

# Windows Server<sup>®</sup> 2008 Administrator's Companion

*Charlie Russel and  
Sharon Crawford*

To learn more about this book, visit Microsoft Learning at  
<http://www.microsoft.com/MSPress/books/11840.aspx>

9780735625051

**Microsoft<sup>®</sup>**  
*Press*

© 2008 Charlie Russel and Sharon Crawford. All rights reserved.

# Table of Contents

*Acknowledgments* .....xxxiii  
*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/](http://www.microsoft.com/learning/booksurvey/)

BitLocker Drive Encryption.....	9
Windows Firewall.....	10
Network Access Protection .....	10
Versions of Windows Server 2008 .....	10
Summary.....	11
<b>2 Introducing Directory Services .....</b>	<b>13</b>
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
<b>3 Planning Namespace and Domains.....</b>	<b>25</b>
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

<b>4 Planning Deployment</b>	<b>39</b>
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

<b>5 Getting Started</b>	<b>51</b>
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
<b>6 Upgrading to Windows Server 2008</b>	<b>79</b>
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
<b>7 Configuring a New Installation . . . . .</b>	<b>95</b>
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
<b>8 Installing Server Roles and Features . . . . .</b>	<b>121</b>
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
<b>9 Installing and Configuring Server Core .....</b>	<b>147</b>
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
<b>10 Managing Printers .....</b>	<b>165</b>
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
<b>11 Managing Users and Groups . . . . .</b>	<b>197</b>
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
<b>13 Group Policy .....</b>	<b>281</b>
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
<b>15 Using Scripts for Consistent Administration . . . . .</b>	<b>383</b>
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
<b>16 Installing and Configuring Directory Services .....</b>	<b>467</b>
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
<b>17 Managing Active Directory .....</b>	<b>535</b>
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
<b>18 Administering TCP/IP .....</b>	<b>573</b>
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
<b>19 Implementing Disk Management .....</b>	<b>615</b>
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
<b>20 Managing Storage .....</b>	<b>651</b>
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
<b>21 Using Clusters .....</b>	<b>699</b>
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

<b>22 Planning Security .....</b>	<b>745</b>
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
<b>24 Administering Network Access Protection .....</b>	<b>799</b>
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
<b>25 Patch Management .....</b>	<b>833</b>
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**

<b>27 Interoperability</b>	<b>903</b>
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
<b>28 Managing Software</b>	<b>933</b>
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
<b>29 Working with Windows Virtualization . . . . .</b>	<b>961</b>
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
<b>30 Deploying Terminal Services . . . . .</b>	<b>1005</b>
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 Services .....1061**

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
<b>33 Disaster Planning .....</b>	<b>1133</b>
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
<b>34 Using Backup .....</b>	<b>1147</b>
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
<b>35 Planning Fault Tolerance and Avoidance .....</b>	<b>1175</b>
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
<b>36 Managing the Registry .....</b>	<b>1193</b>
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
<b>37 Troubleshooting and Recovery .....</b>	<b>1223</b>
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 Services .....1236

Using the System Configuration Utility .....1239

Using the System File Checker .....1240

Using the Shutdown Event Tracker.....1241

Summary.....1242

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

**B Optional Components.....1247**

**C Understanding TCP/IP v4 .....1257**

About the Authors .....1281

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/](http://www.microsoft.com/learning/booksurvey/)

# Implementing Disk Management

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

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](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

