all the operations you perform in Disk Management do automatic conversions. For those few situations in DiskPart where explicit conversion is necessary, use the following commands:

```
DISKPART> select disk <n>  
DISKPART> convert BASIC
```

Where <n> is the disk number you want to convert, and where BASIC can be replaced by DYNAMIC depending on which conversion you need to do.

Conversions can only occur when there are no structures on the disk that are not supported in the target disk type.

Converting a Disk to a GPT Disk

One of the important new features of Windows Server 2008 disk management is full support for GPT disks. GPT disk support was initially only available in 64-bit Itanium versions of Windows Server, but with the release of Windows Server 2003 Service Pack 1 and the initial version of x64 Windows Server 2003, GPT support was added for all versions of Windows Server 2003. In Windows Server 2008, this support is fully integrated.

You can convert a disk between MBR and GPT as long as the disk is completely empty. Unfortunately, once you've created any partitions or volumes on the disk, you can no longer convert between the two types.

To convert a disk to GPT, follow these steps:

1. In Disk Management, delete any existing volumes or partitions.

Note Deleting a volume or partition will delete any data on the volume or partition. It will not destroy the data, however, so that it might be possible to recover the data.

2. Right-click the empty disk and select Convert To GPT Disk, as shown in Figure 19-14.

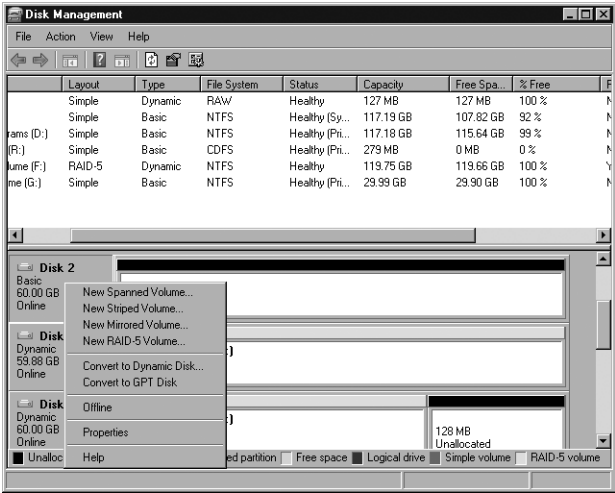


Figure 19-14 Converting from an MBR disk to a GPT disk

- 3. To do the same operation from DiskPart, type the following command:

```
DISKPART> select disk <n>
DISKPART> convert GPT
```

Where <n> is the disk to be converted. That's all there is to it.

Changing the Size of a Volume

Windows Server 2008 allows you to change the size of an existing volume without losing data. You can extend the volume, either by using additional free space on the existing disk, or by spanning onto another disk that has free space. This capability is essentially unchanged from earlier versions of Windows Server. New to Windows Server 2008, however, is the ability to shrink a volume without having to use a third-party product or lose data.

When you extend or shrink a volume, only a simple volume or a spanned volume can be modified: You cannot extend or shrink striped, mirrored, or RAID-5 volumes without deleting the volume and recreating it.

Important Once you extend a volume across multiple disks, you normally cannot shrink it back down onto a single disk without deleting the volume entirely and recreating it. This means you *will* lose data, so consider carefully before you decide to extend a volume across multiple disks.

Extending a Volume

You can add space to a volume without having to back up, reboot, and restore your files if the volume is a simple volume or a spanned volume. To extend a volume, follow these steps:

1. In Disk Management, right-click the volume you want to extend. Choose Extend Volume from the menu to open the Extend Volume Wizard. Click Next.
2. Highlight one or more disks from the list of disks that are available and have unallocated space, as shown in Figure 19-15. Click Add to add the selected disk or disks, and indicate the amount of space you want to add. Click Next.

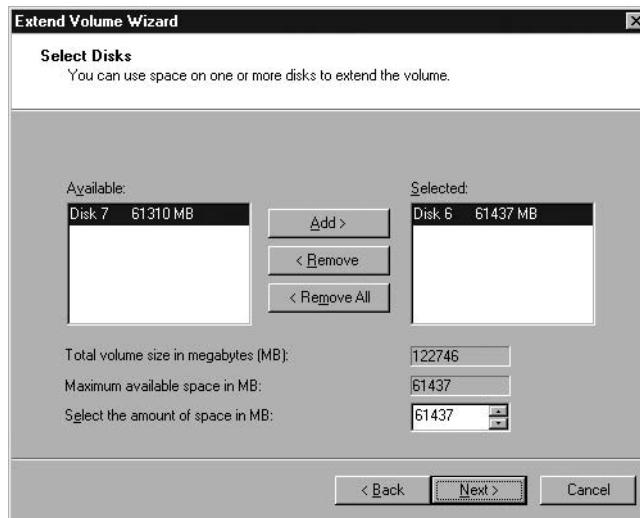


Figure 19-15 Selecting the disks to use to extend the volume

3. The Extend Volume Wizard displays a final confirmation page before extending the volume. Click Finish to extend the volume, or click Cancel if you change your mind. If you need to convert any of the disks to dynamic before extending, you'll get another confirmation prompt.
4. To perform the same steps from the DiskPart command line, use the commands shown in Figure 19-16.

```

[hp350-ts-05] (Administrator)
Copyright (C) 1999-2007 Microsoft Corporation.
On computer: HP350-TS-05

DISKPART> select disk 2
Disk 2 is now the selected disk.
DISKPART> list partition

Partition ###  Type              Size      Offset
-----
Partition 1    Reserved             128 MB      17 KB
Partition 2    Primary              60 GB      129 MB

DISKPART> select partition 2
Partition 2 is now the selected partition.
DISKPART> convert dynamic
DiskPart successfully converted the selected disk to dynamic format.
DISKPART> select disk 6
Disk 6 is now the selected disk.
DISKPART> convert dynamic
DiskPart successfully converted the selected disk to dynamic format.
DISKPART> list volume

Volume ###  Ltr  Label        Fs      Type          Size      Status       Info
-----
Volume 0     G    Stripe      NTFS     Stripe        254 MB    Healthy
Volume 1     F    RAID 5 Uola  NTFS     RAID-5        120 GB    Healthy
Volume 2     D    Data_Progra  NTFS     Partition     117 GB    Healthy
Volume 3     E    OFFICE12     NTFS     Simple         60 GB    Healthy
Volume 4     R    OFFICE12     CDPS     DVD-ROM       280 MB    Healthy
Volume 5     C    OFFICE12     NTFS     Partition     117 GB    Healthy System

DISKPART> select volume 3
Volume 3 is the selected volume.
DISKPART> extend disk=6
DiskPart successfully extended the volume.
DISKPART> _

```

Figure 19-16 Extending a disk using the DiskPart command-line tool

As you can see from the figure, using the command line to extend a volume is quite a few more steps than using Disk Management. Given that we hardly ever extend a volume (see the RealWorld sidebar), it's probably just as well to use Disk Management for this particular task. We're firm believers in using the command line whenever possible, but sometimes it just doesn't make sense.

Note A spanned (extended) volume is actually less reliable than a simple disk. Unlike a mirror or RAID-5 volume, which both have built-in redundancy, a spanned or striped volume will be broken and all data lost if any disk in the volume fails.



Real World Extending—Administrator's Friend or Foe?

Most administrators have wished at some point that they could simply increase the users' home directory space on the fly. Without having to bring the system offline for several hours while the entire volume is backed up and reformatted to add the additional hard disks, the backup is restored, and the share points are re-created. Fun? Hardly. Risky? Certainly. And definitely a job that means coming in on the weekend or staying late at night—in other words, something to be avoided if at all possible.

All this makes Windows Server 2008's ability to create additional space on a volume without the need to back up the volume, reformat the disks, and re-create the volume a seductive feature. However, if you're using conventional hard disks without hardware RAID, you might want to think twice before jumping in. Only spanned or striped volumes allow you to add additional storage on the fly, and, because neither is redundant, using them exposes your users to the risks of a failed drive. Yes, you have a backup, but even under the best of circumstances, you'll lose some data if you need to restore a backup. Further, using spanned volumes actually increases your risk of a hard-disk failure. If any disk used as part of the spanned volume fails, the entire volume is toast and will need to be restored from backup.

Why, then, would anyone use spanning? Because they have hardware RAID to provide the redundancy. This combination offers the best of both worlds—redundancy provided by the hardware RAID controller and flexibility to expand volumes as needed, using Disk Management. Yet another compelling argument for hardware RAID, in case you needed any more.

Shrinking a Volume

While most of the time we're concerned with increasing the size of a volume on the server, there can be occasions when it might be convenient to shrink a volume. For example, if you are using a single large RAID array for multiple volumes, and one of the volumes has empty space while another volume on the same array is running out of space, it would be handy to be able to shrink the volume that has extra space and then extend the one that is running out of room. In the past, the only way you could do this was to back up the volume you wanted to shrink, delete it, extend the volume that needed growing, recreate the volume you deleted, and restore the backup. Possible, certainly. But both risky and highly disruptive to your users. The other alternative was to use a third-party product, such as Acronis Disk Director Server (<http://www.acronis.com/enterprise/products/diskdirector/>).

Now, in Windows Server 2008, you can use Disk Management to shrink a volume without having to delete it and recreate it. While not quite as flexible as products like Acronis Disk Director, this new capability is all that most system administrators will need. To shrink a volume, follow these steps:

1. In Disk Management, right-click the volume you want to shrink. Choose Shrink Volume from the menu to open the Shrink dialog box shown in Figure 19-17.

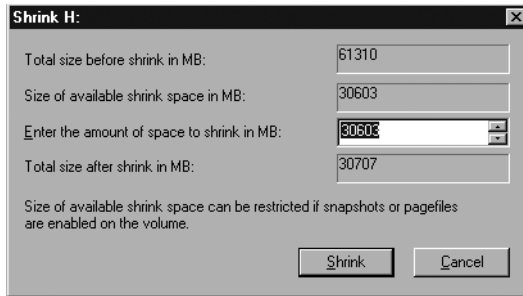


Figure 19-17 Shrinking a volume

2. Select the amount of space to shrink the volume by, and click Shrink.
3. From the command line, the syntax of the DiskPart command is:

```
SHRINK [DESIRED=<N>] [MINIMUM=<N>] [NOWAIT] [NOERR]  
SHRINK QUERYMAX [NOERR]
```

where SHRINK by itself will shrink the selected volume the maximum amount possible.

Note Shrinking a volume is one place where DiskPart is well behaved. If you select a partition on a basic disk and attempt to shrink it, DiskPart doesn't require you to first convert the disk to dynamic before you can shrink the volume.

Adding a Mirror to a Volume

When your data is mission critical and you want to make sure that no matter what happens to one of your hard disks the data is protected and always available, consider mirroring the data onto a second drive. Windows Server 2008 can mirror a dynamic disk onto a second dynamic disk so that the failure of either disk does not result in loss of data. To mirror a volume, you can either select a mirrored volume when you create the volume (as described in the "Creating a Volume or Partition" section earlier in this chapter) or add a mirror to an existing volume. To add a mirror to an existing volume, follow these steps:

1. In the Disk Management console, right-click the volume you want to mirror. If a potential mirror is available, the shortcut menu lists the Add Mirror command, as shown in Figure 19-18.

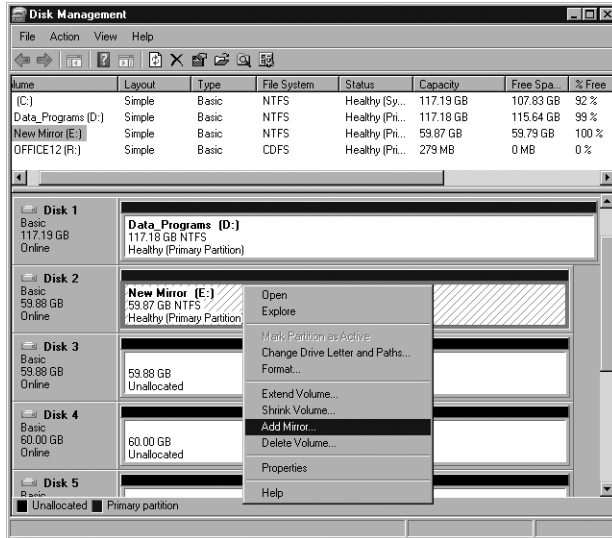


Figure 19-18 The action menu for Disk 2 includes the Add Mirror command

2. Choose Add Mirror to display the Add Mirror dialog box (shown in Figure 19-19), where you can select the disk to be used for the mirror.

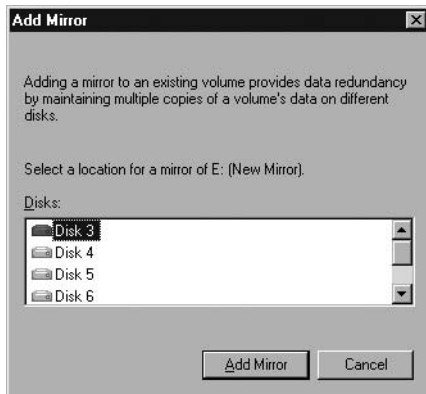


Figure 19-19 The Add Mirror dialog box

3. Highlight the disk that will be the mirror and click Add Mirror. You'll be prompted that this action will convert the disks to dynamic. Click Yes. The mirror is created immediately and starts duplicating the data from the original disk to the second half of the mirror, as shown in Figure 19-20. This process is called *regeneration* or *resynching*. (The process of regeneration is also used to distribute data across the disks when a RAID-5 volume is created.)

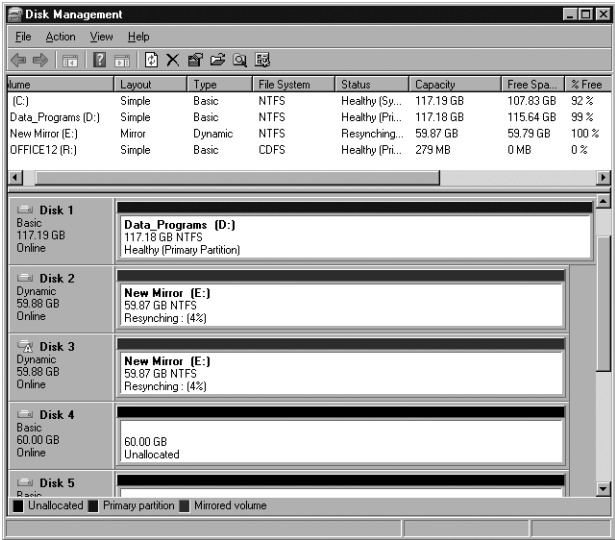


Figure 19-20 A newly created mirrored disk in the process of regeneration

4. Mirroring can also be done from the DiskPart command line. First select the disk and then use the ADD command, which has the following syntax:

ADD DISK=<N> [ALIGN=<N>] [WAIT] [NOERR]

where DISK is the disk that will be added to make the mirror, and ALIGN is used to align with a specific hardware RAID Logical Unit Number (LUN) alignment boundary.

Best Practices Regeneration is both CPU-intensive and disk-intensive. When possible, create mirrors during slack times or during normally scheduled down-time. Balance this goal, however, with the equally important goal of providing redundancy and failure protection as expeditiously as possible.

Best Practices To improve your overall data security and reliability, mirror your volumes onto disks that use separate controllers whenever possible. This process is known as *duplexing*, and it eliminates the disk controller as a single point of failure for the mirror while actually speeding up both reading and writing to the mirror, because the controller and bus are no longer potential bottlenecks.

Drive Failure in a Mirrored Volume

If one of the disks in a mirrored volume fails, you continue to have full access to all your data without loss. If a disk in the mirror set fails, the failed disk is marked missing and offline, and the mirror is unavailable, as shown in Figure 19-21. An alert is sent to the alert log.

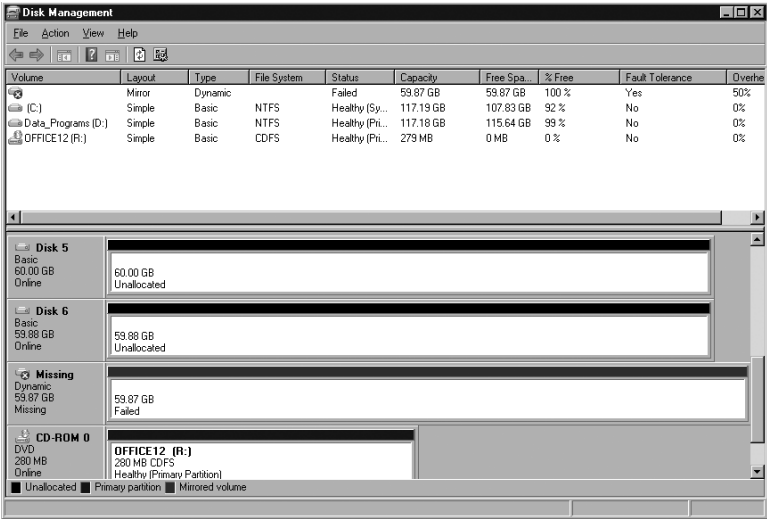


Figure 19-21 Failed disk in mirror shown as missing and offline

Once the mirror is unavailable, you need to remove, or “break,” the mirror, bringing the good disk back online and available. Once the problem disk has been replaced, you can rebuild the mirror by following the steps in the section “Adding a Mirror to a Volume” earlier in the chapter.

To remove the mirror, follow these steps:

1. In Disk Management, right-click either disk and select Remove Mirror from the action menu, as shown in Figure 19-22.

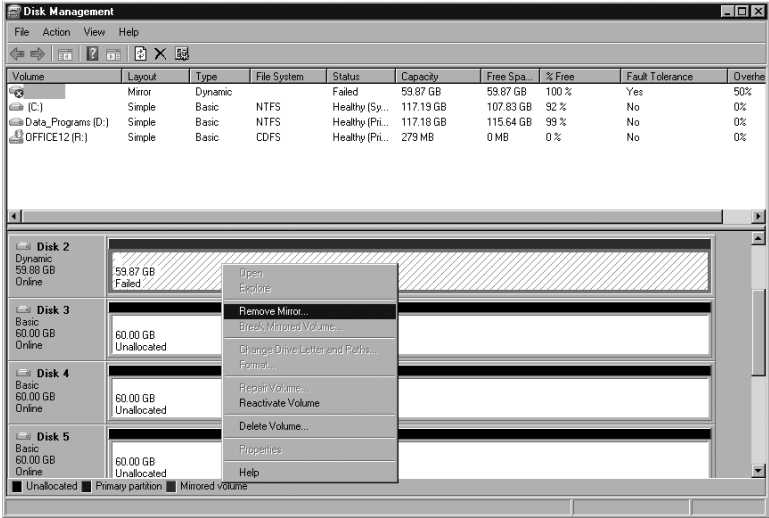


Figure 19-22 Breaking the mirror of a failed mirror pair

2. In the Remove Mirror dialog box, select the failed disk and click Remove Mirror.

After you replace the failed disk or correct the problem and reactivate the failed disk, the mirror automatically starts regenerating if you didn't have to remove the mirror. If you can solve the problem without powering down the system, you can regenerate the mirror on the fly. To reactivate the failed disk, follow these steps:

1. Right-click the icon for the failed disk on the left side of the Disk Management console.
2. Choose Reactivate Disk. Windows Server 2008 warns you about running `chkdsk` on any affected volumes, brings the disk back online, and starts regenerating the failed mirror.



Real World Removing a Mirror

We all know that every system administrator is always fully aware of the ongoing requirements of her servers, and never runs out of disk space without plenty of warning. Oh, wait, this is a Real World sidebar. OK, reality check, then. If you have the luxury of huge budgets and large, flexible, highly redundant Storage Area Networks, you probably haven't been caught short on disk space. But if you're running a more ordinary network where budgets interfere and resources are constrained, we strongly suspect you've certainly had times when you were scrambling to clean up disks to make sure you didn't run out of room for a critical process. Certainly we have. If you have a mirrored volume, you can get yourself out of trouble pretty quickly. But at a significant risk in the long run.

Just remove the mirror from the mirrored volume. When you remove a mirror, the data on one of the disks is untouched, but the other disk becomes unallocated space. You can then use the unallocated space to extend the volume that is short.

