Alerting on Log Events in Nagios Log Server 2024

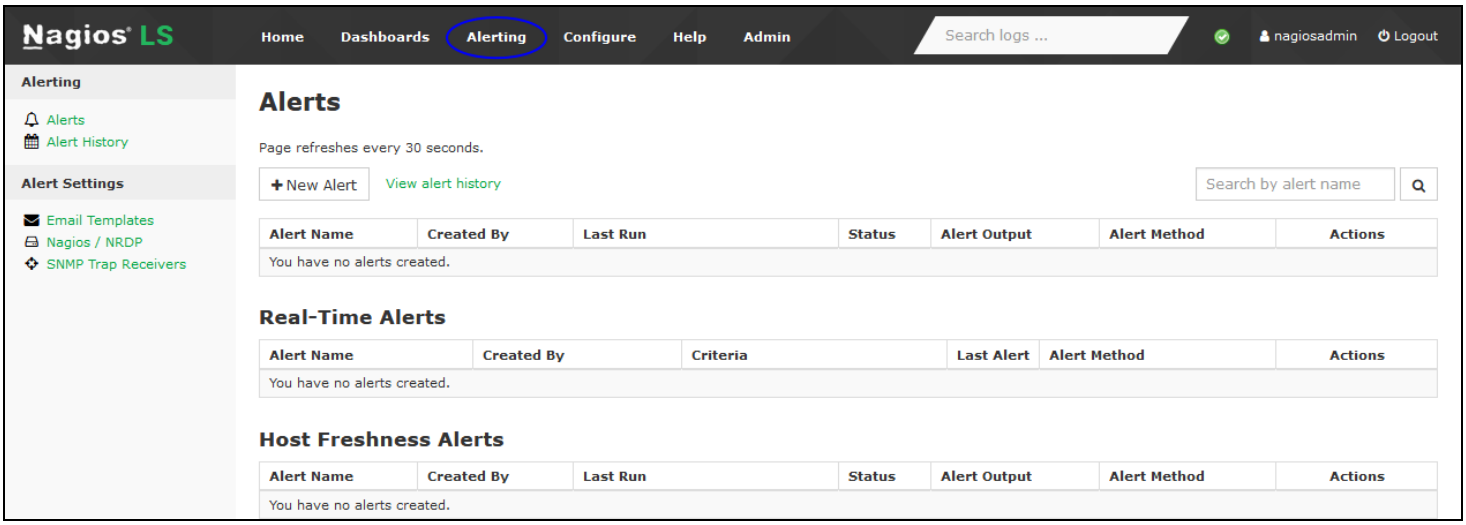
Alert Types

There are three types of alerts in Nagios Log Server can be defined:

- Query
  - These are based on the results of a query that has already been defined (located in the Dashboard menu), hence you will need to have a query defined before creating an alert.
  - With these alerts, data is queried on an interval (usually five minutes) and is checked for any abnormalities. This means that, for a critical issue, alerts may be delayed by up to that check interval.
  - Information on queries can be found in the Analyzing Logs With Nagios Log Server documentation.
- Real-Time
  - Real-time alerts are a way to circumvent the delay associated with interval-based queries. Instead, they exist in the Logstash configuration itself, checking each event as it comes in for that "abnormal" criteria.
  - This feature should be used sparingly, as too many Logstash filters may degrade performance. However, for certain critical events this may be worth the cost.
- Host Freshness
  - Alert based on previously configured hosts where log data is no longer being received by your Nagios Log Server instances from these hosts.

Alerting In Nagios Log Server

In Nagios Log Server select Alerting from the navigation bar.



This is the central location to manage and create alerts. You can also create alerts from the Dashboards menu, they will appear here once created.

There are multiple alert methods available in Nagios Log Server.

- Nagios / NRDP - Send an alert to your Nagios XI or Nagios Core server using NRDP
- Execute Script - Run a custom script and pass variables to the script
- SNMP Traps - SNMP Traps can be sent to other applications using the Nagios MIB
- Email Users - Email Nagios Log Server users
- Nagios XI Log Server Wizard - You can use the Nagios XI Log Server Wizard to alert based on queries saved on your Nagios Log Server

Certain alerts methods require you to define the settings (such as the NRDP server) before you can create an alert. These settings are explained first.

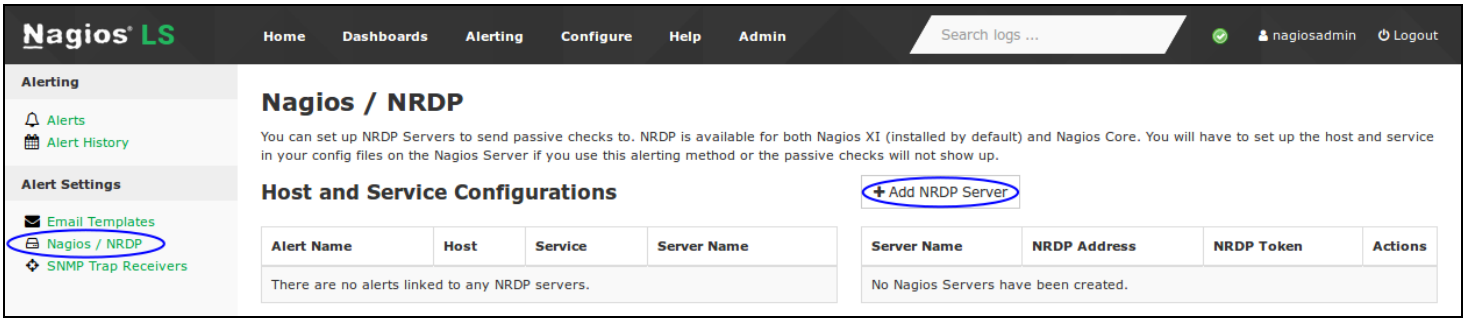
NRDP

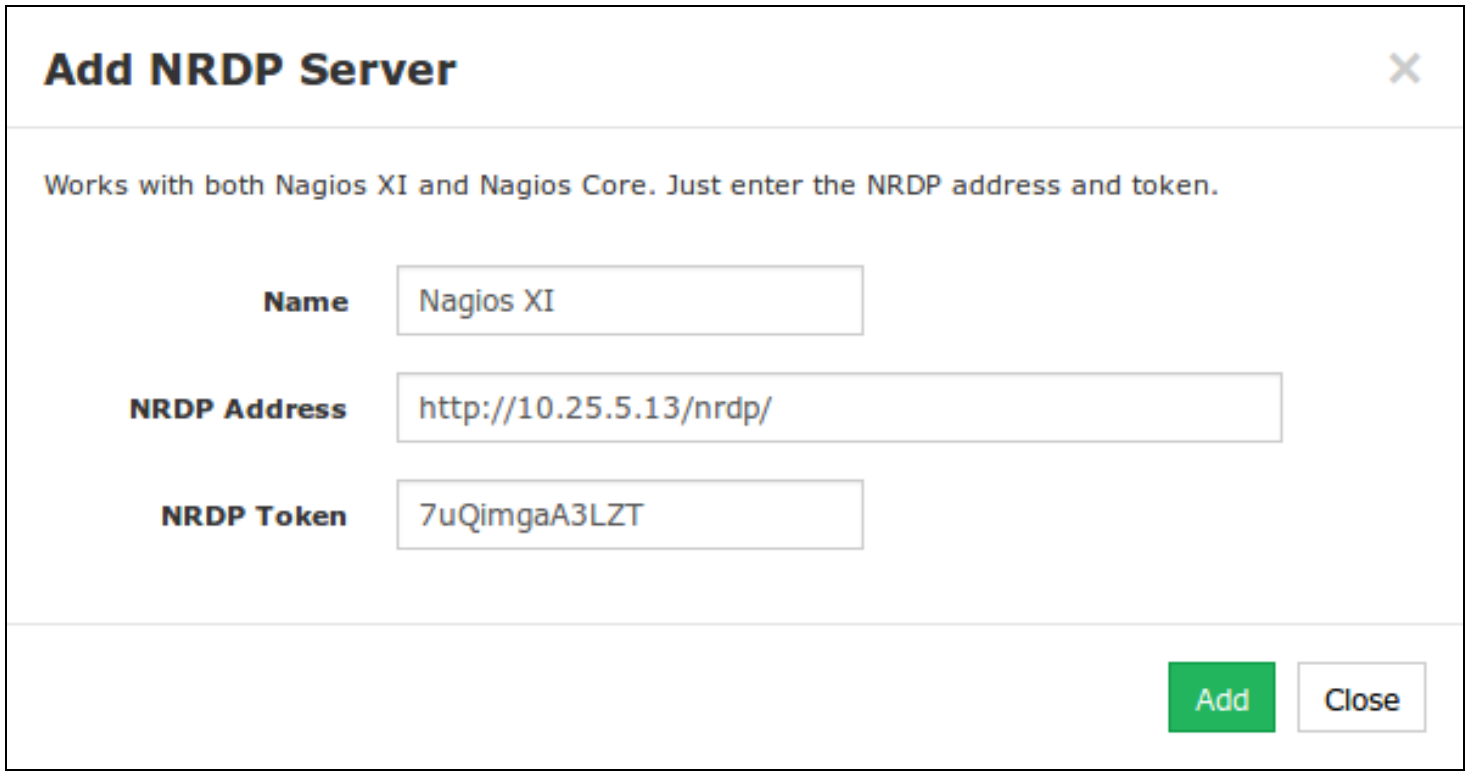
Alerts can be sent to a Nagios XI or Nagios Core server running NRDP. Nagios XI comes pre-installed with NRDP, all that is required is to configure the token you wish to use. If you are using Nagios Core you will need to first install and then configure NRDP. Please refer to the following documentation, it covers configuring both Nagios XI and Nagios Core:

NRDP Overview

Please take note of the NRDP Token you define as you will need it in the following step.

In Nagios Log Server, in the left pane under Alert Settings click Nagios / NRDP, then click the Add NRDP Server button.





You will need to provide the following information:

Name: The name of the NRDP server you are adding.

NRDP Address: The address of the Nagios server NRDP is configured for (you must include the http:// part of the URL).

NRDP Token: Provide the Token you defined on your Nagios XI or Nagios Core server.

Click the Add button to define the NRDP server.

This completes adding an NRDP server as an alert method. Please proceed to the Creating An Alert section in this document to define an alert that uses NRDP.

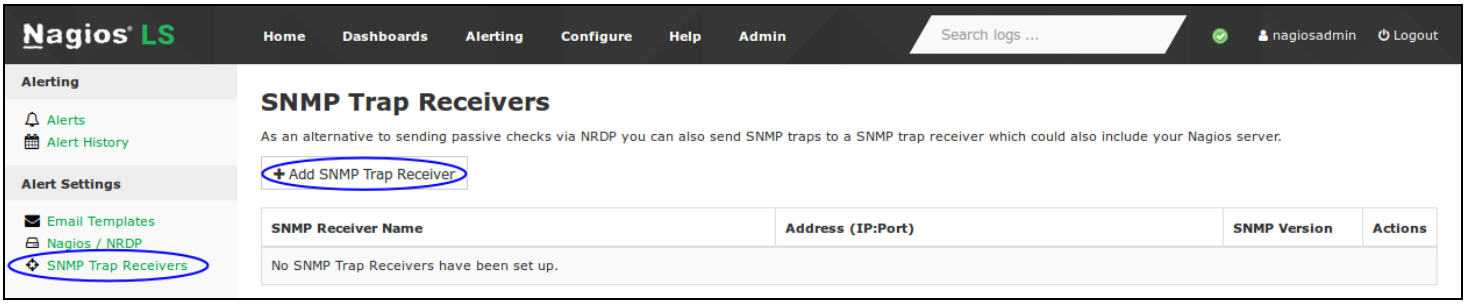
Execute Script

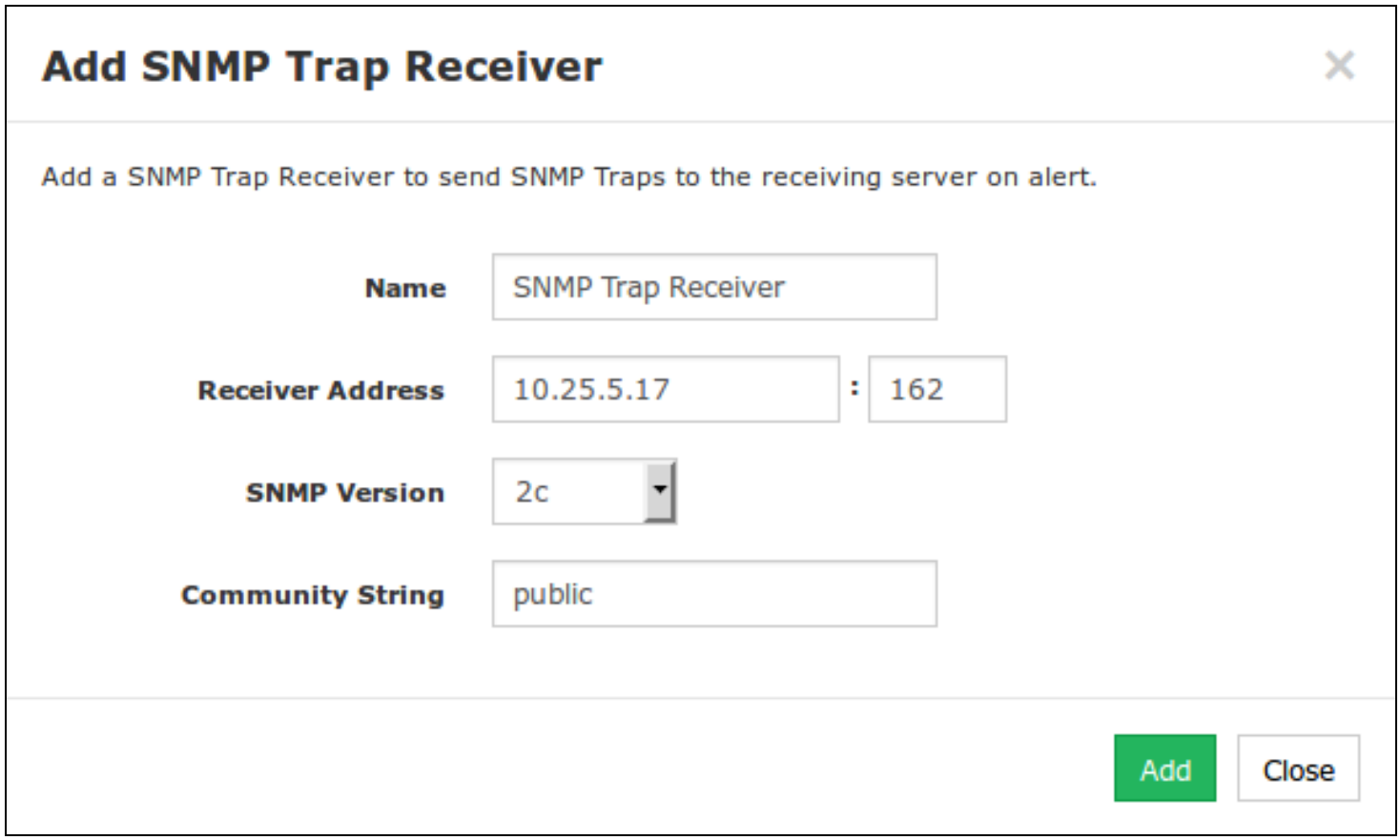
Nagios Log server allows you to execute a script as an alerting method. You will need to make sure that the script exists on all instances in your cluster. The script is executed on the master node of your cluster, this can change at any time to any instance in the cluster, hence why the script needs to be located on all instances.

After placing the script on all of your instances, please proceed to the Creating An Alert section in this document to define an alert that executes a script.

SNMP Trap Receivers

To be able to send alerts to a SNMP Trap receiver you need to define the details of the trap receiver. In Nagios Log Server, in the left pane under Alert Settings click SNMP Trap Receivers, then click the Add SNMP Trap Receiver button.





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.

Click the Add button to define the SNMP Trap Receiver.

This completes adding a SNMP Trap Receiver as an alert method. Please proceed to the Creating An Alert section in this document to define an alert that uses SNMP Traps.

