# IT Essentials 5.0

# 5.3.3.7 Lab - Monitor and Manage System Resources in Windows XP

# Introduction

Print and complete this lab.

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

# **Recommended Equipment**

The following equipment is required for this exercise:

- A computer running Windows XP Professional
- Internet access

### Step 1

You will explore what happens when a service is stopped then started.

Log on to Windows as an administrator.

Click Start > Control Panel > Administrative Tools > Computer Management > expand Services and Applications.

Select Services.

Expand the **Computer Management** window so you see the "Help and Support" service.

File Action View Window He	lp .						_ 8
> 🖻 🔳 💣 🛃 😫	▶ ■    ■>						
Computer Management (Local) System Tools Computer Viewer System Tools Computer Viewer Computer Viewer	Services      Help and Support      Stop the service Restart the service      Description:     Enables Help and Support Center to run     or this computer. If this service is asobled,     any services that explicitly depend on it     will fail to start.	Name Cryptographic Servi Cryptographic Servi DCOM Server Proce DefWatch DHCP Client Distributed Iransac Distributed Iransac Error Reporting Ser Error Reporting Ser Fast User Switching Help and Support HITP SSL HITP SSL HITP SSL Indexing Service JPSEC Services Java Quick Starter Logical Disk Manager	Provides la Manages n Maintains li Coordinate Resolves a Provides m Provides m Enables de Enables de This servic Manages C Indexes co Manages I Prefetches	Status Started Started Started Started Started Started Started Started Started Started Started Started Started Started	Startup Type Automatic Automatic Automatic Automatic Automatic Manual Automatic Automatic Manual Manual Manual Manual Manual Manual Manual Automatic Automatic Manual Manu	Log On As Local System Local System	
		Logical Disk Manage Messenger	Configures Transmits Run portio		Manual Disabled Manual	Local System Local System Local System	
		Microsoft Office Gro MS Software Shado Net Logon	Manages s Supports p		Manual Manual Manual	Local Service Local System Local System	
		Net Logon Net.Tcp Port Sharin NetMeeting Remote	Provides a		Manuai Disabled Manual	Local System Local Service Local System	

What is the Status of the service?

Right-click the Help and Support service > Properties.

The "Help and Support Properties (Local Computer)" window opens.

lelp and Suppo	rt Properties (Local Computer)	X
General Log On	Recovery Dependencies	
Service name:	helpsvc	
Display name:	Help and Support	-
Description:	Enables Help and Support Center to run on this computer. If this service is stopped, Help and	
Path to executat	ole:	
C:\WINDOWS\	System32\svchost.exe -k netsvcs	
Startup type:	Automatic	
Service status:	Started	- 20
Start	Stop Pause Resume	
You can specify from here. Start parameters:	hg the start parameters that apply when you start the service	
	OK Cancel Apply	,

### Click Stop.

**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.

ł	lelp and	Suppor	rt Propert	ies (Local	Computer)		?×
	General	Log On	Recovery	Dependenc	ies		
	Service	name:	helpsvc				
	Display	name:	Help and S	Support			-
	Descrip	tion:			ort Center to r is stopped, H		~
	Path to	executabl	e:				
	C:\WIN	IDOWS\S	ystem32\sv	chost.exe -k r	netsvos		
	Startup	type:	Disabled				~
	Service	status:	Stopped				_
	9	itart	Stop		Pause	Resume	
	You ca from he		he start para	meters that a	pply when you	i start the serv	vice
	Start pa	rameters:					
				OK	Canc	el 🛛	

When the Service Control window closes, set the Startup type field to **Disabled**, and then click **Apply**.

### Click Start > Help and Support.

My Documents	
My Recent Documents 🔸	
👏 My Pictures	
🤔 My Music	
😡 My Computer	
🧐 My Network Places	
Control Panel	
💮 Set Program Access and Defaults	
Printers and Faxes	
Help and Support	
Search	
7 Run	

The "Help and Support Error" window opens.

Help and Support Error 🛛 🔀
Windows cannot open Help and Support because a system service is not running.
To fix this problem, start the service named 'Help and Support'.
<u> </u>

Why will Help and Support not start?

What must be done to correct the error?

Click OK.

What steps must be followed to start the Help and Support service?

Next, you will start up the Help and Support service.

File		Window Help rt Properties (Local Computer)	? ×	1					_
	General Log On	Recovery Dependencies							
	Service name:	helpsvc			1		1		
e	Service name:	helpsvc		Name A	Description	Status	Startup Type	Log On As	
8	Display name:	Help and Support		Background Intellig		Started	Manual	Local System	
6				SclipBook ClipBook	Enables Cli	10336	Disabled	Local System	
J	Description:	Enables Help and Support Center to run on this computer. If this service is stopped, Help and	~	COM+ Event System		Started	Manual	Local System	
		computer. In this service is stopped, Help and	~	COM+ System Appli			Manual	Local System	
	Path to executabl	e.		Computer Browser	Maintains a		Automatic	Local System	
		ivstem32\svchost.exe -k netsvcs		Cryptographic Servi			Automatic	Local System	
	0.10010000000	yatemoz tavenoac.exe ik netavea		e SDCOM Server Proce	. Provides la		Automatic	Local System	
	Startup type:	Automatic	~	SefWatch		Started	Automatic	Local System	
	startup type:	Automatic	×	DHCP Client	Manages n		Automatic	Local System	
				Distributed Link Tra		Started	Automatic	Local System	
	Service status:	Started		Distributed Transac	. Coordinate Resolves a	Started	Manual Automatic	Network S Network S	
	Service status.	stated					Automatic		
	Start	Stop Pause Res	ume	Error Reporting Ser	Enables ev		Automatic	Local System	
				Fast User Switching			Manual	Local System Local System	
		he start parameters that apply when you start the	service	Help and Support	Enables He		Automatic	Local System	
I	from here.			HID Input Service	Enables ge		Automatic	Local System	
I	Start parameters:			HITP SSL	This servic	Started	Manual	Local System	
		L		MAPI CD-Burning C.			Manual	Local System	
				Indexing Service	Indexes co		Manual	Local System	
ľ			1000	IPSEC Services	Manages I	Started	Automatic	Local System	
L		OK Cancel	Apply	Java Quick Starter	Prefetches		Automatic	Local System	
			17		Freietenes	Joarcod	- acomadic	coodi byscom	

Set "Startup type" to Automatic, and then click OK.

Click Start > Help and Support.

Did the Help and Support Center window appear?

Close the "Help and Support Center" window.

Make sure the Computer Management window is open.

Expand Event Viewer, and then select System.

Double-click the most recent Error event. Error events are displayed as a white X in a red circle icon.

