

Installing and Configuring Windows 10

Exam Ref 70-698



OTHERS

in



Exam Ref 70-698 Installing and Configuring Windows 10

Andrew Bettany Andrew Warren PUBLISHED BY Microsoft Press A division of Microsoft Corporation One Microsoft Way Redmond, Washington 98052-6399

Copyright © 2016 by Andrew Bettany and Andrew Warren

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: 2016934334 ISBN: 978-1-5093-0295-6

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 Support at *mspinput@microsoft.com*. Please tell us what you think of this book at *http://aka.ms/tellpress*.

This book is provided "as-is" and expresses the author's views and opinions. The views, opinions and information expressed in this book, including URL and other Internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

Microsoft and the trademarks listed at *http://www.microsoft.com* on the "Trademarks" webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

Acquisitions Editor: Karen Szall Developmental Editor: Karen Szall Editorial Production: Cohesion Technical Reviewer: Randall Galloway; Technical Review services provided by Content Master, a member of CM Group, Ltd. Copyeditor: Kerin Forsyth Indexer: Lucie Haskins Cover: Twist Creative • Seattle

Contents at a glance

	Introduction	xlx
CHAPTER 1	Prepare for installation requirements	1
CHAPTER 2	Install Windows 10	27
CHAPTER 3	Configure devices and device drivers	65
CHAPTER 4	Post-installation configuration	97
CHAPTER 5	Implement Windows in an enterprise environment	135
CHAPTER 6	Configure networking	161
CHAPTER 7	Configure storage	201
CHAPTER 8	Configure data access and usage	237
CHAPTER 9	Implement Apps	273
CHAPTER 10	Configure remote management	297
CHAPTER 11	Configure updates	319
CHAPTER 12	Monitor Windows	349
CHAPTER 13	Configure system and data recovery	385
CHAPTER 14	Configure authorization and authentication	419
CHAPTER 15	Configure advanced management tools	449
	Index	467

This page intentionally left blank

Contents

Chapter

	Introduction	xix
	Organization of this book	XX
	Microsoft certifications	XX
	Acknowledgments	XX
	Free ebooks from Microsoft Press	ххі
	Microsoft Virtual Academy	ххі
	Quick access to online references	ххі
	Errata, updates, & book support	xxi
	We want to hear from you	ххіі
	Stay in touch	xxii
1	Prepare for installation requirements	1
	Skill: Determine hardware requirements and compatibility	2
	Identify hardware requirements for Windows 10	2
	Determine hardware compatibility for Windows 10	3
	Verify application compatibility for Windows 10	6
	Skill: Choose an upgrade or a clean installation	9
	Prepare an upgrade or migration strategy	10
	Perform an in-place upgrade to Windows 10	12
	Perform a migration to Windows 10	13
	Skill: Determine editions by device type	15
	Select a Windows 10 edition	16
	Choose the 32-bit or 64-bit versions	17
	Skill: Determine requirements for particular features	
	General features	18
	Security features	20

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:

	Skill: Identify a strategy and prepare the installation media	21
	Select an installation strategy	21
	Determine the appropriate installation media	21
	Summary	24
	Thought experiment	24
	Thought experiment answer	25
Chapter 2	Install Windows 10	27
	Skill: Perform clean installations	27
	Skill: Upgrade by using Windows Update	30
	Windows Update	31
	Perform the upgrade	31
	Go back to previous version of Windows	38
	Block upgrading to Windows 10	39
	Skill: Upgrade using installation media	41
	Skill: Configure native boot scenarios	43
	View configuration information	43
	Multiboot Windows	45
	Skill: Migrate from previous versions of Windows	47
	Migrate applications by using User Experience Virtualization	48
	Perform a user state migration	49
	Skill: Install Windows 10 to a VHD	52
	Create and configure a native boot VHD	52
	Use Disk Management to attach a VHD	53
	Install Windows inside a VHD	53
	Skill: Boot Windows 10 from VHD	55
	Create an MBR-partitioned VHD	55
	Apply the Windows Image to the VHD	56
	Configure boot options	56
	Skill: Install on bootable USB	57
	Install on bootable USB, using the Media Creation Tool	57
	Manually create a Windows 10 bootable USB	58

	Skill: Install additional Windows features	59
	Use the Windows Features app	59
	Use DISM to add or remove Windows features	60
	Skill: Configure Windows for additional regional and	
	language support	60
	Summary	62
	Thought experiment	63
	Thought experiment answer	63
Chapter 3	Configure devices and device drivers	65
	Skill: Install devices	65
	Install devices	66
	Manage devices and printers	68
	Skill: Update, disable, and roll back drivers	69
	Update device drivers	69
	Prevent driver updates over metered connections	70
	Disable individual driver updates or Windows Updates	71
	Turn on or off automatic device driver installation in	
	Device Installation Settings	/3
	Perform a driver foliback	74
	Skill: Resolve driver issues	76
	Disable updates	76
	Use driver verification tools	//
	Skill: Configure driver settings	79
	View device settings	80
	Support for older hardware	81
	Skill: Driver signing	82
	Skill: Manage driver packages	84
	Use the driver store	84
	Use PnPUtil.exe to manage driver packages	85
	Skill: Download and import driver packages	86
	Download driver packages	87
	Deploy driver packages by using the Windows Imaging And Configuration Designer	88

	Import driver packages	90
	Skill: Use Deployment Image Servicing And Management tool to	01
	Add packages	91
	Manage driver packages with DISM	92
	Summary	94
	Thought experiment	94
	Thought experiment answers	95
Chapter 4	Post-installation configuration	97
-	Skill: Configure and customize the user interface per device type	97
	Customize the user interface	98
	Configure Action Center and taskbar	108
	Skill: Configure accessibility options	115
	Configure and enable Ease Of Access settings	115
	Skill: Configure Cortana	116
	Skill: Configure Microsoft Edge	118
	Skill: Configure Internet Explorer	122
	Skill: Configure Hyper-V	126
	Verifying Hyper-V prerequisites	126
	Installing the Client Hyper-V role	126
	Creating and managing virtual machines	127
	Skill: Configure power settings	130
	Configuring basic power options	130
	Configuring power plans	132
	Summary	132
	Thought experiment	133
	Thought experiment answer	133
Chapter 5	Implement Windows in an enterprise environment	135
	Skill: Provision with Windows Imaging and	
	Configuration Designer tool	135
	Prepare installation media with ICD	135

Skill: Implement activation	137
Select an activation method	138
Implement volume activation	140
Activate Windows 10	142
Skill: Configure and optimize User Account Control.	144
Configure User Account Control	144
Skill: Configure Active Directory, including Group Policy	148
Configure Active Directory	148
Use the Active Directory Administrative Center	152
Configure Group Policy	154
Summary	158
Thought experiment	158
Thought experiment answer	159

Chapter 6 Configure networking

Skill: Configure and support IPv4 and IPv6 network settings161	
Overview of IPv4	162
Subnets	162
Public and private addressing	164
Configuring an IPv4 connection	165
Overview of IPv6	168
IPv6 addressing	168
Configuring an IPv6 connection	169
Skill: Configure name resolution	. 170
Overview of name resolution	170
Configure DNS settings	171
Configure advanced DNS settings	172
Skill: Connect to a network	. 173
Connect to a HomeGroup	173
Configure VPN connections	175
Configure DirectAccess connections	178
Skill: Configure network locations	
Overview of network location profiles	179
Configure network locations	181

ix

Skill: Configure Windows Firewall, including Advanced Security and network discovery	
Configure Windows Firewall	183
Configure Windows Firewall With Advanced Security	185
Configure IPsec	187
Configure network discovery	188
Skill: Configure Wi-Fi settings and Wi-Fi Direct	
Overview of wireless networking standards	189
Configure wireless settings	191
Skill: Troubleshoot network issues	
Network troubleshooting tools	196
Troubleshoot name resolution	196
Summary	
Thought experiment	
Thought experiment answers	
Configure storage	201
Skill: Configure disks, volumes, and file systems	
Configure disks	202
Configure volumes	203
Configure file systems	204
Using disk management tools	207
	211

Configure file systems	204
Using disk management tools	207
Skill: Create and configure virtual hard disks	211
Work with VHDs	211
Create VHDs with Hyper-V Manager	213
Use Disk Management to create VHDs	213
Create VHDs by using Windows PowerShell	215
Link to differencing disks	218
Skill: Create and configure Storage Spaces.	219
Use Storage Spaces and storage pools	219
Configure Storage Spaces	221
Manage Storage Spaces by using Windows PowerShell	224
Skill: Configure removable devices	225
Format removable devices	226

Chapter 7

	Restrict access to removable devices	228
	Skill: Troubleshoot storage issues and removable devices	
	Initialize a basic disk	232
	Import foreign disks	232
	Hard drive failure	232
	Replacing failed disks	234
	Summary	235
	Thought experiment	235
	Thought experiment answer	236
Chapter 8	Configure data access and usage	237
	Skill: Configure file and printer sharing	237
	Server Message Block and Network Discovery	238
	Sharing files by using a sharing wizard	239
	Share a printer	241
	Skill: Configure HomeGroup connections	243
	Create a new HomeGroup	244
	Join a HomeGroup	245
	Skill: Configure folder shares	246
	Create a share	247
	Shared folders permissions	250
	Configure public folders	
	Skill: Configure OneDrive	251
	OneDrive desktop app	252
	OneDrive web portal	252
	Fetch files on your PC	253
	Skill: Configure File System permissions	
	Use File Explorer to manage files and folders	255
	Set file and folder permissions	256
	Understand NTFS inheritance	262
	Skill: Configure OneDrive usage	263
	Share files with OneDrive	263

Secure removable devices

	Recover files from OneDrive	264
	Block access to OneDrive	265
	Skill: Troubleshoot data access and usage	266
	Troubleshoot data access	266
	Troubleshoot share and NTFS permissions	268
	Troubleshoot dynamic access control	269
	Troubleshoot data recovery	269
	Recover BitLocker encrypted drives	270
	Summary	270
	Thought experiment	271
	Thought experiment answer	272
Chapter 9	Implement Apps	273
	Skill: Configure desktop apps	273
	Install desktop apps	274
	Uninstall or change a desktop app	278
	Skill: Configure app startup options	
	Control Windows 10 Fast Startup	280
	Configure app startup behavior	281
	Skill: Configure Windows features	283
	Skill: Implement Windows Store Apps	
	Manage Windows Store Apps	284
	Configure Windows Store App settings	286
	Sideload apps	289
	Distribute apps by using Windows Store for Business	290
	Skill: Create and deploy provisioning packages	291
	Create provisioning packages	291
	Apply provisioning packages	294
	Summary	294
	Thought experiment	295
	Thought experiment answer	295

Chapter 10	Configure remote management	297
	Skill: Choose the appropriate remote management tools	297
	Remote management tools in Windows 10	298
	Selecting the appropriate remote management tool	298
	Skill: Configure remote management settings	299
	Configuring Windows Firewall to enable remote management	299
	Enabling remote management through System Properties	301
	Skill: Configure Remote Assistance	303
	Requesting help using Remote Assistance	303
	Offering help with Remote Assistance	305
	Configuring Remote Assistance with GPOs	306
	Using Remote Assistance to manage a computer remotely	307
	Skill: Configure Remote Desktop	307
	Creating and editing Remote Desktop connections	307
	Configuring Remote Desktop with GPOs	310
	Skill: Configure Windows PowerShell remoting	310
	Skill: Modify settings, using Microsoft Management Console or Windows PowerShell	312
	Using MMC to manage remote computers	313
	Using Windows PowerShell to manage remote computers	314
	Summary	315
	Thought experiment	316
	Thought experiment answer	316
Chapter 11	Configure updates	319
•	Skill: Configure Windows Undate ontions	319
	Configure Windows Update settings	320
	Use Group Policy to configure Windows Update	324
	Troubleshoot Windows Update	327

Use Current Branch

Use Current Branch for Business

331

	Update mobile devices	333
	Implement continuous servicing	333
	Skill: Long-Term Servicing Branch scenarios	334
	Skill: Manage update history	335
	View update history	336
	Hide or show Windows Updates in Windows 10	337
	Skill: Roll back updates	339
	Uninstall a Windows update by using Control Panel	339
	Uninstall a Windows update in Settings	339
	Uninstall a Windows update by using the command prompt	340
	Revert to a previous build of Windows 10	341
	Skill: Update Windows Store apps	344
	Summary	347
		2 47
	I hought experiment.	347
	Thought experiment answer.	347
12	Thought experiment Thought experiment answer	347 348 349
12	Thought experiment. Thought experiment answer. Monitor Windows Skill: Configure and analyze Event Viewer logs.	347 348 349 350
12	Thought experiment. Thought experiment answer. Monitor Windows Skill: Configure and analyze Event Viewer logs Understand event logs	347 348 349 350 350
12	Thought experiment. Thought experiment answer. Monitor Windows Skill: Configure and analyze Event Viewer logs. Understand event logs Create a custom view	347 348 349 350 350 352
12	Thought experiment. Thought experiment answer. Monitor Windows Skill: Configure and analyze Event Viewer logs. Understand event logs Create a custom view Skill: Configure event subscriptions.	347 348 349 350 350 352 353
12	Thought experiment Thought experiment answer Monitor Windows Skill: Configure and analyze Event Viewer logs Understand event logs Create a custom view Skill: Configure event subscriptions View subscriptions	347 348 349 350 350 352 353 353
12	Thought experiment Thought experiment answer Monitor Windows Skill: Configure and analyze Event Viewer logs Understand event logs Create a custom view Skill: Configure event subscriptions View subscriptions Create a subscription	347 348 349 350 350 352 353 353 353
12	Thought experiment Thought experiment answer Monitor Windows Skill: Configure and analyze Event Viewer logs Understand event logs Create a custom view Skill: Configure event subscriptions View subscriptions Create a subscription Access event logs remotely	347 348 349 350 350 352 353 353 353 354 355
12	Thought experiment Thought experiment answer Monitor Windows Skill: Configure and analyze Event Viewer logs Understand event logs Create a custom view Skill: Configure event subscriptions View subscriptions Create a subscription Access event logs remotely Skill: Monitor performance using Task Manager	347 348 349 350 350 352 353 354 355 356
12	Thought experiment	347 348 349 350 350 350 352 353 353 354 355 356 356
12	Thought experiment Thought experiment answer Monitor Windows Skill: Configure and analyze Event Viewer logs Understand event logs Create a custom view Skill: Configure event subscriptions View subscriptions Create a subscription Access event logs remotely Skill: Monitor performance using Task Manager Access Task Manager Processes tab	347 348 349 350 350 352 353 354 355 356 356 356 357

App History tab

Startup tab

Users tab

Details tab

Services tab

Chapter

393	
396	
396	
397	
398	
400	

Skill: Monitor performance using Resource Monitor	361
Skill: Monitor performance using Performance Monitor and Data Collector Sets Run the Performance Monitor data collector Use Performance Monitor	363 363 365
Skill: Monitor system resources Understand baseline performance vs. real-time monitoring Create a performance baseline	367 368 368
Skill: Monitor and manage printers	369 370 371 372
Skill: Configure indexing options Skill: Manage client security by using Windows Defender Understand malware Monitor for malware	374 375 375 377
Skill: Evaluate system stability by using Reliability Monitor Skill: Troubleshoot performance issues Summary Thought experiment Thought experiment answer	379 380 382 383 383
Configure system and data recovery	385
Skill: Configure a recovery drive	386

Chapter 13 Co

Skill: Perform a refresh or recycle	90
Skill: Perform recovery operations using Windows Recovery3	93
Skill: Configure restore points	96
Change restore settings 3	96
Manage disk space 3	97
Create or delete restore points 3	98
Skill: Use Windows Backup And Restore4	00

	Skill: Perform a backup and restore with WBAdmin	403
	Backing up using WBAdmin	403
	Restoring data using WBAdmin	405
	Skill: Configure File History	
	Configuring File History	406
	Recovering Files by using File History	408
	Enterprise considerations for using File History	410
	Skill: Restore previous versions of files and folders	
	Skill: Recover files from OneDrive	
	Recovering files from OneDrive	414
	Using Previous Versions in OneDrive	415
	Summary	416
	Thought experiment	417
	Thought experiment answer	417
Chapter 14	Configure authorization and authentication	419
	Skill: Configure user accounts	420
	Configure local accounts	420
	Configure Microsoft accounts	425
	Configure User Account Control	429
	Skill: Configure Microsoft Passport and Windows Hello	431
	Configure Windows Hello	432
	Configure Microsoft Passport and biometrics	433
	Configure picture passwords	434
	Skill: Manage credential security	435
	Configure Credential Manager	436
	Configure Credential Guard	436
	Skill: Manage device security	438
		420
	Configure Device Guard	438
	Configure Device Guard Configure Device Health Attestation	438 440
	Configure Device Guard Configure Device Health Attestation Skill: Configure HomeGroup, workgroup, and domain settings.	438 440 441
	Configure Device Guard Configure Device Health Attestation Skill: Configure HomeGroup, workgroup, and domain settings. Configure workgroups	438 440 441 442

Configure Device Registration 445
Summary
Thought experiment
Thought experiment answer
hapter 15 Configure advanced management tools 449
Skill: Configure services449
Manage services 450
Use the System Configuration tool 453
Skill: Configure Device Manager455
Skill: Configure and use the MMC
Configure the management console 457
Customize your console by using Taskpad views 458
Skill: Configure Task Scheduler459
Skill: Configure automation of management tasks with `Windows PowerShell
Create simple scripts 462
Enable scripts to run 462
Use Windows PowerShell ISE 463
Summary
Thought experiment464
Thought experiment answer465

Index

What do you think of this book? We want to hear from you! Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

Introduction

This book is intended for IT pros who are seeking certification in the 70-698 Installing and Configuring Windows 10 exam. These professionals typically administer and support Windows 10 devices in corporate, Windows Server domain-based environments with managed access to the Internet and cloud services. The book is also intended to provide skills for Enterprise Device Support Technicians (EDSTs), who provide Tier 2 support to users of Windows 10 in medium-to-large enterprise organizations.

