Purpose

This document describes how to integrate your Squid Proxy server logs into Nagios Log Server.

Target Audience

This document is intended for use by Administrators who want to get logs from their Squid Proxy server.

Overview

This document will detail how to configure a server running Squid to send logs to the Nagios Log Server, and how to configure the Filters in the Nagios Log Server to parse the logs from Squid.

The Nagios Log Server is a powerful tool to manage logs that will allow Admins using Squid Proxy server to quickly and easily see what is accessed and request from users. Our example is using CentOS 7 server with Squid Proxy server installed via yum. For this example:

- The default logs are in `/var/log/squid/`
- There are two log files
  - `access.log` = logs web requests and results
  - `cache.log` = logs error and debug message from squid

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/Squid.txt

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

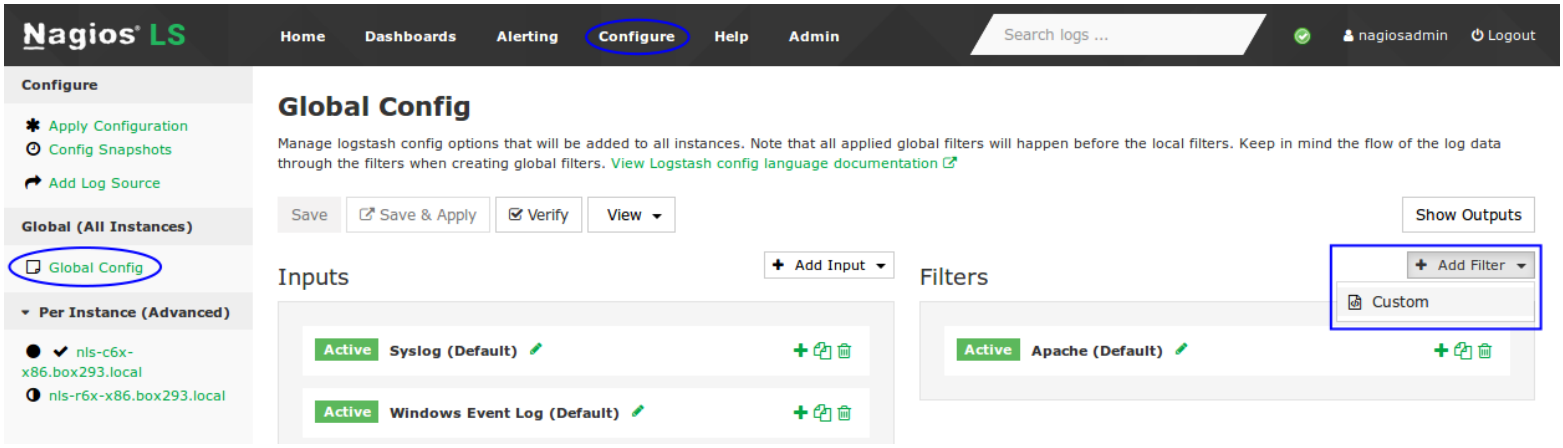
You will need to copy everything from this line to the end of the file into your clipboard:

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

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**.

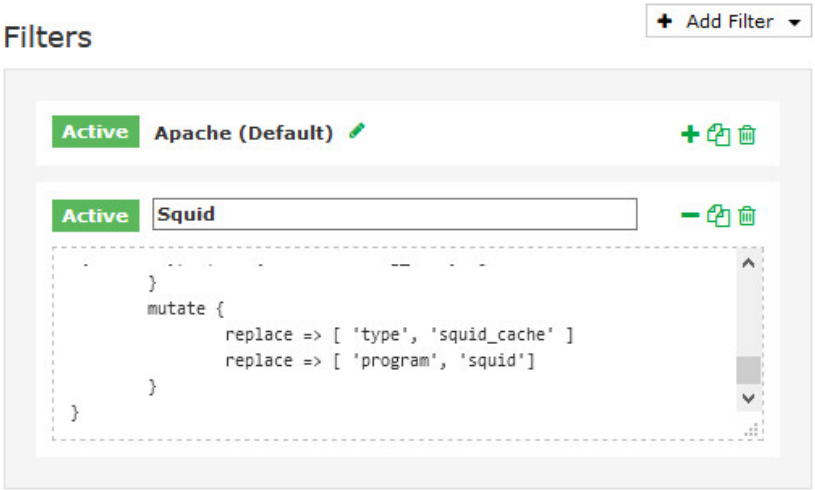


On the right side of the page click the **+ Add Filter** button and select **Custom**.

