Lab 6: Server Administration Tools

The objective of the lab is to familiarize you with various tools used to administrate a Windows Server 2019 management environment. This lab will introduce you to the use of tools such as *Performance Monitor* and *Event Viewer*, two tools that network administrators use heavily in real-world practice.

This is a team assignment, but you must submit it as individuals, with all submitted work being your own.

Actions

Action 1: From your fellow classmates, form teams of no more than four members. Each team has been assigned a Windows Server 2019 instance.

Note: there are twelve (12) Windows Server 2019 instances available for this exercise: one for each four-member team.

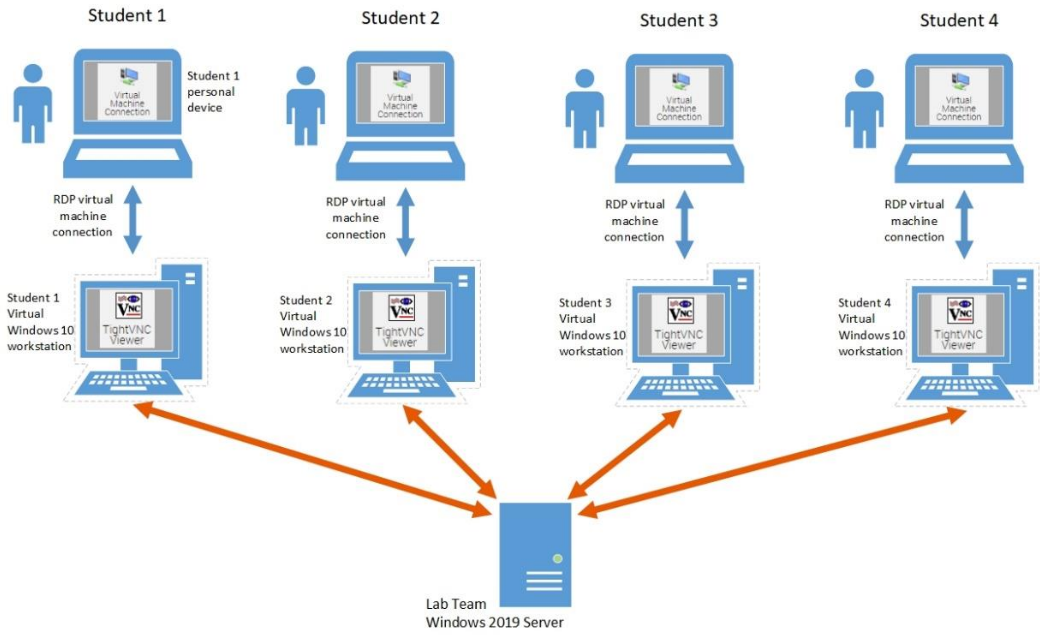
For Deliverable #1, write your name, the number of your team, the name of your partners, and the date.

Connect to the CCI Virtual Environment

Action 2: You will find instructions for connecting to the CCI virtual environment in Actions 1 – 3 of Lab 1: *Access Virtual Lab Environment*.

As advised in *Lab 1: Access Virtual Lab Environment*, you may want to uncheck various local sharing checkboxes, for security reasons.

Once you are connected to your own Windows 10 virtual instance, you will use the TightVNC client on that workstation to connect to your team's Windows 2019 server, as diagrammed below:


Student 1
Student 2
Student 3
Student 4
Virtual Machine Connection
Student 1 personal device
RDP virtual machine connection
Student 1 Virtual Windows 10 workstation
Student 2 Virtual Windows 10 workstation
Student 3 Virtual Windows 10 workstation
Student 4 Virtual Windows 10 workstation
VNC
TightVNC Viewer
Lab Team Windows 2019 Server

This will be exactly as you did during Lab 3, a few weeks ago.

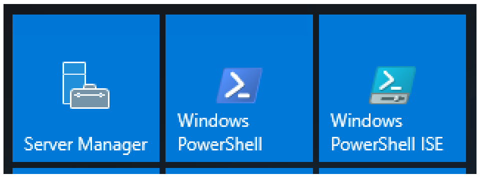
Connect to the CCI Virtual Environment (continued)

Action 3: Have one team member sign in to your team's Microsoft Windows 2019 Server instance using the *AdminLite* account. You were given the password in class.

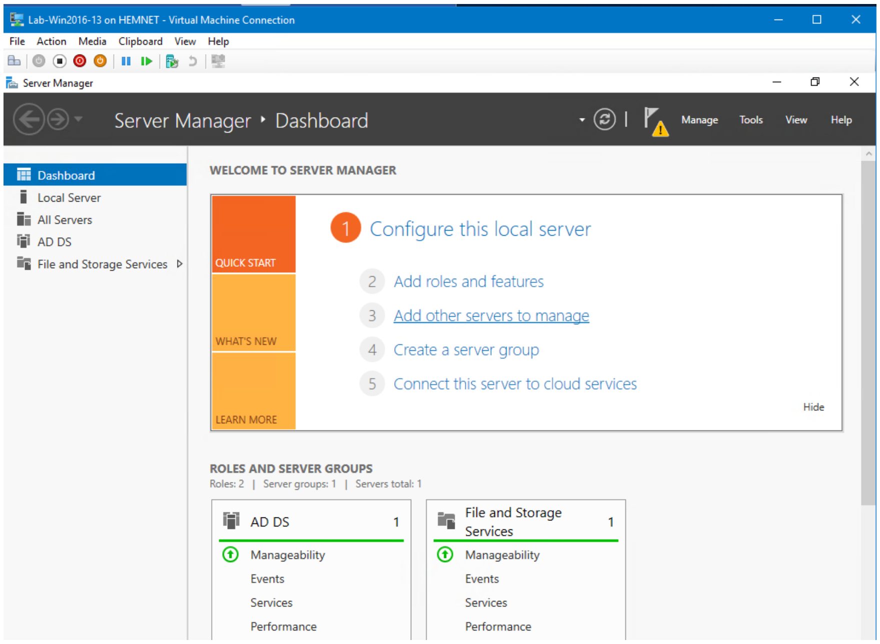
Since this is a Domain account, the full context of the username will be CCI-LAB-DOM\AdminLite

Examine the Windows Server 2019 Server Manager Dashboard

Action 4: From *Start Button*, start *Server Manager*:



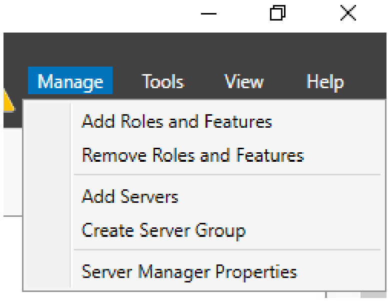
You will now see the *Server Manager Dashboard*, a collection of tools for the administrator:


Lab-Win2016-13 on HEMNET - Virtual Machine Connection
File Action Media Clipboard View Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1
AD DS 1
Manageability
Events
Services
Performance
File and Storage Services 1
Manageability
Events
Services
Performance

Explore the *Server Manager Dashboard*.

For Deliverable #4, what is your general impression of the state of your server? Do you see any errors or warnings? If so, what are they?

