

Introduction

You've already learned how to deal with application and hardware problems, and Windows problems after the OS has started. In this module, you take your troubleshooting skills one step further by learning to deal with startup problems caused by Windows. When Windows fails to start, it can be stressful if important data has not been backed up or the user has pressing work to do with the computer. What helps more than anything else is to have a good understanding of Windows startup and a good plan for approaching startup problems.

We begin the module with a discussion of what happens when you first turn on a computer and Windows starts. The more you understand about startup, the better your chances of fixing startup problems. Then you learn about Windows tools specifically designed to handle startup problems. Finally, you learn about strategies for solving startup problems. As you work, note that the troubleshooting tools and skills for Windows 10 work the same way as for Windows 11, with only a few minor changes in menu options.

15-1 Understanding the Boot Process

Core 2 Objective

- 3.1

Given a scenario, troubleshoot common Windows OS problems.

Knowledge is power. The better you understand what happens when you first turn on a computer until Windows is loaded and the Windows desktop appears, the more likely you will be able to solve a problem when Windows cannot start. Let's begin by noting the differences between a hard boot and a soft boot.

Note 1

Most techies use the terms “boot” and “startup” interchangeably. However, in general, the term “boot” refers to the hardware phase of starting up a computer. Microsoft consistently uses the term “startup” to refer to how its operating systems are booted—I mean, started.

15-1a Different Ways to Boot

Core 2 Objective

- 3.1

Given a scenario, troubleshoot common Windows OS problems.

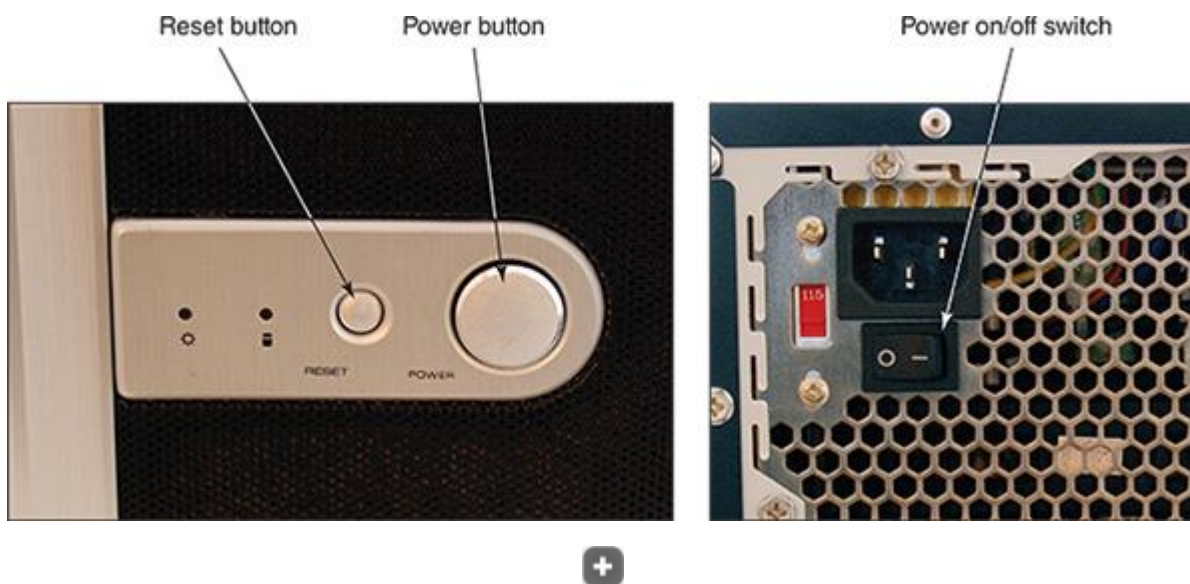
The term **booting** comes from the phrase “lifting yourself up by your bootstraps” and refers to the computer bringing itself up to a working state without the user having to do anything but press the On button. There are two fundamental ways to boot a computer:

- A **hard boot**, or **cold boot**, involves turning on the power with the on/off switch.
- A **soft boot**, or **warm boot**, involves using the operating system to reboot. In Windows, a soft boot is called a restart.

A hard boot takes more time than a soft boot because a hard boot requires the initial steps performed by BIOS/UEFI. Most desktop cases have three power buttons; an example of these buttons on one system is shown in [Figure 15-1](#).

Figure 15-1

This computer case has two power buttons on the front and one power switch on the rear



Here's how the buttons work:

- The power button in front can be configured as a “soft” power button, causing a Windows restart.
- The reset button initializes the CPU so it restarts at the beginning of the BIOS/UEFI startup program. The computer behaves as though the power were turned off and back on and then goes through the entire boot process.
- The switch on the rear of the case simply turns off the power abruptly and is a “hard” power button. If you use this switch, wait 30 seconds before you press the power button on the front of the case to boot the system. This method gives you the greatest assurance that memory will clear. However, if Windows is abruptly stopped, it might give an error message when you reboot.

How the front two buttons work can be controlled in BIOS/UEFI setup. Know, however, that different cases offer different options.

When Windows hangs, first try a restart. If that doesn't work, try a shutdown and then power the system back up. A Windows shutdown closes all open applications, user sessions, services, devices, and system processes and then powers down the computer. If a shutdown does not work, press the reset button on the front of the case. If that doesn't work, turn off the power switch on the rear of the case, wait 30 seconds, turn it back on, and then press the power button on the front of the case.

15-1b Steps to Boot the Computer and Start Windows

Core 2 Objective

- 3.1

Given a scenario, troubleshoot common Windows OS problems.

Recall that BIOS/UEFI is responsible for getting a system up and going and finding an OS to load. [Table 15-1](#) lists the components and files stored on the hard drive that are necessary to start Windows. The table can serve as a guide as you study the steps to see what happens from the time power is turned on until Windows is started. In these steps, we assume the OS is loaded from the hard drive.

Table 15-1

Software Components and Files Needed to Start Windows

Component or File	Partition and Path*	Description
BIOS systems using MBR partitioning		
MBR	The first sector of the hard drive is called the Master Boot Record (MBR)	BIOS looks to the partition table in the MBR to locate the active partition.
System partition	Also called the active partition or System Reserved partition	The system partition holds the Boot Manager, Boot Configuration Data (BCD) store, and other files and folders needed to begin Windows startup. For Windows, these files are stored in the root and \Boot directory of the hidden system partition.
Boot Manager	In the root of the system partition	Windows Boot Manager, bootmgr (with no file extension), accesses the BCD store and locates the Windows Boot Loader.
BCD store	\Boot directory on the system partition	The Boot Configuration Data (BCD) store is a database file named BCD (no file extension), and it is organized the same as a registry hive. It contains boot settings that control

Component or File	Partition and Path★	Description
BIOS systems using MBR partitioning		
		the Boot Manager and can be viewed and edited with the bcdedit command.
UEFI systems using GPT partitioning		
GPT partition table	At the beginning of the hard drive, with a backup copy at the end of the drive	UEFI looks to the GPT partition table to locate the EFI System Partition.
System partition	The EFI System Partition (ESP) is normally 100 MB to 200 MB in size.	The system partition holds the Windows Boot Manager, BCD, and other supporting files. For Windows, the Boot Manager is Bootmgfw.efi and is stored in \EFI\Microsoft\Boot. A backup copy of Bootmgfw.efi is at \EFI\Boot\bootx64.efi.
Boot Manager	For Windows, \EFI\Microsoft\Boot on the ESP	Bootmgfw.efi loads EFI applications based on variables stored in onboard RAM and reads the BCD store to find out other boot parameters (such as a dual boot).
BCD store	\EFI\Microsoft\Boot on the ESP	Entries in the BCD store point the Windows Boot Manager to the location of the Windows Boot Loader program.
All Windows BIOS and UEFI systems		
Windows Boot Loader	C:\Windows\System32★	Windows Boot Manager turns control over to the Windows Boot Loader , which loads and starts essential Windows processes. Two versions of the program file are Winload.exe (BIOS) and Winload.efi (UEFI).
Resume from hibernation	C:\Windows\System32	Windows Boot Loader runs when Windows resumes from hibernation. Two versions of the program are Winresume.exe for BIOS and Winresume.efi for UEFI.
Ntoskrnl.exe	C:\Windows\System32	Windows kernel
Hal.dll	C:\Windows\System32	Dynamic Link Library handles low-level hardware details.
Smss.exe	C:\Windows\System32	Sessions Manager program responsible for starting user sessions
Csrss.exe	C:\Windows\System32	Win32 subsystem manages graphical components and threads
Winlogon.exe	C:\Windows\System32	Logon process
Services.exe	C:\Windows\System32	Service Control Manager starts and stops services
Lsass.exe	C:\Windows\System32	Authenticates users
System registry hive	C:\Windows\System32\Config	Holds data for the HKEY_LOCAL_MACHINE key of the registry
Device drivers	C:\Windows\System32\Drivers	Drivers for required hardware



A successful boot depends on essential hardware devices, BIOS/UEFI, and the operating system all performing without errors. Let's look at the steps to start a Windows computer. Several of these steps are diagrammed in [Figures 15-2](#) and [15-3](#) to help you visually understand how the steps work.

Figure 15-2

Steps to booting the computer and loading Windows

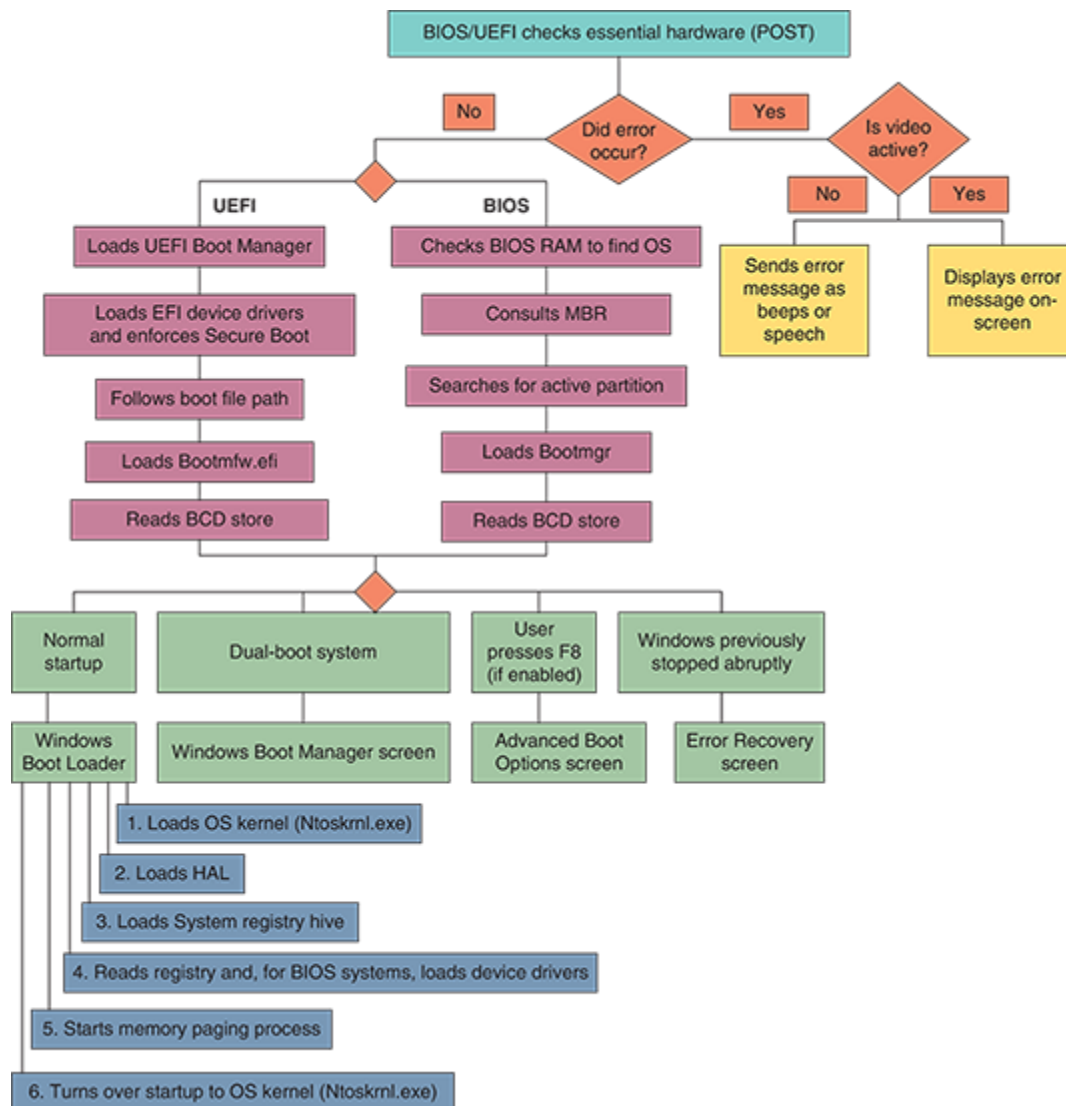
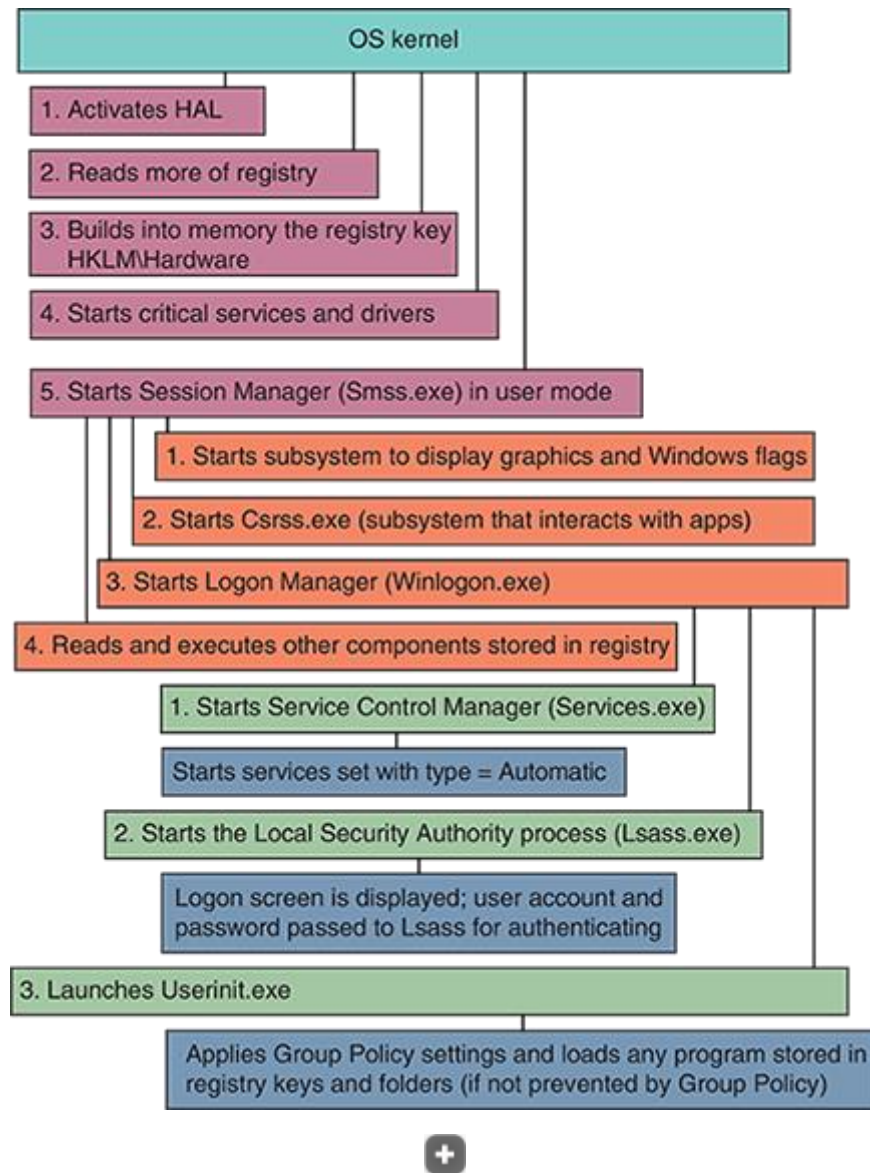


Figure 15-3

Steps to complete loading Windows



Study these steps carefully because the better you understand startup, the more likely you'll be able to solve startup problems:

1. **1**

Startup BIOS/UEFI is responsible for the early steps in the boot process. Onboard RAM accessible to BIOS/UEFI holds an inventory of hardware devices, hardware settings, security passwords, date and time, and startup settings. Startup BIOS/UEFI reads this information and then surveys the hardware devices it finds present, comparing it with the list kept in its RAM.

Note 2

Onboard RAM, also called onboard memory, nonvolatile RAM, or NVRAM, is used by BIOS/UEFI to hold configuration data. Onboard RAM, which keeps its data even when power is turned off, is different from system memory or RAM, which holds programs and data only while the system is turned on.

2. **2**

Startup BIOS/UEFI runs **POST (power-on self-test)**, which is a series of tests to find out if the firmware can communicate correctly with essential hardware components required for a successful boot. Any errors are indicated as a series of beeps, recorded speech, or error messages on the screen (after video is checked). If the key is pressed to request BIOS/UEFI setup, the BIOS/UEFI setup program runs.

3. **3**

Based on information kept in onboard RAM, startup UEFI loads the UEFI boot manager and device drivers. BIOS/UEFI then turns to the hard drive or other boot device to locate and launch the Windows Boot Manager. If BIOS/UEFI cannot find a Windows Boot Manager or cannot turn over operation to it, one of these error messages appears:

Missing operating system

No OS found

Error loading operating system

Windows failed to load

Invalid partition table

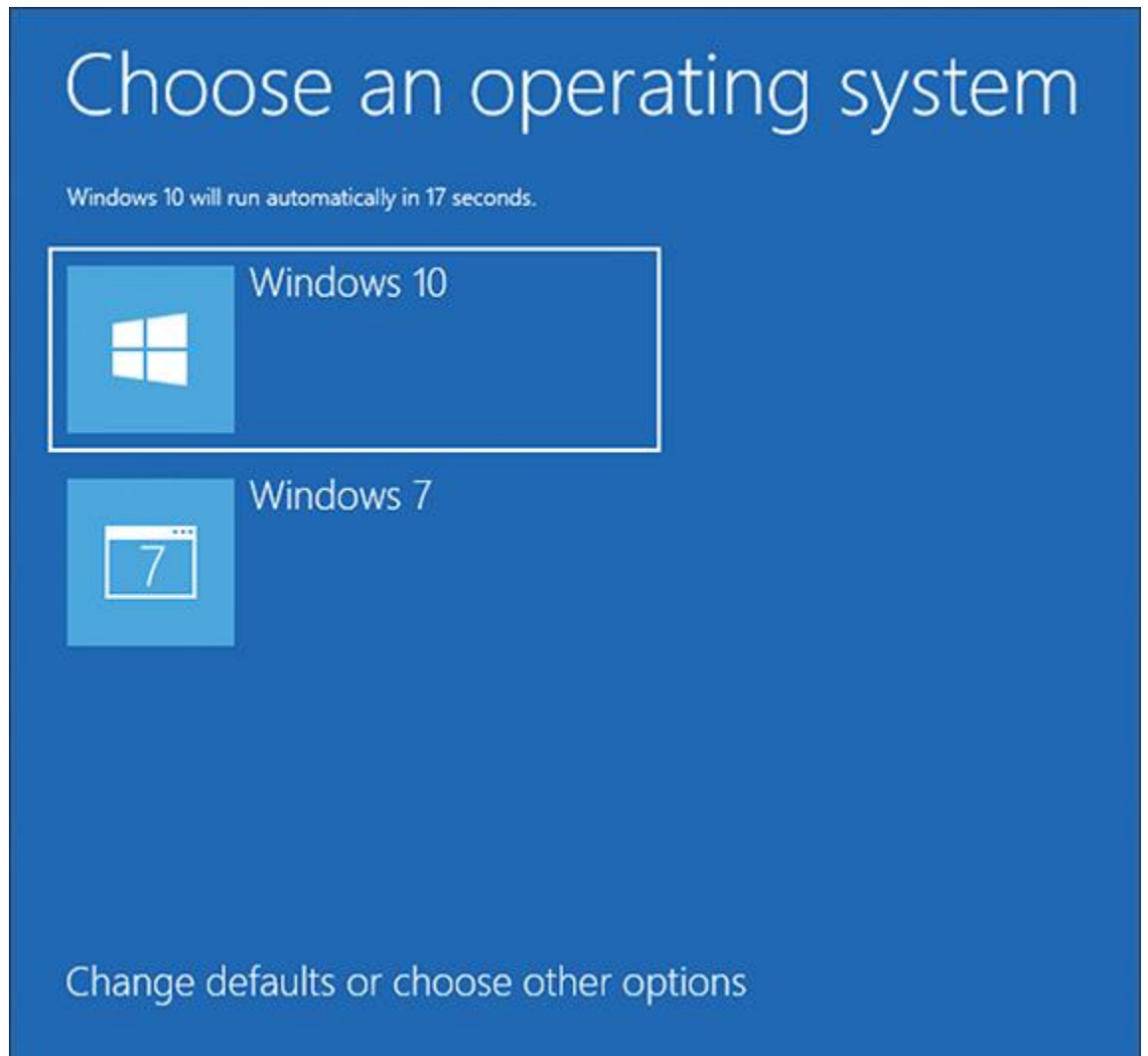
4. **4**

The Windows Boot Manager does the following:

1. It reads the settings in the BCD.
2. The next step depends on entries in the BCD and these other factors:
 - **Option 1.** For normal startups that are not dual booting, no menu appears, and Boot Manager finds and launches the Windows Boot Loader program.
 - **Option 2.** If the computer is set up for a dual-boot environment, Boot Manager displays the message, *Choose an operating system* screen, as shown in [Figure 15-4](#).

Figure 15-4

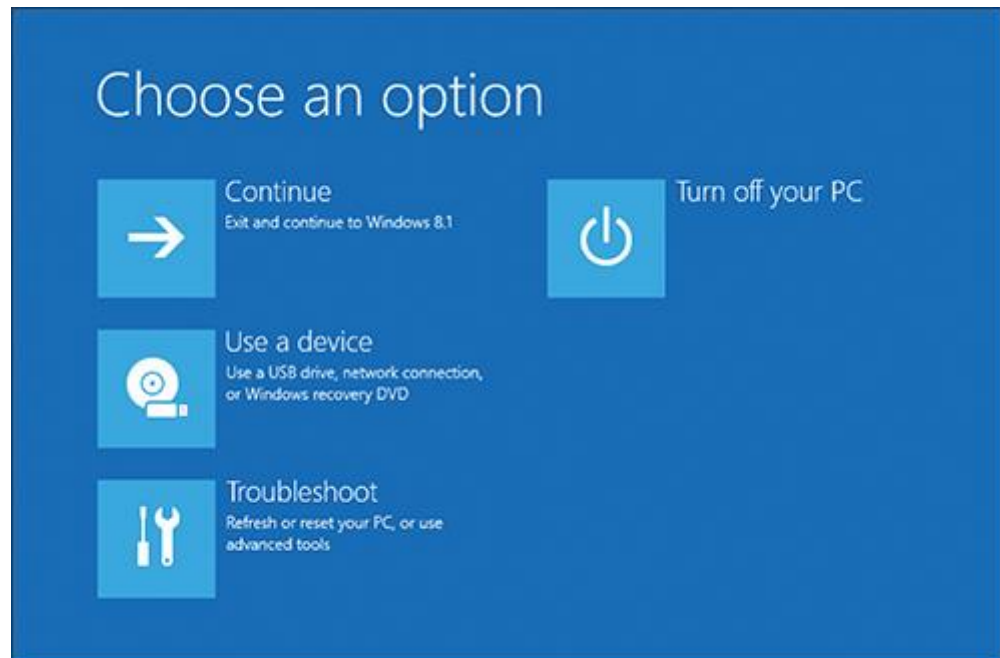
In a dual-boot setup, Windows Boot Manager provides a choice of operating systems



- **Option 3.** If Windows was previously stopped abruptly or another error occurs, the Windows Startup Menu appears (see [Figure 15-5](#)) to give you the option to troubleshoot the problem.

Figure 15-5

The Windows Startup Menu offers the opportunity to troubleshoot a problem with startup



5. **5** Windows Boot Loader (Winload.exe or Winload.efi) is responsible for loading Windows components. It does the following:

1. For normal startups, Boot Loader loads into system memory the OS kernel, Ntoskrnl.exe, but does not yet start it. Boot Loader also loads into memory the hardware abstraction layer (Hal.dll), which will later be used by the kernel.
2. Boot Loader loads into memory the system registry hive (C:\Windows\System32\Config\System).
3. Boot Loader then reads the registry key just created, HKEY_LOCAL_MACHINE\SYSTEM\Services, looking for and loading into memory the device drivers that must be launched at startup. The drivers are not yet started.
4. Boot Loader starts up the memory paging process and then turns over startup to the OS kernel (Ntoskrnl.exe).

