How to Send Nagios Core Logs to Nagios Log Server

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 OpenSearch 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 OpenSearch 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 the following URL:

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

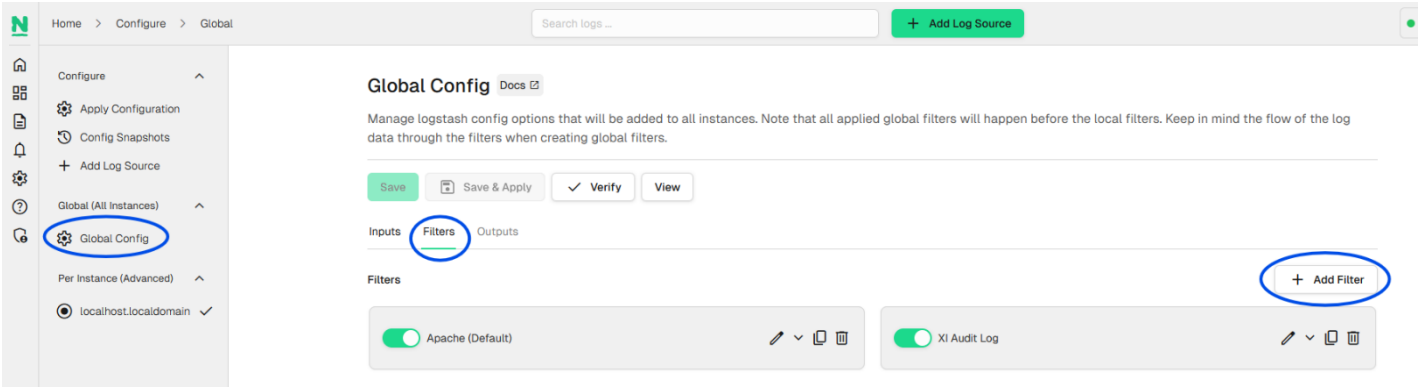
You will need to copy everything from this line (Line 18) to the end of the file into your clipboard:

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

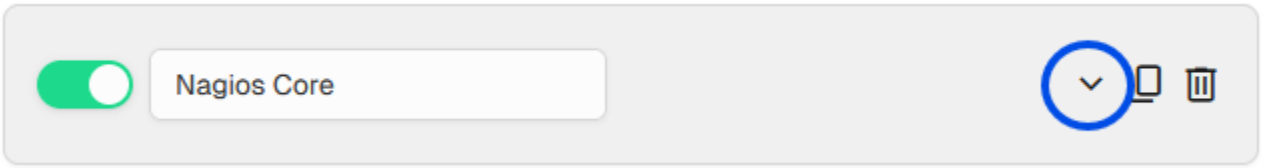
This will be pasted into the new filter that you will create in the next step.

Create Filter

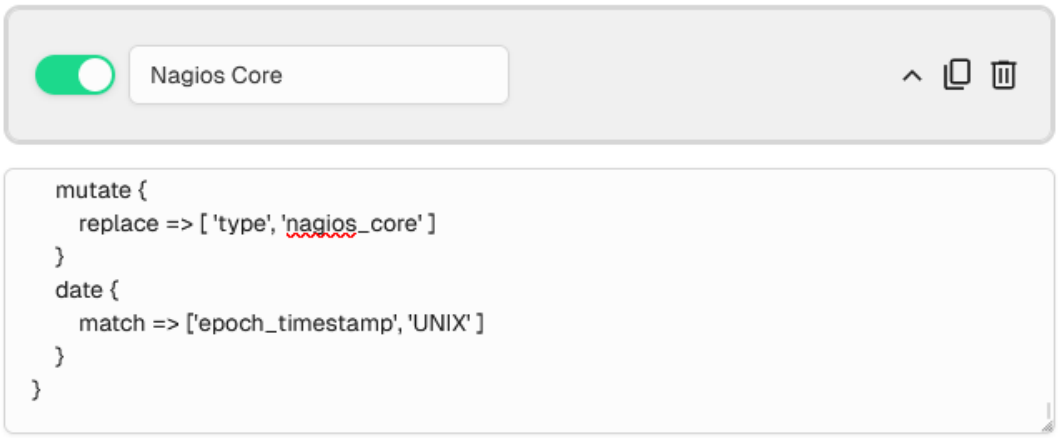
1. Open the web interface for your Nagios Log Server instance as an administrator. Navigate to **Configure** > **Global (All Instances)** > **Global Config**.



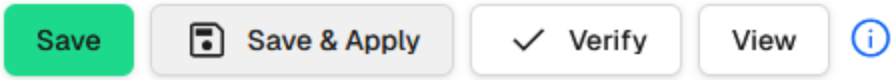
2. Click on the Filter tab. On the right side of the page click the **+ Add Filter** button and select **Custom**.
3. In the new filter that appears you will need to provide a title in the **Block Name** field. Click the down arrow as seen below to expand the filter.



