Lab - Monitor and Manage System Resources in Windows 8

Introduction

In this lab, you will use administrative tools to monitor and manage system resources.

Recommended Equipment

- A computer running Windows 8 with Internet access

Step 1: How to stop and start a service in Windows.

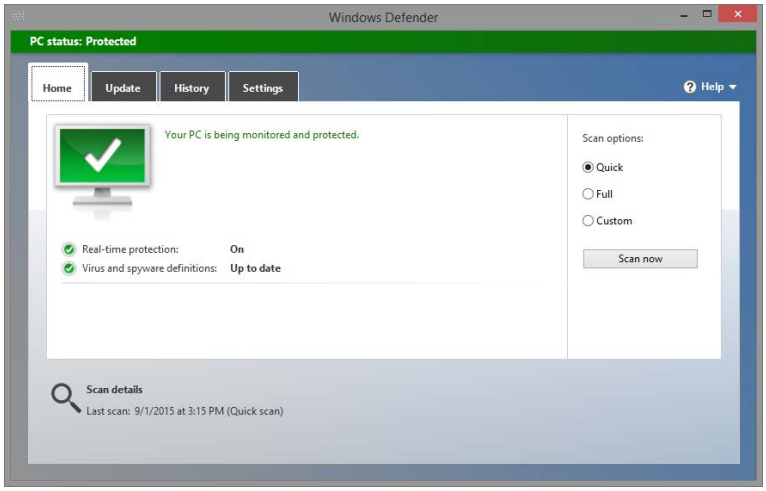
You will explore what happens when a service is stopped then started.

a. Log on to Windows as an administrator.

Note: Some antivirus or antispyware programs must be uninstalled on the computer for Windows Defender to work.

b. To see if Windows Defender is turned off, click **Start** in the **Search programs and files** field, type **Defender** and select **Windows Defender**. **Windows Defender** should be running.

Note: In Windows 8.0, click **Search**, type **Defender,** and select **Windows Defender**.

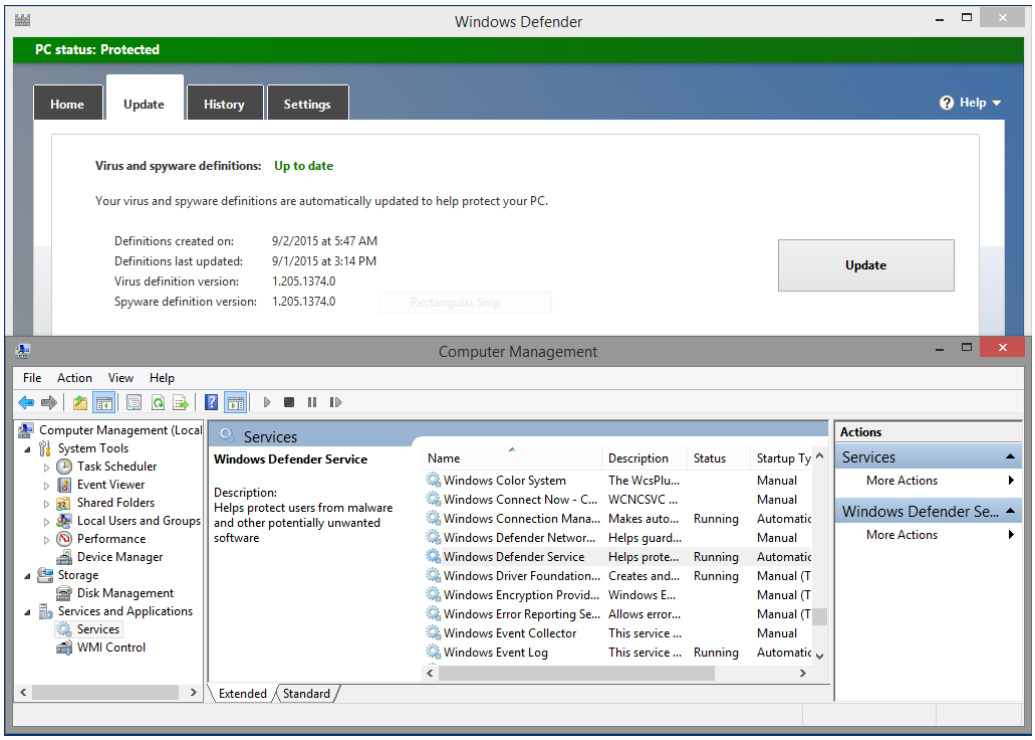


Note: If **Windows Defender** is not running, a warning window will open and **Windows Defender** will not start. To start Windows Defender, click **Control Panel > Action Center**. In **the Virus protection (Important)** section of the **Action Center** window, click **Turn on now**.

c. Without closing **Windows Defender,** open the **Services** console. Click **Control Panel > Administrative Tools > Computer Management**.

d. The **Computer Management** window opens. Under Services and Applications, select **Services**.

e. Close the **Windows Explorer** window but keep the **Windows Defender** and **Computer Management** windows open. Resize and position both windows so they can be seen at the same time.



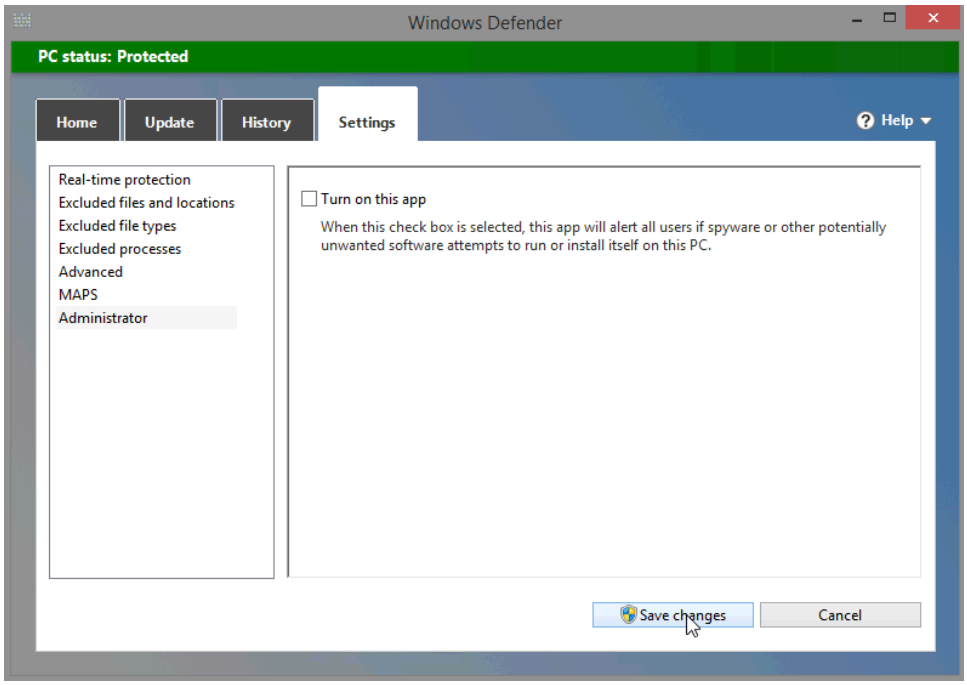
Can Windows Defender check for updates? (Use the **Update Tab** to answer the question) Yes.

f. Scroll the **Computer Management** window so you see the **Windows Defender Service**.

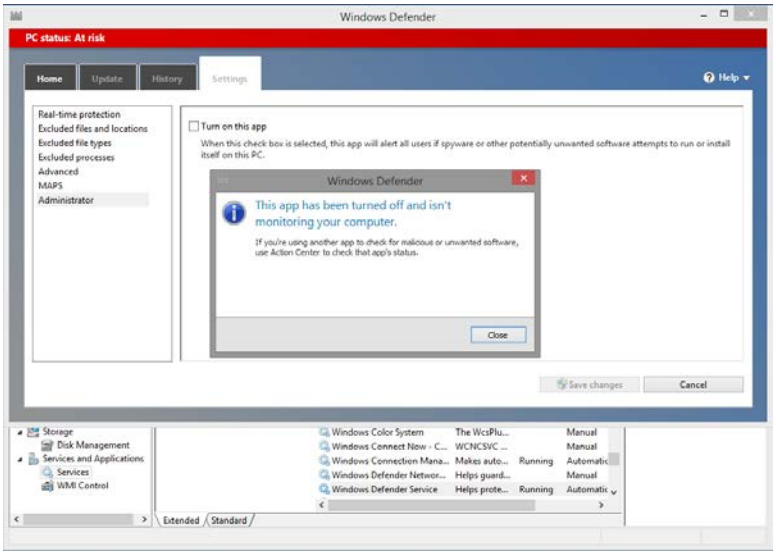
What is the status of the service? Running

Note: While most of the Windows services can be managed through the Services console, it is not possible to stop **Windows Defender** from Windows 8's **Services** console.

g. To turn off **Windows Defender**, make the **Windows Defender** window active. Select the **Settings** tab, and select **Administrator**. Uncheck the **Turn on this app** checkbox, and click **Save changes**.



