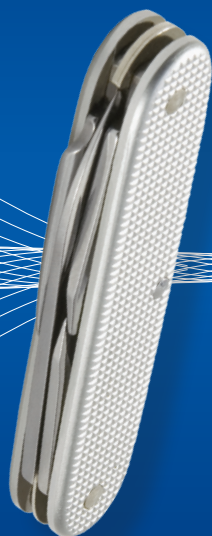


# Windows Server® 2012

William R. Stanek  
*Author and Series Editor*



# Pocket Consultant

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

Copyright © 2012 by William R. Stanek

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

Library of Congress Control Number: 2012944749  
ISBN: 978-0-7356-6633-7

Printed and bound in the United States of America.

First Printing

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at [msspinput@microsoft.com](mailto:msspinput@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 author, Microsoft Corporation, nor its resellers or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

**Acquisitions Editor:** Anne Hamilton

**Developmental Editor:** Karen Szall

**Project Editor:** Karen Szall

**Editorial Production:** Curtis Philips

**Technical Reviewer:** Bob Hogan; Technical Review services provided by Content Master, a member of CM Group, Ltd.

**Copyeditor:** Roger LeBlanc

**Indexer:** William P. Meyers

**Cover:** Twist Creative • Seattle

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

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

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

—WILLIAM R. STANEK





# Contents at a Glance

*Introduction*

xxv

## **PART I      WINDOWS SERVER 2012 ADMINISTRATION FUNDAMENTALS**

---

CHAPTER 1	Windows Server 2012 Administration Overview	3
CHAPTER 2	Managing Servers Running Windows Server 2012	31
CHAPTER 3	Monitoring Processes, Services, and Events	87
CHAPTER 4	Automating Administrative Tasks, Policies, and Procedures	135
CHAPTER 5	Enhancing Computer Security	191

## **PART II      WINDOWS SERVER 2012 DIRECTORY SERVICES ADMINISTRATION**

---

CHAPTER 6	Using Active Directory	217
CHAPTER 7	Core Active Directory Administration	249
CHAPTER 8	Creating User and Group Accounts	295
CHAPTER 9	Managing User and Group Accounts	347

## **PART III      WINDOWS SERVER 2012 DATA ADMINISTRATION**

---

CHAPTER 10	Managing File Systems and Drives	385
CHAPTER 11	Configuring Volumes and RAID Arrays	419
CHAPTER 12	Data Sharing, Security, and Auditing	457
CHAPTER 13	Data Backup and Recovery	519

## **PART IV      WINDOWS SERVER 2012 NETWORK ADMINISTRATION**

---

CHAPTER 14	Managing TCP/IP Networking	559
CHAPTER 15	Running DHCP Clients and Servers	573
CHAPTER 16	Optimizing DNS	615

*Index*

651



# Contents

*Introduction*

xxv

## **PART I      WINDOWS SERVER 2012 ADMINISTRATION FUNDAMENTALS**

---

<b>Chapter 1</b>	<b>Windows Server 2012 Administration Overview</b>	<b>3</b>
	Windows Server 2012 and Windows 8 . . . . .	4
	Getting to Know Windows Server 2012 . . . . .	6
	Power Management Options . . . . .	8
	Networking Tools and Protocols . . . . .	11
	Understanding Networking Options	11
	Working with Networking Protocols	12
	Domain Controllers, Member Servers, and Domain Services . . .	14
	Working with Active Directory	14
	Using Read-Only Domain Controllers	16
	Using Restartable Active Directory Domain Services	16
	Name-Resolution Services . . . . .	17
	Using Domain Name System	18
	Using Windows Internet Name Service	20
	Using Link-Local Multicast Name Resolution	22
	Frequently Used Tools . . . . .	23
	Windows PowerShell 3.0	24
	Windows Remote Management	25

---

### **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](http://microsoft.com/learning/booksurvey)

<b>Chapter 2</b>	<b>Managing Servers Running Windows Server 2012</b>	<b>31</b>
	Server Roles, Role Services, and Features for Windows Server 2012 . . . . .	32
	Full-Server, Minimal-Interface, and Server Core Installations . . .	40
	Navigating Server Core	40
	Installing Windows Server 2012. . . . .	43
	Performing a Clean Installation	44
	Performing an Upgrade Installation	47
	Performing Additional Administration Tasks During Installation	48
	Changing the Installation Type	55
	Managing Roles, Role Services, and Features. . . . .	57
	Performing Initial Configuration Tasks	58
	Server Manager Essentials and Binaries	62
	Managing Your Servers Remotely	65
	Connecting to and Working with Remote Servers	67
	Adding and Removing Roles, Role Services, and Features	70
	Managing System Properties . . . . .	73
	The Computer Name Tab	75
	The Hardware Tab	75
	The Advanced Tab	76
	The Remote Tab	85
<b>Chapter 3</b>	<b>Monitoring Processes, Services, and Events</b>	<b>87</b>
	Managing Applications, Processes, and Performance. . . . .	87
	Task Manager	88
	Viewing and Working with Processes	88
	Administering Processes	91
	Viewing System Services	94
	Viewing and Managing System Performance	95
	Viewing and Managing Remote User Sessions	99
	Managing System Services . . . . .	100
	Navigating Services in Server Manager	100
	Navigating Services in Computer Management	102

Starting, Stopping, and Pausing Services	103
Configuring Service Startup	103
Configuring Service Logon	104
Configuring Service Recovery	106
Disabling Unnecessary Services	107
Event Logging and Viewing . . . . .	108
Accessing Events in Server Manager	109
Accessing Events in Event Viewer	110
Filtering Event Logs	112
Setting Event Log Options	115
Clearing Event Logs	116
Archiving Event Logs	116
Monitoring Server Performance and Activity . . . . .	118
Why Monitor Your Server?	118
Getting Ready to Monitor	119
Using the Monitoring Consoles	119
Choosing Counters to Monitor	122
Performance Logging	124
Viewing Data Collector Reports	128
Configuring Performance Counter Alerts	129
Tuning System Performance. . . . .	130
Monitoring and Tuning Memory Usage	130
Monitoring and Tuning Processor Usage	132
Monitoring and Tuning Disk I/O	133
Monitoring and Tuning Network Bandwidth and Connectivity	134

## **Chapter 4 Automating Administrative Tasks, Policies, and Procedures 135**

Understanding Group Policies. . . . .	138
Group Policy Essentials	138
In What Order Are Multiple Policies Applied?	139
When Are Group Policies Applied?	139
Group Policy Requirements and Version Compatibility	140
Navigating Group Policy Changes . . . . .	141

Managing Local Group Policies . . . . .	143
Local Group Policy Objects	143
Accessing the Top-Level Local Policy Settings	144
Local Group Policy Object Settings	145
Accessing Administrator, Non-Administrator, and User-Specific Local Group Policy	146
Managing Site, Domain, and Organizational Unit Policies. . . .	147
Understanding Domain and Default Policies	147
Using the Group Policy Management Console	148
Getting to Know the Policy Editor	149
Using Administrative Templates to Set Policies	151
Creating and Linking GPOs	152
Creating and Using Starter GPOs	153
Delegating Privileges for Group Policy Management	154
Blocking, Overriding, and Disabling Policies	155
Maintaining and Troubleshooting Group Policy . . . . .	158
Refreshing Group Policy	158
Configuring the Refresh Interval	159
Modeling Group Policy for Planning Purposes	161
Copying, Pasting, and Importing Policy Objects	164
Backing Up and Restoring Policy Objects	165
Determining Current Group Policy Settings and Refresh Status	166
Disabling an Unused Part of Group Policy	166
Changing Policy Processing Preferences	167
Configuring Slow-Link Detection	167
Removing Links and Deleting GPOs	170
Troubleshooting Group Policy	171
Fixing Default Group Policy Objects	172
Managing Users and Computers with Group Policy . . . . .	173
Centrally Managing Special Folders	173
User and Computer Script Management	178
Deploying Software Through Group Policy	181
Automatically Enrolling Computer and User Certificates	186
Managing Automatic Updates in Group Policy	187

<b>Chapter 5</b>	<b>Enhancing Computer Security</b>	<b>191</b>
	Using Security Templates . . . . .	191
	Using the Security Templates and Security Configuration And Analysis Snap-ins . . . . .	193
	Reviewing and Changing Template Settings . . . . .	193
	Analyzing, Reviewing, and Applying Security Templates . . . . .	201
	Deploying Security Templates to Multiple Computers . . . . .	204
	Using the Security Configuration Wizard . . . . .	206
	Creating Security Policies . . . . .	206
	Editing Security Policies . . . . .	211
	Applying Security Policies . . . . .	211
	Rolling Back the Last-Applied Security Policy . . . . .	211
	Deploying a Security Policy to Multiple Computers . . . . .	212

---

## **PART II    WINDOWS SERVER 2012 DIRECTORY SERVICES ADMINISTRATION**

---

<b>Chapter 6</b>	<b>Using Active Directory</b>	<b>217</b>
	Introducing Active Directory . . . . .	217
	Active Directory and DNS . . . . .	217
	Read-Only Domain Controller Deployment . . . . .	219
	Active Directory Features for Windows Server 2008 R2 . . . . .	220
	Active Directory Features for Windows Server 2012 . . . . .	221
	Working with Domain Structures . . . . .	223
	Understanding Domains . . . . .	224
	Understanding Domain Forests and Domain Trees . . . . .	225
	Understanding Organizational Units . . . . .	227
	Understanding Sites and Subnets . . . . .	229
	Working with Active Directory Domains . . . . .	230
	Using Computers with Active Directory . . . . .	230
	Working with Domain Functional Levels . . . . .	231
	Raising or Lowering Domain and Forest Functionality . . . . .	235

Understanding the Directory Structure . . . . .	237
Exploring the Data Store . . . . .	238
Exploring Global Catalogs . . . . .	239
Universal Group Membership Caching . . . . .	240
Replication and Active Directory . . . . .	241
Active Directory and LDAP . . . . .	242
Understanding Operations Master Roles . . . . .	242
Using the Active Directory Recycle Bin . . . . .	244
Preparing Schema for the Recycle Bin . . . . .	244
Recovering Deleted Objects . . . . .	245
 <b>Chapter 7   Core Active Directory Administration</b>	 <b>249</b>
Tools for Managing Active Directory . . . . .	249
Active Directory Administration Tools . . . . .	249
Active Directory Command-Line Tools . . . . .	250
Active Directory Support Tools . . . . .	251
Using Active Directory Users And Computers . . . . .	252
Active Directory Administrative Center and Windows PowerShell . . . . .	256
Managing Computer Accounts . . . . .	259
Creating Computer Accounts on a Workstation or Server . . . . .	259
Creating Computer Accounts in Active Directory Administrative Center . . . . .	260
Creating Computer Accounts in Active Directory Users And Computers . . . . .	261
Viewing and Editing Computer Account Properties . . . . .	263
Deleting, Disabling, and Enabling Computer Accounts . . . . .	264
Resetting Locked Computer Accounts . . . . .	264
Moving Computer Accounts . . . . .	266
Managing Computers . . . . .	267
Joining a Computer to a Domain or Workgroup . . . . .	267
Using Offline Domain Join . . . . .	268
Managing Domain Controllers, Roles, and Catalogs . . . . .	270
Installing and Demoting Domain Controllers . . . . .	270
Viewing and Transferring Domainwide Roles . . . . .	273



Viewing and Transferring the Domain Naming Master Role	275
Viewing and Transferring Schema Master Roles	275
Transferring Roles Using the Command Line	276
Seizing Roles Using the Command Line	276
Configuring Global Catalogs	280
Configuring Universal Group Membership Caching	281
Managing Organizational Units	281
Creating Organizational Units	281
Viewing and Editing Organizational Unit Properties	282
Renaming and Deleting Organizational Units	282
Moving Organizational Units	282
Managing Sites	282
Creating Sites	283
Creating Subnets	284
Associating Domain Controllers with Sites	285
Configuring Site Links	285
Configuring Site Link Bridges	288
Maintaining Active Directory	289
Using ADSI Edit	289
Examining Intersite Topology	291
Troubleshooting Active Directory	292
<b>Chapter 8 Creating User and Group Accounts</b>	<b>295</b>
The Windows Server Security Model	296
Authentication Protocols	296
Access Controls	297
Claims-Based Access Controls	297
Central Access Policies	299
Differences Between User and Group Accounts	300
User Accounts	301
Group Accounts	302
Default User Accounts and Groups	306
Built-in User Accounts	307
Predefined User Accounts	307

Built-in and Predefined Groups	308
Implicit Groups and Special Identities	309
Account Capabilities .....	309
Privileges	310
Logon Rights	312
Built-in Capabilities for Groups in Active Directory	313
Using Default Group Accounts .....	315
Groups Used by Administrators	316
Implicit Groups and Identities	317
User Account Setup and Organization .....	318
Account Naming Policies	319
Password and Account Policies	320
Configuring Account Policies .....	322
Configuring Password Policies	323
Configuring Account Lockout Policies	325
Configuring Kerberos Policies	326
Configuring User Rights Policies .....	327
Configuring Global User Rights	328
Configuring Local User Rights	330
Adding a User Account .....	330
Creating Domain User Accounts	330
Creating Local User Accounts	334
Adding a Group Account .....	335
Creating a Global Group	336
Creating a Local Group and Assigning Members	337
Handling Global Group Membership .....	338
Managing Individual Membership	339
Managing Multiple Memberships in a Group	340
Setting the Primary Group for Users and Computers	340
Implementing Managed Accounts .....	341
Creating and Using Managed Service Accounts	342
Configuring Services to Use Managed Service Accounts	344
Removing Managed Service Accounts	344

Moving Managed Service Accounts	345
Using Virtual Accounts	346
<b>Chapter 9 Managing User and Group Accounts</b>	<b>347</b>
Managing User Contact Information . . . . .	347
Setting Contact Information	347
Searching for Users and Groups in Active Directory	350
Configuring the User's Environment Settings. . . . .	351
System Environment Variables	352
Logon Scripts	353
Assigning Home Directories	354
Setting Account Options and Restrictions. . . . .	355
Managing Logon Hours	355
Setting Permitted Logon Workstations	357
Setting Dial-in and VPN Privileges	358
Setting Account Security Options	360
Managing User Profiles . . . . .	361
Local, Roaming, and Mandatory Profiles	362
Using the System Utility to Manage Local Profiles	365
Updating User and Group Accounts. . . . .	368
Renaming User and Group Accounts	369
Copying Domain User Accounts	371
Importing and Exporting Accounts	372
Deleting User and Group Accounts	373
Changing and Resetting Passwords	373
Enabling User Accounts	374
Managing Multiple User Accounts . . . . .	375
Setting Profiles for Multiple Accounts	376
Setting Logon Hours for Multiple Accounts	377
Setting Permitted Logon Workstations for Multiple Accounts	378
Setting Logon, Password, and Expiration Properties for Multiple Accounts	378
Troubleshooting Logon Problems. . . . .	378
Viewing and Setting Active Directory Permissions . . . . .	380

<b>Chapter 10   Managing File Systems and Drives</b>	<b>385</b>
Managing the File Services Role . . . . .	385
Adding Hard Disk Drives . . . . .	389
Physical Drives	389
Preparing a Physical Drive for Use	392
Using Disk Management	394
Removable Storage Devices	396
Installing and Checking for a New Drive	398
Understanding Drive Status	399
Working with Basic, Dynamic, and Virtual Disks . . . . .	401
Using Basic and Dynamic Disks	401
Special Considerations for Basic and Dynamic Disks	402
Changing Drive Types	402
Reactivating Dynamic Disks	404
Rescanning Disks	404
Moving a Dynamic Disk to a New System	404
Managing Virtual Hard Disks	405
Using Basic Disks and Partitions . . . . .	406
Partitioning Basics	406
Creating Partitions and Simple Volumes	407
Formatting Partitions	410
Compressing Drives and Data . . . . .	411
Compressing Drives	412
Compressing Directories and Files	412
Expanding Compressed Drives	412
Expanding Compressed Directories and Files	413
Encrypting Drives and Data . . . . .	413
Understanding Encryption and the Encrypting File System	414
Encrypting Directories and Files	415
Working with Encrypted Files and Folders	416
Configuring Recovery Policy	417
Decrypting Files and Directories	418

<b>Chapter 11 Configuring Volumes and RAID Arrays</b>	<b>419</b>
Using Volumes and Volume Sets . . . . .	420
Understanding Volume Basics	420
Understanding Volume Sets	422
Creating Volumes and Volume Sets	424
Deleting Volumes and Volume Sets	426
Managing Volumes	426
Improving Performance and Fault Tolerance with RAID. . . . .	426
Implementing RAID on Windows Server 2012 . . . . .	427
Implementing RAID-0: Disk Striping	427
Implementing RAID-1: Disk Mirroring	428
Implementing RAID-5: Disk Striping with Parity	431
Managing RAID and Recovering from Failures. . . . .	432
Breaking a Mirrored Set	432
Resynchronizing and Repairing a Mirrored Set	432
Repairing a Mirrored System Volume to Enable Boot	433
Removing a Mirrored Set	434
Repairing a Striped Set Without Parity	434
Regenerating a Striped Set with Parity	434
Standards-Based Storage Management . . . . .	435
Getting Started with Standards-Based Storage	435
Working with Standards-Based Storage	436
Creating Storage Pools and Allocating Space	438
Creating a Storage Space	439
Creating a Virtual Disk in a Storage Space	440
Creating a Standard Volume	441
Managing Existing Partitions and Drives . . . . .	443
Assigning Drive Letters and Paths	443
Changing or Deleting the Volume Label	444
Deleting Partitions and Drives	445
Converting a Volume to NTFS	445
Resizing Partitions and Volumes	447
Repairing Disk Errors and Inconsistencies	449
Automatically	449
Analyzing and Optimizing Disks	453

<b>Chapter 12 Data Sharing, Security, and Auditing</b>	<b>457</b>
Using and Enabling File Sharing .....	458
Configuring Standard File Sharing .....	461
Viewing Existing Shares	461
Creating Shared Folders in Computer Management	463
Creating Shared Folders in Server Manager	466
Changing Shared Folder Settings	468
Managing Share Permissions .....	469
Various Share Permissions	469
Viewing and Configuring Share Permissions	470
Managing Existing Shares .....	474
Understanding Special Shares	474
Connecting to Special Shares	475
Viewing User and Computer Sessions	476
Stopping File and Folder Sharing	478
Configuring NFS Sharing .....	479
Using Shadow Copies .....	481
Understanding Shadow Copies	481
Creating Shadow Copies	482
Restoring a Shadow Copy	482
Reverting an Entire Volume to a Previous Shadow Copy	483
Deleting Shadow Copies	483
Disabling Shadow Copies	483
Connecting to Network Drives .....	484
Mapping a Network Drive	484
Disconnecting a Network Drive	485
Object Management, Ownership, and Inheritance .....	485
Objects and Object Managers	485
Object Ownership and Transfer	486
Object Inheritance	487

File and Folder Permissions .....	488
Understanding File and Folder Permissions	489
Setting Basic File and Folder Permissions	491
Setting Special Permissions on Files and Folders	493
Setting Claims-Based Permissions	496
Auditing System Resources .....	498
Setting Auditing Policies	498
Auditing Files and Folders	500
Auditing the Registry	502
Auditing Active Directory Objects	502
Using, Configuring, and Managing NTFS Disk Quotas .....	503
Understanding NTFS Disk Quotas and How NTFS Quotas Are Used	504
Setting NTFS Disk Quota Policies	506
Enabling NTFS Disk Quotas on NTFS Volumes	508
Viewing Disk Quota Entries	510
Creating Disk Quota Entries	510
Deleting Disk Quota Entries	512
Exporting and Importing NTFS Disk Quota Settings	512
Disabling NTFS Disk Quotas	513
Using, Configuring, and Managing Resource Manager Disk Quotas .....	513
Understanding Resource Manager Disk Quotas	514
Managing Disk Quota Templates	515
Creating Resource Manager Disk Quotas	518
<b>Chapter 13 Data Backup and Recovery</b>	<b>519</b>
Creating a Backup and Recovery Plan .....	519
Figuring Out a Backup Plan	519
The Basic Types of Backup	521
Differential and Incremental Backups	522
Selecting Backup Devices and Media	522
Common Backup Solutions	523
Buying and Using Backup Media	524
Selecting a Backup Utility	525

Backing Up Your Data: The Essentials. . . . .	526
Installing the Windows Backup and Recovery Utilities	526
Getting Started with Windows Server Backup	527
Getting Started with the Backup Command-Line Utility	529
Working with Wbadmin Commands	531
Using General-Purpose Commands	531
Using Backup Management Commands	532
Using Recovery Management Commands	533
Performing Server Backups . . . . .	534
Configuring Scheduled Backups	535
Modifying or Stopping Scheduled Backups	538
Creating and Scheduling Backups with Wbadmin	538
Running Manual Backups	540
Recovering Your Server from Hardware or Startup Failure	541
Recovering from a Failed Start	544
Starting a Server in Safe Mode	544
Backing Up and Restoring the System State	546
Restoring Active Directory	547
Restoring the Operating System and the Full System	547
Restoring Applications, Nonsystem Volumes, and Files and Folders	550
Managing Encryption Recovery Policy. . . . .	551
Understanding Encryption Certificates and Recovery Policy	551
Configuring the EFS Recovery Policy	553
Backing Up and Restoring Encrypted Data and Certificates . . .	554
Backing Up Encryption Certificates	554
Restoring Encryption Certificates	555



<b>Chapter 14    Managing TCP/IP Networking</b>	<b>559</b>
Navigating Networking in Windows Server 2012 .....	559
Managing Networking in Windows 8 and Windows Server 2012 .....	562
Installing TCP/IP Networking .....	565
Configuring TCP/IP Networking .....	566
Configuring Static IP Addresses	566
Configuring Dynamic IP Addresses and Alternate IP Addressing	568
Configuring Multiple Gateways	569
Configuring Networking for Hyper-V	570
Managing Network Connections .....	571
Checking the Status, Speed, and Activity for Network Connections	571
Enabling and Disabling Network Connections	572
Renaming Network Connections	572
 <b>Chapter 15    Running DHCP Clients and Servers</b>	 <b>573</b>
Understanding DHCP .....	573
Using Dynamic IPv4 Addressing and Configuration	573
Using Dynamic IPv6 Addressing and Configuration	575
Checking IP Address Assignment	578
Understanding Scopes	578
Installing a DHCP Server .....	579
Installing DHCP Components	579
Starting and Using the DHCP Console	581
Connecting to Remote DHCP Servers	582
Starting and Stopping a DHCP Server	583
Authorizing a DHCP Server in Active Directory	583

Configuring DHCP Servers .....	584
Configuring Server Bindings	584
Updating DHCP Statistics	584
DHCP Auditing and Troubleshooting	585
Integrating DHCP and DNS	586
Integrating DHCP and NAP	588
Avoiding IP Address Conflicts	591
Saving and Restoring the DHCP Configuration	591
Managing DHCP Scopes .....	592
Creating and Managing Superscopes	592
Creating and Managing Scopes	593
Creating and Managing Failover Scopes	602
Managing the Address Pool, Leases, and Reservations. ....	605
Viewing Scope Statistics	605
Enabling and Configuring MAC Address Filtering	606
Setting a New Exclusion Range	607
Reserving DHCP Addresses	608
Modifying Reservation Properties	609
Deleting Leases and Reservations	610
Backing Up and Restoring the DHCP Database .....	610
Backing Up the DHCP Database	610
Restoring the DHCP Database from Backup	611
Using Backup and Restore to Move the DHCP Database to a New Server	611
Forcing the DHCP Server Service to Regenerate the DHCP Database	612
Reconciling Leases and Reservations	612

<b>Chapter 16 Optimizing DNS</b>	<b>615</b>
Understanding DNS . . . . .	615
Integrating Active Directory and DNS	616
Enabling DNS on the Network	617
Configuring Name Resolution on DNS Clients . . . . .	620
Installing DNS Servers . . . . .	621
Installing and Configuring the DNS Server Service	622
Configuring a Primary DNS Server	624
Configuring a Secondary DNS Server	627
Configuring Reverse Lookups	628
Configuring Global Names	629
Managing DNS Servers . . . . .	631
Adding and Removing Servers to Manage	631
Starting and Stopping a DNS Server	632
Using DNSSEC and Signing Zones	632
Creating Child Domains Within Zones	634
Creating Child Domains in Separate Zones	635
Deleting a Domain or Subnet	636
Managing DNS Records . . . . .	636
Adding Address and Pointer Records	637
Adding DNS Aliases with CNAME	638
Adding Mail Exchange Servers	638
Adding Name Servers	639
Viewing and Updating DNS Records	640
Updating Zone Properties and the SOA Record. . . . .	641
Modifying the SOA Record	641
Allowing and Restricting Zone Transfers	643
Notifying Secondaries of Changes	644
Setting the Zone Type	645
Enabling and Disabling Dynamic Updates	645

Managing DNS Server Configuration and Security . . . . .	645
Enabling and Disabling IP Addresses for a DNS Server	646
Controlling Access to DNS Servers Outside the Organization	646
Enabling and Disabling Event Logging	648
Using Debug Logging to Track DNS Activity	648
Monitoring a DNS Server	649
<i>Index</i>	651

---

**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](https://microsoft.com/learning/booksurvey)

# Introduction

---

Welcome to *Windows Server 2012 Pocket Consultant*. Over the years, I've written about many different server technologies and products, but the one product I like writing about the most is Microsoft Windows Server. For anyone transitioning to Windows Server 2012 from an earlier release of Windows Server, I'll let you know right up front that I believe this is the most significant update to Windows Server since the introduction of Windows 2000 Server. While the extensive UI changes are a key part of the revisions to the operating system, the deeper changes are below the surface, in the underlying architecture.

The good news is Windows Server 2012 builds off the same code base as Microsoft Windows 8. This means that you can apply much of what you know about Windows 8 to Windows Server 2012, including how Windows works with touch-based user interfaces. Although you might not install Windows Server 2012 on touch UI-capable computers, you can manage Windows Server 2012 from your touch UI-capable computers. If you do end up managing it this way, understanding the touch UI as well as the revised interface options will be crucial to your success. For this reason, I discuss both the touch UI and the traditional mouse and keyboard techniques throughout this book.

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

- **Tap** Tap an item by touching it with your finger. A tap or double-tap of elements on the screen generally is the equivalent of a mouse click or double-click.
- **Press and hold** Press your finger down and leave it there for a few seconds. Pressing and holding elements on the screen generally is the equivalent of a right-click.
- **Swipe to select** Slide an item a short distance in the opposite direction compared to how the page scrolls. This selects the items and also might bring up related commands. If pressing and holding doesn't display commands and options for an item, try using swipe to select instead.
- **Swipe from edge (slide in from edge)** Starting from the edge of the screen, swipe or slide in. Sliding in from the right edge opens the Charms panel. Sliding in from the left edge shows open apps and allows you to easily switch between them. Sliding in from the top or bottom edge shows commands for the active element.
- **Pinch** Touch an item with two or more fingers and then move the fingers toward each other. Pinching zooms in or shows less information.
- **Stretch** Touch an item with two or more fingers and then move the fingers away from each other. Stretching zooms out or shows more information.

Because I've written many top-selling Windows Server books, I was able to bring a unique perspective to this book—the kind of perspective you gain only after working with technologies for many years. Long before there was a product called Windows Server 2012, I was working with the beta product. From these early beginnings, the final version of Windows Server 2012 evolved until it became the finished product that is available today.

As you've probably noticed, a great deal of information about Windows Server 2012 is available on the web and in other printed books. You can find tutorials, reference sites, discussion groups, and more to make using Windows Server 2012 easier. However, the advantage of reading this book is that much of the information you need to learn about Windows Server 2012 is organized in one place and presented in a straightforward and orderly fashion. This book has everything you need to customize Windows Server 2012 installations, master Windows Server 2012 configurations, and maintain Windows Server 2012 servers.

In this book, I teach you how features work, why they work the way they do, and how to customize them to meet your needs. I also offer specific examples of how certain features can meet your needs, and how you can use other features to troubleshoot and resolve issues you might have. In addition, this book provides tips, best practices, and examples of how to optimize Windows Server 2012. This book won't just teach you how to configure Windows Server 2012, it will teach you how to squeeze every last bit of power out of it and make the most of the features and options it includes.

Unlike many other books about administering Windows Server 2012, this book doesn't focus on a specific user level. This isn't a lightweight beginner book. Regardless of whether you are a beginning administrator or a seasoned professional, many of the concepts in this book will be valuable to you, and you can apply them to your Windows Server 2012 installations.

## Who Is This Book For?

---

*Windows Server 2012 Pocket Consultant* covers all editions of Windows Server 2012. The book is designed for the following readers:

- Current Windows system administrators
- Accomplished users who have some administrator responsibilities
- Administrators upgrading to Windows Server 2012 from previous versions
- Administrators transferring from other platforms

To pack in as much information as possible, I had to assume that you have basic networking skills and a basic understanding of Windows Server. With this in mind, I don't devote entire chapters to explaining Windows Server architecture, Windows Server startup and shutdown, or why you want to use Windows Server. I do, however, cover Windows server configuration, Group Policy, security, auditing, data backup, system recovery, and much more.

I also assume that you are fairly familiar with Windows commands and procedures as well as the Windows user interface. If you need help learning Windows basics, you should read other resources (many of which are available from Microsoft Press).

## How This Book Is Organized

---

Rome wasn't built in a day, and this book wasn't intended to be read in a day, in a week, or even in a month. Ideally, you'll read this book at your own pace, a little each day as you work your way through all the features Windows Server 2012 has to offer. This book is organized into 16 chapters. The chapters are arranged in a logical order, taking you from planning and deployment tasks to configuration and maintenance tasks.

Ease of reference is an essential part of this hands-on guide. This book has an expanded table of contents and an extensive index for finding answers to problems quickly. Many other quick-reference features have been added to the book as well, including quick step-by-step procedures, lists, tables with fast facts, and extensive cross references.

As with all Pocket Consultants, *Windows Server 2012 Pocket Consultant* is designed to be a concise and easy-to-use resource for managing Windows servers. This is the readable resource guide that you'll want on your desktop at all times. The book covers everything you need to perform the core administrative tasks for Windows servers. Because the focus is on giving you maximum value in a pocket-size guide, you don't have to wade through hundreds of pages of extraneous information to find what you're looking for. Instead, you'll find exactly what you need to get the job done, and you'll find it quickly.

In short, the book is designed to be the one resource you turn to whenever you have questions regarding Windows Server administration. To this end, the book zeroes in on daily administration procedures, frequently performed tasks, documented examples, and options that are representative while not necessarily inclusive. One of my goals is to keep the content so concise that the book remains compact and easy to navigate while at the same time ensuring that it is packed with as much information as possible.

## Conventions Used in This Book

---

I've used a variety of elements to help keep the text clear and easy to follow. You'll find code listings in monospace type. When I tell you to actually type a command, the command appears in **bold** type. When I introduce and define a new term or use a code term in a paragraph of text, I put it in *italics*.

**NOTE** Group Policy now includes both policies and preferences. Under the Computer Configuration and User Configuration nodes, you find two nodes: Policies and Preferences. Settings for general policies are listed under the Policies node. Settings for general preferences are listed under the Preferences node. When referencing settings under the Policies node, I sometimes use shortcut references, such as User Configuration\Administrative Templates\Windows Components, or specify that the policies are found in the Administrative Templates for User Configuration under Windows Components. Both references tell you that the policy setting being discussed is under User Configuration rather than Computer Configuration and can be found under Administrative Templates\Windows Components.

Other conventions include the following:

- **Best Practices** To examine the best technique to use when working with advanced configuration and maintenance concepts
- **Caution** To warn you about potential problems you should look out for
- **More Info** To provide more information on a subject
- **Note** To provide additional details on a particular point that needs emphasis
- **Real World** To provide real-world advice when discussing advanced topics
- **Security Alert** To point out important security issues
- **Tip** To offer helpful hints or additional information

I truly hope you find that *Windows Server 2012 Pocket Consultant* provides everything you need to perform the essential administrative tasks on Windows servers as quickly and efficiently as possible. You are welcome to send your thoughts to me at [williamstanek@aol.com](mailto:williamstanek@aol.com). Follow me on Twitter at WilliamStanek and on Facebook at [www.facebook.com/William.Stanek.Author](http://www.facebook.com/William.Stanek.Author).

## Other Resources

---

No single magic bullet for learning everything you'll ever need to know about Windows Server 2012 exists. While some books are offered as all-in-one guides, there's simply no way one book can do it all. With this in mind, I hope you use this book as it is intended to be used—as a concise and easy-to-use resource. It covers everything you need to perform core administration tasks for Windows servers, but it is by no means exhaustive.

Your current knowledge will largely determine your success with this or any other Windows resource or book. As you encounter new topics, take the time to practice what you've learned and read about. Seek out further information as necessary to get the practical hands-on know-how and knowledge you need.

I recommend that you regularly visit the Microsoft website for Windows Server ([microsoft.com/windowsserver/](http://microsoft.com/windowsserver/)) and [support.microsoft.com](http://support.microsoft.com) to stay current with the latest changes. To help you get the most out of this book, you can visit my corresponding website at [williamstanek.com/windows](http://williamstanek.com/windows). This site contains information about Windows Server 2012 and updates to the book.



## Errata & Book Support

---

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

*<http://www.microsoftpressstore.com/title/9780735666337>*

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

If you need additional support, email Microsoft Press Book Support at:

*[mspinput@microsoft.com](mailto:mspinput@microsoft.com).*

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

## We Want to Hear from You

---

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

*<http://www.microsoft.com/learning/booksurvey>*

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

## Stay in Touch

---

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



**PART I**

# Windows Server 2012 Administration Fundamentals

- CHAPTER 1** Windows Server 2012 Administration  
Overview **3**
- CHAPTER 2** Managing Servers Running Windows Server  
2012 **31**
- CHAPTER 3** Monitoring Processes, Services, and  
Events **87**
- CHAPTER 4** Automating Administrative Tasks, Policies, and  
Procedures **135**
- CHAPTER 5** Enhancing Computer Security **191**



# Windows Server 2012

## Administration Overview

- Windows Server 2012 and Windows 8 **4**
- Getting to Know Windows Server 2012 **6**
- Power Management Options **8**
- Networking Tools and Protocols **11**
- Domain Controllers, Member Servers, and Domain Services **14**
- Name-Resolution Services **17**
- Frequently Used Tools **23**

Microsoft Windows Server 2012 is a powerful, versatile, full-featured server operating system that builds on the enhancements that Microsoft provided in Windows Server 2008 Release 2. Windows Server 2012 and Windows 8 share a number of common features because they were part of a single development project. These features share a common code base and extend across many areas of the operating systems, including management, security, networking, and storage. Because of this, you can apply much of what you know about Windows 8 to Windows Server 2012.

This chapter covers getting started with Windows Server 2012 and explores the extent to which the architectural changes affect how you work with and manage Windows Server 2012. Throughout this chapter and the other chapters of this book, you'll also find discussions of the many security features and enhancements. These discussions explore all aspects of computer security, including physical security, information security, and network security. Although this book focuses on Windows Server 2012 administration, the tips and techniques it presents can help anyone who supports, develops for, or works with the Windows Server 2012 operating system.

## Windows Server 2012 and Windows 8

---

Before you deploy Windows Server 2012, you should carefully plan the server architecture. As part of your implementation planning, you need to look closely at the software configuration that will be used and modify the hardware configuration on a per-server basis to meet related requirements. For additional flexibility in server deployments, you can deploy servers using one of three installation types:

- **Server With A GUI installation** An installation option that provides full functionality—also referred to as a *full-server installation*. You can configure a server to have any allowed combination of roles, role services, and features, and a full user interface is provided for managing the server. This installation option provides the most dynamic solution and is recommended for deployments of Windows Server 2012 in which the server role might change over time.
- **Server Core installation** A minimal installation option that provides a fixed subset of roles but does not include the Server Graphical Shell, Microsoft Management Console, or Desktop Experience. You can configure a Server Core installation with a limited set of roles. A limited user interface is provided for managing the server, and most management is done locally at a command prompt or remotely using management tools. This installation option is ideally suited to situations in which you want to dedicate servers to a specific server role or combination of roles. Because additional functionality is not installed, the overhead caused by other services is reduced, providing more resources for the dedicated role or roles.
- **Server With Minimal Interface installation** An intermediate installation option where you perform a full-server installation and then remove the Server Graphical Shell. This leaves a minimal user interface, Microsoft Management Console, Server Manager, and a subset of Control Panel for local management. This installation option is ideally suited to situations in which you want to carefully control the tasks that can be performed on a server, as well as the roles and features installed, but still want the convenience of the graphical interface.

You choose the installation type during installation of the operating system. In a significant change from earlier releases of Windows Server, you can change the installation type once you've installed a server. A key difference between the installation types relates to the presence of the graphical management tools and the graphical shell. A Server Core installation has neither; a full-server installation has both; and a minimal-interface installation has only the graphical management tools.

**MORE INFO** Several server features and roles require the graphical shell. They include Fax Server, Remote Desktop Session Host, Windows Deployment Services, and the Internet Printing user interface. Additionally, in Event Viewer, the Details view requires the graphical shell, as does the graphical interface for Windows Firewall.