To get the most from this book, you should have at least two years of experience in the IT field and should already have the following technical knowledge.

- Networking fundamentals, including Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), and Domain Name System (DNS).
- Microsoft Active Directory Domain Services (AD DS) principles.
- Some experience with Windows Server 2016 or Windows Server 2012 R2.
- Experience with a Microsoft Windows client; for example, a working knowledge of Windows 7 or Windows 8.1.

Skills covered by reading this book include the following.

- Install, upgrade, and customize Windows 10.
- Manage apps.
- Configure storage.
- Configure network connectivity.
- Configure data security, device security, and network security.
- Maintain, update, and recover Windows 10.

We expect Windows 10 to continue evolving through regular upgrades, and you should ensure that your study is supplemented with practical experience, using the latest build of Windows 10, because new features are likely to be included in the exam.

This book covers every major topic area found on the exam, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions, and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the "Need more review?" links you'll find in the text to find more information and take the time to research and study the topic. Great information is available on MSDN and TechNet and in blogs and forums.

Organization of this book

This book is organized by the "Skills measured" list published for the exam. The "Skills measured" list is available for each exam on the Microsoft Learning website: *http://aka.ms* /*examlist*. Each chapter in this book corresponds to a major topic area in the list, and the technical tasks in each topic area determine a chapter's organization. If an exam covers six major topic areas, for example, the book will contain six chapters.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO ALL MICROSOFT CERTIFICATIONS

For information about Microsoft certifications, including a full list of available certifications, go to *http://www.microsoft.com/learning*.

Acknowledgments

Andrew Warren Writing any book is a collaborative effort, so I would like to thank my co-author, Andrew Bettany, for helping drive the project forward. Without the guiding hand of an experienced editor, it's doubtful any book would ever see the light of day, so thank you also to Karen Szall at Microsoft Press for ensuring that we kept to the deadlines and kept it brief.

Andrew Bettany I am very grateful to both Karen Szall for providing a firm and steady guiding hand, and my coauthor, Andrew Warren, for his wealth of experience. The writing journey has been enjoyable and culminated in sitting and passing the 70-698 exam and obtaining my MCSA: Windows 10. This book is dedicated to Annette and Tommy. Mwah!

Free ebooks from Microsoft Press

From technical overviews to in-depth information on special topics, the free ebooks from Microsoft Press cover a wide range of topics. These ebooks are available in PDF, EPUB, and Mobi for Kindle formats, ready for you to download at:

http://aka.ms/mspressfree

Check back often to see what is new!

Microsoft Virtual Academy

Build your knowledge of Microsoft technologies with free expert-led online training from Microsoft Virtual Academy (MVA). MVA offers a comprehensive library of videos, live events, and more to help you learn the latest technologies and prepare for certification exams. You'll find what you need at *http://www.microsoftvirtualacademy.com*.

Quick access to online references

Throughout this book are addresses to webpages that the author has recommended you visit for more information. Some of these addresses (also known as URLs) can be painstaking to type into a web browser, so we've compiled all of them into a single list that readers of the print edition can refer to while they read.

Download the list at http://aka.ms/ER698/downloads.

The URLs are organized by chapter and heading. Every time you come across a URL in the book, find the hyperlink in the list to go directly to the webpage.

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

http://aka.ms/ER698/errata

If you discover an error that is not already listed, please submit it to us at the same page.

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

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *http://support.microsoft.com*.

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://aka.ms/tellpress

We know you're busy, so we've kept it short with just a few questions. Your answers go directly to the editors at Microsoft Press. (No personal information will be requested.) Thanks in advance for your input!

Stay in touch

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

Configure devices and device drivers

Windows 10 identifies and configures hardware during the initial installation. Upon delivery of a device running Windows 10, the user will typically want to add their own hardware and peripherals such as a printer, a Bluetooth mouse, or web cam. In this chapter, you learn how Windows 10 installs drivers for new devices and hardware and how you can maintain these drivers, upgrade them, and resolve driver issues that might occur.

Skills covered in this chapter:

- Install devices
- Update, disable, and roll back drivers
- Resolve driver issues
- Configure driver settings
- Driver signing
- Manage driver packages
- Download and import driver packages
- Use Deployment Image And Service Management tool (DISM) to add packages

Skill: Install devices

When you install a hardware component on Windows 10, the operating system requires a device driver to be installed so that you can use it. After it's configured, the device driver loads automatically and is available for Windows to use. This section explains how Windows 10 automatically installs devices and locates the device driver from the Windows Component Store, from Windows Update, or directly from you.

This section covers how to:

- Install devices
- Manage devices and printers

Install devices

For hardware to function properly, it requires special software designed for Windows 10 to communicate with it. This software is referred to as a device driver, and when Windows 10 detects new hardware, the system automatically attempts to install one of the built-in drivers included as part of the operating system, located within the Windows 10 Driver Store, or download them through Windows Update, from the Internet. New and updated hardware device drivers are regularly submitted to Microsoft by the equipment vendor for testing and cataloguing. If the Windows Update feature is enabled, Windows 10 automatically detects the presence of new device drivers, downloads them, and installs them.

New hardware is typically installed automatically when it's added to Windows 10, with the operating system detecting and identifying the new hardware through the Plug and Play feature. Windows 10 supports new hardware connected through a variety of connection methods, including USB (1.0 through 3.1), Wi-Fi, and Bluetooth. In addition to backward compatibility for existing and earlier hardware, emerging technologies such as near-field communication (NFC) and Miracast for wireless displays also have built-in support in Windows 10.

For advanced users or for managing or troubleshooting a hardware device issue, you can use Device Manager. Device Manager provides information about each device, such as the device type, device status, manufacturer, device-specific properties, and device driver information.

There are multiple ways to load the Device Manager, including:

- Right-clicking the Start button and selecting Device Manager.
- Typing Device Manager into Search.
- Opening Control Panel, selecting Hardware And Sound, and then selecting Device Manager.

The Device Manager default view (devices by type) is shown in Figure 3-1.

You can expand and explore each node in Device Manager and then select a device. All devices have properties, and these can be viewed by right-clicking the desired device and selecting the properties. The Properties dialog box for a device is shown in Figure 3-2.



FIGURE 3-1 Device Manager showing the devices by type view



FIGURE 3-2 Device Properties

If you added a new peripheral and Windows 10 does not immediately recognize it, first check that the device is connected properly and that no cables are damaged. You should ensure that the external device is powered on and not in sleep or standby mode. You can also open Device Manager and launch the Scan For Hardware Changes Wizard from the Action menu, which will locate previously undetected hardware and then configure it for you.

Manage devices and printers

Device Manager provides one method of managing devices within Windows 10. Another way to add and manage devices is by using the Devices And Printers app within Control Panel. This Devices And Printers app enables you to add devices and printers by clicking the menu item at the top of the screen. This launches an easy-to-use wizard that searches for devices and walks the user through the process of installing devices, as shown in Figure 3-3.

			×
👝 🖨 Add Printer			
Searching for available printers			
Printer Name	Address		
🖶 WF-3520 Series (EPSON)	192.168.1.69		
		Stop	
The printer that I want isn't liste	ed		
		Next Cance	2

FIGURE 3-3 Add Printer Wizard

After a piece of hardware is installed, you can view it in the Devices And Printers app, and Windows displays photorealistic icons to help you recognize the devices. If you click and open one of the icons, a new view appears that focuses on the device. This window is the device stage and is shown in Figure 3-4. The type of functionality found in the device stage depends on the support provided by the manufacturer of the device that is installed alongside the device driver.



FIGURE 3-4 Device stage

Skill: Update, disable, and roll back drivers

Most computers that you'll work with have different hardware components, such as motherboards, disk controllers, graphics cards, and network adapters. Fortunately, Windows 10 is designed to work with an extensive list of hardware devices and benefits from Plug And Play, which tries to detect new devices automatically and then installs the correct driver software.

If Windows has a problem with a device, you must troubleshoot the cause, and this can involve locating the correct or updated device drivers and installing them. In this chapter, you focus on working with devices and drivers and the corrective and preventive actions you can take to help ensure that the devices you configure are free from problems.

This section covers how to:

- Update device drivers
- Prevent driver updates over metered connections
- Disable individual driver updates or Windows Updates
- Turn on or off automatic device driver installation in Device Installation Settings
- Perform a driver rollback

Update device drivers

Windows 10 automatically attempts to install a device driver and, if one is not available locally, attempts to locate one through Windows Update. For most systems, devices and their associated drivers remain constant and require no further administrative effort. In the following instances, you might need to update, disable, or reinstate a previous driver.

- Windows 10 detects that a newer driver is available through Windows Update.
- You want to install a newer device driver manually, typically obtained from the manufacturer's website.
- The device is not performing or functioning correctly with the current driver.
- A new or beta version of a driver is causing stability issues.

To update a specific driver, select the device in Device Manager and select Update Driver Software from the context menu.

Windows 10 offers you two choices for updating the driver.

- Search Automatically For Updated Driver Software.
- Browse My Computer For Driver Software.

Typically, most users allow Windows to locate, download, and install an updated device driver automatically if one is available through Windows Update. This is the default method.

If you have the installation media that came with the hardware, you can use the browse feature to locate the correct driver. The Windows 10 Update Driver Software Wizard can automatically search through the subfolders in the media and locate all the relevant drivers for the device.

If you have already downloaded a specific device driver from the manufacturer, for example, a video driver from NVIDIA or AMD/ATI, you might need to run the driver installation wizard included in the download files, which includes additional software besides the device driver.

If Windows determines that the current driver is the most up to date or best driver available, you can confirm the version number of the driver by viewing the properties of the driver in Device Manager. If you have a more recent driver that you want to use, you must manually uninstall the current driver and then manually install the more recent driver.

Prevent driver updates over metered connections

Windows 10 enables you to prevent new or updated drivers from being downloaded while the device is connected on a metered connection.

You can check your settings for this behavior by completing the following steps.

- 1. Open Settings and click Devices.
- 2. In Printers & Scanners, scroll down to Download Over Metered Connections.
- 3. The setting should be set to Off by default, as shown in Figure 3-5.



FIGURE 3-5 Configuring the Download Over Metered Connections setting

- **4.** The same setting can also be found in the Connected Device section, which is below the Other Devices section.
- 5. Close Settings.

Windows 10 should automatically detect whether your connection is metered. If you are connecting to the Internet by tethering or a Wi-Fi hotspot, you can manually configure the connection to be a metered connection by using the following steps.

- 1. Connect to the metered Wi-Fi connection.
- 2. Open Settings and choose Network & Internet.
- 3. Under the Wi-Fi section, choose Advanced Options.
- 4. Under Metered Connection, select the On status for the toggle switch.

Disable individual driver updates or Windows Updates

Sometimes it is important to remove a device driver completely from the system. It might be corrupted or incompatible with your system. If Windows determines that the driver is valid and up to date, it is impossible to use another device driver while the current driver is present. To uninstall an unwanted device driver, use the following steps.

- 1. Open Device Manager.
- 2. Locate the device with the problem driver, right-click it, and choose Uninstall.
- **3.** In the Uninstall dialog box, select the Delete The Driver Software For This Device check box, if this option is available, as shown in Figure 3-6.



FIGURE 3-6 Uninstalling device driver software

If the item relates to an unwanted Windows Update, use the following steps.

- **1.** Type **View Installed Updates** in the Search box and then click View Installed Updates Control Panel in the Search results.
- **2.** Locate and uninstall the unwanted update by selecting it from the list and then clicking Uninstall.

If the driver is reluctant to be uninstalled, try restarting the computer and attempting the procedure again. Only as a last resort should you try to delete the software manually. You can use the PnPUtil.exe command-line tool and remove the .inf files that are associated with the device as shown.

PnPUtil.exe -a -d <path to the driver> \<drivername>.inf

The use of the PnPUtil.exe command-line tool is discussed later in this chapter.

NOTE DRIVER INSTALLATION AND REMOVAL ARE ADMINISTRATIVE FUNCTIONS

You must use administrative privileges to install or uninstall a device or driver package by using Device Manager.

Because different hardware types have different functions and features, review the tabs in the properties screen. Not all devices have the same tabs, and some devices do not offer the ability to view or modify the device driver.

Turn on or off automatic device driver installation in Device Installation Settings

Sometimes installing an updated driver can cause your computer to lose functionality, and you might decide to uninstall the driver. Windows 10 automatically attempts to reinstall the driver, which is not desirable. In this situation, you might want to turn off the automatic device driver installation setting by using the following steps.

- 1. Open Control Panel; under Hardware And Sound, click Devices And Printers.
- 2. Under Devices, right-click the icon that represents your computer—it should have your computer name—and click Device Installation Settings, as shown in Figure 3-7.



FIGURE 3-7 Disabling the automatic device driver software installation

- **3.** In the Device Installation Settings dialog box, choose No, (Your Device Might Not Work As Expected). (Yes is the default setting.)
- 4. A further set of choices is presented, offering:
 - Always Install The Best Driver Software From Windows Update (default setting).
 - Never Install Driver Software From Windows Update.
 - Automatically Get The Device App And Info Provided By Your Device Manufacturer (selected by default).
- 5. Click Save Changes.

Perform a driver rollback

Sometimes a driver problem can cause the system to become unstable. In Device Manager, you can roll back an updated driver to its previous version. If the system allows you to start normally, you can perform this task by using the following steps.

- 1. Open Device Manager.
- 2. Right-click the device that you want to roll back and then click Properties.
- 3. In the Properties dialog box, click the Drivers tab and then click Roll Back Driver.
- 4. In the Driver Package Rollback dialog box, click Yes as shown in Figure 3-8.



FIGURE 3-8 Device Driver Package Rollback

The Driver Package Rollback feature can only be used to revert to a previously updated driver. If you have not installed a later driver, the option in Device Manager will be unavailable.

NOTE NO DRIVER ROLLBACK FOR PRINTERS

Although Printers and Print queues appear in Device Manager, you cannot use Driver Package Rollback for these devices. If your system is unstable or won't start up properly because of a faulty driver, such as a video driver, you might need to restart the computer in Safe Mode to access Device Manager and perform the driver rollback. Windows 10 automatically detects startup failures and should boot into the advanced startup menu.

Microsoft removed the ability to restart in Safe Mode by using Shift+F8 in Windows 10 so that the boot process could be quicker.

You can force Windows 10 still to respond to Shift+F8 by enabling the feature by typing the following command within an elevated command prompt.

```
BCDEdit /set {default} bootmenupolicy legacy
```

The command should complete successfully and, the next time you restart your PC, the boot process will take a little longer while Windows 10 checks to see whether you are pressing F8 to invoke the Safe Mode boot experience; follow these steps.

- 1. When your PC restarts, select Troubleshoot from the Choose An Option menu.
- 2. Select Advanced Options.

Select Startup Settings and click Restart. You see the Advanced Boot Options screen as shown in Figure 3-9.

Advanced Boot Options		
Choose Advanced Options for: Microsoft Windows 10 (Use the arrow keys to highlight your choice.)		
Repair Your Computer		
Safe Mode Safe Mode with Networking Safe Mode with Command Prompt		
Enable Boot Logging Enable low-resolution video Debugging Mode Disable automatic restart on system failure Disable Driver Signature Enforcement Disable Early Launch Anti-Malware Driver		
Start Windows Normally		
Description: Start Windows with only the core drivers and services. Use when you cannot boot after installing a new device or driver.		
ENTER=Choose	ESC=Cancel	

FIGURE 3-9 Windows 10 Advanced Boot Options screen

- 3. Select Safe Mode and press Enter.
- 4. Log on to the system and roll back the driver as described earlier.

The rollback feature remembers only the last driver that was installed and doesn't keep copies of multiple drivers for the same device.

Skill: Resolve driver issues

One of the most common issues with device drivers relates to users attempting to install a driver designed for an earlier operating system or a different architecture. In some cases on previous versions of Windows, it might have been possible to install a Windows 7 driver on a Windows 8–based computer, but this is not a supported operation for Windows 10 and should be avoided in a production environment. As is the case with other software installa-tions, you can't use a 32-bit driver for a 64-bit resource. You can't use a 64-bit driver to communicate with a 32-bit resource, either.

In this section, you review how to disable specific device driver updates and tools you can use to verify the drivers on your system.

This section covers how to:

- Disable updates
- Use driver verification tools

Disable updates

Sometimes a specific update or driver will not be compatible with your system. Although all updates and drivers should be thoroughly checked before they are made available for installation, it is almost impossible to test every combination of software and hardware that can coexist on a computer. In some configurations, the new software might produce unsatisfactory results. You saw earlier that one method to avoid this situation is to turn off updates completely.

Disabling automatic driver updates might have a more widespread effect than you want, especially if you only need to disable or prevent the installation of a single driver. To enable you to block a specific update, Microsoft has released the Show Or Hide Updates trouble-shooter package, available from the Microsoft Download Center at *https://support.microsoft .com/kb/3073930*.

This troubleshooter, shown in Figure 3-10, searches for available driver and Windows updates and then enables you to hide them, which prevents Windows from automatically installing them.