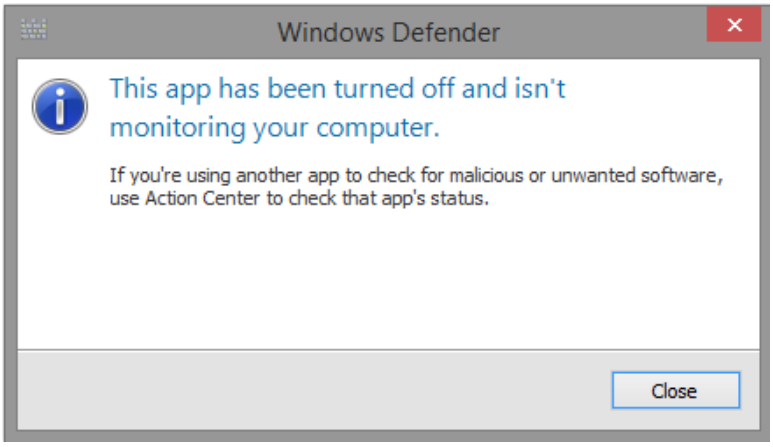
h. A warning window will open. Click **Close**. Notice that the **Windows Defender** application closes completely.



Note: The reason this service will be stopped is so you can easily see the results. When stopping a service to free up system resources the service uses, it is important to understand how the overall system operation will be affected.

Note: Although Windows Defender Service cannot be controlled through the **Computer Management Services** window, Windows Defender's status is still monitored and displayed. It may be necessary to refresh the **Computer Management** window by pressing **F5**.

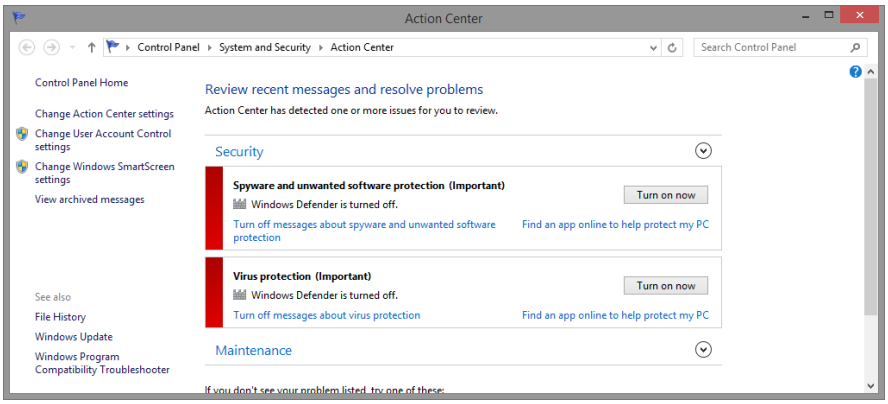
i. Now that **Windows Defender** service is stopped, try to run **Windows Defender** again by clicking **Search**, typing **Defender**, and selecting **Windows Defender**.



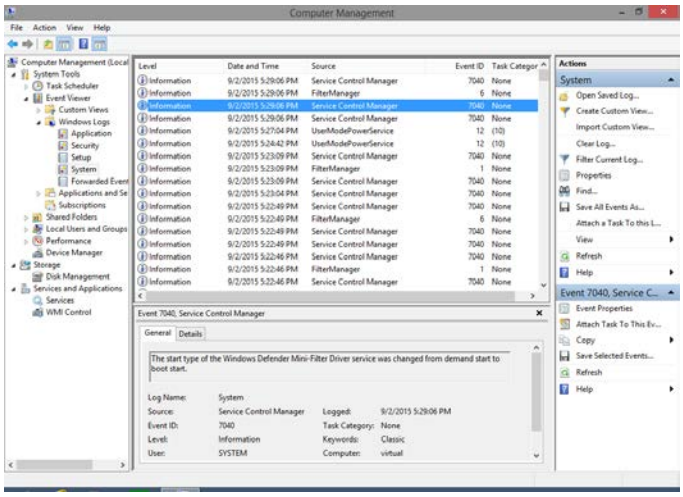
What must be done so Windows Defender can run?

Re-enable Windows Defender in the Action Center. (Windows 10 - Security and Maintenance)

j. Use **Action Center** to start the Windows Defender service. Click **Control Panel > Action Center.** In the **Virus protection (Important)** section**,** click **Turn on now.**



k. The **Windows Defender** window will open, as the service should now be running again. Close the **Windows Defender** window but make sure the Computer Management window is open.



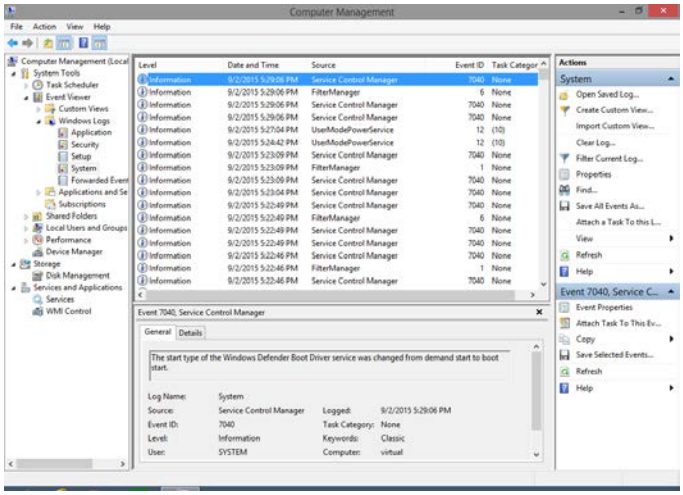
l. Expand **Event Viewer** > **Windows Logs** > select **System**.

m. Select the second **Service Control Manager** event in the list.

Look below the General tab and explain what has happened to the Windows Defender service.

Windows Defender service was changed from demand start to boot/auto start.

n. Click the up arrow button on the keyboard or select the event above the one you just viewed.



Look below the General tab and explain what has happened to the Windows Defender service.

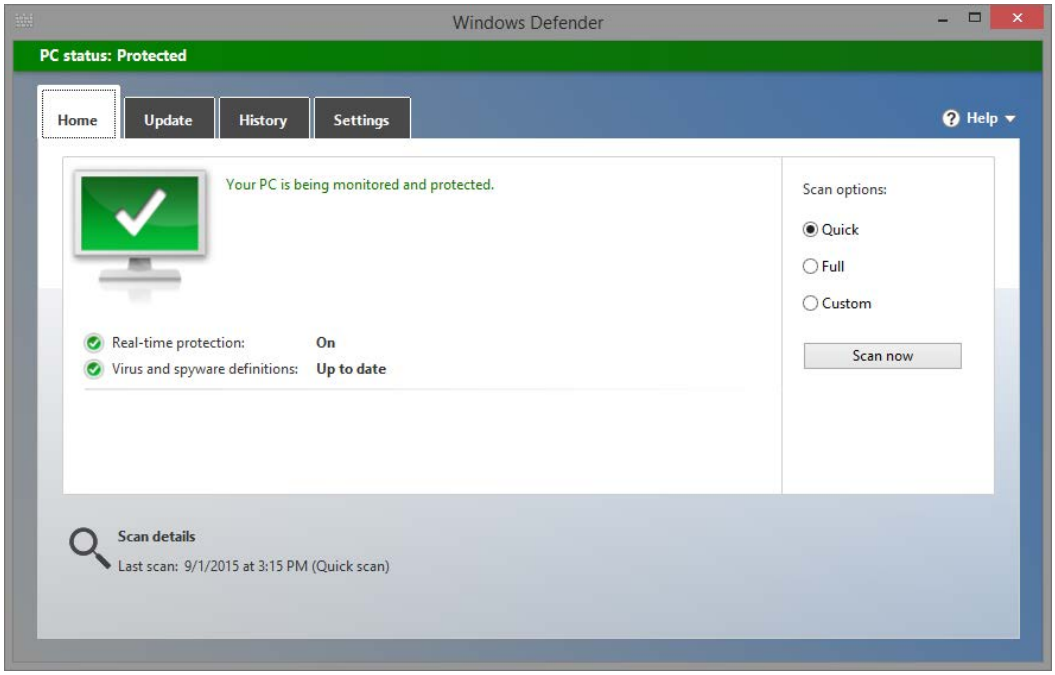
Windows Defender service was changed from boot/auto start to demand start.

o. Close all open windows.

