Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**Module**

**9**

**Performance Tuning and System Recovery**

* [Chapter Introduction](javascript://)
* **9-1**[Performance Tuning Overview](javascript://)
  + **9-1a**[Establishing a Baseline](javascript://)
  + **9-1b**[Recognizing Bottlenecks](javascript://)
  + **9-1c**[Tuning Performance](javascript://)
* **9-2**[Performance Monitoring Tools](javascript://)
  + **9-2a**[Task Manager](javascript://)
  + **9-2b**[Resource Monitor](javascript://)
  + **9-2c**[Performance Monitor](javascript://)
* **9-3**[Performance Options](javascript://)
* **9-4**[Controlling Application Startup](javascript://)
  + **9-4a**[Tools for Managing Application Startup](javascript://)
  + **9-4b**[Startup Methods Used by Applications](javascript://)
* **9-5**[Troubleshooting Windows 10 Errors](javascript://)
  + **9-5a**[Steps Recorder](javascript://)
  + **9-5b**[Reliability Monitor](javascript://)
  + **9-5c**[Event Viewer](javascript://)
* **9-6**[Local File Recovery and Backup](javascript://)
  + **9-6a**[Configuring File History](javascript://)
  + **9-6b**[Configuring Backup and Restore (Windows 7)](javascript://)
  + **9-6c**[Restoring Previous Versions of Files and Folders](javascript://)
* **9-7**[System Recovery](javascript://)
  + **9-7a**[Reset this PC](javascript://)
  + **9-7b**[Windows Recovery Environment](javascript://)
  + **9-7c**[Restore Points](javascript://)
  + **9-7d**[Recovery Drive](javascript://)
* **9-8**[Chapter Review](javascript://)
  + **9-8a**[Summary](javascript://)
  + **9-8b**[Key Terms](javascript://)
  + **9-8c**[Review Questions](javascript://)
  + **9-8d**[Case Projects](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

Chapter Introduction

After reading this module and completing the exercises, you will be able to:

* **1**Describe performance-tuning concepts
* **2**Use Task Manager
* **3**Use Resource Monitor
* **4**Use Performance Monitor
* **5**Configure Performance Options
* **6**Control application startup
* **7**Describe tools that you can use for troubleshooting errors in Windows 10
* **8**Understand recovery and backup of user data
* **9**Describe recovery options for an unstable Windows 10 computer

On most Windows 10 computers, the default configuration provides acceptable performance. When users run applications, the applications respond quickly. When users access files, the files open quickly. On some systems, however, performance can start to deteriorate over time. Performance tuning lets you optimize the performance of Windows 10 to function at acceptable standards. Keep in mind that poor performance and improper operations might not simply be a matter of tweaking the system; problems might have appeared that require corrective actions to remedy.

In this module, you begin by learning about the performance-tuning process and how Performance Monitor allows you to find system bottlenecks. Additionally, you learn how to use Task Manager and Event Viewer to troubleshoot system performance. If you recognize that the problems are significant enough to require a repair of the Windows operating system, this module investigates your options—including recovering old versions of data and application components, or ultimately repairing or reinstalling a Windows operating system.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**9-1**Performance Tuning Overview

[**Performance tuning**](javascript://) is a process that you can use to improve the speed of a computer system. In an ideal world, an effective performance-tuning process is initiated well before problems occur; in most cases, however, performance tuning is not even considered until a performance problem exists.

The performance tuning process consists of:

* Establishing a baseline
* Recognizing bottlenecks
* Tuning performance

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-1aEstablishing a Baseline

To recognize the system bottlenecks that are limiting performance, you must first establish a baseline that defines normal performance. A [**baseline**](javascript://) is a set of performance indicators captured when system performance is acceptable. Effectively, the baseline defines normal performance. The baseline values are compared with future values of performance indicators to isolate performance problems.

Windows 10 reports on a wide variety of performance indicators. Performance indicators are often called [**counters**](javascript://) because they display values for system characteristics. Some examples of counters are:

* % Processor Time
* Disk Read Byte/sec
* Memory: Available Mbytes
* IPv4: Datagrams/sec

When you establish a baseline, it’s important to ensure that you’re measuring the normal state of the performance indicators. If unusual activity is occurring, the baseline performance measurement is not valid, and it will be difficult to use the baseline to identify abnormal activity in the future.

To ensure that you are measuring the normal state when establishing a baseline, you should:

* Verify that no unusual activity is happening on the computer. For example, ensure that no applications are performing large queries to databases or processing batch jobs, unless that is the normal state of the computer.
* Measure performance indicators over time. By measuring performance indicators over time, you can see an average value for the indicators. Average values are less volatile and more accurate than measuring with snapshots of short duration.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-1bRecognizing Bottlenecks

A [**bottleneck**](javascript://) occurs when a limitation in a single computer system component slows down the entire system. For any application, one component in the computer system always is the limiting factor for performance. This component is the bottleneck. Performance tuning attempts to eliminate bottlenecks.

For each activity you perform and each application that you run, the bottleneck might be different. For example, a database application may require fast access to the hard drive, and older spinning disk drives are a common bottleneck. A 3-D rendering program may experience limited processing power as the most common bottleneck. The most common bottlenecks to system performance are in the areas of disk, memory, processor, or the network.

### Disk Bottlenecks

Disk bottlenecks occur when Windows 10 and running applications want to read and write information to the physical disk in the system faster than the disk can manage. For desktop computers running Windows 10, disk bottlenecks are not that common.

You can identify disk bottlenecks by monitoring active time for the disk or the disk queue length. If the active time is at 100% for a sustained period of time, then the disk is too slow. Disk queue length identifies the number of disk requests queued to be serviced. If the disk queue length is consistently greater than one, then the disk is too slow.

If required, disk performance can be increased in a few different ways, such as:

* Upgrade the disks—Disks are capable of certain speeds of data transfer. In less-expensive computers, it is common for manufacturers to include spinning hard drives that perform much slower than solid-state drives (SSDs). In lower-end laptops, slow 5400 RPM hard drives with low power consumption are often used, which are slow even when compared to the 7200 RPM hard drives used in most desktop computers. Upgrading a spinning hard drive to an SSD is a huge performance improvement at minimal cost; it also uses less power.
* Implement mirrored Storage Spaces—Mirrored Storage Spaces volumes increase read and write performance by spreading data manipulation tasks across multiple hard drives. Because it’s not typical for a Windows 10 computer to have multiple hard drives, this option is rarely used.
* Move the paging file to a nonsystem disk—By default, the paging file, which is accessed often by the system, resides on the same disk as the operating system files, which are also accessed often by the system. Putting the paging file on a different physical disk (not just a different partition) can increase performance by reducing the data manipulation that any one disk needs to perform. This is most commonly an issue when a computer has limited memory and forces the paging file to be used more often.

### Memory Bottlenecks

Most memory bottlenecks occur when the applications you are running require more memory than is physically available in the computer. This forces Windows 10 to use virtual memory to accommodate the memory requirements of all the running applications. Virtual memory is a system wherein memory is simulated on disk with a paging file. The least used memory areas are stored in the paging file. When information in the paging file is required, it is taken out of the paging file and placed in physical memory.

Accessing information from disk is much slower than accessing information from physical memory. Reducing the need for virtual memory can significantly improve system performance. You can recognize when virtual memory is being heavily used by a high volume of disk activity.

To reduce the use of virtual memory, you can do the following:

* Increase the amount of physical memory—Adding physical memory to a computer allows more information to be kept in physical memory, which reduces the need for virtual memory.
* Run fewer applications at once—If you are running multiple applications, more information is kept in memory. Reducing the number of applications running at the same time reduces the amount of memory used and, consequently, the need for virtual memory.

If heavy utilization of the paging file is occurring, moving the paging file to a faster disk, such as an SSD, can improve performance. Windows 10 also allows some USB drives to be used for ReadyBoost. ReadyBoost uses a USB drive as a memory cache similar to a paging file. The USB drive is faster than a mechanical disk but offers no performance improvement when an SSD is being used.

### Processor Bottlenecks

A processor bottleneck occurs when a processor has too much work to do. In a newer computer, processors typically have four or more cores. Each core in a processor can work on only one task at a time. The combination of applications and operating system services running in Windows 10 are typically greater than the number of processor cores. To run multiple applications and perform system tasks, the processor switches between the required tasks very quickly to give the illusion of all activities happening at the same time. When too many tasks must be performed, or an individual task requires too much processor time, the processor becomes a bottleneck.

To identify a processor bottleneck, you monitor the percentage of CPU utilization. If CPU utilization is consistently at 100% then the CPU is a bottleneck.

To resolve a processor bottleneck, do the following:

* Change to a processor with higher clock speed—Processor performance is traditionally measured by clock speed. When comparing processors with the same architecture and number of cores, a processor with a higher clock speed can perform more work in a given time frame. For example, a 3 GHz processor is faster than a 2 GHz processor.
* Change to a processor with more cores—Because so many processes are running in Windows 10 at the same time, it might be beneficial to have additional processor cores. With more processor cores, more tasks can be performed at the same time.
* Add additional processors—Some computers can contain multiple physical processors. Windows 10 Professional and Windows 10 Enterprise can support more than one physical processor. Windows 10 Home can support only one. Having multiple processors means that tasks can be completed more quickly because the second processor provides additional cores for processing.

**Caution**

The motherboard in a computer supports a limited range of processors. In most cases, it is not cost-effective or practical to upgrade only the processor. Purchasing a new computer with more processing capacity is typically required.

### Network Bottlenecks

Network bottlenecks are more common for servers than computers running Windows 10. In the rare circumstance where the network is simply too slow, you can replace the existing network with a faster one. For example, if an old 100 Mbps network is slowing down file sharing between computers, you could replace it with a 1 Gbps network. This might involve replacing network cards, cabling, and switches. The slowest networking component between two systems determines the fastest speed that the two computers can communicate with each other. It is common that the maximum speed of a network connection (for example, 1 Gbps) is not fully realized because overhead and random delays occur that use up some of the network’s capacity to carry data. A 1 Gbps network connection might end up limited to around 800 Mbps of effective data transfer, which is not a bottleneck; it is expected because of administrative and operational overhead on the data stream. As wireless networks become more common at home, problems with wireless performance may have less to do with the local computer and more to do with the networking equipment’s age, component position, and local interference.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-1cTuning Performance

The process for performance tuning is consistent regardless of the problems being experienced. In each case, you perform the following steps:

1. 1

Create a baseline for the computer.

1. 2

Compare the baseline with current performance indicators.

1. 3

Identify possible causes for variations from the baseline.

1. 4

Identify possible fixes for variations from the baseline.

1. 5

Select a fix to implement.

1. 6

Implement the fix and monitor for changes.

1. 7

If the problem is not resolved, undo the fix and repeat [Step 5](javascript://).

1. 8

If the problem is resolved, document the solution for future reference.

When selecting a fix to implement, you should take into account the time involved and the likelihood that the fix will resolve the problem. Sometimes, it is better to attempt several simple fixes, even if they are less likely to fix the problem, before attempting a complex fix that is likely to solve the problem.

Documentation during the performance-tuning process is essential. As you attempt each fix, you should document the changes you are making. This allows you to undo each fix before you try the next one.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**9-2**Performance Monitoring Tools

To identify performance bottleneck in Windows 10, you can use performance monitoring tools included in Windows 10. The tool you select for troubleshooting will depend on the situation. For a quick overview of current performance, Task Manager is a good choice. For a more detailed look at current performance, you can use Resource Monitor. For the most detailed understanding of system performance, you can use Performance Monitor to view current performance statistics and log performance data to file for later analysis.

Go to pg.

