

Lab - Monitoring Servers

Overview

Server Monitoring is the process of monitoring a server's resources including CPU Usage, Memory Consumption, I/O, Network, Disk Usage, Process, etc. Server Monitoring helps to understand a server's system resource usage which can help better plan for growth, upgrades and provide a better end-user experience.

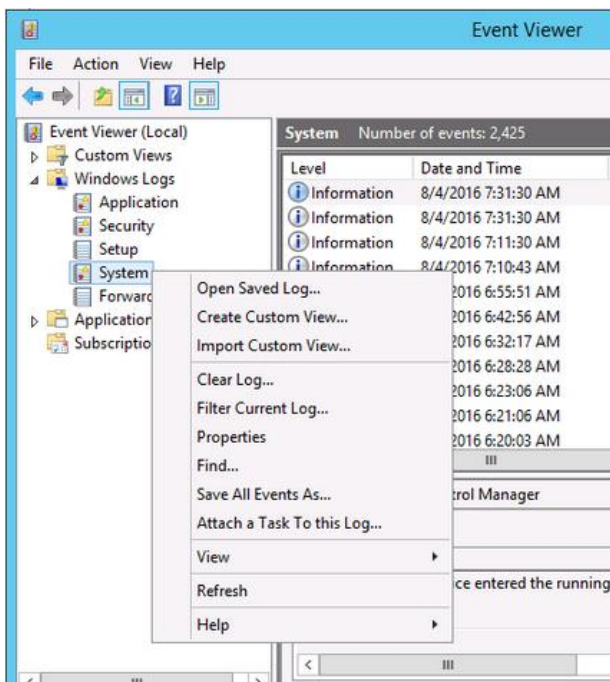
Though this lab is built around a 2012 Server, the s shown in how monitor the system could be applied to just about any Windows operating system with some slight modifications.

Hardware Requirements:

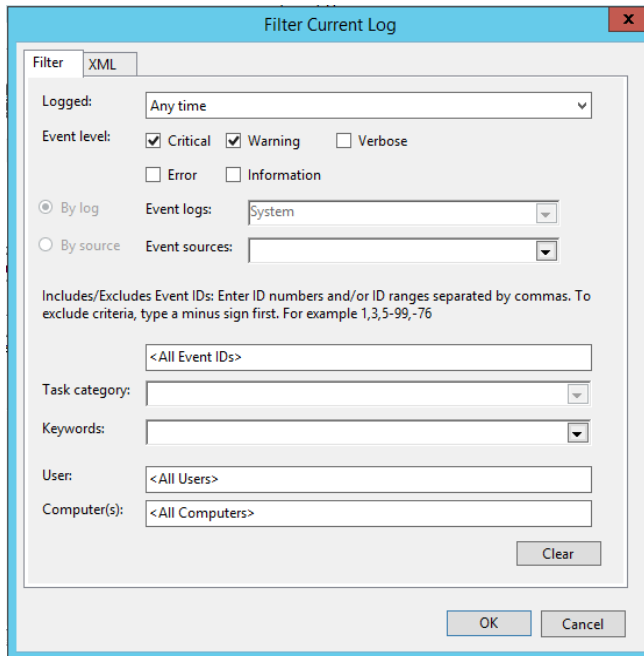
- A virtual install of Server 2012 r2 either as a member server or a domain controller.

Using Event Viewer

- Login to your server as administrator.
- Open Server Manager > Tools > Event Viewer
- Expand the Windows Logs folder by clicking the arrow next to Windows Logs and right-click on the System Log and click Filter Current Log.



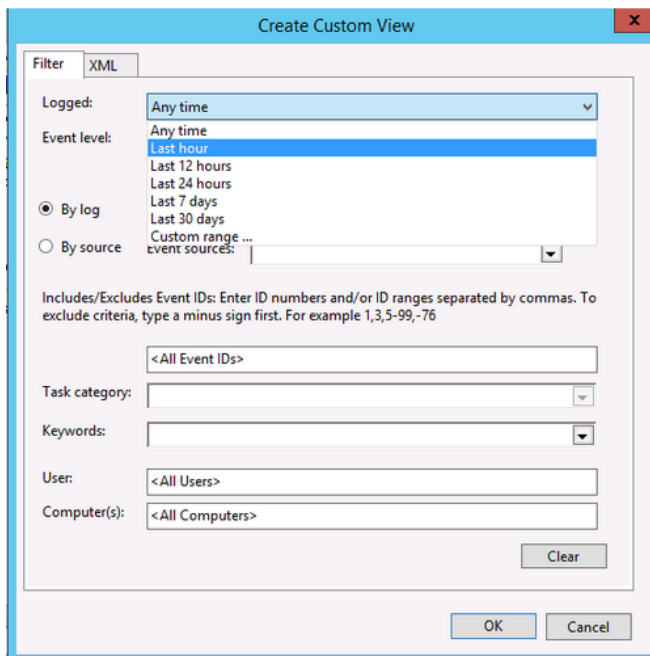
On the *Filter Current Log* page, choose the Critical and Warning check boxes next to Event Level area. Then click OK.



The screenshot shows the 'Filter Current Log' dialog box. It has two tabs: 'Filter' and 'XML'. The 'Filter' tab is active. The 'Logged:' dropdown is set to 'Any time'. The 'Event level:' section has checkboxes for 'Critical' (checked), 'Warning' (checked), 'Error' (unchecked), and 'Verbose' (unchecked). The 'By log' radio button is selected, and the 'Event logs:' dropdown is set to 'System'. The 'By source' radio button is unselected, and the 'Event sources:' dropdown is empty. Below these, there is a text box for 'Includes/Excludes Event IDs' with the placeholder '<All Event IDs>'. There are also dropdowns for 'Task category:', 'Keywords:', 'User:' (set to '<All Users>'), and 'Computer(s):' (set to '<All Computers>'). A 'Clear' button is at the bottom right of the main area. At the very bottom are 'OK' and 'Cancel' buttons.