Step 2: Understanding the Impact of Services.

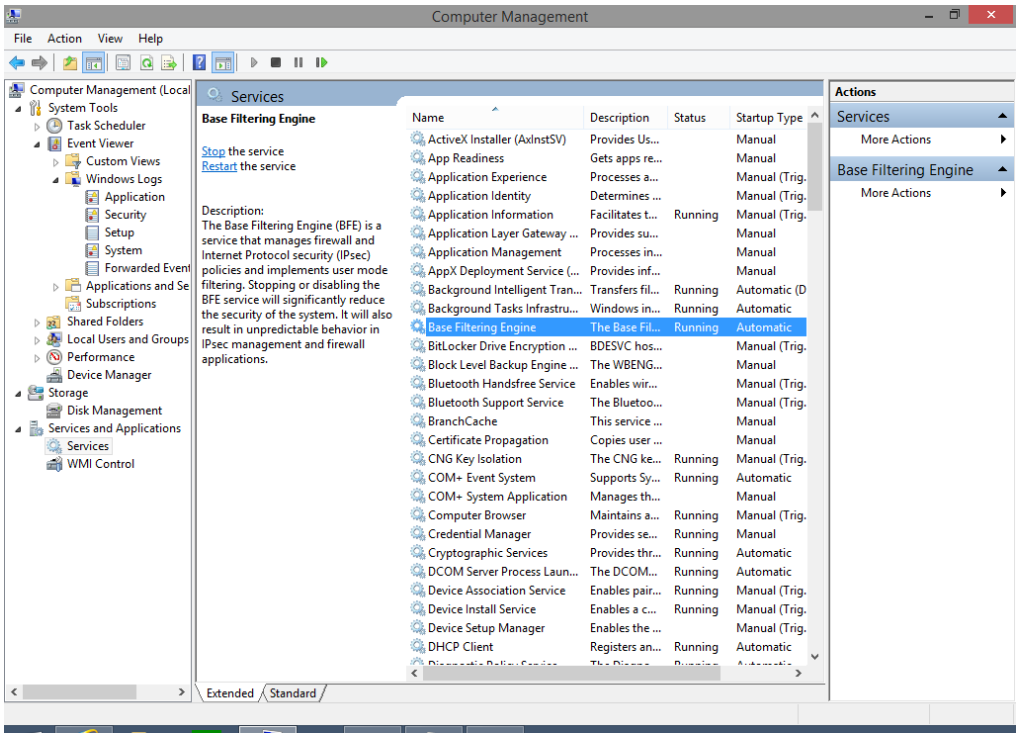
In this section, you will stop **Windows Base Filtering Engine (BFE),** analyze the impact in the system, and restart BFE. BFE is responsible for managing the firewall and a number of other security policies in Windows. BFE is an important Windows service, as many other services depend on it.

a. Ensure **Windows Defender** is running by clicking **Control Panel > Windows Defender**.

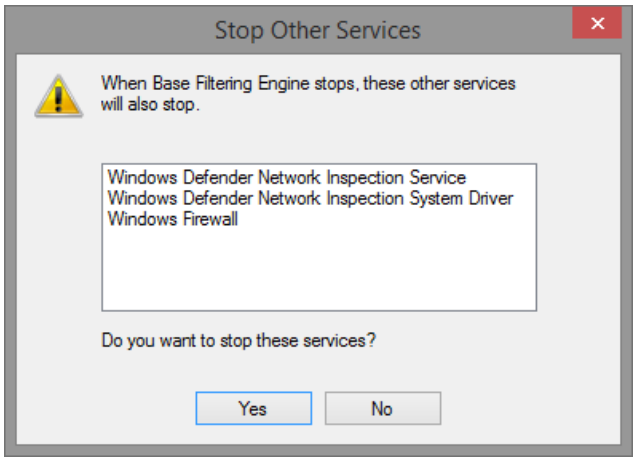


b. Open the Computer Management utility. Click **Control Panel > Administrative Tools > Computer Management**. Select **Service** and locate the **Base Filtering Engine** service.

c. Stop the BFE service by right-clicking it and selecting **Stop.** Alternatively, you can use the stop button on the upper toolbar of the **Services Console** while the BFE service is selected.



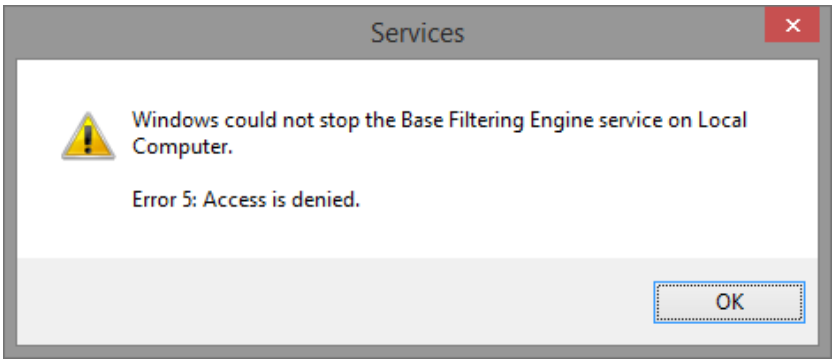
d. Windows will present a warning message to remind you about all the services that depend on BFE. Click **Yes** to stop BFE and its dependent services



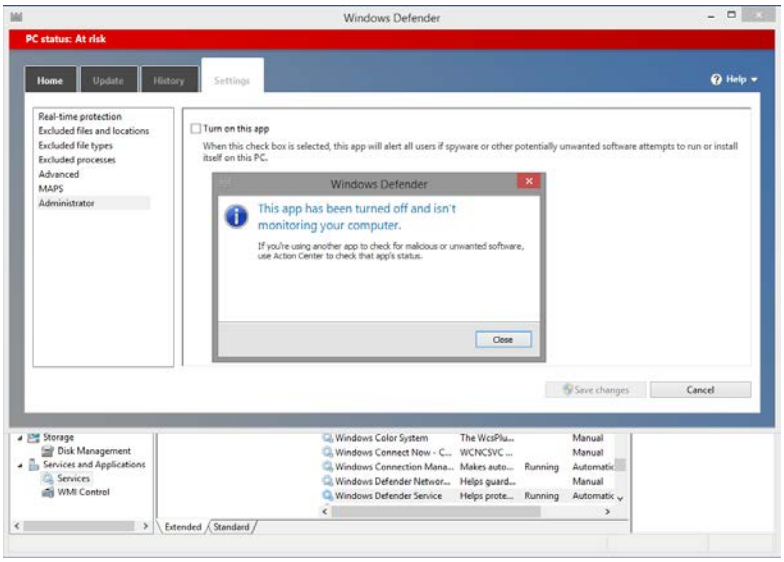
Note: The services listed may differ from this warning message.

e. Windows should not let you stop BFE if the **Windows Defender** service is displayed in the **Stop Other Services** window. Since **Windows Defender** cannot be stopped via the **Services Console**, BFE cannot be stopped via the **Services Console.**

Note: If this error window does not appear, skip to **substep h**.



f. To stop BFE, **Windows Defender** must be stopped first. Open **Windows Defender** and click **stop** on the **Settings** tab. Refer to the beginning of this lab for details.

