Purpose

This document describes how to create various alerts in Nagios Log Server, such as sending them to a Nagios XI or Nagios Core monitoring server using Nagios Remote Data Processor (NRDP), sending an email, sending SNMP traps and executing scripts.

Target Audience

This document is intended for use by Nagios Log Server Administrators and users looking for information on how to setup alerting in Nagios Log Server.

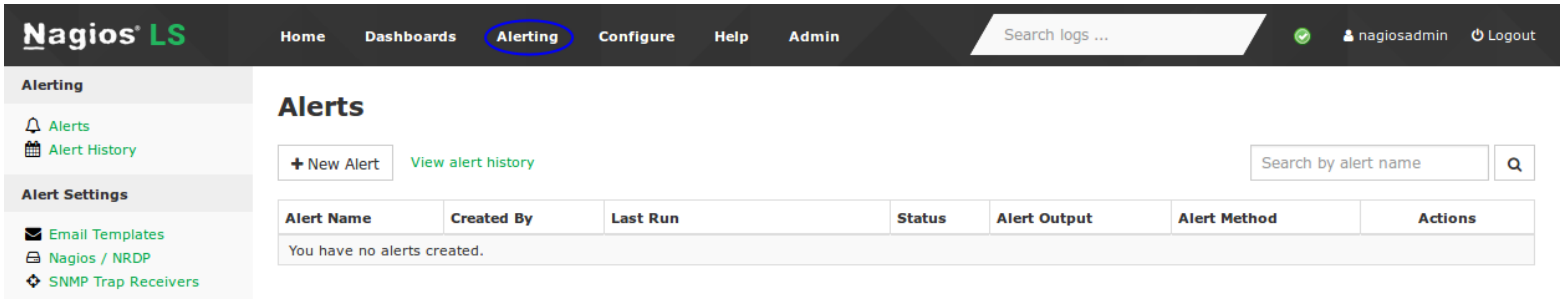
Prerequisites

Alerts 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. Information on queries can be found in the following documentation:

Analyzing Logs With Nagios Log Server

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

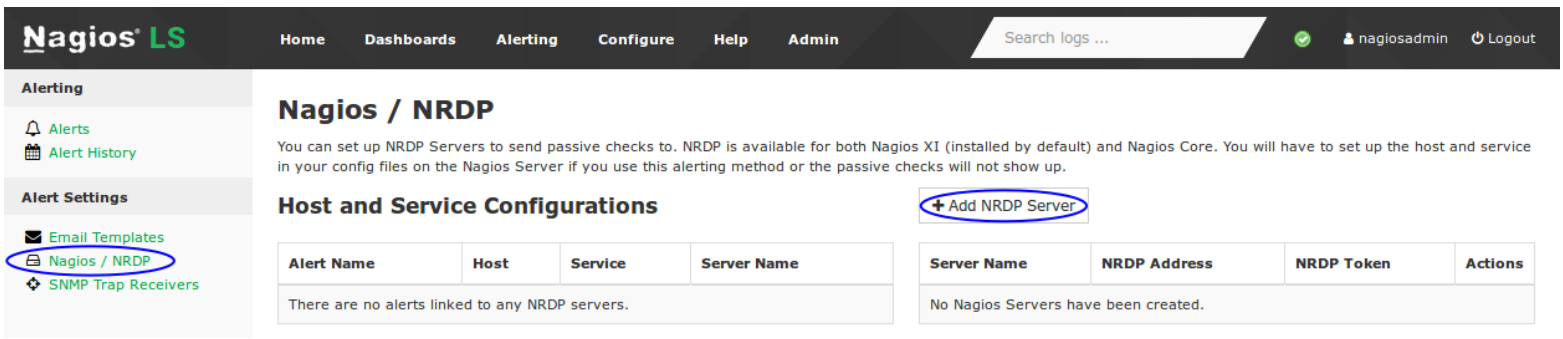
Certain alerts methods require you to define the settings (such as the NRDP server) before you can create an alert. These settings are explained first.

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.

