How Alerting Works in Nagios Network Analyzer 2026

Purpose

This document will help you understand how alerting works in Nagios Network Analyzer 2026, and how to set alerts up.

Prerequisites

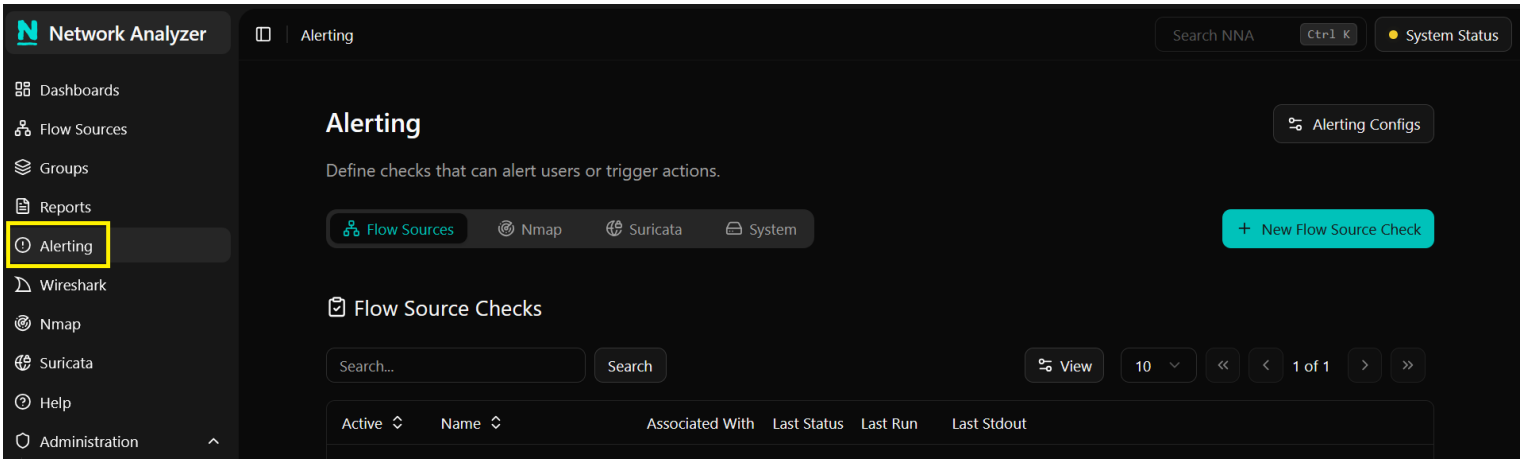
You will need an existing Source to be able to create checks in Nagios Network Analyzer. Information about this can be found in the following documentation:

Understanding Sources And Sourcegroups In Network Analyzer

Alerting In Nagios Network Analyzer

In Nagios Network Analyzer, select **Alerting** from the side navigation bar.

This is the central location to manage and create alerts.



There are multiple alert methods available in Nagios Network Analyzer.

- **Nagios / NRDP** - Send an alert to your Nagios XI or Nagios Core server using NRDP
- **SNMP Receivers** - SNMP Traps can be sent to other applications using the Nagios MIB
- **Commands** - Run a custom command and pass variables to the command
- **Email Users** - Email Nagios Log Server users

For detailed guidance on Nagios / NRDP and the Network Analyzer Wizard, refer to the following comprehensive documentation:

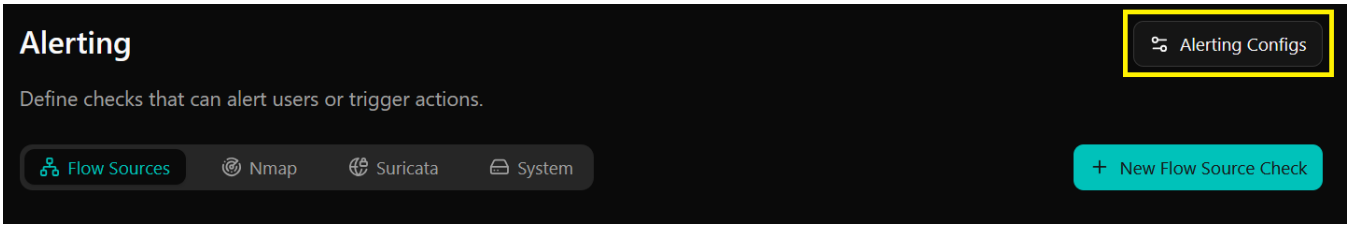
Integrating Nagios Network Analyzer With Nagios XI

The remainder of this documentation will focus on the **Commands**, **SNMP Receivers**, and **Email Users** functionality. The **Commands** and **SNMP Receivers** alert methods require you to define the settings before you can create an alert. These settings are explained first.

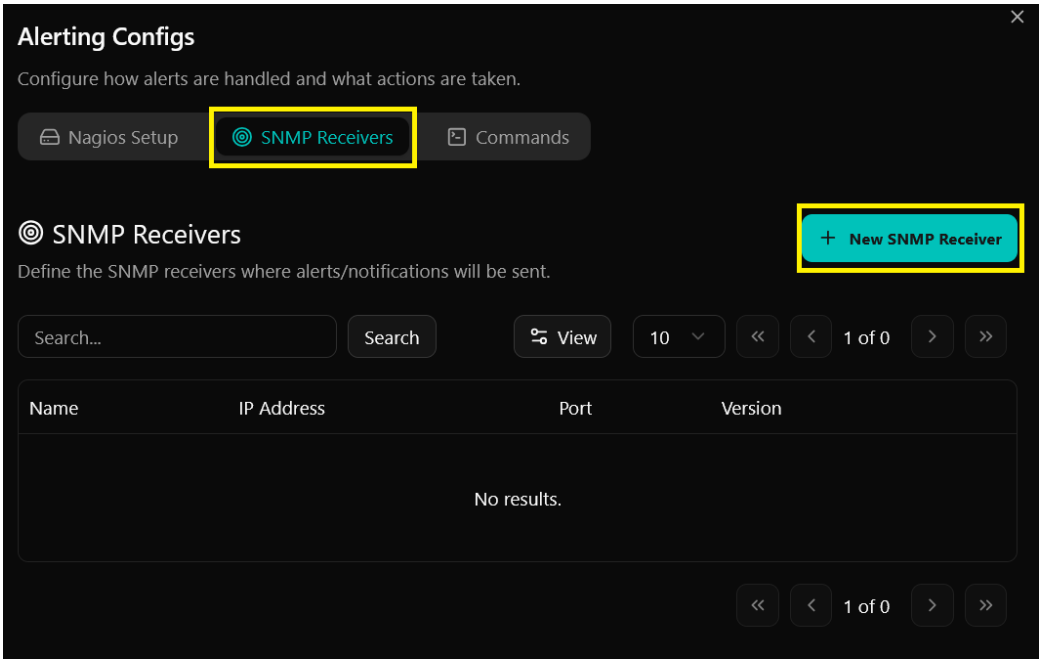
SNMP Receivers

To be able to send alerts to a SNMP Receiver you need to define the details of the receiver.

