

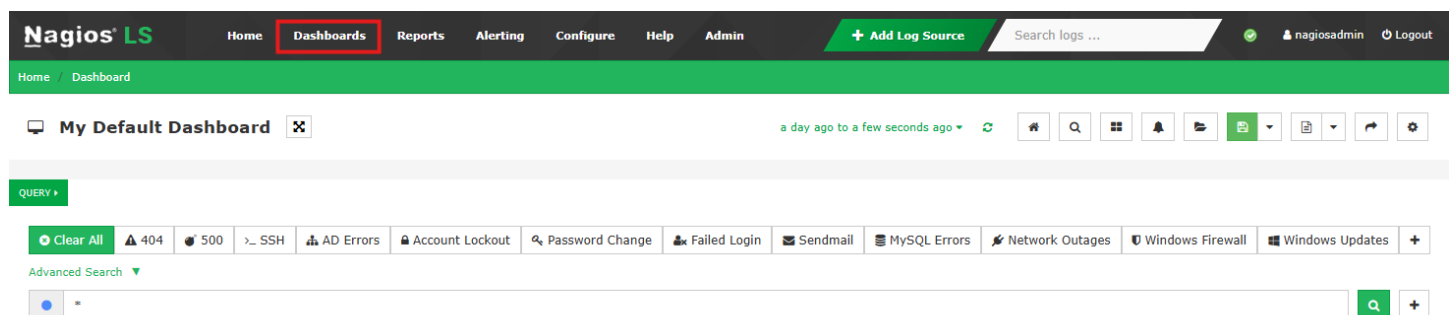
How To Analyze Logs In Nagios Log Server 2024

Purpose

This document describes how to analyze logs using Nagios Log Server.

Navigate

This documentation explains features that are found 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.

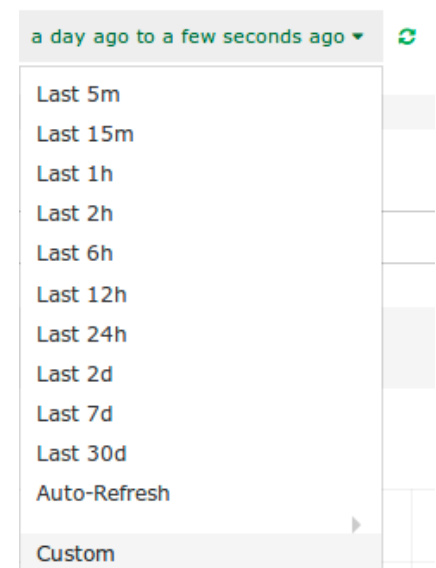
Note: If you navigate away from the **Dashboards** page without clicking the save button, any changes you made will be lost. To keep your customizations, save your dashboards, this process is explained in the [Dashboard Controls](#) section of this document.

Time Period

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

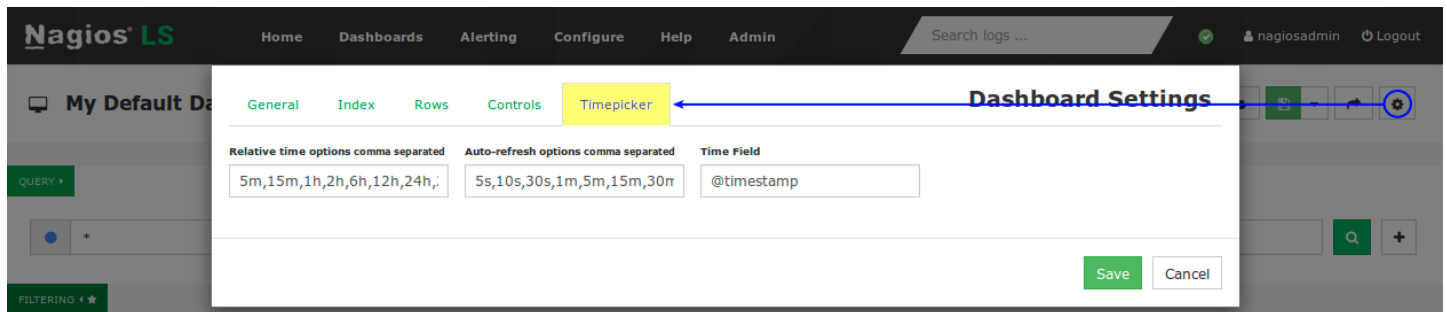
By default, this is set to the past day (**a day ago to a few seconds ago**). Clicking the refresh icon next to the list updates the data on the screen while retaining any custom settings.

