

## Windows 2003 Performance Monitor

The performance monitor, or system monitor, is a utility used to track a range of processes and give a real time graphical display of the results, on a Windows 2003 system. This tool can be used to assist you with the planning of upgrades, tracking of processes that need to be optimized, monitoring results of tuning and configuration scenarios, and the understanding of a workload and its effect on resource usage to identify bottlenecks.

Bottlenecks can occur on practically any element of the network and may be caused by a malfunctioning resource, the system not having enough resources, a program that dominates a particular resource. In fact, 40% network utilization is considered a bottleneck.

Using perfmon will help to identify these bottlenecks and allow you to take action.

It can be opened by navigating to the performance icon in the administrative tools folder in the control panel, from the start menu or by typing perfmon.msc in the run box.

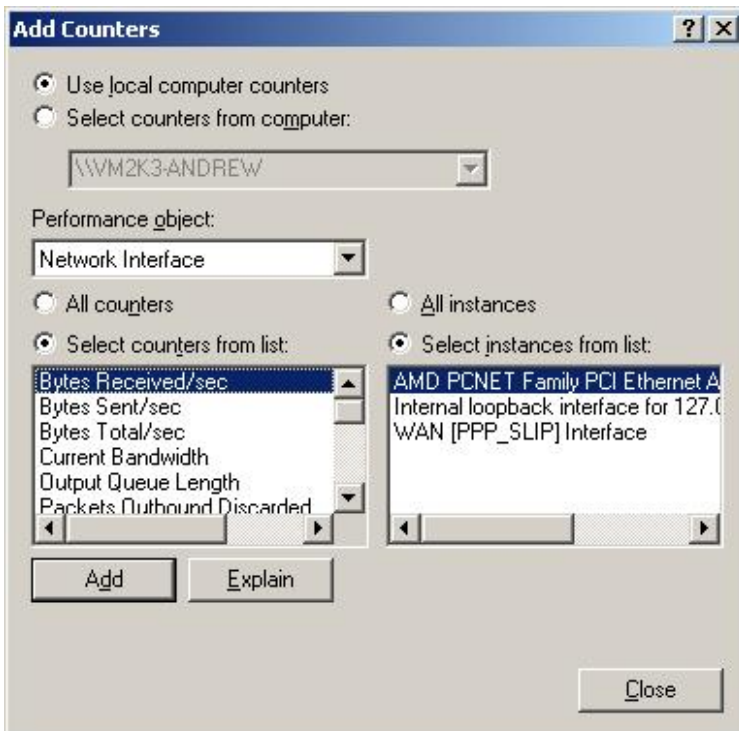
## System Monitor

### Adding a counter

Right click anywhere on the graph and choose Add Counter.

The Add Counter box consists of the following options:

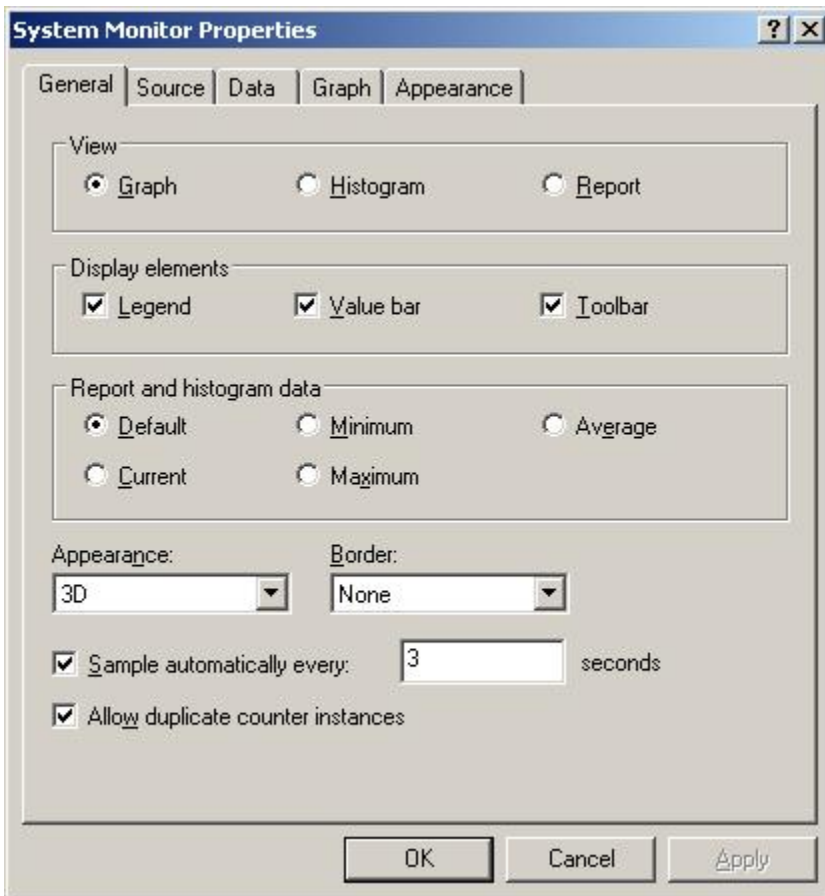
- **Computer:** The source system of the object. You can choose to select the local computer or another computer on your network - type \\computer\_name in the appropriate box.
- **Object:** The subsystem of interest. This refers to the virtual part of the computer that you want to monitor. Memory, Processor or Network Interface, for example.
- **Counter:** The aspect of performance of interest. This refers to what parts of the object you want to monitor - they differ depending on the object.
- **Instance:** The specific object to be measured when multiple objects of the same type exist on a single system. For example, if you go to the Process performance object, the instances list will display all the active processes on the specified computer.



