Nagios XI – How to Integrate SNMP Traps With Nagios XI

Nagios®

The Industry Standard in IT Infrastructure Monitoring

Purpose

This document describes how to configure Nagios® XI™ to receive and process SNMP traps from external devices. Monitoring SNMP traps allows system administrators to monitor real-time events and network incidents in order to ensure an accurate and healthy monitoring environment.

Target Audience

This document is intended for use by Nagios administrators looking to integrate SNMP traps into their monitoring configuration to gain greater insight into their IT infrastructure.

Requirements

Users must be running Nagios XI 2009R1.1 or later to use the instructions and wizards described in this document. Administrators will need to be familiar with configuring network devices to trigger event-based alerts and finding/installing vendor-specific MIBs.

Automated Installation

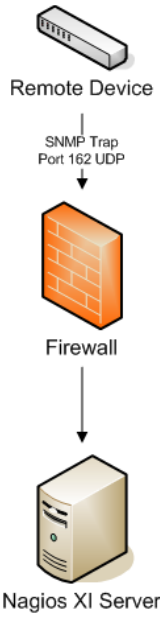
Open a terminal and login to the Nagios XI server as the root user and run the following commands:

```
cd /tmp
wget http://assets.nagios.com/downloads/nagiosxi/scripts/NagiosXI-SNMPTrap-setup.sh
sh ./NagiosXI-SNMPTrap-setup.sh
```

The "NagiosXI-SNMPTrap-setup.sh" script will do the following:

1. Install all of the required prerequisites
2. Download and install supporting files
3. Modify the "snmptt.ini" and "snmptrapd.conf" files
4. Add the snmptt user to the nagios and nagcmd groups
5. Modify some permissions
6. Add a firewall rule in iptables to open UDP port 162
7. Set up the snmptt and snmptrapd daemons to start automatically on boot

Note: If you have an intermediary firewall between the Nagios XI server and the remote device, please, read the next section (Intermediary Firewalls). If you don't – you can skip it and proceed to the "Installing MIBs" section.



Intermediary Firewalls

Before you can configure remote devices to send SNMP traps to Nagios XI you will have to configure any intermediary firewalls between the Nagios XI server and the remote device to allow inbound SNMP traps to be sent to Nagios XI. This involves allowing UDP port 162 traffic from remote devices to the Nagios XI server.

Remember that unlike with most checks, Nagios XI is the server (rather than the client) for SNMP traps, so the packet flow is inbound to the Nagios XI machine.

A firewall rule was added to iptables to open UDP port 162 in the script, NagiosXI-SNMPTrap-setup.sh, which you ran during the Automated Installation section above.

Installing MIBs

You may need to configure **snmptt** on the Nagios XI server to use the MIBs your remote devices are using. This may mean having to load extra MIBs into the `/usr/share/snmp/mibs/` directory on the Nagios XI server. This can be done through the XI interface by browsing to the **Admin** → **Manage MIBs** page via the top navigation bar.
You will then also have to run the following command to import each new MIB into the `/usr/share/snmp/mibs/` directory. Remember to replace <PathToNewMIB> with the path to the MIB file you want to import.

```
addmib <PathToNewMIB>
```

Adjusting Trap Severity

Edit the Trap Translator configuration file located at */etc/snmp/snmptt.conf* and alter the severity of each *EVENT* to match your personal needs. The default severity level is "Normal" (equivalent to an "OK" state in Nagios). You may want to change some events to have a "Warning" or "Critical" severity level (equivalent to "Warning" and "Critical" states in Nagios, respectively). A "<NA>" severity level maps to an "Unknown" state in Nagios.

You'll probably have to modify the snmptt.conf file to get things working the way you want. In our example that follows later in this document, the line in *snmptt.cfg* reading:

```
EVENT linkDown .1.3.6.1.6.3.1.1.5.3 "Status Events" Normal
```

was changed to:

```
EVENT linkDown .1.3.6.1.6.3.1.1.5.3 "Status Events" Critical
```

In these lines:

- `EVENT` describes which attribute is being set
- `linkDown` is the name of the event
- `.1.3.6.1.6.3.1.1.5.3` is the *OID* (Object Identifier) for that type of event
- `Normal` or `Critical` is the severity level.

For more information on OIDs and what a given number is for, see http://www.oid-info.com/. You are encouraged to submit descriptions for any OIDs you know that are not in the repository yet. Not all event names will be as obvious as linkDown, so you may need to do some research to figure out what to use in your configuration. The MIBs you use may come with documentation that describes what event names can be used.

