hp toptools and Windows® 2000 event management

august 2001

a white paper from hp

Table of Contents

executive summary

HP Toptools provides hardware management for network-connected HP PCs; servers; and networking, printing, and some storage devices. Windows® 2000 also has many integrated operating system management features. Some of these management features can be integrated with HP Toptools to provide a single management solution for both the hardware and the operating system.

hp toptools management benefits

HP Toptools is the award-winning hardware management platform for HP hardware. From the web-based console, HP Toptools can perform inventory, fault, configuration, security, and performance management. It utilizes several different industry standards, such as Simple Network Management Protocol [SNMP], Desktop Management Instrumentation [DMI], Windows Management Instrumentation [WMI], and web management consoles. Hardware management is one part of an overall systems management solution that will help reduce the total cost of computer system ownership.

Windows 2000 event management

With the release of Windows 2000, Microsoft® has incorporated many management functions in the operating system that were once provided by third-party applications. Many of these functions can be integrated with HP Toptools and other platforms. This provides for a consistent, central management solution for both HP hardware and operating system management.

service management

One of the new features of Windows® 2000 is the ability to manage services. Previously, when a service failed, an entry would be made in the system event log. However, unless the system administrator monitored each system's event log, they would not find out about the failure until a problem was reported. With Windows 2000, services can be automatically restarted if they fail. Also, when SNMP alert generation is integrated, error messages can be sent to a central management console, at which point the administrator can be automatically notified. This allows administrators to evaluate and respond to issues much more quickly, hopefully before end users notice the problem.

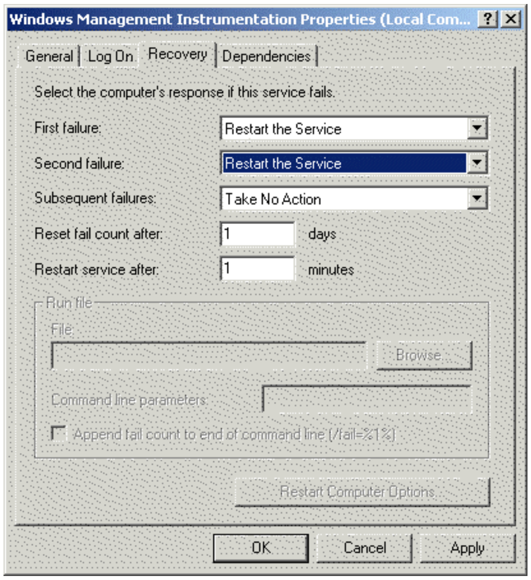
automatic restart

With Windows 2000, services can be configured to automatically restart upon failure. When a service fails, an error message is written to the system; event log. If the service fails during automatic restart, another error message is written to the event log. As we will see later when we discuss SNMP alert generation, these error messages can be monitored, and an SNMP trap can be created and sent to a central management station, such as HP Toptools.

To set up the services to automatically restart, follow these steps:

1. Open the "Services" applet in the Administrative Tools menu.
2. Select a critical service that you want to automatically restart, right click to bring up its menu, and select "Properties".
3. Select the "Recovery" tab.

Figure 1: Service Recovery Properties


Windows Management Instrumentation Properties (Local Com...

Select the computer's response if this service fails.

First failure: Restart the Service

Second failure: Restart the Service

Subsequent failures: Take No Action

Reset fail count after: 1 days

Restart service after: 1 minutes

4. Select “Restart the service” to have the service restart automatically upon the first and second failure. Other options here include “Take No Action,” “Run File,” and “Reboot Computer.” You can also configure how often to reset the failure counter and the delay before restarting the service. Click “OK” when you have finished configuring the service.

In this example, the service has been configured to automatically restart after the first two times the service fails each day, with a one-minute delay before the service restarts. This solution may help solve minor problems automatically before they impact the end user.

