



## Purpose

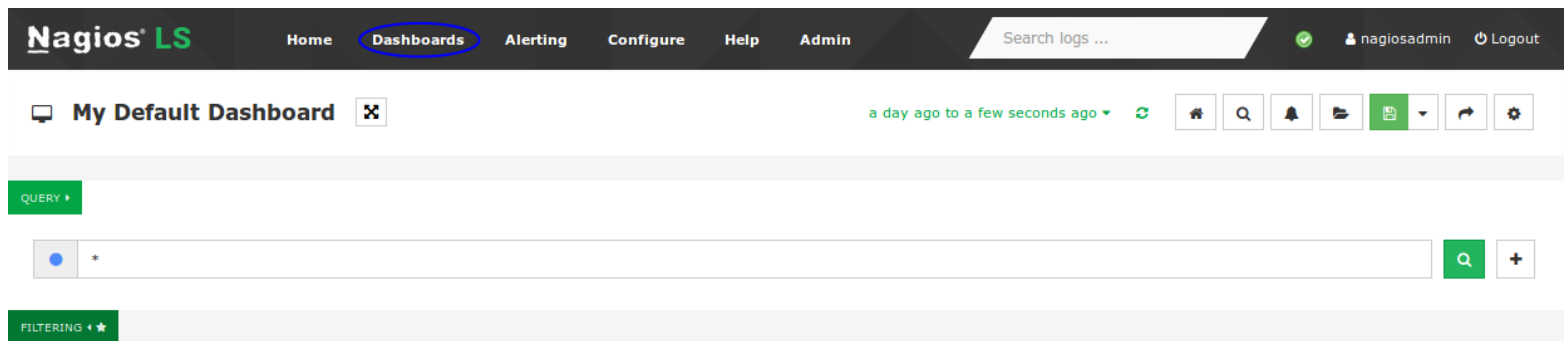
This document describes how to use queries and filters to drill down to see the exact information you are looking for using Nagios Log Server Dashboards.

## Target Audience

This document is intended for use by Nagios Log Server administrators and users who wish to better understand querying, filtering and drilling down the data in Nagios Log Server.

## Navigate

This documentation explains features that are located in the **Dashboards** menu, this is located on the top navigation bar.



Dashboards allow you to create custom views of your log data that are based on queries and filters.

**Note:** when you navigate away from the dashboards page, any changes you have made will be lost (if you did not click the save button). You can save dashboards so your customizations are not lost, this is explained in the [Dashboard Controls](#) section of this document.

# Nagios Log Server

## Analyzing Logs

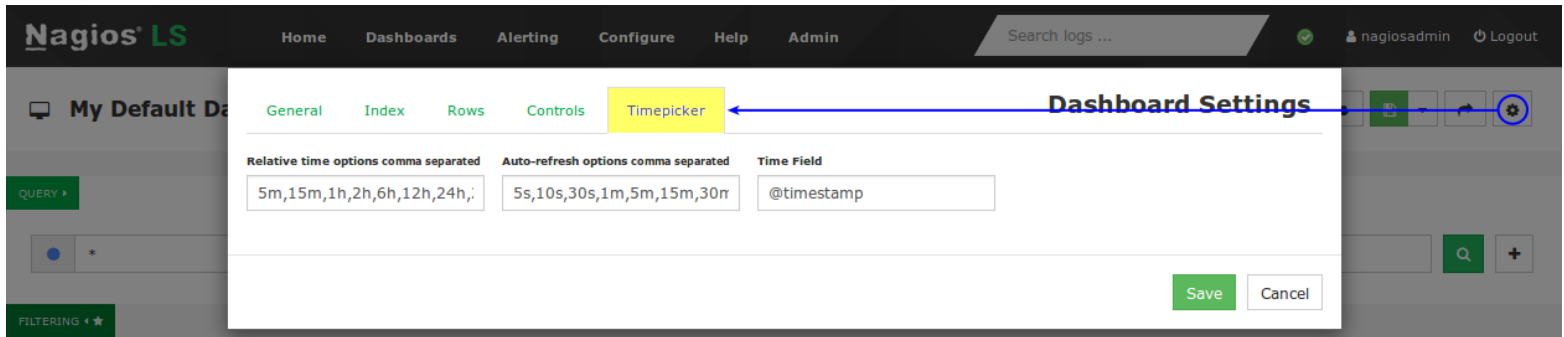
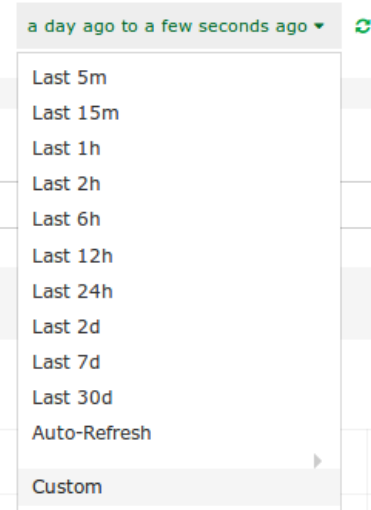
### Time Period

At the top of the screen is a drop down list that lets you select the time period for which you want the dashboard to apply to.

This is by default the past day (**a day ago to a few seconds ago**). When you click the refresh icon next to the list, the data on the screen will refresh while retaining any setting you have customized on the screen.

Using the drop down list allows you to select a pre-defined time range with the custom option available if one of those time frames does not meet your needs.

You can define this list of time frames by clicking the settings icon on the far right.

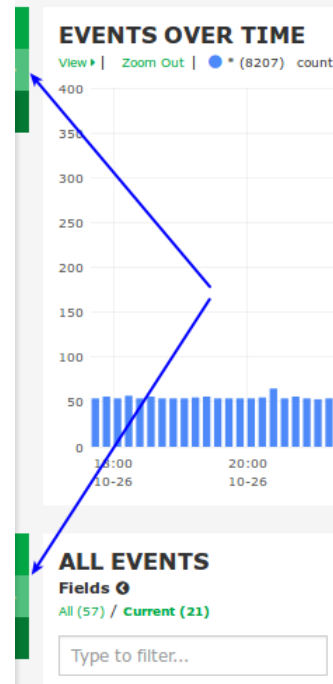


On the **Timepicker** tab you can define these in the fields in the order that you want them to appear.