Of course, you will have lost all redundancy and protection for the data, so you need to take steps to restore the mirror as soon as possible. Plus the volume you've extended is now more susceptible to failure, since it has an extra disk included in it. Until you can buy more disks, you'll want modify your backup schedule for the affected disks. And don't put off buying the new disks—you're at serious risk until you get your system back to where it should be.

Setting Disk Quotas

Windows Server 2008 supports two mutually exclusive methods for setting quotas on the amount of file system resources a user can use—disk quotas or directory quotas. Disk quotas were introduced in Windows 2000, and are applied to specific users and limit the

amount of disk space that user can use on a particular volume. Directory quotas are applied to all users and limit the amount of disk space that users can use in a particular folder and its subfolders. Directory quotas were introduced in Windows Server 2003 R2 with the new File Server Resource Manager, and they are covered in detail in Chapter 20.

Enabling Quotas on a Disk

By default, disk quotas are disabled in Windows Server 2008. You can enable disk quotas on any volume that has been assigned a drive letter. To enable quotas on a volume, follow these steps:

1. In Windows Explorer, right-click a drive letter and open the properties of that drive.
2. Click the Quota tab, shown in Figure 19-23, and then click Show Quota Settings.



Figure 19-23 The Quota tab of a drive's properties

3. Select the Enable Quota Management check box to enable quotas for the disk, as shown in Figure 19-24.

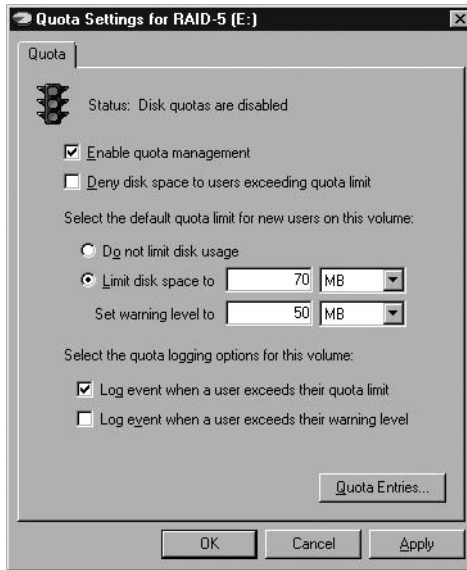


Figure 19-24 The Quota Settings dialog box for a disk

4. To enable hard quotas that can't be exceeded, select the Deny Disk Space To Users Exceeding Quota Limit check box.
5. Set the limits and warning level, as shown in Figure 19-24. You can also enable logging on this page.
6. Click OK to enable the quotas. You'll be prompted one last time to confirm, as shown in Figure 19-25. Click OK and the quotas will be enabled.

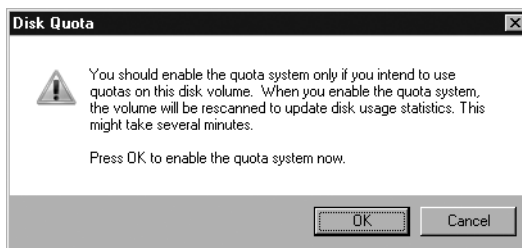


Figure 19-25 The Disk Quota confirmation message

Setting Per-User Quotas

You can set quota limits on individual users, or you can have limits apply equally to all non-administrative users. Unfortunately, you can't set limits on groups of users. And any users who already own files on the disk will have their quotas initially disabled. New users will have the default quotas for the disk applied as you would expect when they first save a file on the disk.

To set the quotas for individual users, follow these steps:

1. In Windows Explorer, right-click a drive letter and open the properties of that drive.
2. Click the Quota tab, and then click Show Quota Settings to bring up the Quota Settings dialog box for that disk.
3. Click Quota Entries to open the Quota Entries dialog box for the disk, as shown in Figure 19-26.

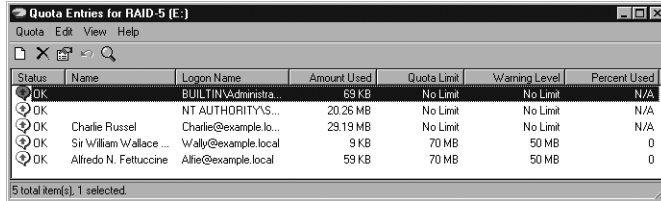


Figure 19-26 The Quota Entries dialog box for a disk

4. To modify the quota for a user already listed, select the user and then click Properties to open the quota settings for that user, as shown in Figure 19-27. Set the quota for the user and click OK to return to the Quota Entries dialog box.

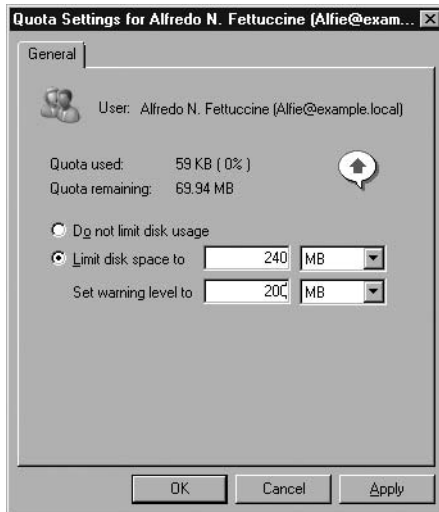


Figure 19-27 The Quota Settings dialog box for an individual user

5. To create a quota for a user who doesn't have one yet, and who needs a quota different from the default for the disk, click New Quota Entry.

6. Select the user or users to apply the new quota to, and click OK to bring up the Add New Quota Entry dialog box, as shown in Figure 19-28.

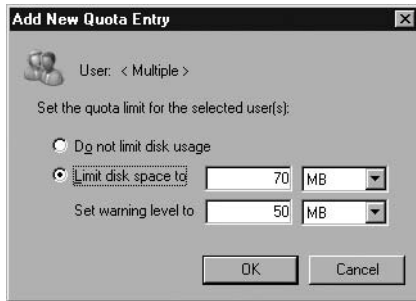


Figure 19-28 The Add New Quota Entry dialog box

7. Click OK to add the new entry and return to the Quota Entries dialog box. Close the Quota Entries dialog box, click OK in the Quota Settings dialog box, and then click OK in the Properties dialog box for the drive.
8. To manage quotas from the command line, you need to use Fsutil.exe. Even for a determined command-line type, it's pretty lame. Stick to the GUI, and use import and export whenever possible.

Importing and Exporting Quotas

Managing disk quotas is a potentially tedious job if you try to use fine-grained control of individual quotas. The best solution is to use a single, general quota that is correct for almost all users, and then do only limited exceptions to that quota for very specialized cases. If you do have complicated quotas, however, and you need to transfer them to another server or another volume, you can export a set of quotas and then import them to another volume.

To export the quotas on a volume, follow these steps:

1. Open the Quota Settings page for the volume you want to export the quotas from.
2. Click Quota Entries to open the Quota Entries dialog box.
3. Highlight the quotas you want to export.
4. Choose Export from the Quota menu. Type in a name and location for the export file and click Save.

To import a quota file to a volume, follow these steps:

1. Open the Quota Settings page for the volume you want to import the quotas to.

2. Click Quota Entries to open the Quota Entries dialog box.
3. Choose Import from the Quota menu. Type in a name and location for the import file and click Open.
4. If there are conflicting quotas, you'll be prompted to replace the existing quotas, as shown in Figure 19-29.

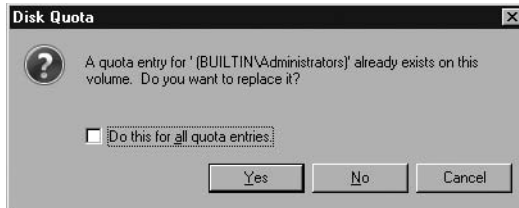


Figure 19-29 Importing quotas can cause an existing quota to be replaced.

5. Choose to replace a quota by clicking Yes or to not keep the existing one by clicking No. You can have the action repeated for any further conflicts by selecting the Do This For All Quota Entries check box.



Real World Just Say No to Disk Quotas

Disk quotas, which were originally introduced in Windows 2000, were a big step forward and gave the Windows system administrator a new and valuable tool to limit the spiraling growth of storage requirements on the server. But like many Microsoft version 1.0 implementations, it wasn't a perfect solution. It's difficult to manage quotas effectively without creating too many exceptions to easily keep track of. You can apply quotas only on a per-drive letter level, and they don't affect mounted volumes at all. And quotas are indiscriminant—they treat document files the same way they treat .MP3 files.

Quotas also arrived too late to the scene. Just about the time disk quotas were introduced, the hard disk industry started a round of massive growth in hard drive size. At the same time, the price of even enterprise-class hard drives came down dramatically.

Finally, with the introduction of the File Server Resource Manager, we now have folder-level quotas and file-type filtering. If you need quotas, we recommend that you use these.

Enabling File Encryption

With the introduction of Windows 2000, Microsoft added the ability to encrypt individual files or entire subdirectories stored on an NTFS volume in a totally transparent way. To their creator, encrypted files look exactly like regular files—no changes to applications are required to use them. However, to anyone except the creator/encryptor, the files are unavailable. Even if someone did manage to gain access to them, they would be gibberish because they're stored in encrypted form.

Encryption is simply an advanced attribute of the file, like compression. However, a file cannot be both compressed and encrypted at the same time—the attributes are mutually exclusive. Encrypted files are available only to the encryptor, but they can be recovered by the domain or machine recovery agent if necessary. You can back up encrypted files by normal backup procedures if the backup program is Windows Server 2008–aware. Files remain encrypted when backed up, and restored files retain their encryption.

Under normal circumstances, no user except the actual creator of an encrypted file has access to the file. Even a change of ownership does not remove the encryption. This prevents sensitive data—such as payroll information, annual reviews, and so on—from being accessed by the wrong users, even ones with administrative rights.

Note Encryption is available only on NTFS. If you copy the file to a floppy disk or to any other file system, the file is no longer encrypted. This means that if you have a USB key drive, for example, that is formatted with FAT, or if you use NFS file systems, copying the file there will remove the encryption.

When you encrypt a folder, all new files created in that folder are encrypted from that point forward. You can also elect to encrypt the current contents when you perform the encryption. However, be warned that if you choose to encrypt the contents of a folder when it already contains files or subfolders, those files and subfolders are encrypted *for the user performing the encryption only*. This means that even files owned by another user are encrypted and available for your use only—the owner of the files will no longer be able to access them.

When new files are created in an encrypted folder, the files are encrypted for use by the creator of the file, not the user who first enabled encryption on the folder. Unencrypted files in an encrypted folder can be used by all users who have security rights to use files in that folder, and the encryption status of the file does not change unless the filename itself is changed. Users can read, modify, and save the file without converting it to an encrypted file, but any change in the name of the file triggers an encryption, and the encryption makes the file available only to the person who triggers the encryption.

Important If you use EFS, it is *essential* that you back up EFS certificates and designate a Recovery Agent to protect against *irreversible* data loss. EFS certificates and recovery agents are covered in Chapter 23, “Implementing Security.”

To encrypt a file or folder, follow these steps:

1. In Windows Explorer, right-click the folder or files you want to encrypt, and choose Properties from the shortcut menu.
2. Click Advanced on the General tab to open the Advanced Attributes dialog box shown in Figure 19-30.

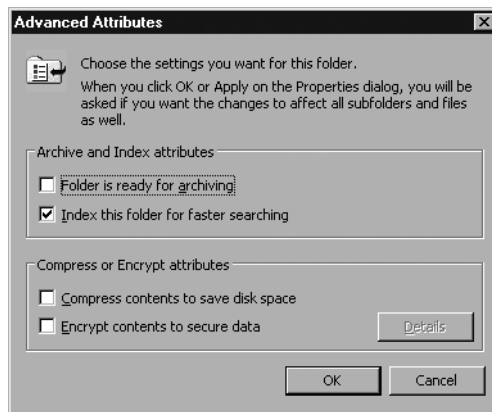


Figure 19-30 The Advanced Attributes dialog box

3. Select the Encrypt Contents To Secure Data check box and click OK to return to the main Properties window for the folder or file. Click OK or Apply to enable the encryption. If any files or subfolders are already in the folder, you're presented with the dialog box shown in Figure 19-31.



Figure 19-31 Choosing whether to encrypt the files already in a folder or just new files

4. If you choose Apply Changes To This Folder Only, all the current files and subfolders in the folder remain unencrypted, but any new files and folders are encrypted by the creator as they are created. If you choose Apply Changes To This Folder, Subfolders, And Files, all the files and folders below this folder are encrypted so that only you can use them, regardless of the original creator or owner of the file.
5. Click OK and the encryption occurs.



Real World The Limitations of EFS

The EFS capabilities of Windows Server 2008 provide a useful way to encrypt folders and files to prevent unauthorized access. However, EFS has limitations, and you need to manage it carefully to not create issues.

Once an EFS folder is created, any files created in the folder will always be encrypted *by the creator of the file*. This is not always what you intend. If you have a publicly available folder that has encryption on it, you need to carefully manage who has access to that folder using NTFS file permissions, share permissions, or other methods of preventing unauthorized access.

Another problem is that anyone who has access to your system drive *can* break EFS encryption. This shouldn't be a big problem on a well-secured server, but it's still a concern. The solution is to enable BitLocker on your server. BitLocker was introduced with Windows Vista as a solution for the mobile laptop, but it has very real possibilities for the enterprise trying to fully secure its environment. For more on BitLocker, see Chapter 23.

Summary

Windows Server 2008 provides the system administrator with a richer set of disk management tools than any previous version of Windows. Disk Management is now smarter, with automatic, seamless conversion between basic and dynamic disks. The full support for GPT disks eliminates the need for extended partitions, and gives Windows Server 2008 the ability to support really *large* disks. And the ability to shrink or extend a volume without taking it offline gives the system administrator much greater flexibility.

In the next chapter, we'll cover the many aspects of storage, including Storage Area Networks, the Storage Resource Manager, and removable and remote storage.

Index

A

- Abstract object class, 558
 - Accelerators, type, in
 - PowerShell, 441–442
 - Acceptable use policy, 664
 - Access control entries (ACEs), 21
 - Access control lists (ACLs), 14, 756
 - configuring, 529–530
 - in delegation, 21
 - in Kerberos authentication, 21
 - NTFS permissions and, 241
 - Access Control Settings, 370
 - Access points, wireless, 893–894
 - Access tokens, 348
 - Accidental deletion, of
 - containers, 201
 - Account Operators Domain
 - local group, 210
 - Account organizations, 472
 - Accounts, 779–784. *See also* Users
 - administrator, 780
 - domain password policies for, 781–784
 - installation security for, 766–767
 - lockout policies for, 6
 - logon events of, 358–359
 - management of, 359
 - standalone server password policies for, 781
 - Actions pane, in IIS, 1069
 - Actions properties, in Data Collection set, 1129
 - Active Directory
 - applications published in, 937
 - architecture of, 19–23
 - as chokepoint, 755
 - attributes in, 17
 - authentication by, 911
 - backup methods of, 271
 - containers in, 17
 - DFS folder published in, 268
 - distinguished names in, 18–19
 - domain controllers added to, 852
 - domain-based namespaces
 - and, 259
 - features of, 15–16
 - file resource shares
 - publication in, 256–257
 - namespaces and, 16, 268
 - objects in, 17
 - printer location naming and, 167, 170
 - schema in, 19
 - shared folders of, 239
 - trees and subtrees in, 17–18
 - UNIX identity management on, 923
 - upgrading and, 82–84
 - Active Directory Application Mode (ADAM), 15, 468
 - Active Directory Certificate Services, 473, 544, 810, 852, 861, 890
 - Active Directory Domain Services (AD DS), 227
 - AD LDS synchronization
 - with, 531–533
 - auditing, 567–571
 - configuring, 567–570
 - enabling, 570–571
 - objects of, 363–366
 - backing up, 541–545
 - frequency of, 544–545
 - need for, 543–544
 - overview of, 541–543
 - Windows Server Backup for, 545
 - database of, 535–541
 - garbage collection in, 537
 - location of, 541
 - offline defragmentation of, 540–541
 - online defragmentation of, 537–538
 - restartable AD DS and, 538–539
 - storage of, 535–536
 - DFS replication and, 262
 - groups and, 197
 - installing, 473–476, 495
 - operations masters roles and managing, 561–564
 - seizing, 566
 - transferring, 564–565
 - overview of, 5–6, 468
 - restoring, 546–552
 - authoritative, 550–552
 - nonauthoritative, 548–550
 - Ntdsutil for domain controller removal in, 546–548
 - schema of, 552–566
 - launching, 554–555
 - modifying, 553–560
 - wireless deployment of
 - remote access and, 889
- Active Directory Domain Services Installation Wizard, 476–491
- deployment configuration in, 478
- domain controller addition and, 484
- domain naming in, 479
- file locations in, 482
- install from media and, 486–487
- installation completion by, 483
- installation verification by, 484–485
- operating system
 - compatibility and, 477–478
- Operations Master roles and, 565
- options of, 485–486
- RODC pre-creation by, 494

- site objects created by, 515, 517
- unattended installation and, 487–489
- uninstalling AD DS by, 489–491
- Windows Server 2008
 - functional level in, 480–482
- Active Directory Domains and Trusts, 506–510
- Active Directory Federation Services (AD FS), 472–473, 1103
- Active Directory Lightweight Directory Services (AD LDS), 521–533
 - AD DS synchronization with, 531–533
 - features of, 522
 - instances and application partitions in, 523–526
 - managing, 526–530
 - overview of, 468–469
 - replication of, 530–531
- Active Directory Restore Mode, 538
- Active Directory Rights Management Services (AD RMS), 469–472
- Active Directory Service Interface (ADSI), 15
- Active Directory Sites and Services, 510–521
 - AD DS replication and, 513–514
 - launching, 515–521
 - overview of, 510–513
- Active Directory Sites and Subnets Console, 169
- Active Directory Users and Computers
 - attributes shown by, 560
 - computer objects and, 503
 - DFS folder publishing and, 268
 - for AD DS object viewing, 499–503
 - groups and, 204–206
 - namespace root publishing and, 268
 - object moving, renaming, and deleting with, 505
 - organizational unit deletion by, 202
 - PDC Emulator and
 - Infrastructure Operations Master roles and, 566
 - printer publishing with, 504–505
 - Published Certificates viewed by, 223
 - remote computer management with, 504
 - shared folder publishing with, 504
 - software distribution and, 940
- Adamsync synchronization, 532–533
- Add Features Wizard, 816, 1018
- Add Printer Wizard, 166
- Add Role Wizard, 63, 134, 168, 770, 853, 966–967, 969, 1018
- Add-Content cmdlet, 395, 416, 430
- Address reservations, for DHCP, 590–591
- Address Space Load Randomization (ASLR), 9
- Admin Approval Mode (AAM), 348–349
- Admin events, 370
- administration.config files, 1098
- Administrators Domain local group, 210
- Admins group, 208, 543, 780
- ADMS special share, 255
- Adprep tool, 83–84, 553
- Advanced Configuration Power Interface (ACPI), 1204
- Advanced mode, of Active Directory Users and Computers, 500–501
- Advanced Simulation Options, 342
- Advanced Technology Attachment (ATA), 618
- Allocation unit, 616
- Allowed RODC Password Replication Domain local group, 210
- Allowed RODC Password Replication Group, 497
- AMD processors, 962
- American National Standards Institute (ANSI), 909
- Anonymous authentication, 1090
- Antivirus software, 81
- AppCmd.exe command line tool, 1071–1072, 1086–1087
- Application pools, 1083, 1086–1087
- Application Server role, 842, 852, 854
- applicationHost.config files, 1098
- Applications. *See also* Interoperability
 - Active Directory Application Mode (ADAM) for, 15
 - Active Directory Lightweight Directory Services and, 523–526
 - chokepoints in, 755
 - delegating management of, in IIS, 1095–1097
 - development modules for, 1064
 - development settings for, 1076–1080
 - directory partition for, 490, 524, 562
 - directory-enabled, 522, 553
 - domain controller restoring and, 543
 - failed, 1118
 - failover clusters and, 720
 - generic application resource type for, 722–723
 - globalization of, 1077
 - Group Policy Objects for deployment of, 940–943