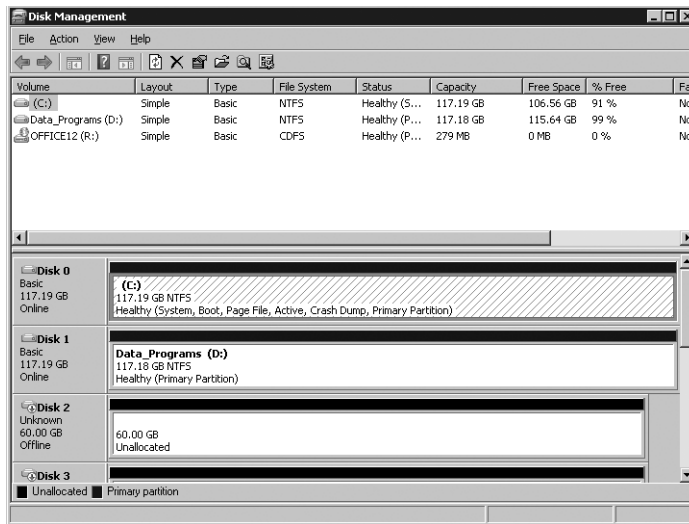
RAID (redundant array of independent disks) is a term used to describe a technique that has gone from an esoteric high-end solution to a normal procedure on most servers. Fifteen years ago, RAID was mostly unheard of, although the original paper defining RAID was written in 1988. In the past, most server 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.

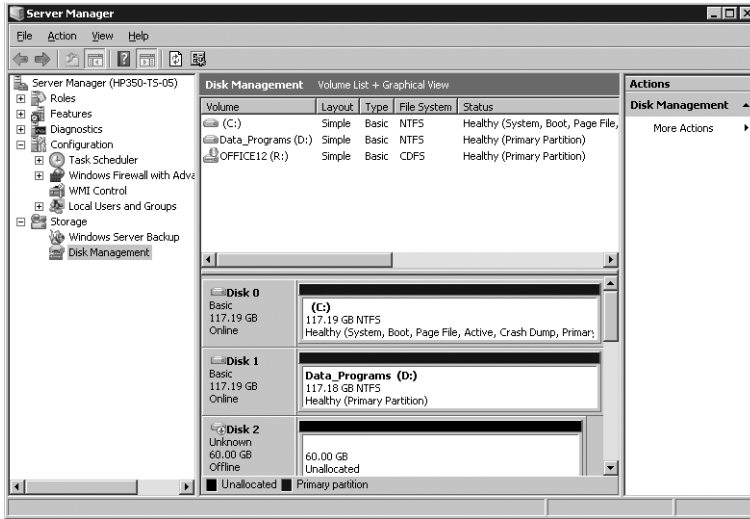


Figure 19-2 The Server Manager console



## 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.

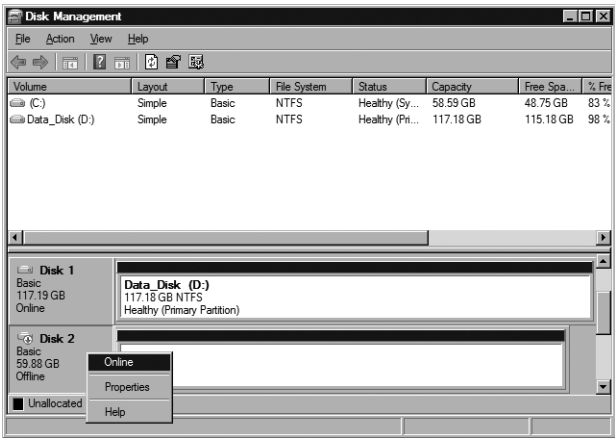
After you install the drive and power up the system again, Windows Server 2008 automatically recognizes the new hardware and makes it available. If the disk is a basic disk that is already partitioned and formatted, you can use it without initializing, but it will initially appear "offline" in Disk Management. 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.

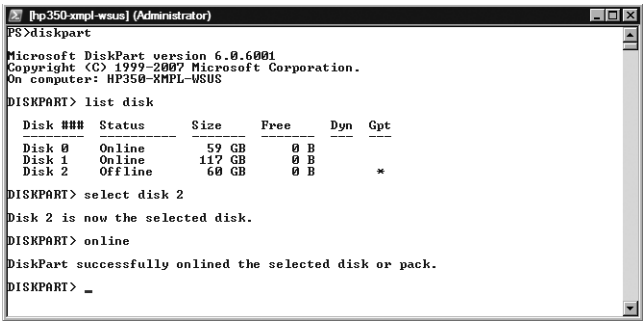
**Setting a Disk Online**

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.



