Answers: 6.1.3.7 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.

PC status: Protected Hone Update Hstory Settings Virus and spyware definitions: Up to date Your virus and spyware definitions: Up to date Your virus and spyware definitions are automatically updated to help protect your PC. Definitions created on: 9/2/2015 at 5:47 AM Definitions trau updated: 9/1/2015 at 3:14 PM Virus definition version: 1.205:1374.0 Recomputer Management Computer Management System Tools Services Vindows Defender Service Vindows Defender Service Services Windows Connect Now -C. Windows Connect Now -C. Windows Defender Service Windows Connect Now -C. Windows Connect Now -C. Windows Defender Service Windows Connect Now -C. Windows Defender Service Windows Defender Service Windows Connect Now -C. Windows Defender Service Windows Services Windows Services Windows Services Windows Services Windows Services Windows Service Windows Services Windows Services Windows Service Windows Services Windows Service Window	1.5.5		Windows Defender				_ 🗆 ×
Hone Update History Settings Image: Computer Management Update Virus and spyware definitions: Up to date Vour virus and spyware definitions are automatically updated to help protect your PC. Definitions created on: 9/2/2015 at 3:14 PM Urus definition version: 1.205.1374.0 Rectangular Smp Update Spyware definition version: 1.205.1374.0 Rectangular Smp Virus definition version: 1.205.1374.0 Spyware definition version: 1.205.1374.0 Rectangular Smp Virus definition version: 1.205.1374.0 Spyware definition version: 1.205.1374.0 Rectangular Smp Virus definition version: 1.205.1374.0 Spyware definition version: 1.205.1374.0 Rectangular Smp Virus definition version: 1.205.1374.0 Spyware definition version: 1.205.1374.0 Rectangular Smp Virus version: Virus version: Spyware definition version: 1.205.1374.0 Rectangular Smp Virus version: Virus version: Spyware definitions are automatically version: Services Name Description: Virus version: Spyware definition: Service user from malware in thelps protect user from malware in dother potentially unwanted in t	PC status: Protected						
Virus and spyware definitions: Up to date Your virus and spyware definitions are automatically updated to help protect your PC. Definitions created on: 9/2/2015 at 5:47 AM Update: Update Virus definition version: 1:205:1374.0 Spyware definition version: 1:205:1374.0 Protect Management (Local Deriver Management (Local Deriver and Groups) Status Startup Ty* More Actions Windows Defender Service Device Manager Status Startup Ty* More Actions Windows Defender Service Windows Connection Non Windows Defender Service Windows Strent Collector Services and Applications Services and Applications Service and Applications Windows Event Collector	Home Update	History Settings					💡 Help 🔻
Vour virus and spyware definitions are automatically updated to help protect your PC. Definitions created on: 9/2/2015 at 5:47 AM Definitions last updated: 9/1/2015 at 3:14 PM Virus definition version: 1.205.1374.0 Spyware definition version: 1.205.1374.0 Rectingular Snp Tile Action View Help Computer Management (Local System Tools System Tools System Tools System Tools System Tools Device Management Device Management Services and Applications Services and App	Virus and spyware d	lefinitions: Up to date					
Definitions created on: 9/2/2015 at 5:47 AM Definitions last updated: 9/1/2015 at 3:14 PM Vinus definition version: 1.205.1374.0 Spyware definition version: 1.205.1374.0 Rectangular Sup Computer Management Image: Computer Management (Local) Services System Tools Services Services Windows Color System The WcSPLu Windows Color System The WcSPLu Manual Windows Defender Service Helps protect: users from malware and other potentially unwanted Windows Defender Service Manual Staragement Services and Applications Windows Encryption Provid Manual (T Windows Encryption Provid Windows Encryption Provid Manual (T Windows Encryption Provid Windows Encryp	Your virus and spywa	are definitions are automatically update	d to help protect your PC.				
Name Description System Tools Services System Tools Services Windows Defender Service Manual Windows Defender Service Manual System Tools Services System Tools Services System Tools Services Windows Defender Service Manual Windows Color System The WcsPlu Manual Manual Windows Connection Man.etc. Manual Windows Connection Man.etc. Manual Windows Defender Networ Helps guard Bervice Management Windows Encryption Provid Services Manual (T Windows Encryption Provid	Definitions create Definitions last u Virus definition v Spyware definitio	Id on: 9/2/2015 at 5:47 AM pdated: 9/1/2015 at 3:14 PM ersion: 1.205.1374.0 in version: 1.205.1374.0					Update
File Action View Help Image: Service of the potential service of the service of t	A.		Computer Management				- • ×
Image: Service of the potentially unwarted of the potential the potentis the potential the potential the potential the potent	File Action View Help						
Computer Management (Local System Tools System Tools Stak Scheduler Exercises Stak Scheduler Stak Scheduler Stak Scheduler Starde Folders Description: Helps protect users from malware Software Device Manager Storage Storage Storage Storage Windows Collector Mindows Conection Man Mindows Conection Man Mindows Conection Man Mindows Connection Man Mindows Connection Man Mindows Connection Man Windows Connection Man Mindows Connection Man	🗢 🄿 🗖 🖬 🗐 🧟 😖	🛛 🖬 🕨 🖬 🕪					
 System Tools Syste	🛃 Computer Management (Local	Services					Actions
 Event Viewer Event Viewer Shared Folders Shared Folders	▲	Windows Defender Service	Name	Description	Status	Startup Ty ^	Services
Lextended Standard / Standard	 Event Viewer Shared Folders Shared Folders Coal Users and Groups Perice Manager Storage Disk Management Services and Applications Services WMI Control 	Description: Helps protect users from malware and other potentially unwanted software	Windows Color System Windows Connection Mana Windows Connection Mana Windows Defender Networ Windows Defender Service Windows Driver Foundation Windows Encyption Provid Windows Encyption Provid Windows Exert Collector Windows Event Collector Windows Event Log <	The WcsPlu WCNCSVC Makes auto Helps guard Helps prote Creates and Windows E Allows error This service	Running Running Running	Manual Manual Automatic Manual Automatic Manual (T Manual Automatic V S	More Actions Windows Defender Se • More Actions

