

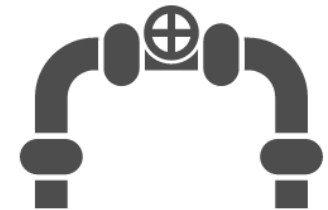


Server Manager

Introduction

The TxRig server is up and running! Let's review tools we can use to ensure it stays that way...

Now that you have installed your server, it is critical that you check the hardware and operating system to ensure everything is in good working order. Servers in a production environment are rarely shut down or restarted. It is critical that servers are available for users to access services and data.



Texas Rig, Inc.

Fueling The Future.

The goal of this lesson is to introduce you to a variety of tools to check the overall health of your computer and to verify your server does not have any issues that need to be addressed. The tools that you will use during this assignment can aid you in monitoring, identifying, configuring and troubleshooting potential issues. When a server needs troubleshooting, several built-in Windows utilities can be used to reveal the source of technical issues.

Objectives

In this lab the student will:

- Explore Resource Monitor, Performance Monitor, Event Viewer, and helpful command line tools

Resources

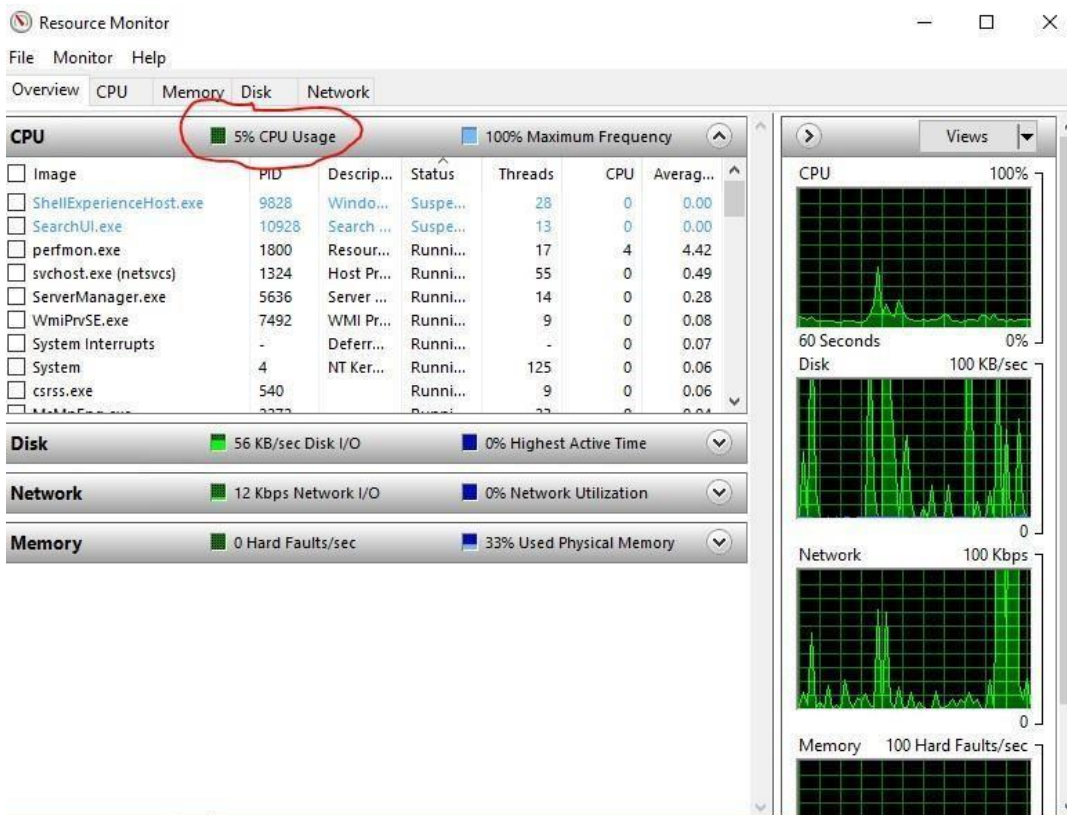
- Computer with Internet access
- VMWare Workstation Pro
- Windows Server and Client VMs created in previous unit

Assignment

Activity 1: In this activity, you open Resource Monitor to assess current CPU, memory, disk, and network activity in Windows Server.

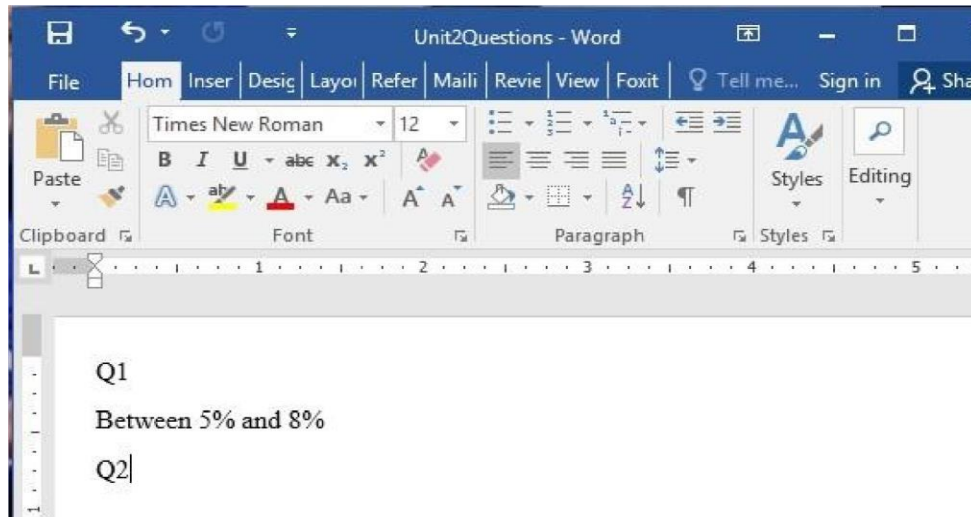
Server Manager offers a quick view of your server health and quick access to a variety of Microsoft Tools. As a technician, Server Manager is a valuable tool to quickly access a variety of Tools to aid collection of information about the overall health of your server.

1. Create a folder on your local host computer for the lab documents. To do this, open **File Explorer**, select "Local Disk C:" in the left pane, click the "New Folder" icon at the top and name the folder "Labs".
2. Open Notepad to record your answers to the questions for this lab and save the file as c:\Labs\Lab2_1_1a.txt.
3. Login to your Windows Server 2019 VM as Administrator with a password of **Itnw1354** (or whatever password you chose instead).
4. Open **Server Manager**.
5. On the menu, select **Tools** and click **Resource Monitor**.
6. Be sure the **Overview** tab is selected.
7. Click the down arrow for **CPU**, if necessary, to view processes associated with CPU activity.



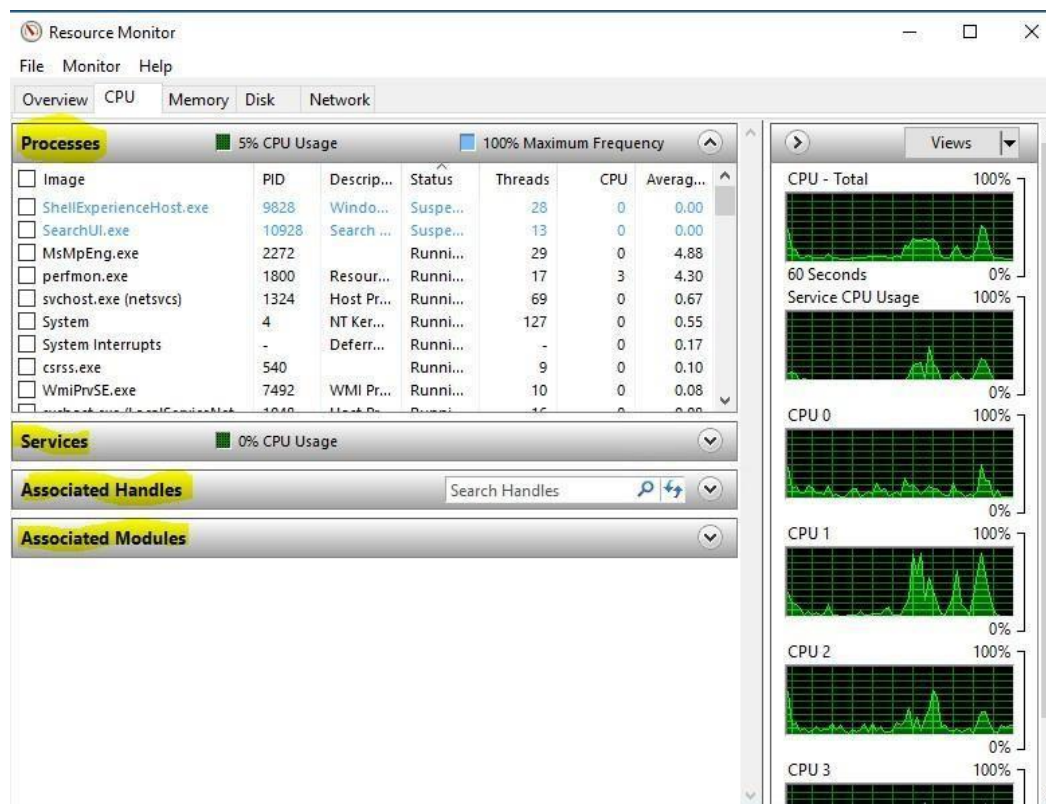
Q1 - What is the % CPU Usage?

8. Type the answer to Q1 in your Lab2_1_1a.txt file. Make sure you label all the questions:



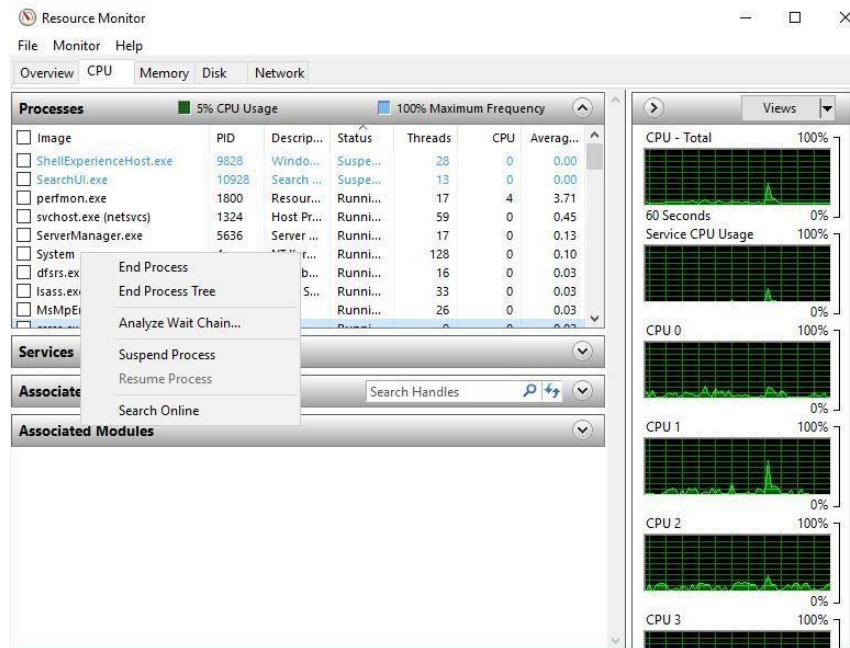
9. Click the **CPU** tab.

Q2 - What four sections of information do you see to view information about CPU activity?



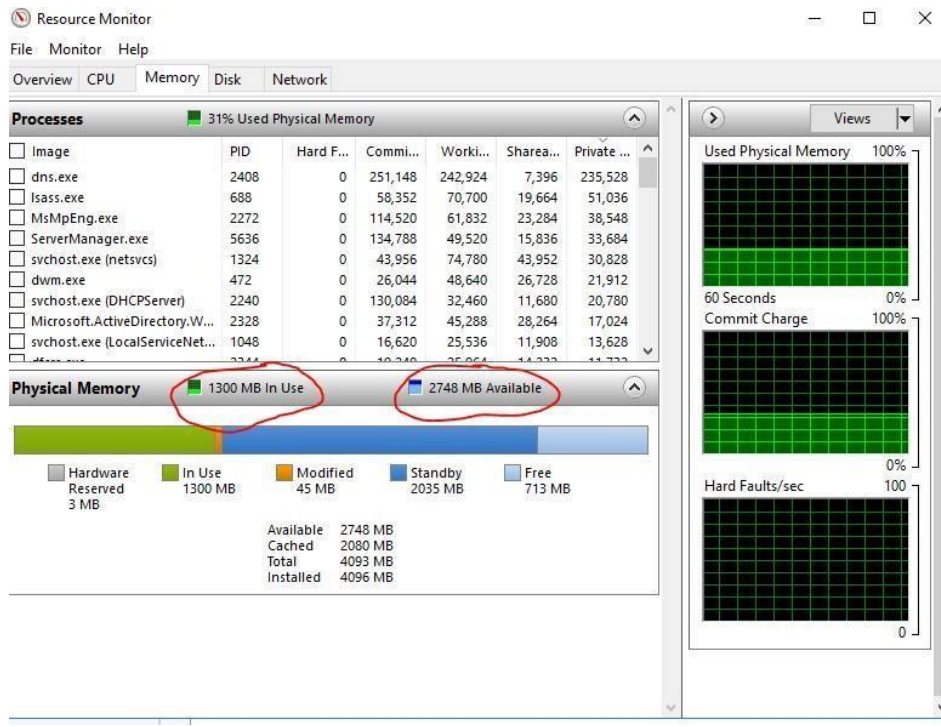
10. Under the **Processes** section in the CPU tab, right-click a process, such as **Server Manager.exe**.