6. **6** The kernel (Ntoskrnl.exe) does the following:

1. It activates the HAL, reads more information from the registry, and builds into memory the registry key HKEY_LOCAL_MACHINE\HARDWARE, using information about the hardware that has been collected.
2. The kernel then starts critical services and drivers that are configured to be started by the kernel during the boot. Recall that drivers interact directly with hardware and run in kernel mode, whereas services interact with drivers. Most services and drivers are stored in C:\Windows\System32 or C:\Windows\System32\Drivers and have an .exe, .dll, or .sys file extension.

After the kernel starts all services and drivers configured to load during the boot, it starts the Session Manager (Smss.exe), which runs in user mode.

7. **7**

The Session Manager (Smss.exe) loads the graphical interface and starts the client/server run-time subsystem (Csrss.exe), which also runs in user mode. Csrss.exe is the Win32 subsystem component that interacts with applications.

8. **8**

Smss.exe starts the Logon Manager (Winlogon.exe) and reads and executes other commands stored in the registry, such as a command to replace system files placed there by Windows Update.

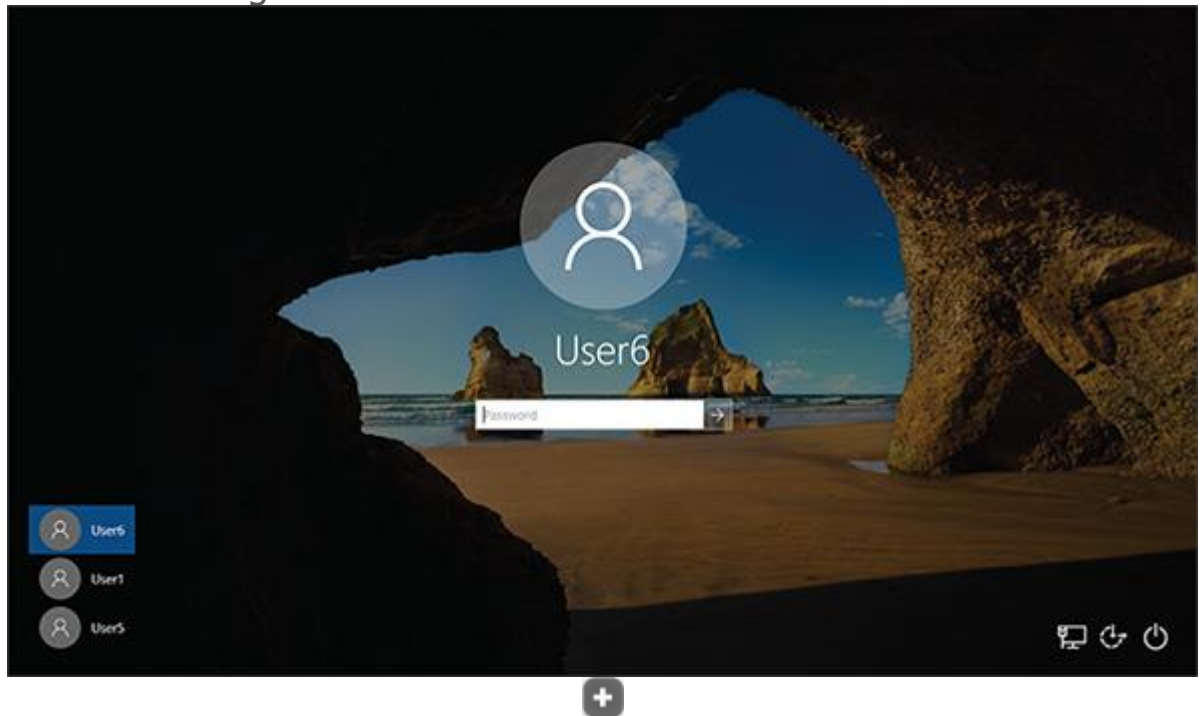
9. **9**

Winlogon.exe does the following:

1. It starts the Service Control Manager (Services.exe), which starts all services listed with the startup type of Automatic in the Services console.
2. Winlogon.exe starts the Local Security Authority process (Lsass.exe). The sign-in screen appears (see [Figure 15-6](#)), and the user account and password are passed to the Lsass.exe process for authenticating.

Figure 15-6

The Windows sign-in screen



3. Winlogon.exe launches Userinit.exe. The Windows desktop is launched.

10.

10

Userinit.exe applies Group Policy settings and any programs not trumped by Group Policy that are stored in startup folders and startup registry keys. See the appendix [“Entry Points for Windows Startup Processes”](#) for a list of these folders and registry keys.

The Windows startup is officially completed when the Windows desktop appears and the pinwheel wait icon disappears.

With this basic knowledge of the boot in hand, let's turn our attention to what you can do to prepare for problems when Windows refuses to load.

15-2 What to Do before a Problem Occurs

Core 2 Objective

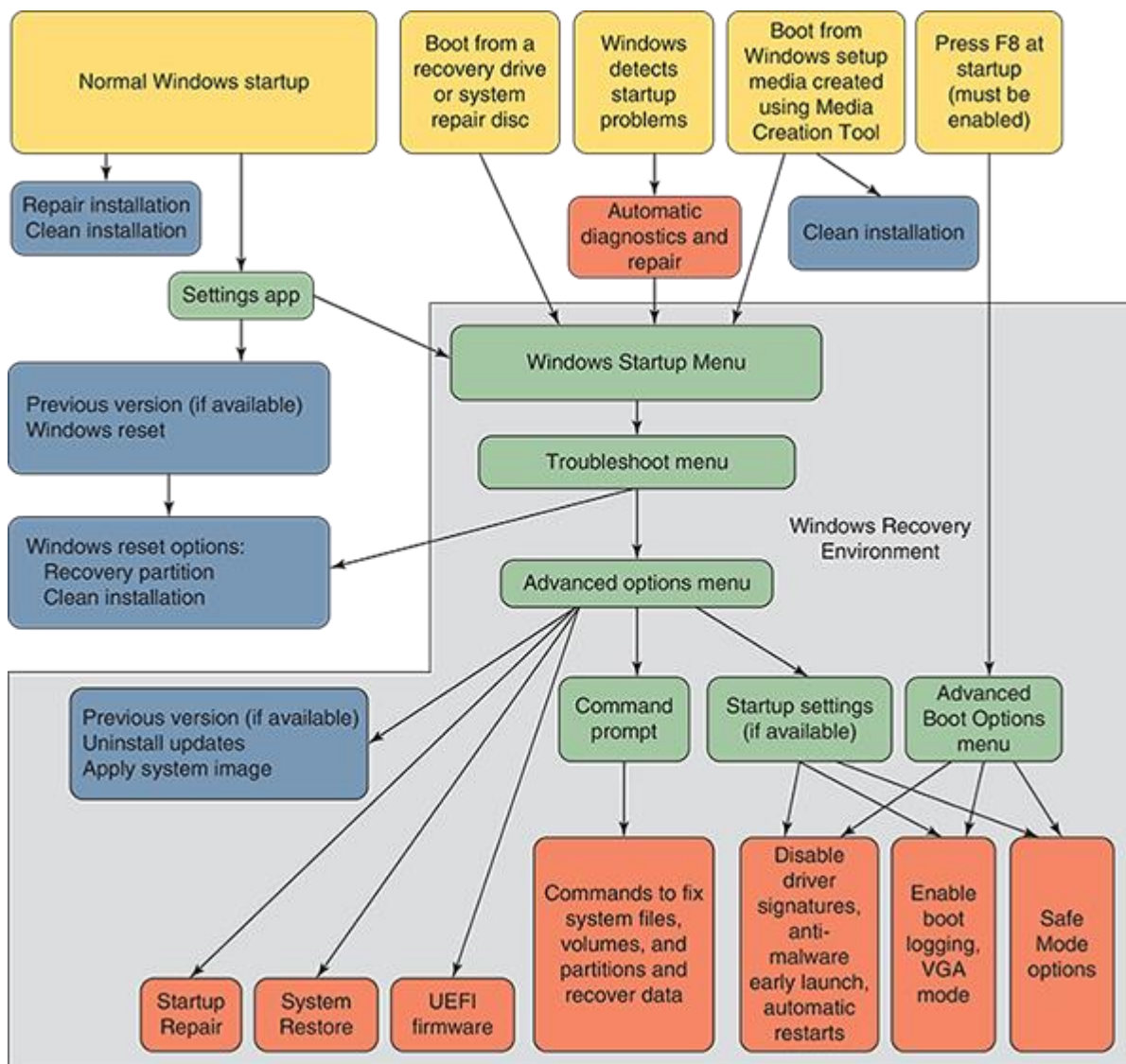
- 3.1

Given a scenario, troubleshoot common Windows OS problems.

When troubleshooting startup, it helps to have a road map, which is the purpose of the diagram in [Figure 15-7](#). It can help you organize in your mind the various ways to boot the system and the menus and procedures available to you depending on how the boot happens.

Figure 15-7

Methods to boot the system, menus that appear, and tools available on menus used to troubleshoot startup problems





As you learn to use each tool, keep in mind that you want to use the tool that makes as few changes to the system as possible to fix the problem. Good preparation will make troubleshooting startup problems much simpler and more successful. When you are responsible for a computer and while the computer is still healthy, be sure to complete the following tasks:

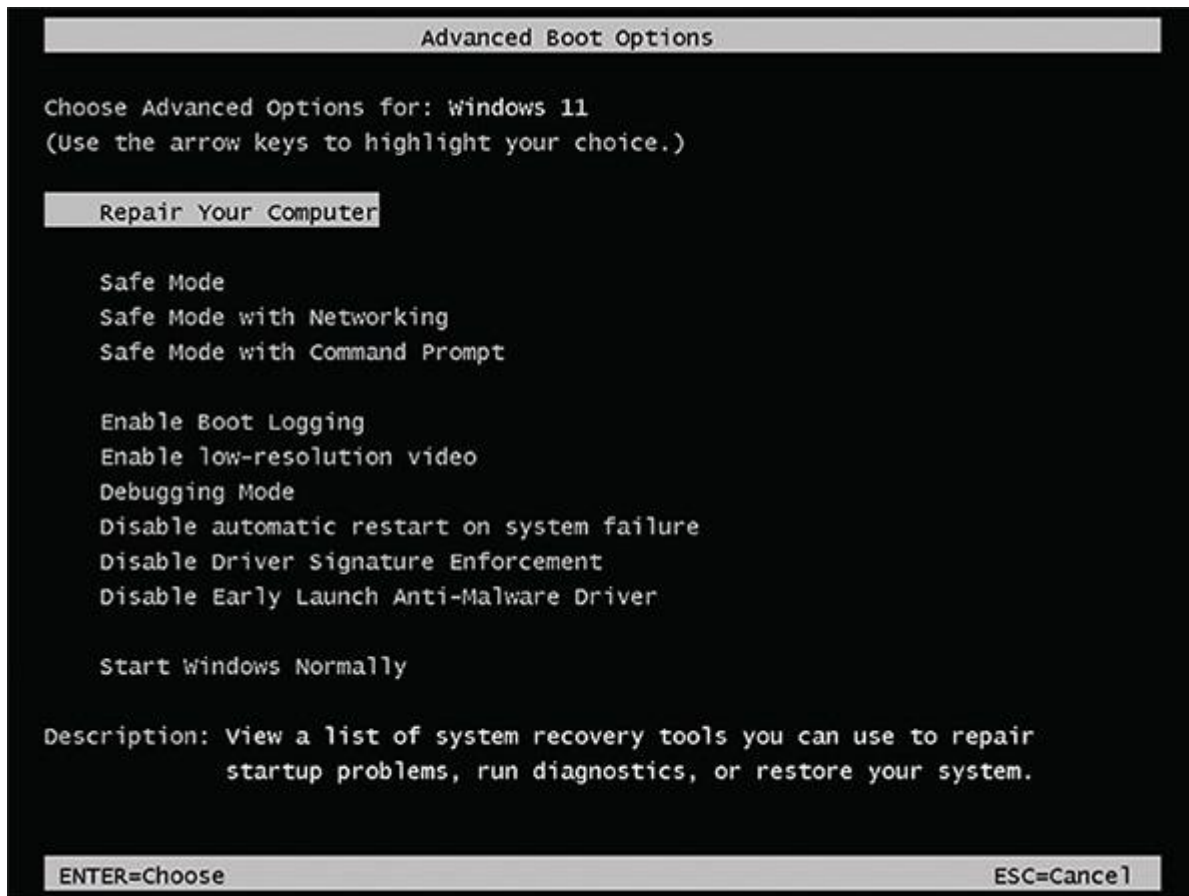
- **Keep good backups.** The module “[Maintaining Windows](#)” covers methods to back up data, applications, and user settings.
- **Turn on System Restore.** Recall from the module “[Maintaining Windows](#)” that by default System Restore is turned off. Use the System Properties dialog box to turn it on.
- **Create a system image.** Recall from the module “[Maintaining Windows](#)” that a system image can be created right after you’ve installed Windows, hardware, applications, and user accounts and customized Windows settings. The image can be updated periodically.
- **Configure Windows to use the F8 key at startup.** The F8 key gives you access to the Advanced Boot Options menu in Windows, which you’ll learn about later in this module. Windows 10/11 has the feature disabled by default. To enable the F8 key at startup, open an elevated command prompt window, and enter this command:

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

[Figure 15-8](#) shows the Advanced Boot Options screen that appears when you press F8 during Windows 11 startup.

Figure 15-8

Use the Advanced Boot Options menu to troubleshoot difficult startup problems



Later, if you want to disable the use of F8 at startup, open an elevated command prompt window, and enter this command:

```
bcdedit /set {default} bootmenupolicy standard
```

Caution

As you learn to troubleshoot Windows startup, don't depend on the F8 key to work during the boot, because you never know when you'll work on a computer that has it disabled. All the tools available on the Advanced Boot Options screen are also available on the Windows 10 Startup Settings screen, which you can access without using F8. You learn about the Startup Settings screen later in this module. For Windows 11, you also learn how to access the Advanced Boot Options screen without using F8.

- **Create recovery boot media.** If Windows can't boot from the hard drive, you may be able to repair the Windows installation using tools available in the **Windows Recovery Environment (Windows RE or WinRE)**. Windows RE is normally stored on a hidden partition on the hard drive and is a lean operating system that can be launched to solve Windows startup problems. It provides both a graphical and command-line interface. The diagram shown earlier in [Figure 15-7](#) shows Windows RE as a gray background. In that figure, menus in Windows RE are in green, tools are in blue and orange, and ways to

launch Windows RE are in yellow boxes. Notice in [Figure 15-7](#) that you can launch Windows RE after a normal Windows startup. However, if Windows won't start, you'll need other recovery boot media to launch it. Although it's possible to use recovery media created on a different computer than the one you are troubleshooting, the process is simplified if you already have these tools on hand. [Figure 15-7](#) shows the three types of recovery boot media:

- Windows 10/11 DVD system repair disc
- Windows 10/11 USB recovery drive
- Windows 10/11 setup media, which was created earlier by the Media Creation Tool

The key to using a system repair disc or recovery drive is to create the disc or drive before it is needed. Let's look at each of the three recovery boot media.

Note 3

All boot media are bit-specific. Use 32-bit media to repair a 32-bit Windows installation and 64-bit media to repair a 64-bit installation.

15-2a Windows 10/11 System Repair Disc

Core 2 Objective

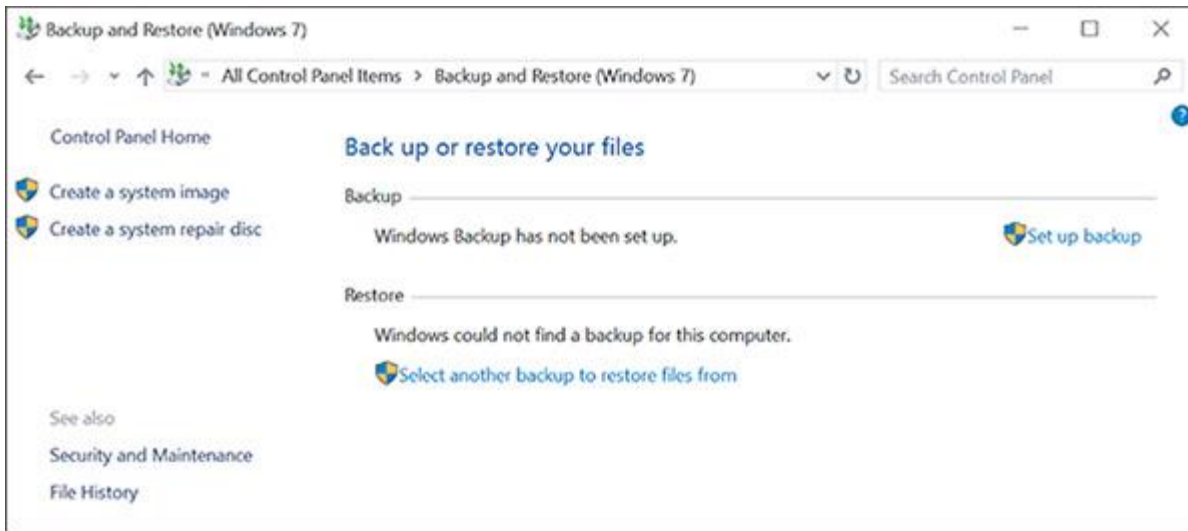
- 3.1

Given a scenario, troubleshoot common Windows OS problems.

A **system repair disc** is a bootable DVD with Windows repair tools that can start the system and fix problems. Using the DVD requires an optical drive. Open **Control Panel** and go to the **Backup and Restore (Windows 7)** window (see [Figure 15-9](#)). Click **Create a system repair disc**. A 32-bit Windows installation will create a 32-bit version of the repair disc, and a 64-bit Windows installation will create a 64-bit version of the repair disc. To use a system repair disc, boot the system from the disc, and select your keyboard layout. Then Windows RE is launched.

Figure 15-9

Create a system image or a system repair disc from Control Panel



15-2b Windows 10/11 Recovery Drive

Core 2 Objective

- 3.1

Given a scenario, troubleshoot common Windows OS problems.

Suppose the hard drive in a laptop completely fails. You can purchase a new hard drive for the system, but a problem might arise when you install Windows on the new drive. Most laptops, all-in-one, and other brand-name computers include an OEM recovery partition on the hard drive that contains a copy of the OS build, device drivers, diagnostics programs, and preinstalled applications needed to restore the system to its factory state. Before a problem occurs, you can back up this OEM recovery partition to a Windows recovery drive. A **recovery drive** is a bootable USB flash drive that can access Windows repair tools; in addition to holding an OEM recovery partition, it is handy when you need to repair a computer that doesn't have an optical drive.

Note 4

A recovery drive is bit-specific: Use a 32-bit recovery drive to repair a 32-bit Windows installation and a 64-bit recovery drive to repair a 64-bit installation.

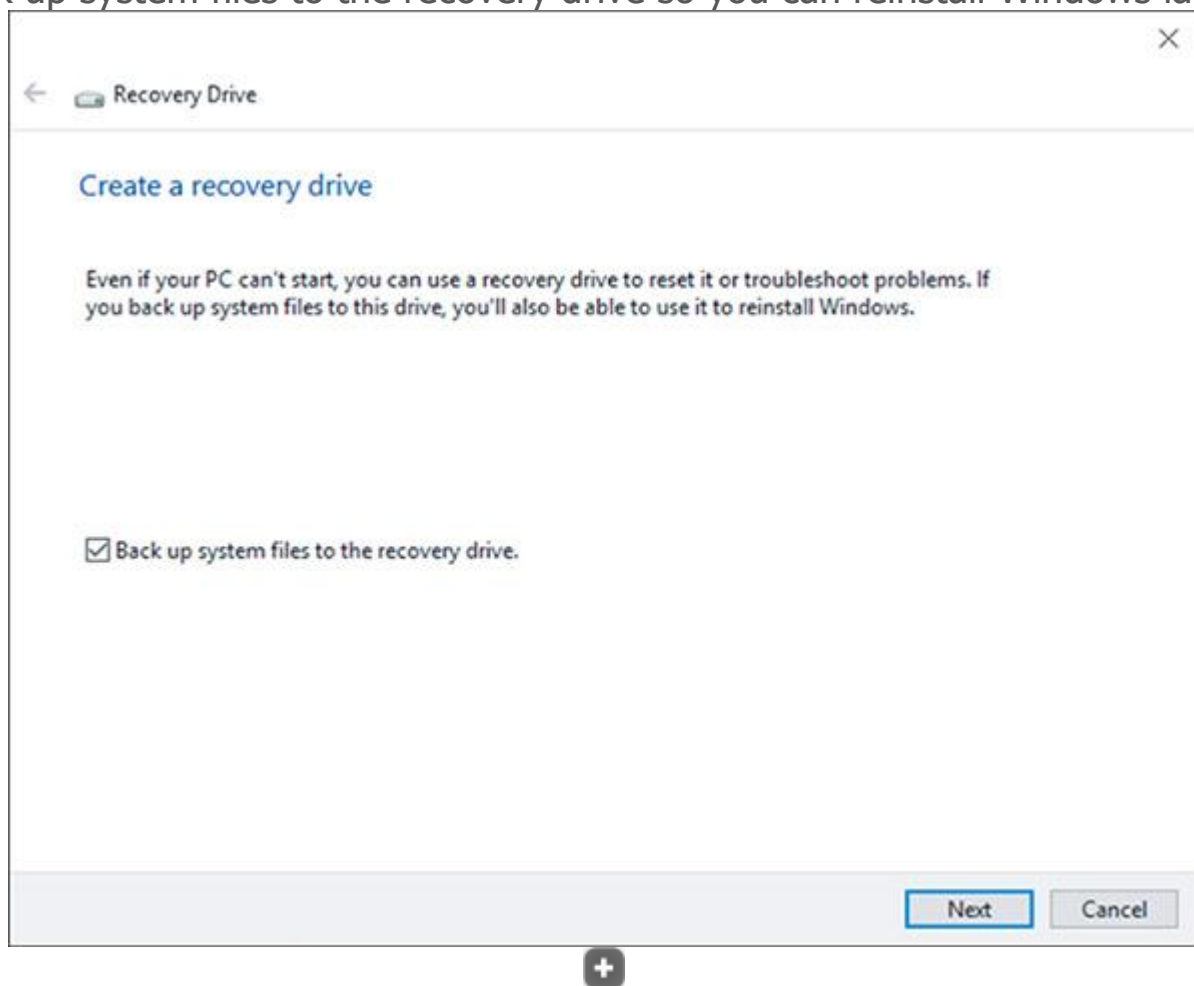
If you include the system files on the recovery drive, you have the option of reinstalling Windows from the recovery drive. As you can see in [Figure 15-7](#), a recovery drive can be used to perform a Windows 10/11 reset, which you learn about later in the module. You can use a recovery drive to repair a computer other than the one on which it was created. However, system files included on a recovery drive may not be compatible with all computers.

Do the following to create a recovery drive:

1. **1** Open **Control Panel** in Classic view, and click **Recovery**. Click **Create a recovery drive**, and respond to the UAC dialog box.
2. **2** Choose whether to include system files (see [Figure 15-10](#)), which will copy the OEM recovery partition to the recovery drive. If the computer doesn't have an OEM recovery partition, the check box on this dialog box is gray and not available. Click **Next** to continue.

