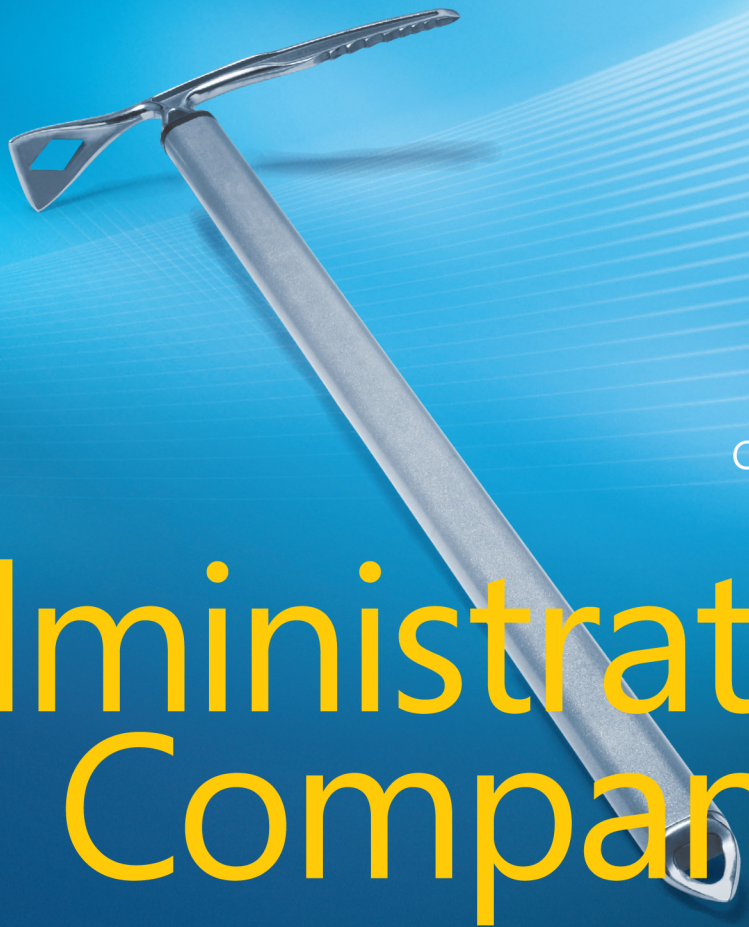
Microsoft

Windows® Small Business Server 2011



Charlie Russel and
Sharon Crawford

Administrator's Companion

Microsoft®

Windows® Small Business Server 2011

Administrator's Companion

Charlie Russel
Sharon Crawford

Copyright © 2011 by Charlie Russel and Sharon Crawford

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

ISBN: 978-0-7356-4911-8

2 3 4 5 6 7 8 9 10 11 TG 6 5 4 3 2 1

Printed and bound in Canada.

This product is printed digitally on demand.

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

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

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

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

Acquisitions Editor: Ken Jones
Developmental Editors: Laura Sackerman and Ken Jones
Production Editor: Teresa Elsey
Proofreader: Nancy Sixsmith
Compositor: Ron Bilodeau
Technical Reviewer: Andrew Edney
Copyeditor: Roger LeBlanc
Indexer: Angela Howard
Cover Design: Twist Creative • Seattle
Cover Composition: Karen Montgomery
Illustrator: Robert Romano

[2011-09-09]

For Dana Epp, always a mensch

This page intentionally left blank

Contents at a Glance

Introduction *xxv*

PART I PREPARATION AND PLANNING

CHAPTER 1 Introducing Windows Small Business Server 2011 1
CHAPTER 2 Understanding 64-Bit Windows 9
CHAPTER 3 Planning Your SBS Network 19
CHAPTER 4 Planning Fault Tolerance and Avoidance 45

PART II INSTALLATION AND SETUP

CHAPTER 5 Installing Small Business Server 2011 67
CHAPTER 6 Configuring SBS in Hyper-V 81
CHAPTER 7 Migrating to Windows Small Business Server 2011 Standard 111
CHAPTER 8 Completing the Getting Started Tasks 181

PART III PERFORMING THE BASIC TASKS

CHAPTER 9 Managing Users and Groups 203
CHAPTER 10 Shares and Permissions 223
CHAPTER 11 Disk Management 243
CHAPTER 12 Storage Management 275
CHAPTER 13 Installing and Managing Printers 315
CHAPTER 14 Managing Computers on the Network 337
CHAPTER 15 Managing Software Updates 363
CHAPTER 16 Configuring Backup 383

PART IV	**PERFORMING ADVANCED TASKS**	
CHAPTER 17	Windows SBS Console vs. Server Manager	439
CHAPTER 18	Configuring and Managing Email	469
CHAPTER 19	Managing Local Connectivity	495
CHAPTER 20	Managing Remote Access	521
CHAPTER 21	Using Group Policy	547
CHAPTER 22	Managing Reports	579
CHAPTER 23	Customizing a SharePoint Site	597
PART V	**PREMIUM EDITION FEATURES**	
CHAPTER 24	Installing the Second Server	627
CHAPTER 25	Installing Microsoft SQL Server 2008 R2 Standard Edition for Small Business	657
CHAPTER 26	Adding a Terminal Server	673
PART VI	**MAINTENANCE AND TROUBLESHOOTING**	
CHAPTER 27	Performance Monitoring	711
CHAPTER 28	Disaster Planning	733
PART VII	**APPENDICES**	
APPENDIX A	Introduction to Networks	751
APPENDIX B	Automating Installation	757
APPENDIX C	Additional Resources	759
	Index	*761*

Contents

Introduction *xxv*

PART I PREPARATION AND PLANNING

Chapter 1 Introducing Windows Small Business Server 2011 1

Windows Small Business Server Editions 1

What's New and Improved 2

SBS Console 3

Remote Web Access 4

Installation and Migration 4

Data Protection 4

Exchange Server 2010 SP1 5

SharePoint Foundation Services 2010 5

Small Business Server 2011 Premium Add-on 6

Hardware Requirements 6

Summary 7

Chapter 2 Understanding 64-Bit Windows 9

Why the Change? 10

What Are the Advantages? 11

Memory 11

Performance 12

Security 13

Virtualization 14

What Are the Challenges? 15

Drivers 15

Hardware and Software Considerations 15

What About Clients? 17

Summary 18

Chapter 3 Planning Your SBS Network 19

Planning the Network Infrastructure 19
Determining Your Needs 21
Choosing an Internet Connection 22
Choosing a Network Type 25
Choosing Network Devices 28
Choosing Server Hardware 34
Choosing Client Hardware and Software 36

Choosing Naming Conventions 37
Choosing a Domain Name for the Network 37
Naming Computers 39

Planning for Security 40
Ensuring Physical Security 40
Securing Client Computers 41
Securing Wireless Networks 43
Securing Internet Firewalls 43

Summary 44

Chapter 4 Planning Fault Tolerance and Avoidance 45

Mean Time to Failure and Mean Time to Recover 46

Protecting the Power Supply 47
Local Power Supply Failure 48
Voltage Variations 50
Sags 52
Short-Term Power Outages 53
Long-Term Power Outages 53

Disk Arrays 55
Hardware vs. Software 55
RAID Levels for Fault Tolerance 55
Hot-Swap and Hot-Spare Disk Systems 61

Redundant Networking 62

Other Spare Parts 62

Summary 63

PART II INSTALLATION AND SETUP

Chapter 5 Installing Small Business Server 2011 67

Planning 67
Planning Partitions 67
Planning Location and Networking 68
Preparing the Server 69
Installation 70
Installation Process 70
Using the SBS Answer File Generator 78
Summary 79

Chapter 6 Configuring SBS in Hyper-V 81

Hyper-V Overview 82
Emulation vs. Hypervisor 83
Requirements 84
Installation 86
Installing on Microsoft Hyper-V Server R2 87
Installing on Full Windows Server 2008 R2 89
Initial Configuration 91
Configuring Networks 91
Server Settings 93
Creating a Virtual Machine 95
Creating a Basic VM 96
Machine Settings 101
Working with a Virtual Machine 105
Starting, Stopping, Saving, Snapshotting 105
Clipboard 106
SBS in Hyper-V 107
Licensing 108
Configuration 108
Summary 109

Chapter 7 Migrating to Windows Small Business Server 2011 Standard 111

The Migration Process 112

Preparing Your Server 114

- Before You Start 114
- Back Up Your Existing SBS Server 115
- Install Current Updates 115
- Network Configuration 116
- Install Router and Firewall 124
- Configuring Active Directory 127
- Best Practices Analyzer 130
- Optimize Exchange Mailboxes 133
- Running the Migration Preparation Tool 134

Creating a Migration Answer File 139

- Administrator Account 139
- Using the SBS Answer File Generator 142

Installing SBS 2011 145

Migrating Settings and Data 146

- Using the Migration Wizard 147
- Re-Enabling Folder Redirection 176

Final Thoughts 178

Summary 179

Chapter 8 Completing the Getting Started Tasks 181

Finish the Installation 182

Connect to the Internet 182

Customer Feedback Options 184

Set Up Your Internet Address 185
Registering a New Domain Name 185
Using an Existing Domain Name 188
Managing Your Domain Name 192
Configure Email 193
Add a Trusted Certificate 193
Protect Your Data 199
Add Users, Computers, and Devices 199
Network Essentials Summary 199
Summary 200

PART III PERFORMING THE BASIC TASKS

Chapter 9 Managing Users and Groups 203
Understanding Groups 203
Creating Groups 205
Setting Up a Distribution Group 205
Creating a Security Group 206
Working with Groups 208
Built-In Universal Groups 209
Built-In Domain Local Groups 209
Built-In Global Groups 212
Managing User Roles 213
The Standard User Role 214
The Standard User with Administration Links 215
Network Administrator Role 215
Creating a New User Role 215
Adding a New User Account 217
Adding Multiple User Accounts 220
Giving Users Access to Computers 221
Summary 222

Chapter 10 Shares and Permissions 223

Share Permissions vs. File Permissions 223
Share Permissions 223
File Permissions 224
NTFS Permissions 225
What Permissions Mean 225
How Permissions Work 227
Considering Inheritance 228
Adding a Shared Folder 229
Removing a Shared Folder 233
Changing Share Permissions 234
Special Shares 235
Ownership and How It Works 236
Effective Permissions 238
Factors Considered in Determining Effective Permissions 239
Defining User Rights 240
Managing Default User Rights Assignments 241
Summary 242

Chapter 11 Disk Management 243

The Search for Disaster Protection 244
Choosing the Storage Solution for Your Network 248
Storage Connection Technologies 249
Managing Disks 250
Partitions and Volumes 252
Adding a Partition or Volume 253
Extending or Shrinking a Volume 263
Adding a Mirror 267
Drive Failure in a Mirrored Volume 268
Breaking a Mirror 271
RAID-5 Volumes 271
Mounting a Virtual Hard Disk 272
Mounting a Volume 273
Summary 274

Chapter 12 Storage Management 275

Distributed File System 275
DFS Terminology 276
Namespace Type 277
Namespace Server Requirements 278
Namespace Client Requirements 278
DFS Replication 279
File Replication Service 279
Replication Topologies 280
Installing DFS Management 281
Creating or Opening a Namespace Root 283
Adding Namespace Servers 285
Adding DFS Folders 285
Changing Advanced Settings 287
Backing Up and Restoring the DFS Folder Targets 289
Using DFS Replication 290

Using File Server Resource Manager 296
Scheduling Storage Reports 296
Using Directory Quotas 300
Creating Quotas and Auto Quotas 301
Viewing and Managing Quotas 302
Creating and Editing Quota Templates 303
Screening Files 306

Summary 313

Chapter 13 Installing and Managing Printers 315

Understanding Print Servers 315

Selecting Printers 316

Planning Printer Placement 317
Naming Printers 318
Naming Printer Locations 318

Installing Printers 319
Adding and Sharing a Network Printer 320
Sharing Locally Connected Printers 324

Adding Client Drivers for Shared Printers 325
Managing Printers from Windows SBS 326
Managing Printers from the Command Line 327
Setting Security Options 328
Determining Printer Availability 328
Group Priorities and Printer Availability 329
Setting Up a Printer Pool 331
Configuring Print Spooling 332
Using the Fax Service 333
Adding a Fax Modem 333
Starting and Configuring the Fax Service 334
Managing Fax Users and Administrators 336
Summary 336

Chapter 14 Managing Computers on the Network 337

Connecting Computers to the Network 337
Creating Computer Accounts 338
Establishing Basic Network Connectivity 338
Using the Small Business Server Connect Computer Wizard 342
Connecting Alternate Clients 349
Using Remote Web Access 351
Connecting to RWA 352
Managing Computers 354
Viewing and Modifying Client Computer Settings 356
Remotely Managing Computers 358
Removing Computers from the Network 361
Summary 362

Chapter 15 Managing Software Updates 363

Why Patching Is Important 364

The Patching Cycle 365

- Assess 366
- Identify 367
- Evaluate and Plan 368
- Deploy 369
- Repeat 370

Using SBS Software Updates 370

- Configuring Software Update Settings 370
- Deploying Updates 376

Third-Party Solutions 381

Summary 381

Chapter 16 Configuring Backup 383

Configuring the Backup Service 383

- Windows Server Backup Using SBS Wizards 385
- Windows Server Backup Using Native Tools 391

Using the Backup Once Wizard 395

Recovering Backups 399

- Recovering Your Server 400
- Recovering Volumes 400
- Recovering Files and Folders from the Local Server 401
- Recovering Files and Folders from Another Server 403
- Recovering Applications and Data 404
- Recovering the Operating System 406
- Restoring a Backup Catalog 411

Using the Command Line to Manage Backups 412

- Using the Windows.Serverbackup PowerShell Snap-in 413
- Using the Wbadmin Command 416

Windows Storage Server 2008 R2 Essentials 422

- Configuring Windows Storage Server 2008 R2 Essentials for an SBS Network 423

Summary 435

PART IV PERFORMING ADVANCED TASKS

Chapter 17 Windows SBS Console vs. Server Manager 439

Adding (and Removing) Roles and Features 439
Roles, Role Services, and Features 441
Adding and Removing Roles 441
Adding and Removing Role Services 450
Adding and Removing Features 454
Adding Features 455

Using the Native Consoles 457
Using the Advanced Mode of the Windows SBS Console 458
Using Server Manager 461
Directly Opening Native Consoles 464

Summary 467

Chapter 18 Configuring and Managing Email 469

Basic Email Configuration 469
Configuring Internet Mail 470

POP3 Email 474
Adding a POP3 Account 475
Setting POP3 Retrieval Frequency 477

Advanced Email Configuration 478
Using Contacts 479
Adding an Additional Email Domain Name 486
Changing the Maximum Message Size 493

Summary 494

Chapter 19 Managing Local Connectivity 495

DHCP and DNS 496
Managing DHCP 496
Managing DNS 503

Wireless Connectivity 508

Windows Firewall. 511
Setting Firewall Policies Using Group Policy 512
Firewall Rule Basics 513
Fixing Network Problems. 519
Summary. 520

Chapter 20 Managing Remote Access 521

Remote Web Access 521
Configuring the RWA Computer List 523
Enabling or Disabling a User for RWA 530
RWA Links List 533
Virtual Private Networks 538
Enabling VPNs 539
Configure VPN Permissions 541
Fixing Network Problems. 542
Summary. 546

Chapter 21 Using Group Policy 547

Components of Group Policy 548
Group Policy Objects 548
Managing Group Policies. 549
Order of Inheritance 551
Order of Implementation 552
Creating a Group Policy Object 553
Deleting a Group Policy Object 554
Managing Group Policy Links 555
Setting the Scope of the GPO 555
Enabling and Disabling GPO Links 556
Disabling a Branch of a GPO 557
Refreshing Group Policy. 557
Backing Up a Group Policy Object. 559
Restoring a Group Policy Object 560

Deploying Applications with Group Policy 560
Publish or Assign Applications 561
Creating a Software Distribution Point 562
Creating a GPO for Software Deployment 563
Configuring the Group Policy Software Installation Extension 564
Group Policy Preferences 568
Using Group Policy Preferences for Windows 571
Configuring Common Options 574
Using Group Policy Preferences for Control Panel 575
Using Group Policy Results 576
Summary 578

Chapter 22 Managing Reports 579

Network Reports 579
Customizing the Summary Report 580
Customizing the Detailed Network Report 582
Creating a New Report 584
Configuring Alerts 585
Alerts for Services 586
Performance Counter Alert 587
Event Log Error Alerts 588
Creating Custom Alerts 588
Creating an Alert for a Stopped Service 589
Custom Alert for Backup Failure 594
Summary 595

Chapter 23 Customizing a SharePoint Site 597

Introducing SharePoint Foundation 2010 597
Understanding SharePoint Items 598
Understanding SharePoint Roles 599
Customizing Companyweb 606
Adding a Workspace 606
Adding RemoteApps Links 613
Summary 624

PART V PREMIUM EDITION FEATURES

Chapter 24 Installing the Second Server 627

Minimum System Requirements 627

Installation and Initial Configuration 629

Installation 630

Initial Configuration 636

Customizing the Server 648

Closing the Initial Configuration Tasks Wizard. 654

Summary. 655

Chapter 25 Installing Microsoft SQL Server 2008 R2 Standard Edition for Small Business 657

Installation Options. 657

Installation Restrictions 658

Installing SQL Server (Part One) 658

Planning 659

Installation 662

Maintenance 663

Tools 663

Resources 663

Advanced 664

Options 665

Installing SQL Server (Part Two) 665

Summary. 671

Chapter 26 Adding a Terminal Server 673

New Remote Desktop Services Features. 673

RD Gateway 674

RemoteApps 674

RD Web Access 674

Concepts 675
Remote Access 675
Central Management 676
Licensing 677
Installing the Remote Desktop Services Role 678
Configuring RD Licensing 688
Installing Remote Desktop Licensing 688
Assigning the Licensing Server and Licensing Mode 692
Configuring RemoteApps 694
RemoteApp Manager 695
Deploying with .rdp and .msi files 698
Adding a RemoteApp to Remote Web Workplace 700
Summary 708

PART VI MAINTENANCE AND TROUBLESHOOTING

Chapter 27 Performance Monitoring 711

Resource Monitor Overview 712
Filtering Information from Resource Monitor 716
Troubleshooting Troublesome Applications 716
Using Performance Monitor 717
Adding Performance Counters 718
Changing the Performance Monitor Display 719
Saving the Performance Monitor Display 720
Using Reliability Monitor 720
Viewing Reliability Monitor on a Remote Computer 721
Creating a Data Collector Set 721
Managing Collected Data 727
Working with Data Log Files 729
Viewing Reports 730
Summary 731

Chapter 28 Disaster Planning 733

Planning for Disaster 733
Identifying the Risks 735
Identifying the Resources 736
Developing the Responses 736
Testing the Responses 740
Iterating 741
Preparing for a Disaster 742
Setting Up A Fault-Tolerant System 742
Backups 743
Restoring from Backup 743
Virtualization and Disaster Planning 747
No USB Support 747
Hardware Independence 748
Summary 748

PART VII APPENDICES

Appendix A Introduction to Networks 751

Servers 751
Clients 752
Media Connecting Servers and Clients 752
Features of the Windows Operating System 752
Domains and Workgroups 753
Do Workgroups Work? 753
Defining Domains 754
Domain Components 755

Appendix B Automating Installation **757**

Appendix C Additional Resources **759**

Microsoft Resources **759**

Other Resources for SBS Users and Consultants **760**

Index *761*

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

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

microsoft.com/learning/booksurvey

Introduction

If you run a small business, you don't need us to tell you that the highly competitive marketplace, unpredictable economic cycles, time pressures, and technological demands are constantly exerting pressure on your bottom line.

Your business needs the same technologies that large companies do. You need the ability to share information with customers, partners, and employees. You have the same worries about spam, malware, and security. And you have the same need to manage resources and employee access to those resources.

The major difference is you probably don't have the luxury of an in-house IT staff.

Windows Small Business Server (SBS) 2011 allows small businesses to operate at the same technology level as much larger organizations, but without the added costs of maintaining a network administration department.

Windows Small Business Server 2011 Administrator's Companion is a reference, assistant, and coach for the busy network administrator, whether the administrator is on the scene or accessing the network from another location.

Conventions

Even though Windows Small Business Server 2011 has automated many, many of the tasks associated with configuring and securing a network, this book is required when you want to do something slightly out of the ordinary—or when you need additional understanding of what a wizard is doing.