If you would like to read more about the format of the *snmptt.conf* file, detailed documentation is available from the upstream project on SourceForge, at http://snmptt.sourceforge.net/docs/snmptt.shtml#SNMPTT.CONF-Configuration-file-format.

Installing The SNMP Trap Wizard (For users running Nagios XI 2012 r1.0 and earlier)

This section only applies to users running Nagios XI 2012 r1.0 and earlier. If you are using a later version you can skip this section as the SNMP Trap Wizard comes pre-installed on your system. If you need to install the SNMP Trap Wizard, you can find the wizard by searching on the Nagios Exchange at:

http://exchange.nagios.org/directory/Addons/Configuration/Configuration-Wizards

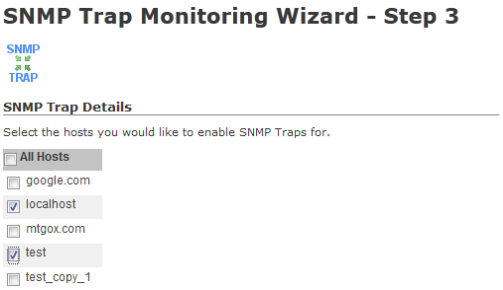
To install the wizard in Nagios XI, use the **Upload** option on the monitoring wizard administration screen. You would do this via the **Admin** → **Manage Wizards** page and uploading the **snmp trap wizard.zip** that was downloaded.

Using The SNMP Trap Wizard

Each host or device that you wish to receive and process SNMP traps for must have a corresponding SNMP Traps service defined in Nagios XI. Nagios XI has a built-in wizard that makes the configuration of these SNMP trap events quick and simple.

To begin using the SNMP Trap Wizard navigate to the **Configure** → **Run the Monitoring Wizard** page via the top navigation bar, and select **SNMP Trap Wizard.**

The first screen says “This wizard allows you to enable SNMP Traps for existing hosts that are being monitored”, select next. The wizard will then ask you which host you wish to add an SNMP trap service. When you have selected all the hosts you want, select next.



You can now select finish if the default notifications options suit your needs, otherwise continue through with the last three pages pertaining to notification and group options.

SNMP Trap Example

As an example of how SNMP traps can be used in Nagios XI, we have a simulated environment using a Netgear Ethernet switch capable of sending SNMP traps.

At the start of our tests Nagios XI reported that everything was okay with the switch:

A patch cable was unplugged from the switch to simulate a network failure.

Host	Service	Status	Duration	Attempt	Last Check	Status Information
192.168.5.42	Ping	Ok	11d 16h 28m 58s	1/5	2010-03-25 10:59:23	OK - 192.168.5.42: rta 4.982ms, lost 0%
	Port 1 Bandwidth	Ok	12d 21h 12m 2s	1/5	2010-03-25 10:56:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 1 Status	Ok	11d 16h 26m 58s	1/5	2010-03-25 10:56:29	OK: Interface Port 1 Gigabit Ethernet (index 1) is up.
	Port 7 Bandwidth	Ok	12d 21h 11m 9s	1/5	2010-03-25 10:56:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 7 Status	Ok	11d 16h 29m 13s	1/5	2010-03-25 10:59:23	OK: Interface Port 7 Gigabit Ethernet (index 7) is up.
	Port 8 Bandwidth	Ok	12d 21h 9m 17s	1/5	2010-03-25 10:59:23	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 8 Status	Ok	11d 16h 28m 38s	1/5	2010-03-25 10:57:36	OK: Interface Port 8 Gigabit Ethernet (index 8) is up.
	SNMP Traps	Ok	10m 39s	1/1	2010-03-25 10:50:35	" A linkUp trap signifies that the SNMP entity, acting in an 3 Port 3 copper link up(ifIndex.3 (INTEGER32):3 enterprises.4526.11.5.4.0 ():Port 3 copper link up"

This resulted in the switch sending a trap to Nagios XI (of type **linkDown**) which we had defined as Critical severity:

Host	Service	Status	Duration	Attempt	Last Check	Status Information
192.168.5.42	Ping	Ok	11d 16h 32m 28s	1/5	2010-03-25 11:04:23	OK - 192.168.5.42: rta 3.044ms, lost 0%
	Port 1 Bandwidth	Ok	12d 21h 15m 32s	1/5	2010-03-25 11:01:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 1 Status	Ok	11d 16h 30m 28s	1/5	2010-03-25 11:01:29	OK: Interface Port 1 Gigabit Ethernet (index 1) is up.
	Port 7 Bandwidth	Ok	12d 21h 14m 39s	1/5	2010-03-25 11:01:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 7 Status	Ok	11d 16h 32m 43s	1/5	2010-03-25 11:04:23	OK: Interface Port 7 Gigabit Ethernet (index 7) is up.
	Port 8 Bandwidth	Ok	12d 21h 12m 47s	1/5	2010-03-25 11:04:23	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 8 Status	Ok	11d 16h 32m 8s	1/5	2010-03-25 11:02:36	OK: Interface Port 8 Gigabit Ethernet (index 8) is up.
	SNMP Traps	Critical	38s	1/1	2010-03-25 11:04:06	" A linkDown trap signifies that the SNMP entity, acting in 3 Port 3 copper link down/ifIndex.3 (INTEGER32):3 enterprises.4526.11.5.3.0 ():Port 3 copper link down"