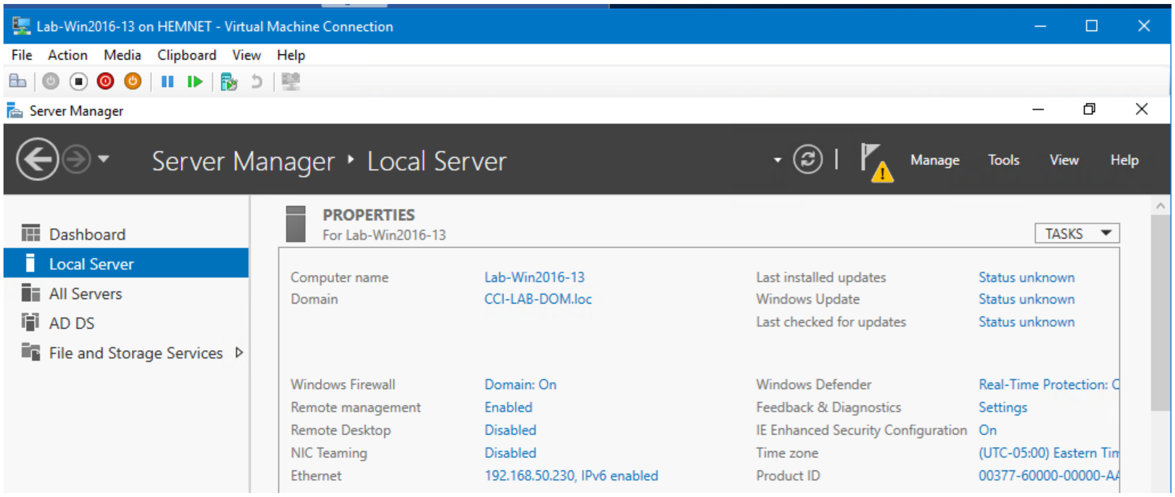
Click *Manage*, in the upper right corner of *Server Manager Dashboard*:



Note that you could add other servers to this dashboard, if desired.

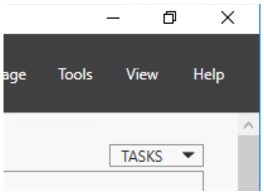
Examine the Windows Server 2019 Server Manager Dashboard (continued)

In the upper left corner of your Server Manager Dashboard, click *Local Server*.


Lab-Win2016-13 on HEMNET - Virtual Machine Connection
File Action Media Clipboard View Help
Server Manager
Server Manager ‣ Local Server
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
File and Storage Services
PROPERTIES
For Lab-Win2016-13
TASKS

Computer name	Lab-Win2016-13	Last installed updates	Status unknown
Domain	CCI-LAB-DOM.loc	Windows Update	Status unknown
		Last checked for updates	Status unknown
Windows Firewall	Domain: On	Windows Defender	Real-Time Protection: C
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-05:00) Eastern Tin
Ethernet	192.168.50.230, IPv6 enabled	Product ID	00377-60000-00000-AA

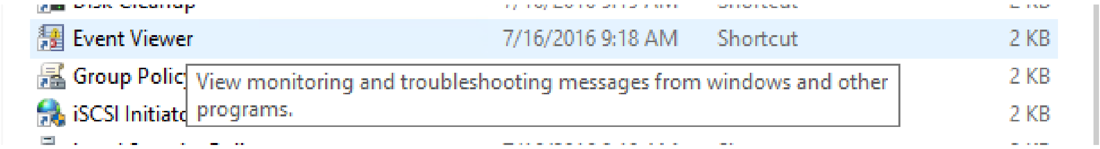
Explore around for a few minutes. Without changing anything, try the *Tasks* tabs on a few of the six general tools displayed:



For Deliverable #5, what are the six general tools visible in this tool? (Hint: *Properties* should be the first of six.) What set(s) of Tasks stood out in your mind?

Examine the Windows Server 2019 Event Viewer

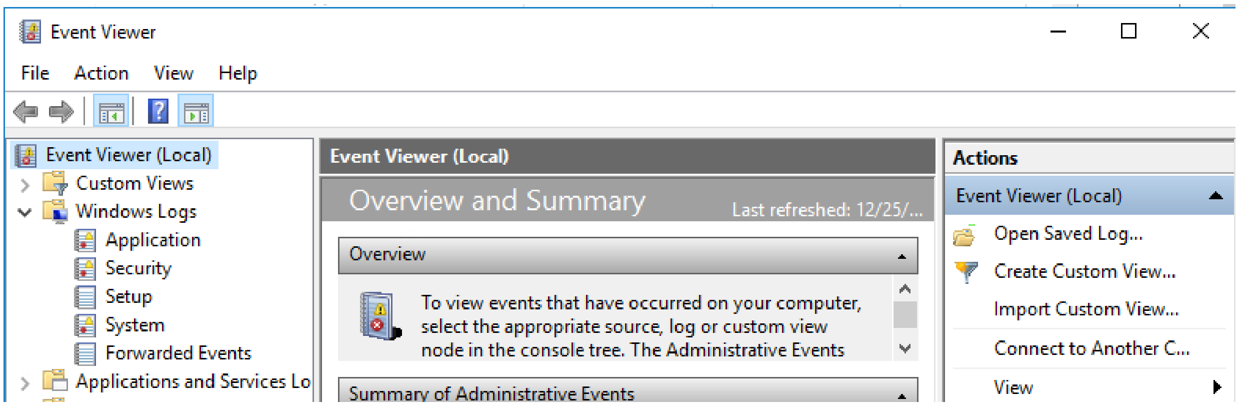
Action 5: From *Start* Button → *Windows Administrative Tools*, open the *Event Viewer*:



Event Viewer	7/16/2016 9:18 AM	Shortcut	2 KB
Group Polic			2 KB
iSCSI Initiat			2 KB

View monitoring and troubleshooting messages from windows and other programs.

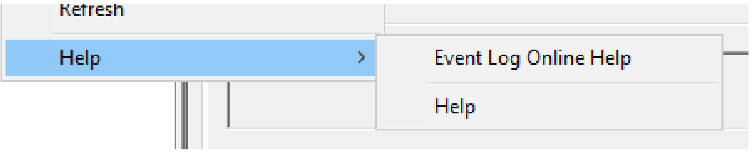
Expand *Windows Logs*:



To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events

Examine the Windows Server 2019 Event Viewer (continued)

Right-click any of the *Windows Logs*, such as *Application*, and select *Help Event Online Help*:



Answer any questions necessary to allow browsing of the Online Help feature. After taking a look around, close the help feature.

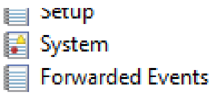
You may find the following article useful:

Event Logs: Microsoft TechNet

https://technet.microsoft.com/en-us/library/cc722404.aspx

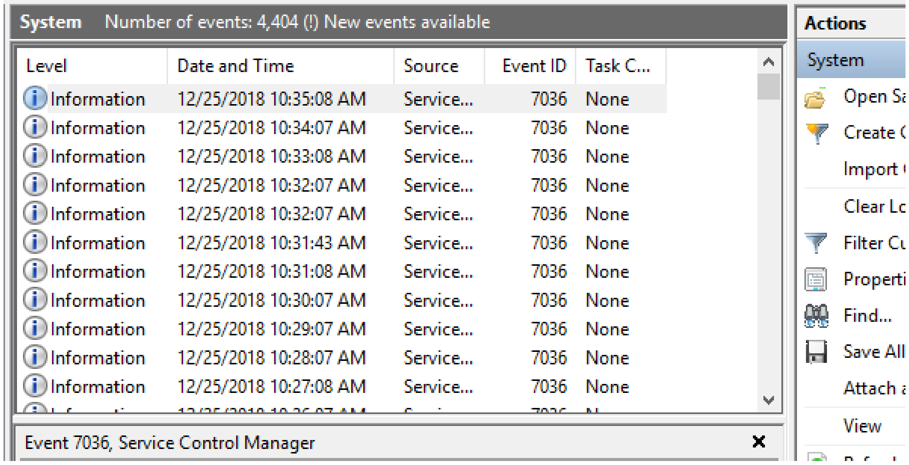
Use the *Event Viewer* to see when your server has been rebooted, and by whom:

Click on *System*:



In the center pane, you will likely see thousands of events. You could cycle through each of them and read the events individually – this has its uses in learning a great deal about how Windows servers function – and you will, for extra credit, but for now, you need answers quickly.