Q3 - What actions can you take from this menu?



11. Click the **Memory** tab.

Q4 - What is the average MB in Use data associated with the Physical Memory section?

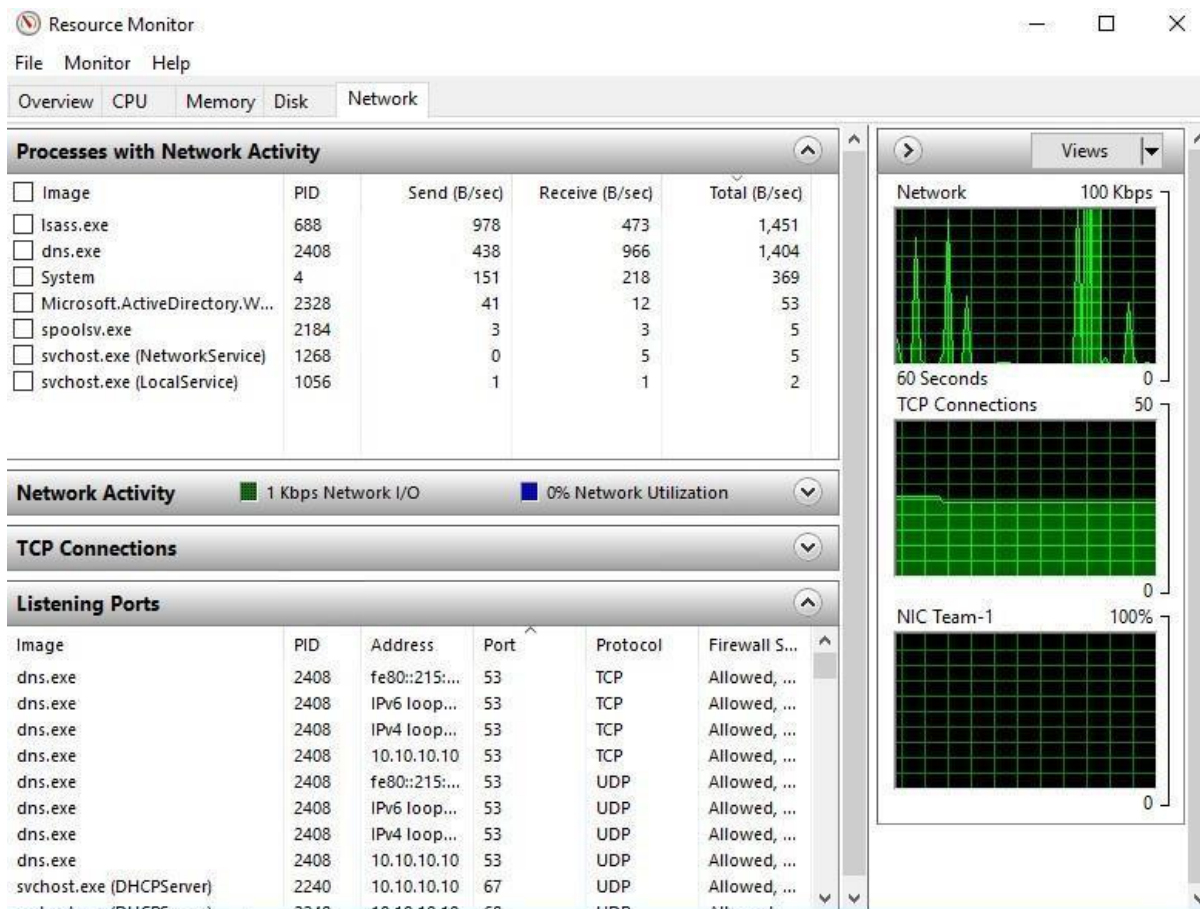


12. Click the **Disk** tab. Click the down arrows to expand the **Disk Activity** and **Storage** sections. Review the information in each of these sections. View the graphs in the right pane showing real-time disk activity information.

13. Click the **Network** tab.

Q5 - What is the current % Network Utilization?

Q6 - Which section of information in the left pane enables you to determine TCP and UDP ports that are active and allowed or not allowed through Windows Firewall?



14. Close **Resource Monitor**, but leave Server Manager open for the next activity.

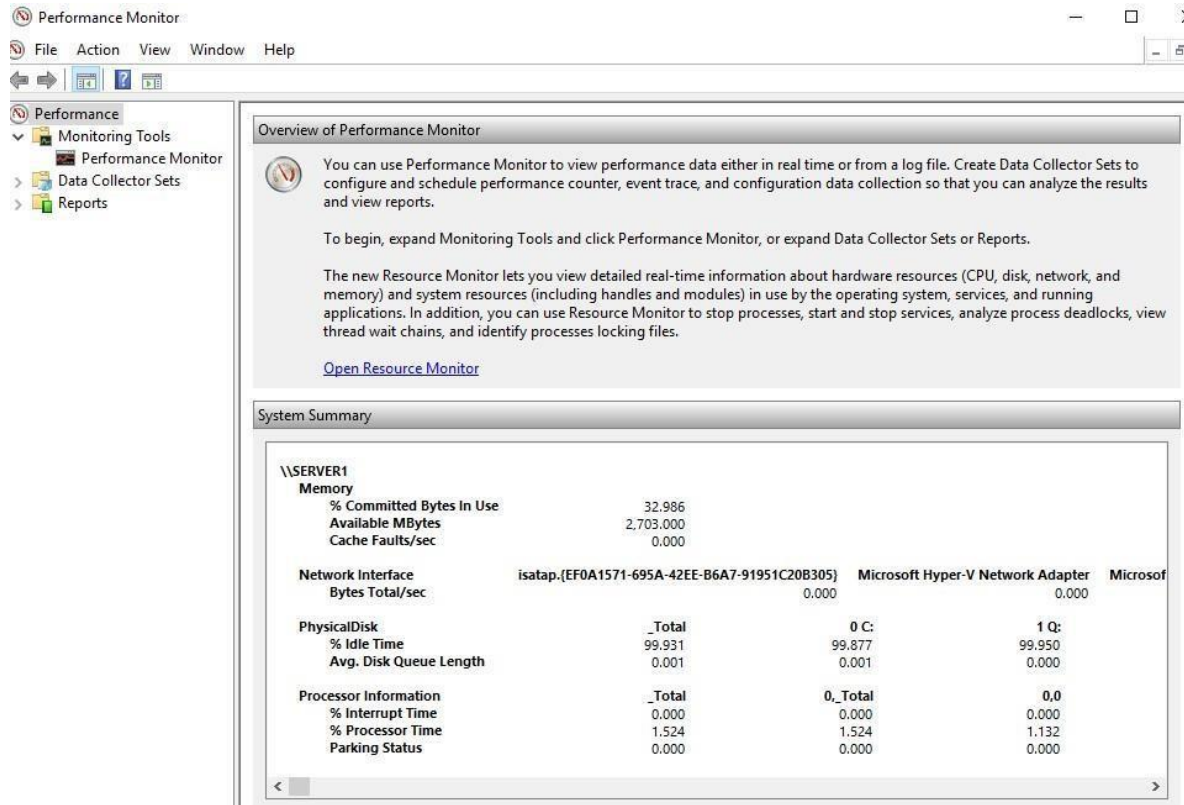
Activity 2: In this activity, you will have an opportunity to practice viewing objects, counters, and instances in Performance Monitor.

1. Login to your Windows 2019 Server and open **Server Manager**, if it is not already open.
2. On the menu, select **Tools** and then click **Performance Monitor**.
3. When the tool starts, ensure that **Performance** is selected in the left pane and read

the **Overview of Performance Monitor**.

4. Next, scroll through the **System Summary** to review basic information about your server.

Q7 - What are the main categories of information provided in the System Summary?



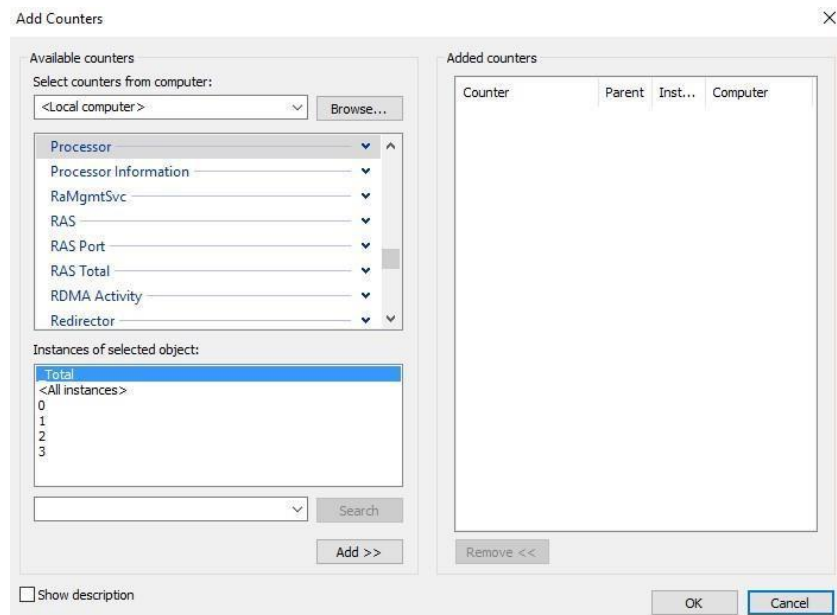
5. If necessary, expand the tree in the left pane and click **Performance Monitor** under **Monitoring Tools**.

6. In the right pane, move your pointer over each of the buttons on the button bar to view its description.

7. Click the **Add** button (a plus sign) in the button bar in the right pane.

Q8 - What computer is selected by default for monitoring?

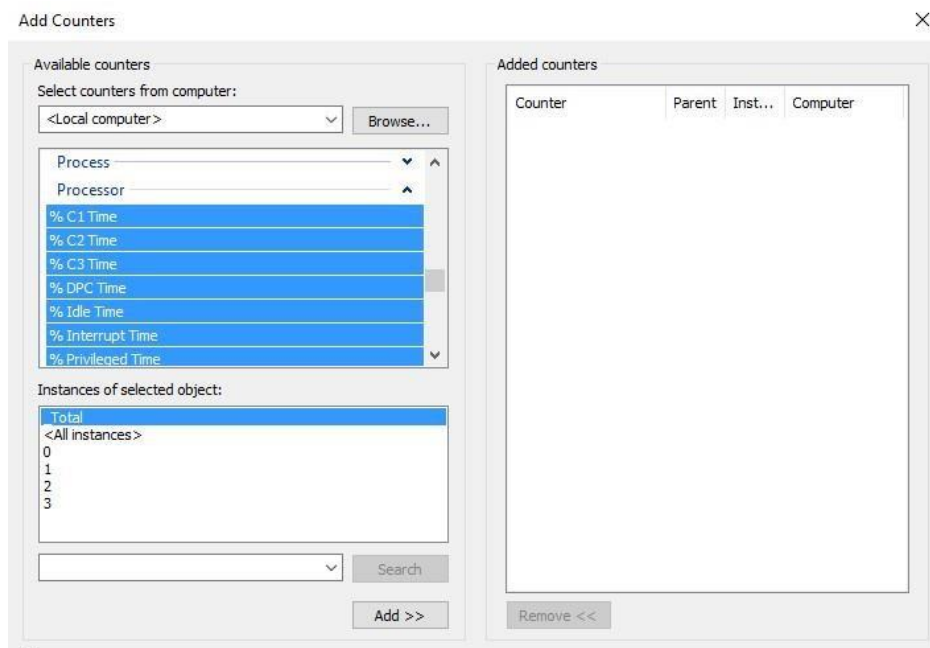
Q9 - How would you monitor activity on a different computer?



8. Scroll through the objects in the box under the computer that is selected.

9. Click the **down** arrow to the right of **Processor**. Scroll to view the counters associated with the Processor object. After you answer the following question and are done viewing, collapse the list by clicking the up arrow to the right of **Processor**.

Q10 - What are the first five counters listed?