	_	Х
~	Show or hide updates	
	Hide updates Updates are available. Select the updates that aren't working, Windows will not install hidden updates. Run this troubleshooter a cyin to show hidden updates so they install automatically.	
	 INTEL driver update for Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 1 - 1 INTEL driver update for Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 8 - 1 INTEL driver update for Xeon(R) processor E3 - 1200 v2/3rd Gen Core processor DRAM INTEL driver update for Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 7 - 1 INTEL driver update for Intel(R) 277 Express Chipset LPC Controller - 1E44 INTEL driver update for Intel(R) 7 Series/C216 Chipset Family SMBus Host Controller - 1 INTEL driver update for Intel(R) 7 Series/C216 Chipset Family SMBus Host Controller - 1 INTEL driver update for Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 5 - 1 INTEL driver update for Windows Defender - KB2267602 (Definition 1.217.1672.0) 	~
	Next Cance	1

FIGURE 3-10 Show Or Hide Updates troubleshooter

Each time you experience an issue with a driver or update that you don't want installed, you can run this troubleshooter and select the updates that you want to disable.

NOTE DEVICE MANAGER ERROR TROUBLESHOOTING

Device Manager marks a device that is not operating normally with a yellow exclamation point. When troubleshooting a device, you can check the error that Device Manager reports. For a detailed list of errors that Device Manager reports, see the article at https://msdn.microsoft.com/library/windows/hardware/ff541422(v=vs.85).aspx.

Use driver verification tools

If you encounter issues with drivers that seem to relate to malware or missing drivers, you can use a command-line tool called Sigverif.exe, which checks whether any drivers have been installed on the computer that have not been signed. The check can take several minutes to complete. To run this tool, perform the following steps.

- 1. Open a command prompt. (Standard user privilege level is OK.)
- 2. Type sigverif.exe and press Enter.

The File Signature Verification Tool appears.

- 3. Review the Advanced options.
- 4. Click Start and view the results, as shown in Figure 3-11.
| Command Prompt | | | | | | 1909S | \times |
|---|---|----------------------------|---|---|---|-------------------|----------|
| Microsoft Windows [Vers:
(c) 2015 Microsoft Corp | ion 10.0.10586]
oration. All rights reserv | ed. | | | | | ^ |
| C:\Users\Andrew>sigveri | f | | | | | | |
| C:\Users\Andrew> | 📴 File Signature Ve | ification | | | | \times | |
| | | | To help maintain t
have been digitally
files can be quick | he integrity of y
y signed so that
ly detected. | our system, critica
any changes to t | ll files
these | |
| | E | k SigVerif
our files ha | ive been scanned | l and verified a | as digitally signe | ×
ed. | |
| | | | | | 0 | К | |
| | | | Stop | Clos | e <u>A</u> dvan | ced | |
| | | | | | | | ~ |

FIGURE 3-11 File Signature Verification tool

The sigverif tool is useful if you need to locate an unsigned driver, but there is a more powerful driver verification tool built into Windows 10, called the Driver Verifier Manager.



EXAM TIP

In the advanced settings of the Signature Verification tool is the file name of the log file, a good thing to know for the exam. Review the log file found at %SystemRoot%\Sigverif.txt after the operation has completed.

With the enhanced kernel mode operation and reliance on signed drivers, Windows 10 should be less prone to frequent Stop errors. Although less likely, even signed drivers can cause problems, especially if you have an exotic combination of hardware inside your computer. If you do encounter instability then, use the built-in Driver Verifier to discover whether a faulty driver is causing the problem.

Driver Verifier Manager can help you troubleshoot, identify, and resolve common device driver problems, and you can then remove, reinstall, or roll back the offending driver with Device Manager.

To run the series of driver tests, follow these steps.

- 1. Open a command prompt (Admin), using administrative privileges.
- 2. Type verifier.exe and press Enter.

The Driver Verifier tool appears.

3. Review the settings in the tool.

Depending on which option you choose, you might need to restart your machine for the tool to recognize all loaded drivers.

4. After you have selected drivers to be tested, restart the computer, restart the application, and then select Display Information About The Currently Verified Drivers.

Driver Verifier Manager tests each specified driver at startup and then enables you to perform live test of each loaded driver by a range of tests, as shown in Figure 3-12. If it detects a problem, the tool can identify the driver, and then you can disable it.

sys	Value 23912		
sys	23912		
vs	6		
sys	31		
allocated	0		
per of allocations	0		
bytes allocated	244		
s program.			
	sys to allocations : bytes allocated	sys 31 31 0 ber of allocations 0 tytes allocated 244 number of allocations 2 s program.	sys 31 sallocations 0 : bytes allocations 244 : number of allocations 2

FIGURE 3-12 Driver Verifier Manager tool

Skill: Configure driver settings

Device drivers provide Windows 10 with the information required to populate the device details that you find in Device Manager. If only a few details are available to view, the device might have been installed using the built-in driver, and you might be able to install a driver from the manufacturer's website, which will give additional information through Device Manager.

In this section, you explore Device Manager, configure driver settings that are available for installed devices, and look at how to view and configure settings for older hardware.

This section covers how to:

- View device settings
- Support older hardware

View device settings

The default Device Manager screen enables users to work directly in the Properties dialog box of a device and provides information about the device that the hardware and device driver provide. The following is a review of Device Manager features that you can use to explore the available information so that you can configure the driver settings.

In Device Manager, explore these four menu options.

- **File** This menu enables you to exit the console and optionally delete the record of the console customizations you make to the console settings.
- Action This menu enables you to access the action-specific tasks relating to the highlighted hardware, including Update Driver Software, Disable, Uninstall, Scan For Hardware Changes, Add Legacy Hardware, Properties, and Help.
- **View** This menu enables you to change how the console view displays advanced information relating to the devices listed in Device Manager. You can view devices by device type or connection or resources by type or connection. Some hardware is also hidden from normal view, and this option can be set to show hidden devices. The Customize option enables you to show or hide items within the console.
- Help This menu offers access to help topics relating to Device Manager and the console, plus a link to the Microsoft TechCenter website, which is part of TechNet.

There are several advanced views in Device Manager that standard users do not normally use. These include the connection type and hidden device views, as follows.

- Show Hidden Devices In previous versions of Windows, printers and non–Plug and Play (PnP) devices could be marked by the device manufacturer as a NoDisplayClass type of device, which prevents it from automatically being displayed in the Device Manager. Devices that have been removed from the computer but whose registry entries are still present can also be found in the hidden devices list.
- Devices By Type This is the default view and shows devices grouped by familiar device name such as Network Adapters, Ports, and Disk Drives. Each node can be expanded by selecting the > symbol to the left of the node name.
- Devices By Connection You can view devices based on the hardware connection, such as physical or virtual.
- Resources By Type Use this option to view resources organized by how they connect to system resources, including Direct Memory Access (DMA), Input/Output (IO), Interrupt Request (IRQ), and Memory. Unless your BIOS allows you to declare that you are not using a Plug And Play–compliant operating system, you will not be able to modify these settings.
- Resources By Connection This view is for advanced users only and is not particularly useful on a modern system. Viewing the device hardware resources by DMA, IO, IRQ, and Memory were useful for earlier versions of Windows prior to the introduction

of Plug And Play, which allowed the operating system to manage automatically the resources required by devices.

Support for older hardware

Some of the advanced settings in Device Manager are seldom used but have been retained for backward compatibility with older devices that do not support Plug And Play. Modern hardware peripherals must support Plug And Play, which allows Windows 10 to assign hardware resources automatically to new devices. If you look on the Resource tab of a device Properties dialog box in Device Manager, you see that a check box is selected indicating that Windows 10 is using automatic settings, as shown in Figure 3-13. The setting is dimmed and not changeable unless you disable the BIOS/UEFI setting, which declares that the operating system is Plug And Play–compliant.

📕 Device Manager					_	\times
File Action View Help						
🗢 🌩 📰 📴 📝 📷 💭	上 🗙 🕒					
DESKTOP Audio inputs and outp	Qualcomm Atheros A	AR8161 PCI-E Gigat	it Ethernet Cont	roller (ND X		^
> 💻 Computer	General	Advanced	Driver	Details		
> 👝 Disk drives	Events	Resources	Power M	anagement		
> 🥃 Display adapters > 🛺 Human Interface Devic > 📹 IDE ATA/ATAPI control	Qualcomm (NDIS 6.30	Atheros AR8161 PCI)	E Gigabit Etheme	t Controller		
> 📑 Imaging devices	Resource settings:					
Keyboards	Resource type	Setting		^		
Monitors	Memory Range	0000000F7C0000	0 - 0000000F7C	3FFFF		
V P Network adapters	I/O Range	D000 - D07F				
Hyper-V Virtual Eth	IRQ	0x00000012 (18)		¥		
Hyper-V Virtual Eth Juniper Networks V Qualcomm Athero	Setting based on:			~		
> Portable Devices		llee automatic eetti	Cha	nan Catting		
> 🛱 Ports (COM & LPT)			Cild	nge seung		
> 📇 Print queues	Conflicting device list	-				
> 🖃 Printers	No conflicts.			~		
> Processors						
> Software devices						
> iii Sound, video and gam				\sim		
> 🍇 Storage controllers						
> Image: System devices Inviversal Serial Bus con			ОК	Cancel		Ŷ

FIGURE 3-13 Automatic resource allocation

The Plug And Play standard for connecting devices to Windows is nearly two decades old. Some hardware still exists that requires the administrator to install it manually. In Device Manager, the Add Hardware Wizard enables you to install hardware that does not support Plug And Play. To install such hardware, perform the following steps.

- 1. Open Device Manager.
- 2. On the Action tab, click Add Legacy Hardware.

- 3. On the Welcome To The Add Hardware Wizard page, click Next.
- 4. Select one of these options:
 - Search For And Install The Hardware Automatically (Recommended)
 - Install The Hardware That I Manually Select From A List
- **5.** Follow the wizard prompts to finish the configuration of the hardware and provide the driver when requested.

NOTE NON-PNP (OLDER) DEVICES ARE NOT SHOWN IN WINDOWS 10

Since Windows 8 and Windows Server 2012, non-PnP devices have not been represented in Device Manager as viewable nodes.

Skill: Driver signing

One of the reasons Windows 10 is more secure than earlier versions of Windows is that kernel mode drivers must now be submitted to and digitally signed by the Windows Hardware Developer Center Dashboard portal. Windows 10 will not load kernel mode drivers that the portal has not signed.

To ensure backward compatibility, drivers that are properly signed by a valid cross-signing certificate will continue to pass signing checks on Windows 10.

NEED MORE REVIEW? DRIVER SIGNING CHANGES IN WINDOWS 10

This MSDN resource provides more depth on driver signing changes in Windows 10 at https://blogs.msdn.microsoft.com/windows_hardware_certification/2015/04/01/driver-signing -changes-in-windows-10/.

Windows 10 also introduces a new Universal Windows driver, which is designed to work on all OneCoreUAP-based editions of Windows, such as Windows 10 for desktop editions (Home, Pro, Enterprise, and Education), Windows 10 Mobile, and Windows 10 Internet of Things Core (IoT Core).

A Universal Windows driver has access to the trusted kernel and has a very limited range of the interfaces that are available to a Windows driver. OEMs can supplement the driver functionality by including additional software, but this will be external to the driver. Windows 10 security is more robust by locking down the kernel to signed drivers and encouraging developers to use the Universal Windows driver model,

For information about how to build, install, deploy, and debug a Universal Windows driver for Windows 10, see Getting Started With Universal Windows Drivers.

NEED MORE REVIEW? WINDOWS 10 UNIVERSAL WINDOWS DRIVERS

This MSDN resource provides more depth on Universal Windows drivers at *https://msdn* .microsoft.com/library/windows/hardware/dn927349(v=vs.85).aspx.

If you have a specific need to install an unsigned driver—for example, if you are a developer and work with drivers, and you want to test the driver functionality without having to sign the driver digitally each time—you can invoke a special boot-time configuration setting that bypasses the security the Windows 10 driver enforcement model provides. To load an unsigned driver (not recommended), you can follow these steps.

- 1. Log out of Windows 10.
- 2. On the logon screen, click the Power button, hold down the Shift key, and click Restart.
- 3. On the Choose An Option screen, choose Troubleshoot.
- 4. Choose Advanced Options.
- On the Advanced Options screen, select Startup Settings and click Restart. Advanced Boot Options appears.
- 6. Choose Disable Driver Signature Enforcement, as shown in Figure 3-14.



FIGURE 3-14 Disable Driver Signature Enforcement

7. Install the unsigned driver and then restart the computer.

Skill: Manage driver packages

When device drivers are created by the original equipment manufacturer (OEM), they are deployed with the hardware in a driver package that includes all the files and information required for Windows 10 to communicate with the hardware. You see how driver packages are managed and how to install, provision, and import driver packages on Windows 10 devices.

This section covers how to:

- Use the driver store
- Use PnPUtil.exe to manage driver packages

Use the driver store

You saw earlier that the driver package can include an information file (.inf file), any files that the .inf file references, and a .cat file that contains the digital signature for the device driver. Windows 10 uses the Driver Store to hold device drivers that have been installed or pre-staged.

All Windows 10 kernel mode drivers must be digitally signed by the Windows Hardware Developer Center Dashboard portal. Windows 10 will prevent the loading of new kernel mode drivers that are not signed by the portal. This is an important change from previous versions of Windows and will make the operating system more secure. Previously, it could be possible for a hacker to gain unauthorized access to a system by using a flaw in an unsigned device driver. Ensuring that all drivers are digitally signed will remove the ability for a hacker to add or modify device driver contents.

If you are creating a custom installation image, or if you build and deploy many computers, you can speed up the driver installation process by pre-loading the Windows 10 driver store with the specific drivers for the peripheral devices that your devices will be using. When Windows 10 finds the drivers it needs in the driver store, located in %SystemRoot% System32\DriverStore, it uses these local drivers and does not download them from Windows Update.

Pre-installing a driver is a two-stage process, and the first stage must be carried out with administrator credentials. You need to add the driver package to the driver store and then ensure that the hardware is attached; Windows 10 then automatically locates and installs the local driver.

There are a few ways to deploy drivers to the driver store, and the most appropriate method will depend on your physical network infrastructure, network connectivity, and level of administrative privileges on devices, among other things.

NOTE AVOID DELETING FILES FROM THE DRIVER STORE

You should take care not to delete driver packages manually from the driver store. Doing so can cause an inconsistency among the INF file, the driver store catalog, and the driver in the driver store. For more information, go to *https://msdn.microsoft.com/library/windows* /hardware/ff546200(v=vs.85).aspx.

Use PnPUtil.exe to manage driver packages

To pre-stage the installation of a specific hardware device, you can install a driver manually before connecting the device, by using the PnPUtil.exe command-line tool. This could be use-ful when distributing a laptop to a remote user who you know has a local printer or scanner. Standard users cannot normally install device drivers, but if the driver package is already in the driver store, this is possible.

Run the PnPUtil.exe command by using administrative privileges, and you can use it to manage the Driver Store, adding, deleting, and listing driver packages. You saw earlier that a driver package consists of all the information Windows 10 requires to install and trust the driver, including the following.

- Driver files Dynamic link library (DLL) files with the .sys file extension.
- Installation files Text files containing all the information needed to install a driver. These .inf files include information such as driver name and location, driver version information, and registry information. These files are copied to the %SystemRoot%\Inf directory during installation. Every installed device must have an .inf file.
- Driver Catalog file Contains a cryptographic hash of each file in the driver package. These hashes are used to verify that the package was not altered after it was published (created). Digitally signing the catalog file proves the file has not been altered, because only the digital signature owner can sign the file.
- Additional files These are files such as a device installation application, device icon, device property pages, and additional files.

For enhanced security, Windows 10 now uses a single kernel model across all editions of Windows 10 and is encouraging the use, now, of a new universal driver model. This universal .inf file is required when deploying device drivers to an offline system image, such as when building a Windows 10 Mobile system (which does not support Plug And Play).

The syntax for the PnPUtil.exe command-line tool is as follows.

PnPUtil.exe -a <path to the driver> \<drivername>.inf

The full list of parameters is shown in Table 3-1.

TABLE 3-1 PnPUtil.exe parameters

Parameter	Description
-a	Adds a driver package to the driver store
-d	Removes a driver package from the driver store
-е	Lists the driver packages that are currently in the driver store
-f	Forces the deletion of the specified driver package from the driver store; cannot be used with the -i parameter.
-i	Installs the driver package on matching devices that are connected to the system. Cannot be used with the -f parameter
/?	Displays help

An example command to add the INF file specified by MyDevice.inf to the driver store (located at %SystemRoot%\System32\DriverStore) is:

```
PnPUtil.exe -a C:\Temp\MyDevice.inf
```



EXAM TIP

After a driver has been added to the driver store, the driver is referenced in the store through its published name, which might be different from the driver package (.inf) name. You can review the published name by viewing the contents of the .inf file.

In addition to the PnPUtil.exe tool, you can use the following Windows PowerShell cmdlets.

- Get-PnpDevice Displays information about PnP devices
- Get-PnpDeviceProperty Displays detailed properties for a PnP device
- **Enable-PnpDevice** Enables a PnP device
- Disable-PnpDevice Disables a PnP device

An example Windows PowerShell command to enable the device with an instance ID of 'USB\VID_5986&;PID_0266&;MI_00\7&;1E5D3568&;0&;0000' is as follows.

```
PS C:\> Enable-PnpDevice -InstanceId 'USB\VID_5986&;PID_0266&;MI_00\7&;1E
5D3568&;0&;0000'
```

For more information about, or for the syntax of, any of the Windows PowerShell cmdlets, you can use the Get-Help *<cmdlet name>* cmdlet such as the following.

Get-Help <cmdlet name> -Examples

Skill: Download and import driver packages

Drivers are packaged together; each driver package consists of all the software components that are needed for your device to work with Windows.

Most drivers are obtained directly by using built-in tools such as Windows Update, but if you are provisioning systems, you might want to deploy the PC with the required drivers already imported and configured.

