Lab - Monitor and Manage System Resources (Instructor Version)

**Instructor Note**: Red font color or gray highlights indicate text that appears in the instructor copy only.

# Introduction

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

# Recommended Equipment

* A computer running Windows with internet access

# Instructions

## Event Viewer

In this part, Windows Defender is used to explore the Event Viewer when the status of a service changes. Windows Defender is the built-in anti-malware component in Windows.

### Verify Windows Defender is running.

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

* + - 1. Log on to Windows as an administrator.
      2. To determine if Windows Defender service is stopped, click **Start**, search for **Windows Security**.
      3. Click **Virus & threat protection**. Scroll down to the **Virus & threat protection settings**. Click **Manage settings**.
      4. Under the Real-time protection heading, verify that it is **On**. Keep the Windows Security window open.

### Explore the Services console.

* + - 1. Right-click **Start** > click **Computer Management**. In the **Computer Management** window, select **Services and Applications** > **Services**.
      2. Scroll down to **Windows Defender Antivirus Network Inspection Service**.

#### Question:

What is the status of the service?

Type your answers here.

The status is Running.

* + - 1. Keep the **Computer Management** window open.
      2. Navigate back to Windows Security. Turn off **Real-time Protection** by clicking the slider to turn it off. Click **Yes** to allow this app to make changes to the device.
      3. Navigate back to **Services**. Click **Action** > click **Refresh**.
      4. Look for **Windows Defender Antivirus Network Inspection**.

Record the Windows Defender status.

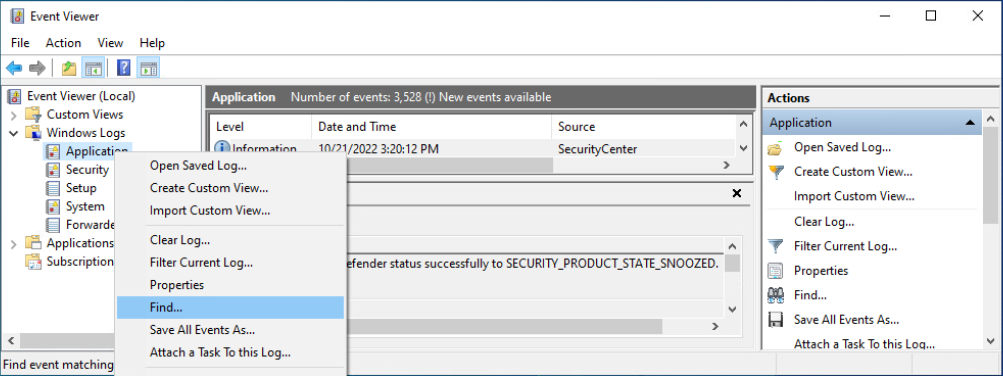
Type your answers here.

There is no status because it is turned off.

* + - 1. Close the **Computer Management** window.

### Explore the Event Viewer.

* + - 1. Navigate to the Event Viewer. Right-click **Start** > select **Event Viewer**.
      2. Expand **Windows Logs** > select **Application**.
      3. In the Application pane, you can find the most recent events related to Windows Defender. Right-click **Application** > select **Find**. Enter **defender** to search Windows Defender related entries and click **Find Next**.



#### Questions:

In the General tab, what is listed as the Source of the event? What is the severity level?

Type your answers here.

The severity level is informational and the source is Security Center.

What is the status of Windows Defender?

Type your answers here.

Windows Defender status is updated to SECURITY\_PRODUCT\_STATE\_SNOOZED.

* + - 1. Navigate to Windows Security and re-enable Real-time protection. Close Windows Security window.
      2. Navigate to the Event Viewer to review the most recent event entries that are related to Windows Defender. Close the Event Viewer window when done.

## Explore the Impact of Services.

In this part, you will stop **Print Spooler** service to explore the impact in the system. The print spooler is responsible for managing the printer jobs and handling the interaction with the printer. With this service turned off, you will not be able to print or see your printers.

### Verify printing service

* + - 1. Open **Notepad**. Click **Start** and search for **Notepad**.
      2. In **Notepad**, click **File** > **Print**. Record a listed printer below. **Note**: You do not need to install a physical printer.

Type your answers here.

Answers may vary. Microsoft XPS Document Writer is a print-to-file driver installed by Windows.

* + - 1. Click **Cancel** to exit the print dialog. Leave Notepad open.

### Stop print spooler.

* + - 1. Right-click **Start** > select **Computer Management**. Expand **Services and Applications** > select **Services** to open the Services console.
      2. Right-click **Print Spooler** and select **Stop**.
      3. Navigate to **Notepad**. Attempt to print.

#### Question:

What message did you receive? How would you fix this?

Type your answers here.

The message received: Before you can perform printer-related tasks such as page setup or printing a document, you need to install a printer. You will need to restart the print spooler.

* + - 1. Click **No** in the message window and click **Cancel** to exit the Print window.