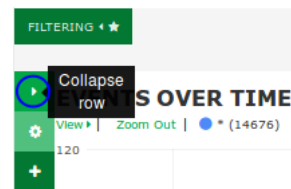
## Row And Panel Overview

Rows and panels are the building blocks for creating dashboards comprised of graphs and tables. When you load the default dashboard, underneath QUERY and FILTERING is the following:

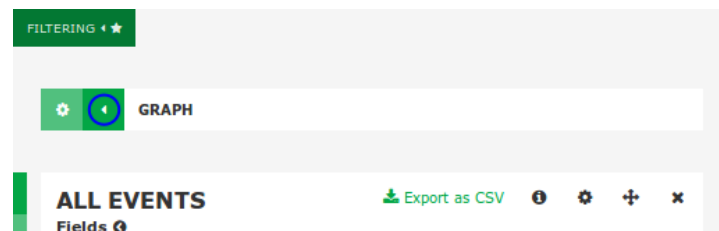
- **EVENTS OVER TIME** and **ALL EVENTS**
- Both of these are called **Panels** and they are contained within a **Row**
  - The screenshot to the right shows the hidden options for a **Row**, these appear at the top left of each row
- A row can have multiple panels
- Rows have a width of 12
- Panels can be a size between 1 - 12, you could have three panels of sizes 3, 5 and, 4
- By default the panels **EVENTS OVER TIME** and **ALL EVENTS** have a width of 12



A row can be collapsed to hide it temporarily from view, click the play icon in the top box to collapse the row.



Here you can see when a row is collapsed, to expand it click the play icon.



Customization of rows and panels is covered in more detail in the [Row And Panel Customization](#) section of this document.

# Nagios Log Server Analyzing Logs

## Queries

When you start collecting log data over a long period of time you will want to look at certain log types and categories. Nagios Log Server queries allow you to perform a search to show you the data you are looking for. Here is a view of the default dashboard inside Nagios Log Server:

**My Default Dashboard** ✕ a day ago to a few seconds ago 🏠 🔍 🔔 📄 📄 ↶ ⚙️

**QUERY** ▶

• \*

**FILTERING** ⬇ ★

**EVENTS OVER TIME** 🔍 ⚙️ + ✕  
 View ▶ | Zoom Out | • \* (39633) count per 10m | (39633 hits)

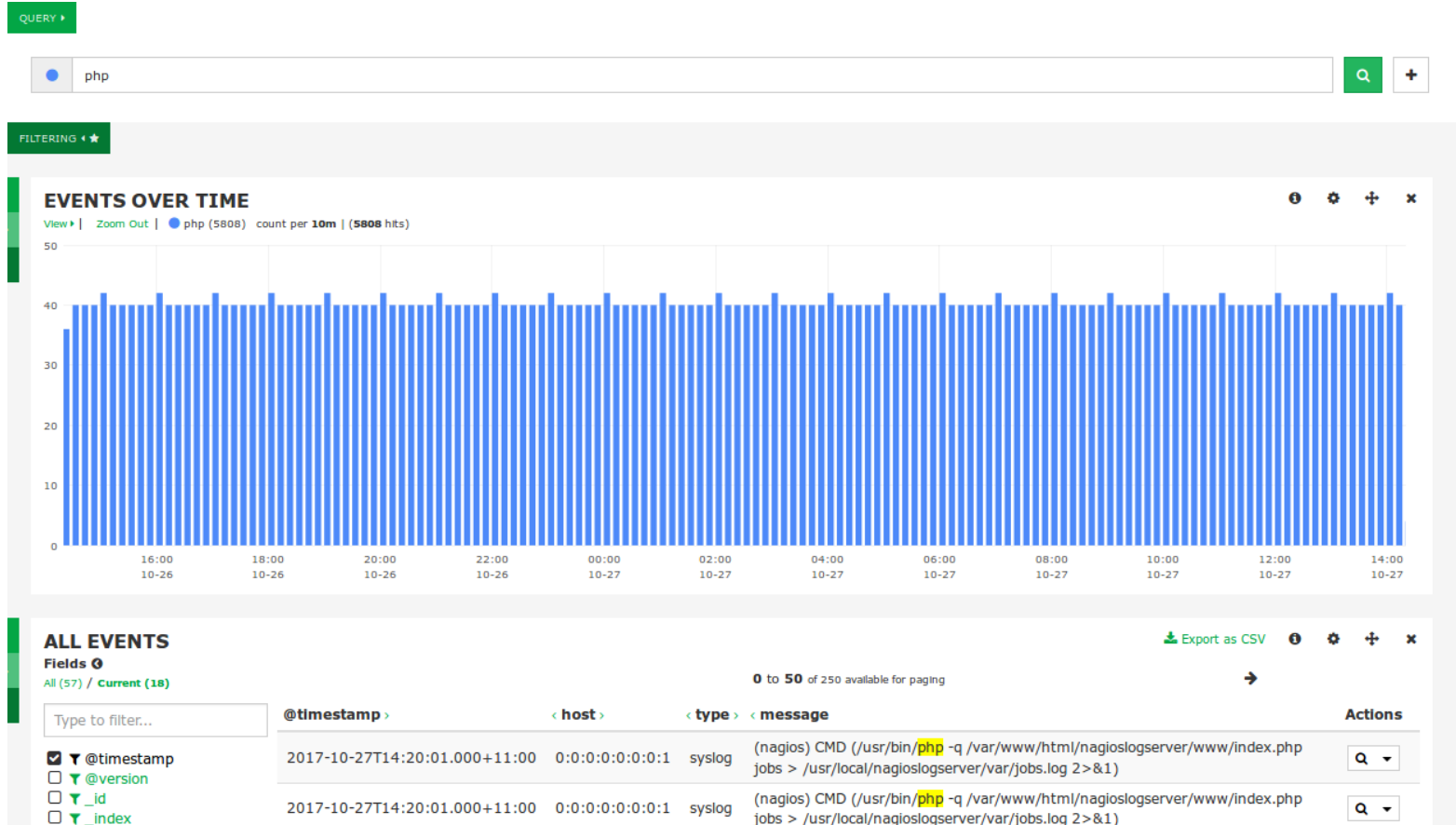
**ALL EVENTS** 📄 🔍 ⚙️ + ✕  
 Fields 🔍  
 All (57) / Current (22) 0 to 50 of 250 available for paging ➔ 📄 Export as CSV