Like Windows 8, Windows Server 2012 has the following features:

- **Modularization for language independence and disk imaging for hardware independence** Each component of the operating system is designed as an independent module you can easily add or remove. This functionality provides the basis for the configuration architecture in Windows Server 2012. Microsoft distributes Windows Server 2012 on media with Windows Imaging Format (WIM) disk images that use compression and single-instance storage to dramatically reduce the size of image files.
- **Preinstallation and preboot environments** The Windows Preinstallation Environment 4.0 (Windows PE 4.0) replaces MS-DOS as the preinstallation environment and provides a bootable startup environment for installation, deployment, recovery, and troubleshooting. The Windows Preboot Environment provides a startup environment with a boot manager that lets you choose which boot application to run to load the operating system. On systems with multiple operating systems, you access pre-Windows 7 operating systems in the boot environment by using the legacy operating system entry.
- **User account controls and elevation of privileges** User Account Control (UAC) enhances computer security by ensuring true separation of standard user and administrator user accounts. Through UAC, all applications run using either standard user or administrator user privileges, and you see a security prompt by default whenever you run an application that requires administrator privileges. The way the security prompt works depends on Group Policy settings. Additionally, if you log on using the built-in Administrator account, you typically do not see elevation prompts.

In Windows 8 and Windows Server 2012, features with common code bases have identical management interfaces. In fact, just about every Control Panel utility that is available in Windows Server 2012 is identical to or nearly identical to its Windows 8 counterpart. Of course, exceptions exist in some cases for standard default settings. Because Windows Server 2012 does not use performance ratings, Windows servers do not have Windows Experience Index scores. Because Windows Server 2012 does not use Sleep or related states, Windows servers do not have sleep, hibernate, or resume functionality. Because you typically do not want to use extended power management options on Windows servers, Windows Server 2012 has a limited set of power options.

Windows Server 2012 does not include the Windows Aero enhancements, Windows Sidebar, Windows Gadgets, or other user-interface enhancements because Windows Server 2012 is designed to provide optimal performance for server-related tasks and is not designed for extensive personalization of the desktop appearance. That said, when you are working with a full-server installation, you can add the Desktop Experience feature and then enable some Windows 8 features on your server.

The Desktop Experience provides Windows desktop functionality on the server. Windows features added include Windows Media Player, desktop themes, Video for Windows (AVI support), Windows Defender, Disk Cleanup, Sync Center, Sound

Recorder, Character Map, and Snipping Tool. Although these features allow a server to be used like a desktop computer, they can reduce the server's overall performance.

Because the common features of Windows 8 and Windows Server 2012 have so many similarities, I will not cover changes in the interface from previous operating system releases, discuss how UAC works, and so on. You can find extensive coverage of these features in *Windows 8 Administration Pocket Consultant* (Microsoft Press, 2012), which I encourage you to use in conjunction with this book. In addition to its coverage of broad administration tasks, *Windows 8 Administration Pocket Consultant* examines how to customize the operating system and Windows environment, configure hardware and network devices, manage user access and global settings, configure laptops and mobile networking, use remote management and remote assistance capabilities, troubleshoot system problems, and much more. This book, on the other hand, zeroes in on directory services administration, data administration, and network administration.

## Getting to Know Windows Server 2012

---

The Windows Server 2012 operating system includes several different editions. All Windows Server 2012 editions support multiple processor cores. It is important to point out that although an edition might support only one discrete-socketed processor (also referred to as a *physical processor*), that one processor could have eight processor cores (also referred to as *logical processors*).

Windows Server 2012 is a 64-bit-only operating system. In this book, I refer to 64-bit systems designed for the x64 architecture as *64-bit* systems. Because the various server editions support the same core features and administration tools, you can use the techniques discussed in this book regardless of which Windows Server 2012 edition you're using.

When you install a Windows Server 2012 system, you configure the system according to its role on the network, as the following guidelines describe:

- Servers are generally assigned to be part of a workgroup or a domain.
- Workgroups are loose associations of computers in which each individual computer is managed separately.
- Domains are collections of computers you can manage collectively by means of domain controllers, which are Windows Server 2012 systems that manage access to the network, to the directory database, and to shared resources.

**NOTE** In this book, *Windows Server 2012* and *Windows Server 2012 family* refer to all editions of Windows Server 2012. The various server editions support the same core features and administration tools.

Unlike Windows Server 2008, Windows Server 2012 uses a Start screen. Start is a window, not a menu. Programs can have tiles on the Start screen. Tapping or clicking a tile runs the program. When you press and hold or right-click on a program, an options panel normally is displayed. The charms bar is an options panel for Start, Desktop, and PC Settings. With a touch UI, you can display the charms by sliding in



from the right side of the screen. With a mouse and keyboard, you can display the charms by moving the mouse pointer over the hidden button in the upper-right or lower-right corner of the Start, Desktop, or PC Settings screen; or by pressing Windows key+C.

Tap or click the Search charm to display the Search panel. Any text typed while on the Start screen is entered into the Search box in the Search panel. The Search box can be focused on Apps, Settings, or Files. When focused on Apps, you can use Search to quickly find installed programs. When focused on Settings, you can use Search to quickly find settings and options in Control Panel. When focused on Files, you can use Search to quickly find files.

One way to quickly open a program is by pressing the Windows key, typing the file name of the program, and then pressing Enter. This shortcut works as long as the Apps Search box is in focus (which it typically is by default).

Pressing the Windows key toggles between the Start screen and the desktop (or, if you are working with PC Settings, between Start and PC Settings). On Start, there's a Desktop tile that you can tap or click to display the desktop. You also can display the desktop by pressing Windows key+D or, to peek at the desktop, press and hold Windows key+Comma. From Start, you access Control Panel by tapping or clicking the Control Panel tile. From the desktop, you can display Control Panel by accessing the charms, tapping or clicking Settings, and then tapping or clicking Control Panel. Additionally, because File Explorer is pinned to the desktop taskbar by default you typically can access Control Panel on the desktop by following these steps:

1. Open File Explorer by tapping or clicking the taskbar icon.
2. Tap or click the leftmost option button (down arrow) in the address list.
3. Tap or click Control Panel.

Start and Desktop have a handy menu that you can display by pressing and holding or right-clicking the lower-left corner of the Start screen or the desktop. Options on the menu include Command Prompt, Command Prompt (Admin), Device Manager, Event Viewer, System, and Task Manager. On Start, the hidden button in the lower-left corner shows a thumbnail view of the desktop when activated, and tapping or clicking the thumbnail opens the desktop. On the desktop, the hidden button in the lower-left corner shows a thumbnail view of Start when activated and tapping or clicking the thumbnail opens Start. Pressing and holding or right-clicking the thumbnail is what displays the shortcut menu.

Shutdown and Restart are options of Power settings now. This means to shut down or restart a server, you follow these steps:

1. Display Start options by sliding in from the right side of the screen or moving the mouse pointer to the bottom right or upper right corner of the screen.
2. Tap or click Settings and then tap or click Power.
3. Tap or click Shut Down or Restart as appropriate.

Alternatively, press the server's physical power button to initiate an orderly shutdown by logging off and then shutting down. If you are using a desktop-class system and the computer has a sleep button, the sleep button is disabled by default,

as are closing the lid options for portable computers. Additionally, servers are configured to turn off the display after 10 minutes of inactivity.

Windows 8 and Windows Server 2012 support the Advanced Configuration and Power Interface (ACPI) 5.0 specification. Windows uses ACPI to control system and device power state transitions, putting devices in and out of full-power (working), low-power, and off states to reduce power consumption.

The power settings for a computer come from the active power plan. You can access power plans in Control Panel by tapping or clicking System And Security and then tapping or clicking Power Options. Windows Server 2012 includes the Power Configuration (Powercfg.exe) utility for managing power options from the command line. At a command prompt, you can view the configured power plans by typing **powercfg /l**. The active power plan is marked with an asterisk.

The default, active power plan in Windows Server 2012 is called Balanced. The Balanced plan is configured to do the following:

- Never turn off hard disks (as opposed to turning off hard disks after a specified amount of idle time)
- Disable timed events to wake the computer (as opposed to enabling wake on timed events)
- Enable USB selective suspend (as opposed to disabling selective suspend)
- Use moderate power savings for idle PCI Express links (as opposed to maximum power savings being on or off)
- Use active system cooling by increasing the fan speed before slowing processors (as opposed to using passive system cooling to slow the processors before increasing fan speed)
- Use minimum processor and maximum processor states if supported (as opposed to using a fixed state)

**NOTE** Power consumption is an important issue, especially as organizations try to become more earth friendly. Saving power also can save your organization money and, in some cases, allow you to install more servers in your data centers. If you install Windows Server 2012 on a laptop—for testing or for your personal computer, for example—your power settings will be slightly different, and you'll also have settings for when the laptop is running on battery.

## Power Management Options

---

When working with power management, important characteristics to focus on include the following:

- Cooling modes
- Device states
- Processor states

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

- Passive cooling reduces system performance but is quieter because there's less fan noise. With passive cooling, Windows lessens power consumption to

reduce the operating temperature of the computer but at the cost of system performance. Here, Windows reduces the processor speed in an attempt to cool the computer before increasing fan speed, which would increase power consumption.

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

Power policy includes an upper and lower limit for the processor state, referred to as the *maximum processor state* and the *minimum processor state*, respectively. These states are implemented by making use of a feature of ACPI 3.0 and later versions called processor throttling, and they determine the range of currently available processor performance states that Windows can use. By setting the maximum and minimum values, you define the bounds for the allowed performance states, or you can use the same value for each to force the system to remain in a specific performance state. Windows reduces power consumption by throttling the processor speed. For example, if the upper bound is 100 percent and the lower bound is 5 percent, Windows can throttle the processor within this range as workloads permit to reduce power consumption. In a computer with a 3-GHz processor, Windows would adjust the operating frequency of the processor between .15 GHz and 3.0 GHz.

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

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

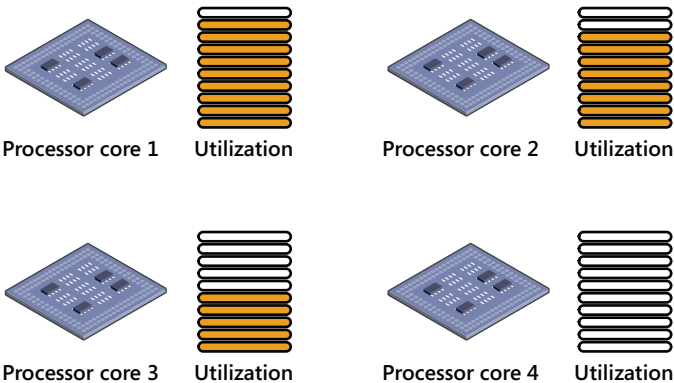
ACPI defines processor performance states, referred to as *p-states*, and processor idle sleep states, referred to as *c-states*. Processor performance states include P0 (the processor/core uses its maximum performance capability and can consume maximum power), P1 (the processor/core is limited below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

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

**MORE INFO** ACPI 4.0 was finalized in June 2009 and ACPI 5.0 was finalized in December 2011. Computers manufactured prior to this time will likely not have firmware that is fully compliant, and you will probably need to update the firmware when a compatible revision becomes available. In some cases, and especially with older hardware, you might not be able to update a computer's firmware to make it fully compliant with ACPI 4.0 or ACPI 5.0. For example, if you are configuring the power options and you don't have minimum and maximum processor state options, the computer's firmware isn't fully compatible with ACPI 3.0 and likely will not fully support ACPI 4.0 or ACPI 5.0 either. Still, you should check the hardware manufacturer's website for firmware updates.

Windows switches processors/cores between any p-state and from the C1 state to the C0 state nearly instantaneously (fractions of milliseconds) and tends not to use the deep sleep states, so you don't need to worry about performance impact to throttle or wake up processors/cores. The processors/cores are available when they are needed. That said, the easiest way to limit processor power management is to modify the active power plan and set the minimum and maximum processor states to 100 percent. Logical processor idling is used to reduce power consumption by removing a logical processor from the operating system's list of nonprocessor-affinitized work. However, because processor-affinitized work reduces the effectiveness of this feature, you'll want to plan carefully prior to configuring processing affinity settings for applications. Windows System Resource Manager allows you to manage processor resources through percent processor usage targets and processor affinity rules. Both techniques reduce the effectiveness of logical processor idling.

Windows saves power by putting processor cores in and out of appropriate p-states and c-states. On a computer with four logical processors, Windows might use p-states 0 to 5, where P0 allows 100 percent usage, P1 allows 90 percent usage, P2 allows 80 percent usage, P3 allows 70 percent usage, P4 allows 60 percent usage, and P5 allows 50 percent usage. When the computer is active, logical processor 0 would likely be active with a p-state of 0 to 5, and the other processors would likely be at an appropriate p-state or in a sleep state. Figure 1-1 shows an example. Here, logical processor 1 is running at 90 percent, logical processor 2 is running at 80 percent, logical processor 3 is running at 50 percent, and logical processor 4 is in the sleep state.



**FIGURE 1-1** Understanding processor states

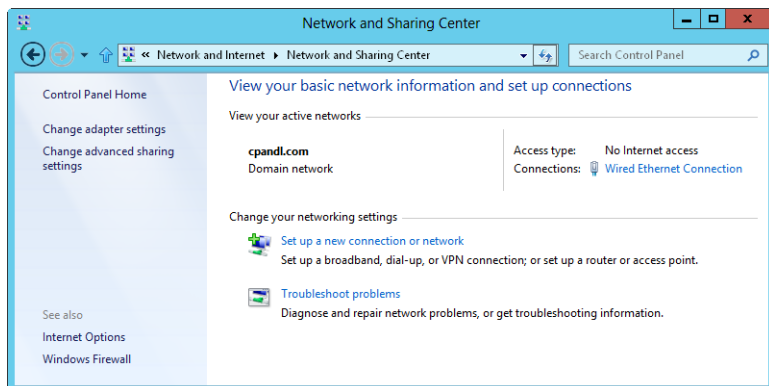
**REAL WORLD** ACPI 4.0 and ACPI 5.0 define four global power states. In G0, the working state in which software runs, power consumption is at its highest and latency is at its lowest. In G1, the sleeping state, in which software doesn't run, latency varies with sleep state and power consumption is less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

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

Devices have power states as well. D0, the fully on state, consumes the highest level of power. D1 and D2 are intermediate states that many devices do not use. D3hot is a power-saving state, where the device is software enumerable and can optionally preserve device context. D3 is the off state, where the device context is lost and the operating system must reinitialize the device to turn it back on.

## Networking Tools and Protocols

Windows Server 2012 has a suite of networking tools that includes Network Explorer, Network And Sharing Center, and Network Diagnostics. Figure 1-2 shows Network And Sharing Center.



**FIGURE 1-2** Network And Sharing Center provides quick access to sharing, discovery, and networking options.

## Understanding Networking Options

The sharing and discovery configuration in Network And Sharing Center controls basic network settings. When network discovery settings are turned on and a server is connected to a network, the server can see other network computers and devices and is visible on the network. When sharing settings are turned on or off, the various sharing options are allowed or restricted. As discussed in Chapter 12, “Data Sharing, Security, and Auditing,” sharing options include file sharing, public folder sharing, printer sharing, and password-protected sharing.

In Windows 8 and Windows Server 2012, networks are identified as one of the following network types:

- **Domain** A network in which computers are connected to the corporate domain to which they are joined.
- **Work** A private network in which computers are configured as members of a workgroup and are not connected directly to the public Internet.
- **Home** A private network in which computers are configured as members of a homegroup and are not connected directly to the public Internet.
- **Public** A public network in which computers are connected to a network in a public place, such as a coffee shop or an airport, rather than an internal network.

These network types are organized into three categories: home or work, domain, and public. Each network category has an associated network profile. Because a computer saves sharing and firewall settings separately for each network category, you can use different block and allow settings for each network category. When you connect to a network, you see a dialog box that allows you to specify the network category. If you select Private, and the computer determines that it is connected to the corporate domain to which it is joined, the network category is set as Domain Network.

Based on the network category, Windows Server configures settings that turn discovery on or off. The On (enabled) state means that the computer can discover other computers and devices on the network and that other computers on the network can discover the computer. The Off (disabled) state means that the computer cannot discover other computers and devices on the network and that other computers on the network cannot discover the computer.

Using either the Network window or Advanced Sharing Settings in Network And Sharing Center, you can enable discovery and file sharing. However, discovery and file sharing are blocked by default on a public network, which enhances security by preventing computers on the public network from discovering other computers and devices on that network. When discovery and file sharing are disabled, files and printers you have shared from a computer cannot be accessed from the network. Additionally, some programs might not be able to access the network.

## Working with Networking Protocols

To allow a server to access a network, you must install TCP/IP networking and a network adapter. Windows Server uses TCP/IP as the default wide area network

(WAN) protocol. Normally, networking is installed during installation of the operating system. You can also install TCP/IP networking through local area connection properties.

The TCP and IP protocols make it possible for computers to communicate across various networks and the Internet by using network adapters. Windows 7 and later releases of Windows have a dual IP-layer architecture in which both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) are implemented and share common transport and network layers. IPv4 has 32-bit addresses and is the primary version of IP used on most networks, including the Internet. IPv6, on the other hand, has 128-bit addresses and is the next-generation version of IP.

**NOTE** DirectAccess clients only send IPv6 traffic across the DirectAccess connection to the DirectAccess server. Thanks to the NAT64/DNS64 support on a Windows Server 2012 DirectAccess server, DirectAccess clients can now initiate communications with IPv4-only hosts on the corporate intranet. NAT64/DNS64 work together to translate incoming connection traffic from an IPv6 node to IPv4 traffic. The NAT64 translates the incoming IPv6 traffic to IPv4 traffic and performs the reverse translation for response traffic. The DNS64 resolves the name of an IPv4-only host to a translated IPv6 address.

**REAL WORLD** The TCP Chimney Offload feature was introduced with Windows Vista and Windows Server 2008. This feature enables the networking subsystem to offload the processing of a TCP/IP connection from the computer's processors to its network adapter as long as the network adapter supports TCP/IP offload processing. Both TCP/IPv4 connections and TCP/IPv6 connections can be offloaded. For Windows 7 and later releases of Windows, TCP connections are offloaded by default on 10 gigabits per second (Gbps) network adapters, but they are not offloaded by default on 1-Gbps network adapters. To offload TCP connections on a 1 or 10 Gbps network adapter, you must enable TCP offloading by entering the following command at an elevated, administrator command prompt: **netsh int tcp set global chimney=enabled**. You can check the status of TCP offloading by entering **netsh int tcp show global**. Although TCP offloading works with Windows Firewall, TCP offloading won't be used with IPsec, Windows virtualization (Hyper-V), network load balancing, or the Network Address Translation (NAT) service. To determine whether TCP offloading is working, enter **netstat-t** and check the offload state. The offload state is listed as *offloaded* or *inhost*. Windows also uses receive-side scaling (RSS) and network direct memory access (NetDMA). You can enable or disable RSS by entering **netsh int tcp set global rss=enabled** or **netsh int tcp set global rss=disabled**, respectively. To check the status of RSS, enter **netsh int tcp show global**. You can enable or disable NetDMA by setting a DWord value under the EnableTCPA registry entry to 1 or 0, respectively. This registry entry is found under HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters.

IPv4's 32-bit addresses are commonly expressed as four separate decimal values, such as 127.0.0.1 or 192.168.10.52. The four decimal values are referred to as *octets* because each represents 8 bits of the 32-bit number. With standard unicast IPv4 addresses, a variable part of the IP address represents the network ID and a variable part of the IP address represents the host ID. A host's IPv4 address and the internal machine (MAC) address used by the host's network adapter have no correlation.

IPv6's 128-bit addresses are divided into eight 16-bit blocks delimited by colons. Each 16-bit block is expressed in hexadecimal form, such as FEC0:0:0:02BC:FF:BECB:FE4F:961D. With standard unicast IPv6 addresses, the first 64 bits represent the network ID and the last 64 bits represent the network interface. Because many IPv6 address blocks are set to 0, a contiguous set of 0 blocks can be expressed as "::", a notation referred to as *double-colon notation*. Using double-colon notation, the two 0 blocks in the previous address can be compressed as FEC0::02BC:FF:BECB:FE4F:961D. Three or more 0 blocks would be compressed in the same way. For example, FFE8:0:0:0:0:0:1 becomes FFE8::1.

When networking hardware is detected during installation of the operating system, both IPv4 and IPv6 are enabled by default; you don't need to install a separate component to enable support for IPv6. The modified IP architecture in Windows 7 and later releases of Windows is referred to as the *Next Generation TCP/IP stack*, and it includes many enhancements that improve the way IPv4 and IPv6 are used.

## Domain Controllers, Member Servers, and Domain Services

---

When you install Windows Server 2012 on a new system, you can configure the server to be a member server, a domain controller, or a standalone server. The differences between these types of servers are extremely important. Member servers are part of a domain but don't store directory information. Domain controllers are distinguished from member servers because they store directory information and provide authentication and directory services for the domain. Standalone servers aren't part of a domain. Because standalone servers have their own user databases, they authenticate logon requests independently.

## Working with Active Directory

Windows Server 2012 supports a multimaster replication model. In this model, any domain controller can process directory changes and then replicate those changes to other domain controllers automatically. Windows Server distributes an entire directory of information, called a *data store*. Inside the data store are sets of objects representing user, group, and computer accounts as well as shared resources such as servers, files, and printers.

Domains that use Active Directory are referred to as *Active Directory domains*. Although Active Directory domains can function with only one domain controller, you can and should configure multiple domain controllers in the domain. This way, if one domain controller fails, you can rely on the other domain controllers to handle authentication and other critical tasks.

Microsoft changed Active Directory in several fundamental ways for the original release of Windows Server 2008. As a result, Microsoft realigned the directory functionality and created a family of related services, including the following:

- **Active Directory Certificate Services (AD CS)** AD CS provides functions necessary for issuing and revoking digital certificates for users, client



computers, and servers. AD CS uses certificate authorities (CAs), which are responsible for confirming the identity of users and computers and then issuing certificates to confirm these identities. Domains have enterprise root CAs, which are the certificate servers at the root of certificate hierarchies for domains and the most trusted certificate servers in the enterprise, and subordinate CAs, which are members of a particular enterprise certificate hierarchy. Workgroups have standalone root CAs, which are the certificate servers at the root of nonenterprise certificate hierarchies, and standalone subordinate CAs, which are members of a particular nonenterprise certificate hierarchy.

- **Active Directory Domain Services (AD DS)** AD DS provides the essential directory services necessary for establishing a domain, including the data store that stores information about objects on the network and makes that information available to users. AD DS uses domain controllers to manage access to network resources. Once users authenticate themselves by logging on to a domain, their stored credentials can be used to access resources on the network. Because AD DS is the heart of Active Directory and is required for directory-enabled applications and technologies, I typically refer to it simply as Active Directory rather than Active Directory Domain Services or AD DS.
- **Active Directory Federation Services (AD FS)** AD FS complements the authentication and access-management features of AD DS by extending them to the World Wide Web. AD FS uses web agents to provide users with access to internally hosted web applications and proxies to manage client access. Once AD FS is configured, users can use their digital identities to authenticate themselves over the Web and access internally hosted web applications with a web browser such as Internet Explorer.
- **Active Directory Lightweight Directory Services (AD LDS)** AD LDS provides a data store for directory-enabled applications that do not require AD DS and do not need to be deployed on domain controllers. AD LDS does not run as an operating system service and can be used in both domain and workgroup environments. Each application that runs on a server can have its own data store implemented through AD LDS.
- **Active Directory Rights Management Services (AD RMS)** AD RMS provides a layer of protection for an organization's information that can extend beyond the enterprise, allowing email messages, documents, intranet web pages, and more to be protected from unauthorized access. AD RMS uses a certificate service to issue rights account certificates that identify trusted users, groups, and services; a licensing service that provides authorized users, groups, and services with access to protected information; and a logging service to monitor and maintain the rights management service. Once trust has been established, users with a rights account certificate can assign rights to information. These rights control which users can access the information and what they can do with it. Users with rights account certificates can also access protected content to which they've been granted access. Encryption ensures that access to protected information is controlled both inside and outside the enterprise.

Microsoft introduced additional changes in Windows Server 2012. These changes include a new domain functional level, called *Windows Server 2012 domain functional level*, and a new forest functional level, called *Windows Server 2012 forest functional level*. The many other changes are discussed in Chapter 6, “Using Active Directory.”

## Using Read-Only Domain Controllers

Windows Server 2008 and later releases support read-only domain controllers and Restartable Active Directory Domain Services. A read-only domain controller (RODC) is an additional domain controller that hosts a read-only replica of a domain's Active Directory data store. RODCs are ideally suited to the needs of branch offices, where a domain controller's physical security cannot be guaranteed. Except for passwords, RODCs store the same objects and attributes as writable domain controllers. These objects and attributes are replicated to RODCs through unidirectional replication from a writable domain controller that acts as a replication partner.

Because RODCs by default do not store passwords or credentials other than for their own computer account and the Kerberos Target (Krbtgt) account, RODCs pull user and computer credentials from a writable domain controller that is running Windows Server 2008 or later. If allowed by a password replication policy that is enforced on the writable domain controller, an RODC retrieves and then caches credentials as necessary until the credentials change. Because only a subset of credentials is stored on an RODC, this limits the number of credentials that can possibly be compromised.

**TIP** Any domain user can be delegated as a local administrator of an RODC without granting any other rights in the domain. An RODC can act in the role of a global catalog but cannot act in the role of an operations master. Although RODCs can pull information from domain controllers running Windows Server 2003, RODCs can pull updates of the domain partition only from a writable domain controller running Windows Server 2008 or later in the same domain.

## Using Restartable Active Directory Domain Services

Restartable Active Directory Domain Services is a feature that allows an administrator to start and stop AD DS. In the Services console, the Active Directory Domain Services service is available on domain controllers, allowing you to easily stop and restart AD DS in the same way as for any other service that is running locally on the server. While AD DS is stopped, you can perform maintenance tasks that would otherwise require restarting the server, such as performing offline defragmentation of the Active Directory database, applying updates to the operating system, or initiating an authoritative restore. While AD DS is stopped on a server, other domain controllers can handle authentication and logon tasks. Cached credentials, smart cards, and biometric logon methods continue to be supported. If no other domain controller is available and none of these logon methods applies, you can still log on to the server using the Directory Services Restore Mode account and password.

All domain controllers running Windows Server 2008 or later support Restartable Active Directory Domain Services—even RODCs. As an administrator, you can start

or stop AD DS by using the Domain Controller entry in the Services utility. Because of Restartable Active Directory Domain Services, domain controllers running Windows Server 2008 or later have three possible states:

- **Active Directory Started** Active Directory is started, and the domain controller has the same running state as a domain controller running Windows 2000 Server or Windows Server 2003. This allows the domain controller to provide authentication and logon services for a domain.
- **Active Directory Stopped** Active Directory is stopped, and the domain controller can no longer provide authentication and logon services for a domain. This mode shares some characteristics of both a member server and a domain controller in Directory Services Restore Mode. As with a member server, the server is joined to the domain. Users can log on interactively using cached credentials, smart cards, and biometric logon methods. Users can also log on over the network by using another domain controller for domain logon. As with Directory Services Restore Mode, the Active Directory database (Ntds.dit) on the local domain controller is offline. This means you can perform offline AD DS operations, such as defragmentation of the database and application of security updates, without having to restart the domain controller.
- **Directory Services Restore Mode** Active Directory is in restore mode. The domain controller has the same restore state as a domain controller running Windows Server 2003. This mode allows you to perform an authoritative or nonauthoritative restore of the Active Directory database.

When working with AD DS in the Stopped state, you should keep in mind that dependent services are also stopped when you stop AD DS. This means that File Replication Service (FRS), Kerberos Key Distribution Center (KDC), and Intersite Messaging are stopped before Active Directory is stopped, and that even if they are running, these dependent services are restarted when Active Directory restarts. Further, you can restart a domain controller in Directory Services Restore Mode, but you cannot start a domain controller in the Active Directory Stopped state. To get to the Stopped state, you must first start the domain controller normally and then stop AD DS.

## Name-Resolution Services

---

Windows operating systems use name resolution to make it easier to communicate with other computers on a network. Name resolution associates computer names with the numerical IP addresses that are used for network communications. Thus, rather than using long strings of digits, users can access a computer on the network by using a friendly name.

Current Windows operating systems natively support three name-resolution systems:

- Domain Name System (DNS)
- Windows Internet Name Service (WINS)
- Link-Local Multicast Name Resolution (LLMNR)

The sections that follow examine these services.

## Using Domain Name System

DNS is a name-resolution service that resolves computer names to IP addresses. Using DNS, the fully qualified host name `computer84.cpandl.com`, for example, can be resolved to an IP address, which allows it and other computers to find one another. DNS operates over the TCP/IP protocol stack and can be integrated with WINS, Dynamic Host Configuration Protocol (DHCP), and Active Directory Domain Services. As discussed in Chapter 15, “Running DHCP Clients and Servers,” DHCP is used for dynamic IP addressing and TCP/IP configuration.

DNS organizes groups of computers into domains. These domains are organized into a hierarchical structure, which can be defined on an Internet-wide basis for public networks or on an enterprise-wide basis for private networks (also known as *intranets* and *extranets*). The various levels within the hierarchy identify individual computers, organizational domains, and top-level domains. For the fully qualified host name `computer84.cpandl.com`, *computer84* represents the host name for an individual computer, *cpandl* is the organizational domain, and *com* is the top-level domain.

Top-level domains are at the root of the DNS hierarchy; they are also called *root domains*. These domains are organized geographically, by organization type, and by function. Normal domains, such as `cpandl.com`, are also referred to as *parent domains*. They’re called parent domains because they’re the parents of an organizational structure. Parent domains can be divided into subdomains that can be used for groups or departments within an organization.

Subdomains are often referred to as *child domains*. For example, the fully qualified domain name (FQDN) for a computer within a human resources group could be `jacob.hr.cpandl.com`. Here, *jacob* is the host name, *hr* is the child domain, and *cpandl.com* is the parent domain.

Active Directory domains use DNS to implement their naming structure and hierarchy. Active Directory and DNS are tightly integrated, so much so that you should install DNS on the network before you can install domain controllers using Active Directory. During installation of the first domain controller on an Active Directory network, you’re given the opportunity to install DNS automatically if a DNS server can’t be found on the network. You are also able to specify whether DNS and Active Directory should be fully integrated. In most cases, you should respond affirmatively to both requests. With full integration, DNS information is stored directly in Active Directory. This allows you to take advantage of Active Directory’s capabilities. The difference between partial integration and full integration is very important:

- **Partial integration** With partial integration, the domain uses standard file storage. DNS information is stored in text-based files that end with the `.dns` extension, and the default location of these files is `%SystemRoot%\System32\Dns`. Updates to DNS are handled through a single authoritative DNS server. This server is designated as the primary DNS server for the particular domain or an area within a domain called a *zone*. Clients that use dynamic DNS updates through DHCP must be configured to use the primary DNS server

in the zone. If they aren't, their DNS information won't be updated. Likewise, dynamic updates through DHCP can't be made if the primary DNS server is offline.

- **Full integration** With full integration, the domain uses directory-integrated storage. DNS information is stored directly in Active Directory and is available through the container for the *dnsZone* object. Because the information is part of Active Directory, any domain controller can access the data and a multimaster approach can be used for dynamic updates through DHCP. This allows any domain controller running the DNS Server service to handle dynamic updates. Furthermore, clients that use dynamic DNS updates through DHCP can use any DNS server within the zone. An added benefit of directory integration is the ability to use directory security to control access to DNS information.

If you look at the way DNS information is replicated throughout the network, you can see more advantages to full integration with Active Directory. With partial integration, DNS information is stored and replicated separately from Active Directory. Having two separate structures reduces the effectiveness of both DNS and Active Directory and makes administration more complex. Because DNS is less efficient than Active Directory at replicating changes, you might also increase network traffic and the amount of time it takes to replicate DNS changes throughout the network.

To enable DNS on the network, you need to configure DNS clients and servers. When you configure DNS clients, you tell the clients the IP addresses of DNS servers on the network. Using these addresses, clients can communicate with DNS servers anywhere on the network, even if the servers are on different subnets.

When the network uses DHCP, you should configure DHCP to work with DNS. To do this, you need to set the DHCP scope options 006 DNS Servers and 015 DNS Domain Name as specified in "Setting Scope Options" in Chapter 15. Additionally, if computers on the network need to be accessible from other Active Directory domains, you need to create records for them in DNS. DNS records are organized into zones; a zone is simply an area within a domain. Configuring a DNS server is explained in "Configuring a Primary DNS Server" in Chapter 16, "Optimizing DNS."

When you install the DNS Server service on an RODC, the RODC is able to pull a read-only replica of all application directory partitions that are used by DNS, including *ForestDNSZones* and *DomainDNSZones*. Clients can then query the RODC for name resolution as they would query any other DNS server. However, as with directory updates, the DNS server on an RODC does not support direct updates. This means that the RODC does not register name server (NS) resource records for any Active Directory-integrated zone that it hosts. When a client attempts to update its DNS records against an RODC, the server returns a referral to a DNS server that the client can use for the update. The DNS server on the RODC should receive the updated record from the DNS server that receives details about the update using a special replicate-single-object request that runs as a background process.

Windows 7 and later releases add support for DNS Security Extensions (DNSSEC). The DNS client running on these operating systems can send queries that indicate support for DNSSEC, process related records, and determine whether a DNS server

has validated records on its behalf. On Windows servers, this allows your DNS servers to securely sign zones and to host DNSSEC-signed zones. It also allows DNS servers to process related records and perform both validation and authentication.

## Using Windows Internet Name Service

WINS is a service that resolves computer names to IP addresses. Using WINS, the computer name COMPUTER84, for example, can be resolved to an IP address that enables computers on a Microsoft network to find one another and transfer information. WINS is needed to support pre-Windows 2000 systems and older applications that use NetBIOS over TCP/IP, such as the .NET command-line utilities. If you don't have pre-Windows 2000 systems or applications on the network, you don't need to use WINS.

WINS works best in client/server environments in which WINS clients send single-label (host) name queries to WINS servers for name resolution and WINS servers resolve the query and respond. When all your DNS servers are running Windows Server 2008 or later, deploying a Global Names zone creates static, global records with single-label names without relying on WINS. This allows users to access hosts using single-label names rather than FQDNs and removes the dependency on WINS. To transmit WINS queries and other information, computers use NetBIOS. NetBIOS provides an application programming interface (API) that allows computers on a network to communicate. NetBIOS applications rely on WINS or the local LMHOSTS file to resolve computer names to IP addresses. On pre-Windows 2000 networks, WINS is the primary name resolution service available. On Windows 2000 and later networks, DNS is the primary name resolution service and WINS has a different function. This function is to allow pre-Windows 2000 systems to browse lists of resources on the network and to allow Windows 2000 and later systems to locate NetBIOS resources.

To enable WINS name resolution on a network, you need to configure WINS clients and servers. When you configure WINS clients, you tell the clients the IP addresses for WINS servers on the network. Using the IP addresses, clients can communicate with WINS servers anywhere on the network, even if the servers are on different subnets. WINS clients can also communicate by using a broadcast method through which clients broadcast messages to other computers on the local network segment requesting their IP addresses. Because messages are broadcast, the WINS server isn't used. Any non-WINS clients that support this type of message broadcasting can also use this method to resolve computer names to IP addresses.

When clients communicate with WINS servers, they establish sessions that have the following three key parts:

- **Name registration** During name registration, the client gives the server its computer name and its IP address and asks to be added to the WINS database. If the specified computer name and IP address aren't already in use on the network, the WINS server accepts the request and registers the client in the WINS database.

- **Name renewal** Name registration isn't permanent. Instead, the client can use the name for a specified period known as a *lease*. The client is also given a time period within which the lease must be renewed, which is known as the renewal interval. The client must reregister with the WINS server during the renewal interval.
- **Name release** If the client can't renew the lease, the name registration is released, allowing another system on the network to use the computer name, IP address, or both. The names are also released when you shut down a WINS client.

After a client establishes a session with a WINS server, the client can request name-resolution services. The method used to resolve computer names to IP addresses depends on how the network is configured. The following four name-resolution methods are available:

- **B-node (broadcast)** Uses broadcast messages to resolve computer names to IP addresses. Computers that need to resolve a name broadcast a message to every host on the local network, requesting the IP address for a computer name. On a large network with hundreds or thousands of computers, these broadcast messages can use up valuable network bandwidth.
- **P-node (peer-to-peer)** Uses WINS servers to resolve computer names to IP addresses. As explained earlier, client sessions have three parts: name registration, name renewal, and name release. In this mode, when a client needs to resolve a computer name to an IP address, the client sends a query message to the server and the server responds with an answer.
- **M-node (mixed)** Combines b-node and p-node. With m-node, a WINS client first tries to use b-node for name resolution. If the attempt fails, the client then tries to use p-node. Because b-node is used first, this method has the same problems with network bandwidth usage as b-node.
- **H-node (hybrid)** Also combines b-node and p-node. With h-node, a WINS client first tries to use p-node for peer-to-peer name resolution. If the attempt fails, the client then tries to use broadcast messages with b-node. Because peer-to-peer is the primary method, h-node offers the best performance on most networks. H-node is also the default method for WINS name resolution.

If WINS servers are available on the network, Windows clients use the p-node method for name resolution. If no WINS servers are available on the network, Windows clients use the b-node method for name resolution. Windows computers can also use DNS and the local files LMHOSTS and HOSTS to resolve network names. Working with DNS is covered in detail in Chapter 16.

When you use DHCP to assign IP addresses dynamically, you should set the name resolution method for DHCP clients. To do this, you need to set DHCP scope options for the 046 WINS/NBT Node Type as specified in "Setting Scope Options" in Chapter 15. The best method to use is h-node. You'll get the best performance and have reduced traffic on the network.