Figure 15-10

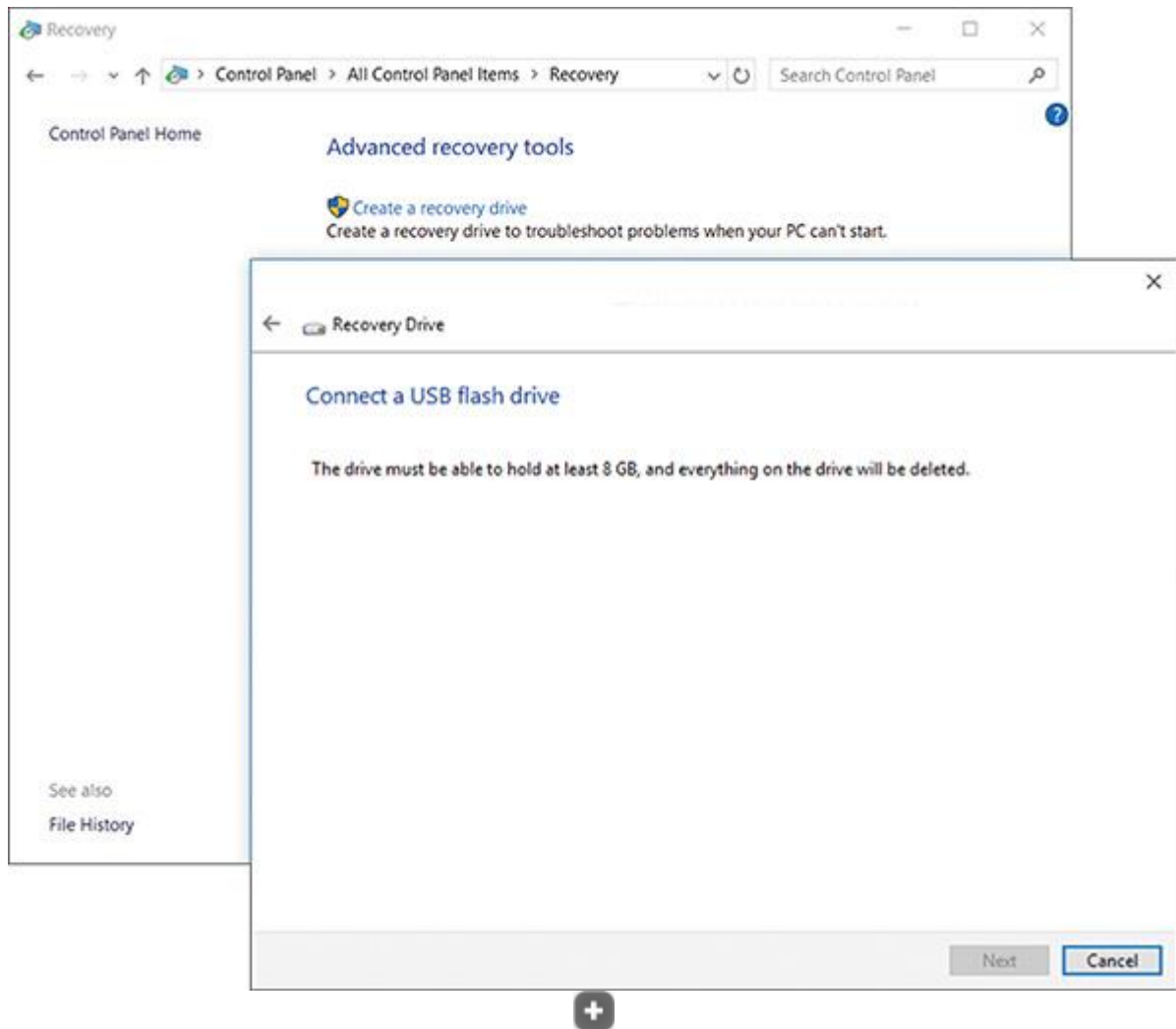
Back up system files to the recovery drive so you can reinstall Windows later



3. **3** Windows reports the size of the USB flash drive needed (see [Figure 15-11](#)). Plug in a USB flash drive that is large enough. Know that the entire USB flash drive will be formatted, and everything on the drive will be lost.

Figure 15-11

Windows reports the size of the USB flash drive needed to hold the recovery drive



4. **4** Windows inspects the size of the drive; if it is large enough, you see it listed among available devices. Be careful to select the USB flash drive because everything on the drive will be lost. Click **Next**. Click **Create** to begin the process. It will take a while to complete. Then click **Finish**.

Be sure to label the flash drive well, and put it in a safe place. For example, you can put it in an envelope, label it “Recovery drive for John Hawkins 64-bit Windows 10 Sony laptop,” and store it in the computer’s documentation file.

Note 5

If you copied the OEM recovery partition to the USB flash drive and are short on hard drive space on the computer, you can use Disk Management to delete the recovery partition and free up some space, and then expand the Windows volume.

15-2c Windows 10/11 Media Creation Tool

Core 2 Objective

- 3.1

Given a scenario, troubleshoot common Windows OS problems.

You can launch Windows RE from a Windows setup DVD or flash drive. For Windows 10/11, recall you can use the Media Creation Tool on a working computer to create a bootable Windows setup ISO file, DVD, or flash drive. You learned how to use the Media Creation Tool in the module “[Installing Windows](#).”

15-3 Tools for Solving Windows Startup Problems

Core 2 Objective

- 3.1

Given a scenario, troubleshoot common Windows OS problems.

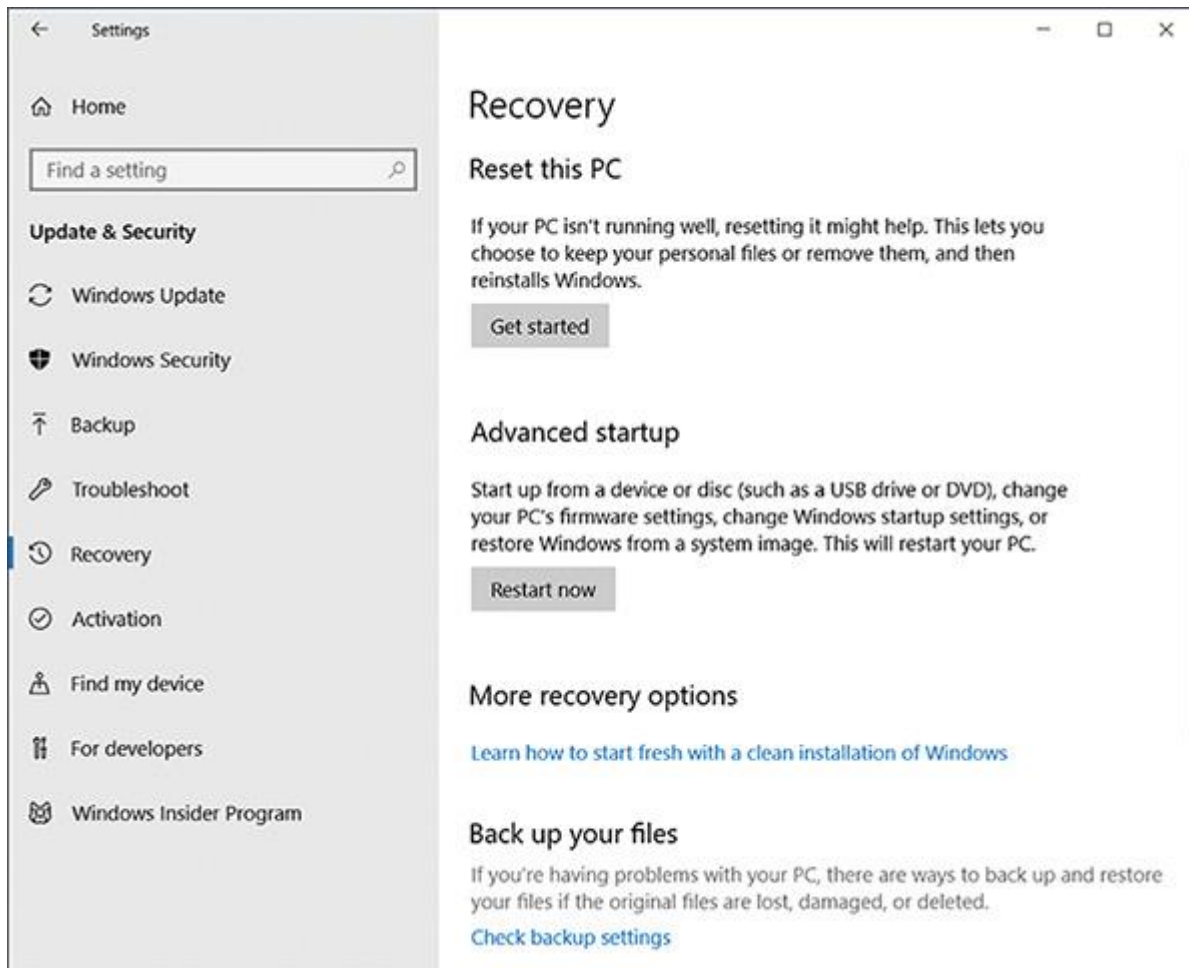
Looking back at the diagram in [Figure 15-7](#), note that tools to diagnose and repair Windows are shown in orange boxes. In this part of the module, we discuss how these tools can help you solve a startup problem. The tools are covered beginning with the least-invasive ones.

If Windows works well enough to get to the Windows desktop, you can use one of the following methods to launch Windows RE:

- **Windows 10/11 Settings app.** Open the **Settings** app and, for Windows 10, click **Update & Security**. For Windows 11, click **System**. In the left pane, click **Recovery**. Under Advanced startup, click **Restart now**. See [Figure 15-12](#).

Figure 15-12

The Windows 10 Recovery page in the Settings app



Note 6

The Advanced startup option is not available on the Recovery window when you are using a remote connection to the computer or when Windows 10/11 is installed in a VM. To force a VM into the recovery environment, in a command prompt window, run the command **reagentc /bootore**, and then restart the VM.

- **Shift+Restart.** From the Windows Start menu, click the **Power** icon. Press and hold the **Shift** key, and click **Restart**.
- **Command prompt.** In a command prompt window, enter **shutdown /r /o**. The /r parameter instructs the computer to restart, and the /o parameter opens Windows RE after the restart.

Note 7

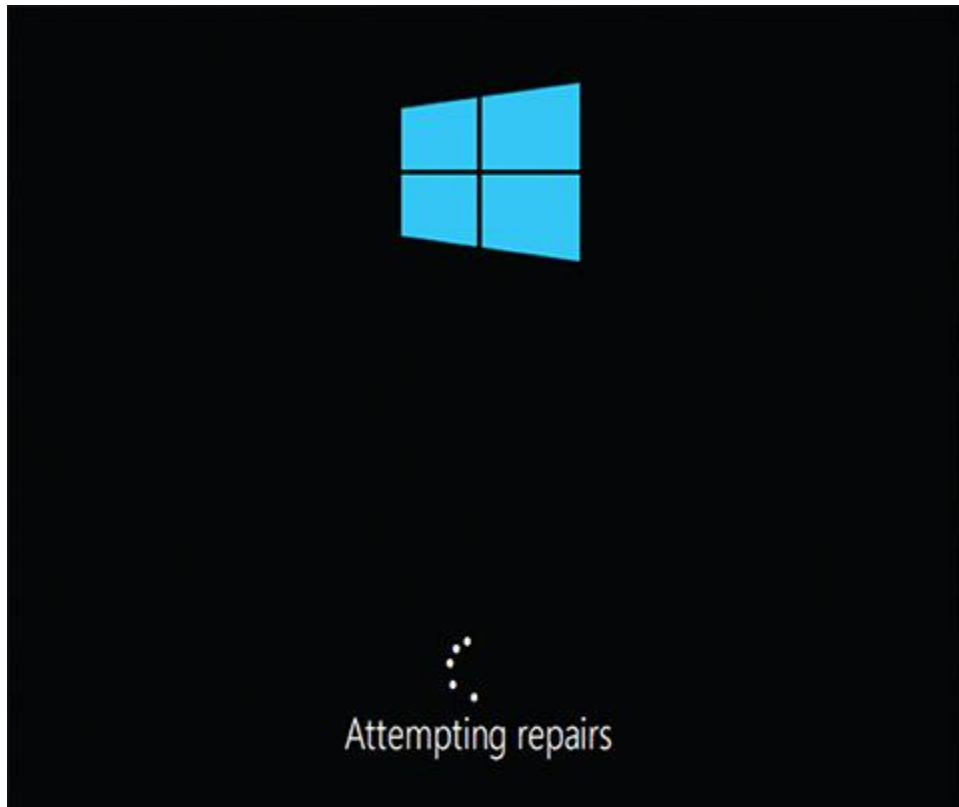
You can also use the shutdown command to remotely shut down computers over the network.

Here are the methods to launch Windows RE when Windows cannot start normally:

- **Windows detects startup problems and launches automatic diagnostics and repairs.** If you restart the computer several times within a few minutes or if Windows detects errors during startup, it automatically launches diagnostics (see [Figure 15-13](#)) and takes you through steps to attempt to repair the system. The process, called Automatic Repair or Startup Repair, includes running both Check Disk and System File Checker.

Figure 15-13

Windows automatically launches diagnostic and repair procedures after several restarts within a few minutes



If Automatic Repair fails, you're given the option to boot into Windows RE, where you have access to other troubleshooting tools.

Note 8

When you are trying to restart a computer while troubleshooting it yourself, you might find that Automatic Repair slows down or interferes with your efforts. In this case, you can disable Automatic Repair as follows: Open an elevated command prompt window, enter `bcdedit /set recoveryenabled no`, and then perform your own repair steps. You can re-enable Automatic Repair later with the command `bcdedit /set recoveryenabled yes`.

- **From the sign-in screen.** If you can get to the sign-in screen, press and hold the **Shift** key as you click **Power** and then **Restart**. Windows RE launches. (This method also works in most VMs.)

- **Reboot Windows several times.** Each time you see the Windows screen appear, turn off power to the computer, wait 10 seconds, and press the power button to turn on the computer. After you do this several times, turn on the computer, and Automatic Repair should launch followed by Windows RE.
- **Boot from a USB recovery drive, DVD system repair disc, or Windows setup DVD or USB drive.** These boot recovery media give you the option to launch Windows RE. You might have to adjust BIOS/UEFI settings to boot from these alternate media. To launch Windows RE from a Windows setup DVD or flash drive, click **Repair your computer** when you see the Windows Setup screen.
- **Press F8 during startup.** Earlier in the module, you learned how to configure Windows to enable F8 at startup. If it is enabled, press **F8** during startup to launch the Advanced Boot Options menu (refer back to [Figure 15-8](#)), which is part of Windows RE.

Applying Concepts

Exploring Windows RE Menus and Options

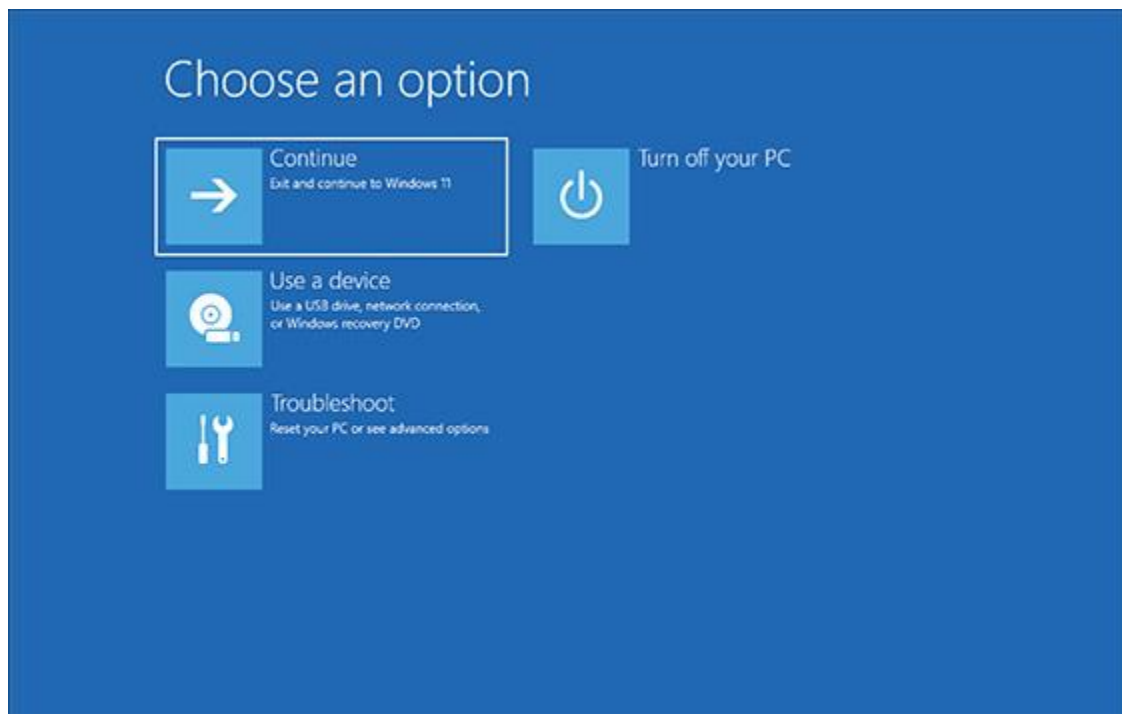
- **Est. Time:** 15 minutes
- **Core 2 Objective:** 3.1

Let's explore the menu screens in Windows RE, which are shown in green boxes in [Figure 15-7](#). Follow these steps to explore Windows RE menus:

1. **1**
Start Windows and use one of the methods listed earlier to launch Windows RE. The first screen you see after Windows RE launches is the Windows Startup Menu or the *Choose an option* screen (see [Figure 15-14](#)) for Windows 11. The Use a device option on the menu is new to Windows 11 and is used to recover a system from a network deployment server or other media.

Figure 15-14

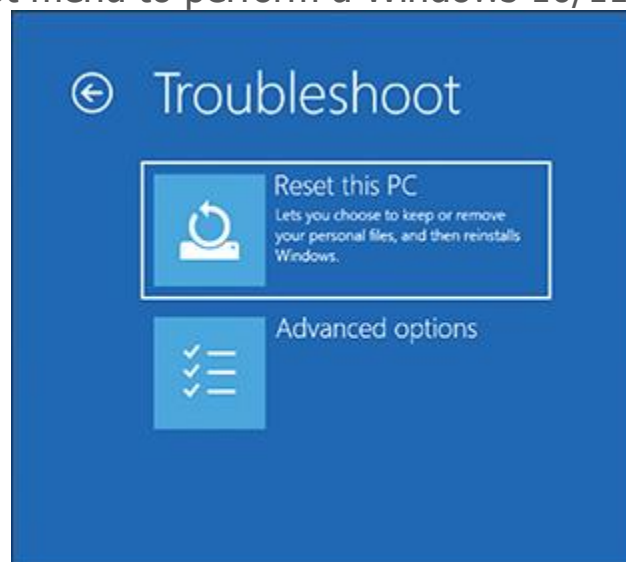
The Windows Startup Menu is the first screen you see after launching Windows RE



2. 2 Click **Troubleshoot** to see the Troubleshoot menu screen (see [Figure 15-15](#)).

Figure 15-15

Use the Troubleshoot menu to perform a Windows 10/11 reset



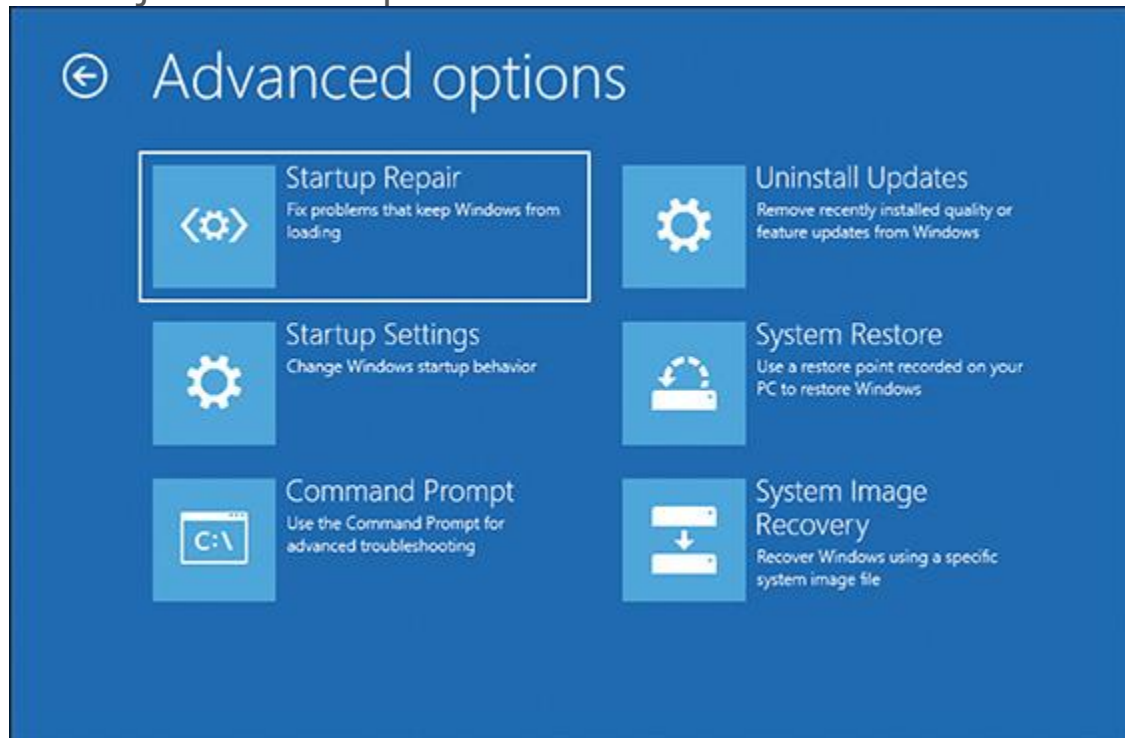
Note 9

Depending on the situation, you might see a seventh option on the Advanced options screen, which is UEFI Firmware Settings. Use this option to change settings in a computer's UEFI firmware.

3. 3 Click **Advanced options** to see the Advanced options screen in [Figure 15-16](#). Some options on this screen are standard, and a few vary depending on the current state of the system.

Figure 15-16

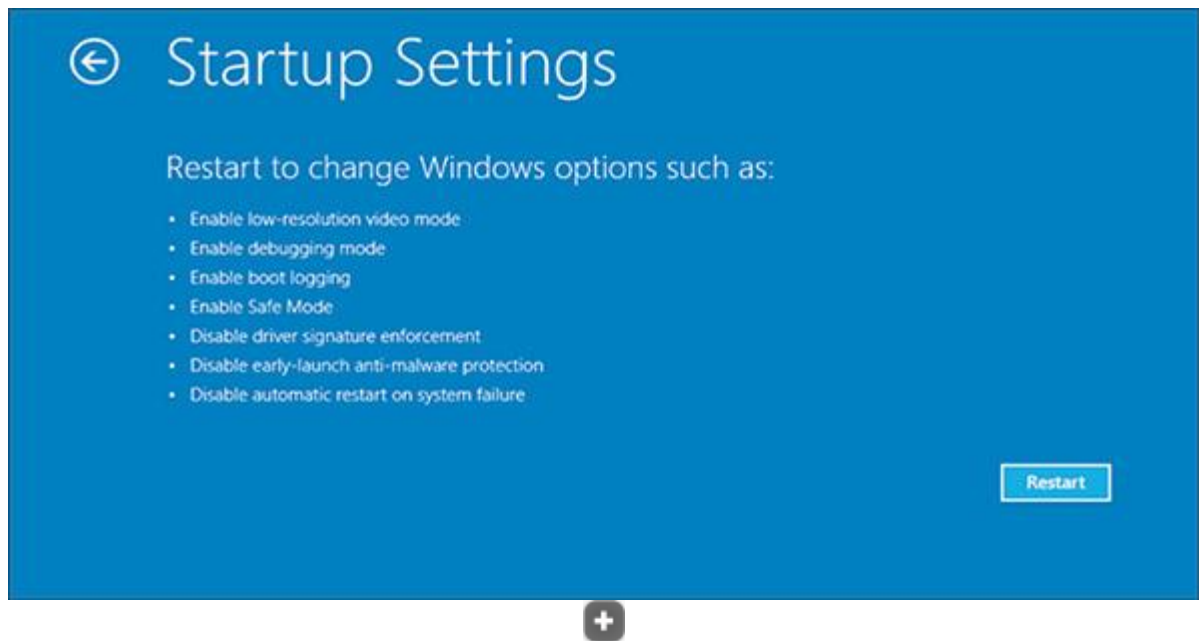
The option to uninstall updates is available because this computer recently received a major Windows update



4. **4** To get a command prompt, click **Command Prompt**. Here you can enter various commands to troubleshoot and solve problems. To exit the command prompt, enter the **exit** command. You are returned to the Advanced options screen.
5. **5** The Startup Settings option is available on the Advanced options screen shown in [Figure 15-16](#) because Windows RE was launched after a normal Windows startup. Click **Startup Settings** to see the startup options shown in [Figure 15-17](#).