Look for book elements such as these:

Under the Hood Because wizards are so efficient at what they do, it can be very difficult to know what's going on in the background. Sidebars titled "Under the Hood" describe the technical operations being performed by the wizard. These sidebars also include methodological information to help you understand Windows Small Business Server.

Real World Everyone can benefit from the experiences of others. "Real World" sidebars contain elaboration on a particular theme or background based on the adventures of other users of Windows Small Business Server.

NOTE **Notes include tips as well as alternative ways to perform a task or information that needs to be highlighted.**

IMPORTANT **Information marked Important shouldn't be skipped. (That's why these elements are called Important.) Here you'll find security notes, cautions, and warnings to keep you and your network out of trouble.**

What's in This Book

Windows Small Business Server 2011 Administrator's Companion is divided into seven parts. The first four parts roughly correspond to the developmental phases of a Windows Small Business Server network. Part V deals with Premium Add-on features, and Part VI covers maintenance and troubleshooting. The last part is made up of appendices with helpful information.

Part I, Preparation and Planning Planning and preparation are the *sine qua non* for any kind of network. It comes down to the old saying, "If you don't have the time to do it right, how will you find the time to do it over?" Chapters 1 through 4 are all about doing it right the first time.

Part II, Installation and Setup Chapters 5 through 8 take you through the process of installing Windows Small Business Server and performing initial configurations using the Getting Started Tasks. This section includes helpful chapters on configuring Windows SBS virtualization and migrating from Windows SBS 2003.

Part III, Performing the Basic Tasks Chapters 9 through 16 cover the day-to-day tasks in running a network: configuring disks, setting up user accounts, arranging the sharing of information among users, adding and removing computers and printers, managing software updates, and backing up and restoring data.

Part IV, Performing Advanced Tasks Chapters 17 through 23 provide insight and information about managing email, connectivity technologies, and using Group Policy. In this part, you'll also find chapters about setting up and managing a SharePoint site.

Part V, Premium Edition Features Chapters 24 through 26 address features found the in Windows SBS 2008 Premium Add-on. These chapters are about installing a second server, installing Microsoft SQL Server, and adding terminal servers to your network.

Part VI, Maintenance and Troubleshooting Chapter 27 covers the extensive library of monitoring tools available in Windows Small Business Server, and Chapter 28 is all about how you save your business, your network, and yourself in the face of the many varieties of disaster that can afflict networks.

Part VII, Appendices The final part consists of appendices with supplemental information. This includes an introduction to networking, instructions for automating installation, and a list of resources for the users of Windows SBS 2011.

About the Companion Web Content

The companion content for this book contains Windows PowerShell scripts for common adminstrative tasks.

These files can be downloaded from the web at:

http://go.microsoft.com/FWLink/?Linkid=217073

Full documentation of the contents and structure of the companion files can be found in the Readme.txt file.

Your Companion eBook

The eBook edition of this book allows you to:

- Search the full text
- Print
- Copy and paste

To download your eBook, please see the instruction page at the back of this book.

Acknowledgments

As most people know, the creation of a book is a collaborative process. The ink-stained wretches who do the actual writing are only part of a large and multi-talented team.

First, thanks to the numerous people at Microsoft who were of great assistance.

Kevin Beares helped us many times in ways from small to very large.

Thanks to Sean Daniels of the SBS product group for more things than we can remember. Sean was the first call whenever we needed something beyond the ordinary.

Thanks to Jonas Svensson for being responsive and effective when we needed builds and resources.

And much gratitude to the entire SBS Product Group for giving us a great product and for pulling out all the stops to get us what we needed. They really went above and beyond.

Thanks to Greg Starks of Hewlett-Packard for his support of the SMB community, and in particular his support of our HP server when we needed it.

Of course, the people at Microsoft Press are the ones that really made the book possible. In particular senior editor Ken Jones, project editor Laura Sackerman, and technical editor Andrew Edney, as well as Teresa Elsey (production editor), Sumita Mukherji (vendor coordinator), Ron Bilodeau (compositor), Rob Romano (illustrator), and the rest of the production team.

We owe a true debt to Roger LeBlanc, who edited this book with a knowing and careful hand. It's a much better book because of his efforts.

Additional and sincere thanks to Richard Siddaway for his blog post on Windows Server Backup and the PowerShell Snap-in for it. And to Sean Wallbridge, SharePoint MVP, whose help in sorting through the changes in how SharePoint Foundation 2010 behaved with Web Parts was indispensable.

Errata

We have made every effort to ensure the accuracy of this book and its companion content. If you do find an error, please report it on our Microsoft Press site:

http://aka.ms/649118

You will find additional information and services for your book on its catalog page. If you need additional support, please email Microsoft Press Book Support at mspinput@microsoft.com.

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

We Want to Hear from You

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

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

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

Stay in Touch

Let us keep the conversation going! We are on Twitter:

http://twitter.com/Microsoft

This page intentionally left blank

CHAPTER 3

Planning Your SBS Network

Before you actually start installing Windows Small Business Server 2011 Standard, you should spend some time and thought planning what your network will look like. Time spent now, *before* you actually start installing anything, will save you time, energy, and complications later. By designing your network infrastructure, naming conventions, and network security before you actually implement them, you'll save costly reconfiguration later.

Planning the Network Infrastructure

The first tasks in designing a network for your company are

- Evaluating the computing needs of the organization
- Choosing an Internet connection method and local network type
- Selecting network devices
- Choosing server hardware
- Choosing client hardware and software

UNDER THE HOOD **Network Operating Systems**

On an ordinary PC, the role of the operating system is to manage the file system; handle the running of applications; manage the computer's memory; and control the input and output to attached devices such as cameras, printers, and scanners. A network operating system expands that role, managing the following:

- **Centralized security**
- **Remote access**
- **Remote file systems**
- **Running shared applications**
- **Input and output to shared network devices**
- **CPU scheduling of networked processes**

When multiple computers are connected in a *workgroup*, as shown in Figure 3-1, the result is called a *peer-to-peer network*: a network without a central server and with no network operating system.

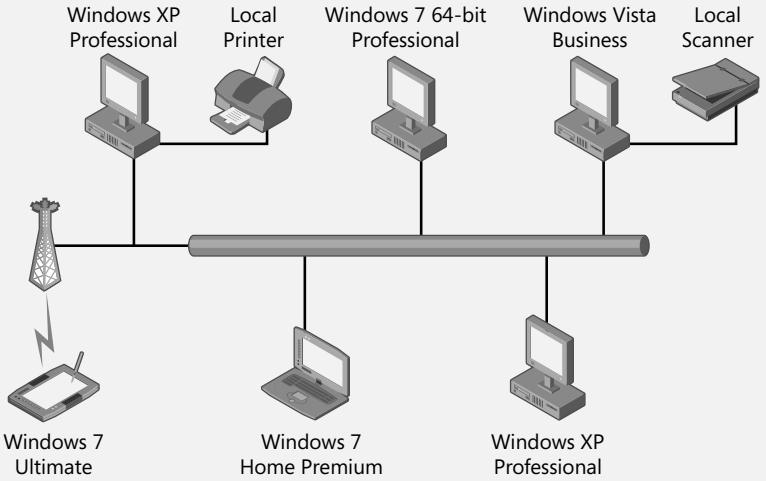


FIGURE 3-1 A peer-to-peer network, which has no central server or management

Adding one or more servers running Windows Server 2008 R2 or a Windows Small Business Server 2011 Standard, as shown in Figure 3-2, is a *client/server-based network*—one or more servers and multiple clients, all sharing a single security policy. The servers provide both the resources and the security policy for the network, and the clients are the computers that use the resources managed by the server.

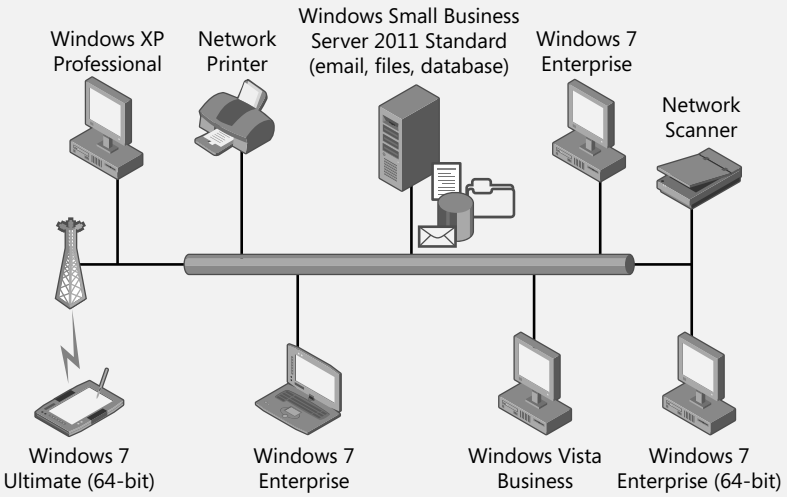


FIGURE 3-2 A client/server network, which has a central management and resource server

Servers Use Network Operating Systems

Because SBS 2011 has to supply services to as many as 75 users, and you're depending on it to run your business, a high-powered, robust operating system and highly reliable hardware are essential. When your users rely on a server to get their work done and keep your business running, you certainly don't want frequent failures—you don't even want to reboot!

In addition to supplying print, file, or other services, the network operating system has to provide network security. Different businesses and organizations have varying security needs, but *all* must have some level of data protection. Therefore, the system must offer a range of configurable security levels, from the relatively nonintrusive to the very stringent.

Clients Use Workstation Operating Systems

Like other computers, client computers on a network need an operating system. However, a client operating system doesn't need to manage the resources for other computers or manage security for the network. Rebooting a workstation can be an annoyance for the user but doesn't usually disrupt anyone else's work.

On a Windows Small Business Server network, clients can run Microsoft Windows XP Professional (including Windows XP Tablet PC Edition and Windows XP Professional x64 Edition) and business editions of Windows Vista or Windows 7. However, for best performance and security, Windows Vista SP1 or Windows 7 should be deployed on clients.

Determining Your Needs

Before designing a network, decide which features of SBS 2011 your business needs; doing so helps ensure that the network design is dictated by business needs rather than by fancy technology. Key needs to consider include

- Centralized user account management
- Centralized update management
- Web and email access for employees
- File sharing and centralized file storage
- Database storage using Microsoft SQL Server
- Printer sharing
- Centralized backup
- Centralized fax server

- Remote access to the internal network via the Internet, including remote access directly to the user's desktop from the web
- Management of remote computers
- Collaboration and document management (SharePoint Foundation 2010)

You also must decide how important the following factors are, as well as what resources are available to support your choices:

- Performance
- Reliability
- Security

PLANNING **Get a thorough idea of what kind of work will be done on the network, when and where it will be done, and by whom. For example, your organization might need to do payroll every other Friday, during which time the file server and printers are under a heavy load.**

Choosing an Internet Connection

To choose an Internet connection method, you must balance an organization's bandwidth needs and budget against the available Internet connection methods. The following sections discuss how to do this, as well as how to choose an Internet service provider (ISP).

Determining Bandwidth Needs

First, determine the baseline level of bandwidth you require. You can then balance this against the organization's budget and performance goals. Allow for 100 kilobits per second (Kbps) of download bandwidth and 50 Kbps of upload bandwidth for each simultaneous user of email and the web. If remote access is important, allow for a minimum of 100 Kbps of upload bandwidth for each simultaneous remote access user. Table 3-1 lists various Internet connection speeds and the number of users supported for each speed, assuming that users will be browsing the web and using email. This table does *not* include requirements for remote connections.

IMPORTANT **Running an Internet-accessible web server on your network requires at least 50 Kbps or more of upload bandwidth per simultaneous visitor, depending on the size of images or files. This can quickly swamp your Internet connection, which is one reason most small businesses pay for web hosting.**

TABLE 3-1 Bandwidth requirements for web browsing and email

DOWNLOAD/UPLOAD SPEED	NUMBER OF USERS
256/128 Kbps	1–5
512/256 Kbps	1–5
1024/512 Kbps	5–10
3072/768 Kbps	10–20
5120/1024 Kbps	15–30

NOTE **These bandwidth numbers are not intended to be definitive—they are a minimum planning baseline. Each organization and its users have different usage patterns and needs, and you should evaluate your needs accordingly. Be prepared to add more bandwidth if necessary. Your users will never complain that the Internet connection is too fast, but they will definitely complain if it's too slow!**

UNDER THE HOOD **Bits and Bytes**

Network speeds are measured in either kilobits per second (Kbps) or megabits per second (Mbps), whereas download speed and hard disks are rated in kilobytes per second (KBps) or megabytes per second (MBps). For example, a 640-Kbps DSL connection might download files at 60 KBps from a fast website, but a 1.5-Mbps cable Internet connection might download at 180 KBps from the same site. (Some of the bandwidth is used up by transmission overhead and inefficiencies.) When you compare network speeds, make sure you're using the same units of measurement.

Types of Internet Connections

To choose an Internet connection method, you need to know which methods are available as well as their performance characteristics. Table 3-2 lists the most common connection methods and their speeds.

TABLE 3-2 Internet connection types

TYPE OF CONNECTION	DOWNLOAD SPEED	UPLOAD SPEED	NOTES
Dial-up	28.8–53 Kbps	28.8–40 Kbps	Analog telephone line. Sometimes referred to as Plain Old Telephone Service (POTS).
ISDN (Integrated Services Digital Network)	64–128 Kbps (one channel or two)	64–128 Kbps (one channel or two)	Must be within 50,000 feet of a telephone company central office (CO). Connection is dial-up (not persistent).
ADSL (Asynchronous Digital Subscriber Line)	256 Kbps–8 Mbps	128 Kbps–1 Mbps	Must be within 18,000 feet of a CO.
IDSL (DSL over ISDN)	128–144 Kbps	128–144 Kbps	Works at greater distances from a CO than other DSL variants.
SDSL (Synchronous DSL)	128 Kbps–2.3 Mbps	128 Kbps–2.3 Mbps	Must be within 20,000 feet of a CO.
Cable	128 Kbps–15 Mbps	128 Kbps–1 Mbps	Must have access to broadband cable service; speed can fluctuate depending on the number of users on a given cable loop.
Microwave wireless	256 Kbps–10+ Mbps	256 Kbps–10+ Mbps	Must be in line of sight to the ISP's antenna; maximum distance 10 miles.
Frame relay/T1	56 Kbps–1.54 Mbps	56 Kbps–1.54 Mbps	Good availability; very reliable; consistent throughput; expensive.
802.11b (WiFi)	Up to 11 Mbps	Up to 11 Mbps	Speed decreases with increasing distance from access point.
802.11g or 802.11a	Up to 54 Mbps	Up to 54 Mbps	Speed decreases with increasing distance from access point.
802.11n	Up to 540 Mbps	Up to 540 Mbps	Speed decreases with increasing distance from access point.
Geosynchronous satellite	150 Kbps–3 Mbps	33.6 Kbps–128 Kbps	Requires line of sight to satellite (southern sky in North America). Unsuitable for real-time multimedia because of high latency.
Ethernet	10 to 1000 Mbps	10 to 1000 Mbps	Limited availability. Backbone connection might be DSL or T1, limiting actual bandwidth.

Choosing ISPs

After determining the preferred connection type and bandwidth, it's time to actually find ISPs. Two websites to check are *http://www.cnet.com/internet-access* and *http://www.dslreports.com*. In addition to speed and cost, look for the following features:

- **Static IP address** To host any kind of Internet-accessible service such as email, Microsoft Outlook Anywhere, remote access, or websites, you need a static IP address or an ISP that supports the Dynamic DNS service, or you need to manage your external DNS with a DNS service that supports dynamic updates, such as *http://www.zoneedit.com*. SBS 2011 includes support for tzo.com dynamic DNS if you use the built-in wizards to register or transfer your domain name.
- **Terms of service and ports** Many ISPs have terms of service (TOS) on consumer-grade accounts that prohibit hosting email servers, or they have a policy that blocks specific ports such as port 25. You need to ask *before* you buy.
- **Transfer limitations** If the ISP has a monthly data transfer limit, make sure the limit isn't lower than your anticipated usage—charges for going beyond the limit can be significant.
- **Web hosting** If you want the ISP to host the organization's Internet website, look for virtual hosting (so that your organization can use its own domain name) with enough disk space on the ISP's web servers.
- **Backup Internet connection** If your business is dependent on always being connected to the Internet, choose a secondary Internet connection with sufficient bandwidth to allow you to maintain minimal service in case the primary Internet connection fails. This second Internet connection should use a different ISP and a different connection technology. You can use a dual WAN router to use both connections simultaneously.

Choosing a Network Type

The next step in designing a network is to choose a network type. (See Table 3-3.) Start by looking at where your computers are physically located. If you can easily run cable between all computers, the choices are simple: Gigabit Ethernet (GigE) or Fast Ethernet (100BaseT). Choose GigE if your wiring supports it; otherwise, stick to Fast Ethernet. If you're installing new cabling, hire a professional cabling expert. Spending money on good wiring now can save you a *lot* of problems in the future.

If the computers are widely scattered or mobile, consider including some wireless *access points* (APs). These are network devices that permit wireless clients access to a wired network. Even Fast Ethernet is virtually as fast as the real-world speeds of the fastest current wireless standard (802.11n), while being far more reliable, more secure, and cheaper as well. For these reasons, use wireless networks to supplement wired networks, not to replace them.

MORE INFO **For more information about wireless access points, see the section "Choosing a Wireless Standard: 802.11a/b/g/n" later in this chapter.**

SECURITY ALERT **All wireless technologies have the potential to introduce security risks. When using wireless networking, always use appropriate security measures, such as Wireless Protected Access (WPA), 802.11i (WPA2), or 802.1x. For more information, see the section "Planning for Security" later in this chapter.**

TABLE 3-3 Common network types

TECHNOLOGY	SPEED	SPEED (REAL WORLD)	CABLING	MAXIMUM DISTANCE	OTHER HARDWARE REQUIREMENTS
Fast Ethernet	100 Mbps	94 Mbps	Cat 5, Cat 5e, Cat 6	328 feet from hub or switch	Fast Ethernet hub or switch
Gigabit Ethernet	1000 Mbps	327 Mbps	Cat 5e or Cat 6	328 feet from hub or switch	Gigabit hub or switch
802.11b (WiFi)	11 Mbps	4.5 Mbps	Wireless	1800 feet (60–150 feet typical indoors)	802.11b or 802.11g access point (AP), 32 users per AP
802.11a	54 Mbps	19 Mbps	Wireless	1650 feet (50–100 feet typical indoors)	802.11a AP, 64 users per AP
802.11g	54 Mbps	13 Mbps	Wireless	1800 feet (60–150 feet typical indoors)	802.11g AP, 32 users per AP
802.11n	540 Mbps	130 Mbps	Wireless	7200 feet (100–500 feet typical indoors)	802.11n AP, 32 users per AP

NOTE **Wireless speeds vary greatly depending on the distance from the access point, and the number and type of walls, floors, and other interference between the access point and the client device.**

BEST PRACTICES **Avoid the consumer-focused HomePNA and HomePlug network types. They're more expensive, slower, less secure, and less reliable than Ethernet or a properly configured 802.11a/b/g/n wireless network.**

Choosing the Right Network Cable

Choosing the right cable for a wired Fast Ethernet (100 Mbps) network is easy—Cat 5 cable. However, there are exceptions to this rule that pertain to existing installations and new construction.

Cables in an existing network might not be usable. 10-megabit Ethernet equipment might be usable for small networks until it can be replaced, but expect to replace it soon—you'll find it slow. Coaxial (thinnet) Ethernet and Cat 3 Unshielded Twisted Pair (UTP) cables are unreliable and slow and should be replaced.

New construction should run several strands of Cat 5e or, ideally, Cat 6. Although Cat 5 cable can be used with Gigabit Ethernet, it is marginal at best. Cat 5e and Cat 6 cables are more reliable and provide headroom for possible 10-Gigabit Ethernet standards. Cables should converge at a reasonably clean, centrally located wiring closet with adequate power, ventilation, and security for all servers and network devices. (Be sure to leave room for future growth.)

Shielded Cat 5, Cat 5e, and Cat 6 cables are available for situations that potentially involve high levels of electromagnetic interference (such as antennas). You should use plenum-grade cable any time wiring is placed in a drop ceiling. (Before running cable in a drop ceiling, talk to the building manager.)