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

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

What is the status of the service?

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**.

	Windows Defender	- 🗆 🗙
PC status: Protected		
Home Update History	7 Settings	🕜 Help ▼
Real-time protection Excluded files and locations Excluded file types Excluded processes Advanced MAPS Administrator	Turn on this app When this check box is selected, this app will alert all users if spyware or other poter unwanted software attempts to run or install itself on this PC.	ıtially
	Save changes Canc	el

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

	Windows Defender	
PC status: At risk Home Update His	tory Serrings	🕜 Help 🔹
Real-time protection Excluded files and locations Excluded file types Excluded processes	Upon this app When this check too is selected, this app will alert all users if spyware or other potentially unwanted software attemp itself on this PC.	ts to run or install
MAPS	Windows Defender	
Admunistrator	This app has been turned off and isn't monitoring your computer. If you're une another top is deals for malicous or unwanted software, we action Center to deal. Not app's status. Core	
	🖞 Sava shanges	Cancel
Storage	Windows Color System The WiciPlu Manual Windows Cennet New - C WCNCSVC Manual Windows Cenneticien Mana, Make auto Running Automatic	
Services and Applications	Windows Defender Network Helps quart Menual	
Services and Applications Services WMI Control	Windows Defender Networ Helps guard Manual Windows Defender Service Helps prote Running Automatic C	

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**.

	Windows Defender ×
1	This app has been turned off and isn't monitoring your computer.
	If you're using another app to check for malicious or unwanted software, use Action Center to check that app's status.
	Close

What must be done so Windows Defender can run?

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.