We then re-attached the patch cable to the switch:

The results show the SNMP trap service in an OK state with a event type **linkUp** in Nagios XI, indicating things were okay again:

Host	Service	Status	Duration	Attempt	Last Check	Status Information
192.168.5.42	Ping	Ok	11d 16h 33m 59s	1/5	2010-03-25 11:04:23	OK - 192.168.5.42: rta 3.044ms, lost 0%
	Port 1 Bandwidth	Ok	12d 21h 17m 3s	1/5	2010-03-25 11:01:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 1 Status	Ok	11d 16h 31m 59s	1/5	2010-03-25 11:01:29	OK: Interface Port 1 Gigabit Ethernet (index 1) is up.
	Port 7 Bandwidth	Ok	12d 21h 16m 10s	1/5	2010-03-25 11:01:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 7 Status	Ok	11d 16h 34m 14s	1/5	2010-03-25 11:04:23	OK: Interface Port 7 Gigabit Ethernet (index 7) is up.
	Port 8 Bandwidth	Ok	12d 21h 14m 18s	1/5	2010-03-25 11:04:23	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 8 Status	Ok	11d 16h 33m 39s	1/5	2010-03-25 11:02:36	OK: Interface Port 8 Gigabit Ethernet (index 8) is up.
	SNMP Traps	Ok	11s	1/1	2010-03-25 11:06:04	" A linkUp trap signifies that the SNMP entity, acting in an 3 Port 3 copper link up/ifIndex.3 (INTEGER32):3 enterprises.4526.11.5.4.0 ():Port 3 copper link up"

Asynchronous Example

An important point to stress with SNMP traps is that they are asynchronous events that can occur at any time. Thus, they are not actively checked by Nagios XI on a regular schedule (e.g. by polling). See the sequence of screen-shots below:

At the start of the example, Port 7 is connected and up:

Host	Service	Status	Duration	Attempt	Last Check	Status Information
192.168.5.42	Ping	Ok	11d 16h 28m 58s	1/5	2010-03-25 10:59:23	OK - 192.168.5.42: rta 4.982ms, lost 0%
	Port 1 Bandwidth	Ok	12d 21h 12m 2s	1/5	2010-03-25 10:56:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 1 Status	Ok	11d 16h 26m 58s	1/5	2010-03-25 10:56:29	OK: Interface Port 1 Gigabit Ethernet (index 1) is up.
	Port 7 Bandwidth	Ok	12d 21h 11m 9s	1/5	2010-03-25 10:56:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 7 Status	Ok	11d 16h 29m 13s	1/5	2010-03-25 10:59:23	OK: Interface Port 7 Gigabit Ethernet (index 7) is up.
	Port 8 Bandwidth	Ok	12d 21h 9m 17s	1/5	2010-03-25 10:59:23	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 8 Status	Ok	11d 16h 28m 38s	1/5	2010-03-25 10:57:36	OK: Interface Port 8 Gigabit Ethernet (index 8) is up.
	SNMP Traps	Ok	10m 39s	1/1	2010-03-25 10:50:35	" A linkUp trap signifies that the SNMP entity, acting in an 3 Port 3 copper link up/ifIndex.3 (INTEGER32):3 enterprises.4526.11.5.4.0 ():Port 3 copper link up"

An SNMP trap fires as soon as the cable on Port 7 is unplugged. The *Port 7 Status* service does not reflect this yet, as it has not been checked since the cable was unplugged:

Host	Service	Status	Duration	Attempt	Last Check	Status Information
192.168.5.42	Ping	Ok	11d 21h 1m 22s	1/5	2010-03-25 15:29:23	OK - 192.168.5.42: rta 8.089ms, lost 0%
	Port 1 Bandwidth	Ok	13d 1h 44m 26s	1/5	2010-03-25 15:31:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 1 Status	Ok	11d 20h 59m 22s	1/5	2010-03-25 15:31:29	OK: Interface Port 1 Gigabit Ethernet (index 1) is up.
	Port 7 Bandwidth	Ok	13d 1h 43m 33s	1/5	2010-03-25 15:31:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 7 Status	Ok	12m 15s	1/5	2010-03-25 15:31:23	OK: Interface Port 7 Gigabit Ethernet (index 7) is up.
	Port 8 Bandwidth	Ok	13d 1h 41m 41s	1/5	2010-03-25 15:29:24	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 8 Status	Ok	11d 21h 1m 2s	1/5	2010-03-25 15:32:36	OK: Interface Port 8 Gigabit Ethernet (index 8) is up.
	SNMP Traps	Critical	13s	1/1	2010-03-25 15:33:25	" A linkDown trap signifies that the SNMP entity, acting in 3 Port 3 copper link down/ifIndex.3 (INTEGER32):3 enterprises.4526.11.5.3.0 ():Port 3 copper link down"

A scheduled check of the *Port 7 Status* service occurs and reflects the down state of Port 7:

Host	Service	Status	Duration	Attempt	Last Check	Status Information
192.168.5.42	Ping	Ok	11d 20h 47m 51s	1/5	2010-03-25 15:19:23	OK - 192.168.5.42: rta 22.135ms, lost 0%
	Port 1 Bandwidth	Ok	13d 1h 30m 55s	1/5	2010-03-25 15:16:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 1 Status	Ok	11d 20h 45m 51s	1/5	2010-03-25 15:16:29	OK: Interface Port 1 Gigabit Ethernet (index 1) is up.
	Port 7 Bandwidth	Ok	13d 1h 30m 2s	1/5	2010-03-25 15:16:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 7 Status	Critical	44s	1/5	2010-03-25 15:19:23	CRITICAL: Interface Port 7 Gigabit Ethernet (index 7) is down.
	Port 8 Bandwidth	Ok	13d 1h 28m 10s	1/5	2010-03-25 15:19:24	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 8 Status	Ok	11d 20h 47m 31s	1/5	2010-03-25 15:17:36	OK: Interface Port 8 Gigabit Ethernet (index 8) is up.
	SNMP Traps	Critical	5m 16s	1/1	2010-03-25 15:14:51	" A linkDown trap signifies that the SNMP entity, acting in 7 Port 7 copper link down/ifIndex.7 (INTEGER32):7 enterprises.4526.11.5.3.0 ():Port 7 copper link down"

When the cable is plugged back in to the switch, an SNMP trap is fired off and the *SNMP Traps* service finds out first:

Host	Service	Status	Duration	Attempt	Last Check	Status Information
192.168.5.42	Ping	Ok	11d 20h 48m 51s	1/5	2010-03-25 15:19:23	OK - 192.168.5.42: rta 22.135ms, lost 0%
	Port 1 Bandwidth	Ok	13d 1h 31m 55s	1/5	2010-03-25 15:16:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 1 Status	Ok	11d 20h 46m 51s	1/5	2010-03-25 15:16:29	OK: Interface Port 1 Gigabit Ethernet (index 1) is up.
	Port 7 Bandwidth	Ok	13d 1h 31m 2s	1/5	2010-03-25 15:16:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 7 Status	Critical	1m 44s	2/5	2010-03-25 15:20:23	CRITICAL: Interface Port 7 Gigabit Ethernet (index 7) is down.
	Port 8 Bandwidth	Ok	13d 1h 29m 10s	1/5	2010-03-25 15:19:24	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 8 Status	Ok	11d 20h 48m 31s	1/5	2010-03-25 15:17:36	OK: Interface Port 8 Gigabit Ethernet (index 8) is up.
	SNMP Traps	Ok	32s	1/1	2010-03-25 15:20:35	" A linkUp trap signifies that the SNMP entity, acting in an 7 Port 7 copper link up/ifIndex.7 (INTEGER32):7 enterprises.4526.11.5.4.0 ():Port 7 copper link up"

A few minutes later, a scheduled check of the *Port 7 Status* service occurs and the status reflects the up state of Port 7:

Host	Service	Status	Duration	Attempt	Last Check	Status Information
192.168.5.42	Ping	Ok	11d 16h 33m 59s	1/5	2010-03-25 11:04:23	OK - 192.168.5.42: rta 3.044ms, lost 0%
	Port 1 Bandwidth	Ok	12d 21h 17m 3s	1/5	2010-03-25 11:01:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 1 Status	Ok	11d 16h 31m 59s	1/5	2010-03-25 11:01:29	OK: Interface Port 1 Gigabit Ethernet (index 1) is up.
	Port 7 Bandwidth	Ok	12d 21h 16m 10s	1/5	2010-03-25 11:01:29	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 7 Status	Ok	11d 16h 34m 14s	1/5	2010-03-25 11:04:23	OK: Interface Port 7 Gigabit Ethernet (index 7) is up.
	Port 8 Bandwidth	Ok	12d 21h 14m 18s	1/5	2010-03-25 11:04:23	OK - Current BW in: 0Mbps Out: 0Mbps
	Port 8 Status	Ok	11d 16h 33m 39s	1/5	2010-03-25 11:02:36	OK: Interface Port 8 Gigabit Ethernet (index 8) is up.
	SNMP Traps	Ok	11s	1/1	2010-03-25 11:06:04	" A linkUp trap signifies that the SNMP entity, acting in an 3 Port 3 copper link up/ifIndex.3 (INTEGER32):3 enterprises.4526.11.5.4.0 ():Port 3 copper link up"

Troubleshooting

SNMP traps can get very complicated and generally require some knowledge and troubleshooting to get working just the way you want. Here is an outline of a general troubleshooting for SNMP traps. Please note that if you are attempting to use this troubleshooting guide without referring to the above install script, your battle will be uphill as the script enables various aspects of **snmptt** that we will use exhaustively.

First thing that is helpful is a separate server that we can send test traps from, this can also be done from the Nagios server although it will not validate any firewall rules that may be in place. The use of this server will be ephemeral. The command we will use is:

```
snmptrap
```

On the test-trap-sending host (NOT the Nagios XI host) we'll need a MIB to use to send a test SNMP trap. This MIB was taken from the net-snmp tutorial. You'll need to create a text file called UCD-TRAP-TEST-MIB.txt in the directory /usr/share/snmp/mibs. In that file you'll need to copy some text into it.

```
cd /usr/share/snmp/mibs
vi UCD-TRAP-TEST-MIB.txt
```

Copy the text below

```
UCD-TRAP-TEST-MIB DEFINITIONS ::= BEGIN
      IMPORTS ucdExperimental FROM UCD-SNMP-MIB;

demotraps OBJECT IDENTIFIER ::= { ucdExperimental 990 }

demoTrap TRAP-TYPE
       ENTERPRISE demotraps
       VARIABLES { sysLocation }
       DESCRIPTION "An example of an SMIv1 trap"
       ::= 17

END
```

End text copy

Now comes the part where we actually send a trap to our Nagios XI host. In the terminal on your test-trap-sending host, enter the following:

```
 snmptrap -v 1 -c public <NAGIOS XI SERVER IP> UCD-TRAP-TEST-MIB::demotraps \
"" 6 17 "" SNMPv2-MIB::sysLocation.0 s "Here"
```

This will send an SNMP trap to your Nagios XI server. Remember to replace <**NAGIOS XI SERVER IP**> with the IP address of your Nagios server.

Now that you've sent the test trap, you should check a few things to make sure its all working. First off, this MIB that we added to the test-trap-sending host does not exist on our Nagios XI server. When the trap gets to the Nagios XI server, it will try to identify the trap by running it against the MIBs in its library. Since the MIB does not exist on the Nagios XI server, it can't identify it and it will dump the trap to the `snmpttunknown.log`, which is where we will check.

To check this log open a terminal on the XI server and run the command below:

```
vi /var/log/snmptt/snmpttunknown.log
```

There should be logs of your test SNMP trap here. If there is not, make sure that there is not some intermediary firewall in the way. Check to make sure iptables is allowing traffic through on ports 161 and 162. Do not progress past this point until you are able to get this test trap.

If you are able to receive a trap, you are ready to start capturing real SNMP traps. Monitor `/var/log/snmptt.log` for SNMP traps that are coming in. Also make sure that traps are not getting relegated to unknown status by keeping an eye on `snmpttunknown.log`.

If you are seeing traps in your `/var/log/snmptt.log` but cannot locate them within your Nagios XI system, it may be that you have not set up your SNMP Traps service for the remote host sending the traps. These traps will continue to be collected in Nagios XI. To view them, navigate within the XI web-interface: **Admin → Monitoring Config → Unconfigured Objects**. You can either set up the SNMP Traps service using the wizard or by clicking on the blue triangle under actions.

Final Thoughts

SNMP traps are a great method for monitoring asynchronous events in your IT infrastructure. The complexity of managing MIBs and the intricacies of the SNMP protocol can often be daunting, but if you get familiar with the in and outs of SNMP, it can be a powerful addition to your IT infrastructure management and allow for advanced, real-time network event monitoring.

For any support related questions please visit the Nagios Support Forums at:

http://support.nagios.com/forum/