- Internet Information Services (IIS) and, 1069–1070, 1093–1094
 - inventory of, 44
 - line-of-business, 493
 - logs of, 370–371
 - media pools for, 690
 - mission-critical, 703–704
 - noncompliant, 348
 - property changes in, 950–952
 - published versus assigned, 937–939
 - recovery of, 1169–1171, 1231–1233
 - Registry data and, 1196
 - site-aware, 511
 - Subsystem for UNIX, 385
 - troubleshooting printing from, 193–194
 - UAC prompts disabled to install, 350–351
 - user profile folder for, 231
 - Web portal, 469
 - WINS-dependent, 579
 - write-intensive, 1185
 - zap files to deploy, 936–937, 949–950
- Architecture
- hardware supported by, 85
 - in upgrading, 82
 - of Active Directory
 - data model in, 20
 - Directory System Agent (DSA) in, 19
 - global catalog in, 22–23
 - naming contexts and partitions in, 22
 - naming formats in, 20
 - schema implementation in, 20
 - security model in, 21–22
 - Service-Oriented, 742
- Archiving logs, 376
- Arguments, in PowerShell, 435–436
- Arithmetic operators, in scripts, 424
- Arrays, in PowerShell, 422–423
- ASP (Active Server Pages), 1077–1078
- ASP.NET Framework, 1061–1062, 1077, 1090
- Assignment operators, in scripts, 424
- AT command, 378–379
- AT&T, Inc., 911
- Attacks
 - cache corruption, 602
 - denial of service (DoS), 358, 575, 748, 751, 756–757
 - dictionary, on passwords, 779
 - DNS poisoning, 602
 - MIME types and, 1076
 - phishing, 747, 837
 - surface for, 347
 - vectors for, 746
 - vulnerabilities to, 751
- Attributes
 - added to classes, 559
 - AppCmd.exe and, 1071–1072
 - classes of, 555–557
 - container object moving and, 505
 - Directory Services events
 - auditing and, 363
 - in Active Directory, 17
 - objectGUID, 17
 - Password Setting Object, 783–784
 - RODC filtered, 492
 - search by, 13–14
- Audio files, screening, 664
- Audit Directory Service Access, 362
- Auditing
 - Active Directory Domain Services (AD DS)
 - configuring, 567–570
 - enabling, 570–571
 - objects of, 363–366
 - categories of, 358–362
 - account logon events in, 358–359
 - account management in, 359
 - directory service access in, 359–360
 - logon events in, 360
 - object access in, 360–361
 - policy change in, 361
 - privilege use in, 361
 - system events in, 361–362
 - directory service events, 362–363
- Dynamic Host Configuration Protocol (DHCP) logs for, 575
- enabling, 367–370
- for security, 796
- global audit policy for, 366–367
- policies for, 285, 357–358, 760
- registry key security and, 1218
- Auditpol.exe command line tool, 365–366, 567–568
- AuthAnvil TFA provider, 784
- Authentication. *See also* Remote access
 - Active Directory, 911
 - Active Directory Sites and Services and, 511
 - AD DS object auditing and, 363
 - certificate-based, 825
 - Challenge Handshake Authentication Protocol (CHAP) for, 674, 680
 - Directory Services Restore Mode (DSRM) for, 483
 - extranet store for, 469
 - for Terminal Services, 1014–1016
 - IIS configuration of, 1089–1091
 - Internet Authentication Service for, 807
 - iSCSI, 679–680
 - Kerberos, 21, 33, 359, 508
 - LanMan hashes and, 797
 - protocols for, 747
 - Server Authentication
 - certificate for, 858–868
 - servers for user profiles and, 233

- two-factor, 780, 784
- UNIX interoperability and, 907
- users and, 212
- Workstation Authentication template for, 811
- Author mode, of MMC, 353
- Authoritative restore, 546, 550–552
- Authorization, 603–605, 1016, 1091
- Auto quotas, 658–660
- Autoenrollment certificates, 890
- Automatic restart option, 1145
- Auto-remediation, in NAP deployment, 807, 818, 832
- Auxiliary object class, 555, 558–560
- Availability
 - as security principle, 748
 - clusters and, 699, 724–725
 - fault tolerance versus, 1175, 1188
 - HPC clusters and, 741
 - of printers, 182–184
- Avenda third-party supplicant, 803

B

- Back doors, security and, 757
- Background processes, PowerShell scripts as, 387
- Backing up, 1147–1174. *See also* Disaster planning; Restoring; Troubleshooting
- Active Directory Domain Services (AD DS)
 - database of, 486
 - frequency of, 544–545
 - need for, 543–544
 - overview of, 541–543
 - Windows Server Backup for, 545
- Backup Once Wizard for, 1157–1159

- Distributed File System (DFS)
 - folder targets, 271
- Group Policy Objects, 338
- hot backups for, 575
- in disaster planning, 1142
- in Windows Server 2008, 8
- installing service for, 1147–1149
- PowerShell cmdlets for, 444
- print servers, 190–191
- Registry, 1221–1222
- SANs and, 671
- schedule for, 1149–1157
 - creating, 1150–1153
 - modifying, 1155–1156
 - of volumes, 1149
 - rotating, 1154–1155
 - stopping, 1156–1157
 - storage location for, 1149–1150
- seeding branch member by, 277
- server recovery and, 1165–1174
 - applications and data in, 1169–1171
 - backup catalog in, 1173–1174
 - files and folders in, 1167–1169
 - operating system in, 1171–1173
 - volumes in, 1166–1167
- upgrading and, 81
- Wbadmin command for, 1159–1165
- Backslash character, 441
- Backtick character, 393, 404, 441
- Backup Operators group, 208, 210, 543
- Basic authentication, 1090
- Basic disks, 616, 622–623
- Basic tasks, 377–378
- Bathtub curve, in electronic failure, 1176
- Berkeley Internet Name Domain (BIND) DNS servers, 573, 595, 602, 609

- Best practices
 - for AD DS naming, 479
 - for Default Domain Controllers Policy, 285
 - for Default Domain Policy, 285
 - for PKI deployment, 803
 - for schema changes, 553
- Beta user deployment, of patches, 840
- Binary operators, in scripts, 425
- BIND. *See* Berkeley Internet Name Domain (BIND)
- DNS servers
- Binding to instances, 527
- Biometric readers, 784
- BitLocker, for security, 773–779
 - encryption with, 9–10, 747, 776–778
 - features role installation in, 775–776
 - recovery with, 779
 - server data volume encryption in, 779
 - volumes set up in, 773–775
- Blue screen of death (BSOD), 1145
- Bluetooth devices, 850
- BOD (bunch of disks), 617
- Boot Configuration Data (BCD) store, 543
- Boot failure, 72–74
- Bottlenecks, 1111
- Branch office deployments, 5, 258, 275–277, 642, 779. *See also* Read only domain controllers (RODC)
- Brownouts, 1181
- Buffer overflow vulnerability, 751
- Burn-in phase, 1176
- Business Desktop Deployment (BDD), 959
- Business needs, deployment and, 41–42

C

- Cache corruption attacks, on DNS, 602
 - Caching
 - at branch offices, 258
 - duration of, 268–269
 - in IIS, 1081
 - integrated disk, 621
 - System File Protection folder for, 959
 - Universal Group membership, 23
 - Capacity
 - of failover clusters, 726–727
 - of network load balancing clusters, 716–717
 - Capture images, 70–71
 - Case sensitivity, 387
 - Catalog Recovery Wizard, 1173
 - Catalog, backup, 1173–1174
 - Category, searching by, 13–14
 - Certificate Authority
 - Enterprise Root, 810
 - for NAP IPsec enforcement, 808, 810, 816–818
 - for Protected Extensible Authentication Protocol (PEAP), 890–892
 - remote access and, 854–855, 857
 - Root, 825, 877
 - security of, 889–890
 - Trusted Root, 879, 896
 - Certificate Import Wizard, 879
 - Certificate Services, 747
 - Group Policy management console and, 816–818
 - NAP server and, 813–816
 - overview of, 473
 - Registry data and, 1195
 - set up of, 809–813
 - Certificate Services DCOM
 - Access Domain local group, 210
 - Certificates
 - Encrypting File System (EFS), 648
 - for servers, 1091–1092
 - for Terminal Services, 1015–1016
 - Group Policy to deploy, 894–897
 - Server Authentication, 858–868
 - software restrictions and, 956, 958
 - Certified for Windows Server
 - 2008 logo requirements, 556, 1024–1025
 - CGI restrictions, 1091
 - Challenge Handshake Authentication Protocol (CHAP), 674, 680, 747
 - Change command, 1025–1027
 - Change management, rule of, 749
 - Checkpoint files, 536
 - Child partitions, 962, 964
 - Chokepoints, security, 754–755
 - Circular logging, 544
 - Citrix MetaFrame, 1038
 - Citrix XenServer virtualization, 1002–1003
 - Classes
 - auxiliary added to structural, 559–560
 - definition of, 399
 - of attributes, 555–557, 559
 - of objects, 558
 - WMI, 402
 - Classification, searching by, 14
 - Clean service shutdown, 9
 - Client Access License (CAL), 1042, 1044
 - Client Certificate Mapping
 - authentication, 1090
 - Client failover, 258, 261, 269
 - Clients
 - Access Point resource type for, 721
 - connection, 877–881
 - namespace, 261
 - printer troubleshooting and, 191–192, 195
 - RADIUS, 892–893
 - upgrading, 88
 - Client-side extensions, 290
 - Clipboard, in Hyper-V Virtual Machines, 999–1000
 - Clocks, configuring, 99–100
 - Clusters, 699–742
 - description of, 699–701
 - DHCP server, 593
 - failover, 592, 718–740
 - capacity of, 726–727
 - concepts of, 718–720
 - configuring, 724–725
 - creating, 727–740
 - defining, 723
 - DFS replication and, 262
 - overview of, 701–702
 - resource types for, 720–723
 - for fault tolerance, 1190–1191
 - HPC (high performance computing), 740–742
 - in disaster planning, 1142
 - in Server Core, 702
 - network load balancing, 706–718
 - capacity of, 716–717
 - concepts of, 706–707
 - creating, 709–716
 - fault tolerance provided by, 717
 - models of, 707–708
 - optimizing, 717–718
 - print server, 191
 - private, 674
 - requirements for, 704–706
 - scenarios for, 703–704
 - Storage Manager connections to, 677
- Cmd.exe commands, 391–392
- Cmdlets, PowerShell, 5
 - definition of, 387
 - for data files, 430
 - for flow control, 431–432
 - for formatting, 433–434
 - Foreach-object, 392
 - Get-ChildItem, 443
 - Get-Command, 406–408
 - Get-Credential, 393
 - Get-Date, 447
 - Get-Help, 407–409

- Get-Member, 407, 409–410, 446
- Get-Process, 465
- Get-Wmiobject, 402
- list of, 394–398
- Select-Object, 464
- server backup, 444
- Stop-Process, 465
- tab completion of, 388
- Code Red-Nimba worm, 763
- Collaboration, DFS replication for, 258
- Com+ Event System services, 767
- Command line tools
 - AppCmd.exe, 1071–1072, 1086–1087
 - Auditpol.exe, 365–366, 567–568
 - Change command, 1025–1027
 - dcpromo.exe, 476–477
 - Dfsradmin, 273–274
 - Dfsradmin Bulk, 276
 - Dfsradmin ConnectionSet, 280
 - Dfsrdiag, 280
 - Diskpart.exe, 60, 623, 626, 630–631, 637, 685, 774
 - Diskraid.exe, 679, 687
 - dsacis, 529
 - for BitLocker installation, 776
 - for disk management, 623
 - for Dynamic Host Configuration Protocol (DHCP), 582, 595
 - for Roles and Features, 772
 - for server features, 144–145
 - for server roles, 135, 138
 - for Windows Firewall, 793–795
 - Fsutil.exe, 623, 645
 - installutil.exe, 414
 - mapadmin.exe, 915
 - Mountvol.exe, 623
 - Mstsc.exe, 427
 - Net session, 256
 - Net Share, 256
 - Net view, 256
 - netdom, 152
 - netsh, 151, 156, 392
 - Ntdsutil.exe, 548, 566
 - Oclis.exe, 444
 - Ocsetup.exe, 157, 160
 - printer management by, 181
 - Reg.exe, 1220
 - Regedit.exe, 1217
 - Rendom.exe, 562
 - RSM View, 693
 - ServerManagerCmd.exe, 445, 965
 - Sysprep.exe, 71
 - Wbadmin.exe, 541–542, 545, 1159–1165, 1221, 1235–1236
 - Wevtutil.exe, 392
- Comments, in PowerShell scripts, 417–418
- Common Engineering Criteria (CEC), 384
- Common names (CNs), 18
- Community Technology Preview (CTP) of PowerShell, 384, 386–387
- Comparison operators, in scripts, 424
- Compatibility, 40, 92–93, 477–478, 842, 1119
- Complete Memory Dump option, 1145
- Compliance solution, Network Access Quarantine as, 800
- Component Object Model (COM), 405, 1202
- Compression, 257, 263, 280, 447, 514, 609, 1081
- Computer Authentication, 896
- Computer objects, 503
- Computer Security Institute (CSI), 748
- Conditional statements, in PowerShell, 426–429
- Confidentiality, 746–747
- Configuration Tasks Wizard, 1023
- Configure And Enable Routing and Remote Access Wizard, 869
- Configuring installations, 95–119. *See also* Server Core
 - computer name and domain in, 103–106
 - error reporting in, 111
 - hardware in, 98–99
 - Initial Configuration Tasks Wizard in, 118–119
 - logon for, 97–98
 - networking in, 101–103
 - PowerShell addition in, 113–115
 - Remote Desktop enabling in, 116–117
 - tasks in, 96–97
 - time zone in, 99–100
 - update and feedback enabling in, 106–111
 - update downloading in, 112
 - Windows Firewall in, 117–118
- Conflict detection, server-based, 593
- Conflict resolution, 271–272
- Connect To A Workplace Wizard, 881–882
- Connect To Server Wizard, 1070
- Connection manager, in IIS, 1069–1070
- Connection objects, 513, 516–517
- Connectivity, 43, 191, 908. *See also* Networks; Remote access
- Consent, prompt for, 350
- Consistency, namespaces
 - polling for, 270
- Consolidation solution, directory, 469
- Consolidation, server. *See* Virtualization
- Constant voltage transformer, 1180–1181
- Constructor, definition of, 399
- Consuming content, 471
- Contacts, 206

- Containers
 - in Active Directory, 17
 - organizational units as, 34
 - permissions applied to, 249–250
 - Content management,
 - permissions for, 1097–1098
 - Control Panel, 306–335
 - data sources in, 306–307
 - devices in, 307–312
 - Internet settings in, 312–314
 - Local Users and Groups in, 314–317
 - Network Options in, 317–320
 - Power Options in, 320–321
 - printers in, 322–326
 - Regional Options in, 326–327
 - Scheduled Tasks in, 327–329
 - Services Group Policy
 - Preferences in, 330–333
 - ConverTo-HTML cmdlet, 430
 - Cookies folder, in user profiles, 231
 - Coordinated Universal Time (UTC), 273, 275, 277
 - Copy-Item cmdlet, 395
 - Corruption of files, 74–75, 1185
 - Cost, of RAID configurations, 1189
 - Cost-benefit analysis, 45
 - Countdown, time, 449–450
 - Counters, performance. *See also* Reliability and Performance Monitor
 - Data Collection set to monitor, 1125–1126
 - Performance Monitor
 - additions of, 1112–1113
 - remote computer to view, 1115
 - CPU usage
 - for Terminal Services, 1009
 - on Reliability and Performance Monitor, 1109
 - PowerShell to check, 455–456
 - virtualization and, 984–986
 - Crash dumps, 111
 - Create Cluster Wizard, 730
 - Create New Data Collector Set Wizard, 1121, 1123
 - Credentials. *See also* Authentication
 - caching of, 492
 - federated trusts and, 472
 - for trust verification, 509
 - PowerShell, 393
 - prompt for, 350
 - Critical updates, 833
 - Cross-reference objects, 562
 - Cross-training, 1140
 - Cryptocard TFA provider, 784
 - Cryptographic Operators
 - group, 209–210
 - Cryptographic Services, 767
 - CSV (Comma-Separated Values) text, 654
 - Custom replication topology, 263
 - Customer Experience Improvement Program (CEIP) settings, 106, 110
 - Cyclic Redundancy Code (CRC), 75
- D**
- Data
 - Control Panel sources of, 306–307
 - corruption of, 1185
 - integrity of, 747
 - managing collection of, 1128–1131
 - PowerShell display of, 410–412
 - recovery of, 1169–1171, 1231–1233
 - scheduling collection of, 1126–1128
 - XML-formatted, 463
 - Data Collector set, 1119–1126
 - manual construction of, 1123–1125
 - Performance Log Users and, 1120
 - Performance Monitor to
 - create, 1123
 - template for, 1120–1122
 - to monitor performance counters, 1125–1126
 - Data mining, 6
 - Data model, in Active Directory, 20
 - Data Protection Manager 2007, 1152–1153
 - Data-based Registry keys, 1208
 - Databases, AD DS, 535–541
 - connection strings for, 1078
 - garbage collection in, 537
 - location of, 541
 - offline defragmentation of, 540–541
 - online defragmentation of, 537–538
 - restartable AD DS and, 538–539
 - storage of, 535–536
 - Datacenter edition, of Windows Server 2008, 10
 - Dates, PowerShell and, 447–449
 - dcpromo.exe command line tool, 476
 - Debugging, 371, 1145
 - Default Domain Controllers Policy, 284–285, 363, 366, 478, 568
 - Default domain NetBIOS name, 486
 - Default Domain Policy, 284–285, 957
 - Default execution policy, 416
 - Default rules, for software restriction, 956
 - Default user profile, 230
 - Default-First-Site-Name, 512, 515
 - Defense in depth, for security, 756, 839
 - Deferred enforcement, of NAP, 807
 - Defragmentation, 6, 88
 - offline, 540–541
 - online, 537–538
 - Delayed start, for services, 1238

- Delegating
 - as security feature, 21–22
 - directory administration, 14
 - DNS authority, 603–605
 - in Internet Information Services (IIS)
 - configuration store and, 1098–1099
 - for content management, 1097–1098
 - for site and application management, 1095–1097
 - shared configuration and, 1099
 - permissions
 - management, 270
 - on Group Policy Objects, 335–336
 - read-only domain controller administration, 493–495
 - tasks, 380–381
- Denial of service (DoS) attacks, 358, 575, 748, 751, 756–757
- Denied RODC Password Replication Domain local group, 211
- Denied RODC Password Replication Group, 497
- Dependencies, 194, 726
- Deployment, 39–48, 53–71
 - automating, 61–63
 - business needs and, 41–42
 - documenting network before, 42–45
 - image additions in, 69–71
 - information technology department and, 40
 - installation method in, 53
 - installation process in, 53–61
 - overview of, 39–40
 - roadmap for, 45–48
 - Windows Deployment Services for, 63–69
- Derived file screens, 668
- Derived quotas, 663
- Desktop display resolution, 155–156
- Desktop Experience, 1020
- Desktop folder, in user profiles, 231
- Destination disk, for backups, 1152
- Destination logs, 373
- Development environment,
 - directory services for, 469
- Device drivers, Registry data and, 1196
- Device Manager, 98
- Devices, on Control Panel, 307–312
- Dfsradmin Bulk command line tool, 276
- Dfsradmin command line tool, 273–274
- Dfsradmin ConnectionSet command line tool, 280
- Dfsrdiag command line tool, 280
- DHTML (Dynamic Hypertext Markup Language), 654, 657
- Diagnostic Report Wizard, 279
- Dial-up networking (DUN), 317, 319–320, 589
- Differencing disks, 986–991
- Digest authentication, 1090
- Digital certificates, 473
- Digital signatures, 473
- Directory Access Protocol (DAP), 15
- Directory partition, 483, 561–562
- Directory Service Access feature, 568
- Directory Services, 13–23
 - Active Directory as, 15–21
 - architecture of, 19–23
 - attributes in, 17
 - containers in, 17
 - distinguished names in, 18–19
 - features of, 15–16
 - namespace and name resolution in, 16
 - objects in, 17
 - schema in, 19
 - trees and subtrees in, 17–18
 - auditing, 359–360, 362–363
 - browsing, 1074
 - File Server Resource Manager (FSRM) and, 657–663
 - File Transfer Protocol (FTP), 1102
 - logs of, 537
 - overview of, 13–14
 - PowerShell and, 443–444
 - recursive file copying and, 459
 - replication of, 522
 - Windows Deployment Services and, 68
 - X.500 and, 15
- Directory Services Restore Mode (DSRM), 6, 483, 539, 541, 548
- Directory Services, installing and configuring, 467–533
 - Active Directory Certificate Services in, 473
 - Active Directory Domain Services (AD DS) in, 468, 473–476
 - Active Directory Domain Services Installation Wizard for, 476–491
 - deployment configuration in, 478
 - domain controller addition and, 484
 - domain naming in, 479
 - file locations in, 482
 - install from media and, 486–487
 - installation completion by, 483
 - installation verification by, 484–485
 - operating system compatibility and, 477–478
 - options of, 485–486
 - unattended installation and, 487–489