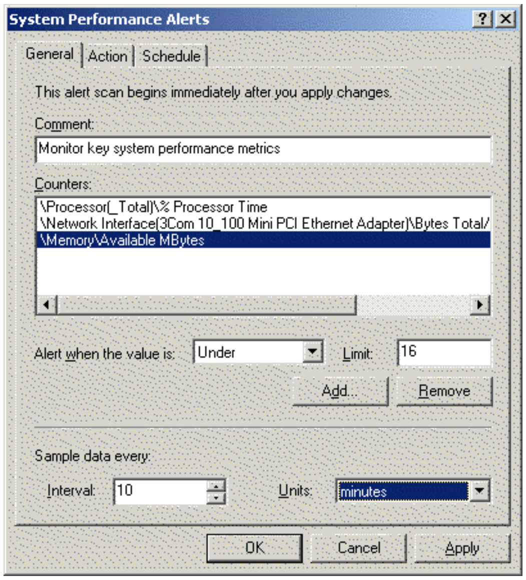
performance management

Windows 2000 also has integrated performance management. A large number of performance metrics can be monitored, and alerts can be generated when a threshold has been exceeded. When SNMP alert generation is integrated, these error messages can be forwarded to HP Toptools or another network or systems management console. This would allow a systems administrator to manage system performance and upgrade the system resources whenever it is necessary.

Complete the following steps to configure Windows 2000 performance management:

1. Select the “Performance” applet from the Administrative Tools menu.
2. Right click on “Alerts” to bring up its menu, and select “New Alert Settings.” Assign the alert a name, such as “System Performance Alerts.”
3. In the “General” property tab, select “Add” to select the performance metrics you wish to monitor. The "Explain" button creates a dialog box that contains a detailed description of the metric.

Figure 2: Performance Alerts Configuration



This alert scan begins immediately after you apply changes.

Comment:
Monitor key system performance metrics

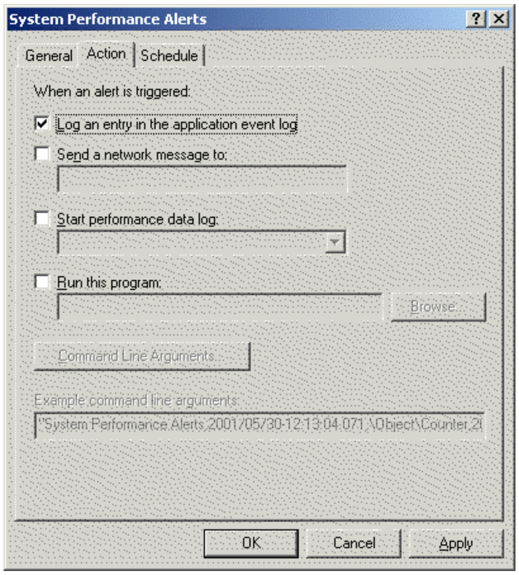
Counters:
\Processor(_Total)\% Processor Time
\Network Interface(3Com 10_100 Mini PCI Ethernet Adapter)\Bytes Total/
\Memory\Available MBytes

Alert when the value is: Under   Limit: 16

Sample data every:
Interval: 10   Units: minutes

4. Once the metrics have been selected, threshold values can be selected for each metric. As an example, here we have configured an alert when "Available Megabytes" is less than 16 Mbytes.
5. Next, the data-sampling rate can be configured. The default value is every five seconds, although in this example it has been set to every 10 minutes.
6. Select the "Action" tab.

Figure 3: Performance Alerts Actions



When an alert is triggered:

☑ Log an entry in the application event log

☐ Send a network message to:

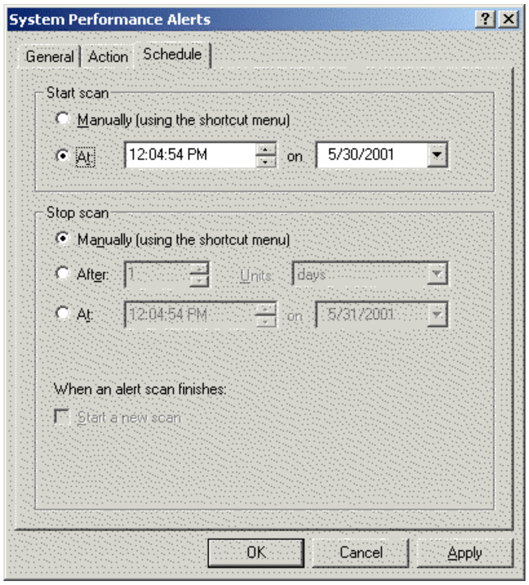
☐ Start performance data log:

☐ Run this program:

Example command line arguments:
"System Performance Alerts,2001/05/30-12:13:04.071,\Object\Counter,2(

7. Select "Log an entry in the application event log" to write any related alerts to the event log. Other options include sending a network message, creating a performance data log, or running another program.
8. Finally, select the "Schedule" tab to configure when the alert monitoring will be run.

