Configuring Windows 2000 and XP Servers to send Windows Event Messages to SNMPc

Summary

The following guide will explain how to use the Microsoft Windows utilities ‘evntcmd’ and ‘evntwin’ to send Windows Event messages directly to SNMPc using SNMP Traps.

This how-to guide has been tested with
Windows XP/2000
SNMPc Version 6.0.9

Please note it will not work with Windows NT

Stage 1

Windows Server Prerequisites
It is assumed that the standard Microsoft SNMP agent has been installed and configured with the SNMPc’s IP address as the Trap host. You do not need to enable the ‘SNMP TRAP Service’ to generate alerts to SNMPc.

To test if SNMP agent is installed correctly.
Go to Control Panel/Administrative Tools/Services. Firstly ensure that the SNMP Service is present. (You can double-click on the service name to make any configuration changes). Highlight the service name and select ‘Restart the service’.

If you have the agent configured correctly you should receive a ‘Cold Start’ alarm in the SNMPc event log. If you do not receive anything ensure that you have added the SNMPc IP address to the ‘Traps’ section of the SNMP Service configuration. The Community string should normally be ‘public’.

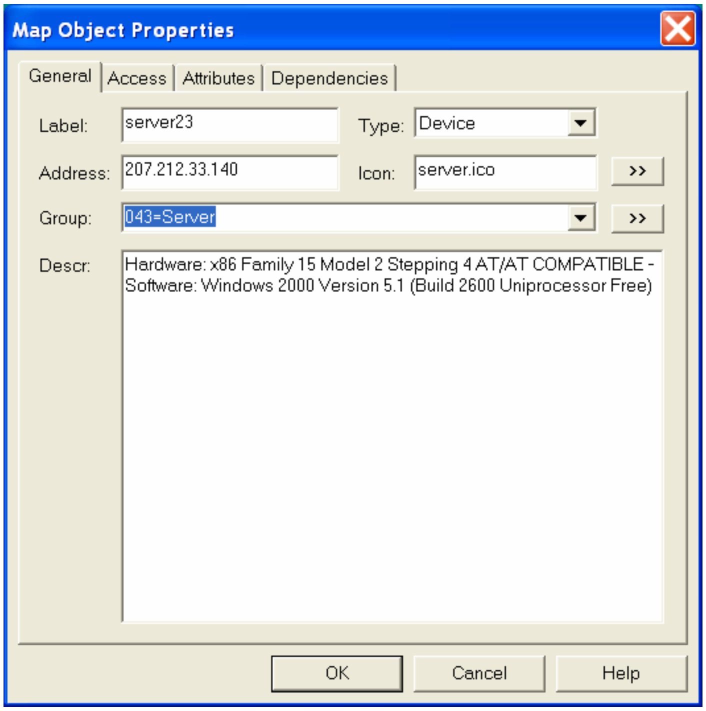
Stage 2

Configuring SNMPc.

The format of the Windows Trap is difficult to match on as it includes the service name as part of the TRAP object ID. For this reason it is recommended that all icons representing the devices are edited to be in the same ‘Group’. We can then use a more generic filter to present the data.

To change the Group setting for an icon

1) Highlight the icon(s) representing the server
2) Right-click and select Properties
3) Change the ‘Group’ setting to be ‘043=Server’



Label: server23

Type: Device

Address: 207.212.33.140

Icon: server.ico

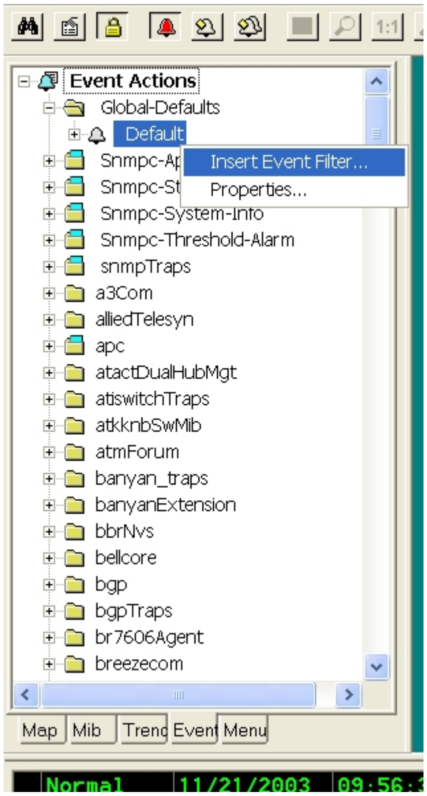
Group: 043=Server

Descr: Hardware: x86 Family 15 Model 2 Stepping 4 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)