The drop-down list includes predefined time ranges, with a **Custom** option available if none of the preset ranges meet your needs.



How To Analyze Logs In Nagios Log Server 2024

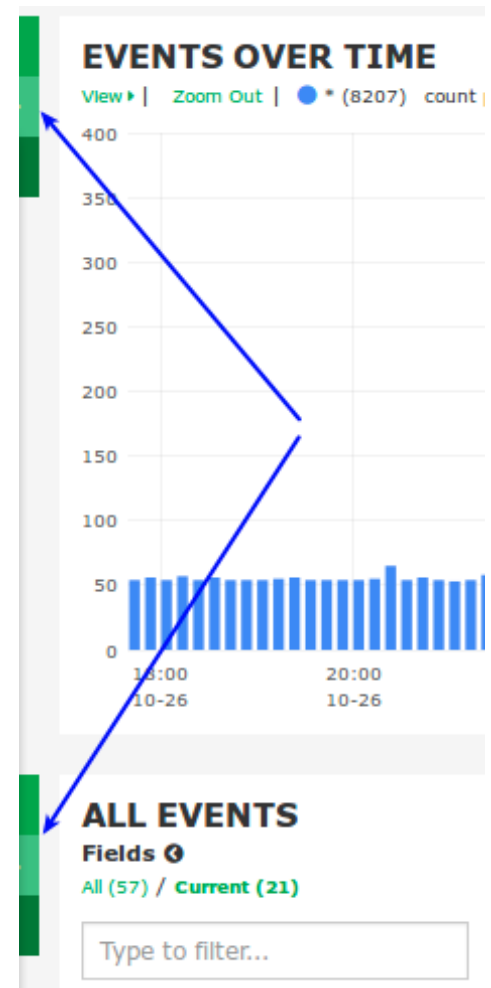
You can modify this list of time frames by clicking the **Configure Dashboard** button on the far right. In the **Timepicker** tab, you can define these time frames and arrange them in the order you prefer.



Row And Panel Overview

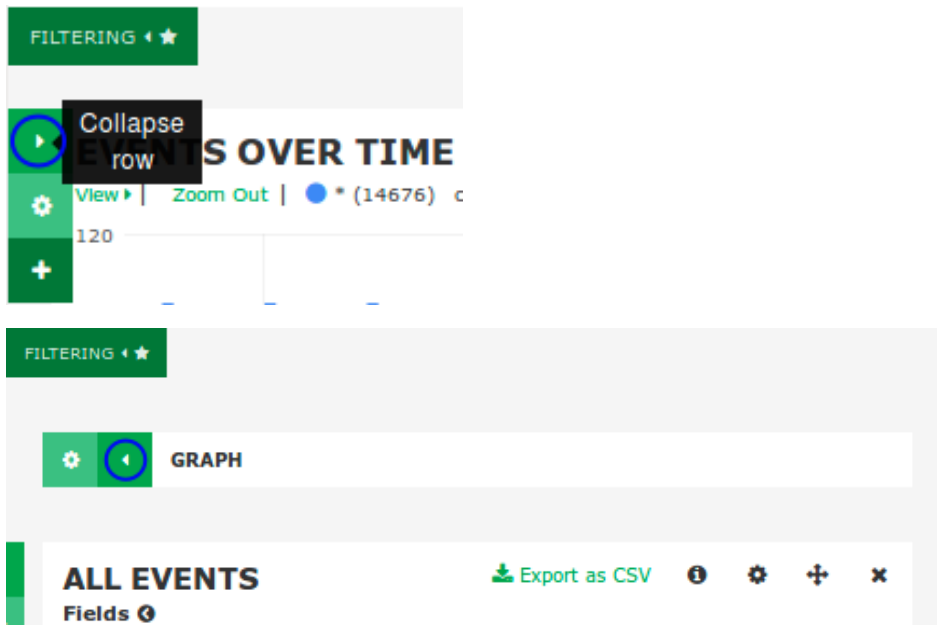
Rows and panels are the building blocks for creating dashboards comprised of graphs and tables. When you load the default dashboard, underneath **QUERY** and **FILTERING** is the following:

- **EVENTS OVER TIME** and **ALL EVENTS**
- Both are called **Panels**, and they are contained within a **Row**
 - The screenshot 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



How To Analyze Logs In Nagios Log Server 2024

A row can be collapsed to temporarily hide it from view. Click the **arrow icon** in the top box to collapse or expand the row.

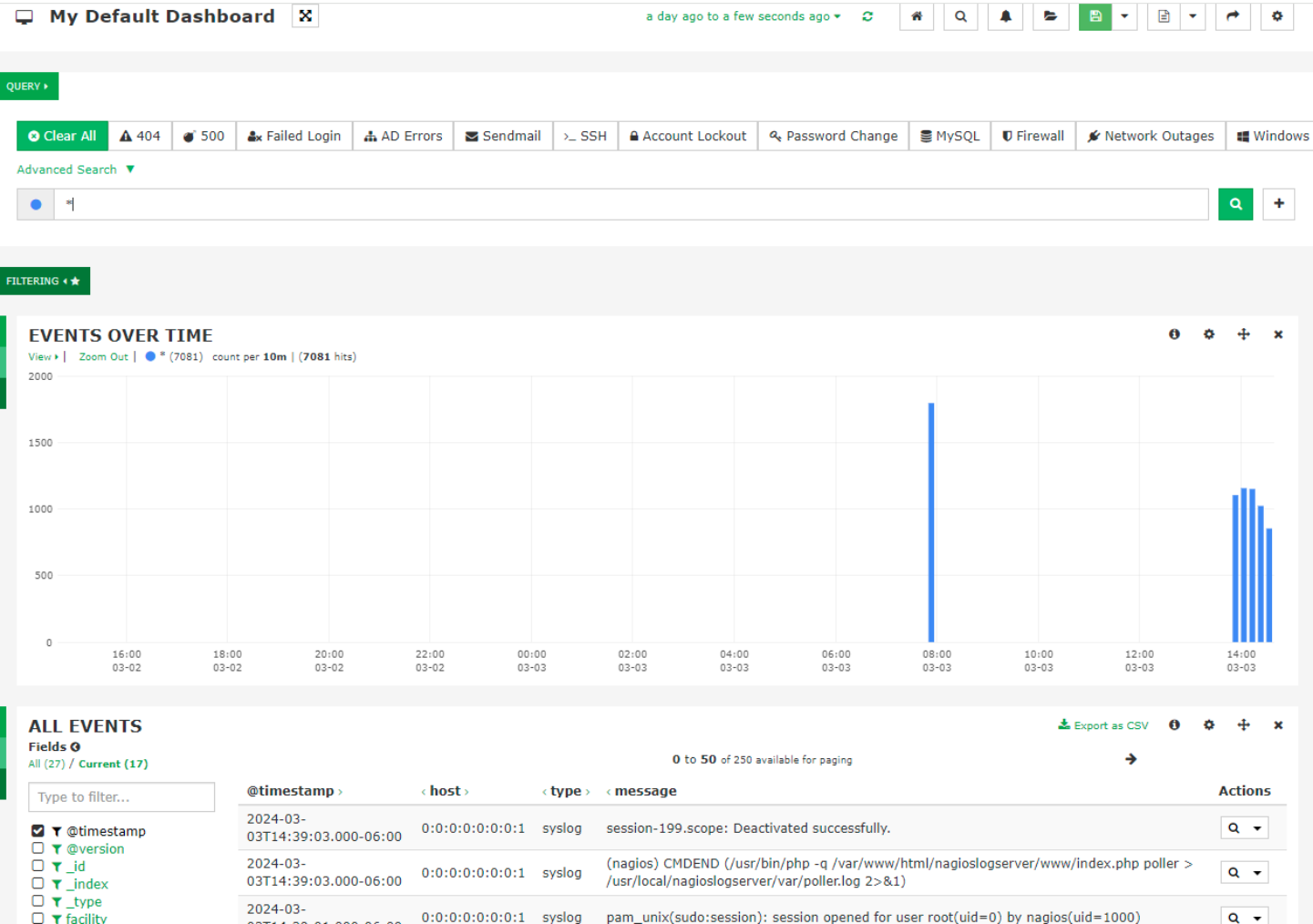