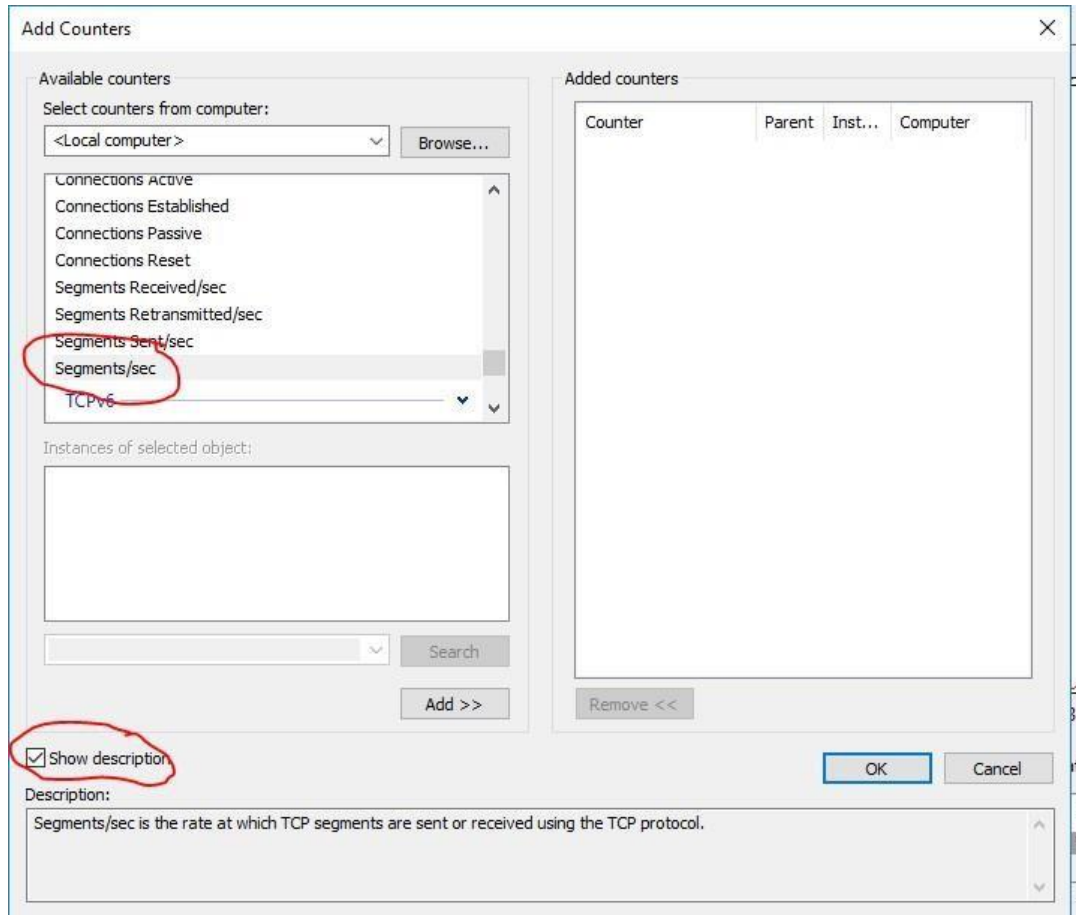
10. Next, select to view the **Server** counters under **Server** (click the down arrow). Scroll through the counters for Server to view them all. Collapse the list for Server after you are finished viewing.

11. Select to view **Process** as the object and view the counters associated with

Process. Collapse the list under Process.

12. Choose to view the **TCPv4** object and the counters for this object. Click the **Segments/sec** counter and click the **Show description** check box.

Q11- What is the description of this counter displayed at the bottom of the window?

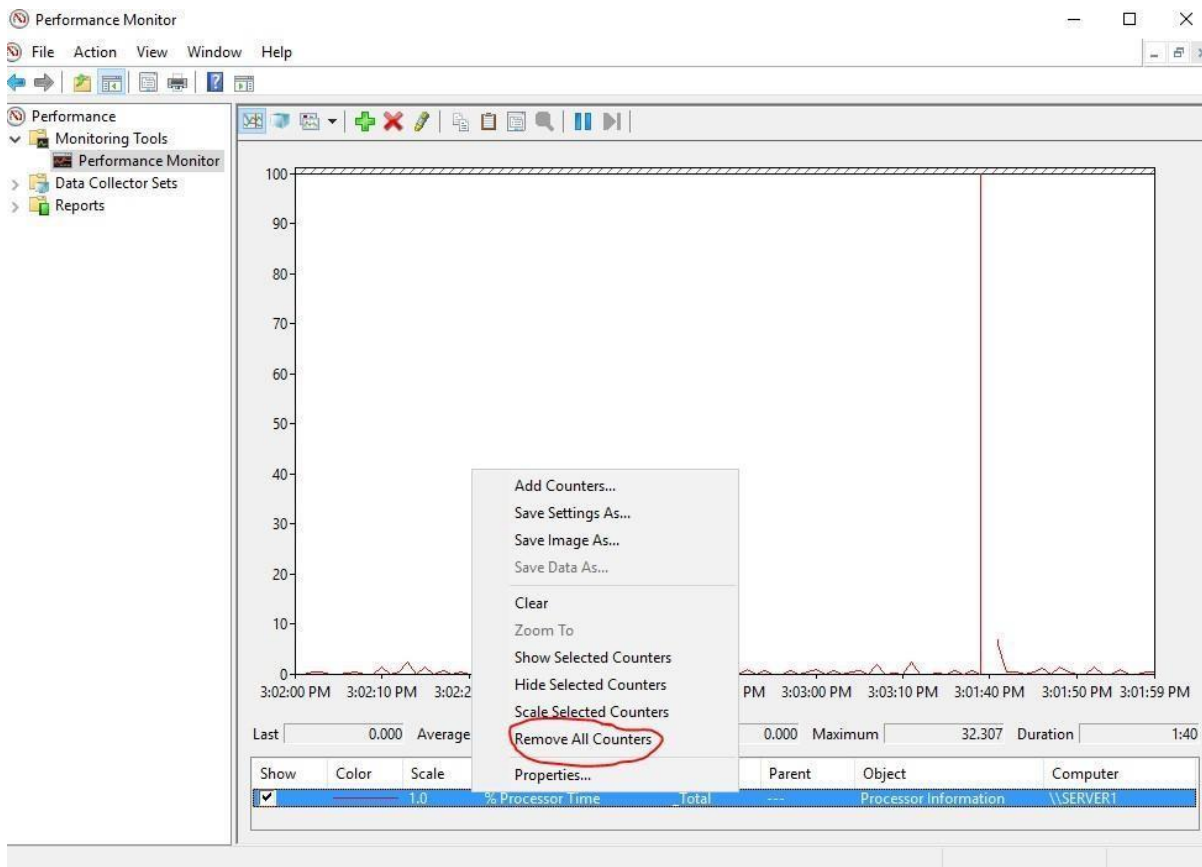


13. Click **Cancel** in the **Add Counters** window, but leave the **Performance Monitor** window open for the next activity.

Activity 3: In this activity, you use Performance Monitor to check for processor bottlenecks, such as the processor's ability to handle the server load and possible

problems caused by hardware.

1. Make sure that the **Performance Monitor** window is already open, and if not, open it to display the Performance Monitor.
2. If any **object/counter** combinations are currently running—by default **% Processor Time** should still be running—right-click anywhere in the right pane, click **Remove All Counters**, and click **OK**.

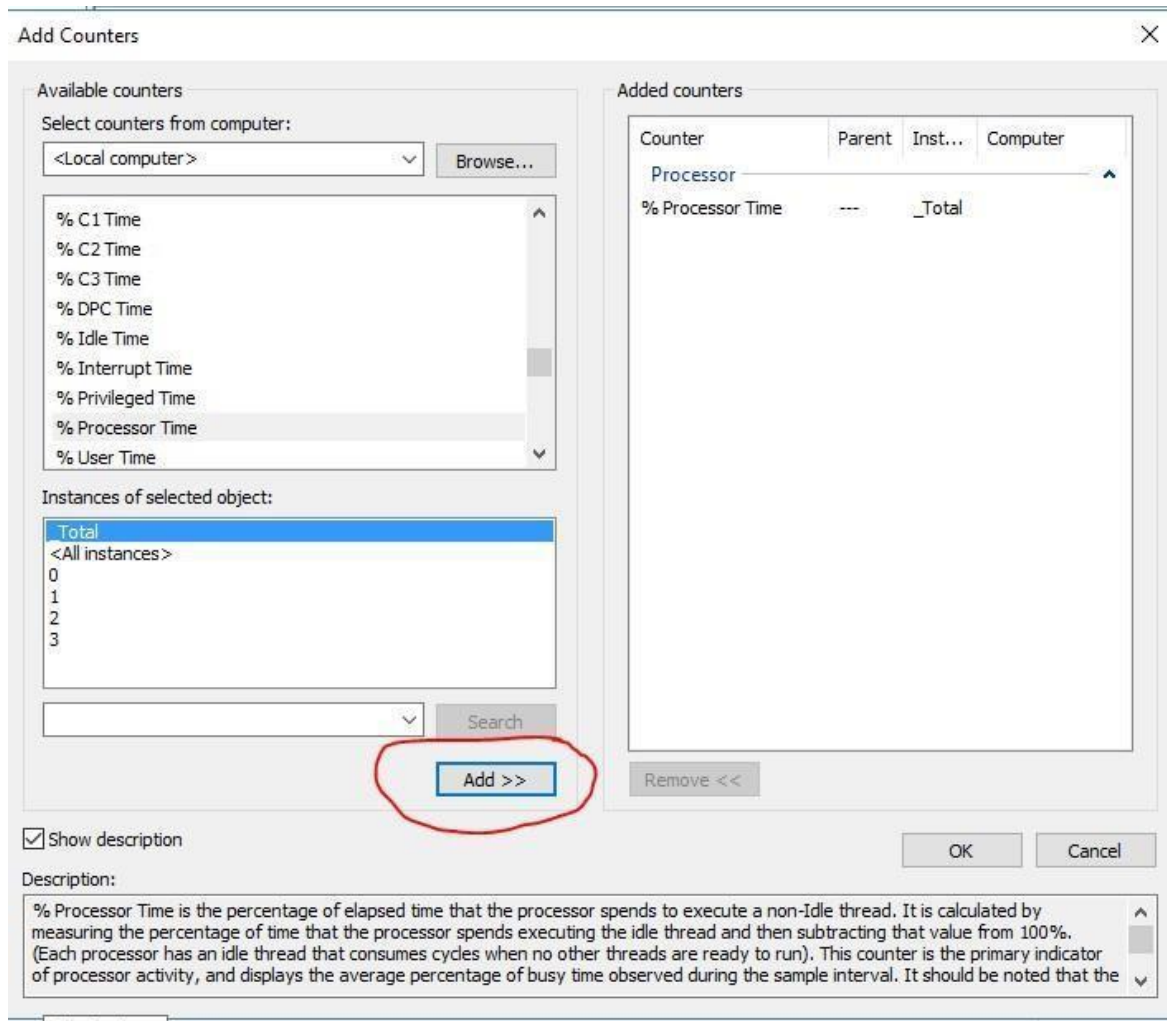


3. Click the **Add** button in the button bar to add counters.
4. Scroll to find the Processor and click its down arrow.
5. Click **% Processor Time**. Leave **_Total** as the default for instances.

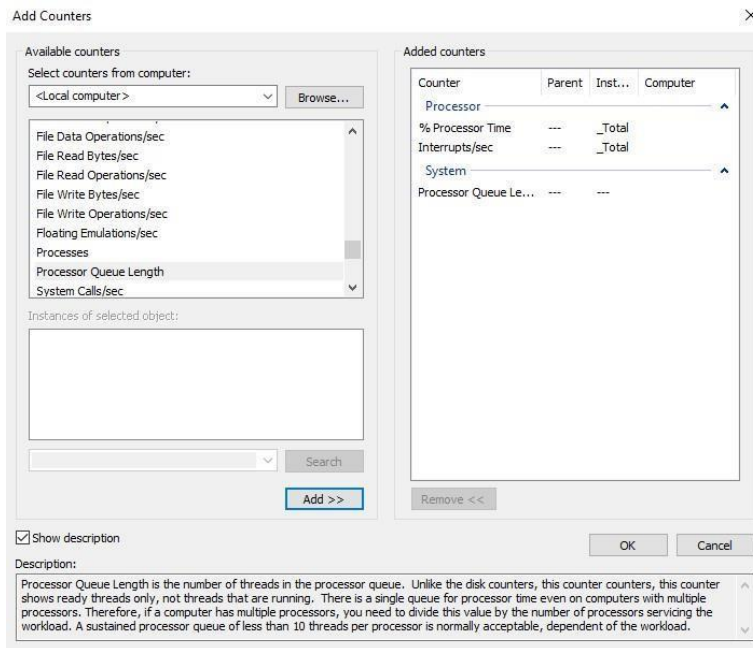
Q12 - What information does this counter provide for the Processor object?

Q13 - How would you find out, if you didn't know?

6. Click the **Add** button in the **Add Counters** dialog box.
7. Click **% Interrupt Time** as the counter for **Processor** and leave **_Total** as the instance. Click **Add**.



8. Scroll the counters list for the **Processor** object and click **Interrupts/sec**. Leave **_Total** as the instance and click **Add**.
9. Scroll to find the **System** object and click its down arrow.
10. Click **Processor Queue Length**. Click **Add**. Click **OK**.



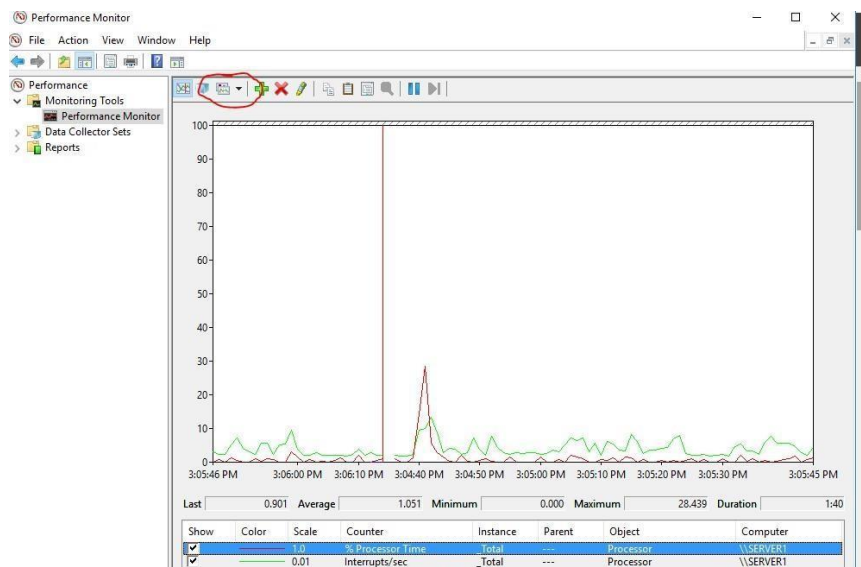
11. Monitor the system for several minutes to determine if there are any processor problems.