Email Users

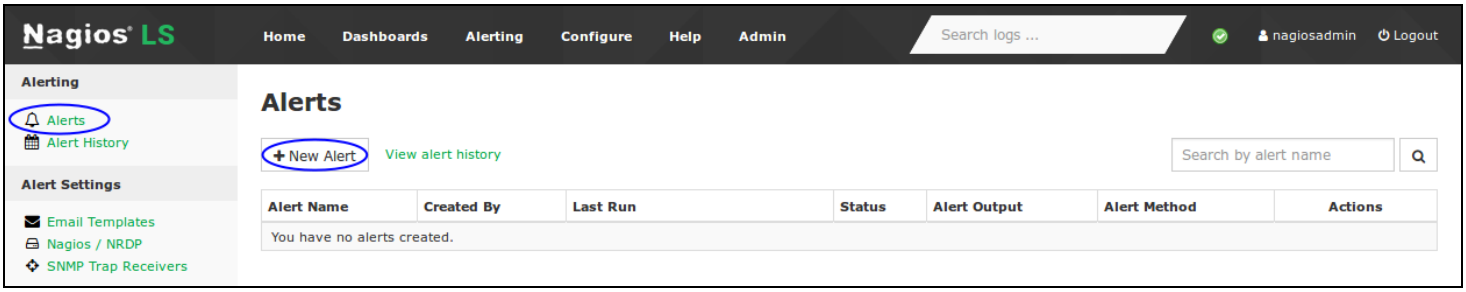
To be able to send email alerts in Nagios Log Server you will need to create Nagios Log Server user accounts with their email addresses correctly defined. The following documentation explains in detail how to create users in Nagios Log Server:

Managing Users In Nagios Log Server

After creating the required users please proceed to the Creating An Alert section in this document to define an alert that uses Email.

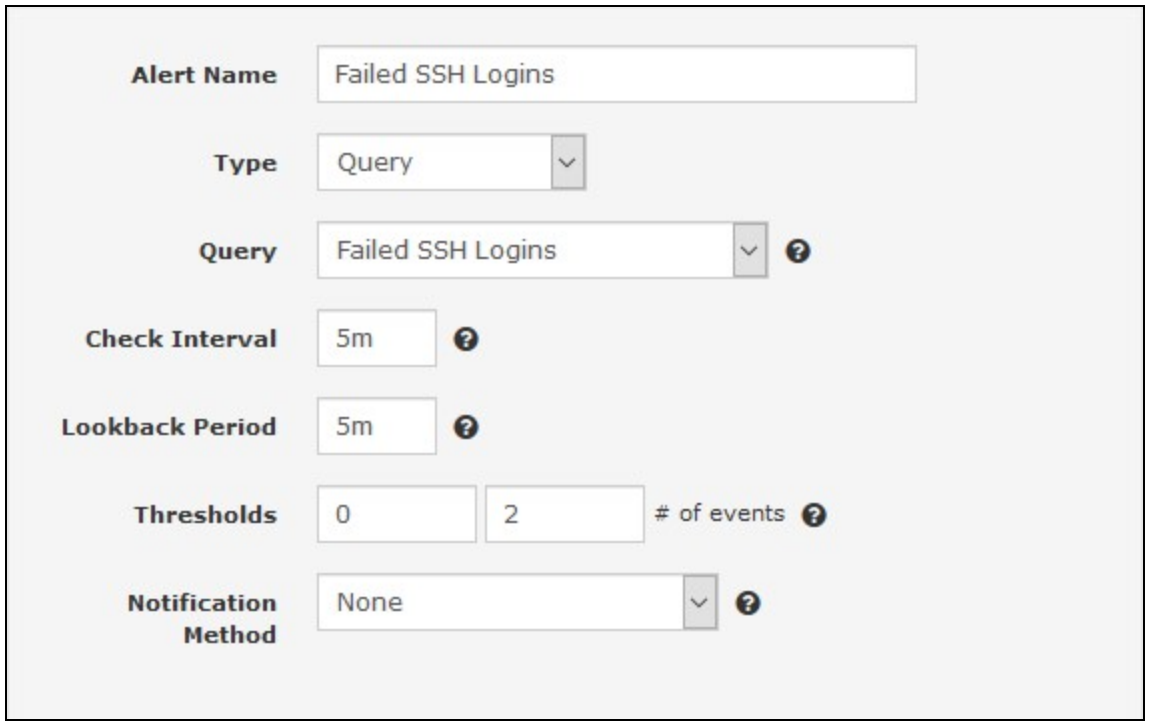
Creating An Alert

Now that you have defined the alert method the next step is to add an alert. In Nagios Log Server, in the left pane under Alerting click Alerts, then click the New Alert button.



The Create an Alert popup is displayed. The last option Alert Method will show additional options based on the method chosen (explained later). All the other options are common to any alert method chosen, these will be explained first. There are separate sections below for each alert method type:

- Query
- Real-Time
- Host Freshness



Creating An Alert - Query

Alert Name - The descriptive name you want to give this alert.

Type - select Query

Query - The predefined query you want this alert to be based on. This example is using the Failed SSH Logins query that is included with Nagios Log Server. Please refer to the section Alert Query for more detailed information.

Check Interval - This is how often you would like this alert to be checked.

Lookback Period - How far in the log data to look back when the query is checked.

Thresholds - This is what defines the severity of the alert. When the query is executed (for the defined lookback period), the number of events returned by the query is the value that the thresholds are tested against. The left field is the warning threshold, the right field is the critical threshold. In this example:

- Warning = 0
    - When more than 0 matches are made the alert will be a WARNING severity
- Critical = 2
    - When more than 2 matches are made the alert will be a CRITICAL severity
- If the thresholds are not triggered then the alert will be an OK or Normal severity.

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

There is an additional common option that is not shown until an Alert Method is chosen.

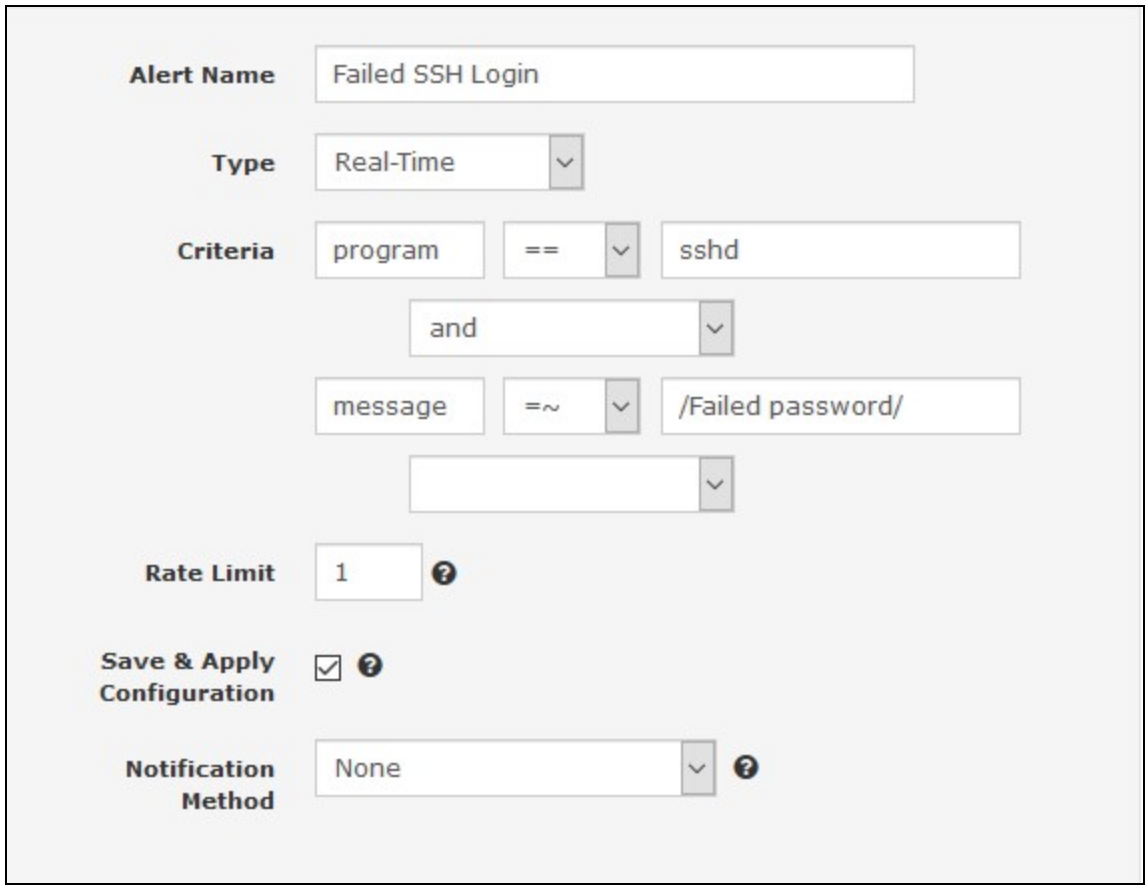
Only alert when Warning or Critical threshold is met is an important option and your selection depends on your requirements. Here are some examples of why you would enable/disable this feature.