Type to filter...	@timestamp >	< host >	< type >	< message >	Actions
<input checked="" type="checkbox"/> @timestamp	2017-10-27T14:14:31.000+11:00	0:0:0:0:0:0:1	syslog	nagios : TTY=unknown ; PWD=/var/www/html/nagioslogserver/www ; USER=root ; COMMAND=/etc/init.d/elasticsearch status	🔍
<input type="checkbox"/> @version					
<input type="checkbox"/> _id					
<input type="checkbox"/> _index					
	2017-10-27T14:14:31.000+11:00	0:0:0:0:0:0:1	syslog	nagios : TTY=unknown ; PWD=/var/www/html/nagioslogserver/www ; USER=root ; COMMAND=/etc/init.d/logstash status	🔍

This graph view (events over time) is showing us all the log data the server is receiving. This is because the default query is an asterisk \*, this will display all log data in the database (*last day by default*). Through this view you can see the log data traffic and trends in a somewhat birds-eye view for the last day.

## Nagios Log Server Analyzing Logs

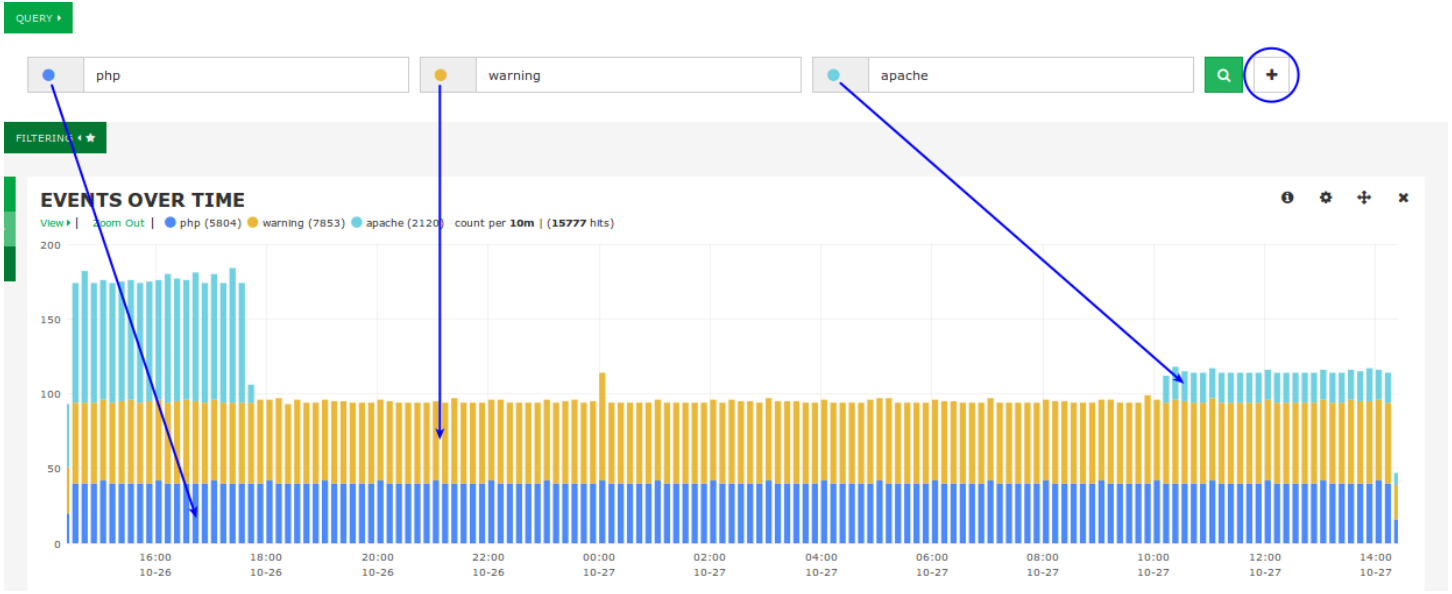
Performing a query is as simple as typing the word you want to search for. Here is a screenshot that shows the results from searching for the word `php`.



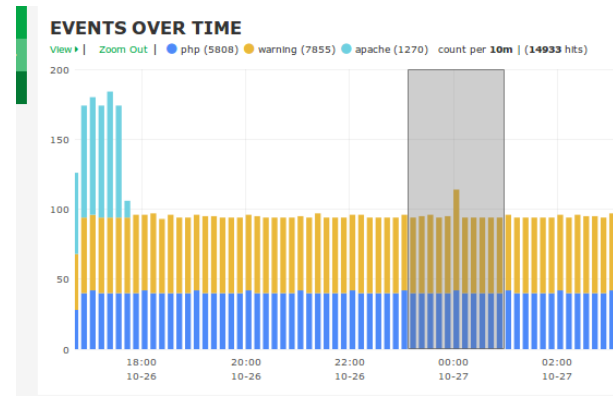
Queries are **not** case-sensitive, so in this example `php` is the same as `PHP`. When you query, Nagios Log Server will check every field in the Elasticsearch database for the string you are searching for.

You are not restricted to just one query, you can define multiple queries by clicking the **+** sign to the right of the Query field. By using multiple queries, Nagios Log Server sets each query as a different color, this helps identify the different queries in the EVENTS OVER TIME graph and in other panels. The screenshot on the following page shows three queries of `php`, `warning` and `apache`, you can see in the graph how the results of each query have a different color.