Microsoft TechNet is an invaluable source of information about Windows servers, but you need to have developed a conceptual framework and search vocabulary prior to using any database effectively.


System Number of events: 4,404 (!) New events available

Level	Date and Time	Source	Event ID	Task C...
Information	12/25/2018 10:35:08 AM	Service...	7036	None
Information	12/25/2018 10:34:07 AM	Service...	7036	None
Information	12/25/2018 10:33:08 AM	Service...	7036	None
Information	12/25/2018 10:32:07 AM	Service...	7036	None
Information	12/25/2018 10:32:07 AM	Service...	7036	None
Information	12/25/2018 10:31:43 AM	Service...	7036	None
Information	12/25/2018 10:31:08 AM	Service...	7036	None
Information	12/25/2018 10:30:07 AM	Service...	7036	None
Information	12/25/2018 10:29:07 AM	Service...	7036	None
Information	12/25/2018 10:28:07 AM	Service...	7036	None
Information	12/25/2018 10:27:08 AM	Service...	7036	None

Event 7036, Service Control Manager

Select one of the System events.

For <u>Deliverable #6</u>, what is the event's level, date and time, and Event ID? Looking in the pane below, in very brief summary, what is the nature of this particular Event ID? Briefly, what does that Event ID denote as having occurred?

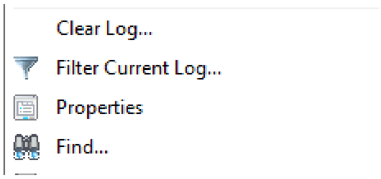
Select another event of a different Event ID.

Examine the Windows Server 2019 Event Viewer (continued)

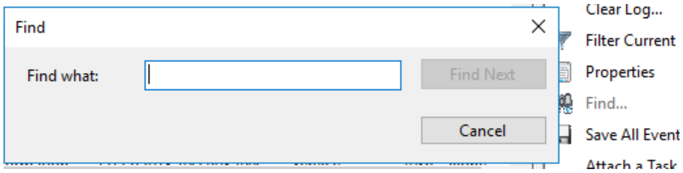
For Deliverable #7, what is the event's level, date and time, and Event ID? Looking in the pane below, in very brief summary, what is the nature of this particular Event ID? Briefly, what does that Event ID denote as having occurred?

One of the things that you should have noticed is that Event IDs signify different types of events. If you wanted to answer the central question of this exercise - *Use the Event Viewer to see when your server has been rebooted, and by whom* – you could manually cycle through thousands of log entries and copy them one by one, but this would take many hours, and subject the result to human oversight or distraction.

A search tool would be nice. In the right Actions pane, there are a number of search and analysis tools:



Try the Find tool:



Use whatever words you think might locate reboot events.

For Deliverable #8, what word(s) did you choose? How effective was this approach in answering the question of when the server was rebooted and by whom?

There are lists of Event IDs and what they mean. Microsoft TechNet has such lists, including this one for Microsoft Windows 2019 Server R2 and Windows 10. (Remember that server and workstation releases typically associate in pairs:

e.g.	Windows NT 4.0 Server	←→	Windows NT 4.0 Workstation (NT 4.0)
	Windows 2000 Server	←→	Windows 2000 Professional (NT 5.0)
	Windows Server 2003	←→	Windows XP Professional (NT 5.2)
	Windows Server 2008	←→	Windows Vista (NT 6.0)
	Windows Server 2008 R2	←→	Windows 7 (NT 6.1)
	Windows Server 2012	←→	Windows 8 (NT 6.2)
	Windows Server 2012 R2	←→	Windows 8.1 (NT 6.3)
	Windows Server 2016	←→	Windows 10 (NT 10.0)
	Windows Server 2019	←→	Windows 10 (NT 10.0)

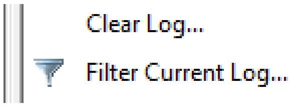
Here is one such list of Security Event IDs:
https://www.microsoft.com/en-us/download/details.aspx?id=50034

Event 1074 is one such event:
https://www.microsoft.com/technet/support/ee/transform.aspx?ProdName=Windows+Operating+System&ProdVer=5.2&EvtID=1074&EvtSrc=User32&LCID=1033

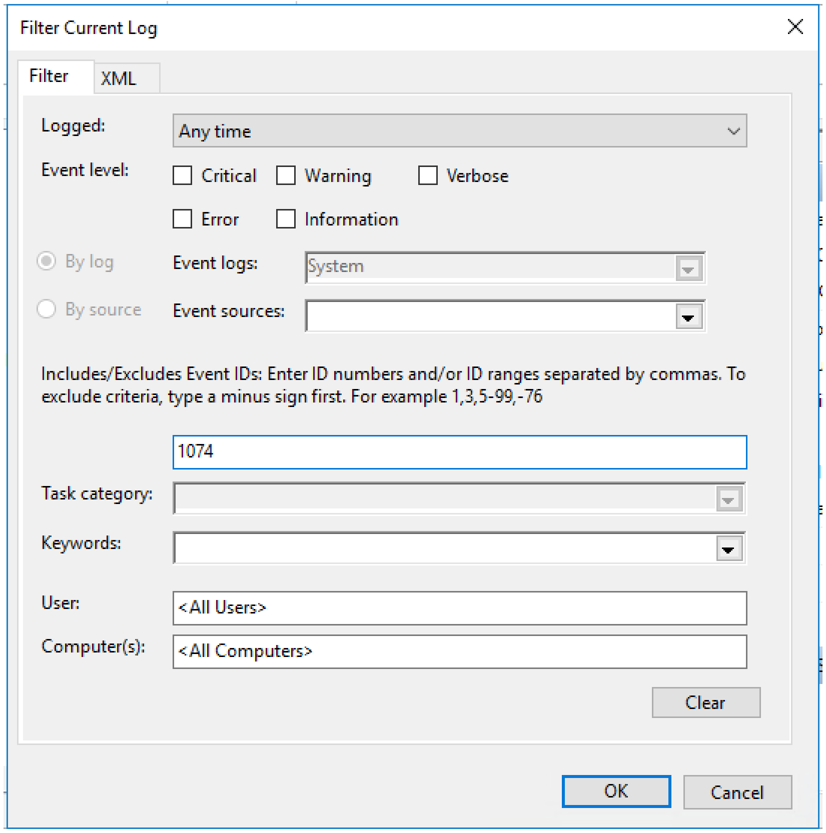
Be mindful that Event IDs tend to be rather specific, and are generated under very specific conditions that may or may not conform to the conditions you're looking for.

Examine the Windows Server 2019 Event Viewer (continued)

Select from the right *Actions* pane *Filter Current Log*



Enter 1074 into the box above the *Task Category* box, and click *OK*.


Filter Current Log

Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: System

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

1074

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

For Deliverable #9, how many times was your server rebooted? When and by whom?

For Extra Credit Deliverable #1, [5 points] do you think that Event ID 1074 represents *all* of the reboots of your team's Windows 2019 Server instance? Why or why not? What other types of reboots might you suspect?