÷.		Co	mputer Managem	vent		- 5	×
File Action View Help				2000			
💠 🔿 🙍 🧰 🖬 📷 🔛							
Computer Management (Local	Level	Date and Time	Source	Event ID	Task Categor ^	Actions	_
(A) Task Scheduler	() Information	9/2/2015 5:29:06 PM	Service Control Mar	nager 7040	None	System	10
. Event Viewer	Information	9/2/2015 5:29:06 PM	FilterManager	6	None	(5 Open Saved Log	
> 😽 Custom Views	Eleformation	9/2/2015 5/29/06 PM	Service Control Mar	nager 7040	None	Y Create Custom View	
# 🙀 Windows Logs	Information	9/2/2015 5:29:06 PM	Service Control Mar	nager 7040	None	Innerst Custom View	
Application	Information	9/2/2015 5:27:04 PM	UserModePowerSer	rvice 12	(10)	ingon coston rien	
Security	Information	9/2/2015 5:24:42 PM	UsetModePowerSer	rvice 12	(10)	Clear Log	
Setup	Information	9/2/2015 5:23:09 PM	Service Control Mar	nager 7040	None	Filter Current Log	
System	Information	9/2/2015 5:23:09 PM	FilterManager		None	Properties	
Forwarded Event	(1) Information	9/2/2015 5:23:09 PM	Service Control Mar	nager 7040	None	20	
Applications and Se	Information	9/2/2015 5:23:04 PM	Service Control Mar	nager 7040	None	Find.	
Subscriptions	Information	9/2/2015 5:2249 PM	Service Control Mar	nager 7040	None	Save All Events As	
> x) Shared Folders	Information	9/2/2015 5:22:49 PM	FilterManager	6	None	Attach a Task To this L.	1
Eccal Users and Groups	(1) Information	9/2/2015 5:22:49 PM	Service Control Mar	nager 7040	None	Man	
> (Performance	Information	9/2/2015 5:22:49 PM	Service Control Mar	nager 7040	None	A 16M	
Device Manager	() Information	9/2/2015 5:22:46 PM	Service Control Mar	nager 7040	None	G Refresh	
a mil Storage	(1) Information	9/2/2015 5:22-46 PM	FilterManager	1	None	Help	
A Services and Applications	(1) Information	9/2/2015 5:22-46 PM	Service Control Mar	nager 7040	None v		
C Services	< C				>	Event 7040, Service C_	*
WMI Control	Event 7040, Service	Control Manager			×	Event Properties	
	General Details					Attach Task To This Ev.	,
	The start type o	f the Windows Defender Mir	i-Filter Driver service	was changed from demand sta	t to	Save Selected Events	
	boot start.					C Refresh	
	Lon Name:	Sustem				Help	
		Farries Cashed Manager	i vinna i i	INVESTIGATE CONTRACTOR			
	Source	service control manager	coggeo	3142 2013 342500 PM			
	Event ID:	7040	rask Category:	roone	199		
	Level	Information	Keywords	Classic			
	User	SYSTEM	Computer:	vietual			

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

		Co	mputer Manager	nent		- Ø ×
File Action View Help						
Computer Management (Local) System Tools) Task Scheduler) Stark Venerer) Custem Views) Windows Logs) Application Security	Level	Date and Time 0/2/2015 5/29/06 PM 9/2/2015 5/29/06 PM 9/2/2015 5/29/06 PM 9/2/2015 5/27/04 PM 9/2/2015 5/27/04 PM	Source Service Control M FilterManager Service Control M Service Control M UserModePowerS UserModePowerS	Event ID anager 7040 anager 7040 ervice 12 anice 12	Task Categor * None None (10) (10) (10)	Actions System Open Saved Log., Create Custom View., Import Custom View., Open Log.,
Setup System Provasted Even Applications and Se Subscriptions	Information	9/2/2015 5/23:09 PM 9/2/2015 5/23:09 PM 9/2/2015 5/23:09 PM 9/2/2015 5/23:04 PM 9/2/2015 5/23:04 PM 9/2/2015 5/22:04 PM 9/2/2015 5/22:04 PM 9/2/2015 5/22:04 PM 9/2/2015 5/22:04 PM	Service Control M FilterManager Service Control M Service Control M Service Control M FilterManager Service Control M Service Control M Service Control M FilterManager	anager 7040 anager 7040 anager 7040 anager 7040 anager 7040 anager 7040 anager 7040	None None None None None None None None	Filter Current Log Proporties Find Save All Events As Attach a Task To this L View G Refresh Help
Cox Management Services G. Services MM Control	Information C Information C Information C Information C Information I	9/2/2015 5:22-46 PM Centrol Manager If the Windows Defender Boo System Service Centrol Manager 2040 Information SYSTEM	Service Control M R Driver service was Logged Task Category Keywords Computer	changer 7040 changed from demand start to I 9/2/2013 5/28/06 PM None Classic visitual	boot	Event 7040, Service C. Event Properties Advantage of the service of

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

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.