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



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



6. 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.
7. Click **Save & Apply** in the page controls to save your changes to the cluster.

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. The above command uses the `-t` option to provide a Filetag value for the logs you will be sending:

```
-t nagios_core
```

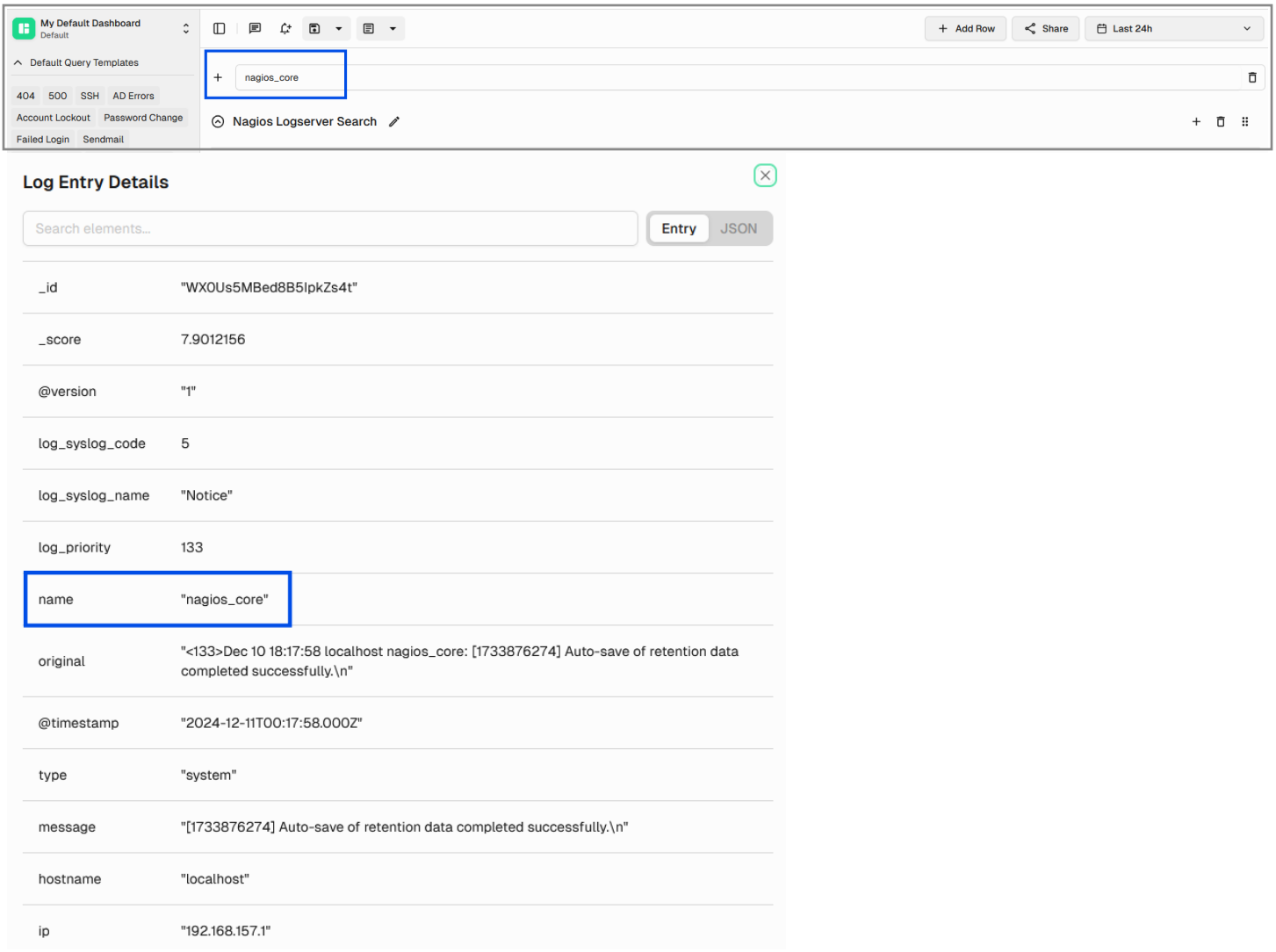
This tells Nagios Log Server that the program these logs are coming from is `nagios_core`. This is how the filter determines if the log should be processed, this is because of the first line of the filter:

```
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:

```
nagios_core
```



You should see a filtered list of logs from your Nagios XI or Nagios Core server. The filetag will be available with the **Name** parameter in the Log Entry Details, as seen here:

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

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 Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum Visit Nagios Knowledge Base Visit Nagios Library