[**help**](javascript://)

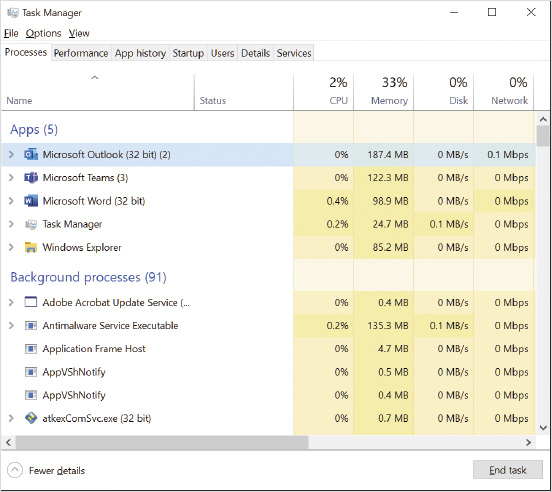
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2aTask Manager

[**Task Manager**](javascript://) provides an overview of the current state of a computer. You often use Task Manager when a computer starts performing poorly and you want to get a quick idea of where the bottleneck might be. The default view in Task Manager shows the applications you are running, but no performance information. You need to switch to the Details view, shown in [Figure 9-1](javascript://), to see the performance information.

**Figure 9-1Task Manager Processes Tab in Details View**



You can access Task Manager in any of the following ways:

* Press Ctrl+Alt+Delete and then click Task Manager.
* Press Ctrl+Shift+Esc.
* Right-click an empty area of the taskbar and then click Task Manager.
* Run taskmgr.exe from a command prompt.

### Processes

The Processes tab in Task Manager shows all user applications running on the computer and background processes. For example, the process Microsoft Word (32-Bit) appears in the list of Apps in [Figure 9-1](javascript://) because it is actively running on that computer. This view provides an easy way to see how much CPU, Memory, Disk, and Network resources are being used overall and by each process. For example, if you see that CPU utilization is at 100%, you can sort the processes by CPU utilization to identify the offending process and then stop it.

The Details tab provides even more detailed information about each process. The process name listed on the Details tab is the name of the executable file instead of the friendly name used on the Processes tab.

**Tip**

To easily find the detailed information about a process, right-click the process on the Processes tab and then select Go to details. This displays the Details tab and highlights the detailed information for the selected process.

For each process on the Details tab, you can see:

* Name—The process executable file.
* PID—The process identifier (PID) is a unique number that is assigned to each process. When multiple instances of an application are running, each has the same name but a unique PID.
* Status—Identifies whether a process is running or suspended. Windows 10 suspends unused processes to save power.
* User name—The user who started the process. You can use this to identify whether a process was started by a user or the system.
* CPU—The percentage CPU utilization of the process.
* Memory—The memory used exclusively by the process.
* UAC virtualization—Identifies whether a process uses UAC virtualization redirect write requests to restricted areas in the file system or registry. For most processes, this is set to Not allowed or Disabled. You can try enabling UAC virtualization for legacy applications that are not able to run properly in Windows 10 with default settings.

**Tip**

You can customize the view on the Processes tab or Details tab by adding more columns of information. Columns are added by right-clicking on any column header and then clicking Select columns.

For each process on the Details tab, you can set the priority of the process. You might be able to boost the performance of an application by raising its priority; however, this is not recommended because raising the priority of one application can be detrimental to other applications.

You can also end a specific process or process tree. Ending a process tree stops the process and all other processes that were started by the process. Ending just the process allows other processes started by the process to continue running.

You can configure a process to run on a specific processor core by setting processor affinity. In the vast majority of situations, system performance will be better if you do not set processor affinity for a process. When processor affinity is not set, Windows 10 optimizes system performance automatically by moving processes among processors as required.

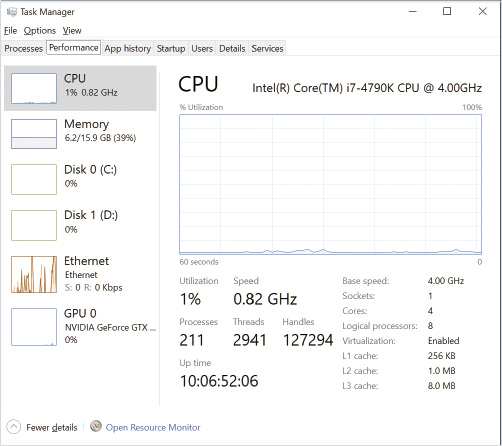
**Tip**

You can view process information similar to Task Manager details in Windows PowerShell by using the Get-Process cmdlet.

### Performance

The Performance tab, shown in [Figure 9-2](javascript://), provides a quick overview of system performance for CPU, memory, disk, Ethernet, Wi-Fi, and GPU (graphics processor). When you select each item on the left side, more detailed information appears on the right side. For example, if you select Disk 0, you see detailed information, such as the brand and model of disk, active time, read and write speed, and response time. As a convenience, a link is also available to start Resource Monitor from this tab.

**Figure 9-2Task Manager Performance Tab**



### Other Task Manager Information

The App history tab shows a summary of what applications have been using resources since the last startup and the total usage of those resources in comparison with one another.

The Startup tab shows a list of applications that start automatically when Windows starts and lets you mark them as enabled or disabled for startup.

The Users tab has a list of users who are currently signed in to the system. If multiple users share a computer and use fast user switching to stay signed in, the users appear in this list. If you expand a user, you can see the processes started by that user. If your account is an administrator, you can sign out users that are disconnected. Signing out users can free up additional memory for better performance or gain access to files that are locked because a user has them open.

The Services tab provides a list of the services running on Windows 10. The information here is approximately the same as the information found in the Services node in Computer Management. From this tab, you can also locate the process associated with a particular service and can start and stop services.

**Activity 9-1**

### Using Task Manager

**Time Required:**10 minutes

**Objective:**Use Task Manager to view system information

**Description:**The primary purpose of Task Manager is to provide a quick overview of system and process performance information. In this activity, you view system information and manage processes by using Task Manager.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, in the search box type **cmd**, and then press **Enter**.

1. 3

In the command prompt window, type **mspaint** and then press **Enter**.

1. 4

Right-click the taskbar and then click **Task Manager**.

1. 5

Note that the initial view for Task Manager lists the running applications but no details. Click the down arrow next to **More details** to expose all of Task Manager’s details if they are not already visible.

1. 6

If necessary, click the **Processes** tab. You can see that both the command prompt and Paint are listed in the Apps section.

1. 7

Expand **Windows Command Processor (2)**. Notice that two processes are listed for this App.

1. 8

Right-click **Windows Command Processor** and then click **Go to details**. This switches to the Details tab, with cmd.exe selected.

1. 9

Right-click **cmd.exe** and then click **End process tree**.

1. 10

Read the warning and then click **End process tree**. This closes both the command prompt and Paint because Paint was started by the command prompt.

1. 11

Click the **CPU** column header once. This sorts the processes by CPU utilization. A down arrow above the column title indicates that the processes are sorted in descending order with the highest CPU utilization at the top of the list.

1. 12

Click the **Services** tab. This tab displays the status of services running on the computer.

1. 13

Click the **Performance** tab. This tab provides some basic CPU and memory utilization information.

1. 14

Click **Ethernet** on the left side of the window. This displays an overview of network utilization and status.

1. 15

Click the **Users** tab. This tab displays a list of all users who are signed in. Multiple users can be signed in at the same time when fast user switching is used.

1. 16

Close the Task Manager window.

Go to pg.

[**help**](javascript://)

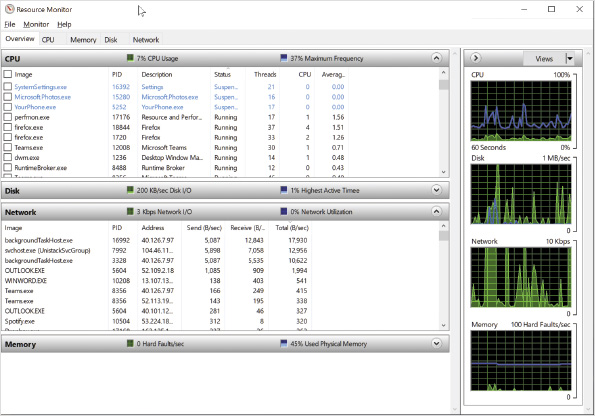
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2bResource Monitor

[**Resource Monitor**](javascript://), shown in [Figure 9-3](javascript://), provides real-time monitoring of the most common system performance indicators that is more detailed than what is provided by Task Manager. On the Overview tab, you can view performance indicators for CPU, disk, network, and memory. Key performance indicators are also summarized in graphs at the side of the screen.

**Figure 9-3Resource Monitor**



Enlarge Image

The data displayed in Resource Monitor are updated in real time while monitoring is active. The constant updating sometimes makes it hard to read the data. Monitoring can be stopped to freeze the displayed values. If you want to view information for only a few processes, you can select those processes to filter the information.

### CPU

The CPU tab is used to monitor processor performance and determine whether the processor is a bottleneck. When you select the CPU tab, a list of running processes is displayed. From this tab, you can sort the list of active processes by their CPU activity, threads spawned, status, or PID.

Selecting a specific process populates the Associated Handles and Associated Modules summary sections with information from that process. The Associated Handles section displays files, registry keys, and other system resources that are being used by the process. The Associated Modules section displays DLL files that are being used by the process.

You can suspend, resume, or end a process. By suspending the operation of a process, you can quickly test its effect on the computer’s performance. Note that suspending a process can cause instability, so this advanced feature should be used with caution.

### Memory

The Memory tab is used to monitor memory performance and determine whether the memory subsystem is a bottleneck. The Memory tab displays memory information for each process. The Physical Memory area displays overall memory usage information in a graphical form detailing how portions of memory have been allocated. The graphical view can help you get a general awareness of the current memory demands.

### Disk

The Disk tab is used to monitor disk performance and determine whether the disk subsystem is a bottleneck. When you select the Disk tab, a list of processes performing disk activity is displayed. When a process has not accessed the disk for 60 seconds, it is removed from the list. The disk activity shown for each process includes which files are being accessed. Sometimes this helps to identify which activity is causing high disk utilization.

The Storage section reports overall activity of each storage location, organized by logical disk. Each logical disk reports the physical disk it is on, the percentage of time that disk is active, space usage, and the number of disk operations waiting to be completed in the disk queue. A high disk queue length is usually indicative of a disk subsystem that is overwhelmed or experiencing technical issues.

### Network

The Network tab is used to monitor network performance and determine whether the network subsystem is a bottleneck. On the Network tab you can see information about network activity and the endpoints that are generating traffic or are capable of receiving network data. TCP connection details are provided and include statistics about packet loss and latency in milliseconds between a listed local and remote address. Heavy packet losses or high latency is a sign that the network connection is oversaturated or experiencing faults somewhere between the two addresses.

**Activity 9-2**

### Using Resource Monitor

**Time Required:**5 minutes

**Objective:**Use the Resource Monitor tool to view performance data

**Description:**The Resource Monitor gives you a quick overview of what is happening on your system with regard to the CPU, disk, network, and memory. In this activity, you use Resource Monitor.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, type **resource**, and then click **Resource Monitor**.

1. 3

Click the **Overview** tab if it is not already selected. Review the graphs at the right side of the screen for CPU, Disk, Network, and Memory.

1. 4

Expand the **CPU** summary bar if it is not already expanded and review the listed processes in the Image column. Scroll down to view processes that are running. Review the column information available for each process.

1. 5

Click the **CPU** column header so that a down arrow appears in the header just to the left of the column title. This sorts the processes from highest to lowest based on their current CPU utilization. If you click again, the sort order is reversed.

1. 6

Collapse the **CPU** summary bar and expand the **Disk** summary bar. Read the information about each process. This area provides disk usage information for each process running on the system.

1. 7

Collapse the **Disk** summary bar and expand the **Network** summary bar. Read the information about each process. This area provides network usage information for each process running on the system.

1. 8

Collapse the **Network** summary bar and expand the **Memory** summary bar. Read the information about each process. This area provides memory usage information for each process running on the system.

1. 9

Click the **CPU** tab, and in the Processes area, click the **Image** column header twice to sort alphabetically from A to Z.

1. 10

Select the **explorer.exe** process and expand the **Associated Handles** summary bar. Scroll down and review the resources being used by explorer.exe.