Figure 15-17

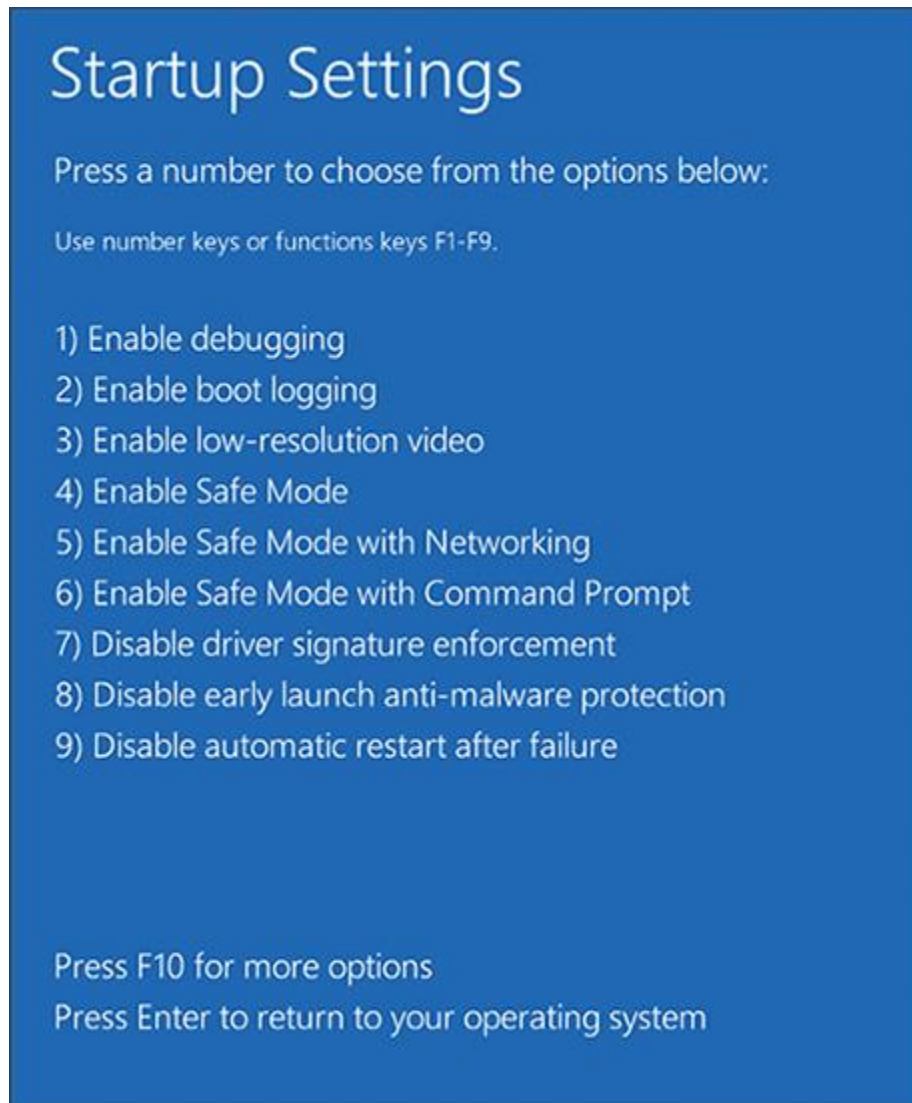
The Startup Settings menu gives options for how Windows starts up



6. **6** Click **Restart**. After the restart for Windows 10, another Startup Settings screen appears (see [Figure 15-18](#)), which has more options than the first one. Press numbers or function keys F1 through F9 to launch the tools on this screen. For Windows 11, after the restart, the Advanced Boot Options screen appears (refer back to [Figure 15-8](#)). Note the tools listed on either screen are the same tools, and you can also reach the Advanced Boot Options screen by pressing F8 at startup, assuming F8 has been enabled.

Figure 15-18

Press a function key or number to restart the system in a given mode



7. **7**

To return to the Windows Startup Menu shown earlier in [Figure 15-14](#), press **F10**. On the *Choose an option* screen, click **Continue** to reload Windows 10/11.

Next, we discuss some tools to repair Windows, including Startup Repair, Startup Settings, System Restore, uninstalling updates, and commands entered in a command prompt window.

15-3a Startup Repair

Core 2 Objective

- 3.1

Given a scenario, troubleshoot common Windows OS problems.

When addressing startup problems, the first tool to try is **Startup Repair**, which is a built-in diagnostic and repair tool. It can fix Windows system files

without changing Windows settings, user data, or applications. You can't cause additional problems with the tool, and it's easy to use.

To run Startup Repair in Windows RE, drill down to the Advanced options screen (refer back to [Figure 15-16](#)) and click **Startup Repair**. Windows RE examines the system, fixes problems, reports what it did, and might offer suggestions for further fixes. A log file of the process can be found at `C:\Windows\System32\LogFiles\SRT\SRTTrail.txt`.

15-3b Changing Startup Settings

Core 2 Objective

- 3.1

Given a scenario, troubleshoot common Windows OS problems.

The Startup Settings option on the Advanced options screen shown in [Figure 15-16](#) is available only when Windows RE is launched from the hard drive rather than other media. Following directions given earlier, launch Windows RE and drill down to the Windows 10 Startup Settings screen shown earlier, in [Figure 15-18](#) or the Windows 11 Advanced Boot Options screen shown earlier in [Figure 15-8](#). Here's a quick rundown of what these tools can do.

Press 1 or F1: Enable Debugging

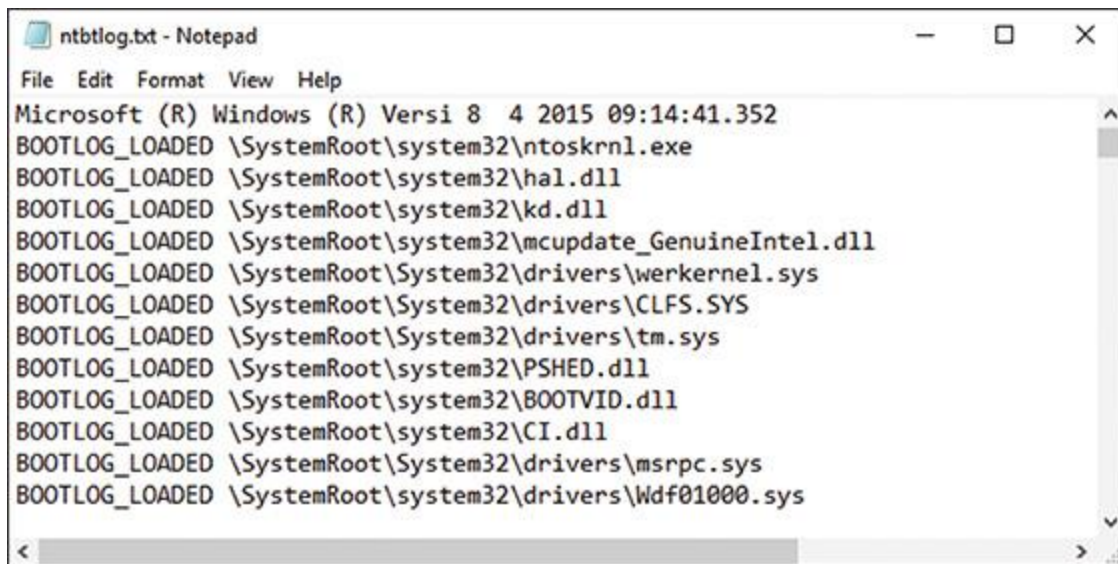
This tool moves system boot logs from the failing computer to another computer for evaluation. The computers must be connected by way of a serial port. For Windows 11, the option is Debugging Mode.

Press 2 or F2: Enable Boot Logging

Windows loads normally and all files used during the load process are recorded in a log file, `C:\Windows\ntbtlog.txt` (see [Figure 15-19](#)). Use this option to see what did and did not load during the boot. For instance, if you have a problem getting a device to work, check `Ntbtlog.txt` to see what driver files loaded. Boot logging is much more effective if you have a copy of `Ntbtlog.txt` that was made when everything worked as it should. Then you can compare the good load with the bad load, looking for differences.

Figure 15-19

A sample `C:\Windows\ntbtlog.txt` log file



```
ntbtlog.txt - Notepad
File Edit Format View Help
Microsoft (R) Windows (R) Versi 8 4 2015 09:14:41.352
BOOTLOG_LOADED \\SystemRoot\\system32\\ntoskrnl.exe
BOOTLOG_LOADED \\SystemRoot\\system32\\hal.dll
BOOTLOG_LOADED \\SystemRoot\\system32\\kd.dll
BOOTLOG_LOADED \\SystemRoot\\system32\\mcupdate_GenuineIntel.dll
BOOTLOG_LOADED \\SystemRoot\\System32\\drivers\\werkernl.sys
BOOTLOG_LOADED \\SystemRoot\\System32\\drivers\\CLFS.SYS
BOOTLOG_LOADED \\SystemRoot\\System32\\drivers\\tm.sys
BOOTLOG_LOADED \\SystemRoot\\system32\\PSHED.dll
BOOTLOG_LOADED \\SystemRoot\\system32\\BOOTVID.dll
BOOTLOG_LOADED \\SystemRoot\\system32\\CI.dll
BOOTLOG_LOADED \\SystemRoot\\System32\\drivers\\msrpc.sys
BOOTLOG_LOADED \\SystemRoot\\system32\\drivers\\Wdf01000.sys
```

Note 10

The Ntbtlog.txt file is also generated when you boot into Safe Mode.

Note 11

If Windows hangs during the boot, try booting using the Enable Boot Logging option. Then look at the last entry in the Ntbtlog.txt file. This entry might be the name of a device driver causing the system to hang.

Press 3 or F3: Enable Low-Resolution Video (640 × 480)

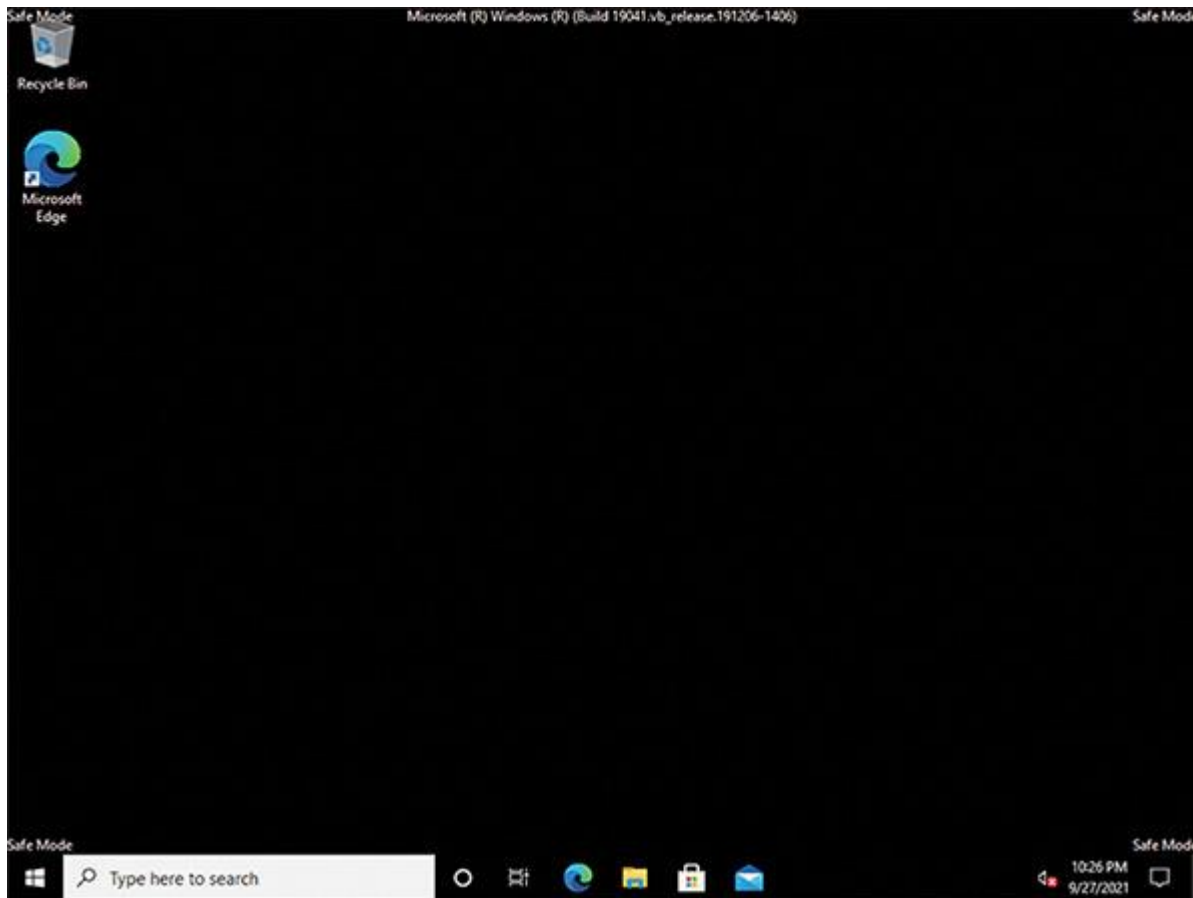
Use this option when the video settings don't allow you to see the screen well enough to fix a bad setting (for example, black fonts on a black background or a corrupted video driver). Booting in this mode gives you a very plain, standard video in VGA mode. You can then go to **Display settings**, correct the problem, and reboot normally. For problems with video drivers, open **Device Manager**, and update, roll back, or uninstall and reinstall the video drivers.

Press 4 or F4: Enable Safe Mode

With this option, the Safe Mode desktop appears (see [Figure 15-20](#)) after the system restarts and you sign in to Windows. Launching Safe Mode and then restarting the system again can sometimes solve a startup problem.

Figure 15-20

The Windows 10 Safe mode desktop



Other tasks you can try in Safe Mode include the following:

- Update Windows.
- Launch anti-malware software to scan the system for malware.
- Open Event Viewer to find events that are helpful in troubleshooting the system.
- Run the System File Checker command (`sfc /scannow`) to restore system files.
- Use Device Manager to roll back a driver.
- Use Memory Diagnostics (`mdsched.exe`) to verify memory.
- Use the `chkdsk /r` command to check for file system errors.
- Configure Windows for a clean boot on the next restart.

Recall from the module “[Troubleshooting Windows After Startup](#)” that you can also launch Safe Mode from the Boot tab on the System Configuration window, where Safe Mode is called Safe boot.



Exam Tip

The A+ Core 2 exam gives you a scenario and expects you to know when and how to use Safe Mode to help resolve a Windows startup problem.

Press 5 or F5: Enable Safe Mode with Networking

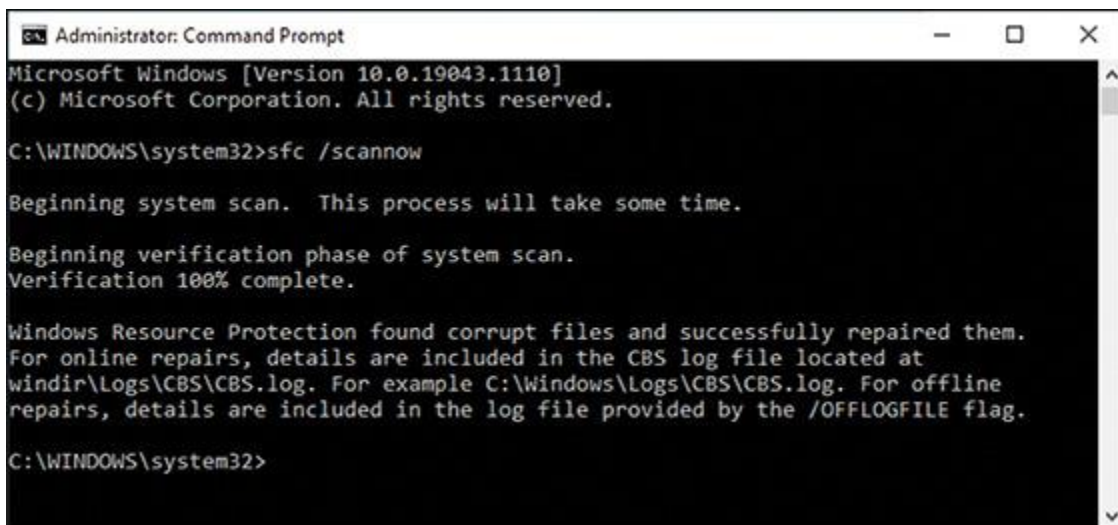
Use this option when you need access to the network to solve the problem. For example, you might need to download updates to your anti-malware software. Also use this mode when the Windows installation files are available on the network, rather than Windows setup media, and you need to access those files.

Press 6 or F6: Enable Safe Mode with Command Prompt

If Safe Mode can't start, try Safe Mode with Command Prompt, which doesn't attempt to load the graphical interface. At the command prompt, use the `sfc /scannow` command to verify system files (see [Figure 15-21](#)). If the problem is still not solved, you can use the `rstrui` command to launch System Restore and then follow the on-screen directions to select a restore point. However, as [Figure 15-22](#) shows, if restore points have not been previously made, System Restore cannot help. As you learn later in the module, you can also use this command prompt to restore a corrupted Windows registry from backups.

Figure 15-21

SFC finds and successfully repairs corrupted system files



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19043.1110]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>sfc /scannow

Beginning system scan. This process will take some time.

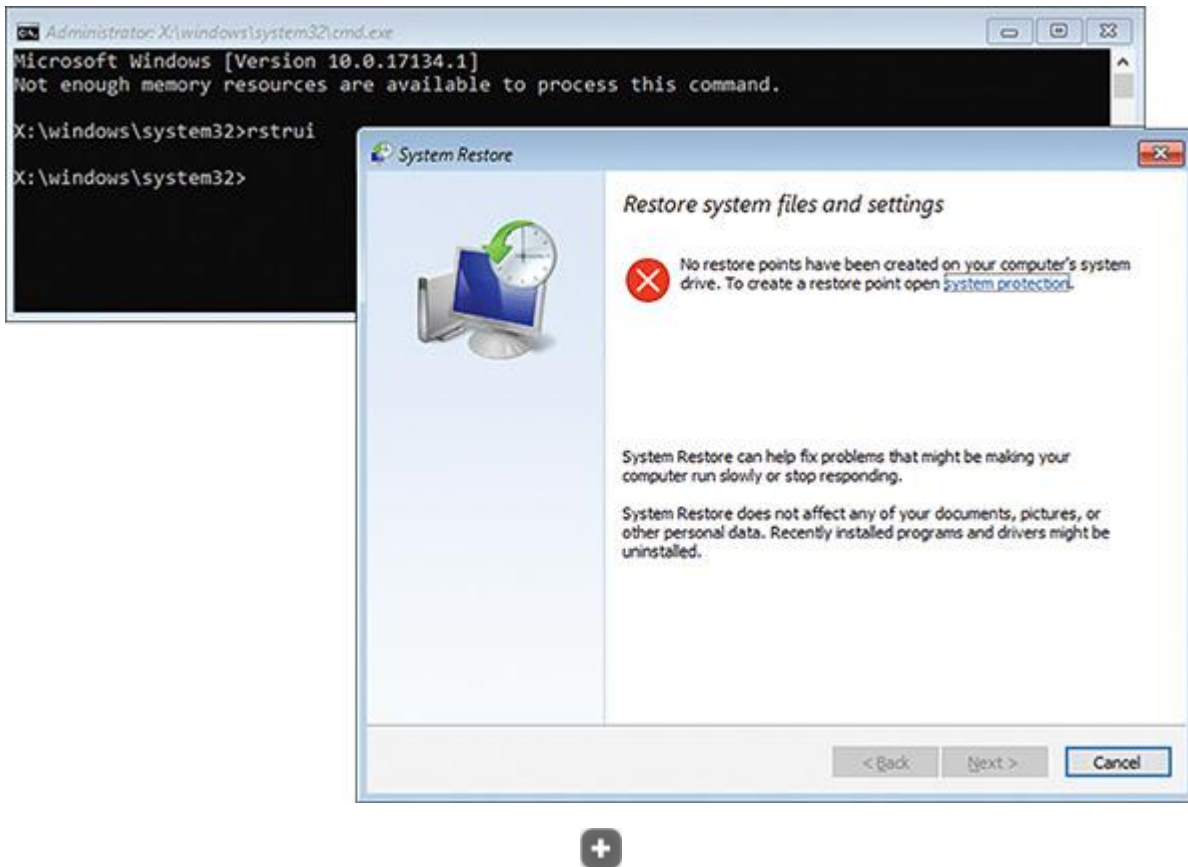
Beginning verification phase of system scan.
Verification 100% complete.

Windows Resource Protection found corrupt files and successfully repaired them.
For online repairs, details are included in the CBS log file located at
windir\Logs\CBS\CBS.log. For example C:\Windows\Logs\CBS\CBS.log. For offline
repairs, details are included in the log file provided by the /OFFLOGFILE flag.