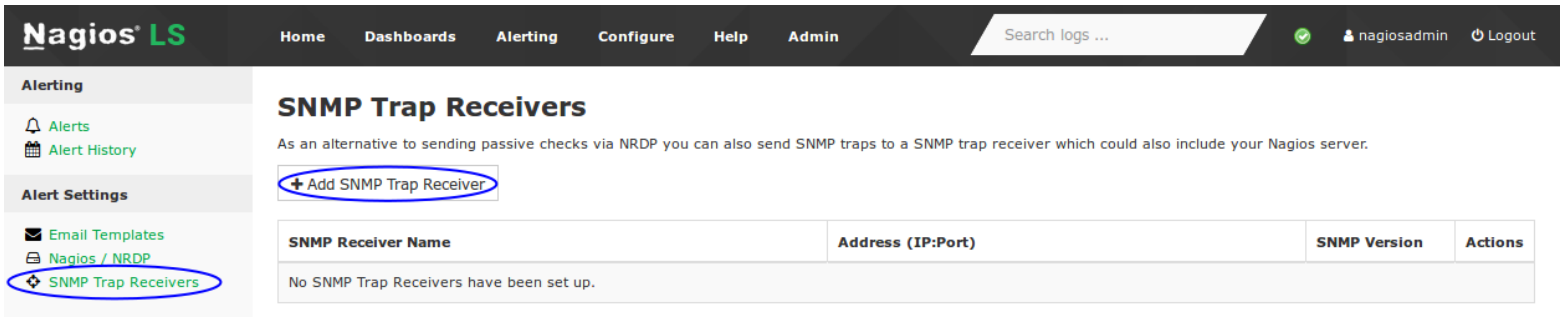
Execute Script

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.

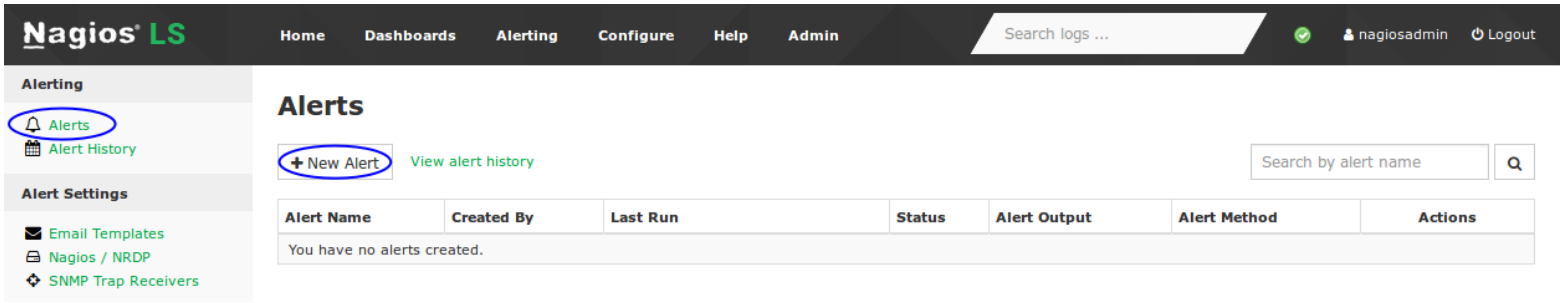
Email Users

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

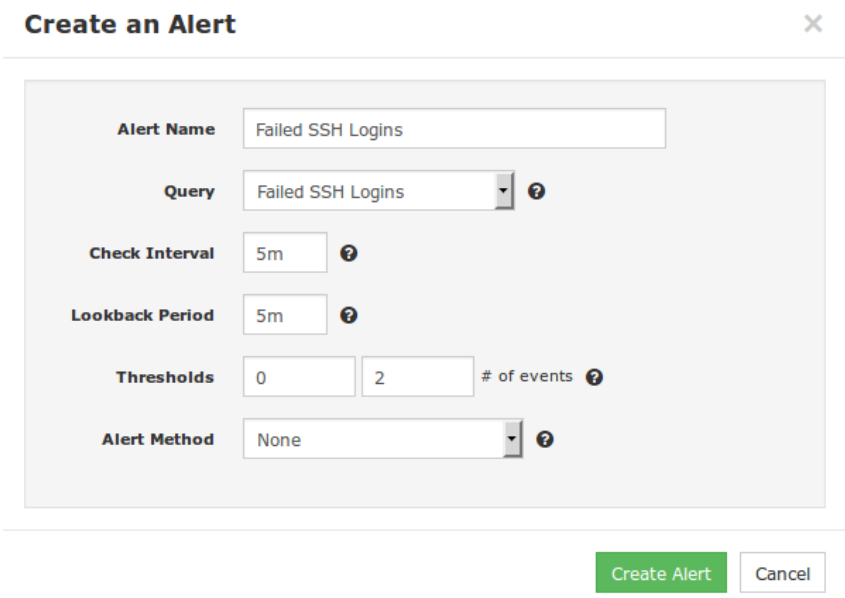
After creating the required users please proceed to the Creating An Alert section in this document to define an alert that uses Email.

