Nagios XI - SNMP Trap v3 Configuration

Article Number: 827 | Rating: Unrated | Last Updated: Tue, Dec 18, 2018 at 5:55 PM

Nagios XI - SNMP v3 Trap Configuration

This KB article explains how to configure your Nagios XI server to accept SNMP v3 traps. 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.

Information on SNMP v2 traps can be located in the following KB article:

Nagios XI - SNMP Trap Hardening

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

Version 2 vs Version 3

The main difference between v2 and v3 traps is the authentication mechanisms. v2 is much simpler by design whereas v3 has multiple layers of authentication to strengthen it. Probably the biggest difference is that the SNMP Trap Daemon (`snmptrapd`) is configured by default to accept v2 traps from any device regardless of what SNMP community is provided. However `snmptrapd` cannot be configured to accept traps v3 from any device, it must be configured before it can receive an SNMP v3 trap.

Once a trap is received and it meets the v2 or v3 authorization requirements defined in the `snmptrapd` configuration, it is passed to the SNMP Trap Translator (`snmptt`). Once it has been handed to `snmptt` the data in the SNMP trap is the same regardless of it being v2 or v3. There are a few specific variables that deal with v2 or v3 traps that `snmptt` can utilize however they do not impact the functionality.

The take away point here is that you must configure `snmptrapd` before it can accept v3 traps, once it has been configured then you can proceed to configure Nagios XI for traps using the Nagios XI Trap Translator (NXTI) or manually in the `snmptt` configuration files.

SNMP v3 Trap Requirements

SNMP v3 traps require the following:

Engine ID

This is an identifier of the device sending the SNMP trap (`engineID`). Every device will have a unique `engineID` which is a hexadecimal number, for example `0x0102030405`. You will need to refer to your device SNMP settings to determine what the `engineID` is.

Username

This is a username that will be used to authenticate the incoming trap, also known as the `securityName`.

Security Level

The security level determines if passphrase(s) are required:

The security level determines if passphrase(s) are required:

- noAuthNoPriv
  - The username does **not** require any passphrases
- authNoPriv
  - The username requires an **authentication passphrase**, example:
    - Auth3nticati0n PASSPHRAS3
  - An **authentication protocol** also needs to be defined
    - MD5 or SHA
- authPriv
  - The username requires an **authentication passphrase** *(see above)* AND an **encryption passphrase**, example:
    - 3ncrypti0n PASSPHRAS3
  - An **encryption protocol** also needs to be defined
    - AES or DES

Once you have gathered this required information you will be ready to configure snmptrapd to accept SNMP v3 traps.

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
```

The **disableAuthorization** directive allows SNMP v2 traps from any device to be sent to Nagios XI. Even if this line exists the Nagios XI server will not be able to receive SNMP v3 traps unless the server has been specifically configured for SNMP v3 traps.

If you did not want your Nagios XI server to accept SNMP v2 traps from any device then you need 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 v3 User - noAuthNoPriv

This example will allow SNMP v3 traps from the user called user_one who is configured for noAuthNoPriv. One the second line you add, the noauth setting is required to tell snmptrapd that it can accept unauthenticated traps.

```
#disableAuthorization yes
createUser -e 0x0102030405 user_one
authUser log,execute user one noauth
```

```
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 v3 User - authNoPriv

This example will allow SNMP v3 traps from the user called `user_two` who is configured for `authNoPriv`. This requires the **authentication protocol** and **passphrase** to be defined.

```
#disableAuthorization yes
createUser -e 0x0102030405 user_one
authUser log,execute user_one noauth
createUser -e 0x0203040506 user_two SHA "Auth3nticati0n PASSPHRAS3"
authUser log,execute user_two
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. When sending a test trap using the `snmptrap` command you'll need to define the security level by using **`-l authNoPriv`** in the command.

Restrict To SNMP v3 User - authPriv

This example will allow SNMP v3 traps from the user called `user_three` who is configured for `authPriv`. This requires the **authentication protocol** and **passphrase** as well as the **encryption passphrase** and **protocol** to be defined.

```
#disableAuthorization yes
createUser -e 0x0102030405 user_one
authUser log,execute user_one noauth

createUser -e 0x0203040506 user_two SHA "Auth3nticati0n PASSPHRAS3"
authUser log,execute user_two
createUser -e 0x0304050607 user_three SHA "Auth3nticati0n PASSPHRAS3" AES "3ncrypti0n PASSPHRAS3"
authUser log,execute user_three
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. When sending a test trap using the `snmptrap` command you'll need to define the security level by using **`-l authPriv`** in the command.

Restrict To Addresses / Subnets

In SNMP v2 it is possible to only allow traps to be received from specific network addresses. This functionality does not exist in SNMP v3, the only way to implement such restriction is by implementing inbound firewall rules or working with the `host.allow` and `hosts.deny` files.

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
```

Further Reading

This KB article only scratches the surface of the SNMP v3 configuration options available, please refer to the following links for mote detailed information:

http://net-snmp.sourceforge.net/wiki/index.php/TUT:SNMPv3_Options

http://net-snmp.sourceforge.net/tutorial/tutorial-4/commands/snmptrap-v3.html

http://net-snmp.sourceforge.net/wiki/index.php/TUT:Configuring_snmptrapd_to_receive_SNMPv3_notifications

Final Thoughts

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

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

Posted by: **tlea** - Tue, Nov 13, 2018 at 7:00 PM. This article has been viewed 4787 times.

Online URL: https://support.nagios.com/kb/article/nagios-xi-snmp-trap-v3-configuration-827.html