Purpose

This document describes how to monitor Linux machines with Nagios XI using SNMP. SNMP is an “agentless” method of monitoring network devices and servers, and is often preferable to installing dedicated agents on target machines.

Target Audience

This document is intended for use by Nagios XI Administrators.

Install SNMP On The Remote Linux Machine

Before you can monitor a Linux machine using SNMP, you'll need to install and configure the necessary. First, you'll need to install the **`net-snmp`** package on the Linux machine. Login to the Linux machine as the root user to complete the next steps.

On RHEL / CentOS systems use the following command:

```
yum install net-snmp
```

On Debian / Ubuntu based systems use the following command:

```
sudo apt-get install snmpd libsnmp-dev
```

Configure SNMP Access On The Remote Linux Machine

Now you must configure access permissions for SNMP on the Linux machine. This guide will focus on SNMP v2c and SNMP v3.

- SNMP v2c
  - Access is granted using a permission, community string and address
  - This documentation will use the following values:
    - Permission: `rocommunity`
    - Community String: `Str0ngC0mmunity`
    - Address: `10.25.5.12`
      - This address is the Nagios XI server address
- SNMP v3
  - Access is granted with a username, permission, security level, authentication and privacy pass-phrases
  - More complicated but also more secure
  - This documentation will use the following values:
    - Username: `nagios`
    - Permission: `rouser`
    - Security Level: `authPriv`
    - Authentication Protocol: `SHA`
    - Authentication Pass-phrase: `Str0ng@uth3ntic@ti0n`
    - Privacy Protocol: `AES`
    - Privacy Pass-phrase: `Str0ngPriv@cy`

SNMP v2c

Using the values defined earlier, the following line will be added to the `/etc/snmp/snmpd.conf` file:

```
rocommunity Str0ngC0mmunity 10.25.5.12
```

The following commands will create a backup of the original file and create a new config file with that line.

On RHEL / CentOS / Oracle Linux systems execute the following commands:

```
cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.bak
echo 'rocommunity Str0ngC0mmunity 10.25.5.12' > /etc/snmp/snmpd.conf
```

On Debian / Ubuntu systems execute the following commands:

```
sudo cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.bak
sudo sh -c "echo 'rocommunity Str0ngC0mmunity 10.25.5.12' > /etc/snmp/snmpd.conf"
```

Now restart the **`snmpd`** service using one of the following commands.

On RHEL / CentOS / Oracle Linux 5.x / 6.x systems execute the following commands:

```
service snmpd restart
```

On RHEL / CentOS / Oracle Linux 7.x systems execute the following commands:

```
systemctl restart snmpd.service
```

On Debian 7.x / Ubuntu 13.x 14.x systems execute the following commands:

```
sudo service snmpd restart
```

On Debian 8.x / 9.x and Ubuntu 15.x /16.x / 17.x systems execute the following commands:

```
sudo systemctl restart snmpd.service
```

SNMP v3

Using the values defined earlier, the following command will create the SNMP v3 user and be added to the `/etc/snmp/snmpd.conf` file AND the `/var/lib/net-snmp/snmpd.conf` file. The following commands will create a backup of the original files, create a new config file with that line, add the SNMP v3 user and then restart the service.

On RHEL / CentOS / Oracle Linux 5.x / 6.x systems execute the following commands:

```
cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.bak
service snmpd stop
echo '' > /etc/snmp/snmpd.conf
net-snmp-create-v3-user -ro -a SHA -A Str0ng@uth3ntic@ti0n -x AES -X Str0ngPriv@cy nagios
service snmpd start
```

On RHEL / CentOS / Oracle Linux 7.x systems execute the following commands:

```
cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.bak
systemctl stop snmpd.service
echo '' > /etc/snmp/snmpd.conf
net-snmp-create-v3-user -ro -a SHA -A Str0ng@uth3ntic@ti0n -x AES -X Str0ngPriv@cy nagios
sudo systemctl start snmpd.service
```

On Debian 7.x / Ubuntu 13.x 14.x systems execute the following commands:

```
sudo cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.bak
sudo service snmpd stop
sudo sh -c "echo '' > /etc/snmp/snmpd.conf"
sudo net-snmp-create-v3-user -ro -a SHA -A Str0ng@uth3ntic@ti0n -x AES -X Str0ngPriv@cy nagios
sudo service snmpd start
```