Windows Defender	- D ×
PC status: Protected Home Update History Settings	😗 Help 🕶
Your PC is being monitored and protected. Image: Seal-time protection: On Image: Virus and spyware definitions: Up to date	Scan options: Quick Full Custom Scan now
Scan details Last scan: 9/1/2015 at 3:15 PM (Quick scan)	

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.

File Action View Help	
E Computer Management (Local Services Actions	
A 1 System Tools Base Filtering Engine Name Description Status Startup Type Services	•
Generation G	tions 🕨
Costom Views Restart the service Costom Views Restart the service Costom Views Cost	ng Engine 🔷 🔺
Application Application Application More Ac	tions 🕨
Security Security The Base Filtering Engine (BFE) is a Application Information Facilitates t Kunning Manual (Ing.	
System Internet Protocol security (IPsec) Application Management Processes in Manual	
Forwarded Event policies and implements user mode Applications and Sel filtering. Stopping or disabling the Rectoround Intelligent Trans Transfers file Running Automatic (D	
Subscriptions BFE service will significantly reduce the security of the system. It will also	
b Shared Folders result in unpredictable behavior in Gase Filtering Engine The Base Filtering Automatic	
BitLocker Drive Encryption BDESVC hos Manual (Trig.	
Durice Manual	
Bluetooth Handsfree Service Enables wir Manual (Trig.	
Schuge Generate Ge	
A Bryces and Applications Galaxies Galaxies Galaxies Galaxies Manual	
Services Manual	
MVI Control School Control Con	
COM+ Event System Supports Sy Running Automatic	
🖓 COM+ System Application Manages th Manual	
🖓 Computer Browser Maintains a Running Manual (Trig.	
🖓 Credential Manager Provides se Running Manual	
🖓 Cryptographic Services Provides thr Running Automatic	
🖓 DCOM Server Process Laun The DCOM Running Automatic	
🖓 Device Association Service Enables pair Running Manual (Trig.	
🖓 Device Install Service 🛛 Enables a c Running Manual (Trig.	
🔍 Device Setup Manager Enables the Manual (Trig.	
G DHCP Client Registers an Running Automatic	
C Discussion Definition Constant Discussion Discussion Automatic Street	
< > Letended (Standard /	

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

	Stop Other Services	×
<u> </u>	When Base Filtering Engine stops, these other services will also stop.	
	Windows Defender Network Inspection Service Windows Defender Network Inspection System Driver Windows Firewall	
	Do you want to stop these services?	
	Yes No	

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.

	Windows Defender	
C status: At risk		
Home Update Hist	tory Settings	😗 Help
Real-time protection Excluded files and locations Excluded file types Excluded processes Advanced	Utim on this app When this check box is selected, this app will alext all users if spyware or other potentially unwanted software attempts itself on this PC.	to run or install
MAPS Administrator	This app has been turned off and isn't monitoring your computer.	
	If you're uang another ago to check for naisoud or unwanted software, use Action Center to check that agr's status.	
	Close Serve changes	Cancel
Storage Disk Management Services and Applications	Windows Color System The WcsPha Manual Windows Connect New - C WCNCSVC Manual Windows Connection Mana Makes auto Parming Automatic	
Services	G Windows Defender Networ Heips guard Manual G Windows Defender Service Helps prote Running Automatic y	

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?

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?

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.