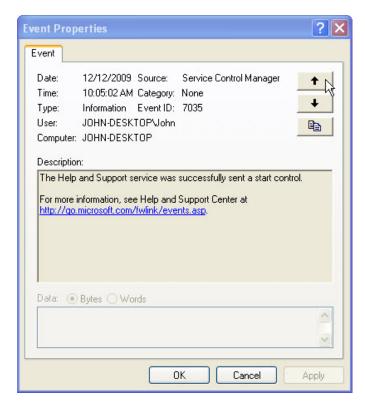
📕 Computer Management							• 🖃 💶	
📃 File Action View Window H	Help							_ <del></del>
← → 🗈 🖬 🖆 🛱 🖆	2							
🖳 Computer Management (Local) 🛛 🔼	Туре	Date	Time	Source	Category	Event	User	^
🖻 🐞 System Tools	Information	12/12/2009	10:05:02	Service Control Manager	None	7036	N/A	_
Event Viewer	Information	12/12/2009	10:05:02	Service Control Manager	None	7035	John	
Application	S Error	12/12/2009	9:56:31 AM	DCOM	None	10005	John	
Internet Explorer	( Information	12/12/2009	9:47:43 AM	Service Control Manager	None	7036	N/A	
Microsoft Office Diag	Information	12/12/2009	9:47:43 AM	Service Control Manager	None	7035	John	
Security	Information	12/12/2009	9:46:10 AM	Service Control Manager	None	7036	N/A	
System	Information	12/12/2009	9:46:10 AM	Service Control Manager	None	7035	John	
Grand Folders	Information	12/12/2009	9:46:06 AM	Service Control Manager	None	7036	N/A	
Local Users and Groups	Information	12/12/2009	9:46:06 AM	Service Control Manager	None	7035	John	
🛨 🙀 Performance Logs and Alı	Information	12/12/2009	9:46:03 AM	Service Control Manager	None	7036	N/A	
🗌 🧮 Device Manager 🛛 💌	Information	12/12/2009	9:46:03 AM	Service Control Manager	None	7035	John	~
	<							>

The "Event Properties" window opens.

Event Pro	perties					? 🗙
Event						
User:	12/12/2009 9:56:31 AM Error JOHN-DESK : JOHN-DESK	Category: Event ID: TOP\John			[	↑ ↓ ₽
Descriptio	on:					
disabled attemptin the serve {833E40	ot error "The se or because it h- ig to start the se r: 10-AFF7-4AC3- information, se <u>information</u> , se	as no enab ervice helps AAC2-9F24 e Help and	led device ivc with a C1457BC Support C	es associate rguments "" E}	d with it. '	•
Data: ()	) Bytes 🔿 Wo	rds				
						~
		(	к	Cancel		Apply

Why was helpsvc not started?

Click the up arrow button.



What has happened to the Help and Support service?

Click the up arrow button.

Event P	roperties		? 🔀
Event			
	10:05:02 AM Category: Information Event ID: N/A uter: JOHN-DESKTOP	None	<ul> <li>↑</li> <li>↓</li> <li>□</li> </ul>
Descri The H	ption: Help and Support service ente	red the running state.	
For m <u>http:/</u>	ore information, see Help and /go.microsoft.com/fwlink/eve	Support Center at <u>nts.asp</u> .	
Data:	Bytes O Words		
			<u> </u>
		)K Cancel	Apply

What has happened to the Help and Support service?

Close all open windows.

## Step 2

You will now monitor what happens when a service is stopped and started.

Click Start > Control Panel. Double-click the Network Connections icon.

Control Panel								
File Edit View Favorites T	ools Help							
Ġ Back 🝷 🕥 🕤 🏂 🍃	🔵 Search 🛛 🍋 Fol	ders 🛄 🕇	Folder 9	Sync				
Address 📴 Control Panel							¥ [	> Go
Control Panel	a 🔥	Ń	đ	-		P	<u>s</u>	
🚱 Switch to Category View	Accessibility Options	Add Hardware	Add or Remov	Administrative Tools	Automatic Updates	Date and Time	Display	
See Also	» 🗹		Sol and a sol	R	P		1	
🍇 Windows Update	Folder Options	Fonts	Game Controllers	Indexing Options	Internet Options	Java	Keyboard	
Help and Support		C		۵		4		
	Mail	Mouse	Network Connections	Network Setup Wizard	Phone and Modem	Power Options	Printers and Faxes	
	<u> </u>		1	۲		Ø,	3	
	Regional and Language	Scanners and Cameras	Scheduled Tasks	Security Center	SoundMAX	Sounds and Audio Devices	Speech	
	1 (Northern State) (Nor			<u> </u>	3	6		
	Symantec LiveUpdate	System	Taskbar and Start Menu	User Accounts	Windows CardSpace	Windows Firewall	Wireless Network Set	

The "Network Connection" window opens.

🔌 Network Connections 🔹 🖬 🗖 🔀
File Edit View Favorites Tools Advanced Help 🥂
G Back - 🕥 - 🏂 🔎 Search 🎼 Folders 🔝 - 🔞 Folder Sync
Address 🗞 Network Connections 🛛 🍷 Go
Network Tasks       An or High-Speed Internet         Create a new connection       Local Area Connection         Set up a home or small office network       Marvell Yukon 88E8001/8003/         Change Windows Firewall settings       High-Speed Internet
See Also

Reduce the size of the "Network Connections" window. Leave this window open.

Once again navigate to the "Control Panel" window by clicking **Start > Control Panel**. Double-click the **Administrative Tools** icon.

Edit View Favorites Tool:	s Help						
) Back 🔹 🕥 - 🏂 🔎	Search 🔀 Fol	ders 🛄 -	Folder :	5ync			
ess 📴 Control Panel							¥ 🗗
Control Panel	Ċ.	Ń	6	-	2	P	1
Switch to Category View	Accessibility Options	Add Hardware	Add or Remov	Administrative Tools	Automatic Updates	Date and Time	Display
iee Also	I		and the	Con	figure adminis	trative settings f	or your computer.
iee Also 🄇 🄇	Folder Options	Fonts	Game Controllers	Indexing Options	Internet Options	Java	Keyboard
Help and Support		(C)		-		4	
	Mail	Mouse	Network Connections	Network Setup Wizard	Phone and Modem	Power Options	Printers and Faxes
	6	<b>S</b>	1			Ø,	×
	Regional and Language	Scanners and Cameras	Scheduled Tasks	Security Center	SoundMAX	Sounds and Audio Devices	Speech
	<b>1</b>				3		***
	Symantec LiveUpdate	System	Taskbar and Start Menu	User Accounts	Windows CardSpace	Windows Firewall	Wireless Network Set

The "Administrative Tools" window opens.