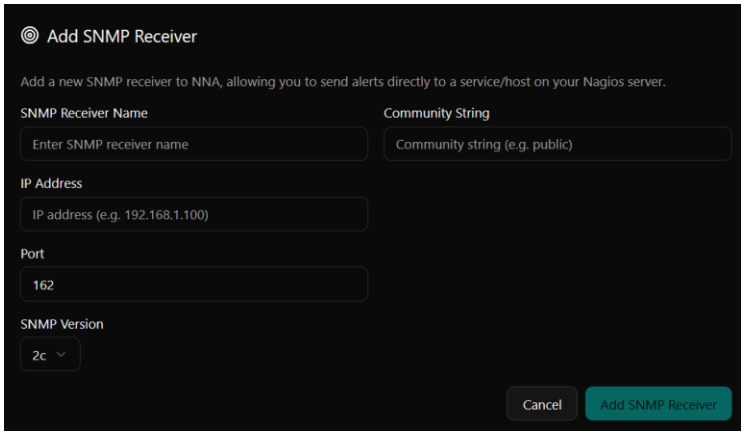
1. On the Alerting page, click **Alerting Configs** button to the right:



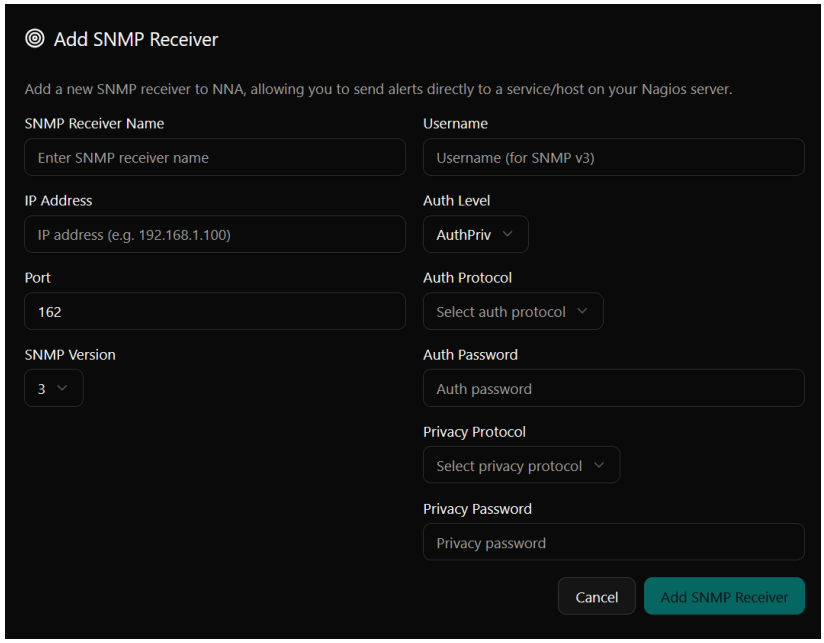
2. Click the middle tab “SNMP Receivers”, then click the blue **+ New SNMP Receiver** button:



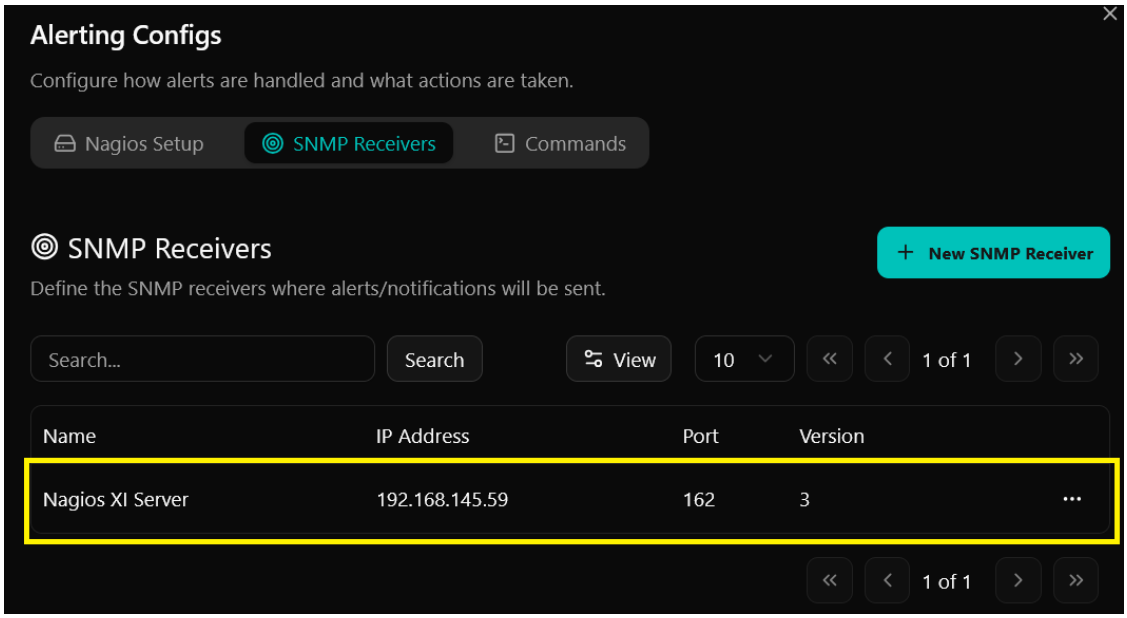
3. You will need to provide the following information:
   - **SNMP Receiver Name:** a friendly name for the SNMP Trap receiver.
   - **IP Address and Port:** The IP address that is receiving traps. Could be an NSTI server or a Nagios XI server that is listening for incoming traps. You also need to define the **Port** the traps can be sent on (162 is the standard default).
   - **SNMP Version:** The version of SNMP you are using; changing the version will change the trap security options available.
     - **Version 2c**



     - **Version 3**



4. Once you have filled in the information, Click **Add SNMP Receiver** button to define the SNMP Receiver. The new command will appear in the list under SNMP Receivers.



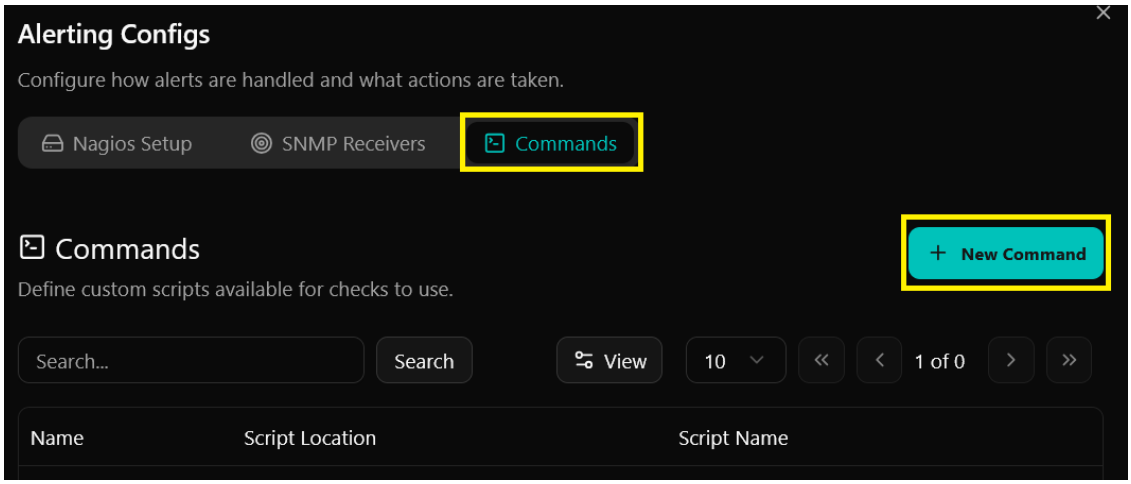
Proceed to the Creating A Check section in this document to define a check that uses the SNMP Receiver.