### Restart print spooler

* + - 1. Navigate to the **Services** console and restart the print spooler. Right-click **Print Spooler** and select **Start**.
      2. Verify that you can print and close Notepad.

### Explore DHCP Client service

The DHCP Client service registers and updates the IP addresses and DNS records for the PC. If this service is stopped, the PC will not receive a dynamic IP address and DNS updates.

* + - 1. In the Services console, search for **DHCP Client**. Right-click **DHCP Client** and select **Stop**.

#### Question:

When DHCP Client stops, what other services will also be stopped?

Type your answers here.

Answer may vary. The other services may include: IP Helper, WinHTTP Web Proxy Auto-Discovery Service, Network List Service, and Network Location Awareness.

* + - 1. Click **No** in the **Stop Other Services** window.

#### Question:

Why is it important to exercise care when managing services?

Type your answers here.

Applications and other services may depend on a given service to work. Stopping a service can compromise the operation of other services.

* + - 1. Verify that **DHCP Client** is still running.

## Monitor and Record System Usage with System Tools

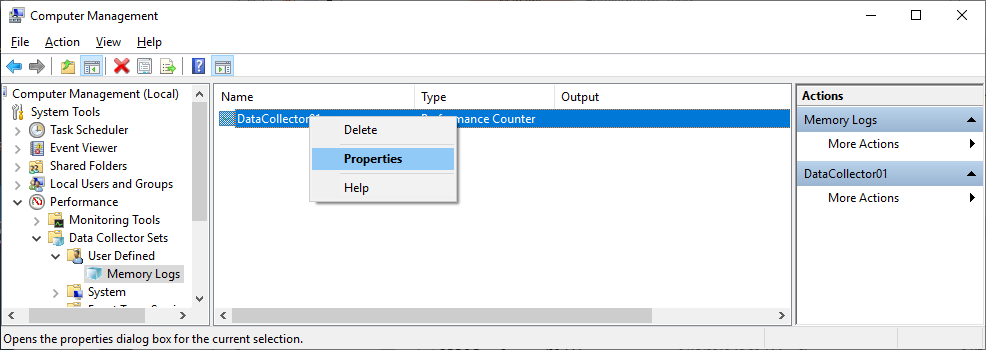
You will configure System Tools features and monitor the usage of system resources of the computer.

### Create a new data collector set.

* + - 1. Right-click **Start**. > select **Computer Management** > expand **System Tools**.
      2. Expand **Performance** > expand **Data Collector Sets**.
      3. In the left pane, right-click **User Defined** > select **New** > click **Data Collector Set**.
      4. In the **Create new Data Collector Set** window, type **Memory Logs** in the Name field. Select the **Create manually (Advanced)** and click **Next** to continue.
      5. In the **What type of data do you want to include?** window, select **Performance counter** and click **Next**.
      6. In the **Which performance counters would you like to log?** Window, click **Add**. From the list of available counters, locate and expand **Memory**. Select **Available MBytes** > **Add** and click **OK** to continue.
      7. Set the **Sample interval**: field to **4** seconds. Click **Next** to continue.
      8. In the **Where would you like the data to be saved?** Window, click **Browse**. Select **Local Disk (C:)** > **PerfLogs**. Click **OK** to continue.
      9. Verify the correct root directory path is displayed (C:\PerfLogs) and click **Finish** to continue.

### Format the data collector set.

* + - 1. Expand **User Defined** and select **Memory Logs** in the left pane. Right-click **Data Collector01** and right-click **Properties**.



* + - 1. In DataCollector01 Properties window, change the Log format: field to **Comma Separated**.
      2. Click the **File** tab.

#### Question:

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

Type your answers here.

Answer may vary. For example: C:\PerfLogs\*DataCollectionName*\DataCollector01.csv

* + - 1. Click **OK** to continue to close the Properties window.

### Collect and view the data.

* + - 1. To start data collection, right-click **Memory Logs** and select **Start**.
      2. To force the computer to use some of the available memory, open and close a browser.
      3. Right-click **Memory Logs** and select **Stop** to stop the data collection set.
      4. Navigate to **Local Disk (C:)\PerfLogs**. Click **Continue** in the Windows warning messages.
      5. Open the folder that was created to store the memory log. Click **Continue** on the Windows warning messages.
      6. Open the **DataCollector01.csv** file. Select **Notepad** or another program that can read comma-separated files (.csv) to open the file if Windows cannot open the file message is displayed.

#### Question:

What does the column farthest to the right show?

Type your answers here.

Available memory in MBytes.

* + - 1. Close the DataCollector01.csv file.

### Clean up

* + - 1. Navigate to the **Computer Management** window. Right-click **Memory Logs** and select **Delete**. Click **Yes** to confirm the deletion.
      2. Navigate to the **Local Drive C: > PerfLogs** folder. Delete the stored memory logs folder (folder with the DataCollector01.csv) created from this lab.
      3. Close all opened windows.

End of Document