- Enabled
    - Alerts are only applied to your Alert Method when the warning or critical threshold is met

    - You would only receive an alert when there is a problem
    - When the problem is no longer occurring you will not be notified
- Disabled
    - Alerts are applied to your Alert Method regardless if the threshold levels are met
    - You will receive an alert every time the alert is run (check interval)
    - This can be noisy when using email alerts
    - If using NRDP, the status in Nagios [XI / Core] will be updated every time the alert is run

Take Ownership - This changes the Created By user to the current user. This prevents the original creator from editing the alert unless they are an administrator.

That covers all the common options for creating a query based alert. You can now proceed to the Alert Methods section that explains the different alert methods.



Creating An Alert - Real-Time

Alert Name - The descriptive name you want to give this alert.

Type - select Real-Time

Criteria - This is where you define what fields will trigger this alert. You should be as specific as possible to ensure you do not receive excessive alerts.

In the screenshot example you can see that two fields have been defined that need to both match because the and operator has been selected.

When you select the operator another field is automatically added, more info about operators will be explained shortly.

Each field has a comparison operator that is used to determine if the field is triggered. In the example above the first field uses a string comparison == to match the program name. The second field uses a regular expression =~ to find the phrase Failed password, this has been enclosed in forward slashes.

- String comparison can be performed with the following operators:
  - == Equals
  - != Not Equals
  - =~ Regular Expression Match
  - !~ Not Regular Expression Match
    - Make sure to enclose regular expression in forward slashes //
  - in Text is in the specified field
    - Enter the searched-for text in the left textbox and the specified field in the right textbox or specify the parameters by using qoutes and brackets (ex. "syslog" in [type]).
  - not in Text is not in the specified field
    - Enter the searched-for text in the left textbox and the specified field in the right textbox or specify the parameters by using qoutes and brackets (ex. "syslog" not in [type]).
- Numeric comparison can be performed with the following operators:
  - == Equals
  - != Not Equals
  - > Greater Than
  - >= Greater Than Or Equals To

    - < Less Than
    - <= Less Than Or Equals To
- The operators available between fields are as follows:
    - and
    - or

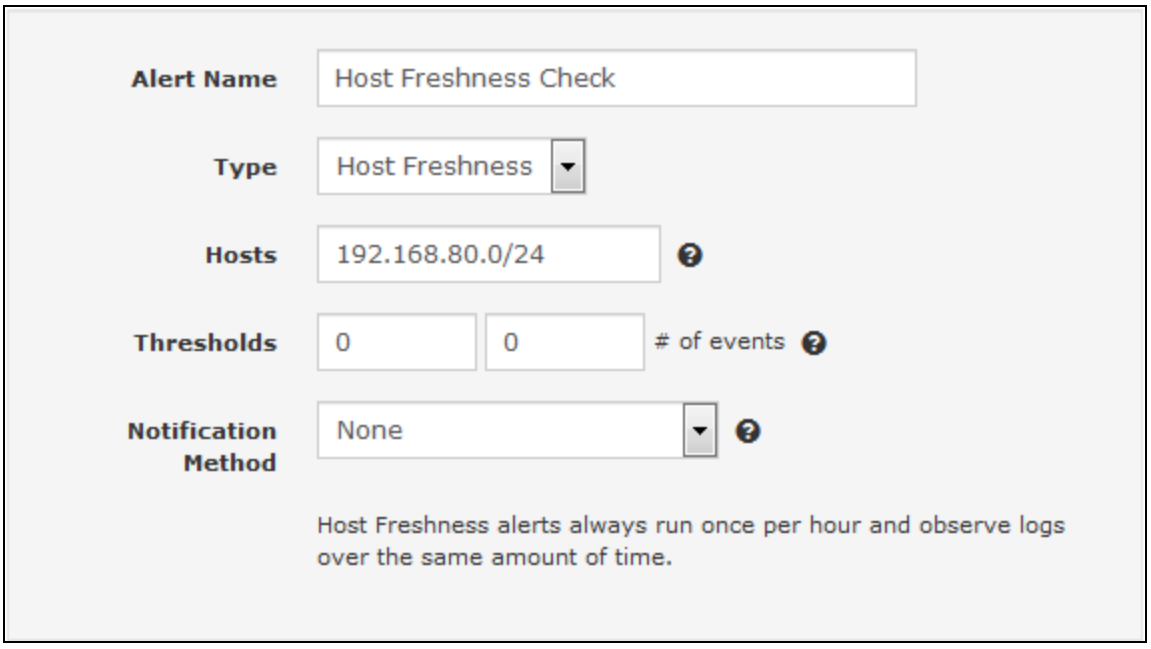
More information on fields can be found in the Analyzing Logs With Nagios Log Server documentation.

Rate Limit exists to combat e-mail spam. Alert at most once every n seconds per instance. E.G. for a 3-node cluster with a rate limit of 5, you would get a maximum of 3 alerts per 5 seconds.

To have the alert become active immediately you need to select Save & Apply Configuration. This will restart the Logstash service which can take several minutes to restart. If you're creating multiple alerts at a time it's recommended to un-check this and then when you've created all of your alerts navigate to the Configure menu to Apply Configuration.

Take Ownership - This changes the Created By user to the current user. This prevents the original creator from editing the alert unless they are an administrator.

That covers all the common options for creating a real-time based alert. You can now proceed to the Alert Methods section that explains the different alert methods.



Creating An Alert - Host Freshness

Alert Name - The descriptive name you want to give this alert.

Type - select Host Freshness

Hosts - Define which hosts to check using CIDR notation. Multiple subnets can be specified using commas, only IPv4 is supported at this time. You can specify individual hosts by using the /32 subnet mask, for example 192.168.130.22/32.

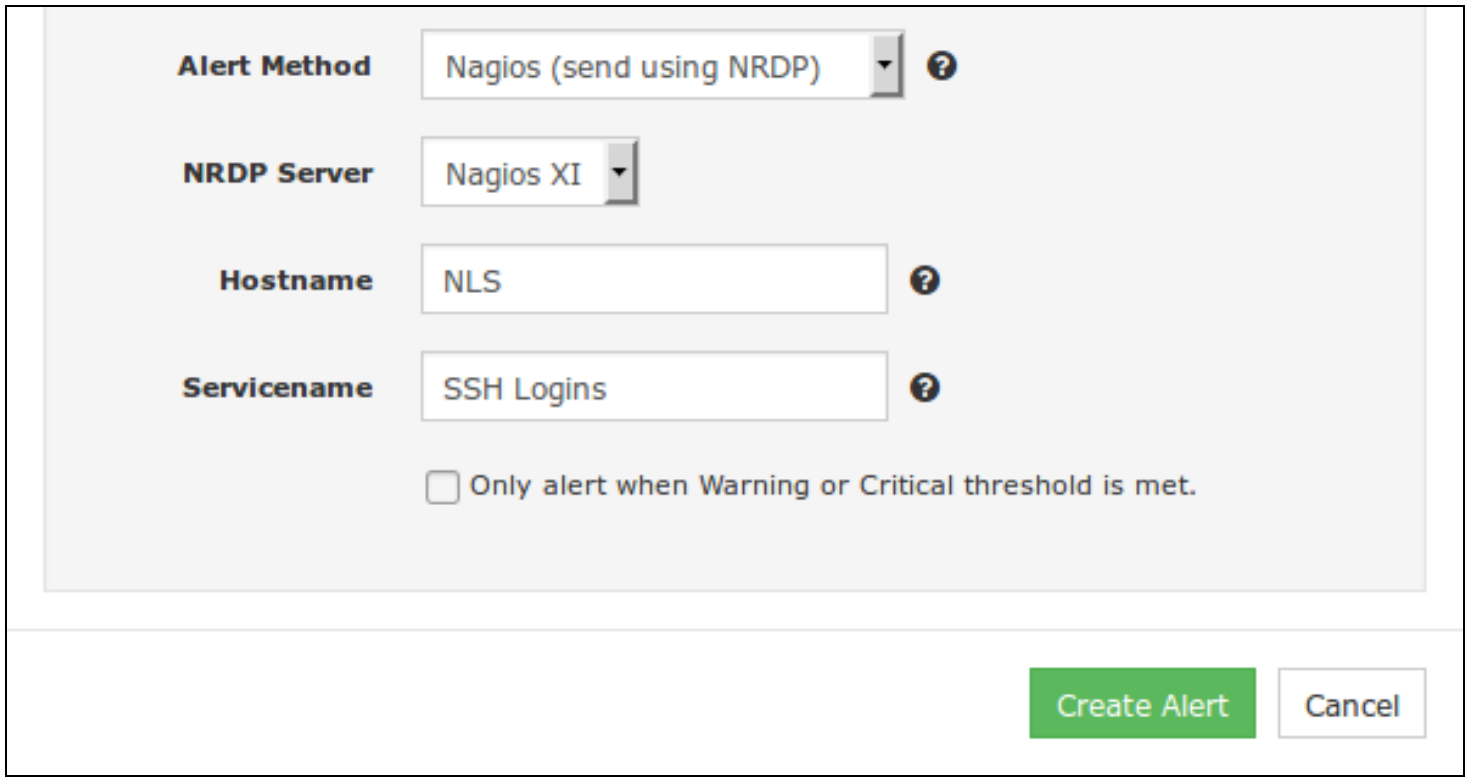
Thresholds - This is what triggers the alert. A common use of the host freshness check is to detect when a host is no longer sending logs to Nagios Log Server. By using 0 for both warning and critical this will trigger a critical condition. Nagios Log Server polls for hosts that have not sent data in 24 hours and populates those hosts in a table. Host Freshness alerts run once per hour to check if the host(s) in their configurations are found in that table.