## Using Link-Local Multicast Name Resolution

LLMNR fills a need for peer-to-peer name-resolution services for devices with an IPv4 address, an IPv6 address, or both, allowing IPv4 and IPv6 devices on a single subnet without a WINS or DNS server to resolve each other's names—a service that neither WINS nor DNS can fully provide. Although WINS can provide both client/server and peer-to-peer name-resolution services for IPv4, it does not support IPv6 addresses. DNS, on the other hand, supports IPv4 and IPv6 addresses, but it depends on designated servers to provide name-resolution services.

Windows 7 and later releases support LLMNR. LLMNR is designed for both IPv4 and IPv6 clients in configurations where other name-resolution systems are not available, such as

- Home or small office networks
- Ad hoc networks
- Corporate networks where DNS services are not available

LLMNR is designed to complement DNS by enabling name resolution in scenarios in which conventional DNS name resolution is not possible. Although LLMNR can replace the need for WINS in cases where NetBIOS is not required, LLMNR is not a substitute for DNS because it operates only on the local subnet. Because LLMNR traffic is prevented from propagating across routers, it cannot accidentally flood the network.

As with WINS, you use LLMNR to resolve a host name, such as COMPUTER84, to an IP address. By default, LLMNR is enabled on all computers running Windows 7 and later releases, and these computers use LLMNR only when all attempts to look up a host name through DNS fail. As a result, name resolution works like the following for Windows 7 and later releases:

1. A host computer sends a query to its configured primary DNS server. If the host computer does not receive a response or receives an error, it tries each configured alternate DNS server in turn. If the host has no configured DNS servers or fails to connect to a DNS server without errors, name resolution fails over to LLMNR.
2. The host computer sends a multicast query over User Datagram Protocol (UDP) requesting the IP address for the name being looked up. This query is restricted to the local subnet (also referred to as the *local link*).
3. Each computer on the local link that supports LLMNR and is configured to respond to incoming queries receives the query and compares the name to its own host name. If the host name is not a match, the computer discards the query. If the host name is a match, the computer transmits a unicast message containing its IP address to the originating host.

You can also use LLMNR for reverse mapping. With a reverse mapping, a computer sends a unicast query to a specific IP address, requesting the host name of the target computer. An LLMNR-enabled computer that receives the request sends a unicast reply containing its host name to the originating host.

LLMNR-enabled computers are required to ensure that their names are unique on the local subnet. In most cases, a computer checks for uniqueness when it



starts, when it resumes from a suspended state, and when you change its network-interface settings. If a computer has not yet determined that its name is unique, it must indicate this condition when responding to a name query.

**REAL WORLD** By default, LLMNR is automatically enabled on computers running Windows 7 and later releases. You can disable LLMNR through registry settings. To disable LLMNR for all network interfaces, create and set the following registry value to 0: HKLM/SYSTEM/CurrentControlSet/Services/Dnscache/Parameters/EnableMulticast.

To disable LLMNR for a specific network interface, create and set the following registry value to 0: HKLM/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/Adapter-GUID/EnableMulticast.

Here, *AdapterGUID* is the globally unique identifier (GUID) of the network-interface adapter for which you want to disable LLMNR. You can enable LLMNR again at any time by setting these registry values to 1. You also can manage LLMNR through Group Policy.

## Frequently Used Tools

---

Many utilities are available for administering Windows Server 2012 systems. The tools you use the most include the following:

- **Control Panel** A collection of tools for managing system configuration. You can organize Control Panel in different ways according to the view you're using. A view is simply a way of organizing and presenting options. You change the view by using the View By list. Category view is the default view, and it provides access to tools by category, tool, and key tasks. The Large Icons and Small Icons views are alternative views that list each tool separately by name.
- **Graphical administrative tools** The key tools for managing network computers and their resources. You can access these tools by selecting them individually from the Administrative Tools program group.
- **Administrative wizards** Tools designed to automate key administrative tasks. You can access many administrative wizards in Server Manager—the central administration console for Windows Server 2012.
- **Command-line utilities** You can launch most administrative utilities from the command prompt. In addition to these utilities, Windows Server 2012 provides others that are useful for working with Windows Server 2012 systems.

To learn how to use any of the .NET command-line tools, type **NET HELP** at a command prompt followed by the command name, such as **NET HELP SHARE**. Windows Server 2012 then provides an overview of how the command is used.

## Windows PowerShell 3.0

For additional flexibility in your command-line scripting, you might want to use Windows PowerShell 3.0. Windows PowerShell 3.0 is a full-featured command shell that can use built-in commands called *cmdlets*, built-in programming features, and standard command-line utilities. A command console and a graphical environment are available.

Although the Windows PowerShell console and the graphical scripting environment are installed by default, several other PowerShell features are not installed by default. They include the Windows PowerShell 2.0 engine, which is provided for backward compatibility with existing PowerShell host applications, and Windows PowerShell Web Access, which lets a server act as a web gateway for managing the server remotely using PowerShell and a web client.

**REAL WORLD** You can install these additional Windows PowerShell features using the Add Roles And Features Wizard. On the desktop, tap or click the Server Manager button on the taskbar. This option is included by default. In Server Manager, tap or click Manage and then tap or click Add Roles And Features. This runs the Add Roles And Features Wizard, which you use to add these features. Note, however, that with Windows Server 2012, not only can you disable a role or feature, but you also can remove the binaries needed for that role or feature. Binaries needed to install roles and features are referred to as *payloads*.

The Windows PowerShell console (Powershell.exe) is a 32-bit or 64-bit environment for working with Windows PowerShell at the command line. On 32-bit versions of Windows, you'll find the 32-bit executable in the %SystemRoot%\System32\WindowsPowerShell\v1.0 directory. On 64-bit versions of Windows, you'll find the 32-bit executable in the %SystemRoot%\SysWow64\WindowsPowerShell\v1.0 directory, and the 64-bit executable in the %SystemRoot%\System32\WindowsPowerShell\v1.0 directory.

On the desktop, you can open the Windows PowerShell console by tapping or clicking the PowerShell button on the taskbar. This option is included by default. On 64-bit systems, the 64-bit version of PowerShell is started by default. If you want to use the 32-bit PowerShell console on a 64-bit system, you must select the Windows PowerShell (x86) option.

You can start Windows PowerShell from a Windows command shell (Cmd.exe) by entering the following:

```
powershell
```

**NOTE** The directory path for Windows PowerShell should be in your command path by default. This ensures that you can start Windows PowerShell from a command prompt without first having to change to the related directory.

After starting Windows PowerShell, you can enter the name of a cmdlet at the prompt, and the cmdlet will run in much the same way as a command-line command. You can also execute cmdlets in scripts. Cmdlets are named using verb-noun pairs. The verb tells you what the cmdlet does in general. The noun tells you what

specifically the cmdlet works with. For example, the `Get-Variable` cmdlet gets all Windows PowerShell environment variables and returns their values, or it gets a specifically named environment variable and returns its value. The common verbs associated with cmdlets are as follows:

- **Get-** Queries a specific object or a subset of a type of object, such as a specified performance counter or all performance counters
- **Set-** Modifies specific settings of an object
- **Enable-** Enables an option or a feature
- **Disable-** Disables an option or a feature
- **New-** Creates a new instance of an item, such as a new event or service
- **Remove-** Removes an instance of an item, such as an event or event log

At the Windows PowerShell prompt, you can get a complete list of cmdlets by typing **get-help \*-\***. To get help documentation on a specific cmdlet, type **get-help** followed by the cmdlet name, such as **get-help get-variable**.

All cmdlets also have configurable aliases that act as shortcuts for executing a cmdlet. To list all aliases available, type **get-item -path alias:** at the Windows PowerShell prompt. You can create an alias that invokes any command by using the following syntax:

```
new-item -path alias:AliasName -value:FullCommandPath
```

Here *AliasName* is the name of the alias to create, and *FullCommandPath* is the full path to the command to run, such as

```
new-item -path alias:sm -value:c:\windows\system32\compmgmtlauncher.exe
```

This example creates the alias *sm* for starting Server Manager. To use this alias, you simply type **sm** and then press Enter when you are working with Windows PowerShell.

**REAL WORLD** Generally speaking, anything you can type at a command prompt can be typed at the PowerShell prompt as well. This is possible because PowerShell looks for external commands and utilities as part of its normal processing. As long as the external command or utility is found in a directory specified by the `PATH` environment variable, the command or utility is run as appropriate. However, keep in mind that the PowerShell execution order could affect whether a command runs as expected. For PowerShell, the execution order is 1) alternate built-in or profile-defined aliases, 2) built-in or profile-defined functions, 3) cmdlets or language keywords, 4) scripts with the `.ps1` extension, and 5) external commands, utilities, and files. Thus, if any element in 1 to 4 of the execution order has the same name as a command, that element will run instead of the expected command.

## Windows Remote Management

The Windows PowerShell remoting features are supported by the WS-Management protocol and the Windows Remote Management (WinRM) service that implements WS-Management in Windows. Computers running Windows 7 and later, as well as Windows Server 2008 R2 or later include WinRM 2.0 or later. If you want to manage

a Windows server from a workstation, you need to be sure that WinRM 2.0 and Windows PowerShell 3.0 are installed and that the server has a WinRM listener enabled. An IIS extension, installable as a Windows feature called WinRM IIS Extension, lets a server act as a web gateway for managing the server remotely using WinRM and a web client.

### Enabling and Using WinRM

You can verify the availability of WinRM 2.0 and configure Windows PowerShell for remoting by following these steps:

1. Tap or click Start, and then point to Windows PowerShell. Start Windows PowerShell as an administrator by pressing and holding or right-clicking the Windows PowerShell shortcut and selecting Run As Administrator.
2. The WinRM service is configured for manual startup by default. You must change the startup type to Automatic and start the service on each computer you want to work with. At the Windows PowerShell prompt, you can verify that the WinRM service is running by using the following command:

```
get-service winrm
```

As shown in the following example, the value of the *Status* property in the output should be *Running*:

Status	Name	DisplayName
-----	----	-----
Running	WinRM	Windows Remote Management

If the service is stopped, enter the following command to start the service and configure it to start automatically in the future:

```
set-service -name winrm -startuptype automatic -status running
```

3. To configure Windows PowerShell for remoting, type the following command:

```
Enable-PSRemoting -force
```

You can enable remoting only when your computer is connected to a domain or a private network. If your computer is connected to a public network, you need to disconnect from the public network and connect to a domain or private network and then repeat this step. If one or more of your computer's connections has the Public Network connection type but you are actually connected to a domain or private network, you need to change the network connection type in Network And Sharing Center and then repeat this step.

In many cases, you are able to work with remote computers in other domains. However, if the remote computer is not in a trusted domain, the remote computer might not be able to authenticate your credentials. To enable authentication, you need to add the remote computer to the list of trusted hosts for the local computer in WinRM. To do so, type the following:

```
winrm set winrm/config/client '@{TrustedHosts"RemoteComputer"}'
```

Here *RemoteComputer* is the name of the remote computer, such as

```
winrm set winrm/config/client '@{TrustedHosts="CorpServer56"}'
```

When you are working with computers in workgroups or homegroups, you must use HTTPS as the transport or add the remote machine to the TrustedHosts configuration settings. If you cannot connect to a remote host, verify that the service on the remote host is running and is accepting requests by running the following command on the remote host:

```
winrm quickconfig
```

This command analyzes and configures the WinRM service. If the WinRM service is set up correctly, you'll see output similar to the following:

```
WinRM already is set up to receive requests on this machine.  
WinRM already is set up for remote management on this machine.
```

If the WinRM service is not set up correctly, you see errors and need to respond affirmatively to several prompts that allow you to automatically configure remote management. When this process is complete, WinRM should be set up correctly.

Whenever you use Windows PowerShell remoting features, you must start Windows PowerShell as an administrator by pressing and holding or right-clicking the Windows PowerShell shortcut and selecting Run As Administrator. When starting Windows PowerShell from another program, such as the command prompt, you must start that program as an administrator.

## Configuring WinRM

When you are working with an elevated, administrator command prompt, you can use the WinRM command-line utility to view and manage the remote management configuration. Type **winrm get winrm/config** to display detailed information about the remote management configuration.

If you examine the configuration listing, you'll notice there is a hierarchy of information. The base of this hierarchy, the Config level, is referenced with the path *winrm/config*. Then there are sublevels for client, service, and WinRS, referenced as *winrm/config/client*, *winrm/config/service*, and *winrm/config/winrs*. You can change the value of most configuration parameters by using the following command:

```
winrm set ConfigPath @{ParameterName="Value"}
```

Here *ConfigPath* is the configuration path, *ParameterName* is the name of the parameter you want to work with, and *Value* sets the value for the parameter, such as

```
winrm set winrm/config/winrs @{MaxShellsPerUser="10"}
```

Here, you set the *MaxShellsPerUser* parameter under *winrm/config/winrs*. This parameter controls the maximum number of connections to a remote computer that can be active per user. (By default, each user can have only five active connections.) Keep in mind that some parameters are read-only and cannot be set in this way.

WinRM requires at least one listener to indicate the transports and IP addresses on which management requests can be accepted. The transport must be HTTP, HTTPS, or both. With HTTP, messages can be encrypted using NTLM or Kerberos encryption. With HTTPS, Secure Sockets Layer (SSL) is used for encryption. You can examine the configured listeners by typing **winrm enumerate winrm/config/listener**. As Listing 1-1 shows, this command displays the configuration details for configured listeners.

---

**LISTING 1-1** Sample Configuration for Listeners

---

```
Listener
  Address = *
  Transport = HTTP
  Port = 80
  Hostname
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint
  ListeningOn = 127.0.0.1, 192.168.1.225
```

By default, your computer is probably configured to listen on any IP address. If so, you won't see any output. To limit WinRM to specific IP addresses, the computer's local loopback address (127.0.0.1) and assigned IPv4 and IPv6 addresses can be explicitly configured for listening. You can configure a computer to listen for requests over HTTP on all configured IP addresses by typing the following:

```
winrm create winrm/config/listener?Address=*&Transport=HTTP
```

You can listen for requests over HTTPS on all IP addresses configured on the computer by typing this:

```
winrm create winrm/config/listener?Address=*&Transport=HTTPS
```

Here, the asterisk (\*) indicates all configured IP addresses. Note that the *CertificateThumbprint* property must be empty to share the SSL configuration with another service.

You can enable or disable a listener for a specific IP address by typing

```
winrm set winrm/config/listener?Address=IP:192.168.1.225&Transport=HTTP
@{Enabled="true"}
```

or

```
winrm set winrm/config/listener?Address=IP:192.168.1.225&Transport=HTTP
@{Enabled="false"}
```

You can enable or disable basic authentication on the client by typing

```
winrm set winrm/config/client/auth @{Basic="true"}
```

or

```
winrm set winrm/config/client/auth @{Basic="false"}
```

You can enable or disable Windows authentication using either NTLM or Kerberos (as appropriate) by typing

```
winrm set winrm/config/client @{TrustedHosts="<local>"}
```

or

```
winrm set winrm/config/client @{TrustedHosts=""}
```

In addition to managing WinRM at the command line, you can manage the service by using Group Policy. As a result, Group Policy settings might override any settings you enter.





# Managing Servers Running Windows Server 2012

- Server Roles, Role Services, and Features for Windows Server 2012 **32**
- Full-Server, Minimal-Interface, and Server Core Installations **40**
- Installing Windows Server 2012 **43**
- Managing Roles, Role Services, and Features **57**
- Managing System Properties **73**

Servers are the heart of any Microsoft Windows network. One of your primary responsibilities as an administrator is to manage these resources. Windows Server 2012 comes with several integrated management tools. The one you'll use for handling core system administration tasks is Server Manager. Server Manager provides setup and configuration options for the local server as well as options for managing roles, features, and related settings on any remotely manageable server in the enterprise. Tasks you can use Server Manager to perform include

- Adding servers for remote management
- Initiating remote connections to servers
- Configuring the local server
- Managing installed roles and features
- Managing volumes and shares on file servers
- Configuring Network Interface Card (NIC) Teaming
- Viewing events and alerts
- Restarting servers

Server Manager is great for general system administration, but you also need a tool that gives you fine control over system environment settings and properties. This is where the System utility comes into the picture. You can use this utility to do the following:

- Change a computer's name
- Configure application performance, virtual memory, and registry settings
- Manage system and user environment variables
- Set system startup and recovery options

# Server Roles, Role Services, and Features for Windows Server 2012

---

Windows Server 2012 uses the same configuration architecture as Windows Server 2008 and Windows Server 2008 Release 2 (R2). You prepare servers for deployment by installing and configuring the following components:

- **Server roles** A server role is a related set of software components that allows a server to perform a specific function for users and other computers on a network. A computer can be dedicated to a single role, such as Active Directory Domain Services (AD DS), or provide multiple roles.
- **Role services** A role service is a software component that provides the functionality for a server role. Each role can have one or more related role services. Some server roles, such as Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP), have a single function, and installing the role installs this function. Other roles, such as Network Policy and Access Services and Active Directory Certificate Services (AD CS), have multiple role services that you can install. With these server roles, you can choose which role services to install.
- **Features** A feature is a software component that provides additional functionality. Features, such as BitLocker Drive Encryption and Windows Server Backup, are installed and removed separately from roles and role services. A computer can have zero or more features installed depending on its configuration.

You configure roles, role services, and features by using Server Manager, a Microsoft Management Console (MMC). Some roles, role services, and features are dependent on other roles, role services, and features. As you install roles, role services, and features, Server Manager prompts you to install other roles, role services, or features that are required. Similarly, if you try to remove a required component of an installed role, role service, or feature, Server Manager warns that you cannot remove the component unless you also remove dependent roles, role services, or features.

Because adding or removing roles, role services, and features can change hardware requirements, you should carefully plan any configuration changes and determine how they affect a server's overall performance. Although you typically want to combine complementary roles, doing so increases the workload on the server, so you need to optimize the server hardware accordingly. Table 2-1 provides an overview of the primary roles and the related role services you can deploy on a server running Windows Server 2012.

**TABLE 2-1** Primary Roles and Related Role Services for Windows Server 2012

ROLE	DESCRIPTION
Active Directory Certificate Services (AD CS)	Provides functions necessary for issuing and revoking digital certificates for users, client computers, and servers. Includes these role services: Certification Authority, Certification Authority Web Enrollment, Online Responder, Network Device Enrollment Service, Certificate Enrollment Web Service, and Certificate Enrollment Policy Web Service.
Active Directory Domain Services (AD DS)	Provides functions necessary for storing information about users, groups, computers, and other objects on the network, and makes this information available to users and computers. Active Directory domain controllers give network users and computers access to permitted resources on the network.
Active Directory Federation Services (AD FS)	Complements the authentication and access management features of AD DS by extending them to the World Wide Web. Includes these role services and subservices: Federation Service, Federation Service Proxy, AD FS Web Agents, Claims-Aware Agent, and Windows Token-Based Agent.
Active Directory Lightweight Directory Services (AD LDS)	Provides a data store for directory-enabled applications that do not require AD DS and do not need to be deployed on domain controllers. Does not include additional role services.
Active Directory Rights Management Services (AD RMS)	Provides controlled access to protected email messages, documents, intranet pages, and other types of files. Includes these role services: Active Directory Rights Management Server and Identity Federation Support.
Application Server	Allows a server to host distributed applications built using ASP.NET, Enterprise Services, and Microsoft .NET Framework 4.5. Includes more than a dozen role services.
DHCP Server	DHCP provides centralized control over IP addressing. DHCP servers can assign dynamic IP addresses and essential TCP/IP settings to other computers on a network. Does not include additional role services.
DNS Server	DNS is a name-resolution system that resolves computer names to IP addresses. DNS servers are essential for name resolution in Active Directory domains. Does not include additional role services.

ROLE	DESCRIPTION
Fax Server	Provides centralized control over sending and receiving faxes in the enterprise. A fax server can act as a gateway for faxing and allows you to manage fax resources, such as jobs and reports, and fax devices on the server or on the network. Does not include additional role services.
File And Storage Services	Provides essential services for managing files and storage, and the way they are made available and replicated on the network. A number of server roles require some type of file service. Includes these role services and subservices: BranchCache for Network Files, Data Deduplication, Distributed File System, DFS Namespaces, DFS Replication, File Server, File Server Resource Manager, Services for Network File System (NFS), File Server VSS Agent Service, iSCSI Target Server, iSCSI Target Storage Provider, and Storage Services.
Hyper-V	Provides services for creating and managing virtual machines that emulate physical computers. Virtual machines have separate operating system environments from the host server.
Network Policy and Access Services (NPAS)	Provides essential services for managing network access policies. Includes these role services: Network Policy Server (NPS), Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP).
Print And Document Services	Provides essential services for managing network printers, network scanners, and related drivers. Includes these role services: Print Server, LPD Service, Internet Printing, and Distributed Scan Server.
Remote Access	Provides services for managing routing and remote access to networks. Use this role if you need to configure Virtual Private Networks (VPN), Network Address Translation (NAT), and other routing services. Includes these role services: DirectAccess and VPN (RAS) and Routing.
Remote Desktop Services	Provides services that allow users to run Windows-based applications that are installed on a remote server. When users run an application on a terminal server, the execution and processing occur on the server and only the data from the application is transmitted over the network.
Volume Activation Services	Provides services for automating the management of volume license keys and volume key activation.

ROLE	DESCRIPTION
Web Server (IIS)	Used to host websites and web-based applications. Websites hosted on a web server can have both static content and dynamic content. You can build web applications hosted on a web server by using ASP.NET and .NET Framework 4.5. When you deploy a web server, you can manage the server configuration using IIS 8 modules and administration tools. Includes several dozen role services.
Windows Deployment Services (WDS)	Provides services for deploying Windows computers in the enterprise. Includes these role services: Deployment Server and Transport Server.
Windows Server Update Services (WSUS)	Provides services for Microsoft Update, allowing you to distribute updates from designated servers.

Table 2-2 provides an overview of the primary features you can deploy on a server running Windows Server 2012. Unlike early releases of Windows, Windows Server 2012 does not install some important server features automatically. For example, you must add Windows Server Backup to use the built-in backup and restore features of the operating system.

**TABLE 2-2** Primary Features for Windows Server 2012

FEATURE	DESCRIPTION
Background Intelligent Transfer Service (BITS)	Provides intelligent background transfers. When this feature is installed, the server can act as a BITS server that can receive file uploads from clients. This feature isn't necessary for downloads to clients using BITS. Additional subfeatures include BITS IIS Server Extension and BITS Compact Server.
BitLocker Drive Encryption	Provides hardware-based security to protect data through full-volume encryption that prevents disk tampering while the operating system is offline. Computers that have Trusted Platform Module (TPM) can use BitLocker Drive Encryption in Startup Key or TPM-Only mode. Both modes provide early integrity validation.
BitLocker Network Unlock	Provides support for network-based key protectors that automatically unlock BitLocker-protected operating system drives when a domain-joined computer is restarted.

FEATURE	DESCRIPTION
BranchCache	Provides services needed for BranchCache client and server functionality. Includes HTTP protocol, Hosted Cache, and related services.
Client for NFS	Provides functionality for accessing files on UNIX-based NFS servers.
Data Center Bridging	Supports a suite of IEEE standards for enhancing LANs and enforcing bandwidth allocation.
Enhanced Storage	Provides support for Enhanced Storage Devices.
Failover Clustering	Provides clustering functionality that allows multiple servers to work together to provide high availability for services and applications. Many types of services can be clustered, including file and print services. Messaging and database servers are ideal candidates for clustering.
Group Policy Management	Installs the Group Policy Management Console (GPMC), which provides centralized administration of Group Policy.
Ink and Handwriting Services	Provides support for use of a pen or stylus and handwriting recognition.
IP Address Management Server	Provides support for central management of the enterprise's IP address space and the related infrastructure servers.
Internet Printing Client	Provides functionality that allows clients to use HTTP to connect to printers on web print servers.
Internet Storage Naming Server (iSNS) Server Service	Provides management and server functions for Internet SCSI (iSCSI) devices, allowing the server to process registration requests, deregistration requests, and queries from iSCSI devices.
LPR Port Monitor	Installs the LPR Port Monitor, which allows printing to devices attached to UNIX-based computers.
Media Foundation	Provides essential functionality for Windows Media Foundation.
Message Queuing	Provides management and server functions for distributed message queuing. A group of related subfeatures is available as well.
Multipath I/O (MPIO)	Provides functionality necessary for using multiple data paths to a storage device.

FEATURE	DESCRIPTION
.NET Framework 4.5	Provides APIs for application development. Additional subfeatures include .NET Framework 4.5, ASP.NET 4.5, and Windows Communication Foundation (WCF) Activation Components.
Network Load Balancing (NLB)	NLB provides failover support and load balancing for IP-based applications and services by distributing incoming application requests among a group of participating servers. Web servers are ideal candidates for load balancing.
Peer Name Resolution Protocol (PNRP)	Provides Link-Local Multicast Name Resolution (LLMNR) functionality that allows peer-to-peer, name-resolution services. When you install this feature, applications running on the server can use LLMNR to register and resolve names.
Quality Windows Audio Video Experience	A networking platform for audio video (AV) streaming applications on IP home networks.
RAS Connection Manager Administration Kit	Provides the framework for creating profiles for connecting to remote servers and networks.
Remote Assistance	Allows a remote user to connect to the server to provide or receive Remote Assistance.
Remote Differential Compression	Provides support for differential compression by determining which parts of a file have changed and replicating only the changes.
Remote Server Administration Tools (RSAT)	Installs role-management and feature-management tools that can be used for remote administration of other Windows Server systems. Options for individual tools are provided, or you can install tools by top-level category or subcategory.
Remote Procedure Call (RPC) over HTTP Proxy	Installs a proxy for relaying RPC messages from client applications to the server over HTTP. RPC over HTTP is an alternative to having clients access the server over a VPN connection.
Simple TCP/IP Services	Installs additional TCP/IP services, including Character Generator, Daytime, Discard, Echo, and Quote of the Day.
Simple Mail Transfer Protocol (SMTP) Server	SMTP is a network protocol for controlling the transfer and routing of email messages. When this feature is installed, the server can act as a basic SMTP server. For a full-featured solution, you need to install a messaging server, such as Microsoft Exchange Server.

FEATURE	DESCRIPTION
Simple Network Management Protocol (SNMP) Services	SNMP is a protocol used to simplify management of TCP/IP networks. You can use SNMP for centralized network management if your network has SNMP-compliant devices. You can also use SNMP for network monitoring via network management software.
Subsystem for UNIX-Based Applications (SUA)	Provides functionality for running UNIX-based programs. You can download additional management utilities from the Microsoft website. (Deprecated)
Telnet Client	Allows a computer to connect to a remote Telnet server and run applications on that server.
Telnet Server	Hosts the remote sessions for Telnet clients. When Telnet Server is running on a computer, users can connect to the server with a Telnet client from a remote computer.
User Interfaces And Infrastructure	Allows you to control the user experience and infrastructure options (Graphical Management Tools And Infrastructure, Desktop Experience, or Server Graphical Shell).
Windows Biometric Framework	Provides functionality required for using fingerprint devices.
Windows Internal Database	Allows the server to use relational databases with Windows roles and features that require an internal database, such as AD RMS, UDDI Services, WSUS, Windows SharePoint Services, and Windows System Resource Manager.
Windows PowerShell	Allows you to manage the Windows PowerShell features of the server. Windows PowerShell 3.0 and the PowerShell ISE are installed by default.
Windows PowerShell Web Access	Allows the server to act as a web gateway for remotely managing servers in a web browser.
Windows Process Activation Service	Provides support for distributed, web-based applications that use HTTP and non-HTTP protocols.
Windows Standards-Based Storage Management	Provides support for managing standards-based storage and includes management interfaces as well as extensions for WMI and Windows PowerShell.
Windows Server Backup	Allows you to back up and restore the operating system, system state, and any data stored on a server.
Windows System Resource Manager (WSRM)	Allows you to manage resource usage on a per-processor basis. (Deprecated)



FEATURE	DESCRIPTION
Windows TIFF IFilter	Focuses on text-based documents, which means that searching is more successful for documents that contain clearly identifiable text (for example, black text on a white background).
WinRM IIS Extension	Provides an Internet Information Services (IIS)-based hosting model. WinRM IIS Extension can be enabled at either the website or virtual-directory level.
WINS Server	A name-resolution service that resolves computer names to IP addresses. Installing this feature allows the computer to act as a WINS server.
Wireless LAN Service	Allows the server to use wireless networking connections and profiles.
WoW64 Support	Supports WoW64, which is required on a full-server installation. Removing this feature converts a full-server installation to a Server Core installation.
XPS Viewer	A program you can use to view, search, set permissions for, and digitally sign XPS documents.

**NOTE** Desktop Experience is now a subfeature of the top-level feature called User Interfaces And Infrastructure. Desktop Experience provides Windows desktop functionality on the server. Windows features added include Windows Media Player, desktop themes, Video for Windows (AVI support), Windows Defender, Disk Cleanup, Sync Center, Sound Recorder, Character Map, and Snipping Tool. Although these features allow a server to be used like a desktop computer, they can reduce the server's overall performance.

As an administrator, you might be asked to install or uninstall dynamic-link libraries (DLLs), particularly if you work with IT development teams. The utility you use to work with DLLs is Regsvr32. This utility is run at the command line.

After you open a Command Prompt window, you install or register a DLL by typing **regsvr32 name.dll**—for example:

```
regsvr32 mylibs.dll
```

If necessary, you can uninstall or unregister a DLL by typing **regsvr32 /u name.dll**—for example:

```
regsvr32 /u mylibs.dll
```

Windows File Protection prevents the replacement of protected system files. You can replace only DLLs installed by the Windows Server operating system as part of a hotfix, service pack update, Windows update, or Windows upgrade. Windows File Protection is an important part of the Windows Server security architecture.

## Full-Server, Minimal-Interface, and Server Core Installations

---

Windows Server 2012 supports full-server, minimal-interface, and Server Core installations. Full-server installations, also referred to as Server With A GUI Installations, have the Graphical Management Tools And Infrastructure and Server Graphical Shell features (which are part of the User And Infrastructure feature) and the WoW64 Support framework installed. Minimal-interface installations, also referred to as Server With Minimal Interface Installations, are full-server installations with the Server Graphical Shell removed. Server Core installations have a limited user interface and do not include any of the User Interfaces And Infrastructure features or the WoW64 Support framework.

As discussed in “Changing the Installation Type” later in the chapter, the installation type can be changed at any time. With a full-server installation, you have a complete working version of Windows Server 2012 you can deploy with any permitted combination of roles, role services, and features. With a minimal-interface installation, you also can deploy any permitted combination of roles, role services, and features. However, with a Server Core installation, you have a minimal installation of Windows Server 2012 that supports a limited set of roles and role combinations. The supported roles include AD CS, AD DS, AD LDS, DHCP Server, DNS Server, File Services, Hyper-V, Media Services, Print And Document Services, Routing And Remote Access Server, Streaming Media Services, Web Server (IIS), and Windows Server Update Server. In its current implementation, a Server Core installation is not a platform for running server applications.

While all three installation types use the same licensing rules and can be managed remotely using any available and permitted remote-administration technique, full-server, minimal-interface, and Server Core installations are completely different when it comes to local console administration. With a full-server installation, you’re provided with a user interface that includes a full desktop environment for local console management of the server. With a minimal interface, you have only Microsoft Management Consoles, Server Manager, and a subset of Control Panel available for management tasks. Missing from both a minimal-interface installation and a Server Core installation are File Explorer, taskbar, notification area, Internet Explorer, built-in help system, themes, Metro-style apps, and Windows Media Player.

### Navigating Server Core

With a Server Core installation, you get a user interface that includes a limited desktop environment for local console management of the server. This minimal interface includes the following:

- Windows Logon screen for logging on and logging off
- Notepad (Notepad.exe) for editing files
- Registry Editor (Regedit.exe) for managing the registry
- Task Manager (Taskmgr.exe) for managing tasks and starting new tasks
- Command prompt (Cmd.exe) for administration using the command line

- PowerShell prompt for administration using Windows PowerShell
- File Signature Verification tool (Sigverif.exe) for verifying digital signatures of system files
- System Information (Msinfo32.exe) for getting system information
- Windows Installer (Msiexec.exe) for managing Windows Installer
- Date And Time control panel (Timedate.cpl) for viewing or setting the date, time, and time zone.
- Region And Language control panel (Intl.cpl) for viewing or setting regional and language options, including formats and the keyboard layout.
- Server Configuration utility (Sconfig), which provides a text-based menu system for managing a server's configuration.

When you start a server with a Server Core installation, you can use the Windows Logon screen to log on just as you do with a full-server installation. In a domain, the standard restrictions apply for logging on to servers, and anyone with appropriate user rights and logon permissions can log on to the server. On servers that are not acting as domain controllers and for servers in workgroup environments, you can use the NET USER command to add users and the NET LOCALGROUP command to add users to local groups for the purposes of logging on locally.

After you log on to a Server Core installation, you have a limited desktop environment with an administrator command prompt. You can use this command prompt for administration of the server. If you accidentally close the command prompt, you can open a new command prompt by following these steps:

1. Press Ctrl+Shift+Esc to display Task Manager.
2. On the File menu, tap or click Run New Task.
3. In the Create New Task dialog box, type **cmd** in the Open text box, and then tap or click OK.

You can use this technique to open additional Command Prompt windows as well. Although you can work with Notepad and Regedit by typing **notepad.exe** or **regedit.exe** instead of **cmd**, you can also start Notepad and Regedit directly from a command prompt by entering **notepad.exe** or **regedit.exe** as appropriate.

The Server Configuration utility (Sconfig) provides a text-based menu system that makes it easy to do the following:

- Configure domain or workgroup membership
- Change a server's name
- Add a local Administrator account
- Configure remote management features
- Configure Windows Update settings
- Download and install Windows updates
- Enable or disable Remote Desktop
- Configure network settings for TCP/IP
- Configure the date and time
- Log off, restart, or shut down

When you are logged on, you can display the Windows Logon screen at any time by pressing Ctrl+Alt+Delete. In a Server Core installation, the Windows Logon screen has the same options as with a full-server installation, allowing you to lock the computer, switch users, log off, change a password, or start Task Manager. At the command prompt, you have all the standard commands and command-line utilities available for managing the server. However, commands, utilities, and programs run only if all of their dependencies are available in the Server Core installation.

Although a Server Core installation supports a limited set of roles and role services, you can install most features. Windows Server 2012 also supports the .NET Framework, Windows PowerShell 3.0, and Windows Remote Management (WinRM) 2.0. This support allows you to perform local and remote administration using PowerShell. You also can use Remote Desktop Services to manage a Server Core installation remotely. Some of the common tasks you might want to perform when you are logged on locally are summarized in Table 2-3.

**TABLE 2-3** Helpful Commands and Utilities for Managing Server Core Installations

COMMAND	TASK
Cscript Scregedit.wsf	Configure the operating system. Use the <i>/cli</i> parameter to list available configuration areas.
Diskraid.exe	Configure software RAID.
ipconfig /all	List information about the computer's IP address configuration.
Netdom RenameComputer	Set the server's name.
Netdom Join	Join the server to a domain.
Netsh	Provide multiple contexts for managing the configuration of networking components. Type <b>netsh interface ipv4</b> to configure IPv4 settings. Type <b>netsh interface ipv6</b> to configure IPv6 settings.
Ocsetup.exe	Add or remove roles, role services, and features.
Pnputil.exe	Install or update hardware device drivers.
Sc query type=driver	List installed device drivers.
Serverwerroptin.exe	Configure Windows Error Reporting.
Slmgr -ato	Windows Software Licensing Management tool used to activate the operating system. Runs <i>Cscript slmgr.vbs -ato</i> .
Slmgr -ipk	Install or replace the product key. Runs <i>Cscript slmgr.vbs -ipk</i> .

COMMAND	TASK
SystemInfo	List the system configuration details.
Wecutil.exe	Create and manage subscriptions to forwarded events.
Wevtutil.exe	View and search event logs.
Winrm quickconfig	Configure the server to accept WS-Management requests from other computers. Runs <i>Cscript winrm.vbs quickconfig</i> . Enter without the <i>quickconfig</i> parameter to see other options.
Wmic datafile where name="FullPath" get version	List a file's version.
Wmic nicconfig index=9 call enabledhcp	Set the computer to use dynamic IP addressing rather than static IP addressing.
Wmic nicconfig index=9 call enablestatic("IPAddress"), ("SubnetMask")	Set a computer's static IP address and network mask.
Wmic nicconfig index=9 call setgateways("GatewayIPAddress")	Set or change the default gateway.
Wmic product get name /value	List installed Microsoft Installer (MSI) applications by name.
Wmic product where name="Name" call uninstall	Uninstall an MSI application.
Wmic qfe list	List installed updates and hotfixes.
Wusa.exe PatchName.msu /quiet	Apply an update or hotfix to the operating system.

## Installing Windows Server 2012

You can install Windows Server 2012 on new hardware or as an upgrade. When you install Windows Server 2012 on a computer with an existing operating system, you can perform a clean installation or an upgrade. With a clean installation, the Windows Server 2012 Setup program replaces the original operating system on the computer, and all user or application settings are lost. With an upgrade, the Setup program performs a clean installation of the operating system and then migrates user settings, documents, and applications from the earlier version of Windows.

Windows Server 2012 supports only 64-bit architecture. You can install the operating system only on computers with 64-bit processors. Before you install Windows Server 2012, you should be sure that your computer meets the minimum

requirements of the edition you plan to use. Microsoft provides both minimum requirements and recommended requirements. If your computer doesn't meet the minimum requirements, you will not be able to install Windows Server 2012. If your computer doesn't meet the recommended requirements, you will experience performance issues.