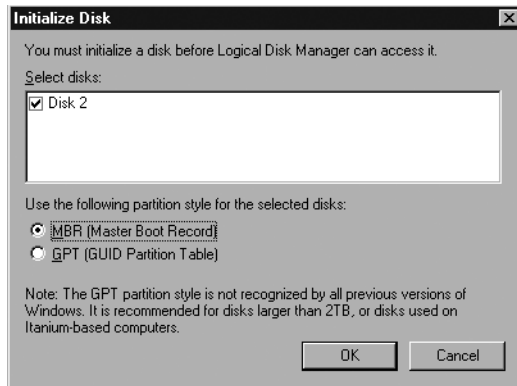
**Figure 19-3** Bringing a disk online using Disk Management  
The command-line equivalent is shown in Figure 19-4.



**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.

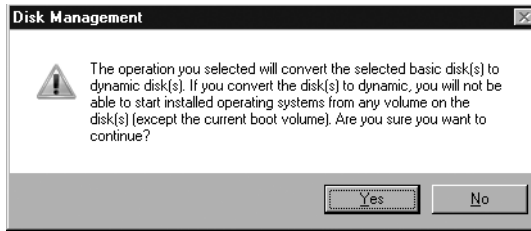
---

## 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.

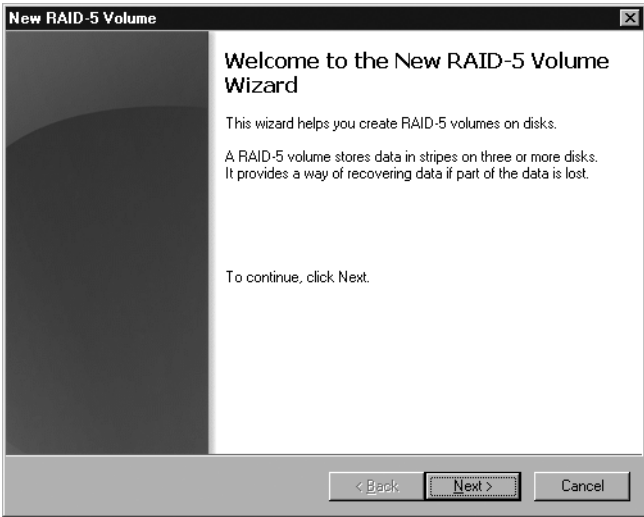


Figure 19-8 The New RAID-5 Volume Wizard

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.

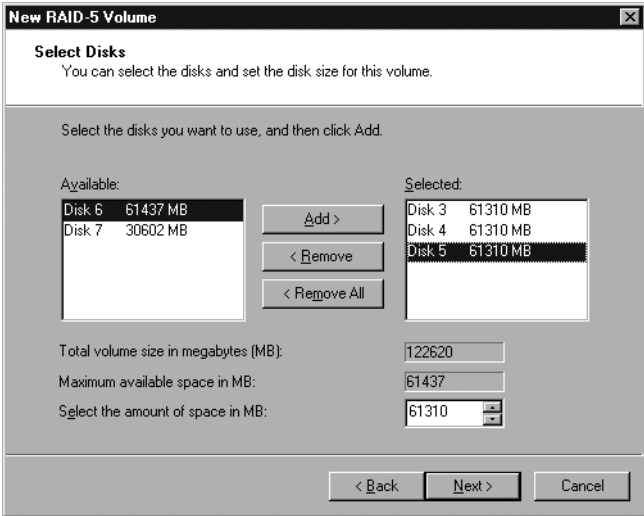
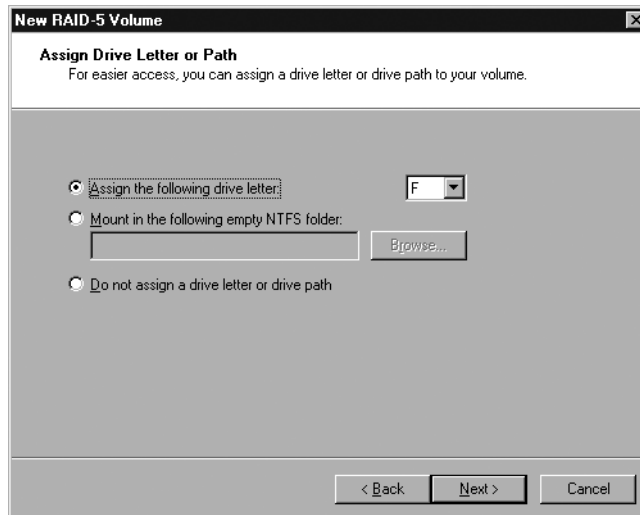