Commands

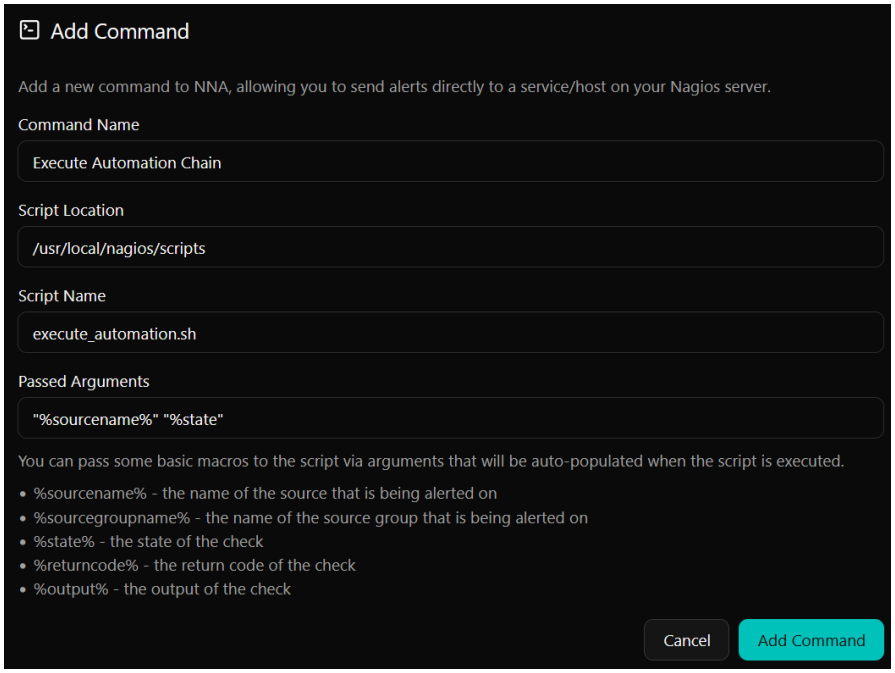
Nagios Network Analyzer allows you to execute a command as an alerting method. This could be a binary command such as `/usr/sbin/sendmail` or your own custom script. If you use your own script you will need to place it somewhere on the system, such as `/usr/local/nagiosna/scripts/`.

Once you've decided on the location of the command you need to define how Nagios Network Analyzer will use it.

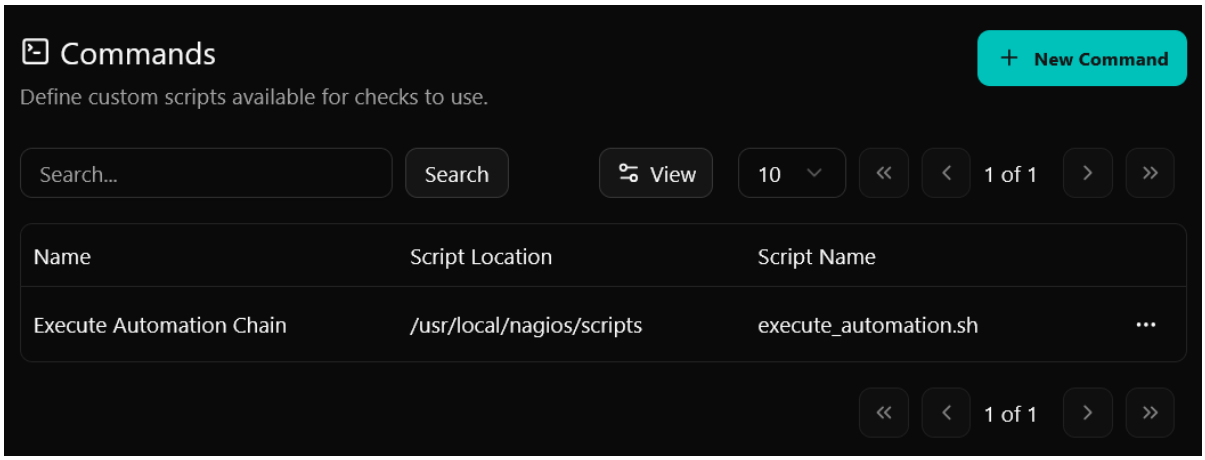
1. On the **Alerting Configs** page, click the **Commands** tab and then click the **+New Command** button.



2. The **Add Command** box will appear.
   - Provide a friendly **Command Name**.
   - Define the **Script Location** and **Script Name**.
   - Define the **Passed Arguments**. This is how you send data to the command, there are Nagios Network Analyzer macros available, and they are explained at the bottom of the modal.
   - Once you've populated all the fields, click the **Add Command** button.



3. The new command will appear in the list on the **Commands** tab.



You can now proceed to the Creating A Check section in this document to define a check that executes the command.

Email Users

To be able to send email alerts in Nagios Network Analyzer you will need to create Nagios Network Analyzer user accounts with their email addresses correctly defined. The following guides provide further details on this part of the setup:

Understanding Email Sending in Nagios Network Analyzer

Managing Users in Nagios Network Analyzer

Once you have done this proceed to the Creating A Check section in this document to define a check that sends emails.

Creating A Check

Checks are how alerts are triggered. The following example creates a check that will notify if a source has no flow data received on the port that the flow data is being received on. After the example, we'll also cover the Nmap and Suricata alert options.

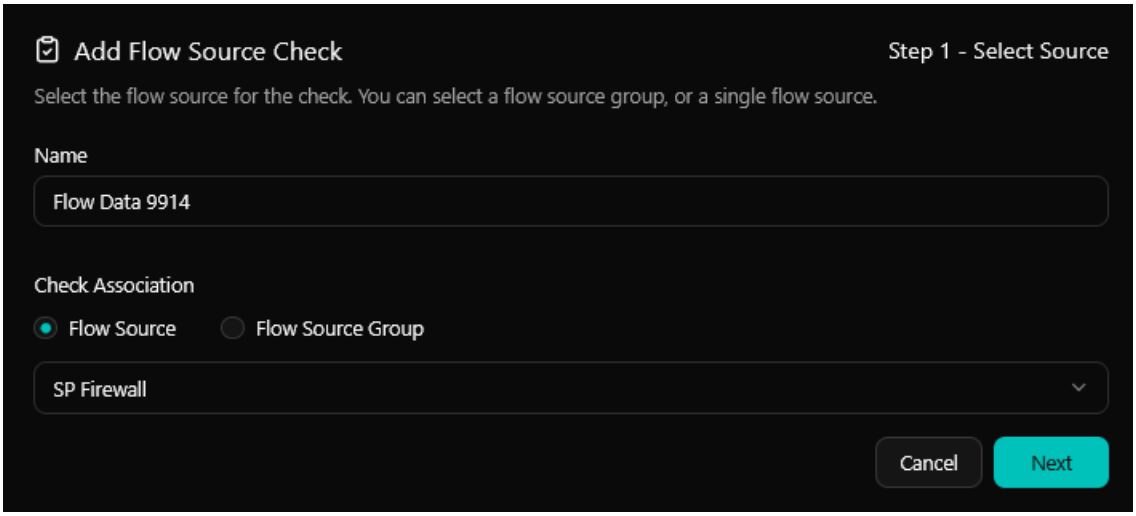
On the **Alerting** page, click the **Flow Sources** tab and then click the **+New Flow Source Check** button.