The above image shows the Add Counters window.

## System monitor properties

Right click anywhere on the graph and choose Properties. This brings up the System Monitor Properties window that will allow you to customize the appearance and settings. You can change the view to graph, report or histogram style, the monitoring time interval and the colour of the counter lines, amongst others.



The above screenshots shows the general tab of the system monitor properties.

## Using the monitor for network related performance.

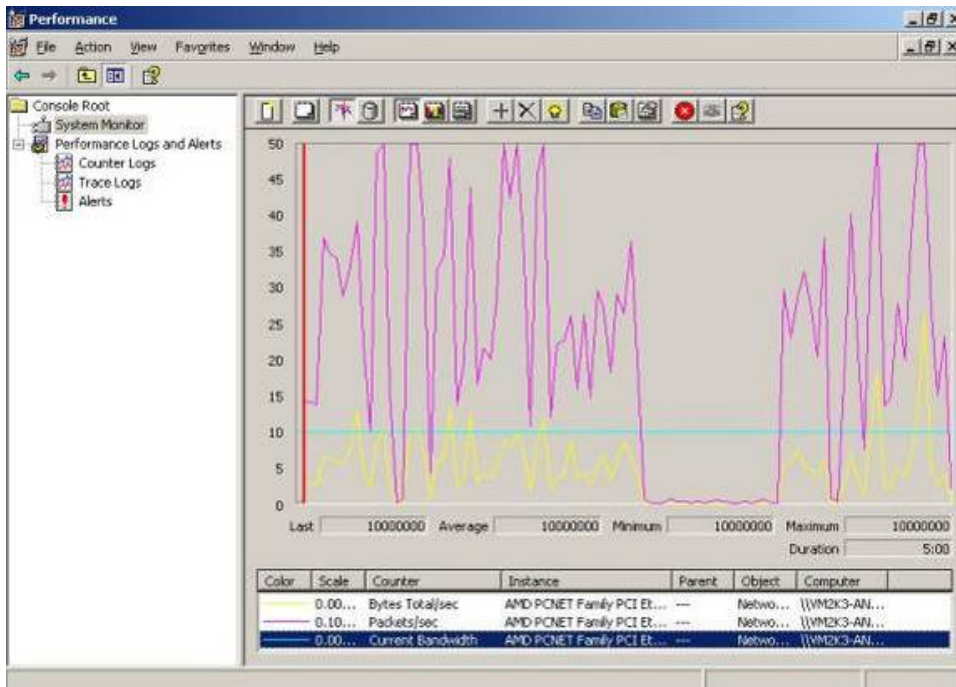
The performance monitor can be a great tool to help with investigating the performance of your network. You are able to monitor things such as the Network Interface, TCP, UDP packet flow, terminal services sessions, and ICMP, amongst others. You can then compare the collected data and keep it as a record or use it for problem analysis.