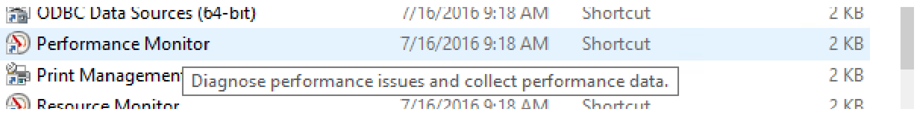
Check the Security logs.

For Deliverable #10, how many times has user *AdminLite* logged into your team server successfully? Unsuccessfully? What tool(s) did you use to answer these questions?

Close the *Computer Management* tool.

Examine the Windows Server 2019 Performance Monitor

Action 6: From *Start* button → *Windows Administrative Tools*, open the *Performance Monitor*:

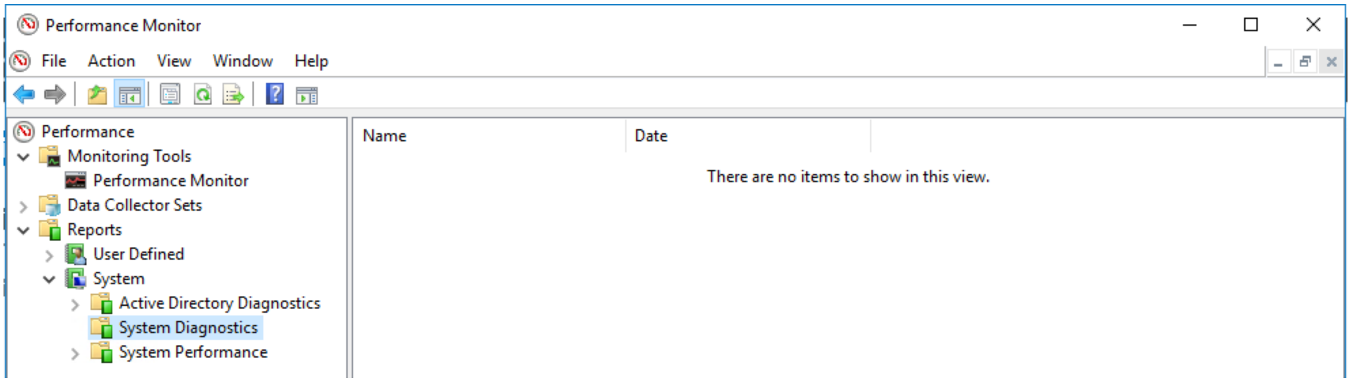


ODBC Data Sources (64-bit)	7/16/2016 9:18 AM	Shortcut	2 KB
Performance Monitor	7/16/2016 9:18 AM	Shortcut	2 KB
Print Managemen			2 KB
Resource Monitor	7/16/2016 9:18 AM	Shortcut	2 KB

Diagnose performance issues and collect performance data.

For Deliverable #11, from the *System Summary*, how many available Mbytes of memory does your team server presently have? What % Committed Bytes in use? Memory is one of the major server subsystems summarized here: what are the other three?

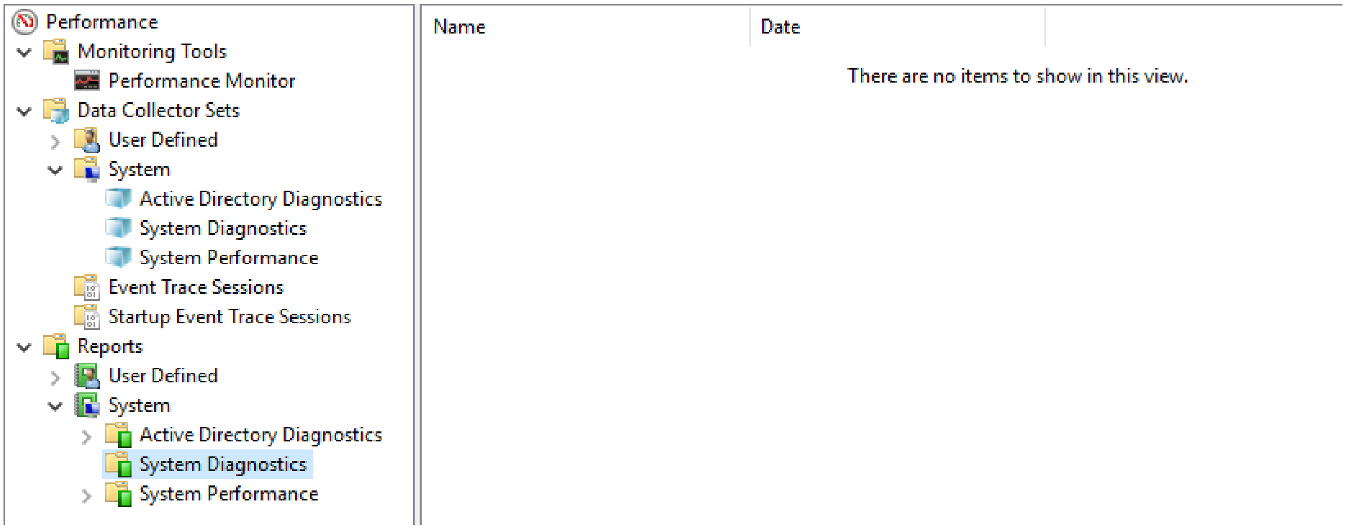
In the left pane, open *Reports* → *System* → *System Diagnostics*, and then click on any report you find there.



There are no items to show in this view.

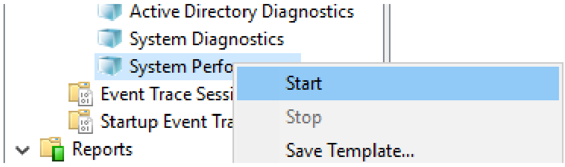
Note that you likely won't see any reports in the right pane, as none have probably yet been scheduled.

To schedule data collection for a report, expand *Data Collector Sets* → *System*, and right-click one of the reports. that appear:



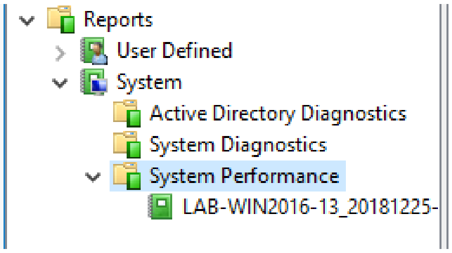
There are no items to show in this view.

Click Start on the desired data collection:

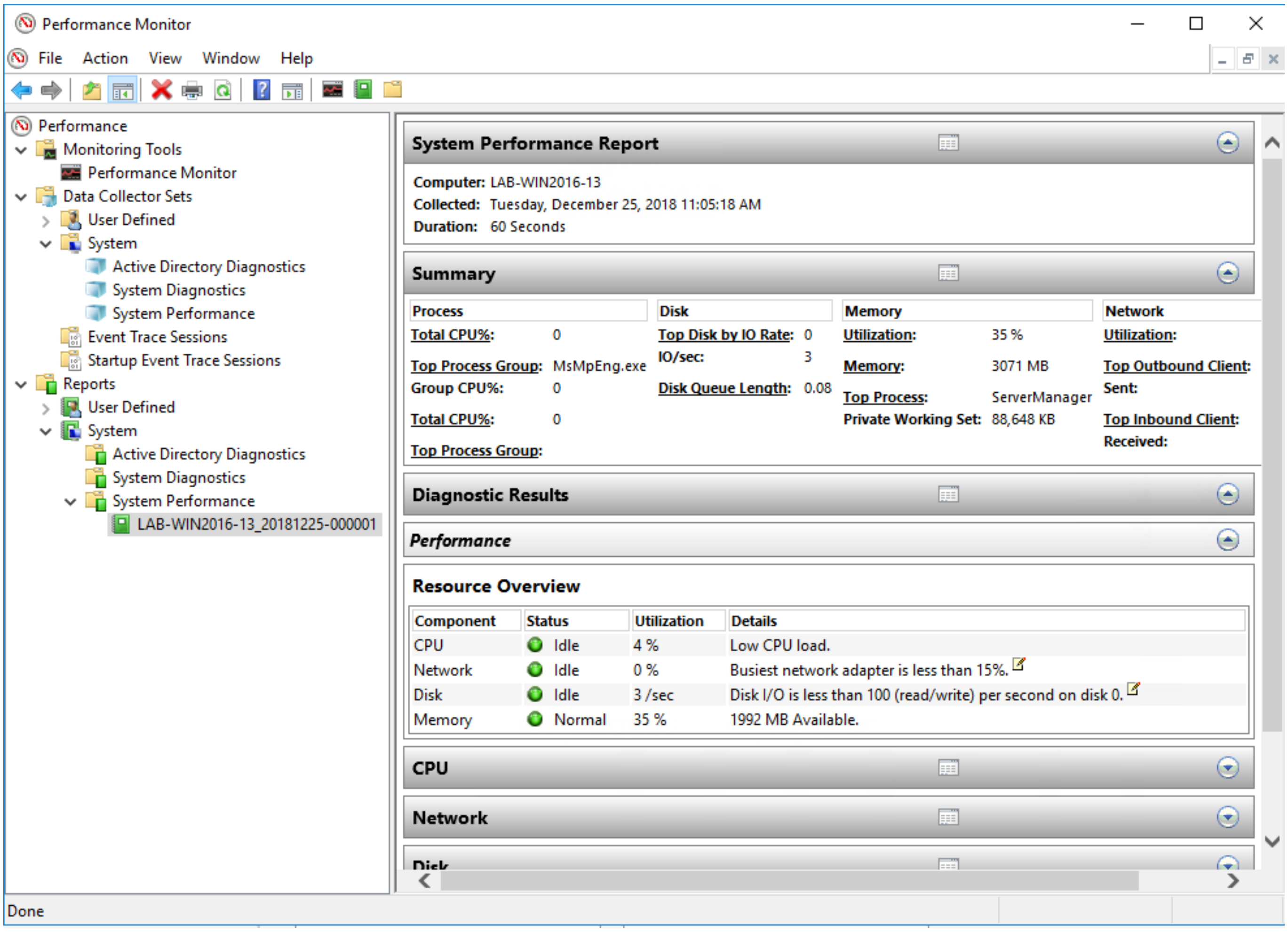


Examine the Windows Server 2019 Performance Monitor (continued)

After a few moments of data collection, a report will appear in the Reports area:



As you can see from the example above, a System Performance Report was run on 12/25/2018, for computer LAB-WIN2019-13.



System Performance Report

Computer: LAB-WIN2016-13
Collected: Tuesday, December 25, 2018 11:05:18 AM
Duration: 60 Seconds

Summary

Process		Disk		Memory		Network
Total CPU%:	0	Top Disk by IO Rate:	0	Utilization:	35 %	Utilization:
		IO/sec:	3			
Top Process Group:	MsMpEng.exe			Memory:	3071 MB	Top Outbound Client:
Group CPU%:	0	Disk Queue Length:	0.08			Sent:
				Top Process:	ServerManager	
Total CPU%:	0			Private Working Set:	88,648 KB	Top Inbound Client:
						Received:
Top Process Group:						

Diagnostic Results

Performance

Resource Overview

Component	Status	Utilization	Details
CPU	● Idle	4 %	Low CPU load.
Network	● Idle	0 %	Busiest network adapter is less than 15%.
Disk	● Idle	3 /sec	Disk I/O is less than 100 (read/write) per second on disk 0.
Memory	● Normal	35 %	1992 MB Available.

CPU

Network

Disk

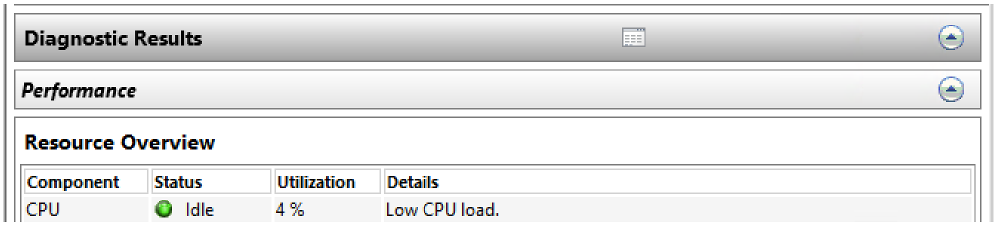
Clicking on the report, produces a view of the report, as you can see in the example above.

Now execute a System Performance report for your own team server, and evaluate the report.

For Deliverable #12, what are three problems with your server that stand out in your mind upon first glance at this report?

Examine the Windows Server 2019 Performance Monitor (continued)

Take a look at *Performance* → *Resource Overview*.



Diagnostic Results

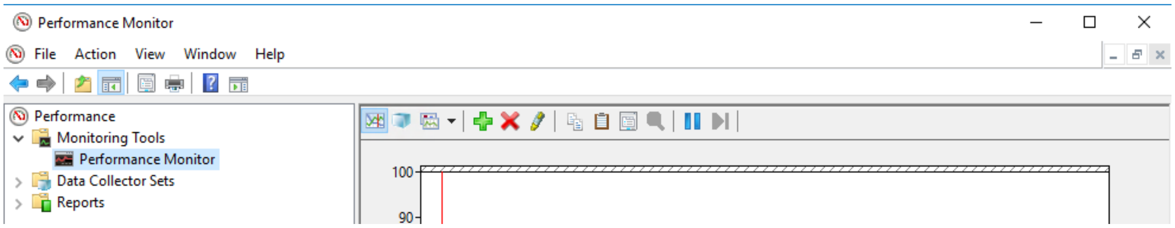
Performance

Resource Overview

Component	Status	Utilization	Details
CPU	● Idle	4 %	Low CPU load.

For Deliverable #13, what are the Status, Utilization, and Details for your CPU, Network, Disk, and Memory for your team server? In your opinion, are these aspects of your server acceptable?

In the left pane, open *Monitoring Tools* → *Performance Monitor*:



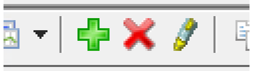
Using the Performance Monitor, you can monitor a vast variety of server processes. In Activity 5, you used the *Event Viewer* to search, view, and analyze discrete events, such as reboot times. This information is extremely useful to system administrators in getting to the bottom of what and who is doing what and when. Performance Monitor trends events over time, graphing them along a timewise X axis, and a Y axis of whatever it is being measured, e.g. Bytes per second or web HTTP hits per second.

Imagine, however, that you are attempting to corroborate a hypothesis that some of these reboots are caused by server crashes, and that some of these server crashes are caused by conditions such as memory issues, or high CPU utilization due to whatever happens to be tasking the CPU.