Q14 - Record any problems that you diagnose from using Performance Monitor.

12. Click the **Change** graph type button down arrow just to the right of the graph's box and click the Histogram bar to see this mode. Monitor in this mode for a few minutes.

13. Click the **Change graph type** button down arrow and click **Report** to see this mode. Monitor in this mode for a few minutes.

14. Click the **Change graph type** button down arrow and click **Line**.

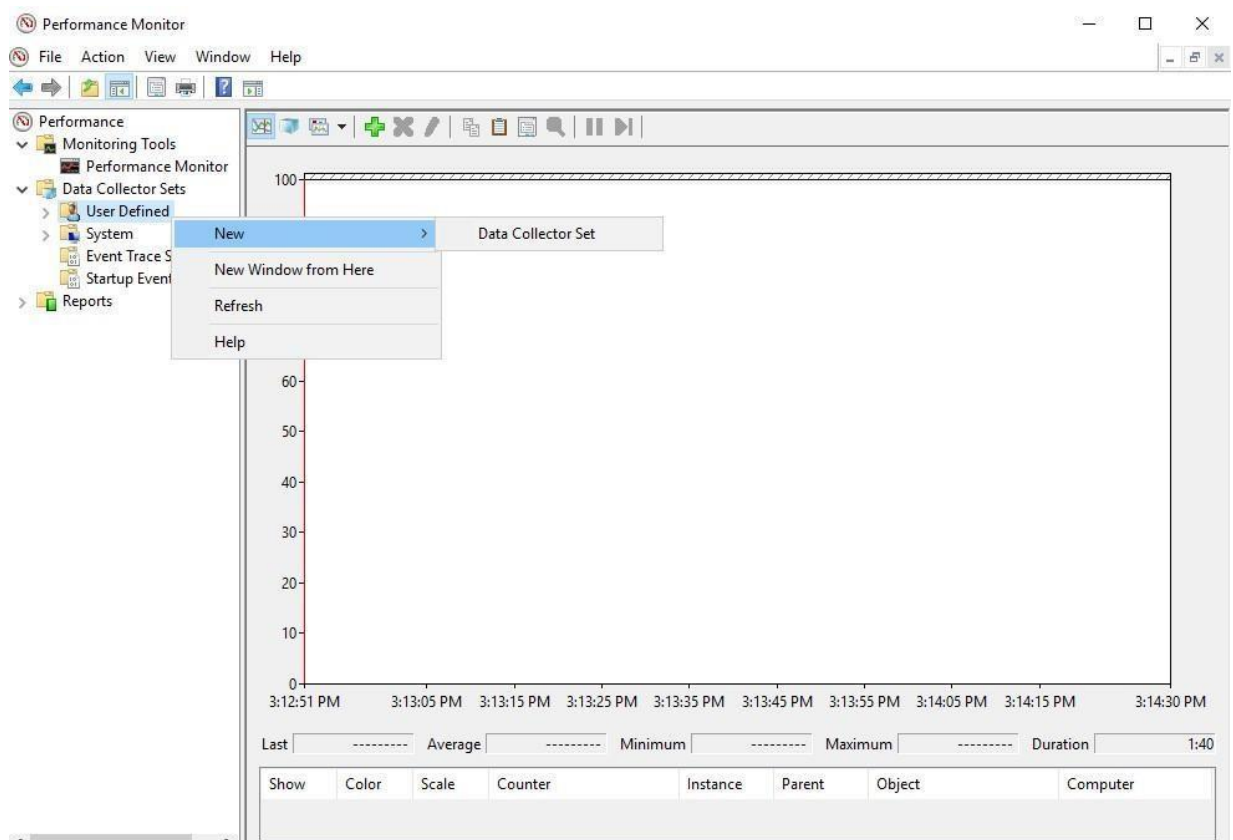


15. Right-click anywhere in the right pane, click **Remove All Counters**, and click **OK**.

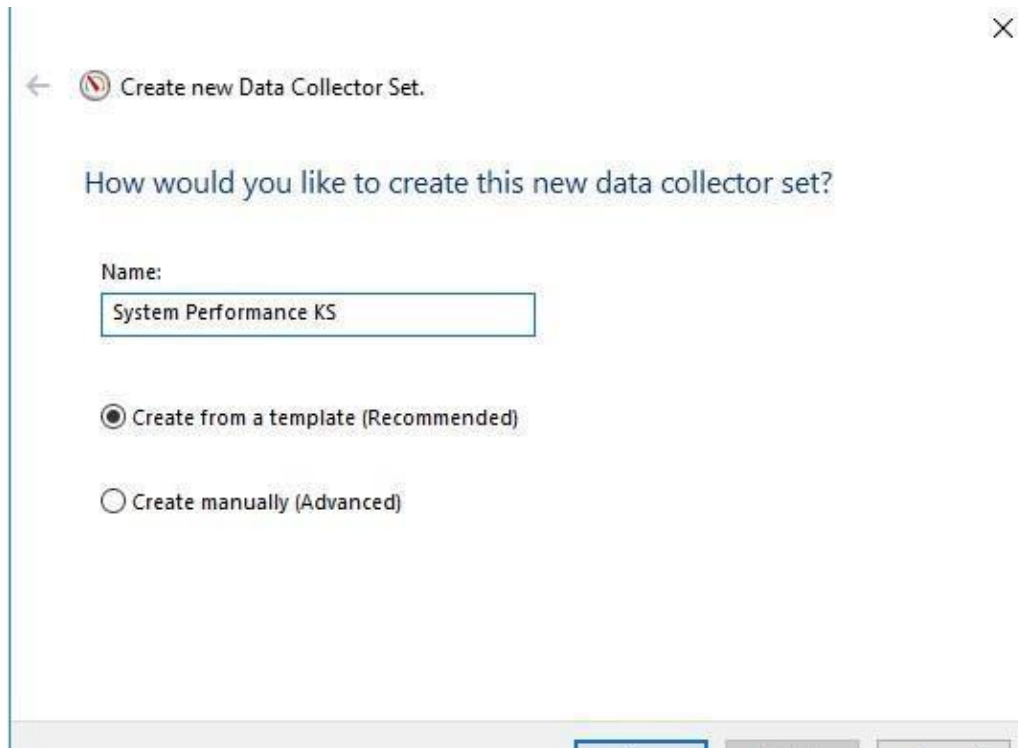
16. Remain logged on and leave the **Performance Monitor** window open.

Activity 4: In this activity, you use the System Performance template to create a data collector set.

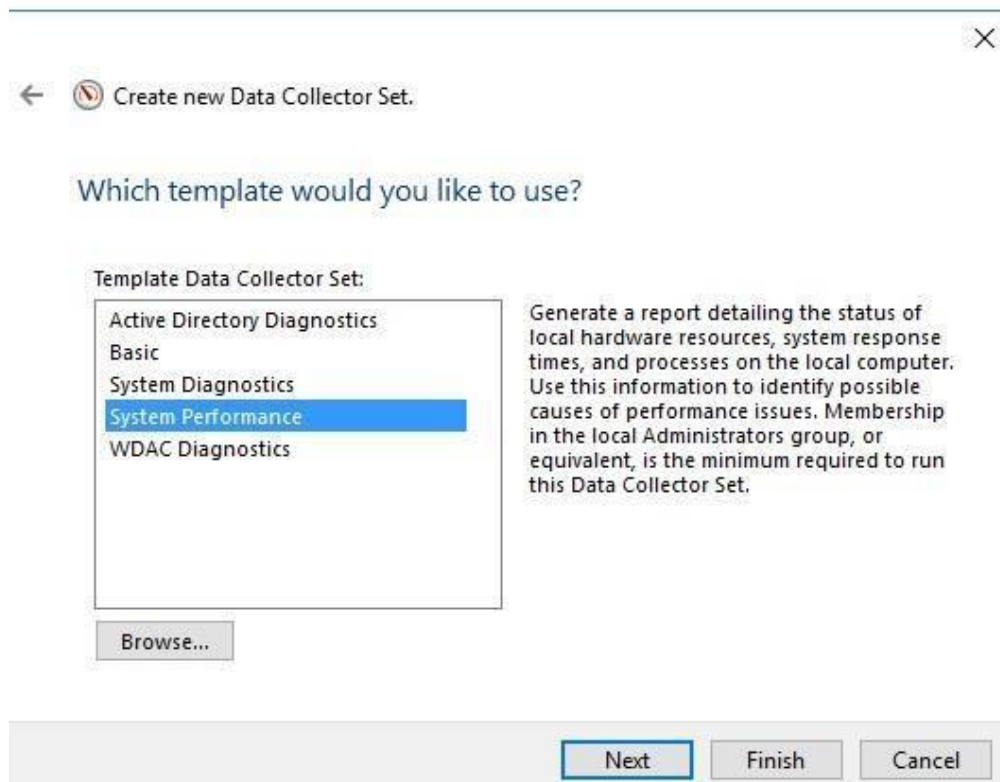
1. Ensure that the Performance Monitor window is already open, and if not, open it.
2. Click the right-pointing arrow in front of **Data Collector Sets** in the tree in the left pane, if necessary, to see the items under it.
3. Right-click **User Defined**, point to **New**, and click **Data Collector Set**.



4. In the **Name** box, enter **System Performance plus your initials**, such as System Performance KS.
5. Ensure that **Create from a template (Recommended)** is selected.
6. Click **Next**.



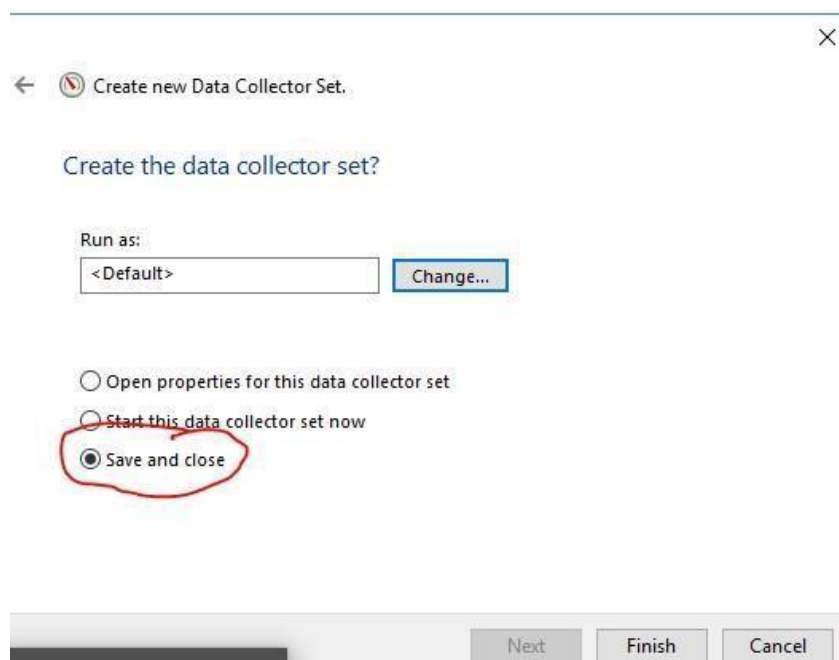
7. Click **System Performance** under Template Data Collector Set and click **Next**.



8. Use the default location in which to save the data and click **Next**.

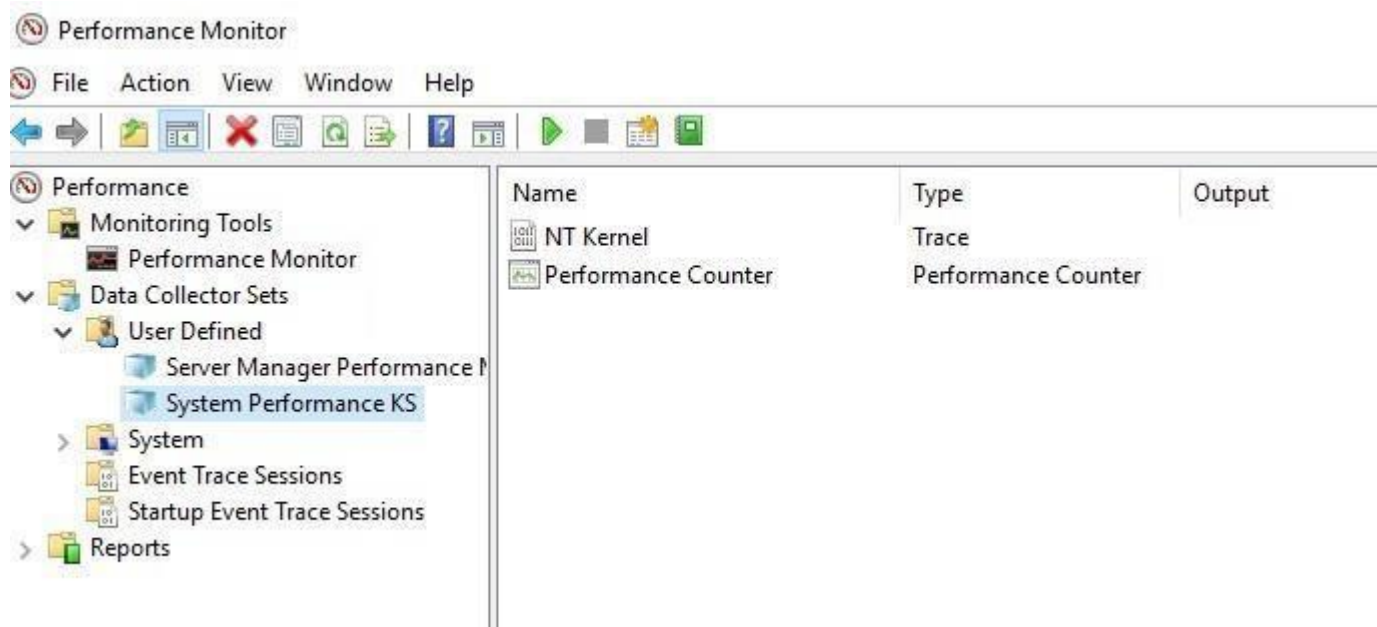
9. Click **Save** and **close**, if it is not selected already.