Windows Server 2012 requires at least 10 GB of disk space for installation of the base operating system. Microsoft recommends that a computer running Windows Server 2012 have 32 GB or more of available disk space. Additional disk space is required for paging and dump files as well as for the features, roles, and role services you install. For optimal performance, you should have at least 10 percent of free space on a server's disks at all times.

When you install Windows Server 2012, the Setup program automatically makes recovery options available on your server as an advanced boot option. In addition to a command line for troubleshooting and options for changing the startup behavior, you can use System Image Recovery to perform a full recovery of the computer using a system image created previously. If other troubleshooting techniques fail to restore the computer and you have a system image for recovery, you can use this feature to restore the computer from the backup image.

## Performing a Clean Installation

Before you start an installation, you need to consider whether you want to manage the computer's drives and partitions during the setup process. If you want to use the advanced drive setup options that Setup provides for creating and formatting partitions, you need to boot the computer using the distribution media. If you don't boot using the distribution media, these options won't be available, and you'll only be able to manage disk partitions at a command prompt using the DiskPart utility.

You can perform a clean installation of Windows Server 2012 by following these steps:

1. Start the Setup program by using one of the following techniques:
  - For a new installation, turn on the computer with the Windows Server 2012 distribution media in the computer's disc drive, and then press any key when prompted to start Setup from your media. If you are not prompted to boot from the disc drive, you might need to select advanced boot options and then boot from media rather than hard disk, or you might need to change the computer's firmware settings to allow booting from media.
  - For a clean installation over an existing installation, you can boot from the distribution media, or you can start the computer and log on using an account with administrator privileges. When you insert the Windows Server 2012 distribution media into the computer's disc drive, Setup should start automatically. If Setup doesn't start automatically, use File Explorer to access the distribution media and then double-tap or double-click Setup.exe.
2. If you started the computer using the distribution media, choose your language, time and currency formats, and keyboard layout when prompted.

Only one keyboard layout is available during installation. If your keyboard language and the language edition of Windows Server 2012 you are installing are different, you might see unexpected characters as you type. Be sure that you select the correct keyboard language to avoid this. When you are ready to continue with the installation, tap or click Next.

3. Choose Install Now to start the installation. After Setup copies the temporary files to the computer, choose whether to get updates for Setup during the installation. If you started Setup after logging on to an existing installation of Windows, choose either Go Online To Install Updates Now or No, Thanks.
4. With volume and enterprise licensed editions of Windows Server 2012, you might not need to provide a product key during installation. With retail editions, however, you need to enter a product key when prompted. Tap or click Next to continue. The Activate Windows When I'm Online check box is selected by default to ensure that you are prompted to activate the operating system the next time you connect to the Internet.

**NOTE** You must activate Windows Server 2012 after installation. If you don't activate Windows Server 2012 in the allotted time, you see an error stating "Your activation period has expired" or that you have a "Non-genuine version of Windows Server 2012 installed." Windows Server 2012 will then run with reduced functionality. You need to activate and validate Windows Server 2012 as necessary to regain full functionality.

5. On the Select The Operating System You Want To Install page, options are provided for full-server and Server Core installations. Make the appropriate selection, and then tap or click Next.
6. The license terms for Windows Server 2012 have changed from previous releases of Windows. After you review the license terms, tap or click I Accept The License Terms, and then tap or click Next.
7. On the Which Type Of Installation Do You Want page, select the type of installation you want Setup to perform. Because you are performing a clean installation to replace an existing installation or configure a new computer, select Custom Install Windows Only (Advanced) as the installation type. If you started Setup from the boot prompt rather than from Windows itself, the Upgrade option is disabled. To upgrade rather than perform a clean install, you need to restart the computer and boot the currently installed operating system. After you log on, you then need to start the installation.
8. On the Where Do You Want To Install Windows page, select the disk or disk and partition on which you want to install the operating system. There are two versions of the Where Do You Want To Install Windows page, so you need to keep the following in mind:
  - When a computer has a single hard disk with a single partition encompassing the whole disk or a single area of unallocated space, the whole disk partition is selected by default, and you can tap or click Next to choose this as the install location and continue. With a disk that is completely unallocated, you might want to create the necessary partition

before installing the operating system, as discussed in “Creating, Formatting, Deleting, and Extending Disk Partitions During Installation” later in this chapter.

- When a computer has multiple disks or a single disk with multiple partitions, you need to select an existing partition to use for installing the operating system or create a partition. You can create and manage partitions as discussed in “Creating, Formatting, Deleting, and Extending Disk Partitions During Installation” later in this chapter.
  - If a disk has not been initialized for use or if the firmware of the computer does not support starting the operating system from the selected disk, you need to initialize it by creating one or more partitions on the disk. You cannot select or format a hard disk partition that uses FAT or FAT32 or has other incompatible settings. To work around this issue, you might want to convert the partition to NTFS. When working with this page, you can access a command prompt to perform any necessary preinstallation tasks. See “Creating, Formatting, Deleting, and Extending Disk Partitions During Installation” later in this chapter.
9. If the partition you select contains a previous Windows installation, Setup provides a prompt stating that existing user and application settings will be moved to a folder named `Windows.old` and that you must copy these settings to the new installation to use them. Tap or click OK.
  10. Tap or click Next. Setup starts the installation of the operating system. During this procedure, Setup copies the full disk image of Windows Server 2012 to the location you selected and then expands it. Afterward, Setup installs features based on the computer's configuration and the hardware it detects. This process requires several automatic restarts. When Setup finishes the installation, the operating system will be loaded, and you can perform initial configuration tasks such as setting the administrator password and server name.

**REAL WORLD** Servers running core installations of Windows Server are configured to use DHCP by default. As long as the server has a network card and a connected network cable, a Server Core installation should be able to connect to your organization's DHCP servers and obtain the correct network settings. You can configure the server by using `Sconfig`, which provides menu options for configuring domain/workgroup membership, the computer name, remote management, Windows Update, Remote Desktop, network settings, date and time, logoff, restart, and shutdown.

Alternatively, you can configure the server by using individual commands. If you want to use a static IP address, use `Netsh` to apply the settings you want. Once networking is configured correctly, use `Slmgr -ipk` to set the product key and `Slmgr -ato` to activate Windows. Enter `timedate.cpl` to set the server's date and time. If you want to enable remote management using the WS-Management protocol, enter `winrm quickconfig`.

Next, you'll probably want to set the name of the computer. To view the default computer name, enter `echo %computername%`. To rename the computer, use `Netdom RenameComputer` with the following syntax: `netdom renamecomputer currentname /newname:newname`, where *currentname* is the current name of the computer and



*newname* is the name you want to assign. An example is **netdom renamecomputer win-k4m6bnovlhe /newname:server18**. You'll need to restart the computer, and you can do this by entering **shutdown /r**.

When the computer restarts, you can join it to a domain by using Netdom Join. For the syntax, enter **netdom join /?**.

## Performing an Upgrade Installation

Although Windows Server 2012 provides an upgrade option during installation, an upgrade isn't what you think it is. With an upgrade, Setup performs a clean installation of the operating system and then migrates user settings, documents, and applications from the earlier version of Windows.

During the migration portion of the upgrade, Setup moves folders and files from the previous installation to a folder named Windows.old. As a result, the previous installation will no longer run.

**NOTE** You cannot perform an upgrade installation of Windows Server 2012 on a computer with a 32-bit operating system, even if the computer has 64-bit processors. You need to migrate the services being provided by the computer to other servers and then perform a clean installation. The Windows Server Migration tools might be able to help you migrate your server. These tools are available on computers running Windows Server 2012.

You can perform an upgrade installation of Windows Server 2012 by following these steps:

1. Start the computer, and log on using an account with administrator privileges. When you insert the Windows Server 2012 distribution media into the computer's DVD-ROM drive, Setup should start automatically. If Setup doesn't start automatically, use File Explorer to access the distribution media and then double-tap or double-click Setup.exe.
2. Because you are starting Setup from the current operating system, you are not prompted to choose your language, time and currency formats, or keyboard layout and only the current operating system's keyboard layout is available during installation. If your keyboard language and the language of the edition of Windows Server 2012 you are installing are different, you might see unexpected characters as you type.
3. Choose Install Now to start the installation. After Setup copies the temporary files to the computer, choose whether to get updates during the installation. Choose either Go Online To Install Updates Now or No, Thanks.
4. With volume and enterprise licensed editions of Windows Server 2012, you might not need to provide a product key during installation of the operating system. With retail editions, however, you are prompted to enter a product key. Tap or click Next to continue. The Automatically Activate Windows When I'm Online check box is selected by default to ensure that you are prompted to activate the operating system the next time you connect to the Internet.

5. On the Select The Operating System You Want To Install page, options are provided for full-server and Server Core installations. Make the appropriate selection, and then tap or click Next.
6. The license terms for Windows Server 2012 have changed from previous releases of Windows. After you review the license terms, tap or click I Accept The License Terms, and then tap or click Next.
7. On the Which Type Of Installation Do You Want page, you need to select the type of installation you want Setup to perform. Because you are performing a clean installation over an existing installation, select Upgrade. If you started Setup from the boot prompt rather than from Windows itself, the Upgrade option is disabled. To upgrade rather than perform a clean install, you need to restart the computer and boot the currently installed operating system. After you log on, you can start the installation.
8. Setup will then start the installation. Because you are upgrading the operating system, you do not need to choose an installation location. During this process, Setup copies the full disk image of Windows Server 2012 to the system disk. Afterward, Setup installs features based on the computer's configuration and the hardware it detects. When Setup finishes the installation, the operating system will be loaded, and you can perform initial configuration tasks such as setting the administrator password and server name.

## Performing Additional Administration Tasks During Installation

Sometimes you might forget to perform a preinstallation task prior to starting the installation. Rather than restarting the operating system, you can access a command prompt from Setup or use advanced drive options to perform the necessary administrative tasks.

### Using the Command Line During Installation

When you access a command prompt from Setup, you access the MINWINPC (mini Windows PC) environment used by Setup to install the operating system. During installation, on the Where Do You Want To Install Windows page, you can access a command prompt by pressing Shift+F10. As Table 2-4 shows, the mini Windows PC environment gives you access to many of the same command-line tools that are available in a standard installation of Windows Server 2012.

**TABLE 2-4** Command-Line Utilities in the Mini Windows PC Environment

COMMAND	DESCRIPTION
ARP	Displays and modifies the IP-to-physical address translation tables used by the Address Resolution Protocol (ARP).
ASSOC	Displays and modifies file extension associations.
ATTRIB	Displays and changes file attributes.

COMMAND	DESCRIPTION
CALL	Calls a script or script label as a procedure.
CD/CHDIR	Displays the name of or changes the current directory.
CHKDSK	Checks a disk for errors and displays a report.
CHKNTFS	Displays the status of volumes. Sets or excludes volumes from automatic system checking when the computer is started.
CHOICE	Creates a list from which users can select one of several choices in a batch script.
CLS	Clears the console window.
CMD	Starts a new instance of the Windows command shell.
COLOR	Sets the colors of the command-shell window.
CONVERT	Converts FAT volumes to NTFS.
COPY	Copies or combines files.
DATE	Displays or sets the system date.
DEL	Deletes one or more files.
DIR	Displays a list of files and subdirectories within a directory.
DISKPART	Invokes a text-mode command interpreter so that you can manage disks, partitions, and volumes using a separate command prompt and commands that are internal to DISKPART.
DISM	Services and manages Windows images.
DOSKEY	Edits command lines, recalls Windows commands, and creates macros.
ECHO	Displays messages or turns command echoing on or off.
ENDLOCAL	Ends localization of environment changes in a batch file.
ERASE	Deletes one or more files.
EXIT	Exits the command interpreter.
EXPAND	Uncompresses files.
FIND	Searches for a text string in files.
FOR	Runs a specified command for each file in a set of files.
FORMAT	Formats a floppy disk or hard drive.
FTP	Transfers files.
FTYPE	Displays or modifies file types used in file-extension associations.

COMMAND	DESCRIPTION
GOTO	Directs the Windows command interpreter to a labeled line in a script.
HOSTNAME	Prints the computer's name.
IF	Performs conditional processing in batch programs.
IPCONFIG	Displays TCP/IP configuration.
LABEL	Creates, changes, or deletes the volume label of a disk.
MD/MKDIR	Creates a directory or subdirectory.
MORE	Displays output one screen at a time.
MOUNTVOL	Manages a volume mount point.
MOVE	Moves files from one directory to another directory on the same drive.
NBTSTAT	Displays the status of NetBIOS.
NET ACCOUNTS	Manages user account and password policies.
NET COMPUTER	Adds or removes computers from a domain.
NET CONFIG SERVER	Displays or modifies the configuration of a server service.
NET CONFIG WORKSTATION	Displays or modifies the configuration of a workstation service.
NET CONTINUE	Resumes a paused service.
NET FILE	Displays or manages open files on a server.
NET GROUP	Displays or manages global groups.
NET LOCALGROUP	Displays or manages local group accounts.
NET NAME	Displays or modifies recipients for messenger service messages.
NET PAUSE	Suspends a service.
NET PRINT	Displays or manages print jobs and shared queues.
NET SEND	Sends a messenger service message.
NET SESSION	Lists or disconnects sessions.
NET SHARE	Displays or manages shared printers and directories.
NET START	Lists or starts network services.
NET STATISTICS	Displays workstation and server statistics.
NET STOP	Stops services.

COMMAND	DESCRIPTION
NET TIME	Displays or synchronizes network time.
NET USE	Displays or manages remote connections.
NET USER	Displays or manages local user accounts.
NET VIEW	Displays network resources or computers.
NETSH	Invokes a separate command prompt that allows you to manage the configuration of various network services on local and remote computers.
NETSTAT	Displays the status of network connections.
PATH	Displays or sets a search path for executable files in the current command window.
PATHPING	Traces routes, and provides packet-loss information.
PAUSE	Suspends the processing of a script, and waits for keyboard input.
PING	Determines whether a network connection can be established.
POPD	Changes to the directory stored by PUSH.D.
PRINT	Prints a text file.
PROMPT	Modifies the Windows command prompt.
PUSH.D	Saves the current directory and then changes to a new directory.
RD/RMDIR	Removes a directory.
RECOVER	Recovers readable information from a bad or defective disk.
REG ADD	Adds a new subkey or entry to the registry.
REG COMPARE	Compares registry subkeys or entries.
REG COPY	Copies a registry entry to a specified key path on a local or remote system.
REG DELETE	Deletes a subkey or entries from the registry.
REG QUERY	Lists the entries under a key and the names of subkeys (if any).
REG RESTORE	Writes saved subkeys and entries back to the registry.
REG SAVE	Saves a copy of specified subkeys, entries, and values to a file.
REGSVR32	Registers and unregisters DLLs.
REM	Adds comments to scripts.
REN	Renames a file.

COMMAND	DESCRIPTION
ROUTE	Manages network routing tables.
SET	Displays or modifies Windows environment variables. Also used to evaluate numeric expressions at the command line.
SETLOCAL	Begins the localization of environment changes in a batch file.
SFC	Scans and verifies protected system files.
SHIFT	Shifts the position of replaceable parameters in scripts.
START	Starts a new command-shell window to run a specified program or command.
SUBST	Maps a path to a drive letter.
TIME	Displays or sets the system time.
TITLE	Sets the title for the command-shell window.
TRACERT	Displays the path between computers.
TYPE	Displays the contents of a text file.
VER	Displays the Windows version.
VERIFY	Tells Windows whether to verify that your files are written correctly to a disk.
VOL	Displays a disk volume label and serial number.

## Forcing Disk Partition Removal During Installation

During installation, you might be unable to select the hard disk you want to use. This issue can arise if the hard-disk partition contains an invalid byte offset value. To resolve this issue, you need to remove the partitions on the hard disk (which destroys all associated data) and then create the necessary partition using the advanced options in the Setup program. During installation, on the Where Do You Want To Install Windows page, you can remove unrecognized hard-disk partitions by following these steps:

1. Press Shift+F10 to open a command prompt.
2. At the command prompt, type **diskpart**. This starts the DiskPart utility.
3. To view a list of disks on the computer, type **list disk**.
4. Select a disk by typing **select disk *DiskNumber***, where *DiskNumber* is the number of the disk you want to work with.
5. To permanently remove the partitions on the selected disk, type **clean**.
6. When the cleaning process is finished, type **exit** to exit the DiskPart utility.
7. Type **exit** to exit the command prompt.
8. In the Install Windows dialog box, tap or click the back arrow button to return to the previous window.

9. On the Which Type Of Installation Do You Want page, tap or click Custom (Advanced) to start a custom install.
10. On the Where Do You Want To Install Windows page, tap or click the disk you previously cleaned to select it as the installation partition. As necessary, tap or click the Disk Options link to display the Delete, Format, New, and Extend partition configuration options.
11. Tap or click New. In the Size box, set the size of the partition in megabytes, and then tap or click Apply.

## Loading Disk Device Drivers During Installation

During installation, on the Where Do You Want To Install Windows page, you can use the Load Driver option to load the device drivers for a hard-disk drive or a hard-disk controller. Typically, you use this option when a disk drive you want to use for installing the operating system isn't available for selection because the device drivers aren't available.

To load the device drivers and make the hard disk available, follow these steps:

1. During installation, on the Where Do You Want To Install Windows page, tap or click Load Driver.
2. When prompted, insert the installation media into a DVD drive or USB flash drive, and then tap or click OK. Setup then searches the computer's removable media drives for the device drivers.
  - If Setup finds multiple device drivers, select the driver to install and then tap or click Next.
  - If Setup doesn't find the device driver, tap or click Browse to use the Browse For Folder dialog box to select the device driver to load, tap or click OK, and then tap or click Next.

You can tap or click the Rescan button to have Setup rescan the computer's removable media drives for the device drivers. If you are unable to install a device driver successfully, tap or click the back arrow button in the upper-left corner of the Install Windows dialog box to go back to the previous page.

## Creating, Formatting, Deleting, and Extending Disk Partitions During Installation

When you are performing a clean installation and have started the computer from the distribution media, the Where Do You Want To Install Windows page has additional options. You can display these options by tapping or clicking Drive Options (Advanced). These additional options are used as follows:

- **New** Creates a partition. You must then format the partition.
- **Format** Formats a new partition so that you can use it for installing the operating system.
- **Delete** Deletes a partition that is no longer wanted.
- **Extend** Extends a partition to increase its size.

The sections that follow discuss how to use each of these options. If these options aren't available, you can still work with the computer's disks. On the Where Do You Want To Install Windows page, press Shift+F10 to open a command prompt. At the command prompt, type **diskpart** to start the DiskPart utility.

## CREATING DISK PARTITIONS DURING INSTALLATION

Creating a partition allows you to set the partition's size. Because you can create new partitions only in areas of unallocated space on a disk, you might need to delete existing partitions to be able to create a partition of the size you want. Once you create a partition, you can format the partition so that you can use it to install a file system. If you don't format a partition, you can still use it for installing the operating system. In this case, Setup formats the partition when you continue installing the operating system.

You can create a new partition by following these steps:

1. During installation, on the Where Do You Want To Install Windows page, tap or click Drive Options (Advanced) to display the advanced options for working with drives.
2. Tap or click the disk on which you want to create the partition, and then tap or click New.
3. In the Size box, set the size of the partition in megabytes and then tap or click Apply to have Setup create a partition on the selected disk.

After you create a partition, you need to format the partition to continue with the installation.

## FORMATTING DISK PARTITIONS DURING INSTALLATION

Formatting a partition creates a file system on the partition. When formatting is complete, you have a formatted partition on which you can install the operating system. Keep in mind that formatting a partition destroys all data on the partition. You should format existing partitions (rather than ones you just created) only when you want to remove an existing partition and all its contents so that you can start the installation from a freshly formatted partition.

You can format a partition by following these steps:

1. During installation, on the Where Do You Want To Install Windows page, tap or click Drive Options (Advanced) to display the advanced options for working with drives.
2. Tap or click the partition that you want to format.
3. Tap or click Format. When prompted to confirm that you want to format the partition, tap or click OK. Setup then formats the partition.

## DELETING DISK PARTITIONS DURING INSTALLATION

Deleting a partition removes a partition you no longer want or need. When Setup finishes deleting the partition, the disk space previously allocated to the partition becomes unallocated space on the disk. Deleting the partition destroys all data on



the partition. Typically, you need to delete a partition only when it is in the wrong format or when you want to combine areas of free space on a disk.

You can delete a partition by following these steps:

1. During installation, on the Where Do You Want To Install Windows page, tap or click Drive Options (Advanced) to display the advanced options for working with drives.
2. Tap or click the partition you want to delete.
3. Tap or click Delete. When prompted to confirm that you want to delete the partition, tap or click OK. Setup then deletes the partition.

## EXTENDING DISK PARTITIONS DURING INSTALLATION

Windows Server 2012 requires at least 10 GB of disk space for installation, and at least 32 GB of available disk space is recommended. If an existing partition is too small, you won't be able to use it to install the operating system. To resolve this, you can extend a partition to increase its size by using areas of unallocated space on the current disk. You can extend a partition with an existing file system only if it is formatted with NTFS 5.2 or later. New partitions created in Setup can be extended as well, provided that the disk on which you create the partition has unallocated space.

You can extend a partition by following these steps:

1. During installation, on the Where Do You Want To Install Windows page, tap or click Drive Options (Advanced) to display the advanced options for working with drives.
2. Tap or click the partition you want to extend.
3. Tap or click Extend. In the Size box, set the size of the partition in megabytes and then tap or click Apply to extend the selected partition.
4. When prompted to confirm that you want to extend the partition, tap or click OK. Setup then extends the partition.

## Changing the Installation Type

Unlike earlier releases of Windows Server, you can change the installation type of any server running Windows Server 2012. This is possible because a key difference between the installation types relates to whether the installation has the following User Interfaces and Infrastructure features:

- Graphical Management Tools And Infrastructure
- Desktop Experience
- Server Graphical Shell

Full-server installations have both the Graphical Management Tools And Infrastructure feature and the Server Graphical Shell feature. They also might have Desktop Experience. On the other hand, minimal-interface installations have only the Graphical Management Tools And Infrastructure feature and Server Core installations have none of these features.

Knowing that Windows also automatically installs or uninstalls dependent features, server roles, and management tools to match the installation type, you can convert from one installation type to another simply by adding or removing the appropriate User Interfaces and Infrastructure features.

## Converting Full-Server and Minimal-Interface Installations

To convert a full-server installation to a minimal-interface installation, you remove the Server Graphical Shell. Although you can use the Remove Roles And Features Wizard to do this, you also can do this at a PowerShell prompt by entering the following command:

```
uninstall-windowsfeature server-gui-shell -restart
```

This command instructs Windows Server to uninstall the Server Graphical Shell and restart the server to finalize the removal. If Desktop Experience also is installed, this feature will be removed as well.

**TIP** As a best practice before you run this or any other command that might have far-reaching effects, you should run the command with the *-Whatif* parameter. This parameter tells Windows PowerShell to confirm exactly what will happen when a command is run.

To convert a minimal-interface installation to a full-server installation, you add the Server Graphical Shell. You can use the Add Roles And Features Wizard to do this, or you can enter the following command at a PowerShell prompt:

```
install-windowsfeature server-gui-shell -restart
```

This command instructs Windows Server to install the Server Graphical Shell and restart the server to finalize the installation. If you also want to install the Desktop Experience, you can use this command instead:

```
install-windowsfeature server-gui-shell, desktop-experience -restart
```

## Converting Server Core Installations

To convert a full-server or minimal-interface installation to a Server Core installation, you remove the user interfaces for Graphical Management Tools And Infrastructure. If you remove the WoW64 Support framework, you also convert the server to a Server Core installation. Although you can use the Remove Roles And Features Wizard to remove the user interfaces, you also can do this at a PowerShell prompt by entering the following command:

```
uninstall-windowsfeature server-gui-mgmt-infra -restart
```

This command instructs Windows Server to uninstall the user interfaces for Graphical Management Tools And Infrastructure and restart the server to finalize the removal. Because many dependent roles, role services, and features might be uninstalled along with the user interfaces, run the command with the *-Whatif* parameter first to get details on what exactly will be uninstalled.

If you installed the server with the user interfaces and converted it to a Server Core installation, you can revert back to a full-server installation with the following command:

```
install-windowsfeature server-gui-mgmt-infra -restart
```

As long as the binaries for this feature and any dependent features haven't been removed, the command should succeed. If the binaries were removed, however, or Server Core was the original installation type, you need to specify a source for the required binaries.

You use the `-Source` parameter to restore required binaries from a Windows Imaging (WIM) mount point. For example, if your enterprise has a mounted Windows Image for the edition of Windows Server 2012 you are working with available at the network path `\\ImServer18\WinS12EE`, you could specify the source as follows:

```
install-windowsfeature server-gui-mgmt-infra -source \\imserver18\wins12ee
```

While many large enterprises might have standard images that can be mounted using network paths, you also can mount the Windows Server 2012 distribution media and then use the `Windows\WinSxS` folder from the installation image as your source. To do this, follow these steps:

1. Insert the installation disc into the server's disc drive, and then create a folder to mount the Installation image by entering the following command: **`mkdir c:\mountdir`**.
2. Locate the index number of the image you want to use by entering the following command at an elevated prompt: **`dism /get-wiminfo /wimfile:e:\sources\install.wim`**, where `e:` is the drive designator of the server's disc drive.
3. Mount the installation image by entering the following command at an elevated prompt: **`dism /mount-wim /wimfile:e:\sources\install.wim /index:2 /mountdir:c:\mountdir /readonly`**, where `e:` is the drive designator of the server's disc drive, `2` is the index of the image to use, and `c:\mountdir` is the mount directory. Mounting the image might take several minutes.
4. Use `Install-WindowsFeature` at a PowerShell prompt with the source specified as **`c:\mountdir\windows\winsxs`**, as shown in this example:

```
install-windowsfeature server-gui-mgmt-infra  
-source c:\mountdir\windows\winsxs
```

## Managing Roles, Role Services, and Features

---

When you want to manage server configurations, you'll primarily use Server Manager to manage roles, role services, and features. Not only can you use Server Manager to add or remove roles, role services, and features, but you can also use Server Manager to view the configuration details and status for these software components.

## Performing Initial Configuration Tasks

Server Manager is your central management console for the initial setup and configuration of roles and features. Not only can Server Manager help you quickly set up a new server, the console also can help you quickly set up your management environment.

Normally, Windows Server 2012 automatically starts Server Manager whenever you log on and you can access Server Manager on the desktop. If you don't want the console to start each time you log on, tap or click **Manage** and then tap or click **Server Manager Properties**. In the **Server Manager Properties** dialog box, select **Do Not Start Server Manager Automatically At Logon** and then tap or click **OK**.

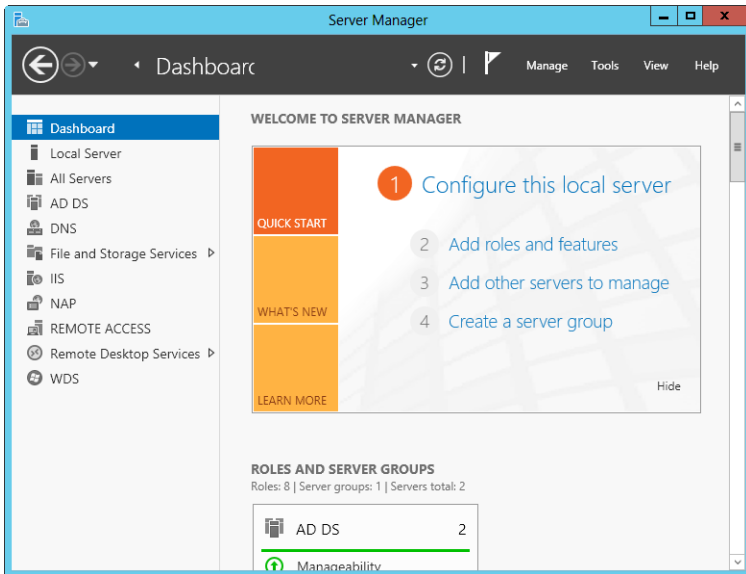
**NOTE** Group Policy can be used to control automatic start of Server Manager as well. Enable or disable the **Do Not Display Server Manager Automatically At Logon** policy setting within **Computer Configuration\Administrative Templates\System\Server Manager**.

As Figure 2-1 shows, Server Manager's default view is the dashboard. The dashboard has quick links for adding roles and features to local and remote servers, adding servers to manage, and creating server groups. You'll find similar options are on the **Manage** menu:

- **Add Roles And Features** Starts the **Add Roles And Features Wizard**, which you can use to install roles, role services, and features on the server.
- **Add Other Servers To Manage** Opens the **Add Servers** dialog box, which you can use to add servers you want to manage. Added servers are listed when you select the **All Servers** node. Press and hold or right-click a server in the **Servers** pane of the **All Servers** node to display a list of management options, including **Restart Server**, **Manage As**, and **Remove Server**.
- **Create Server Group** Opens the **Create Server Group** dialog box, which you can use to add servers to server groups for easier management. Server Manager creates role-based groups automatically. For example, domain controllers are listed under **AD DS**, and you can quickly find information about any domain controllers by selecting the related node.

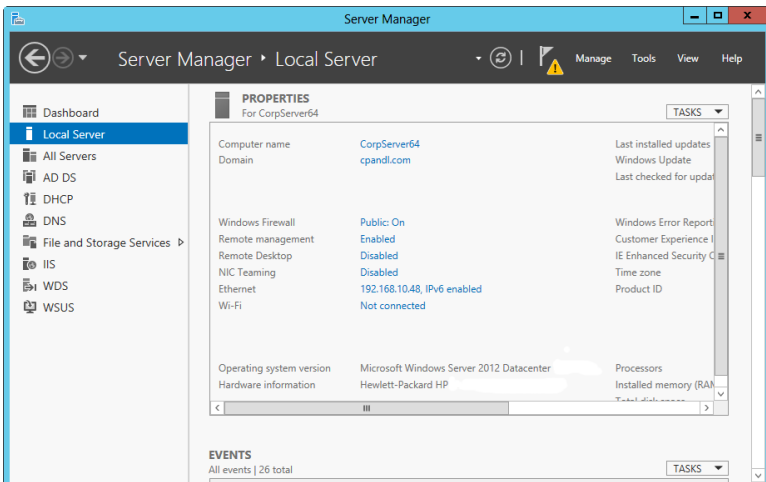
**TIP** When you need to connect to a server using alternate credentials, press and hold or right-click a server in the **All Servers** node and then select **Manage As**. In the **Windows Security** dialog box, enter your alternate credentials and then tap or click **OK**. Credentials you provide are cleared when you exit Server Manager. To save the credentials and use them each time you log on, select **Remember My Credentials** in the **Windows Security** dialog box. You need to repeat this procedure any time you change the password associated with the alternate credentials.

**REAL WORLD** When you are working with Server Core installations, you can use **Sconfig** to configure domain and workgroup membership, the computer's name, remote management, Windows Update, Remote Desktop, network settings, and the date and time. You also can use **Sconfig** to log off, restart, and shut down the server. To start **Sconfig**, simply enter **sconfig** at the command prompt. You can then choose menu options and follow the prompts to configure the server.



**FIGURE 2-1** Use the dashboard for general administration.

In Server Manager's left pane (also referred to as the *console tree*), you'll find options for accessing the dashboard, the local server, all servers added for management, and server groups. When you select **Local Server** in the console tree, as shown in Figure 2-2, you can manage the basic configuration of the server you are logged on to locally.



**FIGURE 2-2** Manage the properties of the local server.

Information about the local server is organized into several main headings, each with an associated management panel:

- **Best Practices Analyzer** Allows you to run the Best Practices Analyzer on the server and review the results. To start a scan, tap or click Tasks and then tap or click Start BPA Scan.
- **Events** Provides summary information about warning and error events from the server's event logs. Tap or click an event to display more information about the event.
- **Performance** Allows you to configure and view the status of performance alerts for CPU and memory usage. To configure performance alerts, tap or click Tasks and then tap or click Configure Performance Alerts.
- **Properties** Shows the computer name, domain, network IP configuration, time zone, and more. Each property can be clicked to quickly display a related management interface.
- **Roles And Features** Lists the roles and features installed on the server, in the approximate order of installation. To remove a role or feature, press and hold or right-click it and then select Remove Role Or Feature.
- **Services** Lists the services running on the server by name, status and start type. Press and hold or right-click a service to manage its run status.

The Properties panel is where you perform much of your initial server configuration. Properties available for quick management include the following:

- **Computer Name/Domain** Shows the computer name and domain. Tap or click either of the related links to display the System Properties dialog box with the Computer Name tab selected. You can then change a computer's name and domain information by tapping or clicking Change, providing the computer name and domain information, and then tapping or clicking OK. By default, servers are assigned a randomly generated name and are configured as part of a workgroup called WORKGROUP. In the Small Icons or Large Icons view of Control Panel, you can display the System Properties dialog box with the Computer Name tab selected by tapping or clicking System and then tapping or clicking Change Settings under Computer Name, Domain, And Workgroup Settings.
- **Customer Experience Improvement Program** Shows whether the server is participating in the Customer Experience Improvement Program (CEIP). Tap or click the related link to change the participation settings. Participation in CEIP allows Microsoft to collect information about the way you use the server. Microsoft collects this data to help improve future releases of Windows. No data collected as part of CEIP personally identifies you or your company. If you elect to participate, you can also provide information about the number of servers and desktop computers in your organization, as well as your organization's general industry. If you opt out of CEIP by turning this feature off, you miss the opportunity to help improve Windows.
- **Ethernet** Shows the TCP/IP configuration of wired Ethernet connections. Tap or click the related link to display the Network Connections console.

You can then configure network connections by double-tapping or double-clicking the connection you want to work with and then tapping or clicking Properties to open the Properties dialog box. By default, servers are configured to use dynamic addressing for both IPv4 and IPv6. You can also display the Network Connections console by tapping or clicking Change Adapter Settings under Tasks in Network And Sharing Center.

- **IE Enhanced Security Configuration** Shows the status of Internet Explorer Enhanced Security Configuration (IE ESC). Tap or click the related link to enable or disable IE ESC. If you tap or click the link for this option, you can turn this feature on or off for administrators, users, or both. IE ESC is a security feature that reduces the exposure of a server to potential attacks by raising the default security levels in Internet Explorer security zones and changing default Internet Explorer settings. By default, IE ESC is enabled for both administrators and users.

**REAL WORLD** In most cases, you should enable IE ESC on a server for both users and administrators. However, enabling IE ESC reduces the functionality of Internet Explorer. When IE ESC is enabled, security zones are configured as follows: the Internet zone is set to Medium-High, the Trusted Sites zone is set to Medium, the Local Intranet zone is set to Medium-Low, and the Restricted zone is set to High. When IE ESC is enabled, the following Internet settings are changed: the Enhanced Security Configuration dialog box is on, third-party browser extensions are off, sounds in web pages are off, animations in web pages are off, signature checking for downloaded programs is on, server certificate revocation is on, encrypted pages are not saved, temporary Internet files are deleted when the browser is closed, warnings for secure and nonsecure mode changes are on, and memory protection is on.

- **NIC Teaming** Shows the status and configuration of NIC teaming. Tap or click the related link to add or remove teamed interfaces and to manage related options.
- **Product ID** Shows the product identifier for Windows Server. Tap or click the related link to enter a product key and activate the operating system over the Internet.
- **Remote Desktop** Tap or click the related link to display the System Properties dialog box with the Remote tab selected. You can then configure Remote Desktop by selecting the configuration option you want to use and tapping or clicking OK. By default, no remote connections to a server are allowed. In the Small Icons or Large Icons view of Control Panel, you can display the System Properties dialog box with the Remote tab selected by double-tapping or double-clicking System and then tapping or clicking Remote Settings in the left pane.
- **Remote Management** Shows whether remote management of this server from other servers is enabled. Tap or click the related link to enable or disable remote management.

- **Time Zone** Shows the current time zone for the server. Tap or click the related link to display the Date And Time dialog box. You can then configure the server's time zone by tapping or clicking Change Time Zone, selecting the appropriate time zone, and then tapping or clicking OK twice. You can also display the Date And Time dialog box by pressing and holding or right-clicking the clock on the taskbar and then selecting Adjust Date/Time. Although all servers are configured to synchronize time automatically with an Internet time server, the time synchronization process does not change a computer's time zone.
- **Windows Error Reporting** Shows the status of Windows Error Reporting (WER). Tap or click the related link to change the participation settings for WER. In most cases, you'll want to enable WER for at least the first 60 days following installation of the operating system. With WER enabled, your server sends descriptions of problems to Microsoft, and Windows notifies you of possible solutions to those problems. You can view problem reports and possible solutions using Action Center. To open Action Center, tap or click the Action Center icon in the notification area of the taskbar and then select Open Action Center.
- **Windows Firewall** Shows the status of Windows Firewall. If Windows Firewall is active, this property displays the name of the firewall profile that currently applies and the firewall status. Tap or click the related link to display the Windows Firewall utility. By default, Windows Firewall is enabled. In the Small Icons or Large Icons view of Control Panel, you can display Windows Firewall by tapping or clicking the Windows Firewall option.
- **Windows Update** Shows the current configuration of Windows Update. Tap or click the related link to display the Windows Update utility in Control Panel, which you can then use to enable automatic updating (if Windows Update is disabled) or to check for updates (if Windows Update is enabled). In the Small Icons or Large Icons view of Control Panel, you can display Windows Update by selecting the Windows Update option.

**NOTE** I've provided this summary of options as an introduction and quick reference. I'll discuss the related configuration tasks and technologies in more detail throughout this and other chapters in the book.