Creating An Alert

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. All the other options are common to any alert method chosen, these will be explained first.



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

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.

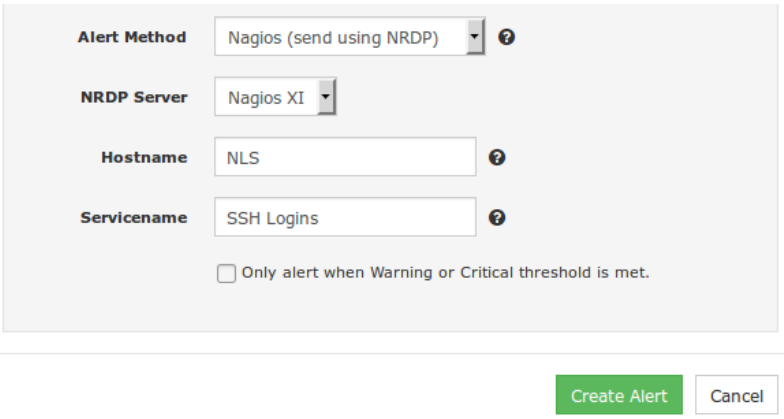
Only alert when Warning or Critical threshold is met is an important option and your selection depends on your requirements. Here are some examples of why you would enable/disable this feature.

- 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

That covers all the common options for creating an alert. The different **Alert Methods** are explained as follows.

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.

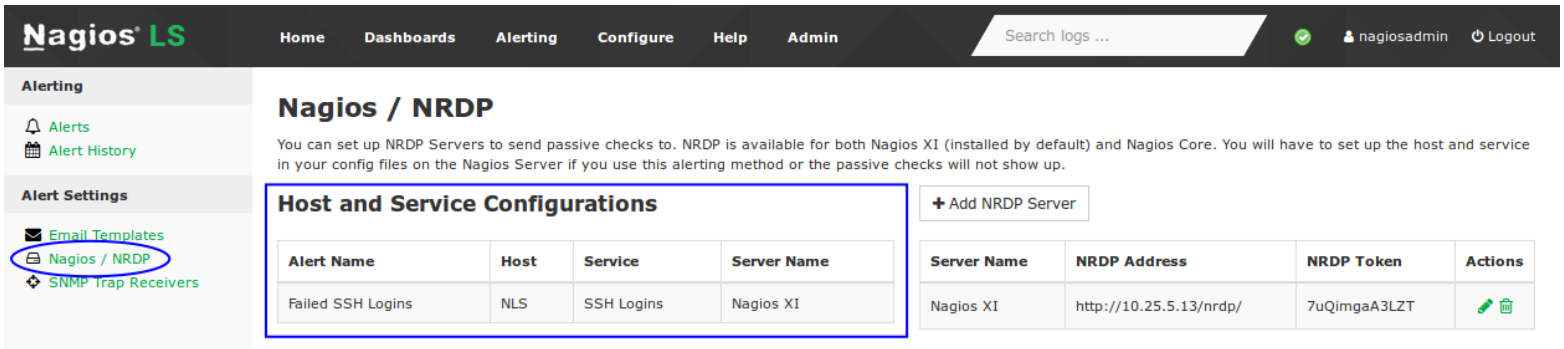
Servicename - The service in Nagios XI or Nagios Core that this alert is going to target.

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.