Choosing a Wireless Standard: 802.11a/b/g/n

Currently, you can choose from four wireless standards: 802.11b, 802.11a, 802.11g, and 802.11n. Here's what you need to know about each (also refer to Table 3-3):

- **802.11b** 802.11b was the first widely deployed standard, though the speed was limited (11 Mbps theoretical; 5 Mbps or even less in the real world). 802.11b supports a maximum of 32 users per AP, and a maximum of 3 simultaneous channels in use in the same location. *Channels* separate wireless networks, with each channel providing 11 Mbps of bandwidth. You should not buy new equipment that supports only 802.11b, and if you currently have 802.11b equipment, you should upgrade it to 802.11n. There are serious security considerations with older wireless hardware that preclude it from being deployed in a business environment.

- **802.11g** 802.11g is faster than 802.11b (54 Mbps theoretical; 13 Mbps real-world) and backward-compatible with 802.11b. 802.11g supports a maximum of 32 users per AP, and a maximum of 3 simultaneous channels in use in the same location.
- **802.11a** 802.11a is faster than 802.11g (54 Mbps theoretical; 19 Mbps real-world) and is more tolerant of microwave interference and network congestion because it uses the 5 GHz frequency band. 802.11a supports a maximum of 64 users per AP, and a maximum of 8 channels in use simultaneously in the same location. 802.11a is not compatible with either 802.11b or 802.11g.

  If you decide to use 802.11a network devices, stick with devices from the same vendor and consider a tri-mode 802.11a/b/g device that will allow other devices, such as laptops with built-in 802.11b/g connectivity, to work on the wireless network. (This strategy also permits the highest network density, with 11 channels available simultaneously for wireless networks.)
- **802.11n** 802.11n is faster than 802.11g (up to 540 Mbps theoretical; 100–130 Mbps real-world) and backward-compatible with 802.11g and 802.11b. Most 802.11n equipment is in the same frequency band (2.4 GHz) as 802.11b/g, but the standard supports dual-band equipment that can also use the 5-GHz range of 802.11a. This dual-band equipment provides the greatest flexibility and compatibility and is especially good at avoiding interference from other equipment. Choosing dual-band equipment from a single OEM is the safest choice for compatibility at the highest speeds. If you're buying new wireless equipment, we strongly recommend 802.11n and prefer dual-band 802.11n where possible.

Choosing Network Devices

After selecting a network type and Internet connection method, create a network diagram to visually show which network devices are needed. Then select the necessary devices for the network, such as switches, wireless access points, firewalls, and network adapters.

BEST PRACTICES **Choose a single brand of network hardware if possible. This ensures greater hardware compatibility, simplifies administration, and makes obtaining vendor support easier.**

Diagramming the Network

Creating a diagram of the network can quickly show which devices you need and where they should be located, as shown in Figure 3-3.

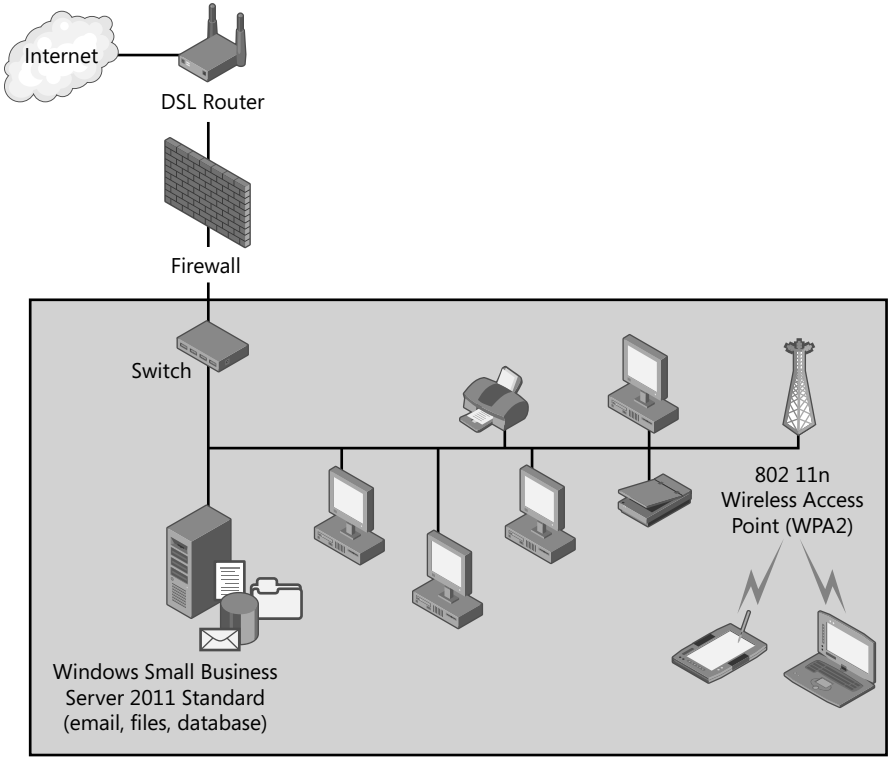


FIGURE 3-3 A network with the Windows Small Business Server computer connected directly to the Internet

Use the following list as a guide when creating the network diagram:

- **Internet connection** The Internet connection usually comes in the form of a telephone or coaxial cable that connects to a DSL or cable router. It is traditionally represented by a cloud at the top of the drawing and a line that connects to the router or firewall.
- **DSL or cable modem** The Internet usually enters the organization in the form of a telephone or cable line that plugs into a DSL or cable modem.

- **Firewall** The DSL or cable modem is then plugged into the firewall, which should be a router or firewall. Some modems are combined with built-in routers that have basic firewall capabilities. Consumer routers or DSL modems are not sufficient protection for a business network.
- **Perimeter network** This is an optional area of the network between the DSL or cable modem and the firewall, where low-security devices such as wireless access points can be placed.
- **Internal network** The internal network includes the SBS computer, the client computers, and any network-connected devices, such as printers.

PLANNING **Wireless access points should be on the internal network and use 802.11i (WPA2) encryption. You can also place access points in the perimeter network when you want to provide Internet access to the general public (such as in a coffee shop, conference room, or lobby).**

Choosing a Network Switch

Ethernet networks use the *star* network topology (also known as *hub and spoke*), which means that all network devices must be plugged into a central hub or switch. Choosing the right switch requires evaluating the following factors:

- **Switch or hub** Don't buy a hub unless you have a specialized need and understand why you're doing it. Get a switch instead. Switches are inexpensive, provide additional performance, and facilitate mixing 10 Mbps, 100 Mbps, and 1 Gbps devices on the same network segment.
- **Number of ports** Make sure that the switch provides more than enough ports for all computers, access points, network printers, and Network Attached Storage (NAS) devices on the network, along with spare ports for expansion or to use in the event of a port failure.
- **Speed** Fast Ethernet (100/10 Mbps) switches offer basic performance for small businesses, but GigE (1000/100/10 Mbps) switches are hardly different in price and provide extra bandwidth for improved performance of file servers and high-quality streaming video where the network cabling will support it.
- **Management** Managed switches provide the ability to view the status of attached devices from a remote connection, which can be useful for off-site technicians. In general, save the cash and stick with an unmanaged switch unless the cost difference is slight or the organization uses an off-site consultant who wants the ability to remotely administer switches.

Choosing Wireless Access Points

As you learned earlier in the chapter, wireless access points permit clients to wirelessly connect to a wired network. Access points are often integrated into routers, but they are also available as stand-alone devices that must be plugged into a switch like any other network device. Avoid wireless "gateway" or router products for connecting to your internal network—they will complicate your network management and TCP/IP configuration. They're fine for externally connected wireless access points. Some wireless routers can be reconfigured to be simple access points.

NOTE **Business-grade access points are more expensive than consumer-oriented access points; however, they are usually more reliable and full-featured.**

When choosing an access point, consider the following features:

- Routers with built-in access points are often no more expensive than stand-alone access points and are useful when creating a perimeter network. But be sure they can be used as a pure access point—many can function only as a router, which will complicate your network setup.
- Access points should support 802.11i (WPA2). WEP is simply not acceptable for any wireless device connected to your internal network, and even WPA should not be considered sufficient protection for an internally connected access point.
- Access points should support 802.1x (RADIUS) authentication if you want to provide the highest level of security and ease-of-use to a wireless network.

SECURITY ALERT **Two "features" that some suggest to improve wireless security are disabling of SSID broadcasts and Media Access Control (MAC) address filtering. Don't bother. They are a significant and ongoing administrative burden, and a hacker with a port scanner can easily defeat them anyway.**

- Some access points have two or more antennas that can be adjusted for better coverage; others support external antennas that can be mounted on a wall for better placement.
- Stand-alone wireless bridges (often referred to as *wireless Ethernet bridges*) and some access points provide the ability to wirelessly bridge (connect) two wired networks that can't be connected via cables. There are a number of different types of bridging modes, including Point-to-Point and AP Client. Point-to-Point uses two wireless bridges to link two wired networks. AP Client uses an AP on the main network (to which wireless clients can connect) and a wireless bridge in AP Client mode on the remote network segment, acting as a wireless client.

Clients on the other side of a wireless bridge will experience slower performance to the main network segment because of the shared wireless link, so use wireless bridges with discretion, and always use bridges and APs made by the same manufacturer.

- Don't include "turbo" or other high-speed modes offered by some manufacturers in your buying criteria. They provide little performance gain, if any, in the real world and can have a deleterious effect on compatibility.

REAL WORLD Placing Access Points for the Best Coverage

Wireless access points have a limited range, especially in the environment of a typical office. The indoor range of 802.11b, 802.11g, and tri-mode 802.11a access points is usually around 60–100 feet at the highest connection speed, and 25–75 feet for first-generation, single-mode 802.11a access points.

That said, 2.4-GHz cordless phones, microwave ovens, and Bluetooth devices can cause serious interference with 802.11b and 802.11g networks (but not with 802.11a networks) when they are turned on. Fluorescent lights, metal walls, computer equipment, furniture, and standing too close to the access point can also reduce the range of wireless networks.

Unfortunately, there is no reliable way to quantify these variables—trial and error is the best way to position access points. With 802.11n, and especially dual-band 802.11n, the effective distance is at least double that of 802.11g, but this still requires full 802.11n deployment and optimal conditions. In our initial tests of 802.11n, it does appear to provide a more stable and reliable signal at a significantly greater distance than our previous 802.11a/g equipment. There are some useful guidelines when selecting access point locations:

- **Place the access point and wireless network card antennas as high as possible to get them above objects that might attenuate the signal.**
- **If you place access points in the plenum (the space inside a drop ceiling or raised floor), make sure you obtain access points or enclosures certified for plenum installation.**
- **Place the access point in the center of the desired coverage area to provide the best coverage while also reducing the publicly exposed "surface area" of the network.**
- **Only use the minimum signal strength (power) required to provide coverage for your office. Most WAPs have multiple levels of signal strength but ship with a default of "maximum."**
- **Use multiple access points as necessary to cover multiple floors or large offices, or to service a large number of clients simultaneously. Twenty clients per 802.11g AP**

is a reasonable maximum, with an average of no more than two to four simultaneously active users per AP yielding the best network performance.

- **Use wireless bridges to place another Ethernet network segment (or another wireless access point) in a location unreachable by cables. Wired clients on this segment communicate with other wired devices on this segment at the speed of the wired network (1000/100/10 Mbps); however, communication with the main network segment takes place at the speed of the wireless network (10–100 Mbps real-world bandwidth).**
- **When selecting channels for access points, *sniff* (search by using a wireless client) for the presence of other networks and then choose an unused channel, preferably one that is four or more channels separated from other channels in use. For example, channels 1, 6, and 11 can be used simultaneously without interference.**

Choosing a Firewall Device or Router

SBS 2011 is designed to connect directly to a firewall and does not provide any direct protection for the rest of the SBS network. This is a major change from earlier versions of SBS that acted as the gateway between the Internet and the internal network when SBS was deployed with two network cards (NICs). Windows Small Business Server 2011 Standard includes the new Windows Firewall that is part of Windows Server 2008 R2 to protect the server, but it should be protected by an additional, separate firewall that will also act to protect the computers on the internal network.

You should look for the following features on your network firewall device:

- **Packet filtering** Firewalls should support inbound packet filtering and Stateful Packet Inspection (SPI).
- **Protection from specific attacks** Firewalls should support protection from the denial-of-service (DoS) attacks and other common attacks such as Ping of Death, SYN Flood, LAND Attack, and IP Spoofing.
- **Network Address Translation (NAT)** NAT is the backbone of most firewall devices, providing basic security and Internet connectivity to internal clients.
- **IPv6 Support** As IPv6 becomes more pervasive, and as our pool of available IPv4 addresses approaches exhaustion, the need to directly support IPv6 for our Internet connection becomes more compelling. Choosing a firewall device that fully supports IPv6 now will save money and time later.
- **VPN pass-through** To permit properly authenticated Internet users to establish VPN connections with a Windows Small Business Server computer behind a firewall, the firewall must support VPN pass-through of the desired VPN protocol (PPTP, L2TP, and/or IPSec).

- **VPN tunnels** Some firewall devices provide direct support for establishing VPN connections. If you do choose to use a firewall device to establish VPN connections with clients and servers in remote offices, make sure the firewall supports the necessary number of simultaneous VPN tunnels.
- **UPnP support** Windows Small Business Server can automatically configure firewalls that support Universal Plug and Play (UPnP) to work with Windows Small Business Server services such as Exchange Server and remote access (by opening the necessary ports on the firewall). UPnP support can be found in most consumer firewall devices as well as in some business firewalls.

NOTE **Enabling UPnP on a dedicated firewall device makes configuring the device to work with Windows Small Business Server easy, but it does have security implications. We suggest using UPnP to do the initial setup of the firewall device, if the device supports it, but then disabling UPnP completely.**

- **Dual-WAN support** Some firewalls come with support for two WAN connections to increase speed and reliability, which is a great solution for networks looking for a reliable Internet connection. Other firewalls provide a serial port so that an external dial-up modem can be used as a backup connection, but this connection is much slower.
- **RADIUS support** RADIUS support on your firewall will enable additional functionality and security, including easily integrating Two Factor Authentication (TFA) into your remote access configuration.
- **Content filtering** Most firewalls make blocking certain websites possible, such as websites containing specified keywords. Many businesses use this feature to reduce the employees' ability to visit objectionable websites, although most content filters are largely ineffective.
- **Built-in wireless access point** Firewalls with built-in access points and switched, GigE, wired ports combine several functions and can be a cost-effective solution. However, their primary function is to protect the network, and that should be the first and most important evaluation criterion.

Choosing Server Hardware

If you have a server that can meet the capacity needs of the network or can be upgraded to do so while allowing for future growth, by all means use this server. But realistically, because there is no in-place upgrade to Windows Small Business Server 2011 Standard, you should plan on buying a new server as part of your migration plan.

MORE INFO **See Chapter 7, "Migrating to Windows Small Business Server 2011 Standard," for more information about migrating to SBS 2011 from an existing SBS domain.**

When evaluating server hardware, see Table 3-4, which lists the effective minimum configurations necessary for adequate performance at different load levels.

MORE INFO **The sidebar "Determining Server Load" later in this chapter provides more information about configuration and performance.**

TABLE 3-4 Minimum server configurations for different load levels

COMPONENT	LIGHT LOAD	MEDIUM LOAD	HEAVY LOAD
CPU	Quad core Intel or AMD processor	Quad core or greater Xeon or Opteron processor	Dual Xeon or Opteron processors, with at least four cores each
Memory	10–12 GB	12–16 GB	12–32 GB
Storage	Two or more hard drives in hardware mirror (RAID-1) with 200 GB available for Windows Small Business Server 2011 Standard	Four-drive, hardware-based RAID using SATA or SAS drives	Four-drive (or more), hardware-based SCSI or SAS RAID
LAN Network Adapter	100/10 Mbps PCI card	1000/100/10 Mbps PCI card	1000/100/10 Mbps PCI-x or PCIe card
Backup	Two or more external USB hard drives	Two or more external eSATA or USB hard drives	Two or more external eSATA or USB hard drives

MORE INFO **See Chapter 11, "Disk Management," for more information on RAID. See Chapter 12, "Storage Management," for more information about choosing the appropriate storage solution. See Chapter 16, "Configuring Backup," for more information about creating a backup strategy and choosing backup devices.**

UNDER THE HOOD Determining Server Load

The appropriate hardware for an SBS 2011 server depends on the load you place it under. Think of load as equal to the number of requests per unit of time multiplied by the difficulty of fulfilling each request.

The easiest way to determine load is to sample the performance of the existing server over a range of conditions. Of course, this is tricky when you're constructing a new network or restructuring an existing network. Consider the following factors:

- **The usage pattern over time (number of requests per unit of time)** **A server that handles an average load can easily become swamped at key times, such as at the beginning and end of a workday, when many users simultaneously log on or log off; during lunch, when users might browse the Internet for personal use; or around deadlines, when many users make heavy use of file, email, or database services.**
- **The kinds of user requests (the complexity of each request)** **This determines which server subsystems are stressed most heavily. Database serving stresses storage, memory, and possibly CPU; file serving stresses mostly storage and I/O; remote access stresses memory and I/O primarily; Exchange Server stresses storage, memory, and to some extent CPU.**

Choosing Client Hardware and Software

When selecting client computers for use on a network, choose systems that are fast enough to perform adequately when running Windows7 Professional. (See Table 3-5 for recommended configurations.) Other operating systems—such as Windows XP, Mac OS X, and Linux—can be made to work on an SBS 2011 network; however, they won't provide full support for many features of SBS.

TABLE 3-5 Recommended client computer configurations

COMPONENT	MINIMUM CONFIGURATION	BETTER CONFIGURATION
Operating System	Windows XP Professional SP3	Windows 7 Professional or Enterprise
CPU	Pentium 4, 2.0 GHz or faster	Dual-core processor, 2.0 GHz or faster
RAM	256 MB	2 GB
Hard drive	30 GB	100 GB
Network Adapter	Fast Ethernet or 802.11g	GigE, 802.11n
Display	15-inch monitor running at 800 x 600 resolution	17-inch monitor running at 1024 x 768 resolution

UNDER THE HOOD **Remote Desktop Services (RDS)**

Computers too slow to adequately run a Windows XP operating system can be put to use as Remote Desktop or Virtual Desktop Infrastructure (VDI) clients. In this configuration, users connect to a separate Windows Server 2008 R2 computer running the RD Session Host or RD Virtualization Host role. This server can provide a full desktop replacement (VDI) or a full desktop session (RD Session Host), or it can be used to supplement the power of the client by running key applications as RemoteApps and displaying them on the client.

This second server *cannot* be the same physical computer as the Windows Small Business Server computer unless virtualization is used to run multiple *virtual machines* (VMs) on a single physical computer. With either RDS or VDI, all processing is done on the server, and the display is sent back to the client computer, which can run any supported RDS client operating system.

This approach can make more efficient use of resources and make central management easier. The new RemoteApps simplifies deploying resource-intensive applications to users without having to upgrade everyone's computer, while the use of VDI allows full-featured Windows 7 desktops to be deployed to less powerful clients. For more information on Remote Desktop Services and VDI, see Chapter 26, "Adding a Terminal Server."

Choosing Naming Conventions

Creating naming conventions makes choosing names for computers, shared folders, and users easier and lends consistency to the network. This consistency results in a more user-friendly network.

MORE INFO **For help with naming users, see Chapter 9, "Managing Users and Groups." For help with naming shared folders, see Chapter 10, "Shares and Permissions."**

Choosing a Domain Name for the Network

The domain name is the most important and politically sensitive name on the network, and it is one you can't change without starting all over and completely rebuilding your network. Do *not* make this decision without consulting everyone who has a stake in the result. By getting others involved in the process, you'll have a much greater chance of acceptance.

Some questions to ask when choosing a domain name include

- Is the name easy to remember, and does it make sense for the company? This could be the company name in its most common form or an abbreviation.
- Is the name 15 characters or shorter? Use only letters, numbers, the underscore, and a hyphen in the name to ensure DNS and NetBIOS compatibility.
- Is the name available? If the name is already in use as an Internet domain name for another company, you'll have to either choose a different name or have a different internal and external domain name.
- If you already have an Internet website, use the same name, without the extension, for your internal domain name. For example, if the company uses *www.example.com* for its Internet website, use *example* for the domain name. The Windows Small Business Server 2011 Standard Installation Wizard will automatically add a .local extension to the name you choose.
- As soon as you choose a domain name, register it (preferably with .com, .net, or .org) on the Internet so that another company can't purchase it.