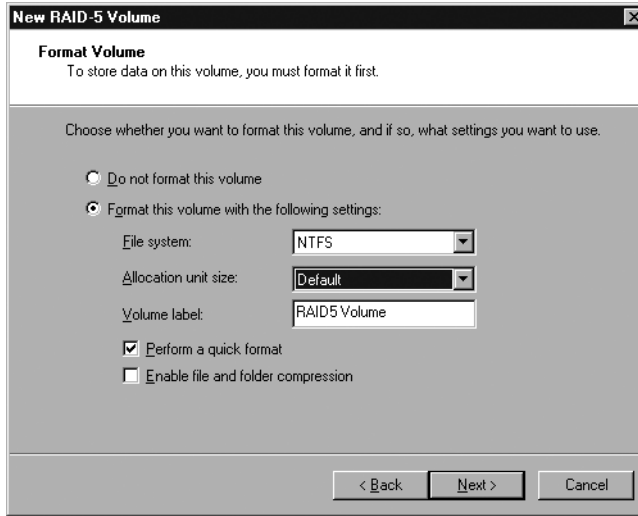
Figure 19-9 Select the disks that will be part of this volume.

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.)



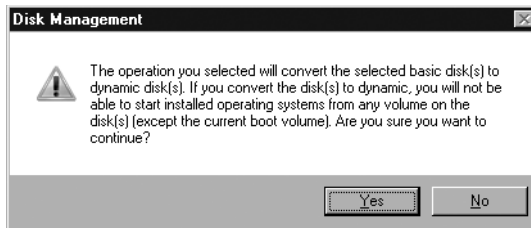
**Figure 19-10** Select a drive letter or mount point for the new volume.

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.

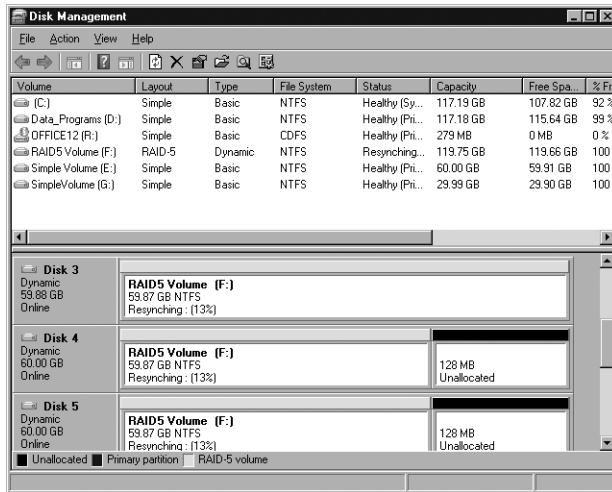


Figure 19-13 The new RAID-5 volume being created

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.