Figure 4: Performance Alert Scheduling



System Performance Alerts

Start scan
○ Manually (using the shortcut menu)
● At: 12:04:54 PM on 5/30/2001

Stop scan
● Manually (using the shortcut menu)
○ After: 1 Units: days
○ At: 12:04:54 PM on 5/31/2001

When an alert scan finishes:
□ Start a new scan

9. Alerts can be started and stopped manually or automatically allowing so a system administrator to monitor performance continually or only at key times.
10. Once the alert is configured, click "OK" to finish.

Once the performance alerts have been set up on one system, they can be exported to a Web file and then loaded onto another system. Exporting the alerts can be done by selecting the alert, right clicking on it, and selecting "Save settings as" from the drop-down menu. The resulting Web page can be imported by other systems by right clicking on "Alerts" and selecting "New Alert settings from" from the drop down menu. After the alert has been imported, right click on it and select "Start" to initiate the performance monitoring.

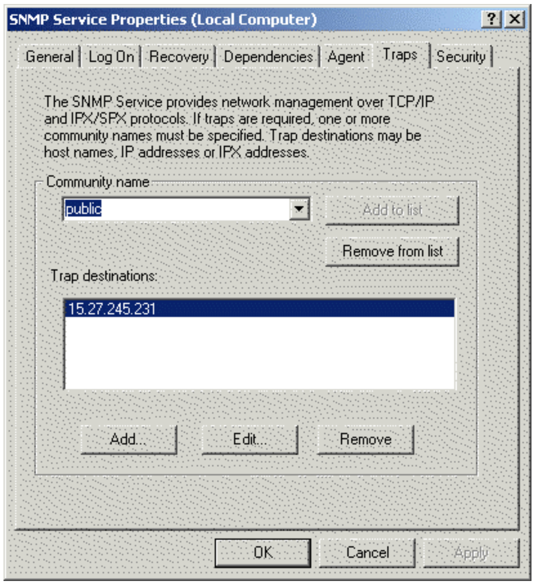
At this point, performance alerts have been configured. Whenever threshold values are exceeded, alerts are created in the application event log for Windows 2000. When this action is combined with SNMP trap generation, system performance alerts can be monitored from HP Toptools.

configuring SNMP services

Before SNMP traps can be generated, SNMP services must be configured. Perform the following steps to do this:

1. Start the "Services" applet from the Administrative Tools menu.
2. Right click on the SNMP service and select "Properties" from the drop-down menu.
3. Select the "Traps" tab. Type in an SNMP community name and select "Add to list." HP Toptools uses the default community name "public."

Figure 5: SNMP Properties



The SNMP Service provides network management over TCP/IP and IPX/SPX protocols. If traps are required, one or more community names must be specified. Trap destinations may be host names, IP addresses or IPX addresses.

Community name: public

Trap destinations: 15.27.245.231

4. Select "Add" and enter the system name or IP address of the HP Toptools device manager, or another network or system management platform console. This is where the SNMP traps will be sent.
5. At this point, you can also configure other SNMP properties, such as "Agent" and "Security", if needed. When that is done, click on "OK."

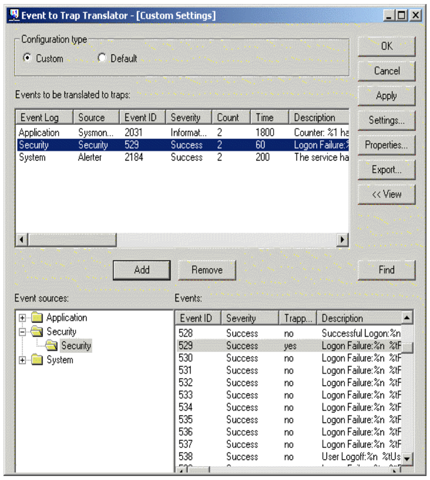
At this point, SNMP has been configured to forward SNMP traps to the HP Toptools device manager.

