Nagios Log Server – Alerting On Log Events

## The Industry Standard in IT Infrastructure Monitoring

Purpose

This document describes how to create various alerts in Nagios Log Server, such as sending them to a Nagios monitoring server using 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.

Set Up Alerting

In your Nagios Log Server user interface select the **Alerting** section from the navigation bar on the top of the page.
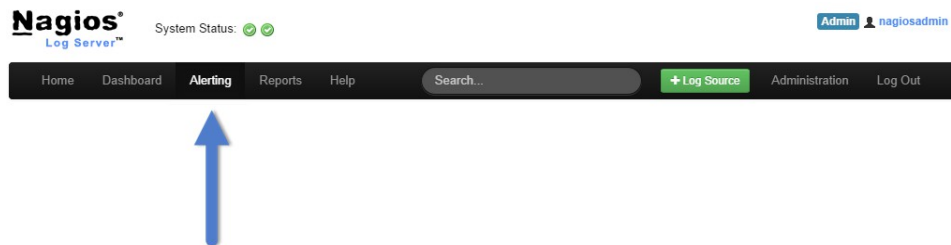
There are **4** ways to trigger alerts on your Nagios Log Server.

1. **Email Users / Execute Script –** General alerting can be done with emailing users or executing a script. This takes very little configuration and can be useful throughout your log management. Email users inside your Nagios Log Server or run a custom script located by path and using context variables.

2. **NRDP –** Nagios Remote Data Processor is designed to be a flexible data transport mechanism and processor for Nagios.

3. **SNMP Traps –** SNMP Traps can be sent to other applications using the Nagios MIB.

4. **Nagios XI Log Server Wizard –** You can use the XI Log Server Wizard to alert based on queries saved on your Nagios Log Server. More information can be found here.

1. Email Users

Select the + New Alert '**New Alert**' button,

Like other alerts set the fields:
- Alert Name
- Query
- Check Interval
- Lookback Period

Then select '**Email Users**' under the Alert Method field. Finish with selecting the Thresholds and users to email the alert to.

Nagios®

Execute Script

Select the **+ New Alert** 'New Alert' button,

Like other alerts set the fields:
- Alert Name
- Query
- Check Interval
- Lookback Period

Select '**Execute Script**' under the Alert Method field.

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. Additionally, some scripts you may want to run require arguments such as -H <hostname> for example.

Alert Method   Execute Script ▼

Script   /usr/local/nagioslogserver/scripts/myscript.sh

Arguments   -H 192.168.0.1 -U test -p hello

Alerts will automatically replace these placeholders:
%count% - The total # of events
%status% - The status (ok, warning, critical)
%output% - The output from the alert
%lastrun% - The timestamp of the last run

☐ Only alert when Warning or Critical threshold is met.

2. Nagios (send using NRDP)   🖶 Nagios Servers (NRDP)

To set up NRDP on a Nagios Core server follow the NRDP overview documentation here:

http://assets.nagios.com/downloads/nrdp/docs/NRDP_Overview.pdf

You can set up Nagios Servers to send passive checks via NRDP. This is available for both Nagios XI and Nagios Core. You will have to set up the host and service in your configuration files on the Nagios Server if you use this alerting method or the passive checks will not show up.

Once you are on the Alerting page select the Nagios Servers (NRDP) on the left side navigation panel under Configure Alert Methods.

Now select the   **+ Add NRDP Server**   '**Add NRDP Server**' button

This is the window that will be displayed:

1. **Name:** The unique nickname of the NRDP server you are adding.

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

3. **NRDP Token:** In Nagios XI this is easy to find by going to **Admin > Inbound Transfers**. The token will be displayed in the second text area. The NRDP Token is the alphanumeric string that is defined in your config.inc.php file under:

    ```
    $cfg['authorized_tokens']
    ```

Your config.inc.php file that located here in your NRDP server:

    ```
    /usr/local/nrdp/server/config.inc.php
    ```

Add NRDP Server   ✕

Can be Nagios Core or Nagios XI as long as you have the NRDP address and token.