10. Click **Finish**.



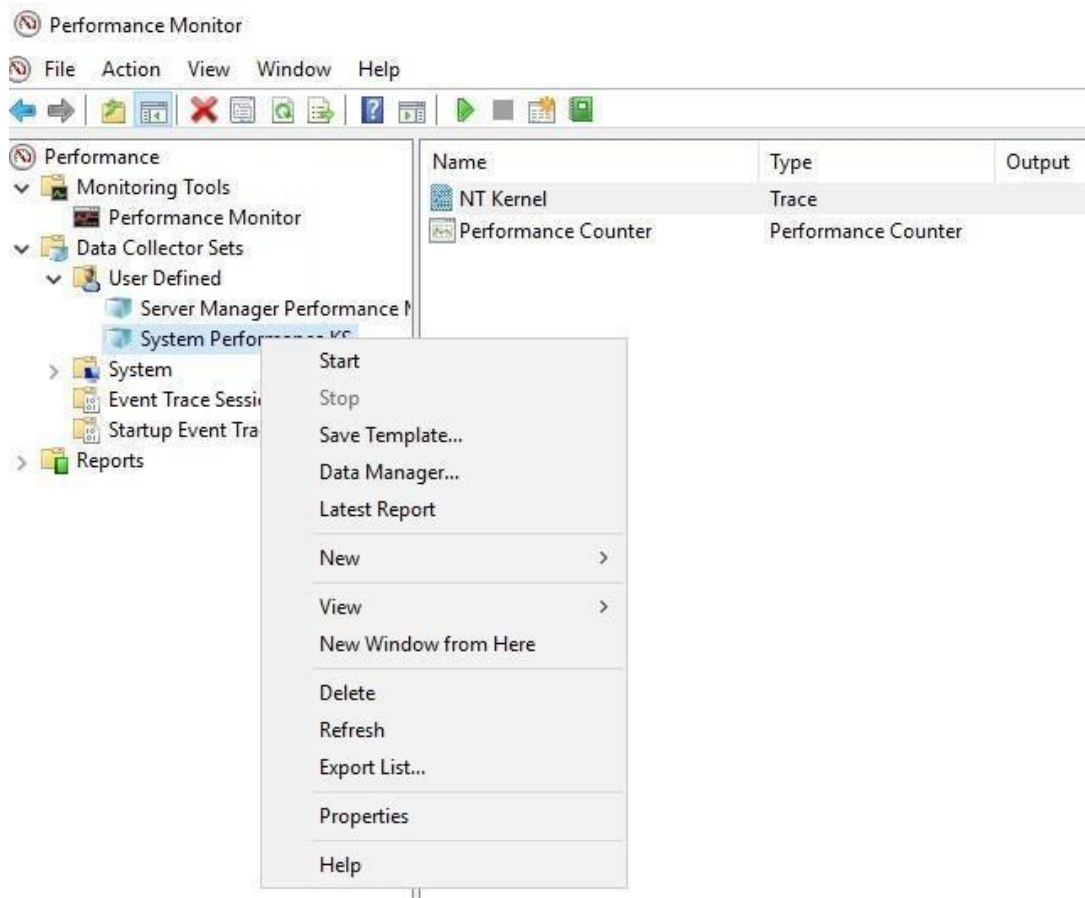
11. Click the right-pointing arrow in front of **User Defined** in the tree, if it is not expanded, and notice the data collector set that you created is listed under **User Defined**.

12. Click the data collector set you created in the tree. In the right pane, notice that it includes **NT Kernel**, which incorporates a trace session of real-time CPU activity, memory, disk, and network activity. The second tracking element is Performance Counter, which is a combination of counters for processes, physical disk, CPU, memory, system, server, and many network counters.

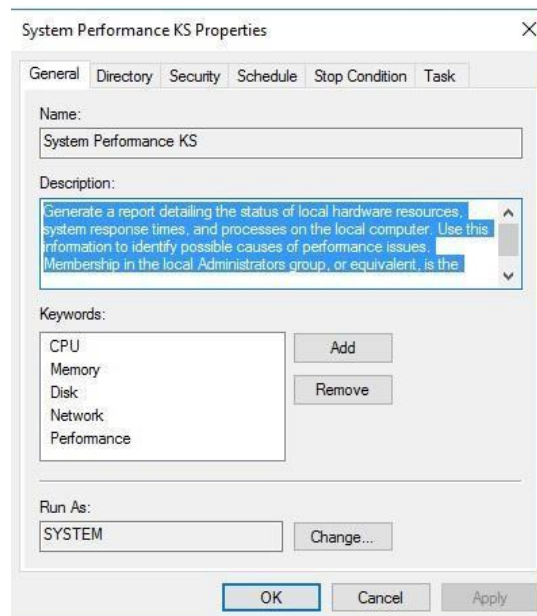


13. Right-click the data collector set you created, such as System Performance KS.

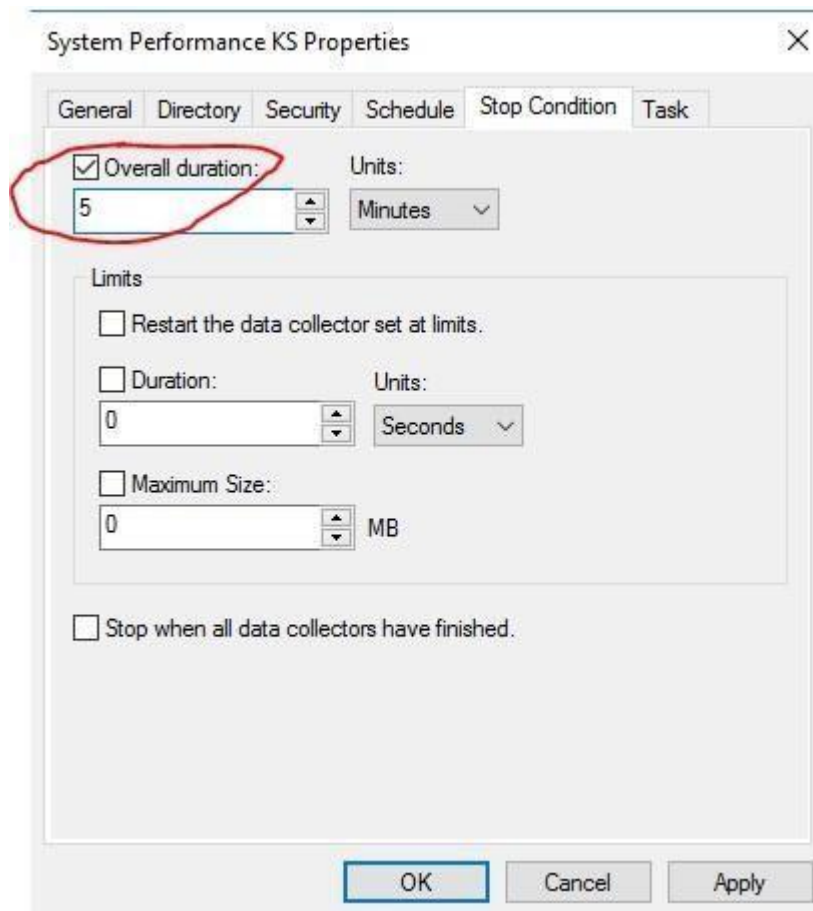
Q15 - What options do you see enabled on the menu?



14. Click **Properties**. On the **General** tab, read the description of the template.



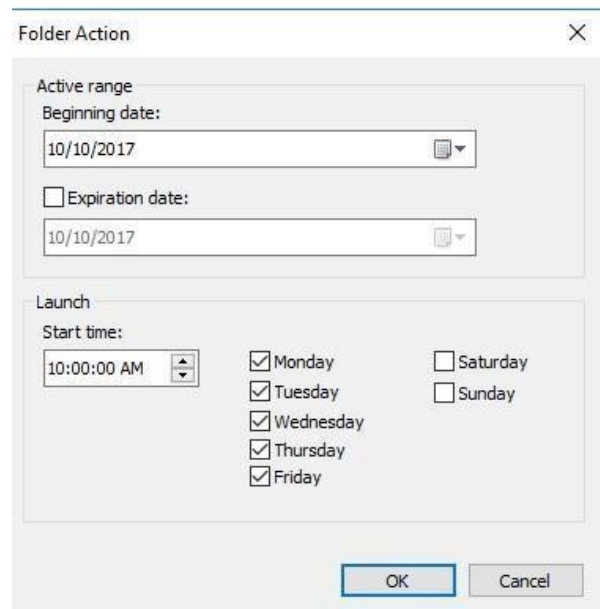
15. Click the **Stop Condition** tab. Under **Overall duration**, set the value to **5** and leave the **Units** value as **Minutes**. This means 5 minutes of data is collected each time you start the data collector set.



16. Click the **Schedule** tab. This tab enables you to schedule a regular start time for collecting data.

17. Click the **Add** button on the **Schedule** tab.

18. In the **Folder Action** dialog box, the default time is 12:00 AM. However, because you are monitoring system performance, it makes more sense to gather data when the system is in full work mode, such as at 10:00 AM or 2:00 PM or whatever time is more appropriate for your organization. For this activity, change the Start time to **10:00:00 AM**. Also, remove the check marks from **Saturday** and **Sunday**.



19. Click **OK** in the Folder Action dialog box.

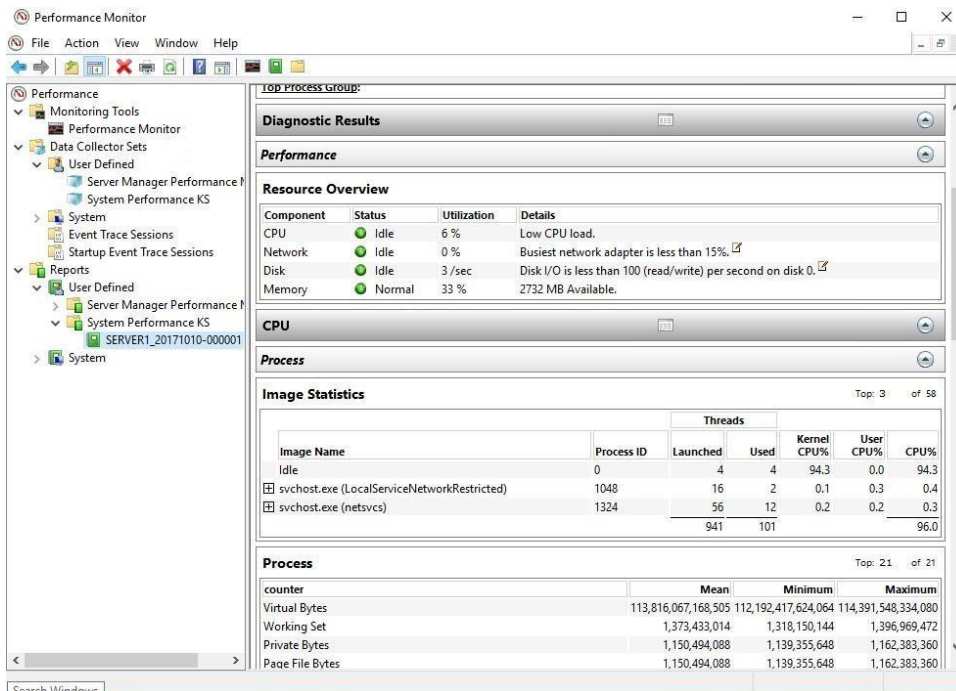
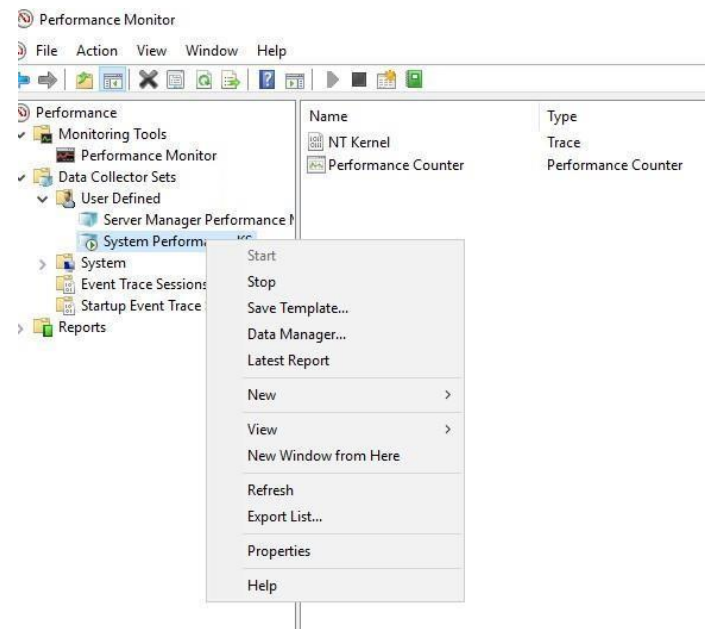
20. Click **OK** in the System Performance (your initials) Properties dialog box.