<u>*</u>	Computer Management	- 🗇 🗙
File Action View Help		
🗢 🌩 🖬 🗟 🖬		
🛃 Computer Management (Loca	al Name	Actions
a 🎁 System Tools	R System Tools	Computer Manageme
Task Scheduler Task	Storage	Mars Astigas
El Event Viewer	Services and Applications	More Actions
Bill Shared Folders		
A N Performance		
Monitoring Tools		
a 📑 Data Collector Sets		
User Defined		
Sys New	Data Collector Set	
Sta	sh	
Report Help		
Device Manager		
Disk Management		
Services and Applications		
·		
< >		
Create a 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.

	×
😑 🔊 Create new Data Collector Set.	
How would you like to create this new data collector set?	٦
Name:	
Memory Logs	
Create from a template (Recommended)	
Oreate manually (Advanced)	
	_
Next Finish Canc	el

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

	×
📀 🔊 Create new Data Collector Set.	
What type of data do you want to include?	
 Create data logs Performance counter Event trace data System configuration information 	
O Performance Counter Alert	
N	ext Finish Cancel

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

Screate new Data Collector Set. Which performance counters would be a set of the set of t	ıld you like to log?
Performance counters:	, ,
	A <u>d</u> d
	<u>R</u> emove
Sample <u>i</u> nterval: <u>U</u> nits:	
15 😫 Seconds 🗸	

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

						L
vailable counters		Added counters				
elect counters from computer:		Counter	Parent	Inst	Computer	٦
<local computer=""> V Br</local>	owse	Memory	rurent	inser.	compater	4
		Available KBytes				
Memory	• • •	Available royces				
% Committed Bytes In Use						
Available Bytes						
Available KBytes						
Available MBytes						
Cache Bytes						
Cache Bytes Peak						
Cache Faults/sec						
Commit Limit	×					
istances of selected object: 						
۲ ۲	Search					
A	.d <u>d</u> >>	<u>R</u> emove <<				
Show description				OK	Cancel	

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

 Create new Data Collector Set. Which performance counters would 	you like to log?
Performance <u>c</u> ounters:	
\Memory\Available KBytes	A <u>d</u> d
	<u>R</u> emove
Sample interval: Units:	
Seconds V	
	Not Einich Con-

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

	×
📀 🔊 Create new Data Collector Set.	
Where would you like the data to be saved?	
Root directory:	
%systemdrive%\PerfLogs\Admin\MemoryLogs Browse	
	_
Next Finish Ca	ncel

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

Browse For Folder	×
Select a root path for the collected data.	
	_
Floppy Disk Drive (A:)	^
🖉 🏪 Local Disk (C:)	
🛛 🖟 inetpub	
퉬 PerfLogs	
Program Files	
Program Files (x86)	
Users	
Windows	- 11
▷ 🚑 DVD Drive (D:)	<u>×</u>
Make New Folder OK Cancel	

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

	×
← S Create new Data Collector Set.	
Where would you like the data to be saved?	
Root directory:	
C:\PerfLogs Browse	
Next Finish Can	:el

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

	×
📀 🔊 Create new Data Collector Set.	
Create the data collector set?	
Run as:	
<default> Change</default>	
○ Open properties for this data collector set	
◯ Start this data collector set now	
Save and close	
Next Finish Can	cel

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

re : ataCollector01	Type Performance Co	Output Delete Properties Help	Actions Memory Logs More Actions DataCollector01 More Actions
ne JataCollector01	Type Performance Co	Output Delete Properties Help.	Actions Memory Logs More Actions DataCollector01 More Actions
lataCoffector01	- Performance Co	Delete Properties Help	Memory Logs More Actions DataCollector01 More Actions
		Delete Properties Help	More Actions DataCollector01 More Actions
		Properties Help	DataCollector01 More Actions
		Help	More Actions
	selection.	selection.	xelection.

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

DataCollector01 Properties		×
Performance Counters File		
Performance counters:		
Wemory Available MBytes	Add	
	Remove	
		_
Log format:		
Binary V		
Tab Separated Units: Maximu	um samples:	-
Binary Seconds V 0	•	
Data source name:		
		4
OK Cancel	Apply	

n. Click the File tab.