Step 1 – Select Source

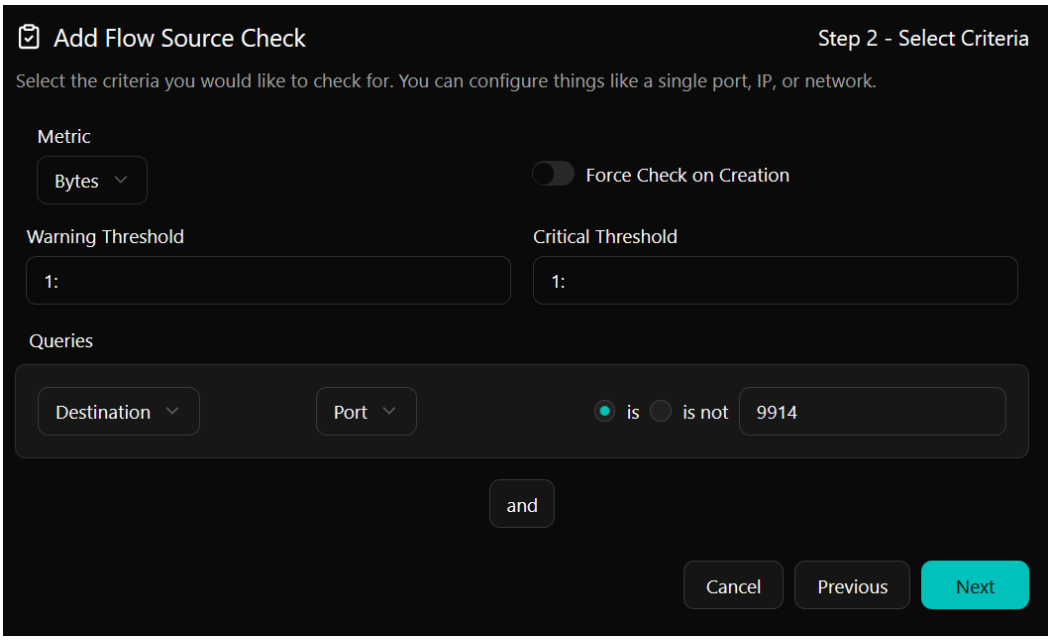
Enter a friendly name for the check for management and organizational purposes. The name can only contain whitespaces and alphanumeric characters.

Select **Flow Source** or **Flow Source Group**. This defines the source/sources the check will get values from.

Click the **Next** button to proceed.



Step 2 – Select Criteria



Metric: Choose the metric to check against. If you want a packet count, choose **Packets**. If you want total bytes, choose **Bytes**. There are multiple traffic dimensions available, and this setting specifies which one will be checked.

Warning threshold is / **Critical threshold is:** After extracting a value from the selected metric, Network Analyzer evaluates it against these thresholds to determine if the state is **WARNING, CRITICAL,** or **OK**. In this example, setting both thresholds to `1:` means that if less than 1 is received, the check will enter a **CRITICAL** state, indicating that no flows were received.

More detailed information on thresholds is explained in the Nagios Threshold Values section of this document.

The bottom half of **this Step** is how you filter what data the check is looking at, as this allows granularity.

In this example, **Flows** is the type of traffic being analyzed. The filter criteria used is:

- **Destination**: Specifies the direction of the flow traffic being examined.
- **Port**: This check is testing to make sure flow data is actually being received, seeing as the flow data is received on a port then this makes it easy to check.
- **is:** Defines the operation; in this case, verify that the **destination port is 9914**.
- **9914:** The specific port number being monitored.

Based on those selections, if no flow data is received it will be in a **CRITICAL** state, otherwise it will be **OK**.

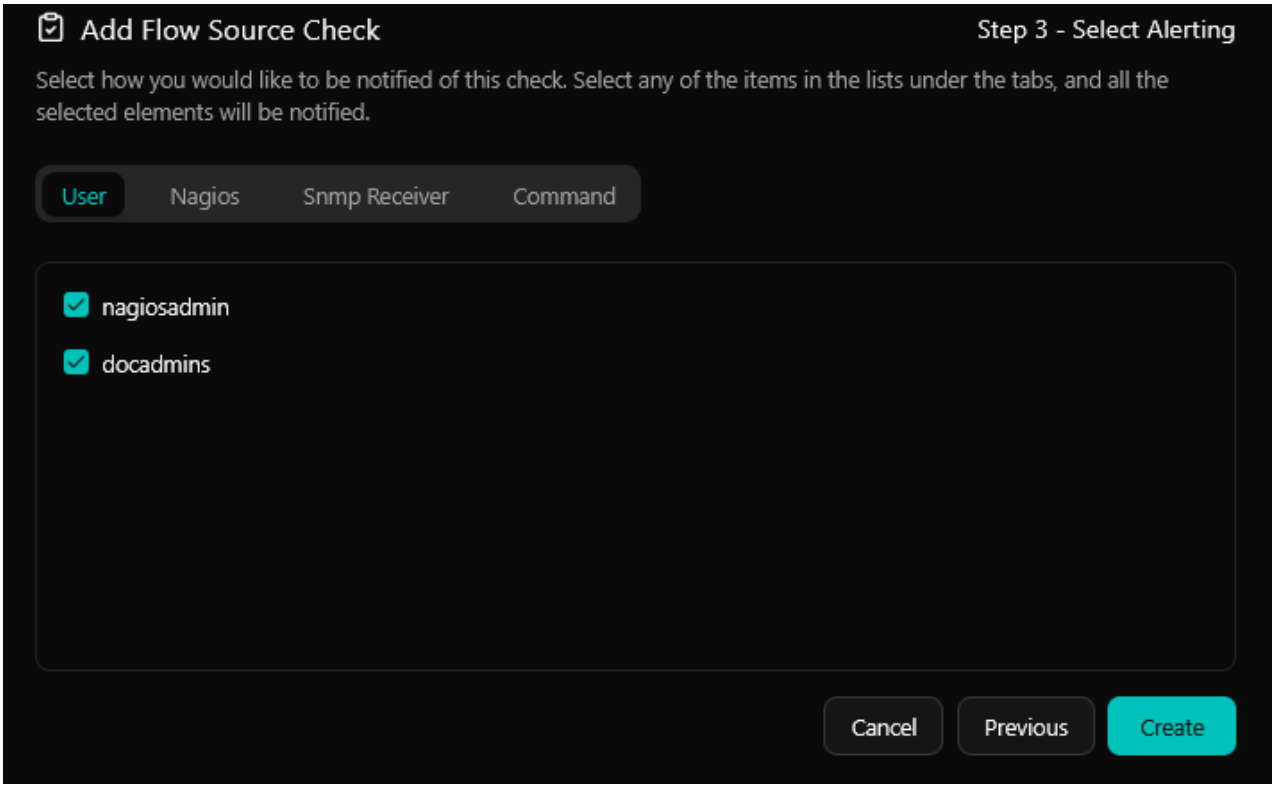
You can specify as many of these filters as you would like by clicking the **and** button. This will add a new box where you can specify additional filters. Please note that it is a Boolean AND, where the traffic must meet all specifications that are chosen for the check to be used.