Take Ownership - This changes the Created By user to the current user. This prevents the original creator from editing the alert unless they are an administrator.

That covers all the common options for creating a host freshness based alert. You can now proceed to the Alert Methods section that explains the different alert methods.

Alert Methods

The final part of creating an alert is to select the alert method and the relevant options.



Nagios (send using NRDP)

NRDP Server - This will be populated with the NRDP server(s) you have already added to Nagios Log Server, select the one you are going to send alerts to.

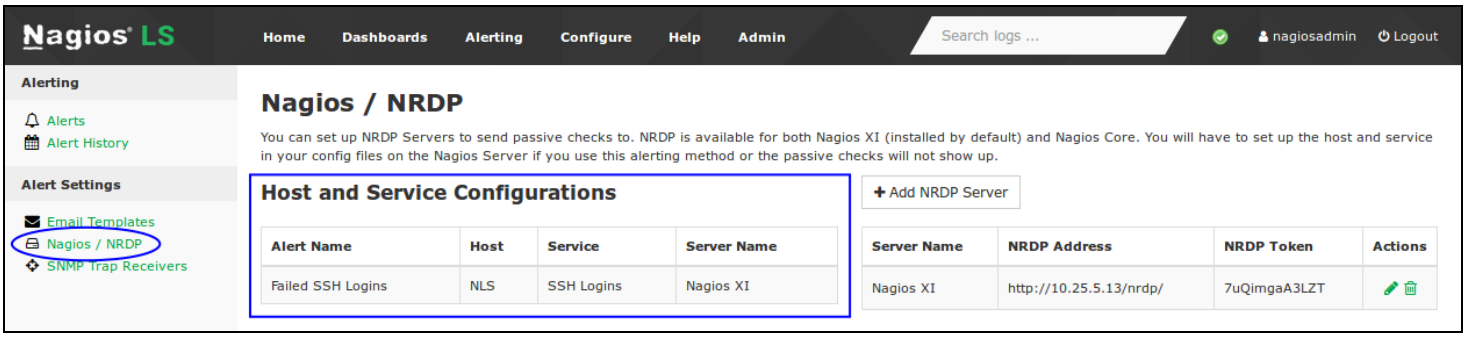
Hostname - The host in Nagios XI or Nagios Core that this alert is going to target.

Servicename - The service in Nagios XI or Nagios Core that this alert is going to target.

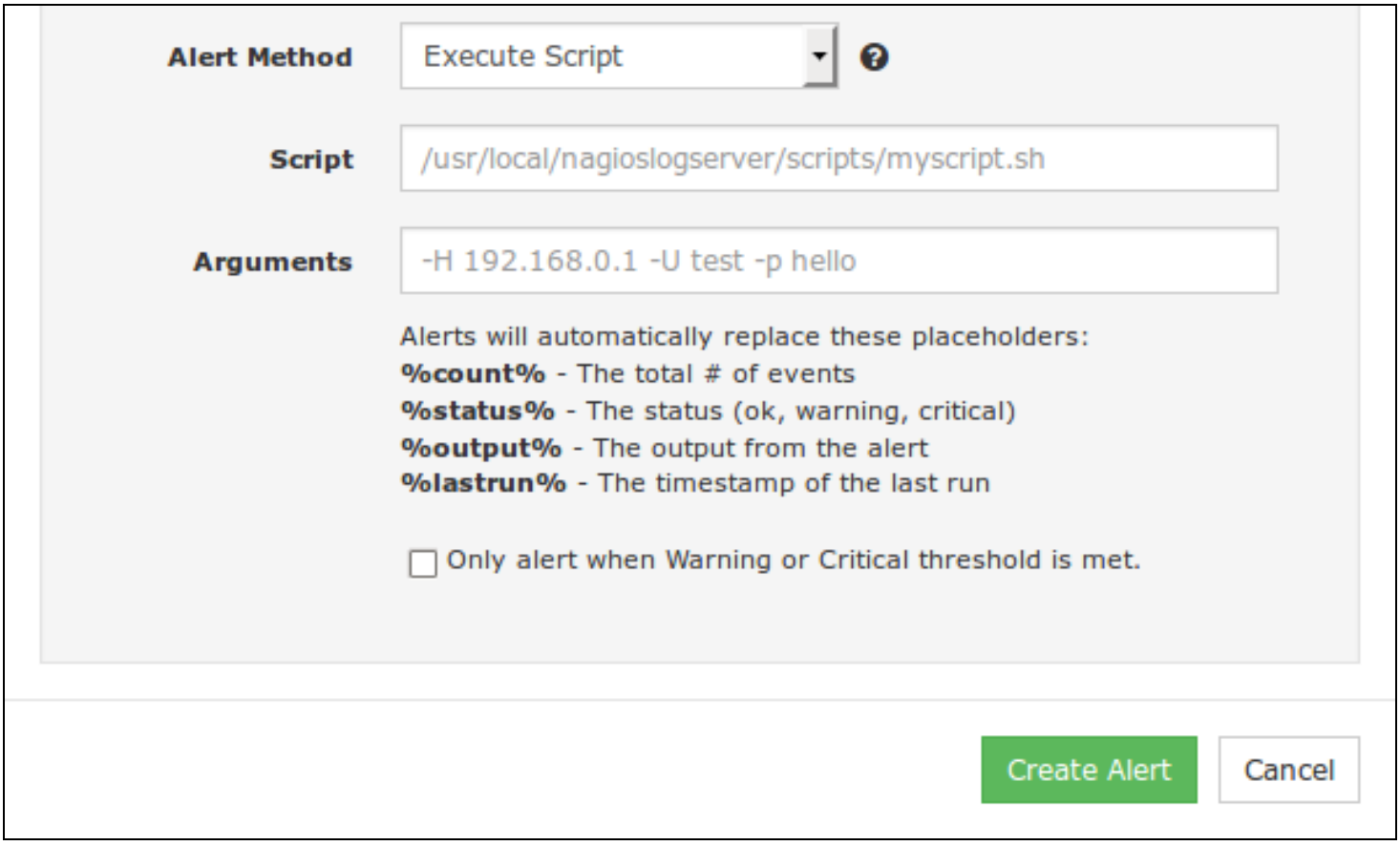
Click the Create Alert button to create your new alert, it will now be displayed under Alerting > Alerts.