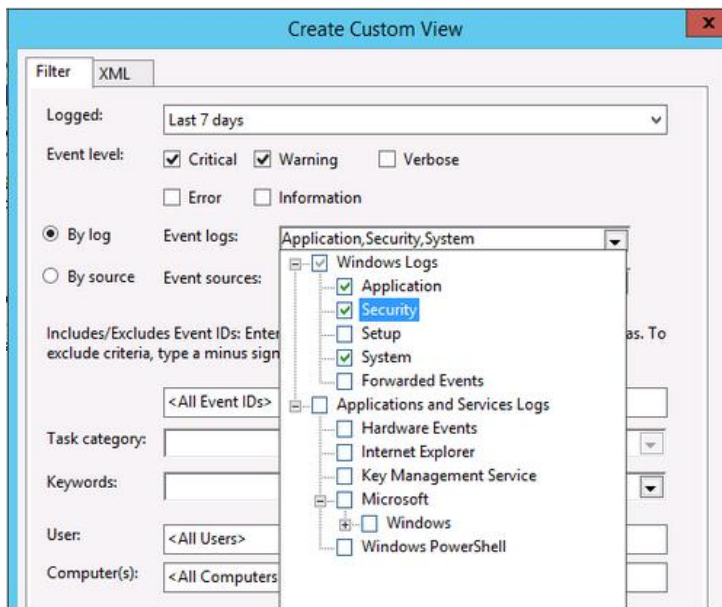
On the *Action menu* on the taskbar or on the far-right pane, click Create Custom View.

On the *Logged drop-down box*, click Last 7 days.

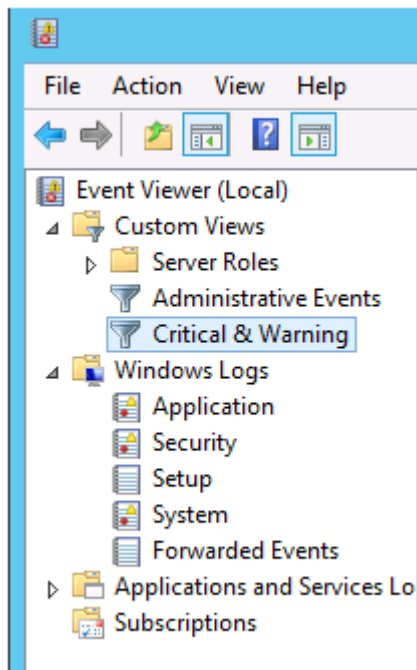


The screenshot shows the 'Create Custom View' dialog box. It has two tabs: 'Filter' and 'XML'. The 'Filter' tab is active. The 'Logged:' dropdown is open, showing a list of options: 'Any time', 'Last hour', 'Last 12 hours', 'Last 24 hours', 'Last 7 days' (which is highlighted in blue), 'Last 30 days', and 'Custom range ...'. The 'Event level:' section has checkboxes for 'Critical' (checked), 'Warning' (checked), 'Error' (unchecked), and 'Verbose' (unchecked). The 'By log' radio button is selected, and the 'Event logs:' dropdown is set to 'System'. The 'By source' radio button is unselected, and the 'Event sources:' dropdown is empty. Below these, there is a text box for 'Includes/Excludes Event IDs' with the placeholder '<All Event IDs>'. There are also dropdowns for 'Task category:', 'Keywords:', 'User:' (set to '<All Users>'), and 'Computer(s):' (set to '<All Computers>'). A 'Clear' button is at the bottom right of the main area. At the very bottom are 'OK' and 'Cancel' buttons.

Leave the *By Log option* selected and in the Event logs drop-down box, choose the Application, Security, and System check boxes. The click OK.



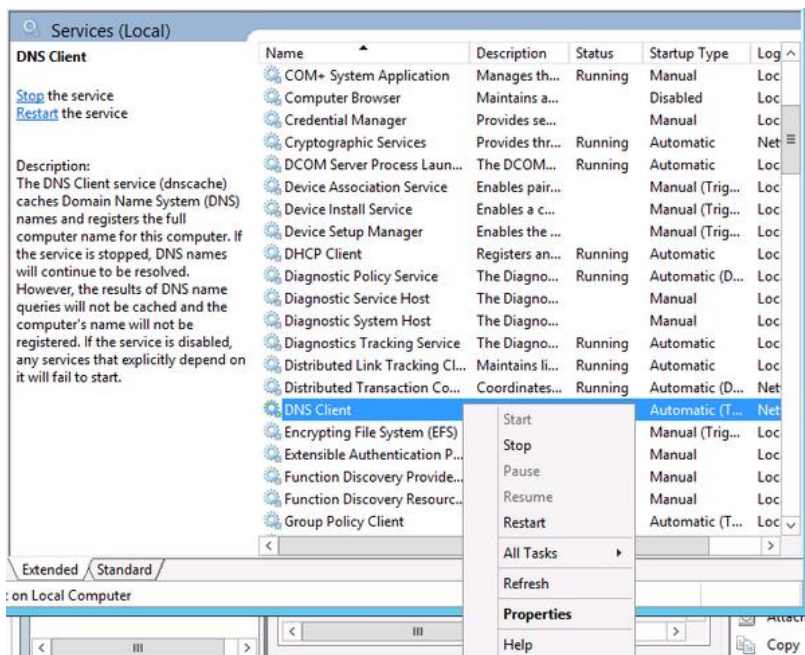
When the *Save Filter to Custom View* box opens, type *Critical Warning*. Then click OK. The *Critical & Warning* custom view is added to Custom View folder.