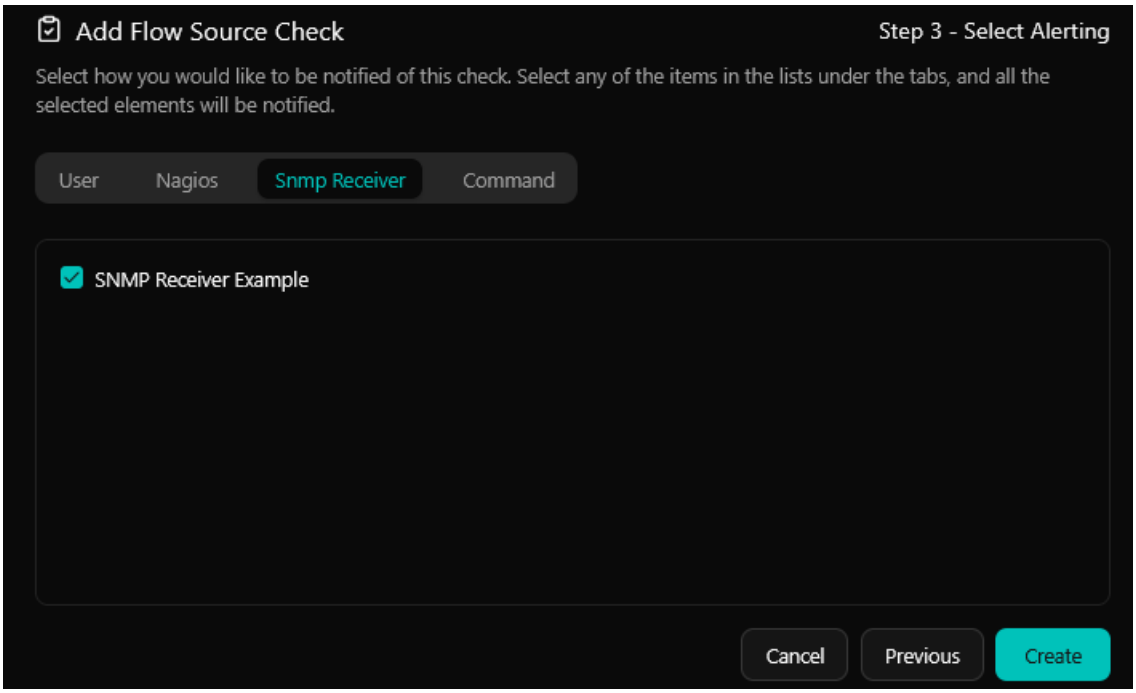
Click the **Next** button to proceed.

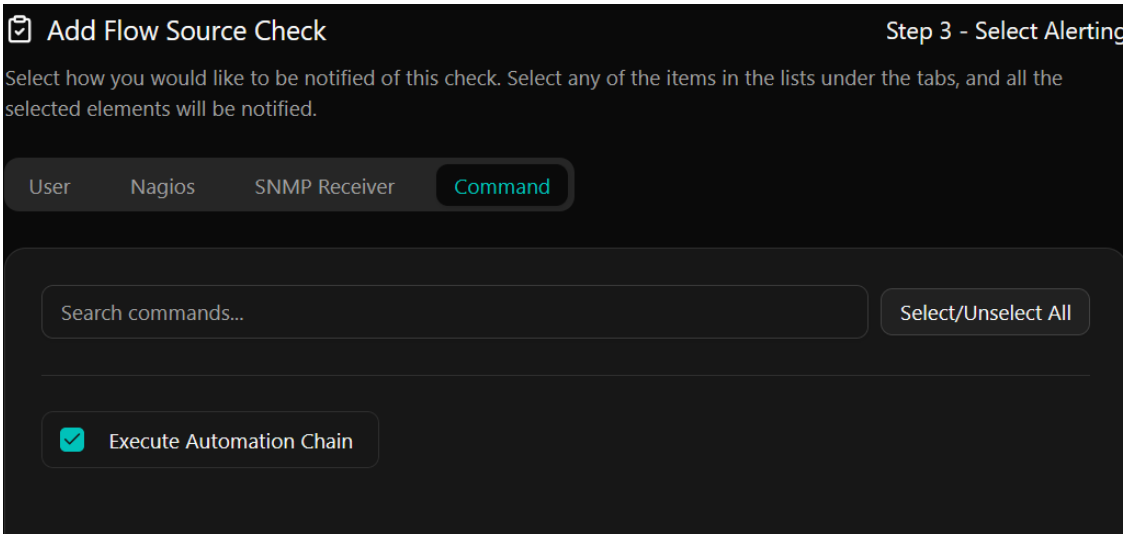
Step 3 – Select Alerting Methods

Here, you choose the alerting method. The following screenshots display the available options. You can select multiple methods across different tabs, for example, sending Emails, and sending an SNMP trap, and executing a Command simultaneously.

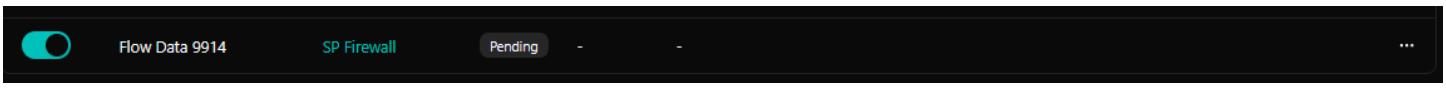
Click the **Create** button to create the alert.



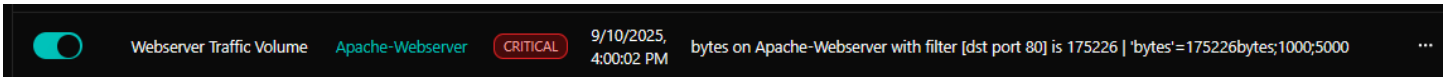




The check will be created and will appear on the screen in a pending state:



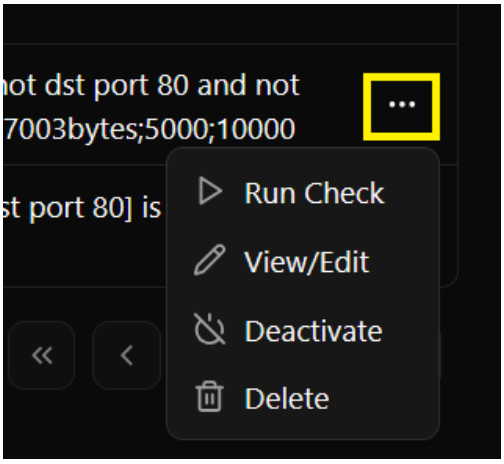
Here is an example of a check in a **CRITICAL** state:



The checks run **every five** minutes, and it's important to understand that each time the check runs, it will send a notification to your alerting method.