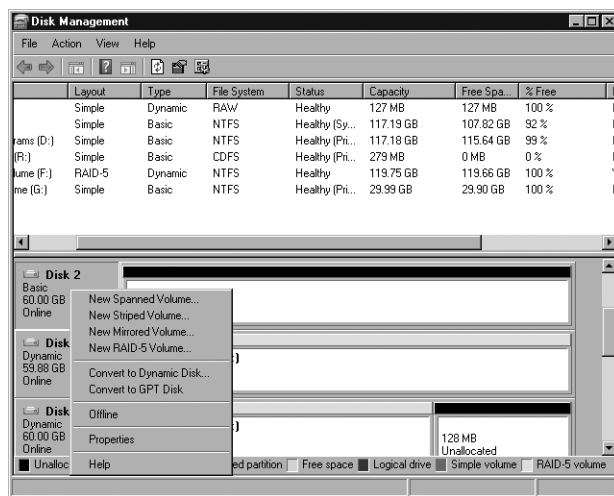


Figure 19-14 Converting from an MBR disk to a GPT disk

- 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.

---

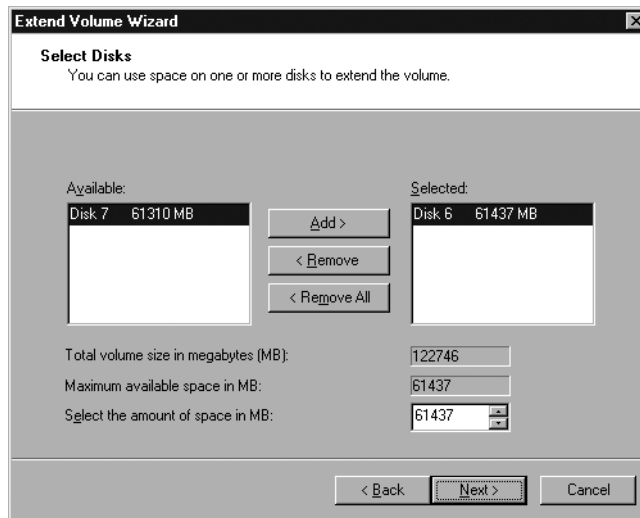
**Important** Once you extend a volume across multiple disks, you normally cannot shrink it back down onto a single disk without deleting the volume entirely and recreating it. This means you *will* lose data, so consider carefully before you decide to extend a volume across multiple disks.



## 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     DUD-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.

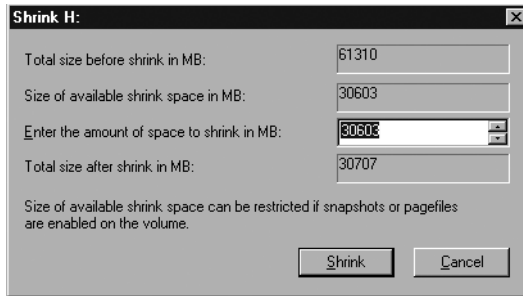
Why, then, would anyone use spanning? Because they have hardware RAID to provide the redundancy. This combination offers the best of both worlds—redundancy provided by the hardware RAID controller and flexibility to expand volumes as needed, using Disk Management. Yet another compelling argument for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