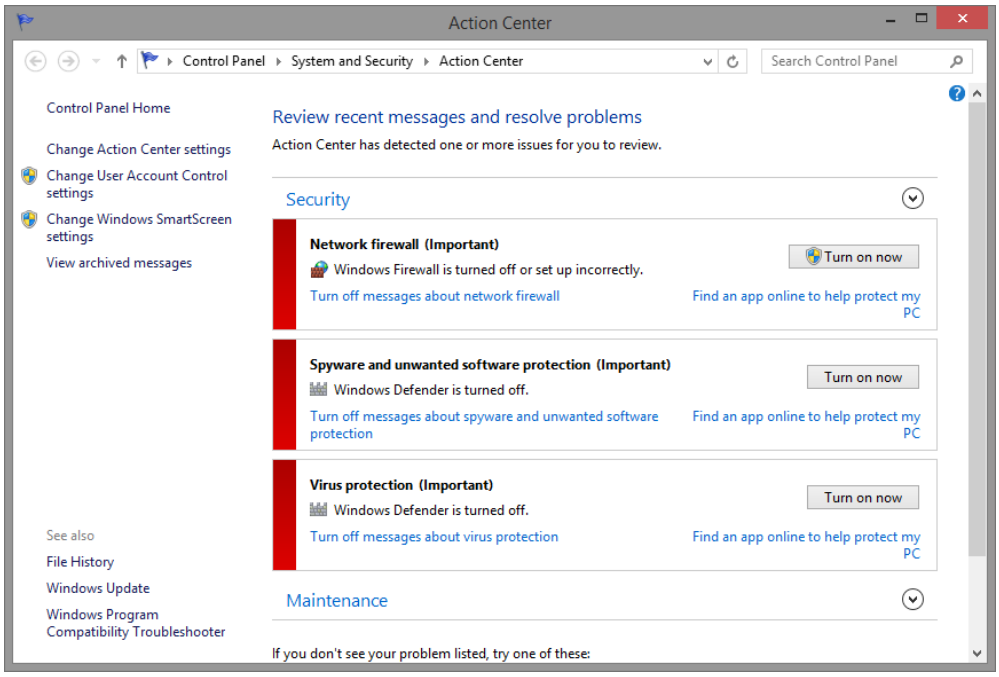


g. Now that **Windows Defender** is stopped, open the **Services Console** and stop BFE. Right-click the BFE service and select **Stop.**

What does the status column of the **Services Console** indicate for the BFE service?

The status column changes from "Running" to a blank line.

h. Since a number of security related services depend on BFE, alerts are issued and can be reviewed in **Action Center**.



Note: The issues listed may differ in the **Action Center**.

Why is it important to exercise care when managing services?

Dependencies. A single service may be used by multiple other services. Stopping a single service may cause other services to stop working. In this case, the computers security was compromised.

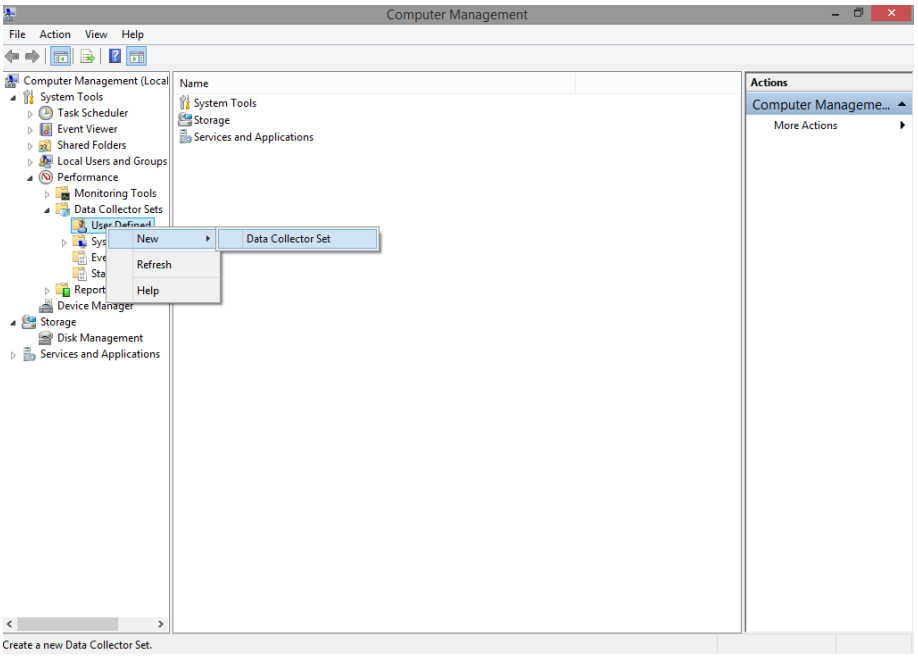
i. Restart any stopped service from the **Action Center** by selecting the service and clicking **Turn on now**.

Step 3: Configure advanced features in Administrative Tools.

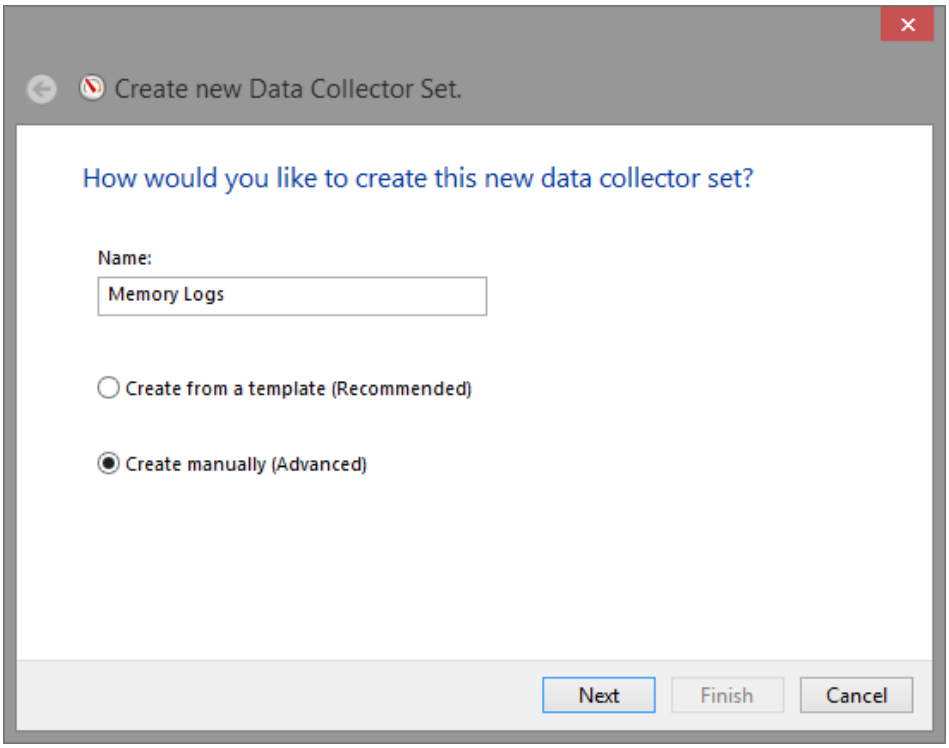
For the rest of this lab, you will configure advanced Administrative Tool features and monitor how this affects the computer.

a. From **Windows Explorer,** right-click **This PC** and select **Manage**. The **Computer Management** window opens.

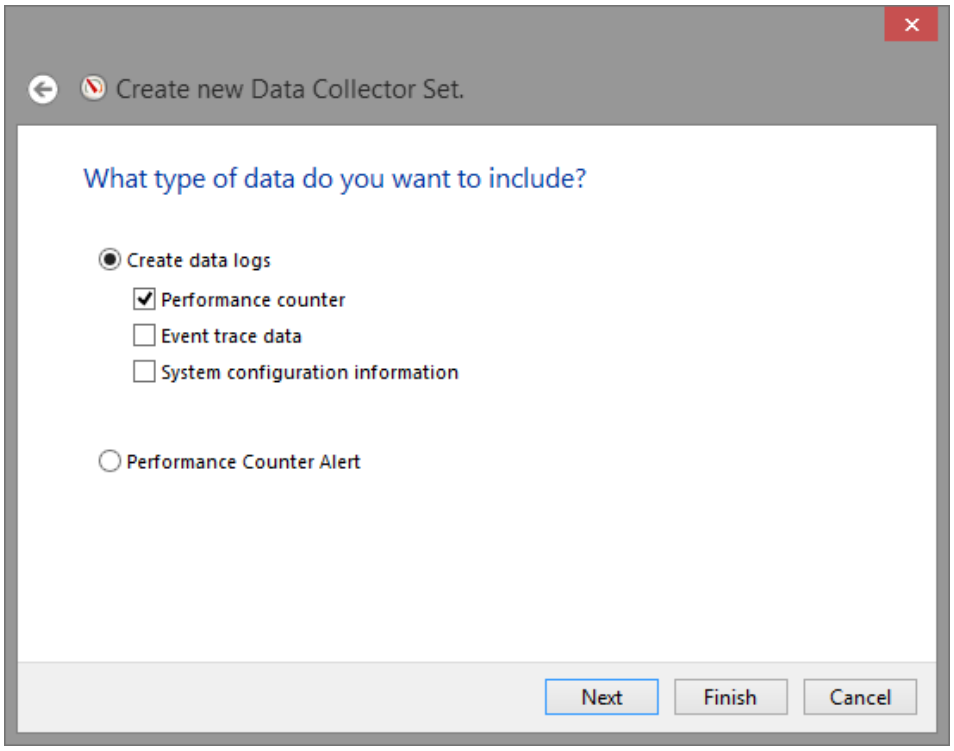
b. Expand **System Tools > Performance >Data Collector Sets.** Right-click **User Defined**, and then click **New** > **Data Collector Set**.