This section covers how to:

- Download driver packages
- Deploy driver packages by using the Windows Imaging and Configuration Designer
- Import driver packages

Download driver packages

Device drivers can be accessed to perform a malicious attack on your systems. Therefore, you should ensure that driver packages are sourced only from reputable locations such as the manufacturer's own website. You should avoid third-party driver repository websites because some sites repackage drivers and include spyware or freeware products in the installation files.

The built-in Windows 10 driver packages are often just the core drivers created by your device manufacturer and provided by Microsoft through the Windows Hardware Quality Labs (WHQL), which tests and digitally signs the drivers. Video drivers often include additional software support and hardware functionality. For example, drivers sourced directly from NVIDIA or AMD for their graphics cards include the NVIDIA Control Panel or the AMD Catalyst control panel, respectively.

If you are seeking the most up-to-date or even beta version of a device driver, you must download this directly from your device manufacturer. In most cases, you will not need to upgrade your device driver after Windows 10 is installed. If everything is working properly, you probably don't need to install extra hardware drivers.

If you are a gamer, it can be beneficial to ensure that your graphics card drivers are using the latest versions so that they support the latest PC games.

You should consider downloading new driver packages in the following scenarios.

- If you play PC games Install the latest graphics drivers directly from your graphics card manufacturer because they are often required to play the latest games. Newer versions can also improve graphics performance.
- When you need a hardware utility Install the latest version if the manufacturerprovided driver package includes a hardware utility, such as a network configuration tool or ink monitor for your printer.
- To resolve a bug Bugs can be found in released drivers and will often be fixed in the most up-to-date version.
- To install hardware manually If Windows Plug And Play does not automatically detect and install the hardware, you might need to download the driver package from the manufacturer and install the device driver.

Deploy driver packages by using the Windows Imaging And Configuration Designer

A new method of deploying customized Windows devices (or applying customizations to an already deployed device) is by using the new Windows Imaging And Configuration Designer (ICD) tool available in Windows 10. This tool is part of the Windows Assessment And Deployment Kit (ADK) for Windows 10, which is available at *http://go.microsoft.com* /fwlink/?LinkId=526803.

NOTE DOWNLOAD THE LATEST VERSION OF THE WINDOWS ADK FOR WINDOWS 10

You must ensure that the Windows ADK for Windows 10, language packs, and Feature-On-Demand (FOD) files are all from the same build with a matching build number.

After you have installed the Windows ADK for Windows 10, you can open the ICD and create a new provisioning package (with the .ppkg file extension), which can then be deployed to the devices requiring customization. You can email the .ppkg file or deploy it physically on a USB drive through Microsoft Intune or Group Policy, or you can build it directly into a new system image if you have not yet deployed the computer.

To deploy a device driver by using the Windows ICD, create a new project but use the following steps.

- 1. Click Start, type ICD, and launch Windows Imaging And Configuration Designer.
- 2. Accept User Account Control (UAC) if prompted.
- 3. Click New Provisioning Package.
- 4. On the Enter Project Details page, name the project **Deploy Scanner Driver**.
- **5.** On the New Project page, select the Common To All Windows Desktop Editions, click Next, and click Next again.
- **6.** On the Available Customizations page, expand Deployment Assets and then click Drivers.
- 7. In the middle pane, next to the Driver folder path, click Browse.
- Browse to your INF-based driver, select the driver, and then click OK.
 The driver .inf file should show up in the Drivers box. (You might need to extract driver files if they have been packaged as .zip or .exe files.)
- 9. In the Name box, type the friendly name for the driver, as shown in Figure 3-15.

NOTE DIGITALLY SIGNING WINDOWS ICD PROVISIONING PACKAGES

If you have a certificate authority (CA), attach an organizational certificate to the package to sign the .ppkg file.

🖙 Windows Imaging and Configur	ation Designer		-	_		Х
File 🗸 📄 Deploy 🖌 📝 Expo	ort v					
Start page Deploy Scanner	Driver 🗙					
Available customizations View: All settings Y Search P Deployment assets Applications Driver set Drivers Features on demand Language packages Reference device data Windows updates P Runtime settings	Driver folder path: [E:\Scanner Drivers\x64 Name: Home Scanner Driver]Force unsigned install. Drivers: ScannerDriver2800ux.inf	Refresh	Selected o	ustor	nizatic	ons
READY 0 Customizations 0 Inva	alid WORKFLOW: PROVISIONING PACKAGE	IMAGE: COMMON TO	ALL WINDOWS	DESK	TOP EDI	TIONS .:

FIGURE 3-15 Windows Imaging And Configuration Designer (ICD) tool

- **10.** Select the Force Unsigned Install check box only if the driver is unsigned.
- **11.** Click Add to add the customization.

This now appears in the right pane. The driver's descriptive name should appear in the Selected Customizations pane. To complete the process, the provisioning package is created by using the following steps.

- 1. On the menu bar, click Export.
- 2. Select Provisioning Package.
- **3.** On the Describe The Provisioning Package page, review the information, modify Owner to be IT Admin, and then click Next.
- 4. On the Select Security Details For The Provisioning Package page, click Next.
- Choose the default name and location or provide a path and file name for the provisioning package to be created and click Next.
- **6.** On the Build The Provisioning Package page, review the information and then click Build.

- 7. When it is complete, click Finish.
- After the provisioning package has been built, use the links provided to locate the created files. You can deploy these files to your remote users on removable media such as USB drives.

Import driver packages

The remote users will import the driver package contained in the provisioning package to their computer by completing the following steps.

- 1. Insert a removable drive containing the provisioning package files (in the media root).
- 2. Open Settings and then click Accounts.
- 3. Click Work Access and then click Add Or Remove A Package From Work Or School.
- 4. On the Provisioning Packages page, click Add A Package.
- **5.** On the Choose A Method page, select Removable Drive from the Add From dropdown list.
- 6. Select the package that you want to install and click Add, as shown in Figure 3-16.

← Settings	(11)	×
ADD A PACKAGE		
Choose a method Add from		
Removable Media \sim		
Select a package		
Deploy Scanner Driver.ppkg		
	Add	

FIGURE 3-16 Adding a provisioning package

- 7. On the UAC page, click Yes.
- On the Is This Package From A Source You Trust page, click Yes, Add It. The package will install in the background.

EXAM TIP WINDOWS DESKTOP DEPLOYMENT AND IMAGING LAB

Windows ICD is new, and you should review this topic because it is likely to be featured in the exam. For more information, go to *https://msdn.microsoft.com/library/windows* //hardware/dn898436(v=vs.85).aspx.

Skill: Use Deployment Image Servicing And Management tool to add packages

You saw earlier that the Deployment Image Servicing and Management (DISM) tool is now included as part of the Windows 10 operating system. It is useful for offline image servicing. DISM is a command-line tool that you can use to maintain images and apply them with Windows Updates. It is also used to add and remove Windows features, including language packs, and to manage device drivers.

This section covers how to:

- Add packages by using DISM
- Manage driver packages with DISM

Add packages using DISM

If you have a custom Windows 10 image, you can use DISM to modify it, and the changes will be visible when you next deploy the image. This can be useful when you know that a driver has been updated since you built the deployment image. Using DISM to inject the new driver saves you from having to rebuild the whole image. Using DISM is similar to using a file compression tool such as WinRAR, whereby you add or remove new files and then WinRAR reseals the .wim, .vhd, or vhdx file ready for deployment.

When you use DISM to install a device driver to an offline image, the device driver is added to the driver store. When the image is booted, Plug And Play (PnP) runs, looks for drivers in the store, and associates them with the corresponding devices on the computer they're being installed on.

To add drivers to an offline image by using DISM, use these steps.

- 1. Right-click the Start button and select Command Prompt (Admin).
- 2. Establish the name or index number for the image that you are servicing by typing:

Dism /Get-ImageInfo /ImageFile:C:\test\images\install.wim

Mount the offline Windows image by typing the following.

```
Dism /Mount-Image /ImageFile:C:\test\images\install.wim /Name:"Windows Offline
Image" /MountDir:C:\test\offline
```

- 4. You can now add the driver, located in the C:\Drivers folder, to the image by typing: Dism /Image:C:\test\offline /Add-Driver /Driver:C:\drivers\New_driver.inf
- If you have additional drivers in a folder, you can use the /Recurse option, which installs all the drivers from a folder and all its subfolders. To do this, type:

Dism /Image:C:\test\offline /Add-Driver /Driver:c:\drivers /Recurse

6. You can review the drivers in the Windows image by typing:

Dism /Image:C:\test\offline /Get-Drivers

In the list of drivers, notice that the added drivers have been renamed Oem*.inf. This ensures that all driver files in the driver store have unique names. For example, the New_Driver1.inf and New_Driver2.inf files are renamed Oem0.inf and Oem1.inf.

7. To complete the operation, commit the changes and unmount the image by typing:

Dism /Unmount-Image /MountDir:C:\test\offline /Commit

NEED MORE REVIEW? DISM

For a detailed reference for the DISM command-line options, you can visit TechNet at https://technet.microsoft.com/library/hh825099.

Manage driver packages with DISM

During the life of a Windows 10 installation, the system downloads and installs multiple versions of device driver packages over time. For devices with small hard-drive capacity, be aware of how to locate and delete outdated driver packages that the system retains.

You can use the built-in Disk Cleanup tool to remove device driver packages that have been kept after newer drivers are installed.

To clean up old device drivers by using the Disk Cleanup tool, perform these steps.

- 1. Click the Start button, type **Disk Cleanup**, and then select the Disk Cleanup app.
- 2. In the Drive Selection dialog box, select (C:) and click OK.
- 3. On the Disk Cleanup results screen, select Clean Up System Files.
- 4. In the Drive Selection dialog box, select (C:) and click OK.
- 5. On the Disk Cleanup results screen, select Device Driver Packages and click OK.
- On the Are You Sure You Want To Permanently Delete These Files page, click Delete Files.

All driver packages that were installed during the Windows 10 setup process are stored in a directory called WinSxS, the side-by-side component store. This folder contains driver packages and operating system components so that you can add devices later without having to supply device drivers. If disk space is limited, you can purge the WinSxS directory contents, because it could occupy a significant amount of disk space.

To analyze the Windows Component Store for driver packages and other files that can be deleted, you can use the DISM command by using the following steps.

1. Right-click the Start button, select Command Prompt (Admin), and type the following.

DISM /Online /Cleanup-Image /AnalyzeComponentStore

The tool analyzes your system. Typical results are shown in Figure 3-17.



FIGURE 3-17 Analyzing the Component Store (WinSxS) with DISM

2. When the analysis is complete, you can initiate a cleanup of the Windows Component Store by typing the following command.

DISM /Online /Cleanup-Image /StartComponentCleanup /ResetBase

IMPORTANT DO NOT DELETE THE WINSXS FOLDER

Do not manually delete the WinSxS directory or its contents to reclaim the space, because Windows creates many hard links from files in the WinSxS folder to locations in system folders.

Summary

- Device Manager is the primary tool for installing and managing devices.
- Device And Printers and Device Stage offer visual alternatives to Device Manager.
- Windows Update automatically updates device drivers.
- To install or pre-stage device drivers manually, use the PnPUtil command-line tool.
- Updated device drivers that are not stable can be rolled back to the previous version.
- You can use the File Signature Verification tool (Sigverif.exe) to check that all drivers are digitally signed and DISM to manage driver packages for offline images.
- Plug And Play is the feature that enables Windows to detect and install the correct device driver automatically for the attached hardware.
- Driver signing is enforced in Windows 10 and protects system security.
- The new Windows Imaging And Configuration Designer (ICD) generates provisioning packages with the .ppkg file extension, which can customize Windows 10.

Thought experiment

In this thought experiment, demonstrate your skills and knowledge of the topics covered in this chapter. You can find answers to this thought experiment in the next section.

Your organization has recently recruited 20 new members to the sales team, who will work across the United States. Your manager wants to issue them the following hardware, which will be shipped to the employee's home address directly from the online reseller.

- Surface Pro 4 tablet
- Bluetooth mouse
- Epson WF-3520 printer

The sales team members have standard user accounts, email accounts, and Internet access at home. You are required to ensure that the sales team members can operate the new equipment without delay and with minimal involvement of the company help desk. The organization holds its own certificate authority for creating certificates.

The company has commissioned a short introduction to Windows 10 and the functions of the Epson printer and mouse, which is available on the company intranet, by email, and of-fline. All users must view the training prior to using Windows 10.

Answer the following questions for your manager:

- 1. Where will you obtain the latest driver software for the mouse and printer drivers?
- 2. How will you provision the mouse and printer drivers on the Surface tablets?
- 3. Can you provision the mouse and printer drivers as one package or only separately?

- 4. How will you ensure that the users trust the provision of drivers?
- 5. How can you ensure that users are familiar with the operation of the Epson printer?

Thought experiment answers

This section contains the solutions to the thought experiment.

- **1.** You would use the media and device driver supplied with the hardware equipment or download the latest version from the manufacturer's official website.
- 2. You would create a provisioning package with the Windows Imaging And Configuration Designer (ICD), export the .ppkg files, and deploy these to the users by email, postal mail, or an intranet site. The users could then run the provisioning packages on their devices. If they required further assistance, they could call the help desk.
- **3.** You can use the ICD to create provisioning packages that deploy single or multiple customizations to Windows 10.
- **4.** You would use only digitally signed device drivers and, additionally, digitally sign the provisioning package with the organizational certificate authority.
- 5. You should ask each member of the remote sales team to access the company intranet site and review the short introduction to Windows 10 and the functions of the Epson printer that will be available there. You could also ensure that they are aware of Device Stage for the Epson printer.

This page intentionally left blank

Index

Numbers and Symbols

6to4 protocol, 178 16-bit applications, 17 32-bit architecture device drivers, 76 Windows 10 versions, 17 64-bit architecture device drivers, 76 Windows 10 versions, 17 802.11x wireless standards, 190

A

access control entry (ACE), 257 access control list (ACL), 50, 257, 260 accessibility options, 115-116 ACE (access control entry), 257 ACL (access control list), 50, 257, 260 ACT (Application Compatibility Toolkit), 7-9 Action Center about, 108-109 notifications area, 111-112 Quick Action tiles, 109-111 Action menu (Device Manager), 80 activation about, 137-138 selecting method, 138-139 volume activation, 140–142 for Windows 10, 142-144 Active command (DiskPart), 210 Active Directory configuring, 148-151 volume activation, 140 Active Directory Administrative Center (ADAC), 148, 152-154 Active Directory Domain Services (AD DS) activation support, 138, 140 blocking Windows Store Apps, 288 configuring domain settings, 443-444 configuring firewall settings, 300 configuring Start with GPOs, 104 configuring UAC, 146-147

configuring Windows Update, 324 Device Registration requirement, 445 disabling UACs, 430 distributing fixes via GPOs, 9 dynamic access control, 269 HomeGroups feature and, 174, 243 implementing DirectAccess, 178-179 installing desktop apps, 274, 276 network location profiles, 180 remote connections, 314 volume licensing, 140 Active Directory Federation Services (AD FS), 445 Active Directory Users And Computers snap-in, 148, 152 active styluses, 19 ActiveX controls, 121 AD DS (Active Directory Domain Services) activation support, 138, 140 blocking Windows Store Apps, 288 configuring domain settings, 443-444 configuring firewall settings, 300 configuring Start with GPOs, 104 configuring UAC, 146-147 configuring Windows Update, 324 Device Registration requirement, 445 disabling UACs, 430 distributing fixes via GPOs, 9 dynamic access control, 269 HomeGroups feature and, 174, 243 implementing DirectAccess, 178-179 installing desktop apps, 274, 276 network location profiles, 180 remote connections, 314 volume licensing, 140 AD DS server role, 150 AD FS (Active Directory Federation Services), 445 ad-hoc mode (wireless networking), 190 ADAC (Active Directory Administrative Center), 148, 152-154 Add-AppxPackage cmdlet, 289 Add command (DiskPart), 210 Add Hardware Wizard, 81-82 Add Mirror Wizard, 234 Add New Tasks Wizard, 458 Add-PhysicalDisk cmdlet, 225 Add-Printer cmdlet, 371

Add Printer Wizard, 68 Add-PrinterDriver cmdlet, 371 Add-PrinterPort cmdlet, 371 Add Roles And Features Wizard, 150–151 ADKsetup.exe tool, 292 Admin Approval Mode, 145 Administrator account about, 420, 429 canceling print jobs, 243 configuring UAC, 144-147 creating, 29 creating or deleting restore points, 398 installing desktop apps, 275 sharing files and folders, 240 WBAdmin tool, 403 workgroup environments, 314 Advanced Boot Options screen, 75, 83 advanced permissions, 258-260 Advanced Sharing Settings dialog box, 188–189 Advanced TCP/IP Settings dialog box DNS tab, 166-167, 172-173 IP Settings tab, 166-167 WINS tab, 166-167 All Apps element (Start), 106 All Settings element (Start), 106 All Settings tile, 110 Allow permission, 260 Allow Print permission, 242 answer files, 22-23 anycast addresses, 168 APIPA (Automatic Private IP Address), 166, 169 AppData folder, 15 Append Data permission, 259 application compatibility 16-bit applications, 17 about, 6 Application Compatibility Toolkit, 7–9 mitigating issues, 9 testing in multiboot configuration, 45 troubleshooting, 42 Application Compatibility Toolkit (ACT), 7-9 application implementation allowing apps through Windows Firewall, 184–185 applying provisioning packages, 294–295 configuring app startup options, 279–282 configuring desktop apps, 273-279 configuring Windows features, 283-284 creating provisioning packages, 291–294 implementing Windows Store apps, 284–290 thought experiment, 295-296 Application log, 351 application tiles configuring, 102–104, 109–111 customizing user interface, 100, 104 aroupina, 104 Quick Action tiles, 109–111 .appx installer file, 289 Assign command (DiskPart), 210 assigned apps, 276

authentication and authorization about, 419 configuring AD DS domain settings, 443-444 configuring device registration, 445-447 configuring HomeGroup settings, 441 configuring Microsoft accounts, 425-428 configuring Microsoft Passport, 433–434 configuring picture passwords, 434-435 configuring UAC, 429-431 configuring user accounts, 420-425 configuring Windows Hello, 432 configuring workgroup settings, 442-443 IPsec rules, 187–188 managing credential security, 435-438 managing device security, 438-441 remote connections, 314 thought experiment, 447-448 two-factor, 20, 433 authentication exemption rules (IPsec), 187–188 auto-hiding taskbar, 113 automatic driver installation, 73, 76 Automatic Private IP Address (APIPA), 166, 169