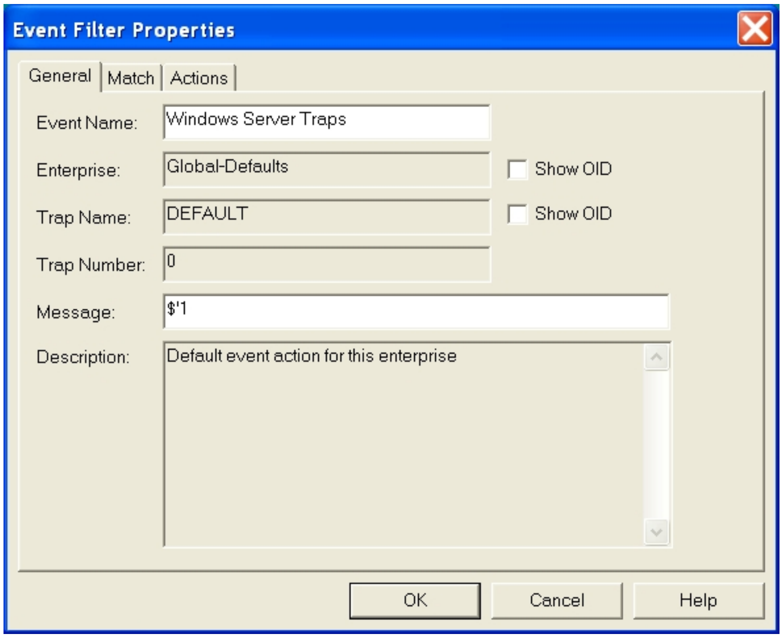
4) Select OK

To create an event filter to display the Windows Event Messages

1) Select the ‘Event’ selection window
2) Click the ‘+’ sign beside the top option ‘Global-Defaults’
3) Right-Click on ‘Default’ and select ‘Insert Event Filter’



4) In the new window Change the ‘Event Name’ to Windows Server Traps
5) Change the ‘Message’ to $’1 (the ‘ is important!)



Event Filter Properties

General | Match | Actions

Event Name: Windows Server Traps

Enterprise: Global-Defaults □ Show OID

Trap Name: DEFAULT □ Show OID

Trap Number: 0

Message: $'1

Description: Default event action for this enterprise

6) Select the Match Tab and change ‘Node Group’ to 043=Server
7) Select the Actions Tab and change the ‘Set-Priority’ to Warning-Blue
8) Select OK

When an event is now received the icon will go blue and a properly formatted event message will be displayed in the event view.

Stage 3

Configuring Server to send Event Messages

Download the file crcevents.cnf from here. This is a file that contains common events such as services starting/stopping or failing. It also will generate alerts for other common issues such as user login failures and Windows shutdown.

From a command line prompt change to the directory where you saved the .cnf file. Type the command…….

```
Evntcmd crcevents.cnf
```

The server should now be configured to send events to the SNMPc server. You can test this by starting and stopping a few services. Event messages should be displayed in the SNMPc logfile.

To display the full syntax of the evntcmd command type ‘evntcmd /?’ With the correct privileges you can install the cnf file remotely to a server.

Notes

You can use the Evntwin command to display which events are generating traps. Using the Evntwin console it is a simple matter to either add new events or delete ones which you do not wish to receive.

If you are generating large numbers of event messages it would be sensible to configure SNMPc to delete older events. The number of days to store events can be configured from the Config/Event Actions menu….

There is no warranty given or implied with this guide. You implement these files at your own risk. Castle Rock Computing is not liable for any downtime or loss suffered as a result of using this information.