1. 11

Collapse the **Associated Handles** summary bar and expand the **Associated Modules** summary bar. Scroll down and review the DLL files being used by explorer.exe.

1. 12

In the Processes area, uncheck **Image** in the column header to show information for all processes again.

1. 13

Click the **Memory** tab and review the available information.

1. 14

Click the **Disk** tab and review the available information.

1. 15

Click the **Network** tab and review the available information.

1. 16

Close all open windows.

Go to pg.

[**help**](javascript://)

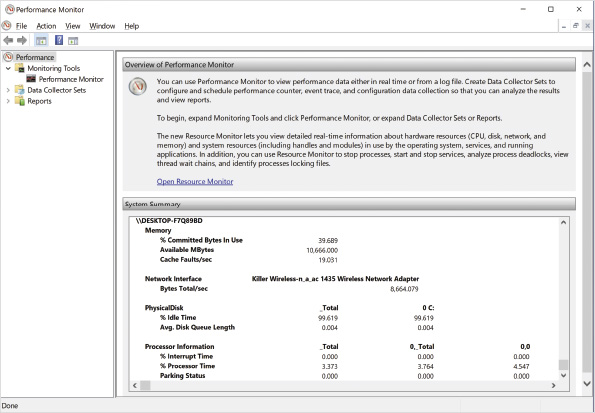
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-2cPerformance Monitor

[**Performance Monitor**](javascript://), shown in [Figure 9-4](javascript://), is a tool that provides access to highly detailed performance information in Windows 10. When you open Performance Monitor, a summary screen with the more commonly monitored counters is displayed, but more advanced functions are typically used. You can create reports or capture and log information over time and display it in a variety of graph types. You can also configure alerts that are triggered by performance counter values.

**Figure 9-4Performance Monitor**



Enlarge Image

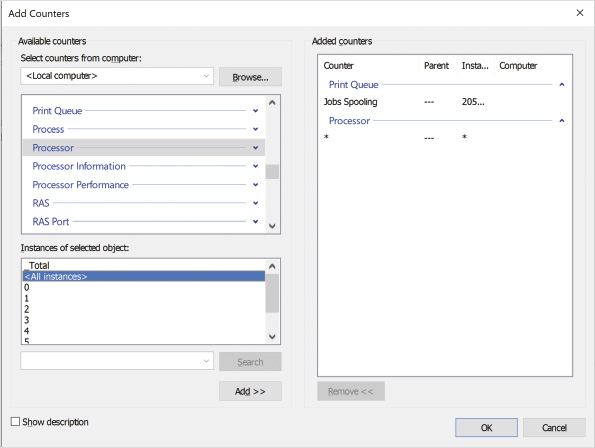
### Counters

Unlike Resource Monitor, Performance Monitor allows you to select the individual counters you want to view. This helps you to focus monitoring on a specific operating system element. In some cases, after finding a general problem by using Resource Monitor, you might want to find more detailed information by using the Performance Monitor. Performance Monitor can also monitor many counters that are not shown in Resource Monitor.

When you add a counter, it can be from the local computer or another computer available over the network. In most cases, you will monitor the local computer. Some counters, however, should be monitored over the network to prevent monitoring from affecting the validity of the data. For example, if you are logging disk activity, you should monitor it over the network to ensure that the logging process is not creating disk activity that affects your results.

Counters are divided into categories, as shown in [Figure 9-5](javascript://). Common counter categories include processor, memory, physical disk, TCPv4, system, and logical disk. Many other categories are also available that offer specialized counters of interest. Some applications, such as Microsoft SQL Server, add new counters when you install the application.

**Figure 9-5Add Counters Dialog Box**



Enlarge Image

For each counter, there might be multiple instances of that counter to choose from. For example, in a computer with multiple processors, each processor is an instance. This allows you to monitor the information about each processor separately, or you can choose to view a combined total for all processor instances. Selecting a counter displays information about that counter’s collected data as a chart type.

Five different chart types are available for viewing performance data, including:

* Line—Displays a line for each selected counter. Each line is displayed in a different color to help distinguish them. This chart type allows you to visualize performance over time. This is the default chart type.
* Histogram bar—Displays a vertical bar for the current value of each performance counter. This chart type is useful for comparing similar types of counters with one another at the same time.
* Report—Displays the current value of each performance counter in decimal format. This is useful when you want to see the exact value of a performance counter rather than compare it with other performance counters.
* Area—Shows data in a similar format to a line chart, but the area below the line is a solid color. This can be useful to identify variances between two values, but a high value for one counter can hide the data for another counter.
* Stacked area—Displays a combined total of the selected counters and each counter’s portion of the total. This can be useful when monitoring parts of a whole resource, such as the cores in a CPU. The total of all cores stacked is equal to the overall CPU utilization.

**Activity 9-3**

### Using Performance Monitor

**Time Required:**10 minutes

**Objective:**Use Performance Monitor to view counter values

**Description:**Performance Monitor allows you to view the value of performance counters. You can choose to display the values in several different formats. The counters allow you to monitor system performance. In this activity, you use Performance Monitor to view system activity.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, type **Performance**, and then click **Performance Monitor**.

1. 3

In the Performance Monitor window, read the information on the summary screen.

1. 4

If necessary, expand **Monitoring Tools**, and select **Performance Monitor**. You can see that by default % Processor Time is displayed. The default report type shown is a line chart.

1. 5

In the toolbar, click the **Add** button (the plus symbol).

1. 6

In the list of Available counters, expand **PhysicalDisk** and click **% Disk Time**. This counter monitors how often the disk is busy.

1. 7

In the Instances of selected object box, click **<All instances>**. This selects disk 0 for monitoring. If multiple disks were present in this computer, multiple instances would be listed.

1. 8

Select the **Show description** check box to enable it. This displays a description of each counter as you select it.

1. 9

Click **Add**.

1. 10

In the list of Available counters, expand **Memory** and then click **Available MBytes**. This counter monitors how much physical memory is free for use by processes.

1. 11

Click **Add** and then click **OK**. Notice that new lines are added to the graph. The graph is scaled from 0 to 100, but the new counters might provide values outside that range.

1. 12

At the bottom of the screen, click **% Disk Time** for the instance \_Total. The Last, Average, Minimum, and Maximum values now reflect what has been measured for % Disk Time. Note the average value. A small value here might not register on the scrolling line graph. A scale value adjusts the counter values to better fit in the graph range from 0 to 100. The default scale value is 1.

1. 13

Right-click **% Disk Time** for the instance \_Total and then click **Properties**. Select a new color for the counter’s displayed line that will be easy to see and differentiate from the other counters.

1. 14

Click the **Scale** arrow, select **10.0** to multiply all counter values for this counter by 10 before displaying them on the line graph, and then click **OK**.

1. 15

At the bottom of the screen, right-click **Available MBytes** and then click **Scale Selected Counters**. This automatically changes the scale used to measure the counter. The line for this counter was previously at the very top of the chart and did not provide useful information.

1. 16

On the toolbar, click the **Change graph type** button. This changes the graph to a bar chart.

1. 17

Click the **Change graph type** button again. This changes the graph to a report.

1. 18

In the left pane, right-click **Performance Monitor** and then click **Properties**. Notice that on the General tab, you can modify the graph sample rate and the time span that is displayed.

1. 19

Click **Cancel** and leave Performance Monitor open for the next activity.

### Data Collector Sets

A [**Data Collector Set**](javascript://) organizes multiple counters into a single unit. This makes monitoring performance easier to manage in much the same way that assigning users to groups makes system security easier to manage for individual users.

A Data Collector Set can monitor and log the following types of data:

* Performance counters—This records data on a timed basis. The value of selected performance counters is recorded at defined intervals, such as 1 second.
* Event trace—This tracks when system events occur. In this way, real-time information is collected about the system rather than samples. The information collected is based on the selection of an event trace provider. For each provider, you can select which specific events are tracked.
* Configuration—This tracks changes to the registry and when they occurred. You can use this to monitor changes made by application installations.

When you configure a Data Collector Set, it is often to log performance information to disk. For event trace data and configuration data, the changes must be logged to disk.

Data Collector Sets are not always running. If they were, very large log files would be generated and system performance would suffer. You can manually start Data Collector Sets when you are performing troubleshooting, or you can start them with an alert. If you are collecting a baseline, you should schedule the Data Collector Set to run at a consistent time.

Data Collector Set scheduling is very flexible, allowing you to create multiple schedules based on a start date, end date, day of week, and time of day. Stopping a Data Collector Set is configured most often based on overall collection duration or a maximum collected data limit. When a Data Collector Set stops, you can run a task. This can be used to process the log files after data collection is complete. For example, you might have a script that looks for specific event values within the logs, or you might simply copy logs to a network location for further analysis.

**Activity 9-4**

### Logging Performance Data

**Time Required:**15 minutes

**Objective:**Log performance data by using a Data Collector Set

**Description:**Data Collector Sets allow you to group counters for easier manageability. If you want to log performance data, it must be done with a Data Collector Set. In this activity, you create a Data Collector Set and log performance data to disk.

1. 1

In the left pane of Performance Monitor, expand **Data Collector Sets** and then click **System**. You can see that two predefined Data Collector Sets are created by the system to perform common maintenance tasks.

1. 2

In the left pane, click **Event Trace Sessions**. These are trace providers used by the system to collect system performance data.

1. 3

In the left pane, click **User Defined**. When you create new Data Collector Sets, they are placed in this folder.

1. 4

Right-click **User Defined**, point to **New**, and then click **Data Collector Set**.

1. 5

In the Name box, type **CPU and Disk logging** and then click **Next**. This Data Collector Set will be created from a template.

1. 6

In the Template Data Collector Set box, select each option and read the description.

1. 7

Click **Basic** and then click **Next**.

1. 8

Accept the default Root directory and then click **Next**.

1. 9

Click **Open properties for this data collector set** and then click **Finish**.

1. 10

In the CPU and Disk logging Properties dialog box, on the General tab, read which user the Data Collector Set will run as.

1. 11

Click the **Directory** tab. This tab shows you where the log files will be stored.

1. 12

Click the **Stop Condition** tab. Notice that, by default, the Data Collector Set will stop after 1 minute.

1. 13

Click **OK**.

1. 14

In the left pane, expand **User Defined** and then click **CPU and Disk logging**.

1. 15

Right-click **Performance Counter** in the right pane and then click **Properties**. Notice that all processor-related counters are selected by default.

1. 16

Click **Add**, in the Available counters box, expand **PhysicalDisk**, select **PhysicalDisk** to select all counters, click **Add**, and then click **OK**. This adds all of the counters for the physical disk.

1. 17

Notice that the log format is binary in the Performance Counter Properties dialog box and then click **OK**.

1. 18

In the left pane, click **User Defined**. Notice that CPU and Disk logging has a status of stopped in the right pane.

1. 19

Right-click **CPU and Disk logging** in the right pane and then click **Start**.

1. 20

Wait 1 minute for the data collection to complete.

1. 21

In the left pane, click **Performance Monitor** and, on the toolbar, click the **View Log Data** button. Note that if you hover the cursor over each toolbar button, the name of the button is displayed as a ScreenTip.

1. 22

Under Data source, click **Log files**, click **Add**, double-click the **Admin** folder, double-click the **CPU and Disk logging** folder, double-click the folder with today’s date, click the file **Performance Counter.blg**, and then click **Open**.

1. 23

Click **Time Range**. This displays the time range in the log file. You can select just a subset of the time range to view if you desire. The default setting is to display the entire time range.

1. 24

Click the **Data** tab to select the counters to display from the log file, click **Remove** as required to remove any existing counters, and then click **Add**.

1. 25

Expand **PhysicalDisk**, click **% Idle Time**, and then click **Add**. This adds the total % Idle Time for all physical disks that were logged.

1. 26

Expand **Processor**, click **% Idle Time**, and click **Add**. This adds the total % Idle Time for all processors that were logged.

1. 27

Click **OK**. Notice that the counters are now listed under Counters.

1. 28

Click **OK** to save the settings and display the data on the Performance Monitor graph. If necessary, change the chart view’s graph type to **Line**.