## Server Manager Essentials and Binaries

The Server Manager console is designed to handle core system administration tasks. You'll spend a lot of time working with this tool, and you should get to know every detail. By default, Server Manager is started automatically. If you closed the console or disabled automatic startup, you can open the console by tapping or clicking the related option on the taskbar. Alternatively, another way to do this is by pressing the Windows key, typing **ServerManager.exe** into the Apps Search box, and then pressing Enter.

Server Manager's command-line counterpart is the ServerManager module for Windows PowerShell. When you are logged on to Windows Server 2012, this module is imported into Windows PowerShell by default. Otherwise, you need to import



the module before you can use the cmdlets it provides. You import the Server-Manager module by entering **Import-Module ServerManager** at the Windows PowerShell prompt. Once the module is imported, you can use it with the currently running instance of Windows PowerShell. The next time you start Windows PowerShell, you need to import the module again if you want to use its features.

At a Windows PowerShell prompt, you can obtain a detailed list of a server's current state with regard to roles, role services, and features by typing **get-windowsfeature**. Each installed role, role service, and feature is highlighted and marked as such, and a management naming component in brackets follows the display name of each role, role service, and feature. By using **Install-Windows-Feature** or **Uninstall-WindowsFeature** followed by the management name, you can install or uninstall a role, role service, or feature. For example, you can install Network Load Balancing by entering **install-windowsfeature nlb**. You can add **-includeallsubfeature** when installing components to add all subordinate role services or features. Management tools are not included by default. To add the management tools, add **-includemanagementtools** when installing components.

Binaries needed to install roles and features are referred to as *payloads*. With Windows Server 2012, payloads are stored in subfolders of the %SystemDrive%\Windows\WinSxS folder. Not only can you uninstall a role or feature, but you also can uninstall and remove the payload for a feature or role using the **-Remove** parameter of the **Uninstall-WindowsFeature** cmdlet. Subcomponents of the role or feature are removed as well. To also remove management tools, add the **-includeallmanagementtools** parameter.

When you want to install a role or feature, you can install the related components and restore any removed payloads for these components using the **Install-WindowsFeature** cmdlet. By default, when you use **Install-WindowsFeature**, payloads are restored via Windows Update.

In the following example, you restore the AD DS binaries and all related subfeatures via Windows Update:

```
install-windowsfeature -name ad-domain-services -includeallsubfeature
```

You can use the **-Source** parameter to restore a payload from a Windows Imaging (WIM) mount point. For example, if your enterprise has a mounted Windows Image for the edition of Windows Server 2012 you are working with available at the network path \\ImServer18\WinS12EE, you could specify the source as follows:

```
install-windowsfeature -name ad-domain-services -includeallsubfeature  
-source \\imserver18\wins12ee
```

Keep in mind that the path you specify is only used if required binaries are not found in the Windows Side-By-Side folder on the destination server. While many large enterprises might have standard images that can be mounted using network paths, you also can mount the Windows Server 2012 distribution media and use the Windows\WinSxS folder from the installation image as your source. To do this, follow these steps:

1. Insert the installation disc into the server's disc drive, and then create a folder to mount the Installation image by entering the following command: **mkdir c:\mountdir**.

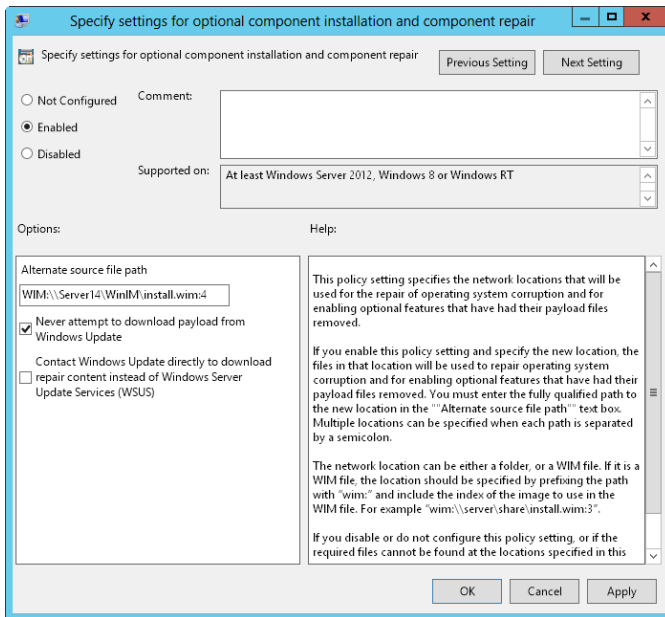
2. Locate the index number of the image you want to use by entering the following command at an elevated prompt: **dism /get-wiminfo /wimfile:e:\sources\install.wim**, where *e*: is the drive designator of the server's disc drive.
3. Mount the installation image by entering the following command at an elevated prompt: **dism /mount-wim /wimfile:e:\sources\install.wim /index:2 /mountdir:c:\mountdir /readonly**, where *e*: is the drive designator of the server's disc drive, 2 is the index of the image to use, and *c:\mountdir* is the mount directory. Mounting the image might take several minutes.
4. Use Install-WindowsFeature at a PowerShell prompt with the source specified as **c:\mountdir\windows\winsxs**, as shown in this example:

```
install-windowsfeature -name ad-domain-services -includeallsubfeature  
-source c:\mountdir\windows\winsxs
```

Group Policy can be used to control whether Windows Update is used to restore payloads and to provide alternate source paths for restoring payloads. The policy you want to work with is Specify Settings For Optional Component Installation And Component Repair, which is under Computer Configuration\Administrative Templates\System. This policy also is used for obtaining payloads needed to repair components.

If you enable this policy (as shown in Figure 2-3), you can do the following:

- Specify the alternate source file path for payloads as a network location. For network shares, enter the UNC path to the share, such as `\\CorpServer82\WinServer2012\`. For mounted Windows images, enter the WIM path prefixed with **WIM:** and including the index of the image to use, such as `WIM:\\CorpServer82\WinServer2012\install.wim:4`.
- Specify that Windows Update should never be used to download payloads. If you enable the policy and use this option, you do not have to specify an alternate path. In this case, payloads cannot be obtained automatically and administrators will need to explicitly specify the alternate source path.
- Specify that Windows Update should be used for repairing components rather than Windows Server Update Services.



**FIGURE 2-3** Control component installation through Group Policy.

## Managing Your Servers Remotely

You can use Server Manager and other Microsoft Management Consoles (MMCs) to perform some management tasks on remote computers, as long as the computers are in the same domain or you are working in a workgroup and have added the remote computers in a domain as trusted hosts. You can connect to servers running full-server, minimal-interface, and Server Core installations. On the computer you want to use for managing remote computers, you should be running either Windows Server 2012 or Windows 8 and you need to install the Remote Server Administration Tools.

With Windows Server 2012, the Remote Server Administration Tools are installed as a feature using the Add Roles And Features Wizard. If the binaries for the tools have been removed, you need to install the tools by specifying a source, as discussed in “Server Manager Essentials and Binaries” earlier in the chapter.

You can get the Remote Server Administration Tools for Windows 8 as a download from the Microsoft Download Center (<http://download.microsoft.com>). Different versions are available for x64 and x86 systems.

By default, remote management is enabled for servers running Windows Server 2012 for two types of applications and commands:

- Applications and commands that use Windows Remote Management (WinRM) and Windows PowerShell remote access for management

- Applications and commands that use Windows Management Instrumentation (WMI) and Distributed Component Object Model (DCOM) remote access for management

These types of applications and commands are permitted for remote management because of exceptions configured in Windows Firewall, which is enabled by default for Windows Server 2012. In Windows Firewall, exceptions for allowed apps that support remote management include the following:

- Windows Management Instrumentation
- Windows Remote Management
- Windows Remote Management (Compatibility)

In Windows Firewall With Advanced Security, there are inbound rules that correspond to the standard firewall allowed apps:

- For WMI, the inbound rules are Windows Management Instrumentation (WMI-In), Windows Management Instrumentation (DCOM-In), and Windows Management Instrumentation (ASync-In).
- For WinRM, the matching inbound rule is Windows Remote Management (HTTP-In).
- For WinRM compatibility, the matching inbound rule is Windows Remote Management - Compatibility Mode (HTTP-In).

You manage these exceptions or rules in either the standard Windows Firewall or in Windows Firewall With Advanced Security, not both. If you want to allow remote management using Server Manager, MMCs, and Windows PowerShell, you typically want to permit WMI, WinRM, and WinRM compatibility exceptions in Windows Firewall.

When you are working with Server Manager, you can select Local Server in the console tree to view the status of the remote management property. If you don't want to allow remote management of the local server, click the related link. In the Configure Remote Management dialog box, clear Enable Remote Management Of This Server From Other Computers and then tap or click OK.

When you clear Enable Remote Management Of This Server From Other Computers and then tap or click OK, Server Manager performs several background tasks that disable Windows Remote Management (WinRM) and Windows PowerShell remote access for management on the local server. One of these tasks is to turn off the related exception that allows apps to communicate through Windows Firewall using Windows Remote Management. The exceptions for Windows Management Instrumentation and Windows Remote Management (Compatibility) aren't affected.

You must be a member of the Administrators group on computers you want to manage by using Server Manager. For remote connections in a workgroup-to-workgroup or workgroup-to-domain configuration, you should be logged on using the built-in Administrator account or configure the *LocalAccountTokenFilterPolicy* registry key to allow remote access from your computer. To set this key, enter the following command at an elevated, administrator command prompt:

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

**NOTE** You also can enable remote management by entering **configure-SMRemoteing.exe –enable** at an elevated, administrator prompt.

**NOTE** If you want to make it possible to remotely manage a computer running Windows 8 using the WS-Management protocol, enter **winrm quickconfig** at an elevated prompt. Then each time you are prompted to make configuration changes, enter **Y**. This will start the Windows Remote Management (WinRM) service, configure WinRM to accept WS-Management requests on any IP address, create a Windows Firewall exception for Windows Remote Management, and configure *LocalAccountTokenFilterPolicy* to grant appropriate administrative rights for remote management.

Many other types of remote management tasks depend on other exceptions for Windows Firewall. Keep the following in mind:

- Remote Desktop is enabled or disabled separately from remote management. To allow someone to connect to the local server using Remote Desktop, you must allow related connections to the computer and configure access as discussed in Chapter 4, “Automating Administrative Tasks, Policies, and Procedures.”
- Remote Service Management must be configured as an allowed app in Windows Firewall to remotely manage a computer’s services. In the advanced firewall, there are several related rules that allow management via Named Pipes (NP) and Remote Procedure Calls (RPC).
- Remote Event Log Management must be configured as an allowed app in Windows Firewall to remotely manage a computer’s event logs. In the advanced firewall, there are several related rules that allow management via NP and RPC.
- Remote Volume Management must be configured as an allowed app in Windows Firewall to remotely manage a computer’s volumes. In the advanced firewall, there are several related rules that allow management of the Virtual Disk Service and Virtual Disk Service Loader.
- Remote Scheduled Task Management must be configured as an allowed app in Windows Firewall to remotely manage a computer’s scheduled tasks. In the advanced firewall, there are several related rules that allow management of scheduled tasks via RPC.

Only Remote Service Management is enabled by default.

You can configure remote management on a Server Core installation of Windows Server 2012 using Sconfig. Start the Server Configuration utility by entering **sconfig**.

## Connecting to and Working with Remote Servers

Using Server Manager, you can connect to and manage remote servers, provided that you’ve added the server for management. To add servers one at a time to Server Manager, complete these steps:

1. Open Server Manager. In the left pane, select All Servers to view the servers that have been added for management already. If the server you want to

work with isn't listed, select **Add Servers** on the **Manage** menu to display the **Add Servers** dialog box.

2. The **Add Servers** dialog box has several panels for adding servers:
  - The **Active Directory** panel, selected by default, allows you to enter the computer name or fully qualified domain name of the remote server that is running Windows Server. After you enter a name, tap or click **Find Now**.
  - The **DNS** panel allows you to add servers by computer name or IP address. After you enter the name or IP address, tap or click the **Search** button.
3. In the **Name** list, double-tap or double-click the server to add it to the **Selected** list.
4. Repeat steps 2 and 3 to add others servers. Tap or click **OK**.

To add many servers to Server Manager, you can use the **Import** process and these steps:

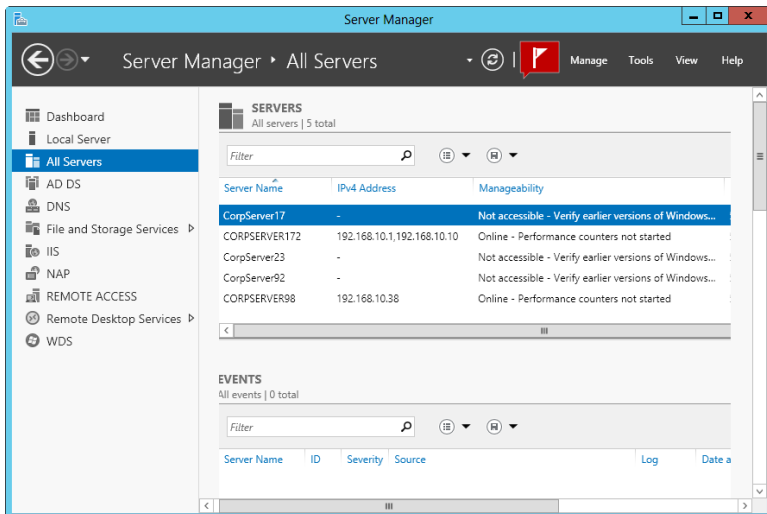
1. Create a text file that has one host name, fully qualified domain name, or IP address per line.
2. In Server Manager, select **Add Servers** on the **Manage** menu. In the **Add Servers** dialog box, select the **Import** panel.
3. Tap or click the options button to the right of the **File** box, and then use the **Open** dialog box to locate and open the server list.
4. In the **Computer** list, double-tap or double-click each server you want to add to the **Selected** list. Tap or click **OK**.

After you add a remote computer, the Server Manager console shows the name of the remote computer in the **All Servers** view. Server Manager always resolves IP addresses to host names. As shown in Figure 2-4, the **All Servers** view also lists the **Manageability** status of the server as well. If a server is listed as "Not accessible," you typically need to log on locally to resolve the problem.

In the **All Servers** view, the servers you add are listed in the **Servers** pane so that you can manage them each time you work with Server Manager. Server Manager tracks the services, events, and more for each added server, and each server is added to the appropriate server groups automatically based on the roles and features installed.

Automatically created server groups make it easier to manage the various roles and features that are installed on your servers. If you select the **AD DS** group, as an example, you see a list of the domain controllers you added for management as well as any critical or warning events for these servers and the status of services the role depends on.

If you want to group servers by department, geographic location, or otherwise, you can create your own server groups. When you create groups, the servers you want to work with don't have to be added to Server Manager already. You can add servers by searching Active Directory or DNS, or by importing a list of host names, fully qualified domain names, or IP addresses. Any server you add to a custom group is added automatically for management as well.



**FIGURE 2-4** Note the Manageability status of each server, and take corrective actions as necessary.

To create a server group, complete these steps:

1. Open Server Manager. Select Create Server Group on the Manage menu to display the Create Server Group dialog box.
2. Enter a descriptive name for the group. Use the panels and options provided to add servers to the group. Keep the following in mind:
  - The Server Pool pane, selected by default, lists servers that have been added for management already. If a server you want to add to your group is listed here, add it to the group by double-tapping or double-clicking it.
  - The Active Directory panel allows you to enter the computer name or fully qualified domain name of the remote server that is running Windows Server. After you enter a name, tap or click Find Now. In the Name list, double-tap or double-click a server to add it to the Selected list.
  - The DNS panel allows you to add servers by computer name or IP address. After you enter the name or IP address, tap or click the Search button. In the Name list, double-tap or double-click a server to add it to the Selected list.
  - The Import panel allows you to import a list of servers. Tap or click the options button to the right of the File box, and then use the Open dialog box to locate and open the server list. In the Computer list, double-tap or double-click a server to add it to the Selected list.
3. Tap or click OK to create the server group.

When you press and hold or right-click a server name in the Servers pane of a server group or in the All Servers view, you display an extended list of management options. These options perform the corresponding task or open the corresponding

management tool with the selected server in focus. For example, if you were to right-click CorpServer172 and then select Computer Management, Computer Management connects to CorpServer172 and then opens.

You can work with a remote computer using an interactive remote Windows PowerShell session. To do this, open an elevated, administrator Windows PowerShell prompt. Type **enter-*pssession ComputerName* -credential *UserName***, where *ComputerName* is the name of the remote computer and *UserName* is the name of a user who is a member of the Administrators group on the remote computer or in the domain of which the remote computer is a member. When prompted to enter the authorized user's password, type the password and then press Enter. You can now enter commands in the session as you would if you were using Windows PowerShell locally. To exit the session, enter **exit-*pssession***.

The following example enters an interactive remote session with Server85 using the credentials of Williams:

```
enter-pssession server85 -credential williams
```

## Adding and Removing Roles, Role Services, and Features

Server Manager automatically creates server groups based on the roles of the servers added for management. As an example, the first time you add a domain controller, Server Manager might create AD DS, DNS, and File And Storage Services groups to help you more easily track the roles of the domain controllers.

When you select a role-based group in the left pane, the Servers panel shows the servers you added for management that have this role. The details for the selected server group provide the following information:

- Summary information about events. Server Manager lists recent warning and error events. If you tap or click an event, you can get more information about the event.
- Summary information about the status of related system services. You can press and hold or right-click a service to manage its run status.

**TIP** By default, Server Manager refreshes details every 10 minutes. You can refresh the details manually by tapping or clicking the Refresh Servers button on the toolbar. If you want to set a different default refresh interval, tap or click Manage and then tap or click Server Manager Properties. Next, set the new refresh interval in minutes and then tap or click OK.

You can manage a service by pressing and holding or right-clicking the service and then tapping or clicking Stop Service, Start Service, Pause Service, Resume Service, or Restart Service as appropriate. In many cases, if a service isn't running as you think it should, you can use the Restart option to resolve the issue by stopping and then starting the service. See Chapter 3, "Monitoring Processes, Services, and Events," for detailed information about working with events and system services.

The Manage menu has two key options for working with roles and features:

- **Add Roles And Features** Starts the Add Roles And Features Wizard, which you can use to install roles and features on a server added for management.



- **Remove Roles And Features** Starts the Remove Roles And Features Wizard, which you can use to uninstall roles and features on a server added for management.

With Windows Server 2012, you can install roles and features on running servers (whether physical machines or virtual) as well as virtual hard disks. Servers must be added for management in Server Manager, and they must be online. Virtual hard disks that you want to work with don't have to be online, but they must be selectable when you are browsing for them. Because of this, you might need to map a network drive to access a network share. With this in mind, you can add a server role or feature by following these steps:

1. In Server Manager, select Add Roles And Features on the Manage menu. This starts the Add Roles And Features Wizard. If the wizard displays the Before You Begin page, read the introductory text and then tap or click Next. You can avoid seeing the Before You Begin page the next time you start this wizard by selecting the Skip This Page By Default check box before tapping or clicking Next.
2. On the Installation Type page, Role-Based Or Feature-Based Installation is selected by default. Tap or click Next.
3. On the Server Selection page, you can choose to install roles and features on running servers or virtual hard disks. Either select a server from the server pool or select a server from the server pool on which to mount a virtual hard disk (VHD). If you are adding roles and features to a VHD, tap or click Browse and then use the Browse For Virtual Hard Disks dialog box to locate the VHD. When you are ready to continue, tap or click Next.

**NOTE** Only servers running Windows Server 2012 and that have been added for management in Server Manager are listed.

4. On the Server Roles page, select the role or roles to install. If additional features are required to install a role, you'll see an additional dialog box. Tap or click Add Features to close the dialog box and add the required features to the server installation. Tap or click Next to continue.

**NOTE** Some roles cannot be added at the same time as other roles. You have to install each role separately. Other roles cannot be combined with existing roles, and you'll see warning prompts about this. A server running a Server Core installation can act as a domain controller and can also hold any of the flexible single-master operations (FSMO) roles for Active Directory.

5. On the Features page, select the feature or features to install. If additional features are required to install a feature you selected, you'll see an additional dialog box. Tap or click Add Features to close the dialog box and add the required features to the server installation. When you are ready to continue, tap or click Next.
6. With some roles, you'll see an extra wizard page, which provides additional information about using and configuring the role. You may also have the opportunity to install additional role services as part of a role. For example, with Print And Document Services, Web Server Role (IIS), and WSUS, you'll see an

additional information page and a page for selecting role services to install along with the role.

7. On the Confirmation page, tap or click the Export Configuration Settings link to generate an installation report that can be displayed in Internet Explorer.
8. If the server on which you want to install roles or features doesn't have all the required binary source files, the server gets the files via Windows Update by default or from a location specified in Group Policy. You also can specify an alternate path for the source files. To do this, click the Specify An Alternate Source Path link, type that alternate path in the box provided, and then tap or click OK. For example, if you mounted a Windows image and made it available on the local server as discussed in "Server Manager Essentials and Binaries" earlier, you could enter the alternate path as **c:\mountdir\windows\winsxs**. For network shares, enter the UNC path to the share, such as **\\CorpServer82\WinServer2012\**. For mounted Windows images, enter the WIM path prefixed with **WIM:** and including the index of the image to use, such as **WIM:\\CorpServer82\WinServer2012\install.wim:4**.
9. After you review the installation options and save them as necessary, tap or click Install to begin the installation process. The Installation Progress page tracks the progress of the installation. If you close the wizard, tap or click the Notifications icon in Server Manager and then tap or click the link provided to reopen the wizard.
10. When the wizard finishes installing the server with the roles and features you selected, the Installation Progress page will be updated to reflect this. Review the installation details to ensure that all phases of the installation were completed successfully.

Note any additional actions that might be required to complete the installation, such as restarting the server or performing additional installation tasks. If any portion of the installation failed, note the reason for the failure. Review the Server Manager entries for installation problems and take corrective actions as appropriate.

You can remove a server role or feature by following these steps:

1. In Server Manager, select Remove Roles And Features on the Manage menu. This starts the Remove Roles And Features Wizard. If the wizard displays the Before You Begin page, read the introductory text and then tap or click Next. You can avoid seeing the Before You Begin page the next time you start this wizard by selecting the Skip This Page By Default check box before tapping or clicking Next.
2. On the Server Selection page, you can choose to remove roles and features from running servers or virtual hard disks. Either select a server from the server pool or select a server from the server pool on which to mount a virtual hard disk (VHD). If you are removing roles and features from a VHD, tap or click Browse and then use the Browse For Virtual Hard Disks dialog box to locate the VHD. When you are ready to continue, tap or click Next.
3. On the Server Roles page, clear the check box for the role you want to remove. If you try to remove a role that another role or feature depends on, a warning prompt appears stating that you cannot remove the role unless you

remove the other role as well. If you tap or click the Remove Features button, the wizard removes the dependent roles and features as well. Note that if you want to keep related management tools, you should clear the Remove Management Tools check box prior to tapping or clicking the Remove Features button and then click Continue. Tap or click Next.

4. On the Features page, the currently installed features are selected. To remove a feature, clear the related check box. If you try to remove a feature that another feature or role depends on, you'll see a warning prompt stating that you cannot remove the feature unless you also remove the other feature or role. If you tap or click the Remove Features button, the wizard removes the dependent roles and features as well. Note that if you want to keep related management tools, you should clear the Remove Management Tools check box and then click Continue prior to tapping or clicking the Remove Features button. Tap or click Next.
5. On the Confirmation page, review the related components that the wizard will remove based on your previous selections and then tap or click Remove. The Removal Progress page tracks the progress of the removal. If you close the wizard, tap or click the Notifications icon in Server Manager and then tap or click the link provided to reopen the wizard.
6. When the wizard finishes modifying the server configuration, you'll see the Removal Progress page. Review the modification details to ensure that all phases of the removal process were completed successfully.

Note any additional actions that might be required to complete the removal, such as restarting the server or performing additional removal tasks.

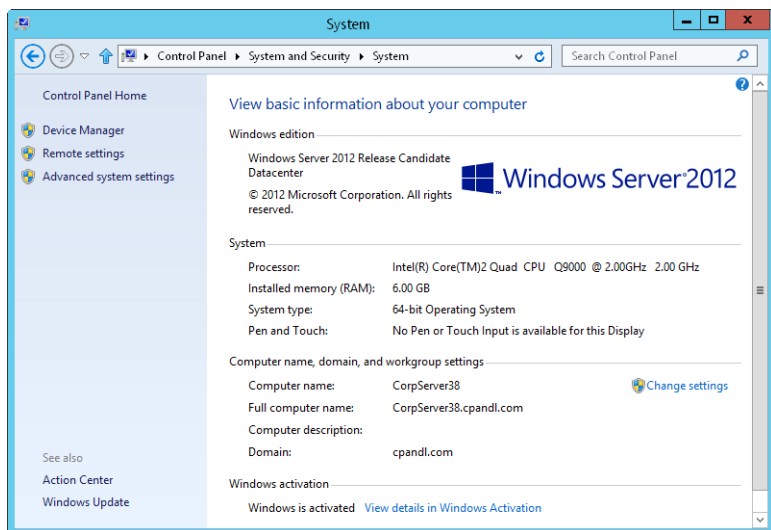
If any portion of the removal failed, note the reason for the failure. Review the Server Manager entries for removal problems and take corrective actions as appropriate.

## Managing System Properties

---

You use the System console to view system information and perform basic configuration tasks. To access the System console, double-tap or double-click System in Control Panel. As Figure 2-5 shows, the System console is divided into four basic areas that provide links for performing common tasks and a system overview:

- **Windows Edition** Shows the operating system edition and version, and lists any service packs you applied.
- **System** Lists the processor, memory, and type of operating system installed on the computer. The type of operating system is listed as 32-bit or 64-bit.
- **Computer Name, Domain, And Workgroup Settings** Provides the computer name, description, domain, and workgroup details. If you want to change any of this information, tap or click Change Settings and then tap or click Change in the System Properties dialog box.
- **Windows Activation** Shows whether you have activated the operating system and the product key. If Windows Server 2012 isn't activated yet, tap or click the link provided to start the activation process and then follow the prompts.



**FIGURE 2-5** Use the System console to view and manage system properties.

When you're working in the System console, links in the left pane provide quick access to key support tools, including the following:

- Device Manager
- Remote Settings
- Advanced System Settings

Although volume-licensed versions of Windows Server 2012 might not require activation or product keys, retail versions of Windows Server 2012 require both activation and product keys. If Windows Server 2012 has not been activated, you can activate the operating system by selecting **Activate Windows Now** under Windows Activation. You can also activate Windows by entering **slmgr -ato** at a command prompt.

You can change the product key provided during installation of Windows Server 2012 to stay in compliance with your licensing plan. At a command prompt, type **slmgr -ipk** followed by the product key you want to use, and then press Enter. When Windows finishes validating the product key, you need to reactivate the operating system.

**NOTE** The Windows Software Management Licensing tool has many other options, including options for offline activation using a confirmation identifier. To view this and other options, enter **slmgr** at a command prompt.

Within the System console, you can access the System Properties dialog box and use this dialog box to manage system properties. Tap or click **Change Settings** under Computer Name, Domain, And Workgroup Settings. The following sections examine

key areas of the operating system you can configure using the System Properties dialog box.

## The Computer Name Tab

You can display and modify the computer's network identification on the Computer Name tab of the System Properties dialog box. The Computer Name tab displays the full computer name of the system and the domain membership. The full computer name is essentially the Domain Name System (DNS) name of the computer, which also identifies the computer's place within the Active Directory hierarchy. If a computer is a domain controller or a certificate authority, you can change the computer name only after removing the related role from the computer.

You can join a computer to a domain or workgroup by following these steps:

1. On the Computer Name tab of the System Properties dialog box, tap or click Change. This displays the Computer Name/Domain Changes dialog box.
  2. To put the computer in a workgroup, select the Workgroup option and then type the name of the workgroup to join.
  3. To join the computer to a domain, select the Domain option, type the name of the domain to join, and then tap or click OK.
  4. If you changed the computer's domain membership, you'll see a Windows Security prompt. Enter the name and password of an account with permission to add the computer to the specified domain or to remove the computer from a previously specified domain, and then tap or click OK.
  5. When prompted that your computer has joined the workgroup or domain you specified, tap or click OK.
  6. You'll see a prompt stating that you need to restart the computer. Tap or click OK.
  7. Tap or click Close, and then tap or click Restart Now to restart the computer.
- To change the name of a computer, follow these steps:

1. On the Computer Name tab of the System Properties dialog box, tap or click Change. This displays the Computer Name/Domain Changes dialog box.
2. In the Computer Name text box, type the new name for the computer.
3. You'll see a prompt stating that you need to restart the computer. Tap or click OK.
4. Tap or click Close, and then tap or click Restart Now to restart the computer.

## The Hardware Tab

The System Properties dialog box's Hardware tab provides access to Device Manager and Driver Installation Settings. To access the Hardware tab, open the System Properties dialog box and then tap or click the Hardware tab.

For installed devices, you can configure Windows Server to download driver software and realistic icons for devices. By default, Windows Server does not do this.

If you want a computer to check for drivers automatically, tap or click the Device Installation Settings button and then select either Yes, Do This Automatically or No, Let Me Choose What To Do. If you want to choose what to do, you can specify the following:

- Always install the best driver software from Windows Update
- Never install driver software from Windows Update
- Automatically get the device apps and info provided by your device manufacturer

The first two options do exactly what they say. The final option tells Windows Update that you want to get metadata and companion applications for devices. Tap or click Save Changes, and then tap or click OK to apply your changes.

## The Advanced Tab

The System utility's Advanced tab controls many of the key features of the Windows operating system, including application performance, virtual memory usage, the user profile, environment variables, and startup and recovery. To access the Advanced tab, open the System Properties dialog box and then tap or click the Advanced tab.

### Setting Windows Performance

Many graphics enhancements were added to the Windows Server 2008 interface, and these enhancements are available in later releases as well. These enhancements include many visual effects for menus, toolbars, windows, and the taskbar. You can configure Windows performance by following these steps:

1. Tap or click the Advanced tab in the System Properties dialog box, and then tap or click Settings in the Performance panel to display the Performance Options dialog box.
2. The Visual Effects tab is selected by default. You have the following options for controlling visual effects:
  - **Let Windows Choose What's Best For My Computer** Enables the operating system to choose the performance options based on the hardware configuration. For a newer computer, this option will probably have the same effect as choosing the Adjust For Best Appearance option. The key distinction, however, is that this option is chosen by Windows based on the available hardware and its performance capabilities.
  - **Adjust For Best Appearance** When you optimize Windows for best appearance, you enable all visual effects for all graphical interfaces. Menus and the taskbar use transitions and shadows. Screen fonts have smooth edges. List boxes have smooth scrolling. Folders use web views and more.
  - **Adjust For Best Performance** When you optimize Windows for best performance, you turn off the resource-intensive visual effects, such as slide transitions and smooth edges for fonts, while maintaining a basic set of visual effects.

- **Custom** You can customize the visual effects by selecting or clearing the visual effects options in the Performance Options dialog box. If you clear all options, Windows does not use visual effects.
3. Tap or click Apply when you have finished changing visual effects. Tap or click OK twice to close the open dialog boxes.

## Setting Application Performance

Application performance is related to processor-scheduling caching options you set for the Windows Server 2012 system. Processor scheduling determines the responsiveness of applications you are running interactively (as opposed to background applications that might be running on the system as services). You control application performance by following these steps:

1. Access the Advanced tab in the System Properties dialog box, and then display the Performance Options dialog box by tapping or clicking Settings in the Performance panel.
2. In the Performance Options dialog box, tap or click the Advanced tab.
3. In the Processor Scheduling panel, you have the following options:
  - **Programs** Use this option to give the active application the best response time and the greatest share of available resources. Generally, you'll want to use this option only on development servers or when you are using Windows Server 2012 as your desktop operating system.
  - **Background Services** Use this option to give background applications a better response time than the active application. Generally, you'll want to use this option for production servers.
4. Tap or click OK.

## Configuring Virtual Memory

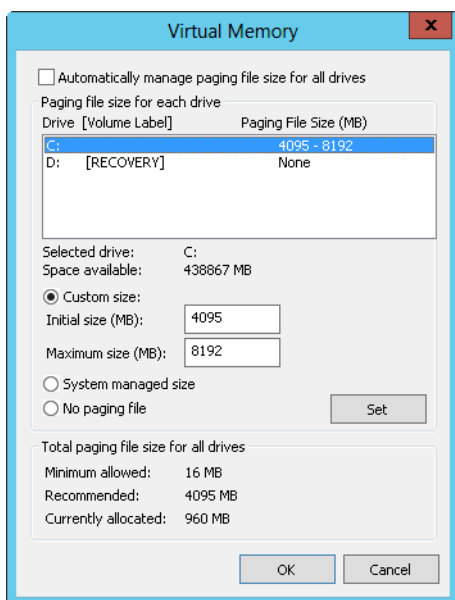
With virtual memory, you can use disk space to extend the amount of memory available on a system by using part of the hard disk as part of system memory. This feature writes RAM to disks by using a process called *paging*. With paging, a set amount of RAM, such as 8192 megabytes (MB), is written to the disk as a paging file. The paging file can be accessed from the disk when needed in place of physical RAM.

An initial paging file is created automatically for the drive containing the operating system. By default, other drives don't have paging files, so you must create these paging files if you want them. When you create a paging file, you set an initial size and a maximum size. Paging files are written to the volume as a file named Pagefile.sys.

**REAL WORLD** Current releases of Windows Server automatically manage virtual memory much better than their predecessors. Typically, Windows Server allocates virtual memory in an amount at least as large as the total physical memory installed on the computer. This helps to ensure that paging files don't become fragmented, which can result in poor system performance. If you want to manage virtual memory manually, you can use a fixed virtual memory size in most cases. To do this, set the initial size and the maximum size to the same value. This ensures that the paging file is consistent and can be written to a single contiguous file (if possible, given the amount of space on the volume). In most cases, for computers with 8 GB of RAM or less, I recommend setting the total paging file size so that it's twice the amount of physical RAM on the system. For instance, on a computer with 8 GB of RAM, you would ensure that the Total Paging File Size For All Drives setting is at least 16,384 MB. On systems with more than 8 GB of RAM, you should follow the hardware manufacturer's guidelines for configuring the paging file. Typically, this means setting the paging file to be the same size as physical memory.

You can configure virtual memory by following these steps:

1. Access the Advanced tab in the System Properties dialog box, and then display the Performance Options dialog box by tapping or clicking Settings in the Performance panel.
2. In the Performance Options dialog box, tap or click the Advanced tab and then tap or click Change to display the Virtual Memory dialog box, shown in Figure 2-6.



**FIGURE 2-6** Virtual memory extends the amount of RAM on a system.



The following information is provided:

- **Paging File Size For Each Drive** Provides information on the currently selected drive, and allows you to set its paging file size. Space Available indicates how much space is available on the drive.
  - **Drive [Volume Label] and Paging File Size** Show how virtual memory is currently configured on the system. Each volume is listed with its associated paging file (if any). The paging file range shows the initial and maximum size values set for the paging file.
  - **Total Paging File Size For All Drives** Provides a recommended size for virtual RAM on the system, and tells you the amount currently allocated. If this is the first time you're configuring virtual RAM, notice that the recommended amount has already been given to the system drive (in most instances).
3. By default, Windows Server manages the paging file size for all drives. If you want to configure virtual memory manually, clear the Automatically Manage Paging File Size For All Drives check box.
  4. In the Drive list, select the volume you want to work with.
  5. Select Custom Size, and then enter values in the Initial Size and Maximum Size boxes.
  6. Tap or click Set to save the changes.
  7. Repeat steps 4–6 for each volume you want to configure.

**NOTE** The paging file is also used for debugging purposes when a Stop error occurs on the system. If the paging file on the system drive is smaller than the minimum amount required to write the debugging information to the paging file, this feature is disabled. If you want to use debugging, you should set the minimum size to equal the amount of RAM on the system. For example, a system with 4 GB of RAM would need a paging file of 4 GB on the system drive.

8. Tap or click OK. If prompted to overwrite an existing Pagefile.sys file, tap or click Yes.
9. If you updated the settings for a paging file that is currently in use, you'll see a prompt indicating that you need to restart the system for the changes to take effect. Tap or click OK.
10. Tap or click OK twice to close the open dialog boxes. When you close the System utility, you'll see a prompt asking if you want to restart the system. Tap or click Restart.

You can have Windows Server 2012 automatically manage virtual memory by following these steps:

1. Access the Advanced tab in the System Properties dialog box, and then display the Performance Options dialog box by tapping or clicking Settings in the Performance panel.
2. Tap or click the Advanced tab, and then tap or click Change to display the Virtual Memory dialog box.
3. Select the Automatically Manage Paging File Size For All Drives check box.

4. Tap or click OK three times to close the open dialog boxes.

**NOTE** If you updated the settings for the paging file currently in use, you'll see a prompt indicating that you need to restart the server for the changes to take effect. Tap or click OK. When you close the System Properties dialog box, you'll see a prompt telling you that you need to restart the system for the changes to take effect. On a production server, you should schedule this reboot outside normal business hours.

## Configuring Data Execution Prevention

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

**NOTE** The 32-bit versions of Windows support DEP as implemented by Advanced Micro Devices (AMD) processors that provide the no-execute page-protection (NX) processor feature. Such processors support the related instructions and must be running in Physical Address Extension (PAE) mode. The 64-bit versions of Windows also support the NX processor feature.