Adding a Task to an Event

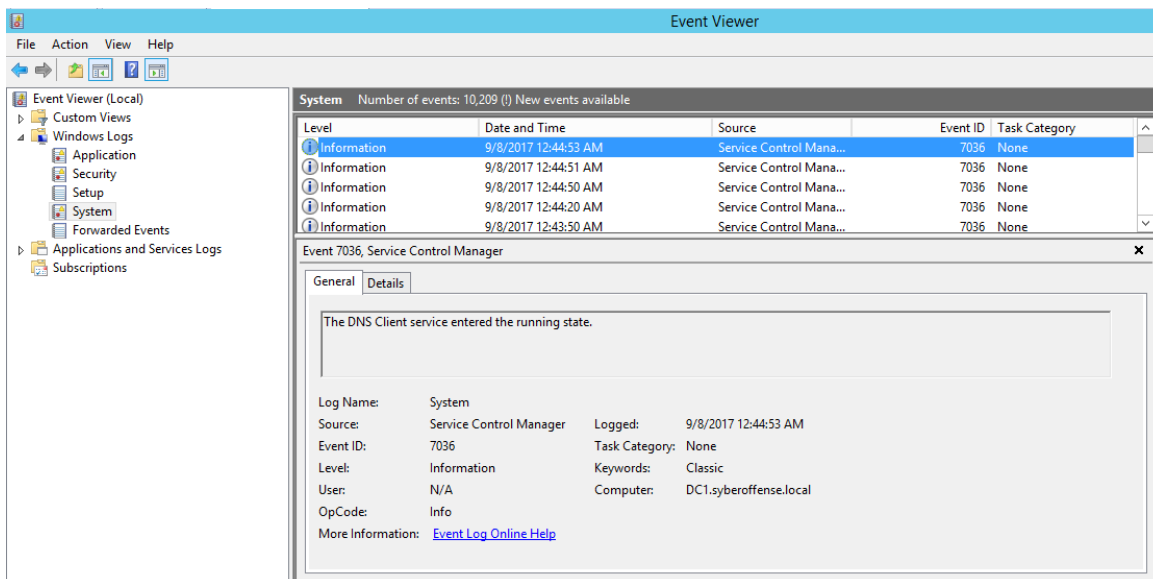
Open Server Manager and click on Tools > Services.

Scroll down in Services to DNS Client and right-click on it and click Restart.

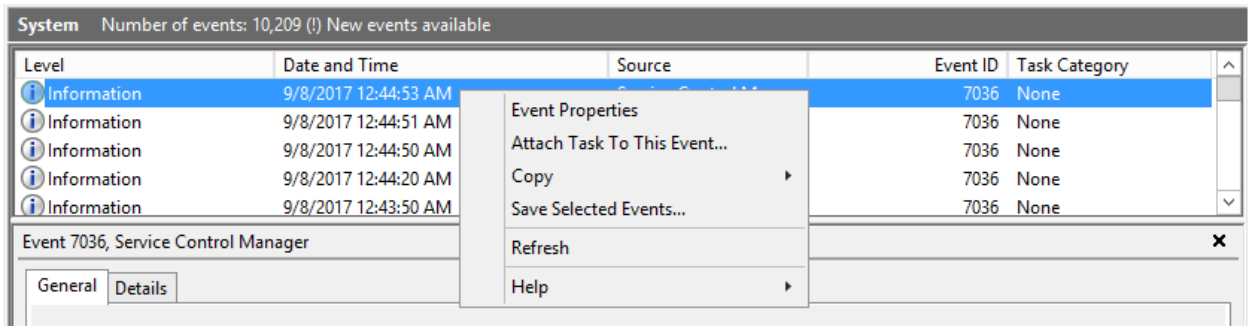


Open Event Viewer by clicking Tools > Event Manager in Server Manager.

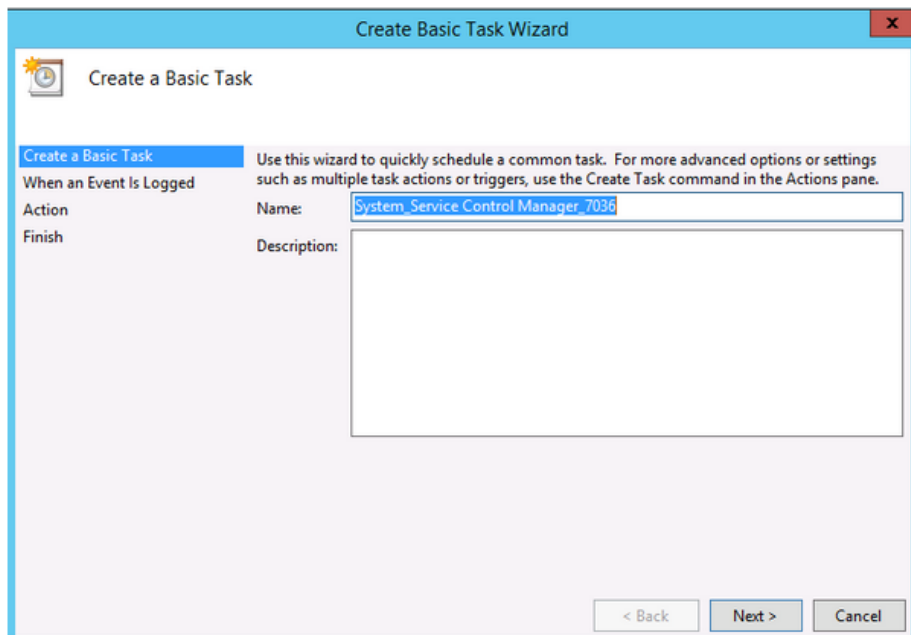
You should see 2 new entries in the *System Logs* with the Event ID of 7036 (Scroll over to the right to see the Event ID).



Right-click on the *Event* and choose Attach Task to This Event.



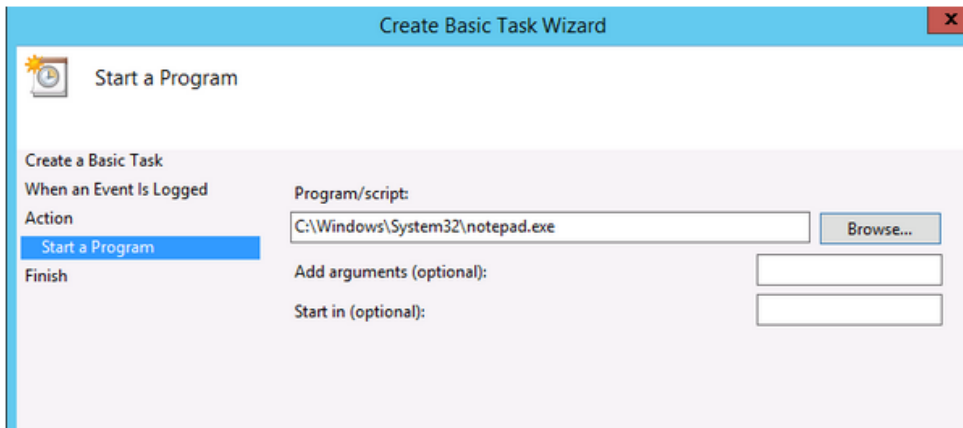
When the *Create Basic Task Wizard* opens, click Next.