In my example I have chosen to use the Network Interface as the performance object.  
The following counters were added:

Current Bandwidth – to display the amount of bandwidth the network interface has.  
Packets/Sec – to display the amount of packets transferred per second.  
Bytes Total/Sec – to display the total amount of bytes per second.

The image below displays a graph of network activity that took place within the space of five minutes. The purple line represents the number of packets per second, the yellow line represents the total bytes per second and the light green line shows how much bandwidth is available.

To simulate this activity I navigated to a share on another computer on the network and browsed through the folders.



## Performance Logs and Alerts

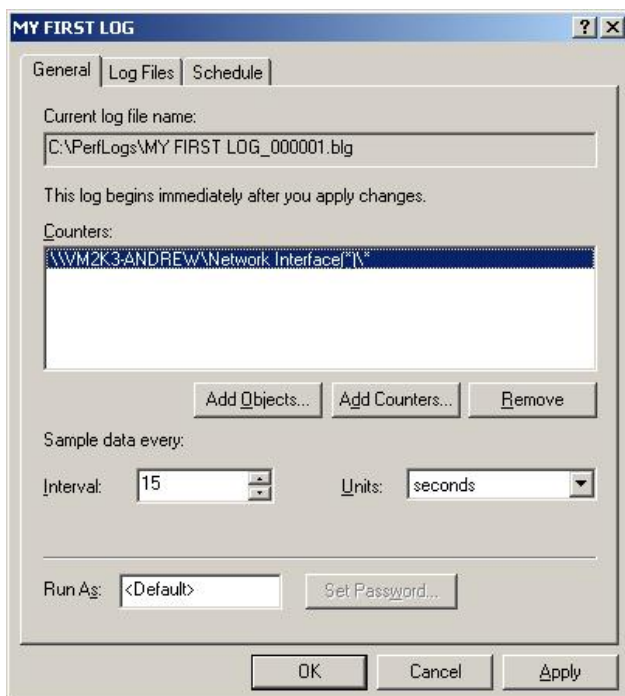
With the use of logs you are able to capture data that you can analyze later. Logged counter data information can be exported to spreadsheets and databases for future review and reporting. Alerts allow you to set an action that will be performed when specified counters reach a given value. These actions include sending a network message, executing a batch file, recording an item in the application log of the event viewer, and to start logging performance data.

You can use Alerts to send out warnings when disk space is running low or when network or level of CPU utilization poses a risk.

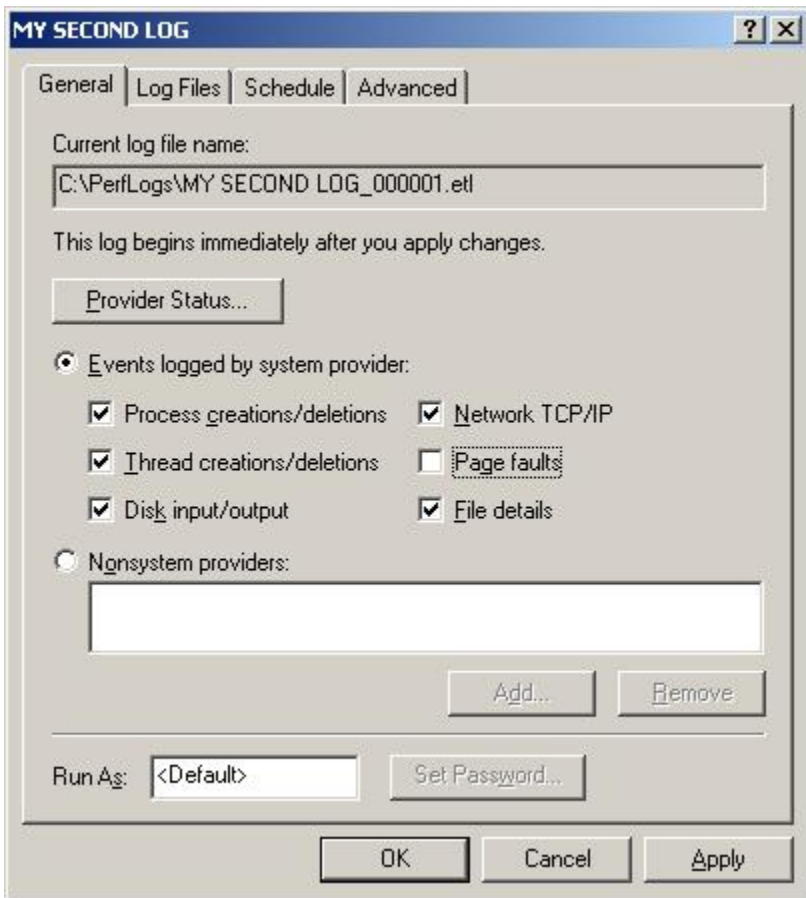
## Logs

There are two types of logging features:

- Counter Logs: are used to record the measurements of specific counters
- Trace Logs: are used to record memory and resource events.



The above image displays the counter log window that allows you to specify which counters should be monitored. The schedule permits you to set the start and stop time of logging. Go to the Log Files tab if you want to customize the name, size and location of the log file.

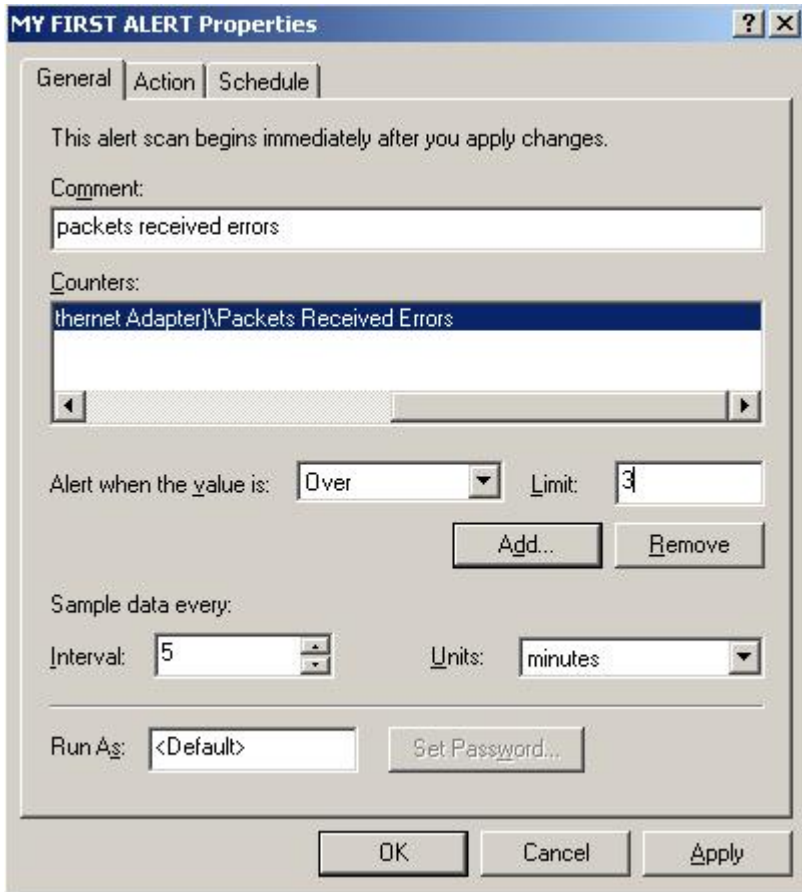


The above displays the trace log window which allows you to change what events will be logged by the system provider. Click 'Provider Status' to bring up a window that will show what system trace log providers and available and their current status. If you wish to add non system providers then select that option and press Add. You can run the this process as a different user, type the username in the Run As box and press the Set Password box to enter the password of the user.

Keep in mind that the more events you choose to log the more space will be required, especially if you choose page faults.

## Alerts

Right click anywhere on the white screen and choose “New Alert Setting” to bring up the properties window for a new alert. In my example I have set it to monitor the packets received errors and if they exceed three then an alert will be triggered. The schedule tab gives you the option to set the start of stop times of the scan.



The image above shows the alert properties box.

Apart from bottlenecks slowing down the entire system, they do not allow you to take full advantage of your network infrastructure. Using the performance monitor on your Windows Server will help you identify where the problem is coming from. If this tool is used with correct configuration and planning to suit your network environment then the administrator can benefit from being able to tackle problems in less time, therefore making the situation more efficient.