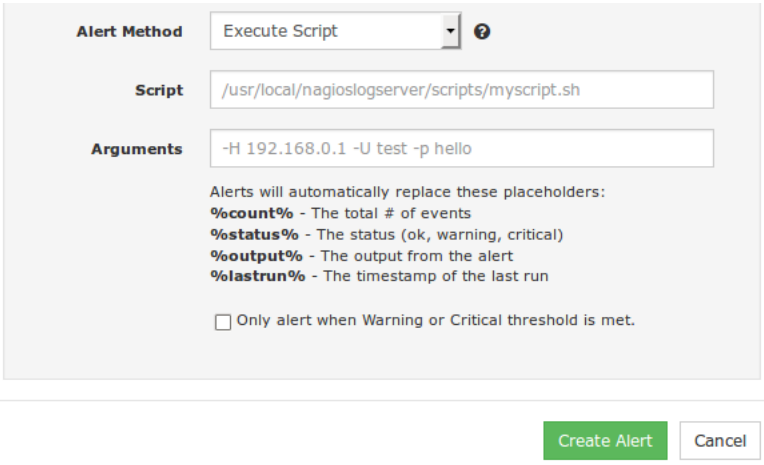
A list of all the Nagios [XI / Core] host and services objects that are being targeted by alerts can be seen under **Alert Settings** > **Nagios / NRDP**.



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.

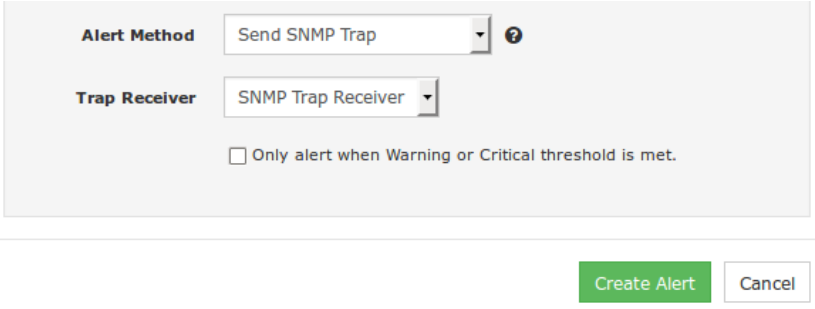


Click the **Create Alert** button to create your new alert, it will now be displayed under **Alerting** > **Alerts**.