On Debian 8.x / 9.x and Ubuntu 15.x /16.x / 17.x systems execute the following commands:

```
sudo cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.bak
sudo systemctl stop snmpd.service
sudo sh -c "echo '' > /etc/snmp/snmpd.conf"
sudo net-snmp-create-v3-user -ro -a SHA -A Str0ng@uth3ntic@ti0n -x AES -X Str0ngPriv@cy nagios
sudo sudo systemctl start snmpd.service
```

Configure Inbound Firewall Rules On The Remote Linux Machine

If you have the operating system firewall enabled you'll need to allow UDP port 161 inbound. The commands for this vary depending on your operating system.

On RHEL / CentOS / Oracle Linux 5.x / 6.x systems execute the following commands:

```
iptables -I INPUT -p udp --destination-port 161 -j ACCEPT
service iptables save
```

On RHEL / CentOS / Oracle Linux 7.x systems execute the following commands:

```
firewall-cmd --zone=public --add-port=161/udp
firewall-cmd --zone=public --add-port=161/udp --permanent
```

On Ubuntu systems execute the following commands:

```
sudo ufw allow snmp
sudo ufw reload
```

On Debian systems execute the following commands:

```
iptables -I INPUT -p udp --destination-port 161 -j ACCEPT
apt-get install iptables-persistent
```

Answer yes to saving existing rules.

Note: On some systems you may need to add the address of your Nagios server to the allowed hosts file `/etc/hosts.allow`.

Configure The SNMP Daemon To Start On Boot

Configure the SNMP daemon to automatically start when the Linux machine reboots.

On RHEL / CentOS / Oracle Linux 5.x / 6.x systems execute the following commands:

```
chkconfig snmpd on
```

On RHEL / CentOS / Oracle Linux 7.x systems execute the following commands:

```
systemctl enable snmpd.service
```

On Debian 7.x / Ubuntu 13.x 14.x systems execute the following commands:

```
sudo update-rc.d snmpd defaults
```

On Debian 8.x / 9.x and Ubuntu 15.x /16.x / 17.x systems execute the following commands:

```
sudo systemctl enable snmpd.service
```

Testing SNMP Communication

Before you continue, you'll need to make sure that the Nagios XI server can communicate with the remote Linux server using SNMP.

To do this, establish a terminal session to your Nagios XI server and execute the following commands to run a test query. The examples here are targeting the Linux server `10.25.13.38` and they are using the values defined above:

```
cd /usr/local/nagios/libexec
```

SNMP v2c

```
./check_snmp_storage.pl -H 10.25.13.37 -C Str0ngC0mmunity -m "^/$" -w 2 -c 4
```

SNMP v3

```
./check_snmp_storage.pl -H 10.25.13.37 -l nagios -x Str0ng@uth3ntic@ti0n -X
Str0ngPriv@cy -L SHA,AES -m "^/$" -w 2 -c 4
```

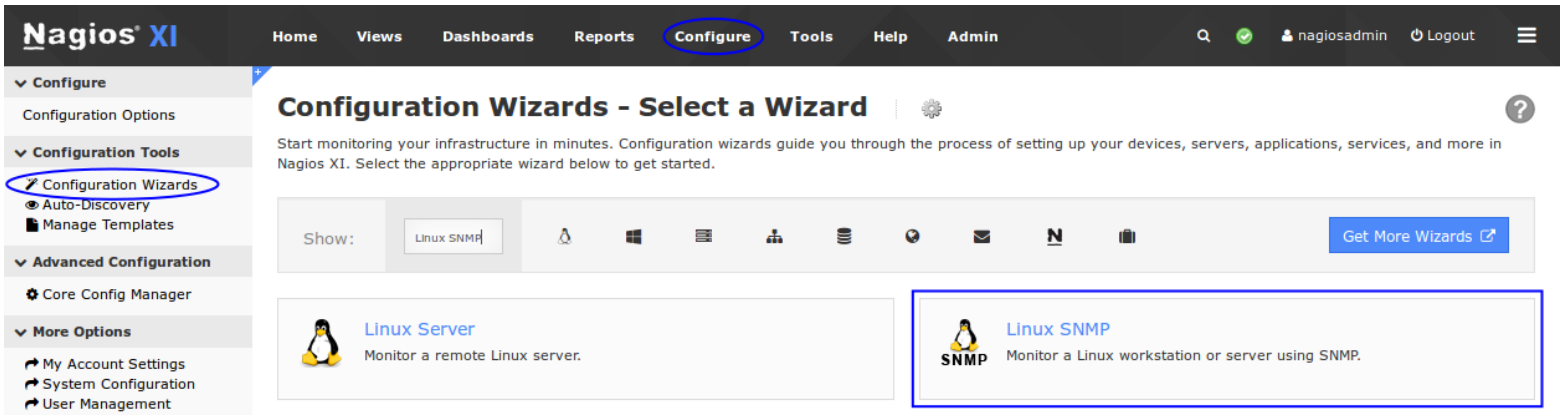
This check should return disk usage information from the remote Linux server, something like:

```
/: 11%used(1550MB/13892MB) (>4%) : CRITICAL
```

