

How To Monitor Linux Using SNMP In Nagios XI 2024 And 2026

Purpose

This document describes how to monitor Linux machines with Nagios XI 2024 and 2026 using SNMP.

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. Log in to the Linux machine as the root user to complete the next steps.

RHEL / CentOS / Oracle

```
yum install net-snmp
```

Debian / Ubuntu

```
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

How To Monitor Linux Using SNMP In Nagios XI 2024 And 2026

- SNMP v3
 - Access is granted with a username, permission, security level, authentication and privacy passphrases
 - More complicated but also more secure
 - This documentation will use the following values:
 - Username: nagios
 - Permission: rouser
 - Security Level: authPriv
 - Authentication Protocol: SHA
 - Authentication Passphrase: Str0ng@uth3ntic@ti0n
 - Privacy Protocol: AES
 - Privacy Passphrase: 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
```

Create Backup

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

RHEL / CentOS / Oracle

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

Debian / Ubuntu

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

How To Monitor Linux Using SNMP In Nagios XI 2024 And 2026

Restart Service

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

RHEL / CentOS / Oracle

```
systemctl restart snmpd.service
```

Debian and Ubuntu

```
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.

RHEL / CentOS / Oracle

```
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
```

Debian and Ubuntu

```
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 systemctl start snmpd.service
```

How To Monitor Linux Using SNMP In Nagios XI 2024 And 2026

Configure Inbound Firewall Rules On The Remote Linux Machine

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

RHEL / CentOS / Oracle

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

Ubuntu

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

Debian

```
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.

RHEL / CentOS / Oracle

```
systemctl enable snmpd.service
```

Debian and Ubuntu

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

How To Monitor Linux Using SNMP In Nagios XI 2024 And 2026

Testing SNMP Communication

Before you continue, you will 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

