

# Understanding Alerting in NNA 2024

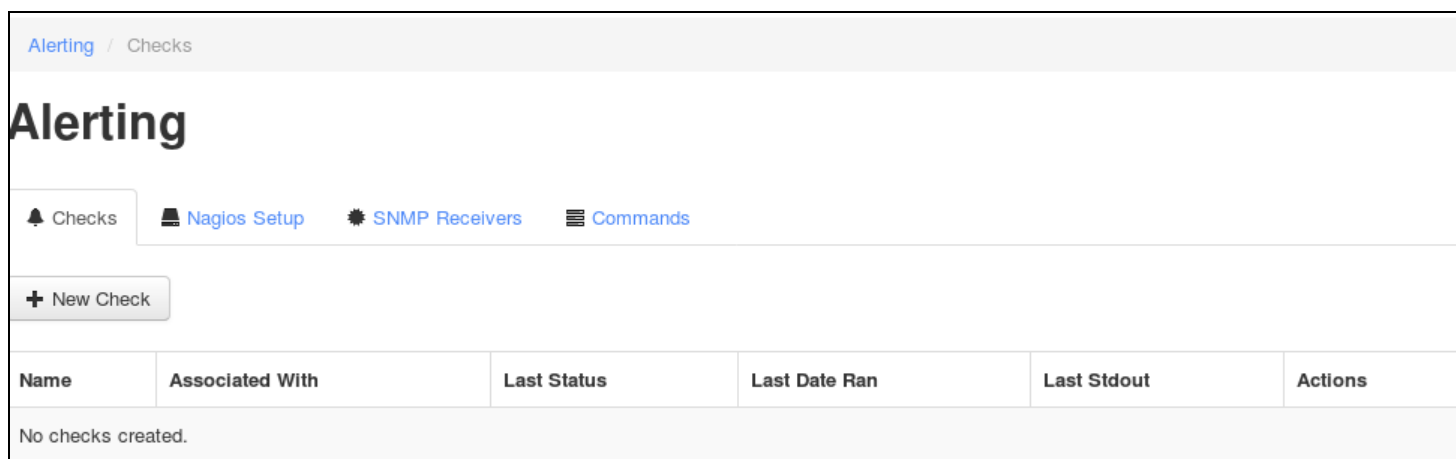
## Prerequisites

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 navigation bar.



Name	Associated With	Last Status	Last Date Ran	Last Stdout	Actions
No checks created.					

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
- Command - Run a custom command and pass variables to the command
- Email Users - Email Nagios Log Server users

- Nagios XI Network Analyzer Wizard - You can use the Nagios XI Network Analyzer Wizard to check your sources for Bytes / Flows / Packets / Abnormal Behavior.

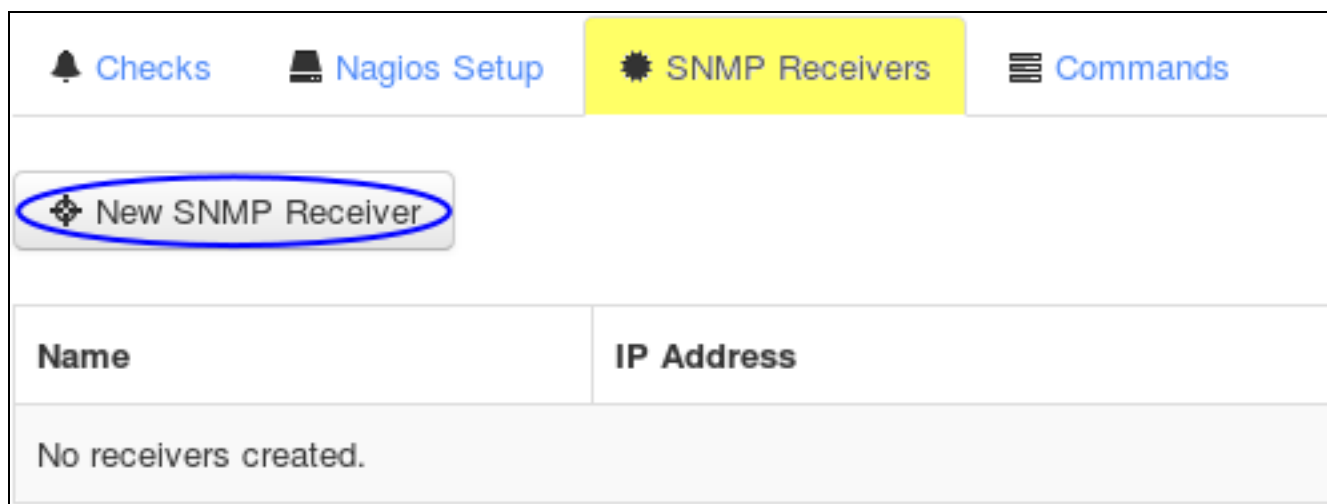
For Nagios / NRDP / Network Analyzer Wizard the following documentation can be used, it is very comprehensive:

[Integrating Nagios Network Analyzer With Nagios XI And Nagios Core](#)

The remainder of this documentation will focus on the Command / SNMP Receivers / Email Users functionality. The Command 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.



The screenshot shows the Nagios XI interface with the 'SNMP Receivers' tab selected. A button labeled 'New SNMP Receiver' is circled in blue. Below the button is a table with two columns: 'Name' and 'IP Address'. The table is currently empty, displaying the text 'No receivers created.'

Name	IP Address
No receivers created.	

1. On the Alerting page click the SNMP Receivers tab.
2. Click the New SNMP Receiver button.

## Enter Information ✕

Enter information about the device that will receive SNMP traps.

Name	<input type="text" value="SNMP Trap Receiver"/>
IP Address	<input type="text" value="10.25.5.13"/>
Port	<input type="text" value="162"/>
SNMP Version	<input type="text" value="2c"/>
Community String	<input type="text" value="public"/>

3. You will need to provide the following information:

**Name:** The name of the SNMP Trap receiver you are adding.

**Receiver Address:** The 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**

**Community String:** The community string that the SNMP Trap receiver will accept traps for. This is commonly public but depends on how your SNMP Trap receiver is configured.

**Version 3**

**Authorization Level:** The authorization method used to send SNMP v3 traps. Your selection here defines the relevant Authorization and Privacy fields that are shown.

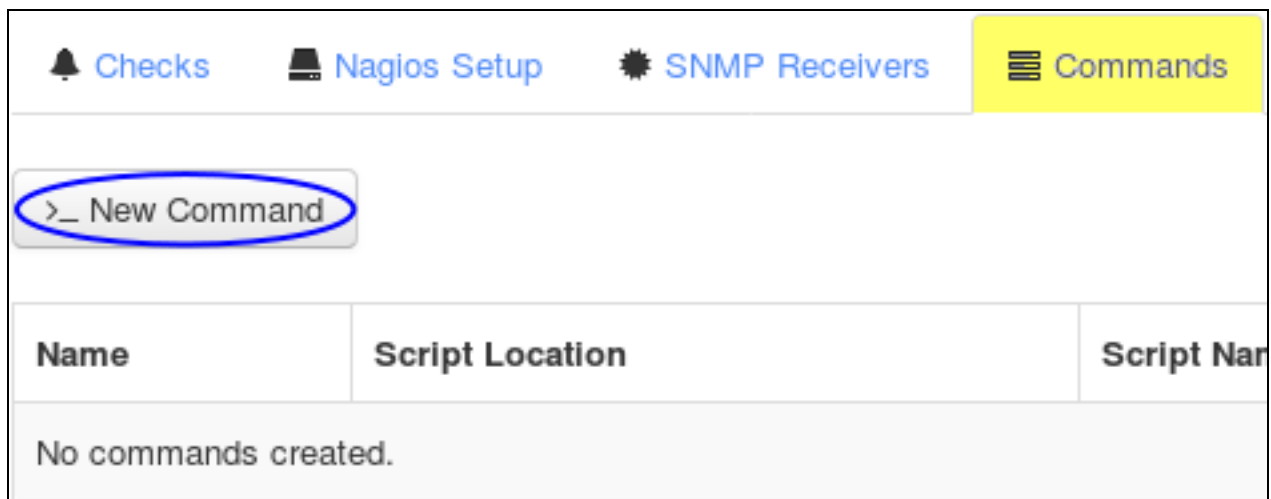
4. Click the Finish & Save button to define the SNMP Receiver. The new command will appear in the list on the SNMP Receivers tab:

Name	IP Address	Version	Actions
SNMP Trap Receiver	10.25.5.13	2	<a href="#">View / Edit</a> <a href="#">Delete</a>

Proceed to the [Creating A Check](#) section in this document to define a check that uses the SNMP Receiver.