IMPORTANT **Changing your internal domain name is impossible without a complete re-installation, so picking a name that will last is critical.**

REAL WORLD Internal Domain Name vs. Internet Domain Name

There are two domain names you need to worry about when setting up your network: the Internet domain name that the outside world sees for your company and email, and the internal domain name that Windows Small Business Server uses. They are usually related but not identical. The public, Internet domain name needs to be globally unique, officially registered with a Domain Naming Service, and clearly identifiable as your company. The internal, Windows name can be anything at all, though it usually is the same as the external, public one, but with a different top-level domain.

So if your company is Example Widgets and your public Internet domain name is example.com, your internal Windows domain name could be something like example.local. This makes it easy to keep track of, and it gives you complete control over managing the internal DNS of your Windows Small Business Server network while allowing you to have a reliable third party manage your public DNS records.

Although it is technically possible to change your public name, it's neither easy nor painless, and it's virtually impossible to change your internal name without having to completely rebuild your network from scratch. So it's worth spending time up front to make sure you're choosing a name that is appropriate and has the support of all parties.

Another possibility is to choose a completely generic name for your internal domain that has nothing whatsoever to do with your company name. This works great if you change your public name because nothing has to change on your network. But it's not an approach we like. We've always preferred naming based on the company name—it's just easier for everyone to understand and remember.

Naming Computers

It's easy for *you* to keep a map of what the different clients and servers are called and where they are on the network, but if you make life hard on users, you pay in the long run. So naming all the computers after Shakespearean characters or Norse gods might make sense to you, but it isn't going to help users figure out that Puck is the Windows Small Business Server computer and Odin is the desktop used for payroll.

On the other hand, using Srv1 for the SBS server tells everyone immediately which computer it is. When naming computers, use a consistent convention and sensible names, such as the following:

- SRV1 or SBSSRV for the Windows Small Business Server 2011 Standard computer
- FrontDesk for the receptionist's computer

In this book, we'll be using a somewhat more complicated naming convention that identifies the physical host computer, the role of the computer, and the IP address of the computer. Thus our SBS server is hp160-SBS2011, signifying that it's running on the Hewlett-Packard DL 160 G6 server, and that it's running Windows Small Business Server 2011 Standard. There are several virtual machines running on that HP server, so it gets a fair workout.

Our naming convention is more complicated than most small businesses need, but it serves our needs where we are continually building and rebuilding test environments for writing projects. Ultimately, it doesn't matter what you name your computers, as long as everyone understands the convention and can find the resources they need.

Planning for Security

It is far easier to implement effective security measures to protect your SBS network if you plan for security *before* you actually start installing software. In the following sections, we'll cover some of the most common attack vectors and the preliminary steps you can take in this planning stage to prepare your defenses:

- **Careless or disgruntled employees and former employees** Internal users and former users are the biggest risk factors to data loss and data theft on most computer networks. Whether from laziness, disregard of security policies, or outright malice, the internal user is often the most dangerous on your network. To help reduce risks related to this, refer to the "Ensuring Physical Security" section of this chapter as well as to Chapter 8, "Completing the Getting Started Tasks."
- **Internet hackers** All computers and devices attached directly to the Internet are subject to random attacks by hackers. According to the Cooperative Association for Internet Data Analysis (CAIDA), during a random three-week time period in 2001 more than 12,000 DoS attacks occurred: 1200–2400 were against home computers and the rest were against businesses. If your organization has a high profile, it might also be subject to targeted attack by hackers who don't like your organization or who are engaging in corporate espionage.

  For more information about securing a network against Internet hackers, see the "Securing Internet Firewalls" section of this chapter.
- **Wireless hackers and theft of service** Wireless access points are exposed to the general public looking for free Internet access and to mobile hackers. To reduce this risk, refer to the "Securing Wireless Networks" section in this chapter.
- **Viruses and worms** Networks are subject to virus exposure from email attachments, infected documents, and worms such as CodeRed and Blaster that automatically attack vulnerable servers and clients. Refer to the "Securing Client Computers" section of this chapter for more information.

Ensuring Physical Security

Although security is not something that can be achieved in absolute terms, it should be a clearly defined goal. The most secure operating system and network in the world is defenseless against someone with physical access to a computer. Evaluate your physical environment to decide what additional security measures you should take, including the following:

- Place servers in a locked server room. And control who has keys!
- Use case locks on your servers, and don't leave the keys in them.
- Place network hubs, routers, and switches in a locked cable room or wiring closet.
- Install case locks on client systems or publicly accessible systems.

- Use laptop locks when using laptops in public.
- Use BitLocker to encrypt the data on laptops that contain sensitive data.

Securing Client Computers

Even a highly secure network can be quickly compromised by a poorly secured client computer—for example, a laptop running an older version of Windows with sensitive data stored on the hard drive. To maximize the security of client computers, use the following guidelines (refer to Chapter 8, "Completing the Getting Started Tasks," and Chapter 14, "Managing Computers on the Network," for more security procedures):

- **Use a secure operating system** Use Windows Vista or Windows 7 on all client computers, with a strong preference for Windows 7 on laptops.
- **Use NTFS, file permissions, BitLocker, and EFS** Use NTFS for all hard drives, and apply appropriate file permissions so that only valid users can read sensitive data. Encrypt sensitive files on laptop computers using the Encrypting File System (EFS), and encrypt at least the system drive on laptops using BitLocker. (BitLocker is available only on Enterprise and Ultimate versions of Windows Vista and Windows 7.)
- **Keep clients updated** Use the Automatic Updates feature of Windows to keep systems updated automatically. Ideally, use the Windows Software Update Service (WSUS), integrated into SBS 2011, to centrally control which updates are installed, as described in Chapter 15, "Managing Software Updates."
- **Enable password policies** Password Policies is a feature of SBS 2011 that requires user passwords to meet certain complexity, length, and uniqueness requirements, ensuring that users choose passwords that aren't trivial to crack.

> ***NOTE*** **Remembering passwords has become an increasingly difficult prospect, leading to the resurgence of the yellow-sticky-note method of recalling them. It's important to discourage this practice, and encourage the use of distinctive but easy-to-remember passphrases. See the Under The Hood sidebar "Beyond Passwords—Two-Factor Authentication" for an alternative to annoyingly complex passwords.**

- **Install antivirus software** Antivirus software should be installed on the SBS 2011 computer as well as on all clients. The best way to do this is to purchase a small-business antivirus package that supports both clients and the server. There are good third-party solutions specifically designed for the SBS market from several vendors.
- **Install antispyware software** Antispyware software should be installed on all client computers on the network and configured for real-time monitoring and daily full scans.
- **Keep web browsers secure** Unpatched web browsers are a significant security issue. Always keep web browsers updated with the latest security updates.

UNDER THE HOOD Beyond Passwords—Two-Factor Authentication

Password policies are a difficult subject for many small businesses. Serious security using only passwords requires long and complex passwords, changed regularly and never repeated. That's a nice goal, but it's also not something users are going to be all that happy with. If your network contains sensitive information—and whose doesn't these days?—you should consider providing an additional layer of security beyond simple passwords.

Windows Small Business Server 2011 Standard sets reasonable, if somewhat minimal, password policies, but even the best of password policies is a balancing act between making the password difficult to crack and making it easy for users to remember and use so that they aren't tempted to write it down on the back of their keyboards. The four kinds of authentication methods or factors are

- Something you know (password)
- Something you have (token or physical key)
- Something you are (biometric)
- Somewhere you are (location)

Of these, only the first three are realistic and usable in a small business environment, though the fourth—location—is starting to be used by banks as one factor to be sure that the person trying to access your bank account is actually you.

Passwords alone are a single-factor authentication method—in this case, something you know. Two-factor authentication requires two of the main three factors, and it provides a definite improvement in the surety that the person authenticating to your network is really who he claims to be. By enabling a second authentication factor, your need for overly draconian password policies is greatly reduced.

For a second authentication factor, we like the simplicity, moderate cost, and effectiveness of a one-time password (OTP). Generated automatically by a token you carry around with you, the combination of the token, a personal identification number (PIN), and your SBS password provides an additional level of security. Requiring administrators and all remote users to use two-factor authentication is a good way to improve the overall security of the sensitive data on your network.

Third-party providers of OTP tokens include AuthAnvil (*http://www.authanvil.com*), CryptoCard (*http://www.cryptocard.com*), and RSA SecureID (*http://www.rsa.com*). Of these, only AuthAnvil is focused on the small business market, with a suite of products that are fully integrated into SBS. Plus their soft tokens run on our users' phones, greatly simplifying token management and deployment. We use AuthAnvil on our SBS network for all laptops and servers, and for all remote users.

Securing Wireless Networks

Wireless networks using the 802.11b, 802.11a, 802.11g, and 802.11n standards are very convenient but can also introduce significant security vulnerabilities if not properly secured. To properly secure wireless networks, follow these recommendations:

- Change the default password of all access points.
- Change the default SSID. Pick a name that doesn't reveal the identity or location of your network.
- Enable 802.11i (WPA2) encryption on the access points.
- If the access points don't support WPA2-Enterprise, don't use them on your internal network.

> ***NOTE*** **WPA2 provides two methods of authentication: an "Enterprise" method that makes use of a RADIUS server, and a "Personal" method known as WPA2-Personal that uses a Pre-Shared Key (PSK) instead of a RADIUS server.**

- Disable the ability to administer access points from across the wireless network.

For more on configuring and protecting wireless networks, see Chapter 19, "Managing Local Connectivity."

Securing Internet Firewalls

Most external firewall devices are secure by default, but you can take some additional steps to maximize the security of a firewall:

- Change the default password for the firewall device! We know this seems obvious, but unfortunately, it is all too often ignored.
- Disable remote administration, or limit it to responding to a single IP address (that of your network consultant).
- Disable the firewall from responding to Internet pings. OK, we admit this is controversial. It's certainly a best practice, but it can also make troubleshooting a connectivity issue remotely a lot harder.
- Enable Stateful Packet Inspection (SPI) and protection from specific attacks, such as the Ping of Death, Smurf, and IP Spoofing.
- Leave all ports on the firewall closed except those needed by the SBS 2011 server.
- Regularly check for open ports using trusted port-scanning sites. We use *http://www.dslreports.com*.
- Require two-factor authentication for all access to the firewall.
- Keep the firewall updated with the latest firmware versions, which are available for download from the manufacturer's website.

Summary

In this chapter, we covered how to design or prepare a network prior to installing Windows Small Business Server 2011 Standard. We also covered basic naming conventions and how to plan for adequate network security.

The next chapter covers planning for fault tolerance and fault avoidance on your SBS network to help you build a reliable SBS network that can support your business.

Index

Symbols

$ (dollar sign) appended to shares, 235, 238
16-bit applications, not supported, 17
32-bit applications, support for, 16–17
32-bit architecture, 2
  for client computers, 17–18
  limited RAM access with, 2, 10–12
64-bit architecture, 2, 9–18
  32-bit application support with, 16–17
  for client computers, 17–18
  driver requirements for, 15
  hardware requirements for, 15
  increased RAM access with, 2, 10–12
  legacy software, potential problems with, 16–17
  registers with, 12
  security with, 13–14
  transitioning to, 9–10
  virtualization with, 14–15, 82
100BaseT (Fast Ethernet), 25, 26
500 account, 77, 139–142
802.1X standard (RADIUS authentication), 31, 34, 510
802.11a standard, 28
  for Internet connection, 24
  for network, 26
  range and interference issues, 32
802.11b standard, 27
  for Internet connection, 24
  for network, 26
  range and interference issues, 32
802.11g standard, 28
  for Internet connection, 24
  for network, 26
  range and interference issues, 32
802.11i standard (WPA2 encryption), 31, 43, 508–509, 510
802.11n standard, 28
  for Internet connection, 24
  for network, 26
  range and interference issues, 32

A

acceptable use policy, 307–308
access control, 755. *See also* permissions; security; shared resources
access point (AP), wireless, 31–33
  antennas for, 31
  authentication for, 31
  bridges and, 31
  built-in to firewall, 34
  built-in to router, 31
  channels for, 33
  interference of, 32
  placement of, 32–33
  range of, 32
  requirements for, 31
  security for, 31, 509
  supplementing wired network, 25
Access This Computer From The Network, logon right, 240
Account Operators domain local group, 210
accounts
  administrator accounts, 76, 77, 139–142
  computer accounts, 338
  POP3 email accounts, 474–478
  service accounts, SQL Server, 668
  Standard User domain accounts, 348–349
  user accounts
    adding, 217–221, 338, 754
    computer access, granting, 221
    migrating, 166–170

Active Directory
configuring, for migration, 127–129
publishing software to, 561–562
Active Directory Domains and Trusts, 465
Active Directory Services Interface (ADSI) Editor, 465
Active Directory Sites and Services, 465
Active Directory Users and Computers, 465
ActiveX controls, 32- and 64-bit, 16
Addftroot command, Dfsutil, 284–285
Add Hardware Wizard. Control Panel, 466
addresses
DHCP addresses
leased, viewing, 497–498
email addresses
for additional domain name, 486–492
for distribution groups, 205
for security groups, 207, 423
for user account, 217
IP address
range for, setting for migration, 119, 123–124
static, 25, 498–499
Addstdroot command, Dfsutil, 284–285
-addtarget parameter, Wbadmin, 417
Add-WBBackupTarget cmdlet, PowerShell, 413
Add-WBBareMetalRecovery cmdlet, PowerShell, 414
Add-WBFileSpec cmdlet, PowerShell, 413
Add-WBSystemState cmdlet, PowerShell, 414
Add-WBVolume cmdlet, PowerShell, 413
Add-WindowsFeature cmdlet, PowerShell, 86, 456
ADMIN$ special share, 235
administrative shares, 235–236
Administrator 500 account, 77, 139–142
administrator accounts, 76, 77, 139–142. *See also* Standard User domain accounts
Administrators domain local group, 210
Admin Tools Group universal group, 209
ADSI (Active Directory Services Interface) Editor, 465
Adsiedit.msc tool, 465
ADSL (Asynchronous Digital Subscriber Line) Internet connection, 24
ADUC (Active Directory Users and Computers) console, 458
Advanced Encryption Standard. *See* AES
Advanced Technology Attachment. *See* ATA
AES (Advanced Encryption Standard), 509
AIK (Automated Installation Kit), 757–758
alerts, 585–588
custom, creating, 588–595
for backup failure, 594–595
event associated with, 590
GUID for, 589–590, 594–595
report for, generating, 592–593
for stopped service, 589–593
viewing, 593
.xml file for, 591–593, 594–595
Event Log Error alerts, 588
Performance Counter alert, 587
services alerts, 586–587
-allCritical parameter, Wbadmin, 417
allocation unit, 244, 261
Allowed RODC Password Replication Group domain local group, 210
Allow Logon Locally, logon right, 240
Allow Logon Through Terminal Services, logon right, 240
AMD processors, compatibility with Intel, 15
Analysis Services, SQL Server, 667
answer file
for clean install, 78–79
for migration, 142–145
antispyware software, 41
antivirus software, 41
AP (access point), wireless. *See* access point (AP), wireless
AP Client bridges, 31
Append Data file permission, 226, 227
application buffer overflow, 13–14
applications
16-bit applications, not supported, 16–17
32-bit applications, support for, 16–17
deploying, with Group Policy, 560–568
adding to GPO, 567–568
assigning to users, 561–562
creating GPO for, 563–564
distribution point for, 562–563
installation options for, 564–566
publishing to Active Directory, 561–562
deploying with RemoteApp Manager, 695–700
legacy software, potential problems with, 16–17
recovering from backups, 404–406
running remotely. *See* RemoteApps
unresponsive, handling, 716–717
updates to
alerts regarding, on SBS Console, 199
assessing vulnerabilities and priority for, 366
availability of, determining, 367–368

configuring for second server, 644–648
cycle for, 365–370
declined, deploying after, 378–379
declining, 376
deploying, 369–370, 376–380
deployment reports for, 379
EULA (End User License Agreement) for, 376
evaluating need for, 368–369
importance of, 364
managed by WSUS, 115, 370, 381
Microsoft's schedule for, 365
for SQL Server, 662
synchronization of, 380
types of, 363–364
VPN for, 538
Appwiz.cpl tool, 466
Asynchronous Digital Subscriber Line. *See* ADSL Internet connection
audio capabilities, for RDS, 685, 686–688
audio files, controlling use of, 307–308
AuthAnvil OTP tokens, 42
AuthAnvil RWA agent, 532–533
authentication
Password Policies for, 41
passwords
for administrator account, 77, 140, 143
for built-in domain local groups, 210
OTP (one-time password), 42–43, 353, 532
for POP3 email accounts, 475
for SQL Server service accounts, 668
for Standard User domain account, 349
for trusted certificate, 197
for user account, 218–219
for Windows Server, 635
for workgroups, 753
for RDS (Remote Desktop Services), 682
TFA (Two Factor Authentication), 34, 508
for RWA (Remote Web Access), 352–353, 531–533
implementing, 42–43
for wireless access points, 31
Authorization Manager, 465
Automated Installation Kit. *See* AIK
auto quotas, 300, 301–302
auxiliary generator, 53–54
availability, maintaining. *See* disaster planning; fault tolerance
Azman.msc tool, 465

B

Backup Once Wizard, 395–399
Backup Operators domain local group, 210
backups, 4
alerts regarding, on SBS Console, 199
catalog for, restoring, 411–412
configuring
changing configuration, 388–391, 395
for client computers, 422–434
for second server, 649
with Configure Server Backup Wizard, 383–384, 385–391
with Wbadmin command, 416–422
with Windows Server Backup console, 391–395
with Windows.Serverbackup PowerShell snap-in, 413–416
for disaster planning, 743
of existing server, before migration, 115
failure of, custom alert for, 594–595
of GPOs (Group Policy objects), 559–560
hardware requirements for, 35
history for, viewing, 391
one backup, performing, 395–399
recovering
applications and data, 404–406
files and folders, 401–404
operating system, 406–411
server, 400
volumes, 400–401
schedule for, 387, 390, 392–393
storage locations for, 386, 388–389, 393
tools for, 383–384, 412
-backupTarget parameter, Wbadmin, 417
bandwidth, of Internet connection, 22–23
Baseline Configuration Analyzer 2.0, 114
basic disks, 245, 250, 252
Best Practices Analyzer. *See* BPA
BigFix, 381
BIND, vulnerabilities in, 506
BIOS, for VM (virtual machine), 101
BitLocker, 41
BPA (Best Practices Analyzer), 114, 130–133
bridges, wireless, 31, 33
browser, security of, 41
buffer overflow, 13–14
Business Intelligence Development Studio, SQL Server, 667

C

cable, for network, 27
cable Internet connection, 24
cable modem, 29
cache-corruption attack, 506
CAL (Client Access License)
  for SBS 2011, maximum number of, 70
  for RDS (Remote Desktop Services), 677–678
Cat 5 cable, 26, 27
Cat 5e cable, 26, 27
Cat 6 cable, 26, 27
Catalog Recovery Wizard, 400, 411–412
CEICW (Configure E-Mail and Internet Connectivity Wizard), 495, 519, 543. *See also* FMNW (Fix My Network Wizard)
CEIP (Customer Experience Improvement Program), 646–647
Certificate Authority Manager, 465
Certificate Service DCOM Access domain local group, 210
Certificates Manager, 465
certificates, trusted, 193–198
  exporting, 195–197
  importing, 197–198
  for migration, 143
  purchasing, 194–195
Certification Templates Console, 465
Certmgr.msc tool, 465
Cert Publishers domain local group, 210
Certsrv.msc tool, 465
Certtmpl.msc tool, 465
Change Permissions file permission, 226, 227
Change share permission, 224
child (guest) partition, for Hyper-V, 15, 83
Client Access License. *See* CAL
client computers, 752
  accounts for, creating, 338
  automating deployment of, 758
  backups for, 422–434
  configuring for DHCP, 338–341
  connecting to network, 337–351
    with Connect Computer Wizard, 342–349
    manually, 349–351
  excluding from automatic software updates, 374–375
  hardware requirements for, 36
  local access to, controlling, 357–358
  managing, 354–361
  naming, 39
  operating system for, 17–18, 21, 36, 337, 349, 350
  remote access to. *See also* RWA (Remote Web Access)
    connecting remotely, 360–361
    controlling, 356–357
  Remote Assistance on, providing, 358–359
  removing from network, 361
  requirements for, 756
  security for, 41
  status of, viewing, 354–356
  user access to, setting, 524–526
client/server-based network, 20
clients, Windows. *See also* Windows Server 2003; Windows Server 2008 R2 Standard
  for client computers, 17–18, 36, 756
  DFS namespace requirements for, 278–279
  security of, 41
  Windows 7
    for client computers, 18
    configuring for DHCP, 339–341
    connecting to network, 342–349
    sharing printer connected to, 325
    transitioning to, 9
  Windows 2000, connecting to network, 349–350
  Windows Vista
    for client computers, 18
    configuring for DHCP, 339–341
    connecting to network, 342–349
    sharing printer connected to, 324
  Windows XP
    for client computers, 18
    configuring for DHCP, 341
    connecting to network, 342–349
    sharing printer connected to, 325
Client Tools Backwards Compatibility, SQL Server, 667
Client Tools Connectivity, SQL Server, 667
Client Tools SDK, SQL Server, 667
clipboard, for VM (virtual machine), 106–107
clock settings, 74
clusters, 261. *See also* allocation unit
  failover clustering, 661, 662, 663, 664
  Hyper-V Server supporting, 86
  server cluster, stand-alone namespace on, 277, 283
Code Red worm, 13
collaboration
  DFS replication for, 280
  FRS for, 280
  SharePoint Foundation 2010 for, 280, 597–606