C:\WINDOWS\system32>
```

Figure 15-22

Use System Restore after booting to Safe Mode with Command Prompt



Press 7 or F7: Disable Driver Signature Enforcement

All 64-bit editions of Windows require that kernel-mode drivers be digitally signed. Developers use this option to disable driver signature enforcement when they test kernel-mode device drivers that are not yet digitally signed. Use this option for troubleshooting with caution because doing so might allow malware drivers to load.

Note 12

Suppose a recent Windows update that includes device driver updates has caused the system to hang. When you try to fix the problem by applying a restore point, the system hangs again. The problem is caused by device drivers in conflict. To fix the problem, you can disable driver signature enforcement, undo system restore, and apply the restore point again. This time, it should work.

Press 8 or F8: Disable Early Launch Anti-Malware Protection

Windows allows anti-malware software to launch a driver before any third-party drivers are launched so it can scan these drivers for malware. Unless you're sure a driver is the problem, don't disable this security feature.

Press 9 or F9: Disable Automatic Restart after Failure

By default, Windows automatically restarts immediately after a blue screen of death (BSOD) stop error, which is described in more detail later in this

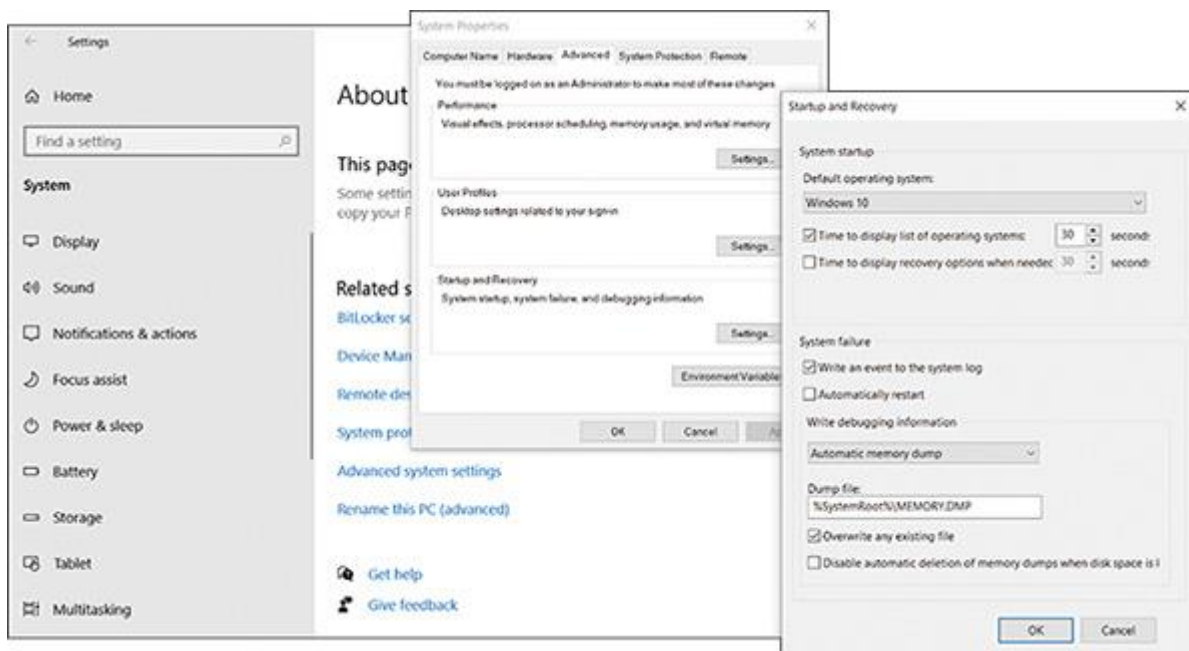
module. The error can cause the system to continually reboot rather than shut down. Press **F9** to disable automatic restarts and stop the rebooting.

Note 13

To permanently disable automatic restarts, right-click **Start**, click **System**, and in the About window, click **Advanced system settings**. In the Startup and Recovery group of the System Properties dialog box, click **Settings**. In the Startup and Recovery dialog box, uncheck **Automatically restart** (see [Figure 15-23](#)). Click **OK** twice and close the About window.

Figure 15-23

Permanently disable automatic restarts



Press F10: Return to the Startup Settings Screen

Press F10 to return to the Windows 10 Startup Menu screen shown previously in [Figure 15-14](#). For Windows 11, select **Start Windows Normally** to restart Windows.

Note 14

As you use these startup settings tools, be sure to reboot after each attempt to fix the problem to make sure it has not been resolved before you try another tool. To exit Windows RE and relaunch Windows, press Enter on the Startup Settings screen.

15-3c System Restore

Core 2 Objective

- 3.1

Given a scenario, troubleshoot common Windows OS problems.

Windows gives you several opportunities during the startup troubleshooting process to use System Restore to restore the system to an earlier point in time when a restore point was made. You can select System Restore from the Windows RE Advanced options screen (refer back to [Figure 15-16](#)). You can also perform System Restore in Safe Mode or from a command prompt with the `rstrui` command.

System Restore can cause problems of its own because Windows updates and updates to anti-malware software can be lost, and hardware devices and applications might need to be reinstalled. System Restore won't help if the file system is corrupted or the registry is trashed. In these situations, the command prompt might help.

15-3d Uninstall Updates

Core 2 Objective

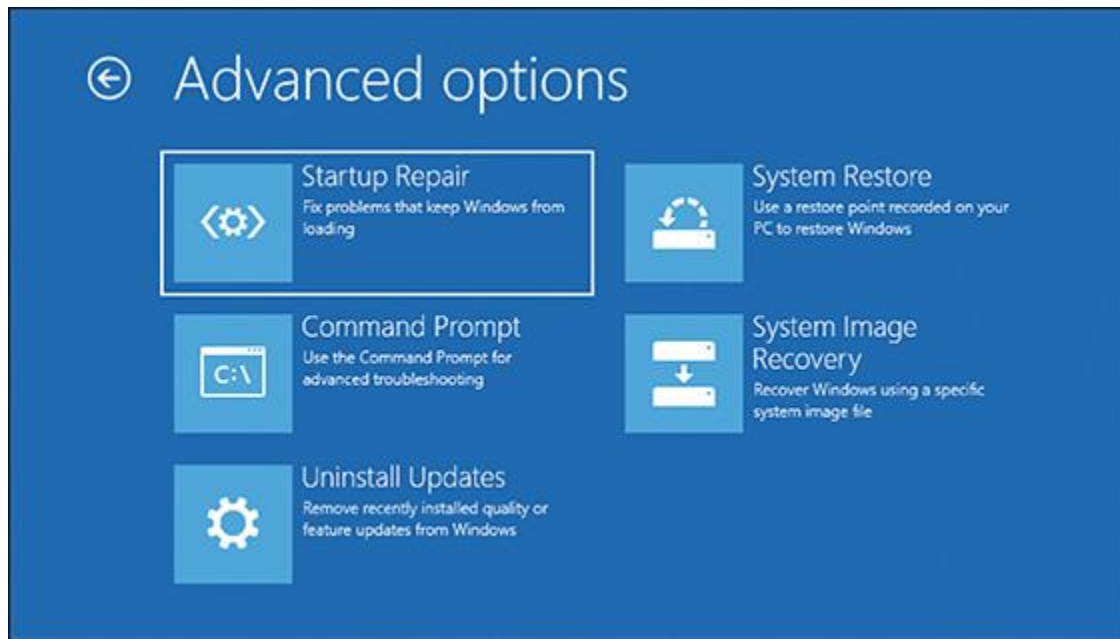
- 1.9

Given a scenario, perform OS installations and upgrades in a diverse OS environment.

If you suspect a recent Windows update is preventing Windows from starting, you can uninstall or **roll back updates**. To uninstall a Windows update, you would normally use the Update & Security window in the Settings app or the Programs and Features window in Control Panel. But if Windows refuses to start, use the Advanced options screen in Windows RE. If there are recent updates, the screen shows the option to Uninstall Updates (see [Figure 15-24](#)). Click **Uninstall Updates** and follow directions on-screen. This method works well when the system fails to start because a critical driver is corrupted. In a project at the end of this module, you learn to use the DISM commands to roll back an update that refuses to uninstall by normal means.

Figure 15-24

After recent Windows updates, the option to roll back an update appears on the Advanced options screen



15-3e The Command Prompt Window in Windows RE

Core 2 Objective

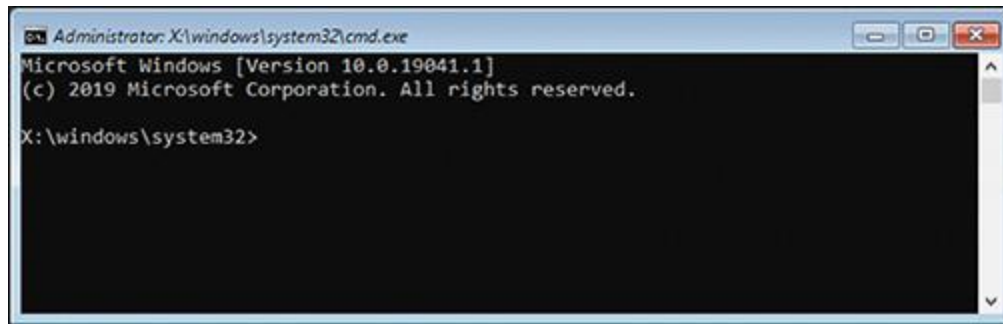
- 3.1

Given a scenario, troubleshoot common Windows OS problems.

Use the command prompt window in Windows RE when the graphical interface is missing or corrupted or when you want to use a specific command to fix a problem when Windows refuses to start. To access the Windows RE command prompt, click **Command Prompt** on the Windows Advanced options screen (refer back to [Figure 15-16](#)). After you have signed in with an account with administrative privileges, you have full read and write access to all files on all drives. The command prompt you first see in the window (see [Figure 15-25](#)) is `X:\windows\system32>` because Windows RE assigns drive X: to the drive containing the Windows installation. Many commands you learned about in module “[Maintaining Windows](#)” can be used at this command prompt.

Figure 15-25

The command prompt window in Windows RE



Next are some examples of how to use the Windows RE command prompt to repair a system. After you try each fix, reboot the system to see if the problem is solved before you try the next fix:

- **Manage data files and system files.** As you learned in the module [“Troubleshooting Windows After Startup,”](#) you can use the SFC or DISM commands to restore critical Windows system files. The cd, copy, rename, and delete commands can be used to manage data files and system files.
- **Repair the hard drive file system.** A corrupted file system can cause a failure to boot. To repair the file system, try the `chkdsk /r` command.
- **Wipe the hard drive clean to prepare for a new Windows installation.** If you decide the hard drive is so corrupted you must start over with a fresh installation of Windows, you can use the `diskpart` command to totally wipe the hard drive clean of everything, including the partitioning system, before you install Windows again using Windows setup media. You learned to do this in module [“Installing Windows.”](#)
- **Enable networking.** Networking is not normally available from the Windows RE command prompt. Use the `wpeinit` command to enable networking. The `wpeinit` command initializes Windows PE. Recall from the module [“Installing Windows”](#) that Windows PE is the preinstallation-environment operating system that is launched prior to installing Windows in a clean install and includes networking components.
- **Repair the BCD and boot sectors.** A failure to boot can be caused by a corrupted BCD. Startup Repair should fix the problem. But on some legacy systems, you will need to manually repair the BCD. Use the `bootrec` command to repair the BCD and boot sectors. Use the `bcdedit` command to manually edit the BCD. (Be sure to make a copy of the BCD before you edit it.) Use the `bootsect` command to repair a dual-boot system. To get helpful information about these commands, enter the command followed by `/?`, such as `bcdedit /?`. Some examples of the `bootrec` and `bcdedit` commands are listed in [Table 15-2](#).

Table 15-2

Bootrec and bcdedit Commands to Repair System Files and the File System

Command Line	Description
bootrec /scanOS	Scans the hard drive for Windows installations not stored in the BCD
bootrec /rebuildBCD	Scans for Windows installations and rebuilds the BCD
bootrec /fixboot	Repairs the boot sector of the system partition
bootrec /fixmbr	Repairs the MBR for hard drives using the MBR partitioning system
bcdedit /enum	Displays the contents of the BCD



Although a Startup Repair should solve the problem when you get an error message at startup that “Bootmgr is missing,” rebuilding the BCD store should also be able to resolve the same problem on a legacy BIOS and MBR system.

15-4 Tools to Reinstall Windows

Core 2 Objectives

- 1.9

Given a scenario, perform OS installations and upgrades in a diverse OS environment.

- 3.1

Given a scenario, troubleshoot common Windows OS problems.

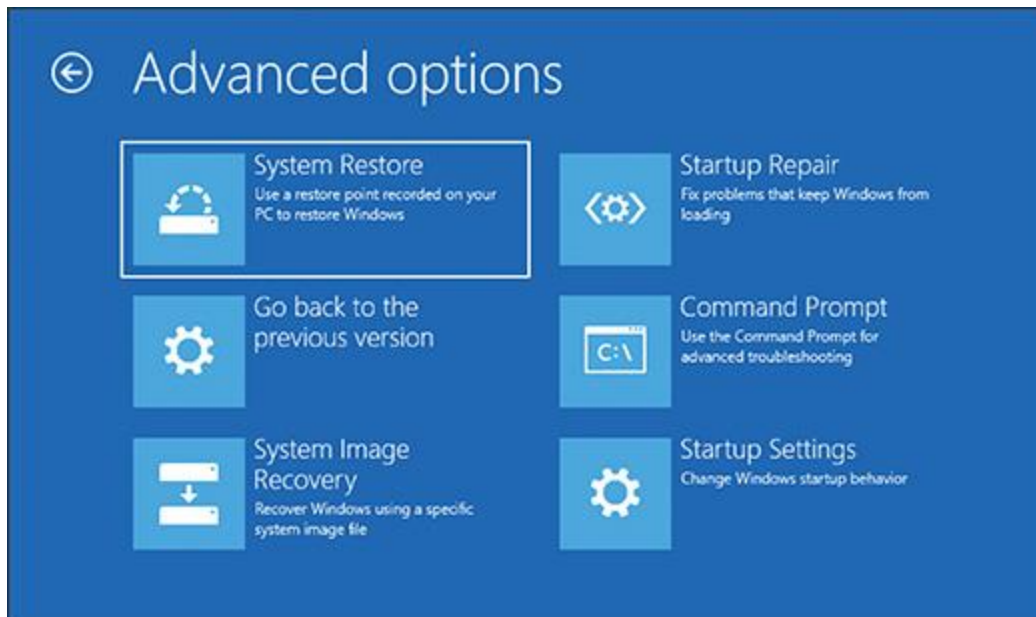
After you have made reasonable efforts to repair a Windows installation, your next option is to reinstall Windows. The tools discussed in this section of the module affect the entire Windows installation on a computer rather than a few files or settings. Look back at [Figure 15-7](#) and notice that these tools to reinstall Windows are shown in blue boxes; you can also see how to reach each tool. Some of these options allow you to keep personal data, and other options remove that data; the tools are listed here, starting with the least intrusive solutions:

- 1.

Go back to the previous version of Windows. After you have upgraded to Windows 10/11 and the system is giving problems, you can go back to the previous version of Windows. This option is available on the Advanced options screen after upgrading to Windows 10/11 if the upgrade is not too old and the Windows.old folder is present. See [Figure 15-26](#). In addition, you’ll find the option in the Settings app: go to **Update & Security** and click **Recovery**.

Figure 15-26

The option to go back to a previous version is available because this computer was recently upgraded to Windows 10



- 2.

Windows 10/11 repair installation. Install Windows 10/11 as an upgrade over the existing installation, keeping personal data, apps, Windows settings, and device drivers.

- 3.

Reimage Windows 10/11. Use a system image or deployment image to replace everything on the Windows volume. Current user data, Windows settings, apps, and device drives are lost.

- 4.

Install Windows 10/11 from the OEM recovery partition. Laptops, all-in-ones, and brand-name computers may have an OEM recovery partition on the hard drive that can be used to restore the system to factory state. Some manufacturer procedures allow user data to be kept.

- 5.

Windows 10/11 reset. Do a clean Windows 10/11 installation from the Microsoft cloud, recovery media, or the recovery partition on the hard drive. User data and preinstalled apps in a recovery partition can be restored.

- 6.

Windows 10/11 clean install from setup media. This method, which is covered in module "[Installing Windows](#)," may allow you to keep user data on the hard drive.

Let's see how the Windows repair installation, reimage, OEM recovery partition, and reset work.

15-4a Windows 10/11 Repair Installation

Core 2 Objective

- 1.9

Given a scenario, perform OS installations and upgrades in a diverse OS environment.

If you're having problems with Windows updates or basic Windows functionality but you can still boot into Windows, you might consider performing a repair installation, also known as a repair upgrade or in-place upgrade. A **repair installation** is a nondestructive installation of Windows 10/11 over an existing Windows installation. This is not the same as a full reinstall because the Windows volume will not be reformatted. Just as with an upgrade from Windows 8 to Windows 10, you can keep personal files, apps, and Windows settings. Essentially, you trick the machine into thinking it's being upgraded while potentially repairing the Windows installation.

Keep these points in mind when doing a repair installation:

- Create Windows setup media, on either DVD or USB, or save an ISO file on the local hard drive.
- Make sure that you can fully boot into Windows 10/11. If you can't, you'll have to use a different troubleshooting tool.
- Even though all data, apps, and settings should be protected in a repair installation, make a backup just in case.
- Gather all product keys for all installed apps to make reinstallation of these apps easier should it become necessary.

Note 15

Belarc Advisor (belarc.com) is a free tool that is quick and easy to use. It will produce a list of all installed devices and apps along with their product keys if that information is available. Print a copy of the report, and keep it in a safe place.

Applying Concepts

Performing a Repair Installation

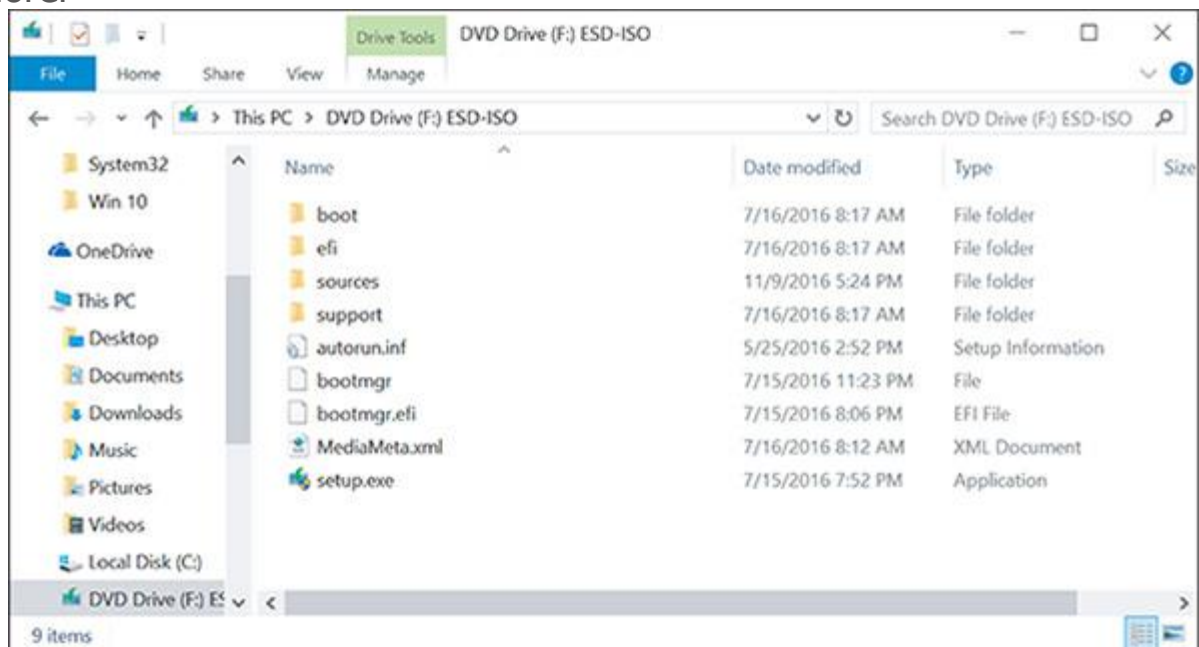
- **Est. Time:** 30 minutes
- **Core 2 Objective:** 3.1

The easiest way to perform a repair installation is to start with an ISO file created by the Media Creation Tool, as described in the module "[Installing Windows](#)." Complete the following steps:

1. **1**
Sign in to Windows using an administrator account. Back up all personal data using one of the methods you learned about in the module “[Maintaining Windows](#).”
2. **2**
Following steps in the module “[Installing Windows](#),” download the correct ISO file for the Windows installation you’re currently using on the computer to be repaired.
3. **3**
In Explorer, double-click the ISO file that you created with the Media Creation Tool. This mounts the image and shows the included files.
4. **4**
Double-click **setup.exe**, as shown in [Figure 15-27](#). Click **Yes** in response to the UAC dialog box, and follow the directions on-screen.

Figure 15-27

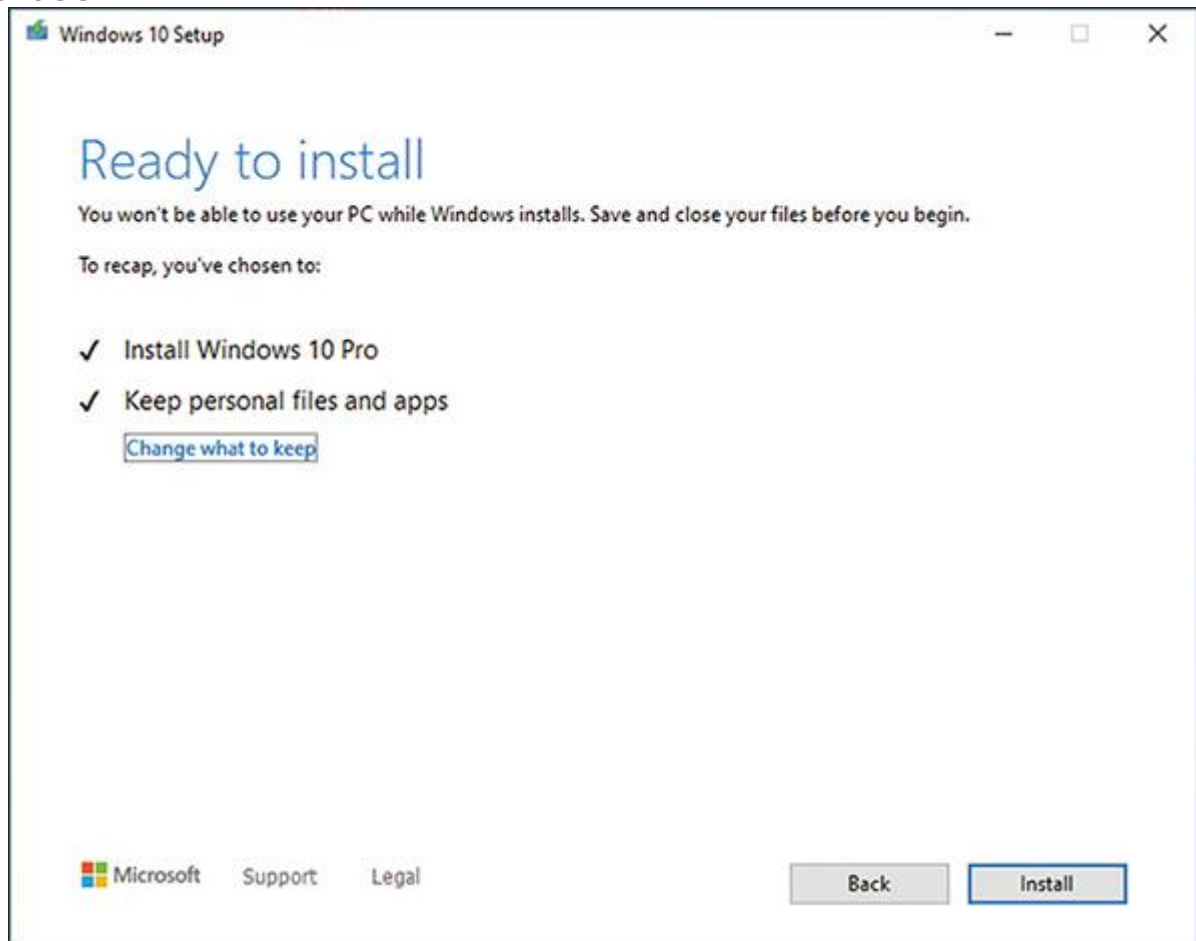
To begin the repair installation, double-click setup.exe on the virtual DVD in Explorer



5. **5**
When you get to the *Choose what to keep* window, decide whether to keep personal files and apps, personal files only, or nothing. Sometimes setup makes these decisions for you and skips directly to the *Ready to install* window.
6. **6**
On the *Ready to install* window, make sure **Keep personal files and apps** appears and is checked, as shown in [Figure 15-28](#). If it does not, click **Change what to keep** and select **Keep personal files and apps**, and then click **Next** to return to the *Ready to install* window. Click **Install** to begin the installation process, which will take a while and require several restarts. Enjoy a cup of tea or coffee while you wait.

Figure 15-28

You can keep user data and settings and third-party apps during a repair installation



7. **7**

When the sign-in screen appears, sign in to Windows. Once you see the desktop, all your files, apps, and settings should still be in place.

15-4b Applying a Windows System Image

Core 2 Objectives

- 1.9

Given a scenario, perform OS installations and upgrades in a diverse OS environment.

- 3.1

Given a scenario, troubleshoot common Windows OS problems.

You learned how to create a system image in the module “[Maintaining Windows](#).” System image recovery, sometimes called a **reimage**, tends to be

an all-or-nothing recovery option with which you replace the entire contents of a hard drive with whatever operating system state and personal data are saved in the system image. It recovers all personal files, system files, and installed apps that were in place at the time the system image was most recently created or updated. If your system image is updated regularly, this option could work very well for you when repairing or replacing hardware, such as a failed hard drive. However, if a software-related problem has been building for a while, a recently updated system image won't necessarily fix the root of the problem.

To reimage Windows using a system image file stored locally (for example, on a flash drive or on the local network,) reboot the computer into Windows RE, drill down to the **Advanced options** screen (refer back to [Figure 15-16](#)), and select **System Image Recovery**.

Recall from the module "[Installing Windows](#)" that in an enterprise environment, you can install Windows from a deployment image on the network. Go into BIOS/UEFI setup and look for an advanced setup screen to enable PXE Support. Then reboot the computer to the network where it finds and loads Windows PE on the deployment server. The computer then boots to the Preboot eXecution Environment (PXE), and PXE then searches for a server on the network to provide the deployment image.



Exam Tip

The A+ Core 2 exam expects you to know how to use a preinstallation environment and a recovery image to reimage Windows.

15-4c OEM Factory Recovery Partition

Core 2 Objectives

- 1.3

Given a scenario, set up and configure accessories and ports of mobile devices.

- 1.9

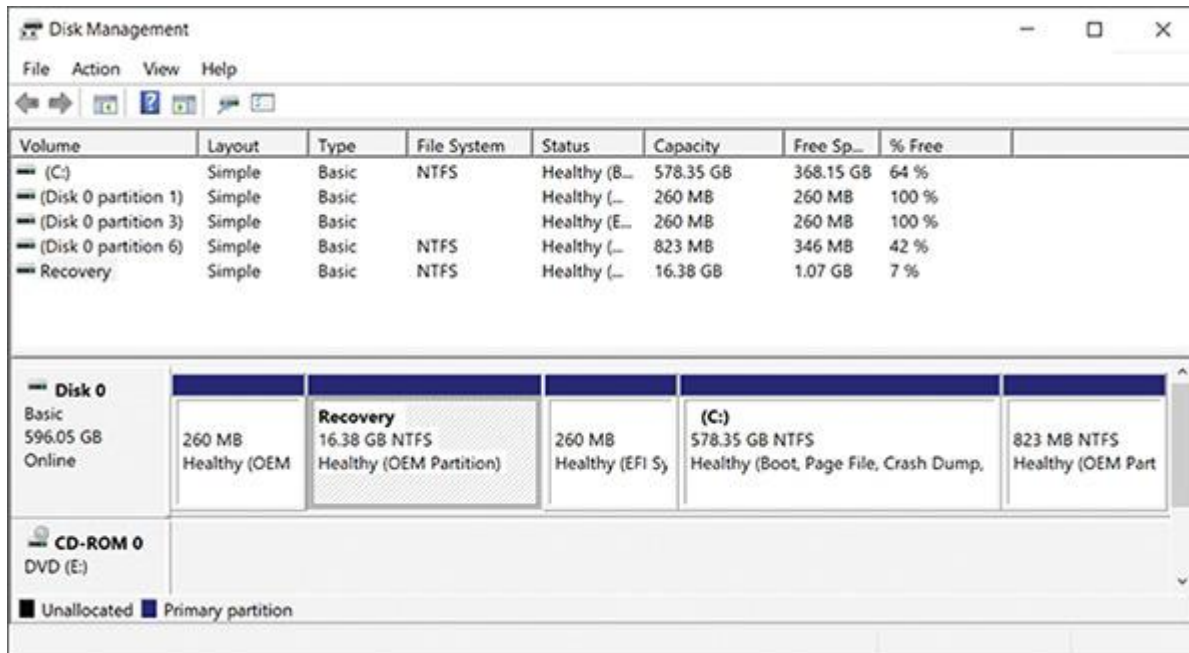
Given a scenario, perform OS installations and upgrades in a diverse OS environment.

Laptops, all-in-one computers, and brand-name desktops come with the OS preinstalled at the factory. This OEM (original equipment manufacturer) build of the OS is likely to be customized, and for laptops, the drivers might be specific to proprietary devices installed in the laptops.

Recall that a laptop or brand-name computer is likely to have a recovery partition on the hard drive used to restore the system to its factory state. This partition might or might not be hidden. For example, [Figure 15-29](#) shows the Disk Management information for a hard drive on one laptop that has a 16.38 GB recovery partition.

Figure 15-29

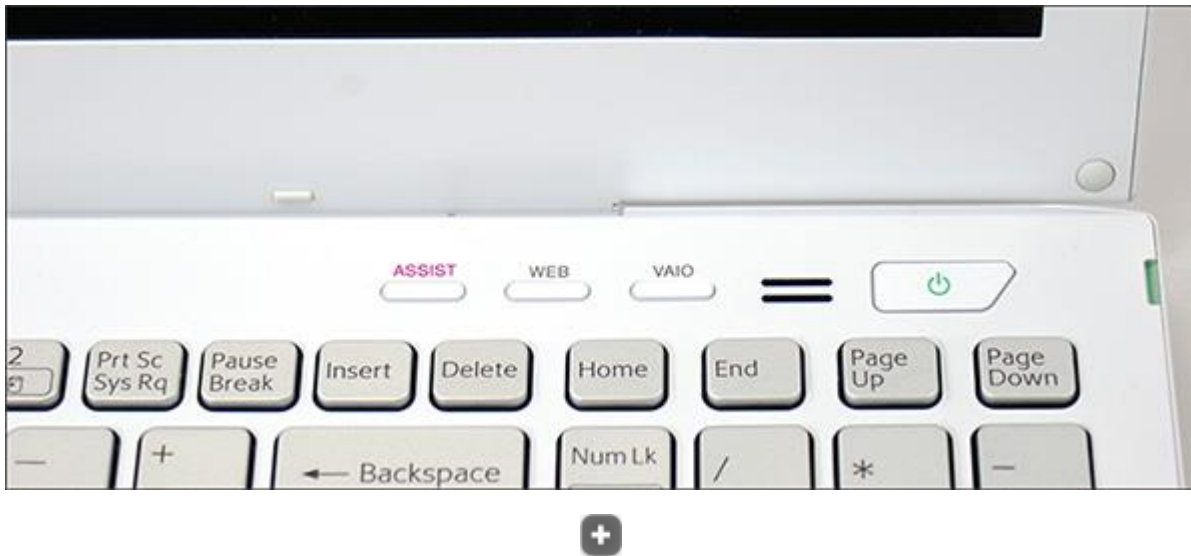
This laptop hard drive has a 16.38 GB recovery partition that can be used to recover the system