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.



Nagios®

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

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 Squid Server To Send The Logs

Now that the filter has been created you need to configure your Squid server to send the `access.log` and `cache.log` files 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
bash setup-linux.sh  -s xxx.xxx.xxx.xxx -p 5544 -f /var/log/squid/access.log -t squid_access
bash setup-linux.sh  -s xxx.xxx.xxx.xxx -p 5544 -f /var/log/squid/cache.log -t squid_cache
```

After executing these commands your Squid server should be sending the Squid logs to your Nagios Log Server. You should be able to search for **`squid`** on the Dashboards page and see the results coming in, confirming that everything is correctly configured.

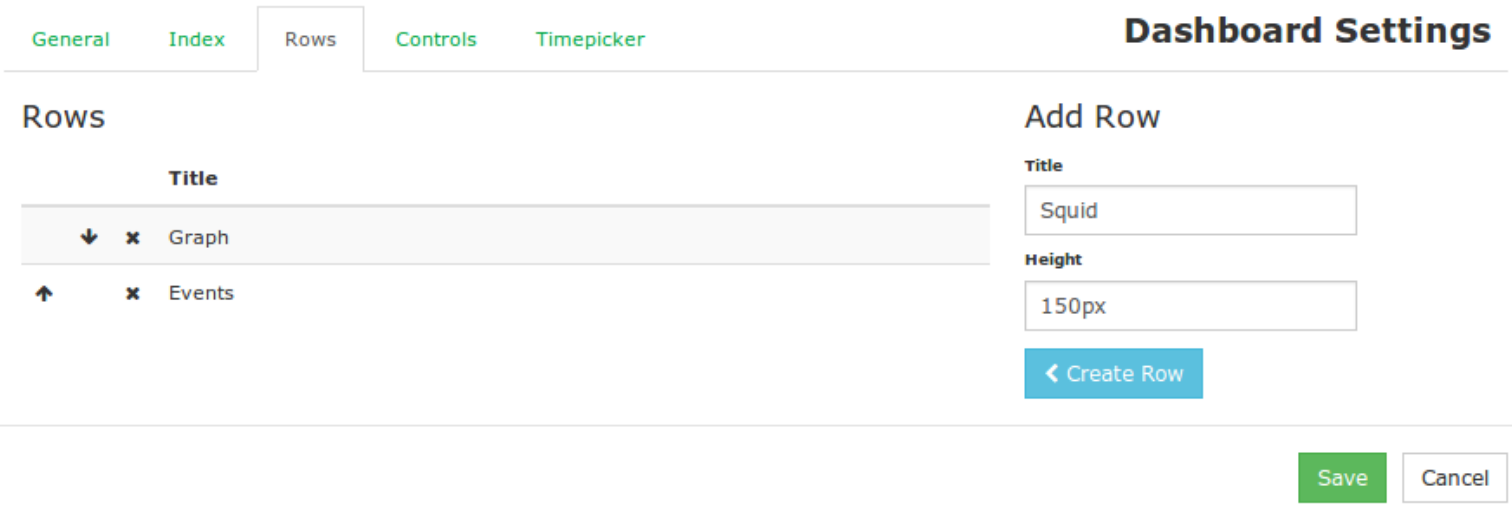
@timestamp	host	type	message	Actions
2017-11-01T17:16:51.000+11:00	10.25.10.1	squid_access	1509517009.468 61497 2001:44b8:3132:25:10:25:254:50 TCP_TUNNEL/200 4213 CONNECT collector.githubapp.com:443 - HIER_DIRECT/52.0.125.114 -	