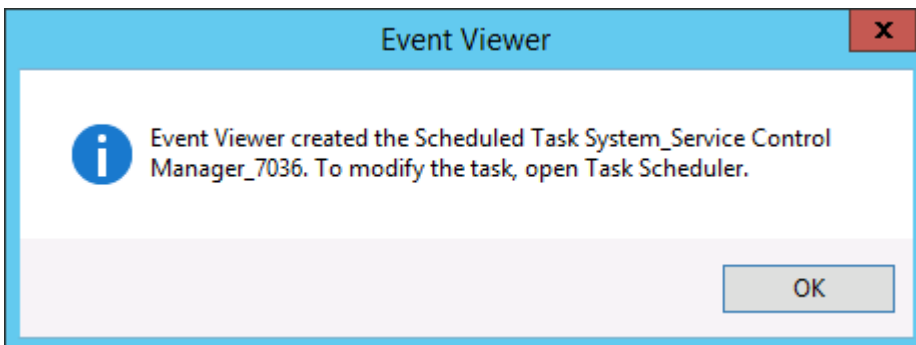
The *When a Specific Event Is Logged* page opens, then click Next.

On the *Action* page, make sure Start a Program is chosen and click Next.

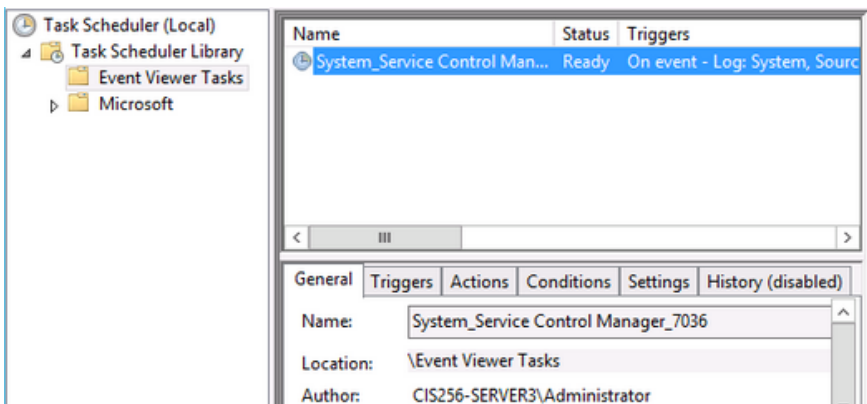
On the *Start, a Program* page, click the browse button and choose Notepad.exe or type the location (C:\Windows\System32\notepad.exe). Then click Next.



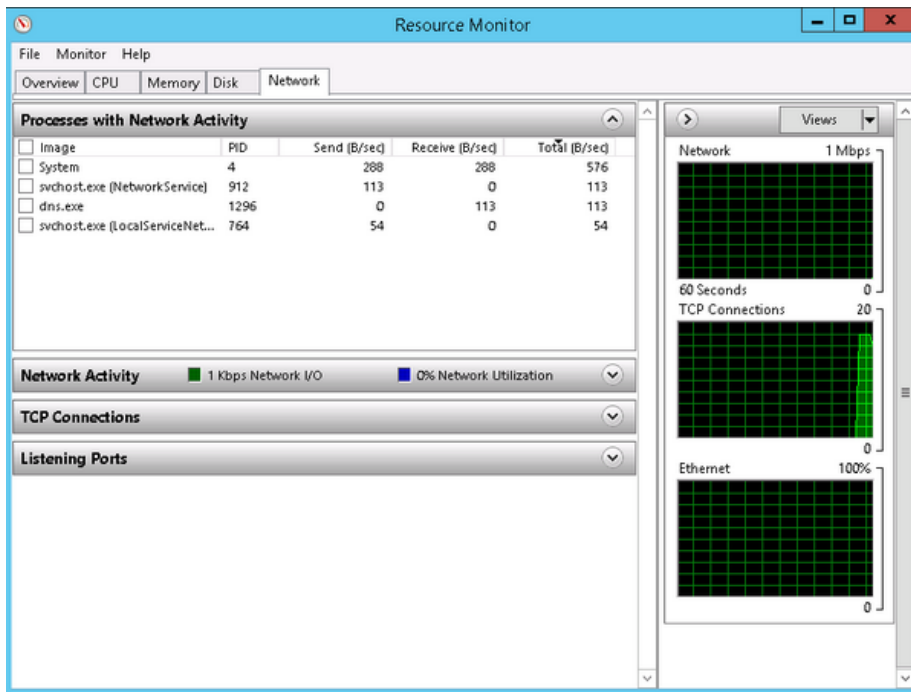
On the *Summary* page, click **Finish** and OK if a warning opens up.