1. 29

Click the **Add** button on the toolbar. Notice that only the PhysicalDisk and Processor counters are available because only those counters were logged.

1. 30

Expand **PhysicalDisk**. Notice that you can select any counter in the category because they were all logged.

1. 31

Click **Cancel** to close the Add Counters window.

1. 32

Leave Performance Monitor open for the next activity.

### Alerts

For performance counters, you can configure an [**alert**](javascript://) instead of logging to disk. After selecting the performance counter you desire for an alert, you also state a threshold value and configure whether the alert is triggered by going above or below the threshold value. For example, you can trigger an alert when the \Memory\AvailableBytes counter drops below 50 MB.

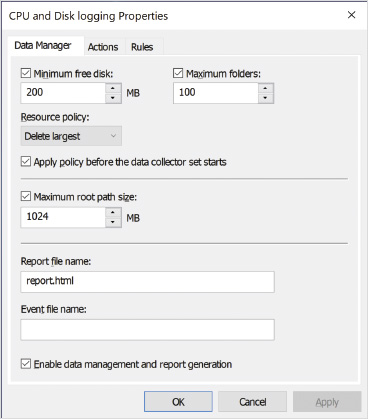
When an alert triggers, the following can be performed:

* Log an entry in the application event log—Placing an event in the application log allows you to search for the event later and incorporate it into your normal system monitoring process.
* Start a Data Collector Set—If you have an ongoing problem that you are trying to monitor, you can start a Data Collector Set when the alert is triggered. For example, if disk utilization is high, you can start a collector set with various counters that help you find the source of the problem.
* Run a scheduled task—Running a task can start any program. In most cases, you will want to run a script. For example, you could run a script that sends the administrator an email notification.

### Data Manager

[**Data Manager**](javascript://) allows you to automatically control the log files and reports that can be generated by Data Collector Sets, as shown in [Figure 9-6](javascript://). You can apply a policy and specify actions. Using Data Manager, you can specify parameters such as minimum free disk space, maximum number of folders, report generation, and deletion preferences to make room for new data.

**Figure 9-6Data Manager Settings**



### Reports

Reports are used to process log file data and display it in a meaningful way. You add rules for report processing in Data Manager for the Data Collector Set. In theory, you could create your own rules for processing log files, but most administrators will never need to do so. Windows 10 includes the rules you are likely to need and runs them automatically.

**Activity 9-5**

### Viewing Reports

**Time Required:**10 minutes

**Objective:**View a report generated by Performance Monitor

**Description:**Performance Monitor can generate reports from log files. To do this, XML-based rules files are applied to the log data. Several system reports are available. In this activity, you view an existing system report.

1. 1

In the left pane of Performance Monitor, below Data Collector Sets, click **User Defined**.

1. 2

Right-click **CPU and Disk logging** in the right pane and then click **Start**.

1. 3

Wait approximately 1 minute for data collection to complete.

1. 4

Right-click **CPU and Disk logging** and then click **Latest Report** on the shortcut menu. The left navigation pane changes focus to highlight the most recent report, and the report’s details are opened in the right pane.

1. 5

Review the information available in the report. Locate the Summary section and read the information available there.

1. 6

Expand **Application Counters** and read the information.

1. 7

Expand each remaining section of the report and read the information.

1. 8

Close Performance Monitor and close all other open windows.

Go to pg.

[**help**](javascript://)

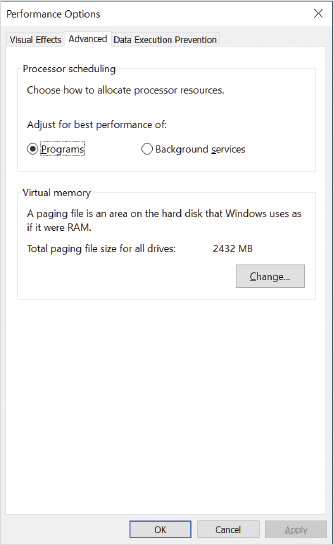
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**9-3**Performance Options

Windows 10 includes the Performance Options dialog box, shown in [Figure 9-7](javascript://), to optimize visual effects, processor scheduling, and virtual memory. To access the Performance Options dialog box, search for the word *performance* in Settings, and then select Adjust the appearance and performance of Windows.

**Figure 9-7Performance Options**



The Visual Effects tab allows you to configure a wide variety of settings that improve how the Windows 10 interface performs. On systems with poor graphics processing performance, disabling some of these features can improve performance. By default, the Let Windows choose what’s best for my computer option is selected.

The Advanced tab lets you select whether processor time is allocated to optimize performance for programs or background services. If Programs is selected, the program running in the active window is given a slightly higher priority than other applications. This ensures that the program you are using is the most responsive on the system. If you select Background services, all programs are given the same priority.

The Advanced tab also gives you access to the settings for [**virtual memory**](javascript://). Virtual memory settings control how the paging file that is used to simulate memory on disk is configured. By default, the paging file is managed automatically by Windows. As more of the paging file is required, it is expanded from the minimum size to the maximum size.

You can manually configure the paging file if you prefer. This allows you to optimize the placement of the paging file. Moving the paging file to its own hard disk optimizes system performance because less contention for disk resources when accessing the paging file will occur. Alternatively, you can spread the paging file over multiple disks to speed access to the file.

Most Windows 10 computers have only a single hard disk, and increasing performance is not possible by adjusting the virtual memory settings. You might, however, want to move the paging file to a different partition to free space on the C: drive if it is almost full.

It is also possible to specify that no paging file is to be used; however, this is not recommended as performance will suffer. Even when systems have sufficient physical memory to hold all active processes and their data, system performance suffers when the paging file is disabled.

**Caution**

Moving the paging file to another volume on the same physical disk provides no performance improvement.

[**Data Execution Prevention (DEP)**](javascript://) is a processor feature that Windows 10 is capable of using. DEP monitors processes to ensure that they do not access unauthorized memory spaces, which is done by various types of malware, to take control of systems. Despite the value of DEP in preventing malware, there is a performance cost. By default, DEP is enabled for only essential Windows programs and services. This protects the core components of the operating system that are likely to be targeted by malware and still preserves system performance. You can enable DEP for all programs and services (and specify exceptions), but this has a significant performance impact and is not recommended.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**9-4**Controlling Application Startup

When you sign in to Windows 10, some applications are started automatically. Most of these applications are small utilities that provide status information or run in the background waiting for communications. For example, messaging clients like Microsoft Teams typically start automatically so that they can provide notifications and accept incoming communication.

On computer systems with limited resources, you might find that having too many applications running at startup causes performance issues. During startup, many applications attempting to start simultaneously can cause a high level of disk activity that overwhelms traditional hard drives and causes the sign-in process to be very slow. After signing in, too many applications running simultaneously might use a large amount of memory and not leave enough for applications you are actively using. To resolve these issues, you might want to stop some applications from starting automatically.

**Tip**

Some malware configures Windows 10 to start the malware executable automatically at startup. Understanding all of the methods for controlling automatic startup can be useful when removing malware.

Go to pg.

[**help**](javascript://)

Application Opened

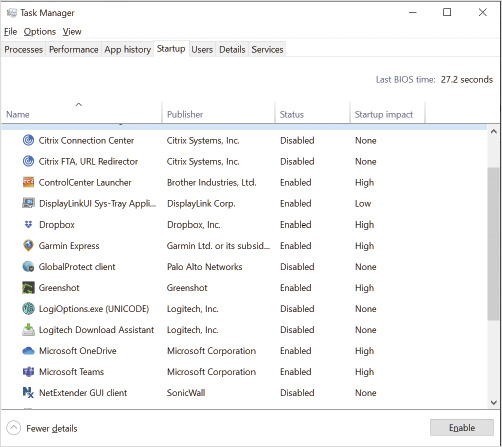
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-4aTools for Managing Application Startup

Most applications that start automatically when you sign in have an option in the application settings to enable or disable automatic startup. If an application has this setting, then modifying this setting is the preferred method for controlling automatic startup. Applications can use multiple methods to configure automatic startup, and using the setting in the application avoids the need to determine which method is being used.

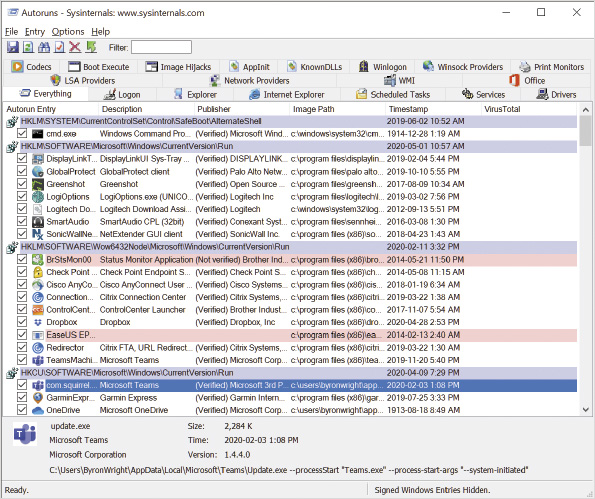
Task Manager is another tool that allows you to control application startup without knowing the exact mechanism that the application is using. On the Startup tab, shown in [Figure 9-8](javascript://), you can enable or disable startup for applications. You can also see the startup impact caused by applications.

**Figure 9-8Task Manager Startup Tab**



For more advanced management of applications and add-ons that start in Windows 10, you can use Autoruns, shown in [Figure 9-9](javascript://). The main advantage of using this tool is that it goes beyond identifying and managing simple application startup. Autoruns also analyzes add-ons that are hooked into networking, File Explorer, and other Windows functions.

**Figure 9-9Autoruns**



Enlarge Image

Autoruns is particularly useful when looking for malware that has embedded itself in Windows. It shows how the add-on or application is starting, the file location, and whether the application publisher is verified. Files in nonstandard locations and with unverified publishers should be investigated. You have the option to delete an item listed in Autoruns if you determine it shouldn’t be there.

**Note 1**

Autoruns is not included as part of Windows 10, but you can download it from the Microsoft website at [https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns](https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns" \t "_blank).

Go to pg.

[**help**](javascript://)

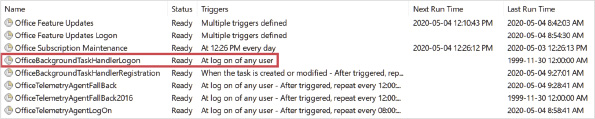
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-4bStartup Methods Used by Applications

Applications can be started by a scheduled task that is triggered at sign in. [Figure 9-10](javascript://) shows a scheduled task that is configured to start when any user signs in. You can disable or delete the scheduled task to stop this behavior, but carefully consider the impact on the application before you make this change.

**Figure 9-10Scheduled Tasks**



Enlarge Image

Several registry keys can be used to automatically start applications. They exist in both HKEY\_LOCAL\_MACHINE and HKEY\_CURRENT\_USER. If they are configured in HKEY\_LOCAL\_MACHINE, the applications start automatically for all users. If they are configured in HKEY\_CURRENT\_USER, the applications start automatically for only the current user.

The registry keys for starting applications automatically are:

* HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
* HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run
* HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
* HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

The RunOnce registry keys apply only one time and then are removed. These are typically used as part of application installation when an application needs to run a configuration routine after install. The Run registry keys are permanent and are triggered each time a user signs in. These keys are ignored if you start in Safe Mode.

In earlier versions of Windows, a Startup folder was visible on the Start menu. Placing a shortcut to an application in this folder caused the application to start automatically when the user signed in. This folder still exists in Windows 10, but it is not visible on the Start menu; however, shortcuts in this folder are still automatically started at sign in. Items in the notification area are commonly started from here.

**Tip**

You can access the Startup folder by navigating to C:\Users\username\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup. You can also type shell:startup in the address bar in the File Explorer window and then press Enter.

**Activity 9-6**

### Configuring Automatic Application Startup

**Time Required:**15 minutes

**Objective:**Configure automatic application startup

**Description:**In this activity, you configure automatic application startup using multiple methods. You also verify that your configuration was successful.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, type **registry**, and then click **Registry Editor**.