National Administrative Tools	• E _ D 🛛
File Edit View Favorites Tools Help	<i>A</i> *
Sack • 🕥 • 🏂 🔎 Search 🎼 Folders 🛄 • 🔞 Folder Sync	
Address 🙀 Administrative Tools	🖌 🄁 Co
File and Folder Tasks  Component Services Shortcut KB Component Services Component Servic	
Move this file     Copy this file     Publish this file to the	
Web E-mail this file Delete this file Local Security Policy Shortcut 2 KB Delete this file Shortcut	
Other Places         Microsoft .NET Framework 1.1         Performance Shortcut           Shortcut         2 KB         KB         KB	
Control Panel Shortcut My Documents Shortcut Shared Documents	
Wy Computer My Network Places	
Details	
Performance Shortcut	
Date Modified: Friday, June	

Double-click the **Performance** icon.

The "Performance" window opens.

🖬 Performance 🔹 🖬 🗖 🗙			
📷 File Action View Favorites	Window Help	×	
← → 🗈 🖬 😫			
Console Root	📋 🗔 🌾 🕄 🛄 🗐 🕂 🗙 🌾 🗈 😂 🚳 🧶 🐲	2	
System Monitor ⊕ ∰ Performance Logs and Alerts	100		
	80		
	60		
	40		
		000	
	Maximum 19.001 Duration 1	:40	
	Color Scale Counter Instance Parent Object Computer		
	1.000 Pages/sec Memory \\JOHN-DE3     100 Avg. Disk QuTotal Physic \\JOHN-DE3		
		_	

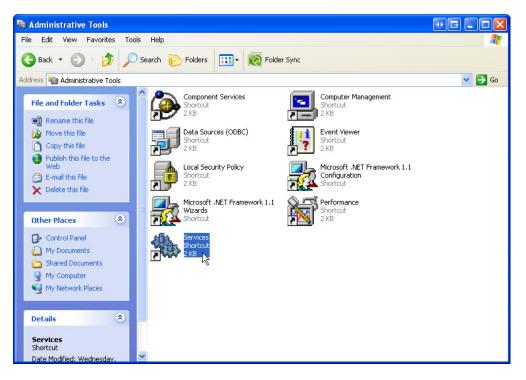
Make sure the System Monitor in the left pane is highlighted.

Click the Freeze Display icon to stop the recording.

🐹 Performance		
👹 File Action View Favorites	Window Help	_ & ×
← → 🗈 🖬 😫		
Console Root ∰ System Monitor ⊕ ∰ Performance Logs and Alerts	Maximum         0.000         Dura           Color         Scale         Counter         Instance         Parent         C           1.000         Pages/sec          M           100         Avg. Disk Qu         Total          P	imum 0.000 ation 1:40 Dbject Computer emory (JJOHN-DES hysic (JJOHN-DES) roces (JJOHN-DES)

Click the **Clear Display** icon to clear the graph. Leave this window open.

Navigate to the "Administrative Tools" window by clicking **Start > Control Panel > Administrative Tools**. Double-click the **Services** icon.



Expand the width of the "Services" window so you have a clear view of the content.

le Action View	Help					
Services (Local)	Services (Local)					
	Routing and Remote Access	Name 🔺	Description	Status	Startup Type	Log On As
		QoS RSVP	Provides n		Manual	Local System
	Description:	Remote Access Auto Conn	Creates a		Manual	Local System
	Offers routing services to businesses in local area and wide area network	🔹 Remote Access Connectio	Creates a	Started	Manual	Local System
	environments.	🏶 Remote Desktop Help Ses	Manages a		Manual	Local System
		🏶 Remote Procedure Call (R	Provides th	Started	Automatic	Network S
		🏶 Remote Procedure Call (R	Manages t		Manual	Network S
		🆓 Remote Registry	Enables re	Started	Automatic	Local Service
		Removable Storage			Manual	Local System
		Routing and Remote Access			Disabled	Local System
		Seagate Sync Service	beagate S		Automatic	Local System
		Secondary Logon	Enables st	Started	Automatic	Local System
		Security Accounts Manager	Stores sec	Started	Automatic	Local System
		Security Center	Monitors s	Started	Automatic	Local System
		Server 5	Supports fil	Started	Automatic	Local System
		Shell Hardware Detection	Provides n	Started	Automatic	Local System
	Extended Standard	68	M		Manage 1	Caral Caralian

Scroll down in the right pane until you see the service Routing and Remote Access.

#### Double-click Routing and Remote Access.

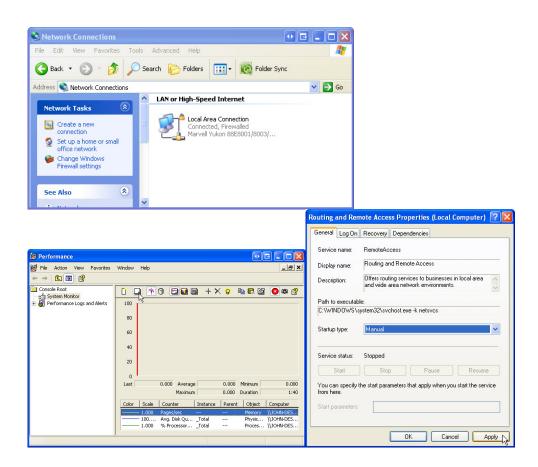
The "Routing and Remote Access Properties (Local Computer)" windows opens.

Routing and R	emote Access Properties (Local Computer) ? 🔀
General Log O	n Recovery Dependencies
Service name:	RemoteAccess
Display name:	Routing and Remote Access
Description:	Offers routing services to businesses in local area and wide area network environments.
Path to execut	able:
C:\WINDOWS	\system32\svchost.exe -k netsvcs
Startup type:	Manual 💙
Service status:	Stopped
Start	Stop Pause Resume
You can specil from here. Start paramete	y the start parameters that apply when you start the service

In the Startup type select Manual. Click Apply.

The Start button is now active; do not click the button yet. Leave this window open.

Position the following three windows so you can clearly see them at the same time: Network Connections, Routing and Remote Access Properties (Local Computer), and Performance.



Click the "Performance" window so it is activated. Click the Freeze Display icon to start the recording.

Performance	
👹 File Action View Favorites	Window Help
← → 🗈 🖬 😫	
Console Root	🗋 🗀 🎠 🥱 🖼 🖬 🖶 🖊 🖌 😫 🔜 📾 🔗
Performance Logs and Alerts	100
	80
	60
	40
	20
	0
	Last 0.000 Average 0.000 Minimum 0.000
	Maximum 0.000 Duration 1:40
	Color Scale Counter Instance Parent Object Computer
	1.000 Pages/sec Memory \\JOHN-DES
	100 Avg. Disk QuTotal Physic \\JOHN-DE5 1.000 % ProcessorTotal Proces \\JOHN-DE5
	1.000 % ProcessorTotal Proces \\JOHN-DE5

Click the "Routing and Remote Access Properties (Local Computer)" window so it is activated. To start the Service click **Start**.

A window with a progress bar opens.