# Nagios Log Server Analyzing Logs



With the EVENT OVER TIME graph you can also drag your mouse over a time period to zoom in for a closer look at those log events, this is demonstrated in the screenshot to the right.



In the query examples above you have seen how you can search for specific words. These queries are searching all the fields in the Elasticsearch database for the time period you are currently viewing. You can also perform the queries on specific fields. To give you an example as to what fields are available, the following screenshot shows the ALL EVENTS table where you can see the "type" field has been highlighted.

**ALL EVENTS** Export as CSV

Fields  All (57) / Current (22)

Type to filter...

- @timestamp
- @version
- \_id
- \_index
- \_type
- epoch\_timestamp
- facility
- facility\_label
- host

0 to 50 of 250 available for paging

@timestamp >	host <	type <	message	Actions
2017-10-27T00:58:47.000+11:00	0:0:0:0:0:0:1	syslog	nagios : TTY=unknown ; PWD=/var/www/html/nagioslogserver/www ; USER=root ; COMMAND=/etc/init.d/logstash status	Q
2017-10-27T00:58:47.000+11:00	0:0:0:0:0:0:1	syslog	nagios : TTY=unknown ; PWD=/var/www/html/nagioslogserver/www ; USER=root ; COMMAND=/etc/init.d/logstash status	Q
2017-10-27T00:58:41.000+11:00	10.25.5.2	nagios_core	Warning: Return code of 255 for check of service 'Open Files' on host 'centos01' was out of bounds.	Q
2017-10-27T00:58:41.000+11:00	10.25.5.2	nagios_core	Warning: Return code of 255 for check of service 'Total Processes' on host 'centos01' was out of bounds.	Q

1295 Bandana Blvd N, St. Paul, MN 55108 [sales@nagios.com](mailto:sales@nagios.com) US: 1-888-624-4671 INTL: 1-651-204-9102

# Nagios Log Server Analyzing Logs

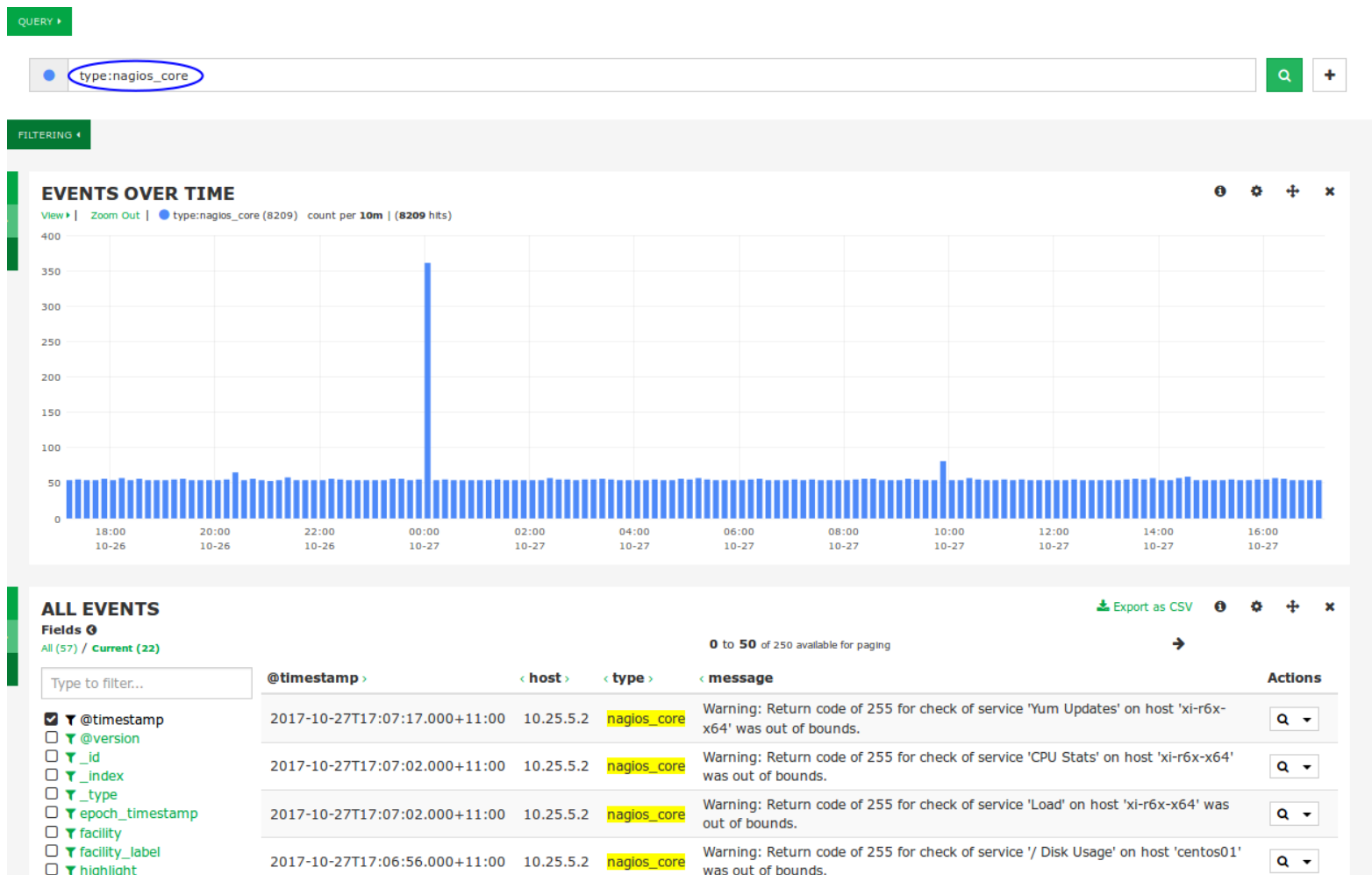
To perform a query for a value in a specific field the syntax is as follows:

```
<field_name>:<query>
```

For example

```
type:nagios_core
```

Here is a screenshot showing that query:



1295 Bandana Blvd N, St. Paul, MN 55108 [sales@nagios.com](mailto:sales@nagios.com) US: 1-888-624-4671 INTL: 1-651-204-9102



## Filters

A filter is similar to a query however it's purpose is to reduce the amount of data a query is performed against. For example you may only be interested in logs that have the `severity_label` of `Notice`.