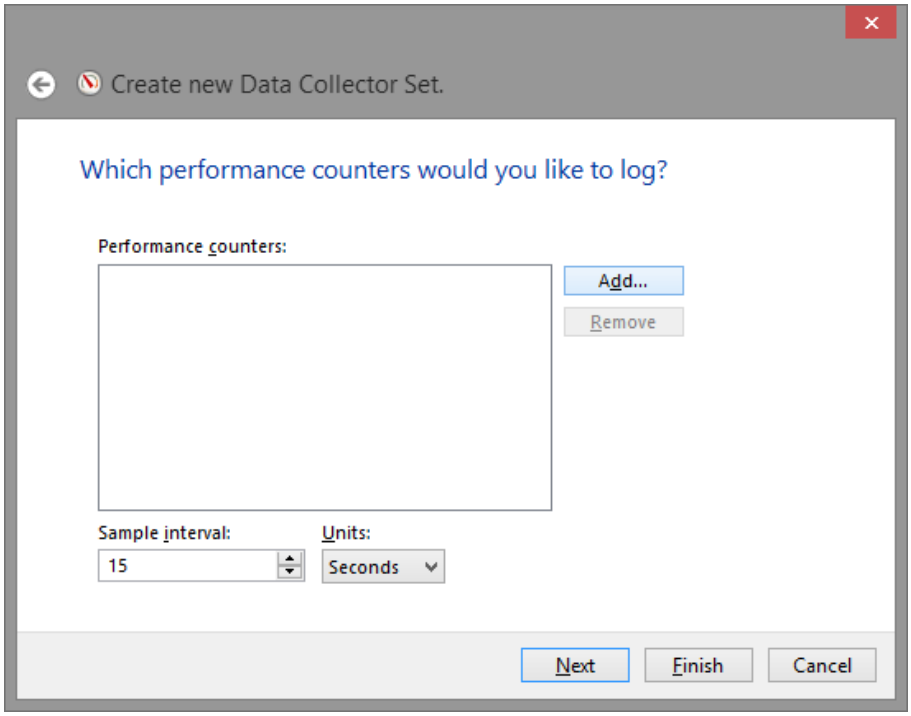
c. The **Create new Data Collector Set** window opens. In the Name field, type **Memory Logs**. Select the **Create manually (Advanced)** radio button and click **Next**.



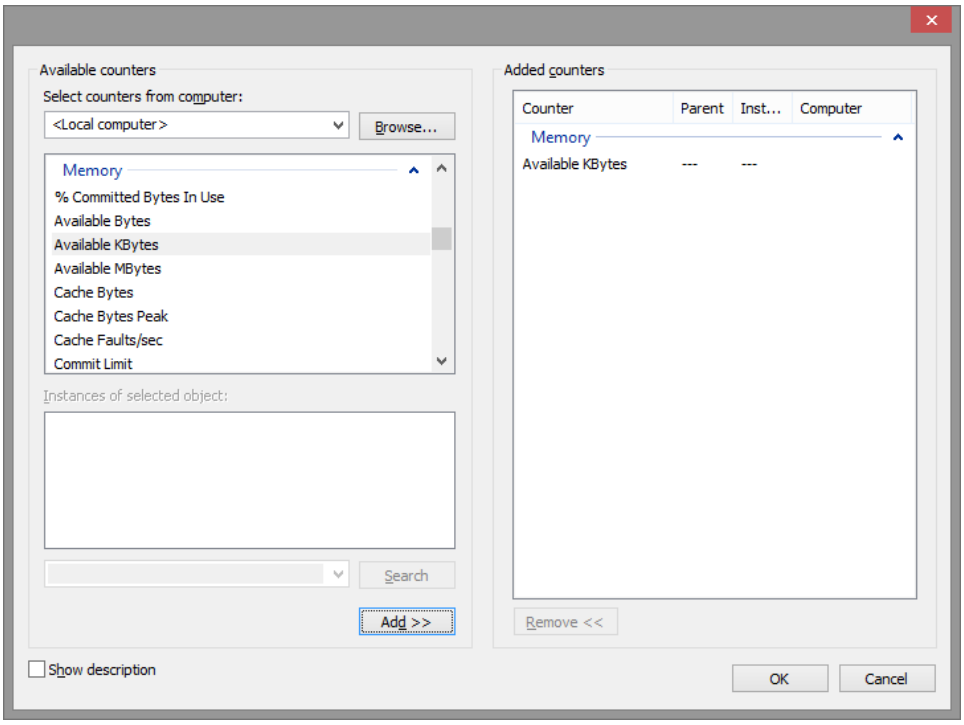
d. The **What type of data do you want to include?** window opens. Check the **Performance counter** box and click **Next**.



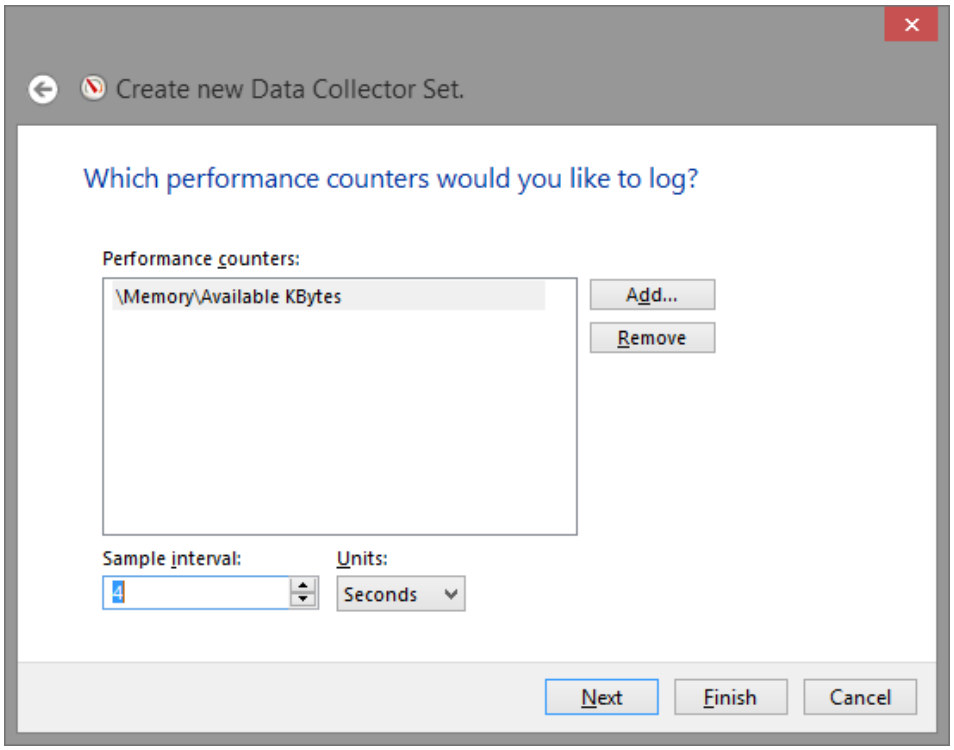
e. The **Which performance counters would you like to log?** window opens. Click **Add**.