B

Background setting (Desktop), 106 backing up Backup And Restore tool, 269, 400-403, 411 data files, 12 operating systems, 34 WBAdmin tool, 403-405 Backup And Restore tool, 269, 400-403, 411-413 Backup Operators group, 403 Balanced power plan, 132 baseline performance, 368-369 basic permissions, 258-260 Battery Saver tile, 110 BCD (Boot Configuration Data) Store, 44 BCD Editor (Bcdedit.exe), 44-45, 75 BCDboot tool, 56-57 biometrics Microsoft Passport, 433-434 two-factor authentication, 20, 433 Windows Hello, 20, 432 **BitLocker Drive Encryption** about, 20 enterprise considerations, 411 recovering encrypted drives, 270 removable devices, 226-228 upgrading systems with, 38 virtual hard disks and, 54 BitLocker Drive Encryption Wizard, 227 BitLocker To Go, 226-228, 411 bloatware, 27 blocking upgrading to Windows 10, 39-41 blocking Windows Store App, 288 Bluetooth tile, 110

Boot Configuration Data (BCD) Store, 44 boot scenarios about, 43 configuring boot options, 56–57 multiboot Windows, 45–47 spanned volumes and, 204 USB drives, 210–211 viewing configuration information, 43–45 virtual hard disks, 52–54 bootable USBs, 57–58 Brightness tile, 110 Browser Helper Objects, 121 Build Wizard, 294

С

CA (certificate authority) Device Guard, 439 Device Registration, 446 driver packages, 89 Windows Store Apps, 289 .cat files, 84 certificate authority (CA) Device Guard, 439 Device Registration, 446 driver packages, 89 Windows Store Apps, 289 Challenge Handshake Authentication Protocol (CHAP), 176 Change permission, 250 Change Permissions permission, 259 CHAP (Challenge Handshake Authentication Protocol), 176 Chat task (Remote Assistance), 307 Checkpoint-Computer cmdlet, 389 checkpoints (virtual machines), 128 Choose An Option dialog box, 342 Choose How Updates Are Delivered dialog box, 322-323 Choose How Updates Are Installed dialog box, 321-322 Choose People To Share With dialog box, 240 Choose What To Do With This Disc dialog box, 274 Choose When To Be Notified About Changes To Your Computer dialog box, 146-147, 430 CIDR (Classless Interdomain Routing), 164 class A addresses, 163, 165 class B addresses, 163, 165 class C addresses, 163, 165 class D addresses, 163 class E addresses, 163 classful addressing, 163 classless addressing, 164 Classless Interdomain Routing (CIDR), 164 clean installations (wipe-and-load migrations) considerations for, 12-13 methods for, 10 migrating user data and settings, 14-15

performing, 27-30, 42 side-by-side migration, 10, 13 Clear-Disk cmdlet, 209, 215 Clear-DnsClientCache cmdlet, 196 Client Hyper-V feature 64-bit version, 17 about, 18-19 configuring, 283 installing role, 126–127 Closed Captions setting (Ease of Access), 115-116 CMAK (Connection Manager Administration Kit), 177 collector computer, 354 collector-initiated subscriptions, 354-355 Colors setting (Desktop), 106 Compatibility Administrator, 7–9 Compatibility Modes dialog box, 8 Compatibility View (Internet Explorer), 123 **Computer Management** creating folder shares, 247 managing local user accounts, 421-423 shared folders permissions, 250 viewing installed accounts, 420-421 Computer Name/Domain Changes dialog box, 442, 444 computer viruses, 376 computer worms, 376 Computers dialog box, 355 configuration information, viewing, 43-45 **Configuration Manager** deploying apps, 277-278 VPN profiles, 177-178 zero-touch installation, 276 Config.xml file, 51 Connect An USB Flash Drive dialog box, 387 Connect tile, 110 Connect To A Workplace Wizard, 175 Connection Manager Administration Kit (CMAK), 177 connection security rules IPsec, 187-188 Windows Firewall With Advanced Security, 186 Continuum feature, 19 Control Panel. See also specific apps Automatic Updates setting, 325 configuring remote management settings, 299 configuring Windows features, 283 disabling UAC, 146, 430 indexing options, 374 installing published apps, 156, 276 managing locally connected printers, 371 managing user accounts, 423-424 recovery tools, 386, 396 Theme settings, 107 uninstalling desktop apps, 103, 278–279 uninstalling updates, 322, 339 viewing Installed Updates, 337 Convert command (DiskPart), 210 Convert-VHD cmdlet, 215 Cortana feature about, 19 accessing Task Manager, 356

configuring, 116-118 enabling, 37 CRC (cyclic redundancy check), 202 Create A Basic Task Wizard, 460 Create A HomeGroup Wizard, 174, 243-244 Create A Recovery Drive Wizard, 386-387 Create A Shared Folder Wizard, 247–248 Create And Attach Virtual Hard Disk Wizard, 52, 214 Create command (DiskPart), 210 Create Files permission, 259 Create Folders permission, 259 Create New Application Fix dialog box, 8 Create New Data Collector Set Wizard, 368 Credential Guard, 436-438 Credential Manager, 436 credential security, 435-438 Current Branch for Business servicing option (upgrades), 332 Current Branch servicing option (upgrades), 331-332 custom rules IPsec, 188 Windows Firewall With Advanced Security, 186-187 cyclic redundancy check (CRC), 202

D

DAC (dynamic access control), 269 DACL (discretionary access control list), 248, 257 Data Collection And Preview Builds node (Group Policy), 326 data collector sets, 363-367 data management backing up data files, 12 configuring file and printer sharing, 237-243 configuring file system permissions, 254-263 configuring folder shares, 246-250 configuring HomeGroup connections, 243-246 configuring OneDrive, 251-254 configuring OneDrive usage, 263-266 configuring public folders, 250–251 migrating user data and settings, 14-15, 49-50 restricting access to removable devices, 228-231 thought experiment, 271-272 troubleshooting data access, 266-268 troubleshooting data recovery, 269-270 troubleshooting dynamic access control, 269 troubleshooting share and NTFS permissions, 268-269 data recovery. See system and data recovery default accounts, 420 default gateway addresses, 162 default printers, 372-373 DefaultAccount, 420 Delete permission, 259 Delete Subfolders and Files permission, 259 Delivery Optimization node (Group Policy), 326-327 Deny permission, 260

Deploy stage (enterprise servicing), 333 Deployment Image Servicing and Management (DISM) about, 22 adding driver packages, 91–93 applying Windows 10 image, 56 configuring Windows features, 283-284 enterprise recovery options, 392 managing driver packages, 92-93 modifying Windows features, 60 sideloading apps, 289 Desktop customizing settings, 106-107 multiple desktops, 108–109 desktop apps about, 273 Device Guard, 439 installing, 274-278 OneDrive service, 252-254, 263-264 uninstalling, 278–279 uninstalling from Start, 103 desktop mode, 109 Device Guard, 438-440 Device Health Attestation feature, 20, 440-441 Device Installation Settings dialog box, 73 Device Manager about, 455-456 Action menu, 80 administrative privileges, 72 configuring, 455-456 Details tab, 456 device property options, 456 Devices By Connection view, 80 Devices By Type view, 80 disabling driver updates, 71-72 Driver tab, 456 error troubleshooting, 77 Events tab, 456 File menu, 80 General tab. 456 Help menu, 80 installing devices, 66-68 managing devices and printers, 68-69 Power Management tab, 456 Resources By Connection view, 80-81 Resources By Type view, 80 Resources tab, 456 rolling back drivers, 74-76 Show Hidden Devices view, 80 support for older hardware, 81–82 updating device drivers, 70 View menu, 80 viewing device settings, 80-81 **Device Registration** about, 445, 447 enabling, 446 requirements, 445 devices and device drivers. See also specific devices about, 66 adding driver packages, 91–92

automatic installation, 73, 76 clean installations, 29 configuring device registration, 445-447 configuring driver settings, 79-82 configuring removable devices, 225-231 connecting to Microsoft accounts, 426-428 customizing user interface based on device type, 98-114 deploying driver packages, 88-90 determining editions by device type, 15-18 device health attestation feature, 20 disabling driver updates, 71-73, 76-77 downloading driver packages, 87 driver signing, 82-85, 89 driver verification tools, 77-79 from earlier versions of Windows, 3 importing driver packages, 90-91 installing devices, 65-69 inventorving and assessing devices, 4-5 managing device security, 438-441 managing devices, 68-69 managing driver packages, 84-86, 92-93 optimizing drive usage, 224 print class drivers, 241-242 recovering encrypted drives, 270 resolving driver issues, 76-79 rolling back drivers, 74-76 thought experiment, 94-95 two-factor authentication, 20 updating device drivers, 69-71 updating mobile devices, 333 verifying hardware compatibility, 3-4 **Devices And Printers app** about, 68-69, 369, 371 adding and sharing printers, 242 automatic device driver installation setting, 73 managing printers, 369, 371 setting security permissions, 242-243 Devices By Connection view (Device Manager), 80 Devices By Type view (Device Manager), 80 DHCP (Dynamic Host Configuration Protocol), 22, 166 differencing disks, linking to, 218-219 digital entitlement, 138-139 digital signatures about, 82-83 Device Guard, 439 driver packages, 84-85, 89 Windows Store Apps, 289 DirectAccess clients, 178–179 DirectAccess servers, 178 DirectAccess service, 168, 178–179 Disable-ComputerRestore cmdlet, 389 Disable Inheritance button, 262 Disable-LocalUser cmdlet, 425 Disable-NetFirewallRule cmdlet, 187 Disable-PnpDevice cmdlet, 86 Disable-WindowsOptionalFeature cmdlet, 60, 284 discretionary access control list (DACL), 248, 257 Disk Activity Properties dialog box, 367

Disk Cleanup Wizard preparing for upgrades, 42 regular maintenance with, 380 removing device driver packages, 92 removing restore points, 398-399 Disk Management snap-in (diskmgmt.msc) attaching VHDs, 53 creating MBR-partitioned VHDs, 55-56 creating native boot VHDs, 52-53 creating VHDs, 213-215 expanding volumes, 42 failed disks and, 234 importing foreign disks, 232 initializing basic disks, 232 shrinking partitions, 46 tasks supported, 207–208 viewing configuration information, 43-44 DiskPart tool, 53, 58, 210-212 DISM (Deployment Image Servicing and Management) about, 22 adding driver packages, 91–92 applying Windows 10 image, 56 configuring Windows features, 283-284 enterprise recovery options, 392 managing driver packages, 92–93 modifying Windows features, 60 sideloading apps, 289 display resolution, minimum requirements, 2 djoin.exe (offline domain join), 444 DLL (dynamic link library) files, 85 DNS (Domain Name System) about, 162 configuring settings, 171-173 Device Registration requirement, 445 name resolution, 170–171 Task Manager view, 358 DNS Manager, 149–150 DNS resolver cache, 171, 196–197 Document Properties dialog box, 157 document version control, 231 domain controllers (Active Directory component), 149, 436-437 Domain Name System (DNS) about, 162 configuring settings, 171-173 Device Registration requirement, 445 name resolution, 170–171 Task Manager view, 358 domain networks, 180, 183 domain trees (Active Directory component), 149 domains (Active Directory component), 149, 443-444 Drive Selection dialog box, 92 Driver Package Rollback dialog box, 74 driver packages adding, 91-92 deploying, 88-90 downloading, 87 importing, 90-91 managing, 84-86, 92-93

driver store

driver store, 84–85 Driver Verifier Manager (verifier.exe), 78–79 DVD installation, 22, 28 dynamic access control (DAC), 269 dynamic disks, 203, 210, 232 Dynamic Host Configuration Protocol (DHCP), 22, 166 dynamic link library (DLL) files, 85

E

EAP (Extensible Authentication Protocol), 176-177 Ease of Access settings, 115–116 Easy Connect, 304–305 Edb.chk file, 151 Edb.log file, 151 editions. See Windows 10 editions EFS (Encrypting File System), 226 802.11x wireless standards, 190 Electronic Software Download (ESD) file format, 33 Enable-ComputerRestore cmdlet, 389 Enable-LocalUser cmdlet, 425 Enable-NetFirewallRule cmdlet, 187 Enable-PnpDevice cmdlet, 86 Enable-PSRemoting cmdlet, 312 Enable-WindowsOptionalFeature cmdlet, 60, 127, 283 Encrypting File System (EFS), 226 Enter A Product Key dialog box, 143 Enter-PSSession cmdlet, 315 enterprise environment CB and CBB update servicing options, 331-334 configuring Active Directory, 148-154 configuring Group Policy, 154-158 configuring UAC, 144-147 configuring Windows Update options, 319-327 feature upgrades, 320 File History feature, 410-411 implementing activation, 137-144 implementing continuous service, 333 implementing Insider Preview, 327-331 LTSB scenarios, 334-335 managing update history, 335-338 provisioning with Windows ICD, 135-137 recovery options, 392 rolling back updates, 339-344 thought experiment, 158-159 updating Windows Store Apps, 344-347 upgrade build branches, 328, 331 Windows Hello and, 432 Enterprise Mode (Microsoft Edge), 122 Enterprise Mode Site List Manager tool, 122 ESD (Electronic Software Download) file format, 33 Evaluate stage (enterprise servicing), 333 event collector computer, 354 Event ID, 352 event logs about, 350-352 accessing remotely, 355-356

creating subscriptions, 354-355 custom views, 352 viewing subscriptions, 353-354 event source computer, 354 event subscriptions, 354 about, 353 accessing event logs remotely, 355-356 creating, 354-355 viewing, 353-354 Event Viewer (eventvwr.msc) about, 196, 452 accessing event logs remotely, 355-356 configuring and analyzing logs, 350–352 creating custom views, 352 viewing subscriptions, 353-355 Excel, MAP assessment report in, 5-6 .exe installer file, 275 Execute File permission, 259 exFAT file system, 203, 206, 226-227 Exit-PSSession cmdlet, 315 Explicit Allow permission, 260 Explicit Deny permission, 260 Export-StartLayout cmdlet, 104, 133 exporting provisioning packages, 294 Extend command (DiskPart), 210 Extensible Authentication Protocol (EAP), 176-177

F

Fast Startup feature, 280-281 FAT file system about, 206 configuring volumes, 203 logical failures, 233 removable devices, 226 Fat16 file system, 227 FAT32 file system about, 206 configuring volumes, 203 removable devices, 58, 226-227 fault tolerance mirrored volumes, 203 striped volumes, 204 Feature-On-Demand (FOD) files, 88 feature upgrades, 320 FhManagew.exe tool, 408 Fibre Channel protocol, 219 file and folder management. See also system and data recovery about, 237-238 configuring file system permissions, 254-263 configuring folder shares, 246-250 configuring public folders, 250-251 fetching files with OneDrive, 253-254 folder redirection, 156-157 HomeGroups access, 245 managing files and folders, 255-256

network discovery, 239 NTFS inheritance, 262-263 recovering files from OneDrive, 264-265, 413-416 restoring previous versions, 411-413 Server Message Block, 238–239 setting file and folder permissions, 256-261 shared network folder installation, 23, 28 sharing files, 237-240 sharing files with OneDrive, 263-264 troubleshooting share and NTFS permissions, 268-269 **File Explorer** creating HomeGroups, 244 managing files and folders, 255-256 NTFS inheritance, 262-263 OneDrive folder, 252, 414 Previous Version feature, 411-413 recovering deleted files, 264-265 setting file and folder permissions, 256-261 sharing files, 239-240 sharing folders, 248 File History feature about, 406 backup location, 409 configuring, 406-408 enterprise considerations, 410-411 Previous Versions feature and, 411-413 recovering files, 408-409 File menu (Device Manager), 80 File Sharing Wizard, 239–240 File Signature Verification (Sigverif.exe) tool, 77–78 file systems. See specific file systems Films & TV app, 37 Find-Module cmdlet, 425 firmware Credential Guard and, 437 Device Guard and, 439 failures, 233 upgrades, 28 fixed provisioning, 221 Flight Mode tile, 110 folder redirection, 156-157 folder shares about, 246 creating, 247-249 multiple, 250 permissions, 250 public, 250-251 shared network folder installation, 23, 28 forests (Active Directory component), 149, 179, 437 Format command (DiskPart), 210 Format-Volume cmdlet, 209 Forwarded Events log, 351 FQDN (fully qualified domain name), 170–171, 175 Full Control permission, 256, 258-259 Full permission, 250 fully qualified domain name (FQDN), 170-171, 175