COM (Common Object Model), 16
Comexp.msc tool, 465
command line shortcuts, 465
Comma-Separated Values (CSV), storage reports in, 296
Common Object Model. *See* COM
company information, setting at installation, 75
Companyweb SharePoint site, 111, 597–598
  changing permissions for section of, 602–606
  migrating, 165
  RemoteApps links on, 613–624
  workspace, adding, 606–613
Compmgmt.msc tool, 465
Component Services Console, 465
COM ports, for VM (virtual machine), 102, 105
compression, 262
Computer Management Console, 465
computers. *See* client computers; servers
Configure E-mail and Internet Connectivity Wizard (CEICW), 495, 519, 543. *See also* FXMN (Fix My Network Wizard)
Configure Server Backup Wizard
  configuring server, 385–391
  requirements for, 383–384
conflict folder, DFS replication, 295
Connect Computer Wizard, 342–349
connectivity
  to Internet, 22–25, 182–184
  local, 495
    DHCP for, 496–503
    DNS for, 503–507
    Windows Firewall for, 511–519
    wireless, 508–510
  remote. *See* RDS (Remote Desktop Services); RemoteApps; RWA (Remote Web Access); VPN (virtual private network)
  troubleshooting, with FMNW, 519–520, 542–546
consoles, command line shortcuts for, 465
constant voltage transformer. *See* CVT
contacts
  in Active Directory, enabling, 480–484
  adding, 484–486
  creating, 458–461
  OU (organizational unit) for, 459, 486
Contribute permission, SharePoint, 600–601
cost
  of NAS (Network Attached Storage), 248
  of OTP (one-time password), 353, 532
  of printers, 315, 316–317
  of RAID, 61
  of WMS as alternative to Premium Add-on, 655
CPU cores, limits of, 11
CPU sockets, limits of, 11
CPUs (processors)
  client requirements for, 36
  Intel and AMD, compatibility between, 15
  monitoring, 712–714
  performance of, 6
  registers on, 12–13
  requirements for, 6, 7
  server requirements for, 35
  for VM (virtual machine), 101, 102–103
Create File file permission, 226
Create Folders file permission, 226, 227
critical updates, 363
CryptoCard OTP tokens, 42
Cryptographic Operators domain local group, 210
Cscript command, 327
CSV (Comma-Separated Values), storage reports in, 296
Customer Experience Improvement Program. *See* CEIP
Customer Feedback Options, 184
custom topology, 281
CVT (constant voltage transformer), 51, 52

D

data
  application data, recovering from backup, 404–406
  backing up. *See* backups
  in files and folders, recovering from backup, 401–404
  migrating to SBS 2011, 146–178
Database Engine Services, SQL Server, 667
data collector sets, 721–727
  creating from a template, 721–723
  creating from performance counters, 723–724
  creating manually, 724–725
  exporting templates for, 723
  importing templates for, 723
  log files from, 729–730
  managing data collected by, 727–730
  for monitoring performance counters, 725–726
  reports from, 730–731
  scheduling data collection for, 726–727
data execution bit. *See* DEP bit

Data Manager, configuring for data collector sets, 727–729
Date and Time, Control Panel, 466
Dcpromo.exe application, 127
Delete file permission, 226, 227
Delete Subfolders and Files file permission, 226, 227
Dell Remote Access Card. *See* DRAC
denial-of-service (DoS) attack, 33
Denied RODC Password Replication Group domain local group, 210
DEP (data execution protection) bit, 13
Design permission, SharePoint, 599
Desk.cpl tool, 466
Detailed Network Report, 580, 582–584
Device Manager, 465
Devmgmt.msc tool, 465
-dfsAuth parameter, Wbadmin, 417
Dfscmd utility
  backing up folder targets, 289
  creating a folder, 286
DFS (Distributed File System), 275–277
  folders, 276
    adding, 285–287
    for software distribution point, 562–563
    replicating, 291
  folder targets, 276–277, 289
  managing. *See* FSRM (File Server Resource Manager)
  namespace root, 276
    creating or opening, 283–285
  namespaces, 275, 276
    cache duration, changing, 287–288
    client requirements for, 278–279
    domain-based, 277
    failback settings, changing, 287–288
    permissions, changing, 288–289
    polling settings, changing, 289
    publishing shared folder to, 233
    referral settings, changing, 287–288
    server requirements for, 278
    stand-alone, 277
  namespace server, 276, 285
  replication, 275–276, 290–296
    compared to FRS, 279–280
    conflict folder, 295
    conflict resolution, 290
    health report for, 295
    of folders, 291
    requirements for, 279
    staging folder, 295
    topologies for, 280
    topology for, verifying, 295
  replication groups
    creating, 290, 292–294
    for branch office, creating, 292–293
    managing, 288–289
    multipurpose, creating, 293–294
DFS Management
  creating a replication group, 292–294
  folders, adding, 285–287
  installing, 281–283
  managing replication groups, 294–296
  namespace root, creating or opening, 283–285
  namespace server, adding, 285
  replicating a folder, 291
  replication groups, creating, 290
DFS Replication role service, 279
Dfsutil utility
  adding a namespace server, 285
  creating namespaces, 284–285
  optimizing namespace for scalability, 289
DHCP console, 465
  DNS updates, enabling, 502–503
  exclusions, creating, 498–499
  leased addresses, viewing, 497–498
  options, setting, 501–502
  reservations, creating, 500–501
DHCP (Dynamic Host Control Protocol), 496–503
  addresses
    leased, viewing, 497–498
  configuring computers for, 338–341
  DNS updates, enabling, 502–503
  exclusions
    creating, 498–499
  options
    scope of, 497
    setting, 501–502
  reconfiguring, for migration, 117–118
  reservations
    adding, 462–464
    creating, 499–501
    scope of, 497
Dhcpmgmt.msc tool, 117, 465
DHCP servers, 496, 497
DHTML (Dynamic HTML), storage reports in, 296
dial-up Internet connection, 24
differencing disks, 104

directory quotas, 300–306
creating, 301–302
quota templates, 300
creating and editing, 303–306
for shared folders, setting, 232
types of, 300
viewing and managing, 302–303
disable backup subcommand, Wbadmin, 420
disaster planning, 733–734. *See also* fault tolerance
backups for, 743
escalation procedures, 739–740
fault tolerance, ensuring, 742
generators, 53–54
hard copies of procedures for, 738–739
iterative process of, 733–734, 741–742
recovering from backups, 743–747
resources for, identifying, 736
responses
developing, 736–740
testing, 740
risks, identifying, 735–736
size of business affecting, 734
SOPs (standard operating procedures) for, 737–739
virtualization, considerations for, 747–748
discussions, SharePoint, 599
disk management, 243–246. *See also* backups; DFS; file system; FSRM; hard disks; SharePoint Foundation Services 2010
partitions, 244
adding, 253–263
compared to volumes, 252
deleting, 262
extended partition, 244, 250, 263
GPT (GUID Partition Table) for, 244
for Hyper-V virtualization, 14–15, 83–84, 107–109
logical drives on, 245
MBR (Master Boot Record) for, 244
planning, 67–68
primary partition, 244, 250
storage solution technologies, 246–249, 251–252, 253–254, 271–272
types of disks, choosing, 252
virtual hard disk
mounting, 272–273
volumes, 244, 250
adding, 253–263
compared to partitions, 252
deleting, 262
extended volume, 245
logical drive/volume, 245
mirror volume, 267–271
mounting, 273–274, 274
naming, 272
RAID-0 (striping), 245, 250
RAID-1 volume, 250, 259–262
RAID-5 volume, 246, 250, 259–262, 271–272
recovering from backup, 271–272
shrinking, 263–264
simple volume, 244, 255–259
spanned volume, 245, 250
special shares for, 235–236
Disk Management console, 250, 465
mirror
adding, 267–268
breaking, 271
removing, 269–271
partitions, creating, 255–259
virtual hard disk
mounting, 272–273
volume
mounting, 274
RAID-1 or RAID-5, creating, 259–262
shrinking, 263–264
simple, creating, 255–259
Diskmgmt.msc tool, 250, 465
Diskpart.exe application, 250, 258, 259, 262, 635
disk quotas, 300
disk space
client requirements for, 36
server requirements for, 6, 7, 35
display
client requirements for, 36
server requirements for, 6, 7
Display Settings, Control Panel, 466
Distributed COM Users domain local group, 210
Distributed File System role service, 281
distribution groups, 203, 204, 205–206
DLLs, 32- and 64-bit, 16
DnsAdmins domain local group, 210
DNS (Domain Name Service), 503–507
automatic management of, 503–504
email routing, 470–471, 473–474
lookup zones for, 503
split DNS, 503
updates of
enabling from DHCP, 502–503

DNS forwarding
migrating to SBS 2011, 157
root servers as default for, 505
setting to ISP servers, 506–507
DNS Manager console, 465
DNS forwarding, setting, 506–507
DNS records, adding, 504–505
Dnsmgmt.msc tool, 465, 504
DNS poisoning attacks, 506
DNS records
adding, 191, 504–505
for Internet domain name, 191
updates of, enabling from DHCP, 502–503
DnsUpdateProxy global group, 212
dollar sign ($) appended to shares, 235, 238
Domain Admins global group, 212
domain-based namespaces, 277
Domain Computers global group, 213
domain controllers, 755
multiple, 337–338
second server as, 627
Domain Controllers global group, 213
Domain Guests global group, 213
domain level, for Active Directory, 127–129
domain local scope, 208, 209–212
Domain.msc tool, 127, 465
domain name
email
adding, 486–492
registering, 185–188
setting up, 188–193
internal
for network, 37–39, 75, 76
for second server, 641–644
Internet domain name
choosing, 38, 185
DNS records for, 191
existing, using, 188–191
managing, 190, 192
new, registering, 185–188
managing, 190–191
Domain Profile, for Windows Firewall, 512
domains, compared to workgroups, 753–756
Domain Users global group, 213
DoS (denial-of-service) attack, 33
DRAC (Dell Remote Access Card), 62
drivers
installing, 637
for printers, 325–326
requirements for, 15, 628
signed for authenticity, 15, 628
Dsa.msc tool, 465, 650, 678
DSL modem, 29
DSL over ISDN. *See* ISDL Internet connection
DSRM Administrator account, 77
Dssite.msc tool, 465
dual-WAN router, 62
Duell, Charles H. (U.S. Patent Office), 1
duplexing, 246. *See also* mirroring (RAID 1)
DVD ROM drive, requirements for, 6
dynamic disks, 104, 245, 250
compared to fixed-size disks, 99
for software RAID, 55
when to use, 253
Dynamic Host Control Protocol. *See* DHCP (Dynamic Host Control Protocol)
Dynamic HTML (DHTML), storage reports in, 296
dynamic memory allocation, 102–103

E

EFS (Encrypting File System), 41
802.11a standard, 28
for Internet connection, 24
for network, 26
range and interference issues, 32
802.11b standard, 27
for Internet connection, 24
for network, 26
range and interference issues, 32
802.11g standard, 28
for Internet connection, 24
for network, 26
range and interference issues, 32
802.11i standard (WPA2 encryption), 31, 43, 508–509, 510
802.11n standard, 28
for Internet connection, 24
for network, 26
range and interference issues, 32
802.1X standard (RADIUS authentication), 31, 34, 510
email
contacts
adding, 484–486
in Active Directory, enabling, 480–484

DNS routing for, 470–471, 473–474
domain name for
registering, 185–188
setting up, 188–193
email domains, adding, 486–492
maximum message size, 493–494
POP3 email accounts for, 474–478
SMTP forwarding with Smart Host, 470, 471–473
email addresses
for additional domain name, 486–492
for distribution groups, 205
for security groups, 207, 423
for user account, 217
email distribution groups. *See* distribution groups
emulation virtualization, 83–84
enable backup subcommand, Wbadmin, 419–420
error reporting (feedback), 644–647
eSATA (External SATA), 249
Essentials edition of SBS 2011, 1
Ethernet Internet connection, 24
EULA (End User License Agreement), 376
Event Log Error alerts, 588
Event Log Readers domain local group, 210
Event Viewer, 465, 590
Eventvwr.msc tool, 465
ExchangeDefender, 470
Exchange mailboxes, migrating, 133–134, 158–164
Exchange Management Console
contacts
adding, 484–486
in Active Directory, enabling, 480–484
email domains, adding, 487–492
Exchange Server 2010, 5, 469
-excludeDisks parameter, Wbadmin, 417
Execute File file permission, 226
Extended Markup Language. *See* XML
extended partition, 244, 250, 263
extended volume, 245, 264–267
external virtual network, 91

F

failover clustering, 661, 662, 663, 664
Fast Ethernet (100BaseT), 25, 26
FAT32 file system format, 261
FAT file system format, 261
fault tolerance, 45. *See also* disaster planning
device health, notification of, 50
for Internet connection, 62
metrics for, 46–47
power supply, protecting, 47–54
RAID for, 55–61
redundant networking, 62
spare parts for, 48–49, 62
Fax Administrators universal group, 209
fax data, migrating, 166
fax service, 333–336
administrators of, setting, 336
configuring, 334–336
modem for, installing, 333–334
starting, 334
users of, setting, 336
Fax Users universal group, 209
features for Windows Server 2008 R2, 441
adding, 455–456
removing, 456–457
feedback (error reporting), 644–647
Fibre Channel, 249
file groups, 311–313
file permissions, NTFS, 41, 224–229
applied to shared folders, 230
effective, viewing, 238–239
how applied, 227–228
inherited, 228–229
recommended settings for, 223
for software distribution point, 562–563
types of, 226–227
File Replication Service. *See* FRS
files. *See also* data
compression of, 262
Group Policy Preferences for, 573–574
ownership of, 236–238
recovering from backup, 401–404
file screens, 306–313
acceptable use policy and, 307–308
creating, 307–308
exceptions to, 308–309
file groups and, 311–313
templates for, 309–311
File Server Resource Manager. *See* FSRM
File Services Manager, 465
File Services role, 279, 281, 296, 441
file storage. *See* disk management; hard disks
file system. *See* DFS (Distributed File System); FSRM (File Server Resource Manager)

filtering. *See also* file screens
MAC address, 509
packets, 33
Resource Monitor, 716
of websites, by firewall, 34
firewall
access point built-in to, 34
adding, for migration, 111, 116–117, 124–125
diagramming, 30
requirements for, 33–34
securing, 43
Windows Firewall, 511–519
configuring, for second server, 654
policies, setting with Group Policy, 512–519
profiles for, 511–512
rules for, 513
Firewall.cpl tool, 466
FireWire, 249
500 account, 77, 139–142
fixed-size disks, 99, 104
Fix My Network Wizard (FMNW), 519–520, 542–546
Flexible Single Master Operation roles. *See* FSMO roles
floating-point operations, performance of, 12
FMNW (Fix My Network Wizard), 519–520, 542–546
Folder Redirection Accounts universal group, 209
folders. *See also* data
compression of, 262
DFS, 276
adding, 285–287
replicating, 291
ownership of, 236–238
permissions for. *See* NTFS file permissions
quotas for. *See* directory quotas
recovering from backup, 401–404
redirection, re-enabling after migration, 176–178
shared
adding, 229–233
file screen for, 232
for software distribution point, 562–563
NTFS file permissions applied to, 230
permissions on. *See* share permissions
protocol for, 230
publishing to DFS namespaces, 233
quotas for, 232
removing, 233
share permissions for, changing, 234–235
special shares, 235–238
storage for, 230
folder targets, DFS, 276–277, 289
forest functional level, for Active Directory, 127–129
forward lookup zones, DNS, 503
frame relay/T1 Internet connection, 24
FRS (File Replication Service), 279–280
Fsmgmt.msc tool, 465
FSMO (Flexible Single Master Operation) roles, 70, 337
FSRM (File Server Resource Manager), 296–313
command line shortcut for, 465
creating quotas, 301–302
creating quota templates, 303–306
screening files, 306–313
storage reports, scheduling, 296–300
Fsrm.msc tool, 465
Full Control file permission, 226–227
Full Control permission, SharePoint, 599
Full Control share permission, 224
full mesh topology, 280
Full-Text Search, SQL Server, 667

G

GDT (global descriptor table), 14
generators, 53–54
geosynchronous satellite Internet connection, 24
Get-Excommand command, PowerShell, 492
getmac command, 500
get status subcommand, Wbadmin, 422
get versions subcommand, Wbadmin, 422
Get-WBBackupSet cmdlet, PowerShell, 413
Get-WBBackupTarget cmdlet, PowerShell, 413
Get-WBBareMetalRecovery cmdlet, PowerShell, 414
Get-WBDisk cmdlet, PowerShell, 413
Get-WBFileSpec cmdlet, PowerShell, 414
Get-WBJob cmdlet, PowerShell, 413
Get-WBPolicy cmdlet, PowerShell, 413
Get-WBSchedule cmdlet, PowerShell, 413
Get-WBSummary cmdlet, PowerShell, 413
Get-WBSystemState cmdlet, PowerShell, 414
Get-WBVolume cmdlet, PowerShell, 413
Get-WBVssBackupOptions cmdlet, PowerShell, 414
GigE (Gigabit Ethernet), 25, 26
global descriptor table. *See* GDT
global scope, 208, 212–213
GPC (Group Policy Container), 548
Gpedit.msc tool, 465

GPMC (Group Policy Management console)
Block Inheritance, setting, 552
command line shortcut for, 465
firewall policies, creating, 515–519
GPO (Group Policy object)
adding software package to, 567–568
backing up, 559–560
creating, 553–554
creating, for software development, 563–564
deleting, 554
node of, disabling, 557
refreshing after changes, 558–559
restoring, 560
scope of, setting, 555–556
software installation options for, 564–566
viewing or editing, 549–550
GPO link
disabling, 556
enabling, 556
enforcing, 551
viewing, 555
Group Policy Preferences
devices, settings for, 575–576
files, settings for, 573–574
mapped drives, settings for, 571–573
viewing, 570
Gpmc.msc tool, 465
Gpme.msc tool, 465
GPO (Group Policy Object). *See* Group Policy, GPO
Gptedit.msc tool, 465
GPT (Group Policy Template), 548–549
GPT (GUID Partition Table), 244
Group Policy, 547–549
compared to Group Policy Preferences, 569
GPO (Group Policy Object), 548–549
backing up, 559–560
components of, 548–549
computer-related policies in, 548
creating, 553–554
creating, for applications, 560–568
creating, for firewall policies, 515–519
deleting, 554
disabling policy branch of, 557
inheritance of, 551–552
order of implementation for, 552–553
refreshing after changes, 557–559
restoring, 560
scope of, setting, 555–556
user-related policies in, 548
viewing or editing, 549–550
GPO link
disabling, 556
enabling, 556
enforcing, 551
managing, 555–557
RemoteApps deployed with, 694, 695, 698, 700
Group Policy Creator Owners global group, 213
Group Policy Editor, 465
Group Policy Management console. *See* GPMC (Group Policy Management console)
Group Policy Management Editor, 465
Group Policy Object. *See* Group Policy, GPO
Group Policy Object Editor, 554
Group Policy Preferences, 568–576
common options for, 574–575
compared to Group Policy, 569
devices, settings for, 575–576
files, settings for, 573–574
mapped drives, settings for, 571–573
results of, viewing, 576–577
viewing, 570
Group Policy Results Wizard, 576–577
Group Policy Starter GPO Editor, 465
Group Policy Template. *See* GPT
groups, 203–204. *See also* user accounts
benefits of, 204
built-in domain local groups, 209–212
built-in global groups, 212–213
built-in universal groups, 209
distribution groups, 203, 204, 205–206
migrating, 166–170
security groups, 203
creating, 206–207
group scope for, 203
securable objects in, 203
user rights for, 204
SharePoint. *See also* security groups, SharePoint
guest (child) partition, for Hyper-V, 15, 83
Guests domain local group, 210
GUID (globally unique identifier), 139
for administrator account, 77
for custom alert, acquiring, 589–590, 594–595
GUID Partition Table. *See* GPT