DataCollector01 Properties	x
Performance Counters File	
Log file name:	
DataCollector01	
File name format:	
>	
Prefix file with computer name	
Log mode	
Overwrite	
Append	
Circular (requires a non-zero maximum file size)	
Example file name: C:\PerfLogs\virtual_20150903-000001\DataCollector01.csv	
OK Cancel Apply	

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

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.

<u></u>		Computer Manage	ment	- 🗇 🗙
File Action View Help				
🗢 🄿 🗖 📰 🗙 🗟 🗟 📄	? 📊 🕨 🔳 📸 🖬			
Computer Management (Local)	Name	Туре	Output	Actions
Tisk Scheduler	🔤 DataCollector01	Performance Counter	C:\PerfLogs\virtual_20150903-000002\DataCollect	Memory Logs
 Ison of the address Ison of the address Ison of the address 				More Actions
Shared Folders				
Eccal Users and Groups				
Monitoring Tools				
a 📑 Data Collector Sets				
User Defined				
System				
Event Trace Sessions				
Startup Event Trace Se				
Device Manager				
🔺 📇 Storage				
🔤 Disk Management				
Services and Applications				
· · · · · · · · · · · · · · · · · · ·			2	1

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.

<u>*</u>		Computer Manage	ment	- 0 ×				
File Action View Help								
🛃 Computer Management (Local)	Name	Туре	Output	Actions				
System Tools	M DataCollector01	Performance Counter	C:\PerfLogs\virtual 20150903-000002\DataCollect	Memory Logs				
Task Scheduler				Menoly Logs				
Event Viewer				More Actions				
Shared Folders								
Eccal Users and Groups								
Manitarian Taola								
Data Collector Sets								
Memory Logs								
System								
Event Trace Sessions								
🔚 Startup Event Trace Se								
Reports								
🚔 Device Manager								
a 🔄 Storage								
🔤 Disk Management								
Services and Applications								
*	•		>	<u> </u>				

What change do you notice for the Memory Logs icon?

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.

🍱 l 💽 🚺 🗢 l	virtual_20150903-000001		- 🗆 🗙
File Home Share	e View		~ ?
🔄 🄄 🔻 🛉 📕 « P	erfLogs > virtual_20150903-000001	✓ C Search virte	ual_20150903-00 🔎
Desktop ^	Name	Date modified	Туре
Downloads	DataCollector01.csv	9/3/2015 1:31 PM	CSV File
BitTorrent Sync			
🤣 Homegroup			
🖳 This PC			
膧 Desktop			
Documents			
🗼 Downloads			
🔰 Music			
E Pictures			
📔 Videos			
🚢 Local Disk (C:) 🗸	<		>
1 item			=

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.

DataCollector01.csv - Notepad	-		x
File Edit Format View Help			
<pre>["(PDH-CSV 4.0) (Eastern Daylight Time)(240)","\\virtual\Memory\Available "09/03/2015 13:30:45.765","1336" "09/03/2015 13:30:43.765","1343" "09/03/2015 13:30:57.750","1343" "09/03/2015 13:31:01.751","1344" "09/03/2015 13:31:05.754","1261" "09/03/2015 13:31:03.750","1215" "09/03/2015 13:31:13.765","1225" "09/03/2015 13:31:17.750","1267"</pre>	МВу	tes"	< >
			>

What does the column farthest to the right show?

- u. Close the DataCollector01.csv file and Windows Explorer.
- v. Select the Performance Monitor window.

튪		Computer Management – 🗇						
File Action View Help								
Computer Management (Local)	Name	Туре	Output	Actions				
System Loois A Task Scheduler	MataCollector01	Performance Counter	C:\PerfLogs\virtual_20150903-000002\DataColle	Memory Logs				
Event Viewer				More Actions				
Shared Folders								
Derformance								
🕟 🔂 Monitoring Tools								
Data Collector Sets								
Memory Logs								
System	Start							
Event Trace Ses	Stop							
Startup Event II Reports	Save Template							
📇 Device Manager	Data Manager							
a 🔄 Storage	Latest Report							
Disk Management Services and Applications	New +							
	View +							
	Delete							
	Refresh							
	Export List							
	Properties							
	Help							
< 2	× <		>					
Deletes the current selection.								

- 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.