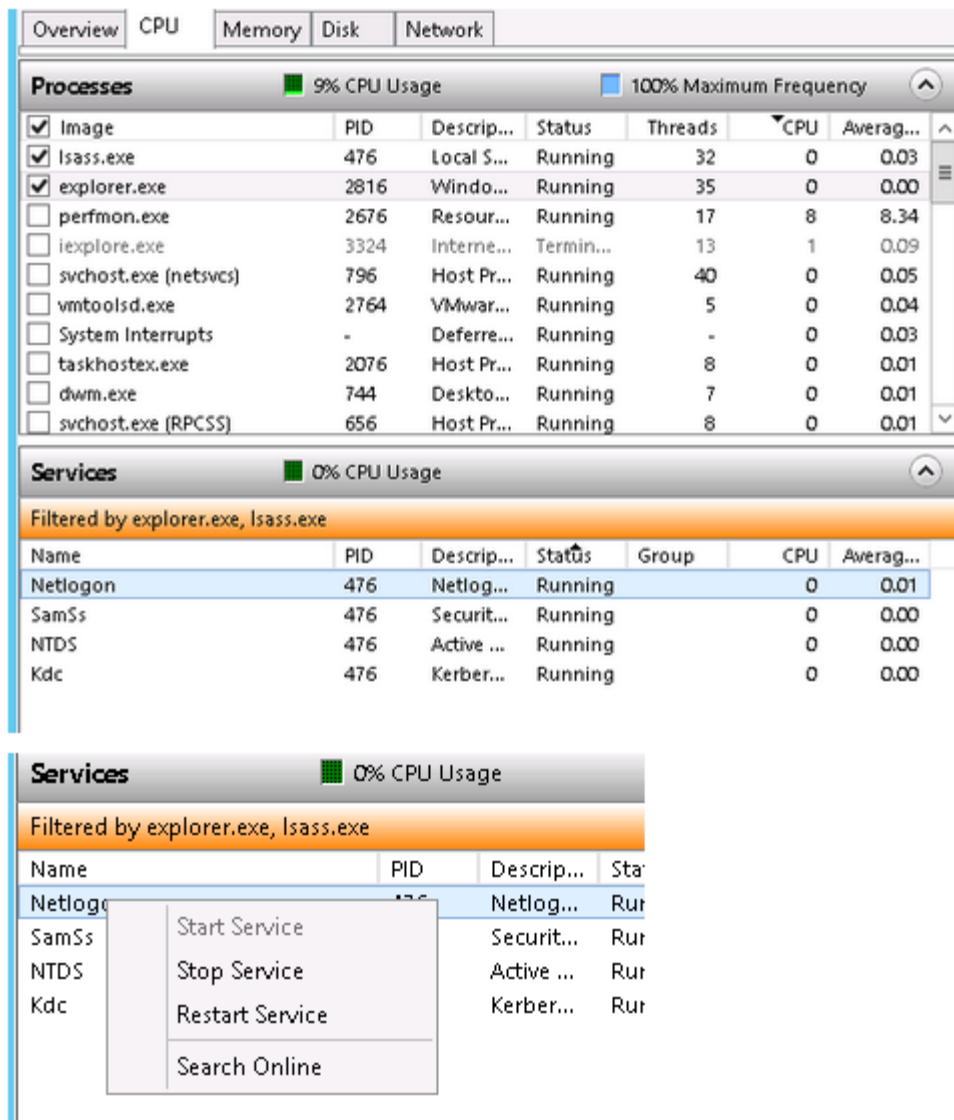
- Go to the Service page in Tools in Server Manager, and click on DNS Client. click Restart. Notepad should open.
- On Server Manager, click Tools > Task Scheduler.
- Expand Task Scheduler Library and click Event Viewer Tasks.
- Right-click on the System Service Control Manager_7036 and click Delete. Then Yes.



- Close any open windows from this lab.
- Using Resource Monitor
- From Server Manager, click Tools > Resource Monitor.

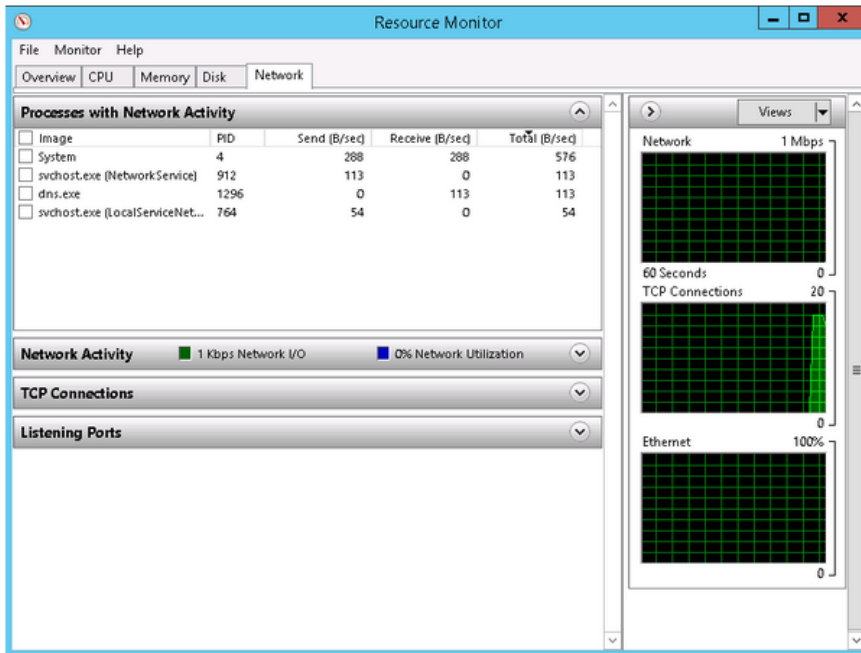


- Click the CPU tab.
- In the Process section, click on the title of Image to make the listing alphabetically.
- Click on the CPU column name to sort processes by CPU consumption.
- Click on the CPU tab, In the Process section, in Image column, click explorer.exe and Isass.exe.
- Click on *Services bar* and look at the process hosted by the selected services.
- Right-click on Netlogon and click Search Online. A webpage of Internet links will open with information about the service.

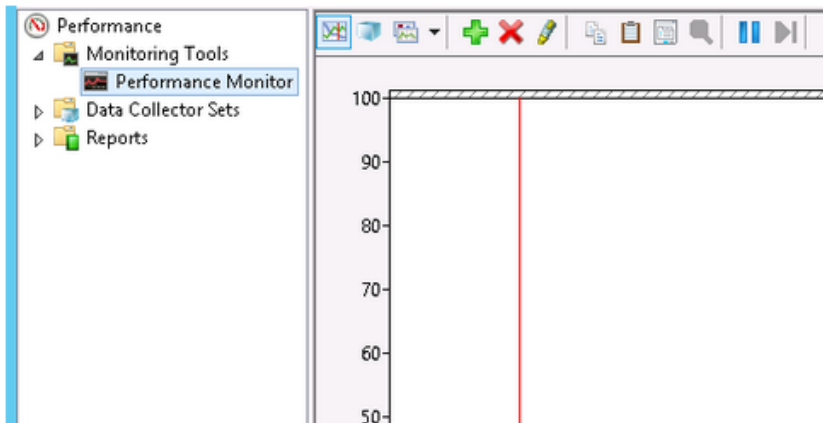


Using Performance Monitor

From Server Manager, click Tools > Performance Monitor.