2017-11-01T17:16:51.000+11:00	10.25.10.1	squid_access	1509517009.468 61497 2001:44b8:3132:25:10:25:254:50 TCP_TUNNEL/200 4271 CONNECT collector.githubapp.com:443 - HIER_DIRECT/52.0.125.114 -	
2017-11-01T17:16:51.000+11:00	10.25.10.1	squid_access	1509517009.468 61497 2001:44b8:3132:25:10:25:254:50 TCP_TUNNEL/200 4213 CONNECT collector.githubapp.com:443 - HIER_DIRECT/52.0.125.114 -	

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

Dashboards

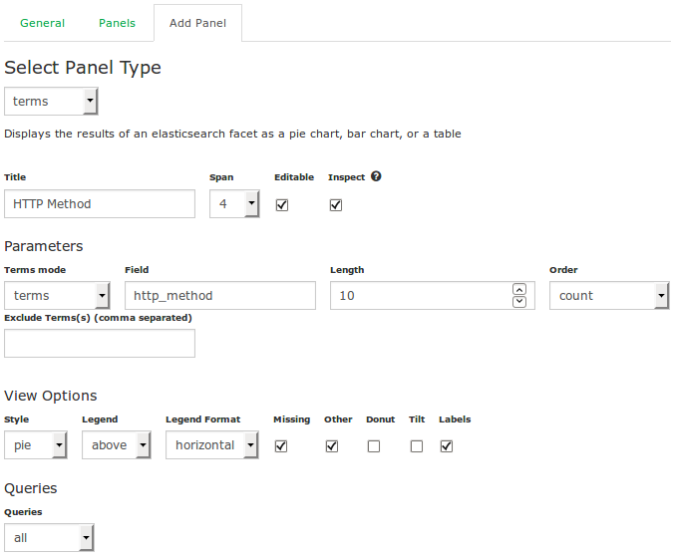
Once you've received some log data you will be able to visualize that data using panels. Start off by adding a new row. At the bottom right of the screen click the **+ ADD A ROW** link.

- Give the row a **Title** and then click the **Create Row** button
- Use the up arrow icon to move it to the top of the list
- Click **Save**



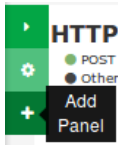
On the new row click the **Add panel to empty row** button.

- Select the Panel Type of **terms**
- Give it the title of **HTTP Method**
- Field = `http_method`
- Style = **pie**
- Click **Save**