The filter section is collapsed by default. Click the **FILTERING** icon to expand it and show the options available for filtering.

FILTERING ▾

New filters can be added by clicking the + icon.

time must ✓ ✕ + Add a query filter

field : @timestamp

from : now-24h

to : now

However it can be much simpler to add a filter by using the data in the **ALL EVENTS** table. To view the data about a specific event, in the ALL EVENTS table click on a log entry.

In this screenshot, the left column shows all the fields that are available for this specific log entry.

In this screenshot you can see the spyglass icon has been highlighted.

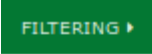
By clicking the spyglass icon for the `severity_label` field you will create a **MUST** filter for the value of `Notice`.

@timestamp >	< host >	< type >	< message >	Actions
2017-10-27T17:14:16.000+11:00	0:0:0:0:0:0:1	syslog	nagios : TTY=unknown ; PWD=/var/www/html/nagioslogserver/www ; USER=root ; COMMAND=/etc/init.d/logstash status	Q ▾

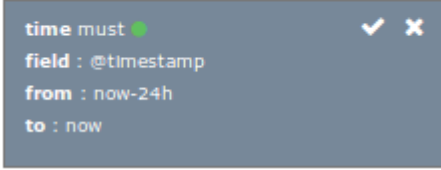
View: [Table](#) / [JSON](#) / [Raw](#)

Field	Action	Value	Search
<input checked="" type="checkbox"/> @timestamp	Q 🔍 🗄	2017-10-27T06:14:16.000Z	Q ▾
<input type="checkbox"/> @version	Q 🔍 🗄	1	Q ▾
<input type="checkbox"/> _id	Q 🔍 🗄	AV9cd4SUplMWNT2xD65g	Q ▾
<input type="checkbox"/> _index	Q 🔍 🗄	logstash-2017.10.27	Q ▾
<input type="checkbox"/> _type	Q 🔍 🗄	syslog	Q ▾
<input type="checkbox"/> facility	Q 🔍 🗄	10	Q ▾
<input type="checkbox"/> facility_label	Q 🔍 🗄	security/authorization	Q ▾
<input checked="" type="checkbox"/> host	Q 🔍 🗄	0:0:0:0:0:0:1	Q ▾
<input type="checkbox"/> logsource	Q 🔍 🗄	nls-c6x-x86	Q ▾
<input checked="" type="checkbox"/> message	Q 🔍 🗄	nagios : TTY=unknown ; PWD=/var/www/html/nagioslogserver/www ; USER=root ; COMMAND=/etc/init.d/logstash status	Q ▾
<input type="checkbox"/> priority	Q 🔍 🗄	85	Q ▾
<input type="checkbox"/> program	Q 🔍 🗄	sudo	Q ▾
<input type="checkbox"/> severity	Q 🔍 🗄	5	Q ▾
<input type="checkbox"/> severity_label	Q 🔍 🗄	Notice	Q ▾
<input type="checkbox"/> timestamp	Q 🔍 🗄	Oct 27 17:14:16	Q ▾
<input checked="" type="checkbox"/> type	Q 🔍 🗄	syslog	Q ▾

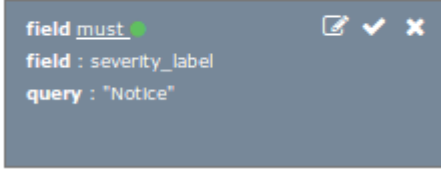



 FILTERING ▶

Here you can see new newly added filter.

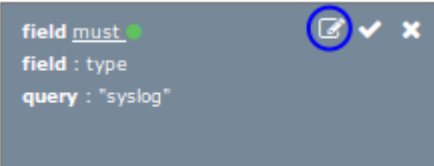


```
time must
field : @timestamp
from : now-24h
to : now
```



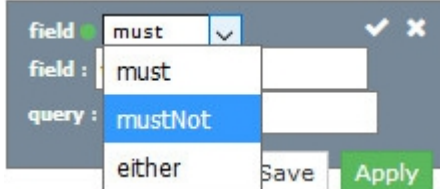
```
field must
field : severity_label
query : "Notice"
```

Here is another example. A filter was created by clicking the spyglass icon where the `type` is `syslog`. Now on the newly created entry click the **Edit** icon.



```
field must
field : type
query : "syslog"
```

The filter will now change to an edit mode. Use the field drop down list, select **mustNot** and then click **Apply**. The screen will refresh and the **EVENTS OVER TIME** and **ALL EVENTS** panels will apply the updated filters.



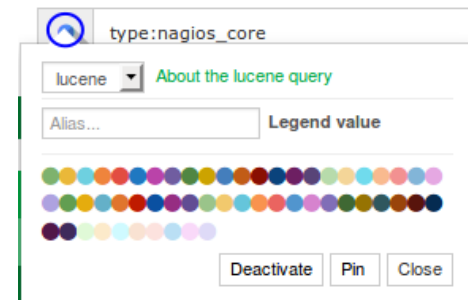
```
field must
field : must
query : mustNot
either
```

You can see how using the spyglass on the **ALL EVENTS** table makes adding filters easy.

## Query Options

There are several options available for a query, clicking the colored circle next to the query will display these options.

There are three types of queries available: **lucence**, **regex** and **topN**. Each query type has a link next to it that provides a modal with more information (**About the xxx query**). These will not be discussed here as this is an advanced topic, the help provided in the modal is a good starting point.



