



Purpose

This document describes how to send Nagios Core logs to Nagios Log Server. This documentation also applies to Nagios XI as it uses Nagios Core in the backend.

Target Audience

This document is intended for use by Nagios Administrators who wish to analyze their Nagios Core logs.

Overview

This documentation walks you through creating a Filter in Nagios Log Server that takes the Nagios Core log data and stores it into fields in the Elasticsearch database. Once the filter has been created, your Nagios XI or Nagios Core server will be configured to send logs to your Nagios Log Server instance. Using custom Nagios dashboards you will be available to analyze the received log data.

Download Filter

A Filter is how the received log data is broken up into fields that are stored in the Elasticsearch database, it uses regular expressions to break apart the data and hence can be quite complicated. This documentation will not go into the specifics as to how a filter works, all that is required by you is to download a filter from the internet and copy/paste it into a new filter on your Nagios Log Server instance. Navigate to the following URL:

https://github.com/T-M-D/NLS-Collection/blob/master/Filters/Nagios_Core.txt

You will need to copy everything from this line to the end of the file into your clipboard:

```
if [program] == 'nagios_core' {
```

This will be pasted into the new filter that you will create in the next step.

Create Filter

Open the web interface for your Nagios Log Server instance as an administrator. Navigate to **Configure** > **Global (All Instances)** > **Global Config**.

The screenshot shows the Nagios Log Server web interface. The top navigation bar includes 'Home', 'Dashboards', 'Alerting', 'Configure' (circled in blue), 'Help', and 'Admin'. A search bar for logs is on the right. The left sidebar has a 'Configure' section with 'Apply Configuration', 'Config Snapshots', and 'Add Log Source'. Below that is 'Global (All Instances)' with 'Global Config' (circled in blue) and 'Per Instance (Advanced)'. The main content area is titled 'Global Config' and contains instructions, buttons for 'Save', 'Save & Apply', 'Verify', and 'View'. It is divided into 'Inputs' and 'Filters' sections. The 'Inputs' section lists Syslog, Windows Event Log, and Import Files (Raw and JSON). The 'Filters' section shows 'Apache (Default)' and a '+ Add Filter' button (circled in blue) with a dropdown menu showing 'Custom' (circled in blue).

On the right side of the page click the **+ Add Filter** button and select **Custom**.

In the new filter that appears you will need to provide a title in the *Block Name* field.

In the text area field paste the filter that you previously copied into your clipboard.

Click the **Save** button to create the new filter.

Filters

The screenshot shows the 'Filters' section of the Nagios Log Server web interface. A '+ Add Filter' button is at the top right. Below it, a new filter named 'Nagios Core' is being created. The filter configuration is shown in a text area, containing a 'replace' rule and a 'date' rule with a 'match' rule.

```

    replace => [ 'type', 'nagios_core' ]
  }
  date {
    match => ['epoch_timestamp', 'UNIX' ]
  }
}

```

At this point you should click the **Verify** button to ensure the filter you just created is valid. Once the verify is successful you need to apply the configuration. In the left pane under **Configure** click **Apply Configuration**. Click the **Apply** button and then click **Yes, Apply Now** when prompted.

Configure Nagios XI Or Nagios Core Server

Now that the filter has been created you need to configure your Nagios XI or Nagios Core server to send the `nagios.log` file to your Nagios Log Server instance.

In the following steps you will need to replace `xxx.xxx.xxx.xxx` with the address of your Nagios Log Server instance that will be receiving the logs.

Establish a terminal session to your Nagios XI or Nagios Core server and execute the following commands:

```
cd /tmp
curl -s -O http://xxx.xxx.xxx.xxx/nagioslogserver/scripts/setup-linux.sh
sudo bash setup-linux.sh -s xxx.xxx.xxx.xxx -p 5544 -f "/usr/local/nagios/var/nagios.log" -t nagios_core
```

Once you've executed these commands, any new entries in the `nagios.log` file will be sent to your Nagios Log Server instance. It's worth pointing out this part of the command:

```
-t nagios_core
```

This tells Nagios Log Server that the program these logs are coming from is `nagios_core`. This is how the filter determines if the log should be processed, this is because of the first line of the filter:

```
if [program] == 'nagios_core' {
```

Review Logs

At this point you can see if the logs are being received by using a dashboard query. On your Nagios Log Server instance open the **Dashboards** page. In the query field type the following:

```
program:nagios_core
```

You should see a filtered list of logs from your Nagios XI or Nagios Core server.