Click on Monitoring Tools\Performance Monitor.



Overview CPU Memory Disk Network

Processes 9% CPU Usage 100% Maximum Frequency

Image	PID	Descrip...	Status	Threads	CPU	Averag...
<input checked="" type="checkbox"/> Image						
<input checked="" type="checkbox"/> lsass.exe	476	Local S...	Running	32	0	0.03
<input checked="" type="checkbox"/> explorer.exe	2816	Windo...	Running	35	0	0.00
<input type="checkbox"/> perfmom.exe	2676	Resour...	Running	17	8	8.34
<input type="checkbox"/> iexplore.exe	3324	Interne...	Termin...	13	1	0.09
<input type="checkbox"/> svchost.exe (netsvc)	796	Host Pr...	Running	40	0	0.05
<input type="checkbox"/> vmtoolsd.exe	2764	VMwar...	Running	5	0	0.04
<input type="checkbox"/> System Interrupts	-	Deferre...	Running	-	0	0.03
<input type="checkbox"/> taskhost.exe	2076	Host Pr...	Running	8	0	0.01
<input type="checkbox"/> dwm.exe	744	Deskto...	Running	7	0	0.01
<input type="checkbox"/> svchost.exe (RPCSS)	656	Host Pr...	Running	8	0	0.01

Services 0% CPU Usage

Filtered by explorer.exe, lsass.exe

Name	PID	Descrip...	Status	Group	CPU	Averag...
Netlogon	476	Netlog...	Running		0	0.01
SamSs	476	Securit...	Running		0	0.00
NTDS	476	Active ...	Running		0	0.00
Kdc	476	Kerber...	Running		0	0.00

Services 0% CPU Usage

Filtered by explorer.exe, lsass.exe

Name	PID	Descrip...	Sta
Netlogon	476	Netlog...	Rur
SamSs		Securit...	Rur
NTDS		Active ...	Rur
Kdc		Kerber...	Rur

Start Service

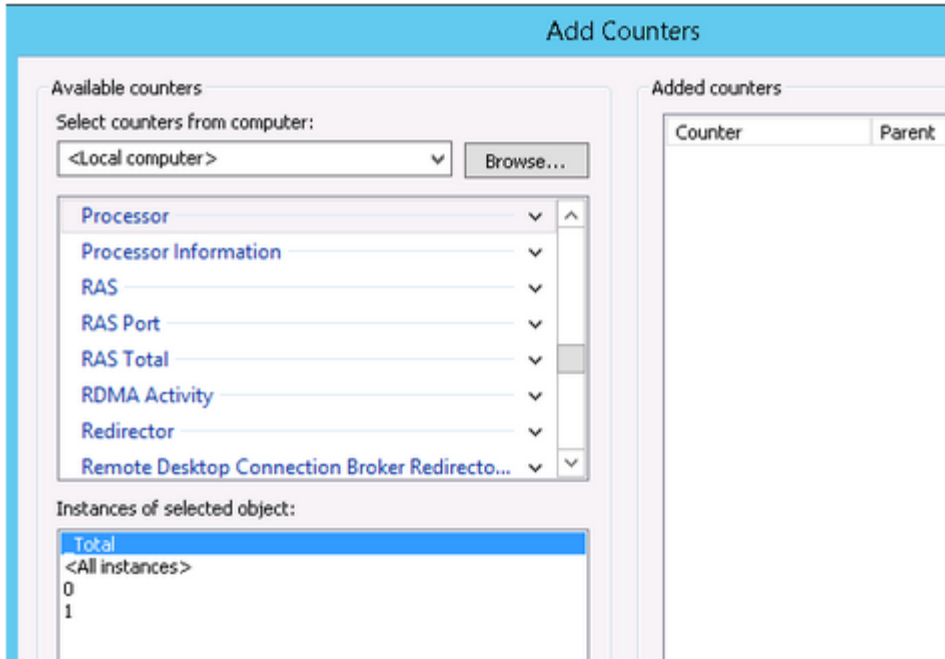
Stop Service

Restart Service

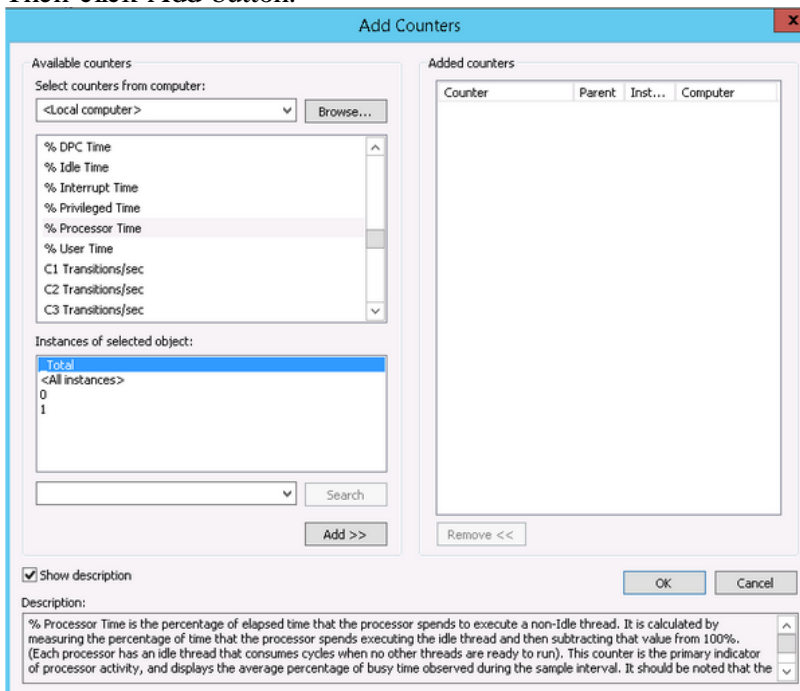
Search Online

Click % Processor Time at the bottom of the screen and click the **red X** at the top of the screen to delete.

Click the *Add button (Green Plus(+)) icon next to the Red X* to add a counter. The Add Counter page opens.



On Available Counters, open Processors by clicking on the down arrow to expand the selection and click on % Processor Time at the bottom, click the checkbox that says Show Description and the description of the counter will be displayed at the bottom of the screen. Then click Add button.