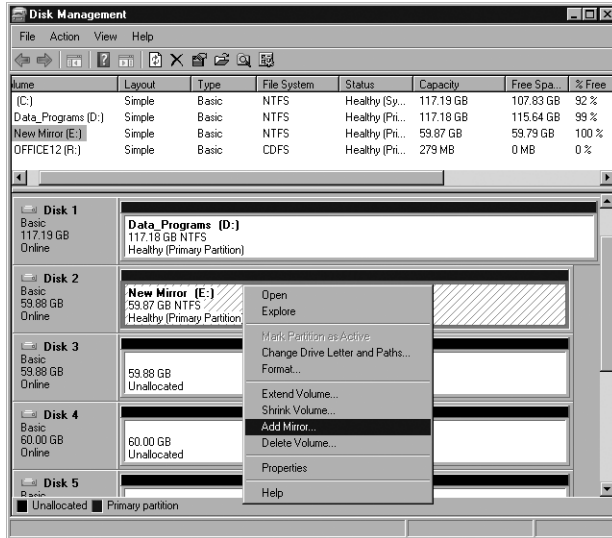
---

**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

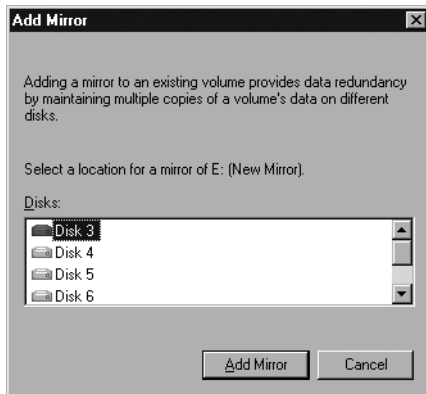
When your data is mission critical and you want to make sure that no matter what happens to one of your hard disks the data is protected and always available, consider mirroring the data onto a second drive. Windows Server 2008 can mirror a dynamic disk onto a second dynamic disk so that the failure 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.)