The screenshot shows the Nagios Log Server (LS) interface. The top navigation bar includes 'Home', 'Dashboards', 'Alerting', 'Configure', 'Help', and 'Admin'. A search bar is present with the text 'Search logs ...'. The user is logged in as 'nagiosadmin'.

The main content area shows a dashboard titled 'My Default Dashboard'. A query field contains the text 'program:nagios_core'. Below the query field, there is a 'FILTERING' section with a star icon.

The 'EVENTS OVER TIME' section displays a bar chart showing the count of events per 10s for the query 'program:nagios_core (79)'. The chart shows a significant spike at 14:59:00.

The 'ALL EVENTS' section shows a list of events. The table has columns for '@timestamp', 'host', 'type', 'message', and 'Actions'. The events are filtered to show 24 current events out of 41 total.

@timestamp	host	type	message	Actions
2017-10-25T15:00:06.000+11:00	10.25.5.2	nagios_core	Warning: Return code of 255 for check of service 'Yum Updates' on host 'xi-r6x-x64' was out of bounds.	Q
2017-10-25T14:59:56.000+11:00	10.25.5.2	nagios_core	Warning: Return code of 255 for check of service 'CPU Stats' on host 'xi-r6x-x64' was out of bounds.	Q
2017-10-25T14:59:53.000+11:00	10.25.5.2	nagios_core	Warning: Return code of 255 for check of service 'Load' on host 'xi-r6x-x64' was out of bounds.	Q
2017-10-25T14:59:36.000+11:00	10.25.5.2	nagios_core	Warning: Return code of 255 for check of service '/' Disk Usage' on host 'centos01' was out of bounds.	Q

The results will vary depending on how much log activity your Nagios XI or Nagios Core server generates.

Uploading Dashboards

There are several dashboards available to help analyze the Nagios log data, they are designed to work with the fields generated by the filter you created. You will need to download them from the following location:

<https://github.com/T-M-D/NLS-Collection/tree/master/Dashboards>

Once you've downloaded a dashboard you'll need to upload it. On the **Dashboards** page click **Load > Advanced > Browse**.