To know how to access the recovery tools stored on a recovery partition, see the manufacturer's website or look for a message at the beginning of the boot, such as "Press ESC for diagnostics" or "Press F12 to recover the system." For one Sony laptop, you press the red **ASSIST** button during the boot (see [Figure 15-30](#)). When you press the key or button, a menu appears with options to diagnose the problem, to repair the current OS installation, or to completely rebuild the entire hard drive to its factory state.

Figure 15-30

For this laptop, press the ASSIST button during the boot to launch programs on the recovery partition



If the laptop doesn't have a recovery partition or if the partition is corrupted, look for the option to download recovery media from the manufacturer's website, and use it to create a bootable USB flash drive or DVD. You can then use the media to install Windows to its factory state.

Note 16

When you first become responsible for a laptop, use a USB flash drive to make a Windows recovery drive that includes the OEM recovery partition in case you must replace the laptop's hard drive. Know that if the laptop is more than three years old, the manufacturer might no longer provide the recovery media. You learned how to create a recovery drive earlier in the module. It is also important to save a copy of the power-on password in a safe place.

! Caution

Before upgrading a laptop to Windows 10/11, make sure the laptop manufacturer provides Windows 10 or Windows 11 drivers for laptop components.

15-4d Windows 10/11 Reset

Core 2 Objective

- 1.9

Given a scenario, perform OS installations and upgrades in a diverse OS environment.

A Windows 10/11 reset performs a clean installation of Windows with three options, as shown in [Table 15-3](#).

Table 15-3

Windows 10/11 Reset Options

	Keep My Files	Remove Everything	Reinstall Preinstalled Apps
Option 1: My files and no bloatware	Yes	No	No
Option 2: My files with factory state	Yes	No	Yes
Option 3: Factory state	No	Yes	Yes



All options remove apps and drivers installed by the user and all changes made to settings. After the reset, a list of apps deleted from the system is stored on the Windows desktop. You'll then need to reinstall the apps you want to keep. Here are the ways in which the options differ:

- Option 1 keeps all personal files. All apps and settings are lost, and you get a clean installation of Windows.
- Option 2 keeps all personal files. If the computer came from a manufacturer with Windows 10/11 preinstalled, you can decide to restore the preinstalled apps (sometimes called bloatware) from the manufacturer. The apps, drivers, and diagnostics programs are reinstalled using the recovery partition on the hard drive or a recovery drive you created earlier.
- Option 3 removes everything on the drive, and you can also choose to clean the drive. Then Windows is reinstalled. If a recovery partition or recovery drive is present, the system is restored to factory state. This is an excellent choice if you are planning to sell, donate, or recycle your computer.

Applying Concepts

Resetting a Windows 10/11 Computer

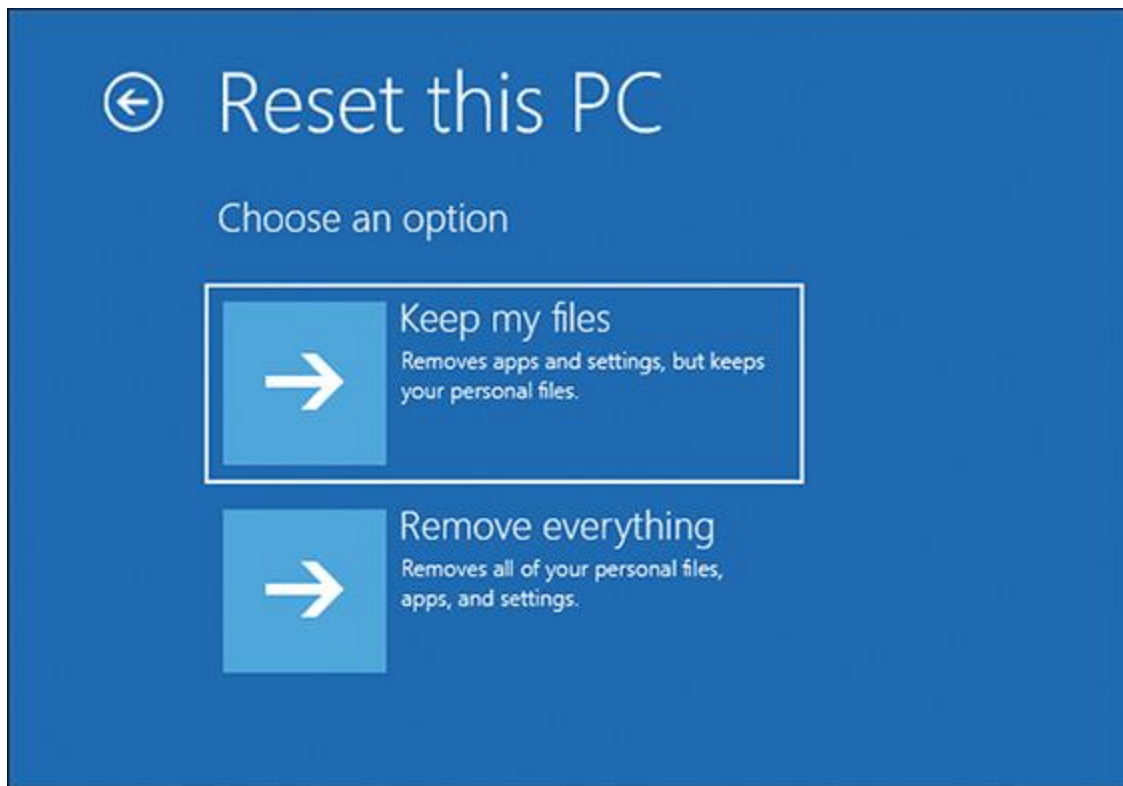
- **Est. Time:** 15 minutes
- **Core 2 Objective:** 3.1

If you are not able to start Windows, you can use Windows 10/11 setup media or a recovery drive to launch Windows RE. Do the following:

1. **1**
Drill down to the Troubleshoot screen (refer back to [Figure 15-15](#)), and click **Reset this PC** to start the reset.
2. **2**
On the next screen (see [Figure 15-31](#)), you can choose to keep personal files or remove everything.

Figure 15-31

Windows reset can keep personal files or remove everything on your computer and reinstall Windows

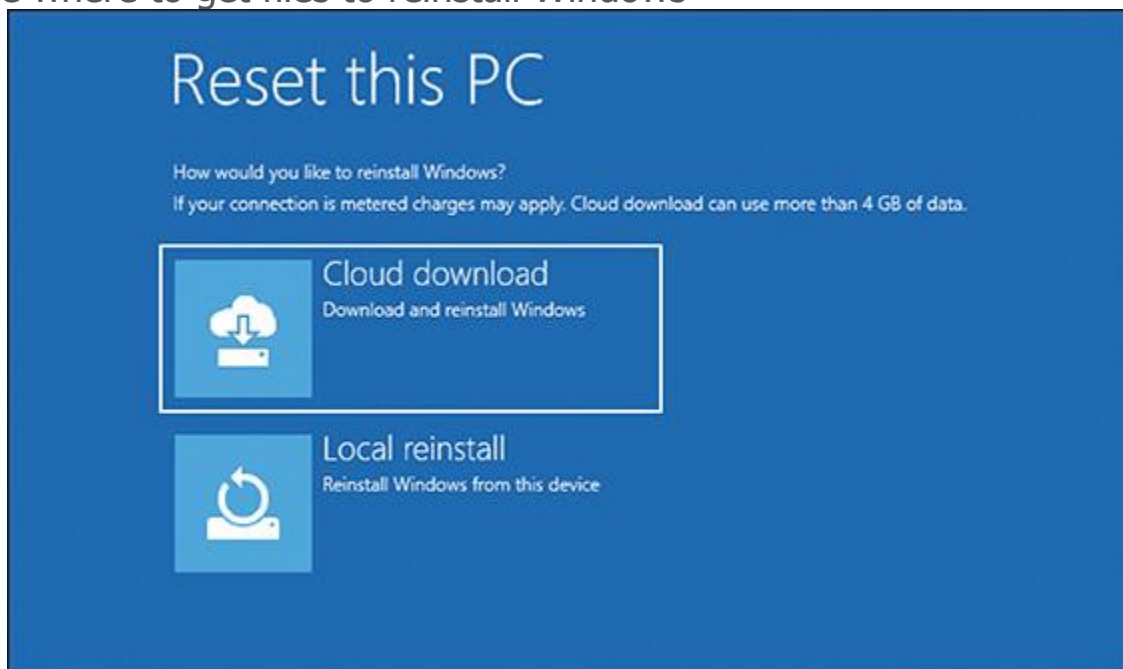


3. **3**

On the next screen (see [Figure 15-32](#)), you decide where installation files come from. If a recovery partition or recovery drive that has Windows 10/11 on it is present, you are next asked whether you want to restore preinstalled apps. Finally, click **Reset** to start the process.

Figure 15-32

Choose where to get files to reinstall Windows



4. **4**

If Windows can start, you can use the Settings app to reset Windows. In the Windows 10 Settings app, open the **Update & Security** window, and click **Recovery**, as shown earlier, in [Figure 15-12](#). Under *Reset this PC*, click **Get started** and follow the directions on-screen. For Windows 11, in the Settings app, open the **System** window, click **Recovery**, click **Reset PC**, and follow directions on-screen.

15-5 Troubleshooting Windows Startup

Core 2 Objective

- 3.1

Given a scenario, troubleshoot common Windows OS problems.

And now the fun begins! With your understanding of the boot process and Windows tools for troubleshooting startup in hand, let's work through a bunch of errors and problems that can affect Windows startup and see what can be done about them. As with any computer problem, follow the troubleshooting steps you've learned in previous modules:

1. To identify the problem, interview the user, back up important data or verify that you have current backups, research and identify any error messages, and determine what has just changed that might be the source of the problem.
2. Establish your theory of probable cause. Be sure to search the web on error messages and symptoms. You're then ready to
3. test your theory and
4. resolve the problem. After you think the problem is solved, and
5. verify all is working as it should, implement preventive measures.
Don't forget to
6. document your findings, actions, and outcomes.

When you know the source of the problem, decide which tool will be the least invasive to use yet still fix the problem. If that doesn't work, move on to the next tool. Remember that the tools are described earlier in the module in order from least to most invasive.

15-5a Important Data on the Hard Drive

Core 2 Objective

- 3.1

Given a scenario, troubleshoot common Windows OS problems.

Working on a computer problem should always start with the most important question: Is there important data on the hard drive that's not

backed up? Even if data is lost or corrupted, you might be able to recover it using Windows tools, third-party file recovery software, or commercial data recovery services. One good product is GetDataBack by Runtime Software (runtime.org), which can recover data and program files even when Windows cannot recognize the drive.

For less than \$30, you can purchase a SATA-to-USB converter kit (see [Figure 15-33](#)) that includes a data cable and power adapter. You can use one of these kits to temporarily connect a desktop or laptop hard drive to a USB port on a working computer. Set the drive beside your computer and plug one end of the data cable into the drive and the other into the USB port. The AC adapter supplies power to the drive. While power is getting to the drive, be careful not to touch the circuit board on the drive.

Figure 15-33

Use a SATA-to-USB converter to recover data from a drive using a SATA connector



Using Explorer, you can browse the drive and copy data to other media. After you have saved the data, you can use diagnostic software from the hard drive manufacturer to examine the drive and possibly repair it or return the drive to its own computer and start troubleshooting there.

15-5b Error Messages and Problems

Core 2 Objective

- 3.1

Given a scenario, troubleshoot common Windows OS problems.

Problems that prevent Windows from booting can be caused by hardware, device drivers, services, applications, or Windows. This section covers what to do when error messages appear on a black or blue screen or when Windows gets corrupted.

Startup Error Messages on a Black Screen

Generally, problems that present as white text on a black screen are caused by hardware. Here are some possible error messages:

- No OS found
- A disk read error occurred
- Invalid boot disk
- Hard drive not found
- Disk boot failure
- No boot device found

Here is what's happening and what to do about it:

1. Start with the error message. Research the text shown on the screen so you understand the problem and get solutions from trusted websites.
2. If you see spinning white dots on a black screen, Windows may be installing updates before it launches. Wait. It may take some time for the update installations to complete. If the system hangs indefinitely, the updates might be causing a problem. If a reboot doesn't solve the problem, boot into Windows RE, and roll back updates or return to a previous version of Windows. Next try System Restore.
3. Consider that startup BIOS/UEFI might not be able to communicate with the hard drive. Check BIOS/UEFI setup for the boot sequence. Update the boot order so you can try booting from another device.
4. Try going into BIOS/UEFI setup and disabling any quick boot features. This causes BIOS/UEFI to do a more thorough job of POST and reports more information on the screen as it performs POST.
5. Windows might halt and show a black screen when it encounters a video problem at startup. Try restarting the system in Safe Mode, as you learned to do earlier in the module. Then check Event Viewer for clues, update Windows, use Device Manager to roll back drivers or disable or uninstall the video adapter, and use System File Checker. If you cannot boot into Safe Mode, launch Windows RE, and use Startup Repair, Memory Diagnostics, and the `chkdsk /r` command to check Windows, memory, and the hard drive.
6. The hard drive might be failing. To recover data from the drive, move it to another computer, and install it as a second hard drive.

Problems with User Profiles

If Windows bogs down right after the user signs in, the problem might be with loading the user profile. For a slow profile load, the user might see a

black screen with spinning dots for several minutes. To fix the problem, try these tasks listed in the least invasive order:

1. Make sure Windows updates are applied.
2. Use the `sfc /scannow` command to fix problems with system files.
3. Reduce startup items. Compare the time to load a user profile when starting Windows normally and during a clean boot.
4. Apply a restore point that was created before the problem started.
5. Perform a repair installation.
6. Create a new user profile. You can copy user data files from the old profile into the new user profile namespace. (Locations of these files are given in the module "[Troubleshooting Windows After Startup](#).”)

If the user profile gets corrupted, it might not load at all, and you might see the error message, “The User Profile Service failed the logon.” To rebuild the user profiles, do the following to repair Windows system files that affect the corrupted profiles:

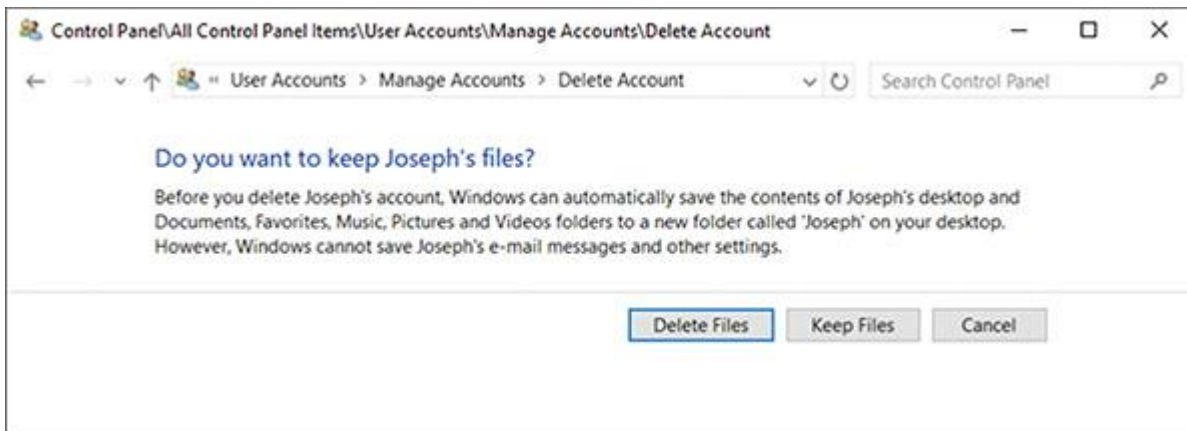
- Do as many of the previous steps as you can do when a single user profile is slow to load.
- Following directions given in the module "[Troubleshooting Windows After Startup](#),” use the DISM commands to repair corrupted Windows system files.
- Perform a Windows reset. Be sure to back up data before you do a reset.

Sometimes you can recover a user account by deleting it without deleting its files and then creating a new one with the same name.

To delete the account and keep its files, open **Control Panel**, click **User Accounts**, select the account, and click **Delete the account**. In the Delete Account window (see [Figure 15-34](#)), click **Keep Files** and then click **Delete Account**. The files are stored in a folder on your desktop, and the account and its settings are deleted. Create a new account with the same name. Then you can copy the files saved to your desktop folder to the new user profile namespace.

Figure 15-34

Delete a user account and its settings, and keep the files in the user profile



If this doesn't work, you can edit the registry to delete an old profile or repair a corrupted one:

- 1.

Launch the **Registry Editor** and back up this registry key:

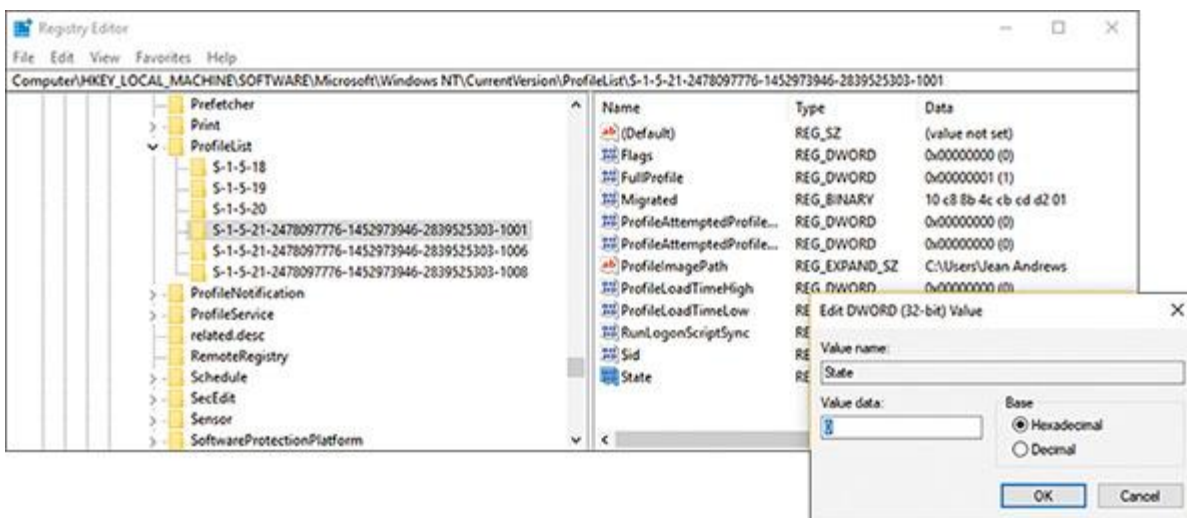
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

- 2.

Drill down into each S-1-5 folder in the key in Step 1 until you find the correct user profile in the ProfileImagePath subkey (see [Figure 15-35](#)). If the profile has a State subkey, set it to **0**, as shown in the figure. If the profile has a RefCount subkey, set it to **0**.

Figure 15-35

Set the State subkey value to 0



- 3.

Close the Registry Editor, and restart the computer.

Note 17

If you're searching for the correct S-1-5 folder and it has .bak in the name, remove .bak from the folder name. To rename a folder, right-click it and click Rename.

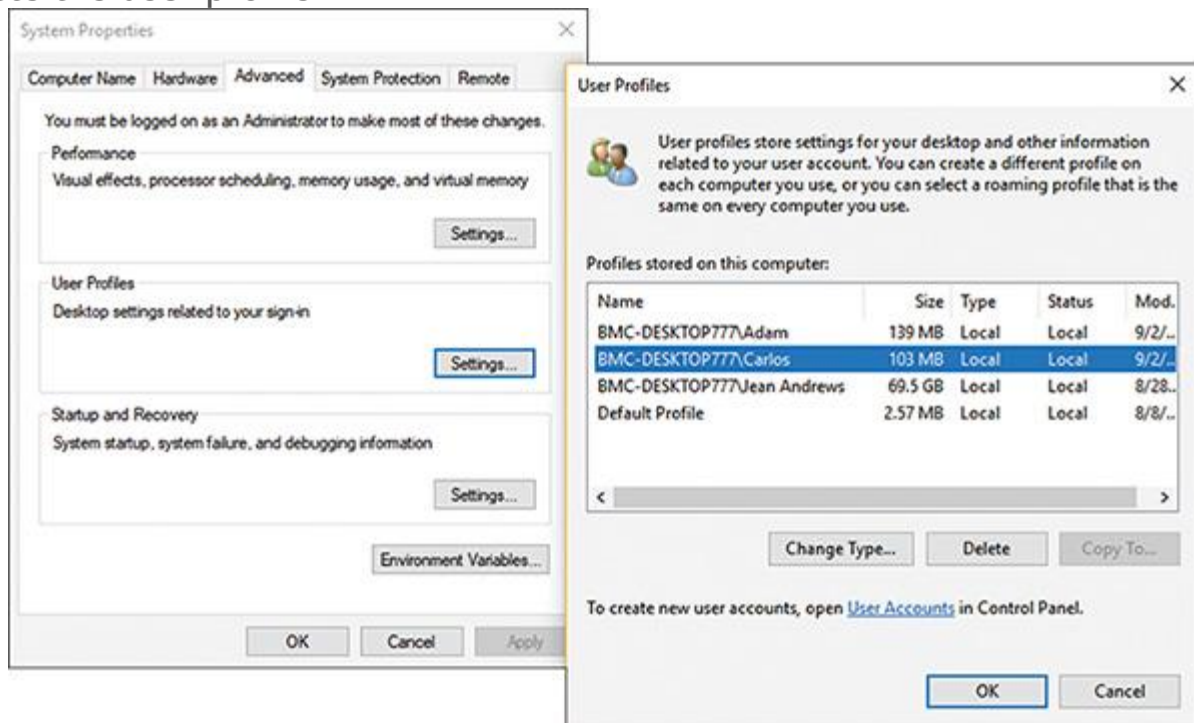
If you see two S-1-5 folders with the same name, except one has .bak at the end, you must switch the names: First rename the folder that does not contain .bak to .hold. Then remove the .bak from the other folder name. Next, rename the .hold folder to .bak. Then edit the S-1-5 folder that does not have .bak in the name.

If you still have problems with a user profile, you can follow these steps to delete the profile:

1. **1** Manually copy any important data files in the user profile namespace to a new location. Recall that you can find these files in the C:\Users*username* subfolders.
2. **2** Go to **Control Panel** and open the **System** window. Click **Advanced system settings**. In the System Properties dialog box, select the **Advanced** tab, and click **Settings** under User Profiles. See [Figure 15-36](#). In the list of user profiles, select the profile and click **Delete**.

Figure 15-36

Delete the user profile



Launch the **Registry Editor**, back up the **ProfileList** key as you learned to do earlier, and locate the **S-1-5** folder for the user profile you want to delete. Right-click the **Sid** key and click **Delete**.

4. **4**

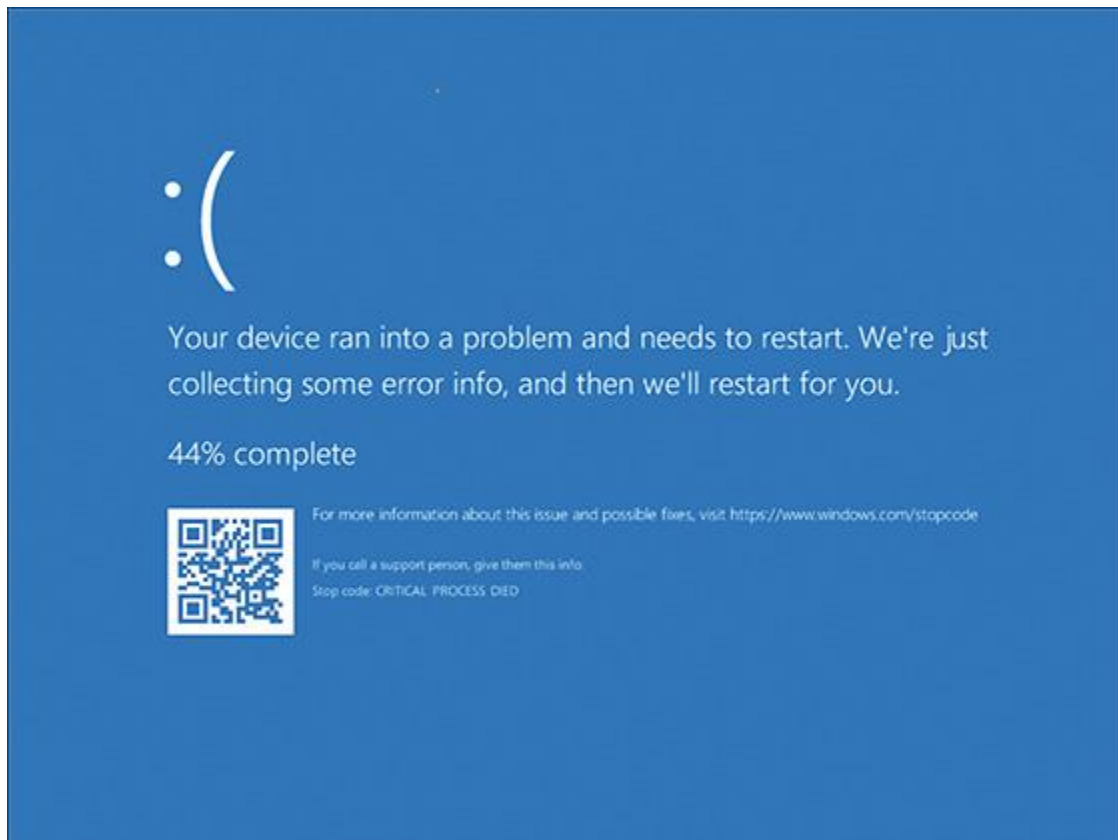
Restart the computer and create a new profile.

Error Messages on a Blue Screen

Hardware and software errors can present as error messages on a Windows **blue screen of death (BSOD)** and are called stop errors. Also, sometimes Windows hangs with the pinwheel spinning, continuously restarts, or does an abrupt and improper shutdown. A BSOD, or stop error, happens when processes running in kernel mode encounter a problem and Windows must stop the system. [Figure 15-37](#) shows a Windows 10 blue screen stop error.

Figure 15-37

A Windows 10 stop error screen

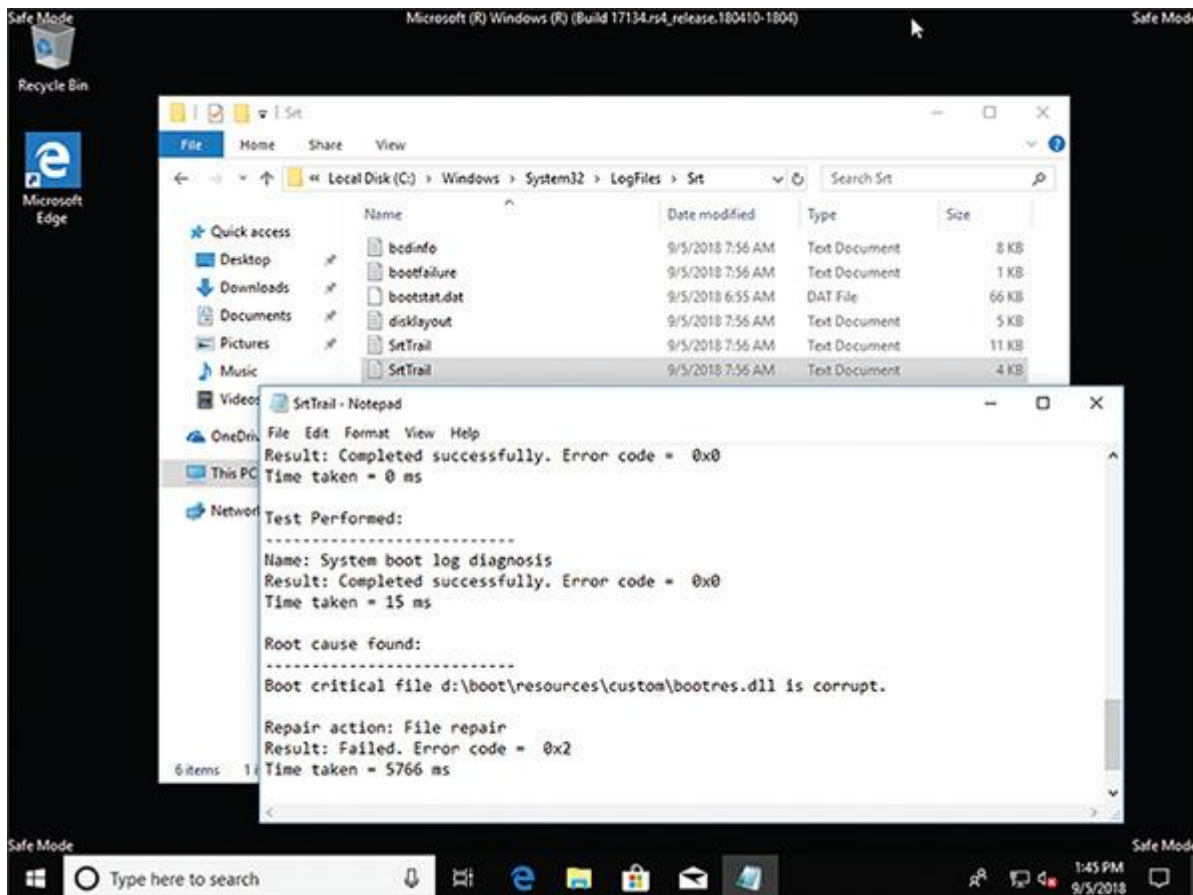


A stop error can be caused by a corrupted Windows update, a corrupted registry, a system file that is missing or damaged, a device driver that is missing or damaged, bad memory, or a corrupted or failing hard drive. Stop errors can occur during or after startup. Here's what to do when you get a stop error:

1. As for the tools that are useful in solving stop errors, put the web at the top of your list! (But don't forget that some sites are unreliable, and others mean you harm.) Search the Microsoft websites on the text labeled in [Figure 15-37](#), or use your smartphone to scan the QR code, which takes you directly to the BSOD webpages by Microsoft.
2. Disconnect any peripheral devices that might be causing trouble, such as a docking station, USB device, projector, or extra monitor.
3. Reboot the system. Immediately after a reboot following a stop error, Windows displays an error message box or bubble with useful information. Follow the links in the box.
4. If possible, restart the system and enable boot logging. Check the `C:\Windows\ntbtlog.txt` file to see if the correct driver files loaded.
5. Restart the computer a couple of times. Sometimes that's all you need to do to solve a problem. If Windows encounters errors, it will launch an automatic repair. If that doesn't fix the problem, you can launch Windows RE and restart Windows in **Safe Mode with Networking**. In Safe Mode, examine the log file created by Automatic Repair at `C:\Windows\System32\LogFiles\Srt\SrtTrail.txt`. See [Figure 15-38](#). Also, recall that Safe Mode creates its own log file at `C:\Windows\ntbtlog.txt`.

Figure 15-38

Examine the log file left by Automatic Repair





Note 18

If the stop error prevents Windows from loading the desktop and F8 has not yet been enabled at startup, you can force automatic repair by turning off the computer a couple of times as Windows launches.

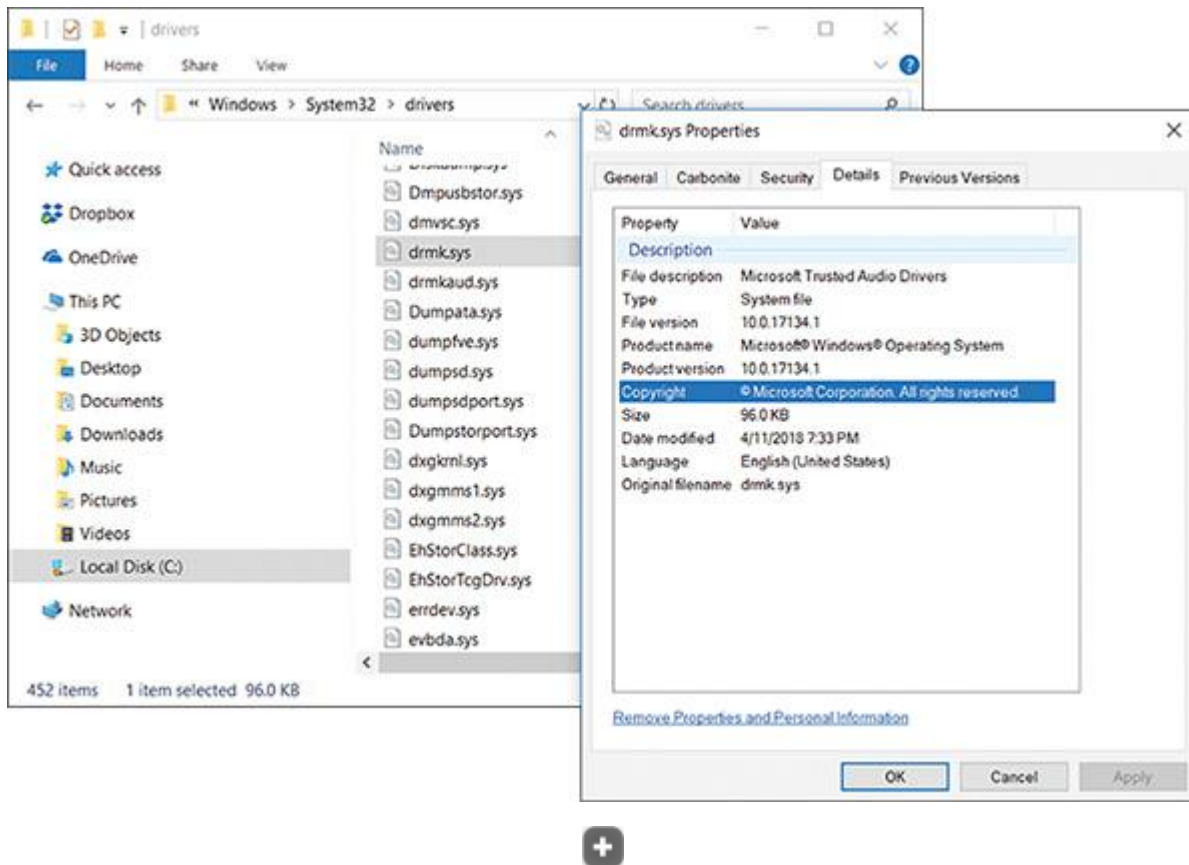
Errors with Hardware and Device Drivers

If the blue screen names a device or device driver that caused the problem, do the following:

- 1.
A Windows update might fix the problem. Open the **Settings** app, and update Windows.
- 2.
If the driver has been recently updated and the Safe Mode desktop is loaded, open **Device Manager** and roll back the driver.
- 3.
Consider that the device driver might have been updated along with a Windows update. For recent Windows updates, try to roll back the updates or return to a previous version of Windows.
- 4.
Use Device Manager to uninstall the device. When given the option, select **Delete the driver software for this device**. Then reboot the system.
- 5.
If the stop error does not identify the device but names a program file, open **Explorer** on a working computer to locate the program file. Driver files are stored in the C:\Windows\System32\drivers folder. Right-click the file and select **Properties** from the shortcut menu. The Details tab of the Properties dialog box tells you the purpose of the file (see [Figure 15-39](#)). You can then reinstall the device or program that caused the problem.