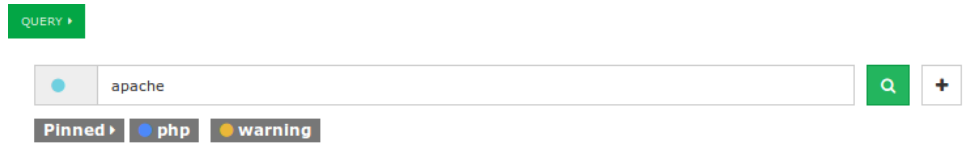
The two most commonly used options are the **Legend value** and the **color** associated with the query.

- Defining a **Legend value** makes it easy to identify the query when creating panels
- The color selected is what appears in graphs and charts for this query

## Nagios Log Server Analyzing Logs

When you click the **Deactivate** button the query will not be part of the results in the other rows and panels. Deactivating allows you to temporarily stop using the query, it saves you from having to delete and re-add it.

The **Pin** button allows a query to be collapsed, this is useful when you have many queries. The pinned queries appear next the the **Pinned** button. You can also click the **Pinned** button to hide the list of pinned queries, very helpful for conserving screen real estate.



## Row And Panel Customization

As explained earlier, rows and panels are the building blocks for creating dashboards comprised of graphs and tables. Now that the basic concepts of queries have been explained you will see how these queries can be used to visualize your log data.

To create a new row click the **+Add Row** link at the bottom right of the Dashboards page.



This will bring up the **Dashboard Settings** modal with the **Rows** tab selected. On the right provide a **Title** for the row, define the height and then click the **< Create Row** button.

A screenshot of the Nagios Log Server Dashboard Settings modal. The 'Rows' tab is selected. On the left, there is a list of rows with columns for 'Title', a collapse icon (down arrow), and a delete icon (x). The rows are 'Graph' and 'Events'. On the right, there is an 'Add Row' form with fields for 'Title' (containing 'New Row') and 'Height' (containing '200px'). Below the form is a blue button labeled '&lt; Create Row'. At the bottom right of the modal are 'Save' and 'Cancel' buttons.

# Nagios Log Server Analyzing Logs

A newly created row is placed at the bottom of the Rows list. You can use the arrow icons to change the order the rows are displayed on the dashboard.

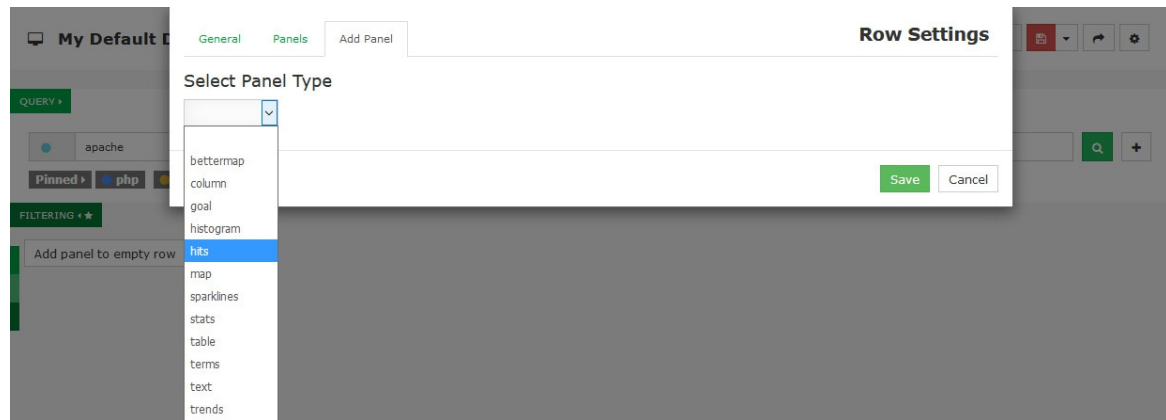
Here you can see the **New Row** has been moved to the top of the list. Click the **Save** button to apply these changes to the dashboards page.

Rows			Rows		
		Title			Title
	↓ ×	Graph		↓ ×	New Row
	↑ ↓ ×	Events		↑ ↓ ×	Graph
	⬆ ×	New Row		↑ ×	Events

When the dashboard is refreshed you'll see the row has been added and it is empty. There's no point in having an empty row so click the **Add panel to empty row** button.

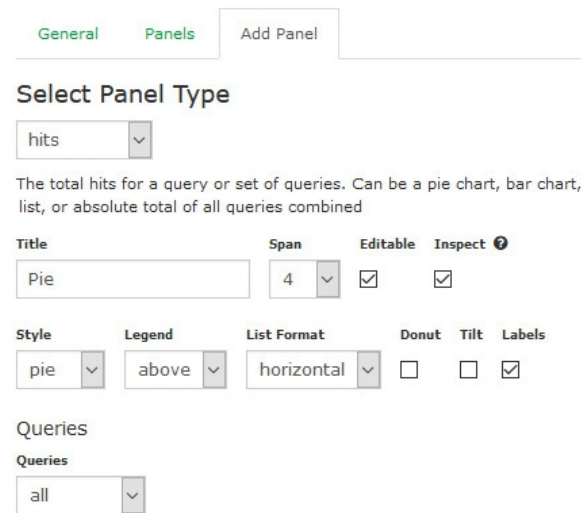


The **Row Settings** modal appears with the **Add Panel** tab selected. You will need to select a panel type from the drop down list, this example is going to use the **hits** panel type.