Check Actions

There are some actions available for the checks you have defined. On the **Alerting** page, click the **Actions** icon (three horizontal dots) on the line of the alert:



Run Check

Run the check immediately.

View / Edit

Review an existing check and make any changes required.

Deactivate

Deactivate the check without deleting it for future checks.

Delete

Delete the check, no more alerts will be sent.

Nagios Threshold Values

Nagios Thresholds can be complicated to initially understand, but once you grasp them, they can be very powerful. Documentation on Nagios thresholds is available here:

https://nagios-plugins.org/doc/guidelines.html#THRESHOLDFORMAT

The Nagios Threshold standards were designed with many different use cases, including those where negative numbers are valid values. However, in the case of Nagios Network Analyzer, the alert value being tested will always be 0 or greater (no negative numbers are involved).

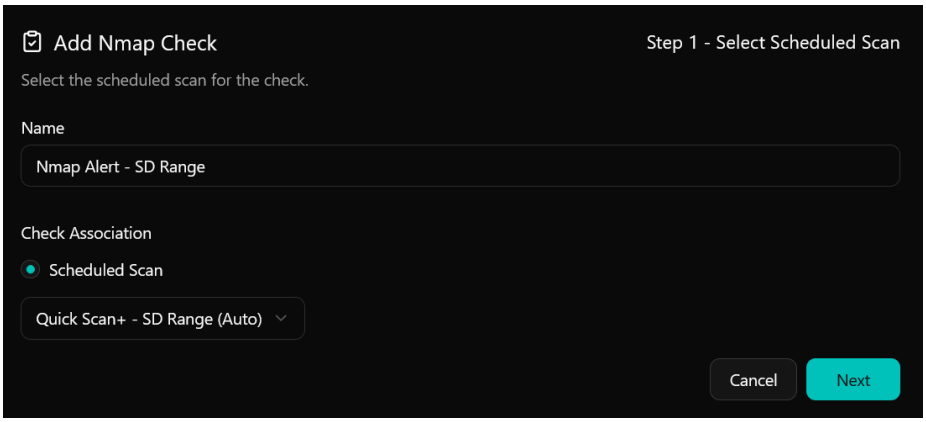
Nmap Alerts

Nmap alerts enable you to monitor the number of open or closed ports found by a Scheduled scan. You can learn more about installing and using Nmap in Network Analyzer 2026 here:

Using Nmap with Network Analyzer 2026

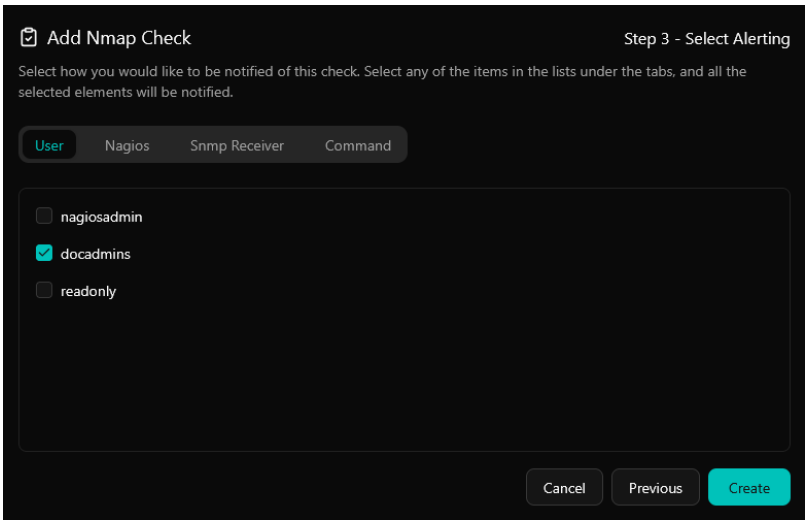
To begin, select the Nmap tab in **Alerting**, then click **+ New Nmap Check**.

Next, input a friendly **Name** for the alert, and choose a Scheduled Scan from the dropdown, then click **Next**.

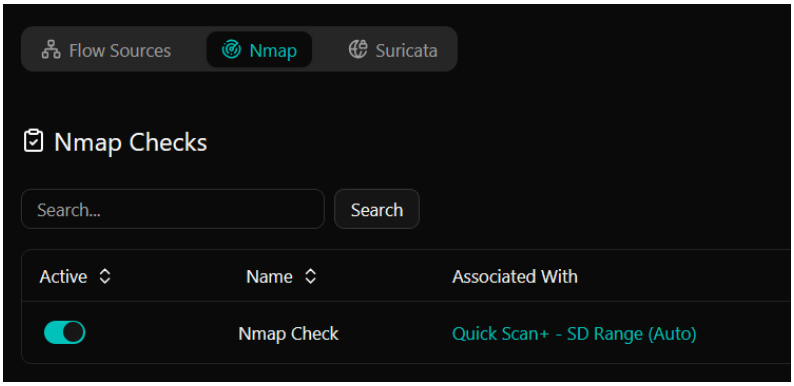


Now choose either Ports Open or Ports Closed from the **Metric** dropdown, and enter your Warning and Critical Threshold values, then click **Next**.

Finally, choose your notification options, and click **Create**.



Your Nmap check will now appear in the **Nmap** tab of the **Alerting** menu.



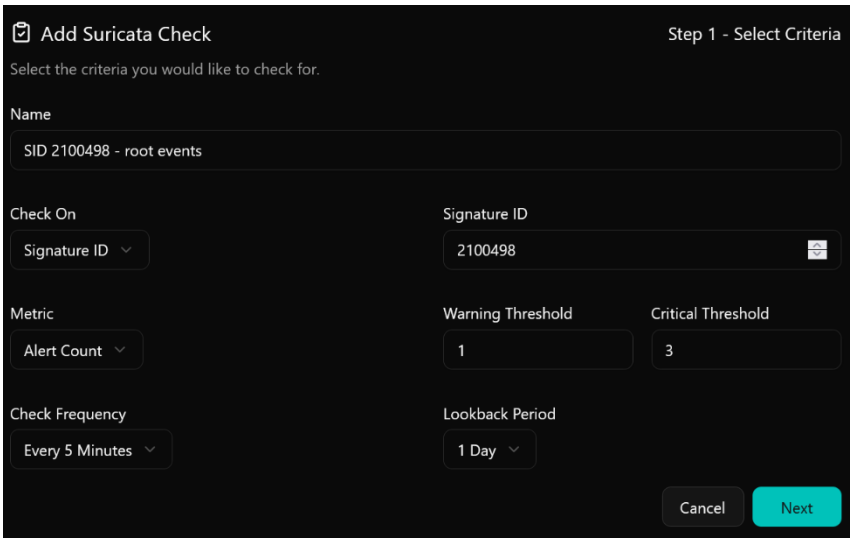
Suricata Alerts

Suricata alerts enable you check for the presence of certain Signature IDs in your Suricata Alerts. You can learn more about installing and using Suricata in Network Analyzer 2026 here:

Using Suricata with Network Analyzer 2026

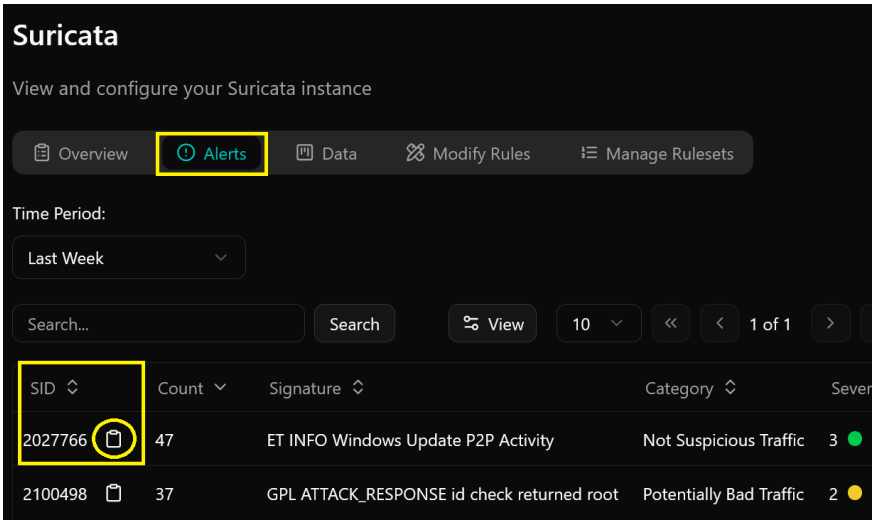
To begin, select the Suricata tab in **Alerting**, then click **+ New Suricata Check**.

In the first page of the **Add Suricata Check** dialog, you'll define a friendly **Name** for the alert, choose the **Signature ID** (SID, see note below) to check for, and define your **Threshold** values, **Check Frequency**, and **Lookback Period** (how far to look back in your Suricata data for matching results).

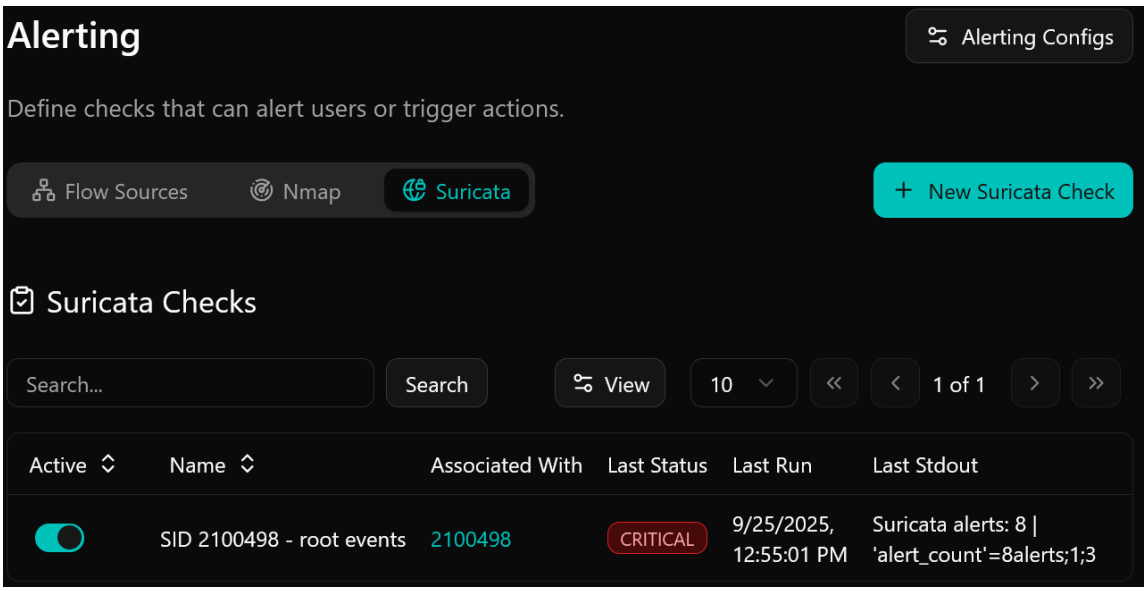


Finding Alert SIDs

You can easily find the SID of your Suricata Alerts in the **Alerts** tab of the Suricata menu. Click the clipboard icon to copy the SID.



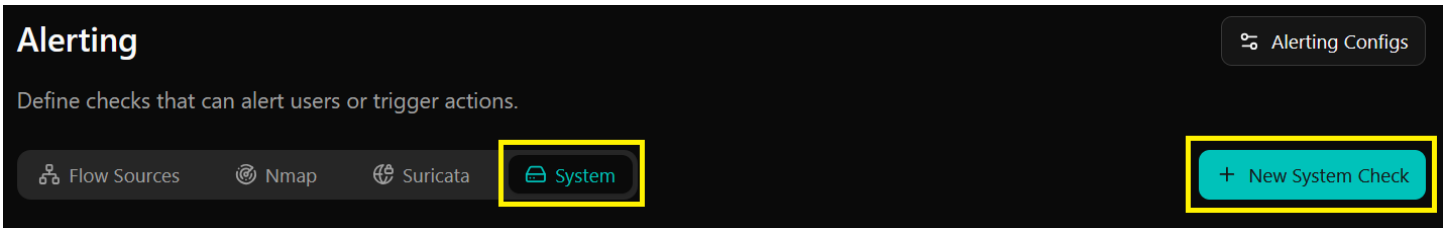
Finalize your Suricata alert by choosing your notification methods, then click **Create**. Your new Suricata check will now appear in the Suricata tab of the Alerting menu.