H

hackers, 40
hard disks. *See also* disk management
  adding, 254–255
  allocation unit of, 244, 261
  backups stored on, 386, 388–389, 393
  basic disks, 245, 250, 252
  compression of, 262
  dynamic disks, 245. *See* dynamic disks
  formatting options for, 261–262
  monitoring, 712, 714–715
  partitions on, 244
    adding, 253–263
    compared to volumes, 252
    deleting, 262
    extended partition, 244, 250, 263
    GPT (GUID Partition Table) for, 244
    for Hyper-V virtualization, 14–15, 83–84, 107–109
    logical drives on, 245
    MBR (Master Boot Record) for, 244
    planning, 67–68
    primary partition, 244, 250
  reliability of, 47
  space required on. *See* disk space
  virtual. *See* VHD (virtual hard disk)
  volumes on, 244, 250
    adding, 253–263
    compared to partitions, 252
    deleting, 262
    extended volume, 264–267
    logical drive/volume, 245
    mirror volume. *See* mirror volume
    mounting, 273–274
    naming, 272
    RAID-0 (striping), 245, 250
    RAID-1 volume, 250, 259–262
    RAID-5 volume, 246, 250, 259–262, 271–272
    recovering from backup, 271–272
    shrinking, 263–264
    simple volume, 244, 255–259
    spanned volume, 245, 250
    special shares for, 235–236
hardware RAID, 55, 61, 251–252, 253–254
hardware requirements, 6–7, 15
  for backups, 35
  for client computers, 36
  for firewall, 33–34
  for Hyper-V virtualization, 84–85
  for printers, 316–317
  for RD Session Host role, 676–677
  for router, 33–34
  for SBS on Hyper-V child partition, 108–109
  for second server, 627–629
  for server, 34–36
  for SQL Server, 659
  for wireless access points, 31
Hdwwiz.cpl tool, 466
health reports. *See also* monitoring; troubleshooting
  for devices, using SNMP, 50
  for DFS replication, 295
  for network, 199
Help command, PowerShell, 492
host (parent) partition, for Hyper-V, 14, 83–84
hotfixes, 364
hot-spare RAID, 61
hot-swap RAID, 61
HTML (Hypertext Markup Language), storage reports in, 296
hub and spoke network topology, 30, 280
hubs, 30
HyperSnap utility, 107
Hypertext Markup Language (HTML), storage reports in, 296
Hyper-V child partition, SBS on, 107–109
  configuration for, 108–109
  licensing for, 108
hypervisor virtualization. *See* Hyper-V virtualization
Hyper-V Manager console, 91, 466
  network configuration, 92–93
  server configuration, 93–95
  VM (virtual machine)
    machine settings for, 101–105
Hyper-V role, 82
  installing, 89–90
  on main SBS server, 107–108
  other roles limited by, 86, 108
  requirements for, 84–85
  support for, 17
Hyper-V Server 2008 R2, 84, 86
  configuring, 93–95
  installing, 87–88
Hyper-V virtualization, 14–15, 81–85
  configuring, 91–95

disaster planning issues for, 747–748
on Hyper-V Server 2008 R2, 86, 87–88
installing, 86–90
network configuration, 91–93
network, types of, 91
partitions for, 14–15, 83–84, 107–109
RAID level for, 85
reasons for, 82
requirements for, 84–85
second server as, 627
server configuration, 93–95
version of, choosing, 86
VM (virtual machine)
creating, 95–100
machine settings for, 101–105
using, 105–106
on Windows Server 2008 R2, 86, 89–90

I

ICT (Initial Configuration Tasks) Wizard, 635–636, 637
closing, 654
computer name and domain, setting, 642–644
roles and features, adding, 648–653
time zone, setting, 637–638
updates and feedback, enabling, 644–647
updates, downloading and installing, 647–648
IDE controllers, for VM (virtual machine), 101, 103
IDE (Integrated Device Electronics), 246, 249
IDSL (DSL over ISDN) Internet connection, 24
IDT (interrupt descriptor table), 14
IEEE 802.1X standard, 31, 34, 510
IEEE 802.11a standard, 28
for Internet connection, 24
for network, 26
range and interference issues, 32
IEEE 802.11b standard, 27
for Internet connection, 24
for network, 26
range and interference issues, 32
IEEE 802.11g standard, 28
for Internet connection, 24
for network, 26
range and interference issues, 32
IEEE 802.11i standard (WPA2 encryption), 43, 508–509, 510
IEEE 802.11n standard, 28
for Internet connection, 24
for network, 26
range and interference issues, 32
IIS_IUSRS domain local group, 210
iLO (integrated Lights Out) port, 62–63
-include parameter, Wbadmin, 417
Incoming Forest Trust Builders domain local group, 210
Inetcpl.cpl tool, 466
inheritance
of file permissions, 228–229
of Group Policy, 551–552
Initialize Disk Wizard, 254–255
inkjet printers, 317
installing DFS Management, 281–283
installing drivers, 637
installing Hyper-V virtualization, 86–90
installing printers, 319–325
installing SBS 2011, 4, 67–80
answer file for, 78–79
automating, 757–758
disks, partitioning, 67–68
layout, planning, 68
problems with, resolving, 182
process for, 70–77
server, preparing, 69–70
when migrating to, 145–146
installing SQL Server 2008 R2 for Small Business
help for, 661
options for, 657, 662, 664–665
planning for, 659–665
process for, 658, 665–671
restrictions on, 658
installing Windows Server 2008 R2 Standard, 70–73, 630–636
Integrated Device Electronics. *See* IDE
integrated lights out port. *See* iLO port
Integrated Services Digital Network. *See* ISDN Internet connection
Integration Services, SQL Server, 667
Intel processor, compatibility with AMD, 15
interference of wireless networks, 32
internal virtual network, 91
Internet address
configuring, for migration, 152–157
setting up, 185–198
Internet Address Management Wizard, 469–470
domain name, registering, 185–188
domain name, setting up, 188–193

Internet connection, 22–25. *See also* email
backup for, 25
bandwidth needs for, 22–23
connecting to, 182–184
diagramming, 29
fault tolerance for, 62
ISPs for, 25
requirements for, 7
speed of, 23–24
types of, 23–24
Internet domain name, 37–39
choosing, 38, 185
DNS records for, 191
existing, using, 188–191
managing, 190–193
new, registering, 185–188
Internet Explorer, 32- and 64-bit versions of, 16
Internet hackers, 40
Internet Properties (Internet Explorer), Control Panel, 466
Internet Protocol version 6. *See* IPv6
Internet Security and Acceleration. *See* ISA
Internet Small Computer Systems Interface. *See* iSCSI
interrupt descriptor table. *See* IDT
Intl.cpl tool, 466
I/O
performance of, 12–13
virtualization and, 85
IP address
range for, setting for migration, 119, 123–124
static, 25
DHCP exclusions for, 498–499
IPC$ special share, 235
ipconfig command, 499
IP spoofing, 33
IPv6 (Internet Protocol version 6), 33
ISA (Internet Security and Acceleration) server
migrating from, 111, 125
removing from SBS 2003, 125
iSCSI (Internet SCSI), 245, 249
initiator for, 245
target for, 245
ISDN (Integrated Services Digital Network) Internet connection, 24
ISP servers, setting DNS forwarding to, 506–507
ISPs (Internet Service Providers), 25
-items parameter, Wbadmin, 418
-itemtype parameter, Wbadmin, 418

J

JBOD (just a bunch of disks), 246

K

kaizen, 741
Kaseya, 381
Kbps (kilobits per second), 23
KBps (kilobytes per second), 23
kernel, security for, 14
keycode locks, 69

L

LAND attack, 33
laser printers, 316–317
Launcher.exe application, 338, 343
libraries, SharePoint, 598
licensing
CAL (Client Access License), 70, 677–678
EULA (End User License Agreement), for updates, 376
for RDS (Remote Desktop Services), 677–678, 683
for Windows Server, 108
licmgr.exe application, 689
Limited Access permission, SharePoint, 599
Line Printer Daemon. *See* LPD
Link Users universal group, 209
List Folder Contents file permission, 226
List Folder file permission, 226
lists, SharePoint, 599
local administrator accounts. *See* Standard User domain accounts
local connectivity, 495
DHCP for, 496–503
DNS for, 503–507
Windows Firewall for, 511–519
wireless, 508–510
local power supply, failure of, 48–50
Local Security Policy Console, 465
Local Users and Groups Manager, 465
location name, for printers, 318
log files, from data collector sets, 729–730
logical drive/volume, 245. *See also* partitions
logical printers, 316
configuring usage of, 329–330

creating, 329
viewing in SBS Console, 330–331
Logical Unit Number. *See* LUN
logon rights, 240–242
long-term power outages, 53–54. *See also* disaster planning
lookup zones, DNS, 503
LPD (Line Printer Daemon), 315–316
Lpq command, 327
Lpr command, 327
Lumension Endpoint Management and Security Suite, 381
LUN (Logical Unit Number), 245
Lusrmgr.msc tool, 465, 616

M

-machine parameter, Wbadmin, 418
MAC (Media Access Control) address
determining for a device, 499–500
filtering, 509
Mac OS/X clients, 350–351
Main.cpl tool, 466
Manage Documents permission, 328
managed switches, 30
Management Framework Core, 114
Management Tools, SQL Server, 667
Manage Printers permission, 328
Map command, Dfscmd, 286
mapped drives, Group Policy Preferences for, 571–573
Master Boot Record. *See* MBR
Mbps (megabits per second), 23
MBps (megabytes per second), 23
MBR (Master Boot Record), 244
MDT (Microsoft Deployment Toolkit), 758
mean time to failure. *See* MTTF
mean time to recover. *See* MTTR
Media Access Control address. *See* MAC address
megabits per second. *See* Mbps
megabytes per second. *See* MBps
member server. *See* second server
Members group, SharePoint, 599, 600–602
memory
dynamic memory allocation, 102–103
physical memory (RAM)
access to, with 32- and 64-bit architectures, 2, 10–11
client requirements for, 36
for VM (virtual machine), 101, 102–103
server requirements for, 6, 7, 35
usage, monitoring, 712, 715
virtual memory address space, 10, 11, 12
MFM (Modified Field Modification), 246
Microsoft Baseline Configuration Analyzer 2.0. *See* Baseline Configuration Analyzer 2.0
Microsoft Deployment Toolkit. *See* MDT
Microsoft Exchange Server 2010. *See* Exchange Server 2010
Microsoft Hyper-V Server 2008 R2. *See* Hyper-V Server 2008 R2
Microsoft Internet Explorer. *See* Internet Explorer
Microsoft .NET Framework 2.0 SP1. *See* .NET Framework 2.0 SP1
Microsoft print server. *See* Windows print server
Microsoft SBS 2003 Best Practices Analyzer. *See* SBS 2003 Best Practices Analyzer
Microsoft SharePoint Foundation Services 2010. *See* SharePoint Foundation 2010
Microsoft SQL Server 2008 R2 for Small Business. *See* SQL Server 2008 R2 for Small Business
Microsoft Sync Framework, SQL Server, 667
Microsoft Virtual Server 2005 R2. *See* Virtual Server 2005 R2
microwave wireless Internet connection, 24
Middleton, Jeff (Microsoft MVP for SBS), 113
migrating to SBS 2011, 4, 111–113
answer file, creating, 142–145
data and settings, migrating, 147–176
Companyweb SharePoint site, 165
fax data, 166
Group Policies, removing, 164–165
Internet address configuration, 152–157
logon settings, removing, 164–165
network configuration, 150–152
network settings, 157–158
shared data, 165
users and groups, 166–170
Exchange mailboxes, 133–134, 158–164
existing server
Active Directory, configuring, 127–129
backing up, 115
BPA, running for, 130–133
demoting and removing, 170–176
DHCP reconfiguration, 117–118
IP address range for, 119, 123–124

migrating to SBS 2011 *(cont.)*
existing server *(cont.)*
Migration Preparation Tool, running, 134–139
network configuration for, 116–124
preparing, 114–139
synchronizing to external time source, 138
updating, 115
firewall for, 116–117, 124–125
folder redirection, configuring, 176–178
installing SBS 2011, 145–146
Microsoft migration guides for, 112
router for, 116–117, 124–125
Swing Migration, 113
time to complete, limit for, 111, 146
VPNs, disabling, 126
Migration Preparation Tool, 114, 134–139
Migration Wizard, 147–171
mirrored striped disks, 57
mirroring (RAID 1), 56, 60, 61
mirroring (RAID-1), 250, 259–262
mirror volume, 246
breaking, 271
failure of, recovering from, 268–271
Mmsys.cpl tool, 466
Modified Field Modification. *See* MFM
Modify file permission, 226–227
monitor. *See* display
monitoring. *See also* troubleshooting
health reports
for devices, using SNMP, 50
for DFS replication, 295
for network, 199
performance counters
adding, 718–719
creating data collector sets from, 723–724
monitored by data collector sets, 725–726
Performance Monitor, 465, 711, 717–718
data collector sets, 721–727
display, customizing, 719–720
Reliability Monitor, 720–721
Resource Monitor, 712–717
Mouse Properties, Control Panel, 466
MS-DOS applications, not supported, 17
.msi files, 698–700
mstsc.exe application, 360
MTTF (mean time to failure), 46–47
MTTR (mean time to recover), 46–47

N

namespace root, DFS, 276
creating or opening, 283–285
namespaces, DFS, 275, 276
cache duration, changing, 287–288
client requirements for, 278–279
domain-based, 277
failback settings, changing, 287–288
permissions, changing, 288–289
polling settings, changing, 289
publishing shared folder to, 233
referral settings, changing, 287–288
server requirements for, 278
standalone, 277
namespace server, DFS, 276, 285
naming conventions, 37–39
for client computers, 39
for domain name, 37–39, 76, 185
for printer locations, 318
for printers, 318
for second server, 641–644
for server, 39
for volumes, 272
Napclcfg.msc tool, 465
NAP (Network Access Protection) Client Configuration Console, 465
NAS (Network Attached Storage), 248, 249, 251
native consoles
direct access to, 464–466
from Native Tools Management console, 457
from SBS Console, 457–458
from Server Manager console, 461–462
Native Tools Management console, 457
NAT (Network Address Translation), 33
Ncpa.cpl tool, 466
.NET Framework 2.0 SP1, 114
NETLOGON special share, 235
Net print command, 327
Net start command, 327
network, 751–756
cable for, 27
client hardware and software for, 36
client/server-based, 20
configuring, for Hyper-V, 91–93
configuring, for migration, 116–124, 150–152, 157–158
connecting computers to, 337–351

connections used in, 752
diagramming, 29–30
domain controllers for, 337–338, 627, 755
domain name for, 37–39, 75, 76
firewall for, 33–34
health of, from SBS Console, 199
Internet connection for, 22–25, 182–184
layout for, planning, 68
monitoring. *See* monitoring
needs of, determining, 21–22
peer-to-peer, 20
ports for, 30, 62–63
redundant networking, 62
removing computers from, 361
router for, 33–34
server hardware for, 34–36
speed requirements for, 30
switch (hub) for, 30
topology for, 30
troubleshooting with FMNW, 519–520, 542–546
types of, 25–28
wireless access points for. *See* wireless access points
Network Access Protection (NAP) Client Configuration Console, 465
network adapters
client requirements for, 36
for VM (virtual machine), 102, 105
server requirements for, 6, 35
Network Address Translation. *See* NAT
Network Administrator role, 215
Network Attached Storage. *See* NAS
network card teaming, 62
Network Configuration Operators domain local group, 211
Network Connections, Control Panel, 466
network devices. *See* firewall; router; wireless access point
Network File System. *See* NFS
network interface card. *See* NIC
network operating systems, 19–21
Network Policy And Access Services role, 447
Network Policy Server Console, 465
network reports
creating, 584–585
Detailed Network Report, 580, 582–584
Summary Network Report, 579–582
New-MailContact cmdlet, PowerShell, 479
New-WBBackupTarget cmdlet, PowerShell, 413
New-WBFileSpec cmdlet, PowerShell, 413
New-WBPolicy cmdlet, PowerShell, 413
NFS (Network File System)
for shared folders, 230
mounted volumes not supported with, 273
NIC (network interface card)
DRAC (Dell Remote Access Card), 62
number of
migration issues with, 111, 116–117, 118
spare, in case of failure, 62
teaming, 62
-noInheritAcl parameter, Wbadmin, 417
Non-Uniform Memory Architecture. *See* NUMA
-notrestoreacl parameter, Wbadmin, 418
-noVerify parameter, Wbadmin, 418
Nps.msc tool, 465
Ntbackup utility, 384, 416
NTFS file permissions, 41, 224–229
applied to shared folders, 230
effective, viewing, 238–239
how applied, 227–228
inherited, 228–229
recommended settings for, 223
for software distribution point, 562–563
types of, 226–227
NTFS file system format, 261

O

OCA (Online Crash Analysis), 647
100BaseT (Fast Ethernet), 25, 26
one-time password. *See* OTP
Online Crash Analysis. *See* OCA
oobe.exe application, 652, 654
operating system. *See also* Mac OS/X clients; Windows clients
for client computers, 17–18, 21, 36, 337, 349, 350
for server, 19–21
recovering from backup, 406–411
OTP (one-time password), 42–43, 353, 532
OU (organizational unit)
for contacts, 459, 486
for GPO (Group Policy object), 552, 553–554, 558, 563
SBSComputers OU, 428–429, 527
SBSServers OU, 515–516, 527
SBSUsers OU, 141–142, 486
for Windows Server, 650, 678

Outlook Anywhere
DNS records for, 191
RWA (Remote Web Access) for, 522
split DNS for, 503
-overwrite parameter, Wbadmin, 418
Owners group, SharePoint, 599
ownership of files or folders, 236–238

P

packet filtering, 33
PAE (Physical Address Extension), 12
parent (host) partition, for Hyper-V, 14, 83–84
partitions, 244
adding, 253–263
compared to volumes, 252
deleting, 262
extended partition, 244, 250, 263
GPT (GUID Partition Table) for, 244
for Hyper-V virtualization, 14–15, 83–84, 107–109
logical drives on, 245
MBR (Master Boot Record) for, 244
planning, 67–68
primary partition, 244, 250
pass-through disks, 104
-password parameter, Wbadmin, 418
Password Policies, 41
passwords. *See also* authentication; security
for administrator account, 77, 140, 143
for built-in domain local groups, 210
OTP (one-time password), 42–43, 353, 532
for POP3 email accounts, 475
for SQL Server service accounts, 668
for Standard User domain account, 349
for trusted certificate, 197
for user account, 218–219
for Windows Server, 635
for workgroups, 753
patches. *See* software updates
PatchGuard technology, 14
pattern matching, defining file groups using, 313–314
peer-to-peer network, 20
Perfmon.msc tool, 465
performance
of floating-point operations, 12
of I/O operations, 12–13
of processors, 6
of RAID levels, 60
storage reports affecting, 299–300
Performance Counter alert, 587
Performance Log Users domain local group, 211
Performance Monitor, 465, 711, 717–718
data collector sets, 721–727
display, customizing, 719–720
performance counters
adding, 718–719
creating data collector sets from, 723–724
monitored by data collector sets, 725–726
Reliability Monitor, 720–721
Resource Monitor, 712–717
Performance Monitor Users domain local group, 211
perimeter network, 30
permissions
effective, viewing, 238–239
for printers, 328
for VPN, 541–542
NTFS file permissions, 41, 224–229
applied to shared folders, 230
effective, viewing, 238–239
how applied, 227–228
inherited, 228–229
recommended settings for, 223
for software distribution point, 562–563
types of, 226–227
share permissions, 223–224, 237–238
changing, 234–235
hiding, 238
recommended settings for, 223
setting, 231–232
users applied to, 224
SharePoint, 599–606
user rights and, 204, 240–242
PFM (Pulse Frequency Modulation), 246
.pfx files, 197
Phone and Modem Options, Control Panel, 466
Physical Address Extension. *See* PAE
physical drive, 244. *See also* hard disks
physical memory (RAM)
access to, with 32- and 64-bit architectures, 2, 10–12
client requirements for, 36
server requirements for, 6, 7, 35
for VM (virtual machine), 101, 102–103
physical security, 40, 68
PID (process identification), 714–715
PID (Product ID), 629