Important: If the command doesn't return data, it likely means that SNMP is not configured properly, or that a firewall issue exists on the remote server. In that case, go through the steps in the previous section to ensure everything is configured properly.

Using The Linux SNMP Wizard

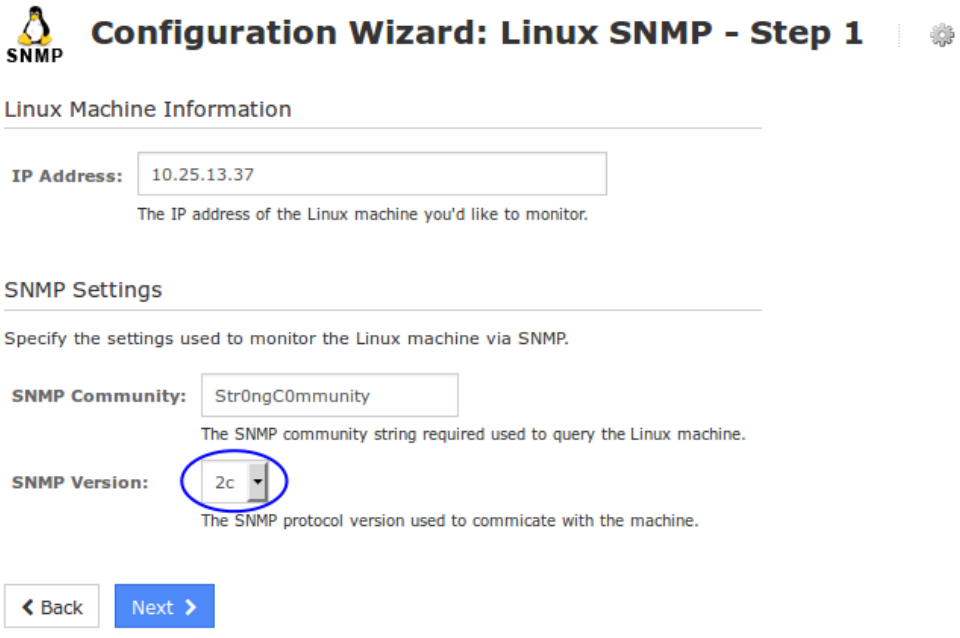
To begin using the Linux SNMP wizard navigate via the top menu bar to **Configure** > **Run a configuring wizard**, and select the **Linux SNMP** wizard. In the following screenshot you can see how the search field allows you to quickly find a wizard.



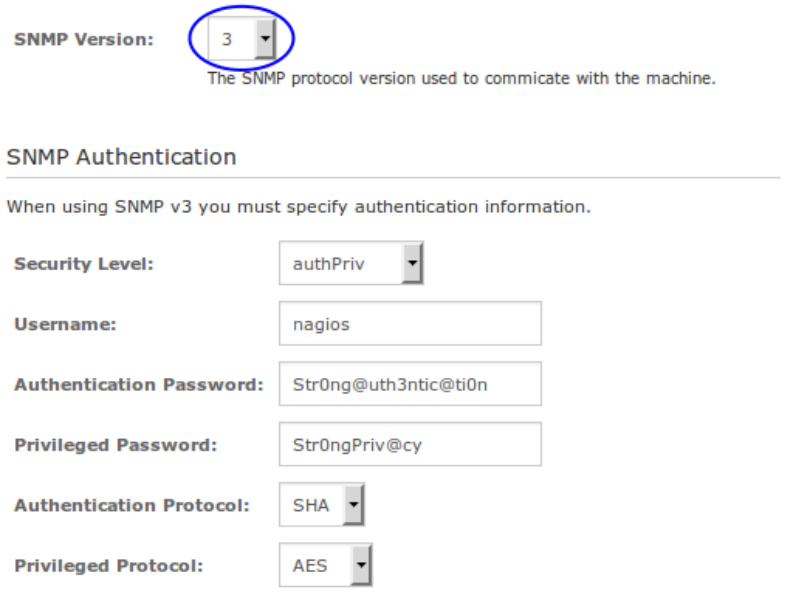
On Step 1 you will be asked to supply the **address** of the server you will monitor via SNMP.