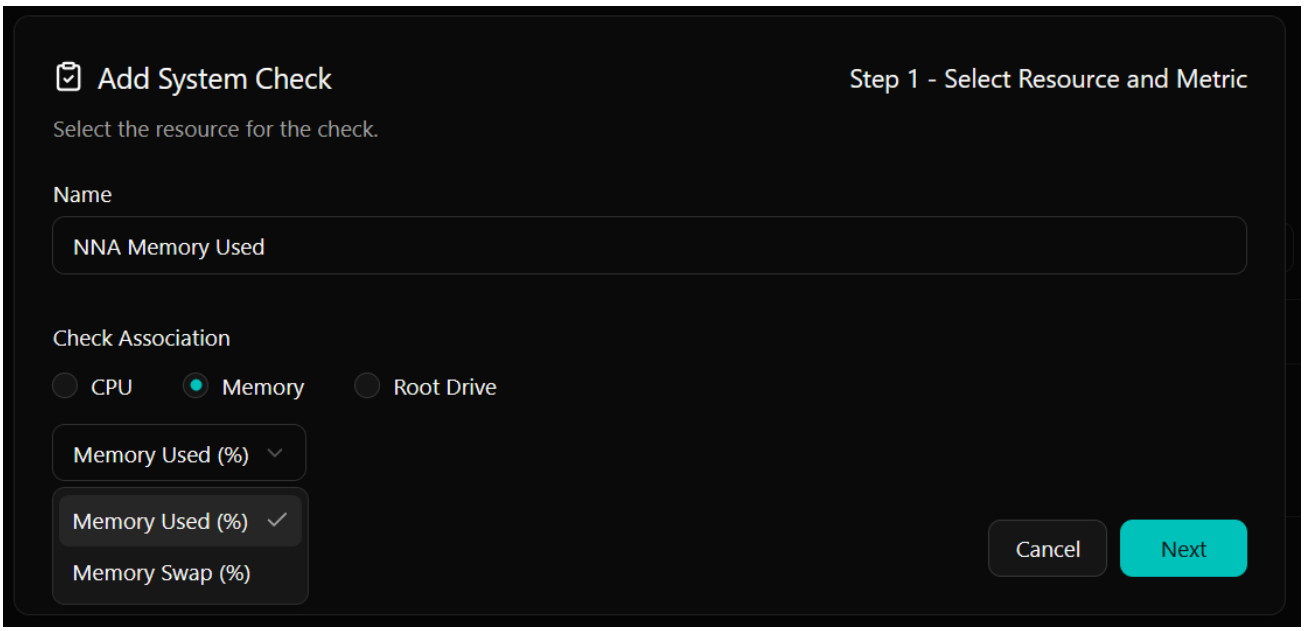
System Alerts

System alerts enable you to run basic checks of resource utilization on your Network Analyzer server, including CPU, Memory, and Root Drive usage.

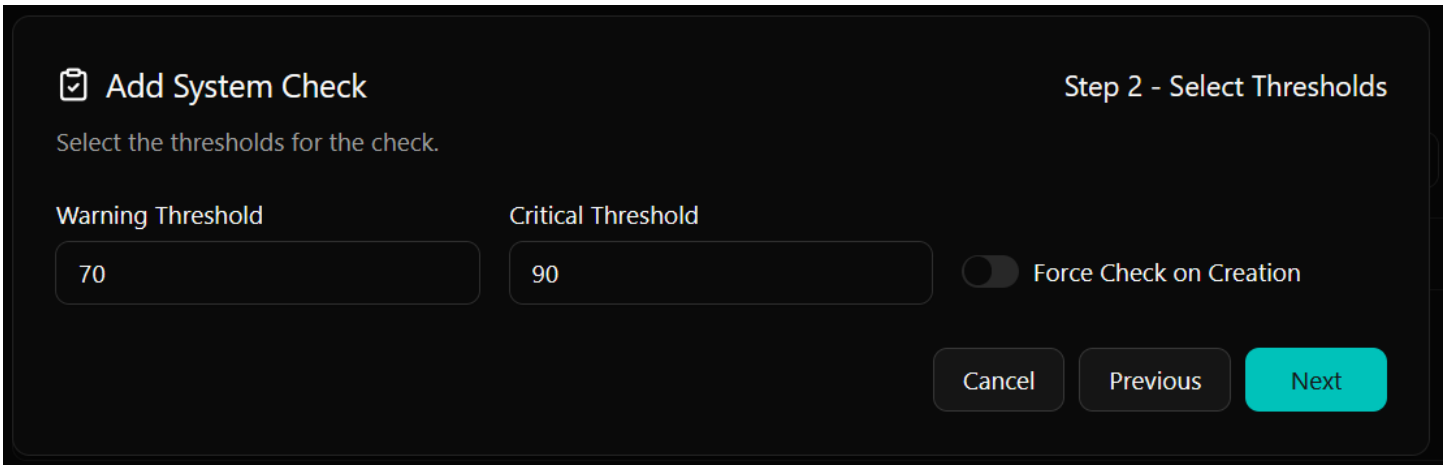
To begin, select the **System** tab in **Alerting**, then click **+ New System Check**:



Next, enter a **Name** for the check, and select the **Check Association**, in **Step 1**:

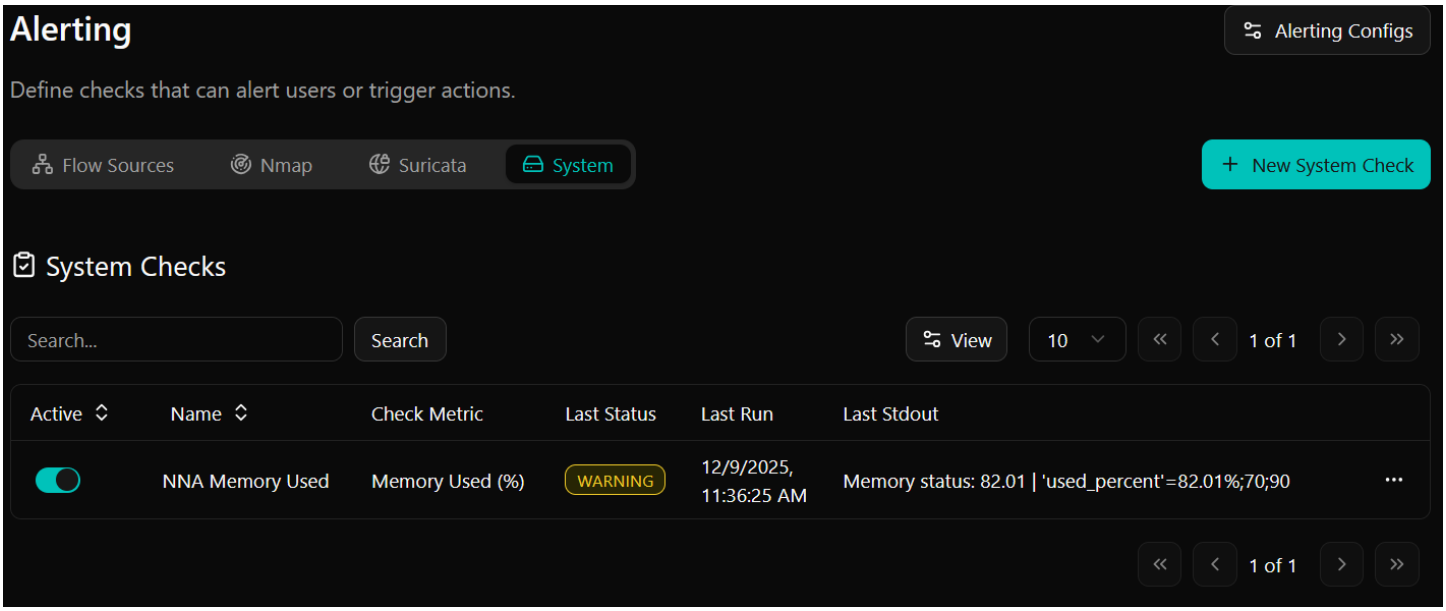


In **Step 2**, define your Warning and Critical thresholds, and choose whether the check should be run immediately after creation with the **Force Check on Creation** toggle (if left off, the check will run for the first time the next time checks are normally scheduled to execute).



Finalize your System check by choosing your notification options in **Step 3**, then click **Create**.

Your new System check will appear in the Alerting menu list:



Finishing Up

This completes the documentation on Understanding Alerting in Nagios Network Analyzer 2026. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum Visit Nagios Knowledge Base Visit Nagios Library