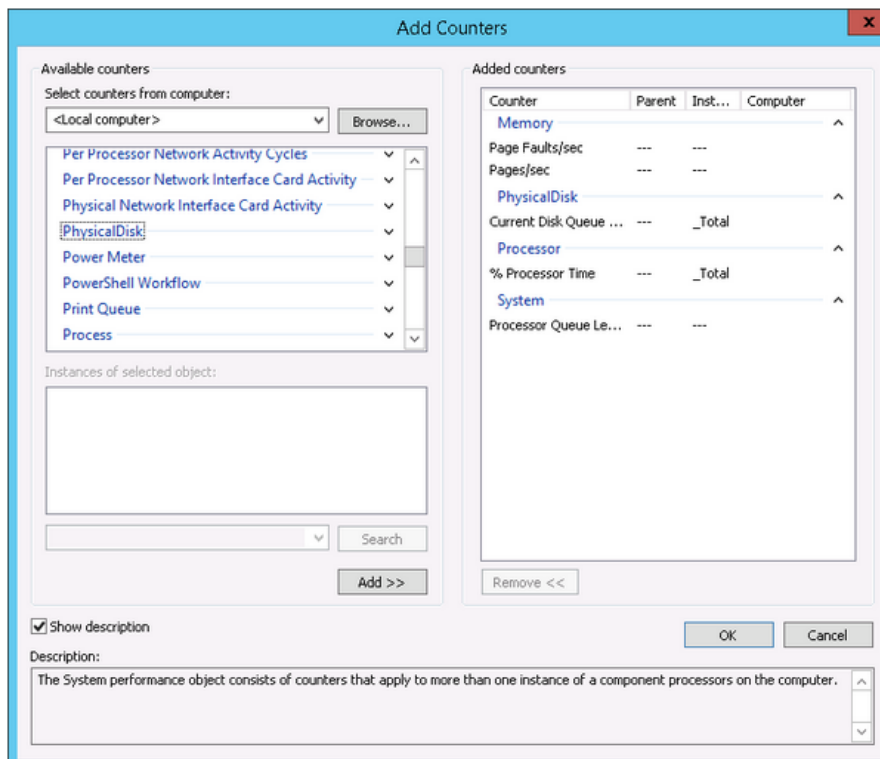


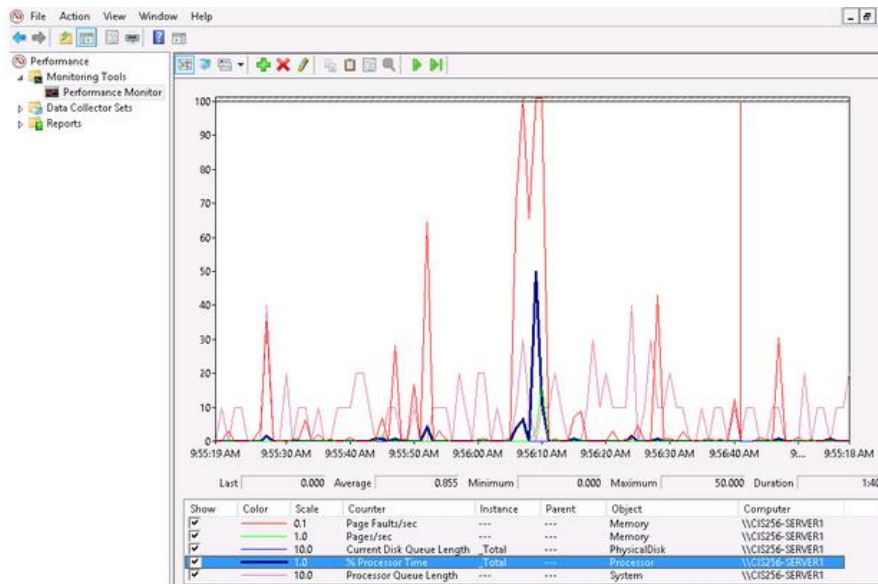
Add the following:

- a. System: Processor Queue Length

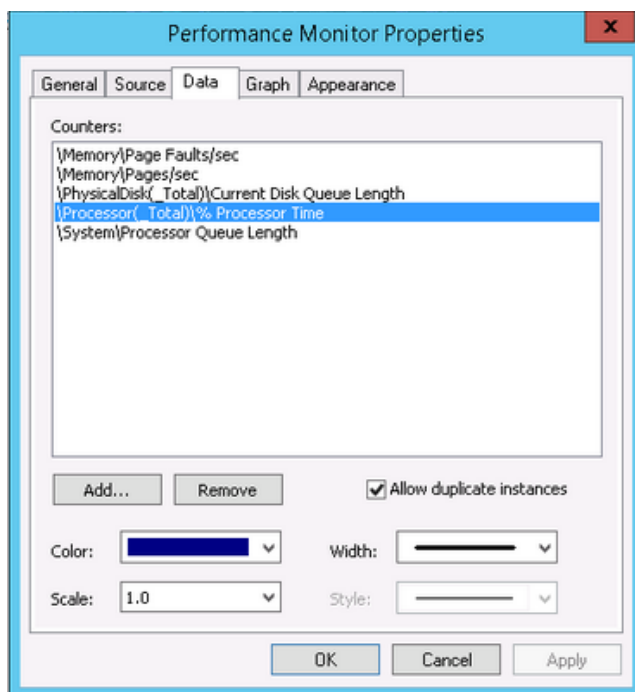
- Add available counters (blue text)
- Highlight system
- Click down arrow
- Choose Processor Queue Length (black text)
- Click Add
- Close the options by clicking the up arrow.
 - a. Memory:Page Faults/sec
 - b. Memory:Pages/sec
 - c. PhysicalDisk:Current Disk Queue Length

Click OK on Add Counters page.