Note this is a single long command with \ line continuation character after the first line

```
./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:

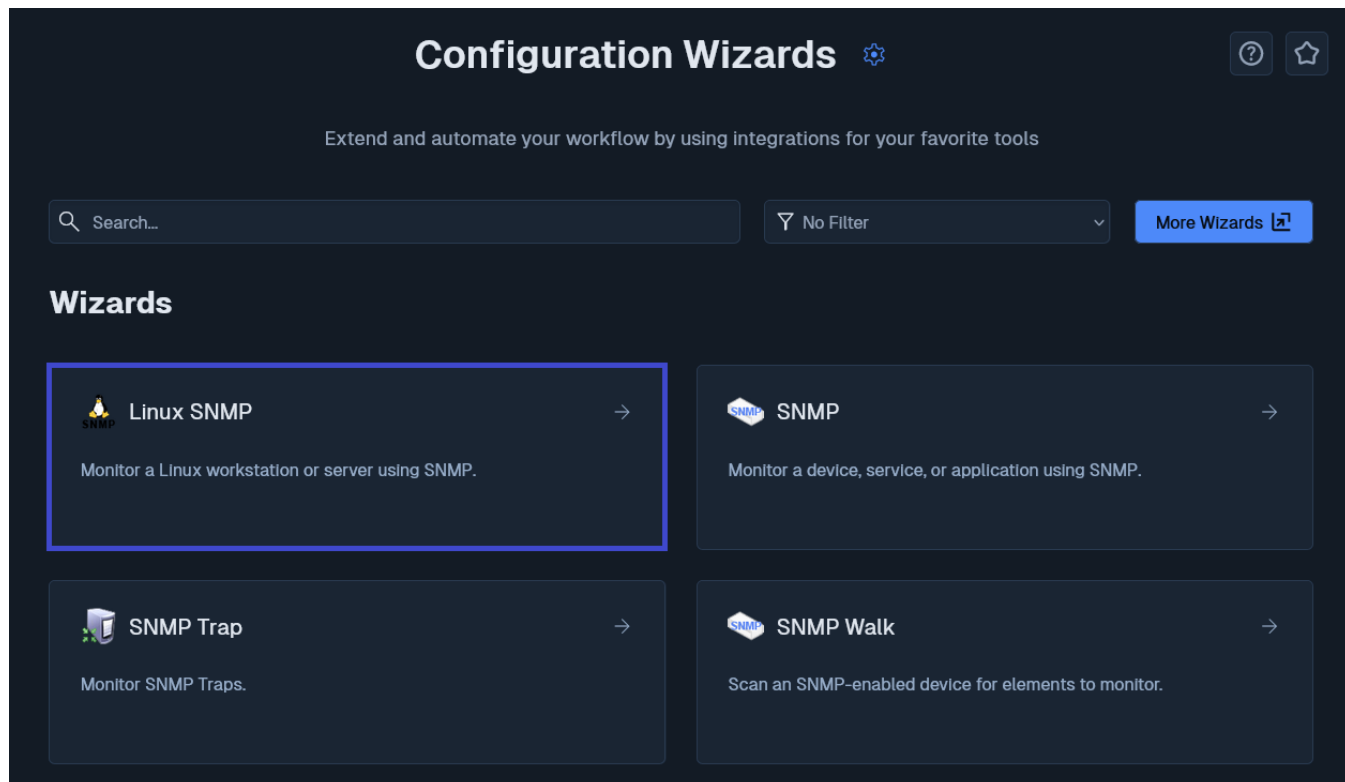
```
/: 11%used(1550MB/13892MB) (>4%) : CRITICAL
```

Important Note: If the command does not 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.

How To Monitor Linux Using SNMP In Nagios XI 2024 And 2026

Using The Linux SNMP Wizard

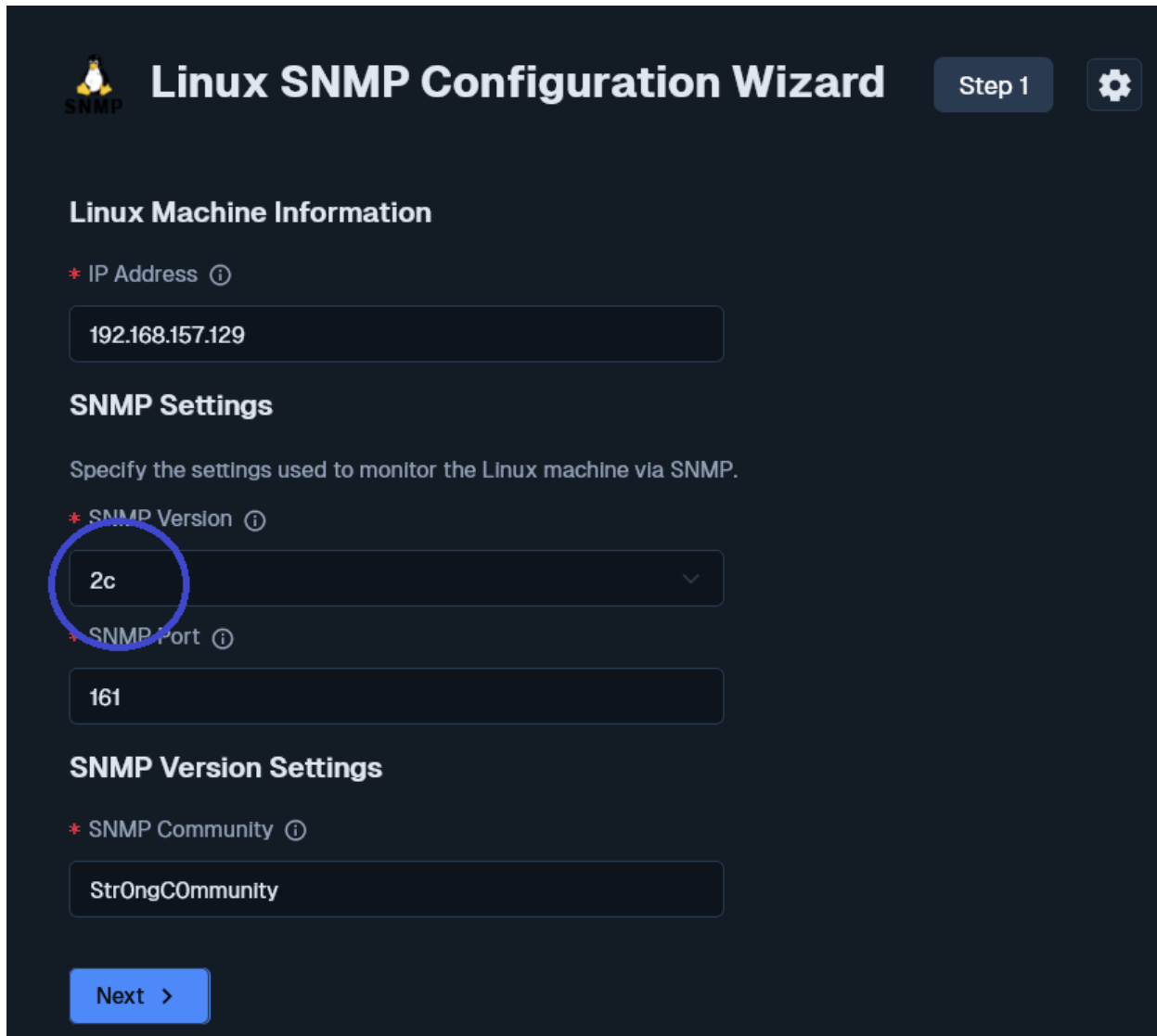
1. To begin using the Linux SNMP Wizard navigate to **Configure > Run a configuring wizard** and select the **Linux SNMP Wizard**. In the following screenshot you can see how the search field allows you to quickly find a wizard.



How To Monitor Linux Using SNMP In Nagios XI 2024 And 2026

2. On **Step 1** provide the following details:
 - a. Supply the **IP Address** of the server you will monitor via SNMP.
 - b. Provide the appropriate **SNMP Settings**.

This screenshot shows **SNMP v2c** settings.



Linux SNMP Configuration Wizard Step 1

Linux Machine Information

* IP Address ⓘ

SNMP Settings

Specify the settings used to monitor the Linux machine via SNMP.

* SNMP Version ⓘ

2c

* SNMP Port ⓘ

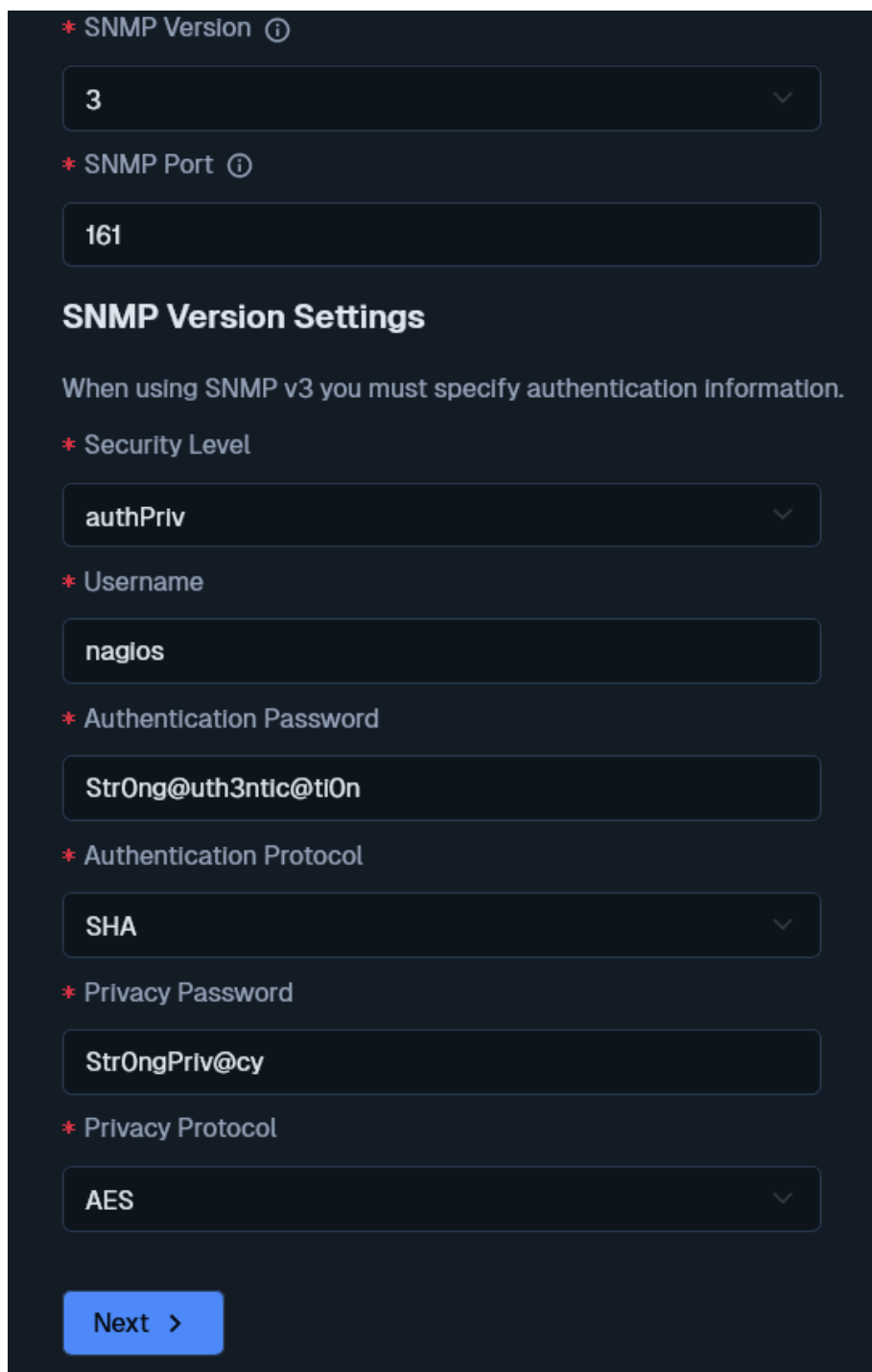
SNMP Version Settings

* SNMP Community ⓘ

Next >