Service Control	×
Windows is attempting to start the following service on Local Computer	
Routing and Remote Access	_
Close	

The "Routing and Remote Access Properties (Local Computer)" window now shows the Stop and Pause button active. Leave this window open.

eneral Log On	Recovery Dependencies	
Service name:	RemoteAccess	
Display name:	Routing and Remote Access	
Description:	Offers routing services to businesses in local area and wide area network environments.	<
Path to executa	ble:	
C:\WINDOWS\	system32\svchost.exe -k netsvcs	
Startup type:	Manual	~
Service status:	Started	
Start	Stop Pause Resume	
You can specify from here.	the start parameters that apply when you start the servi	се
Start parameters		
oran parameters		

Click the "Network Connections" window so it is activated.

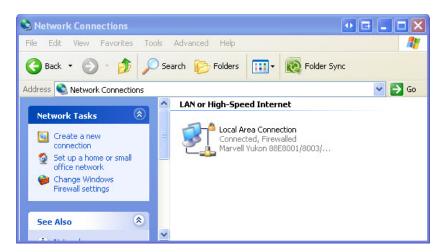
Setwork Connections		• • • • •
File Edit View Favorites Tools	Advanced Help	A.
🔇 Back 🔹 🕥 - 🏂 🔎 S	Search 🎼 Folders 🔝 🛛 🔞 Folder Sync	
Address 🔇 Network Connections		💌 🄁 Go
Network Tasks	Incoming	
Network Tasks         Image: Create a new connection           Image: Set up a home or small frier network	Incoming Connections No clients connected	
😂 Change Windows	LAN or High-Speed Internet	
Firewall settings		
See Also	Marvell Yukon 88E8001/8003/	
Network     Troubleshooter		
Other Places 🛞		
🚱 Control Panel		
My Network Places		
Hy Documents		
Details 🙁		
Network Connections System Folder	2	

What changes appear in the right pane, after starting the Routing and Remote Access service?

Click the "Routing and Remote Access Properties (Local Computer)" window so it is activated. Click Stop.

Routing and Rer	note Access Properties (Local Computer) ? 🔀
General Log On	Recovery Dependencies
Service name:	RemoteAccess
Display name:	Routing and Remote Access
Description:	Offers routing services to businesses in local area and wide area network environments.
Path to executab	le:
C:\WINDOWS\s	ystem32\svchost.exe -k netsvcs
Startup type:	Manual
Service status:	Started
Start	Stop Pause Resume
You can specify from here.	the start parameters that apply when you start the service
Start parameters:	
	OK Cancel Apply

Click the "Network Connections" window so it is activated.



What changes appear in the right pane, after stopping the Routing and Remote Access service?

Click the "Performance" window so it is activated. Click the Freeze Display icon to stop the recording.

😽 Performance	
👹 File Action View Favorites	Window Help
← → 🗈 🖪 😫	· · · · · · · · · · · · · · · · · · ·
<ul> <li>Console Root</li> <li> <sup>→</sup> System Monitor         System Monitor     </li> <li> <sup>→</sup> Ø Performance Logs and Alerts     </li> </ul>	
	Last 0.000 Average 0.050 Minimum 0.000
	Maximum 2.000 Duration 1:40
	Color Scale Counter Instance Parent Object Computer
	1.000         Pages/sec          Memory         \JOHN-DES           100         Avg. Disk Qu        Total          Physic         \JOHN-DES           1.000         % Processor        Total          Proces         \JOHN-DES

Which Counter is being recorded the most in the graph (hint: look at the graph color and Counter color)?

Click the View Report icon.

😽 Performance		
Performance         File       Action       View       Favorites         Console Root       System Monitor         Performance Logs and Alerts	Window Help	R) 10 al 12 al

List the values of the three counters.

Click the "Routing and Remote Access Properties (Local Computer)" window so it is activated.

ieneral Log	On Recovery Dependencies
Service nam	e: RemoteAccess
Display nam	e: Routing and Remote Access
Description:	Offers routing services to businesses in local area and wide area network environments.
Path to exec	utable:
C:\WINDOV	VS\system32\svchost.exe -k netsvcs
Startup type:	Disabled 🗸 🗸
Startup type: Service statu Start	
Service statu	us: Stopped
Service statu Start You can spe	us: Stopped Stop Pause Resume cify the start parameters that apply when you start the service

In the Startup type select **Disabled** and then click **OK**.

Click the "Services" window so it is activated.

- → 💽 😭	Help						
Services (Local)	🏇 Services (Local)						
	Routing and Remote Access	Name 🛆	Description	Status	Startup Type	Log On As	
	-	Portable Media Serial Num	Retrieves t		Manual	Local System	
	Description:	Print Spooler	Loads files	Started	Automatic	Local System	
	Offers routing services to businesses in local area and wide area network	Protected Storage	Provides pr	Started	Automatic	Local System	
	environments.	QoS RSVP	Provides n		Manual	Local System	
		Remote Access Auto Conn	Creates a		Manual	Local System	
		Remote Access Connectio	Creates a	Started	Manual	Local System	
		Remote Desktop Help Ses	Manages a		Manual	Local System	
		Remote Procedure Call (R	Provides th	Started	Automatic	Network S	
		Remote Procedure Call (R	Manages t		Manual	Network S	
		Remote Registry	Enables re	Started	Automatic	Local Service	
		Removable Storage			Manual	Local System	
		Routing and Remote Access	Offers rout		Disabled	Local System	
		Seagate Sync Service	Seagate S		Automatic	Local System	
		Secondary Logon	Enables st	Started	Automatic	Local System	
		Security Accounts Manager	Stores sec	Started	Automatic	Local System	
		6Bu		Charles	A. 4		_

What is the Status and Startup Type for Routing and Remote Access?

Click the "Performance" window so it is activated.

📓 Performance	• • • • •
🗑 File Action View Favorites	Window Help
← →   🗈 💽 😫	
Console Root	🗋 🖵 🎠 🗇 🔛 🛄 🖶 + X 😒 ங 🖴 😂 🝳 🛎 🔮
gi System Monitor F 🎆 Performance Logs and Alerts	100
	80
	60
	40
	20 /\
	Last 0.000 Average 0.050 Minimum 0.000
	Maximum 2.000 Duration 1:40
	Color Scale Counter Instance Parent Object Computer

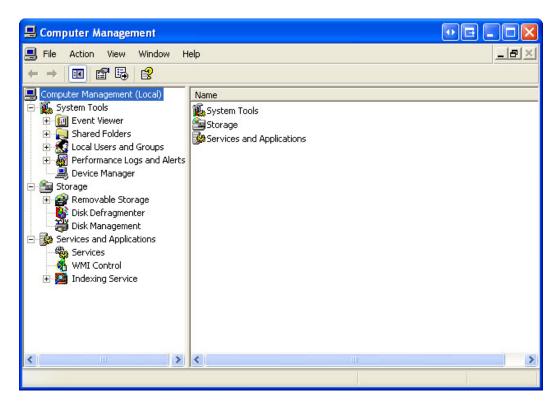
Click the Freeze Display icon to start the recording.