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	

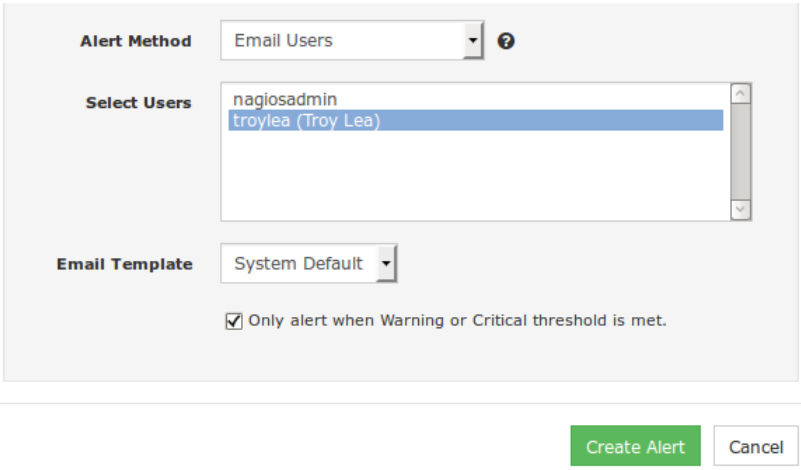
Here is an example of a received trap that was sent by Nagios Log Server:

```
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.

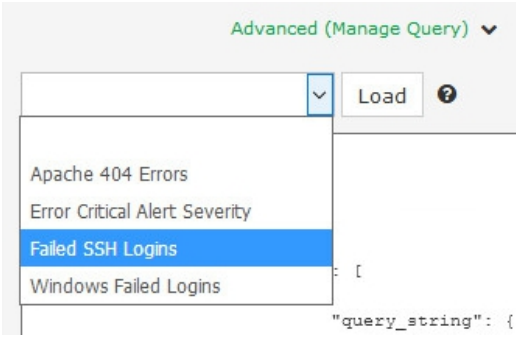
If you were to later change the original query on the Dashboards page, this change will not be reflected in the alert definition.

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.

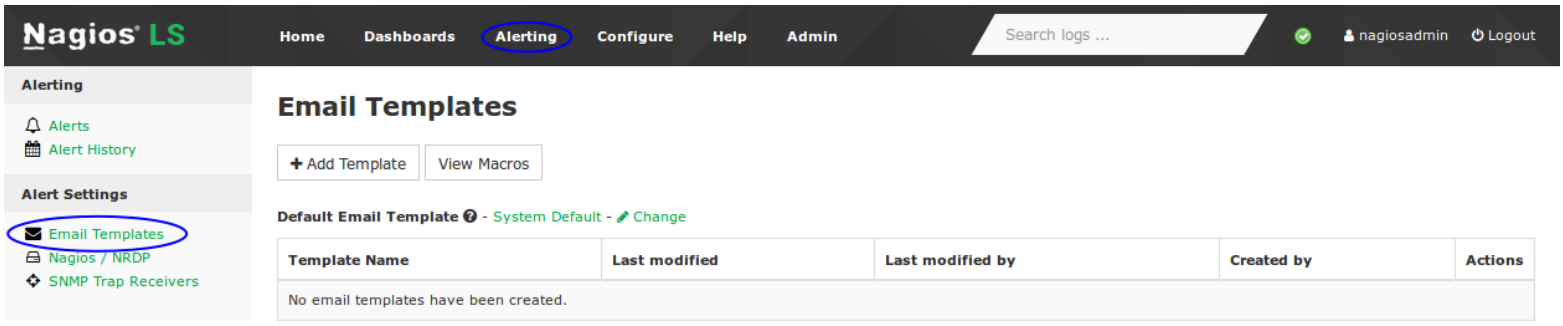
To update the alert to use the new query, select it from the drop down list and then click the Load button (this will replace the query text below).

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

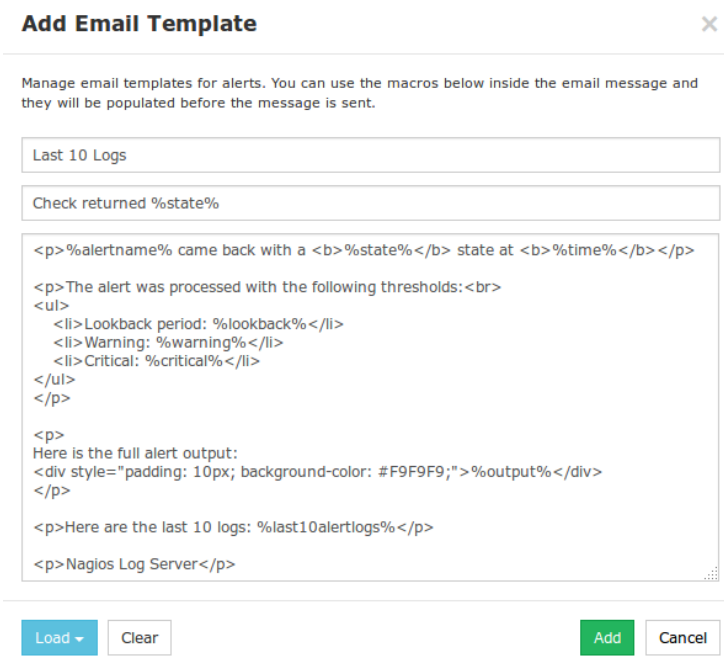
When you are creating email templates there are macros you can use to add dynamic data to your emails, for example `%state%` is the state of the alert (OK / WARNING / CRITICAL / UNKNOWN). The **View Macros** button provides a list of macros that can be used in the templates along with an explanation.

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

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

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

Click the **Add** button to create the template.



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

Default Email Template - System Default - Change

Template Name	Last modified	Last modified by	Created by	Actions
Last 10 Logs	Tue, 07 Nov 2017 08:43:18 +1100	nagiosadmin	nagiosadmin	

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

Finishing Up

This completes the alerting on log events documentation for Nagios Log Server.

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