Customization of rows and panels is covered in more detail in the [Row And Panel Customization](#) section of this document.

How To Analyze Logs In Nagios Log Server 2024

Queries

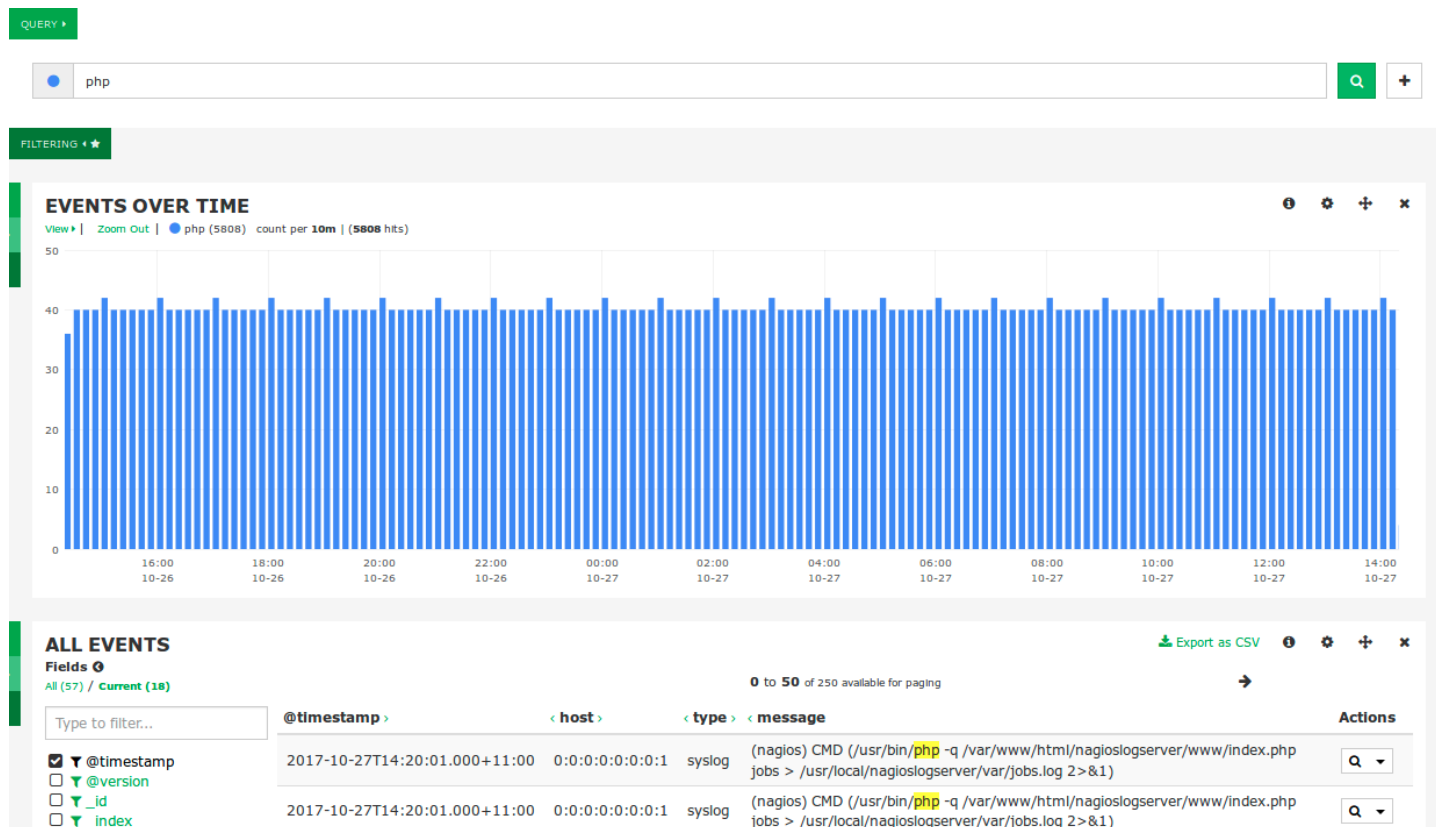
When you start collecting log data over a long period of time you will want to look at certain log types and categories. Nagios Log Server queries allow you to perform a search to show you the data you are looking for. Here is a view of the default dashboard in Nagios Log Server:



The **EVENTS OVER TIME** graph displays all log data received by the server. The default query is an asterisk (*), which retrieves all log data from the database (showing the last day by default). This view provides a high-level overview of log data traffic and trends over the past day.

How To Analyze Logs In Nagios Log Server 2024

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.



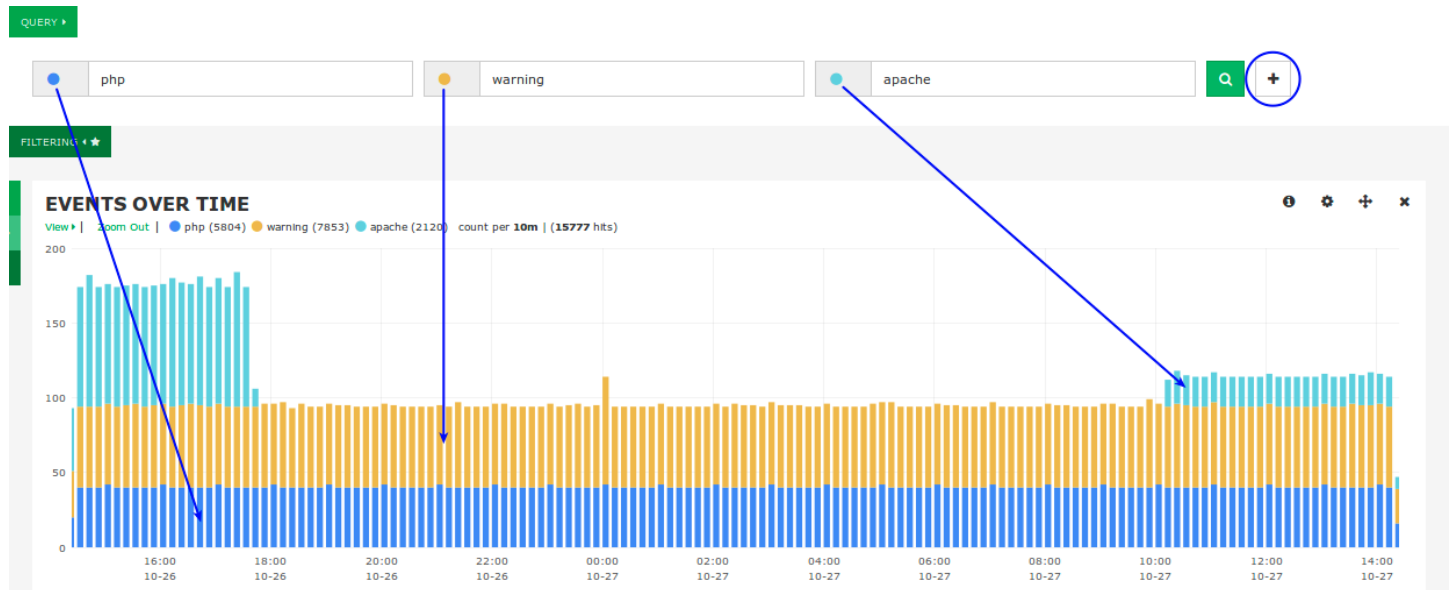
Queries are not case-sensitive, so in this example php is the same as PHP. When you query, Nagios Log Server will check every field in the Elasticsearch database for the string you are searching for.

Note: Boolean operators (AND, OR, etc...) in the query are case sensitive. They must be in uppercase.