How To Monitor Linux Using SNMP In Nagios XI 2024 And 2026

This screenshot shows SNMP v3 settings



The screenshot displays the configuration interface for SNMP v3 settings in Nagios XI. The settings are as follows:

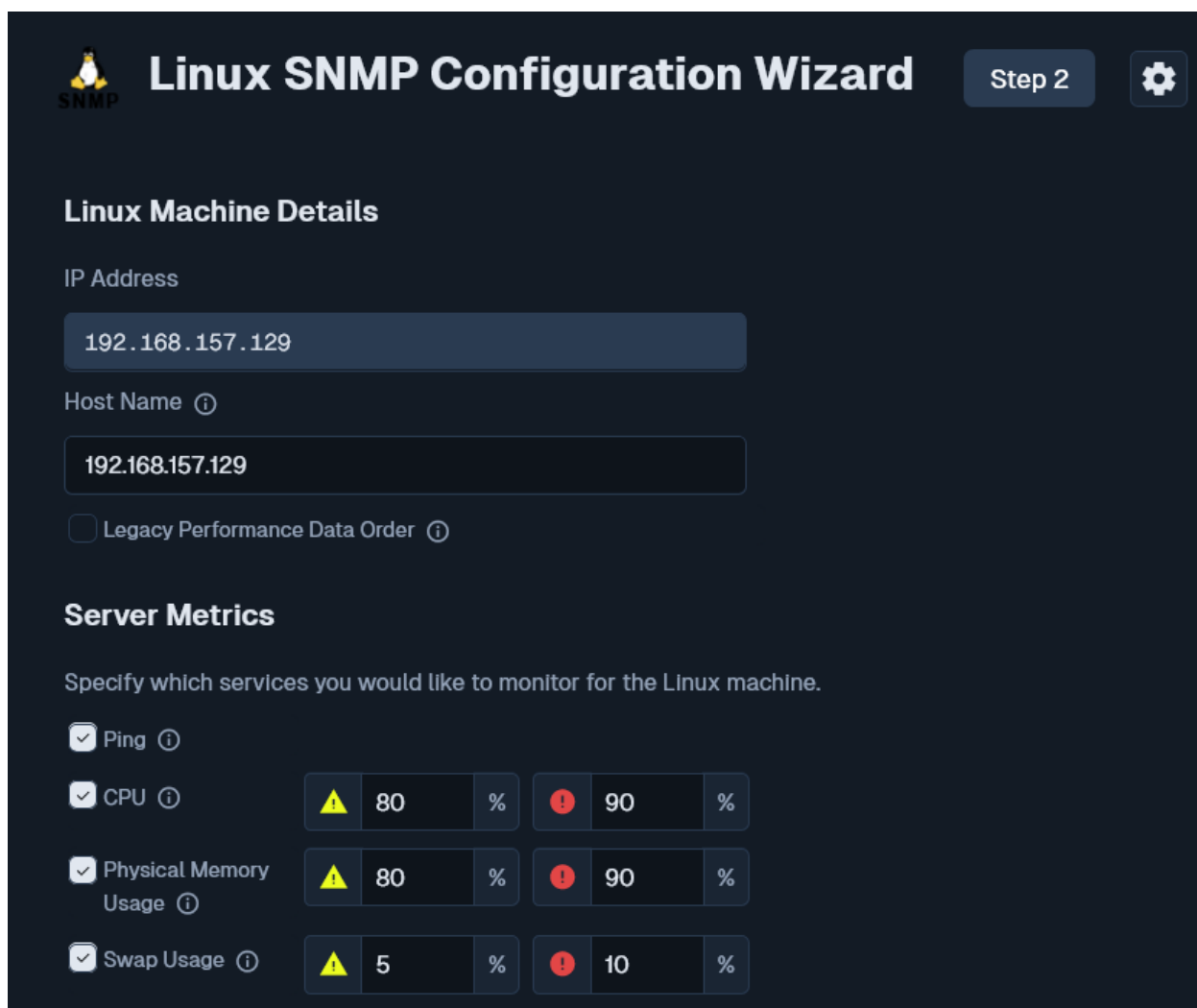
- SNMP Version:** 3
- SNMP Port:** 161
- SNMP Version Settings:** When using SNMP v3 you must specify authentication information.
- Security Level:** authPriv
- Username:** nagios
- Authentication Password:** Str0ng@uth3ntic@ti0n
- Authentication Protocol:** SHA
- Privacy Password:** Str0ngPriv@cy
- Privacy Protocol:** AES

A blue button labeled "Next >" is located at the bottom of the configuration panel.

c. Click **Next** to progress to **Step 2**.

How To Monitor Linux Using SNMP In Nagios XI 2024 And 2026

3. 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.
 - a. Select the **server metrics** you wish to monitor and adjust the thresholds as required.



The screenshot shows the 'Linux SNMP Configuration Wizard' interface at 'Step 2'. The title bar includes the Nagios logo and a settings gear icon. The main heading is 'Linux Machine Details'. Below this, there are two input fields: 'IP Address' with the value '192.168.157.129' and 'Host Name' with the value '192.168.157.129'. A checkbox for 'Legacy