The default metric being graphed by *Performance Monitor* happens to be Processor → *% Processor Time*

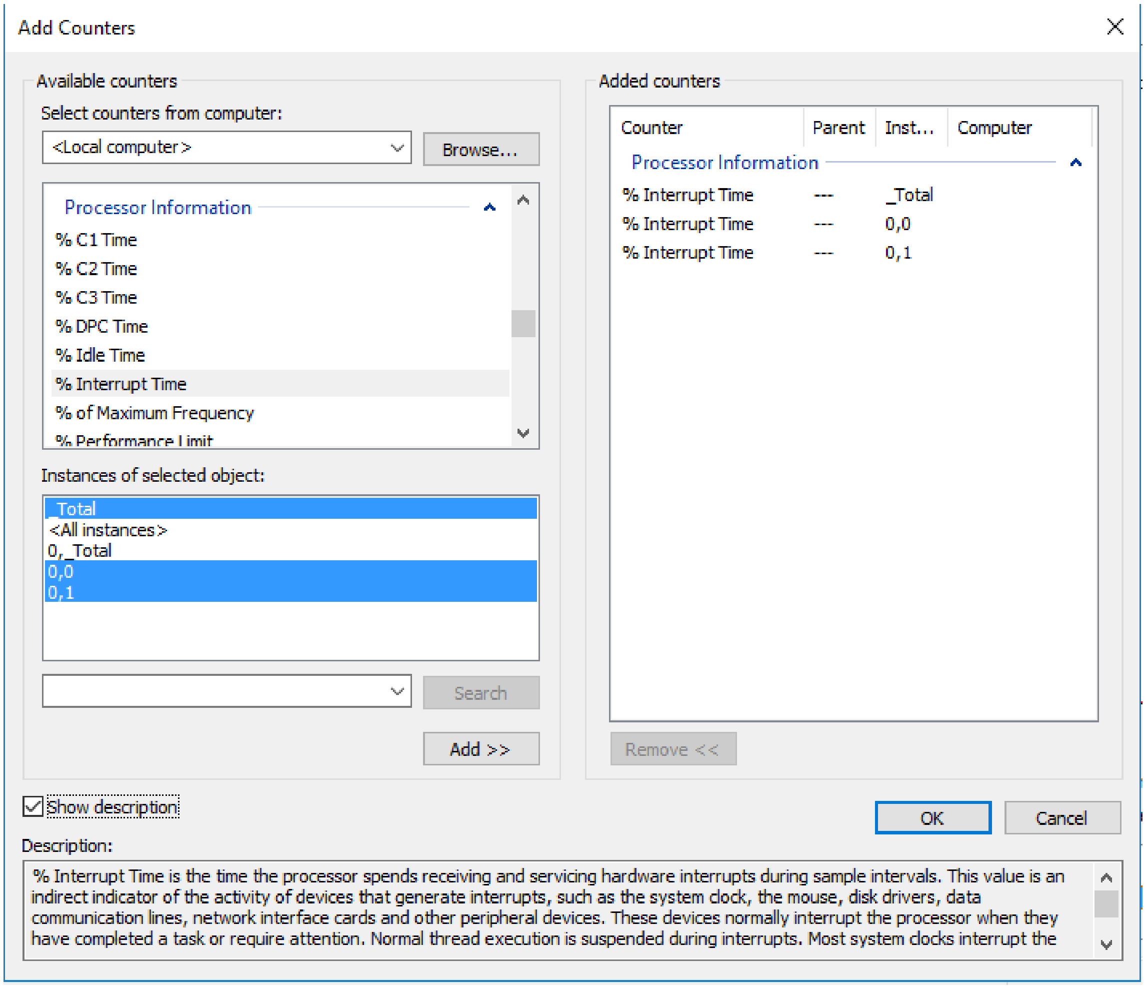
If you wanted, for example, to trend over time how much processor time is being devoted to addressing the network interface card, you could graph that as well. Go ahead and do so at this time:

Use the Add Counters button to add a counter:



Examine the Windows Server 2019 Performance Monitor (continued)

Under Per Processor Network Interface Card Activity → Interrupts/Sec Total, add a counter for % Processor Time:



Counter	Parent	Inst...	Computer
Processor Information			
% Interrupt Time	---	_Total	
% Interrupt Time	---	0,0	
% Interrupt Time	---	0,1	

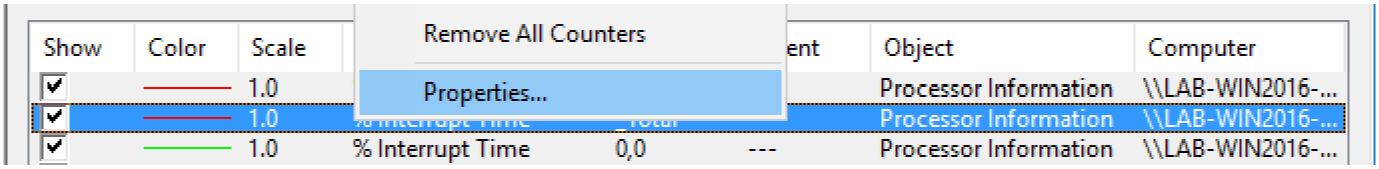
% Interrupt Time is the time the processor spends receiving and servicing hardware interrupts during sample intervals. This value is an indirect indicator of the activity of devices that generate interrupts, such as the system clock, the mouse, disk drivers, data communication lines, network interface cards and other peripheral devices. These devices normally interrupt the processor when they have completed a task or require attention. Normal thread execution is suspended during interrupts. Most system clocks interrupt the

You could check Show Description if you wanted to know exactly what you are monitoring.

Don't forget to select any and all processors allocated to your team server, e.g. 0,0 and 0,1.

Click *Add>>* to add the counter to your graph, and then *OK*.

If the graph line color is the same for both measured metrics, this could be difficult to differentiate. Right-click *Interrupts/Sec* → *Properties*, and then change the color to something else, like dark blue and then *Apply*:



Show	Color	Scale			ent	Object	Computer
☑	🟥	1.0				Processor Information	\\LAB-WIN2016-...
☑	🟥	1.0	% Interrupt Time	Total		Processor Information	\\LAB-WIN2016-...
☑	🟩	1.0	% Interrupt Time	0,0	---	Processor Information	\\LAB-WIN2016-...

For Deliverable #14, what is the peak Interrupts/Sec on your graph after two minutes? Is there any apparent correlation between Network Interface Card (NIC) interrupts per second and total processor utilization?

If you intend to complete the extra credit remainder of this lab, do not close the Performance Monitor that you just used to answer Deliverable #14.

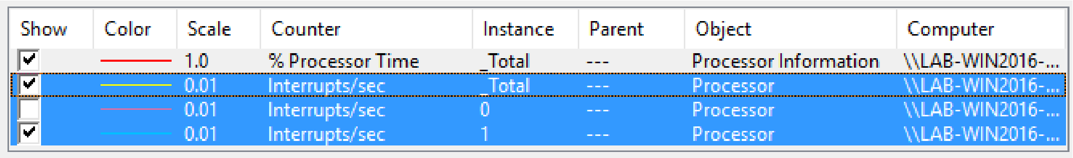
[Extra Credit] [5 points] Create a Data Collector Set [5 points] [Extra Credit]

You may find the following Microsoft TechNet article useful:

Creating Data Collector Sets
https://technet.microsoft.com/en-us/library/cc749337.aspx

Create a Data Collector Set

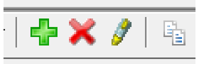
Action 7: Un-check all *Interrupts/Sec* item at the bottom of the running *Performance Monitor*:



Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	🟥	1.0	% Processor Time	_Total	---	Processor Information	\\LAB-WIN2016-...
☑	🟨	0.01	Interrupts/sec	_Total	---	Processor	\\LAB-WIN2016-...
☐	🟪	0.01	Interrupts/sec	0	---	Processor	\\LAB-WIN2016-...
☑	🟦	0.01	Interrupts/sec	1	---	Processor	\\LAB-WIN2016-...