### USING AND CONFIGURING DEP

You can determine whether a computer supports DEP by using the System utility. If a computer supports DEP, you can also configure it by following these steps:

1. Access the Advanced tab in the System Properties dialog box, and then display the Performance Options dialog box by tapping or clicking Settings in the Performance panel.
2. In the Performance Options dialog box, tap or click the Data Execution Prevention tab. The text at the bottom of this tab indicates whether the computer supports execution protection.
3. If a computer supports execution protection and is configured appropriately, you can configure DEP by using the following options:
  - **Turn On DEP For Essential Windows Programs And Services Only** Enables DEP only for operating system services, programs, and components. This is the default and recommended option for computers that support execution protection and are configured appropriately.
  - **Turn On DEP For All Programs Except Those I Select** Configures DEP, and allows for exceptions. Select this option, and then tap or click Add to specify programs that should run without execution protection. With this option, execution protection will work for all programs except those you select.
4. Tap or click OK.

If you turned on DEP and allowed exceptions, you can add or remove a program as an exception by following these steps:

1. Access the Advanced tab in the System Properties dialog box, and then display the Performance Options dialog box by tapping or clicking Settings in the Performance panel.
2. In the Performance Options dialog box, tap or click the Data Execution Prevention tab.
3. To add a program as an exception, tap or click Add. Use the Open dialog box to find the executable file for the program you are configuring as an exception, and then tap or click Open.
4. To temporarily disable a program as an exception (this might be necessary for troubleshooting), clear the check box next to the program name.
5. To remove a program as an exception, tap or click the program name and then tap or click Remove.
6. Tap or click OK to save your settings.

## Understanding DEP Compatibility

To be compatible with DEP, applications must be able to mark memory explicitly with Execute permission. Applications that cannot do this will not be compatible with the NX processor feature. If you experience memory-related problems running applications, you should determine which applications are having problems and configure them as exceptions rather than disable execution protection completely. This way, you still get the benefits of memory protection and can selectively disable memory protection for programs that aren't running properly with the NX processor feature.

Execution protection is applied to both user-mode and kernel-mode programs. A user-mode execution protection exception results in a STATUS\_ACCESS\_VIOLATION exception. In most processes, this exception will be an unhandled exception, resulting in termination of the process. This is the behavior you want because most programs violating these rules, such as a virus or worm, will be malicious in nature.

You cannot selectively enable or disable execution protection for kernel-mode device drivers the way you can with applications. Furthermore, on compliant 32-bit systems, execution protection is applied by default to the memory stack. On compliant 64-bit systems, execution protection is applied by default to the memory stack, the paged pool, and the session pool. A kernel-mode execution protection access violation for a device driver results in an ATTEMPTED\_EXECUTE\_OF\_NOEXECUTE\_MEMORY exception.

## Configuring System and User Environment Variables

Windows uses environment variables to track important strings, such as a path where files are located or the logon domain controller host name. Environment variables defined for use by Windows—called *system environment variables*—are the same no matter who is logged on to a particular computer. Environment variables

defined for use by users or programs—called *user environment variables*—are different for each user of a particular computer.

You configure system and user environment variables by means of the Environment Variables dialog box, shown in Figure 2-7. To access this dialog box, open the System Properties dialog box, tap or click the Advanced tab, and then tap or click Environment Variables.

### CREATING AN ENVIRONMENT VARIABLE

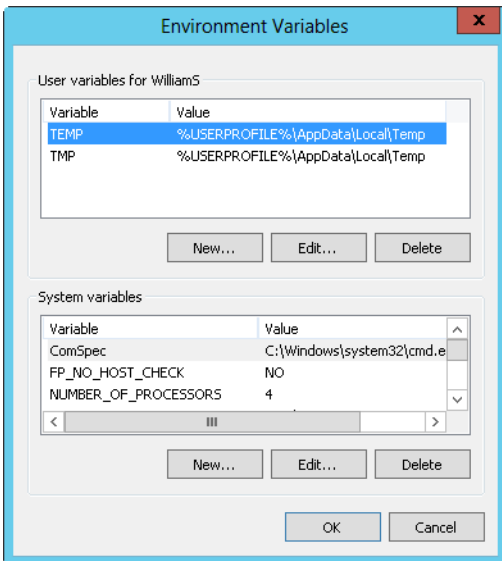
You can create an environment variable by following these steps:

1. Tap or click New under User Variables or under System Variables, whichever is appropriate. This opens the New User Variable dialog box or the New System Variable dialog box, respectively.
2. In the Variable Name text box, type the variable name. In the Variable Value text box, type the variable value.
3. Tap or click OK.

### EDITING AN ENVIRONMENT VARIABLE

You can edit an environment variable by following these steps:

1. Select the variable in the User Variables or System Variables list.
2. Tap or click Edit under User Variables or under System Variables, whichever is appropriate. The Edit User Variable dialog box or the Edit System Variable dialog box opens.
3. Type a new value in the Variable Value text box, and then tap or click OK.



**FIGURE 2-7** Configure system and user environment variables in the Environment Variables dialog box.

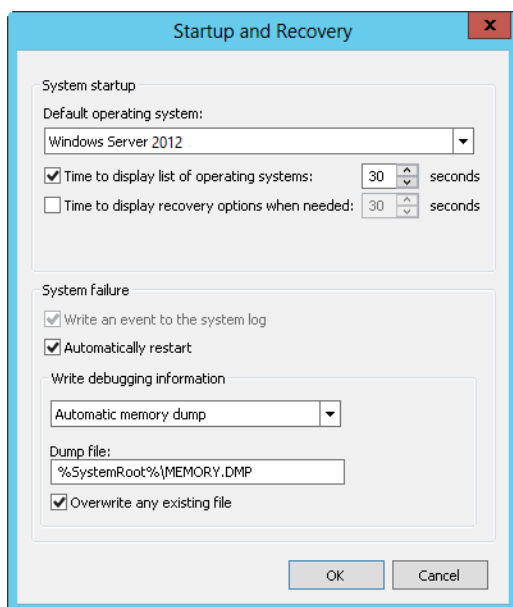
## DELETING AN ENVIRONMENT VARIABLE

To delete an environment variable, select it and tap or click Delete.

**NOTE** When you create or modify environment variables, most of the variables are valid immediately after they are created or modified. With system variables, some changes take effect after you restart the computer. With user variables, some changes take effect the next time the user logs on to the system.

## Configuring System Startup and Recovery

You configure system startup and recovery properties in the Startup And Recovery dialog box, shown in Figure 2-8. To access this dialog box, open the System Properties dialog box, tap or click the Advanced tab, and then tap or click Settings in the Startup And Recovery panel.



**FIGURE 2-8** Configure system startup and recovery properties in the Startup And Recovery dialog box.

## SETTING STARTUP OPTIONS

The System Startup area of the Startup And Recovery dialog box controls system startup. To specify the default operating system for a computer with multiple bootable operating systems, select one of the operating systems listed in the Default Operating System list. These options change the configuration settings used by the Windows Boot Manager.

Upon startup of a computer with multiple bootable operating systems, Windows Server displays the startup configuration menu for 30 seconds by default. You can change this by performing either of the following actions:

- **Boot immediately to the default operating system** by clearing the Time To Display List Of Operating Systems check box.
- **Display the available options for a specific amount of time** by selecting the Time To Display List Of Operating Systems check box and then setting a time delay in seconds.

On most systems, you'll generally want to use a value of 3 to 5 seconds. This is long enough for you to make a selection, yet short enough to expedite the system startup process.

When the system is in a recovery mode and booting, a list of recovery options might be displayed. As you can with the standard startup options, you can configure recovery startup options in one of two ways. You can set the computer to boot immediately using the default recovery option by clearing the Time To Display Recovery Options When Needed check box, or you can display the available options for a specific amount of time by selecting Time To Display Recovery Options When Needed and then setting a time delay in seconds.

## SETTING RECOVERY OPTIONS

You control system recovery with the System Failure and Write Debugging Information areas of the Startup And Recovery dialog box. Administrators use recovery options to control precisely what happens when the system encounters a fatal system error (also known as a Stop error). The available options for the System Failure area are as follows:

- **Write An Event To The System Log** Logs the error in the system log, allowing administrators to review the error later using Event Viewer.
- **Automatically Restart** Select this option to have the system attempt to reboot when a fatal system error occurs.

**NOTE** Configuring automatic reboots isn't always a good thing. Sometimes you might want the system to halt rather than reboot to ensure that the system gets proper attention. Otherwise, you would know that the system rebooted only when you viewed the system logs or if you happened to be in front of the system's monitor when it rebooted.

You use the Write Debugging Information list to choose the type of debugging information you want to write to a dump file. You can use the dump file to diagnose system failures. The options are as follows:

- **None** Use this option if you don't want to write debugging information.
- **Small Memory Dump** Use this option to dump the physical memory segment in which the error occurred. This dump is 256 KB in size.
- **Kernel Memory Dump** Use this option to dump the physical memory area being used by the Windows kernel. The dump file size depends on the size of the Windows kernel.

- **Complete Memory Dump** Use this option to dump all physical memory. The dump file size depends on the amount of physical memory being used, up to a maximum file size equal to the total physical RAM on the server.
- **Automatic Memory Dump** Use this option to let Windows determine which type of memory dump is best and create the dump file accordingly.

If you elect to write to a dump file, you must also set a location for it. The default dump locations are %SystemRoot%\Minidump for small memory dumps and %SystemRoot%\Memory.dmp for all other memory dumps. You'll usually want to select Overwrite Any Existing File as well. Selecting this option ensures that any existing dump files are overwritten if a new Stop error occurs.

**BEST PRACTICES** You can create the dump file only if the system is properly configured. The system drive must have a sufficiently large memory-paging file (as set for virtual memory on the Advanced tab), and the drive the dump file is written to must have sufficient free space. For example, my server has 8 GB of RAM and requires a paging file on the system drive of the same size—8 GB. In establishing a baseline for kernel memory usage, I found that the server uses between 892 and 1076 MB of kernel memory. Because the same drive is used for the dump file, the drive must have at least 9 GB of free space to create a dump of debugging information. (That's 8 GB for the paging file and about 1 GB for the dump file.)

## The Remote Tab

The Remote tab of the System Properties dialog box controls Remote Assistance invitations and Remote Desktop connections. These options are discussed in Chapter 4.

# Index

## Symbols & Numbers

\$ (special share symbol), 474–475  
32-bit processes, 92–93  
64-bit systems, 6, 43–44

## A

access controls, 297–300. *See also*  
permissions

Account Lockout Policy, 194–195, 321–322,  
325–326

account policies

Default Domain Policy GPO, 147  
lockout, 194–195, 321–322, 325–326  
security templates for, 193–195  
setting, 321–322

accounts

Administrator, 307–308, 317  
computer. *See* computer accounts  
default and predefined, 306–308  
deleting, 373  
disk quotas with, 504  
domain. *See* domain accounts  
expiration dates, changing, 375, 378  
exporting, 372  
group. *See* group accounts  
group memberships of, managing,  
339–340  
Guest account, 308  
importing, 372  
locked out accounts, 373–374  
lockout policies, 194–195, 321–322,  
325–326  
logon rights for, 312–313  
managed service accounts, 341–345  
naming policies, 319–320  
passwords for. *See* passwords  
security options, 360–361  
tools for creating, 318  
updating, 368–369  
user. *See* user accounts  
virtual accounts, 346

ACEs (access control entries), 297

ACLs (access control lists), 252

ACPI (Advanced Configuration and Power  
Interface), 8–11

Act As Part Of The Operating System privi-  
lege, 310

Action Center, 542, 564

activation, 45, 73–74, 221

active cooling mode, 8–9

Active Directory

2008 R2 features, 220–221

activation feature, 221

Administration Tool, 252. *See also*

LDAP (Lightweight Directory Access  
Protocol)

Administrative Center. *See* Active Direc-  
tory Administrative Center

Adprep command, 250

ADSI use for communications, 242

auditing objects of, 502–503

authentication mechanism assurance,  
220

CAs (certificate authorities), 14–15, 33,  
75

Certificate Services, 14–15, 33

claims-based policy controls, 221

client computer requirements for, 230

command-line tool summary, 250–251

Configuration Wizard, 218–219

data stores, 14

deferred index creation, 221

DHCP integration options, 19–20. *See  
also* DHCP (Dynamic Host Configura-  
tion Protocol)

diagnosing problems, tool for, 252,  
289–290

Directory Services Restore Mode, 16–17

distribution of updated data. *See*  
replication

DNS integration with, 18–20, 217–218,  
616–617, 625–626, 628

Domain Services, 15, 33

Domains And Trusts snap-in, 226–227

domains, structural overview of,  
223–224. *See also* domains

Ds commands, list of, 251



### Active Directory, *continued*

Enhanced Fine-Grained Password Policy, 222

exporting accounts, 372

features, table of key, 221–223

Federation Services, 15, 33

forests, domain, 225–227, 317

FSMO (flexible single-master operations) roles, 71, 273, 276

full integration with DNS, 19

functional levels of domains, 225–227, 231–237

Group Managed Service Accounts, 222

Group Policy, relation to, 138

importing accounts, 372

installing, 218, 270–272

interoperability with other directory services, 242

Kerberos with. *See* Kerberos

LDAP for. *See* LDAP (Lightweight Directory Access Protocol)

Lightweight Directory Services, 15, 33

maintenance while stopped, 16–17

managed accounts, 220

mechanism of, overview, 237–238

multiple domain controllers with, 14

Ntdsutil command, 251

offline domain join feature, 220

off-premises domain join, 222

partial integration with DNS, 18–19

permissions, setting, 380–381

ports used by, 292–293

PowerShell, module for, 220–221, 259

publishing shares, 469

read-only domain controllers, 16

recovery of deleted objects, 245–248

Recycle Bin, 220, 222, 244–248

Relative ID soft ceilings and warnings, 223

Restartable Active Directory Domain Services, 16–17

restoring, 547

Rights Management Services, 15, 33

RODC with DNS issues, 19

schemas of. *See* schemas

searching for directory objects, 254–256, 258

searching for users and groups, 350–351

Server Manager integration, 223

servers running. *See* domain controllers sites, 138

structures provided by, 223

support tools, table of, 251–252

tools for, snap-ins, 249–250

trees, domain, 225–227

troubleshooting, 292–294

Users And Computers tool. *See* Active Directory Users And Computers

virtual domain controller cloning, 223

Web Services, 221, 259

Windows Firewall issues with, 250

### Active Directory Administrative Center

adding members to groups, 339–340

capabilities of, 221, 256

central access rules, 299–300

contact information, setting, 349–350

creating computer accounts with, 260–261

creating domain user accounts, 333–334

deleting, disabling, and enabling com-

puter accounts, 264

domains, connecting to, 257–258

editing properties of computer ac-

counts, 263

enabling disabled accounts, 374

global group creations, 336–337

moving computer accounts, 266

multiple user accounts, managing, 375–378

Organization panel, 349

OUs (organizational units), managing, 281

primary group selection, 340

resetting locked computer accounts, 264–266

searching with, 258–259

unlocking accounts, 373–374

### Active Directory Domain Services, 230

### Active Directory Domain Services Installation Wizard, 282

### Active Directory Installation Wizard, 270–272

### Active Directory Sites And Services, 229–230, 280–289

### Active Directory Users And Computers

adding members to groups, 339–340

Advanced Features, 253

auditing objects of, 502–503

contact information, setting for user accounts, 347–349

copying domain user accounts, 371

creating computer accounts with, 261–263

creating domain user accounts, 330–334

- deleting, disabling, and enabling computer accounts, 264
- domains and controllers, connecting to, 254
- editing properties of computer accounts, 263
- enabling disabled accounts, 374
- folder set of, 252–253
- global group creations, 336
- home directory specification, 354–355
- listing accounts or resources, 368–369
- Logon Hours settings, 355–357
- moving computer accounts, 266
- multiple accounts, working with, 373
- multiple user accounts, managing, 375–378
- opening, 252
- operations masters, viewing, 273–274
- OUs (organizational units), managing, 228, 253, 281–282
- permissions, setting, 380–381
- primary group selection, 340
- renaming user accounts, 369–371
- resetting locked computer accounts, 264–265
- scope, selecting for a new group, 336, 337
- searching for directory objects, 254–256
- searching for users and groups, 350–351
- user profiles, setting for multiple accounts, 376–377
- active partitions, 402, 445
- AD CS (Active Directory Certificate Services), 14–15, 33
- AD DS (Active Directory Domain Services). *See also* Active Directory
  - adding to a server, 218
  - centrality to Active Directory, 15
  - Configuration Wizard, 218–219, 271–272
  - DNS, installing first, 616
  - Group Policy with. *See* GPMC (Group Policy Management Console)
  - installing domain controllers, 270–272
  - Restartable AD Domain Services, 16–17
  - role description, 33
- AD FS (Active Directory Federation Services), 15, 33, 297
- AD LDS (Active Directory Lightweight Directory Services), 15, 33
- AD RMS (Active Directory Rights Management Services), 15, 33
- Add Roles And Features Wizard, 70–72, 526–527
- Add Workstations To Domain privilege, 310
- Add Workstations To The Domain right, 267–268
- Adjust Memory Quotas For A Process privilege, 310
- administrative shares, 474–476
- administrative templates, 151–152
- Administrative Tools program group, 23
- Administrator account, 307–308, 317
- administrators, 315–317, 486–487
- Administrators group, 315–317, 486
- ADMX format, 141–142
- Adprep command, 232–235, 250–251
- ADSI (Active Directory Service Interface), 242
- ADSI Edit tool, 252, 289–290
- Adsiedit.msc, 252
- Advanced Configuration and Power Interface (ACPI), 8–11
- Advanced tab, System Properties dialog box, 76–85
- ADWS (Active Directory Web Services), 259
- Aero, Windows, 5
- AES (Advanced Encryption Standard), 361, 552
- alerts, performance counter, 129–130
- allocation units, 409, 411, 425, 442
- alternate credentials, 58
- alternate IP addressing, 568–569
- Anonymous Logon identity, 317
- antimalware software, 546
- Apple computers, 340, 463, 479–481
- application directory partitions, 238
- Application Server, 33
- applications
  - Applications log, 108
  - Apps, 7, 137, 363
  - backups of data files, 528, 534
  - performance settings, 77
  - restoring, 550–551
  - Server Core installations not for running, 40
  - updates for, 541–542
- applications and services logs, 108–109
- Apps, 7, 137, 363
- archive attribute, 521
- archives, event logs, of, 116–118
- ARP command, 48
- ARP test, 574
- attached storage, standards-based techniques, 419

audio, 37

auditing

- Active Directory objects, 502–503
- DHCP server, 585–586
- file or folder specific, 500–502
- Generate Security Audits privilege, 311
- logon failures, 379
- registry, of the, 502
- rights required to change, 498
- setting policies for, 210, 498–503

authentication. *See also* accounts; passwords

- Active Directory authentication mechanism assurance, 220
- Active Directory Domain Services role in, 15
- Authenticated Users identity, 317
- claims-based access controls, 496–498
- Kerberos for. *See* Kerberos protocols for, 296–297
- remote server management issues, 26–27
- Rights Management Services, 15
- security policies for, 209–210

autoenrollment, 186–187

autoloader tape systems, 523

Automatic Updates, 135–136, 187–190

- WSUS (Windows Server Update Services), 189–190

## B

Background Intelligent Transfer Service (BITS), 35

background processes, 87

backups

- application data, 528, 534
- archive attribute, 521
- Back Up Files And Directories privilege, 310
- cloud-based, 525, 527
- configuring, 527–533
- copy backups, 521
- critical volumes only option, 534
- daily, 521, 532
- differential backups, 521–522, 525
- DVDs for, 525, 535, 541
- encryption certificates, of, 554–555
- full, 521, 525
- of GPOs (Group Policy Objects), 165
- hardware considerations, 520, 522–524
- incremental backups, 521–522, 525, 528–529

LTO drives, 523

manual, 540–541

media options for, 524

Microsoft Online Backup Service, 525, 527

normal, 521

off-site backups, 520

permissions for, 528

planning considerations, 519–521

remote shared folders for, 534, 539, 541

restoring data from. *See* restoring

scheduling automatic, 535–540

scheduling considerations, 520

shadow copies as supplements to, 481–484, 520

storage location specification, 534–535

system state, 528, 546

utilities for, list of, 525

volume options for, 534

Wbadmin. *See* Wbadmin backup command

Windows Server Backup for. *See* Windows Server Backup

Balanced power plan, 8

baseline metrics, establishing, 119

basic disks, 395, 401–404, 421

basic permissions, 488–493

batch scripts, 49, 178–179, 317

BCD Editor, 433–434

Best Practices Analyzer, 60

binaries, 24, 57, 63–65, 72, 218

biometric security, 38

BitLocker Drive Encryption, 35, 136, 404

BITS (Background Intelligent Transfer Service), 35

boot logging, enabling, 545

booting

BCD Editor, 433–434

boot partitions, 402, 433–434, 443

setting default startup OS, 83–84

Startup Repair (StR), 543

Windows Boot Manager, 83–84, 447

Windows Preboot Environment, 5, 447–449

BOOTP (Bootstrap Protocol), 601

BranchCache, 36, 386

BranchCache for Network Files, 34

bridgehead servers, 291–292, 293

built-in accounts, 306

built-in capabilities for groups, 313–315

built-in groups, 308–309

built-in local groups, 303

built-in user accounts, 307  
 Bypass Traverse Checking privilege, 310

## C

Cached statistic, 98  
 CALL command, 49  
 callback parameters, 359  
 CAPI2 (CryptoAPI Version 2), 563  
 CAs (certificate authorities), 14–15, 33, 75  
 cellular network policies, 168  
 central access rules, 298–300  
 certificate authorities (CAs), 14–15, 33, 75  
 certificates  
   AD CS (Active Directory Certificate Services), 14–15  
   autoenrollment, 186–187  
   backing up, 554–555  
   CAs (certificate authorities), 14–15, 33, 75  
   DNSSEC, 632–634  
   file encryption, 414  
   recovery of, 551–553  
   Rights Management Services, 15  
   roaming profiles with, 362  
   role services for, 33  
 Change Permissions special permission, 490–491  
 Change share permission, 470  
 Change Time privileges, 310  
 Character Map, 5–6  
 charms, 6–7  
 Check Disk, 49, 450–453  
 child domains, 18, 218, 616, 634–636  
 child objects, 487  
 chkdisk, 49, 450–453  
 CHKNTFS command, 49  
 claims policy, 221  
 Claims-Aware Agent, 33  
 claims-based access controls, 297–299, 496–498  
 clean installations, 43–47  
 Client for NFS, 36  
 clustering, 36  
 cmdlets, 24–25. *See also* Windows PowerShell 3.0  
 CNAME (canonical name) records, 636, 638  
 commands. *See also specific commands*  
   console for. *See* Windows PowerShell 3.0  
   mini Windows PC, table of, 48–52  
   NET HELP command, 23  
   opening new command prompts, 41

  safe mode with prompt, 545  
   Search box execution of, 137  
 Comma-Separated Value Directory Exchange (CSVDE), 372  
 components, removability of, 5  
 compound identities, 297–298  
 compression, 49, 410–412, 425  
 computer accounts  
   auditing, 503  
   claims-based access controls, 496–498  
   Create Account Objects privilege, 268  
   creating, 259–263  
   editing properties of, 263  
   group memberships of, 496  
   groups, adding computers to, 339–340  
   listing, 368–369  
   managed computer accounts, 262–263  
   managing, 264  
   moving, 266  
   name protection, 586  
   objects for, 231  
   passwords for, 264–266  
   permissions, setting, 380–381  
   protected, 264  
   resetting locked, 264–266  
 computer groups, 339–340, 503  
 Computer Management  
   archiving event logs, 116–118  
   clearing event logs, 116  
   closing file shares, 478  
   configuring share permissions, 470–472  
   creating shared folders, 463–466  
   disabling services, 107  
   event logs options, setting, 115–116  
   Event Viewer, 111–112, 116–117  
   file shares, viewing, 462  
   file sharing, viewing sessions of, 476–478  
   joining computers to domains or workgroups, 267–270  
   Open Files node, 477–478  
   opening, 102, 267  
   pausing services, 103  
   publishing shares, 469  
   remote servers, working with, 102  
   service configuration, 101–107  
   sessions, ending, 477  
   starting services, 103  
   stopping services, 103  
   stopping sharing on folders, 478–479  
 Computer Name tab, 74–75

- contact information, setting for user accounts, 347–350
- contacts, adding to groups, 340
- containers, 138–139
- Control Panel, 7, 23, 151, 542
- Convert utility, 445–447
- cooling modes, 8–9
- copy backups, 521
- COPY command, 49
- core installations. *See* Server Core installations
- cores, multiple, 6, 10–11
- costed networks, 168
- counters, performance, 122–126, 129–133
- crashes
  - automatic rebooting on fatal errors, 84
  - crash dump partitions, 402
  - improvements in recovery mechanisms for, 541–542
  - Microsoft Online Crash Analysis, 543–544
  - Stop errors, 84–85
- Create Files/Write Data special permission, 490–491
- Create Folders/Append Data special permission, 490–491
- Create privileges, 310–311
- Creator identities, 317
- credentials, preventing delegation of, 361
- Critical events, 112
- CryptoAPI Version 2 (CAPI2), 563
- Cscript command, 42
- c-states, 10–11
- CSVDE (Comma-Separated Value Directory Exchange), 372

## D

- D states, 11
- daily backups, 521, 532
- DAT (digital audio tape) drives, 523
- Data Center Bridging, 36
- data collector sets, 124–130
- Data Deduplication service, 34, 386
- Data Execution Prevention (DEP), 80–81, 92
- data scrubbers, 393
- data stores, 14, 238–239
- DATE command, 49
- Dcgpofix, 172–173
- DCOM Server Process Launcher, 106
- Debug Programs privilege, 311
- decrypting files and directories, 418
- deduplication, 34, 386, 436, 441
- Default Domain Controller Policy GPO, 147, 172–173
- Default Domain Controllers GPO, 497
- Default Domain Policy GPO, 172–173
- default gateways, 568–570
- default group accounts, 315–318
- defragmenting drives, 453–455
- DEL command, 49
- delegation, 311, 361
- Delete special permission, 490–491
- Delete Subfolders And Files special permission, 490–491
- DEP (Data Execution Prevention), 80–81, 92
- deploying software using Group Policy, 181–186
- descriptions, user, 348
- desktop, 7, 151
- Desktop Experience, 4–6, 39, 56, 136
- device drivers, 42, 53, 75–76, 311, 545
- devices
  - accounts for. *See* computer accounts
  - claims, 495–498
  - power states of, 11
- DFS (Distributed File System), 34, 109, 142, 151, 252, 386–387
- DHCP (Dynamic Host Configuration Protocol)
  - DHCPIDs, 586
  - DNS integration with, 586–587, 616, 618
  - DNS with, 19–20
  - failover service, 574–575
  - hot standby mode, 574–575
  - IP address conflicts, avoiding, 591
  - IPv4 addressing, 573–575
  - IPv6 configuration, 575–577
  - leases, 574, 577–578, 591, 594–598, 601, 609
  - load balance mode, 574
  - name protection, 586
  - NAP with, 588–591
  - number of servers needed, 574
  - relay agents, 575, 577, 579
  - reserving addresses, 608–609
  - responsibilities of, 573
  - router advertisement messages, 576–577
  - scopes with, 578–579, 582
  - server. *See* DHCP server
  - Server Core default, 46
  - stateful mode, 575–577
  - stateless mode, 575–577

- WINS with, 21
- DHCP server
  - activation and deactivation of scopes of, 601
  - auditing, 585–586
  - authorizing in Active Directory, 583
  - backing up the database, 610–611
  - bindings, configuring, 584
  - credentials specification, 580–581
  - database files for, 610
  - deleting leases and reservations, 610
  - deleting scopes, 602
  - DHCP console, 581–582
  - DNS integration with, 586–587
  - exclusion ranges, setting, 607–608
  - failover scopes, 602–605
  - forcing database regeneration, 612
  - groups delegated for administration, 580
  - installing, 579–581
  - IP address conflicts, avoiding, 591
  - MAC address filtering, 606–607
  - modifying reservation properties, 609
  - moving the database, 611–612
  - multicast scopes, 598
  - multiple scopes, 602
  - Network Policy Server, setting up as, 588–591
  - normal scopes, 593–598
  - reconciliation, 612–613
  - remote connections, 582–583
  - reserving addresses, 608–610
  - restoring the database, 611
  - role description, 33
  - saving configurations, 591–592
  - scope indicators, 582
  - scope options, 599–601
  - service, 583
  - source files for, 580
  - starting and stopping, 583
  - statistics configuration, 584
  - status indicators, 582
  - superscopes, 579, 592–593
  - viewing scope statistics, 605
- dial-up users, 317, 358–360, 359
- differential backups, 521–522, 525
- direct reports, setting for users, 350
- DirectAccess, 13, 34
- directories, domain. *See* Active Directory
- directories, file, 49, 412–413, 415–416. *See also* folders
- Directory Service log, 109
- directory services. *See* Active Directory
- Directory Services Access Control Lists Utility, 252
- Directory Services Restore Mode, 16–17
- Disable Automatic Restart On System Failure, 545
- disable- cmdlets, 25
- discovery, network, 12, 560–562
- Disk Cleanup, 5
- disk controllers, duplexing, 429
- disk drives. *See* hard disk drives
- disk I/O performance tuning, 133
- Disk Management
  - active partitions, marking, 402
  - assigning drive letters, 443–444
  - converting basic disks to dynamic disks, 402–403
  - creating partitions, 407–410
  - creating shadow copies, 482
  - creating volumes, 407–410, 424–425
  - deleting partitions, 445
  - disk mirroring with, 429–431
  - disk striping with parity, 431
  - drive path management, 443
  - drive status values, table of, 399–400
  - extending volumes, 449
  - hot swapping disks, 398
  - initializing disks, 399
  - moving dynamic disks to new systems, 404–405
  - Optimize Drives, 453–455
  - partition color coding scheme, 407
  - properties, viewing, 395–396
  - remote management limitations, 394, 396
  - removing a mirror, 434
  - Rescan Disks command, 398, 405
  - resizing partitions, 447–449
  - shrinking volumes, 448–449
  - striped set creation, 428
  - VHDs (virtual hard disks), managing, 405–406
  - views, 394
  - volume status issues, table of, 422–423
  - volumes, viewing properties of, 420–421
- disk mirroring, 426–434
- disk quotas
  - application issues, 504
  - NTFS. *See* NTFS disk quotas
  - Resource Manager, 503–504, 514–518
- disk striping, 426–428, 431, 434–435, 440
- DISKPART command, 49

Diskraid.exe, 42  
 display names, 319, 331, 333–334  
 displays, 7, 76–77  
 Distributed File System (DFS), 34, 109, 142, 151, 252, 386–387  
 distribution groups, 303  
 DLLs (dynamic-link libraries), 39, 51  
 DNS (Domain Name System)  
     Active Directory, integrating with, 616–617, 625–626, 628  
     Active Directory, use by, 217–218  
     aliases, 638  
     assigning for IP address configuration, 568–569  
     child domains, 18, 281, 616  
     clients, 617–621  
     configuring in Advanced TCP/IP Settings, 620–621  
     DHCP integration with, 19, 586–587, 616, 618  
     DNSSEC, 19–20, 632–634  
     domains vs. Active Directory domains, 230  
     dynamic update options, 626, 645  
     enabling on a network, 617–619  
     FQDNs, 218–219, 616  
     full integration with Active Directory, 19, 616  
     GlobalNames zone, 619, 629–630  
     host name structure, 615  
     intranets, relation to, 615  
     IPv6 with, 617–618  
     LLMNR with, 618  
     log, DNS Server, 109  
     Manager console. *See* DNS Manager console  
     name protection, 586  
     organization of, 18–20  
     parent domains, 18, 218, 615–616  
     partial integration with Active Directory, 18–19, 616  
     port used by, 293  
     record types for, 636–637  
     replication across networks, 616–617  
     RODCs with, 19, 219, 619  
     security issues, 626–627, 632–634  
     servers. *See* DNS servers  
     single-label name resolution, 619  
     SOA (start of authority) records, 637, 641–642  
     structure of, 615–616  
     zones, 616–617, 625–630

DNS Manager console  
     adding or removing servers, 631–632  
     address and pointer records, adding, 636–638  
     child domain creation, 634–636  
     CNAME records, adding, 638  
     configuring servers, 623–627  
     debugging, logging, 648–649  
     deleting domains or subnets, 636  
     DNSSEC configuration, 632–634  
     dynamic update settings, 645  
     editing records, 640  
     event logging settings, 648  
     expiration parameter, 642  
     forwarding options, setting, 646–648  
     IP addresses, disabling, 646  
     monitoring options, 649–650  
     MX (mail exchange) records, 637–639  
     name servers, adding, 639–640  
     primary server designation, 642  
     record management with, 636–640  
     refresh intervals, 642  
     responsible persons, 642  
     serial numbers, 642  
     SOA record modification, 641–642  
     starting or stopping DNS servers, 632  
     structure of, 631  
     TTL parameters, 642  
     viewing records, 640  
     zone properties, setting, 641–645

DNS servers  
     Active Directory–integrated primary servers, 621  
     configuring during setup, 623–624  
     configuring primary servers, 624–627, 642  
     configuring secondary servers, 627, 643–644  
     dynamic update options, 626, 645  
     event logging, 648  
     forwarding options, 646–648  
     forward-only servers, 622  
     GlobalNames zone configuration, 619, 629–630  
     installing services for, 622–624  
     IP addresses, disabling, 646  
     Manager console. *See* DNS Manager console  
     new zone configuration, 625–626  
     primary servers, 621, 624–627, 642  
     restart times, 617  
     reverse lookups, 624, 628–629

- role, DNS Server, 33
- root hints, 624
- secondary servers, 622, 627, 643–644
- server addresses, order of use, 620
- service, 616–617, 622–623, 632
- starting or stopping from Manager
  - console, 632
- startup tasks of, 617
- troubleshooting, 252, 649–650
- well-known site-local addresses of servers, 617
- DNS64 support, 13
- Dnscmd.exe, 252
- DNSSEC (DNS Security Extensions), 19–20, 632–634
- domain accounts
  - creating, 330–334
  - display names of, 319
  - expiration dates, changing, 375
  - listing, 368–369
- Domain Admins group, 309, 315–317
- Domain Computers group, 339
- domain controllers
  - AD DS (Active Directory Domain Services), 15
  - bridgehead servers, 291–293
  - claims-based policy for, 497
  - creation with Active Directory Domain Services, 230
  - default GPOs of, 147
  - demoting, 272–273
  - Directory Services Restore Mode, 16–17
  - DNS installation, 622
  - Domain Controllers group, 339
  - functional levels of, 225–227
  - global catalogs, designation of, 239–240
  - grouping, 58
  - infrastructure masters, 239, 243, 273–280
  - installing, 270–273
  - multimaster replication model, 14
  - names of, changing, 75
  - operations masters, 230–231
  - ports used by, 292–293
  - purpose of, 6, 14
  - read-only, 16, 19, 219, 619
  - refreshing Group Policy, 158–161, 166
  - replication of directory data, 230–231
  - restoring system state, 547
  - sites, associating with, 285
  - states of Active Directory, 17
  - Synchronize Directory Service Data privilege, 312
  - verifying installations of, 218–219
  - virtual domain controller cloning, 223
- domain joins, off-premises feature, 222
- domain local groups, 303–306
- Domain Name System (DNS). *See* DNS (Domain Name System)
- domain naming master role, 242, 244, 275–276, 276–280
- domain networks, 560
- domain user accounts
  - copying to create new, 371
  - creating, 330–334
  - definition of, 301
  - deleting, 373
  - logon troubleshooting, 379
  - properties, configuring, 375–378
- Domain Users group, 338
- domains
  - AD DS. *See* Active Directory; AD DS (Active Directory Domain Services)
  - CAs (certificate authorities) for, 14–15, 33, 75
  - child domains, 18, 218, 634–636
  - controllers. *See* domain controllers
  - default GPOs, 147
  - definition of, 6
  - DNS vs. Active Directory, 230
  - Domain network type, 12
  - forests of, 225–227
  - FQDNs (fully qualified domain names), 101, 218–219, 301–302, 616
  - functional levels of, 225–227
  - GPMC Domains node, 149
  - joining computers to, 75, 267–270
  - local GPO issues in, 143
  - member servers of, 14
  - name system. *See* DNS (Domain Name System)
  - parents, 218
  - permissions to manage Group Policy, 155
  - remote management within, 65
  - root domains, 18
  - structural overview of, 223
  - subdomains, 18
  - time synchronization, 137
  - top-level (TLDs), 218
  - trees in, 225–227
  - Windows Domain Manager, 252



Domains And Trusts snap-in, 226–227

drive letters

- assigning, 407, 408, 425, 443–444
- changing on standards-based systems, 436
- moved disks, of, 405
- standard volumes, assigning to, 442

drive paths, 407, 443

Driveletter\$ share, 475

drivers, device, 42, 53, 75–76, 311, 545

drives

- basic, 395, 401–404, 421
- dynamic. *See* dynamic drives
- hard disk. *See* hard disk drives
- network drives, 484–485
- partitioning. *See* partitions
- tape drives, 523–525
- volumes on. *See* volumes

Ds commands, list of, 251

DsacIs.exe, 252

Dsquery commands, 242–243, 251

dual boot systems, 421

dump files, 84–85

DVDs for backups, 525, 535, 541

dynamic drives

- capabilities of, 401
- compared to other types, 395, 421
- converting to and from basic disks, 402–404
- drive section types, 402
- moving to new systems, 404–405
- RAID capabilities of, 420
- reactivating, 404
- UNIX compatibility of, 402