- uninstalling AD DS by, 489–491
- Windows Server 2008 functional level in, 480–482
- Active Directory Domains and Trusts in, 506–510
- Active Directory Federation Services (AD FS) in, 472–473
- Active Directory Lightweight Directory Services (AD LDS) in, 468–469, 521–533
- AD DS synchronization with, 531–533
- features of, 522
- instances and application partitions in, 523–526
- managing, 526–530
- replication of, 530–531
- Active Directory Rights Management Services (AD RMS) in, 469–472
- Active Directory Sites and Services in, 510–521
- AD DS replication and, 513–514
- launching, 515–521
- overview of, 510–513
- Active Directory Users and Computers in, 498–505
- computer objects and, 503
- for AD DS object viewing, 499–503
- object moving, renaming, and deleting with, 505
- printer publishing with, 504–505
- remote computer management with, 504
- shared folder publishing with, 504
- read-only domain controllers (RODC) in, 492–498
- delegating, 493–495
- description of, 492–493
- password replication policies in, 496–498
- uses of, 493
- Directory System Agents (DSAs), 17, 19
- Directory-enabled applications, 522, 553
- DisableNameChecking registry value, 190
- Disaster planning, 1133–1145. *See also* Backing up; Restoring
 - backing up in, 544, 1142
 - fault-tolerant system for, 1141–1142
 - iterating in, 1140–1141
 - recovery options in, 1144–1145
 - resource identification in, 1135
 - responses in, 1136–1140
 - risk identification in, 1134–1135
 - system repair for, 1142–1144
- Discretionary Access Control Lists (DACLS), 747
- Disk management, 615–649
 - cluster disk resource type for, 723
 - command line for, 623
 - differencing, 988–991
 - disk additions and, 623–625
 - Disk Management console for, 620–621
 - dynamic disks in, 622–623
 - failures and, 1118
 - file encryption for, 647–649
 - for fault tolerance, 1183–1190
 - hardware versus software, 1183
 - hot-swap and hot-spare, 1189
 - RAID levels for, 1183–1189
 - hardware RAID for, 621–622
 - in troubleshooting installations, 75–76
 - operating system recovery and, 1233
 - partitions and volumes in, 625–641
 - creating, 626–631
 - dynamic disk conversions and, 631–632
 - GPT disk conversions and, 632–633
 - logical drives on, 631
 - mirror added to, 637–641
 - size changes of, 633–637
 - PowerShell and, 458–459
 - quorum, 704
 - quotas for, 641–646
 - RAID (redundant array of independent disks) in, 619–620
 - Reliability and Performance Monitor and, 1110
 - remote management in, 622
 - software distribution and, 942
 - space requirements in, 81
 - terminology in, 616–619
 - virtualization and, 986–989
 - Windows operating system upgrades and, 948
 - witness, 704, 719–720
- Diskpart.exe command line tool, 60, 623, 626, 630–631, 637, 685, 774
- Diskraid.exe command line tool, 679, 687
- Dismounting media, 695–696
- Display resolution, desktop, 155–156
- Distinguished names, 18–19
- Distributed COM Users group, 209, 211
- Distributed File System (DFS), 651, 721, 739. *See also* Namespaces; Storage
 - backing up and restoring folder targets of, 271
 - folders of, 239, 267–268
 - for fault tolerance, 1190
 - replication of, 271–280
 - branch office group for, 275–277
 - folders, 272–274, 511
 - group for, 271–272
 - managing groups for, 278–280

- multipurpose group for, 277–278
 - overview of, 262–263
 - software distribution points and, 939
 - terminology of, 258–260
- Distribution groups, 198–199
- Do while and Do until statements, in PowerShell, 429
- Documentation
 - in disaster planning, 1137–1138
 - network, 42–45
 - security, 754
- Documents
 - default, 1074
 - folder redirection and, 340–341
 - in user profiles, 231
 - redirecting, 934
- Dollar signs
 - in PowerShell, 435, 438–439
 - in share names, 256, 339
- Domain Admins group, 343, 476
- Domain controllers. *See also* Namespaces
 - account logon events and, 358
 - AD DS Installation Wizard and, 481–482
 - addition of, 484
 - as schema operations masters, 553
 - audit policy settings for, 569–570
 - backing up, 543
 - backup, 563
 - default policy for, 284–285, 363, 366, 478, 568
 - fine-grained password policies and, 781
 - forced removal of, 491
 - Ntdsutil.exe to remove, 546–548
 - replication and, 486, 511
 - tombstones and, 537
 - user profiles and, 233
 - Windows Server 2008, 852
 - wireless remote access and, 889
- Domain Group Policy Objects, 283
- Domain local groups, 203, 210–212
- Domain local scope, 198
- Domain Name System (DNS)
 - AD DS installation prerequisites for, 475
 - description of, 573
 - read-only, 493
 - servers for, 14, 539, 595–613
 - as Active Directory locator service, 16
 - forwarders in, 610–613
 - interoperating between, 609
 - resource records added to, 605–608
 - setting up, 596–602
 - subdomains for, 603–605
 - zone transfers in, 608–609
 - VPN gateway server and, 859
- Domain Naming operations
 - master role, 561–562, 564, 566
- Domain profile, for Windows Firewall, 785–786
- Domain-based namespaces, 259–260, 265
- DomainDNSZones, 642
- Domains, 32–38. *See also* Active Directory Domain Services (AD DS)
 - Active Directory Users and Computers to change, 501
 - authorization for, 917
 - default policy for
 - designing structure of, 34–35
 - forest root, 476, 478–479
 - Fully Qualified Domain Name (FQDN) for, 713
 - functional levels of, 94, 480, 506, 781
 - in configuration, 103–106
 - IPv4-based restrictions on, 1088–1089
 - multiple, 36–38
 - naming of, 479
 - NAP deployment and, 807–808
 - Network Information System (NIS), 926
 - object types for, 500
 - organizational units versus, 33–34, 36, 200
 - password policies in, 781–784
 - security for, 35–36
 - Server Core joining, 152–155
 - tree-root, 476
 - trust relationships between, 507–509
 - UNIX SMB servers for, 911
 - upgrading and, 87–88
 - users accounts in, 220–221
- Door timeouts, for libraries, 694
- DOS batch commands, 385, 391
- Dot-sourcing, in PowerShell, 434–435
- Downloads folder, in user profiles, 231
- Drain Mode, Terminal Services, 8
- Drive Maps, 291–293
- Driveletter\$ special share, 255
- Drivers
 - NLB, 706
 - printer, 188–189
 - Registry data and, 1196
 - rolling back, 1226–1227
 - signed, 52, 82
 - troubleshooting, 1226
 - updated, 81
- Drives, 980
 - failure of, 639–641
 - hidden shares for, 255
 - hot-swap and hot-spare, 621
 - in libraries, 694
 - installation to, 58–60
 - logical, 474, 616, 631
 - NTFS, 631
 - physical, 616
 - Storage Manager node for, 675

- troubleshooting, 1226
- virtualization and, 992–994
- Dsacls command line tool, 529
- Dsdbutil tool, 528–529
- DSN (Database System Name), 1130
- Dump, memory, 1145
- Duplexing, mirror volumes and, 639
- Dynamic disks, 616, 622–623, 631–632, 1183
- Dynamic Host Configuration Protocol (DHCP), 14, 190, 356, 574–595, 721
 - address reservations for, 590–591, 893
 - authorizing server and
 - activating scope for, 589–590
 - command line administration of, 595
 - deployment of, 802
 - description of, 573
 - Network Access Quarantine and, 800
 - network design for, 574–576
 - relay agent of, 593–595
 - Relay Agents of, 874–875
 - routing and remote access setup and, 874
 - scope creation for, 582–589
 - server role for, 576–582, 592–593
- Dynamic RPC, 790
- Dynamic updates, 600–602
- Dynamically expanding disks, 986–987

E

- Easy Print. *See* Terminal Services
- Edb.chk checkpoint file, 536
- Edb.log transaction log, 536
- Edbres00001.jrs reserved log files, 536
- Edbtmp.log temporary log, 536
- Edge Traversal, 791
- Edit.com, 909
- Effective permissions, 1218

- Elapsed time, 449–450
- Elevation, 349–352. *See also* Privileges
- E-mail
 - plain-text, 837
 - PowerShell and, 446–447
 - scripts to verify address for, 422
 - SMTP, 1076, 1080
- Emulation, as virtualization method, 1002
- Encrypting File System (EFS), 473, 648–649, 747
- Encryption
 - BitLocker for, 9–10, 776–778
 - data volume, 779
 - for wireless remote access, 849
 - in disk management, 647–649
 - in Terminal Services Gateway, 7
 - iSCSI, 679–680
 - machine key, 1078
 - of SMTP traffic, 519
- Enterprise Admins group, 343, 476
- Enterprise directory store, 469
- Enterprise edition, of Windows Server 2008, 10
- Enterprise features, 771–772
- Enterprise roles, 770–771
- Environment Group Policy
 - Preference extensions, 293–294
- Errors. *See also* Troubleshooting
 - Group Policy Preferences and, 305
 - IIS custom page for, 1075
 - PowerShell and, 391, 439–441
 - reporting of, 106, 109, 111
- Escape character, 393, 442
- Ethernet Jumbo Frames, 674
- Ethernet switch, 672, 674
- Event logs
 - Distributed File System, 279
 - managing, 375–377
 - PowerShell to check, 453–455
 - readers group for, 209, 211

- security and, 760
- warning events on, 186–187
- Event trace providers, 1124
- Event Viewer, 370–375
 - applications and services logs in, 370–371
 - custom views of, 371–372
 - forwarding and collecting events in, 372–373
 - on remote computer, 374
 - subscriptions in, 373–374
 - task running and, 375
 - Windows logs in, 370
- Events
 - account logon, 358–359
 - auditable file system, 369–370
 - logon, 360
 - Shutdown Event Tracker for, 1241–1242
 - system, 362
- Exceptions, in screening files, 666
- Exchange Management Console (EMC), 385. *See also* Microsoft Exchange Server 2007
- Execution policy, 115, 416
- Expiration date, 218, 1127
- Explicit permissions, 245, 284
- Export-Clixml cmdlet, 430
- Export-Csv cmdlet, 395, 430
- Exporting
 - Network File System and, 917
 - quotas, 645–646, 663
 - Registry data, 1214–1215
 - Starter GPO, 288
 - templates, 1122
 - virtual machines, 1000–1002
- Express Full technology, 1153
- Extend Volume Wizard, 634
- Extended partitions, 616, 631
- Extended volume, 616, 622, 633–636
- Extensible schemas, 522
- Extensible storage engine (ESENT), 474
- External connectivity, 43
- External trusts, 508

External virtual networks, 969
 Extranet authentication store,
 469

F

Failback, 723
 Failed request tracing rules, in
 IIs, 1081
 Failover clusters, 592, 718–740
 capacity of, 726–727
 concepts of, 718–720
 configuring, 724–725
 creating, 727–740
 defining, 723
 DFS replication and, 262
 HPC clusters and, 741
 in disaster planning, 1142
 mission-critical applications
 and, 703
 overview of, 701–702
 resource types for, 720–723
 Failures
 events as, 358–359, 362
 mean time to, 1176–1177
 to find hard disks, 75–76
 Fast Logon Optimization, 946
 FAT volumes, 81
 Fault tolerance, 1175–1191
 clustering for, 717, 1190–1191
 disk arrays for, 1183–1190
 hardware versus software,
 1183
 hot-swap and hot-spare,
 1189
 RAID levels for, 1183–1189
 Distributed File System for,
 1190
 for DHCP servers, 575
 in disaster planning, 1141–
 1142
 mean time to failure and
 recovery, 1176–1177
 namespace servers for, 266
 power supply protection for,
 1177–1182
 local failure of, 1178–1179
 long-term outages in, 1182
 short-term outages in, 1182

 voltage variations in, 1179–
 1181
 Favorites folder, in user profiles,
 231
 FBI Computer Crime Unit, 748
 Features wizards, 770–772
 Features, server. *See* Servers
 Federation Services, 472–473
 Feedback, enabling, 106–111
 Fibre Channel, 671–672, 674,
 677, 681, 722, 1011, 1190
 File encryption, 647–649
 File extensions, OLE and, 1202
 File groups, 668–670
 File permissions, 240–242
 File Replication Service (FRS),
 262–263, 539
 File resources, 239–280
 Active Directory publication
 of shares for, 256–257
 advanced settings changes
 and, 268–271
 Distributed File System (DFS)
 for
 backing up and restoring
 folder targets of, 271
 folders for, 267–268
 overview of, 257–258
 replication of, 262–263,
 271–280
 terminology of, 258–260
 inheritance and, 245–246
 namespaces for
 client for, 261
 root for, 265–266
 server for, 260–261, 266–
 267
 Net Share command line tool
 for, 256
 NTFS permissions for, 242–
 244
 ownership of, 250–252
 permissions and
 assignments of, 247
 file, 241–242
 folder, 246–247
 operations of, 244–245
 share, 240
 special, 248–250

 share and storage
 management for, 252–
 256
 shared folders and, 252
 shared types of, 239
 File Screening Management,
 664
 File Server for Macintosh
 (FSM), 932
 File Server Resource Manager
 (FSRM)
 directory quotas for, 657–663
 installation and configuration
 of, 652–654
 reports from, 654–657
 screening files and, 663–670
 File Server, as resource type, 721
 File Services role, 157
 File system events, 369–370
 File Transfer Protocol (FTP)
 for UNIX interoperability, 908
 Internet Information Services
 (IIS) installation of,
 1100–1103
 PowerShell and, 445
 File Type association settings,
 311–312
 File-type filtering, 646
 Filtering
 as function, 426
 by ISAPI (Internet Server
 Application
 Programming Interface),
 1083
 file-type, 646
 ingress and egress, 748
 IP packet, 875–877
 Windows Firewall, 785
 Windows Management
 Instrumentation (WMI),
 786–788
 Fine grained group controls,
 760
 Fine-grained password policies,
 6, 781
 FIPS-certified, 909
 Firewalls. *See also* Windows
 Firewall
 FTP support of, 1102

- host-based, 748
 - in defense-in-depth security, 756
 - Performance Logs and Alerts exception for, 1115
 - ports of, 917
 - Firmware, 81
 - Five-nines system, 1175
 - Fixed-size disks, 986–987
 - Flexible Single Master Operations (FSMO) roles, 83–84, 561
 - Flow control, in PowerShell, 431–432
 - Folders
 - Group Policy Preferences for, 296–297
 - permissions for, 246–247
 - quotas for, 646
 - redirection of, 282, 339–341
 - For statement, in PowerShell, 429
 - ForEach statement, in PowerShell, 429
 - ForEach-Object cmdlet, 392, 395, 431
 - Forest root domains, 476, 478–479
 - ForestDNSZones, 642
 - Forestrep utility, 553
 - Forests
 - creating, 37–38
 - DFS replication and, 262
 - functional levels of, 94, 480, 506
 - in namespace planning, 26–27
 - need for, 37
 - trusts of, 508
 - User Principal Name (UPN) suffixes for, 509–510
 - Formatting cmdlets, in PowerShell, 395, 412, 433–434
 - Forms authentication, 1090
 - Forwarders, DNS, 481, 602, 610–613
 - Fragmentation of disks, 986
 - Free media pools, 690
 - Fsutil.exe command line tool, 623, 645
 - Full mesh replication topology, 263, 273
 - Fully Qualified Domain Name (FQDN), 479, 713, 782, 809
 - Functions, in PowerShell, 425–426, 434
- G**
- Garbage collection, 537
 - Gateway, Terminal Services. *See* Terminal Services
 - Generic application resource type, 722–723
 - Generic script resource type, 723
 - Generic service resource type, 723
 - Geographical naming convention, 29
 - Get-Alias cmdlet, 395
 - Get-ChildItem cmdlet, 395, 443
 - Get-Command cmdlet, 395, 406–408
 - Get-Content cmdlet, 395, 423
 - Get-Credential cmdlet, 393, 396
 - Get-Date cmdlet, 447
 - Get-Eventing cmdlet, 396
 - Get-Help cmdlet, 396, 407–409, 422
 - Get-Item cmdlet, 396
 - Get-Itemproperty cmdlet, 396
 - Get-Location cmdlet, 396
 - Get-Member cmdlet, 396, 407, 409–410, 418, 446
 - Get-Process cmdlet, 396, 431, 465
 - Get-Service cmdlet, 396, 411, 413
 - Get-Variable cmdlet, 396
 - Get-Wmiobject cmdlet, 396, 402
 - Gigabit Ethernet switch, 672
 - Global audit policy, 366–367
 - Global catalog (GC), 22–23, 482
 - Global local groups, 203, 212–213
 - Global scope, for groups, 198
 - Globalization, of applications, 1077
 - Globally unique identifiers (GUIDs), 17
 - GPT (GUID Partition Table) disks, 625, 632–633, 702
 - Group Policy. *See also* Group Policy Objects; Group Policy Preferences
 - applications updating and, 938–939
 - certificates and, 816–818, 894–897
 - components of, 282
 - Default Domain Controller, 366
 - for folder redirection, 339–341
 - for printer deployment, 176–179
 - for printer location tracking, 171
 - for software management, 935, 947–950, 952
 - for Windows Firewall, 786–788
 - groups and, 201
 - installation extension of
 - application deployment GPO in, 940–943
 - configuring, 943–947
 - distribution point setup in, 939–940
 - overview of, 933–935
 - new features of, 281–282
 - Object Editor for, 363
 - PDC Emulator operations master and, 564
 - refreshing, 337–338
 - Registry keys and, 1202
 - Resultant Set of Policy (RSOP) tool for, 341–343
 - Windows operating system upgrades and, 948
 - Windows XP processing of, 946

- Group Policy Management Editor, 825
 - Group Policy Objects (GPOs). *See also* Group Policy Preferences
 - applications published and, 937
 - backing up, 338
 - container object moving and, 505
 - creating, 284
 - delegating permissions on, 335–336
 - deleting, 285
 - disabling branches of, 337
 - editing, 284–285
 - for application deployment, 934, 940–943
 - implementation order of, 282–283
 - inheritance order of, 283–284
 - IPsec boundaries and, 823–824
 - moving organizational units and, 202
 - restoring, 338–339
 - searching for, 285–286
 - Starter, 286–288
 - Group Policy Preferences, 288–335
 - as Group Policy component, 282
 - Drive Maps, 291–293
 - Environment, 293–294
 - Files, 294–295
 - Folders, 296–297
 - for Control Panel, 306–335
 - data sources in, 306–307
 - devices in, 307–312
 - Internet settings in, 312–314
 - Local Users and Groups in, 314–317
 - Network Options in, 317–320
 - Power Options in, 320–321
 - printers in, 322–326
 - Regional Options in, 326–327
 - Scheduled Tasks in, 327–329
 - Services in, 330–331
 - Start Menu in, 331–333
 - targeting items in, 333–335
 - Ini Files, 297–298
 - Network Shares, 298–300
 - options for, 305–306
 - overview of, 288–291
 - Registry, 300–303
 - Shortcuts, 303–305
 - Group Policy Results, 943
 - Group-Object cmdlet, 396
 - Groups, 197–213
 - Admin, 543
 - Allowed RODC Password Replication, 497
 - Backup Operators, 543
 - built-in domain local, 210–212
 - built-in global local, 212–213
 - built-in local, 208–210
 - creating, 204–205
 - deleting, 205
 - Denied RODC Password Replication, 497
 - Domain Admins, 380, 476
 - Enterprise Admins, 476
 - folder redirection and, 340–341
 - for Distributed File System (DFS) replication
 - in branch offices, 275–277
 - management of, 270, 278–280
 - multipurpose, 277–278
 - overview of, 271–272
 - for guests, 209
 - for security, 795–796
 - Full Control permission to, 244
 - in Control Panel, 314–317
 - in Terminal Services Manager, 1028–1030
 - organizations units for, 200–202
 - permission assigned to, 247
 - RADIUS server, 807, 829
 - Remediation Server, 832
 - remote access users, 888
 - Resultant Set of Policy and, 343
 - scopes of, 198–200
 - shadow, 781
 - strategy for, 202–203
 - users added to, 205–208
 - users rights and, 216–217
 - Guests, group for, 209
- ## H
- Handler Mappings, IIS, 1084
 - Hard disk space, 474
 - Hard faults, 1110
 - Hard links, 906–907
 - Hard quotas, 661
 - Hardware
 - failures of, 1118–1119
 - RAID for, 621–622, 671
 - virtualization and, 980–984
 - Hardware abstraction layer (HAL), 1204
 - Hardware Data Execution Protection (DEP), 964
 - Hash rules, for software restriction, 956, 958
 - Hashtables, in PowerShell, 424
 - Head utility, from UNIX, 464–466
 - Health and diagnostics
 - modules, in IIS, 1064
 - Health Policy, for NAP, 804–808, 818–819
 - Health Registration Authority
 - role, 814–815, 817–818
 - Here strings, in PowerShell, 420–421
 - High Security level, 767
 - HIPAA (Health Insurance Portability and Accountability Act), 800
 - History, of tasks, 378
 - Hives, Registry, 1208–1209, 1216
 - HKCR tree, in Registry, 1203
 - HKLM HARDWARE Registry subkey, 1203–1204

