Lab - Monitor and Manage System Resources

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

Part 1: 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.

Step 1: Verify Windows Defender is running.

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

a. Log on to Windows as an administrator.

b. To determine if Windows Defender service is stopped, click **Start**, search for **Windows Defender**.

In Windows 10, click **Virus & threat protection**. Scroll down to the **Virus & threat protection settings**. Click **Manage settings**. Under the Real-time protection heading, verify that it is **On**.

In Windows 8.1, in the **Home** tab, verify that the Real-time protection is On. If Windows Defender does not open, navigate to **Action Center** (click **Start** > search for **Action Center**. Click **Turn on now** for Spyware and unwanted software protection (Important) and Virus protection (Important).

In Windows 7, you will receive the message **This program is turned off** in the Windows Defender window. Click **click here to turn it on** in the window and click **Close** to continue.

c. Keep Windows Defender open.

Step 2: Explore the Services console.

Note: While most of the Windows services can be managed through the Services console, it is not possible to stop **Windows Defender** from Windows **Services** console in Windows 10 and 8.1.

a. Click **Start** > search for **Control Panel**. In the Control Panel in the Small icons view, click **Administrative Tools** > click **Computer Management**. In the **Computer Management** window, expand **Services and Applications**, and select **Services**.

b. Scroll to the Computer Management window under the Services heading so you see the **Windows Defender Antivirus Network Inspection Service** (Windows 10) or **Windows Defender Service** (Windows 8.1) or **Window Defender** (Windows 7).

Question:

What is the status of the service?

Type your answers here.

c. Close the **Computer Management** window. Navigate back to the Windows Defender and turn it off.

In Windows 10, click **Virus & threat protection**. Scroll down to the **Virus & threat protection settings**. Click **Manage settings**. Under the Real-time protection heading, click the slider to turn it off. Click **Yes** to allow this app to make changes to the device.

In Windows 8.1, in the **Settings** tab, select the **Settings** tab. In the Settings tab, select **Administrator**. Click **Turn on this application** to turn off Windows Defender. Click **Save changes** to turn off Windows Defender. Click **Close** in the pop-up window as necessary.

In Windows 7, click **Tools**. Click **Options**. In the Options window, select **Administrator** > click **Use this program**. Click **Save** to stop Windows Defender. Click **Close** to continue when a message informing you that you have turned it off.

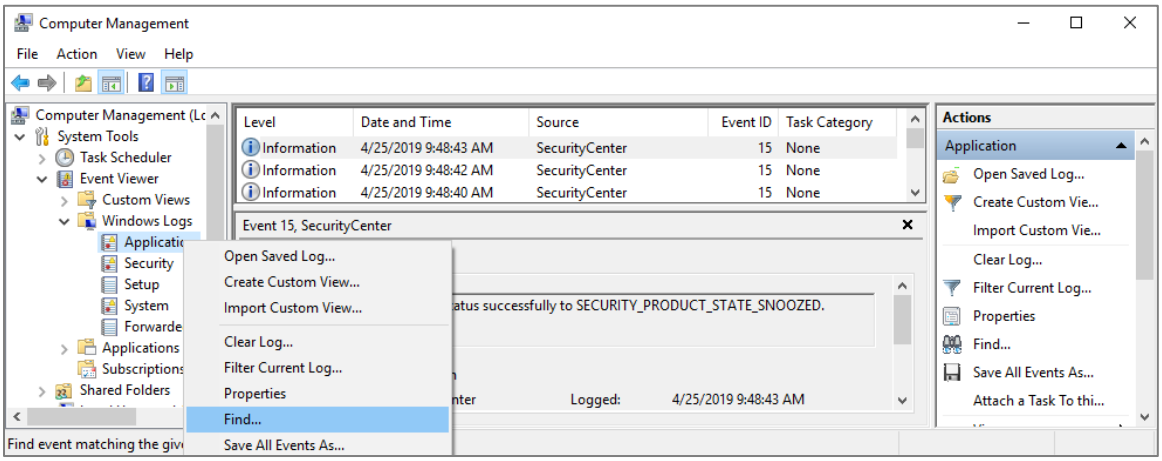
d. Navigate back to Services. (**Control Panel** in Small icons view > **Administrative Tools** > **Services**). Click **Action** > click **Refresh**.

Look for **Windows Defender Antivirus Network Inspection Service** (Windows 10) or **Windows Defender Service** (Windows 8.1) or **Window Defender** (Windows 7). Record the Windows Defender status.

Type your answers here.

e. Navigate to the Event Viewer. In the Computer Management window, expand **System Tools** > expand **Event Viewer** > expand **Windows Logs** > select **Application** (Windows 10), select **System** (Windows 8.1 and 7).

f. In the Application or System pane, you can find the most recent events are related to Windows Defender. Right-click the interested log, select **Find**. Enter **defender** to search Windows Defender related entries.