Performance Data Order' is present and unchecked. The 'Server Metrics' section is titled 'Specify which services you would like to monitor for the Linux machine.' and contains four checked items: 'Ping', 'CPU', 'Physical Memory Usage', and 'Swap Usage'. Each item has associated warning and critical threshold values and units.

Service	Warning Threshold	Warning Unit	Critical Threshold	Critical Unit
Ping	-	-	-	-
CPU	80	%	90	%
Physical Memory Usage	80	%	90	%
Swap Usage	5	%	10	%

How To Monitor Linux Using SNMP In Nagios XI 2024 And 2026

- b. 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.

The screenshot shows the 'Disk Usage' configuration interface. At the top, a message indicates that the SNMP wizard detected 8 disks and mounts on the IP 192.168.157.129. Below this is a table for configuring disk usage checks. The table has columns for 'Drive', 'Warning' (with a yellow triangle icon and a percentage field), and 'Critical' (with a red exclamation mark icon and a percentage field). The 'Scanned Disk List' on the right contains the following paths: /boot, /dev/shm, /run, /run/lock, /run/snapped/ns, /run/user/0, and /run/user/1001. At the bottom of the table, there are 'Add Row' and 'Delete Row' buttons.

Drive	Warning	Critical	Scanned Disk List (double click to add)