1. 3

In the User Account Control dialog box, click **Yes**.

1. 4

In the Registry Editor window, navigate to HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce.

1. 5

Click **Edit** on the menu bar, point to **New**, and then click **String Value**.

1. 6

Type **Paint** and then press **Enter** to name the value.

1. 7

Double-click **Paint**, in the Value data box, type **C:\Windows\System32\mspaint.exe**, and then click **OK**.

1. 8

Close the Registry Editor window.

1. 9

On the taskbar, click **File Explorer**.

1. 10

In the File Explorer window, in the address bar, type **shell:startup** and then press **Enter**.

1. 11

Right-click an open area, point to **New**, and then click **Shortcut**.

1. 12

In the Create Shortcut wizard screen, in the Type the location of the item text box, type **C:\Windows\System32\notepad.exe** and then click **Next**.

1. 13

In the Type a name for this shortcut text box, type **AutoNotepad** and then click **Finish**.

1. 14

Close the File Explorer window.

1. 15

Right-click the taskbar and then click **Task Manager**.

1. 16

In the Task Manager window, click the **Startup** tab and read the items listed. Notice that the Notepad shortcut you created is present but not the Paint application in the RunOnce registry key.

1. 17

Close the Task Manager window.

1. 18

Sign out and then sign in again. Both Notepad and Paint start automatically.

1. 19

Exit Notepad and Paint.

1. 20

Click the **Start** button, type **registry**, and then click **Registry Editor**.

1. 21

In the User Account Control dialog box, click **Yes**.

1. 22

In the Registry Editor window, if necessary, navigate to HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce. Notice that the value you created has been deleted.

1. 23

Close the Registry Editor window.

1. 24

Right-click the taskbar and then click **Task Manager**.

1. 25

In the Task Manager window, click the **Startup** tab and read the items listed. Notice that the Notepad shortcut you created is still present.

1. 26

Click **Notepad** and then click **Disable**.

1. 27

Close the Task Manager window.

1. 28

Sign out and then sign in again. Neither Notepad nor Paint start automatically.

1. 29

On the taskbar, click **File Explorer**.

1. 30

In the File Explorer window, in the address bar, type **shell:startup** and then press **Enter**.

1. 31

Right-click **AutoNotepad** and then click **Delete**.

1. 32

Close the File Explorer window.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**9-5**Troubleshooting Windows 10 Errors

Sometimes Windows 10 or apps installed on Windows 10 become unstable and start to generate errors. Sometimes an error message is displayed on the screen that provides an obvious solution, but more often you need to use additional tools to troubleshoot further. The more information you have about a problem, the more likely it is that you can find a solution. Using precise search terms in a search engine generates results that are most likely to be applicable to your specific problem.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-5aSteps Recorder

When a user reports an error, the information provided by the user is not always accurate. Rather than accepting a description of the error at face value, you are better off to have the user demonstrate the steps to reproduce the error. If you cannot visit or view the user desktop, you can ask the user to record the steps with [**Steps Recorder**](javascript://).

When Steps Recorder is activated, it captures a screenshot each time the user clicks on a screen item. The screenshots and user actions are saved in a report that can be sent via email or saved to a shared storage location. The report is an .mht file that contains both text and the screenshots. To keep the report size small, it is compressed in a .zip file.

Text typed by the user is not captured by Steps Recorder. If information being typed is important, the user needs to add a comment that includes the information being typed.

Go to pg.

[**help**](javascript://)

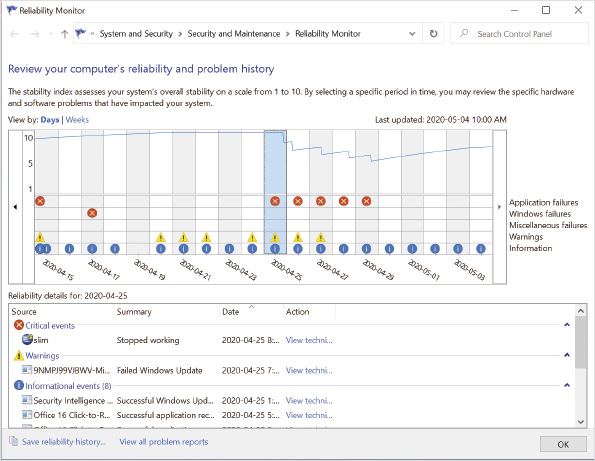
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-5bReliability Monitor

Sometimes a computer has become unstable over time and you would like to identify when the stability problem began. [**Reliability Monitor**](javascript://), shown in [Figure 9-11](javascript://), rates the system stability of Windows 10 and lets you monitor the events that contribute to system stability.

**Figure 9-11Reliability Monitor**



Enlarge Image

Reliability Monitor collects the following data:

* Software installs and uninstalls—Software tracked here includes driver and operating system updates.
* Application failures—Any application that stops responding is logged here.
* Windows failures—Any system failure that results in blue screen errors and boot failures is logged here.
* Miscellaneous failures—Any event not included in other categories is logged here. One type of failure recorded here is improper shutdowns.

The Reliability Monitor graph lets you see the point in time at which significant reliability events occurred. You can use the graph to drill down and find out what event occurred in that time frame and correct the problem. For example, if frequent failures occur after adding a new driver, the driver is the likely cause of the stability problem and it should be removed.

Go to pg.

[**help**](javascript://)

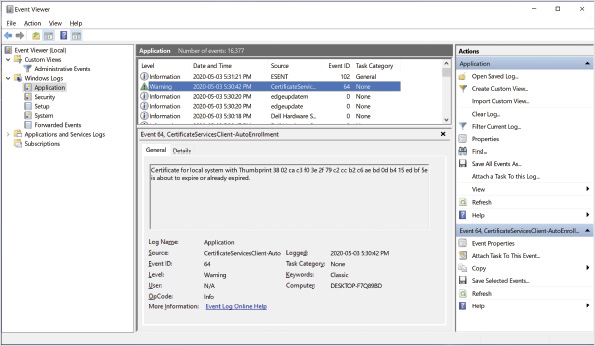
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-5cEvent Viewer

Event Viewer is used to browse and manage events stored in system event logs, as shown in [Figure 9-12](javascript://). You can start Event Viewer as a stand-alone administrative tool or use it in Computer Management. When you are troubleshooting, events in these logs can be a valuable source of information. Sometimes, Error events provide a description of how to fix the problem. In other cases, you can use Error event information in an Internet search engine to find a solution.

**Figure 9-12Event Viewer**



Enlarge Image

The logs in the Windows Logs node of Event Viewer are the most commonly used for troubleshooting. Most non-Microsoft apps and many Microsoft apps write their events to the Application log. The Security log contains Audit Success and Audit Failure events. The System log contains general operating system events, such as services starting and stopping or IP address conflicts.

The Applications and Services Logs node contains event logs for many operating system services. It also contains logs for some management software, such as User Experience Virtualization and App-V. In general, each service or app has its own log.

The Custom Views node is used to create filtered views that can contain specific event types from specific sources. You can create a view that gathers events you require for working with a specific application that writes information to various logs. The Administrative Events view shows Critical, Error, and Warning events from all logs.

You can use the Subscriptions node to copy events from a remote computer to yours. This can be useful when you are monitoring several computers. By default, the events from a subscription are copied into the Forwarded Events log.

### Finding Events

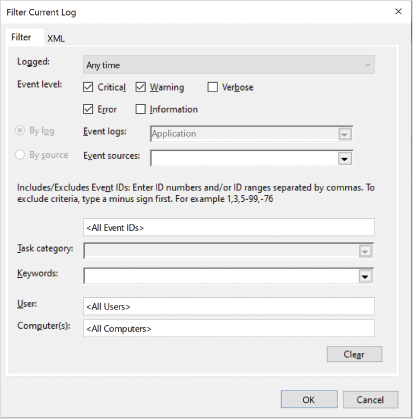
By default, when you view an event log, you see all of the events listed in it. Sometimes, you can scroll up and down in the list of events to find helpful information, but it can be useful to limit the visible events to only those in which you’re interested.

If you have a general idea of what you’re looking for during troubleshooting, but you don’t know the event ID or event source, then you can search for a specific word by using the Find option. When you use Find, the search applies to all text in the events for a single log.

You can also filter individual logs to find the events you want to see, as shown in [Figure 9-13](javascript://). You can use this dialog box to filter by time, event level, event source, event ID, keyword, user, and computer. It is most common to filter by:

* Event level to see only errors or warnings when searching for general information
* Event ID to see instances of only specifically identified events that you know are relevant
* Event source to see all events from a subsystem you are troubleshooting

**Figure 9-13Event Log Filtering Options**



If you are using a filter often, you can create a custom view that applies that filter. Then you can select the view instead of recreating the filter each time. When you create a custom view, you can include events from multiple logs. This is useful when you are troubleshooting an application or subsystem that writes events in multiple logs.

### Managing Event Logs

Most of the time you don’t need to do anything to manage event logs. The default configuration is sufficient in most cases; however, you can configure the following:

* Maximum log size—Sometimes on a busy system you increase the maximum log size to allow more events to be retained.
* Log behavior when maximum log size is reached—By default, the oldest events in the log are removed when new events are added. If you want to ensure that older events are not lost before you can review them, you can archive the log when full or choose not to overwrite events. If you archive the log when full, you’ll need to periodically remove the archives to ensure that the C: drive does not run low on space. If you choose Do not overwrite events, then new events are not recorded when the log is full, and you need to manually clear the log before new events are recorded.

### Triggering Scheduled Tasks

You can also attach a scheduled task to a specific event. When the event appears in the event log, the scheduled task is triggered. This can be useful if you want to be notified when a specific event occurs. This can also be used to resolve problems that can be resolved simply with a script. For example, the script could restart a service when the service generates an error.

### Event Log Forwarding

Most of the time, you use Event Viewer to view events generated on the local computer, but sometimes it’s useful to see events generated on multiple computers in a single place. For example, you might want to monitor performance for a specific application that is installed on multiple computers. Event subscriptions allow events to be copied from the computer that generates the event to another computer that collects the events.

When you configure a collector-initiated subscription, the collector computer queries Windows Remote Management (WinRM) on the event source to retrieve the events. Windows 10 does not configure WinRM by default; you need to configure it by issuing the winrm quickconfig command at a command prompt or a Windows PowerShell prompt.

**Caution**

The quick configuration for WinRM allows any computer to connect. You can use advanced configuration options to limit connections to only allowed IP addresses.

On the collector computer, you also need to enable and configure Windows Event Collector Service. If you do not configure it before attempting to create a subscription, you will be prompted to configure it automatically. If you issue the wecutil qc command at a command prompt or Windows PowerShell prompt, it will be configured before starting the subscription.

**Note 2**

For more detailed information about event log subscriptions see the Windows Event Collector page at [https://docs.microsoft.com/en-us/windows/win32/wec/windows-event-collector](https://docs.microsoft.com/en-us/windows/win32/wec/windows-event-collector" \t "_blank).

On a domain-based network, to give the collector computer permission to access event logs, you need to make the computer account of the collector computer a member of the Event Log Readers Group on the source computer. In a workgroup environment, you need to configure a user account as a member of the Event Log Readers Group instead.

**Tip**

Security events are not accessible to members of the Event Log Readers Group. If you want to collect security events, the user account needs to be a member of the Administrators group.

**Activity 9-7**

### Using Event Viewer

**Time Required:**10 minutes

**Objective:**Use Event Viewer to view logged events

**Description:**In this activity, you configure automatic application startup using multiple methods. You also verify that your configuration was successful.

1. 1

If necessary, startup your computer and sign in.

1. 2

Click the **Start** button, type **event**, and then click **Event Viewer**.

1. 3

In the Event Viewer window, in the Summary of Administrative Events area, expand **Error**, and scroll down to review the events. You can use this to get an overview of Error events in all logs.

1. 4

In the navigation pane, expand **Windows Logs** and then click **System**.

1. 5

Double-click the top event to view the details and then click **Close**.