- HKLM SAM Registry subkey, 1204
 - HKLM SECURITY Registry subkey, 1204
 - HKLM SOFTWARE Registry subkey, 1205
 - HKLM SOFTWARE
 - Wow6432Node Registry subkey, 1205
 - HKLM SYSTEM
 - CurrentControlSet, 1205–1206
 - HKLM SYSTEM
 - MountedDevices, 1206
 - Home folders, 228–229
 - Host Bus Adapter (HBA), 672, 674
 - Host headers configuration, 1087–1088
 - Hosts
 - DNS server records for, 603
 - firewalls of, 748
 - NLB cluster and, 716
 - servers of, 672
 - Windows Communication Foundation (WCF), 742
 - Hot backups, 575
 - Hotfixes, 834
 - Hot-swap and hot-spare drives, 621, 1186, 1189
 - HP Array Configuration Utility
 - Command Line Interface (HPACUCLLEXE), 1187
 - HPC (high performance computing) clusters, 740–742
 - HTTP downloads, 446
 - HTTP modules, in IIS, 1064
 - HTTP redirection, 1075
 - HTTP settings for servers, 1074–1076
 - HTTP URLs, 20
 - HTTP.sys, 1061–1063
 - Hub and spoke replication
 - topology, 263, 273, 275, 277
 - Hybrid cluster infrastructure, 702
 - HyperSnap screen capture utility, 1000
 - Hypertext Markup Language (HTML), 16
 - Hypertext Transfer Protocol (HTTP), 16
 - Hyper-V virtualization, 86
 - alternatives to, 1002–1003
 - initial configuration for, 968–974
 - installation of, 965–968
 - overview of, 962–965
- I**
- IDE controllers, 980, 986
 - IDE VHD, 977
 - Identity management, for UNIX, 914, 923–932
 - Identity mapping, 917
 - IEEE 802.x standards, 802, 827–830, 848, 850
 - Images
 - additions of, 69–71
 - corruption of, 74
 - Windows Image (WIM) files for, 53
 - Immediate and proper response, rule of, 751
 - Immediate Tasks, 329
 - Impersonation, 190, 1090
 - Import-Clixml cmdlet, 430
 - Import-Csv cmdlet, 396, 430
 - Importing
 - media pools, 690
 - quotas, 645–646, 663
 - Registry data, 1214–1215
 - Starter GPO, 288
 - templates, 1122
 - virtual machines, 1000–1002
 - Incoming Forest Trust Builders
 - domain group, 211
 - Independent Computing Architecture (ICA) protocol, 1038
 - Independent software vendors (ISVs), 704
 - Indigo service-oriented framework, 1062
 - Inf settings, 298
 - Information Technology Infrastructure Library (ITIL), 62, 1175
 - Infrastructure Operations
 - Master roles, 84, 564, 566
 - Inheritance
 - as security feature, 21–22
 - file resources and, 245–246
 - of Group Policy Objects, 283–284
 - vulnerability, 758
 - Ini Files, 297–298
 - Initial Configuration Tasks
 - Wizard, 61, 775
 - closing, 118–119
 - computer settings and, 99
 - hardware configuration and, 98
 - server customizing and, 112–113, 116–117
 - update and feedback settings of, 106
 - update downloading and, 112
 - Initialize And Convert Disk Wizard, 623
 - Initialize TPM Security
 - Hardware Wizard, 777
 - Inject-eject port timeouts, for libraries, 694
 - Input box creation, 405–406
 - Install from media (IMF), 486–487
 - Install Windows Wizard, 55–56, 92, 774, 1172
 - Installation. *See* Windows Server 2008, installing
 - Installutil.exe command line tool, 414
 - Instances, 523–527
 - Integrated Device Electronics (IDE), 618
 - Integrated disk caching, 621
 - Integration Services, for virtualization
 - Integrity principle of security, 747
 - Intel processors, 962
 - IntelliMirror, 934–935, 959

- Interactivity, PowerShell, 390–391
- Interconnects, networks as, 719
- Internal virtual networks, 969
- International Organization for Standardization
 - Electrotechnical Commission (ISO-IEC), 15
- International
 - Telecommunications Union (ITU), 15, 555–557
- Internet Assigned Numbers Authority (IANA), 811
- Internet Authentication Service (IAS), 807, 848
- Internet Explorer, 312–314, 657, 747, 753, 863, 868
- Internet Explorer Enhanced Security Configuration (IE ESC), 780
- Internet Group Multicast Protocol (IGMP) support, 718
- Internet Information Server 6, 841–842
- Internet Information Services (IIS), 908, 1061–1104, 1195
 - administration tools for, 1068–1073
 - AppCmd.exe as, 1071–1072
 - IIS Manager as, 1068–1070
 - Windows Management Instrumentation as, 1073
 - architecture of, 1062–1065
 - delegation and permissions in, 1094–1099
 - configuration store and, 1098–1099
 - for content management, 1097–1098
 - for site and application management, 1095–1097
 - shared configuration and, 1099
 - Directory Services and, 16
- FTP Publishing Service
 - installed by, 1100–1103
- installing, 1065–1067
- remote administration by, 1099–1100
- server management by, 1073–1084
 - HTTP settings for, 1074–1076
 - monitoring in, 1081–1082
 - performance optimization in, 1081
 - request processing in, 1082–1084
 - Web application
 - development settings for, 1076–1080
- site management by, 1084–1093
 - application pool
 - configuration in, 1086–1087
 - binding adding in, 1086
 - host headers configuration in, 1087–1088
 - security configuration in, 1088–1093
 - site adding in, 1084–1086
 - site viewing in, 1084
 - stopping and starting, 1088
- virtual directories
 - management by, 1094
- Web applications
 - management by, 1093–1094
- Internet Information Systems
 - IUSRS group, 209, 211
- Internet protocol address
 - resource type, 722
- Internet Protocol security (IPsec), 473, 674, 680, 747
- Internet Security and Acceleration (ISA) server, 961
- Internet settings, on Control Panel, 312–314
- Internet Storage Name Server (iSNS), 126
- Interoperability, 903–932
 - MacIntosh, 932
 - Network File System, 912–923
 - legacy user name mapping for, 914–916
 - server for, 916–923
 - UNIX, 903–912
 - connectivity for, 908
 - file listings for, 904–906
 - file systems for, 910–911
 - file transfer protocol for, 908
 - identity management for, 923–932
 - permissions and security for, 904
 - printing for, 912
 - privilege levels for, 907–908
 - symbolic links for, 906–907
 - Telnet for, 909–910
- Intersite Messaging, 539
- Intersite replication, 514
- Inter-Site Transport container, 515, 518, 521
- Intrasite replication, 513–514
- Intrusion-detection sensors, 756
- Inventorizing libraries, 693–694
- Invoke-Expression cmdlet, 396, 420
- IP addresses, 573
 - DHCP scope and, 583–589
 - for Server Core, 151–152
 - range and exclusions of, 576
- IP packet filtering, 875–877
- IP security (IPsec), 800, 802, 819–821. *See also*
 - Network Access Protection (NAP)
- ipconfig command, 391
- IPCS special share, 255
- IPsecurity (IPsec), 785
- ISAPI (Internet Server Application Programming Interface) filters, 1083, 1091
- iSCSI
 - failover clustering and, 1190

- Gigabit Ethernet switch and, 672
 - iSNSClusRes resource type for, 722
 - network considerations for, 673–674
 - security for, 679–680
 - Storage Manager and, 675, 677
 - support for, 670
 - targets of, 678–680
 - ISO 27002, 800
 - ISO Name Registration Authority, 556
 - Isolation, 824, 1102–1103
 - Itanium-Based Systems, 85
- J**
- Job Scheduler, HPC, 742
- K**
- Kaizen, in disaster planning, 1140–1141
 - Kerberos authentication, 21, 33, 359, 508, 747
 - Kerberos Key Distribution Center (KDC), 539
 - Kernel mode, 82
 - Keys, Registry
 - data-based, 1208
 - deleting, 301
 - removal of, 1214
 - renaming, 1216
 - search of, 1212–1213
 - security of, 1217–1219
 - updating, 301
 - volatile, 1208
 - Knowledge Consistency Checker (KCC), 513–514, 516–517
 - Korn Shell scripts, 385
- L**
- LAN switch, 672
 - Language, 326–327, 377
 - LanMan hashes, 797
 - Laptops, scopes supporting, 589
 - Layer 2 Tunneling Protocol (L2TP), 848, 877
 - Layers, security, 755–756
 - Ldp.exe tool, 527–528
 - Lease durations, for networks, 589
 - Least privilege security theory, 241–242, 749, 760
 - Legacy hardware and software, 40, 44, 86
 - Legacy network adapters, 980, 984
 - Legacy user name mapping, 914–916
 - Libraries, removable storage and, 691, 693–695
 - Licenses, 470–471, 1014–1015, 1027, 1038, 1042–1044
 - Lightning strikes, 1179
 - Lightweight Directory Access Protocol (LDAP), 15, 19–20, 34, 468. *See also* Active Directory Lightweight Directory Services
 - Line -of-business applications, 493
 - Line Printer Remote (LPR) printer ports, 173
 - Linked Group Policy Objects, 283
 - Link-local addresses, 101
 - Links
 - hard, 906–907
 - in user profiles, 231
 - Mklink command for, 906–907
 - symbolic, 906–907
 - Linux systems, 435, 573, 722, 803
 - Load balancing, 8, 724–725, 850, 939, 1006. *See also* Network load balancing clusters
 - Load shedding, 725
 - Local Group Policy Editor, 365
 - Local groups, 208–210
 - Local profiles, 232
 - Local Security Policy console, 349
 - Local service account, 766
 - Local settings folder, in user profiles, 231
 - Local system account, 766–767
 - Local System Authority (LSA) subsystem, 19
 - Local user accounts, 221–222
 - Local user profiles, 230, 232
 - Location tracking, 169–172
 - Location-naming convention, for printers, 167–168, 170
 - Logical drives, 474, 616, 631
 - Logical operators, in scripts, 424
 - Logical Units (LUNs), 681–689
 - assigning, 684–687
 - description of, 673
 - extending, 687–689
 - full format of new volumes on, 687
 - in Provision Storage Wizard list, 683
 - MPIO software and, 677
 - Storage Manager node for, 675
 - types of, 682–683
 - Logical volume, 616
 - Logon events, 360
 - Logon rights, 213–216
 - Logon scripts, 176, 236
 - Logs
 - applications and services, 370–371
 - audit, 575
 - circular, 544
 - data, 1129–1131
 - destination, 373
 - Edb.log transaction, 536
 - event, 209, 211, 375–377
 - Internet Information Service (IIS), 1082
 - of Distributed File System events, 279
 - Performance, 209, 211
 - Performance Log Users and, 1114, 1120, 1125–1126

- PowerShell to check, 453–455
- Resultant Set of Policy mode
 - for, 343
- rotating, 460
- transaction, 541
- Windows, 370
- Loopback processing, 342
- Looping statements, in
 - PowerShell, 429–430, 434

M

- MAC (Media Access Control)
 - addresses, 591, 983
- Machine key encryption, 1078
- machine.config files, 1098
- MacIntosh interoperability, 932
- Majority Node Set (MNS)
 - cluster infrastructure, 702, 704
- Mandatory user profiles, 230, 235
- mapadmin.exe command line
 - tool, 915
- .maphosts file, 915
- Master Boot Record (MBR)
 - partition style, 625
- Mean time to failure, 1176–1177
- Mean time to recover, 1176–1177
- Measure-Object cmdlet, 396
- Media
 - physical, 695–696
 - pools of, 690, 695
 - removable storage
 - identification of, 691
 - robotic libraries of, 690
 - states of, 691–693
- Members, definition of, 399
- Memory
 - Complete Memory Dump
 - option for, 1145
 - failures of, 1118
 - on Reliability and
 - Performance Monitor, 1110–1111
 - PowerShell to check, 455–456

- virtualization and, 979, 984–986
- Memory Manager, 9
- Message Passing Interface (MPI), 741–742
- Message Queuing, 126
- Message routing, 511
- Messaging Application
 - Programming Interface (MAPI), 19
- Methods, definition of, 399
- Microsoft Advanced Server
 - technology, 911
- Microsoft Baseline Security Analyzer, 846
- Microsoft Data Protection
 - Manager 2007, 385
- Microsoft Exchange 2003, 613
- Microsoft Exchange Server
 - 2007, 385, 511, 553, 1152
- Microsoft iSCSI Initiator
 - Control Panel tool, 677
- Microsoft Management Console (MMC), 353–381, 841–842
 - AT command and, 378–379
 - auditing AD DS objects in, 363–366
 - auditing categories and, 358–362
 - account logon events in, 358–359
 - account management and, 359
 - directory service access in, 359–360
 - logon events in, 360
 - object access in, 360–361
 - policy change in, 361
 - privilege use in, 361
 - process tracking in, 361–362
 - system events in, 362
 - auditing directory service events in, 362–363
 - auditing enabling by, 367–370
 - auditing policy and, 357–358
 - distributing, 356

- event logs and, 375–377
- Event Viewer and, 370–375
 - applications and services
 - logs in, 370–371
 - custom views of, 371–372
 - forwarding and collecting events in, 372–373
 - on remote computer, 374
 - subscriptions in, 373–374
 - task running and, 375
 - Windows logs in, 370
- global audit policy in, 366–367
- New Taskpad View Wizard
 - for, 355–356
- options for, 353–354
- remote administration with, 356–357
- Server Core administration
 - and, 4
 - snap-ins to create, 354–355
 - task delegation with, 380–381
 - Task Scheduler and, 377–378
- Microsoft MPIO Multipathing
 - Support for iSCSI, 675
- Microsoft Operations
 - Framework (MOF), 62, 1175
- Microsoft Operations Manager (MOM) 2007, 385
- Microsoft Product Support
 - Services, 834
- Microsoft Report Viewer, 842
- Microsoft Security Response
 - Center (MSRC) Bulletin Severity Rating system, 805
- Microsoft Solution Accelerator
 - for Business Desktop Deployment (BDD), 959
- Microsoft SQL Server 2008, 385
- Microsoft System Center
 - Configuration Manager (ConfigManager), 933, 935–936
- Microsoft Virtual Machine
 - Manager 2007, 385
- Microsoft Virtual Server, 840, 848, 963

- Microsoft Windows HPC Server 2008, 385
- Migration, 47
- MIME (Multipurpose Internet Mail Extensions) types, 1076
- Mirror
 - hardware and software, 1183, 1185
 - SAN, 683
 - volume, 617, 622, 633, 635, 637-641
- Mission-critical applications, 703-704
- Mixed naming convention, 29
- Mklink command, 906-907
- Mobile systems, 589, 800-801.
 - See also* Remote access
- Modified Field Modification (MFM) disk
 - management, 618
- Modules, IIS, 1063-1065, 1083
- Monitoring, IIS, 1081-1082
- Mounted volumes, 631
- Mounting media, 695-696
- Mountvol.exe command line tool, 623
- Move-Item cmdlet, 397
- MPICH2 specification, of
 - Argonne National Laboratory, 742
- MS Blaster worm attack, 763-764, 799-800
- MS-AD LDS-Display
 - Specifiers.ldf file, 529
- MS-CHAP v2, 888
- .msi files, 1053-1056
- Mstsc.exe command line tool, 427
- Multicast mode, network
 - adapters in, 708, 718
- Multicast scopes, 586
- Multimaster replication system, 14, 513, 561
- Multipath IO (MPIO) software, 674, 677
- Music folder, in user profiles, 231
- My Group, in Terminal Services, 1028-1030
- N**
- Names
 - common (CNs), 18
 - computer, 103-106
 - conventions for, 68, 219
 - Database System, 1130
 - default domain NetBIOS, 486
 - Default-First-Site, 512, 515
 - distinguished, 18-19
 - duplication of, 71
 - for user accounts, 218
 - for virtual private network (VPN) connections, 882
 - formats for, 20
 - Fully Qualified Domain (FQDN), 713
 - group, 202-203
 - legacy user mapping for, 914-916
 - NetBIOS, 256, 926
 - Network Name resource and, 726
 - of domains, 479
 - of printers, 166-168
 - PowerShell for renaming files and, 460-461
 - publicly resolvable DNS, 859
 - Registry key and value, 1216
 - relative distinguished (RDNs), 18
 - renaming user accounts and, 226
 - resolution of, 16, 30-32
 - universal principal (UPN), 807-808
 - User Name Mapping Server for, 239
 - User Principal, 509-510
 - World Wide (WWN), 677
- Namespaces. *See also*
 - Distributed File System (DFS); Domains
 - .NET Framework and, 399
 - client for, 261
 - contiguous, for zones, 603
 - DFS Publishing page for, 739
 - in Active Directory, 16
 - management of, 270
 - planning, 25-32
 - contiguous, 37
 - for trees and forests, 26-27
 - name resolution in, 30-32
 - naming convention in, 27-29
 - polling settings for, 270-271
 - root for, 265-266
 - server for, 260-261, 266-267
 - terminology for, 258
- Naming contexts, 22
- Navigation toolbar, in IIS, 1069
- .NET Framework
 - compilation in, 1076
 - globalization in, 1077
 - performance counters access by, 457
 - PowerShell and, 398-402
 - trust levels in, 1077
 - version 2.0 of, 841-842
- Net session command line tool, 256
- Net Share command line tool, 256
- Net view command line tool, 256
- NET.MSMQ protocol listener, 1062
- NET.PIPE protocol listener, 1062
- NET.TCP protocol listener, 1062
- NetBIOS (Network Basic Input-Output System) names, 14, 256, 486, 926. *See also* Windows Internet Naming Service (WINS)
- netdom command-line tool, 152
- NetHood folder, in user profiles, 231
- NETLOGON special share, 255
- netsh command line tool, 151, 156, 392, 595, 793-795
- Network Access Protection (NAP), 10, 759, 799-832
 - certificate server for, 809-818