G

Get-Acl cmdlet, 260 Get-Command cmdlet, 372 Get-ComputerRestorePoint cmdlet, 389 Get-Disk cmdlet, 209, 215 Get-DnsClientCache cmdlet, 197 Get-EventLog cmdlet, 315 Get Going Fast page, 29-30, 37 Get-Help cmdlet, 86 Get-LocalUser cmdlet, 425 Get-NetFirewallRule cmdlet, 187 Get-NetIPAddress cmdlet, 167, 170 Get-NetIPConfiguration cmdlet, 311 Get-NetIPv4Protocol cmdlet, 167 Get-NetIPv6Protocol cmdlet, 170 Get-Partition cmdlet, 209 Get-PnpDevice cmdlet, 86 Get-PnpDeviceProperty cmdlet, 86 Get-PrintConfiguration cmdlet, 371 Get-Printer cmdlet, 371 Get-PrinterDriver cmdlet, 371 Get-PrinterPort cmdlet, 371 Get-Service cmdlet, 453, 462 Get-SmbConnection cmdlet, 238 Get-SmbShare cmdlet, 249-250 Get-SmbShareAccess cmdlet, 249 Get-StoragePool cmdlet, 225 Get-VHDSet cmdlet, 216 Get-VirtualDisk cmdlet, 225 Get-Volume cmdlet, 44, 209, 216 Get Windows 10 dialog box, 32 Get Windows 10 (GWX) notification utility about, 3 blocking upgrading, 39-41 downloading, 31-32 Get-WindowsOptionalFeature cmdlet, 60 Get-WmiObject cmdlet, 420 GetPrinterProperty cmdlet, 371 Getting Ready notification, 29 Getting Things Ready dialog box, 342 global catalog servers, 149 global scope (IPv6 addressing), 168 gpedit.msc (Group Policy editor), 39-40, 229, 265 GPMC (Group Policy Management Console), 154–155, 157 GPOs (Group Policy Objects) blocking access to OneDrive, 265-266 blocking upgrading to Windows 10, 39-41 blocking Windows Store Apps, 288 configuring, 154-158 configuring DirectAccess, 178-179 configuring Fast Startup, 281 configuring firewall settings, 300 configuring Microsoft Passport settings, 434 configuring Remote Assistance, 306–307 configuring Remote Desktop, 310

configuring Start, 104-106 configuring UAC, 146-147 configuring Windows Update, 324–327 disabling File History, 411 disabling notifications, 113 disabling UACs, 430 distributing fixes, 9 installing desktop apps, 274, 276 Internet Explorer settings, 125 network discovery settings, 239 removing apps deployed, 279 securing removable devices, 228-231 Windows Store settings, 346–347 GPT (GUID Partition Table), 55, 202–203 Gpupdate.exe command, 105, 288 Grant-SmbShareAccess cmdlet, 249 graphics cards driver packages, 87 minimum requirements, 2 Groove Music app, 37 Group Policy editor (gpedit.msc), 39-40, 229, 265 Group Policy Management Console (GPMC), 154-155, 157 Group Policy Management Editor, 156–157 Group Policy Objects (GPOs) blocking access to OneDrive, 265-266 blocking upgrading to Windows 10, 39-41 blocking Windows Store Apps, 288 configuring, 154–158 configuring DirectAccess, 178-179 configuring Fast Startup, 281 configuring firewall settings, 300 configuring Microsoft Passport settings, 434 configuring Remote Assistance, 306-307 configuring Remote Desktop, 310 configuring Start, 104-106 configuring UAC, 146-147 configuring Windows Update, 324-327 disabling File History, 411 disabling notifications, 113 disabling UACs, 430 distributing fixes, 9 installing desktop apps, 274, 276 Internet Explorer settings, 125 network discovery settings, 239 removing apps deployed, 279 securing removable devices, 228-231 Windows Store settings, 346-347 Guest account, 420 guest networks, 180 GUID Partition Table (GPT), 55, 202-203 GWX (Get Windows 10) notification utility about, 3 blocking upgrading, 39-41 downloading, 31-32

Η

hard disks configuring, 202-203 disk management tools, 207–211 failures, 232-234, 410 importing foreign, 232 initializing, 232 managing disk space, 397 minimum space requirements, 2, 41-42 monitoring software, 233 performance counters, 381 replacing failed, 234-235 specifying unit measurement, 397 turning off system protection, 399 hardware compatibility analyzing report, 5-6 inventorying and assessing devices, 4-5 support for older hardware, 81-82 troubleshooting, 42 verifying for multiple devices, 3-4 hardware requirements. See also specific devices Hyper-V prerequisites, 126 identifying for Windows 10, 2, 31, 41-42 Help menu (Device Manager), 80 hibernation mode, 54 High Contrast setting (Ease of Access), 115–116 High Performance power plan, 132 high-touch deployment, 21 HKEY_CURRENT_USER registry subtree, 14, 282 HKEY_LOCAL_MACHINE registry subtree, 282 HomeGroups about, 243 configuring settings, 441 connecting to, 173-174 creating, 243-245 joining, 245–246 troubleshooting, 245, 268 host ID, 162-163 host names, 170-171 How Will This Person Sign In dialog box, 424 Hyper-V about, 211 installing Client Hyper-V role, 126–127 managing virtual machines, 127-129 New-VHD cmdlet and, 218 verifying prerequisites, 126 Virtual Secure Mode, 20 Hyper-V Manager, 128, 213

IANA (Internet Assigned Numbers Authority), 165 ICACLS utility, 260–261, 268–269 ICD (Imaging And Configuration Designer) tool about, 22 creating provisioning packages, 291–293 deploying driver packages, 88–91 exporting provisioning packages, 294 preparing installation media, 135-137 recovery options, 392 IKEv2 (Internet Key Exchange version 2), 176 image-based installation, 22 Imaging And Configuration Designer (ICD) tool about, 22 creating provisioning packages, 291–293 deploying driver packages, 88–91 exporting provisioning packages, 294 preparing installation media, 135-137 recovery options, 392 importing driver packages, 90-91 in-place upgrades, 10–12 inbound rules (Windows Firewall With Advanced Security), 186 Indexing Options dialog box, 374-375 indexing process, 374-375 .inf (information) files, 84-85, 88 infrastructure mode (wireless networking), 190 Inherited Allow permission, 260 Inherited Deny permission, 260 Initialize-Disk cmdlet, 209, 215 Initialize Disk dialog box, 214 Insider Preview Program, 327–331, 341 Install-Module cmdlet, 425 installation media preparing, 21-24, 27 preparing with ICD, 135-137 upgrading using, 41-43 installation requirements and preparation choosing upgrades or clean installations, 9-15 determining editions by device type, 15–18 determining hardware requirements and compatibility, 3-9 determining requirements for particular features, 18-20 identifying strategy, 21 preparing installation media, 21–24 thought experiment, 24-25 installing desktop apps automatically, 275-278 interactively, 274–275 installing Windows 10 additional resources, 42 on bootable USB, 57-58 booting from VHD, 55-57 configuring additional regional and language support, 60-62 configuring native boot scenarios, 43-47 installing additional features, 59-60 migrating from previous versions, 47–51 performing clean installations, 27–30, 42 thought experiment, 63-64 upgrading using installation media, 41-43

upgrading using Windows Update, 30-41 to virtual hard disks, 52-54 Install.wim installation image, 22 Internet Assigned Numbers Authority (IANA), 165 Internet Explorer, 119, 122–125 Internet Explorer SmartScreen Filter, 375 Internet Kev Exchange version 2 (IKEv2), 176 Internet of Things Core (IoT Core), 82 Internet Options dialog box Advanced tab, 125 Connections tab, 125 Content tab. 125 General tab, 124 opening, 123-124 Privacy tab, 124-125 Programs tab, 125 Security tab, 124 Internet Protocol version 4 (IPv4) about, 162 configuring DNS settings, 171-173 configuring IPv4 connection, 165–168 public and private addressing, 164–165 subnets, 162–164 Internet Protocol Version 4 (TCP/IPv4) Properties dialog box Advanced button, 172 Alternative Configuration tab, 166 General tab. 165 Internet Protocol version 6 (IPv6) about, 168 configuring DNS settings, 171–173 configuring IPv6 connection, 169-170 IPv6 addressing, 168-169 Internet Protocol Version 6 (TCP/IPv6) Properties dialog box, 169-170, 172 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), 178 Inventory And Assessment Wizard All Computers Credentials page, 5 Credentials Order page, 5 Discovery Methods page, 4 Inventory Scenarios page, 4 Windows Networking Protocols page, 4 Invoke-Command cmdlet, 314–315 IoT Core (Internet of Things Core), 82 IPConfig tool, 194, 196–197 IPsec, configuring, 187–188 IPv4 networking protocol about, 162 configuring DNS settings, 171-173 configuring IPv4 connection, 165–168 public and private addressing, 164–165 subnets, 162–164 tunneling communications, 178–179 IPv6 networking protocol about, 168 configuring DNS settings, 171-173 configuring IPv6 connection, 169–170 IPv6 addressing, 168–169

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), 178 ISCSI protocol, 219 Isolation rules (IPsec), 187

J

Join A HomeGroup Wizard, 245–246 Jump lists element (Start), 106

K

Kerberos tickets, 436 Key Management Service (KMS), 138, 140–141 Keyboard setting (Ease of Access), 115–116 KMS (Key Management Service), 138, 140–141

L

L2TP/IPsec (Layer Two Tunneling Protocol with IPsec), 176 landscape mode, 109 language support, configuring, 60–62 Laplink software reseller, 48 Layer Two Tunneling Protocol with IPsec (L2TP/IPsec), 176 Let Windows Manage My Default Printer setting, 372-373 Let's Create Your Account dialog box, 425 licensing, volume, 139 line-of-business (LOB) apps, 290, 334 Link Layer Topology Discovery (LLTD), 239 link-local (IPv6 addressing), 168-169, 171 linking to differencing disks, 218-219 List Folder Contents permission, 259 List Folder permission, 259 lite-touch installation (LTI), 276 LLTD (Link Layer Topology Discovery), 239 Load-State component (USMT), 15, 50-51 LOB (line-of-business) apps, 290, 334 Local Security Authority process, 437 local user accounts, 420-425, 451 Location tile, 110 Lock screen setting (Desktop), 106-107 LockDown feature (VPNs), 177 locking taskbar, 112-113 log files, 350-352 logical unit number (LUN), 219 Long-Term Servicing Branch (LTSB), 320, 334-335 low-touch deployment, 21 Lpksetup command, 61-62 LTI (lite-touch installation), 276

LTSB (Long-Term Servicing Branch), 320, 334–335 LUN (logical unit number), 219

Μ

Magnifier setting (Ease of Access), 115-116 MAK (Multiple Activation Key), 140, 142 malware about, 375-377 monitoring for, 377-378 removable devices and, 230-231 Manage Documents Allow permission, 242 Manage Storage Spaces console, 222, 224 management tools. See specific tools MAP (Microsoft Assessment And Planning) Toolkit analyzing reports, 5-6 downloading, 4 inventorying and assessing devices, 4-5 verifying hardware compatibility, 3-4 MAPS (Microsoft Active Protection Service), 378 master boot record (MBR), 55-56, 202-203 master file table (MFT), 233 MBAM (Microsoft BitLocker Administration And Monitoring) tool, 270 MBR (master boot record), 55-56, 202-203 MCT (Media Creation Tool), 41, 57-58 MDM (Multiple Device Management) Device Health Attestation, 440 Microsoft Passport, 434 provisioning packages, 291 Windows Hello, 432 mdsched.exe (Memory Diagnostic tool), 382 MDT (Microsoft Deployment Toolkit) image-based installation, 21-22, 392 installing desktop apps, 274 zero-touch installation, 276-277 mean time between failures (MTBF), 232 Media Creation Tool (MCT), 41, 57-58 Memory Diagnostic tool (mdsched.exe), 382 memory management 64-bit version, 17 Hyper-V prerequisites, 126 performance counters, 381 Windows 10 minimum requirements, 2, 41 metered connections, preventing driver updates over, 70-71 MFT (master file table), 233 Microsoft accounts about, 425 connecting to devices, 426-428 setting up, 428 signing up for, 426 Microsoft Active Protection Service (MAPS), 378 Microsoft Application Compatibility Toolkit (ACT), 7-9 Microsoft Azure, 212, 425 Microsoft BitLocker Administration And Monitoring (MBAM) tool, 270

Microsoft CHAP Version 2 (MS-CHAP v2), 177 Microsoft Deployment Toolkit (MDT) image-based installation, 21-22, 392 installing desktop apps, 274 zero-touch installation, 276-277 Microsoft Desktop Optimization Pack, 48 Microsoft Developer Network (MSDN), 28, 82–83 Microsoft Edge, 37, 118-122 Microsoft Excel, MAP assessment report in, 5-6 Microsoft Internet Explorer, 119, 122-125 Microsoft Intune deploying apps, 278 deploving driver packages, 88 distributing VPN profiles, 177-178 Microsoft accounts, 425 Microsoft Management Console (MMC) about, 298-299 configuring, 457 customizina, 458-459 disk management, 207-208 downloading, 155 managing remote computers, 312-314 Taskpad views, 458-459 Microsoft Office 365, 251, 253, 425 Microsoft Office Online, 253 Microsoft Passport, 433-434 Microsoft System Center Configuration Manager, 21–22 Microsoft TechCenter website, 80 Microsoft User Experience Virtualization (UE-V), 48-49 Microsoft volume licensing, 139 Microsoft Volume Licensing Service (MVLS), 28 MigApp.xml file, 49-51 MigDocs.xml file, 49, 51 migration strategies considerations for, 12–13 methods for, 10 migrating user data and settings, 14–15 from previous versions of Windows, 47-51 side-by-side migration, 10, 13 wipe-and-load migration, 10, 12-15, 27-30, 42 MigUser.xml file, 49, 51 Miracast feature, 19, 66 mirrored spaces, 220, 223 mirrored volumes, 203-204, 234 MMC (Microsoft Management Console) about, 298-299 adding or removing snap-ins, 457 configuring, 457 customizing, 458-459 disk management, 207-208 downloading, 155 managing remote computers, 312-314 Taskpad Views, 458-459 Modify permission, 258-259 monitoring hard disks, 233 Monitoring node, 185 monitoring Windows about, 349 Data Collector Sets, 363-367

event subscriptions, 353-356 Event Viewer logs, 350-352 indexing options, 374-375 Performance Monitor, 363–367 printers, 369-373 Reliability Monitor, 379-380 Resource Monitor, 361–363 system resources, 367-369 Task Manager, 356–361 thought experiment, 383-384 troubleshooting performance issues, 380-382 Windows Defender, 375-378 Most Used element (Start), 106 Mouse setting (Ease of Access), 115-116 MS-CHAP v2 (Microsoft CHAP Version 2), 177 Msconfig.exe (System Configuration tool), 453–454 MSDN (Microsoft Developer Network), 28, 82-83 .msi installer file, 275 Msiexec.exe command, 275 Msinfo32 (System Information tool), 204-205 Msra.exe (Remote Assistance) about, 298 allowing through Windows Firewall, 299-300 configuring with GPOs, 306-307 enabling, 301-302 managing computers remotely, 307 offering help with, 305-306 requesting help using, 303-305 Windows Firewall and, 314 Mstsc.exe (Remote Desktop Connection app) Advanced tab, 309 Display tab, 308 Experience tab, 308 General tab, 308 Local Resources tab, 308 opening, 307, 309 MTBF (mean time between failures), 232–234 multiboot configuration implementing, 45-47 from VHDs, 55-57 multicast addresses, 168, 171 Multiple Activation Key (MAK), 140, 142 multiple desktops, 108–109 Multiple Device Management (MDM) Device Health Attestation, 440 Microsoft Passport, 434 provisioning packages, 291 Windows Hello, 432 MVLS (Microsoft Volume Licensing Service), 28

Ν

name resolution about, 170–171 configuring DNS settings, 171–173 DirectAccess requirements, 179 troubleshooting, 196–198 Narrator setting (Ease of Access), 115–116 NAT (network address translation), 165 native boot scenarios about, 43 configuring boot options, 56-57 multiboot Windows, 45-47 spanned volumes and, 204 USB drives, 210-211 viewing configuration information, 43-45 virtual hard disks, 52-54 near-field communication (NFC), 66 Net share command, 248-249 Net start command, 452 Net stop command, 452 Net user command, 420 Net view command, 250 NetBIOS names, 171 Netsh.exe tool configuring DNS settings, 172 configuring IPv4 settings, 167 configuring IPv6 settings, 169 configuring Windows Firewall, 184 managing wireless network settings, 194-195 network address translation (NAT), 165 Network And Internet Settings app. 244 Network And Sharing Center accessing network troubleshooting tools, 196 configuring DNS settings, 172 configuring file and printer sharing, 237 configuring IPv4 settings, 166-167 configuring IPv6 settings, 169–170 configuring network discovery, 188-189 configuring public folders, 251 configuring VPN connections, 174–176 configuring Windows Firewall settings, 183 configuring wireless networks, 193 creating HomeGroups, 173-174, 245-246 joining HomeGroups, 245-246 viewing assigned network location profiles, 179–180 network discoverv configuring, 188-189 file and printer sharing, 239 network ID, 162-164 network location profiles about, 179–180 changing, 181-182 HomeGroups and, 174 Windows Firewall settings, 183 Windows Remote Management and, 312 Network Location Server (NLS), 178 networking configuring IPsec, 187–188 configuring IPv4 network settings, 161-168 configuring IPv6 network settings, 168-170 configuring name resolution, 170–173 configuring network discovery, 188-189 configuring network locations, 179–182 configuring Wi-Fi Direct, 194-195 configuring Windows Firewall, 183–185

configuring Windows Firewall With Advanced Security, 185-187 configuring wireless network settings, 189–194 connecting to networks, 173-179 shared network folder installation, 23, 28 thought experiment, 198-199 troubleshooting issues, 195–198 New-LocalUser cmdlet, 425 New-NetFirewallRule cmdlet, 185, 187 New-Partition cmdlet, 209 New Project Wizard, 292-293 New-PSWorkflowSession cmdlet, 315 New-SmbShare cmdlet, 249 New-StoragePool cmdlet, 225 New Taskpad View Wizard, 458 New User dialog box, 421 New-VHD cmdlet, 215-218 New Virtual Machine Wizard, 128 New-VirtualDisk cmdlet, 225 NFC (near-field communication), 66 NLS (Network Location Server), 178 Note tile, 110 notifications Action Center, 111–112 Windows Firewall, 183 NSLookup tool, 196–197 Ntds.nit file, 151 NTFS file system about, 205-206 Backup And Restore support, 402 file and folder permissions, 256–261 inheritance considerations, 262-263 removable devices, 226-227 shared folders and, 246, 250 simple volumes and, 203 Storage Spaces support, 219, 222 System Restore feature, 389 troubleshooting permissions, 268-269 UEFI and, 58

