Nagios XI - SNMP Trap Hardening

Article Number: 826 | Rating: 1/5 from 1 votes | Last Updated: Tue, Dec 18, 2018 at 5:55 PM

Nagios XI - SNMP Trap Hardening

This KB article explains how to harden your Nagios XI server to only accept SNMP traps from authorized sources. By default the Nagios XI server will accept inbound SNMP v2 traps from any device.

SNMP v3 traps will not be accepted by Nagios XI unless the server is specifically configured for SNMP v3 traps. SNMP v3 traps are a more complicated topic and are covered in the SNMP Trap v3 Configuration KB article.

Editing Files

In the steps of this article you will be required to edit files. This documentation will use the **vi** text editor. When using the vi
editor:

- To make changes press **i** on the keyboard first to enter insert mode
- Press **Esc** to exit insert mode
- When you have finished, save the changes in vi by typing **:wq** and press Enter

Send Test Trap

When working through this documentation you may want to test the changes by sending a test trap. The following KB article provides examples on how to send a test trap, which can be very helpful:

SNMP Trap - How To Send A Test Trap

When a test trap is received on the Nagios XI server it should be logged in the `/var/log/snmptt/snmpttunknown.log` file.

Default Configuration

The default SNMP Trap configuration is stored in the `/etc/snmp/snmptrapd.conf` file and contains just two lines:

```
disableAuthorization yes
traphandle default /usr/sbin/snmptthandler
```

It is the **disableAuthorization** directive that allows SNMP traps from any device to be sent to Nagios XI.

The first step is to comment out the **disableAuthorization** directive by adding a **#** to the beginning of the line:

```
#disableAuthorization yes
```

```
traphandle default /usr/sbin/snmptthandler
```

The remaining steps in this KB article demonstrate different authorization methods that can be used. You will see in the examples that multiple authorization methods can be defined in the config file.

Restrict To SNMP v2 Community

A simple hardening method is to accept traps from any devices that supply a specific community string.

This example shows how to allow traps for the **`Sup3rStr0ng`** community string:

```
#disableAuthorization yes
authCommunity execute Sup3rStr0ng
traphandle default /usr/sbin/snmptthandler
```

After making the change you will need to restart the snmptrapd service for the settings to become effective and then you could send a test trap to confirm the settings are correct.

Restrict To SNMP v2 Community AND Network Address

A more advanced hardening method is to accept traps from specific devices that supply a specific community string.

This example shows how to allow traps for the **`M3g@Str0ng`** community string which come from the **`10.25.5.15`** network address:

```
#disableAuthorization yes
authCommunity execute Sup3rStr0ng
authCommunity execute M3g@Str0ng 10.25.5.15
traphandle default /usr/sbin/snmptthandler
```

After making the change you will need to restart the snmptrapd service for the settings to become effective and then you could send a test trap to confirm the settings are correct.

Restrict To SNMP v2 Community AND Network Subnet

Another hardening method is to accept traps from devices in a network subnet that supply a specific community string.

This example shows how to allow traps for the **`Ultr@Str0ng`** community string which come from the **`10.25.0.0/16`** network subnet:

```
#disableAuthorization yes
authCommunity execute Sup3rStr0ng
authCommunity execute M3g@Str0ng 10.25.5.15
authCommunity execute Ultr@Str0ng 10.25.0.0/16
```

```
traphandle default /usr/sbin/snmptthandler
```

After making the change you will need to restart the snmptrapd service for the settings to become effective and then you could send a test trap to confirm the settings are correct.

Restart SNMPTRAPD Service

Whenever you make a change to the `/etc/snmp/snmptrapd.conf` file you are required to restart the `snmptrapd` service with the following command:

RHEL 6 | CentOS 6 | Oracle Linux 6

```
service snmptrapd restart
```

RHEL 7 | CentOS 7 | Oracle Linux 7 | Debian | Ubuntu 16/18

```
systemctl restart snmptrapd.service
```

Ubuntu 14

```
service snmpd restart
```

Final Thoughts

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

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

Posted by: **tlea** - Tue, Nov 6, 2018 at 6:28 PM. This article has been viewed 2275 times.

Online URL: https://support.nagios.com/kb/article/nagios-xi-snmp-trap-hardening-826.html