SNMP trap generation

Now that the SNMP service has been configured to send SNMP traps to the HP Toptools device manager, services have been configured to create alerts, and performance alerts have been configured, we just need to translate the alerts into SNMP traps. You can do this with the Evntwin utility, as shown in the following steps:

1. Run Evntwin <system name> using the "Run" command.
2. In the Event to Trap Translator utility, select "Edit" to bring up a window listing all of the events that can be translated into SNMP traps.

Figure 6: Event to Trap Translation



Configuration type: ● Custom ○ Default

Events to be translated to traps:

Event Log	Source	Event ID	Severity	Count	Time	Description
Application	Sysmon...	2031	Informat...	2	1800	Counter: %1 ha
Security	Security	529	Success	2	60	Logon Failure:%
System	Alerter	2184	Success	2	200	The service ha

Event sources:

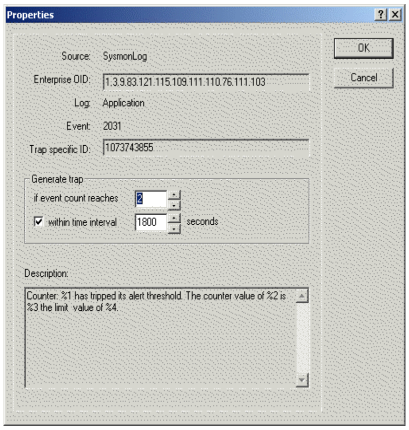
- Application
- Security
  - Security
- System

Events:

Event ID	Severity	Trapp...	Description
528	Success	no	Successful Logon:%n
529	Success	yes	Logon Failure:%n %tF
530	Success	no	Logon Failure:%n %tF
531	Success	no	Logon Failure:%n %tF
532	Success	no	Logon Failure:%n %tF
533	Success	no	Logon Failure:%n %tF
534	Success	no	Logon Failure:%n %tF
535	Success	no	Logon Failure:%n %tF
536	Success	no	Logon Failure:%n %tF
537	Success	no	Logon Failure:%n %tF
538	Success	no	User Logoff:%n %tUs

3. Select the events that you want SNMP traps created for. In this example, event 2031 was selected from the sysmonlog group in the application log. This translates the event that is generated when a performance threshold is exceeded, as was set up in the Performance Alerts section. Click "Add" to bring up the properties page for the alert. Run Evntwin <system name> using the "Run" command.

Figure 7: Event Translation Property page



Source: SysmonLog

Enterprise OID: 1.3.9.83.121.115.109.111.110.76.111.103

Log: Application

Event: 2031

Trap specific ID: 1073743855

Generate trap

if event count reaches 2

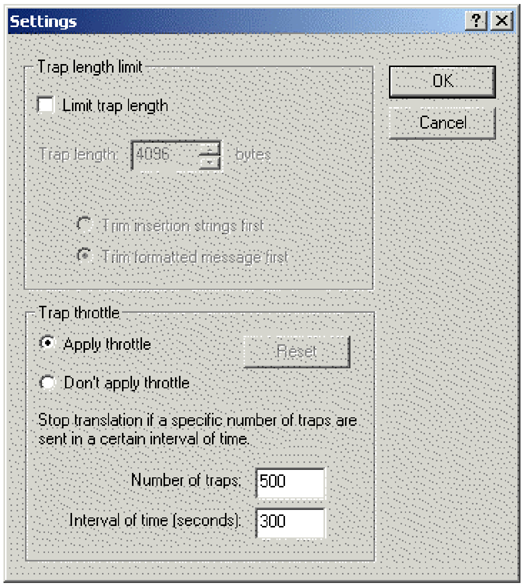
☑ within time interval 1800 seconds

Description:

Counter: %1 has tripped its alert threshold. The counter value of %2 is %3 the limit value of %4.