0

OEM scenario (activation), 139 offline domain join (djoin.exe), 444 OneDrive For Business service, 251 OneDrive service about, 19, 251, 263 blocking access to, 265–266 configuring volumes, 203 desktop app, 252–254, 263–264 fetching files from PCs, 253–254 File History feature and, 407 Previous Versions feature and, 415–416 recovering files from, 264–265, 413–415 sharing files with, 263–264 synchronization and, 264–266, 270 web portal, 252–253, 263–264 OOBE (out-of-box-experience), 37, 392 operating systems backing up, 34 checking versions, 343-344 Device Registration requirement, 445 Hyper-V prerequisites, 126 migrating components, 50 in multiboot configuration, 45-47 OneDrive support, 252 reverting to previous, 39 volume considerations, 203 operations masters (Active Directory component), 149 Optimize-StoragePool cmdlet, 225, 235 Optimize-VHD cmdlet, 216 Optimize-VHDSet cmdlet, 216 optimizing drive usage, 224 OptionalFeatures.exe (Windows Features app), 58-59 Options dialog box, 458 organizational units (OUs), 148-149 Other Options setting (Ease of Access), 115–116 OUs (organizational units), 148-149 out-of-box-experience (OOBE), 37, 392 outbound rules (Windows Firewall With Advanced Security), 186

Ρ

page-description language (PDL), 241 parity spaces, 220, 223 partitions GPT, 55, 202 MBR, 55-56, 202 shrinking, 46, 209 passive styluses, 19 passwords accessing shared resources, 174 administrative user accounts, 29 HomeGroups, 243-244 picture, 434-435 PINs and, 427–428 System Restore feature, 390 two-factor authentication, 20 during upgrade process, 36-37 Patch Tuesday updates, 335 Pathping tool, 196 PCL (Printer Control Language), 241 PCmover Express, 48-49 PDF (Portable Document Format), 241 PDL (page-description language), 241 Perfect Forward Secrecy (PFS) encryption, 253 performance 64-bit version, 17 monitoring system resources, 367-369 monitoring with Performance Monitor, 363-367 monitoring with Task Manager, 356–361 optimizing drive usage, 224 with Resource Monitor, 361-362

simple volumes, 203 striped volumes, 204 troubleshooting issues, 362, 380-382 virtual hard disks, 212 performance counters, 365–369, 381 Performance Monitor (perfmon) about, 363 monitoring system resources, 368-369 running data collector, 363-364 using, 365-367 performance object instances, 365–367 performance objects, 365-367 permissions configuring for file systems, 254-263 configuring for folder shares, 246, 250 configuring for public folders, 251 installing desktop apps, 275 OneDrive service, 263-264 setting for files and folders, 240, 256-261 setting for printer security, 242-243 troubleshooting, 266-269 WBAdmin tool, 403 PFS (Perfect Forward Secrecy) encryption, 253 Photos app, 37 picture passwords, 434–435 PID (Process ID), 360 Pilot stage (enterprise servicing), 333 PIN gestures, 433 Ping tool, 196–197 PINs, 427-428, 433-434 PKI (public key infrastructure), 179, 439, 445 Plug And Play standard, 80-82, 91, 241 PnPUtil.exe tool, 72, 85-86 Point-to-Point Tunneling Protocol (PPTP), 176 port rules (Windows Firewall With Advanced Security), 186-187 Portable Document Format (PDF), 241 Portable Workspace, 43 portrait mode, 109 post-installation configuration accessibility options, 115-116 Cortana feature, 116-118 Hyper-V, 126-129 Internet Explorer, 122–125 Microsoft Edge, 118–122 power settings, 130-133 thought experiment, 133-134 user interface, 97-114 PostScript, 241 Power element (Start), 106 Power Saver power plan, 132 power settings configuring basic options, 130–131 configuring power plans, 132 Fast Startup, 280–281 PowerShell ISE, 216-217, 463 PowerShell (Windows). See also specific cmdlets about, 196, 298 Active Directory module, 148, 150, 152

ADAC support, 154 automating management tasks, 461-463 configuring DNS client settings, 172 configuring IPv4 settings, 167–168 configuring IPv6 settings, 170 configuring remoting, 310-312 configuring System Restore, 388-389 configuring Windows features, 283-284 configuring Windows Firewall, 184–185 configuring Windows Firewall With Advanced Security, 187 creating VHDs, 215–218 disk management tasks, 208–210 exporting Start layout, 104, 133 installing Hyper-V feature, 127 listing local user accounts, 420 managing driver packages, 86 managing file and folder permissions, 260 managing printers, 371–372 managing remote computers, 310-312, 314-315 managing services, 453 managing Storage Spaces, 224-225 managing user accounts, 425 RSAT support, 155 running DISM within, 60 running scripts, 462-463 sharing folders, 249 sideloading apps, 289 troubleshooting name resolution, 196–197 viewing configuration information, 44 viewing SMB version, 238 .ppkg files, 88-89 PPTP (Point-to-Point Tunneling Protocol), 176 Pre-Boot Execution Environment (PXE), 22 predefined rules (Windows Firewall With Advanced Security), 186 preparing for installation. See installation requirements and preparation Previous Versions feature about, 269 OneDrive service and, 415-416 restoring previous versions of files and folders, 411-413 print job output, 241 print jobs, 241 Print Management tool (Printmanagement.msc), 241, 370-371 Print Spooler service, 243 Printer Control Language (PCL), 241 printer drivers, 241 printer management about, 68-69 adding printers, 242 default printer behavior, 372-373 driver rollbacks, 74 monitoring and managing printers, 369-373 network discovery, 239 restarting printer spooler, 243

Server Message Block, 238–239

setting security permissions, 242–243 sharing printers, 237-238, 241-243 printer ports, 241 Printers & Scanners screen, 369, 372–373 printing devices, 241 private IPv4 addressing, 164-165 private networks, 180-181, 183 Process ID (PID), 360 processors Hyper-V prerequisites, 126 performance counters, 381 Windows 10 minimum requirements, 2 product keys, 138-139, 142-143 program rules (Windows Firewall With Advanced Security), 186 **Programs And Features** configuring Windows features, 283 uninstalling desktop apps, 278–279 uninstalling Windows Updates, 339-340 Project tile, 110 Promote This Server To A Domain Controller Wizard, 150 Properties dialog box device drivers, 74 devices, 66-67, 80-81 services, 450-451 provisioning packages about, 291 applying, 294-295 creating, 291-294 public folders, configuring, 250–251 public IPv4 addressing, 164–165 public key infrastructure (PKI), 179, 439, 445 public networks, 180-181, 183, 312 published apps, 156, 276 PXE (Pre-Boot Execution Environment), 22

Q

QoS (quality of service), 239 quality of service (QoS), 239 Quick Access (File Explorer), 255–256 Quick Action tiles, 109–111 Quiet Hours tile, 110

R

RAID-0 volumes, 204 RAID-1 volumes, 203 RAID-5 volumes, 204 ransomware, 376 RAW file system, 226 RDP (Remote Desktop Protocol), 298 Read Attributes permission, 259 Read Data permission, 259 Read & Execute permission, 258–259 Read Extended Attributes permission, 259 read-only domain controllers (RODC), 149 Read permission, 240, 250, 258-259 Read Permissions permission, 259 Reception Printer Properties dialog box, 242-243 Recima.exe utility, 393 Recovery Drive dialog box, 386–387 recovery drives, configuring, 386-387 Recycle Bin, 264-265, 414 recycling computers, 390-393 redundancy, mirrored volumes, 203, 234 refresh or recycle feature, 390-393 ReFS (Resilient File System) file system about, 201-202, 205-207 file and folder permissions, 256–258 inheritance considerations, 262 simple volume support, 203 Storage Spaces support, 219–220, 222–223 troubleshooting data recovery, 270 Regedit.exe (Registry editor) blocking upgrading to Windows 10, 39-41 configuring UAC, 147 HKEY_CURRENT_USER registry subtree, 14 viewing app startup information, 282 regional support, configuring, 60-62 Reliability Monitor, 379–380 Remote Assistance (Msra.exe) about, 298 allowing through Windows Firewall, 299-300 configuring with GPOs, 306-307 enabling, 301-302 managing computers remotely, 307 offering help with, 305-306 requesting help using, 303-305 Windows Firewall and, 314 Remote Desktop about, 298-299 configuring with GPOs, 310 creating and editing connections, 307-309 enabling, 302 Windows Firewall and, 314 Remote Desktop Connection app (Mstsc.exe) Advanced tab, 309 Display tab, 308 Experience tab, 308 General tab, 308 Local Resources tab, 308 opening, 307, 309 Remote Desktop Protocol (RDP), 298 Remote Event Log Management, 314 Remote Event Monitor, 314 remote management about, 297 configuring PowerShell remoting, 310-312 configuring Remote Assistance, 303-307 configuring Remote Desktop, 307-310 configuring settings, 299-302 modifying settings, 312-315

tools supported, 298–299 viewing events, 356 remote printers, 371 Remote Scheduled Tasks Management, 314 Remote Server Administration Tools (RSAT), 155 Remote Service Management, 314 Remote Shut-down, 314 Remote Volume Management, 314 removable devices. See also specific types of removable devices about, 225 formatting, 226 restricting access to, 228-231 securing, 226-228 troubleshooting, 231-235 Remove-LocalUser cmdlet, 425 Remove-PhysicalDisk cmdlet, 225 Remove-Printer cmdlet, 372 Remove-PrinterDriver cmdlet, 372 Remove-PrintJob cmdlet, 372 Remove-SmbShare cmdlet, 249 Remove-StoragePool cmdlet, 225 Rename-LocalUser cmdlet, 425 Rename-Printer cmdlet, 372 Repair-VirtualDisk cmdlet, 225 report management analyzing MAP assessment reports, 5-6 Device Manager error reports, 77 System Performance Report, 364 Request Control task (Remote Assistance), 307 Res1.loa file, 151 Res2.log file, 151 reset feature, 392 Resilient File System (ReFS) file system about, 201-202, 205-207 simple volume support, 203 Storage Spaces support, 219–220, 222–223 Resize-Partition cmdlet, 209 resizing tiles, 102 Resmon.exe (Resource Monitor), 361-363 Resolve-DnsName cmdlet, 197 resolver cache, 171, 196-197 Resource Monitor (Resmon.exe), 361–363 Resources By Connection view (Device Manager), 80-81 Resources By Type view (Device Manager), 80 Restart-PrintJob cmdlet, 372 Restart-Service cmdlet, 453 restarts during upgrades, 36 Restore Files dialog box, 402 restore points about, 396 changing settings, 396-397 creating, 388, 398-399, 402 deleting, 398-399 managing disk space, 397 Previous Versions feature and, 411–413 restoring to previous, 388-389 Resume-PrintJob cmdlet, 372 Retail scenario (activation), 139

reverting to previous versions, 38–39 roaming profiles, 15 RODC (read-only domain controllers), 149 rolling back device drivers, 74–76 rolling back updates about, 339 reverting to previous builds, 322, 341–344 uninstalling Windows Updates, 322, 339–341 Rotation Lock tile, 109 router discovery, 168 RSAT (Remote Server Administration Tools), 155 rules IPsec, 187–188 Windows Firewall With Advanced Security, 186–187 Run key, 282

S

SACL (system access control list), 257 Safe Mode, 75-76, 398, 453-454 SAS (Serially Attached SCSI) disks, 220 SATA (Serial Advanced Technology Attachment) drives, 29, 220 Save BitLocker Recovery Key As dialog box, 227 Sc query command, 452 Sc start command, 453 Sc stop command, 453 Scan For Hardware Changes Wizard, 68 ScanState component (USMT), 15, 50-51 Scheduled Tasks feature, 388 scheduling upgrades, 34–35 Schtasks.exe tool, 461 scripts creating, 462 running, 156, 462-463 Sdbinst.exe command-line tool, 9 SDHC (Secure Digital High-Capacity) memory cards, 225-226, 386 second-level address translation (SLAT), 17-18 Secure Boot about, 20 Credential Guard, 437 Device Guard, 439 UEFI and, 42 Secure Digital High-Capacity (SDHC) memory cards, 225-226, 386 Secure Socket Tunneling Protocol (SSTP), 176 security considerations. See also authentication and authorization 64-bit version, 17 administrative privilege elevation, 144-147 credential security, 435-438 deferring upgrades, 322 device security, 438-441 driver enforcement, 83 event logs, 350-356 network traffic and, 182-189

OneDrive web portal, 253 printer permissions, 242-243 removable devices, 226-231 security features supported, 20 security templates, 157 troubleshooting data access, 266-268 Windows Defender, 375–378 Security log, 351 security tokens, 437 Select A Drive dialog box, 407 Select Computer dialog box, 356 Select User Or Group dialog box, 258 Serial Advanced Technology Attachment (SATA) drives, 29, 220 Serial ATA (SATA), 220 Serially Attached SCSI (SAS) disks, 220 Server Manager, 150, 155 Server Message Block (SMB), 238-239, 246 server-to-server rules (IPsec), 188 service logs, 351 Service Set Identifier (SSID), 358 services. See also specific services about, 449 command-line tools, 452-453 Event Viewer, 452 managing, 450-453 Services snap-in, 450-451 System Configuration tool, 453-454 servicing updates, 319-320 Set-Acl cmdlet, 260 Set-Disk cmdlet, 209, 216 Set-DNSClientServerAddress cmdlet, 172 Set-ExecutionPolicy cmdlet, 462–463 Set-NetFirewallRule cmdlet, 187 Set-NetIPAddress cmdlet, 167-168, 170 Set-NetIPv4Protocol cmdlet, 167 Set-NetIPv6Protocol cmdlet, 170 Set-Partition cmdlet, 209 Set-PhysicalDisk cmdlet, 225 Set-PrintConfiguration cmdlet, 372 Set-Printer cmdlet, 372 Set-PrinterProperty cmdlet, 372 Set-Service cmdlet, 453 Set-SmbShare cmdlet, 249 Set-StoragePool cmdlet, 225 Set Up A PIN dialog box, 428 Settings app Backup And Restore tool, 400 configuring basic power options, 130 configuring Cortana, 116 configuring default device behavior, 101 configuring PCs for CBB, 332 configuring picture passwords, 434-435 configuring Quick Action tiles, 110 configuring Windows features, 283 configuring Windows Store App settings, 287 configuring Windows Update options, 321-322, 325-327 creating HomeGroups, 244

customizing Desktop, 106 enabling Device Registration, 446 enabling remote management, 301 File History feature, 408 implementing Insider Preview, 329-331 managing user accounts, 421, 423-425 monitoring and managing printers, 369, 372 monitoring for malware, 378 refresh or recycle process, 391 resetting PCs, 322-323 rolling back updates, 339, 341 Setup log, 351 Setupact.log file, 36, 41, 43 Setupapi log file, 36 SetupCleanupTask utility, 39 Setuperr.log file, 42 shadow copies (snapshots), 411 Share With Other Home Computers dialog box, 174 shared folders about, 246 creating, 247-249 multiple, 250 permissions, 250 public, 250-251 shared network folder installation, 23, 28 Shared Folders snap-in, 247-248 shim, 9 Show Hidden Devices view (Device Manager), 80 Show or Hide Updates troubleshooter, 337-338 Show Or Hide Updates troubleshooter package, 76–77 Shrink command (DiskPart), 210 Shrpubw.exe tool, 248 side-by-side migrations, 10, 13 sideloading apps, 289 Sigverif.exe (File Signature Verification) tool, 77–78 silent installation, 275 simple IPv4 subnetting, 163 simple spaces, 220, 223 simple volumes, 203 single sign-on (SSO), 445 site-local (IPv6 addressing), 168–169 sites (Active Directory component), 149 16-bit applications, 17 6to4 protocol, 178 64-bit architecture device drivers, 76 Windows 10 versions, 17 SLAT (second-level address translation), 17-18 sleep mode, 54, 68 Slmgr.vbs command, 143 smart cards, 20 SMART software, 233 SmartScreen Filter (Internet Explorer), 375 SMB (Server Message Block), 238-239, 246 snapshots (shadow copies), 411 solid-state drives (SSDs) disk striping and, 204 hard drive failures and, 233-234