You will be presented with all the options available for the panel type selected. In this example:

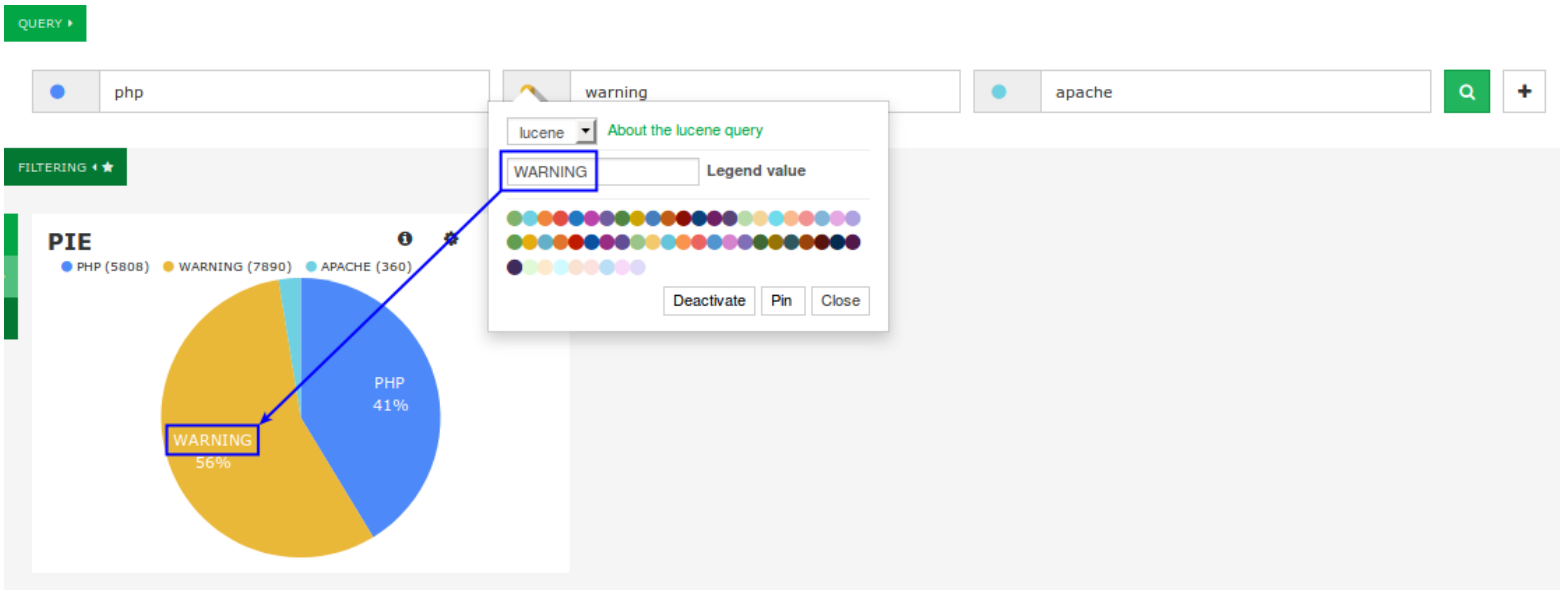
- The **Title** field has been given the name **Pie**
- The **Span** width is **4**
- The **Style** of **pie** was selected



Click the **Save** button to add the panel to the row.

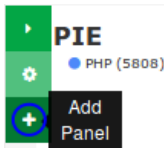
# Nagios Log Server Analyzing Logs

When the dashboard refreshes you will see the new panel added to the row.



You can see in the screenshot above how the **Legend value** that is provided for the query is shown on the pie chart itself, this makes it very easy for you to customize what you see. This could also be turned off, when you look at the panel settings on the previous page there is a **Labels** check box that can disable / enable this.

There is still space for more panels to be added to the dashboard. To add another panel, using the row options menu click the bottom **+** option.



In this example the **terms** panel is being used. This can be used to provide information about the fields in the log data. You can see how the field **host** has been defined.

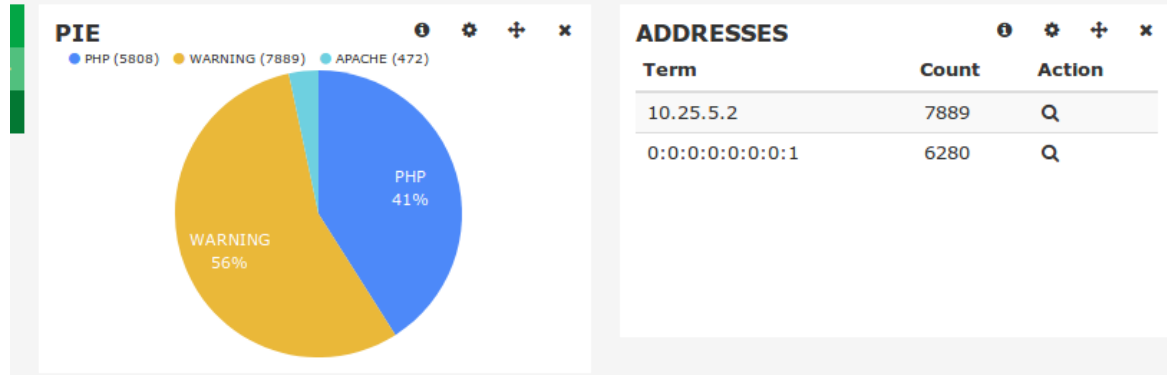
Under the View Options, the style has been set to **table**, the **Missing** and **Other** boxes have been deselected.

Click the **Save** button to add the panel to the row.

The screenshot shows the 'Add Panel' configuration window with the following settings:

- General** tab selected.
- Select Panel Type:** 'terms' (dropdown).
- Title:** 'Addresses' (input field).
- Span:** '4' (dropdown).
- Editable:**
- Inspect:**
- Parameters:**
  - Terms mode:** 'terms' (dropdown)
  - Field:** 'host' (input field)
  - Length:** '10' (input field)
  - Order:** 'count' (dropdown)
- Exclude Terms(s) (comma separated):** 'host', 'host.raw' (input field)
- View Options:**
  - Style:** 'table' (dropdown)
  - Font Size:** '10pt' (dropdown)
  - Missing:**
  - Other:**
- Queries:** 'all' (dropdown)

When the dashboard refreshes you can see how the terms panel can provide a breakdown of data in a specific field.



For the final panel the type of **hits** has been selected again.

This time it is going to be the **bar** style.

Under Queries you can see that **selected** is the chosen option. To the right is the list of queries and you can see that PHP and APACHE have been clicked. The border surrounding the queries indicate which ones have been chosen. You can see how the **Legend value** that is defined on the query makes it easy to identify the different queries.