21. In the tree, right-click the data collector set you created, such as System Performance KS, and click **Start** to commence gathering data.

22. Wait a few minutes (you don't have to wait for five minutes because you can manually stop the data collection sooner). Right-click the data collector set in the tree and click **Stop**.

23. Right-click the data collector set in the tree again and click **Latest Report**.

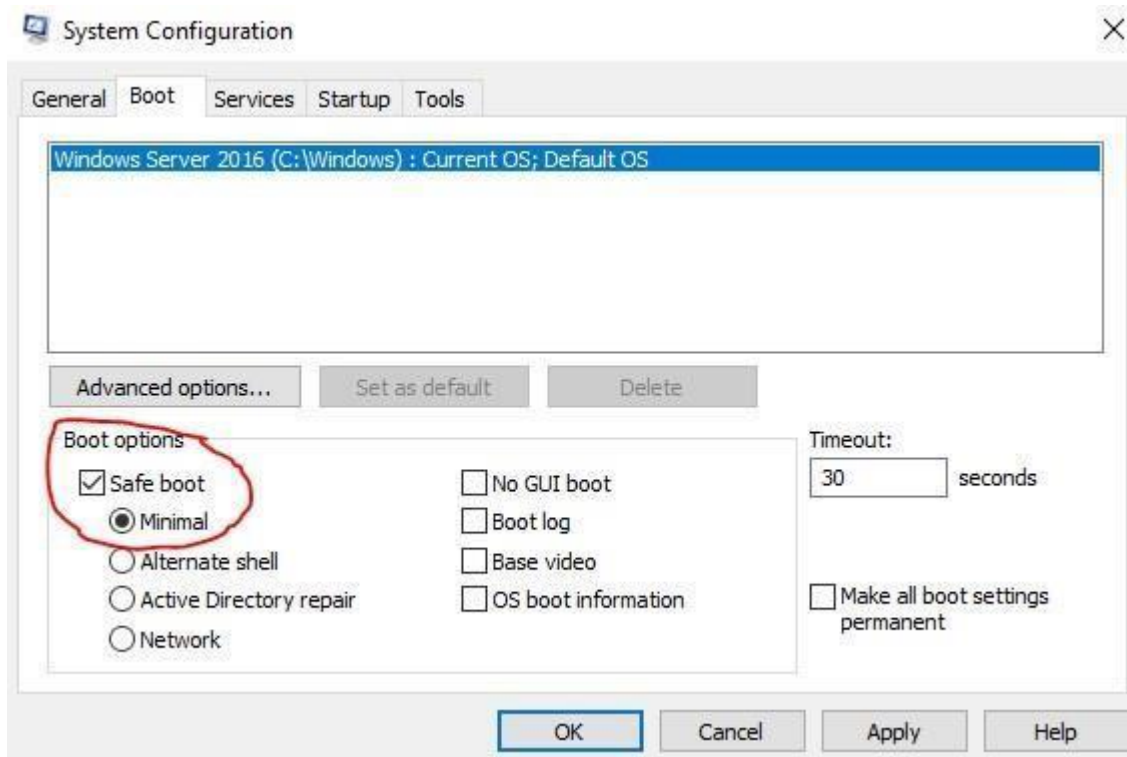
24. In the right pane, you'll see the report of information you have collected so far.



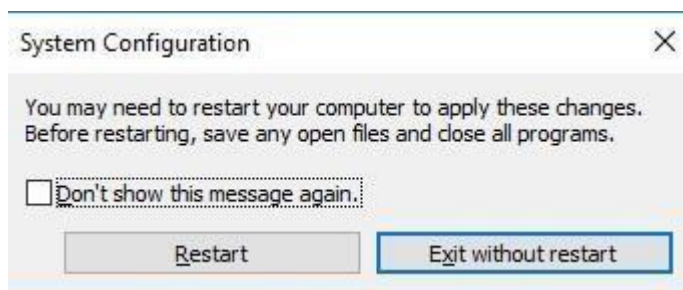
25. Close Performance monitor but remain logged on for the next activity.

Activity 5: In this activity, you practice accessing the advanced boot options on a server and then you boot into the Safe Mode.

1. Select **System Configuration** from the **Tools** menu in **Server Manager**.
2. Click on the **Boot** tab and place a check in the **Safe boot** checkbox and leave **Minimal** selected. Click **OK**.



3. Click **Restart** on the System Configuration pop-up dialog box.



4. After the server restarts, login as **Administrator**.

Q16 - How is the Windows Server desktop display different in Safe Mode from when you boot normally?

Q17 - What else is different in Safe Mode?

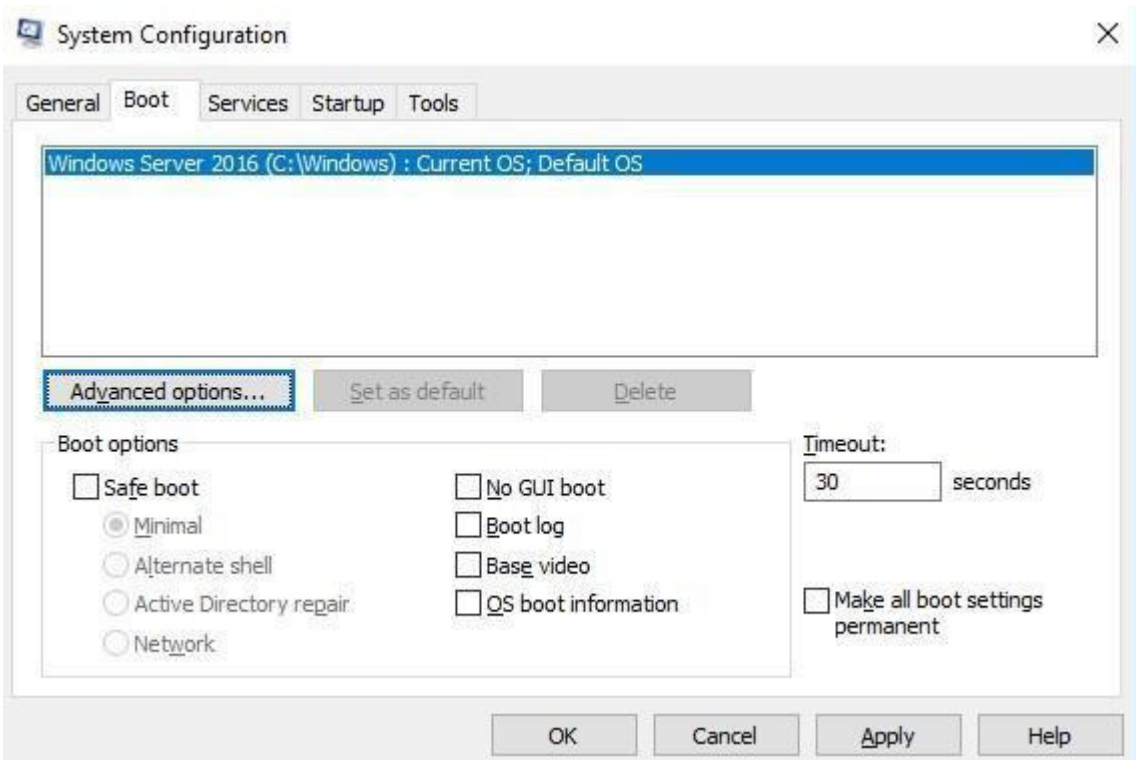
5. Open **Server Manager**, then open **Active Directory Users and Computers**.

Q18 - Were you successful?

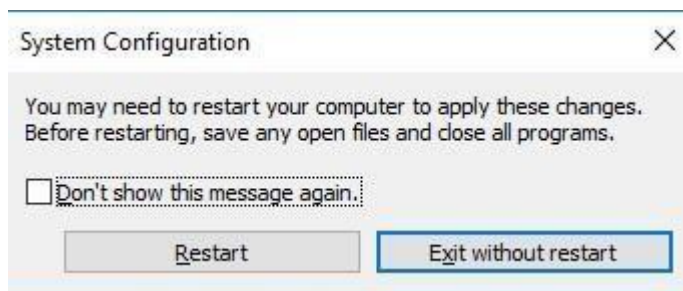
Q19 - Why?

6. Click **Start** and type **System Configuration** and open the **System Configuration** app.

7. Click on the **Boot** tab and remove the check in the **Safe boot** checkbox and click **OK**.



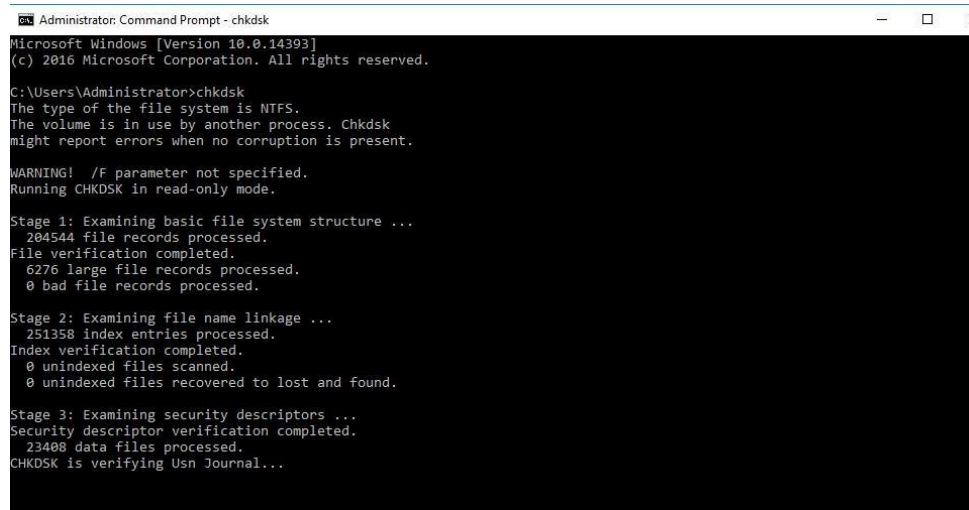
8. Click **Restart** on the System Configuration pop-up dialog box.



9. After the server restarts, login as Administrator.

Activity 6: In this activity, you use the `chkdsk` utility from the command line.

1. Open a command prompt window and type **chkdsk** to check the file system and press **Enter**. When **chkdsk** is finished, take a screenshot and upload it.



```
Administrator: Command Prompt - chkdsk
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>chkdsk
The type of the file system is NTFS.
The volume is in use by another process. Chkdsk
might report errors when no corruption is present.

WARNING! /F parameter not specified.
Running CHKDSK in read-only mode.

Stage 1: Examining basic file system structure ...
204544 file records processed.
File verification completed.
6276 large file records processed.
0 bad file records processed.

Stage 2: Examining file name linkage ...
251358 index entries processed.
Index verification completed.
0 unindexed files scanned.
0 unindexed files recovered to lost and found.

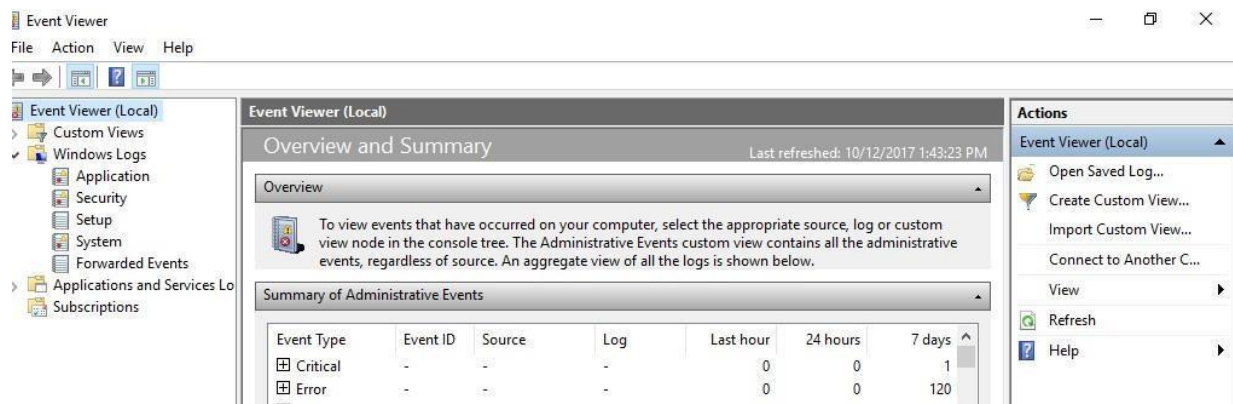
Stage 3: Examining security descriptors ...
Security descriptor verification completed.
23400 data files processed.
CHKDSK is verifying Usn Journal...
```

2. Type **exit** and press **Enter** to close the Command Prompt window.

Activity 7: In this activity, you use Event Viewer to examine system log events, and you practice using a filter.