Close all open windows.

Navigate to the "Control Panel" window by clicking **Start > Control Panel**. Double-click the **Computer Management** icon.



The "Computer Management" window opens.



Expand the three categories by clicking on the **plus sign** next to: System Tools, Storage and Services, and Applications.

Click the **plus sign** next to Event Viewer.

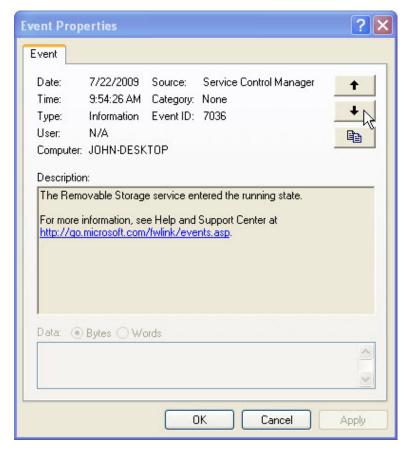
File Action View Window	Н	lelp							_ 8
主 🔳 🖆 🗟	ß	?							
Computer Management (Local)	^	Туре	Date	Time	Source	Category	Event	User	
🍇 System Tools		Information	7/22/2009	9:54:26 AM	Service Control Manager	None	7036	N/A	
Event Viewer		Information	7/22/2009	9:54:26 AM	Service Control Manager	None	7035	SYSTEM	
Application		Information	7/22/2009	9:32:11 AM	Service Control Manager	None	7036	N/A	
Internet Explorer		Information	7/22/2009	9:32:06 AM	Service Control Manager	None	7035	John	
Microsoft Office Diag		Warning	7/22/2009	9:31:42 AM	RemoteAccess	None	20192	N/A	
Microsoft Office Sess		Information	7/22/2009	9:31:42 AM	Service Control Manager	None	7036	N/A	
Security		Information	7/22/2009	9:31:42 AM	Service Control Manager	None	7035	John	
E Shared F		Information	7/22/2009	8:18:08 AM	Service Control Manager	None	7036	N/A	
E Cocal Users and Groups		Information	7/22/2009	8:18:03 AM	Service Control Manager	None	7035	John	
+ Performance Logs and Al		Warning	7/22/2009	8:17:35 AM	RemoteAccess	None	20192	N/A	
Device Manager		Information	7/22/2009	8:17:35 AM	Service Control Manager	None	7036	N/A	
Storage		(1) Information	7/22/2009	8:17:35 AM	Service Control Manager	None	7035	John	
🗄 🤮 Removable Storage		(i) Information	7/22/2009	8:17:25 AM	Service Control Manager	None	7036	N/A	
🛛 🚱 Disk Defragmenter		(1) Information	7/22/2009	8:17:20 AM	Service Control Manager	None	7035	John	
🗃 Disk Management		Warning	7/22/2009	8:05:03 AM	RemoteAccess	None	20192	N/A	
Services and Applications		Information	7/22/2009	8:05:02 AM	Service Control Manager	None	7036	N/A	
Services		(1) Information	7/22/2009	8:05:02 AM	Service Control Manager	None	7035	John	
- 🍓 WMI Control	~	(i) Information	7/22/2009	7:29:59 AM	Service Control Manager	None	7036	N/A	
		<							>

Then select System.

File Action View Window H	ielp							_ <del>_</del> _ <del>_</del> _
🗈 📧 🗗 🗗 🔓 🖆	}							
Computer Management (Local) 🛛 🔼	Туре	Date	Time	Source	Category	Event	User	^
🐞 System Tools	Information	7/22/2009	9:54:26 AM	Service Control Manager	None	7036	N/A	
Event Viewer	Information	7/22/2009	9:54:26 AM	Service Control Manager	None	7035	SYSTEM	
Application	Information	7/22/2009	9:32:11 AM	Service Control Manager	None	7036	N/A	
Internet Explorer	Information	7/22/2009	9:32:06 AM	Service Control Manager	None	7035	John	
Microsoft Office Diag     Microsoft Office Sess	🔥 Warning	7/22/2009	9:31:42 AM	RemoteAccess	None	20192	N/A	
Security	Information	7/22/2009	9:31:42 AM	Service Control Manager	None	7036	N/A	
System	Information	7/22/2009	9:31:42 AM	Service Control Manager	None	7035	John	
Grand Folders	Information	7/22/2009	8:18:08 AM	Service Control Manager	None	7036	N/A	
E Cocal Users and Groups	( Information	7/22/2009	8:18:03 AM	Service Control Manager	None	7035	John	
A Performance Logs and Ale	🔥 Warning	7/22/2009	8:17:35 AM	RemoteAccess	None	20192	N/A	
Device Manager	Information	7/22/2009	8:17:35 AM	Service Control Manager	None	7036	N/A	
🚵 Storage	Information	7/22/2009	8:17:35 AM	Service Control Manager	None	7035	John	
🗄 😭 Removable Storage	(1) Information	7/22/2009	8:17:25 AM	Service Control Manager	None	7036	N/A	
- Disk Defragmenter	(1) Information	7/22/2009	8:17:20 AM	Service Control Manager	None	7035	John	
🗃 Disk Management	Warning	7/22/2009	8:05:03 AM	RemoteAccess	None	20192	N/A	
Services and Applications	(1) Information	7/22/2009	8:05:02 AM	Service Control Manager	None	7036	N/A	
Services	() Information	7/22/2009	8:05:02 AM	Service Control Manager	None	7035	John	
- 🔏 WMI Control 🛛 🛛 😽	Information	7/22/2009	7:29:59 AM	Service Control Manager	None	7036	N/A	~
	<			101				>

Double-click the first event in the window.

The "Event Properties" window appears for the event.



Click the down arrow key to locate an event for Routing and Remote Access.

You should find four events that describe the order for starting and stopping the Routing and Remote Access service.