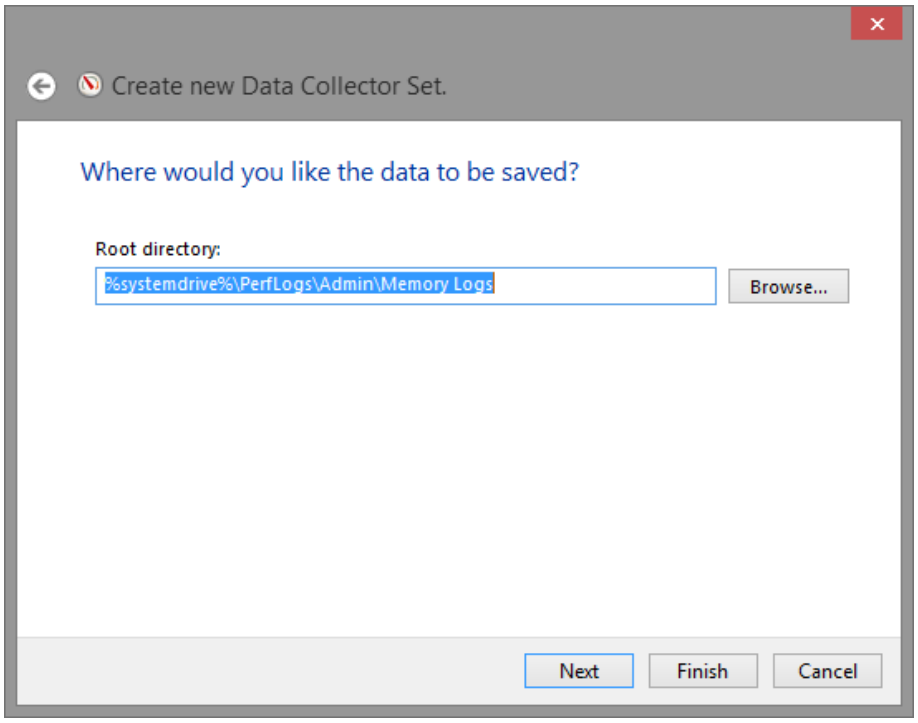
f. From the list of available counters, locate and expand **Memory**. Select **Available MBytes > Add** and click **OK.**



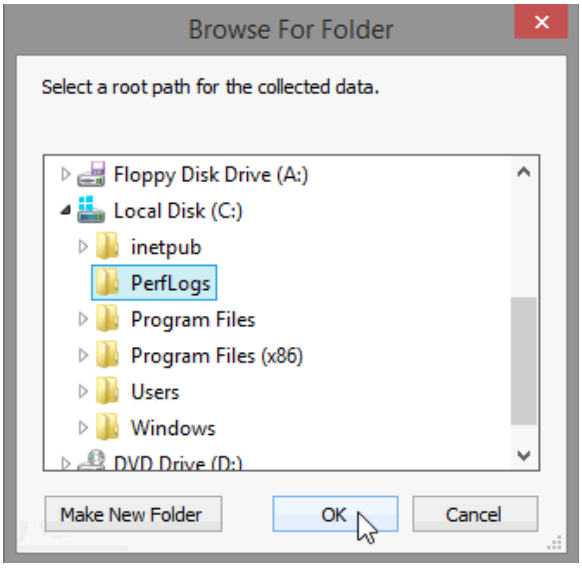
g. Set the **Sample interval**: field to **4** seconds. Click **Next**



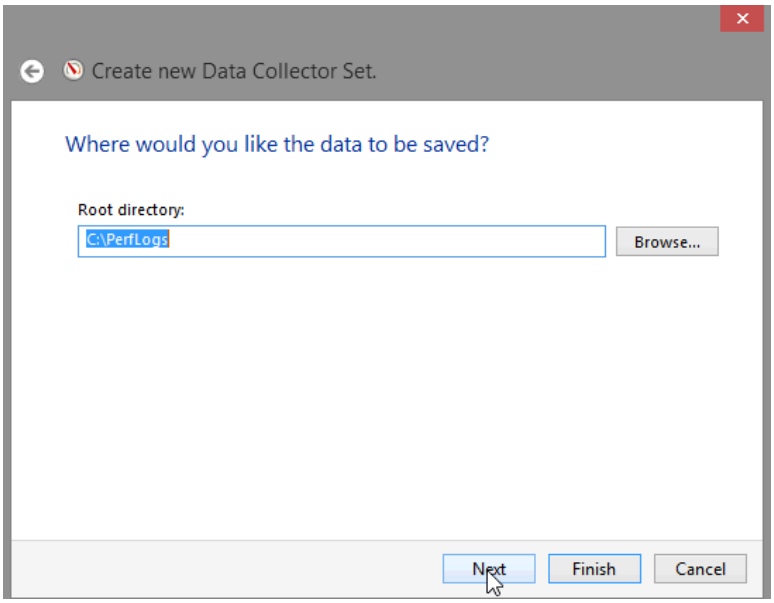
h. The **Where would you like the data to be saved?** window opens. Click **Browse…**.



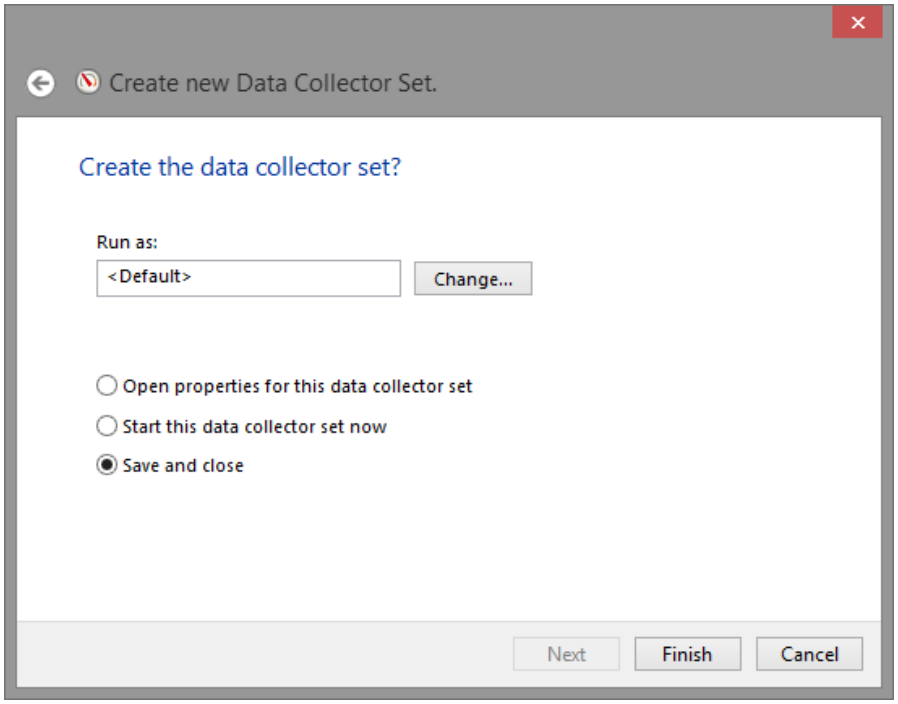
i. Select Local Disk (**C:),** and then select the **\PerfLogs** folder. Click **OK**.



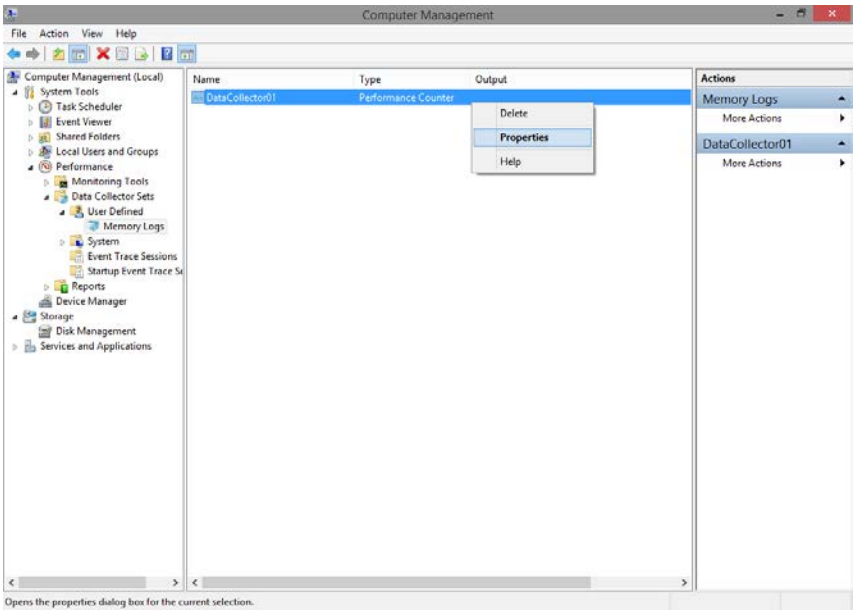
j. Verify the correct root directory path is selected, and click **Next**.