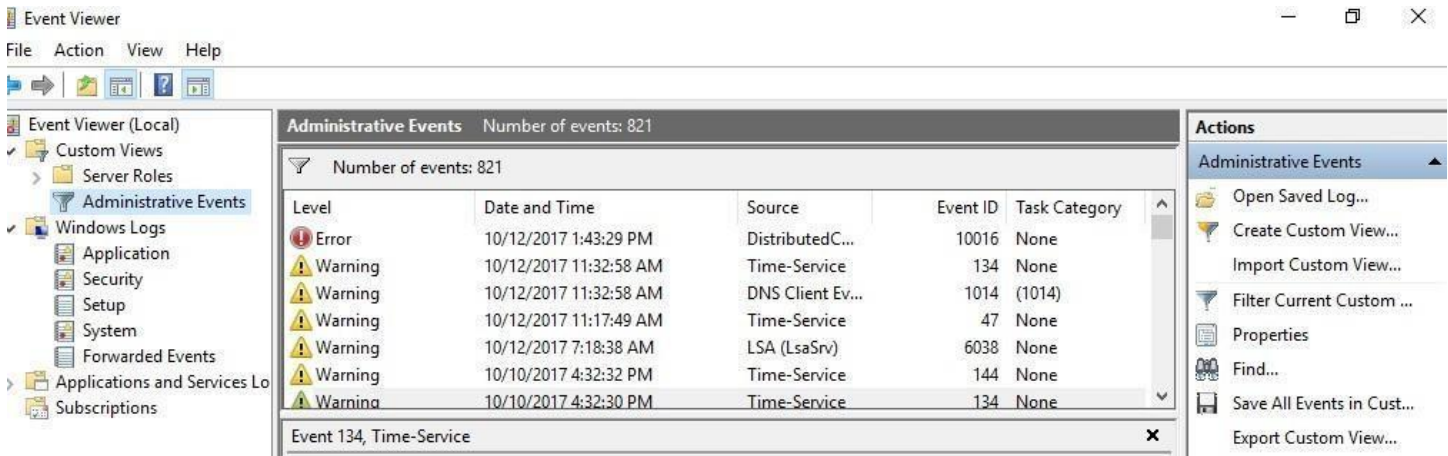
1. Open **Server Manager**, if it is not open.
2. Click **Tools** and click **Event Viewer**.
3. In **Event Viewer**, click the right-pointing arrow in front of **Windows Logs** (under Event Viewer (Local)).

Q20 - What five logs do you see?



4. Click each log to view the information displayed for it in the middle pane.

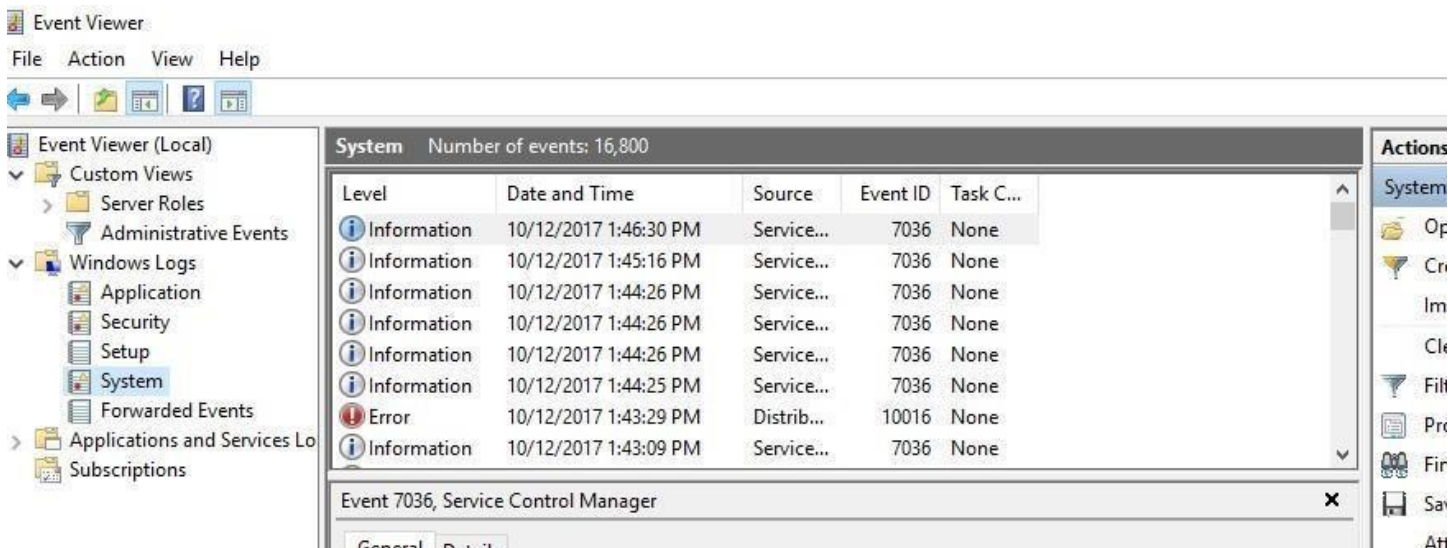
- Click the right-pointing arrow in front of **Custom View** in the left pane.
- Click **Administrative Events** under Custom View in the left pane. The middle pane shows a compilation of errors and warnings from all administrative logs. Administrative Events is a default filter created for viewing important events and can be a good place to start looking for a problem.



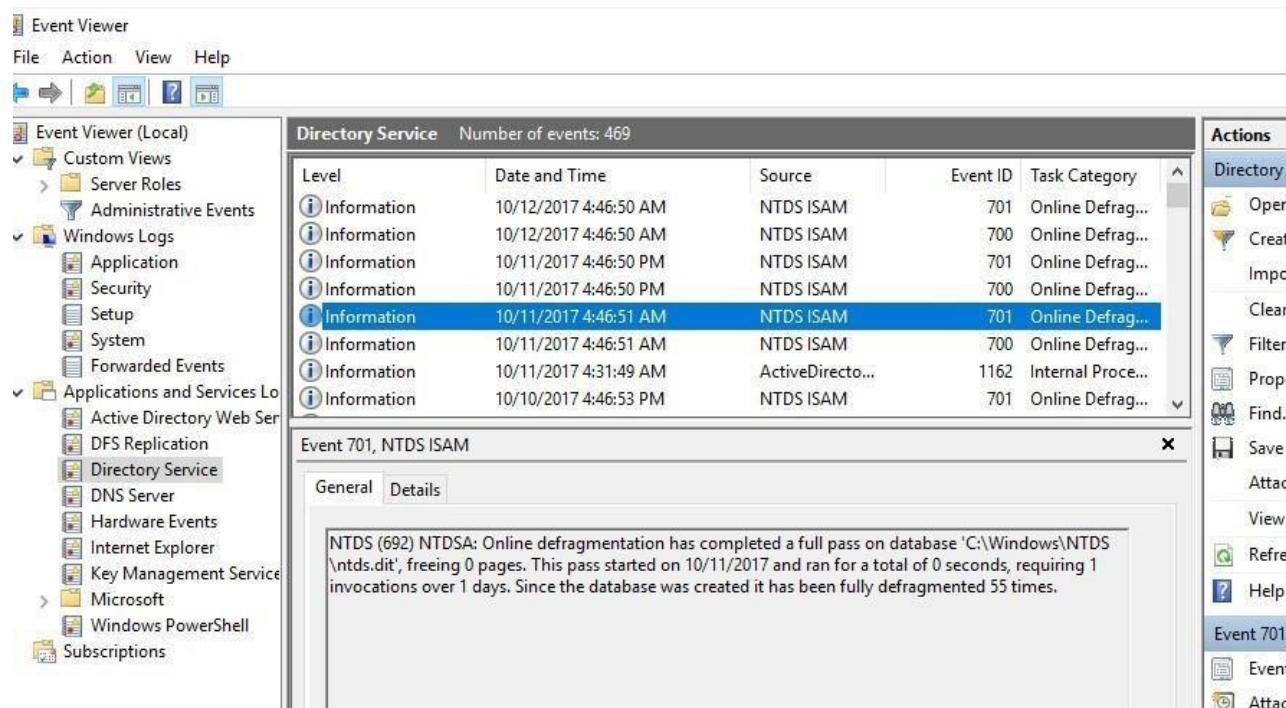
- Click **System** in the left pane to view the system log contents. In the middle pane, briefly scroll through the listed events.

Q21 - Are any errors or warnings reported?

If so, find out more about one or two of the errors or warnings by clicking them and viewing the details.

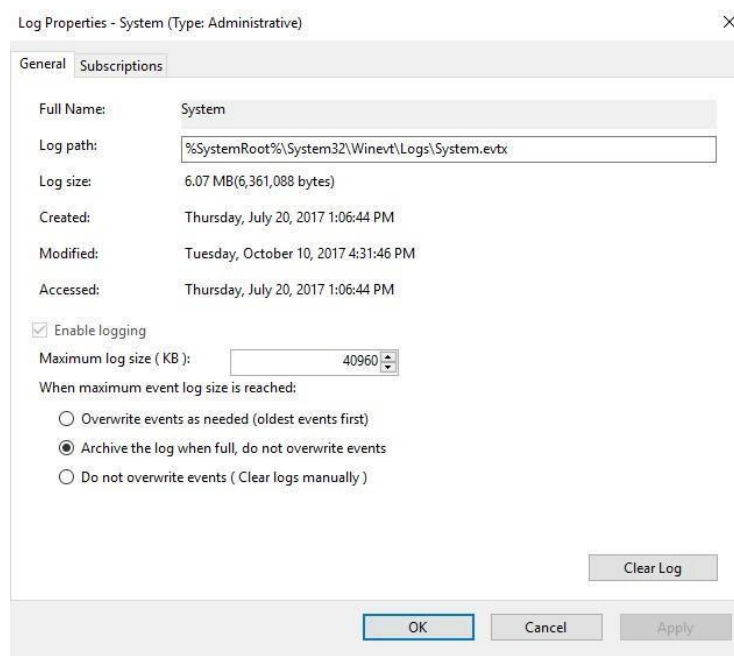


- Click the right-pointing arrow in front of **Applications and Services Logs** in the left pane. Click each log to view its contents in the middle pane and click on one or two events for each log.



9. Click the **View** menu at the top of the window and click **Show Analytic and Debug Logs**, if there is no check mark already in front of this selection.

10. Right-click **System** under Windows Logs in the tree and click **Properties**. In the **Log Properties—System (Type: Administrative)** dialog box, the default selection for managing the system log is to Overwrite events as needed (oldest events first). Click **Archive the log when full, do not overwrite events**. This option enables you to keep historic log information, but you will need to periodically delete archived logs you do not need. Notice the location of the system log as shown in the Log path box. This is useful information so that you know where to maintain the logs.

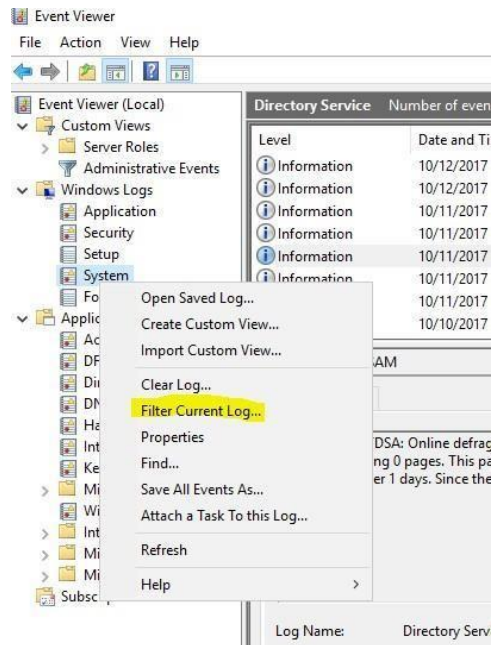


11. Change the **Maximum log size (KB)** to **40960**.

12. Click **OK** in the **Log Properties—System (Type: Administrative)** dialog box.

13. Click **System** under Windows Logs in the tree, if it is not already selected.

14. In the right pane, click **Filter Current Log**.



15. Click the down arrow for Event sources to view the options you can use for filtering. If you were to select one or more of these options, only events for these sources would be displayed in the system log (but the events for other sources would still be tracked and saved so you could change the filter to view them later). Click the pointer in a blank area of the dialog box to close the listing.

16. Click the down arrow for **Keywords** and notice the keywords you can use to build a filter (events containing the keywords you select would be displayed). Click the pointer in a blank area of the dialog box to close the listing of keywords.