Write down the description for each of the four events. Do not include any URL information.

vent Pro	perties			? 🛛
Event				
Date: Time:	7/22/2009 9:31:42 AM		Service Control Manager None	+
Туре:	Information	Event ID:	7035	+
	JOHN-DESK			B
Compute	r: JOHN-DESK	TUP		19 A.
Descripti	on:			
Data: 0	Bytes () Wo	rds		
D'ata.	S Dytes () wit	nus		
				~
			K Cancel	Apply

ent Pro	perties			?
Event				
User: Compute	7/22/2009 9:31:42 AM Information N/A r: JOHN-DESK	Category: Event ID:	None	<ul> <li>↑</li> <li>↓</li> <li>▲</li> </ul>
Compute Descripti		TOP		
-		te Access s	ervice entered the running st	ate.
The Rou For more	uting and Remo	e Help and	Support Center at	ate.
The Rou For more	uting and Remo	e Help and	Support Center at	ate.
The Rou For more	uting and Remo	e Help and	Support Center at	ate.
The Rou For more <u>http://g</u>	uting and Remo	e Help and /fwlink/eve	Support Center at	ate.
The Rou For more <u>http://g</u>	uting and Remo e information, se a.microsoft.com	e Help and /fwlink/eve	Support Center at	ate.
The Rou For more <u>http://g</u>	uting and Remo e information, se a.microsoft.com	e Help and /fwlink/eve	Support Center at	ate.

vent Pro	perties			?
Event				
User:	7/22/2009 9:32:06 AM Information JOHN-DESK ar: JOHN-DESK	Category: Event ID: TOP\John	None	<ul> <li>↑</li> <li>↓</li> <li>●</li> </ul>
Descript The Ro control.		te Access s	ervice was successfully se	ent a stop
			Support Center at	
http://d	o.microsoft.com	/twlink/eve	<u>nts.asp</u> .	
Data: (	🖲 Bytes 🔿 Wo	urde		
D dtd.	S Bytes () We	103		~
				~
			IK Cancel	Apply

Event Pro	perties			? 🛛
Event				
	7/22/2009 9:32:11 AM Information N/A er: JOHN-DESK	Event ID:	None	<ul> <li>↑</li> <li>↓</li> <li>■</li> </ul>
Descript		e Access s	ervice entered the stopped st	ate.
For morth	e information, se o.microsoft.com	e Help and /fwlink/eve	Support Center at <u>nts.asp</u> .	
Data: (	● Bytes ◯ Wo	rds		
			IK Cancel	Apply

Close all open windows.

### Step 3

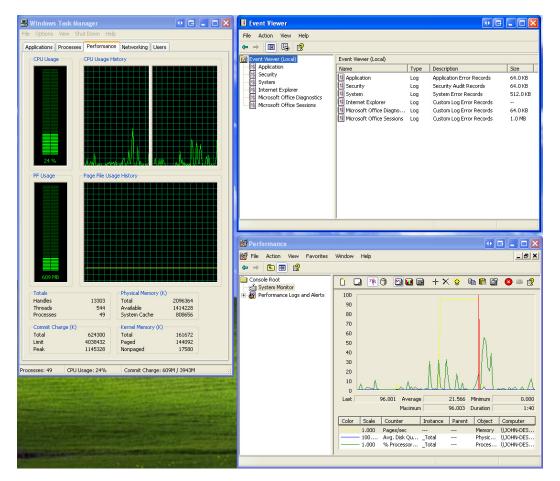
For the rest of this lab, you will configure advanced Administrative Tool features and monitor how this affects the computer system.

Press Ctrl-Alt-Delete. When the "Windows Task Manager" window opens, select the Performance tab.

Click **Start > Control Panel > Administrative Tools**. Open the following tools: Event Viewer and Performance.

Close the "Administrative Tools" window.

Resize and position all three windows so they can be seen at the same time.



Select the "Performance" window.

Expand "Performance Logs and Alerts".

M Performance	
😥 File Action View Favorites Window Help	a ×
	is is
Create a new performance counter log configuration	

Right-click Counter Logs > New Log Settings.

In the Name field, type Memory Counter.

📓 Performance	
👹 File Action View Favorites	Window Help
⇐ ⇒ 🗈 🖬 😫	
Console Root System Monitor Performance Logs and Alerts Counter Logs Trace Logs Alerts	Image: Conter       Image: Conter         Image: Conter
	1.000         Pages/sec          Memory         \\JOHN-DES           100         Avg. Disk Qu         Total          Physic         \\JOHN-DES
	1.000 % ProcessorTotal Proces \\JOHN-DE5
Create a new performance counter log c	onfiguration

Click OK.

When the "Memory Counter" window appears, click Add Counters.

Memory Counter 🔹 🤶 🔀
General Log Files Schedule
Current log file name:
C:\PerfLogs\Memory Counter_000001.blg
This log begins immediately after you apply changes.
Counters:
Add Objects Add Counters. Remove
Sample data every:
Interval: 15 💭 Units: seconds 💽
Run As: <default> Set Password</default>

The "Add Counters" window opens.

Add Counters	? 🗙
<ul> <li>Use local computer counters</li> <li>Select counters from computer:</li> </ul>	
WOHN-DESKTOP	~
Performance object:	
Memory 🗠	
O All counters	O All instances
<ul> <li>Select counters from list</li> </ul>	Select instances from list:
% Committed Bytes In Use Available Bytes	
Available KBytes Available MBytes	
Cache Bytes 💦 🙀	
Cache Butes Peak	
Add N Explain	1 / <u>-</u>
	Close

Set the Performance object field to Memory.

Set the "Select counters from list" field to Available Mbytes, and then click Add > Close.

Memory Counter
General Log Files Schedule
Current log file name:
C:\PerfLogs\Memory Counter_000001.blg
This log begins immediately after you apply changes.
Counters:
\\JOHN-DESKTOP\Memory\Available MBytes
Add Objects Add Counters Remove
Sample data every:
Interval: 5 🛟 Units: seconds 🗸
Run As: <a href="https://www.example.com">Common As: </a></a></a></a></a></a></a>
OK Cancel Apply

Change the Interval field to 5.

Select the Log Files tab.

Memory Counter
General Log Files Schedule
Log file type and name Log file type: Text File (Tab delimited)
Configure Log Files
Location:
C:\PerfLogs Browse
File name:
Memory Counter
Log file size     Maximum limit     Limit of:
1 мв
OK Cancel
OK Cancel Apply

Set the Log file type field to Text File (Tab delimited).

#### Click Configure.

What is the default location for the log files?

Click **OK** to close the "Configure Log Files" window.

A folder not found information window opens. Click Yes to create the folder.



Click the **Schedule** tab.

lemory Cour	iter			? >
General Log	Files Schedule			
Start log O Manua	illy (using the shor	tcut menu)		
💽 At	12:44:55 PM	😂 on	12/12/2009	~
Stop log Manua	Illy (using the shor	tcut menu)		
O After:	1	Units: da	ays	~
◯ At:	12:44:55 PM	💲 on	12/13/2009	~
() When	the log file is full.			
When a lo	ig file closes:			
Start a	new log file			
🔄 Run th	is command:			
			Bro	wse
<u> </u>				
	C	ок 🖓	Cancel	Apply

Keep the default settings and click **OK**.