You're going to delete this metric from the running *Performance Monitor*.

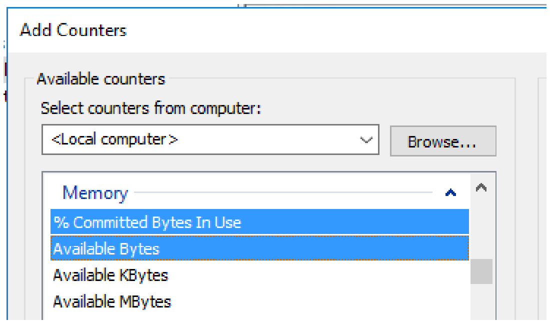
At the top of the running *Performance Monitor*, click the red X to delete this item:



Use the Add Counters button to add some new counters.

Under *Memory*, add the following counters:

% Committed Bytes
Available Mbytes
Pages/sec



Add Counters

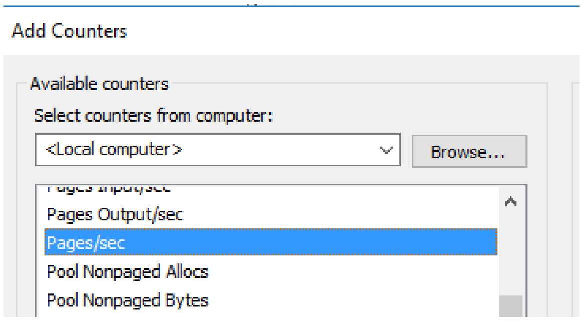
Available counters

Select counters from computer:

<Local computer> Browse...

Memory

% Committed Bytes In Use
Available Bytes
Available KBytes
Available MBytes



Add Counters

Available counters

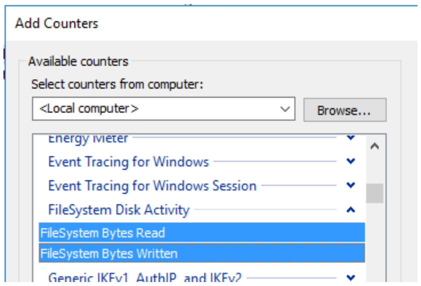
Select counters from computer:

<Local computer> Browse...

Pages Input/sec
Pages Output/sec
Pages/sec
Pool Nonpaged Allocs
Pool Nonpaged Bytes

Under *Filesystem Disk Activity*, add the following counters:

FileSystem Bytes Read
FileSystem Bytes Written



Add Counters

Available counters

Select counters from computer:

<Local computer> Browse...

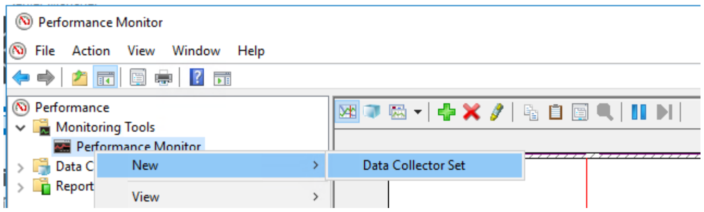
Energy Meter
Event Tracing for Windows
Event Tracing for Windows Session
FileSystem Disk Activity
FileSystem Bytes Read
FileSystem Bytes Written
Generic IKEv1, AuthIP, and IKEv2

Check the *Show Description* box if you wish to see what these counters measure.

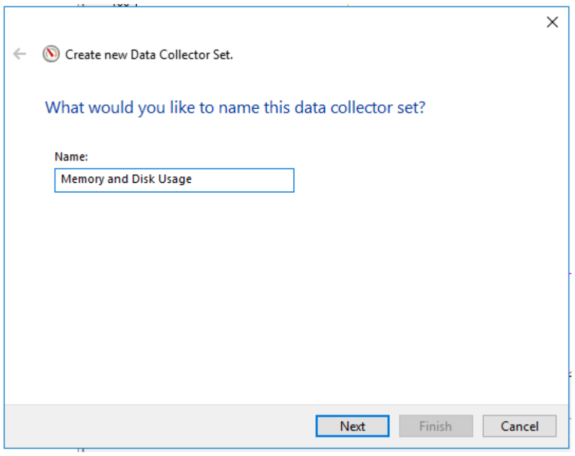
Click *OK* to close *Add Counters*.

[Extra Credit] [5 points] Create a Data Collector Set (continued)

In the left pane of *Performance Monitor*, right-click *Performance Monitor* and select *New* → *Data Collector Set*.



Create a new Data Collector set and name it "Memory and Disk Usage".

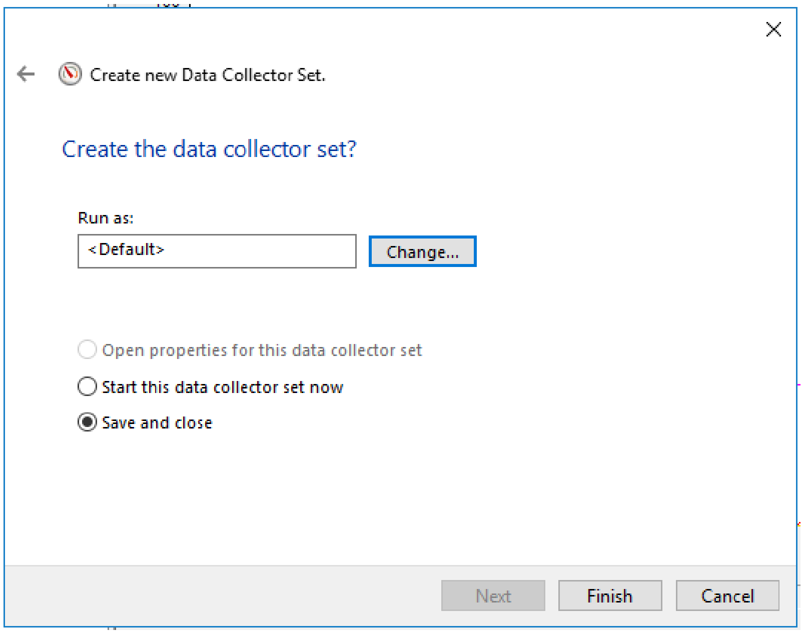


Create new Data Collector Set.

What would you like to name this data collector set?

Name: Memory and Disk Usage

Click Next until you get to *Create the data collector set?*



Create new Data Collector Set.

Create the data collector set?

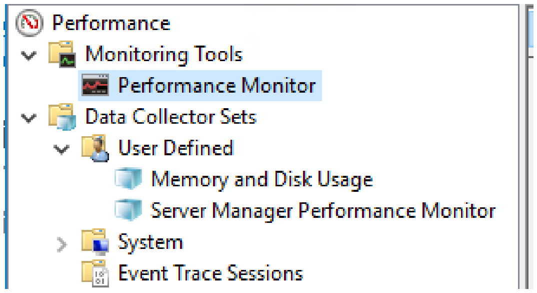
Run as: <Default>

○ Open properties for this data collector set
○ Start this data collector set now
● Save and close

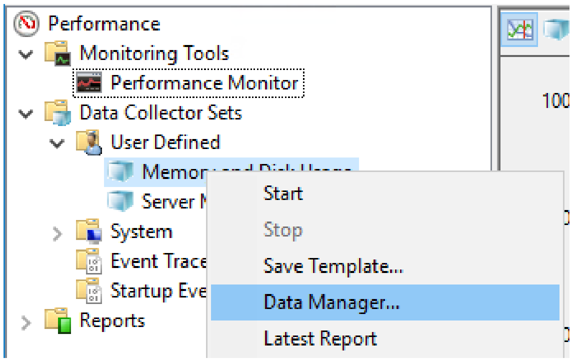
Select *Save and close* and click *Finish*.