You will also have to provide the appropriate **SNMP Settings**.

This screenshot shows SNMP v2c settings.



This screenshot shows SNMP v3 settings.

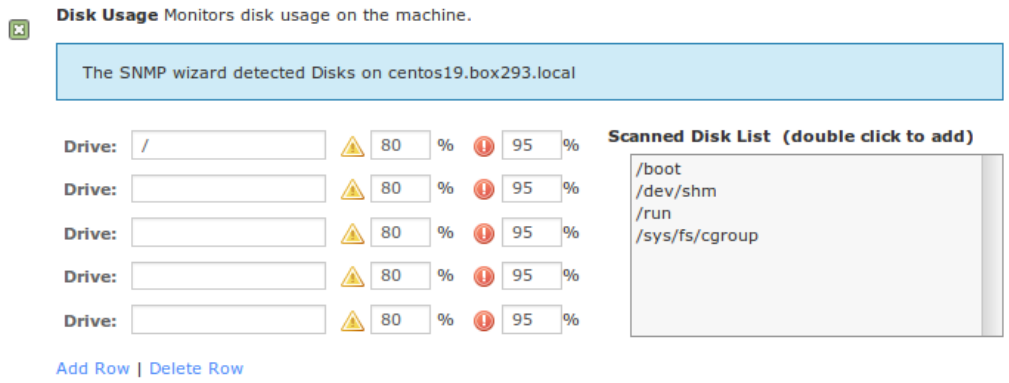


Click Next to progress to step 2.

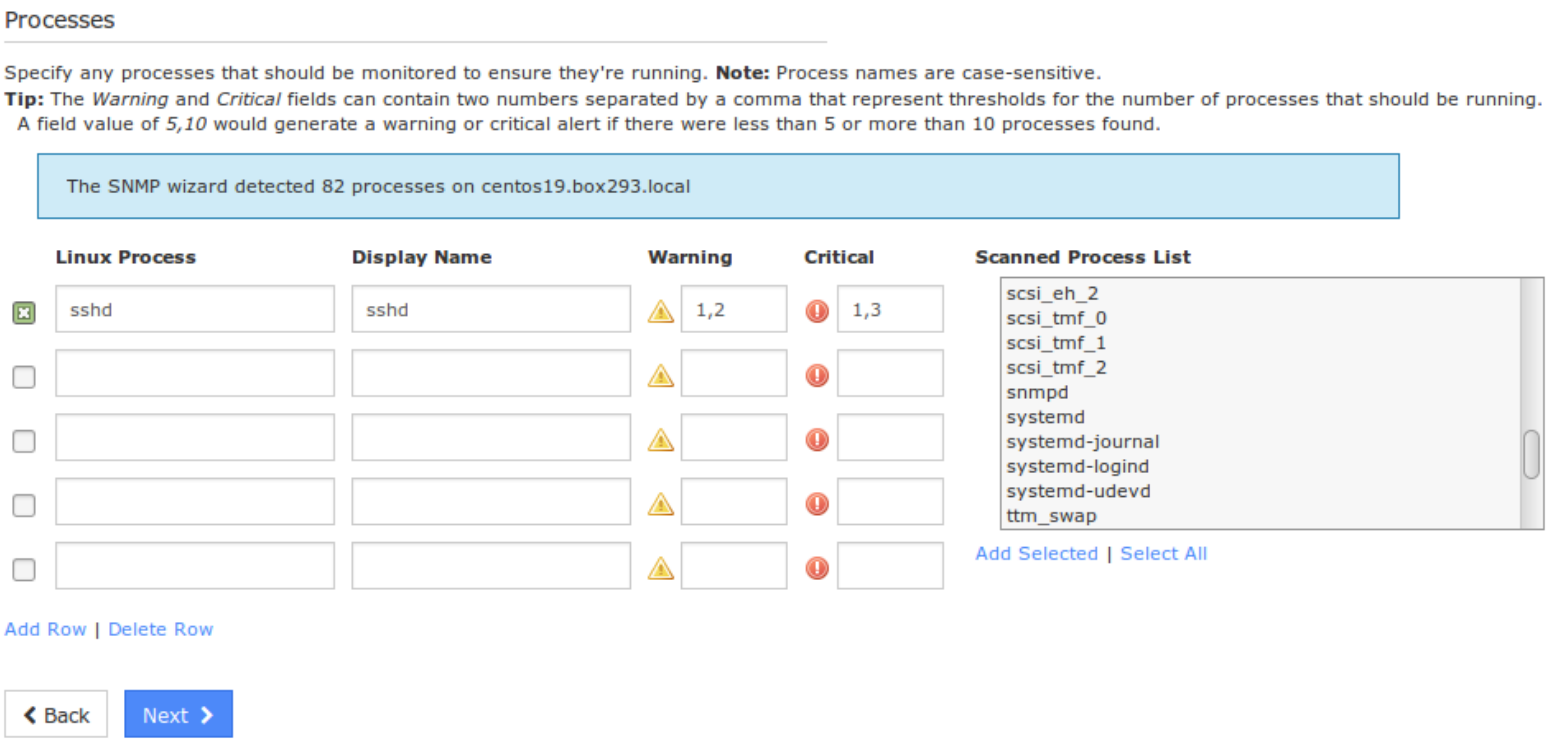
When you proceed to Step 2, the wizard will perform an SNMP query against the Linux server to get a list of the available disks and processes.