Alert Name	Created By	Last Run	Status	Alert Output	Alert Method	Actions
Failed SSH Logins	nagiosadmin	Never	PENDING	Waiting for check to be ran...	NRDP on **Nagios XI** (As NLS - SSH Logins)	

Please refer to the section Nagios Passive Services For NRDP in this document for more information about setting up the Nagios XI or Nagios Core services that will receive these alerts.



A list of all the Nagios [XI / Core] host and services objects that are being targeted by alerts can be seen under Alert Settings > Nagios / NRDP.



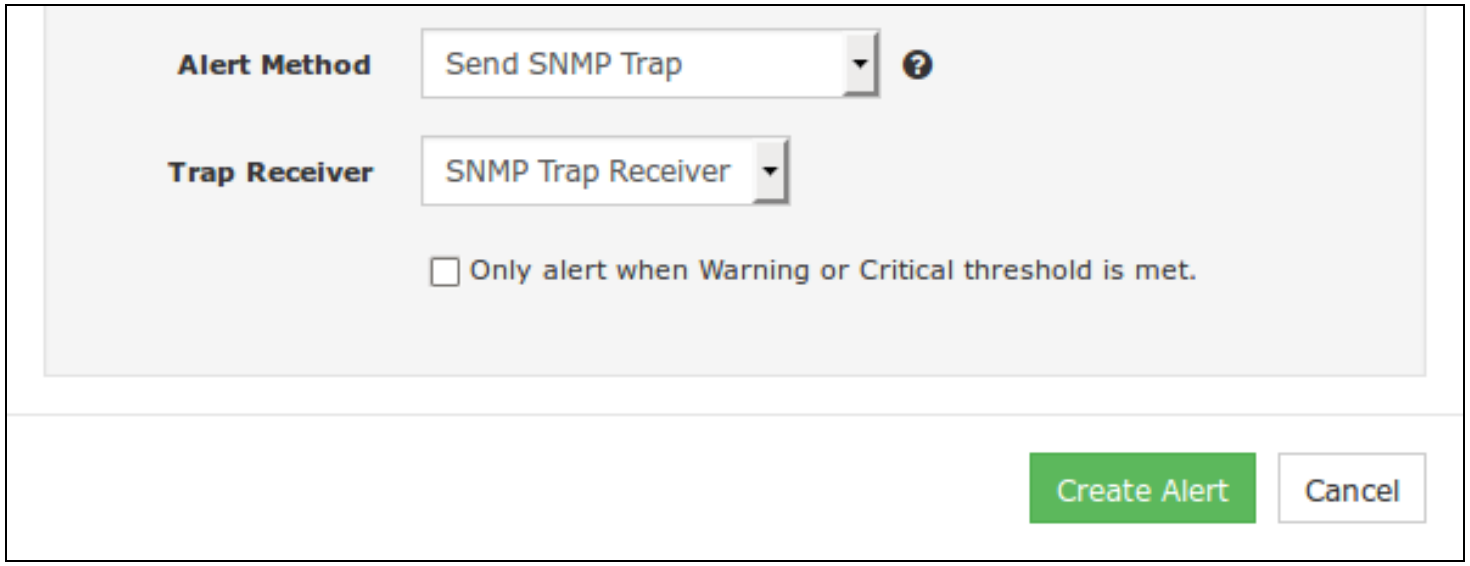
Execute Script

Script - Add the absolute file path of the script your want to access on your local Nagios Log Server.

Arguments - Here you will indicate what the script will accept as arguments. There is also a list of context variables that will be replaced by the status of the alert being acted upon, these variables can be used in the Arguments field.

Click the Create Alert button to create your new alert, it will now be displayed under Alerting > Alerts.

Alert Name	Created By	Last Run	Status	Alert Output	Alert Method	Actions
Failed SSH Logins	nagiosadmin	Never	PENDING	Waiting for check to be ran...	Executing script **myscript.sh**	



Send SNMP Trap

Trap Receiver - This will be populated with the SNMP Trap server(s) you have already added to Nagios Log Server, select the one you are going to send alerts to.

Click the Create Alert button to create your new alert, it will now be displayed under Alerting > Alerts.

Alert Name	Created By	Last Run	Status	Alert Output	Alert Method	Actions
Failed SSH Logins	nagiosadmin	Never	PENDING	Waiting for check to be ran...	SNMP Trap to **SNMP Trap Receiver (10.25.5.17:162)** using SNMP v2c	

Here is an example of a received trap that was sent by Nagios Log Server:

1490057206

nls-c6x-x64.box293.local

UDP: [10.25.5.84]:45184->[10.25.5.17]:162

DISMAN-EVENT-MIB::sysUpTimeInstance 1:1:15:53.53

SNMPv2-MIB::snmpTrapOID.0 SNMPv2-SMI::enterprises.20006.1.7

SNMPv2-SMI::enterprises.20006.1.3.1.2 "NagiosLogServer"

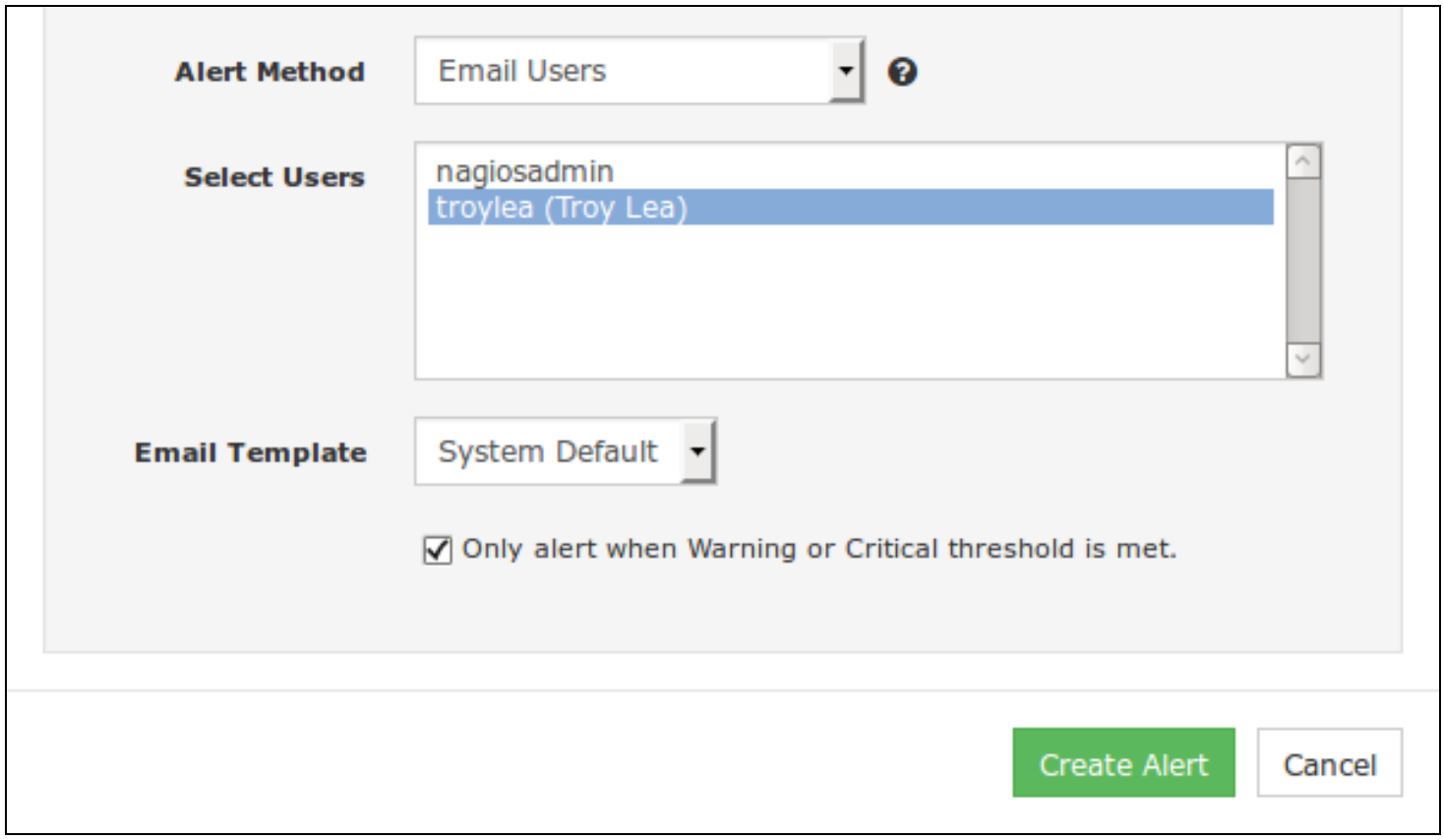
SNMPv2-SMI::enterprises.20006.1.3.1.6 "Failed SSH Logins"

SNMPv2-SMI::enterprises.20006.1.3.1.7 1

SNMPv2-SMI::enterprises.20006.1.3.1.17 "WARNING: 1 matching entries found |logs=1;0;2"

Here is how the alert appears in the Nagios Log Server interface:

Alert Name	Created By	Last Run	Status	Alert Output	Alert Method	Actions
Failed SSH Logins	nagiosadmin	Tue, 21 Mar 2017 11:46:46 +1100	WARNING	WARNING: 1 matching entries found |logs=1;0;2	SNMP Trap to **SNMP Trap Receiver (10.25.5.17:162)** using SNMP v2c	



Email Users

Select Users - Select all the users that you want this alert to be emailed to.