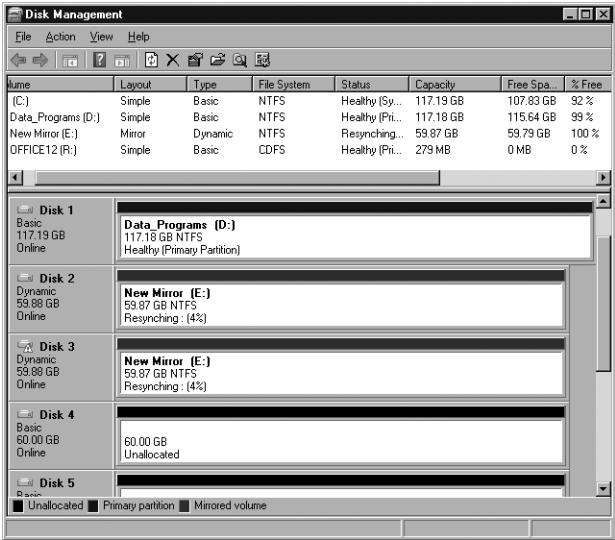


Figure 19-20 A newly created mirrored disk in the process of regeneration

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]
```

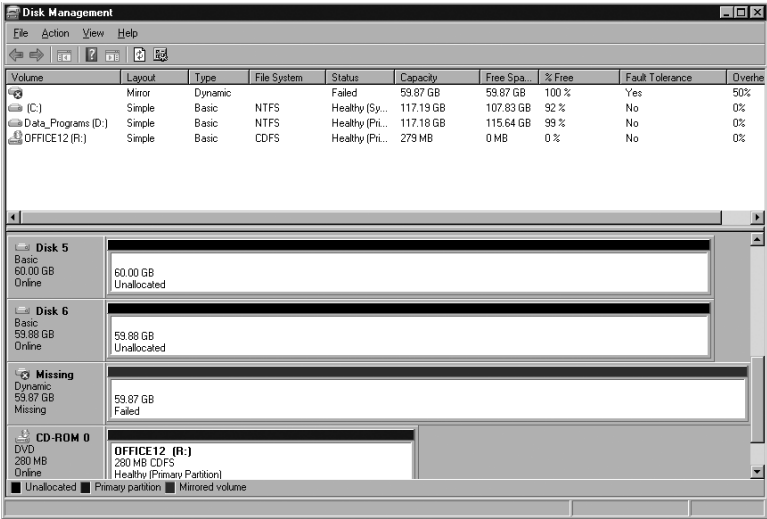
where DISK is the disk that will be added to make the mirror, and ALIGN is used to align with a specific hardware RAID Logical Unit Number (LUN) alignment boundary.

**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.

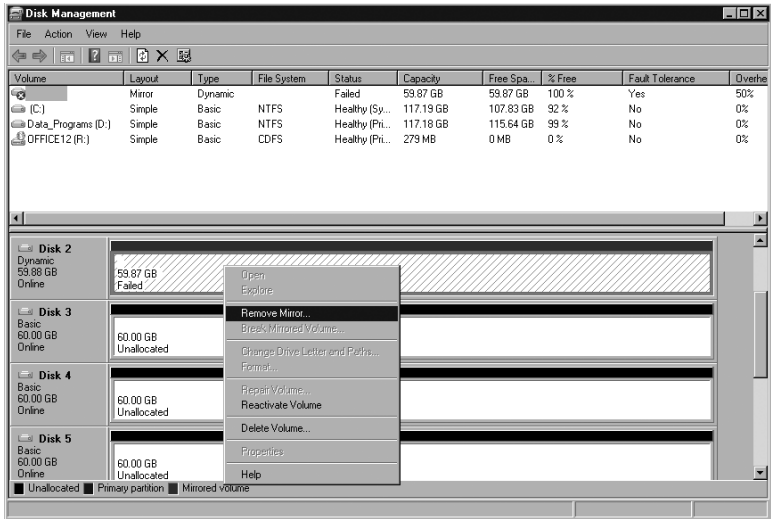


**Figure 19-21** Failed disk in mirror shown as missing and offline

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

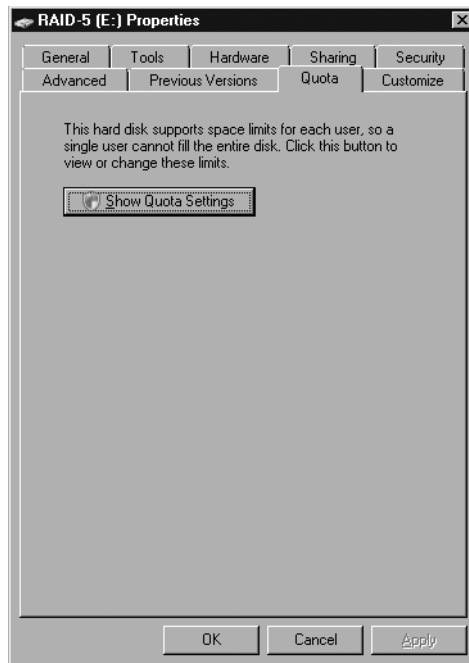


amount of disk space that user can use on a particular volume. Directory quotas are applied to all users and limit the amount of disk space that users can use in a particular folder and its subfolders. Directory quotas were introduced in Windows Server 2003 R2 with the new File Server Resource Manager,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

## Enabling Quotas on a Disk

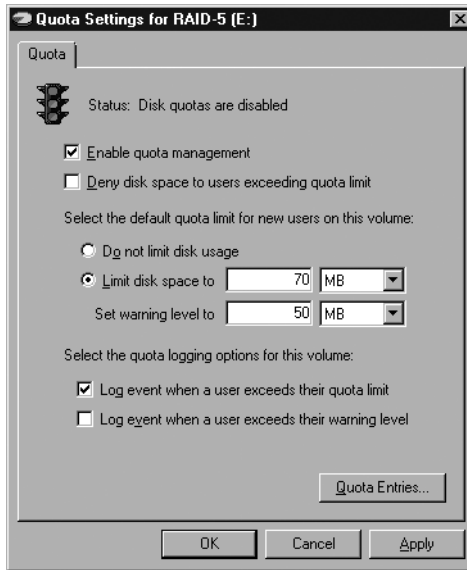
By default, disk quotas are disabled in Windows Server 2008. You can enable disk quotas on any volume that has been assigned a drive letter. To enable quotas on a volume, follow these steps:

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.