**Command**

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/`.



The screenshot shows the Nagios Alerts interface. At the top, there are four tabs: 'Checks', 'Nagios Setup', 'SNMP Receivers', and 'Commands'. The 'Commands' tab is highlighted in yellow. Below the tabs, there is a button labeled '>\_ New Command' which is circled in blue. Below the button is a table with three columns: 'Name', 'Script Location', and 'Script Name'. The table is currently empty, and the text 'No commands created.' is displayed below it.

Name	Script Location	Script Name
No commands created.		

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 page click the Commands tab and then click the >\_ New Command button.

## New Command ✕

Specify a script to run when an alert happens.

Name	<input type="text" value="Log Alert"/>
Script Location	<input type="text" value="/usr/local/nagiosna/scripts"/>
Script Name	<input type="text" value="log_alert.sh"/>
Passed Arguments	<input "%output%"="" "%state%"="" type="text" value="%sourcename%"/>

You can pass some basic macros to the script via arguments that will be auto-populated when the script is executed.

- **%sourcename%** - the name of the source that is being alerted on
- **%state%** - the alert state (ok, warning, critical, unknown)
- **%returncode%** - the return code of the check (0 to 3)
- **%output%** - the full output of the check

The New Command modal will appear.

2. Provide a Name for the command.

3. You will need to define the Script Location and Script Name.

4. You will also need to define the arguments passed to the script. This is how you send data to the command, there are Nagios Network Analyzer macros available and they are explained on the modal.
5. Once you've populated all the fields click the Create button.
6. The new command will appear in the list on the Commands tab:

Name	Script Location	Script Name	Passed Arguments	Actions
Log Alert	/usr/local/nagiosna/scripts	log_alert.sh	"%sourcename%" "%state%" "%output%"	<a href="#">Edit</a> • <a href="#">Delete</a>

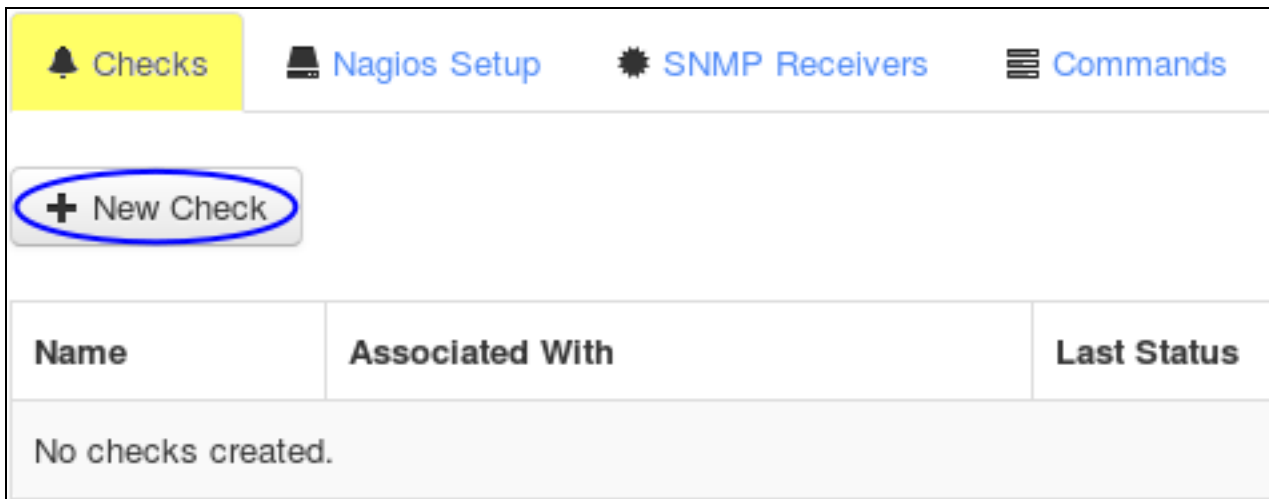
You can now proceed to the [Creating A Check](#) section in this document to define a check that executes the command.

## 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. 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 an check that will notify if a source has no flow data received on the port that the flow data is being received on.