- Group Policy management
 - console and, 816–818
 - NAP server and, 813–816
 - set up of, 809–813
 - client settings for, 819–826
 - IPsec boundaries for, 823–826
 - IPsec enforcement enabling in, 819–821
 - on workstations, 821–823
 - deployment planning for, 801–804
 - deployment politics and, 830–832
 - Health Policy for, 804–808
 - Health Policy server for, 818–819
 - IEEE 802.x standard and, 827–830
 - need for, 799–801
 - Secure Sockets Tunneling Protocol (SSTP) versus, 850
- Network Access Quarantine Control (NAQ), 800
- Network Access Translation (NAT) devices, 573, 871
- Network and Sharing Center, 883
- Network Attached Storage (NAS), 651, 671. *See also* Storage
- Network Configuration
 - Operators group, 209, 211
- Network File System (NFS), 43.
 - See also* File resources
 - as resource type, 722, 737
 - folders for, 239
 - legacy user name mapping for, 914–916
 - mounted volumes and, 631
 - server for, 916–923
 - client configuration for, 923
 - configuring, 921–922
 - NFS share connection to, 922
 - NFS share on, 917–921
 - UNIX systems and, 240, 910
- Network Information System (NIS), 923–924, 926
- Network interface cards (NICs), 706, 741, 964
- Network Load Balancing (NLB), 8, 1006
- Network load balancing clusters
 - capacity of, 716–717
 - concepts of, 706–707
 - creating, 709–716
 - fault tolerance and, 717, 1189–1190
 - for redundancy, 703
 - models of, 707–708
 - optimizing, 717–718
 - overview of, 700
- Network Name resource, 726
- Network Policy Server (NPS), 807
 - for Terminal Services, 1007, 1018
 - network policy configuration for, 887–889
 - overview of, 848
 - per user configuration for, 887
 - planning for, 848–849
 - wireless deployment of
 - remote access and, 890
- Networks. *See also* Remote access; Virtualization
 - AD DS installation
 - prerequisites for, 475
 - boot failure from distribution
 - points of, 72–74
 - chokepoints in, 755
 - configuring, 101–103
 - Control Panel options for, 317–320
 - DHCP and, 574–576, 592
 - documenting, 42–45
 - failover clusters and, 719
 - Group Policy Preferences and, 298–300
 - IP addresses and, 518
 - iSCSI and, 673–674
 - lease durations for, 589
 - on Reliability and Performance Monitor, 1110
 - patch testing for, 839–840
 - performance of, 199
 - print server clusters on, 191
 - printers and, 169–170, 174–175
 - security for, 746
 - service account for, 766
 - site-aware services for, 511
 - slow connections of, 342
 - storage network switch and, 672
 - Terminal Services need for, 1010
 - troubleshooting, 191
 - virtual private, 473, 747–748
 - virtualization and, 991
 - WDS settings for, 69
 - Windows Server Update Services (WSUS) settings for, 844
 - wireless, 473
 - zone rules for software restriction in, 956, 958
- New Connection Security Rule Wizard, 825
- New Namespace Wizard, 265–266
- New Replicated Folder Wizard, 280
- New Replication Group Wizard, 275, 277
- New Scope Wizard, 585, 587
- New Taskpad View Wizard, 355–356
- New Virtual Machine Wizard, 974–975, 978, 990
- New Volume Wizard, 627
- New-Alias cmdlet, 397
- New-Item cmdlet, 397
- New-Itemproperty cmdlet, 397
- New-Object cmdlet, 397
- New-Variable cmdlet, 397
- Nfsmgmt.msc management
 - console, 916
- No auditing events, 358

- No topology option, for replication topology, 273
 - Node Template Generation Wizard, 741
 - Nodes, in failover clusters, 719
 - Non Sensitive Privilege Use, 361
 - Nonauthoritative restore, 546, 548–550
 - Nonredundant storage, 631
 - Normal mode, of Active Directory Users and Computers, 500–501
 - Notification
 - area icon for, 7
 - standard escalation procedures for, 1139
 - thresholds for, 662
 - NT LAN Manager (NTLM) authentication, 747
 - Ntbackup.exe, 1148–1149
 - Ntds.dit file, 474
 - Ntdsutil.exe command line tool
 - for AD DS database moving, 541
 - for domain controller removal, 546–548
 - for DRSM administrator account password, 548
 - Operations Master roles and, 566
 - NTFS volumes, 631
 - content management permissions on, 1098
 - directory quotas and, 658
 - encryption available on, 647
 - permissions for, 240–244, 736, 738
 - software distribution points and, 940
 - Ntuser file, 230, 236
- O**
- Obfuscation, security by, 780
 - Object IDs (OIDs), 556, 811
 - objectGUID attribute, 17
 - Objects
 - access to, 360–361
 - accidental deletion of, 543
 - Active Directory Domain Services, 499–503
 - Active Directory Users and Computers and, 503, 505
 - AppCmd.exe and, 1071–1072
 - auditing settings for, 368–370
 - auxiliary class of, 559–560
 - classes of, 558
 - connection, 513, 516–517
 - cross-reference, 562
 - Default-First-Site-Name, 515
 - definition of, 399
 - in Active Directory, 17
 - Password Setting, 748
 - permissions applied to, 249
 - replication, 515
 - server, 513, 516–517
 - site, 515–516
 - site link, 518–520
 - site link bridge, 520–521
 - structural class of, 559–560
 - subnet, 512, 517–518
 - System String
 - taking ownership of, 250–251
 - tombstones as, 537
- Oclist.exe command line tool, 444
- Ocsetup.exe command line tool, 157, 160
- ODBC manager, 1130
- Offline defragmentation, 540–541
- OLE class identifiers, 945, 1202
- One-time passwords, 784
- Online Crash Analysis (OCA), 111
- Online defragmentation, 537–538
- On-media identifiers, 691
- Open Database Connectivity (ODBC), 306
- Open With preference items, 310–311
- Operating system
 - compatibility of, 477–478
 - connectivity of, 43
 - network, 44
 - recovery of, 1171–1173, 1233–1234
- Operational events, 371
- Operations masters roles
 - managing, 561–564
 - seizing, 566
 - transferring, 564–565
- Operator requests, removable storage and, 696–697
- Operators, in PowerShell, 424–425, 441
- Organizational naming convention, 28
- Organizational units (OUs)
 - Active Directory and, 16, 18
 - Active Directory Users and Computers creation of, 498–499
 - domains versus, 33–34, 36
 - for groups, 200–202
 - Group Policy Objects of, 283
 - restoring hierarchy of, 552
 - server core installation and, 152
 - task delegation to, 380
- Original equipment manufacturers (OEMs), 704
- Out Of Box Experience (OOBE), 97
- Outlook 2003, 837
- Output caching, in IIS, 1081
- Overhead network traffic, 43
- Ownership, 244, 250–252
- P**
- Packages, software
 - management, 947–955
 - application properties changes and, 950–952
 - Group Policy and, 947–950
 - modifications to, 953–955
 - removing and redeploying, 955
 - upgrades for, 952–953
 - Packet filtering, 875–877
 - Page faults, 1110
 - Page table entries (PTEs), 1009
 - Param statement, in PowerShell, 436–438

- Parameters, in PowerShell, 391, 412–414, 440–441, 457, 464
- Parent disks, 988–989
- Parent partitions, 962, 964
- Partial failover, 725
- Partitions, 625–641
 - Active Directory Lightweight Directory Services and, 523–526
 - BitLocker, 774
 - creating, 626–631
 - definition of, 616
 - directory, 483, 490, 522, 524, 561–562
 - drive options for, 59–60
 - dynamic disk conversions and, 631–632
 - extended, 616
 - GPT disk conversions and, 632–633
 - home folders on, 229
 - Hyper-V, 962, 964
 - in Active Directory, 22
 - logical drives on, 631
 - MBR versus GPT, 625
 - mirror volume and, 637–641
 - NTFS, 81
 - parent, 962, 964
 - primary, 616
 - volume size changes and, 633–637
- Passphrase, 220
- passthru parameter, in PowerShell, 464
- Password Setting Objects (PSOs), 748, 781, 783–784
- Passwords
 - dictionary attacks on, 779
 - domain local groups and, 210–211
 - DRSM administrator account, 548
 - for users accounts, 219–220
 - in scripts, 451
 - one-time, 784
 - policies for
 - domain, 781–784
 - fine-grained password, 6
 - overview of, 680, 780
 - replication, 496–498
 - standalone server, 781
 - resetting, 227
 - rules for, 219–220
 - strong, 483
 - synchronization of, 923–924
 - theft of, 746
 - USB Flash drive for saving, 777
- Patch management, 833–846
 - cycle of, 835–839
 - assessment phase in, 836
 - deployment phase in, 838
 - evaluation phase in, 838
 - identification phase in, 836–838
 - repeat phase in, 839
 - deployment testing in, 839–841
 - importance of, 834–835
 - terminology in, 833–834
 - third-party products for, 845–846
 - update obtaining in, 841–845
 - automatic, 841
 - Systems Center Configuration Manager for, 845
 - Windows Server Update Services for, 841–845
- Path rules, for software restriction, 956, 958
- Path-to-page name form, 20
- PDC Emulator Operations
 - Master roles, 563–564, 566
- Peak usage for quotas, 660
- Per-computer connections, 176
- PerfectDisk (Raxco), 88
- Performance. *See also* Reliability and Performance Monitor
 - counters for, 456–458
 - fault tolerance and, 1188–1189
 - HPC (high performance computing) clusters and, 740–742
 - IIS modules for, 1065
 - network, 199
 - of print servers, 187–188
 - of SANs with iSCSI protocol, 673–674
 - optimization of, 1081
 - storage and, 657
- Performance Log Users group, 209, 211
- Perl scripts, 385
- Permissions. *See also* Authentication
 - AD DS installation
 - prerequisites for, 476
 - assignments of, 247
 - delegating, 270, 335–336
 - Delegation Of Control Wizard and, 380
 - Encrypting File System (EFS) and, 649
 - explicit, 284
 - file, 240–242
 - folder, 246–247
 - for printers, 182
 - for UNIX interoperability, 904–905
 - in ASP.NET code access policy, 1077
 - in Internet Information Services (IIS)
 - configuration store and, 1098–1099
 - for content management, 1097–1098
 - for site and application management, 1095–1097
 - shared configuration and, 1099
 - limiting, 760
 - NTFS, 242–244, 736, 738, 940
 - Operations Master roles and, 561
 - operations of, 244–245
 - registry key security and, 1217–1219
 - share, 240, 252
 - special, 248–250
 - user rights and, 213

- Persistent usage policies, 470
- Personal digital assistants (PDAs), 589
- Personal identification number (PIN), 773
- Personalization data, 469
- Per-user connections, 176
- Per-user quotas, 643–645
- Per-user rules, for Windows Firewall, 785
- Phishing attacks, 747
- Physical disks, 726
- Physical states, of media, 692
- Physical to virtual (P2V) conversions, 86
- Pictures folder, in user profiles, 231
- Pipeline, PowerShell, 387, 438–439
- Plain-text e-mail handling, 837
- Plug and Play Manager, 1204
- Point-to-Point Tunnelling Protocol (PPTP), 848, 877
- Poisoning attacks, on DNS, 602
- Popup creation, 405–406
- Ports, 464, 992–994
- POSIX compliance, 928
- Power supply, 1177–1182
 - local failure of, 1178–1179
 - long-term outages in, 1182
 - short-term outages in, 1182
 - voltage variations in, 1179–1181
- Power users, 209, 1009
- Power, Control Panel options for, 320–321
- PowerShell, 904
 - as server feature, 126
 - backup scheduled by, 1147
 - basics of, 386–390
 - Cmd.exe commands and, 391–392
 - cmdlets in, 394–398
 - compressing files and, 447
 - configuring, 113–115
 - console input and, 450–451
 - data display in, 410–412
 - dates and, 447–449
 - DHCP administration and, 595
 - disk space usage checking with, 458–459
 - elapsed time and, 449–450
 - error avoidance in, 391
 - file or directory existence testing in, 443–444
 - file system tasks in, 442–443
 - File Transfer Protocol (FTP) and, 445
 - Flexible Single Master Operations (FSMO) identification by, 83–84
 - Get-Command cmdlet in, 406–408
 - Get-Help cmdlet in, 407–409
 - Get-Member cmdlet in, 407, 409–410
 - HTTP downloads and, 446
 - installation of, 541
 - interactivity in, 390–391
 - memory and CPU information and, 455–456
 - multiple targets and, 462–463
 - open port checking with, 464
 - overview of, 5, 384
 - parameters in, 412–414
 - performance counters access with, 456–458
 - Registry and, 459, 1219
 - renaming files with, 460–461
 - rotating logs with, 460
 - scheduling tasks with, 461–462
 - scripting in, 414–442
 - .ps1 script creation in, 415–417
 - arrays in, 422–423
 - comments in, 417–418
 - conditional statements in, 426–429
 - dot-sourcing in, 434–435
 - error handling in, 439–441
 - escaping characters in, 442
 - exiting from, 434
 - flow control in, 431–432
 - formatting cmdlets for, 433–434
 - From and To files in, 430–431
 - functions in, 425–426
 - hashtables in, 424
 - here strings in, 420–421
 - looping statements in, 429–430
 - operators in, 424–425
 - overview of, 414–415
 - param statement in, 436–438
 - passing arguments to, 435–436
 - pipeline in, 438–439
 - redirection operators in, 441
 - scope of, 418–419
 - strings in, 419–420
 - type accelerators in, 441–442
 - variables in, 418
 - wildcards and regular expressions in, 421–422
 - secure information storage and, 451
 - server backup cmdlets in, 444
 - Server Core management with, 444
 - server support of, 385
 - service and process checking with, 451–453
 - SMTP e-mail and, 446–447
 - snap-in for, 414
 - UNIX utilities and, 464–466
 - user credentials for, 393
 - Windows Event Log checking with, 453–455
 - Windows infrastructure for, 398–406
 - .NET Framework in, 398–402
 - Component Object Model (COM) in, 405
 - popup and input boxes created in, 405–406

- Windows Management
 - Instrumentation (WMI)
 - in, 402–404
 - Windows Remote Management (WRM) in, 404–405
 - XML and, 445, 463
 - PPP authentication, 852
 - Pre-boot Execution
 - Environment PXE server, 64–65
 - Preferred DNS Server setting, 481
 - Preventative action, rule of, 750, 752
 - Preventative maintenance (PM) program, 1182
 - Pre-Windows 2000 Compatible
 - Access domain group, 211
 - Primary domain controllers (PDCs), 16
 - Primary partition, 616
 - Primary zones, 598, 600–601
 - Principal name suffix, 218
 - Principal, in ACEs, 21
 - Print Operators group, 209, 211
 - Printer Migration Wizard, 172–173, 190
 - Printers, 165–195
 - Active Directory Users and Computers and, 504–505
 - availability of and group priorities for, 182–184
 - command line management for, 181
 - creating print server for, 168–169
 - deploying, 166–168
 - drivers for, 188–189
 - Group Policy for deploying, 176–179
 - installing, 174–175
 - job management for, 179–181
 - location tracking for, 169–172
 - MacIntosh interoperability and, 932
 - migrating servers for, 172–174
 - on Control Panel, 322–326
 - pools of, 189–190
 - print spooling and, 185–187, 721–722
 - security for, 182
 - separator pages for, 184–185
 - server failure and, 190–191
 - server performance and, 187–188
 - shared, 255
 - Terminal Services Easy Print for, 7, 1006
 - troubleshooting, 191–195
 - UNIX interoperability and, 912
 - WMI to install, 403–404
 - PrintHood folder, in user profiles, 231
 - Private networks, 719
 - Private profile, for Windows Firewall, 785–786, 824
 - Private virtual networks, 970
 - Private-key security, 21
 - Privileges
 - account lockout policies and, 6
 - applications installed with, 936
 - auditing and, 361
 - rule of least, 241–242, 749, 760
 - UNIX interoperability and, 907–908
 - Process Monitor, 457–458
 - Product Identification (PID) code, 53–54
 - Productivity, availability and, 748
 - Profiles. *See also* Users
 - for Windows Firewall, 785–786, 824
 - PowerShell default scripts for, 389
 - Promotion, of domain controllers, 473
 - Properties, definition of, 399
 - Protected Extensible Authentication Protocol (PEAP)-CHAP v2, 848, 888, 890–893, 896–898
 - Protocol listeners, 1062
 - Provider, PowerShell, 387
 - Provision A Shared Folder Wizard, 252, 918–920
 - Provision Storage Wizard, 681, 683, 685
 - Provisioning
 - SANS and, 671
 - Proxy settings, for WSUS, 844
 - .ps1 script creation, 415–417
 - Public key infrastructure (PKI)
 - Active Directory Certificate Services and, 473
 - best practices for, 803
 - remote access deployment and, 888
 - SMTP site links and, 519
 - Windows Server-based, 856, 868
 - wireless remote access deployment and, 889
 - Public networks, 719
 - Public profile, for Windows Firewall, 785–786, 824
 - Public-key security, 21
 - Pulse Frequency Modulation (PFM) disk management, 618
 - PushPrinterConnection.exe tool, 176–179
 - PXE server, 65, 68, 72–73
- Q**
- Quorum disk, 704, 727
 - Quotas
 - disk management, 641–646
 - File Server Resource Manager (FSRM), 657–663
 - for shared folders, 253
 - software distribution and, 942
- R**
- RADIUS**
- Network Policy Server (NPS) and, 1007
 - proxy for, 848
 - server for, 807, 829, 848, 889

- wireless deployment of
 - remote access for, 892–893
 - RAID (redundant array of independent disks)
 - for fault tolerance, 717, 1183–1189
 - for Terminal Services, 1011
 - in disk management, 617–622
 - in storage management, 683
 - virtualization and, 964
 - RAID-5 SAN, 683
 - RAID-5 volume, 617, 622, 630, 633, 635–636
 - RAM, for Terminal Services, 1009
 - .rdp files, 1053–1056
 - Read-Host cmdlet, 397
 - Read-only domain controllers (RODCs), 492–498
 - backup domain controller
 - role of, 16, 33
 - delegating, 493–495
 - description of, 492–493
 - installation media for, 487
 - overview of, 5
 - password replication policies in, 496–498
 - security for, 798
 - upgrades and, 83
 - uses of, 493
 - Realm trusts, 508
 - Recent folder, in user profiles, 231
 - Recovery. *See also* Troubleshooting
 - in disaster planning, 1144–1145
 - mean time to, 1176–1177
 - of servers, 1227–1236
 - applications and data in, 1231–1233
 - files and folders in, 1229–1231
 - operating system in, 1233–1234
 - system state in, 1234–1236
 - volumes in, 1227–1228
 - of services, 331
 - system, 1222, 1225–1227
 - Recovery Agent, 648
 - Recovery Wizard, 1166–1169
 - Recursion process, 610
 - Redirection
 - configuration for, 1098
 - folder, 282, 339–341
 - HTTP, 1075
 - in IntelliMirror, 934
 - in Registry, 1199
 - PowerShell operators for, 441
 - Redundancy
 - domain-based namespaces and, 259
 - HPC clusters and, 741
 - in disaster planning, 1142
 - mounted volumes for, 631
 - multiple DHCP servers for, 592–593
 - of volumes, 636, 641
 - RAID for, 617
 - secondary DNS servers for, 596
 - staff, 760
 - Web server clustering for, 703
 - Reflections for Secure IT, 909
 - Refreshing Group Policy, 337–338
 - .reg files, 1215
 - Reg.exe command line tool, 1220
 - Regedit.exe, 1217
 - Regedt32, 1211
 - Regeneration, mirror volumes and, 638–639
 - Regional Options, on Control Panel, 326–327
 - Registrars, Internet, 479
 - Registry, 1193–1222
 - backing up and restoring, 1221–1222
 - damaged, 1239
 - Group Policy Preference extensions for, 300–303
 - origin of, 1194–1195
 - PowerShell and, 459
 - Registry Editors for, 1211–1220
 - data importing and
 - exporting by, 1214–1215
 - hive loading and unloading by, 1216
 - key security and, 1217–1219
 - keys and values and, 1212–1214, 1216
 - overview of, 1211–1212
 - Reg.exe in, 1220
 - Regedt32 and, 1211
 - remote connection by, 1216
 - value contents editing by, 1213
 - Registry Wizard for, 1209–1210
 - structure of, 1198–1209
 - data storage in, 1206–1209
 - root keys in, 1201–1203
 - sixty-four and thirty-two bit keys in, 1199–1201
 - subkeys in, 1203–1206
 - troubleshooting, 1226
 - use of, 1195–1196
 - virtualization of, 348–349
 - Windows Server 2008
 - changes in, 1196–1198
- Regular expressions, in PowerShell, 421–422
- Relational security, 756–759
- Relative distinguished names (RDNs), 18
- Relay agents, DHCP, 592–595, 874–875
- Reliability, 639, 671
- Reliability and Performance Monitor, 1107–1132
 - data collection managing in, 1128–1131
 - data collection scheduling in, 1126–1128
 - Data Collector set in, 1119–1126
 - manual construction of, 1123–1125
 - Performance Log Users and, 1120
 - Performance Monitor to create, 1123