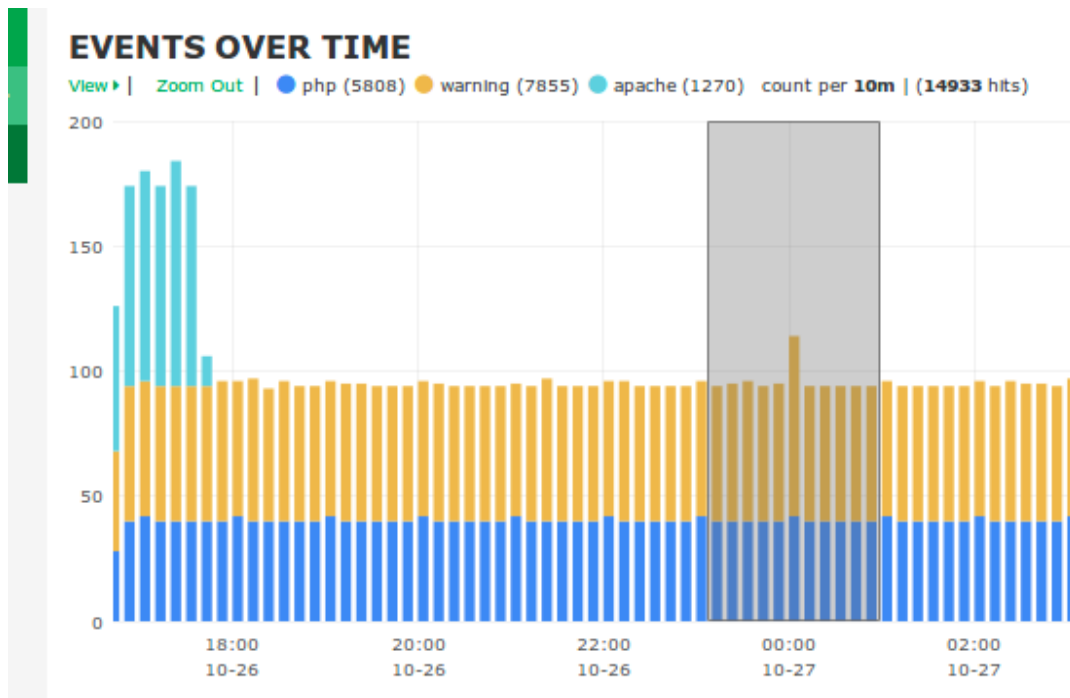
You are not restricted to just one query; you can define multiple queries by clicking the + sign to the right of the query field. By using multiple queries, Nagios Log Server sets each query as a different color, this helps identify the different queries in the **EVENTS OVER TIME** graph and in other panels.

How To Analyze Logs In Nagios Log Server 2024

This screenshot displays three queries: php, warning, and apache. The graph uses different colors to distinguish the results of each query.

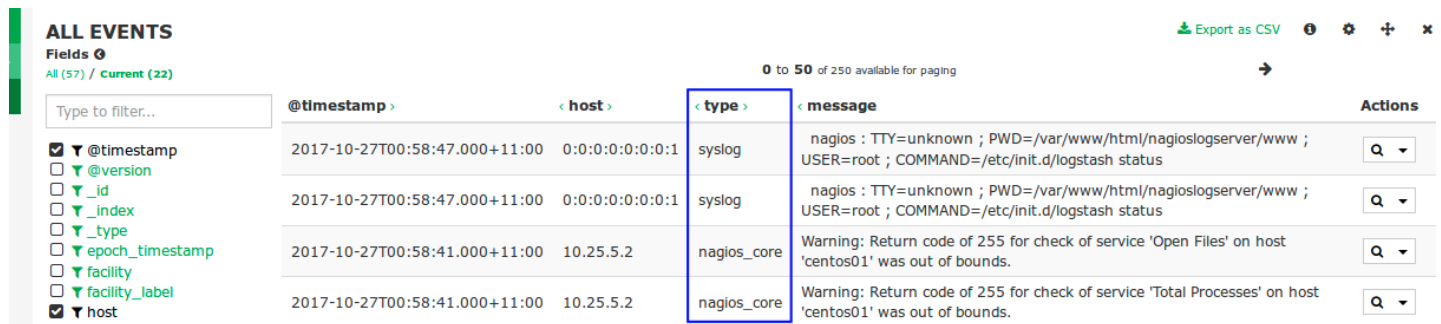


With the **EVENTS OVER TIME** graph, you can also drag your mouse over a time period to zoom in for a closer look at those log events.