Ping of Death attack, 33
pings, disabling, 43
PKI (Private Key Infrastructure) Viewer, 465
Pkiview.msc tool, 465
PM (preventive maintenance), for generators, 54
Point-to-Point bridges, 31
pools
  non-paged, 11, 12
  paged, 10
  printer pools, 316, 331–332
POP3 email accounts, 474–478
  adding, 475–477
  retrieval frequency for, 477–478
ports
  COM ports, for VM (virtual machine), 102, 105
  firewall ports, scanning, 43
  iLO (integrated Lights Out) port, 62–63
  number of, for network, 30
Powercfg.cpl tool, 466
Power Options, Control Panel, 466
PowerPivot for SharePoint, 662
PowerShell 2.0, 114
  for controlling local access to a computer, 357–358
  for Exchange Management, 492
  for managing backups, 413–416
  for opening multiple Remote Desktop sessions, 361
  for opening native consoles, 464
power strips, 50
power supply. *See also* disaster planning; fault tolerance
  failure, types of, 47
  local (for server)
    failure of, 48–50
    replacing, 49
  long-term outages, 53–54
  short-term outages, 53
  voltage sags, 52
  voltage variations, 50–51
Preboot Execution Environment. *See* PXE
Premium Add-on for SBS 2011, 1, 6–7
  alternative to, 654–655
  hardware requirements for, 7
  Hyper-V virtualization and, 86
  SQL Server included with. *See* SQL Server 2008 R2 for Small Business
  Windows Server included with. *See* Windows Server 2008 R2 Standard
Pre-Shared Key. *See* PSK
preventive maintenance (PM), for generators, 54
Pre-Windows 2000 Compatible Access domain local group, 211
primary partition, 244, 250
PRINT$ special share, 235
Print command, 327
printer pools, 316, 331–332
printers
  availability of, setting, 328–331
  cost of, 315, 316–317
  drivers for, 325–326
  installing, 319–325
  local, 319, 324–325
  location name for, 318
  location of, 49
  logical printer for, 316
    configuring usage of, 329–330
    creating, 329
    viewing in SBS Console, 330–331
  managing
    from command line, 327–328
    from SBS Console, 326–327
  naming, 318
  network-attached, 319
    adding and sharing, 320–323
    viewing in SBS Console, 322–323
  permissions for, 328
  placement of, 317–318
  requirements for, determining, 316–317
  security for, 328–331
  server-grade, 15–16
  shared
    drivers for, 325–326
    local printers, 324–325
    network-attached printers, 320–323
    share name for, 318
  share name for, 318
Print Operators domain local group, 211
Print permission, 328
print servers, 315–316
print spooling, 332–333
Private Key Infrastructure (PKI) Viewer, 465
Private Profile, for Windows Firewall, 512
private virtual network, 91
privileges, 240
processes, unresponsive, 716–717
process identification. *See* PID

processors (CPUs)
client requirements for, 36
Intel and AMD, compatibility between, 15
monitoring, 712–714
performance of, 6
registers on, 12
requirements for, 6, 7
server requirements for, 35
for VM (virtual machine), 101, 102–103
Product ID. *See* PID
profiles, for Windows Firewall, 511–512
Programs and Features, Control Panel, 466
PSK (Pre-Shared Key), 508, 509
PTE. *See* system PTE
Public Profile, for Windows Firewall, 512
Pulse Frequency Modulation. *See* PFM
PXE (Preboot Execution Environment), 757

Q

-quiet parameter, Wbadmin, 419
quotas
directory quotas, 300–306
creating, 301–302
for shared folders, setting, 232
types of, 300
viewing and managing, 302–303
disk quotas, 300
quota templates, 300
creating and editing, 303–306

R

RADIUS (802.1X standard), 31, 34, 510
RAID 0+1, 57, 59, 60, 251
RAID-0 (striping), 56, 250
RAID-1 (mirroring), 56, 60, 61, 250, 259–262
RAID-3, 56, 58
RAID-4, 56, 58
RAID-5, 56, 60, 246, 250, 259–262, 271–272
RAID-6, 56, 58, 59, 60
RAID-10, 57, 59, 60, 251
RAID (redundant array of independent disks), 55–61, 245
hardware RAID, 55, 61, 251–252, 253–254
level of, choosing, 57–61, 85
levels of, 55–58
software RAID, 55, 58
RAM (random access memory). *See* physical memory
access to, with 32- and 64-bit architectures, 2, 10–12
client requirements for, 36
server requirements for, 6, 7, 35
for VM (virtual machine), 101, 102–103
range of wireless networks, 32
RAS And IAS Servers domain local group, 211
RDC (Remote Differential Compression), 275
efficiency of, 295
RD Licensing role service, 450, 453, 678
assigning to RD Session Host, 692–694
installing, 688–692
.rdp files, 698–700, 701
RD (Remote Desktop) Gateway role service, 673, 674, 700
RD (Remote Desktop) Web Access, 673, 674, 700
RD Session Host role, 37, 673. *See also* terminal server
adding, 678–688
assigning licensing server to, 692–694
enabling for RWA, 526
requirements for, 676–677
RDS (Remote Desktop Services), 37, 360–361, 673–678
audio and video capabilities for, 685, 686–688
authentication for, 682
installing role and role service for, 678–688
licensing for, 677–678, 683
logon rights through, 240
for second server, 650–653
users allowed to access, setting, 683–684
Windows MultiPoint Server 2011 for, 654–655
RD Virtualization Host role, 37
Read Attributes file permission, 226
Read Data file permission, 226
Read & Execute file permission, 226–227
Read Extended Attributes file permission, 226
Read file permission, 226–227
Read-Only Domain Controllers global group, 213
Read Permissions file permission, 226, 227
Read permission, SharePoint, 599
Read share permission, 224
recovering from backups
applications, 404–406
files and folders, 403–404
for disaster planning, 743–747
GPOs (Group Policy objects), 560

operating system, 406–411
server, 400
volumes, 400–401
with Wbadmin command, 416–422
-recoveryTarget parameter, Wbadmin, 418
Recovery Wizard, 400
for applications and data, 404–406
for files and folders, 401–404
for volumes, 400–401
-recreateDisks parameter, Wbadmin, 418
-recursive parameter, Wbadmin, 419
redundant array of independent disks. *See* RAID (redundant array of independent disks)
redundant networking, 62
redundant power supply, 48
Regional and Language Options, Control Panel, 466
registers, 12
Reliability Monitor, 720–721
relog command, 729
remote access
RDS (Remote Desktop Services), 37, 360–361, 673–678
audio and video capabilities for, 685, 686–688
authentication for, 682
installing role and role service for, 678–688
licensing for, 677–678, 683
logon rights through, 240
for second server, 650–653
users allowed to access, setting, 683–684
Windows MultiPoint Server 2011 for, 654–655
RemoteApps, 673, 674
adding to RWA landing page, 700–708
configuring, 694–700
links for, adding to Companyweb, 613–624
number of simultaneous users, 677
RWA (Remote Web Access), 4, 521–523, 674
as alternative to VPN, 126
computer list for, configuring, 523–526
connecting to, 351–354
links on home page, customizing, 533–537
RemoteApps added to landing page, 700–708
terminal server, accessing, 526–529
TFA (Two Factor Authentication) for, 531–533
users allowed to access, setting, 530–531
when to use, 538
VPN (virtual private network), 510, 538–542
disabling, for migration, 126
enabling, 539–541
permissions for, 541–542
when to use, 538
RemoteApp Manager console, 695–700
RemoteApps, 673, 674
adding to RWA landing page, 700–708
configuring, 694–700
links for, adding to Companyweb, 613–624
number of simultaneous users, 677
Remote Assistance, 358–359
Remote Desktop Connection Client, 351
Remote Desktop Gateway. *See* RD Gateway role service
Remote Desktops Console, 466
Remote Desktop Services. *See* RDS
Remote Desktop Services role, 441, 447, 450, 453
Remote Desktop Users domain local group, 211
Remote Desktop Web Access. *See* RD Web Access
Remote Differential Compression. *See* RDC
remote procedure call. *See* RPC
Remoteprograms.msc tool, 465, 695, 701
Remote Registry Service, 721
Remote Web Access. *See* RWA
Remote Web Workplace. *See* RWW
Remote Web Workplace Users universal group, 209
-removetarget parameter, Wbadmin, 419
Remove-WBBackupTarget cmdlet, PowerShell, 413
Remove-WBBareMetalRecovery cmdlet, PowerShell, 414
Remove-WBFileSpec cmdlet, PowerShell, 413
Remove-WBPolicy cmdlet, PowerShell, 413
Remove-WBSystemState cmdlet, PowerShell, 414
Remove-WBVolume cmdlet, PowerShell, 413
Remove-WindowsFeature cmdlet, PowerShell, 447
replication, DFS, 275–276, 290–296
compared to FRS, 279–280
conflict folder, 295
conflict resolution, 290
health report for, 295
of folders, 291
replication groups
branch office, creating, 292–293
creating, 290
managing, 288–289, 294–296
multipurpose, creating, 293–294
requirements for, 279
staging folder, 295
topologies for, 280, 295

replication groups, DFS
creating, 292–294
managing, 294–296
Replicator domain local group, 211
Reporting Services, SQL Server, 667
reports, 579–585
creating, 584–585
deployment reports for updates, 379
Detailed Network Report, 580, 582–584
for custom alerts, 592–593
from data collector sets, 730–731
network reports, 579–585
Summary Network Report, 579–582
reservations, DHCP
creating, 499–501
scope of, 497
Resource Monitor, 712–717
filtering, 716
unresponsive applications in, handling, 716–717
resources, shared
data, migrating, 165
folders
adding, 229–233
file screen for, 232
protocol for, 230
publishing to DFS namespaces, 233
quotas for, 232
removing, 233
share permissions for, changing, 234–235
for software distribution point, 562–563
special shares, 235–238
storage for, 230
IPC$ special share for, 235
NTFS file permissions for, 237
printers
drivers for, 325–326
local printers, 324–325
network-attached printers, 320–323
share name for, 318
resources (websites and blogs), 759–760
Restartable AD DS, 77
-restoreAllVolumes parameter, Wbadmin, 419
restoring from backups. *See* recovering from backups
Resulting Set of Policies Console, 465
reverse lookup zones, DNS, 503
rights
licensing rights for Windows Server, 108
user rights, 204, 240–242
roles
server roles. *See* server roles
SharePoint roles, 599–606
user roles, 213–217
creating, 215–217
Network Administrator role, 215
Standard User role, 214–215
Standard User with Administration Links role, 215
role services, 441
adding, 444–445, 450–452
removing, 452–454
Rootscalability command, Dfsutil, 289
root servers, for DNS forwarding, 505
routers
access points built-in to, 31
adding, for migration, 116–117, 124–125
dual-WAN router, 62
requirements for, 33–34
Routing and Remote Access Manager, 465
RPC (remote procedure call), 16
Rrasmgmt.msc tool, 465
RSA SecureID OTP tokens, 42
Rsop.msc tool, 465
rules, for firewall policies, 513
RWA (Remote Web Access), 4, 521–523, 674
as alternative to VPN, 126
computer list for, configuring, 523–526
connecting to, 351–354
links on home page, customizing, 533–537
RemoteApps added to landing page, 700–708
terminal server, accessing, 526–529
TFA (Two Factor Authentication) for, 531–533
users allowed to access, setting, 530–531
when to use, 538
RWW (Remote Web Workplace), 4, 674. *See also* RWA (Remote Web Access)

S

sags, power, 52
SAN (storage area network), 230, 249, 252
SAS (Serially Attached SCSI), 247, 249
SATA RAID controllers, 247
SATA (Serial Advanced Technology Attachment), 247, 249
satellite, geosynchronous, Internet connection, 24

SBS 2011. *See* Small Business Server (SBS) 2011
SBSAfg.exe application, 78
SBS Answer File Generator, 78–79, 142–145
SBSAnswerFile.xml file, 79, 145
SBS Backup. *See* Windows Server Backup
SBSComputers OU, 428–429, 527
SBS Console, 3, 181–182. *See also* Administrative Tools menu
  Advanced Mode of, 458–461
  alerts, viewing, 585–588
  client computers
    remote access to, controlling, 356–357
    removing from network, 361
    status of, viewing, 354–356
    user access to, setting, 524–526
  compared to Server Manager console, 439
  DNS email routing, enabling, 473–474
  logical printers, viewing, 330–331
  network health summary, 199
  POP3 email accounts
    adding, 475–477
    retrieval frequency for, 477–478
  printers
    managing, 326–327
    viewing, 322–323
  Remote Assistance, providing, 358–359
  reports
    creating, 584–585
    Detailed Network Report, 582–584
    Summary Network Report, 580
  RWA links, customizing, 533–537
  Smart Host, enabling, 471–473
  software updates
    deploying or declining, 377–379
    deployment reports, viewing, 379
    excluding computers from, 374–375
    synchronizing, 380
    update groups, changing, 375–376
    update level, setting, 371–372
    update schedule, setting, 372–374
  Summary Network Report, 579
  users, RWA access for, 530–531
  VPN
    enabling, 539–541
    permissions for, configuring, 541–542
SBSServers OU, 515–516, 527
SBS Software Updates. *See* WSUS (Windows Server Update Service)
SBSUsers OU, 141–142, 486
-schedule parameter, Wbadmin, 419
sconfig utility, installing Hyper-V using, 86, 88
scope level DHCP options, 497
Scorpion Software AuthAnvil. *See* AuthAnvil
screen captures, 107
screening files, 306–313
  acceptable use policy and, 307–308
  file groups, 311–313
  file screens
    creating, 307–308
    exceptions to, 308–309
    templates for, 309–311
SCSI controllers, for VM (virtual machine), 102, 103
SCSI (Small Computer System Interface), 246, 249
SDSL (Synchronous DSL) Internet connection, 24
second server. *See* servers, second server on network
Secpol.msc tool, 465
securable objects, 203
security, 40–43. *See also* Group Policy; permissions; user rights
  of 64-bit architecture, 13–14
  alerts regarding, on SBS Console, 199
  authentication
    for RDS (Remote Desktop Services), 682
    TFA (Two Factor Authentication), 34, 42–43, 352–353, 508, 531–533
    for wireless access points, 31
  of browser, 41
  for client computers, 41
  DEP bit for, 13
  DNS poisoning attacks, 506
  DoS (denial-of-service) attack, 33
  drivers, authenticity of, 15
  firewall
    access point built-in to, 34
    adding, for migration, 111, 116–117, 124–125
    diagramming, 30
    requirements for, 33–34
    securing, 43
  for GDT (global descriptor table), 14
  for IDT (interrupt descriptor table), 14
  for kernel, 14
  LAND attack, 33
  network operating system providing, 21
  Password Policies, 41

security *(cont.)*
passwords
for administrator account, 77, 140, 143
for built-in domain local groups, 210
for POP3 email accounts, 475
for SQL Server service accounts, 668
for Standard User domain account, 349
for trusted certificate, 197
for user account, 218–219
for Windows Server, 635
for workgroups, 753
OTP (one-time password), 42–43, 353, 532
physical security, 40, 68
Ping of Death attack, 33
for printers, 328–331
for server, 40
software updates and, 364
for SQL Server, 660
SYN Flood attack, 33
for system service dispatch tables, 14
types of potential attacks, 40
UAC (User Account Control), 224–225
of Windows clients, 41
Windows Firewall, 511–519
configuring, for second server, 654
policies, setting with Group Policy, 512–519
profiles for, 511–512
rules for, 513
for wireless access points, 31, 509
for wireless connections, 508–510
for wireless (WiFi) network, 43
security groups, SBS 2011, 203
creating, 206–207
group scope for, 203, 208
securable objects in, 203
user rights for, 204
security groups, SharePoint, 599, 602
security updates, 363
self-issued certificates, 193
Serial ATA. *See* SATA
Serially Attached SCSI. *See* SAS
server level DHCP options, 497
ServerManagerCmd.exe application
installing Hyper-V using, 86
removing a role using, 447
Server Manager console, 440, 466
compared to SBS Console, 439
features
adding, 455–456
removing, 456–457
roles
adding, 441–446
managing, 461–464
removing, 447–450
role services
adding, 450–452
removing, 452–454
Servermanager.msc tool, 466
Server Message Block. *See* SMB
Server Operators domain local group, 211
server roles, 441
adding, 441–446
File Services role, 279, 281, 296, 441
FSMO (Flexibile Single Master Operations) roles, 70, 337
Hyper-V role, 82
installing, 89–90
other roles limited by, 86, 108
partitions for, 14
requirements for, 84–85
support for, 17
with SBS in Hyper-V, 107–108
incorporating in naming conventions, 39
managing, 461–464
Network Policy And Access Services role, 447
RD Session Host role, 37
RD Virtualization Host role, 37
Remote Desktop Services role, 441, 447, 450, 453
removing, 447–450
Web Server (IIS) role, 447
servers, 751–752
DHCP servers, 496, 497
DNS server, SBS 2011 as, 496
Exchange Server 2010, 5, 469
Hyper-V Server. *See* Hyper-V Server 2008 R2
Internet domain name managed by, 190–191
ISA server, 111, 125
ISP servers, DNS forwarding to, 506–507
load of, determining, 35–36
namespace server, DFS, 276, 285
naming, 39, 75
operating system for, 19–21
physical location of, 49, 68
physical security for, 40
power supply for, failure of, 48–50

print servers, 315–316
recovering from backups, 400
requirements for, 34–36
SBS 2011. *See* Small Business Server (SBS) 2011
second server on network
Windows Server as. *See* Windows Server 2008 R2 Standard
SQL Server. *See* SQL Server 2008 R2 for Small Business
terminal server, 526–529
trusted certificates for, 193–198
exporting, 195–197
for migration, 143
importing, 197–198
purchasing, 194–195
Windows Server. *See also* Windows Server 2008 R2 Standard
service accounts, SQL Server, 668
service packs, 364
services
alerts for, 586–587
role services, 441
adding, 444–445, 450–452
removing, 452–454
stopped, custom alert for, 589–593
Services.msc tool, 466, 721
Services tool, 466
Set-WBPolicy cmdlet, PowerShell, 413
Set-WBSchedule cmdlet, PowerShell, 413
Set-WBVssBackupOptions cmdlet, PowerShell, 414
Share and Storage Management Console, 466
shared resources
data, migrating, 165
folders
adding, 229–233
file screen for, 232
protocol for, 230
publishing to DFS namespaces, 233
quotas for, 232
removing, 233
share permissions for, changing, 234–235
for software distribution point, 562–563
special shares, 235–238
storage for, 230
IPC$ special share for, 235
NTFS file permissions for, 237
printers
drivers for, 325–326
local printers, 324–325
network-attached printers, 320–323
share name for, 318
share permissions, 223–224, 237–238
changing, 234–235
hiding, 238
recommended settings for, 223
setting, 231–232
users applied to, 224
SharePoint Foundation 2010, 5, 597–606
Companyweb SharePoint site. *See* Companyweb SharePoint site
discussions, 599
libraries, 598
lists, 599
permissions, 599–606
changing for a group, 600–602
changing for section of Companyweb, 602–606
roles, 599–606
security groups, 599, 602
tasks, 599
web pages, 599
SharePoint_MembersGroup universal group, 209
SharePoint_OwnersGroup universal group, 209
SharePoint_VisitorsGroup universal group, 209
Shavlik NetChk Protect, 381
short-term power outages, 53
-showsummary parameter, Wbadmin, 419
Simple Network Management Protocol. *See* SNMP
simple volume, 244, 255–259
single large expensive disk. *See* SLED
16-bit applications, not supported, 17
64-bit architecture, 2, 9–18
32-bit application support with, 16–17
for client computers, 17–18
driver requirements for, 15
hardware requirements for, 15
increased RAM access with, 2, 10–12
legacy software, potential problems with, 16–17
registers with, 12
security with, 13–14
transitioning to, 9–10
virtualization with, 14–15, 82
-skipBadClusterCheck parameter, Wbadmin, 419
SLED (single large expensive disk), 246
Small Business Server (SBS) 2003, migration issues, 111
Small Business Server (SBS) 2011
64-bit architecture of, 2
editions of, 1