The screenshot shows the Nagios web interface. At the top, there are four navigation tabs: 'Checks' (highlighted in yellow), 'Nagios Setup', 'SNMP Receivers', and 'Commands'. Below the tabs, there is a button labeled '+ New Check' which is circled in blue. Below the button is a table with three columns: 'Name', 'Associated With', and 'Last Status'. The table is currently empty, displaying the text 'No checks created.'

Name	Associated With	Last Status
No checks created.		

On the Alerting page click the Checks tab and then click the New Check button.



## Step 1 - Select Source ✕

Please name the check for management: (Required)

Source  Sourcegroup

Source

View

### Step 1

You must enter a name for the check for management/organizational purposes. It can contain only whitespaces and alphanumeric characters.

Then you need to select your source or source group. This is the source the check will get values from. If you select a source, you can select a view to test against as well.

Click the Step Two button to proceed to Step 2.

### Step 2

## Step 2 - Select Criteria ✕

Analyze traffic for:

Warning threshold is:

Critical threshold is:

Where The:

is

is not

(required)

Analyze traffic for - This is the metric you would like to get the number for to check against. If

you want a packet count, pick Packets. If you want total bytes, pick Bytes. There are several other options, but the point is there are multiple dimensions to the traffic on your network, and this specifies which one will be checked.

Warning and Critical - Once Network Analyzer has extracted a number from the metric you selected, it will use these thresholds to determine if the number is in a WARNING, CRITICAL or OK state. In this example 1: means that if less than 1 was received then it will be in a CRITICAL state (meaning no flows were received).

More detailed information on thresholds is explained in the [Nagios Threshold Values](#) section of this document.

The bottom half of step 2 is how you filter what data the check is looking at, this allows granularity.

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

- Destination - The direction of the flow traffic being looked at
- Port - This check 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 - This is the operation, we want to make sure the destination port IS 9914
- 9914 - Here the port number 9914 has been defined

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 at the bottom. It 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.

## Step 3 - Select Alerting Methods ✕

Select how you would like to be notified of these checks. Select any of the items in the lists under the tabs, and all the selected elements will be notified.

**Email Users**   Nagios   SNMP Traps   Commands

Select the users to be email with check results. Hold ctrl and click to un-select users.

- nagiosadmin
- readonly

Click the Step Three button to proceed to Step 3.

Here you select the alerting method.

The following screenshots show the possible selections you can make.

You can select as many items on the separate tabs as required, hence you can send Emails AND have a Command executed.

## Step 3 - Select Alerting Methods ✕

Select how you would like to be notified of these checks. Select any of the items in the lists under the tabs, and all the selected elements will be notified.

[Email Users](#)[Nagios](#)[SNMP Traps](#)[Commands](#)

Select the SNMP trap receivers to send traps to regarding this check. Removing: Hold ctrl and click to un-select SNMP trap receivers.

SNMP Trap Receiver

[Cancel](#)[◀ Step Two](#)[Finish & Save](#)

## Step 3 - Select Alerting Methods ×

Select how you would like to be notified of these checks. Select any of the items in the lists under the tabs, and all the selected elements will be notified.

[Email Users](#)   [Nagios](#)   [SNMP Traps](#)   **Commands**

Select local scripts or commands to be ran when the check happens. Hold ctrl and click to un-elect commands.

Log Alert

Click the Finish and Save button to create the alert.

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

Name	Associated With	Last Status	Last Date Ran	Last Stdout	Actions
Flow Data 9914	Firewall Public	PENDING	N/A		<a href="#">View / Edit</a> • <a href="#">Delete</a>

Here is an example of the check when it had a CRITICAL state:

Name	Associated With	Last Status	Last Date Ran	Last Stdout	Actions
Flow Data 9914	Firewall Public	CRITICAL	2017-12-05 14:45:01	flows on Firewall Public with filter [dst port 9914] is 0   flows=0;1;1;0	<a href="#">View / Edit</a> • <a href="#">Delete</a>

The checks are run every five minutes, it's important to understand that every five minutes the check will fire off 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 Checks tab, the Actions has the following:

### View / Edit

Review an existing check and make any changes required.

### Delete

Delete the check, no more alerts will be sent.

## Nagios Threshold Values

Nagios Thresholds can be complicated to initially understand, however once grasped 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, for example 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).