Email Template - Select the template that will be used when the email is sent. More information about defining custom email templates can be found Email Template in the Email Templates section of this document.

Click the Create Alert button to create your new alert, it will now be displayed under Alerting > Alerts.

Alert Name	Created By	Last Run	Status	Alert Output	Alert Method	Actions
Failed SSH Logins	nagiosadmin	Never	PENDING	Waiting for check to be ran...	Email to **Troy Lea (troylea)**	

Alert Actions

Navigate to Alerting > Alerts to see all the alerts that have been defined. There are several options in the Actions column which are explained as follows:

 Show alert in Dashboard

This will open the query used by this alert in the dashboard including the lookback period defined for the alert

 Run the alert now

Causes the alert query to be run immediately

 Deactivate / Activate this alert

Allows you to activate or deactivate the alert

 Edit the alert

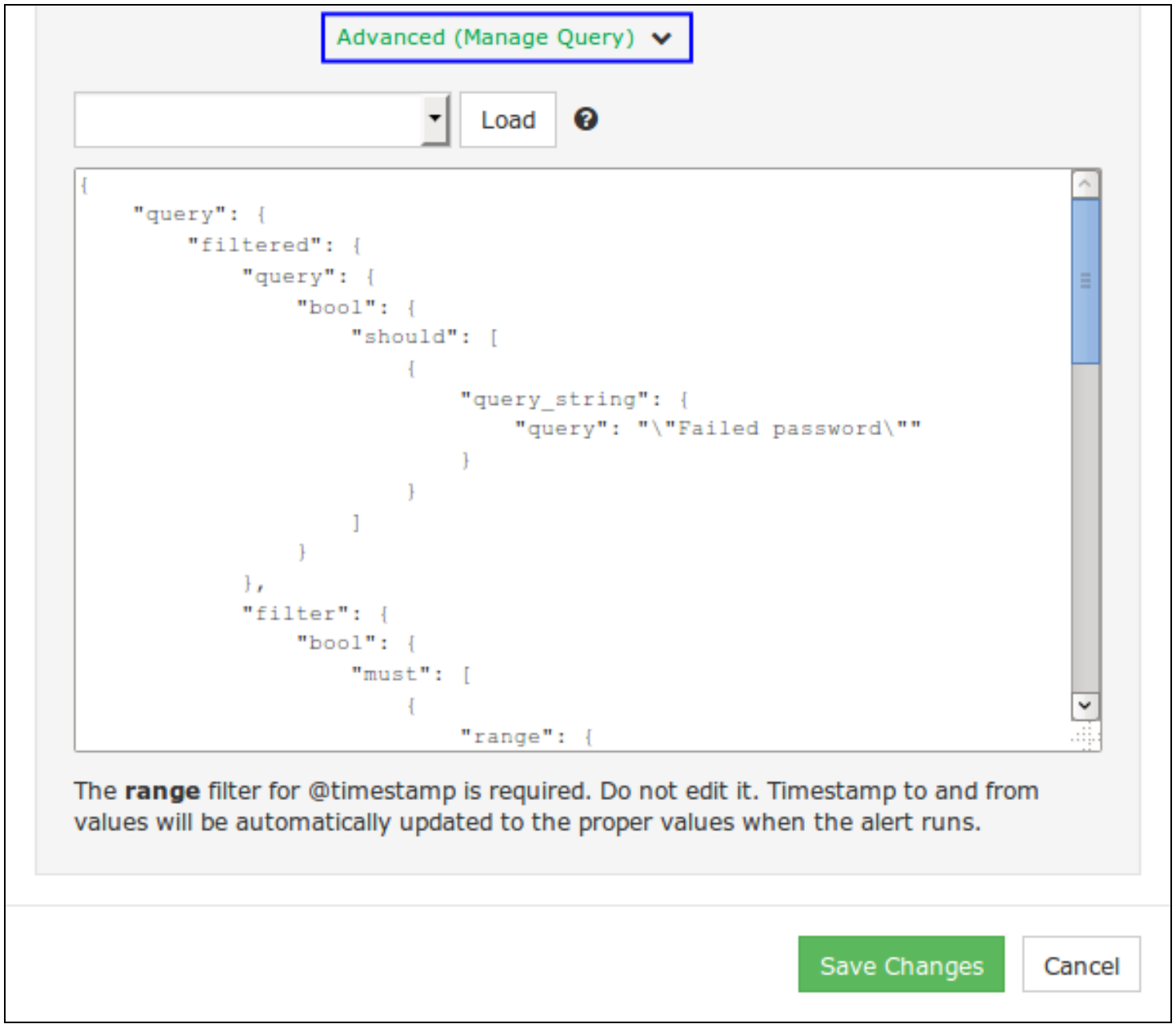
Make changes to the existing alert you have defined

 Remove

Allows you to remove alerts you no longer required

Alert Query

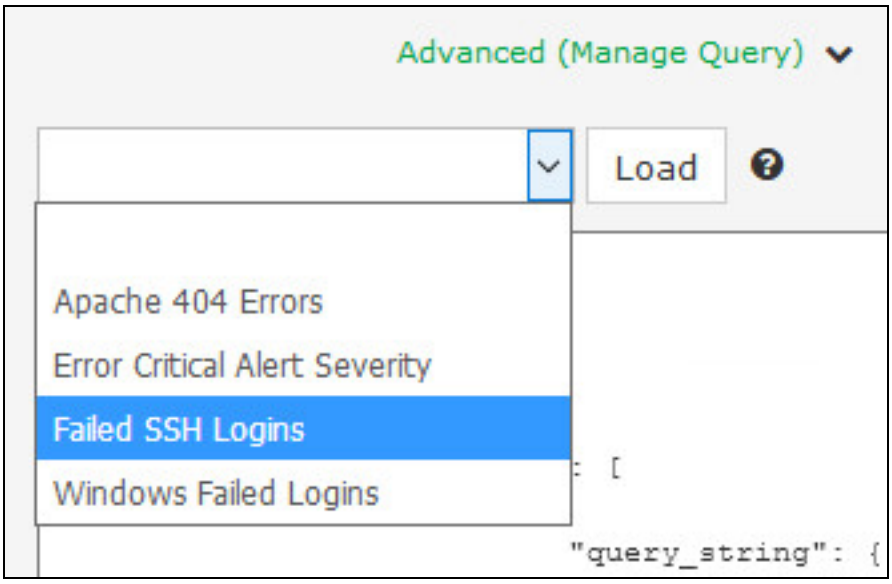
When adding a New Alert you will be presented with a drop down list of already defined queries. After selecting the desired query and creating the alert, this creates a copy of the query you selected.



If you were to later change the original query on the Dashboards page, this change will not be reflected in the alert definition.

If you want to update your alert query, edit the existing alert and then click the Advanced (Manage Query) link.

In the screenshot to the right you can see the raw query, this is the query used by the alert.