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

Type your answers here.

g. Navigate to Windows Defender and turn it on. Close Windows Defender.

h. Navigate to the Event Viewer to review the most recent event entries that are related to Windows Defender.

Part 2: 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.

Step 1: Verify printing service

a. Open **Notepad**. Click **Start** and search for **Notepad**.

b. In **Notepad**, click **File** > **Print**. Record a listed printer below. **Note**: You do not need to install a physical printer.

Type your answers here.

c. Click **Cancel** to exit the print dialog.

Step 2: Stop print spooler

a. Open the Services console. (Control Panel > Administrative Tools > Services)

b. Right-click **Print Spooler** and select **Stop**.

c. Navigate to **Notepad**. Attempt to print.

Question:

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

Type your answers here.

d. Click **OK** or **No** in the message window and click **Cancel** to exit the Print window.

Step 3: Restart print spooler

a. Navigate to the **Services** console and restart the print spooler. Right-click **Print Spooler** and select **Start**.

b. Verify that you can print.

Step 4: 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.

a. 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.

b. Click **No** in the **Stop Other Services** window.

Question:

Why is it important to exercise care when managing services?

Type your answers here.

c. Verify that **DHCP Client** is still running.

Part 3: Monitor and record system usage with Administrative Tools

You will configure advanced Administrative Tool features and monitor the usage of system resources of the computer.

Step 1: Create a new data collector set.

a. Navigate to Control Panel > click Administrative Tools > click Computer Management > Expand System Tools.

b. Expand **Performance** > Expand **Data Collector Sets** > in the left pane, right-click **User Defined** > select **New** > click **Data Collector Set**.

c. 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.

d. In the What type of data do you want to include? window, select Performance counter and click Next.

e. 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.

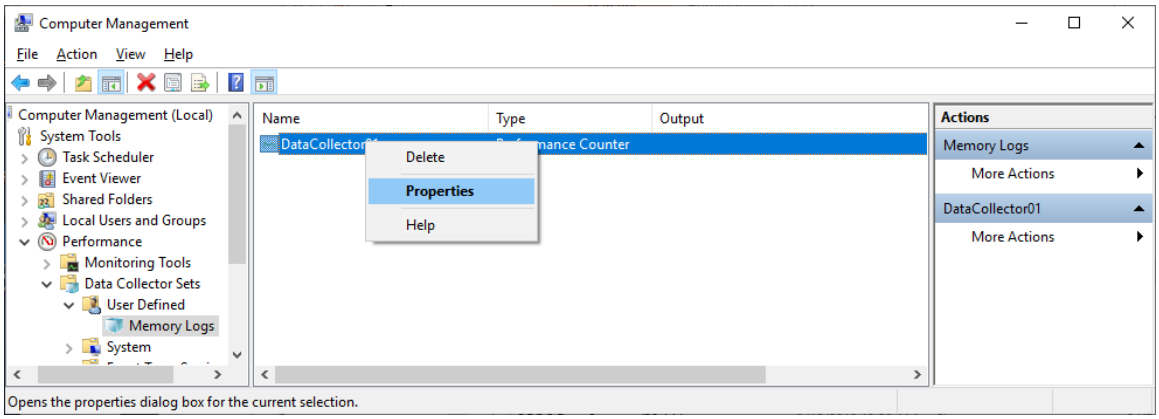
f. Set the **Sample interval**: field to **4** seconds. Click **Next** to continue.

g. In the Where would you like the data to be saved? Window, click Browse. Select Local Disk (C:) and select PerfLogs. Click OK to continue.

h. Verify the correct root directory path is displayed (C:\PerfLogs), and click **Finish** to continue.

Step 2: Format the data collector set.

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



b. In DataCollector01 Properties window, change the Log format: field to **Comma Separated**.

c. Click the **File** tab.

Question:

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

Type your answers here.

d. Click **OK** to continue to close the Properties window.

Step 3: Collect and view the data.

a. Select the **Memory Logs** icon in the left pane of the **Computer Management** window. Right-click **Memory Logs** and select **Start**.

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

c. Right-click **Memory Logs** and select **Stop** to stop the data collection set.

Navigate to **Local Disk (C:)\PerfLogs**. Click **Continue** in the Windows warning messages.

d. Open the folder that was created to store the memory log. Click **Continue** on the Windows warning messages. Open the **DataCollector01.csv** file.

Select **Notepad** or another program that can read comma-separated files (.csv) to open the file if the Windows cannot open the file message is displayed.

Question:

What does the column farthest to the right show?

Type your answers here.

e. Close the DataCollector01.csv file.

Step 4: Clean up

a. Navigate to the **Computer Management** window. Select **Performance** > click **Data Collection Sets** > click **User Defined**. Right-click **Memory Logs** and select **Delete**. Click **Yes** to confirm the deletion.

b. Navigate to the **Local Drive C: > PerfLogs** folder. Delete the stored memory logs folder (folder with the DataCollector01.csv) created from this lab.

c. Close all opened windows.