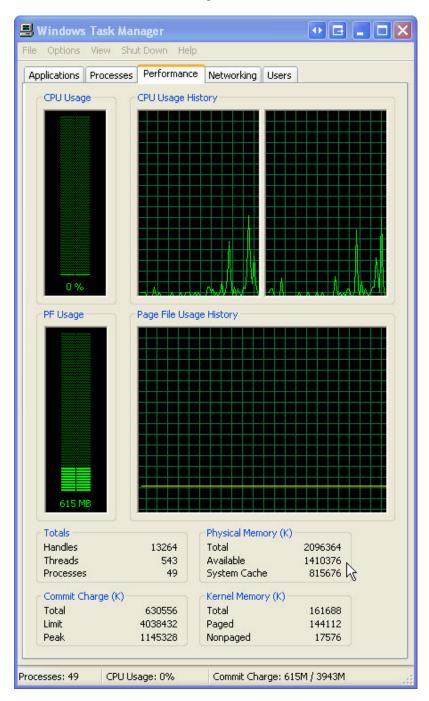
The "Performance" window opens.

📓 Performance 🔹 🖬 🗖 🔜				
👹 File Action View Favorites	Window Help			_ & ×
← → 🗈 🗷 🚯 😫				
Console Root	Name	Comment	Log File Type	Log File Name
System Monitor Performance Logs and Alerts Counter Logs Trace Logs Alerts Alerts	System Overview	This sample log provides an o	Text File ( Binary File	C:\PerfLogs\M C:\PerfLogs\S}
	<			

In the "Performance" window, select Counter Logs.

The Memory Counter log icon turns green once it has started.

Select the "Windows Task Manager" window.



What amount of Physical Memory (K) is available?

Subtract about 10 MB of the available memory. Example: 1410376 – 10000 = 1400376.

How much available memory is left over?

Make sure the "Performance" window is active.

🙀 Performance				
🗑 File Action View Favor	ites Window Help			_ & ×
← → 🗈 🖬 🔮 🗟 (	<b>3</b>   D   → ■			
Console Root	Name	Comment	Log File Type	Log File Name
System Monitor	ts System Overview	This sample log provides an o	Text File ( Binary File	C:\PerfLogs\M C:\PerfLogs\S\
New Alert Se	ttings FNSm			
Help				
	<			
Create a new performance alert co	nfiguration			

Right-click Alerts > New Alert Settings.

🙀 Performance			• •	
👹 File Action View Favorites	Window Help			_ & ×
← → 🗈 🖬 😰 🗟 😫				
Console Root	Name	Comment	Log File Type	Log File Name
System Monitor     System Monitor     Performance Logs and Alerts     Counter Logs     Trace Logs     Alerts	System Overview	This sample log provides an o	Text File ( Binary File	C:\PerfLogs\Mı C:\PerfLogs\S\
	New Alert Settings	▣?⊠		
Na	me:			
Memory Alert				
		OK Cancel		
	<			>
Create a new performance alert configu	ration			

In the Name field, type Memory Alert, then click OK.

The "Memory Alert" window appears.

Memory Alert	2 🛛
General Action Schedule	
This alert scan begins immed	fiately after you apply changes.
Comment:	
Counters:	
Alert when the value is:	Limit:
	Add Remove
Sample data every:	,
Interval: 5	
Run As: <default></default>	Set Password
	OK Cancel Apply

Click Add.

The "Add Counters" window opens.

Memory Alert	? 🛛
General Action Schedule	
Add Counters	? 🛛
O Use local computer counters Select counters from computer:	
VUOHN-DESKTOP	<b>~</b>
Performance object:	
Memory 🔽	
All counters	O All instances
<ul> <li>Select counters from list</li> </ul>	<ul> <li>Select instances from list:</li> </ul>
% Committed Bytes In Use       Available Bytes       Available KBytes       Available MBytes       Cache Bytes       Cache Bytes       Cache Bytes       Cache Bytes	
Add Explain	
	Close

Set the "Performance object" field to Memory.

Set the "Select counters from list" field to **Available MBytes**. Click **Add > Close**.

Fill in the window fields.

Aemory Alert	? 🗙
General Action Schedule	
This alert scan begins immediately after you apply changes.	
Comment:	
Counters:	
\UOHN-DESKTOP\Memory\Available MBytes	
Alert when the value is: Under Vinit: 140	00376
Add	Remove
Sample data every:	
Interval: 5 🗢 Units: seconds	~
Run As: <default> Set Password</default>	
OK Cancel	Apply

Set the following field values for the General tab:

Alert when the value is: **Under** Limit: **enter physical memory minus 10MB** (use the physical memory found in the Task Manager earlier in this lab). Example – 1400376 Interval: **5** Units: **seconds** 

Click the **Action** tab.

Memory Alert 🔹 🔀
General Action Schedule
When an alert is triggered:
Log an entry in the application event log
Send a network message to:
Start performance data log:
Run this program:
Command Line Arguments
Example command line arguments:
"Memory Alert,2009/12/12-13:23:18.156,\Object\Counter,20.0,over 10.0"
OK Cancel Apply

Click **OK** to keep default settings.

In the "Performance" window, select Alerts.

📓 Performance			• = = = 🗙
👹 File Action View Favorites	Window Help		_ & ×
← → 🗈 🗷 🚯 🔮			
Console Root	Name	Comment	
System Monitor Performance Logs and Alerts Counter Logs Trace Logs Alerts	Memory Alert		
	<		>

How can you tell that the Memory Alert has started?

To force the computer to use some of the available memory, open and close a browser. Example: Internet Explorer or FireFox.

Right-click the **Memory Alert** icon **> Stop**.

Rerformance			
🗑 File Action View Favorites	Window Help		<u>_ 8 ×</u>
← → 🗈 💌 🗙 📽 🗟	8 🔒 🗅 🕨		
Console Root	Name	Comment	
୍ଥି System Monitor ଚାର୍ଣ୍ଣ Performance Logs and Alerts	Memory Alert	Start	
- 🔯 Counter Logs		Stop N	
Alerts		Save Sottings As	
		Delete	
	-	Refresh	
		Properties	
		Help	]
			-
	<		>
Stop the selected log or alert			

Notice the "Memory Alert" icon has changed to a red color.

📓 Performance			•	▣ - □ 🛛
📷 File Action View Favorites	Window Help			_ 8 ×
⇔ → 🗈 🖬 🖗 🚱 🔮				
Console Root System Monitor Performance Logs and Alerts Counter Logs Trace Logs Alerts	Name Memory Alert	Comment		
	<u>  &lt;  </u>			

Select Counter Logs.

File Action View Favorites Window Help      Image: System Monitor       System Monitor          Performance Logs and Alerts          Counter Logs          Trace Logs  Onsole Root Cost Root  Counter Logs Trace Logs Alerts  Memory Counter Text File (, C:\PerfLogs\M Trace Logs Alerts Memory Counter Text File (, C:\PerfLogs\M Text File (, C:\	🗑 Performance			• •	
Console Root System Monitor Performance Logs and Alerts Counter Logs Trace Logs Alerts Name Comment Log File Type Log File Name System Overview This sample log provides an o Binary File C:\PerfLogs\M Text File ( C:\PerfLogs\M	🗑 File Action View Favorites	Window Help			_ & ×
System Monitor Performance Logs and Alerts Counter Logs Trace Logs Alerts System Overview This sample log provides an o Binary File C:\PerfLogs\5\ Memory Counter Text File ( C:\PerfLogs\M	← → 🗈 📧 🔂 🔂				
Performance Logs and Alerts     Counter Logs     Trace Logs     Alerts     Alerts		Name	Comment	Log File Type	Log File Name
	Performance Logs and Alerts     Counter Logs     Trace Logs		This sample log provides an o		
		1			

Right-click the Memory Counter icon and select Stop.