17. Assume that you only want to view the error messages in the system log. Click the box for **Error**.

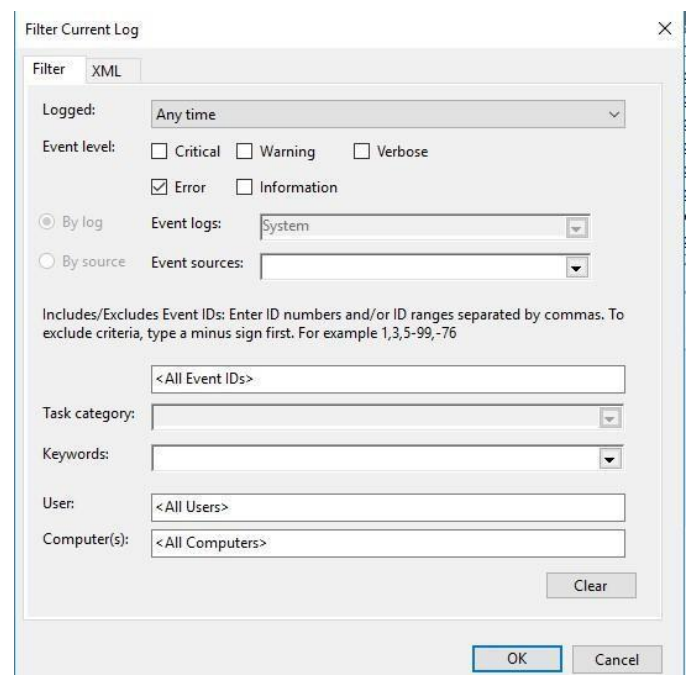
18. Click **OK** in the **Filter Current Log** dialog box.

Q22 - How does using the filter change what you view in the system log?

Q23 - Does this mean that the events you viewed before creating the filter are deleted, or simply not displayed?

19. Leave Event Viewer open for the next activity

Activity 8: In this activity, you use Event Viewer to backup the Security Log and clear



the Security Log.

1. Create a folder on your Windows 2019 VM to store more Lab documents. To do this, open **File Explorer**, select "Local Disk C:" in the left pane, click the "New Folder" icon at the top and name the folder "Labs".

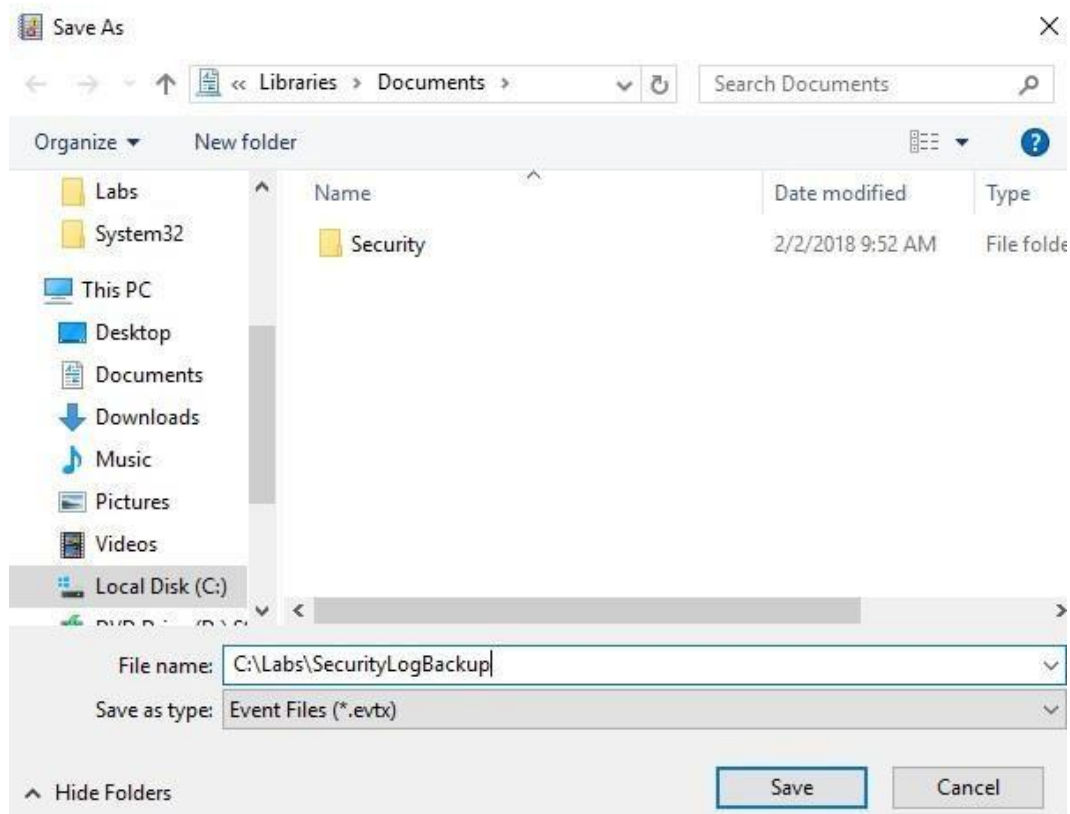
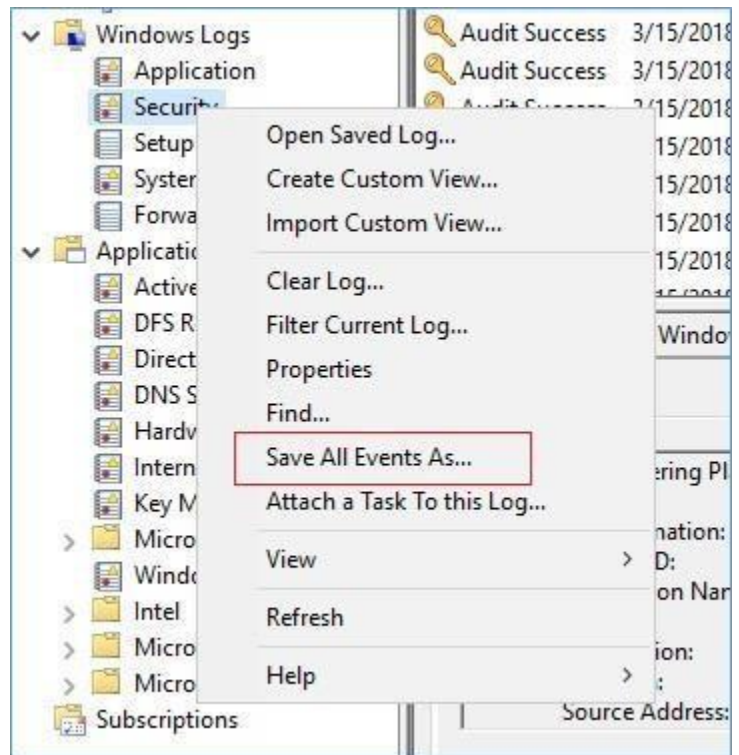
2. Open **Server Manager**, if it is not open.

3. Open the **Event Viewer** from the **Tools** menu.

4. Click on the Security Log to select it

5. Right click on the Security log and select Save All Events As...

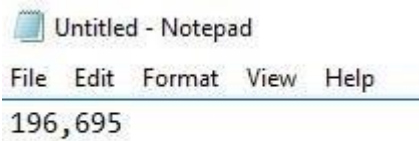
6. In the File name: box type in C:\Labs\SecurityLogBackup



7. Click Save to save the Security log

8. Click OK on the Display Information popup

9. Open Notepad and record the number of events in **your** Security Log.

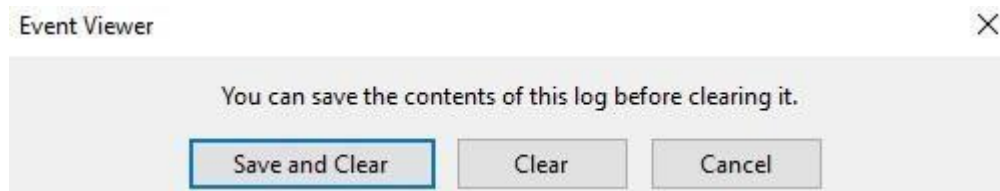


My security log has 196,695 events. Yours may have more or less.

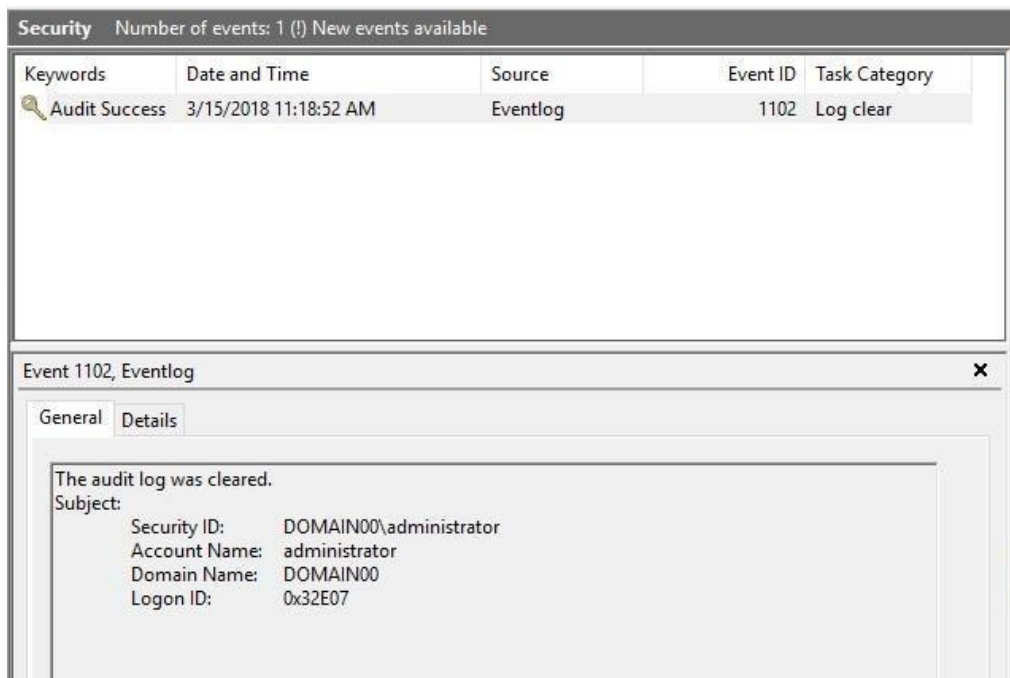
10. Save your text document as C:\Labs\SecLogNumber.txt and leave the document open

11. Right click the Security log and choose Clear Log...

12. On the popup click Clear (usually you would choose Save and Clear, but we have already saved the log).

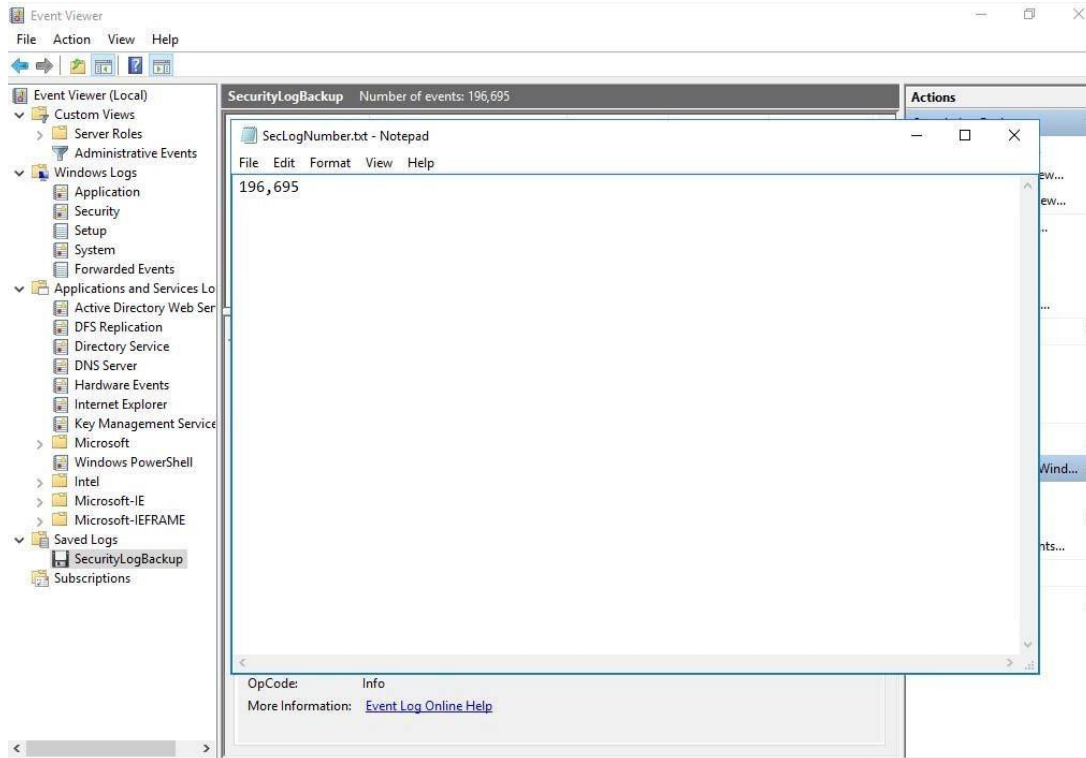


13. Notice that there is one event, even though we just cleared the Event Log.



Clearing the Event Log is an Event. So if a user does something questionable and clears any event log trying to cover their tracks, the event log will at least record that they cleared the log.

14. Right click on the Security log and choose Open Saved Log...
15. Navigate to the C:\Labs folder (if necessary) and click on the SecurityLogBackup.evtx file
16. Click Open
17. Click OK on the Open Saved Log popup
18. Compare the number of events in the SecurityLogBackup with the number you recorded in Notepad.



19. Save your Lab2_1_1a.txt file and close all open programs.

Rubric

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1 - 23: Correct answers to 23 questions. (4 points each)	
	Criteria #24: (PrtScr24.png) Chkdsk screenshot correct. (8 points)	