performance issues, 381 SATA drives and, 29 source computer, 354 source computer-initiated subscriptions, 354 spanned volumes, 203-204 Special Permissions permission, 258 spyware, 376 SOL Server databases, 7 SRV resource records, 149-150 SSDs (solid-state drives) disk striping and, 204 hard drive failures and, 233-234 performance issues, 381 SATA drives and, 29 SSID (Service Set Identifier), 358 SSO (single sign-on), 445 SSTP (Secure Socket Tunneling Protocol), 176 Standard User Analyzer, 7 standby mode, 68 Start screen/menu configuring tiles, 102–104 configuring with GPOs, 104-106 convertible devices, 101-102 customizing, 98-100 arouping tiles, 104 uninstalling desktop apps, 103 Start-Service cmdlet, 453 Start setting (Desktop), 107 Start size element (Start), 106 Starting BitLocker Wizard, 227 stateful configuration, 168 stateless configuration, 168 status screen (upgrades), 36 Stop-Service cmdlet, 453 storage management about, 201-202 configuring disks, 202-203 configuring file systems, 204-207 configuring volumes, 203-204 creating and configuring Storage Spaces, 219-225 creating and configuring VHDs, 211-219 disk management tools, 207-211 Hyper-V prerequisites, 126 thought experiment, 235-236 troubleshooting issues, 231-235 Windows Store Apps, 286–287 storage pools, 219-222, 235 Storage Spaces about, 219 configuring, 221-224 creating, 219-220 dynamic disks and, 210 failed disks and, 234-235 managing with Windows PowerShell, 224-225 provisioning schemes, 221 RAID-5 and, 204 storage pools and, 220 troubleshooting data recovery, 270 streaming media, HomeGroups access, 245
striped volumes, 203-204 styluses, 19 subnet ID, 162–164 subnet masks, 162-164 subnets about, 162 complex networks, 163-164 simple networks, 163 subscriptions about. 353-354 accessing event logs remotely, 355-356 creating, 354-355 viewing, 353-354 Suggestions element (Start), 106 Sync Your Settings feature, 19 system access control list (SACL), 257 system and data recovery Backup And Restore tool, 400–403 configuring File History, 406-411 configuring recovery drives, 386-387 configuring restore points, 396-399 configuring System Restore, 387-390 recovering files from OneDrive, 264-265, 413-416 refresh or recycle feature, 390-393 reset feature, 392 restoring previous versions of files and folders, 411-413 rolling back updates, 322, 339-344 thought experiment, 417-418 troubleshooting, 269-270 using Windows Recovery, 393–396 WBAdmin tool, 403-406 System And Security app configuring AD DS domain settings, 443-444 configuring UAC, 146, 430 configuring Windows Firewall to enable remote management, 299 configuring workgroups, 442 launching Windows Backup and Restore, 400 requesting help using Remote Assistance, 303 Windows Backup And Restore, 400 System Center Configuration Manager, 21–22, 274, 392 System Configuration tool (Msconfig.exe), 453–454 System Diagnostics data collector set, 363 System Host, 42 System Information tool (Msinfo32), 204-205 System log, 351-352, 452 System Performance data collector set, 363 System Performance Report, 364 System Properties dialog box configuring AD DS domain settings, 443 configuring System Restore, 387–389 configuring workgroups, 442 enabling Remote Assistance, 301–302 enabling Remote Desktop, 302 System Protection dialog box, 388 System Protection For Local Disk dialog box, 387, 398 system resources about, 367

baseline performance, 368–369 real-time monitoring, 368 System Restore feature, 269–270, 387–390 System settings app, 130–131

T

Tablet mode, 19, 101-102, 109 Tablet Mode tile, 109 Take Ownership permission, 259 Task Manager accessing, 356-357 App History tab, 357, 359 Details tab, 357, 360 Performance tab, 357–359, 361–362 Processes tab, 357-358 Services tab, 357, 360-361 Startup tab, 281–282, 357, 359–360 Users tab, 357, 360 Task Scheduler, 388, 401, 459-461 taskbar, configuring, 112-114 Taskpad Views (MMC), 458-459 TCP ports (remote management), 312, 356 Temp.edb file, 151 Teredo protocol, 178 Test-Connection cmdlet, 197 testing in multiboot configuration, 45 Themes setting (Desktop), 107 thin provisioning, 221 32-bit architecture device drivers, 76 Windows 10 versions, 17 Touch feature, 19 TPM (Trusted Platform Module) BitLocker and, 20, 227 Credential Guard and, 437 Device Guard and, 439 Device Health Attestation, 440 Tracert tool, 196 traffic filters (VPNs), 177 Traverse Folder permission, 259 Trojan horses, 376 troubleshooting compatibility issues, 42 data access, 266-268 data recovery, 269-270 device driver issues, 76-79 dynamic access control, 269 HomeGroups, 245, 268 name resolution, 196-198 network issues, 195–196 performance issues, 362, 380-382 Show or Hide Updates troubleshooter, 337-338 Volume Shadow Copy Service, 413 Windows Update, 327 Trusted Platform Module (TPM) BitLocker and, 20, 227

Credential Guard and, 437 Device Guard and, 439 Device Health Attestation, 440 trustlets, 20 tunnel rules (IPsec), 188 Turn Windows Features On Or Off dialog box, 283 two-factor authentication, 20, 433 Type 4 Print Class Driver, 241

U

UAC dialog box, 217 UAC (User Account Control) about, 431 configuring, 144-147, 429-431 ICD tool and, 88 installing desktop apps, 275 UE-V (User Experience Virtualization), 48-49 UEFI (Unified Extensible Firmware Interface) Credential Guard and, 437 Device Guard and, 439 disk partitioning schemes and, 202-203 Fast Startup and, 280 file format recommendations, 58 Secure Boot and, 20, 42 Windows Recovery Environment, 393 unattended installation, 22 UNC (Universal Naming Convention) addresses, 250 Undo feature (OneDrive), 264-265 unicast addresses, 168-169 Unified Extensible Firmware Interface (UEFI) Credential Guard and, 437 Device Guard and, 439 disk partitioning schemes and, 202-203 Fast Startup and, 280 file format recommendations, 58 Secure Boot and, 20, 42 Windows Recovery Environment, 393 Uninstall An Update dialog box, 340 Uninstall dialog box, 71-72 uninstalling desktop apps, 103, 278-279 uninstalling device drivers, 71-72 uninstalling Windows Updates, 339-341 unit measurement, disk space size, 397 Universal Naming Convention (UNC) addresses, 250 Universal Windows drivers, 82-83 Universal Windows Platform (UWP), 344, 439 unpinning tiles, 102 unsigned drivers, 83 unsigned scripts, 462 Update And Security app activating Windows 10, 142-143 configuring File History, 407 implementing Insider Preview builds, 329-331 refresh or recycle process, 391 viewing update history, 336-337, 339 Windows Defender, 378

Update Driver Software Wizard, 70 Update-StoragePool cmdlet, 225, 235 updates. See also Windows Update about, 319 choosing delivery method, 322-323 Current Branch choice, 331–332 Current Branch for Business choice, 332 device drivers, 69-70 disabling for drivers, 71-72, 76-77 implementing continuous service, 333 implementing Insider Preview, 327-331 Long-Term Servicing Branch scenarios, 334–335 managing history, 335-338 to mobile devices, 333 preventing driver updates over metered connections, 70-71 rolling back, 339-344 thought experiment, 347-348 viewing history, 322, 336-337 Windows Store Apps, 285-286, 344-347 upgrades about, 9–10, 320 blocking to Windows 10, 39-41 CB and CBB servicing options, 331–332 deferring, 322, 325 firmware, 28 in-place upgrades, 10–12 restarts during, 36 reverting to previous versions, 38-39 selecting suitable methods, 10 status screen, 36 supported upgrade paths, 10–11 systems with BitLocker, 38 using installation media, 41-43 using Windows Update, 30–38 USB drives backing up to, 400 bootable, 57-58 configuring for recovery, 386 creating bootable, 210-211 failures, 233 formatting, 58, 226 installing from, 22, 28 restricting access to, 228-231 securing, 226-228 Storage Spaces and, 220 storing virtual hard disks, 54 Windows.old folder, 34-35 Use Developer Features dialog box, 289 User Account Control Settings dialog box, 423 User Account Control (UAC) about, 431 configuring, 144-147, 429-431 ICD tool and, 88 installing desktop apps, 275 user accounts about, 420 Active Directory and, 148 configuring UAC, 429-431

default, 420 Group Policy and, 154 local, 420-425, 451 Microsoft, 425-428 removing, 391 setting up, 428, 443 workgroups and, 442–443 user data and settings, migrating, 14-15, 49-50 User Experience Virtualization (UE-V), 48-49 user interface about, 97-98 configuring Action Center, 108-109 configuring notifications, 111-112 configuring Quick Action tiles, 109-111 configuring taskbar, 112-114 customizing desktop, 106-108 customizing Start, 98-106 User State Migration Tool (USMT), 13–15, 49–51, 292 User tile element (Start), 106 USMT (User State Migration Tool), 13-15, 49-51, 292 UsmtUtils component (USMT), 51 UWP (Universal Windows Platform), 344, 439

V

VAMT (Volume Activation Management Tool), 141-142 vaults (credentials), 436 VBScript, 121 verification by cell phone, 428 verifier.exe (Driver Verifier Manager), 78-79 version control, documents, 231 VHD format, 211-213, 219 VHDS format, 212-213 VHDs (virtual hard disks) about, 52, 127, 211-212 applying Windows 10 image, 56 attaching with Disk Management, 53 booting Windows 10 from, 55-57 creating MBR-partitioned, 55-56 creating with Disk Management, 213-215 creating with Hyper-V Manager, 213 creating with Windows PowerShell, 215–218 installing Windows inside, 53-54 linking to differencing disks, 218-219 multibooting Windows from, 55-57 native boot, 52-53 VHDX format, 211-213, 219, 402 View menu (Device Manager), 80 virtual hard disks (VHDs) about, 52, 127, 211-212 applying Windows 10 image, 56 attaching with Disk Management, 53 creating MBR-partitioned, 55-56 creating with Hyper-V Manager, 213 creating with Windows PowerShell, 215-218 installing Windows inside, 53-54

linking to differencing disks, 218–219 multibooting Windows from, 55-57 native boot, 52-53 Virtual Machine Monitoring, 314 virtual machines configuring settings, 127-128 core components, 127 creating, 127 managing checkpoints, 128 running, 128 virtual private networks (VPNs) configuring connections, 175–178 creating VPN profiles, 177 Virtual Secure Mode feature, 20 virtual smart card feature, 20 virtual switches, 127 virtualization-assisted security, 437 viruses (computer), 376 VLK (volume license kev), 140 VLSC (Volume Licensing Service Center), 41, 334-335 volume activation, 140-142 Volume Activation Management Tool (VAMT), 141–142 Volume Activation Services server role, 140 volume license key (VLK), 140 volume licensing programs, 139 Volume Licensing Service Center (VLSC), 41, 334–335 Volume Shadow Copy Service (VSS) Backup And Restore tool, 402 Previous Versions feature, 411 System Restore feature, 389 troubleshooting, 413 volumes (disks) about, 202 configuring, 203-204 creating, 209 VPN profiles, 177 VPN tile, 110 VPNs (virtual private networks) configuring connections, 175–178 creating VPN profiles, 177 VSS (Volume Shadow Copy Service) Backup And Restore tool, 402 Previous Versions feature, 411 System Restore feature, 389 troubleshooting, 413 Vssadmin add shadowstorage command, 413 Vssadmin create shadow command, 413 Vssadmin delete shadows command, 399, 413 Vssadmin delete shadowstorage command, 413 Vssadmin list providers command, 413 Vssadmin list shadows command, 399, 413 Vssadmin list shadowstorage command, 397-398, 413 Vssadmin list volumes command, 413 Vssadmin list writers command, 413 Vssadmin resize shadowstorage command, 397, 413

W

Wbadmin enable backup command, 404 Wbadmin get items command, 404 Wbadmin get versions command, 404-405 Wbadmin start backup command, 403-404 Wbadmin start recovery command, 404-405 WBAdmin tool about, 403 backing up using, 403-405 restoring data using, 405-406 WDS (Windows Deployment Services), 21-23, 28 wecutil gc command (Windows Event Collector service), 353 WEP (Wired Equivalent Privacy) standard, 191 WHQL (Windows Hardware Quality Labs), 87 Wi-Fi Direct mode (wireless networking), 190, 194-195 Wi-Fi Protected Access (WPA) standard, 191 Wi-Fi Status dialog box, 193-194 Wi-Fi tile, 110 WIM file format, 33 Windows 10 editions 32-bit or 64-bit versions, 17 determining by device type, 15-18 listed, 16-17 upgrading using Windows Update, 31 Windows Assessment and Deployment Kit (Windows ADK). See also specific tools downloading, 9, 291 Feature-On-Demand files, 88 language packs, 88 testing and fixing applications, 7 Windows Biometric Framework, 20 \$WINDOWS.BTNewOS folder, 36 Windows Component Store, 92–93 Windows Defender, 336, 375-378 Windows Deployment Services (WDS), 21-23, 28 Windows Deployment Wizard, 277 Windows Easy Transfer, 14, 48 Windows Event Collection Service dialog box, 354 Windows Event Collector service (wecutil gc command), 353 Windows Features app (OptionalFeatures.exe), 58-59 Windows Firewall allowing apps through, 184-185 configuring settings, 183 configuring to enable remote management, 299-300 remote management features, 314, 356 Windows Firewall Allowed apps window, 184 Windows Firewall Remote Management, 314 Windows Firewall With Advanced Security configuring, 185 creating rules, 186-187 types of rules, 186 Windows Hardware Developer Center Dashboard portal, 82, 84 Windows Hardware Quality Labs (WHQL), 87

Windows Hello, 20, 432 Windows Imaging And Configuration Designer (ICD) tool about, 22 creating provisioning packages, 291–293 deploying driver packages, 88–91 exporting provisioning packages, 294 preparing installation media, 135-137 recovery options, 392 Windows Insider Preview Program, 327-331, 341 Windows Installer, 29 Windows logs, 351 Windows Management Instrumentation (WMI), 314. 340-341 Windows Memory Diagnostic tool (mdsched.exe), 382 Windows Network Diagnostics, 196 Windows.old folder backups in, 34, 36, 341 confirming existence of, 38, 342-343 migrating user settings from, 51 recovery from, 38-39, 341-343 Windows PE (Windows Preinstallation Environment), 22-24, 28, 292 Windows PowerShell. See also specific cmdlets about, 196, 298 Active Directory module, 148, 150, 152 ADAC support, 154 automating management tasks, 461-463 configuring DNS client settings, 172 configuring IPv4 settings, 167–168 configuring IPv6 settings, 170 configuring remoting, 310-312 configuring System Restore, 388-389 configuring Windows features, 283-284 configuring Windows Firewall, 184–185 configuring Windows Firewall With Advanced Security, 187 creating VHDs, 215-218 disk management tasks, 208-210 exporting Start layout, 104, 133 installing Hyper-V feature, 127 listing local user accounts, 420 managing driver packages, 86 managing file and folder permissions, 260 managing printers, 371–372 managing remote computers, 310-312, 314-315 managing services, 453 managing Storage Spaces, 224–225 managing user accounts, 425 RSAT support, 155 running DISM within, 60 running scripts, 462-463 sharing folders, 249 sideloading apps, 289 troubleshooting name resolution, 196–197 viewing configuration information, 44 viewing SMB version, 238 Windows PowerShell ISE, 216-217, 463 Windows PowerShell remoting, 310-312, 314-315

Windows RE (Windows Recovery Environment), 393-396, 403, 405 Windows Registry (Regedit.exe) blocking upgrading to Windows 10, 39-41 configuring UAC, 147 HKEY_CURRENT_USER registry subtree, 14 viewing app startup information, 282 Windows Remote Management service (winrm quickconfig command), 311-312, 314, 353-354 Windows Run dialog box, 305 Windows Security dialog box, 444 Windows Setup, 34 Windows SIM (Windows System Image Manager), 23 Windows Software Update Services (WSUS), 241, 319, 337 Windows Store Apps about, 273, 284 blocking, 288 configuring settings, 286–288 distributing, 290 managing, 284-286 sideloading, 289-290 updating, 285-286, 344-347 Windows Store for Business, 290 Windows Update about, 30, 319 checking for updates, 40 configuring language support, 61 configuring options, 319-320 configuring settings, 320-323 configuring with Group Policy, 324-327 Current Branch, 331–332 Current Branch for Business, 332 disabling, 72 hiding in Windows 10, 337-338 identifying editions supported, 31 performing upgrades, 31–38 printer drivers, 241 scheduling, 34-35 showing in Windows 10, 337-338 troubleshooting, 327 uninstalling, 339-341 updating device drivers, 69–70 Windows Update dialog box, 34-35 Windows Update node (Group Policy), 324-325 Windows Update Stand-Alone Installer (Wusa.exe) tool, 340-341 WinRAR tool, 91 WinRE (Windows Recovery Environment), 36 winrm quickconfig command (Windows Remote Management service), 311-312, 314, 353-354 WinSxS directory, 92–93 wipe-and-load migrations (clean installations) considerations for, 12–13 methods for, 10 migrating user data and settings, 14-15 performing, 27-30, 42 side-by-side migration, 10, 13 Wired Equivalent Privacy (WEP) standard, 191

wireless access point (wireless AP), 166 wireless networking configuring settings, 191–194 standards overview, 189–191 WMI (Windows Management Instrumentation), 314, 340-341 workaroups configuring, 442-443 managing remote computers, 314 worms (computer), 376 WPA (Wi-Fi Protected Access) standard, 191 WPA2 security standard, 191 Write Attributes permission, 259 Write Data permission, 259 Write Extended Attributes permission, 259 Write permission, 240, 258-259 WSUS (Windows Software Update Services), 241, 319, 337 Wusa.exe (Windows Update Stand-Alone Installer) tool, 340-341

X

Xcopy tool, 58 XML layout file, 104 XML Paper Specification (XPS), 241 XPS (XML Paper Specification), 241

Ζ

zero-touch installation (ZTI), 21, 276 ZTI (zero-touch installation), 21, 276