Figure 15-39

Use the Details tab of a driver's Properties dialog box to identify the purpose of the driver



- 6.

If you cannot start Windows in Safe Mode, use Windows RE to open a command prompt window. Then back up the registry, and open the Registry Editor using the regedit command. Drill down to the service or device key. The key that loads services and drivers can be found in this location:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

Disable the service or driver by changing the Start value to 0x4. Close the Registry Editor and reboot. If the problem goes away, use the copy command to replace the service or driver program file, and restart the service or driver.

! Caution

Consider that the device might be physically damaged. If you feel excessive heat coming from the computer case or a peripheral device, immediately unplug the device or power down the system. Don't turn the device or system back on until the problem is solved; you don't want to start a fire! Other symptoms that indicate potential danger are strong electrical odors, unusual noises, no noise (such as when the fan is not working to keep the system cool), liquid spills on a device, and visible damage such as a frayed cable, melted plastic, or smoke. In these situations, turn off the equipment immediately.

Improper or Frequent Shutdowns

Problems with improper or frequent shutdowns can be caused by overheating, a hardware problem, or the Windows kernel. After a restart, check Event Viewer for clues, apply Windows updates, verify memory with Memory Diagnostics, and use Check Disk (chkdsk /r) to check the hard drive for errors.

Next, consider that Windows might be corrupted. First try the least invasive solutions to repair Windows, including updating Windows, System File Checker, Startup Repair, running the system in Safe Mode, and System Restore.

If you decide the Windows installation is beyond repair, it's time to reimage or reinstall Windows. As you learned in this module, the tools to use in the least intrusive order are roll back Windows updates, Windows previous version (if available), Windows 10/11 repair installation, reimage Windows, reinstall Windows from the OEM recovery partition, and Windows 10/11 reset. After you have Windows up and running again, you can restore the user data from backups.

Module Review

15-6a **Module Summary**

Understanding the Boot Process

- When you first turn on a system, startup BIOS/UEFI on the motherboard takes control and performs POST to examine hardware components and then find an operating system to load.
- Windows startup is managed by the Windows Boot Manager. For a BIOS system, the program is Bootmgr. For a UEFI system, the program is Bootmgfw.efi. The Windows Boot Loader is Winload.exe or Winload.efi. The Boot Configuration Data (BCD) store contains Windows startup settings.
- The Session Manager (Smss.exe) runs in user mode and interacts with applications.

What to Do before a Problem Occurs

- Before a startup problem occurs, you can keep good backups, turn on System Restore, create a system image, configure the F8 key at startup, and create recovery boot media.

Tools for Solving Windows Startup Problems

- The Windows Recovery Environment (Windows RE or WinRE) can be started from within Windows, from the Windows setup DVD or flash drive, from a recovery drive, or from a system repair disc.
- Tools for startup troubleshooting include Windows RE; Startup Repair; startup settings; System Restore; Safe Mode; enabling boot

logging; uninstalling updates; SFC; and the chkdsk, diskpart, bootrec, and bootsect commands.

Tools to Reinstall Windows

- Tools that can be used to reinstall Windows are Windows 10/11 previous version, repair installation, reimaging Windows, recovery partition, and reset. Some manufacturers offer a recovery partition on the hard drive to restore a computer to factory state. You can also reinstall Windows from Windows setup media.

Troubleshooting Windows Startup

- If a hard drive contains valuable data but will not boot, you might be able to recover the data by installing the drive in another system as the second, nonbooting hard drive.
- Use the web to research stop errors by the QR code, error title, and error number listed on a black or blue screen.
- Slow profile loads can be solved by updating Windows, System File Checker, reducing startup items, System Restore, repair installation, and new user profiles.
- When a device or service causes the system to hang during a normal boot, boot into Safe Mode or perform a clean boot and uninstall and install the device or service. System Restore can return the system to a previously saved restore point before the problem occurred.
- Improper and frequent shutdowns are most likely hardware related. Event Viewer might record failures. Use Memory Diagnostics and chkdsk to check memory and the hard drive. Consider overheating or a corrupted Windows installation as a source of the problem.

Thinking Critically

These questions are designed to prepare you for the critical thinking required for the A+ exams and may use information from other modules and the web.

1. As a computer starts up, you see an error message about the HAL. At what point in startup does this error occur?
 1. When BIOS/UEFI is searching for an OS using devices listed in the boot priority order
 2. When Windows attempts to load the user profile
 3. When Windows attempts to launch critical device drivers
 4. When Windows attempts to launch the Windows kernel
2. Which Windows program must be running before a user can sign in to Windows?
 1. Kernel.exe
 2. Userinit.exe
 3. Explorer.exe
 4. Lsass.exe

5. All of the answers are correct.
3. As a computer starts up, you see an error message about a missing operating system. At what point in startup does this error occur?

1. When BIOS/UEFI is searching for an OS using devices listed in the boot priority order

2. When Windows attempts to load the user profile
3. When Windows attempts to launch critical device drivers
4. When Windows attempts to launch the Windows kernel
4. Your friend sees an error message about a corrupted bootmgr file during Windows startup. They have another computer with a matching configuration and decide to copy the bootmgr file from the working computer to the computer with the problem. Where is the bootmgr file stored?

1. C:\Boot\bootmgr

2. System Reserved\Boot\bootmgr

3. System Reserved\bootmgr

4. All of the answers are correct.

5. Your friend mentioned in [question 4](#) is having problems finding the bootmgr file and asks for your help. What is your best response?

1. Use diskpart commands to “unhide” and locate the file.

2. Use the File Explorer options applet to unhide the hidden bootmgr file.

3. Explain to your friend that performing a Startup Repair is a better option.

4. Explain to your friend that they can use the bootrec command to fix the bootmgr file without having to copy another file to the computer.

6. You see multiple errors about device drivers failing to launch at startup. Of the following, which is the best option to try first? Second?

1. Apply a restore point.

2. Perform a clean installation of Windows from setup media.

3. Perform a Startup Repair.

4. Perform a Windows reset.

7. A stop error halts the Windows 10 system while it is booting, and the booting starts over in an endless loop of restarts. How can you solve this problem?

1. Use the Windows Startup Settings screen to disable automatic restarts.

2. Press F8 at startup, and then disable automatic restarts.

3. Launch Windows 10 from setup media, and perform a Windows 10 reset.

4. Press F9 at startup, and then disable automatic restarts.

8. If you are having a problem with a driver, which of the following should you try first? Second?

1. Update the driver.

2. Use System Restore to apply a restore point.

3. Update Windows.

4. Perform a clean boot.

9. When error messages indicate that the Windows registry is corrupted and you cannot boot from the hard drive, what tool or method is the first best option to fix the problem? The second-best option?
1. Use bootable media to launch Windows RE, and use System Restore to apply a restore point.
 2. Use bootable media to launch Windows RE and perform a Startup Repair.
 3. Use bootable media to launch Windows RE, and then use commands to recover the registry from backup.
 4. Reimage Windows using a system image.
10. Your Windows system boots to a blue screen stop error and no desktop. What do you do first?
1. Reinstall Windows.
 2. Use the web to research the stop error messages and numbers.
 3. Attempt to boot into Windows RE using the Windows setup DVD or a recovery drive.
 4. Verify that the system is getting power.
11. You have important data on your hard drive that is not backed up, and your Windows installation is so corrupted you know that you must reinstall Windows. What do you do first?
1. Use System Restore to apply a restore point.
 2. Make every attempt to recover the data.
 3. Perform a repair installation of Windows.
 4. Reformat the hard drive and reinstall Windows.
12. Your computer displays the error message, "A disk read error occurred." You try to boot from the Windows setup DVD, and you get the same error. What is most likely the problem?
1. The Windows setup DVD is scratched or damaged in some way.
 2. The hard drive is so damaged the system cannot read from the DVD.
 3. Both the optical drive and the hard drive have failed.
 4. The boot device order is set to boot from the hard drive before the optical drive.
13. When a driver is giving problems in Windows 10, which tool offers the least intrusive solution?
1. Device Manager
 2. Windows Update
 3. System Restore
 4. Registry Editor
14. An error message is displayed during Windows startup about a service that has failed to start, and then the system locks up. You try to boot into Safe Mode, but you get the same error message. What should you try next?
1. Use the command prompt to edit the registry.
 2. Boot to Windows RE, and enable boot logging.

3. Perform a repair installation of Windows.

4. Boot to Windows RE, and perform a Startup Repair.

15. Stop errors happen when which types of processes encounter an error?

1. Processes created by applications

2. Processes created by Windows components running in user mode

3. Processes created by Windows components running in kernel mode

4. Processes created by anti-malware software

16. What is the command to use the System File Checker to immediately verify and repair system files?

17. What is the path and name of the log file created when you enable boot logging on the Windows 10 Startup Settings menu?

18. What information is contained in the C:\Windows\System32\LogFiles\Srt\SrtTrail.txt file?

19. Which tool is the least invasive solution to repair Windows?

1. System Restore

2. Startup Repair

3. Windows reset

4. Uninstall updates

20. On a computer with Windows 11 installed, you have used Disk Management to verify that a laptop has a recovery partition, but when you do a Windows reset, you don't see the option to restore preinstalled apps. What is the most likely problem?

1. Windows reset is not working properly.

2. Windows 11 Home is installed, and it does not offer the option to restore preinstalled apps.

3. The laptop factory state uses an OS other than Windows 11.

4. The recovery partition is corrupted.

21. A customer reports their recently purchased computer does not consistently run their old applications. Application errors occur intermittently, and data files get corrupted. They have tried uninstalling and reinstalling the apps, and the problems persist. As you troubleshoot the problem, you reboot the system and get a BSOD error. The customer tells you the BSOD has occasionally appeared. Which subsystem is most likely causing the problem, and what is the next best step?

1. Windows is corrupted; reinstall Windows.

2. Windows Update is not working; use System Restore.

3. Memory is faulty; run Memory Diagnostics.

4. Applications are faulty; uninstall and reinstall the applications causing errors.

22. You have used Disk Management to verify that a laptop has a recovery partition, but when you do a Windows reset, you don't see the option to restore preinstalled apps. What is the most likely problem? The laptop factory state uses an OS other than Windows 10.

15-6d Hands-On Projects

Hands-On Project 15-1

Using Boot Logs and System Information to Research Startup

- **Est. Time:** 30 minutes
- **Core 2 Objective:** 3.1

Boot logs can be used to generate a list of drivers that were loaded during a normal startup and during a Safe Mode startup. Do the following to use boot logs to research startup:

1. **1**
Boot to the normal Windows desktop with boot logging enabled. Save the boot log just created to a different name or location so it will not be overwritten on the next boot.
2. **2**
Reboot the system in Safe Mode, which also creates a boot log. Compare the two logs, identifying differences in drivers loaded during the two boots. You can print both files and lay them side by side for comparison. An easier method is to compare the files using the Compare tool in Microsoft Word.
3. **3**
Use the System Information utility or other methods to identify the hardware devices loaded during normal startup but not loaded in Safe Mode. Which devices on your system did not load in Safe Mode?

As you identify the drivers not loaded during Safe Mode, these registry keys might help with your research:

- Lists drivers and services loaded during Safe Mode:
HKLM\System\CurrentControlSet\Control\SafeBoot\Minimal
- Lists drivers and services loaded during Safe Mode with Networking:
HKLM\System\CurrentControlSet\Control\SafeBoot\Network

Hands-On Project 15-2

Taking Ownership and Replacing a Windows System File

- **Est. Time:** 15 minutes
- **Core 2 Objective:** 1.9

In the module "[Troubleshooting Windows After Startup](#)," you learned to use SFC and DISM commands to find and replace corrupted Windows system files. SFC keeps a log of its actions at C:\Windows\Logs\CBS\CBS.log, and DISM keeps a log at C:\Windows\Logs\DISM\dism.log. Sometimes these logs or BSOD error screens reveal the name and location of corrupted system or device driver files that Windows tools cannot replace. In this situation, you can manually replace the file. To do so, you can use the takeown command to take ownership of a file and the icacls command to get full access to the file. The Microsoft Knowledge Base Article 929833 at support.microsoft.com explains how to use these two commands.

Do the following to practice manually replacing a system file:

1. **1**
Boot the computer into Safe Mode with Command Prompt.
2. **2**
Take ownership and gain full access to the C:\Windows\System32\jscript.dll file. What commands did you use?
3. **3**
Rename the Jscript.dll file to Jscript.dll.hold. Run the **sfc /scannow** command. Did SFC restore the Jscript.dll file? What is the path and file name of the log file that lists repairs?
4. **4**
SFC restores a file using files accessed from Windows Update or stored on the Windows setup DVD or other folders on the hard drive. If SFC cannot restore a file, you might find a fresh copy in the C:\Windows\winsxs folder or its subfolders. Search these folders. Did you find a version of Jscript.dll that is the same file size as the one in C:\Windows\System32? Other than the C:\Windows\winsxs folder, where else can you find a known good copy of a corrupted system file or device driver file?

Note 19

To use a command prompt window to search for a file in a folder and its subfolders, use the `dir /s` command.

Hands-On Project 15-3

Viewing the BCD Store

- **Est. Time:** 15 minutes
- **Core 2 Objective:** 1.9

On two or more computers, open an elevated command prompt window, and use the `bcdedit /enum` command to view the BCD store. One BCD store is shown in [Figure 15-40](#).

Figure 15-40

A BCD store on a computer that uses the GPT partitioning system

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>bcdedit /enum

Windows Boot Manager
-----
identifier                {bootmgr}
device                    partition=G:
description                Windows Boot Manager
locale                    en-US
inherit                    {globalsettings}
default                    {current}
resumeobject               {358ebcf5-39df-11e7-a591-e188b1e0f934}
displayorder               {current}
toolsdisplayorder         {memdiag}
timeout                    300

Windows Boot Loader
-----
identifier                {current}
device                    partition=C:
path                      \WINDOWS\system32\winload.exe
description                Windows 10
locale                    en-US
inherit                    {bootloadersettings}
recoverysequence           {72f318ad-39df-11e7-a591-e188b1e0f934}
displaymessageoverride     StartupRepair
recoveryenabled             Yes
allowedinmemorysettings    0x15000075
osdevice                   partition=C:
systemroot                 \WINDOWS
resumeobject               {358ebcf5-39df-11e7-a591-e188b1e0f934}
nx                          OptIn
bootmenupolicy              Standard
hypervisorlaunchtype       Auto
```