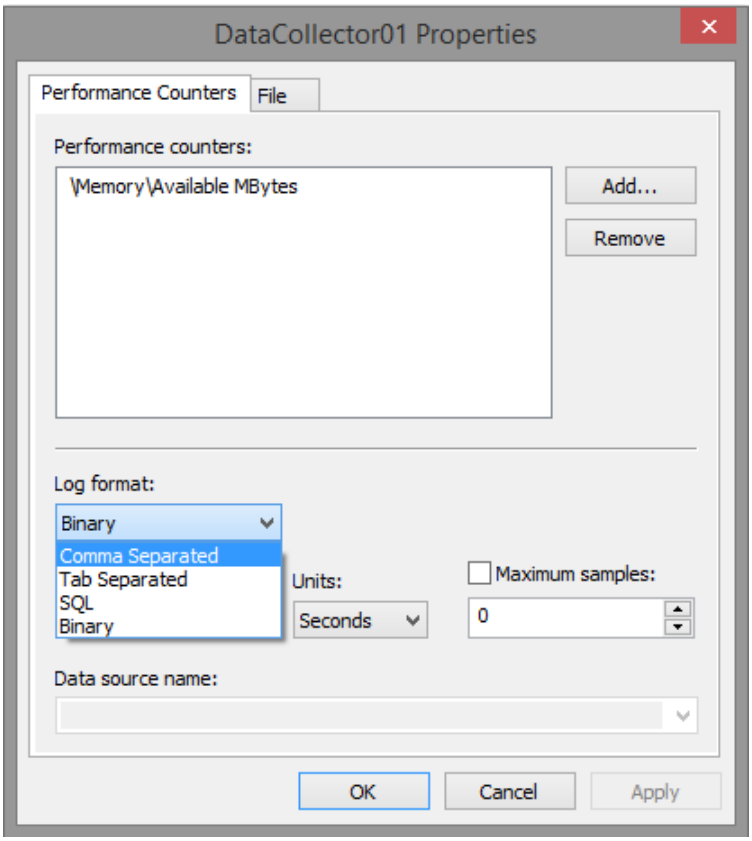
k. The **Create the data collector set?** window opens. Click **Finish**.



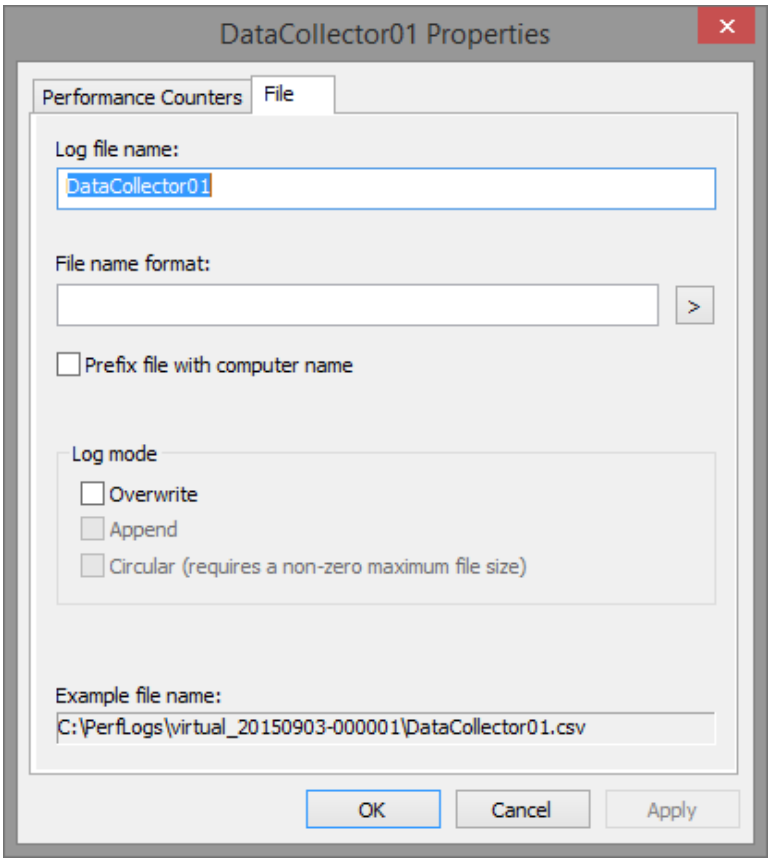
l. Expand **User Defined** and select **Memory Logs.** Right-click **Data Collector01** and select **Properties**.



m. The **DataCollector01 Properties** window opens. Change the **Log format:** field to **Comma Separated**.



n. Click the **File** tab.

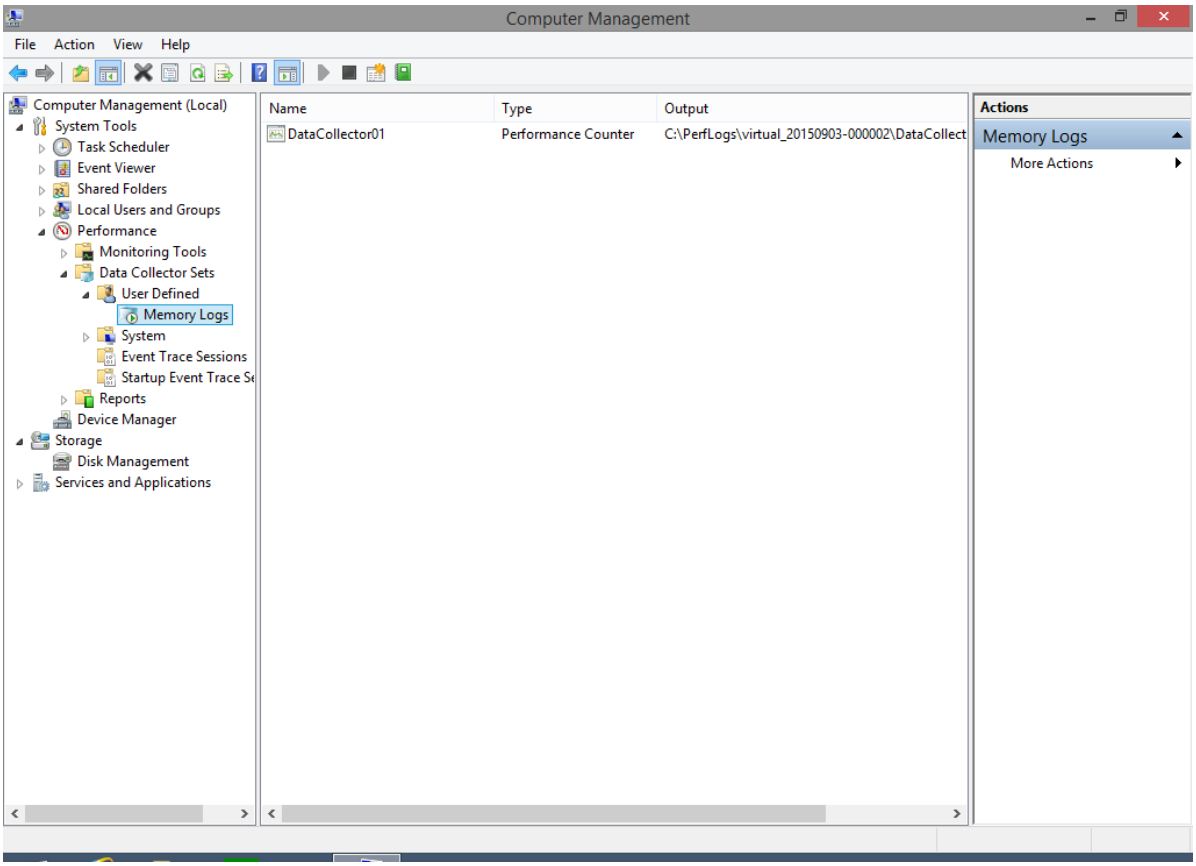


What is the full path name to the example file name?