1. 6

Right-click **System** and then click **Filter Current Log**.

1. 7

In the Filter Current Log dialog box, click the Event sources arrow, scroll down, select **Kernel-General,** and then click **OK**. Only events from the Kernel-General source are displayed.

1. 8

Right-click **System** and then click **Clear Filter**.

1. 9

Right-click **System** and then click **Find**.

1. 10

In the Find dialog box, in the Find what text box, type **Time** and then click **Find Next**.

1. 11

Click **Cancel** and then double-click the selected event to view it.

1. 12

Read the event information and identify where the word time is located. It might be part of a larger word.

1. 13

Click the Details tab, read through the detailed information, and then click **Close**.

1. 14

In the left navigation pane, expand Applications and Services Logs, expand Microsoft, click **Windows**, and then read the list of event logs for Windows services.

1. 15

In the left navigation pane, expand Custom Views and then click **Administrative Events**. This view shows Error and Warning events from multiple event logs.

1. 16

Close the Event Viewer window.

### Viewing Events by Using Windows PowerShell

You can use Windows PowerShell to view event log contents on the local computer or remote computers. Most people find it much easier to work with Event Viewer than the Get-WinEvent cmdlet in Windows PowerShell. So, Get-WinEvent is typically used only when you have a specific need to create a script that analyzes event log contents.

**Note 3**

For detailed information about how to use Get-WinEvent, see the Get-WinEvent page at [https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.diagnostics/get-winevent?view=powershell-5.1](https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.diagnostics/get-winevent?view=powershell-5.1" \t "_blank)

**Activity 9-8**

### Use Windows PowerShell to View Events

**Time Required:**10 minutes

**Objective:**Use Windows PowerShell to view logged events

**Description:**In this activity, you configure automatic application startup using multiple methods. You also verify that your configuration was successful.

1. 1

If necessary, start your computer and sign in.

1. 2

Right-click the **Start** button and then click **Windows PowerShell (Admin)**.

1. 3

In the User Account Control window, click **Yes**.

1. 4

At the Windows PowerShell prompt, type **Get-WinEvent -Listlog \*** and then press **Enter**. This lists all event logs.

1. 5

Type **Get-WinEvent -Listlog S\*** and then press **Enter**. This lists all event logs that start with the letter S.

1. 6

Type **Get-WinEvent -LogName System -MaxEvents 10** and then press **Enter**. This lists the most recent 10 events from the System log.

1. 7

Type **Get-WinEvent -LogName System -MaxEvents 1 | Format-List \*** and then press **Enter**. This shows the details of the most recent event in the System log.

1. 8

Close the Windows PowerShell prompt window.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**9-6**Local File Recovery and Backup

If user data is stored on a Windows 10 computer, it should be backed up to ensure that it can be recovered in case of a hardware failure. In most large organizations, files are stored on central servers where they can easily be backed up and restored by administrators. When users need to keep files locally on their computer, such as when they are in a workgroup or while using a mobile computer while traveling, the best solution is to store data in a cloud service, such as OneDrive. When you synchronize files with OneDrive, they are stored locally and automatically backed up offsite. Your data is protected if you lose you device or if there is a major disaster, such as your house burning down.

File History is the current tool that you should use to make local backups of data to an external hard drive or network location. Backup and Recovery (Windows 7) is still present in Windows 10, but it is primarily there to support restoring data from older Windows 7 backups.

Go to pg.

[**help**](javascript://)

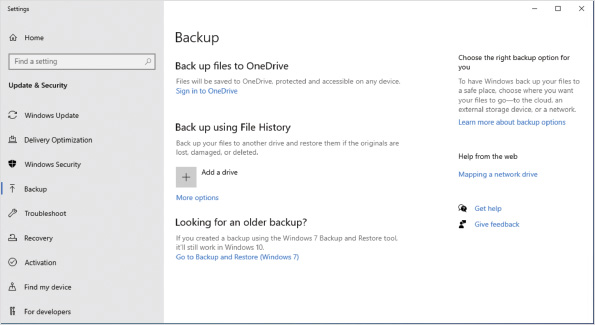
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-6aConfiguring File History

[**File History**](javascript://) backs up data to an external hard drive or a network location. The configuration of File History is user specific and is meant to backup only user data. File History does not perform a complete system backup. You configure File History from the Backup settings shown in [Figure 9-14](javascript://). File History is disabled by default, because you need to pick a location to store backup data that will be available if the primary drive fails.

**Figure 9-14Backup Settings**



Enlarge Image

**Tip**

To specify a network location for File History, you need to use the File History settings in Control Panel.

When you attach an external hard drive and configure it for use by File History, the drive does not get erased. Backup data is added to the drive using the drive’s free space. Note that if the source files include any EFS-protected files, the external drive should be formatted with NTFS to back up the source data properly.

File History creates a series of folders at the root of the drive selected to hold File History data. The path is F:\FileHistory\username\workstationName where F: is replaced with the drive letter assigned to the external drive selected for use by File History on that system.

You can customize File History to include or exclude specific folders, but the default configuration includes Libraries, Desktop, Contacts, and Favorites. Libraries includes common folders, such as Documents and Pictures.

The first backup takes a copy of all files monitored by File History. The backup process happens in the background and doesn’t require monitoring. The initial backup generates disk activity that might be noticed on systems with poor disk performance but is not noticeable on most systems. Future backups are much smaller and copy only files that have changed. New instances of a file are saved in the same backup folder, but with a different date and time stamp within parentheses added to the title.

**Caution**

File History content is not compressed or encrypted on the external drive. Anyone who steals the drive will have ready access to the drive’s contents unless it is encrypted with a technology, such as BitLocker.

Files are backed up every hour by default. The backup frequency can be changed to as little as every 10 minutes or as much as every 24 hours. The retention period for backup data can be changed so the oldest backup data will be deleted when space is needed for newer backup files, kept for a range from one month to two years, or to be kept forever (the default).

**Caution**

If the external drive selected for File History runs out of space, backups stop. To avoid this, select to keep backups Until space is needed.

Only one backup drive can be configured for use by File History at a time. If you want to switch from using one drive to another, you must first stop using the current drive and add the new one. When you stop using a drive with File History, the backed-up data on that drive is not deleted.

**Activity 9-9**

### Configuring File History

**Time Required:**10 minutes

**Objective:**Configure File History settings

**Description:**In this activity, you simulate a separate internal disk drive by adding a virtual disk to the system and then configuring it for use with File History. Note that using a virtual disk drive is for lab purposes only and is not recommended for backing up production machines, because the virtual disk does not remain attached after the system is restarted.

1. 1

If necessary, start your computer and sign in.

1. 2

Right-click the **Start** button and then click **Disk Management**.

1. 3

Click **Action** on the menu bar and then click **Create VHD**.

1. 4

In the Location box, type **C:\VHD Storage\VHDFileHistory.vhdx**.

1. 5

Change the Virtual hard disk size unit from MB to GB.

1. 6

In the Virtual hard disk size text box, type **4**.

1. 7

In the Virtual hard disk format area, click **VHDX**.

1. 8

Confirm that **Dynamically expanding (recommended)** in the Virtual hard disk type area is selected and then click **OK**.

1. 9

In the bottom pane, scroll to the new 4 GB disk, right-click the disk name, and then click **Initialize disk**. Accept the default settings in the Initialize Disk dialog box and then click **OK**.

1. 10

Right-click the 3.98 GB of unallocated space on that disk and then select **New Simple Volume**.

1. 11

In the new Simple Volume Wizard, click **Next** twice to accept the default volume size, and note the assigned drive letter here: .

1. 12

Click **Next** to accept the assigned drive letter.

1. 13

In the Volume label box, type **File History Data** and then click **Next**.

1. 14

Click **Finish** to create the new virtual disk. If you are prompted to format the disk before using it, you can safely cancel the prompt.

1. 15

Close the Disk Management window.

1. 16

Click the **Start** button and then click the **Settings**.

1. 17

Click **Update & security** and then click **Backup**.

1. 18

Under the heading Back up using File History, click **Add a drive**.

1. 19

When the drive search completes, click the drive labeled **File History Data**. Note that the Add a drive section is replaced with a toggle switch to enable or disable automatic back up of files.

1. 20

Click the **More options** link.

1. 21

In the Back up my files box, select **Every 10 minutes**.

1. 22

In the Keep my backups box, select **Until space is needed**.

1. 23

Below Overview, click **Back up now**. Note that the status changes in the Overview section, but no progress window opens.

1. 24

Close the Settings window.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-6bConfiguring Backup and Restore (Windows 7)

[**Backup and Restore (Windows 7)**](javascript://) is included in Windows 10 primarily to allow access to older backups created in Windows 7. A common scenario for using this would be migrating data from an older computer running Windows 7 to a new computer running Windows 10. It is possible to configure Backup and Restore (Windows 7) to perform daily backups to an external disk, just like you could in Windows 7, but you should use File History instead.

One feature available in Backup and Restore (Windows 7) that’s not found in File History is a complete system backup. This is referred to as a system image in Backup and Restore (Windows 7). A system image is a complete copy of the computer, including the operating system, applications, and data.

**Caution**

The System Image Backup option is deprecated beginning in Windows 10 version 1709. Microsoft recommends using a third-party backup solution if you want to back up system images.

Go to pg.

[**help**](javascript://)

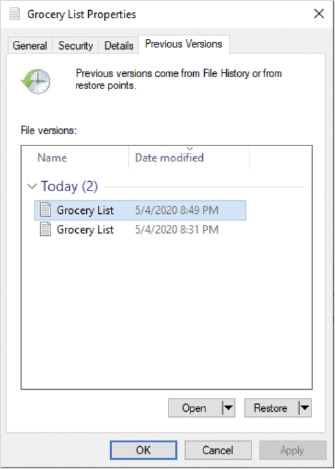
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-6cRestoring Previous Versions of Files and Folders

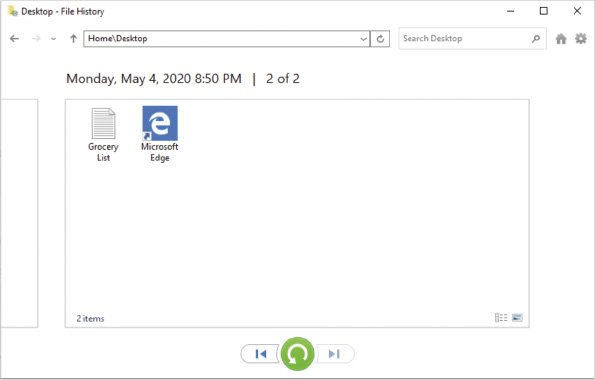
If File History or Backup and Restore (Windows 7), or both, have been configured to protect data, that data can be recovered using a feature called [**Previous Versions**](javascript://). You can browse to a location in File Explorer and open the properties of a file or folder to view the Previous Versions tab, as shown in [Figure 9-15](javascript://). A list of known previous versions is displayed. You can recover an old version of the content and restore it in the same place or to an alternate location for inspection.

**Figure 9-15Previous Versions of a File**



If a file has been deleted, you can’t view the previous versions by selecting the file in File Explorer. You can, however, view the previous versions for a folder to display files that have been deleted, as shown in [Figure 9-16](javascript://). In this window, you use arrows to move back and forth between available versions and click the green arrow to restore.

**Figure 9-16File History for a Folder**



Enlarge Image

**Activity 9-10**

### Restoring Previous Versions of Files

**Time Required:**20 minutes

**Objective:**Restore files from File History

**Description:**In this activity, you create a sample Grocery List file that will be backed up with multiple versions and restored to identify supporting backup data elements.

1. 1

If necessary, start your computer and sign in.

1. 2

Right-click anywhere on the Desktop, point to **New**, and then click **Text Document**.

1. 3

Edit the name of the new document to be **Grocery List** and then press **Enter** to save the change.

1. 4

Double-click the **Grocery List** text document on the desktop to open it. In the Notepad editor window, enter the text **Version one – eggs**.

1. 5

Exit Notepad and when prompted to save your changes, click **Save**.