Small Business Server (SBS) 2011 *(cont.)*
Exchange Server 2010 in. *See* Exchange Server 2010
hardware requirements, 6–7, 15
for backups, 35
for client computers, 36
for firewall, 33–34
for Hyper-V virtualization, 84–85
for printers, 316–317
for RD Session Host role, 676–677
for router, 33–34
for SBS on Hyper-V child partition, 108–109
for second server, 627–629
for server, 34–36
for SQL Server, 659
for wireless access points, 31
installing, 4, 67–80
answer file for, 78–79
automating, 757–758
disks, partitioning, 67–68
layout, planning, 68
problems with, resolving, 182
process for, 70–77
server, preparing, 69–70
when migrating to, 145–146
migrating to. *See* migrating to SBS 2011
new features in, 2–5
Premium Add-on for, 1, 6–7
alternative to, 654–655
hardware requirements for, 7
Hyper-V virtualization and, 86
SQL Server included with. *See* SQL Server 2008 R2 for Small Business
Windows Server included with. *See* Windows Server 2008 R2 Standard
resources for, 759–760
SBS Console for. *See* SBS Console
security for. *See* security
SharePoint Foundation Services in. *See* SharePoint Foundation 2010
troubleshooting. *See* troubleshooting
Small Computer System Interface. *See* SCSI
Smart Host, 470, 471–473
SMB (Server Message Block)
for shared folders, 230–231
SMTP forwarding with Smart Host, 470, 471–473
snapshots, for VM (virtual machine), 94, 95, 106
SNMP (Simple Network Management Protocol), 50
software. *See* applications
software RAID, 55, 58
software updates
alerts regarding, on SBS Console, 199
assessing vulnerabilities and priority for, 366
availability of, determining, 367–368
configuring for second server, 644–648
cycle for, 365–370
declined, deploying after, 378–379
declining, 376
deploying, 369–370, 376–380
deployment reports for, 379
EULA (End User License Agreement) for, 376
evaluating need for, 368–369
importance of, 364
managed by WSUS, 115, 370
excluding computers from, 374–375
third-party alternatives to, 381
update groups, changing, 375–376
update level, setting, 370–372
update schedule, setting, 372–374
Microsoft's schedule for, 365
for SQL Server, 662
synchronization of, 380
types of, 363–364
VPN for, 538
solid state drive. *See* SSD
SOPs (standard operating procedures), 737–739
Sound, Control Panel, 466
spanned volume, 245, 250. *See also* extended volume
spare parts, 62
location of, 49
power supply, 48–49
special shares, 235–238
spikes, power, 50–51
SPI (Stateful Packet Inspection), 33, 43
split DNS, 503
SQL Client Connectivity SDK, SQL Server, 667
SQL Server 2008 R2 for Small Business, 6
configuration checker for, 660, 663
documentation for, 659–662, 671
failover clustering for, 661, 662, 663, 664
features available for, 667–668
installed features discovery for, 663
installing
help for, 661
options for, 657, 662, 664–665
planning for, 659–665

process for, 658, 665–671
restrictions on, 658
maintenance for, 663
PowerPivot for SharePoint with, 662
release notes for, 660
requirements for, 659
security documentation for, 660
service accounts for, 668
updates for, 662
Upgrade Advisor for, 661
upgrade documentation for, 662
upgrading, 662
upgrading Integration Services Packages, 663
SQL Server Books Online, SQL Server, 667
SQL Server Installation Center, 658–665
SQL Server Replication, 667
SQL Slammer worm, 13
SSD (Solid State Disk), 247, 249
SSE/SSE2 registers, 13
SSID hiding, 509
staging folder, DFS replication, 295
stand-alone namespaces, 277
stand-alone wireless bridges, 31
Standard edition of SBS 2011, 1
standard operating procedures (SOPs), 737–739
Standard User domain accounts, 348–349
Standard User role, 214–215
Standard User with Administration Links role, 215
star network topology, 30
start backup subcommand, Wbadmin, 420
start recovery subcommand, Wbadmin, 420–421
start sysrecovery subcommand, Wbadmin, 421
start systemstatebackup subcommand, Wbadmin, 421
start systemstaterecovery subcommand, Wbadmin, 421
Start-WBBackup cmdlet, PowerShell, 413
static IP address, 25
DHCP exclusions for, 498–499
for secondary servers, 341
stop job subcommand, Wbadmin, 420
storage. *See* DFS (Distributed File System); disk management; hard disks
storage area network. *See* SAN
storage capacity. *See* disk space
Storage Explorer Console, 466
Storagemgmt.msc tool, 466
storage reports, FSRM, 296–300
Storexpl.msc tool, 466
striped mirrored disks, 57
striping (RAID-0), 56, 245, 250
Summary Network Report, 579–582
surge protectors, 50
surges, power, 51
Swing Migration, 113
switches, 30
Synchronous DSL. *See* SDSL Internet connection
SYN Flood attack, 33
Sysdm.cpl tool, 466
System Center Virtual Machine Manager. *See* SCVMM
System Configuration Checker, 660, 663
System Properties, Control Panel, 466
system PTE, limits of, 11
system requirements, 6–7, 15. *See also* Mac OS/X clients; operating system; Windows clients
for backups, 35
for client computers, 36
for firewall, 33–34
for Hyper-V virtualization, 84–85
for printers, 316–317
for RD Session Host role, 676–677
for router, 33–34
for SBS on Hyper-V child partition, 108–109
for second server, 627–629
for server, 34–36
for SQL Server, 659
for wireless access points, 31
system service displatch tables, security for, 14
System Stability Index, 720
SYSVOL special share, 235

T

Take Ownership file permission, 226, 227
Tapimgmt.msc tool, 466
Taskschd.msc tool, 466
Task Scheduler, 466
tasks, SharePoint, 599
teamed networking, 62
Telephon.cpl tool, 466
Telephony Console, 466
templates
for file screens, 309–311
for quotas, 300, 303–306
terminal server, 526–529. *See also* RD Session Host role
Terminal Server License Servers domain local group, 211

Terminal Services
logon rights through, 240
Remote Desktop Services as replacement for, 673, 674
Terminal Services Configuration, 466
Terminal Services Gateway Manager, 466
Terminal Services Manager, 466
terms of service. *See* TOS
TFA (Two Factor Authentication), 34, 508
for RWA (Remote Web Access), 352–353, 531–533
implementing, 42–43
theft of service, 40
32-bit applications, support for, 16–17
32-bit architecture, 2
for client computers, 17–18
limited RAM access with, 2, 10–12
registers with, 12
Timedate.cpl tool, 466
time zone, setting, 74, 637–638
token, authentication using. *See* OTP (one-time password)
TOS (terms of service), 25
Tpm.msc tool, 466
TPM (Trusted Platform Module) Management, 466
Traverse Folder file permission, 226
troubleshooting. *See also* monitoring
affected by combining share and NTFS permissions, 223
affected by disabling Internet pings, 43
connectivity issues, FMNW for, 519–520, 542–546
DHCP reservations and, 496, 504
nonresponsive applications, 716–717
reverse lookup zones for, 503
screen captures for, 107
Server Manager and, 440
trusted certificates, 193–198
exporting, 195–197
for migration, 143
importing, 197–198
purchasing, 194–195
Trusted Platform Module (TPM) Management, 466
Tsadmin.msc tool, 466
Tsconfig.msc tool, 466, 693
Tsgateway.msc tool, 466
Tsmmc.msc tool, 466
TS RemoteApp Manager, 465
Two Factor Authentication. *See* TFA

U

UAC (User Account Control), 224–225
unattend.xml file, 757
uninterruptible power supply. *See* UPS
Universal Plug and Play. *See* UPnP
universal scope, 208, 209
update rollups, 364
updates
alerts regarding, on SBS Console, 199
assessing vulnerabilities and priority for, 366
availability of, determining, 367–368
configuring for second server, 644–648
cycle for, 365–370
declined, deploying after, 378–379
declining, 376
deploying, 369–370, 376–380
deployment reports for, 379
EULA (End User License Agreement) for, 376
evaluating need for, 368–369
importance of, 364
managed by WSUS, 115, 370
excluding computers from, 374–375
third-party alternatives to, 381
update groups, changing, 375–376
update level, setting, 370–372
update schedule, setting, 372–374
Microsoft's schedule for, 365
for SQL Server, 662
synchronization of, 380
types of, 363–364
VPN for, 538
upgrading to SBS 2011. *See* migrating to SBS 2011
UPnP (Universal Plug and Play), 34
UPS (uninterruptible power supply), 51–52
USB (Universal Serial Bus), 249
User Account Control. *See* UAC
user accounts. *See also* groups
adding, 217–221, 338, 754
computer access, granting, 221
migrating, 166–170
-user parameter, Wbadmin, 419
user rights, 204, 240–242
user roles, 213–217
creating, 215–217
Network Administrator role, 215
Standard User role, 214–215
Standard User with Administration Links role, 215

User Roles universal group, 209
users
  assigning software to, 561–562
  computer list for, configuring, 523–526
  RDS access by, setting, 683–684
  RWA access for, enabling or disabling, 530–531
  types of, affected by share permissions, 224
Users domain local group, 211

V

VDI (Virtual Desktop Infrastructure), 37
-version parameter, Wbadmin, 419
VFD (virtual floppy drive), 102, 105
VHD files, 94, 95
VHD (virtual hard disk)
  differencing disks, 104
  dynamic disks, 104, 245, 250
    compared to fixed-size disks, 99
    for software RAID, 55
    when to use, 253
  fixed-size disks, 99, 104
  mounting, 272–273
video adapter, 6
video capabilities, for RDS, 685, 686–688
video files, controlling use of, 307–308
View command, Dfscmd, 289
Virtmgmt.msc tool, 466
Virtual Desktop Infrastructure. *See* VDI
virtual floppy drive. *See* VFD
virtual hard disk. *See* VHD
virtualization
  emulation virtualization, 83–84
  Hyper-V virtualization, 14–15, 81–85
    configuring, 91–95
    disaster planning issues for, 747–748
    on Hyper-V Server 2008 R2, 86, 87–88
    installing, 86–90
    network configuration, 91–93
    network, types of, 91
    partitions for, 14–15, 83–84, 107–109
    RAID level for, 85
    reasons for, 82
    requirements for, 84–85
    second server as, 627
    server configuration, 93–95
    version of, choosing, 86
    VM, creating, 95–100
    VM, machine settings for, 101–105
    VM, using, 105–106
    on Windows Server 2008 R2, 86, 89–90
virtual machine. *See* VM
virtual memory address space, 10, 11, 12
virtual networks, types of, 91
Virtual Server 2005 R2, 83
viruses, 40
Visitors group, SharePoint, 599
VM (virtual machine)
  BIOS for, 101
  clipboard for, 106–107
  COM ports for, 102, 105
  creating, 95–100
  disk types for. *See* VHD (virtual hard disk)
  IDE controllers for, 101, 103
  machine settings for, 101–105
  memory for, 101, 102–103
  naming, 97
  network adapters for, 102, 105
  pausing, 106
  processors for, 101, 102–103
  running incompatible software on, 17
  saving, 106
  screen captures for, 107
  SCSI controllers for, 102, 103
  snapshots for, 94, 95, 106
  starting, 105
  stopping, 106
  VFD for, 105
voltage variations, 50–51
volumes, 244, 250
  adding, 253–263
  compared to partitions, 252
  deleting, 262
  extended volume, 264–267
  logical drive/volume, 245
  mirror volume, 246
    breaking, 271
    failure of, recovering from, 268–271
  mounting, 273–274
  naming, 272
  RAID-0 (striping), 245, 250
  RAID-1 volume, 250, 259–262
  RAID-5 volume, 246, 250, 259–262, 271–272
  recovering from backup, 400–401
  shrinking, 263–264

volumes *(cont.)*
simple volume, 244, 255–259
spanned volume, 245, 250
special shares for, 235–236
Volume Shadow Service. *See* VSS
VPN pass-through, 33
VPN tunnels, 34
VPN (virtual private network), 510, 538–542
disabling, for migration, 126
enabling, 539–541
permissions for, 541–542
when to use, 538
-vssFull parameter, Wbadmin, 419
VSS (Volume Shadow Service), 404, 414

W

WAN connection, dual-WAN support with, 34
Wbadmin command, 416–422
Wbadmin.msc tool, 466
WBFileSpec object, 414
WBSchedule object, 414
WCN (Windows Connect Now), 509
web hosting, ISP providing, 25
web pages, SharePoint, 599
Web Part
adding to Companyweb, 621–624
enabling, 616–619
folder for, 620–621
registering as safe, 619–620
Web Server (IIS) role, 447
websites, 759–760
Weilbacher, Kevin (Microsoft MVP for SBS), 125
WEP (Wired Equivalent Privacy), 508, 509
WET (Windows Easy Transfer) Wizard, 361
Wf.msc tool, 466, 511
WiFi Internet connection, 24
WiFi network. *See* wireless (WiFi) network
Wi-Fi Protected Access. *See* WPA
Windows 7 Automated Installation Kit, 757–758
Windows Authorization Access Group domain local group, 211
Windows clients. *See also* Windows Server 2003; Windows Server 2008 R2 Standard
for client computers, 17–18, 36, 756
DFS namespace requirements for, 278–279
security of, 41
Windows 7
for client computers, 18
configuring for DHCP, 339–341
connecting to network, 342–349
sharing printer connected to, 325
transitioning to, 9
Windows 2000, connecting to network, 349–350
Windows Vista
for client computers, 18
configuring for DHCP, 339–341
connecting to network, 342–349
sharing printer connected to, 324
Windows XP
for client computers, 18
configuring for DHCP, 341
connecting to network, 342–349
sharing printer connected to, 325
Windows Connect Now (WCN), 509
Windows Deployment Services, 757
Windows Easy Transfer Wizard. *See* WET Wizard
Windows Firewall, 511–519
configuring, for second server, 654
policies, setting with Group Policy, 512–519
profiles for, 511–512
rules for, 513
Windows Firewall, Control Panel, 466
Windows Firewall with Advanced Security console, 466, 511
Windows Installation disc, 406–411
Windows Installer Package. *See* .msi files
Windows Management Instrumentation. *See* WMI
Windows Management Instrumentation (WMI) Manager, 466
Windows MultiPoint Server 2011, 654–655
Windows on Windows 64-bit. *See* WOW64
Windows PowerShell 2.0, 114
for controlling local access to a computer, 357–358
for Exchange Management, 492
for managing backups, 413–416
for opening multiple Remote Desktop sessions, 361
for opening native consoles, 464
Windows print server, 315–316
Windows Recovery Environment, 400, 406–411, 422
Windows SBS Admin Tools Group universal group, 209
Windows SBS Fax Administrators universal group, 209
Windows SBS Fax Users universal group, 209
Windows SBS Folder Redirection Accounts universal group, 209

Windows SBS Link Users universal group, 209
Windows SBS Remote Web Workplace Users universal group, 209
Windows SBS SharePoint_MembersGroup universal group, 209
Windows SBS SharePoint_OwnersGroup universal group, 209
Windows SBS SharePoint_VisitorsGroup universal group, 209
Windows SBS Virtual Private Network Users universal group, 209
Windows Server 2003
  configuring for DHCP, 341
  connecting to network, 342–349
Windows Server 2008 R2 Standard, 2, 6, 752–753
  as second server on network, 627, 755–756
    backups, enabling, 649
    computer name for, 641–644
    configuring, 636–648
    domain name for, 641–644
    feedback, enabling, 644–647
    hardware drivers, installing, 637
    installing, 630–636
    networking, configuring, 639–641
    Remote Desktop for, 650–653
    requirements for, 627–629
    time zone, setting, 637–638
    updates, downloading and installing, 647–648
    updates, enabling, 644–647
    Windows Firewall, configuring, 654
  configuring for DHCP, 339–341
  connecting to network, 342–349
  Hyper-V virtualization on, 86, 89–90. *See* Hyper-V virtualization
  installing, 70–73
  licensing rights for, 108
  limitations on, from SBS, 70
Windows Server Backup. *See also* backups
  configuring
    with Configure Server Backup Wizard, 383–384, 385–391
    with Windows Server Backup console, 391–395
  installing for second server, 649
  SBS Backup as, 383
Windows Server Backup console, 391–395, 466
Windows.Serverbackup PowerShell snap-in, 413–416
Windows Server Update Service. *See* WSUS
Windows Setup disc, 400, 406–411
Windows SharePoint Services. *See* SharePoint Foundation 2010
Windows Small Business Server 2011. *See* Small Business Server (SBS) 2011
Windows Storage Server 2008 R2 Essentials. *See* WSSE
Wired Equivalent Privacy. *See* WEP
wireless access points, 31–33
  antennas for, 31
  authentication for, 31
  bridges and, 31
  built-in to firewall, 34
  built-in to router, 31
  channels for, 33
  interference of, 32
  placement of, 32–33
  range of, 32
  requirements for, 31
  security for, 31, 509
  supplementing wired network, 25
wireless bridges, 31, 33
wireless connectivity, 508–510
  MAC address filtering for, 509
  SSID hiding for, 509
  TFA (Two Factor Authentication) for, 508
  VPN (virtual private network) for, 510
  WEP (Wired Equivalent Privacy) for, 508, 509
  WPA2 encryption for, 43, 508–509, 510
  WPA (Wi-Fi Protected Access) for, 508, 510–512
wireless hackers, 40
wireless (WiFi) network, 26
  security for, 43
  standards for, 27–28
Wmimgmt.msc tool, 466
WMI (Windows Management Instrumentation) Manager, 466
workgroups, 20, 753. *See also* peer-to-peer network
workspace, Companyweb, 606–613
workstations. *See* client computers
worms, 40
WOW64 (Windows On Windows 64-bit), 16
WPA2 encryption (802.11i standard), 31, 43, 508–509, 510
WPA (Wi-Fi Protected Access), 508, 510–512
Write Attributes file permission, 226, 227
Write Data file permission, 226
Write Extended Attributes file permission, 226, 227
Write file permission, 226–227

WSSE (Windows Storage Server 2008 R2 Essentials), 248, 252, 383, 422–434
connecting to client computers, 430–433
connecting to SBS domain, 423–429
Launchpad for, 433–434
WSUS (Windows Server Update Services), 115, 370
excluding computers from, 374–375
third-party alternatives to, 381
update groups, changing, 375–376
update level, setting, 370–372
update schedule, setting, 372–374

X

XML (Extended Markup Language)
for custom alert, creating, 591–593, 594–595
storage reports in, 296

About the Authors

Charlie Russel is an information technology consultant, specializing in combined Windows and UNIX networks. He is also a Microsoft Most Valuable Professional for Windows Server and Security. Together with Sharon Crawford, Charlie authored *Windows Server 2008 Administrator's Companion* and *Windows Small Business Server 2008 Administrator's Companion*. Charlie also coauthored the *Windows Essential Business Server 2008 Administrator's Companion*.

Sharon Crawford is a veteran writer of computer books. Together with Charlie Russel, Sharon authored *Windows Server 2008 Administrator's Companion* as well as the *Windows Small Business Server 2008 Administrator's Companion*.

Microsoft

How To Download Your eBook

To download your eBook, go to
http://aka.ms/PressEbook
and follow the instructions.

Please note: You will be asked to create a free online account and enter the access code below.

Your access code:

XLTWSBS

Windows Small Business Server 2011
Administrator's Companion

Your PDF eBook allows you to:

- Search the full text
- Print
- Copy and paste

Best yet, you will be notified about free updates to your eBook.

If you ever lose your eBook file, you can download it again just by logging in to your account.

Need help? Please contact:
mspinput@microsoft.com.

Please note: This access code is non-transferable and is void if altered or revised in any way. It may not be sold or redeemed for cash, credit, or refund.