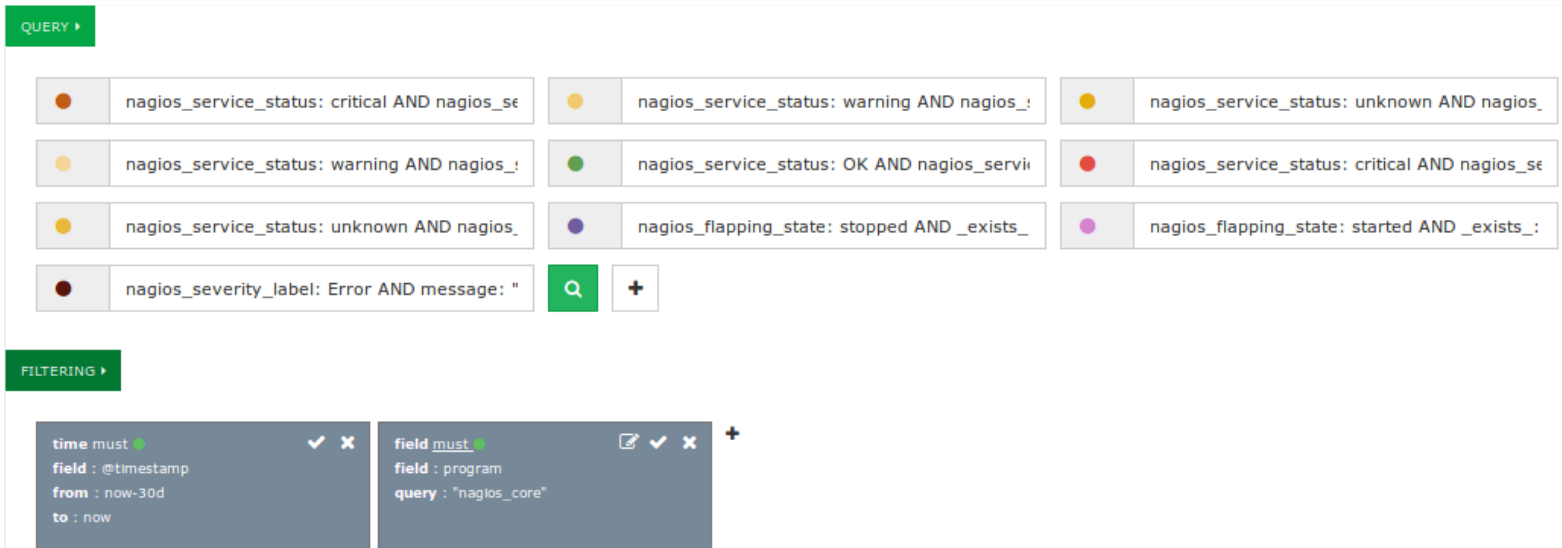
The screenshot shows the Nagios Log Server interface. The 'Dashboards' tab is selected in the top navigation bar. A search query 'program:nagios_core' is entered. The 'EVENTS OVER TIME' chart is visible. A 'Load' button is circled in blue, and a dropdown menu is open, showing a list of dashboards: Apache Dashboard, Empty Dashboard, My Default Dashboard, Nagios Log Server Search, Top Sources and Types, and Advanced. The 'Advanced' dashboard is also circled in blue. A 'Browse...' button is circled in blue, and a blue arrow points from it to the 'Advanced' dashboard in the dropdown menu.

Locate the Dashboard file you downloaded in the browse window, once you open it the dashboard page will refresh with the uploaded dashboard. Here is an example of the first row on the **Nagios - Services** dashboard.

The screenshot shows the Nagios - Services dashboard. It features several widgets: a 'CRITICAL' status indicator, a 'HARD VS SOFT' bar chart, 'SPARKLINES' for CRITICAL HARD and CRITICAL SOFT, '7 DAY TRENDS' showing 17.82% (CRITICAL HARD) and 25.68% (CRITICAL SOFT), and a 'TOP SERVICES' table.

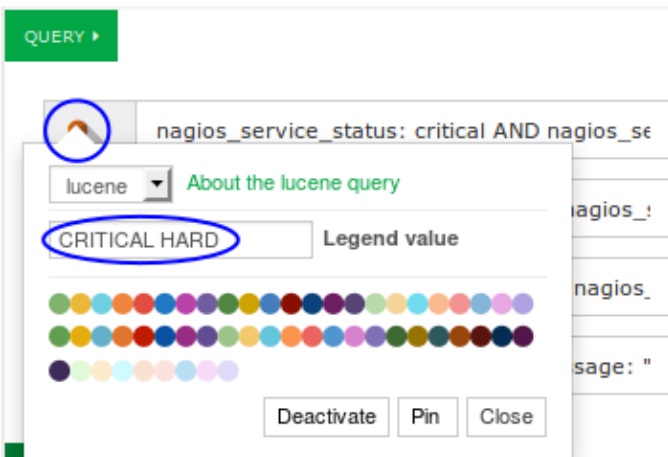
Term	Count	Action
Memory Usage	143	Q
CPU Usage	128	Q
Swap Usage	115	Q
Ping	98	Q
Service Status: MSDTC	73	Q

When you click the **QUERY** and **FILTERING** buttons you can see how multiple queries are defined, this is how the dashboard panels provide different information.



In the screenshot above, the **must** filter for the field **program** where the query is **nagios_core** reduces the amount of log data that your queries at the top must process.

In the screenshots below, the left shows how a query can have a legend. The right shows how a panel can select specific queries, the legend defined on a query makes it easy to identify when selecting it.



Finishing Up

This completes the documentation on how to send Nagios Core Logs to 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>