1. 6

Click the **Start** button, type **backup**, and then click **Backup settings**.

1. 7

Below Back up using File History, click **More options** and then click **Back up now**. You are triggering a manual backup to avoid waiting 10 minutes for the file to be backed up.

1. 8

Leave the Settings window open for later in the Activity.

1. 9

On the Desktop, double-click the **Grocery List** text document.

1. 10

In the Notepad editor window, edit the text to read **Version two – eggs, apples**.

1. 11

Exit Notepad and when prompted to save your changes, click **Save**.

1. 12

In the Settings window, click **Back up now**.

1. 13

On the Desktop, right-click the **Grocery List** document and then click **Restore previous versions**. Note that the Properties window for the file opens and the Previous Versions tab is selected by default.

1. 14

Select the oldest version of the file in the list and then click **Restore**.

1. 15

In the Replace or Skip Files dialog box, click **Replace the file in the destination**. Note that a progress indicator is temporarily displayed and then File Explorer opens to show the restored content.

1. 16

In File Explorer, double-click the **Grocery List** file and note that the original version of the document has replaced version two.

1. 17

Exit Notepad and close the Grocery List Properties dialog box.

1. 18

In File Explorer, click the **Home** tab on the ribbon and then click **History** in the Open group on the ribbon.

1. 19

If necessary, in the address bar, remove **Grocery List.txt** from the path and then press **Enter**. The previous versions for the Desktop folder are shown.

1. 20

Click the **left arrow** at the bottom of the File History window until you reach the first File History backup. Note that the Grocery List file is not listed because the first File History backup was made before the file existed.

1. 21

Click the **right arrow** at the bottom of the File History window until you reach the latest File History backup.

1. 22

Double-click the **Grocery List** file within the last File History backup, which previews the contents of the file in the File History window. In this preview mode, the arrows at the bottom of the screen allow you to examine different versions of the content.

1. 23

Confirm that version two of the Grocery List content is displayed and then click the **Restore to original location** (green circular arrow) button.

1. 24

In the Replace or Skip Files dialog box, click **Replace the file in the destination**.

1. 25

Close the File History window.

1. 26

In the Settings window, scroll to the bottom and click **Stop using drive**. If you receive an error here, a window is open that is viewing File History information.

1. 27

On the taskbar, click File Explorer and then browse to the drive letter you noted in [Step 11](javascript://) of [Activity 9-9](javascript://).

1. 28

Navigate to the folder H:\FileHistory\UserX\PcX\Data\C\Users\UserX\Desktop, where H: is the drive letter noted in [Step 11](javascript://), UserX is the user you are signed in as, and PcX is the name of your computer.

1. 29

Review the versions of the Grocery List file in that folder and note the difference in the file names based on time.

1. 30

Close all open windows.

1. 31

Do not restart your computer or sign out before proceeding to the next activity to ensure that the File History Data virtual hard drive remains attached and available.

Go to pg.

[**help**](javascript://)

Application Opened

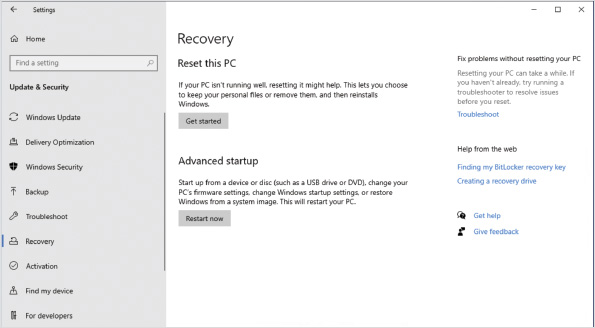
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**9-7**System Recovery

If a computer running Windows 10 has minor problems, you might be able to resolve those errors by researching the issue and finding help online. Sometimes, however, it is not an effective use of time to spend hours troubleshooting and tinkering when you can perform a system recovery instead. If a computer running Windows 10 does not boot, you must perform a system recovery.

Windows 10 has two primary recovery options, shown in [Figure 9-17](javascript://). Reset this PC sets your computer back to the state of a newly installed instance of Windows 10. This is much like performing a factory reset on a tablet or phone. Advanced startup provides a number of options for troubleshooting startup or recovering from backup.

**Figure 9-17Recovery Options**



Enlarge Image

Go to pg.

[**help**](javascript://)

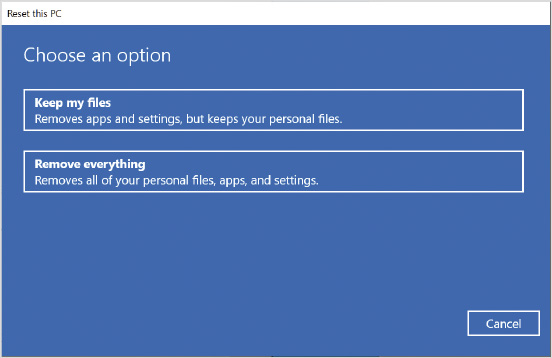
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-7aReset this PC

When you choose [**Reset this PC**](javascript://) as a recovery method, it removes all apps and puts settings back at their default values; however, you have the option to keep your data files and settings, as shown in [Figure 9-18](javascript://). When you keep files and settings, all user accounts and profiles are retained, but not application files in AppData.

**Figure 9-18Reset This PC Options**



You also get the option to choose whether to perform a local reinstall or a cloud download. A local reinstall uses Windows 10 installation files that are already cached on your computer. A local reinstall avoids downloading installation files, but if you’re concerned that malware might have infected those files, you should choose to perform a cloud download. A cloud download obtains the Windows 10 installation files over the Internet from Microsoft to avoid any risk of malware infecting the installation files.

**Caution**

A cloud download will take significantly longer to perform than a local reinstall on a slow network connection because a large amount of data must be downloaded.

If your computer came from the factory with applications installed and you selected to keep your files, you will likely have the option to restore the apps and settings that came with the computer. No option is available to retain apps that you have installed. A list of apps being removed will be displayed before the reset is performed.

**Note 4**

For a detailed description of the steps performed during a reset, see Optimize Windows 10 PC reset using the cloud at [https://insider.windows.com/en-us/articles/optimize-windows-10-pc-reset-using-the-cloud/](https://insider.windows.com/en-us/articles/optimize-windows-10-pc-reset-using-the-cloud/" \t "_blank).

Most of the time, you will choose to keep your files; however, if you are resetting the computer so that you can sell it or give it away, you can select the option to erase everything. This option removes all personalization and returns the computer to its initial configuration after a Windows installation.

Some vendors include customized restore information, and the option to restore factory settings might be displayed. This performs the system reset and takes you back to an experience similar to when you first unpacked the computer.

**Activity 9-11**

### Performing a System Reset

**Time Required:**60 minutes

**Objective:**Perform a system reset

**Description:**In this activity, you identify the reset options available in Settings and then perform a system reset. After performing a system reset, user data will be retained, but all custom settings will be removed.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button and then click **Settings**.

1. 3

In the Settings window, click **Update & Security** and then click **Recovery**.

1. 4

Below Reset this PC, click **Get started**.

1. 5

In the Reset this PC window, click **Remove everything**.

1. 6

Select **Local reinstall**.

1. 7

On the Additional settings screen, click **Change settings**.

1. 8

On the Choose settings screen, read the available options and then click **Cancel**.

1. 9

In the Settings window, below Reset this PC, click **Get started**.

1. 10

In the Reset this PC window, click **Keep my files**.

1. 11

Select **Local reinstall**.

1. 12

On the Additional settings screen, click **Change settings**.

1. 13

On the Choose settings screen, read the available options and then click **Confirm**.

1. 14

On the Additional settings screen, click **Next**.

1. 15

On the Ready to reset this PC screen, click **View apps that will be removed**.

1. 16

Read the list of apps and then click **Back**.

1. 17

Click **Reset**.

1. 18

Wait for the reset to be performed. This may take from 30 to 60 minutes depending on processing capacity and disk speed. The system will reboot several times as the Windows installation files are extracted and then Windows is reinstalled.

1. 19

Sign in to your computer and verify that the **Grocery List** file is still on the desktop. Notice that a Removed Apps webpage has been added to the desktop.

Go to pg.

[**help**](javascript://)

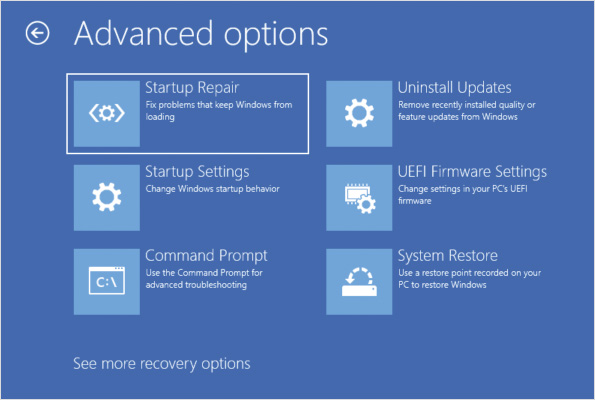
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-7bWindows Recovery Environment

The Advanced startup option in recovery settings allows you to restart your computer in the [**Windows Recovery Environment (WinRE)**](javascript://). WinRE is a small instance of Windows 10 that includes several options for troubleshooting and repairing Windows 10. During installation, Windows 10 creates a recovery partition to store WinRE (winre.wim). If Windows 10 is in a state where it does not start properly, the system might start in WinRE automatically. [Figure 9-19](javascript://) shows some of the options available in WinRE.

**Figure 9-19WinRE, Advanced Options**



Enlarge Image

Some of the available options in WinRE are:

* Use a device—This option allows you to select an alternate boot device. You can use this to boot from a USB drive, network connection, or a recovery DVD. To use a recovery DVD, you must have manually created one before you need to perform a recovery.
* Reset this PC—This provides the same options as Reset this PC within Windows 10, but is accessible when Windows 10 doesn’t start properly.
* Startup Repair—This is an automated tool that attempts to fix common issues that prevent Windows 10 from starting.
* Startup Settings—This allows you to select from a variety of startup modes with limited functionality, such as low-resolution video or Safe Mode. Sometimes you can use these limited modes to start Windows 10 and perform further troubleshooting when Windows 10 won’t start.
* Uninstall Updates—Use this option to remove the most recent quality or feature update. This is useful when a recent update has created a problem and Windows won’t start.
* UEFI Firmware Settings—Restarts your computer to edit UEFI settings. This is an alternative to pressing a function before Windows starts to access these settings.
* System Restore—Allows you to restore system files to a point in time. To use this option, you need to have previously enabled restore points. Restore points are not enabled by default.
* Command Prompt—This starts a limited version of Windows 10 that includes command-line utilities, such as bcdedit.exe and bootrec.exe, that can be used to repair Windows 10. Attempt a fix by using Startup Repair before using this option.
* System Image Recovery—This option allows you to restore Windows 10 from a system image created by using Backup and Recovery (Windows 7).

**Activity 9-12**

### Using WinRE

**Time Required:**20 minutes

**Objective:**Use WinRE to repair Windows 10

**Description:**In this activity, you start WinRE and explore recovery options. You will perform a startup repair, use startup settings, and access a command prompt.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button and then click **Settings**.

1. 3

In the Settings window, click **Update & Security** and then click **Recovery**.

1. 4

Below Advanced startup, click **Restart now**.

1. 5

On the Choose an option screen, click **Use a device**. This displays possible boot devices that you can use to boot recovery media.

1. 6

Click the back arrow and then click **Troubleshoot**.

1. 7

On the Troubleshoot screen, click **Advanced options**.

1. 8

On the Advanced options screen, click **Startup Repair**.

1. 9

On the Startup Repair screen, click **User1**, type your password, and then click **Continue**. To perform this task, you need to sign in as a user that is an administrator.

1. 10

Wait a few moments for the repair to complete and then read the results onscreen. It reports that no repairs are necessary.

1. 11

Click **Advanced options**, click **Troubleshoot**, and then click **Advanced options**.

1. 12

On the Advanced options screen, click **Startup Settings**.

1. 13

Read the information about Startup Settings and then click **Restart**.