/	80 %	95 %	/boot
	80 %	95 %	/dev/shm
	80 %	95 %	/run
	80 %	95 %	/run/lock
	80 %	95 %	/run/snapped/ns
	80 %	95 %	/run/user/0
	80 %	95 %	/run/user/1001

- c. 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.

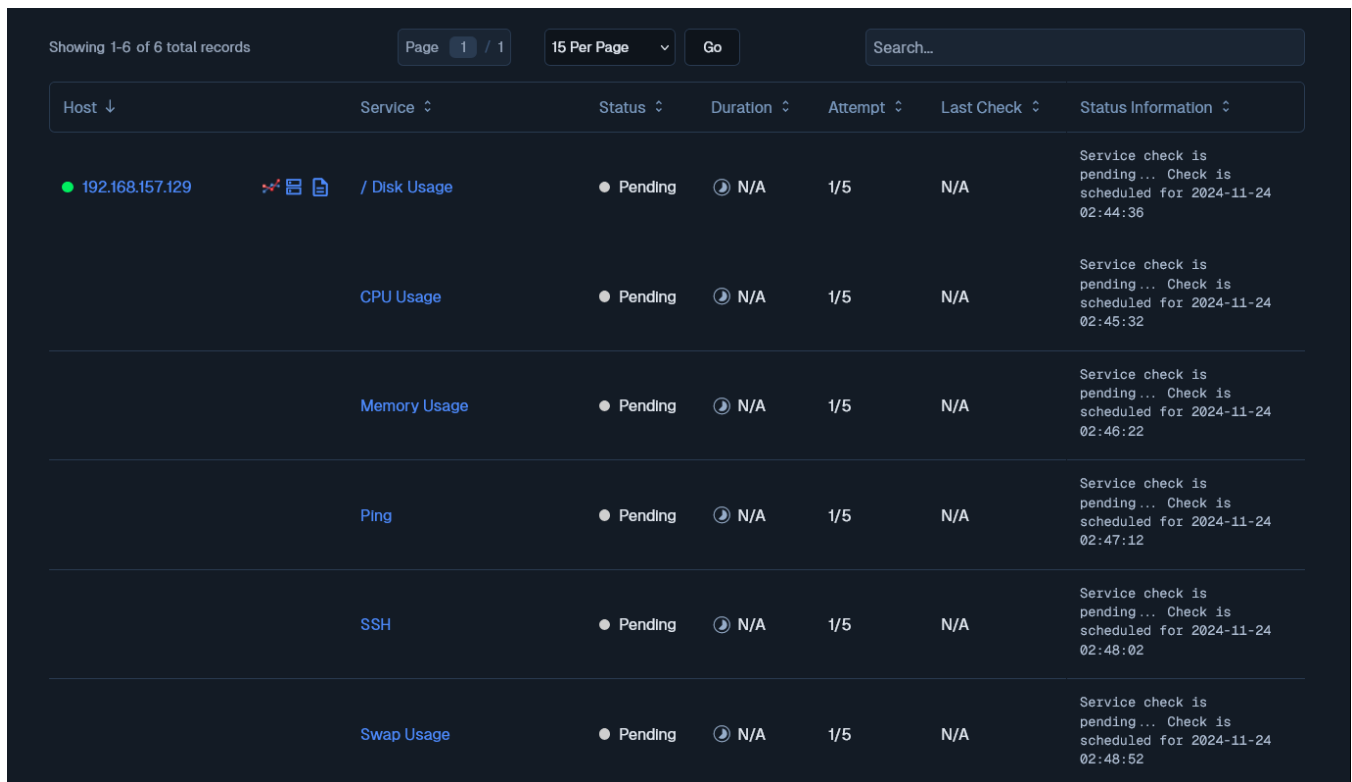
Important: When you enter one number in each of the **Warning** and **Critical** fields, a WARNING alert will be generated when the number of processes is below the number specified in the **Warning** field. A CRITICAL alert will be generated when the number of processes is equal to or below the number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

The screenshot shows the 'Processes' configuration interface. It includes a 'Tips' section and a table for configuring process monitoring. The table has columns for 'Linux Process', 'Display Name', 'Warning Count', and 'Critical Count'. The 'ssh' process is selected and has a Warning Count of 2 and a Critical Count of 3. Other processes listed include httpd (Apache), mysqld (MySQL), and empty rows. At the bottom of the table, there are 'Add Row' and 'Delete Row' buttons.

Linux Process	Display Name	Warning Count	Critical Count
<input type="checkbox"/> httpd	Apache	Warning	Critical
<input type="checkbox"/> mysqld	MySQL	Warning	Critical
<input checked="" type="checkbox"/> sshd	SSH	2	3
<input type="checkbox"/>		Warning	Critical
<input type="checkbox"/>		Warning	Critical

How To Monitor Linux Using SNMP In Nagios XI 2024 And 2026

- 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 **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.



Showing 1-6 of 6 total records

Page 1 / 1 15 Per Page Go Search...

Host ↓	Service ↓	Status ↓	Duration ↓	Attempt ↓	Last Check ↓	Status Information ↓
● 192.168.157.129	/ Disk Usage	● Pending	🕒 N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-11-24 02:44:36
	CPU Usage	● Pending	🕒 N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-11-24 02:45:32
	Memory Usage	● Pending	🕒 N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-11-24 02:46:22
	Ping	● Pending	🕒 N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-11-24 02:47:12
	SSH	● Pending	🕒 N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-11-24 02:48:02
	Swap Usage	● Pending	🕒 N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-11-24 02:48:52

More Information

[Using Configuration Wizards](#)

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 the Nagios Support Forum, Nagios Documentation Hub, or Nagios Library:

[Visit Nagios Support Forum](#)

[Visit Documentation Hub](#)

[Visit Nagios Library](#)