Answer the following questions:

1. Can you view the BCD store and determine if the system is using the MBR or GPT partitioning system? Why or why not?
2. Explain how you can look at the BCD store and tell if the system is a single boot or multiboot system.

Hands-On Project 15-4

Researching Laptop Online Resources

- **Est. Time:** 15 minutes
- **Core 2 Objective:** 1.9

Suppose the hard drive in a laptop has failed, and you must replace the hard drive with a new one and then install Windows on the new drive. What online resources can help you? Do the following to find a service manual and recovery files for a laptop to which you have access, such as one you or a friend owns:

1. What are the brand, model, and serial number of the laptop?

2. What is the website of the laptop manufacturer? Save or print a webpage on that site that shows you what recovery files you can download to install Windows on a new hard drive for the laptop.
3. If the website provides a service manual, download the manual and print the pages that show how to replace the hard drive.
4. Based on what you have learned about online support for this laptop, what backups or recovery media do you think need to be created now, before a hard drive crash occurs?

Hands-On Project 15-5

Practicing Using System Recovery Options

- **Est. Time:** 30 minutes
- **Core 2 Objective:** 1.9

Launch Windows RE and do the following:

1. **1**
Execute the Startup Repair process. What were the results?
2. **2**
Launch **System Restore**. What is the most recent restore point? (Do not apply the restore point.)
3. **3**
Using the command prompt window, open the **Registry Editor**. What command did you use? Close the editor.
4. **4**
Using the command prompt window, copy a file from your Documents folder to a flash drive. Were you able to copy the file successfully? If not, what error message(s) did you receive?

Hands-On Project 15-6

Using Startup Repair

- **Est. Time:** 15 minutes
- **Core 2 Objective:** 3.1

When Startup Repair attempts to fix a system, it creates a log file with information about the steps taken during the repair process. If Startup Repair doesn't fix the system, you can use the log file to investigate the problem and perhaps manually fix it. Do the following to practice using Startup Repair and examine its log file:

1. **1**
Use the **Settings** app in Windows to launch Windows RE. From the initial Windows Startup Menu, click **Troubleshoot, Advanced options**, and then **Startup Repair**.
2. **2**
Diagnostics of the system are made, and the location of the log file appears. Note the path and name of the file. The default location of the log file is

C:\Windows\System32\LogFiles\Srt\SrtTrail.txt. Click **Advanced options**. You are returned to the Windows Startup Menu.

3. **3**
To view the log file from the Windows RE command prompt, click **Troubleshoot** and click **Command Prompt**.
4. **4**
In the command prompt window, enter the command `c:` to access the hard drive. (You might need to use a different drive depending on the log file location reported in [Step 2](#).)
5. **5**
Enter the following command to go to the directory where the log file is located:

`cd \Windows\System32\LogFiles\SRT`
6. **6**
To use Notepad to view the file contents, enter the following command:

`notepad.exe SRTTrail.txt`
7. **7**
In the log file, look for information about a failed test.

Hands-On Project 15-7

Using the DISM Commands

- **Est. Time:** 15 minutes
- **Core 2 Objective:** 3.1

Sometimes a Windows update crashes the system, and uninstalling the update doesn't work in the Settings app and in Windows RE. Another way to roll back the update is with the DISM commands. Do the following:

1. **1**
Launch the Windows RE command prompt window.
2. **2**
Enter this command to get a list of installed updates: `dism /online /get-packages`
3. **3**
Search through the list, and find the most recent one. Find the Package Identity. It's a long string that you will need to copy by selecting it and pressing **Ctrl+C**.
4. **4**

Don't uninstall the update. But if you intended to uninstall the update, you would use this command: `dism /online /remove-package /PackageName:[Insert the copied Package Identity here]`

5. **5**

DISM keeps a log at C:\Windows\Logs\DISM\dism.log. Open the log file in Notepad. Can you find the Package Identify string you copied in [step 3](#)? Where do you think DISM got its information about installed updates?

15-6e Real Problems, Real Solutions

Real Problem 15-1

Sabotaging a Windows System

- **Est. Time:** 30 minutes
- **Core 2 Objective:** [3.1](#)

In a lab environment, follow these steps to find out if you can corrupt a Windows system so that it will not boot, and then repair the system. (This problem can be done using a Windows installation in a virtual machine.) Don't forget about the powerful `takeown` and `icacls` commands discussed in this module.

1. **1**

Rename or move one of the program files listed in [Table 15-1](#). Which program file did you select? In what folder did you find it?

2. **2**

Restart your system. Did an error occur? Check in Explorer. Is the file restored? What Windows feature repaired the problem?

3. **3**

Try other methods of sabotaging the Windows system, but carefully record exactly what you did to sabotage the boot. Can you make the boot fail?

4. **4**

Now recover the Windows system. List the steps you took to get the system back to good working order.

Real Problem 15-2

Recovering Data from a Hard Drive

- **Est. Time:** 30 minutes
- **Core 2 Objective:** [3.1](#)

To practice recovering data from a hard drive that won't boot, create a folder on a Windows 10 or Windows 11 VM. Put data files in the folder. What is the name of your folder? Move the hard drive to another working VM, and install it as a second hard drive in the system. Copy

the data folder to the primary hard drive in this second VM. Now return the hard drive to the original VM, and verify that the VM starts with no errors. List the steps you used in this project.

<p>After holding the Shift key and clicking Restart, your PC enters the Windows Recovery Environment. Click Troubleshoot, then Advanced options. Next click Command Prompt. The option of accessing the Command Prompt allows you to use Windows command-based tools to execute commands. Our boot drive is the D: drive. Enter D: at the prompt.</p>	<p>Click Start, then Power. Hold the Shift key and click Restart to access the Windows RE. Choose Troubleshoot, then Advanced options and Startup Repair. Startup repair diagnoses your system and reports no problems. Click Advanced options.</p>
<p>Now on the D: drive, use the cd command to move to the SRT directory with this command:</p> <p>cd \Windows\System32\LogFiles\SRT</p> <p>Remember, Windows commands are NOT case-sensitive.</p>	<p>In the search bar, enter cmd and open the Command Prompt. Using the command prompt window, open the Registry Editor using regedt32.exe. Respond to the UAC. In the Registry Editor, expand HKEY_LOCAL_MACHINE, then expand Software. Collapse the entire registry key without any changes. Close the editor using the File menu and Exit.</p>
<p>View the contents of this directory by entering the dir command. You'll see all the contents listed. We want to review the boot log. It is named SrtTrail.txt. To see the log, at the prompt enter:</p> <p>notepad SrtTrail.txt</p>	<p>C:\users\labco_8q8</p> <p>Now back at the Command Prompt, change to your Documents folder with cd documents and take a directory listing with dir. Copy the Testfile.txt file from your Documents folder to a flash drive E: Use the copy command as follows: copy testfile.txt E: When the copy is successful, close the Command Prompt to return to the desktop and move to the exercises for this lab.</p>
<p>In Notepad, check the log for failed tests. Scroll down to see all the entries. Look for any unsuccessful tests and note the boot status test result. Close the file using the File menu and clicking Exit. Then close the Command Prompt window by clicking the red X.</p>	<p>System restore = troubleshoot, advanced Registry editor= regedit</p>

Test Performed: ----- Name: Boot status test Result: Completed successfully. Error code = 0x0 Time taken = 16 ms Root cause found: ----- Boot status indicates that the OS booted successfully.	
Now back in the WinRE, click Continue to exit the Recovery Environment and start Windows 10. Log in with the username shown and enter the password P@ssw0rd. The desktop displays. Click Next to proceed to the exercises. First drive = x: First choice = troubleshoot	

Backup and recovery are critical for the long-term preservation of our data. Every day, a variety of events can occur that can have an impact on our data. Examples include natural disasters, drive failures, accidental deletion, and cyber-attacks. Backups are our method of restoring that data. It's also important to consider where the data is kept and how it is kept. Some industries, such as the payment card or healthcare industries, have strict rules that govern how data is stored, where it can be stored, and how long it must be kept. Other data types may be identified in the backup and recovery strategy. There are several methods for creating backups, and schemes that use the various styles can be combined to create stronger backup processes, save storage space, and/or speed up recovery time. Good backup practices can also help to thwart cyber-attacks. This module will look at full, incremental, differential, and synthetic backups. You will go over file history and the advantages of enabling it and discuss backup storage, frequency, and testing. You will go over different types of recovery sites and their benefits and drawbacks.

Task 1 - Create a Full Backup

A full backup is an exact duplicate of all user-created data files that have been scheduled to be backed up. Administrators or users who are authorized to run and schedule backups will determine the scope of what will be backed up. Typically, files used by applications, metadata, logs, tracking files, and other control and management files will be copied. Applications, operating systems, and other software are typically not copied during a full backup. Other techniques and clean installs with backed-up data can be used to recreate that information.

The archive bit is used to recognize what needs to be backed up. It is a bit that is activated whenever a file is changed. The computer searches for this archive bit to determine what to backup. The archive bit will then be reset for each changed file following a full backup. If any data is missing and a drive fails, you will lose it; a full backup will be the starting point for all backup schemes.

A full backup is the most expensive backup we'll look at because it takes up the most disk space compared to other backups. A full backup is not the only type of backup used in most business environments. The high cost of storing the same data multiple times outweighs the benefits. This type of backup is also the most time-consuming to complete. Due to the high cost, network traffic and time of day should be considered. This task will typically be done at the end of the day when the user has closed out all of the files and logged off for the day.

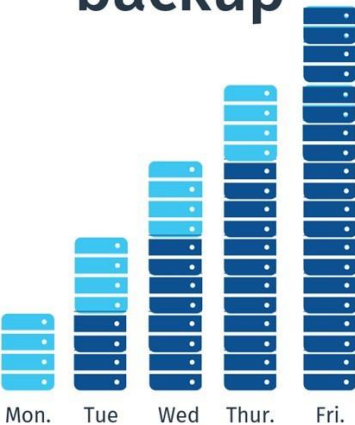
Another thing to consider in security would be if the file were to become compromised, a threat actor would access all the files and data. Proper storage and secure measures need to be taken with backups to ensure data safety. When it comes to backend recovery, a full backup is the quickest because it is the only recovery file required. Another advantage is that full backup files are much easier to manage than others.

Incremental Backups

Incremental backups will begin with a full backup. After a changes made to the files are tracked by the archive bit. If configured for incremental backups, any changes made up, and the archive bit will be reset. Every Sunday, for backup is run. The remaining days will be incremental. As a changes made on Monday will be backed up, and the On Tuesday, any changes made would be backed up, and reset. This takes up less space than full backups because backups only record changes to the data each day. It will to do these incremental backups because less data is up.

When it comes to backend recovery, incremental backups to restore because each backup file must be loaded order to restore the data. The full backup would be followed by Monday's changes, Tuesday's changes, and so on, until the restoration is complete. With the number of backups being created, this type of backup can also become very time-consuming to maintain. Third-party software or the use of scripting, PowerShell, and Azure cloud platform can be used to create this backup strategy.

incremental backup



full backup, any the system is will be backed example, a full result, any archive bit reset. the archive bit incremental also be quicker being backed

take the longest sequentially in uploaded first,

Figure 1.61: Displaying an incremental backup.

Differential Backups

Differential backups will always start with a full backup. The archive bit tracks any changes made to files after a full backup. If differential backups are enabled, any changes made will be backed up, and the archive bit will not be reset. A full-back, for example, is run every Sunday. The remainder of the days will be differential. As a result, any changes made on Monday will be backed up, and the archive bit will be kept enabled. On Tuesday, any changes made and the changes made on Monday would be backed up, and the archive bit would be left on. Wednesday would include the changes from Monday, Tuesday and Wednesday. This requires less space than full backups but more than incremental backups because you are capturing each day's differential and all previous changes that have occurred since the last full backup.

Differential backups will also be faster than a full backup but slower than an incremental backup. Less data is backed up than full backups, but the same data plus redundant data is backed up in each backup compared to incremental. When it comes to backend recovery, differential backups take longer to restore than full backups but less time than incremental backups. The full backup would be uploaded first, followed by the last differential, because the last differential contains all of the changes made since the last full backup, instead of uploading each of those days sequentially as in an incremental. Third-party software or the use of scripting, PowerShell, and the Azure cloud platform can be used to create this backup strategy.

differential backup

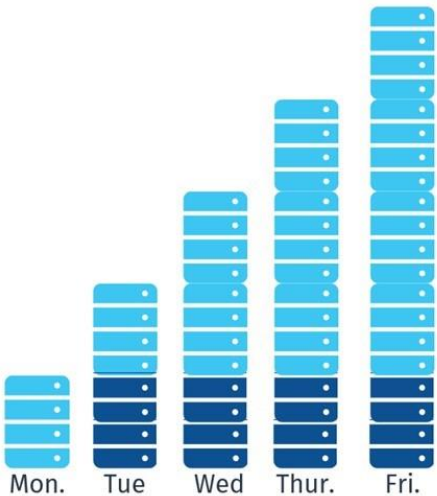


Figure 1.62: Displaying a differential backup.

Synthetic Full Backups

This backup technology combines full backups with incremental backups. As an example, on Sunday, a full backup will be taken. The remainder of the week will be devoted to incremental backups. An incremental backup will be taken when the full synthetic backup day arrives. Following that, a full synthetic backup will be created by combining the original full backup with all incremental backups. When finished, the synthetic backup will contain all of the original information from the first full backup as well as all of the changes that occurred. The incremental will be removed, and the space will be made available. The full synthetic backup will be the new backup starting point, and changes will be tracked using incremental until the next synthetic backup.

Utilizing this technology will be faster at backing up the information because incremental is being used. Backend recovery will be similar to incremental backups in terms of recovery. The full synthetic backup would be the first to be uploaded, followed by Monday's changes, Tuesday's changes, and so on, until the restoration was completed. Because the number of backups is combined and reduced on each synthetic day, using this style of backup aids in backup organization and maintenance.

Frequency of Backups & Testing

The frequency of backups will be determined by the needs of the company and the type of data being stored. Continuous backups may be required, or data may be backed up less frequently. The first thing to look into is laws and regulations to see what should be done with the different types of data that are being stored. Then, a backup strategy must be devised, which includes where the data will be stored, what types of media will be used to keep it, and the frequency with which it must be completed. In general, important information should be backed up daily, but this may need to be increased or decreased depending on the data's criticality.

Backups are not simply stored and forgotten about once they are created. They must be tested to ensure that they will work and that the backup and recovery plan will work. They will not be tested in a live production environment but rather in a sandbox environment where the restoration process will have no effect if it fails. If a failure occurs, there is enough time to redo the backup and not lose data.

The storage of this data can quickly consume a lot of space. Files are archived to help with this, which groups multiple data files into a single file to reduce storage space or even compression. When information stored on a hard drive or a tape drive is no longer required on that drive, it is returned to the backup rotation and overwritten. The quality of the drives and tape drives degrades over time, so rotation is required to ensure the longest possible life.

On-Site vs Off-Site

On-Site backups are those that are kept in the same location. They are kept there for easy access and quick data restoration. Typically, hard drives or tape drives will be used to store the data. There is software that can automate the process and keep backups. One advantage of on-site data backup is that the organization is solely responsible for data storage and security. The data would be in the hands of the cloud provider if cloud services were used. Some industries may have rules in place to prevent this from happening and may require you to manage the data. A disadvantage is that if there is a disaster, there is the potential to lose all the backup information.

Offsite backups are backups that are kept in a separate location. These could be a centralized location where all backup tapes and drives are shipped to and stored for the required period of time, or they could be a situation where a cloud provider is used. When using cloud services, the data is typically stored on a server in a data center. The type of data stored will determine whether cloud services can be used or whether the organization must maintain data control at all times. Although these data centers are heavily fortified, cloud breaches do occur and must be considered a threat. This type of backup is critical for when natural disasters occur because the data can be downloaded from anywhere where there is an internet connection, allowing the operation to be restored and up and running as quickly as possible.

Hot Site, Warm Site, vs Cold Site

These are three different types of recovery sites for when disasters happen. Each of the sites listed has its benefits and drawbacks. One thing in common with the three types of sites is that these sites should be located somewhat close to the original site. If the site is affected, the employees will need to be able to drive to the new site to perform their work. Usually something within a 75 - 100 miles radius from the original site. This is a general suggestion; each situation will need to be judged on the true need.

Cold Site

This site is not immediately available during the recovery phase and takes the longest duration to setup and run. Networking equipment must be installed, including servers, end-user computers, and software. The data upload must be completed. Typically, this type of site is not configured except for the power to the building and environmental controls such as cooling for the server room. Compared to a warm and hot-site, one advantage of this setup is that it does not have a high cost. The downside is that this type of site can take several days or even weeks to setup.

Warm Site

This type of recovery site is exactly what it sounds like, right in the middle of cold and hot sites. All of the features of a cold site are present, but it also has the necessary equipment and a network connection. In the event of a disaster, additional resources may need to be brought in for the setup, which is an expensive process. This facility's data will be out of date. In the event of a disaster, any other setup will be completed, and the data will be uploaded. This type of facility can typically be up and running in a matter of hours.

Hot Site

This site has everything set up and ready to go. There is a structure, electricity, computers, and a network in place, and the data is backed up in real-time. This type of site has very little downtime and can be up and running almost immediately. There is a financial cost associated with the hot site. The energy required to power the servers and cool the building may be prohibitively expensive for most businesses. The cloud is becoming an increasingly appealing option for meeting this need because of the on-demand features and the ability to spin up virtual machines in the cloud and operate remotely without the overhead of an expensive building, electricity, and cooling.

Grandfather-Father-Son

This backup scheme was designed to keep a complete backup of the machine while requiring the least amount of storage space. The backup types of names are Grandfather, Father, and Son. In most cases, the grandfather will be a machine image that will be stored offsite at another branch or possibly in the cloud in case of disaster recovery. This type of backup is typically performed every month. The father would then take a full backup of the machine but save the information locally for faster access and recovery. The backup is typically performed every week. Son will typically use incremental backups and will be the most commonly used type of backup done every other day. An additional backup, the great-grandfather, which is a yearly image of the machine, can be added.

To visualize this look on a calendar. Every Sunday, full backups will be created (father). Every other day will be incremental (son) except the last day of the month when an image of the machine will be taken and stored in the cloud (grandfather). This type of backup necessitates extensive planning and preparation, but it provides a high level of redundancy with multiple recovery points that can be used to restore the data. The use of incremental helps to save storage space but can make the recovery process time consuming and resource intensive. Third-party software or the use of scripting, PowerShell, and the Azure cloud platform can be used to create this backup strategy. An example of the setup is below:

Week 1 - Sunday Father - **Monday Son** - Tuesday Son - **Wednesday Son** - Thursday Son - **Friday Son** - Saturday Son

Week 2 - Sunday Father - **Monday Son** - Tuesday Son - **Wednesday Son** - Thursday Son - **Friday Son** - Saturday Son

Week 3 - Sunday Father - **Monday Son** - Tuesday Son - **Wednesday Son** - Thursday Son - **Friday Son** - Saturday Son

Week 4 - Sunday Father - **Monday Son** - Tuesday Son - **Wednesday Son** - Thursday Son - **Friday Son** - **Saturday Grandfather**

3-2-1 Backup Rule

The 3-2-1 backup rule specifies where your data should be stored and how many copies should be kept. According to this backup method, the data should be duplicated at least three times. The second number in 3-2-1 indicates that two of the three copies should be kept on-site but not on the same media. For example, data can be stored on a hard drive in the PC, as well as a tape drive or an external hard drive. Keeping two copies on-site allows faster recovery from failed drives and quicker uploads to fix issues. But what happens when there is a disaster like a tornado, hurricane, earthquake or flooding? The final copy of the three comes into play. The 1 in 3-2-1 is for the copy that should be kept offsite for disaster recovery purposes. There is no such thing as a perfect strategy, but this is a solid choice that gives the administrator flexibility with data recovery options.

- System Restore will allow users to revert back to a snapshot in time of how the computer was at that period. It is not enabled by default and will need to be turned on.
- File History enables users to backup contacts, documents, pictures, music, videos, desktop, downloads, OneDrive, and other data to another internal or external hard drive or the cloud on a regular basis.
- A full backup is an exact duplicate of all user-created data files that have been scheduled to be backed up.
- The Grandfather-Father-Son backup scheme was designed to keep a complete backup of the machine while requiring the least amount of storage space. The backup types of names are Grandfather, Father, and Son.

Task 3 - Configure File History

Unlike other complex backup tools, File History is designed to be quick and simple to enable. File History enables users to backup contacts, documents, pictures, music, videos, desktop, downloads, OneDrive, and other data to another internal or external hard drive or the cloud on a regular basis, such as every few minutes, every few hours, or daily. Restoration is quick, and several versions of the file can be restored.

System Restore will allow users to revert back to a snapshot in time of how the computer was at that period. It is not enabled by default and will need to be turned on.

File History enables users to backup contacts, documents, pictures, music, videos, desktop, downloads, OneDrive, and other data to another internal or external hard drive or the cloud on a regular basis.

A full backup is an exact duplicate of all user-created data files that have been scheduled to be backed up.

The Grandfather-Father-Son backup scheme was designed to keep a complete backup of the machine while requiring the least amount of storage space. The backup types of names are Grandfather, Father, and Son.

Full = expensive

3-2-1 = where and how many

Hot site = high cost immediate recovery

Intervals archive bit reset = Incremental Backup

Win 10 auto backup tool = system restore