General Panels Add Panel

### Select Panel Type

hits

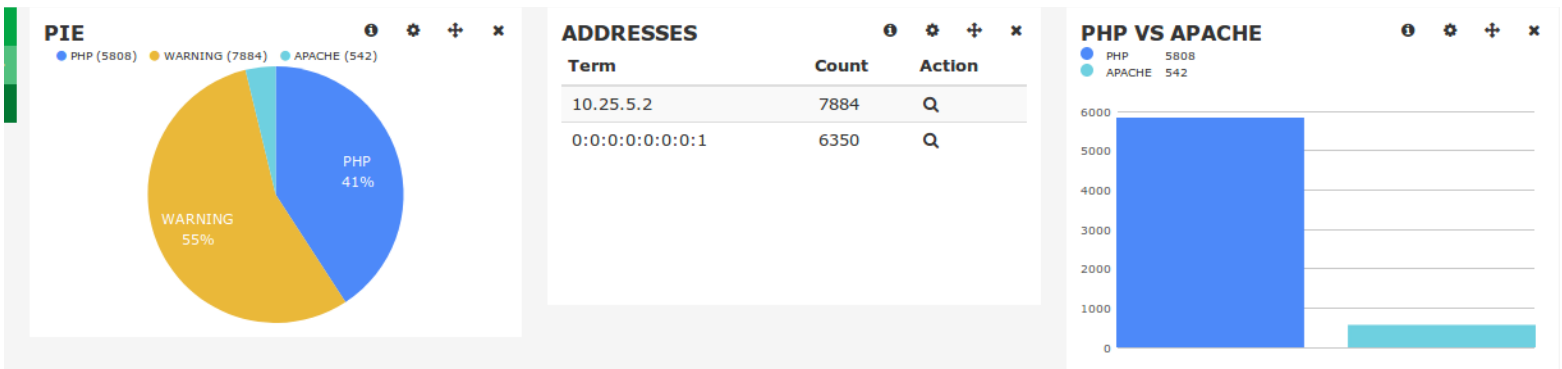
The total hits for a query or set of queries. Can be a pie chart, bar chart, list, or absolute total of all queries combined

Title: PHP vs APACHE Span: 4 Editable:  Inspect:

Style: bar Legend: above List Format: vertical

Queries: selected Selected Queries: PHP WARNING APACHE

Once you save the panel you'll see it added to the row when the dashboard refreshes. There are many different panel types available allowing you to build a dashboards that visualizes your log data.



## Panel Controls

Panels have four icons in the top right, they are explained as follows:

### Inspect

Open a modal that shows how to obtain the panel data using a `curl` command

### Configure

Change any of the panel options, these are the same as when adding a panel

### Move

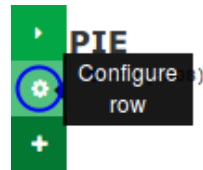
Use the mouse to move the panel to a different row location, either on the same row or another row

### Remove

Delete the panel

## Configure Row

To change the settings of a row use the row options and click the **Configure row** icon. This will bring up the **Row Settings** modal, these are self explanatory and do not need explaining.



## Dashboard Controls

The top of the Dashboards page has a common set of controls which are explained as follows.

### Toggle Fullscreen / Exit Fullscreen

The fullscreen mode removes the top menu bar and the bottom status bar

### Home

Load the dashboard that has been saved as the default

This can be changed via **Save** (drop down) > **Advanced** > **Set as Default Dashboard**

### Manage Queries

This icon brings up the manage queries modal, explained in detail in the [Manage Queries](#) section

### Create an alert

This allows you to create an alert using the current query

Please refer to the [Alerting On Log Events](#) documentation



## Nagios Log Server Analyzing Logs



### Load

Load any dashboard that you previously saved

Clicking the icon presents a drop down menu with all the dashboards that you have saved, click a dashboard to load it

Global dashboards are indicated by the  icon to the left of the dashboard title

You can delete a dashboard from the load list by clicking the  to the right of the dashboard title

Use with caution as you won't be able to recover a deleted dashboard

The Advanced link at the bottom of the list allows you import an dashboard from a file





### Save

This saves all the customizations you have made such as queries, filter, graphs, tables, colors etc  
The icon will have a red color when there are changes to your dashboard that have not been saved  
If you have not saved the current dashboard with a name, click the drop down arrow and then:

Type a name for the dashboard

Click the appropriate save button:

-  Save as a private dashboard, only you can see this dashboard
-  Save as a **Global** dashboard that all users will have access to

*Only Admins can save global dashboards*

The Advanced link underneath allows you to:

Set this dashboard as the default dashboard that is loaded when you navigate to the Dashboards page via the top menu bar

Export the dashboard to a file



### Share

Provides you with a URL that you can give to other users to access your dashboard

The user will be required to have a Nagios Log Server user account to be able to view the URL



### Configure

Displays the **Dashboard Settings** modal for the current dashboard

These settings are self explanatory and do not need explaining



## Manage Queries

The Manage Queries modal appears as follows:

### Manage Queries

✕

Make global ?

---

Queries Available

Name	Created By	Actions
Apache 404 Errors	NAGIOS	
Error Critical Alert Severity	NAGIOS	
Failed SSH Logins	NAGIOS	
Windows Failed Logins	NAGIOS	

Filters are also included as part of a query, so any references here to a query includes filters.

To save your current dashboard query type a value in the top field and then click the **Create** button. You can optionally check the **Make global** box to save the query for other users to access (*only Admins can create global queries*).

The **Import** button allows you to import a saved query from file.

In the list of queries, in the Name column if you click the icon it will load the query into your dashboard. Be aware that this will overwrite the existing queries already defined in your dashboard.

The **Actions** column provides the following:

 Export

Export the current query to a file

 Overwrite

Overwrite this saved query with the contents of your current dashboard

 Delete

Delete the saved query

Use with caution as you won't be able to recover a deleted query

## Finishing Up

This completes the documentation on how to analyze logs in 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>