How can you tell the Memory Counter has stopped?

Make sure the "Event Viewer" window is active.

Select Application, and double-click the event at the top of the list.

Event Viewer	Event Properties ?	×٤
File       Action       View       Help            ←         →           Eie          Eie	Event Date: 12/12/2009 Source: SysmonLog Time: 1:53:22 PM Category: None Type: Information Event ID: 2031 User: N/A Computer: JOHN-DESKTOP Description: Counter: \\UDHN-DESKTOP\Memory\Available MBytes has tripped its alert threshold. The counter value of 1352 is under the limit value of 1400376 For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp. Data:  Bytes \Words	
	OK Cancel Apply	

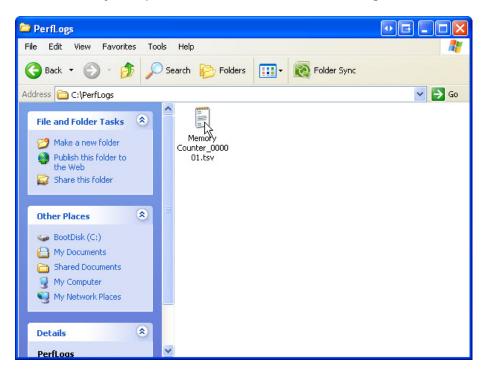
Does the event indicate that the available MBytes has tripped the alert threshold?

If you answered yes to the above question, what was the counter value that tripped the alert event?

If you answered no, click the down arrow a few times until you find the alert event. If you do not find an alert event ask the instructor for assistance.

Close the "Event Properties" window, click OK.

Click Start > My Computer > double-click drive C: > PerfLogs.



Double-click Memory Counter file.

Memory Counter_000001.tsv - Not	epad 🛛 💀 🖬 🗖 🔀
File Edit Format View Help ["(PDH-TSV 4.0) (Pacific Stand "\\JOHN-DESKTOP\Memory\Availa "12/12/2009 13:13:33.859" "12/12/2009 13:13:38.859"	ble MBytes" "1368" "1370"
"12/12/2009 13:13:43.859"	"1368"
"12/12/2009 13:13:48.859"	"1370"
"12/12/2009 13:13:53.859"	"1370"
"12/12/2009 13:13:58.859"	"1370"
"12/12/2009 13:14:03.859"	"1369"
"12/12/2009 13:14:08.859"	"1369"
"12/12/2009 13:14:13.859"	"1367"
"12/12/2009 13:14:18.859"	"1369"
"12/12/2009 13:14:23.859"	"1369"
"12/12/2009 13:14:23.859"	"1369"
"12/12/2009 13:14:28.859"	"1369"
"12/12/2009 13:14:33.859"	"1369"
"12/12/2009 13:14:38.859"	"1369"
"12/12/2009 13:14:43.859"	"1369"
"12/12/2009 13:14:48.859"	"1369"
"12/12/2009 13:14:53.859"	"1373"
"12/12/2009 13:14:58.859"	"1373"
"12/12/2009 13:15:03.859"	"1373"
"12/12/2009 13:15:03.859" "12/12/2009 13:15:08.859" "12/12/2009 13:15:13.859" "12/12/2009 13:15:18.859" "12/12/2009 13:15:23.859" "12/12/2009 13:15:28.859"	"1374" "1374" "1374" "1374" "1374"
"12/12/2009 13:15:33.859"	"1374"
"12/12/2009 13:15:38.859"	"1374"
"12/12/2009 13:15:43.859"	"1374"
"12/12/2009 13:15:48.859"	"1374"

What does the column on the right show?

Close the Memory Counter file, PerfLogs folder, and Windows Task Manager.

In the "Event Viewer" window click **Application > Action > Clear All Events**. Click **No** when you are asked to save the events to a file.

	Action View Help								
-	Open Log File	•	ß						
Ev	Save Log File As		Application 79	Application 79 event(s)					
	New Log View Clear all Events		Туре	Date	Time	Source	Category	Ever	
4	1		Information	12/12/2009	1:53:22 PM	SysmonLog	None	203	
1	Rename		Information	12/12/2009	1:53:17 PM	SysmonLog	None	203	
13	Refresh		Information	12/12/2009	1:53:12 PM	SysmonLog	None	203	
	Export List		Information	12/12/2009	1:53:07 PM	SysmonLog	None	203	
2	Properties		Information	12/12/2009	1:53:02 PM	SysmonLog	None	203	
-		-1-	Information	12/12/2009	1:52:57 PM	SysmonLog	None	203	
	Help		Information	12/12/2009	1:52:52 PM	SysmonLog	None	203	
		_	Information	12/12/2009	1:52:47 PM	SysmonLog	None	203:	
			Information	12/12/2009	1:52:42 PM	SysmonLog	None	203	
			Information	12/12/2009	1:52:37 PM	SysmonLog	None	203	
			Information	12/12/2009	1:52:32 PM	SysmonLog	None	203:	
			Information	12/12/2009	1:52:27 PM	SysmonLog	None	203	
			Information	12/12/2009	1:52:22 PM	SysmonLog	None	203	
			Information	12/12/2009	1:52:17 PM	SysmonLog	None	203	
			Information	12/12/2009	1:52:12 PM	SysmonLog	None	203	
			Information	12/12/2009	1:52:07 PM	SysmonLog	None	203:	
			Information	12/12/2009	1:52:02 PM	SysmonLog	None	203:	
			<li>Information</li>	12/12/2009	1:51:57 PM	Sysmool on	None	203	

In the "Performance" window, click **Counter Logs >** right-click **Memory Counter > Delete**.

🗑 Performance 💿 🖻 🗖							
👹 File Action View Favorites	Window Help			_ & ×			
← → 🗈 💌 🗙 😭 🗟	) 😫 🗋 🕨 🔳						
Console Root	Name	Comment	Log File Type	Log File Name			
System Monitor	System Overview	This sample log provides an o	Binary File	C:\PerfLogs\S			
Performance Logs and Alerts     Counter Logs     Trace Logs     Alerts     Alerts	Memory Counter	Start Stop Save Settings As Delete Refresh Properties Help	Text File (	C:\PerfLogs\M			
Deletes the current selection.	<			>			

Select Alerts > Memory Alert > right-click Memory Alert > Delete.

Open drive C:.

Right-click the **PerfLogs** folder.

Click **Delete > Yes**.

Close all open windows.