Name   Nagios XI Server

NRDP Address   http://192.168.4.50/nrdp

NRDP Token   01fe4g734k2lfv0000

Add   Close

Nagios®
Enterprises

Nagios Enterprises, LLC
P.O. Box 8154
Saint Paul, MN 55108
USA

US: 1-888-NAGIOS-1
Int'l: +1 651-204-9102
Fax: +1 651-204-9103

Web: www.nagios.com
Email: sales@nagios.com

Page 2

Copyright © 2010-2014 Nagios Enterprises, LLC
Revision 1.0 – February, 2017

Now we can add the alert to Nagios Log Server. Select the [+ New Alert] **'New Alert'** button,

Create an Alert

1. **Alert Name** – The display name for the alert.

2. **Check Interval –** The time between checks.

3. **Lookback Period –** How far in the logs to look back when counting messages.

4. **Thresholds** – Number of events in a threshold, Warning / Critical.

5. **Alert Method** – Here, choose Nagios (send using NRDP).

6. **NRDP Server** – This should populate with the NRDP server you added to Nagios Log Server, select the one you are going to alert with.

7. **Hostname** – The hostname you want the alert to display as in Nagios.

8. **Servicename** – The servicename that will be assigned to the hostname your alerts will display on in Nagios.

9. At the bottom there is a checkbox that does exactly as it claims: Alert only on when Warning/ Critical Threshold is met.

|	
Alert Name	Nagios XI NRDP Alert
Check Interval	5m
Lookback Period	5m
Thresholds	5 / 10 / # of events
Alert Method	Nagios (send using NRDP)
NRDP Server	Nagios XI Server
Hostname	Nagios XI Server (.27)
Servicename	Nagios Log Server Alert

[Create Alert] [Close]

Once the alert is added it will display under the **Alerting** page in Nagios Log Server under **Alerting > Nagios Servers (NRDP)**. The left column shows alerts set up with NRDP and the right column displays NRDP servers that have been added to Nagios Log Server.

Navigate back to the **Alerting** main page and you will see the **Nagios XI NRDP Alert** that we just set up. Select the '**Run the Alert Now**' button under the **Actions** column to test this alert. This will trigger the alert, show the status under the status column, and show the alert output.

This will verify that your NRDP settings were added correctly, Nagios Log Server is able to communicate with NRDP and Nagios XI and that your tokens are correct.

Actions
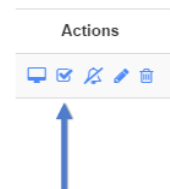
3. SNMP Trap ✧ SNMP Trap Recievers

As an alternative to sending passive checks via NRDP you can also send SNMP traps to a SNMP trap receiver which could also include your Nagios server. If you need help setting up your Nagios XI server to receive SNMP Traps, please consult this document.

Once you are on the Alerting page select the SNMP Trap Receivers in the left side navigation panel under Configure Alert Methods. You will see the below screen:

SNMP Trap Receivers

As an alternative to sending passive checks via NRDP you can also send SNMP traps to a SNMP trap receiver which could also include your Nagios server.

[+ Add SNMP Trap Receiver]

SNMP Receiver Name	Address (IP:Port)	SNMP Version	Actions
No SNMP Trap Receivers have been set up.			

Nagios Enterprises, LLC
P.O. Box 8154
Saint Paul, MN 55108
USA

US: 1-888-NAGIOS-1
Int'l: +1 651-204-9102
Fax: +1 651-204-9103

Web: www.nagios.com
Email: sales@nagios.com

Page 3

Copyright © 2010-2014 Nagios Enterprises, LLC
Revision 1.0 – February, 2017

Nagios®

Click the **'Add SNMP Trap Receiver'** [+ Add SNMP Trap Receiver] button, and fill out the fields:

Name: The name of the SNMP Trap alert in Nagios Log Server

Receiver Address: The address that is receiving traps. Could be an NSTI server or a Nagios XI server that is being sent traps. The receiver will need to be configured to accept traps from the IP and community string that is set here.

SNMP Version: The version of SNMP you are using. This will be in your snmpd.conf file.

Community String: Usually either set to 'public' or 'private' depending on how your snmp handler it set in the configuration file, however it could be a slightly more convoluted string for security purposes.

Add SNMP Trap Receiver

Add a SNMP Trap Receiver to send SNMP Traps to the receiving server on alert.

Name [   ]

Receiver Address [192.168.1.150] : [4503]

SNMP Version [2c ▼]

Community String [   ]

[Add] [Close]

Now once your SNMP Trap alert is set up you should receive alerts in the form of a trap from Nagios Log Server to the receiver you indicated.

Finishing Up

If you have questions about Nagios Log Server or of its capabilities, contact our support team via our online form at:

http://support.nagios.com/forum