1. 14

Read the list of available options, consider when each of these might be useful, and then press **F4** to enter Safe Mode. Safe Mode has a limited set of drivers to avoid most startup problems related to Windows 10 configuration.

1. 15

Sign in to your computer. Safe Mode text is displayed on the Desktop.

1. 16

On the taskbar, click **Microsoft Edge**. An error is displayed indicating that no network connectivity is found. This is expected in Safe Mode.

1. 17

Click the **Start** button and then click **Settings**.

1. 18

In the Settings window, click **Update & Security** and then click **Recovery**.

1. 19

Under Advanced startup, click **Restart now**.

1. 20

Click **Troubleshoot** and then click **Advanced options**.

1. 21

On the Advanced options screen, click **Command Prompt**.

1. 22

On the Command Prompt screen, click **User1**, type your password, and then click **Continue**. To perform this task, you need to sign in as a user that is an administrator.

1. 23

At the command prompt, type **bcdedit** and then press **Enter**.

1. 24

Read the boot information provided by bcdedit. Windows 10 is configured to boot from the C: drive. The X: drive currently used at the command prompt is a limited version of Windows 10 used for recovery.

1. 25

Type **bcdedit /?** and then press **Enter**. Review the help information for bcdedit.

1. 26

Type **dir \*.exe** and then press **Enter**. Review the list of executables available in the recovery environment.

1. 27

Type **bootrec /?** and then press Enter. Review the help information for bootrec.

1. 28

Type **dism /image:C:\ /cleanup-image /scanhealth** and then press **Enter**. If this command reports errors, you can use the /restorehealth option to attempt to repair it.

1. 29

Type **exit** and then press **Enter**.

1. 30

On the Choose an option screen, click **Continue**.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

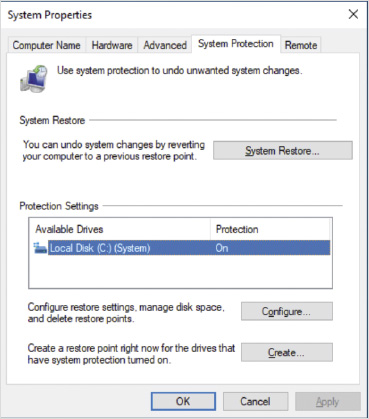
## 9-7cRestore Points

Restore points can offer a quick way to recover from an application or operating system update that is causing stability problems in Windows 10. A [**restore point**](javascript://) is a snapshot of system files and settings created at a specific point in time. User data files are not included in a restore point.

You can create restore points manually, but they are typically done automatically when an application or operating system update is performed. More than one restore point can be saved, creating a series of point-in-time snapshots of the system. When the storage space dedicated to restore points becomes too large, the oldest restore point is automatically removed.

System protection, shown in [Figure 9-20](javascript://), is disabled by default. You need to enable system protection before you can create restore points. The most important drive to be protected by System Restore is C: because it contains the operating system and applications.

**Figure 9-20System Properties, System Protection Tab**



An administrator can also use PowerShell commands in an elevated PowerShell session to update and automate the configuration of System Restore. The five cmdlets available include:

* Enable-ComputerRestore—Turn System Restore on for specified drives.
* Disable-ComputerRestore—Turn System Restore off for a specified drive.
* Checkpoint-Computer—Create a new restore point.
* Get-ComputerRestorePoint—Show all available restore points.
* Restore-Computer—Roll back to a specified restore point.

You can also start the Restore system files and settings utility from an elevated command prompt using the rstrui.exe command. This can be useful when you can only start the computer in Safe Mode with Command Prompt.

**Activity 9-13**

### Configuring System Restore Points

**Time Required:**15 minutes

**Objective:**Configure system restore points

**Description:**In this activity, you configure system restore points and create an initial restore point manually. After the restore point is created, you use it to roll back the computer configuration to that earlier configuration.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, type **restore**, and then click **Create a restore point**.

1. 3

In the System Properties dialog box, click **Local Disk (C:) (System)** and then click the **Configure**.

1. 4

Move the slider in the Disk Space Usage section to change the maximum usage to **10%**.

1. 5

Click **Turn on system protection** and then click **OK**.

1. 6

Click **Create** to manually create a restore point.

1. 7

In the System Protection dialog box, type **First manual restore point** and then click **Create**.

1. 8

Wait for the status message that the restore point was created successfully and then click **Close**.

1. 9

Click **System Restore**.

1. 10

On the Restore system files and settings screen, click **Next**.

1. 11

Select **First manual restore point** and then click **Scan for affected programs**. This checks to see if any programs or drivers will change as a result of rolling back the computer configuration to this restore point.

1. 12

Verify that no changes to programs or drivers are detected and then click **Close**.

1. 13

Click **Next** to proceed to the review screen.

1. 14

On the Confirm your restore point screen, click **Finish**, and when prompted to confirm the action, click **Yes**.

1. 15

Wait for the restore to complete and then sign in.

1. 16

Note the message that the restore has completed successfully and then click **Close**.

**Caution**

It is common for computer accounts to lose their trust relationship with the domain when you roll back to a restore point. This is because the password for the computer account has changed since the restore point was configured. You can rejoin the domain to fix this error.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 9-7dRecovery Drive

A [**recovery drive**](javascript://) is bootable media that you can use to repair or reinstall Windows 10. Using a recovery drive is an alternative when you can’t access the recovery partition for your Windows 10 installation. When you boot from a recovery drive, you see the same WinRE interface as when you choose the Advanced startup option in recovery settings.

**Caution**

A recovery drive does not contain applications or user data.

To create a recovery drive, you use an external drive. All data on the external drive is erased when you create the recovery drive. So, verify the external drive contents before you create the recovery drive.

When you create a recovery drive, the WinRE files take about 500 MB of disk space. If you select to backup system files, a full copy of Windows 10 is also stored on the recovery drive and about 16 GB of disk space is used.

A recovery drive is bit-specific. If you create a recovery drive from a 64-bit version of Windows 10, then that recovery drive can be used to repair only a 64-bit version of Windows 10 and not a 32-bit version of Windows 10.

If a local drive in the computer already was identified as a recovery drive, you might be asked if you want it deleted now that you have an external recovery drive. Unless you need to reclaim disk space, leave the existing recovery drive. It is more convenient to use the local recovery drive when possible.

**Tip**

The option create a recovery drive is available in Control Panel.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 9-8a**Summary**

* Establishing a baseline for performance tuning allows you to recognize variations from normal system behavior and identify system bottlenecks. The four main areas that cause bottlenecks are disk, memory, processor, and network.
* Task Manager allows you to quickly view system process information. Process information includes memory utilization and processor utilization. In addition, you can monitor network utilization.
* Resource Monitor provides more detailed information than Task Manager, such as the network utilization of each process. You can also filter by process to monitor all the resources a specific process is using.
* Performance Monitor can be used to monitor system performance and reliability, create alerts, log performance activity, and generate reports.
* Performance Options allow you to configure visual effects, processor scheduling, virtual memory, and Data Execution Prevention (DEP). In most cases, the default configuration for these settings is acceptable.
* Applications that start automatically can affect system performance. To configure application startup, you can use application settings, Task Manager, or Autoruns. Applications can be configured to start automatically in registry keys, the Startup folder of the Start menu, and scheduled tasks.
* To gather information to help troubleshoot errors in Windows 10 or apps, you can use Steps Recorder, Reliability Monitor, and Event Viewer.
* To protect user data, you can use Windows 10 features such as File History and Backup and Restore (Windows 7). After these options are configured, you can access previous versions of files.
* The Windows 10 operating system has many tools available for improved operating system recovery, including recovery disk, system image backup, system restore points, and the WinRE environment.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 9-8b**Key Terms**

* [**Alert**](javascript://)
* [**Backup and Restore (Windows 7)**](javascript://)
* [**baseline**](javascript://)
* [**bottleneck**](javascript://)
* [**counters**](javascript://)
* [**Data Collector Set**](javascript://)
* [**Data Execution Prevention (DEP)**](javascript://)
* [**Data Manager**](javascript://)
* [**File History**](javascript://)
* [**Performance Monitor**](javascript://)
* [**performance tuning**](javascript://)
* [**Previous Versions**](javascript://)
* [**recovery drive**](javascript://)
* [**Reliability Monitor**](javascript://)
* [**Reset this PC**](javascript://)
* [**Resource Monitor**](javascript://)
* [**restore point**](javascript://)
* [**Steps Recorder**](javascript://)
* [**Task Manager**](javascript://)
* [**virtual memory**](javascript://)
* [**Windows Recovery Environment (WinRE)**](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 9-8c**Review Questions**

1. Performance monitoring is the act of changing a system’s configuration systematically and carefully observing performance before and after such changes. True or False?

True

False

1. Which of the following can Task Manager monitor? (Choose all that apply.)
   1. memory utilization for each process
   2. network utilization for each process
   3. CPU utilization for each process
   4. disk utilization for each process
2. Which of the following can be used to start Task Manager? (Choose all that apply.)
   1. Ctrl+Alt+Delete
   2. running taskman.exe
   3. Ctrl+Shift+Esc
   4. right-clicking the taskbar
   5. restart in Safe Mode
3. In Performance Monitor, all performance objects have the same counters. True or False?

True

False

1. Which Performance Monitor component records log files?
   1. Performance Monitor
   2. Reliability Monitor
   3. Data Collection Sets
   4. Alerts
   5. Reports
2. Each Data Collector Set can contain only a single counter. True or False?

True

False

1. What is the most common physical symptom of insufficient memory?
   1. excessive heat coming from the computer
   2. graphics displayed incorrectly on the monitor
   3. a memory error code displayed on the screen
   4. high levels of disk activity
   5. three short beeps from the computer
2. File History is designed to roll back device drivers. True or False?

True

False

1. When a component is the slowest part of a process, it is referred to as a(n) .
2. You know that you will be making some major changes to your computer and you want to back up all your user data and the local operating system. This can be accomplished by selecting all drive data to create a:
   1. recovery drive
   2. WinRE environment
   3. System Image disk
   4. File History
   5. previous version
3. The event logs most commonly used for troubleshooting are located in the Applications and Services Logs node. True or False?

True

False

1. Which backup and restore function can you use to set a computer back to its factory default settings without any additional media?
   1. System Restore
   2. File History
   3. Windows Recovery Environment (WinRE)
   4. Recovery Drive
   5. Reset this PC
2. Which backup and restore function can you use to create a system image that includes the apps you have installed?
   1. System Restore
   2. File History
   3. Windows Recovery Environment (WinRE)
   4. third-party backup software
   5. System Reset
3. Which tool can you use to gather screenshots of a user demonstrating a problem?
   1. Remote Desktop
   2. Steps Recorder
   3. Reliability Monitor
   4. Event Viewer
   5. Remote Assistance
4. Which tool can you use to identify the point in time at which a computer running Windows 10 started to become unstable?
   1. Remote Desktop
   2. Steps Recorder
   3. Reliability Monitor
   4. Event Viewer
   5. Remote Assistance
5. Resource Monitor can be used to monitor the amount of data sent over various network connections. True or False?

True

False

1. Which is the best solution for backing up user data?
   1. OneDrive
   2. File History
   3. Backup and Restore (Windows 7)
   4. Previous Versions
   5. Cloud History
2. What is the first option you should investigate when you want a program to stop running when users sign in?
   1. a registry value in HKLM:\Software\Microsoft\Windows\CurrentVersion\Run
   2. a shortcut in the Startup menu of the Start menu
   3. a registry value in HKCU:\Software\Microsoft\Windows\CurrentVersion\Run
   4. the application settings
   5. schedule tasks
3. Which Event Viewer feature should you use to view events in multiple logs?
   1. Filter
   2. Find
   3. Custom view
   4. Subscription
   5. Custom log
4. Which command do you need to run on the source computer to allow remote access to event logs for a subscription?
   1. wecutil qc
   2. winrm quickconfig
   3. eventvwr subsetup
   4. net set event
   5. enable-WinRM

Go to pg.

[**help**](javascript://)