- template for, 1120–1122
 - to monitor performance counters, 1125–1126
- Performance Monitor in, 1111–1115
- Reliability Monitor in, 1115–1119
- reports of, 1131–1132
- Resource View of, 1107–1111
- Remediation Server Group, 832
- Remote access, 160, 847–899
 - clustering and, 703
 - configuring, 116–117
 - disk management and, 622, 685
 - Event Viewer and, 374
 - for Reliability Monitor viewing, 1116–1117
 - Internet Information Services (IIS) for, 1099–1100
 - Microsoft Management Console (MMC) for, 356–357
 - Network Policy Server (NPS) for
 - network policy configuration for, 887–889
 - overview of, 848
 - per user configuration for, 887
 - planning for, 848–849
 - Performance Monitor for, 1115
 - policies for, 849–850
 - PowerShell and, 386, 427–429
 - Registry Editors for, 1194, 1216
 - Resultant Set of Policy and, 343
 - Secure Sockets Tunnelling Protocol (SSTP) for, 850–886
 - configuring, 852–857
 - connection clients for, 877–881
 - connection troubleshooting for, 883–886
 - connections for, 881–883
 - process of, 851–852
 - routing and remote access installation for, 868–877
 - Server Authentication certificate for, 858–868
 - Server Core management and, 4, 156
 - support for, 850
 - Terminal Services for, 1008
 - Windows Management Instrumentation (WMI) and, 455–456
 - wireless deployment of, 889–898
 - access points for, 893–894
 - for RADIUS clients, 892–893
 - overview of, 889–890
 - prerequisites for, 890–892
 - secure configuration for, 894–898
- Remote Authentication Dial-In User Service (RADIUS). *See* RADIUS
- Remote Data Protocol (RDP), 1038–1042
- Remote Desktop Protocol (RDP), 116. *See also* Terminal Services
- Remote Desktop Users group, 209, 211
- Remote Desktop Web Connection, 1057–1058
- Remote differential compression (RDC) algorithm, 257, 263, 280
- Remote Web Workplace, 1055
- RemoteApps. *See* TS RemoteApps
- Removable storage
 - libraries and, 693–695
 - media pools and, 695
 - operator requests and, 696–697
 - physical media and, 695–696
 - terminology for, 689–693
 - work queue and, 696
- Remove Access VPN
 - connections, 802
- Remove-Item cmdlet, 397
- Remdome.exe command line tool, 562
- Repair, system, 1142–1144
- Replicate Folder Wizard, 272
- Replication
 - Active Directory Sites and Services and, 511
 - domain as unit of, 34
 - DSA connections for, 19
 - multimaster, 14, 561, 608
 - objects of, 515
 - of Active Directory Domain Services, 513–514
 - of Active Directory Lightweight Directory Services, 530–531
 - of directory, 522
 - of directory partition, 483
 - of Distributed File System (DFS), 271–280
 - branch office group for, 275–277
 - folders, 272–274
 - for collaboration, 258
 - for synchronization, 258
 - groups for, 270–272
 - managing groups for, 278–280
 - multipurpose group for, 277–278
 - overview of, 262–263
 - of domain controllers, 473, 486
 - of passwords, 496–498
 - software distribution points and, 939
 - unidirectional, 492
- ReplicationSourceDC value, 159
- Replicator group, 209, 211
- Reporting mode, 830
- Reports
 - File Server Resource Manager (FSRM), 654–657
 - of Starter GPO settings, 287
 - Reliability and Performance Monitor, 1131–1132

- Request processing, in IIS, 1082–1084
- Reservations, for DHCP address, 590–591, 893
- Reserved variable, in PowerShell, 435
- Resistance to change, deployment and, 40
- Resource organizations, 472
- Resources. *See also* File resources
 - as Server Core installation benefit, 149
 - creating clustered, 732–740
 - DNS records of, 605–608
 - failover cluster types of, 720–723
 - identification of, 1135
 - Resource View for, 1107–1111
 - standard escalation procedures for, 1139
- Responses, in disaster planning, 1136–1140
- Responsibility division, for security, 759–761
- Restartable Active Directory Domain Services, 6, 538–539
- Restoring. *See also* Backing up; Disaster planning
 - Active Directory Domain Services (AD DS), 546–552
 - authoritative, 550–552
 - nonauthoritative, 548–550
 - Ntdsutil for domain controller removal in, 546–548
 - Distributed File System (DFS) folder targets, 271
 - Group Policy Objects, 338–339
 - Registry, 1221–1222
 - seeding branch member by, 277
- Restriction policies for software, 955–959
- Resultant Set of Policy (RSOP), 341–343, 943
- Resynching, mirror volumes and, 638
- Retention policy, for logs, 376–377
- Return on investment (ROI), 41, 45
- RFC 822 names, 20
- RID Operations Master roles, 562–564
- Rights Management Services, 469–472, 747
- Rights, user. *See* Users
- Risks
 - identification of, 1134–1135
 - in clusters, 705
 - in deployment, 47–48
 - UAC turn off and, 352
- Roadmap for deployment, 45–48
- Roaming profiles, 230, 232–235, 339, 935
- Robotic media libraries, 690–691, 693, 695
- Role separation, of administrators, 493
- Roles wizards, 770–772
- Roles, server. *See* Servers
- Roll Back Driver button, 1226–1227
- Rollback semantics, 474
- Rolling upgrade, 723
- Rollup, update, 834
- Root Certificate Authority, 825, 877, 889–890
- Root domains, 35, 37
- Root hints, 481
- Root keys, Registry, 1198, 1201–1203
- Root namespace, 258, 265–266
- Root users, 908
- Routing and Remote Access Service (RRAS), 868–877
- RPC Endpoint Mapper, 790–791
- RSA SecureII TFA provider, 784
- RSM View command line tool, 693
- S**
- Safe Mode, 1238
- Sags, in power voltage, 1181
- Samba SMB-based UNIX solution, 910–911
- SAN (Storage Area Network) Manager
 - advantages and disadvantages of, 671–672
 - console for, 675–676
 - installing, 674–675
 - iSCSI security for, 679–680
 - iSCSI targets for, 678–680
 - logical units (LUNs) for, 681–689
 - server connections for, 676–677
 - terminology for, 672–674
- Sarbanes-Oxley Act of 2002, 800
- Saved Games folder, in user profiles, 231
- Saving event logs, 377
- Savlik NetChk Protect updating, 111
- Scalability, 270, 700
- Scheduled Tasks
 - on Control Panel, 327–329
 - Powershell for, 461–462
 - Volume Shadow Copy Service and, 657, 723
- Schema
 - extensible, 522
 - Group Policy printer deployment and, 175
 - in Active Directory, 19–20
 - in Active Directory Domain Services (AD DS), 552–566
 - launching, 554–555
 - modifying, 553–560
 - Operations Master Roles management in, 561–566
- Schema Admins group, 83
- Schema Operations Master roles, 83, 553, 561, 564
- Scope
 - DHCP activating, 589–590

- creating, 582–589
 - group, 198–200, 206
 - in splitting address space, 592
 - of PowerShell, 418–419
- Screen capture utilities, 470, 1000
- Screening files, 663–670
 - audio and video, 664
 - creating screens for, 664–665
 - exceptions for, 666
 - file groups and, 668–670
 - templates for, 667–668
- Scripts. *See also* PowerShell
 - DiskPart.exe command line tool and, 630
 - for printer connections, 176
 - for user profiles, 236
 - generic script resource type for, 723
 - in Group Policy, 282
 - in Visual Basic, 157
 - initial Server Core
 - configuration, 153–155
 - server-side, 1077–1078
- SCSI (Small Computer System Interface), 618, 980, 986, 1003, 1011
- Searches folder, in user profiles, 231
- Searching, 13–14, 174–175
- Secondary DNS servers, 596–597
- Secondary zones, 598, 601
- Secure Shell (SSH), 909
- Secure Sockets Layer (SSL), 473, 747, 1091, 1093, 1102
- Secure Sockets Tunnelling Protocol (SSTP), 850–886
 - configuring, 852–857
 - connection clients for, 877–881
 - connection troubleshooting for, 883–886
 - connections for, 881–883
 - process of, 851–852
 - routing and remote access
 - installation for, 868–877
- Server Authentication
 - certificate for, 858–868
 - VPNs of, 848
- Secured Password (EAP-MSCHAP v2), 888, 893
- Secure-Multipurpose Internet Mail Extensions (S-MIME), 473
- Security, 745–761, 763–798. *See also* Network Access Protection (NAP); Patch management
 - access control lists (ACLs) for, 14
 - at installation, 764–767
 - default services in, 764–766
 - system account roles in, 766–767
 - auditing for, 796
 - availability principle of, 748
 - BitLocker for startup, 773–779
 - encryption enabling in, 776–778
 - features role installation in, 775–776
 - recovery with, 779
 - server data volume
 - encryption in, 779
 - volumes set up in, 773–775
 - chokepoints for, 754–755
 - Code Access Security Policy
 - for
 - confidentiality principle of, 746–747
 - connection sharing and, 882
 - delegating permissions and, 336
 - directory browsing and, 1074
 - Directory Service Changes
 - feature and, 567
 - for accounts, 779–784
 - disabling administrator account in, 780
 - domain password policies
 - for, 781–784
 - standalone server password policies for, 781
 - for domains, 35–36
 - for Dynamic Host Configuration Protocol (DHCP), 575–576
 - for Internet Explorer, 863, 868
 - for iSCSI, 679–680
 - for PowerShell, 386–387
 - for printers, 182, 190
 - for Server Core, 148, 767–769
 - for site management, 1088–1093
 - for UNIX interoperability, 904, 907, 911
 - for wireless deployment of remote access, 894–898
- forwarders and, 610
- Group Policy settings for, 282
- groups for, 795–796
- IIS modules for, 1065
- in Active Directory
 - architecture, 21–22
 - in mirror volumes, 639
 - integrity principle of, 747
 - LanMan hashes and
 - authentication for, 797
 - layers of, 755–756
 - least privilege theory for, 241–242
 - Local Security Policy console
 - for, 349
 - Local Security Policy MMC
 - snap-in for, 1120
 - Microsoft Baseline Security Analyzer for, 846
 - of certificates, 889
 - of Registry keys, 1217–1219
 - of SANs with iSCSI protocol, 673–674
 - password policies for, 680
 - read-only domain controllers
 - and, 5, 798
 - relational, 756–759
 - responsibility division for, 759–761
 - roles and features wizards
 - and, 770–773
 - rules of, 748–751
 - Schema Admins group and, 83, 554

- shared printer preference items and, 324
- SMBv2 for, 797
- software restriction policies and
- SQL Slammer worm and, 751–752
- updates for, 833, 837
- User Policy Option for, 305
- Windows Firewall for, 785–795
 - command line management of, 793–795
 - Group Policy for, 786–788
 - policy for, 791–793
 - rule basics for, 788–789
 - rule definitions for, 789–791
- Windows Server 2008
 - overview of, 9–10
- WMI to update, 403
- WPA2 wireless, 848
- zones for, 753–754
- Security access control lists (SACLs), 1194
- Security Accounts Manager (SAM), 14, 1204
- Security Functionality Triad, 746
- Security groups, 198
- Security Identifier (SID), 21, 71, 562, 914
- Security principal name (SPN), 218
- Select-Object cmdlet, 397, 464
- Select-String cmdlet, 397
- Semi-trusted (DMZ) zone, for security, 753
- SendTo folder, in user profiles, 231
- Sensitive Privilege Use, 361
- Separation, rule of, 750
- Separator pages, for printers, 184–185
- Serial Advanced Technology Attachment (SATA), 618, 621, 672
- Serially Attached SCSI (SAS), 618–619, 672, 1011, 1141, 1189–1190
- Server Authentication
 - certificate, 858–868
- Server Core, 147–164. *See also* Windows Server 2008, installing
 - backups of, 1148
 - benefits of, 148–149
 - clusters in, 702
 - Dynamic Host Configuration Protocol (DHCP) server for, 589
 - Hyper-V virtualization on, 963
 - initial configuration of, 150–160
 - activating, 157
 - desktop display resolution in, 155–156
 - domain joining in, 152–155
 - example settings for, 150–151
 - IP Address in, 151–152
 - remote management enabling in, 156
 - roles installation in, 157–160
 - installing, 4, 149–150
 - managing, 160–163
 - remote shell for, 162
 - task workarounds for, 160–161
 - Terminal Server RemoteApp for, 162–163
 - netsh command for, 794
 - PowerShell management of, 444
 - security for, 767–769
 - server role installation on, 521
 - WINS and, 574
- Server Manager
 - AD DS installation and, 476
 - Diskmgmt.msc in, 620
 - for roles and features installation, 121–122, 130
 - overview of, 8
 - printer troubleshooting and, 194
 - to add roles, 131–135
 - to add server features, 143
 - to remove roles, 136–138
 - to remove server features, 144–145
- Server Message Block (SMB), 253, 477, 910–912
- Server Message Block-Common Internet File System (SMB-CIFS) protocol, 671, 738
- Server objects, 513, 516–517
- Server operators group, 211
- Server Roles Wizard, 1065–1066
- ServerManagerCmd.exe
 - command line tool, 445, 965
- Servers, 121–145. *See also* Domain Name System (DNS); Dynamic Host Configuration Protocol (DHCP); Virtualization
 - certificates for, 1091–1092
 - data volume encryption in, 779
 - delegation of, 1095–1096
 - features of
 - adding, 143–144
 - list of, 127–129
 - removing, 144–145
 - for PowerShell, 385
 - home folders created on, 228–229
 - host, 672
 - Internet Information Services (IIS) and, 1073–1084
 - connections to, 1069–1070
 - HTTP settings for, 1074–1076
 - monitoring in, 1081–1082
 - performance optimization in, 1081
 - request processing in, 1082–1084

- Web application
 - development settings for, 1076–1080
- Internet Security and Acceleration (ISA), 961
- ISAPI (Internet Server Application Programmiing Interface), 1083
- load balancing for, 1006
- namespace, 258, 260–261, 266–267
- Network Access Policy, 848
- Network Access Protection (NAP)
 - needs for, 802–803
 - placement of, 807
 - setting up, 813–816
- Network File System (NFS)
 - client configuration for, 923
 - configuring, 921–922
 - share connection to, 922
 - share on, 917–921
- NPS on member, 808
- password policies for, 781
- PowerShell backup cmdlets for, 444
- Pre-boot Execution Environment PXE, 64–65
- print
 - creating, 168–169
 - failure of, 190–191
 - migrating, 172–174
 - performance of, 187–188
 - troubleshooting, 191–195
- RADIUS, 848
- recovery of, 1227–1236
 - applications and data in, 1169–1171, 1231–1233
 - backup catalog in, 1173–1174
 - files and folders in, 1167–1169, 1229–1231
 - operating system in, 1171–1173, 1233–1234
 - system state in, 1234–1236
 - volumes in, 1166–1167, 1227–1228
- Resource Manager for, 646
- roles of
 - adding, 131–135
 - adding services to, 139–141
 - list of, 122–126
 - removing, 135–138
 - removing services from, 141–142
 - value of, 130
- SAN (Storage Area Network)
 - Manager connected to, 676–677
 - starting and stopping, 1070
- UNIX SMB domain, 911
- User Name Mapping, 239
- virtualization and, 45
- Web, 703
- Server-side scripting, 1077–1078
- Service Level Agreements (SLAs), 110, 1175
- Service packs, 834
- Service-Oriented Architecture (SOA), 742
- Services
 - failover clusters and, 720
 - for software management, 935–939
 - generic service resource type for, 723
 - installation default, 764–766
 - logs of, 370–371
 - on Control Panel, 330–331
 - PowerShell to check, 451–453
 - status verification of, 1236–1239
- Services for UNIX (SFU), 909, 914
- Set-Alias cmdlet, 397
- Set-Content cmdlet, 397
- Set-Item cmdlet, 397
- Set-Itemproperty cmdlet, 397
- Set-Location cmdlet, 397
- Set-Variable cmdlet, 398
- Shadow command, 1036
- Shadow group, of global security group, 781
- Shadow service, 657, 723, 1169, 1231
- Share and Storage Management tool, 252–256
- Share names, 166
- Share or Publish Replicated Folder Wizard, 280
- Share permissions, 240, 252. *See also* File resources
- Shared configuration, 1099
- Shared documents folder, in user profiles, 231
- Shared Folder Wizard, 735
- Shared folders, 239, 252, 504–505
- Shared nothing clustering, 703
- Shared secret, 893
- SharePoint Server, 258, 262, 1152
- Shavlik's NetChk Protect, 846, 938
- Shortcut trusts, 508
- Shortcuts, as Group Policy Preferences, 303–305
- Shoulder surfing, 746
- Shutdown Event Tracker, 1241–1242
- Shutting down, 9
- Side states, of media, 692–693
- Simple Main Transport Protocol (SMTP) site links, 519
- Simple SAN, 683
- Simple volume, 616
- Simulation options, 342
- Single point of failure, 639, 755
- Single Quorum cluster
 - infrastructure, 702
- Single sign-on access, 473
- Site link bridge objects, 520–521
- Site link objects, 518–520
- Site management, 1084–1093. *See also* Active Directory Sites and Services
 - application pool
 - configuration in, 1086–1087
 - bindings added in, 1086
 - delegating, in IIS, 1095–1097
 - geographical naming convention and, 29

- host headers configuration in, 1087–1088
- IIS connections and, 1069–1070
- in Advanced Simulation Options, 342
- organizational naming convention and, 28
- security configuration in, 1088–1093
- site adding in, 1084–1086
- site viewing in, 1084
- stopping and starting, 1088
- Site objects, 515–516
- Site-aware network services, 511
- Site-specific service locator (SRV) records, 511
- Sixty-four bit environment, 11
- Sixty-four bit keys, Registry, 1199–1201
- SLED (single large expensive disk), 617
- slmgr.vbs-ipk command line, 54
- Smart cards, 473, 784, 888, 893
- SMBv2, 797
- SMTP e-mail, 446–447, 1076, 1080
- Snap-in, PowerShell, 387, 414
- Snapshot files, 657, 995, 998–999
- Social engineering, 746
- Software management, 933–959
 - Group Policy installation extension for application deployment
 - GPO in, 940–943
 - configuring, 943–947
 - distribution point setup in, 939–940
 - overview of, 933–935
 - Group Policy settings for, 282
 - packages for, 947–955
 - application properties changes and, 950–952
 - Group Policy and, 947–950
 - modifications to, 953–955
 - removing and redeploying, 955
 - upgrades for, 952–953
 - restriction policies in, 955–959
 - creating, 957–959
 - operations of, 956–957
 - services for, 935–939
 - troubleshooting, 1226
 - updates and, 834
 - Windows Deployment Services (WDS) for, 959
- Sort-Object cmdlet, 398
- Source integrity, for security, 747
- Spanned SAN, 683
- Spanned volume, 617, 622, 628, 633, 635–636
- Special permissions, 248–250
- Specialized Security-Limited Functionality guidelines, 766–767
- Spikes, in power voltage, 1179–1180
- Spooling, print, 185–188, 194, 721–722
- Spyware, 837
- SQL Server, 841, 1152
- SQL Slammer worm, 751–752, 758
- Staging folder, 279
- Stand-alone namespaces, 259–260
- Standard edition, of Windows Server 2008, 10
- Standard escalation procedures (SEPs), 751, 1136, 1138–1139
- Standard operating procedures (SOPs), 1136–1138
- Standard Port Monitor, 173
- Start Menu, 231, 331–333
- Start Terminal Server Licensing Wizard, 1044
- Starter Group Policy Objects, 286–288
- Start-Process cmdlet, 398
- Start-Service cmdlet, 398
- Start-Transcript cmdlet, 398
- Startup Repair tool, in WRE, 1162
- Startup Repair Wizard, 1143
- Start-up scripts, 176
- States, of Active Directory Domain Services, 539
- Static IPv6 address, 475, 482
- Stop errors, 76
- Stop-Process cmdlet, 465
- Stop-Service cmdlet, 398
- Stop-Transcript cmdlet, 398
- Storage, 651–697. *See also* Disk management
 - File Server Resource Manager and, 651–670
 - directory quotas for, 657–663
 - installation and configuration of, 652–654
 - reports from, 654–657
 - screening files and, 663–670
 - of AD DS databases, 535–536
 - of file resources, 252–256
 - of Registry data, 1206–1209
 - PowerShell and, 451
 - removable, 689–697
 - libraries and, 693–695
 - media pools and, 695
 - operator requests and, 696–697
 - physical media and, 695–696
 - terminology for, 689–693
 - work queue and, 696
- SAN (Storage Area Network) Manager for, 670–689
 - console for, 675–676
 - installing, 674–675
 - iSCSI security for, 679–680
 - iSCSI targets for, 678–680
 - logical units (LUNs) for, 681–689
 - SAN advantages and disadvantages and, 671–672
 - server connections for, 676–677
 - terminology for, 672–674