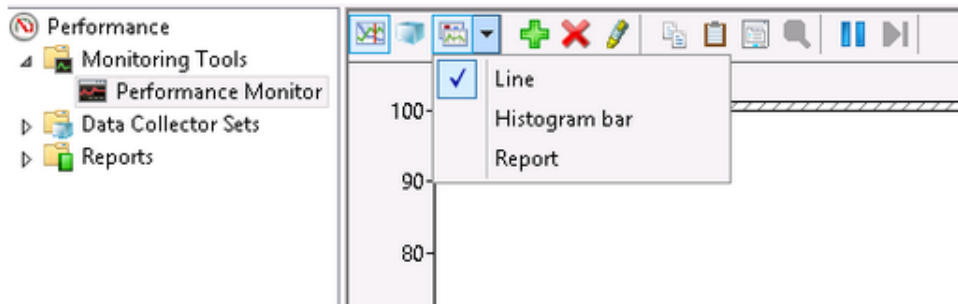


Click on %Processor Time at bottom and right click on Properties.

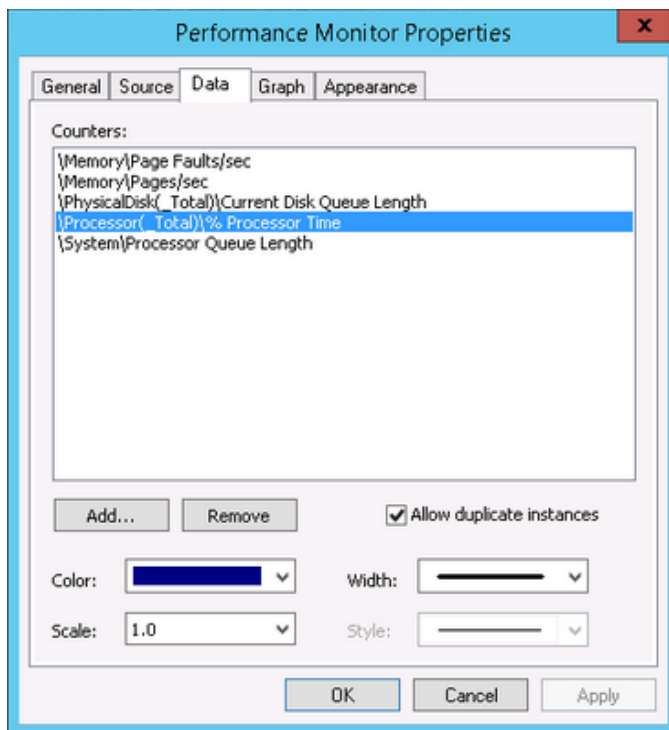


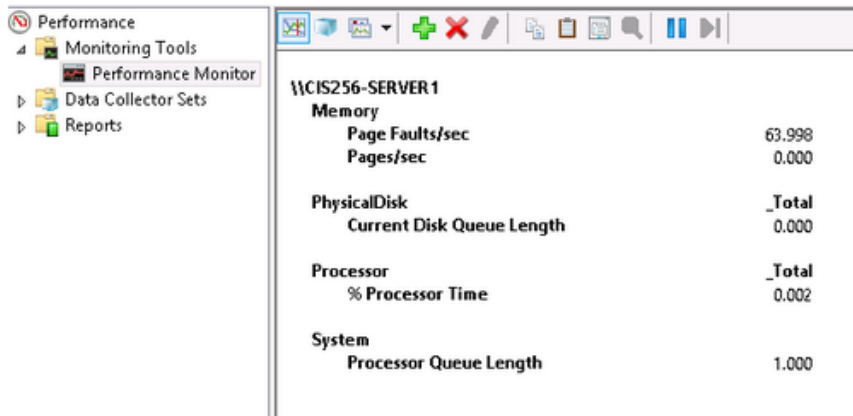
Change the color to a dark blue color and change the width to a heavy line. Click OK.

Click on the taskbar at the top of graph screen on 3rd icon from the left (one with a down arrow next to it) and click histogram bar report.

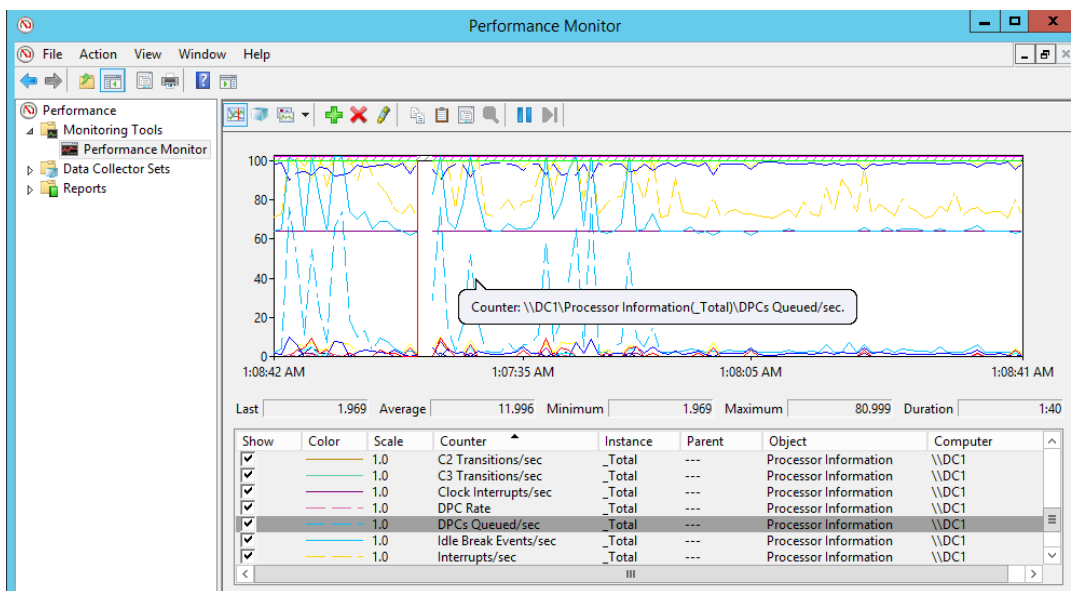


Click on the report type of graph.





Click on any spike in the graph, and it tells you the name of the counter.



Summary

PerfMon and ResourceMon have with windows since Windows 98. When you're first learning the operating system, it's nice to be able to see under the hood, kick the tires and rev the engine but after a while, you start to realize there are a lot of third-party monitoring tools on the market and they all do pretty much the same thing. Of all the monitoring tools, the event viewer is the one that has proven itself most useful.

End of the lab!