Dynamic Host Configuration Protocol. *See* DHCP (Dynamic Host Configuration Protocol)

dynamic IP addressing, 568–569

dynamic updates, 645. *See also* DHCP (Dynamic Host Configuration Protocol)

dynamic-link libraries (DLLs), 39, 51

## E

ECHO command, 49

editions of Windows Server 2012, 6

EFS (Encrypting File System)

- backing up certificates, 554–555
- copying encrypted files, 416
- data recovery system of, 414–415, 417
- decrypting files and directories, 418

- granting special access to encrypted files, 416
- mechanics of, 414
- NTFS with, 413
- ownership of files, 414
- recovery policy, configuring, 417, 551–553
- restoring certificates, 555
- roaming profiles with, 362
- steps for encrypting files, 415–416

elevation prompts, 5, 6, 93

email

- distribution groups, 303
- setting for user accounts, 348
- SMTP Server, 37

enable- cmdlets, 25

encryption

- AES (Advanced Encryption Standard), 361
- backing up certificates, 554–555
- BitLocker Drive Encryption, 35
- compression not allowed with, 413
- copying encrypted files, 416
- data recovery system for files, 414–415, 417
- decrypting files and directories, 418
- drive hardware encryption, 391
- EFS. *See* EFS (Encrypting File System)
- mechanics of, 414
- NTFS, with, 413, 416
- recovery policy for, 551–553
- restoring certificates, 555
- SMB, 457, 459
- steps for encrypting files, 415–416
- user profiles for certificates, 414

End Task command, 89–90, 94

enhanced Active Directory recycle bin, 247–248

Enhanced Fine-Grained Password Policy, 222

Enhanced Storage, 36, 386

Enterprise Admins group, 315–317

environment variables

- configuring, 81–83
- SET commands, 52
- %UserName%, 352–353, 355, 363–364, 376–377

errors. *See also* events

- event levels of, 112
- improvements in recovery mechanisms for, 541–542
- Microsoft Online Crash Analysis, 543–544

- Stop errors, 84–85
- eSATA, 397
- event logs. *See also* logs
  - archives, of, 116–118
  - clearing, 116
  - custom views, creating, 112–114
  - data collector sets, 124–130
  - Data column, 112
  - DNS servers, of, 648
  - Event Viewer, 111–115
  - filtering, 112–115
  - Forwarded Events log, 108
  - levels of events, 111–112
  - list of available, 108–109
  - Log Properties dialog box, 115–116
  - options for, setting, 115–116
  - overwriting modes, 116
  - properties, columns of, 110, 112
  - remote management of, 67
  - security templates for, 193–195
  - Server Manager for viewing, 109–115
  - size, setting maximum, 115
  - task categories of, 112
  - viewing archives of, 118
  - Windows Event Log service, 108–109
- Event Viewer, 4, 111–115
- events
  - Audit Success or Failure, 112
  - command-line commands for configuring, 43
  - Critical, 112
  - Error, 112
  - Event Viewer, 111–115
  - Events, Server Manager, 60
  - IDs of, 110, 112
  - informational, 111
  - levels of, 111–112
  - properties of, 110
  - Server Manager for viewing, 109–115
  - task categories of, 112
  - traces, data collector sets, 125
  - Warning, 112
- Everyone group
  - Full Control share permission default, 468
  - Guest account membership in, 308
- Everyone identity, 318
- EXIT command, 49
- expired accounts, 375
- exporting accounts, 372
- extended partitions, 407

## F

- Failover Clustering, 36
- failover scopes, DNS, 579, 602–605
- failures, system, recovery mechanisms for, 541–544
- fan speeds, 8
- FAT file systems, 392–393, 445–447, 451–452, 458
- fault tolerance, RAID for, 426–427
- Fax Server, 4, 34
- FAX\$ share, 474
- features
  - Add Roles And Features Wizard, 58, 70–72
  - adding with ServerManager, 63
  - add-windowsfeature command, 63
  - associations with types of installations, 55–56
  - configuring, tool for, 32
  - get-windowsfeature command, 63
  - Remove Roles And Features Wizard, 71, 72–73
  - subordinates, adding all, 63
  - table of, 35–39
- federation services, 15, 33, 297
- File And Storage Services, 34, 394, 468–469
- file compression, 49, 410–412, 425
- File Explorer
  - Control Panel access from, 7
  - decrypting files and directories, 418
  - file encryption with, 415–416
  - network drives, 484–485
  - object ownership, 486–487
  - permissions, setting, 487–488, 491–495
  - restoring shadow copies, 482–483
  - special shares, connecting to, 475–476
  - viewing permissions, 488–489
- file paths, security templates for, 198–201
- File Replication Service log, 109
- File Server Resource Manager (FSRM), 387, 513–518
- File Server role service, 34, 387
- File Server VSS Agent Service, 387
- file servers, 385–389, 488
- file sharing
  - administrative shares, 474–476
  - advanced management properties, 468
  - Advanced Sharing Settings, 460–461
  - central access policies, 459
  - claims-based access controls, 459

file sharing, *continued*

- clients currently accessing, viewing
  - number of, 462
- closing open shares, 478
- creating shared folders, 463–468
- Enable Access-Based Enumeration option, 467
- File And Printer Sharing, enabling or disabling, 461
- file systems supporting, 458
- get-smbshare cmdlet, 461
- hidden shares, 464, 474–476
- Hyper-V issues, 468
- modifying settings for folders, 468–469
- multiple shares on single folders, 465–466
- naming shares, 464, 466
- net session command, 476–477
- net share command, 461
- NFS for, 34, 36, 463, 466, 479–481
- NTFS permissions, viewing, 488
- offline setting options, 464–465, 467
- permissions for. *See* share permissions
- public folder sharing, 458–460
- publishing shares, 469
- quota templates, 468
- SMB protocol for, 209, 457, 459, 461, 466, 468
- special shares, 474–476
- standard, 457–468
- stopping sharing on folders, 478–479
- viewing existing shares, 461–463
- viewing sessions of, 476–478

file systems

- allocation unit size, setting, 409, 411
- changing on standards-based systems, 436
- determining type of, 421
- FAT, 392–393, 445–447, 451–452, 458
- list of supported, 392–393
- MFT (master file table), 393
- NTFS. *See* NTFS file system
- organization of, 385
- partitions, relation to, 392
- ReFS (Resilient File System), 393, 449, 459, 504
- repairing errors, 437
- selecting for partitions, 409, 411
- standard volumes, formatting with, 442

files

- basic permissions for, 491–493

- compressing, 412
- encrypting, 415–416, 551–553. *See also* EFS (Encrypting File System)
- expanding compressed, 413
- inheritance options for, 495
- restoring, 550–551
- searching for, 7
- special permissions for, 490, 493–495

FIND command, 49

fingerprint-based authentication, 38

FireWire, 396–397

firmware, ACPI version compliance, 10

folders

- encrypting, 415–416
- inheritance options for, 495
- NTFS permissions, viewing, 488
- parent-child relationships, 487
- redirection, 173–177
- restoring nonsystem, 550–551
- security templates for, 200–201
- setting permissions for, 491–495
- sharing. *See* file sharing; shared folders
- special permissions for, 491

FOR command, 49

Force Shutdown From A Remote System privilege, 311

foreground processes, 87

forests, domain, 148, 225–227, 317

FORMAT command, 49

formatting partitions, 407, 409–411, 425

forward lookups, 624

Forwarded Events log, 108

FQDN (fully qualified domain name)

- group account names using, 302
- logon names using, 301–302
- services, identifying for, 101
- structure of, 218–219, 616

FSMO (flexible single-master operation)

- role, 71, 273, 276. *See also* operations masters

FSRM (File Server Resource Manager), 387

Fsutil, 389

FTP command, 49

full backups, 521, 525, 528–529

Full Control permission, 489

Full Control share permission, 470

full-server installations

- features included in, 4, 40
- minimal-interface installations, converting to and from, 56

- functional levels
  - 2003 mode, 231, 232–233, 235–236
  - 2008 mode, 231, 233–234
  - 2012 mode, 231–232, 235
  - 2008 R2 mode, 231–232, 234–235
  - Adprep for upgrading, 232–235
  - lists and descriptions of, 225–227, 231–232
  - minimal level requirement, 232
  - raising, 236–237

## G

- G states, 11
- Gadgets, Windows, 5
- gateways, 568–570
- Generate Security Audits privilege, 311
- get- cmdlets, 25
- get-help cmdlet, 25
- get-service command, 26
- get-smbshare command, 461
- global catalogs
  - authentication role of, 231
  - configuring, 239, 280
  - domain controller assignment of, 239–240
  - ports used by, 292
  - universal membership caching, 281
- global groups
  - accounts, creating, 336–337
  - best use of, 305–306
  - definition of, 303
  - scope capabilities, 304
- global user rights configuration, 328–329
- GlobalNames zone, 619
- gpedit.msc command, 144
- GPMC (Group Policy Management Console)
  - Active Directory, use of, 149
  - Add Forest command, 148
  - administrative templates, 150–152
  - ADMX format, 141–142
  - auditing, configuring, 498–500
  - autoenrollment, 186–187
  - Automatic Update management, 187–190
  - backing up GPOs, 165
  - blocking inheritance, 156–158
  - central store, 142
  - Computer Configuration node, 149–150
  - copying GPOs, 164
  - creating GPOs, 152–153
  - creating local policies, 146
  - delegation of privileges to manage, 154–155
  - deleting GPOs, 170–171
  - deploying software, 183
  - disabling GPOs, 144, 166
  - Domains node, 149
  - editing a GPO, 144–145, 149
  - Editor choices, 141
  - enforcing inheritance, 157–158
  - gpmc.msc command, 148
  - Group Policy Modeling node, 149
  - Group Policy Object Editor, 141
  - Group Policy Results node, 149
  - importing GPOs, 164–165
  - inheritance, managing, 155–158
  - installing, 141
  - link order, changing, 156
  - link removal, 170–171, 213
  - linking GPOs to containers, 152–153
  - links vs. accessing actual GPOs, 149
  - local GPOs, 143–146
  - Local Object Editor, 141
  - loopback processing settings, 167
  - Modeling Wizard, 161–163
  - node structure, 148
  - opening, 148
  - opening local policies, 146
  - OS version issues, 141–143
  - permissions to manage GPOs, granting, 155
  - Policies node, 150
  - precedence preferences, setting, 156, 167
  - Preferences node, 150
  - redirecting special folders, 174–177
  - refreshing Group Policy, 158–161, 166
  - restoring GPOs, 165–166
  - Results node, 166, 171
  - RSoP (Resultant Set of Policy), 166, 171–172
  - script assignment with, 178–181
  - security template deployments, 205
  - shortcuts, 150
  - Sites node, 149
  - slow-link detection, configuring, 167–170
  - Software Settings node, 150
  - starter GPOs, 141, 153
  - troubleshooting, 171–172
  - User Configuration node, 150
  - Windows Settings node, 150

- GPOE (Group Policy Object Editor). *See* GPMC (Group Policy Management Console)
- GPOs (Group Policy Objects)
  - account policies, setting, 321–322
  - administrative templates, 151–152
  - Administrators and Non-Administrators local layer, 143–144, 146
  - auditing, configuring, 498–503
  - backing up, 165
  - blocking inheritance, 156–158
  - central stores for, 142
  - claims-based policy deployment, 299–300
  - conflict resolution, 144
  - containers, 138–139
  - copying, 164
  - creating, 152–153
  - default domain policies, 147, 172–173
  - definition of, 138
  - delegation of privileges to manage, 154–155
  - deleting, 170–171
  - disabling local, 144
  - disabling unused parts of, 166
  - editing. *See* GPMC (Group Policy Management Console)
  - event log, 143
  - folder for domain policies, 148
  - Folder Redirection, editing, 173–177
  - gpedit.msc command, 144
  - importing, 164–165
  - inheritance, 138–139, 155–158
  - link order, changing, 155–156
  - link removal, 170–171
  - linking to containers, 152–153
  - local, 143–146
  - local Group Policy Object, 143–146
  - logon/logoff script assignment with, 180–181
  - loopback processing settings, 167
  - Machine folder, 145–146, 148
  - precedence of, 152, 155–158, 167
  - priority of local GPOs, 144
  - refreshing, 158–161, 166
  - replication of, 142
  - restoring, 165–166
  - RSOP (Resultant Set of Policy), 171–172
  - security policies, including in, 212
  - security template deployments, 204–205
  - shutdown script assignment with, 178–179
  - starter GPOs, 153
  - startup script assignment with, 178–179
  - User folder, 145–146, 148
  - user rights assignments to, 328
  - User-specific local Group Policy layer, 144, 146
- Gpresult command, 171–172
- GPT (GUID partition table), 392, 399, 403, 407
- Gpupdate, 161
- Graphical Management Tools And Infrastructure, 57
- Graphical Shell, 4, 56
- group accounts
  - basic operation of, 302–303
  - built-in capabilities for, 313–315
  - creating, 335, 336–338
  - default groups used by administrators, 315–317
  - deleting, 373
  - global, creating, 336–337
  - implicit groups, 317–318
  - local, creating, 337–338
  - logon rights for, 312–313
  - names of, 302
  - privileges available, table of, 310–312
  - SIDs of, 304–305
  - tools for creating, 318
  - user accounts compared to, 300–301
- Group Managed Service Accounts, 222
- Group Policy
  - Active Directory, relation to, 138
  - administrative templates, 151–152
  - auditing, configuring, 498–503
  - autoenrollment, 186–187
  - Automatic Updates, managing, 187–190
  - blocking inheritance, 156–158
  - capabilities of, 138
  - claims-based policy, 298
  - compatibility with OS versions, 140
  - console. *See* GPMC (Group Policy Management Console)
  - containers, 138–139
  - delegation of privileges to manage, 154–155
  - deleting, 170–171
  - deploying software using, 181–188
  - disabling unused parts, 166
  - disk quota issues with, 504

- EFS recovery agents, 553
  - folder redirection management with, 173–177
  - gpedit.msc command, 144
  - GPMC. *See* GPMC (Group Policy Management Console)
  - inheritance, 155–158
  - links, 149, 152–153, 156, 170–171
  - local, 138, 327–330
  - logging of, 143
  - loopback processing settings, 167
  - Management Console, 36
  - managing, 141–161. *See also* GPMC (Group Policy Management Console)
  - manual refreshes, 161
  - mobile devices, for, 168
  - Modeling Wizard, 161–163
  - NTFS disk quota policy, 505–508
  - objects. *See* GPOs (Group Policy Objects)
  - order of application, 139
  - permissions to manage, 154–155
  - precedence of, 152, 155–158, 167
  - recovery policy configuration, 417
  - refreshing, 140, 158–161, 166
  - replication of, 142
  - requirements, 140
  - Restricted Groups settings, 195–196
  - RSOP (Resultant Set of Policy), 154, 166, 171–172
  - script assignment with, 178–181
  - security template deployments, 204–205
  - security templates for. *See* security templates
  - sequence of application, 139–140
  - slow-link detection, 167–170
  - troubleshooting, 171–172
  - user rights, for, 327–330
  - user vs. computer policies, 139–140
  - Windows Update for payloads, 64–65
  - Wired Network node, 562
  - Wireless Network node, 562–563
  - Group Policy Client service recovery setting, 106
  - Group Policy Management Console (GPMC). *See* GPMC (Group Policy Management Console)
  - Group Policy Management Editor, 321–322
  - Group Policy Object Editor (GPOE), 141. *See also* GPMC (Group Policy Management Console)
  - groups
    - accounts of. *See* group accounts
    - adding members to, 339–340, 375
    - auditing, 502–503
    - best use of types of, 305–306
    - built-in, 308–309
    - built-in capabilities for, 313–315
    - claims-based access controls, 496–498
    - computer, 339–340, 503
    - configuring by scope, 306
    - finding in Active Directory, 350–351
    - Guests group, 308
    - implicit, 308–309, 317–318
    - listing, 368–369
    - local. *See* local groups
    - permissions, setting, 380–381
    - policy for. *See* Group Policy
    - primary, 340
    - rights of members of, 327
    - scopes of, 303–304
    - server, remote management of, 68–70
    - types of groups, 302
  - Guest account, 308
  - Guests group, 308
  - GUIDs (globally unique identifiers), 262
- ## H
- handles
    - I/O, utilization of, 97
    - process, 92
  - hard disk drives. *See also* drives
    - active partitions, 402
    - Advanced Format drives, 389
    - allocation unit size, setting, 409, 411, 425, 442
    - analyzing, 453–454
    - average seek time, 390–391
    - backups of. *See* backups
    - basic, 395, 401–404, 421
    - boot partitions, 402
    - capacity property of, 421
    - Check Disk, 450–453
    - compression, enabling, 410–412, 425
    - crash dump partitions, 402
    - defragmenting, 453–455
    - disk controllers, duplexing, 429
    - Disk Management for configuring, 394–396
    - Disks node options, Server Manager, 437–438

hard disk drives, *continued*

- drive interface architectures supported, 390
- drive paths, 407
- drive section types, 402
- drivers for, loading during installations, 53
- dynamic. *See* dynamic drives
- expanding compressed drives, 412–413
- fault tolerance, 426–427
- file systems of. *See* file systems
- Foreign status, 400
- FORMAT command, 49
- Free Space, 394
- GPT (GUID partition table), 392, 399, 403, 407
- hardware encryption, 391
- hot swapping, 398
- initializing, 398–399
- installing, 398–399
- listing for a computer, 405
- logical drives, 392, 401, 404, 407
- manager for. *See* Disk Management
- maximum sustained data transfer rate, 391
- MBR (master boot record), 392, 399, 403, 406–407
- mean time to failure, 391
- moving to new systems, 404–405
- network drives, 484–485
- No Media status, 400
- Not Initialized status, 400
- Offline status, 399, 404
- Online status, 399, 404
- optimizing, 453–455
- paging, configuring, 77–80
- partitions. *See* partitions
- physical drive formats, 389–392
- physical sector sizes, 389
- planning considerations, 389
- preparing for use, 392–394
- properties, viewing, 395–396
- reactivating, 404
- removable disks, 395
- removable storage devices, 396–398
- removing, 405
- rescanning all drives, 404
- resetting, 437
- Resource Monitor Disk usage statistics, 120
- rotational speed, 390–391

- selecting for inclusion in volumes, 424–425
- self-healing NTFS, 450–451
- Standard Format drives, 389
- standard volumes, creating, 441–443
- status values, table of, 399–400
- system volumes, 402
- temperature characteristics, 391
- Transactional NTFS, 449–450
- types of disk configurations, 395
- uninstalling, 405
- unmounted drives, 443
- Unreadable status, 400, 404
- Unrecognized status, 400
- VHD (virtual hard disk), 395
- virtual. *See* standards-based storage; virtual disks
- virtual hard disks, adding or removing roles, 71–72
- volume status issues, table of, 422–423

hardware

- backups, options for, 522–524
- built-in diagnostics for, 543
- configuration, 6
- CPUs. *See* processors
- disks. *See* hard disk drives
- Hardware Events log, 109
- Hardware tab access to configuration, 75–76
- independence, modularization for, 5
- hibernate state, absence of, 5
- hidden shares, 474–476
- home directories, user accounts, 351, 353–355, 371, 373, 377
- Home network type, 12
- hot swapping, 398
- hotfixes, 43
- Hyper-V
  - file sharing issues, 468
  - network configuration for, 570–571
  - service description, 34

I

- Identity Federation Support service, 33
- idle processor states, 10–11
- IE ESC (Internet Explorer Enhanced Security Configuration), 61
- IIS (Internet Information Services)
  - IIS (Web Server) role, 35
  - service accounts for, 341

- WinRM Extension for, 39
- images, Windows
  - DISM command, 49
  - features, installing from PowerShell, 63–64
- Impersonate A Client privilege, 311
- implicit accounts, 306
- implicit groups
  - Everyone group, 308
  - list of, 317–318
  - role of, 309
- importing accounts, 372
- Increase privileges, 311
- incremental backups, 521–522, 525, 528–529
- indexes, 221
- InetOrgPerson object, 301
- infrastructure masters
  - duties of, 243
  - global catalogs, relation to, 239
  - seizing, 276–280
  - transferring, 276
  - viewing, 273–274
- inheritance
  - ACEs, of, 297
  - GPOs, of, 138–139, 155–158
  - object permissions, of, 487–488
  - options for, 495
- Ink and Handwriting Services, 36
- installations
  - 64-bit processor requirement, 43–44
  - changing the type, 55–56
  - clean, steps for, 44–47
  - clean vs. upgrades, 43
  - command line use during, 48–49
  - disk space required for, 44
  - full-server installations, 4, 40, 56
  - hardware requirements, 43–44
  - keyboard layouts, 44–45
  - licensing terms, 45
  - minimal-interface installations, 4, 40, 56
  - partitions, managing during, 52–55
  - product keys, 45, 47
  - Server Core installations, 4, 40–47, 56–58, 526
  - Server With A GUI installations, 4. *See also* full-server installations
  - Server With Minimal Interface installation, 4, 40, 56
  - type of, choosing, 45, 48
  - types changeable after installation, 4
  - upgrades, steps for performing, 47–48
  - Where Do You Want to Install Windows, 45–46
- Interactive identity, 318
- Internet Explorer, 61
- Internet Printing, 4, 34, 36
- Internet Storage Naming (iSNS) Server Service, 36
- intersite replication topology, 291–292
- intranets, 15, 18
- IP addresses
  - assignment methods for, 566
  - conflicts, avoiding, 591
  - dial-in connections, assigning static, 359–360
  - disabling for DNS, 646
  - DNS records mapping to, 636–637
  - dynamic configuration of. *See* DHCP (Dynamic Host Configuration Protocol)
  - exclusion ranges, setting, 607–608
  - IP Address Management Server, 36
  - IPAM servers for managing, 137
  - multicast scopes, 598
  - name resolution for. *See* name resolution
  - normal scopes for, 593–598
  - reserving DHCP, 607–610
  - scopes of, 578–579, 582, 599–601
  - static addresses, 566–568
  - superscopes, 579, 592–593
- IPC\$ share, 474
- ipconfig
  - all parameter, 42
  - autoconfiguration addresses, 578
  - MAC addresses, 606–607
  - Mini Windows PC version, 50
  - releasing reserved addresses, 609–610
- IPv4 addresses
  - BOOTP (Bootstrap Protocol), 601
  - configuring, 564–569, 573–575, 591
  - conflicting addresses, avoiding, 591
  - decimal expressions of, 13–14
  - dynamic addressing, 573–575
  - failover scopes, 602–605
  - MAC address filtering, 606–607
  - normal scopes for addresses, 593–597
  - reserving addresses, 608
- IPv6 addresses
  - configuring, 564–569
  - decimal expressions of, 13–14
  - dynamic addressing with, 575–577



- IPv6 addresses, *continued*
  - enabling for client computers, 617–618
  - LLMNR for name resolution, 22–23
  - normal scopes for, 579, 596–598
  - reserving addresses, 608–609

## iSCSI

- iSCSI Target role services, 387
- iSNS Server Service, 36
- new virtual disk, creating, 436
- role services for, 436
- Target Server service, 34
- ISTG (Inter-Site Replication Topology Generator), 291–292

## J

- joining computers to domains or workgroups, 267–270

## K

### Kerberos

- account security options for, 361
- with Armoring, 222, 297–298, 496
- authentication with, 296
- claims-based access controls, 496–498
- configuring policies for, 321–322, 326–327
- constrained delegation across domains, 222
- preauthentication, 361
- tickets, 327
- Kerberos with Armoring, 222, 297–298, 496
- kernel, OS
  - Kernel Transaction Manager (KTM), 450
  - memory statistics, 98
  - usage, tracking, 96
- key masters, 633–634
- keyboard layouts, 44–45
- KTM (Kernel Transaction Manager), 450

## L

- LABEL command, 50
- LAN Manager authentication, 209–210
- language independence, modularization for, 5
- laptops running Windows Server, 8
- Last Known Good Configuration, 545
- latency, network, 134
- LDAP (Lightweight Directory Access Protocol)

- Active Directory Administration Tool, 252
- Active Directory use of, 242
- importing files with LDAP attributes, 372
- InetOrgPerson object for, 301
- ports used by, 292
- Security Configuration Wizard setting for, 209

### Ldp.exe, 246

- level 0, RAID, 426–428, 434
- level 1, RAID, 426–434
- level 5, RAID, 426–427, 431, 434–435
- licensing, 34, 42
- Linear Tape Open (LTO), 523
- link-layer filtering, 606–607
- Link-Local Multicast Name Resolution (LLMNR), 22–23
- List Folder Contents permission, 489
- List Folder/Read Data special permission, 490–491
- LLMNR (Link-Local Multicast Name Resolution), 22–23, 37, 618
- load balancing
  - of failover scopes, 602–605
  - Network Load Balancing (NLB), 37, 63
- local groups
  - adding users to, 338
  - creating, 337–338
  - local GPOs, 143–146
  - Local Group Policy Editor, 313–315
  - local policies, 327–330
  - security templates for local policies, 193–195
  - types of, 303

### local profiles

- changing types of, 368
- creating, 363, 366
- managing, 366–368
- names of, 365
- purpose of, 362
- local user accounts
  - assigning to local groups, 337–338
  - creating new, 334–335
  - definition of, 301

### Local Users And Groups

- local group creation, 337–338
- passwords, resetting, 373
- LocalService account, 307, 504
- LocalSystem account, 307
- locked out accounts, 373–374, 379
- lockout policies, 325–326
- logging. *See* auditing; logs

- logical drives, 392, 401, 404, 407–408, 445
- logical processors, 6, 10–11
- logical structures, domain, 223
- logoff scripts, 180–181
- logon names
  - creating for an account, 331, 333–334
  - naming schemes for, 320
  - numeric code assignment, 320
  - parts of, 301–302
  - pre-Windows 2000, issues with, 331, 333
  - rules for, 319
- logon rights, 312–313
- logon scripts
  - assigning, 180–181
  - environment variable for path, 352
  - paths, setting, 351
  - renaming, 371
  - specifying, 353–354
  - %UserName% in, 376–377
- logons
  - Anonymous Logon identity, 317
  - authentication protocols for, 296–297
  - error messages from, 379–380
  - failures, logging, 379
  - forcibly disconnecting users when logon
    - hours expire, 357
  - hours allowed for, managing, 355–357, 377
  - lockout policies, 325–326
  - names for. *See* logon names
  - options for controlling, 378
  - passwords for. *See* passwords
  - permitting by workstation, 357–358, 378, 380
  - rights, 312–313
  - scripts. *See* logon scripts
  - security tokens generated by, 305
  - Server Core, 40–41
  - troubleshooting, 378–380
  - user profile issues, 361. *See also* user profiles
  - validation of. *See* authentication
- logs
  - archives, of, 116–118
  - auditing with. *See* auditing
  - clearing, 116
  - data collector sets, 124–130
  - DHCP logs, 585–586
  - Event Viewer, 111–115
  - Hardware Events log, 109
  - levels of events, 111–112
  - list of available, 108–109

- Log Properties dialog box, 115–116
  - overwriting modes, 116
  - properties, columns of, 110, 112
  - Server Manager for viewing, 109–115
  - size, setting maximum, 115
  - Stop error logging, 84
  - Windows Event Log service, 108–109
- loopback processing, Group Policy, 167
- Lpd.exe, 252
- LPR Port Monitor, 36
- LTO (Linear Tape Open), 523
- LUNs. *See* virtual disks

## M

- MAC address filtering, 606–607
- MAC addresses, 13–14
- Manage Auditing And Security Log privilege, 312
- managed service accounts, 341–344
- mandatory user profiles, 362, 364, 379–380
- mapping network drives, 475–476, 484–485
- masters. *See* operations masters
- maximum processor state, 8–11
- MBR (master boot record)
  - basic to dynamic disk conversions, 403
  - GPT compared to, 392
  - number of allowed partitions, 406–407
  - selecting during initialization, 399
- Media Foundation feature, 36
- member servers, relation to domains, 14
- memory
  - allocating between OS and applications, 130
  - available, guideline for, 131
  - built-in diagnostics for, 543
  - Cached statistic, 98
  - counters, table of, 131–132
  - Data Execution Prevention, 80–81
  - dump files, 84–85
  - Lock Pages In Memory privilege, 312
  - NP (nonpaged) pool, 92
  - page faults, 92, 131–132
  - peak working set, process, 92
  - Performance tab, Task Manager for
    - statistics, 97–98
  - performance tuning, 130–132
  - processes, reserved for, 90
  - Resource Monitor usage statistics, 120
  - virtual, configuring, 77–80
  - Windows Memory Diagnostic Tools, 548
- Message Queuing, 36

MFT (master file table), 393  
 Microsoft Exchange Server  
     service accounts for, 341  
     Windows Server Backup with, 527  
 Microsoft Management Console, 4  
 Microsoft Online Backup Service, 525, 527  
 Microsoft Online Crash Analysis, 543–544  
 Microsoft Update, 35  
 MicrosoftWindows log, 109  
 migration, 47  
 mini Windows PC commands, 48–52  
 minimal-interface installations, 4, 40, 56  
 minimum processor state, 8–11  
 MINWINPC commands, 48–52  
 mirrored sets, 426–434  
 mobile device networking, 168  
 Modeling Wizard, Group Policy, 161–163  
 Modify Firmware Environment privilege, 312  
 Modify permission, 489  
 modularization, 5  
 monitoring servers, 118–119. *See also*  
     performance  
 monitors, 7, 76–77  
 MPIO (Multipath I/O), 36, 386  
 MS-DOS, RAID noncompliance of, 427  
 MSI (Microsoft Installer), 43, 182–183  
 multicast scopes, 579, 598  
 multimaster replication model, 14  
 Multipath I/O (MPIO), 36, 386  
 multiple operating systems, 83–84  
 multiple processor cores support, 6  
 multiple processor systems, 96, 122

## N

name protection, 586  
 name resolution  
     appending suffixes automatically, 620  
     client computer settings for, 620–621  
     Computer Name tab, 74–75  
     DNS for. *See* DNS (Domain Name System)  
     DNSSEC (DNS Security Extensions), 19–20, 632–634  
     forward lookups, 624  
     LLMNR for, 22–23  
     reverse lookups, 624, 628–629  
     services supported, 17  
     single-label name resolution, 619  
     WINS for, 20–21  
  
 name servers, adding, 639–640  
 names of computers, 46–47, 75  
 naming contexts, 289–290  
 NAP (Network Access Protection), 588–591  
 NAT64/DNS64 support, 13  
 NDF (Network Diagnostic Framework), 564  
 net commands  
     list of, 50–51  
     net help command, 23  
     net session command, 476–477  
     net share command, 461  
 .NET Framework, 37  
 NetBIOS, 20–21, 50, 618  
 Net-DMA (network direct memory access), 13  
 Netdom commands, 42, 252, 265–266, 279–280  
 NETLOGON share, 474  
 Netmon, 564  
 Netsh command, 42, 46, 51, 564, 591  
 Network Access Protection (NAP), 588–591  
 network adapters  
     adding, assessing need for, 99  
     DHCP server bindings, configuring, 584  
     discovery settings, 560–561  
     installing TCP/IP, 565–566  
     MAC addresses, 13–14  
     network connections of, 571–572  
     NIC Teaming, 61  
     performance issues, 134  
     utilization statistics, 98  
     virtual, for Hyper-V, 570–571  
 Network And Sharing Center  
     Advanced Sharing Settings, 460–461  
     alternate IP addressing, 568–569  
     DNS settings, 620–621  
     IP addressing, 567–569  
     multiple gateway configurations, 569–570  
     network connections, 571–572  
     Network Connections page, 562  
     settings, basic, 12  
     status indicators of, 561–562  
     troubleshooting options, 562  
 network authentication, 296–297  
 Network Awareness, 560  
 network connections, 571–572, 584  
 network device configuration, 6  
 Network Device Enrollment Service, 33  
 Network Diagnostic Framework (NDF), 564

- Network Diagnostics, 559, 564
- network direct memory access (Net-DMA), 13
- Network Discovery, 12, 560–562
- network drives, 484–485
- Network Explorer, 559–561
- Network File System. *See* NFS (Network File System)
- Network Load Balancing (NLB), 37, 63
- Network Location Awareness, 143
- Network Monitoring, 564
- Network Policy and Access Services (NPAS), 34, 588–591
- Network Policy Server, 588–591
- Network Unlock, 391–392
- networking
  - addresses, network, 13–14. *See also* IP addresses
  - administrative template policies for, 151
  - costed networks, 168
  - DirectAccess, 13
  - discovery, 12, 560–562
  - DNS64 support, 13
  - domain names. *See* DNS (Domain Name System)
  - dynamic address assignment. *See* DHCP (Dynamic Host Configuration Protocol)
  - Ethernet properties configuration, Server Manager, 60–61
  - Home network type, 12
  - Hyper-V with, 570–571
  - IPv4. *See* IPv4 addresses
  - IPv6. *See* IPv6 addresses
  - latency issues, 134
  - mobile device policies, 168
  - name servers, without, 22–23
  - NAT64/DNS64 support, 13
  - Netsh command, 42, 46, 51, 564, 591
  - Network identity, 318
  - performance tuning, 134
  - ping command, 567
  - private networks, 12, 626–627
  - profile management, 562
  - public networks, 12, 626–627
  - Resource Monitor usage statistics, 120
  - security features, list of, 563
  - security policy configuration, 209
  - sharing settings, 12
  - TCP Chimney Offload, 13
  - TCP/IP. *See* TCP/IP protocol
  - Teredo, 564
  - tool suite for, 11–12
  - tools for, list of, 559–560
  - types of networks, 12, 560
  - utilization statistics, 98
  - Work network type, 12
- NetworkService account, 307, 504
- new- cmdlets, 25
- new features of Windows Server 2012, 6–7
- Next Generation TCP/IP stack, 14
- NFS (Network File System)
  - Client for NFS, 36
  - file sharing with, 463, 479–481
  - role service for, 34
  - Server for NFS role service, 387
  - share profile options, 466
- NLB (Network Load Balancing), 37, 63
- No Access share permission, 469
- normal backups, 521, 525, 528–529
- normal scopes, 579, 593–598
- Notepad, 41
- NP (nonpaged) pool, 92, 98
- NPAS (Network Policy and Access Services), 34
- NPS (Network Policy Server), 358
- ntdsutil command, 251, 276
- NTFS disk quotas
  - enabling on per-volume basis, 508–510
  - Group Policy for, 505–508
  - importing and exporting, 512–513
  - limits, 504
  - managing, 510–513
  - vs. Resource Manager disk quotas, 503
- NTFS file system
  - compression, enabling, 410
  - converting volumes to, 445–447
  - encryption with, 413, 416
  - file sharing, advantages for, 463
  - permissions, 458, 488
  - quotas. *See* NTFS disk quotas
  - self-healing NTFS, 450–451
  - structure of volumes, 393
  - Transactional NTFS, 449–450
- NTLM authentication, 296
- NX (no-execute) processor feature, 80

## O

## objects

- editing permissions for, 487
- group. *See* GPOs (Group Policy Objects)
- inheritance with, 487–488
- managers and management tools for, 485–486
- ownership of, 486–487
- types of, 485–486

Ocsetup.exe, 42

OCSP (Online Certificate Status Protocol), 563

offline domain join, 268–270

Online Certificate Status Protocol (OCSP), 563

Online Responder, 33

operating system recovery. *See* system recovery

## operations masters

- assignment of, 243
- definition of, 231
- domain naming master role, 242, 244
- infrastructure master role. *See* infrastructure masters
- PDC emulator role, 243–244
- relative ID master role, 242, 244
- required roles for Active Directory, 242–243
- schema master role, 242, 244
- seizing roles, 276–280
- single domain controller scenario, 243
- standby operations masters, 243
- transferring roles, 274–276
- viewing, 273–274

Optimize Drives, 453–455

Organization panel, 349

organizational units. *See* OUs (organizational units)