- Share and Storage
 - Management tool for, 252–256
- Strings, 419–421, 433, 1078
- Striped SAN, 683
- Striped volume, 617, 622, 633
- Striped with Parity SAN, 683
- Strong secrets, 680
- Structural object class, 558–560
- Stub zones, 598, 601
- Subdomains, 603–605
- Subkeys, Registry, 1198, 1203–1206
- Subnet objects, 512, 517–518
- Subscriptions, 372–374
- Subsystem for UNIX
 - Applications (SUA), 43, 903, 908, 928–932
- Subsystems, Storage Manager
 - node for, 675
- Subtractive permissions, 240
- Subtrees, in Active Directory, 17–18
- Success events, 358–360, 362–363
- Suffixes, User Principal Name (UPN), 509–510
- Super users, 908
- Superscopes, 586, 592
- Surge protectors, 1179, 1181–1182
- Surges, in power voltage, 1180–1181
- Switch statements, in PowerShell, 429
- Symbolic links, 906–907
- Synchronization, 844–845
 - DFS replication for, 258
 - of AD DS with AD LDS, 531–533
 - of AD LDS and
 - metadirectories, 469
 - password, 923–924
- Sysprep.exe command line tool, 71
- System Access Control Lists (SACLs), 359–360, 363, 570

- System Center Configuration Manager (SCCM), 111, 806, 1006
- System Center Operations Manager (OpsManager), 670, 936
- System Center Virtual Machine Manager, 86, 974
- System configuration utility, 1239–1240
- System file checker, 1240
- System File Protection cache folder, 959
- System recovery, 1222
- System Stability Index, 1115, 1117–1119
- System String object
- Systems Center Configuration Manager, 836, 845
- SYSVOL shares, 255, 474, 482

T

- Tab completion, of PowerShell cmdlets, 388
- Tail utility, from UNIX, 464–466
- Taskpad View Wizard, New, 355–356
- Tasks. *See also* Internet Information Services (IIS)
 - delegation of, 380–381
 - event occurrences and, 375
 - Immediate, 329
 - PowerShell for scheduling, 461–462
 - Task Scheduler for, 327–329, 377–378, 449, 657, 723
- TCP Offload Engines (TOE), 674
- Tee utility, from UNIX, 464–466
- Telnet, 909–910
- Temp. edb temporary files, 536
- Templates
 - for Data Collector set, 1120–1122
 - for screening files, 667–668
- HPC Node Template
 - Generation Wizard for, 741
 - quota, 658, 660–663
 - user profile folder for, 231
 - Workstation Authentication, 811
- Terminal emulation, 909
- Terminal Servers License
 - Servers group, 212
- Terminal Services, 1005–1059
 - as chokepoint, 755
 - clustering and, 703
 - concepts of, 1007–1008
 - configuration of, 1037–1042
 - installation of, 1011–1027
 - program installation and, 1024–1027
 - remote desktop for
 - administration of, 1023–1024
 - steps in, 1011–1020
 - user experience
 - improvement and, 1020–1023
 - licensing of, 1042–1044
 - overview of, 7–8, 1005–1007
 - RemoteApps in, 1044–1056
 - adding, 1050–1052
 - deploying, 1052–1056
 - for Server Core, 162–163
 - TS Gateway settings for, 1046–1047
 - TS Web Access to
 - distribute, 1047–1050
 - requirements of, 1009–1011
 - Terminal Services Manager
 - for, 1027–1037
 - connections managed by, 1030–1037
 - My Group in, 1028–1030
 - overview of, 1028
 - TS Web Access in, 1056–1059
- Terminal Services connection
 - authorization policy (TS CAP), 1016
- Terminal Services resource
 - authorization policy (TS RAP), 1016

- Terminal Services Session Broker, 8, 703
 - Testing, 223, 1139–1140. *See also* Virtualization
 - Test-Path cmdlet, 398
 - Thirty-two bit keys, Registry, 1199–1201
 - Three-fold process, rule of, 750
 - Time, setting, 99–100, 449–450. *See also* Coordinated Universal Time (UTC)
 - Tombstones, 537
 - Total cost of ownership (TCO), 41
 - Touch utility, from UNIX, 464–466
 - TPM-based mode, 777–778
 - Tracking printer locations, 169–172
 - Transaction logs, locations of, 541
 - Transforms, package
 - modifications as, 953–955
 - Transitive trust relationships, 33–34
 - Transitive two-way trusts, 507
 - Transmission Control Protocol-Internet Protocol (TCP-IP), 102, 573–614
 - Domain Name System (DNS) Servers and, 595–613
 - forwarders in, 610–613
 - interoperating between, 609
 - resource records added to, 605–608
 - setting up, 596–602
 - subdomains for, 603–605
 - zone transfers in, 608–609
 - Dynamic Host Configuration Protocol (DHCP) and, 574–595
 - address reservations for, 590–591
 - authorizing server and activating scope for, 589–590
 - command line
 - administration of, 595
 - network design for, 574–576
 - relay agent of, 593–595
 - scope creation for, 582–589
 - server role for, 576–582, 592–593
 - printers and, 174–175, 324–327
 - Windows Internet Naming Service (WINS) and, 613
 - Transport Layer Security (TLS), 473
 - Tree-root domains, 476
 - Trees
 - in Active Directory, 17–18
 - in multiple domain structure, 35
 - in namespace planning, 26
 - in single domain structure, 35
 - Troubleshooting, 1223–1242. *See also* Recovery
 - installations, 72–76
 - boot failure, 72–74
 - corrupt files, 74–75
 - failure to find hard disks, 75–76
 - stop errors, 76
 - printers, 191–195
 - priorities in, 1223–1225
 - scripts, 425
 - Secure Sockets Tunnelling Protocol (SSTP), 883–886
 - server recovery, 1227–1236
 - applications and data in, 1231–1233
 - files and folders in, 1229–1231
 - operating system in, 1233–1234
 - system state in, 1234–1236
 - volumes in, 1227–1228
 - service status verification for, 1236–1239
 - Shutdown Event Tracker for, 1241–1242
 - system configuration utility for, 1239–1240
 - system file checker for, 1240
 - system information for, 1236
 - systems recovery, 1225–1227
 - Terminal Services sessions, 1035
 - Trust levels, 1077
 - Trust relationships, 33–34, 507–509
 - Trust, rule of, 749, 760
 - Trusted computing base (TCB), 21
 - Trusted entities, 470
 - Trusted Root Certificate Authority, 879, 896
 - Trusted zone, for security, 753
 - TS Easy Print, 1006
 - TS Gateway, 1007, 1012, 1046–1047
 - TS RemoteApps, 7, 1044–1056
 - adding, 1050–1052
 - deploying, 1052–1056
 - for Server Core, 162–163
 - TS Gateway settings for, 1046–1047
 - TS Web Access programs in, 1058–1059
 - TS Web Access to distribute, 1047–1050
 - TS Session Broker, 1006
 - TS Web Access, 7, 1006, 1012, 1047–1050, 1052–1053, 1056–1059
 - Two-factor authentication, 780, 784
 - Type accelerators, in PowerShell, 441–442
 - Type. definition of, 399
- ## U
- Ultra-Wideband IEEE 802.15.3 technology, 850
 - Unattend.xml file, 150
 - Unattended installation and, 487–489
 - Unicast mode, network
 - adapters in, 706, 708, 718

- Uniform Naming Convention (UNC), 20
 - Uniform Resource Locators (URLs), 20
 - Uninterruptible power supply (UPS), 1142, 1177, 1180–1181
 - Universal groups, 22, 203
 - Universal principal names (UPN), 807–808
 - Universal scope, for groups, 199
 - Universal Serial Bus (USB), 722
 - UNIX systems
 - backslash character in, 441
 - file systems based on, 240
 - interoperability of
 - connectivity for, 43, 908
 - file listings for, 904–906
 - file systems for, 910–911
 - file transfer protocol for, 908
 - identity management for, 923–932
 - permissions and security for, 904
 - printing for, 912
 - privilege levels for, 907–908
 - symbolic links for, 906–907
 - Telnet for, 909–910
 - man command of, 408
 - Network File System (NFS)
 - resource type and, 722, 737
 - PowerShell and, 385
 - sourcing files in, 435
 - Subsystem for Applications
 - of, 385
 - systems of, 573
 - utilities of, 464–466
 - Unknown Publisher warning, 1058
 - Unrecognized media pools, 690
 - Untrusted zone, for security, 753
 - Update sequence number (USN), 263, 551
 - Updates. *See also* Patch management
 - downloading, 112
 - dynamic, 600–602
 - enabling, 106–111
 - installation and, 93
 - Upgrading, 79–94
 - Active Directory, 83–84
 - architecture in, 82
 - business results of, 41
 - clients, 88
 - domain and computer
 - preparation for, 87–88
 - hardware support for, 85–86
 - matrix for, 79–80
 - performing, 88–94
 - pre-upgrade steps in, 81–82
 - rolling, 723
 - software management
 - packages, 952–953
 - software support for, 86–87
 - UPS devices, 81
 - USB Flash drive, 773, 777
 - USB keys, security and, 759
 - User Account Control (UAC), 88, 347–353
 - Admin Approval Mode (AAM)
 - in, 348
 - disabling aspect of, 349–352
 - least privilege security theory
 - in, 241–242
 - ownership and, 250
 - registry virtualization and, 348–349
 - turning off, 352–353
 - User Datagram Protocol (UDP), 910
 - User experience improvement, 1020–1023
 - User mode, of MMC, 354
 - User Name Mapping Server, 239, 915
 - User Principal Name (UPN), 509–510
 - Users
 - accounts for, 218–223
 - deleting, 226
 - disabling and enabling, 225–226
 - domain, 220–221
 - finding, 224–225
 - local, 221–222
 - moving, 226
 - naming, 218
 - options for, 218–219
 - passwords for, 219–220, 227
 - properties of, 222–223
 - renaming, 226
 - testing, 223
 - unlocking, 227–228
 - groups for, 205–209, 212
 - home folders for, 228–229
 - in Control Panel, 314–317
 - PowerShell credentials for, 393
 - profiles for, 230–236
 - folders in, 230–231
 - local, 232
 - logon script assigned to, 236
 - roaming, 232–235, 339, 935
 - rights of, 213–217
 - group assignment of, 216–217
 - local assignment of, 217
 - logon, 214–217
- ## V
- Validate A Configuration Wizard, 730
 - Validation tool, for clusters, 701, 718
 - Values, Registry
 - contents of, 1213
 - definition of, 1198
 - deleting, 301
 - removal of, 1214
 - renaming, 1216
 - search of, 1212–1213
 - updating, 301
 - Variables, PowerShell, 418, 435
 - VBScripts, 385, 405–406, 462
 - VDS hardware, 675
 - Version-control system, 1138
 - Video files, screening, 664
 - Videos folder, in user profiles, 231
 - Virtual directories, 1094

- Virtual Local Area Networks (VLANs), 674
- Virtual PC 2007, 1002
- Virtual private networks (VPNs), 473
 - gateway server name for, 859
 - meaningful name for, 882
 - Network Access Protection and, 800, 802
 - Network Access Translation (NAT) and, 871
 - Network Options preference item and, 317–319
 - Root Certificate Authority certificate of, 877
 - Secure Sockets Tunnelling Protocol (SSTP) and, 848, 850
 - security for, 747–748
 - terminal services gateway versus, 7
- Virtual Server 2005 R2, 1002
- VirtualBox virtualization, 1002–1003
- Virtuallron virtualization, 1002
- Virtualization, 961–1003
 - basic virtual machine for, 974–978
 - for legacy servers, 86
 - for network configuration testing, 848, 852
 - Hyper-V for
 - alternatives to, 1002–1003
 - initial configuration for, 968–974
 - installation of, 965–968
 - overview of, 962–965
 - in failover cluster
 - configuration, 725
 - machine settings for, 978–994
 - differencing disks and, 988–991
 - for COM ports and floppy drives, 992–994
 - for disks and controllers, 986–988
 - for hardware additions, 980–984
 - for memory and CPU, 984–986
 - for network adapters, 991
 - overview of, 978–980
 - management settings for, 994–997
 - of legacy applications, 44
 - overview of, 4
 - patch testing and, 839
 - Registry, 348–349
 - server load and, 45
 - Windows Server
 - Virtualization for, 750
 - Windows Virtualization Technology for, 619
 - working with, 998–1002
 - Virus infection, 1239
 - Visual Basic scripts, 157
 - VMware virtualization, 1002–1003
 - VMware Workstation, 839–840
 - Volatile Registry keys, 1208
 - Voltage variations, in power supply, 1179–1181
 - Volume Shadow Copy Service (VSS), 657, 723, 1169, 1231
 - Volumes, 625–641
 - backing up, 1149, 1151, 1154, 1156
 - BitLocker, 773–775
 - creating, 626–631
 - critical, 543
 - definition of, 616
 - dynamic disk conversions and, 631–632
 - encryption of data, 779
 - extended, 616
 - GPT disk conversions and, 632–633
 - hidden shares for, 255
 - logical, 616
 - mirror, 617, 637–641
 - partition logical drives and, 631
 - RAID-5, 617
 - recovery of, 1166–1167, 1227–1228
 - simple, 616
 - size changes of, 633–637
 - spanned, 617
 - striped, 617
 - Vulnerability to attacks, 751, 758

W

 - Wbadmin.exe command line tool
 - features of, 541–542
 - for Registry backup, 1221
 - for troubleshooting, 1235–1236
 - in backing up, 545, 1159–1165
 - Weakest link, rule of, 750
 - Web applications
 - development settings for, 1076–1080
 - Internet Information Services (IIS) and, 1093–1094
 - portal, 469
 - Web edition, of Windows Server 2008, 10
 - Web enrollment certificate, 877
 - Web Server (IIS) Support role service, 842
 - Web server clusters, 703
 - web.config files, 1098
 - Wevtuil.exe command line tool, 392
 - whatif parameter, in PowerShell, 391, 457
 - Where-Object cmdlet, 398, 431–432
 - While statement, in PowerShell, 429
 - Wide Area Network (WAN) connectivity, 43
 - Wildcards, in PowerShell, 421–422
 - Windows authentication, 1090
 - Windows Authorization Access group, 212
 - Windows Communication Foundation (WCF) Hosts, 742

- Windows Complete PC Restore Wizard, 1233
- Windows Compute Cluster Server (CCS), 740
- Windows Deployment Services (WDS), 53, 62–69
 - components of, 62–63
 - configuration for, 64–67
 - for automating deployment, 62
 - for software management, 935, 959
 - in Windows HPC Server, 741
 - installation steps for, 63–64
 - Remote Installation Services (RIS) versus, 62
 - setting properties for, 68–69
 - WinPE connecting to, 74
- Windows Event Collector service, 373
- Windows Explorer, 231, 644, 648, 1152
- Windows Firewall, 785–795
 - automatic enabling of, 764
 - command line management of, 793–795
 - configuring, 117–118
 - Group Policy for, 786–788
 - in Vista, 88
 - Network Access Protocol (NAP) and, 824–825
 - overview of, 10
 - policy for, 791–793
 - rule basics for, 788–789
 - rule definitions for, 789–791
 - software distribution and, 943
- Windows Image (WIM) files, 53
- Windows Installer packages, 936
- Windows Internal Database, 841–842
- Windows Internet Naming Service (WINS), 14, 190, 573–574, 579, 613, 721
- Windows Kernel Trace provider, 1109
- Windows Load Balancing, 706
- Windows logs, 370
- Windows Management Instrumentation (WMI)
 - for Windows Firewall, 786–788
- Internet Information Services (IIS) and, 1073
- PowerShell and, 402–404
- PushPrinterConnections.exe tool and, 178–179
- remote use of, 455–456
- Resultant Set of Policy and, 343
- scheduling tasks with, 462
- Windows Package Manager, 1066–1067
- Windows Process Activation Service (WAS), 1061–1063
- Windows Recovery Environment (WRE), 1160, 1162, 1171
- Windows Remote Management (WRM), 404–405
- Windows Remote Shell, 162
- Windows Scripting Host (WSH), 405
- Windows Security Health Agent (SHA), 804, 806
- Windows Security Health Validator (WSHV), 804, 806, 818
- Windows Server 2008, 3–11
 - Active Directory Domain Services in, 5–6
 - backup feature of, 8
 - functional level of, 480–482
 - PowerShell and, 5
 - read-only domain controllers (RODCs) of, 5
 - Registry changes in, 1196–1198
 - security features of, 9–10
 - Server Core of, 4
 - Server Manager of, 8
 - shutting down, 9
 - Terminal Services in, 7–8
 - versions of, 10–11
 - virtualization with, 4
- Windows Server 2008,
 - installing, 51–77
 - deployment environment for, 53–71
 - automating deployment in, 61–63
 - image additions in, 69–71
 - installation method in, 53
 - installation process in, 53–61
 - Windows Deployment Services in, 63–69
 - system requirements for, 51–52
 - troubleshooting, 72–76
 - boot failure, 72–74
 - corrupt files, 74–75
 - failure to find hard disks, 75–76
 - stop errors, 76
- Windows Server Backup
 - for AD DS, 545
 - for Registry, 1221
 - for system state data, 542
- Windows Server Update Services (WSUS), 93, 111, 841–845, 936
 - as trusted source, 837
 - configuration of, 844–845
 - installing, 841
 - prerequisites for, 842–844
 - Setup Wizard for, 843
- Windows Server Virtualization, 750, 839–840, 848
- Windows Small Business Server 2003, 1055
- Windows Software Update Services, 803
- Windows System Resource Manager (WSRM), 1018
- Windows Virtualization Technology, 619
- Windows Vista, 3
 - Folder Options items for, 309–310
 - Group Policy and, 938, 946
 - IEEE 802.1x enforcement and, 829

- Network Access Protection (NAP) on, 759
 - PushPrinterConnection.exe tool and, 178–179
 - Remote Desktop Client in, 116
 - Secure Sockets Tunnelling Protocol (SSTP) and, 848
 - SMBv2 supported by, 797
 - SSTP VPN requirements of, 877
 - Start Menu items for, 331–332
 - upgrading clients to, 88
 - wireless client configuration for, 896
 - Windows XP
 - Folder Options items for, 308–309
 - Group Policy and, 938, 946
 - Immediate Task Items of, 329
 - Power Options item for, 320–321
 - Power Scheme item for, 321
 - Start Menu items for, 332–333
 - Winnt32.msi package, 948
 - WinPE, 73–74
 - WinRM service type, 372
 - Wire Equivalent Privacy (WEP), 850
 - Wireless deployment of remote access, 889–898
 - access points for, 893–894
 - for RADIUS clients, 892–893
 - overview of, 889–890
 - prerequisites for, 890–892
 - secure configuration for, 894–898
 - Wireless networks, 473
 - Witness disk, 704, 719–720
 - Work queue, 696
 - Worker processes, in IIS, 1082
 - Workgroup security, for UNIX, 911
 - Workspace, in IIS, 1069
 - Workstation Authentication template, 811
 - World Wide Name (WWN), 677
 - World Wide Web Publishing Service, 1061–1063
 - WOW64, 87
 - WPA2 wireless security, 848–849, 896–898
 - Write-Host cmdlet, 398, 416
- X**
- X.{five}500 standard, 15, 18
 - XML, 411, 445, 463, 654
- Z**
- Zap files, for applications deployment, 936–939, 949–950
- Zones**
- contiguous namespace for, 603
 - for redundancy, 600–601
 - network rules for, 956, 958
 - security, 753–754
 - transfers of, in DNS, 608–609