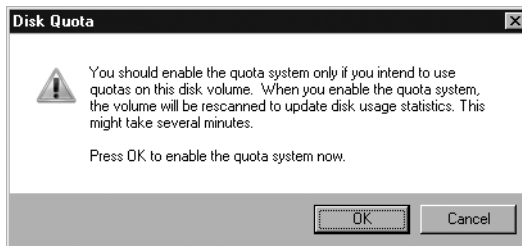
**Figure 19-23** The Quota tab of a drive's properties

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.



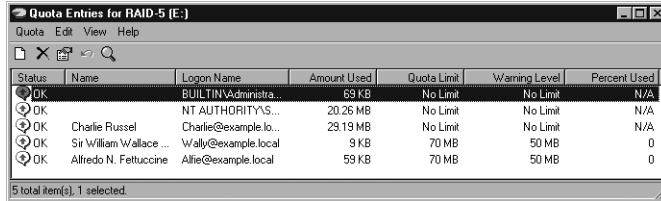
**Figure 19-25** The Disk Quota confirmation message

## 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.

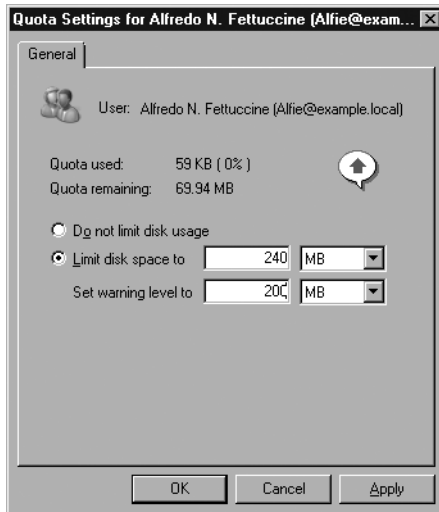
To set the quotas for individual users, follow these steps:

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

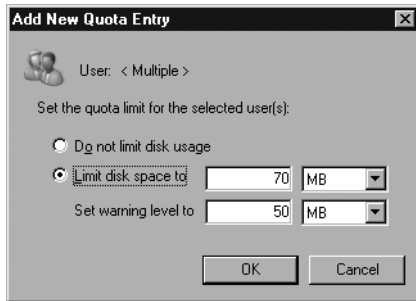
4. To modify the quota for a user already listed, select the user and then click Properties to open the quota settings for that user, as shown in Figure 19-27. Set the quota for the user and click OK to return to the Quota Entries dialog box.



**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.

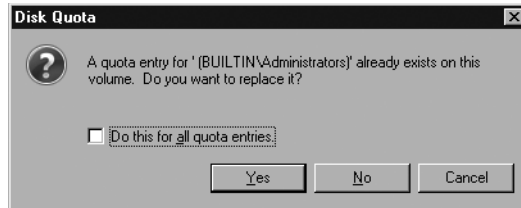
To export the quotas on a volume, follow these steps:

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.

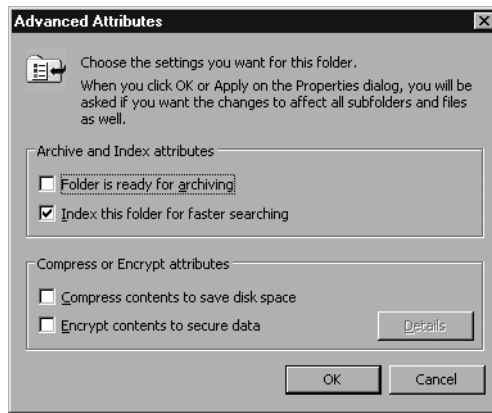
When you encrypt a folder, all new files created in that folder are encrypted from that point forward. You can also elect to encrypt the current contents when you perform the encryption. However, be warned that if you choose to encrypt the contents of a folder when it already contains files or subfolders, 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.