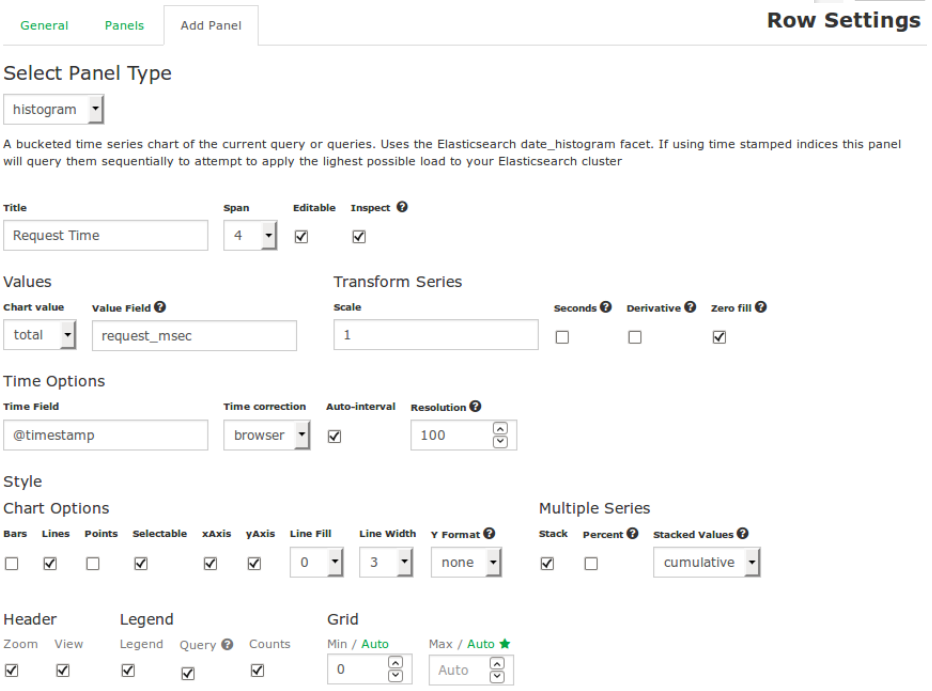


© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

Click the **Add panel** button

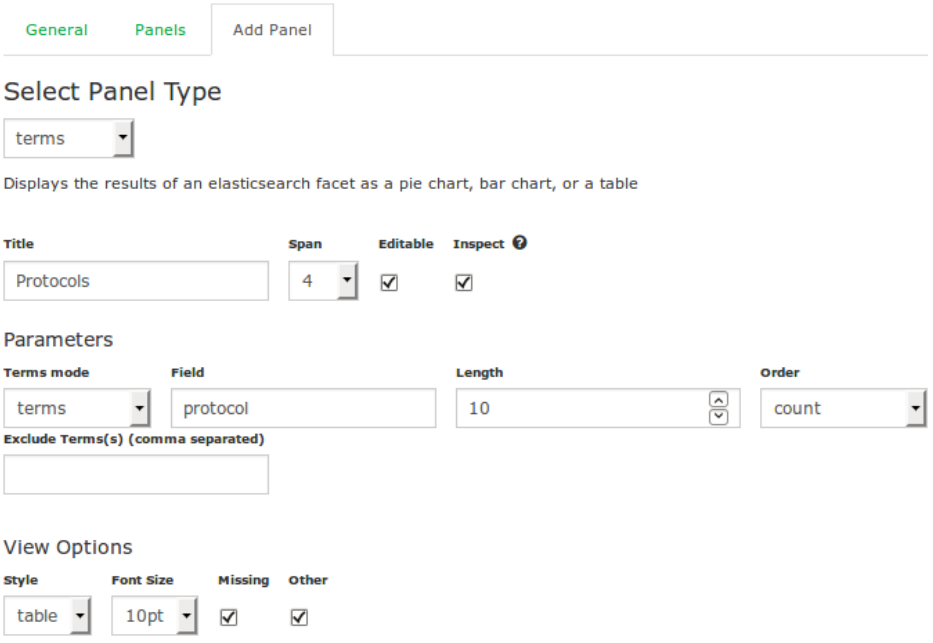


- Select the Panel Type of **histogram**
- Give it the title of **Request Time**
- Chart value = **total**
- Value Field = `request_msec`
- Chart Options
  - Un-check **Bars**
  - Check **Lines**
- Click **Save**



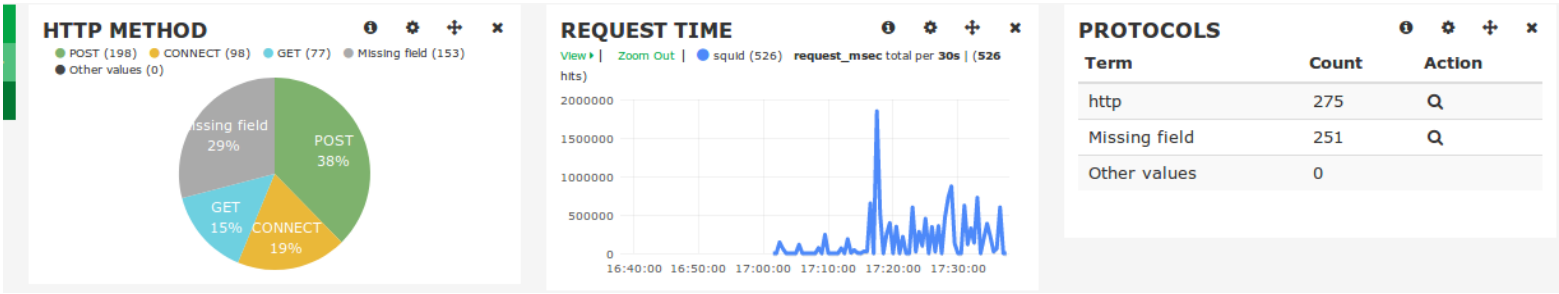
Click the **Add panel** button

- Select the Panel Type of **terms**
- Give it the title of **Protocols**
- Field = `protocol`
- Style = **table**
- Click **Save**



© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

Here is what your row will now look like after adding those panels.



Additional Resources

More info about Squid logs can be found here:

- http://www.squid-cache.org/
- http://wiki.squid-cache.org/SquidFaq/SquidLogs

Finishing Up

This completes the documentation on how to monitor a Squid Proxy Server with 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

© 2017 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.