4. In the performance alerts management section, we configured the polling to happen every 10 minutes. If you are not interested in receiving SNMP traps when a single threshold is exceeded, but only if multiple thresholds are exceeded within a relatively short time frame, use the property page to control when SNP traps are generated. In this example, a SNMP trap will be generated when two alerts are generated within 30 minutes (1800 seconds). The SNMP trap will be forwarded to HP Toptools.
5. Another event that was selected was event 2184 from the "Alerter" group in the "System" event log. This event, "Service not started", corresponds to the automatic service restart that has already been configured. In this case, the event has been configured so that an SNMP trap will be generated when the "Service not started" error is found twice in the system event log within 200 seconds, or just over three minutes. This corresponds attempts to restart the failing service, with a one-minute delay between attempts to restart the service.
6. At this point, any additional events for which SNMP traps need to be created can be added and configured.

Figure 1: Event Translation Settings



Settings

Trap length limit

□ Limit trap length

Trap length: 4096 bytes

○ Trim insertion strings first

● Trim formatted message first

Trap throttle

● Apply throttle

○ Don't apply throttle

Stop translation if a specific number of traps are sent in a certain interval of time.

Number of traps: 500

Interval of time (seconds): 300

7. Finally, select the "Settings" button to configure general setting. This would include limiting the trap length and applying a throttle.

At this point, the Windows 2000 system is configured to automatically restart any failed services, monitor the system's performance, and forward the related alerts to the HP Toptools device manager.

hp toptools device manager configuration

The HP Toptools device manager does not need any special configuration to handle the SNMP traps. It will automatically show the SNMP traps in the "Alerts" log and change the alert icon in the device selector to the appropriate color. This allows the system administrator to view alerts either by system or in the central alert log.

Since many administrators do not monitor a console at all times, HP Toptools device manager can be configured to automatically forward alerts, including SNMP alerts, to either an e-mail address, a pager, or the Windows NT event log. Also, an action can be created to run a program. These actions are configured using the "Actions on alerts" menu item in the HP Toptools device manager. More information on setting up these actions can be found Hp Toptools help or the HP Toptools user manual.

Finally, SNMP Mib files can be imported into HP Toptools to translate the SNMP trap into a more descriptive format. This is accomplished with the Mib-2 Import utility (mib2imp.exe) included with HP Toptools in the program files\hptt\bin directory. More information on this program can be found in HP Toptools help or the HP Toptools user manual.

hp toptools system performance advisor

Readers who are familiar with HP Toptools will note that the performance management feature detail above is substantially similar to the HP Toptools
System Performance Advisor [SPA} utility. Basically, SPA does perform a similar function, but in a different way. With SPA, a number of performance metrics are sampled periodically (by default, once a minute). Once every 15 minutes, the HP Toptools device manager polls each monitored system and collect the performance samples.

It averages the samples for each metric from the last 15-minute sample to create a current value. A warning or critical alert is generated if the sample average for a performance metric exceeds a customizable threshold. So far, SPA is similar to the performance monitoring described earlier. However, the additional value of SPA is in its storage and reporting of performance data.

SPA stores the sample values that it collects. From this database, reports can be generated that show the maximum, minimum, and average values for the performance metrics over a selected time frame, such as the previous 24 hours. This allows the administrator to get an overall picture of the systems utilization rather than just finding out when the utilization exceeded a threshold. Also, reports on the same system or groups of systems can be run periodically, such as once a quarter, and compared for trend analysis. Utilization trend analysis is a very useful tool that a system administrator can use to do capacity planning.

More information on System Performance Advisor is available from the HP Toptools Web site at http://www.hp.com/toptools, in the HP Toptools user manual, or in HP Toptools online help.

hp toptools integration into network management applications

While HP Toptools provides hardware management and, with the information included in this white paper, some basic operating system management, it also allows the end user to integrate these features into a network or systems management platform such as HP Openview NNM, CA Unicenter TNG, or Tivoli Enterprise Management. More information on the versions of HP Toptools that link HP Toptools to another platform, known as HP Toptools enterprise products, is available on the Web at http://www.hp.com/toptools/solutions/entsols.html. These products are available free of charge and can also be downloaded from the Web site.