C:\PerfLogs\ADONIS_20180922-000001\DataCollector01.csv

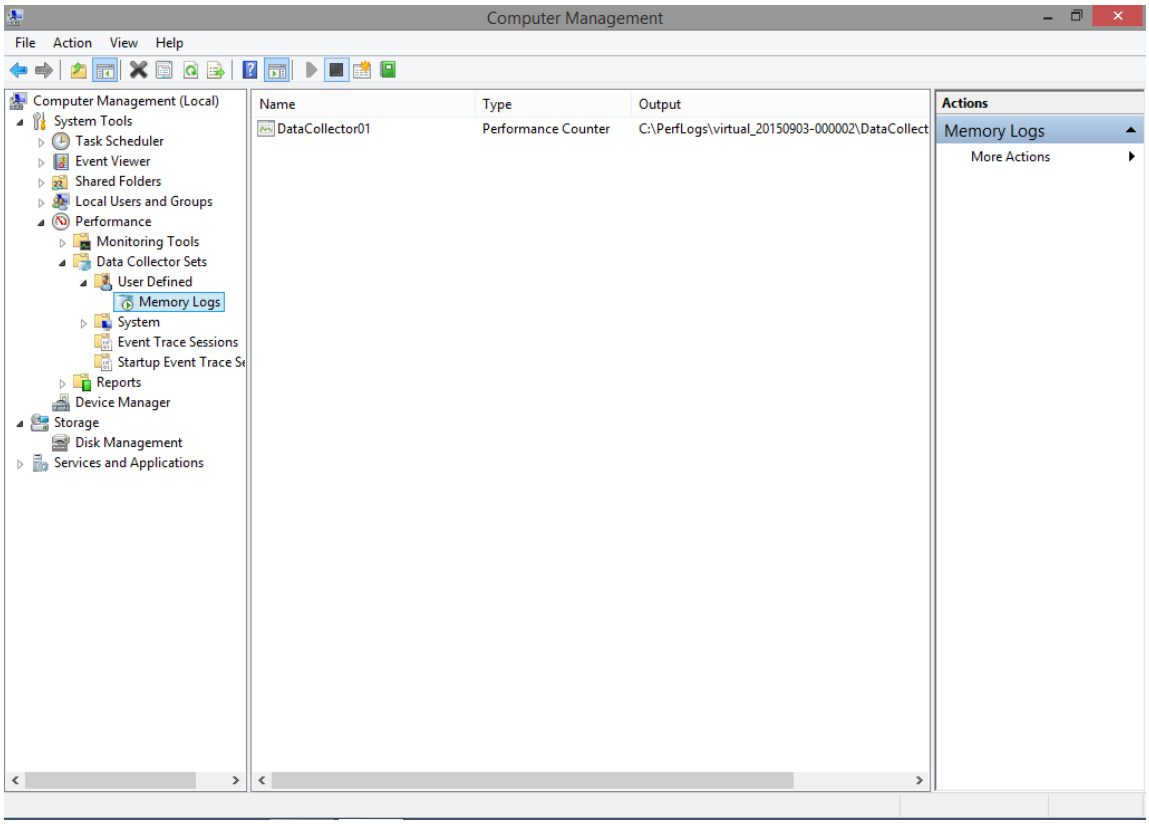
o. Click **OK**.

p. Select the **Memory Logs** icon in the left pane of the **Performance Monitor** window. Click the **green arrow** icon to start the data collection set. Notice a green arrow is placed on top of the **Memory Logs** icon.



q. To force the computer to use some of the available memory, open and close a browser.

r. Click the **black square** icon to stop the data collection set.

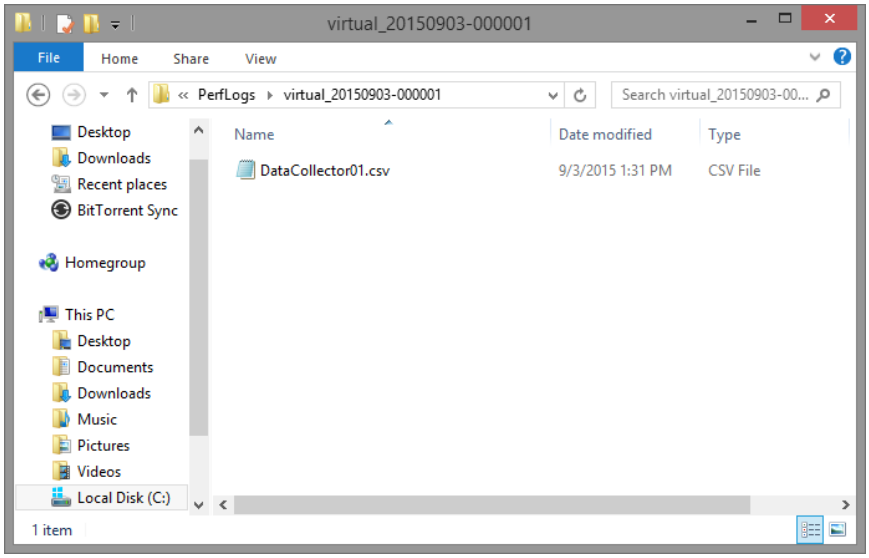


What change do you notice for the Memory Logs icon?

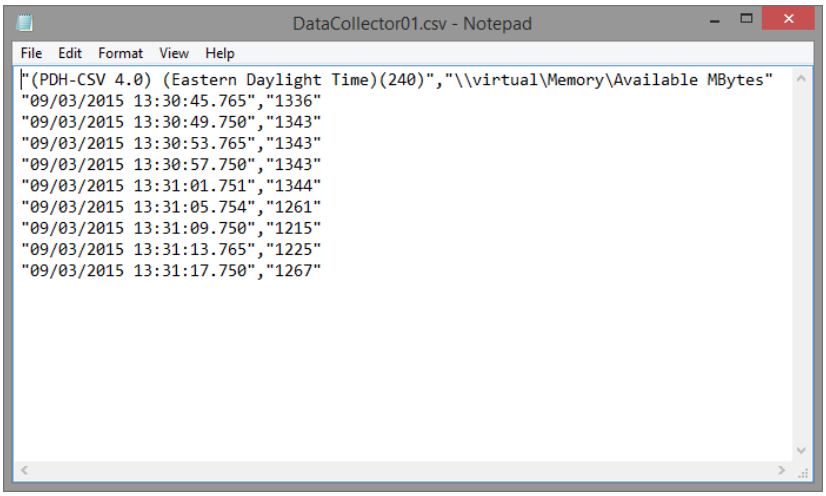
The green arrow (running arrow) disappeared

s. Open **Windows Explorer**, and click **Local Disk (C:) > PerfLogs.** Click on the folder that was created to store the memory log and double-click the **DataCollector01.csv** file.

Note: Click **Continue** on the Windows warning messages.



t. If the **Windows cannot open the file:** message is displayed, select the radio button **Select a program from a list of installed programs > OK > Notepad > OK**.

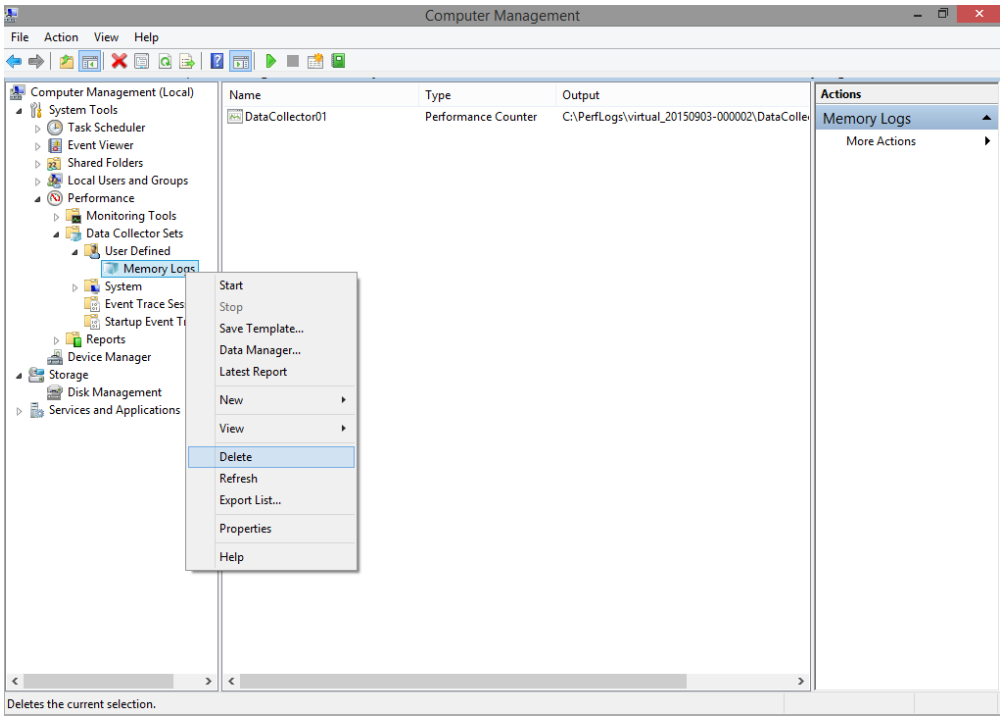


What does the column farthest to the right show?

Available MBytes

u. Close the **DataCollector01.csv** file and **Windows Explorer**.

v. Select the **Performance Monitor** window.



w. Right-click **Memory Logs > Delete** and click **Yes**.

x. Open **Windows Explorer**, click **Local Drive C: > PerfLogs** folder. Right-click the folder that was created to store the memory logs, and click **Delete**.

y. Close all open windows.