[Extra Credit] [5 points] Create a Data Collector Set (continued)

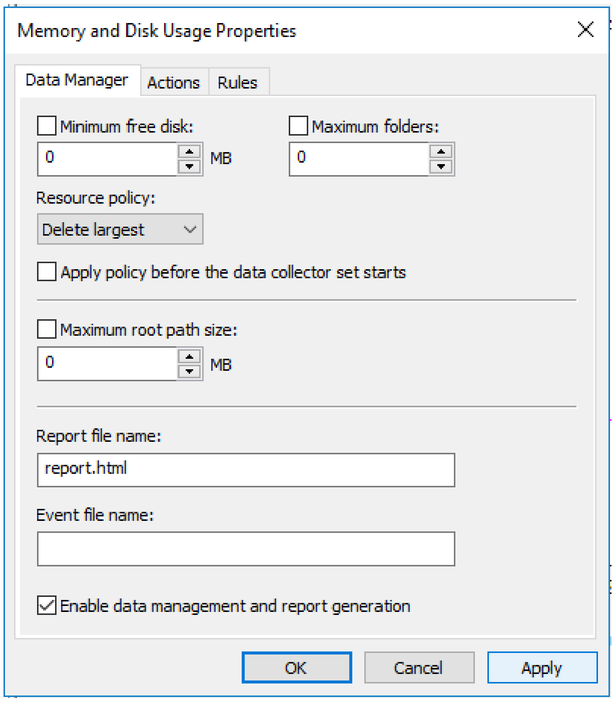
In the left pane, you will now see the User-Defined Data Collection Set that you created:



Right-click the Data Collector Set that you just created – *Memory and Disk Usage* – and select *Data Manager*:



Check the *Enable data management and report generation* box, and then click *Apply*:



☐ Minimum free disk: 0 MB

☐ Maximum folders: 0

Resource policy: Delete largest

☐ Apply policy before the data collector set starts

☐ Maximum root path size: 0 MB

Report file name: report.html

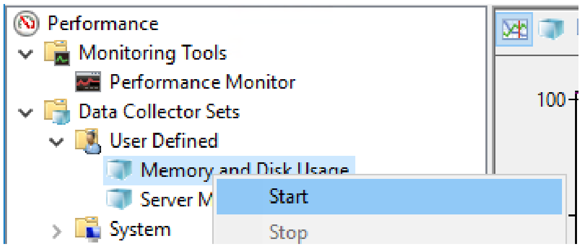
Event file name:

☑ Enable data management and report generation

Click *OK* to close.

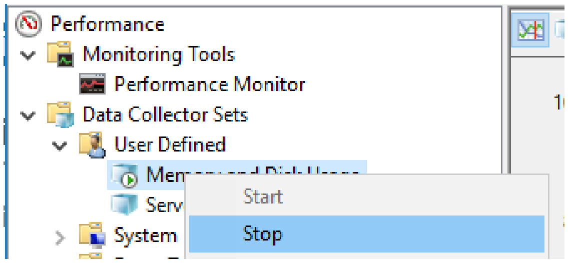
[Extra Credit] [5 points] Create a Data Collector Set (continued)

Right-click the *Memory and Disk Usage* User-Defined Data Collector Set and select *Start*:

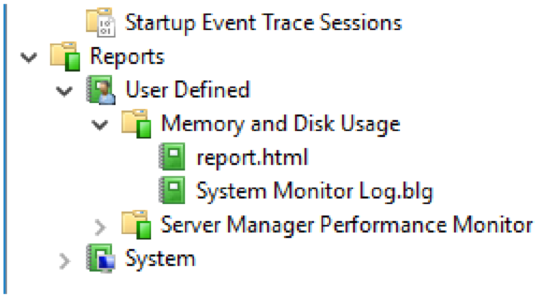


You are now collecting data for these metrics.

Let the data collection proceed for several minutes. When you have collected enough data and are ready to read reports based on that collected data, right-click the *Memory and Disk Usage* User-Defined Data Collector Set and select *Stop*:



In the left pane, expand Reports, if you haven't already. You should now see a report for the Data Collection Set that you created:



Click on the report for the Data Collector set that you created.

For <u>Extra Credit Deliverable #2</u>, answer the following:

What was the duration of the data collection sample you took?

What were the minimum, mean, and maximum Available Mbytes?

What were the minimum, mean, and maximum Available Committed Bytes?

What were the minimum, mean, and maximum Available Pages/Sec?

Which metrics were the spikiest, and which metrics were relatively flat?

Deliverables

Deliverable 1: From Action 1, write your name, the number of your team, the name of your partners, and the date.

Deliverable 2: From Action 2, what utility are you using to connect to your virtual instance for this lab? Is it Microsoft Remote Desktop, or is it something else?

Deliverable 3: From Action 3, what resources local to the machine from which you are attempting to create a remote connection (e.g. the lab iMac) would be accessible by the virtual instance by default?

Deliverable 4: From Action 4, what is your general impression of the state of your server? Do you see any errors or warnings? If so, what are they?

Deliverable 5: From Action 4, what are the six general tools visible in this tool? (Hint: *Properties* should be the first of six.) What set(s) of Tasks stood out in your mind?

Deliverable 6: From Action 5, what is the event's level, date and time, and Event ID? Looking in the pane below, in very brief summary, what is the nature of this particular Event ID? Briefly, what does that Event ID denote as having occurred?

Deliverable 7: From Action 5, what is the event's level, date and time, and Event ID? Looking in the pane below, in very brief summary, what is the nature of this particular Event ID? Briefly, what does that Event ID denote as having occurred?

Deliverable 8: From Action 5, what word(s) did you choose? How effective was this approach in answering the question of when the server was rebooted and by whom?

Deliverable 9: From Action 5, how many times was your server rebooted? When and by whom?

Deliverable 10: From Action 5, how many times has user *AdminLite* logged into your team server successfully? Unsuccessfully? What tool(s) did you use to answer these questions?

Deliverable 11: From Action 6, from the System Summary, how many available Mbytes of memory does your team server presently have? What % Committed Bytes in use? Memory is one of the major server subsystems summarized here: what are the other three?

Deliverable 12: From Action 6, what are three problems with your server that stand out in your mind upon first glance at this report?

Deliverable 13: From Action 6, what are the Status, Utilization, and Details for your CPU, Network, Disk, and Memory? In your opinion, are these aspects of your server acceptable?

Deliverable 14: From Action 6, what is the peak Interrupts/Sec on your graph after two minutes? Is there any apparent correlation between Network Interface Card (NIC) interrupts per second and total processor utilization?

Extra Credit Deliverables [5 points each]

Extra Credit Deliverable 1: From Action 5, do you think that Event ID 1074 represents all of the reboots of your team's Windows 2019 Server instance? Why or why not? What other types of reboots might you suspect?

Extra Credit Deliverable 2: From Action 7, answer the following:

What was the duration of the data collection sample you took?

What were the minimum, mean, and maximum Available Mbytes?

What were the minimum, mean, and maximum Available Committed Bytes?

What were the minimum, mean, and maximum Available Pages/Sec?

Which metrics were the spikiest, and which metrics were relatively flat?