Select the server metrics you wish to monitor and adjust the thresholds as required.

With the **Disk Usage** checks, double click a disk in the **Scanned Disk List** to add it to the Drive field. Adjust the thresholds as required.



With the Processes checks, double click a process in the Scanned Process List to add it to the Linux Process field. Adjust the thresholds as required.



When you enter one number in each of the Warning and Critical fields, a WARNING alert will be generated when the amount of processes is below the number specified in the Warning field. A CRITICAL alert will be generated when the number of processes is equal to or below the number specified in the Critical field.

Tip: When you enter two numbers (delimited by a comma), you are specifying a range that is acceptable for the number of processes to be running. In the instance of the `sshd` in the example screenshot, a WARNING alert will be generated if there are (1 or less) **or** (3 or more) instances of sshd running. A CRITICAL alert will be generated if if there is (1 or less) **or** (4 or more) instances running.

Once you've finished selecting all the items you wish to monitor click Next and then complete the wizard by choosing the required options in Step 3 - Step 5.

To finish up, click on **Finish** in the final step of the wizard. This will create the new hosts and services and begin monitoring. Once the wizard applies the configuration, click the **View status details for xxxxx** link to see the new host and services that were created.

Host	Service	Status	Duration	Attempt	Last Check	Status Information
10.25.13.37	/ Disk Usage	Ok	1h 5m 14s	1/5	2016-12-06 11:51:34	/: 10%used(1398MB/14190MB) (<80%) : OK
	CPU Usage	Ok	1h 2m 54s	1/5	2016-12-06 11:49:07	1 CPU, load 1.0% < 80% : OK
	Memory Usage	Ok	1h 4m 42s	1/5	2016-12-06 11:47:18	Physical memory: 23%used(426MB/1840MB) (<80%) : OK
	Ping	Ok	1h 4m 15s	1/5	2016-12-06 11:47:46	OK - 10.25.13.37: rta 0.064ms, lost 0%
	sshd	Critical	1m 14s	4/5	2016-12-06 11:51:45	4 process named sshd (> 1) (> 3 : CRITICAL)
	Swap Usage	Ok	1h 6m 10s	1/5	2016-12-06 11:50:45	Swap space: 0%used(0MB/1640MB) (<80%) : OK

Finishing Up

This completes the documentation on monitoring Linux using SNMP with Nagios XI.

If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

https://support.nagios.com/forum

The Nagios Support Knowledgebase is also a great support resource:

https://support.nagios.com/kb