OS X file sharing with NFS, 463, 479–481

## OUs (organizational units)

- advantages of creating, 227–228
- default domain policies, 147
- definition of, 138
- managing, 228, 281–282
- permissions to manage Group Policy, 155

ownership of objects, 486–487

## P

packages for deploying software with Group Policy, 182

page faults, 92, 131

paged pool, 92, 98, 132

paging, 77–80, 402

parent domains, 18, 218, 615

parent objects, 487

parity checking, 426

## partitions

active, 402, 445

basic to dynamic disk conversions, 402

boot, 402, 433–434, 443

clean installations, options for, 44

compression, enabling, 410–412

crash dump, 402

creating, 54, 407–410

deleting, 52–55, 445

DiskPart utility, 49, 52–53

extended, 55, 407

file system format, selecting, 409, 411

formatting, 54, 407, 409–411, 425

GPT (GUID partition table), 392, 399, 403, 407

installations, changing during, 53–55

labeling, 409, 425

logical drives in, 392, 401, 404, 407

MBR (master boot record), 392, 399, 403, 406–407

mounting in empty NTFS folders, 408

number allowed per drive, 407

preparing, 392–394

primary, 407

quick formats, 410–411

resizing, 447–449

structure of, 406–407

system partitions, 402

passive cooling mode, 8–9

## passwords

Account Lockout policies, 325–326

Administrator accounts, for, 308

computer accounts, for, 264–266

managed service accounts, for, 343–345

new, creating for accounts, 332–333

options for controlling, 378

options for, setting at creation, 332–333

policies governing, 321–323

PSOs (password-setting objects), 222

resetting, 373

secure channel passwords, 264–266

secure password strategies, 320–321

- security account options for, 360–361
- security templates for, 193–195
- single sign-on, 296–297
- user accounts, relationship to, 302
- payloads, 24, 57, 63–65, 72, 218
- PDC emulator role, 243–244, 273–274, 276–280
- Peer Name Resolution Protocol, 37
- peer-to-peer networks with LLMNR, 22–23
- performance
  - alerts, 60, 129–130
  - applications options, 77
  - built-in diagnostics for, 543
  - CPU usage statistics, 96–97
  - c-states, 10–11
  - data collector sets, 124–130
  - Data Execution Prevention options, 80–81
  - disk striping for I/O speed, 426–428
  - graphics for, 76–77, 95–96
  - memory, tuning, 130–132
  - monitoring, goals for, 118
  - monitoring tool. *See* Performance Monitor
  - network tuning, 134
  - paging, configuring, 77–80
  - power option effects on, 8–11
  - processors, tuning, 132–133
  - Profile privileges, 312
  - p-states, 10–11
  - Server Manager Performance panel, 60
  - Task Manager Performance tab, 95–99
  - virtual memory, configuring, 77–80
- Performance Monitor
  - alerts, 129–130
  - counters, 121, 122–124
  - credentials needed for, 123
  - Data Collector Sets node, 124–130
  - graphic display, 121
  - instances, 122–123
  - objects, performance, 123
  - opening, 121
  - purpose of, 119
  - Reports, data collector, 128–129
  - views, 122
- permissions
  - Active Directory, setting, 380–381
  - backups, for, 528
  - basic, 488–493
  - claims-based access controls, setting for, 496–498
  - editing for objects, 487
  - file and folder permissions, table of, 489
  - file sharing. *See* share permissions
  - folder, security templates for, 200–201
  - Group Policy management permissions, 154–155
  - inheritance of, 487–488, 495
  - logon rights, granted by, 312–313
  - network drives, 484
  - NFS, 479–481
  - privileges, relation to, 310
  - security tokens for, 305
  - setting for files and folders, 491–493, 493–495
  - special, 489–491, 493–495
  - system services, setting, 197
- physical drives. *See* hard disk drives
- physical processors, 6
- physical structures, domain, 223
- ping command, 51, 567
- planning with Modeling Wizard, 161–163
- Pnputil.exe, 42
- PNRP (Peer Name Resolution Protocol), 37
- policy editors. *See* GPMC (Group Policy Management Console)
- policy objects. *See* GPOs (Group Policy Objects)
- ports used by Active Directory, 292–293
- power options, 5–11
- PowerShell. *See* Windows PowerShell 3.0
- preboot environment, 5
- predefined accounts, 306
- preinstallation environment, 5
- Previous Versions, 482–483
- primary computers
  - for folder redirection, 173
  - for restricting roaming, 363
- primary groups, 340
- primary partitions, 407
- printing, 34, 51, 151, 475
- private networks, 12, 560, 626–627
- privileges
  - processes, viewing for, 92
  - table of, for users and groups, 310–312
  - user accounts, granting to, 309–310
- problems, viewing current, 542
- process working set privilege, 311
- processes
  - dependencies of, 93–94
  - End Task command, 89–90, 94
  - executables, finding related, 90
  - foreground vs. background, 87
  - memory reserved for, 90, 91

processes, *continued*

- PIDs of, 90, 93–95
- properties of, columns for, 91–93
- publishers of, 90
- session IDs, 93
- status, determining, 89, 91
- thread counts, 93
- trees of, 94
- types of, 90
- waiting for locked resources, 93

## processors

- affinity settings, 10
- counters for, 132–133
- CPU usage statistics, 96–97
- c-states, 10–11
- logical processor idling, 10
- logical, viewing number of, 96
- multiple processor cores support, 6
- NX (no-execute) processor feature, 80
- performance tuning, 132–133
- power states of, 8–11
- processor architecture environment variable, 353
- p-states, 10–11
- scheduling options, 77
- thread queuing issue, 132
- throttling, 8–11
- usage, monitoring, 133

## product identifiers, 61

## product keys, 45, 46, 47, 73–74

profiles, user. *See* user profiles

## programs

- Apps, 7, 137, 363
- Debug Programs privilege, 311
- DEP exceptions for, 80–81
- deploying, 181–186
- directory data stores specific to, 15
- opening, options for, 7

## PROMPT command, 51

## properties

- resource, 298–299
- server, viewing in Server Manager, 60–62

## Proxy identity, 318

## PSOs (password-setting objects), 222

## p-states, 10–11

## Public folder, 458–460

## public networks, 12, 560–561, 626–627

## publishing

- data stores, 238
- process publishers, 90

## shares, 469

## software, 182

## trusted publisher list, 564

## Q

## Quality Windows Audio Video Experience, 37

## R

## RACTask, 122

## RAID

- backup systems using, 523–524
- deleting volumes, 426
- disk mirroring, 426–434
- disk striping, 426–428, 431, 434–435
- Diskraid.exe, 42
- level 0, 426–428, 434
- level 1, 426–433
- level 5, 426–427, 431, 434–435
- parity checking, 426
- queue length counter, 133
- repairing, 432–435
- supported levels of, 420

## RAS Connection Manager, 37

## Read Attributes special permission, 490–491

## Read permission, 489

## Read Permissions special permission, 490–491

## Read share permission, 470

## read-only domain controllers (RODCs), 16, 19, 219, 619

## reads, disk performance for, 133

recovery. *See also* restoring

- Active Directory, 245–248, 547
- EFS based, 414–415, 417
- encryption certificates, of, 551–553
- improvements in Windows Server 2012 for, 541–542
- nonsystem volumes with Windows Server Backup, 550–551
- policy, configuring, 417
- RECOVER command, 51
- Recovery screen options, 544
- safe mode startups, 544–546
- services, configuring for, 106–107
- Startup And Recovery dialog box, 83–85
- system. *See* system recovery
- system image recovery, 44, 544
- tools for, installing, 526–527
- Wbadm backup recovery commands, 533

- recovery point objective (RPO), 520–521
- recovery time objective (RTO), 520–521
- Recycle Bin, Active Directory, 222, 244–248
- redirected folders, 173–177, 363
- refreshing Group Policy, 158–161, 166
- ReFS (Resilient File System), 393, 449, 459, 504
- Regedit, 41
- register cache utilization, 96–97
- registry
  - administrative templates, 151–152
  - auditing, 502
  - data collectors for, 127–128
  - REG commands, list of, 51
  - security policy configuration, 209–210
  - security templates for, 198–200
- Regsvr32, 39
- relative ID master role
  - managing, 273–274
  - placement of, 244
  - purpose of, 242
  - seizing, 276–280
  - SID generation task, 302
  - transferring, 276
- Reliability Monitor, 119–122
- Remote Access service, 34, 358–360
- remote assistance, 6, 37, 136
- Remote Desktop
  - clients, viewing, 100
  - disconnecting, 100
  - managing, 136
  - RDP file signing, 564
  - Remote Desktop Services User identity, 318
  - remote management, independence of, 67
  - Services, 34, 61
  - Session Host, 4
  - Task Manager for managing, 99–100
  - utilization statistics, 100
- Remote Differential Compression, 37
- remote management
  - adding servers to Server Manager, 67–68
  - blocking for the local server, 66
  - credentials required for, 66–67
  - Disk Management capabilities, 394, 396
  - groups, 68–70
  - PowerShell for, 70
  - PowerShell Web Access for, 24
  - properties, 61
  - Remote Desktop independence of, 67
  - RSAT for, 37, 65, 135, 256
  - tasks available through, 65–67
  - tools available for, 65
  - web client WinRM IIS Extension, 26
  - Windows Firewall, applications enabled for, 66–67
  - WinRM, 25–29
- Remote Server Administration Tools (RSAT), 37, 65, 135, 256
- Remote Service Management, 67
- removable storage devices, 395–398, 443
- remove- cmdlets, 25
- Remove Computer From Docking Station privilege, 312
- Remove Roles And Features Wizard, 71, 72–73, 272–273
- Repadmin.exe, 252, 277, 293–294
- Repair Your Computer, 525
- Replace A Process Level Token privilege, 312
- replication
  - application directory partitions with, 238
  - bridgehead servers, 291–292, 293
  - cmdlets for viewing, 278–279
  - DFS Replication role service, 387
  - of directory data by domain controllers, 230–231
  - DNS configuration for, 625–626
  - domain controller multimaster model, 14
  - File Replication Service log, 109
  - of GPOs using DFS, 142
  - intersite replication topology, 291–292
  - listing data about, 293–294
  - recovering from failures of, 291
  - Repadmin.exe, 277–278, 293–294
  - Replication Diagnostics tool, 252
  - service dependencies of, 292
  - site links, 285–286
  - troubleshooting, 292–294
  - types of data replicated, 238–239, 241–242
  - USNs (update sequence numbers), 277, 293
- reports, data collector, 128–129
- rescanning all drives, 404
- Resource Manager disk quotas, 503–504, 514–518
- Resource Manager, Windows System, 10, 38
- Resource Monitor, 119–120



## resources

- properties, 298–299
- sessions, viewing, 476–478
- Restart Manager, 542
- Restartable Active Directory Domain Services, 16–17
- restarting servers, 7–8
- restoring. *See also* recovery
  - Active Directory, 244–248, 547
  - default Group Policy Objects, 172–173
  - DHCP configurations, 591–592
  - encryption certificates, 554–555
  - GPOs (Group Policy Objects), 165–166
  - mirrored drive sets, 432–433
  - nonsystem volumes, 550–551
  - Restore Files And Directories privilege, 312
  - security settings from GPOs, 213
  - security settings with rollback templates, 204
  - shadow copies, 482–483
  - system state, 546
- Restricted Groups settings, 195–196
- Restricted identity, 318
- Resultant Set of Policy (RSOP), 154, 166
- resume functionality, absence of, 5
- reverse lookups, 624, 628–629
- RID (Relative ID)
  - master role. *See* relative ID master role
  - soft ceilings and warnings, 223
- rights, 15, 327–330. *See also* permissions
- roaming
  - encryption certificates in profiles, 414, 552
  - roaming profiles, 362–364, 368, 552
- RODCs (read-only domain controllers), 16, 19, 219, 619
- role services
  - adding with ServerManager module, 63
  - Ocsetup.exe for configuring, 42
  - server roles, relation to, 32
- roles, server. *See* server roles
- root domains, 18
- RPCs (Remote Procedure Calls)
  - RPC over HTTP Proxy, 37
  - RPC over IP, site links with, 286
  - Windows Firewall with, 67
- RPO (recovery point objective), 520–521
- RSAT (Remote Server Administration Tools), 37, 65, 135, 256

- RSOP (Resultant Set of Policy), 154, 166, 171–172
- RSS (receive-side scaling), 13
- RTO (recovery time objective), 520–521

## S

- safe mode, 544–546
- SATA (Serial ATA), 390, 397
- scanning, 34
- scheduled tasks, 67
- schemas
  - Active Directory Recycle Bin, preparing for, 244–245
  - default, 239
  - functional levels required for feature support, 220–221
  - master role, 242, 244, 275–280
  - Schema Admins group, 315–317
- Sconfig (Server Configuration), 41, 46, 58
- scope, group, 336–337
- scopes of IP addresses
  - classes and types of, 578–579
  - exclusion ranges, 607–608
  - failover scopes, 602–605
  - icon indicators for, 582
  - managing, 601–602
  - normal scopes, 593–598
  - scope options, 599–601
  - statistics, viewing, 605
  - superscopes, 579, 592–593
- scripts, 178–179
- SCSI (Small Computer System Interface), 390
- Scwcmd command, 206, 212
- Search box, Start options panel, 7
- searching
  - accounts, listing, 368–369
  - Active Directory for users and groups, 350–351
  - for Active Directory objects, 254–256, 258
  - Apps, installed, 7
  - Search box focus, 137
  - Windows TIFF IFilter, 39
- Secure Socket Tunneling Protocol (SSTP), 563
- Secure Sockets Layer (SSL), 563
- Secured Boot, 391–392
- security
  - account options, 360–361
  - Administrator accounts, steps to secure, 307–308

- Configuration Wizard. *See* Security Configuration Wizard
- Data Execution Prevention, 80–81
- Default Domain Policy GPO, 147
- DNS issues, 626–627, 632–634
- identifiers. *See* SIDs (security identifiers)
- networking features for, 563
- permissions. *See* permissions
- policies for. *See* security policies
- refreshing Group Policy, 158–161, 166, 168–169
- Security Configuration And Analysis snap-in, 192–193, 201–204
- Security log, 108
- service accounts, considerations, 105
- services, disabling unnecessary, 107
- slow-link detection effects, 168–169
- templates for. *See* security templates
- tokens, 305
- user verification. *See* authentication
- Security Configuration And Analysis, 192–193, 201–204
- Security Configuration Wizard
  - capabilities of, 206
  - configuration sections, 206–207
  - network configuration, 209
  - registry settings configuration, 209–210
  - security policies, managing, 207, 210–213
  - server roles, services, and features, 208–209
  - templates, adding, 210
  - viewing security configuration data-bases, 207–208
- security descriptors, 297, 303
- security groups, 303, 305
- security log, auditing, 498–503
- security policies
  - applying, 211
  - audit policy configuration, 210
  - creating, 207
  - editing, 211
  - folders for, default, 210
  - multiple computers, deploying to, 212
  - network configuration, 209
  - purpose of, 206
  - registry settings configuration, 209–210
  - rolling back, 211–213
  - Save Security Policy options, 210
  - Scwcmd command, 206, 212
  - security templates, adding, 210
  - server roles configuration, 208
  - services and features, configuring, 208–209
  - viewing security configuration data-bases, 207–208
- security prompts, 5, 6, 93
- security templates
  - applicability of, 191
  - configuring, 201–204
  - creating, 192, 193
  - file path settings, 198–201
  - folders for, 193
  - multiple computer deployments, 204–205
  - policy settings, 193–195
  - registry settings, 198–200
  - Restricted Groups settings, 195–196
  - rollback templates, 203–204
  - Security Configuration And Analysis, 192–193, 201–204
  - security policies, incorporating in, 206, 210
  - steps for using, general, 192
  - system services policy settings, 196–197
- security zones, 61
- seizing server roles, 276–280
- Self identity, 318
- self-healing NTFS, 450–451
- Server Core installations
  - backup tool options, 526
  - command prompts, opening new, 41
  - converting other installation types to or from, 56–57
  - DHCP default, 46
  - features that can be installed, 42
  - limited functionality of, 4
  - roles supported by, 40
  - Sconfig with, 41–42, 58
  - setup commands, 46–47
  - user interface of, 40–41
  - Windows Logon, 40–41
- Server Graphical Shell, 4, 56
- Server Manager
  - Active Directory integration, 223
  - Add Other Servers To Manage, 58
  - Add Roles And Features Wizard, 24, 58, 70–72, 218
  - adding servers to, 67–68
  - administrative wizard access from, 23

Server Manager, *continued*

- All Servers view, 68
- alternate credentials for servers, 58
- alternate credentials for servers, entering, 58
- Best Practices Analyzer, 60
- capabilities of, 32, 57–58
- command-line version, 63–64
- console tree options, 59
- Create Server Group, 58
- default view, 58–59
- demoting domain controllers, 272–273
- dependencies, notifications of, 32
- DHCP console, 581–582
- Disks node, 437–438
- Events panel, 60, 109–115
- File And Storage Services node, 436–439
- file shares, viewing, 462–463
- Group Policy tool. *See* GPMC (Group Policy Management Console)
- grouping servers, 58
- initial configuration with, 58–62
- Local Server properties, 59
- opening, 62
- Performance panel, 60
- permissions, setting, 493, 495
- Properties panel, 60–62
- remote management requirements, 65–66
- Remove Roles And Features Wizard, 71–73
- role-based group management, 70–73
- Roles And Features panel, 60
- Services panel, 60, 100–101. *See also* services
- share permission configuration, 472–474
- shared folder management, 463–469
- startup options, 58
- stopping sharing on folders, 478–479
- storage pool creation, 438–440
- task capabilities of, 31
- Volumes node, 436–437

server roles

- Add Roles And Features Wizard, 58, 70–72
- binaries for, 72
- definition of, 32
- hardware requirement considerations, 32
- managing with Server Manager, 70–73
- managing with ServerManager module, 63

- Ocsetup.exe for configuring, 42
- Remove Roles and Features Wizard, 71–73
- Roles And Features panel, Server Manager, 60
- security policy configuration for, 208
- table of available, 33–35

Server With A GUI installations, 4. *See also* full-server installations

Server With Minimal Interface installations, 4, 40, 56

ServerManager module for PowerShell, 63–64

Service identity, 318

services. *See also specific services*

- Computer Management, configuration with, 102–107
- disk quotas with accounts, 504
- group organization of, 101
- logon accounts of, viewing, 102
- logon configuration, 104–105
- managed accounts for, 341–344
- managing, 103, 107
- names of, 101–102
- recovery configuration, 106–107
- Remote Service Management, 67
- restrictions, running under, 94–95
- security considerations for, 105
- security policy configuration for, 208–209
- Server Manager Services panel, 60, 100–101
- start types of, viewing, 101
- startup configuration, 103–104
- status of, viewing, 101–102
- stopping, 95, 103
- system, 94–95, 196–197
- Task Manager Services tab, 94–95

session IDs, 93, 99

sessions

- managing, 476–478
- type, viewing, 99

set- cmdlets, 25–26

SET commands, 52

Setup

- command-line commands, table of, 48–52
- installation steps, 44–48
- log, 108

shadow copies, 481–484, 520

- share permissions
  - configuring in Computer Management, 470–472
  - configuring in Server Manager, 472–474
  - file sharing role of, 458
  - list of, 469–470
  - options for, 465, 467–468
- shared folders
  - administrative template policies for, 151
  - claims-based permissions for, 498
  - public folder sharing, 458
  - removable disks with, 398
- sharing
  - administrative shares, 474–476
  - files. *See* file sharing
  - hidden shares, 464, 474–476
  - network options for, 12
  - permissions for. *See* share permissions
  - public folder sharing, 458
  - shadow copies of shared folders, 481–484
  - special shares, 474–476
  - standard file model, 457–458
- shutting down
  - methods for, 7–8
  - scripts for, 178–179
  - Shut Down The System privilege, 312
  - shutdown command, 47
- Sidebar, Windows, 5
- SIDs (security identifiers)
  - group accounts with, 304–305
  - NTFS disk quotas, use with, 506
  - renaming user accounts, 369–371
  - structure of, 302
- Simple Network Management Protocol (SNMP), 38
- simple volumes, 420. *See also* volumes
- single-label name resolution, 619
- single sign-on, 296–297
- sites, Active Directory
  - Active Directory Sites And Services for managing, 229–230
  - bridgehead servers, 291–293
  - creating, 282–283
  - domain controllers, associating with, 285
  - GPMC Sites node, 149
  - intersite replication topology, 291–292
  - links between, configuring, 285–289
  - permissions to manage Group Policy, 155
  - structural relations of, 138, 229
  - subnets, associating with, 284
  - well connected ideal for, 229
- 64-bit systems, 6, 43–44
- Sleep state, server, 5
- sleep states, processor, 10–11
- Slmgr commands, 42
- slow-link detection, 159, 167–170
- smart cards, 302, 320, 360
- SMB (server message block)
  - advantages for file sharing, 459
  - encryption of shares option, 468
  - enhancements in version 3.0, 457
  - get-smbshare cmdlet, 461
  - port used by, 293
  - security policy configuration for, 209
  - share profile options, 466
- SMTP (Simple Mail Transfer Protocol), 37, 286
- Snipping Tool, 5–6
- SNMP (Simple Network Management Protocol), 38
- SOA (start of authority) records, 637, 641–642
- Sound Recorder, 5–6
- spanned volumes
  - managing, 424–426, 447–449
  - status issues, table of, 422–423
  - vs. simple volumes, 420
- special folders, redirecting, 173–177
- special identities, 306
- special permissions, 489–491
- special share symbol (\$), 474–475
- SQL Server, 341
- SSL (Secure Sockets Layer), 563
- SSTP (Secure Socket Tunneling Protocol), 563
- standalone servers, 14
- standard file sharing, 457–468
- standard volumes, creating, 441–443
- standards-based storage
  - abstraction, 435
  - deduplication, 436
  - Disks node options, Server Manager, 437–438
  - layers of, 436
  - shares, creating, 437
  - storage pools, 435, 438–440
  - storage spaces, 435
  - subsystems, 436, 439

- standards-based storage, *continued*
  - traditional storage compared to, 419–420
  - virtual disk creation in storage spaces, 440–441
  - volume management, 436, 437, 441–443
  - Windows Standards-Based Storage Management, 38, 436
- Start screen, 7, 151
- starter GPOs, 153
- startup
  - debugging mode, 545
  - DHCP server mechanism for, 574
  - restore options from, 545
  - safe mode, 544–546
  - scripts for, 178–179
  - settings options, Recovery screen, 544
  - Startup And Recovery dialog box, 83–85
  - Startup Recovery Options, 548
  - Startup Repair (StR), 543, 545, 548
  - Windows Preboot Environment, 5
- static IP addresses, 566–568
- Stop errors, 84–85
- storage. *See also* hard disk drives
  - attached, 419
  - BitLocker Drive Encryption, 35, 136, 404
  - Enhanced Storage, 36
  - I/O performance tuning, 133
  - iSNS Server Service, 36
  - PhysicalDisk counters, 133
  - removable media, 443
  - removable storage devices, 396–398
  - Resource Monitor Disk usage statistics, 120
  - standards-based techniques. *See* standards-based storage
  - Storage Services role service, 387
  - subsystems, 436, 439
  - traditional vs. standards-based techniques, 419
  - Windows Standards-Based Storage Management, 38
- storage pools
  - creating, 438–440
  - physical disks, handling by, 439
  - primordial pools, 439
  - standards-based storage, role in, 435
  - virtual disk creation in, 440–441
- Storage Services, 34
- StR (Startup Repair), 543, 545, 548
- striped volumes, 424–428, 431, 434–435
- SUA (Subsystem for UNIX-Based Applications), 38
- subdomains, 18
- subnet masks, 566–567, 574
- subnets
  - creating and associating with sites, 284
  - deleting from DNS servers, 636
  - name resolution with LLMNR, 22–23
  - place in overall domain structures, 223–224
  - reverse lookup zones for, 628–629
  - sites, relation to, 138
- Subsystem for UNIX-Based Applications, 38
- superscopes, 579, 592–593
- Support Dynamic Access Control And Kerberos Armoring policy, 496–497
- Svchost.exe, 95
- Sync Center, 5
- system account disk quotas, 504
- System console, 73, 75–85
- system environment variables
  - common, list of, 352–353
  - configuring, 81–83
- system files
  - backing up, 528, 534
  - Startup Repair, 543, 545
- System identity, 318
- System Idle Process, 93
- System Image Recovery feature, 44
- System log, 108, 143
- system partitions, 402
- System Properties dialog box, 75–85
- system recovery
  - full system recovery issues, 548
  - restoring system state, 546
  - Server Core recovery, 557
  - tools for, 547–549
- system services, 94–95, 196–197
- system settings, template, 151
- System utility
  - console, 73, 75–85
  - local profile management, 365–368
  - task capabilities of, 31
- system volume drive letters, 443
- SystemInfo command, 43
- SYSVOL share, 475

## T

- Take Ownership Of Files Or Other Objects privilege, 312
- Take Ownership special permission, 490–491
- tape drives, 523–525
- Task Manager
  - Details tab, 91–94
  - End Task command, 89–90, 94
  - options for, 88, 90
  - Performance tab, 95–99
  - Processes tab, 88–94
  - Remote Desktop, managing, 99–100
  - Services tab, 94–95
  - Status column, processes, 89, 91
  - Users tab, 99–100
- Task Scheduler, 136, 539–540
- taskbars, template policies for, 151
- TCP Chimney Offload, 13, 564
- TCP/IP protocol
  - addresses for. *See* IP addresses
  - dual layer architecture of, 12–14
  - dynamic configuration of. *See* DHCP (Dynamic Host Configuration Protocol)
  - Group Policy settings for, 559
  - installing, 565–566
  - name resolution for. *See* DNS (Domain Name System)
  - Simple TCP/IP Services, 37
- telephone numbers, user contact, 348–350
- telnet, 38
- Teredo, 564
- themes, desktop, 5
- 32-bit processes, 92–93
- threads, 93, 97, 132
- throttling, processor, 8–11
- tickets, Kerberos, 327
- time
  - TIME command, 52
  - Time Zone property, 62
  - Windows Time feature, 137
- TLDs (top-level domains), 218
- tokens, 305
- trace data, collecting, 125, 127
- Transactional NTFS, 449–450
- Transport Server role service, 35
- Traverse Folder/Execute File special permission, 490–491
- trees, domain, 225–227
- troubleshooting

- Active Directory, 292–294
- DNS servers, 649–650
- improvements in recovery mechanisms, 541–542
- logon problems, 378–380
- problems, viewing current, 542
- safe mode for, 544–546
- Startup Repair Wizard, 548

## trust

- Rights Management Services, 15
- transitive trust relationships, 230

tuning performance. *See* performance

types of installations

- changing, 55–58
- choosing, 45, 48
- list of, 4

## U

- UAC (User Account Control), 5, 6, 93
- universal groups, 231, 239–241, 281, 304–306
- UNIX, 38, 463, 479–481
- unmounted drives, 443
- Up Time system property, 97
- updates
  - applications, for, 541–542
  - using Group Policy, 185–186
  - Windows Server Update Services, 35
  - Wusa.exe command for, 43
- upgrade installations, 47–48
- upgrading software using Group Policy, 185–186
- USB interface, 396–397
- User Account Control (UAC), 5–6
- user accounts
  - built-in, 307
  - capabilities, types of, 309–310
  - contact information, setting, 347–350
  - credentials, preventing from delegating, 361
  - deletion effects, 302
  - disabled status, 360, 378–380
  - domain. *See* domain user accounts
  - enabling disabled accounts, 374
  - environment variables for, 352–353
  - global user rights configuration, 328–329
  - group accounts compared to, 300–301

- group membership, managing, 339–340, 375
- home folders, setting, 351, 371
- local. *See* local user accounts
- local user rights configuration, 330
- locked out accounts, 373–374, 379
- logon names identified with, 301–302
- logon rights for, 312–313
- logon script name, renaming, 371
- logon script paths, setting, 351
- managing, 373, 375–380
- naming policies, 319–320. *See also* user names
- passwords for, 302
- permissions, setting, 380–381
- predefined, 307–308
- privileges of, 309–312
- profile paths, setting, 351, 371
- properties, configuring, 375–378
- public certificates for, 302
- renaming, 369–371
- rights management for, 327–330
- security options, 360–361
- SIDs (security identifiers), 302
- smart cards for, 302
- tools for creating, 318
- types of, 301
- updating, 368–369
- user claims, 496–497
- user environment variables, 81–83
- User Interfaces And Infrastructure, 38–39
- user names
  - changing, role of SIDs, 302
  - environment variable for, 352
  - logon names, construction from, 301–302
  - naming policies, 319–320
- user objects, 301
- user profiles
  - app deployment issues, 363
  - caching of, 362
  - EFS with roaming profiles, 362
  - encryption certificates in, 414
  - local profiles, 362–368
  - managing, 361, 363–368, 373
  - mandatory profiles, 362, 364, 379–380
  - multiple accounts, setting for, 376–377
  - names of, 365
  - paths for, setting, 351
  - primary computers with, 363
  - roaming profiles, 362–364

- user publishing method for software deployment, 182
- %UserName% variable, 352–353, 355, 363–364, 376–377
- USNs (update sequence numbers), 277, 293
- USNs folder binaries, 64–65
- UUIDs (universally unique identifiers), 262

## V

- VHD (virtual hard disk), 395, 405–406, 526
- video
  - Quality Windows Audio Video Experience, 37
  - Video for Windows, 5
- virtual accounts, 346
- virtual disks
  - creating in storage pools, 439–441
  - iSCSI, 436
  - layout options, 439–440
  - place in standards-based storage, 435–436
  - roles, adding or removing, 70–73
  - Server Manager display of, 437
  - standard volumes, creating, 441–443
  - storage pool creation, 438–440
- virtual domains, 223
- virtual memory
  - Committed Bytes counter, 131
  - Committed statistic, 97
  - configuring, 77–80
  - Resource Exhaustion Detection And Recovery, 542
- Visual Effects options, 76–77
- Volume Activation Services, 34
- volume sets. *See also* spanned volumes
  - advantages of, 422
  - creating, 424–425
  - definition of, 420
  - deleting, 426
  - drive letter assignment, 425
  - sizing segments by disk, 424–425
  - status issues, table of, 422–423
- Volume Shadow Copy Service (VSS), 525
- volumes
  - active, 402
  - allocation unit size, setting, 425
  - boot, 402, 433–434, 443
  - capabilities of, 421
  - CHKNTFS command, 49
  - compression, enabling, 410–412

- converting to NTFS, 445–447
  - creating, 407–410, 424–425, 437
  - deleting, 426, 436
  - drive letter assignment, 408, 425
  - drive paths for, 407
  - extending, 436, 447–449
  - Failed status, 422
  - File System property of, 421
  - Free Space property of, 421
  - Healthy status, 423
  - labeling, 409, 411, 425, 444–445
  - Layout property of, 420
  - logical drives as, 407–408
  - mirrored, 426–434
  - MOUNTVOL command, 50
  - NTFS disk quotas, enabling on, 508–510
  - number of active, limitation of, 407
  - paging, configuring, 77–80, 443
  - Perform Volume Maintenance Tasks
    - privilege, 312
  - remote management of, 67
  - resizing, 447–449
  - restoring nonsystem, 550–551
  - reverting entire to shadow copies, 483
  - simple, 420
  - size of, specifying, 408
  - standard, creating, 441–443
  - standards-based
    - storage
  - status issues, 421–423
  - striped, 424–428, 431, 434–435
  - system volumes, 402, 443
  - Type property of, 420
  - VOL command, 52
  - Volumes node, Server Manager, 436–437
  - VPNs (Virtual Private Networks), 34, 358–360, 563
  - VSS (Volume Shadow Copy Service), 525, 535
- W**
- wait chains, viewing, 93
  - WANs (wide area networks), 224, 565
  - Wbadmin backup command
    - commands available in, 530–533, 537–539
    - compared to other backup utilities, 525
    - critical volumes only option, 534
    - deleting system state backups, 532
    - disabling daily backups, 532
    - enabling daily backups, 532
    - help, 530
    - modifying scheduled backups, 538
    - parameters, 531
    - running, 529
    - scheduling automatic backups, 538–540
    - storage location specification, 534–535
    - system state, 546
    - Task Scheduler with, 539–540
    - volume options for, 534
  - WDS (Windows Deployment Services), 4, 35, 262–263
  - web applications, internal, 15
  - Web edition, 6
  - web page, setting for users, 348, 350
  - web servers
    - domain controller, unable to run as, 6
    - Web Server (IIS) role, 35
  - Web Services, Active Directory, 221
  - Wecutil command, 43
  - WER (Windows Error Reporting), 42, 62
  - Wevutil command, 43
  - Wi-Fi. *See* wireless networks
  - WIM (Windows Imaging Format), 5, 57, 64–65
  - Windows 8, 3, 5, 65, 67
  - Windows Aero, 5
  - Windows Biometric Framework, 38
  - Windows Boot Manager
    - configuring, 83–84
    - resizing possible with, 447
  - Windows Defender, 5
  - Windows Deployment Services, 4, 35, 262–263
  - Windows Domain Manager, 252
  - Windows Error Recovery mode, 544
  - Windows Error Reporting (WER), 42, 62
  - Windows Event Log service, 108–109
  - Windows File Protection, 39
  - Windows Firewall
    - accessing, 137
    - Active Directory issues from, 250
    - exceptions, 66–67
    - graphical shell requirement, 4
    - Properties panel, 62
  - Windows Gadgets, 5
  - Windows Imaging Format (WIM), 5
  - Windows Internal Database, 38



- Windows Internet Name Service (WINS), 20–21
- Windows key, 7
- Windows Logon, 40–42
- Windows logs, 108
- Windows Management Instrumentation (WMI), 66
- Windows Media Foundation, 36
- Windows Media Player, 5
- Windows Memory Diagnostics, 543
- Windows NT PDC emulation, 243
- Windows PE (Preinstallation Environment) 4.0, 5
- Windows PowerShell 3.0
  - Active Directory module for, 220–221, 259
  - aliases, 25
  - backward compatibility of, 24
  - cmdlets, 24–25
  - disabling remote management for local server, 66
  - event log for, 109
  - execution order issues, 25
  - features, 24
  - listing cmdlets, 25
  - remote management, 25–29, 65–66, 70
  - script support, 178
  - Search box command execution, 137
  - Server Manager function, 63–64
  - starting, 24
- Windows Preboot Environment, 5
- Windows Process Activation Service, 38
- Windows Remote Management (WinRM).
  - See WinRM (Windows Remote Management)
- Windows Server Backup
  - advantages of, 525–526
  - application data, 528, 534
  - command line option to. *See* Wbadmin backup command
  - compared to other backup utilities, 525
  - configuring, 527–529
  - critical volumes only option, 534
  - destination type options, 537
  - excluding selected locations or file types, 535
  - full system recovery issues, 548
  - installing, 386, 525–527
  - manual backups, 540–541
  - Microsoft Exchange Server with, 527
  - modifying scheduled backups, 538
  - permissions for, 528
  - recovering nonsystem volumes, 550–551
  - remote shared folders for, 534, 539, 541
  - scheduling automatic backups, 535–538
  - starting, 527
  - stopping scheduled backups, 538
  - storage location specification, 534–535
  - system state data, 528, 534
  - volume options for, 534
  - VSS Settings, 535
- Windows Server Migration tools, 47
- Windows Server Update Services (WSUS), 189–190
- Windows Sidebar, 5
- Windows Software Licensing Management tool, 42, 74
- Windows Standards-Based Storage Management, 38, 436
- Windows System Resource Manager, 10, 38
- Windows TIFF IFilter, 39
- Windows Time, 137
- Windows Token-Based Agent, 33
- Windows Update
  - managing with Group Policy, 187–190
  - payloads, Group Policy for, 64–65
  - Properties panel, 62
  - restoring payloads with, 218
- WinRM (Windows Remote Management)
  - authentication issues, 26–27, 28–29
  - configuring, 26–28
  - disabling for local server, 66
  - Group Policy affecting, 29
  - IIS Extension, 39
  - listeners, 28
  - requirements for, 25–26
  - web gateway with, 26
- Windows 8, enabling remote management of, 67
- Windows Firewall exceptions for, default, 66
- WINS (Windows Internet Name Service), 20–21
- wireless networks
  - policies for, 168, 562–563
  - Wireless LAN Service, 39, 135
- Wmic commands, 43
- Work network type, 12
- workgroups
  - Active Directory Lightweight Directory Services, 15
  - Administrator accounts for, 308

- CAs (certificate authorities), 15
- definition of, 6
- joining computers to, 75, 267–270
- remote management within, 65
- time synchronization, 137

- WoW64, 39

- Write Attributes special permission, 490–491

- Write Extended Attributes special permission, 490–491

- Write permission, 489

- writes, disk performance for, 133

- WSH (Windows Script Host), 178

- WS-Management, 43

- WSRM (Windows System Resource Manager), 10, 38

- WSUS (Windows Server Update Services), 35, 189–190

## X

- X.500 directory service migrations, 301

- XPS Viewer, 39

## Z

- ZAW (.zap) files, 182–183

- zones, DNS

- Active Directory integration, 616–617

- adding records to, 636–640

- child domains, creating in, 634–636

- configuring new, 625–628

- DNSSEC configuration, 20, 632–634

- integration modes, setting, 645

- properties, setting, 641–645

- secondary servers, notifications to, 644

- SOA (start of authority) records, 637, 641–642

- transfer restrictions, 643–644

- types, setting, 645



# About the Author

---



**WILLIAM R. STANEK** (<http://www.williamstanek.com/>) has more than 20 years of hands-on experience with advanced programming and development. He is a leading technology expert, an award-winning author, and a pretty-darn-good instructional trainer. Over the years, his practical advice has helped millions of programmers, developers, and network engineers all over the world. His current and forthcoming books include *Windows 8 Administration Pocket Consultant* and *Windows Server 2012 Inside Out*.

William has been involved in the commercial Internet community since 1991. His core business and technology experience comes from more than 11 years of military service. He has substantial experience in developing server technology, encryption, and Internet solutions. He has written many technical white papers and training courses on a wide variety of topics. He frequently serves as a subject matter expert and consultant.

William has an MS with distinction in information systems and a BS in computer science, magna cum laude. He is proud to have served in the Persian Gulf War as a combat crew member on an electronic warfare aircraft. He flew on numerous combat missions into Iraq and was awarded nine medals for his wartime service, including one of the United States of America's highest flying honors, the Air Force Distinguished Flying Cross. Currently, he resides in the Pacific Northwest with his wife and children.

William recently rediscovered his love of the great outdoors. When he's not writing, he can be found hiking, biking, backpacking, traveling, or trekking in search of adventure with his family!

Find William on Twitter at WilliamStanek and on Facebook at [www.facebook.com/William.Stanek.Author](http://www.facebook.com/William.Stanek.Author).

# What do you think of this book?

We want to hear from you!

To participate in a brief online survey, please visit:

[microsoft.com/learning/booksurvey](https://microsoft.com/learning/booksurvey)

Tell us how well this book meets your needs—what works effectively, and what we can do better. Your feedback will help us continually improve our books and learning resources for you.

Thank you in advance for your input!

**Microsoft**  
Press