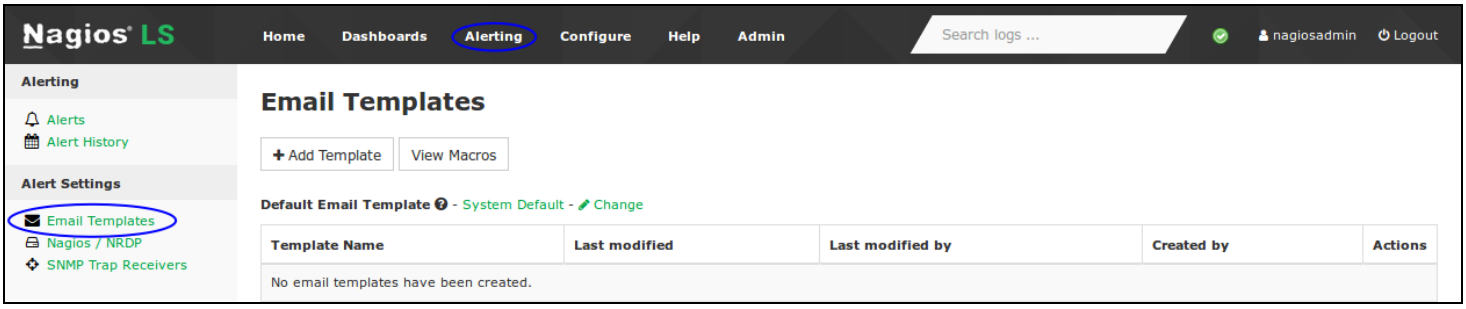


To update the alert to use the new query, select it from the drop down list and then click the Load button (this will replace the query text below).

Alternatively you can edit the query in the text area field.

Email Templates

Nagios Log Server allows you to create custom email templates, allowing you to have differently formatted alert emails. Navigate to Alerting > Alert Settings > Email Templates.



Email Template Macros

When you are creating email templates there are macros you can use to add dynamic data to your emails, for example %state% is the state of the alert (OK / WARNING / CRITICAL / UNKNOWN). The **View Macros** button provides a list of macros that can be used in the templates along with an explanation.

Email Template Macros

The following macros will be interpreted before sending emails. If a macro is used for an alert with an unsupported type, it may be filled with irrelevant information.

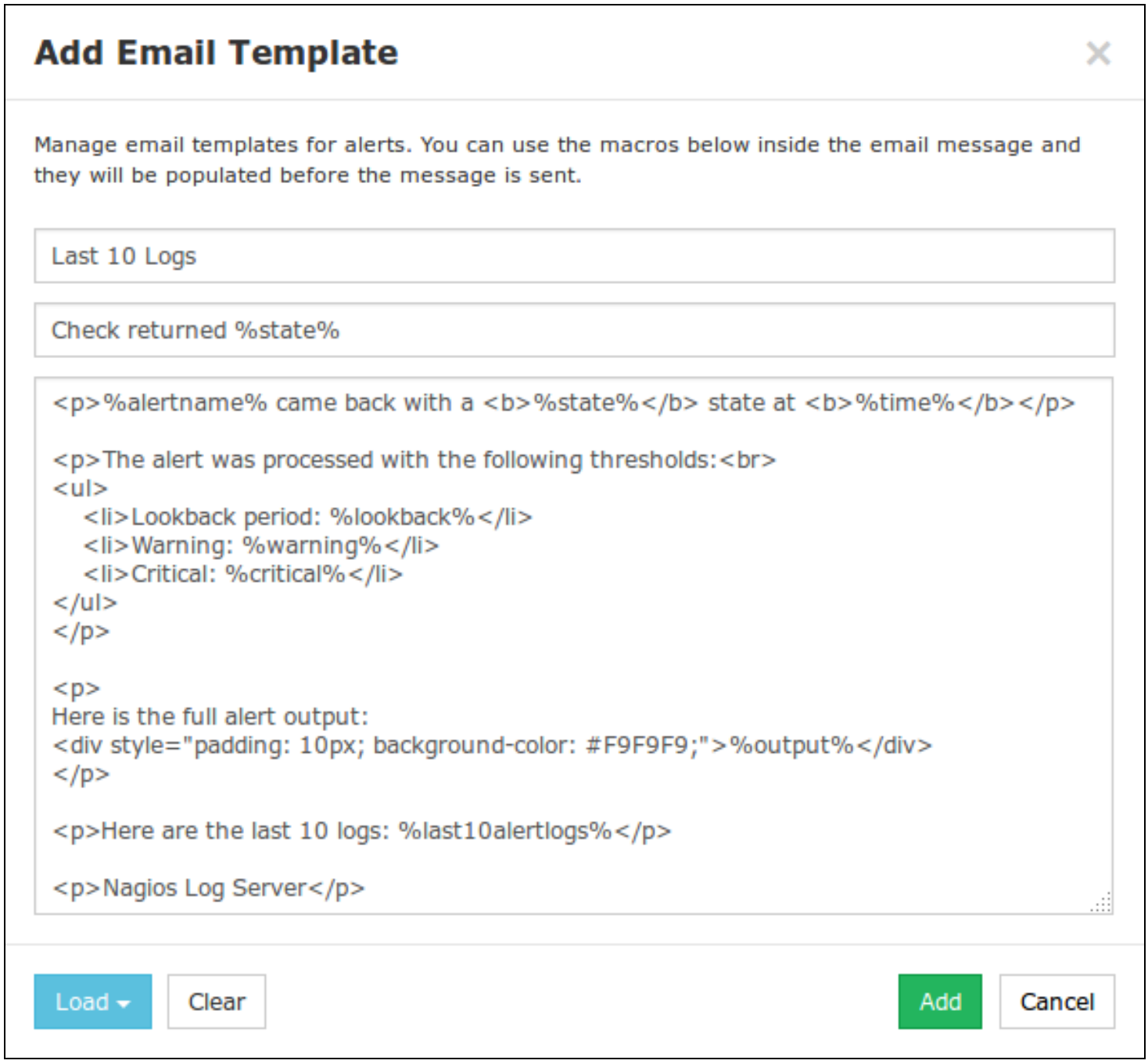
Macro Name	Supported Types	Description
%time%	Any	The time the alert was sent
%alertname%	Any	The name of the alert that is sending a message
%count%	Any	The total number of events
%state%	Any	The state of the alert, OK, WARNING, CRITICAL, UNKNOWN
%lookback%	Query	The alert lookback period (example: 5m)
%warning%	Query, Host Freshness	The warning threshold value
%critical%	Query, Host Freshness	The critical threshold value
%fields.[fieldname]%	Query, Real Time	The data in the specified [fieldname] Example: %fields.message% This will include the message from the last included log in the alert

Message Body Only - These values can only be used in the body of the email, not the title.

Macro Name	Supported Types	Description
%output%	Any	The command line check output
%url%	Query	The url that will show the data returned from the alert
%uniquehosts%	Query	A newline separated list of unique hosts in the alert query. Example: 192.68.1.5 (28) 192.168.5.112 (1220) The value inside the parentheses is the amount of matching logs for the alert time period for the hosts.
%lastalertlog%	Query, Real Time	The last log from the alert query. Can only use one of %lastalertlog% OR %last10alertlogs% per email.
%last10alertlogs%	Query, Real Time	The last 10 logs from the alert query. Can only use one of %lastalertlog% OR %last10alertlogs%s per email.

You can add log fields to your email template using the %fields.[fieldname]% macro noted above.

Adding a New Template



1. To create a new template click the **+ Add Template** button.

2. You will need to populate the Template Name, Subject and Message Body fields.

3. The Load button can be used to populate all the fields based off the System Default or Current Default template.

4. Click the Add button to create the template.

The Email Templates screen shows the newly created template in the list.

The Actions column allows you to Edit and Remove the templates in the list.

In the screenshot above you can see that the Default Email Template is currently the System Default. You can change this by clicking the Change link and selecting the preferred template. This setting applies to all alerts that have System Default selected.

You can also modify the actual System Default template by clicking the System Default link above.

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 Log Server, when an alert query is executed (for the defined loopback period), the number of events returned by the query is the value that the thresholds are tested against. With this in mind, the alert value will always be 0 or greater (no negative numbers are involved).

Nagios Passive Services For NRDP

NRDP alerts received by Nagios XI or Nagios Core are called passive checks. This means that Nagios XI or Core will need to be configured with services for these passive checks, otherwise the received alerts will be ignored. Nagios XI has built in functionality to create services for check results it has received, please refer to the following documentation for detailed steps:

Monitoring Unconfigured Objects With XI

In Nagios Core you will need to create the service definition in your configuration files for these check results. Details on how to do this are outside the scope of this documentation however the following KB article provides examples:

NRDP - Passive Host And Service Definitions