How To Analyze Logs In Nagios Log Server 2024

In the query examples above, you have seen to 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 in specific fields. For example, the following screenshot shows the **ALL EVENTS** table where the **type** field has been highlighted.



The screenshot shows the Nagios Log Server interface. On the left, there's a sidebar with 'ALL EVENTS' and a list of fields to filter by. The main area displays a table of events. The 'type' column is highlighted with a blue box. The table has columns: @timestamp, host, type, message, and Actions.

@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

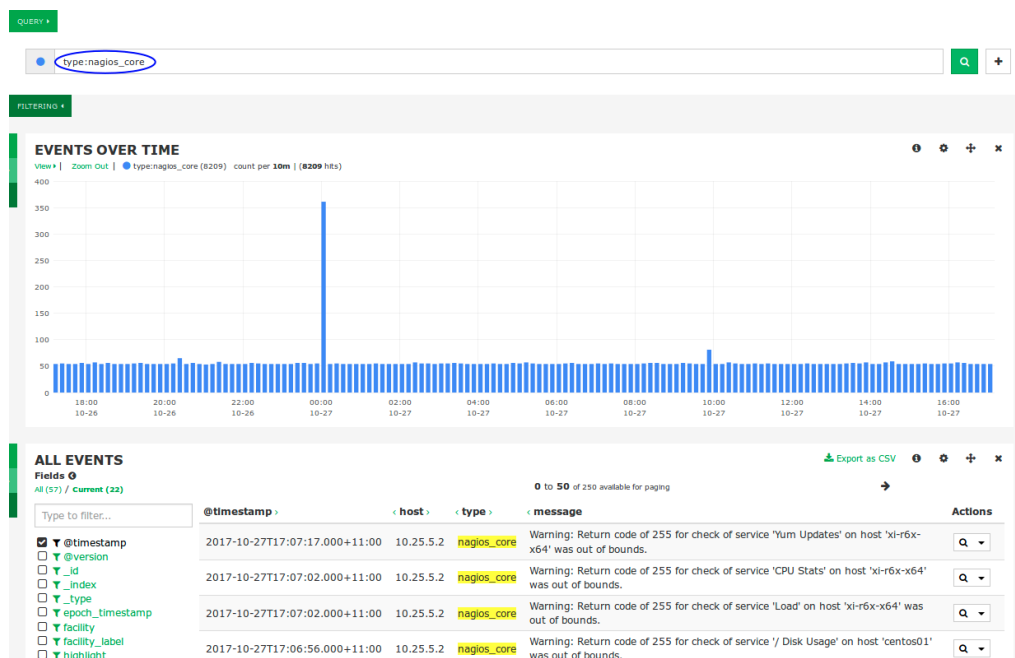
To perform a query for a value in a specific field use the following syntax:

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

For example:

```
type:nagios_core
```

Here is a screenshot showing that query:

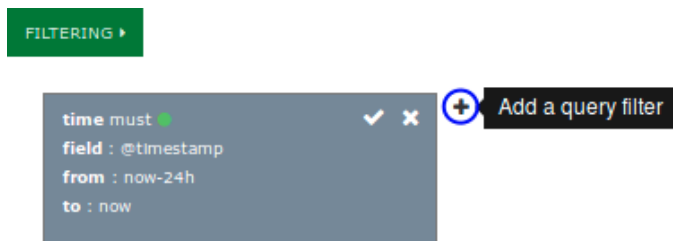


How To Analyze Logs In Nagios Log Server 2024

Filters

A filter is similar to a query; however, its 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 **FILTERING** section is collapsed by default. Click the **FILTERING** button to expand it and show the available filtering options. New filters can be added by clicking the **+** icon.

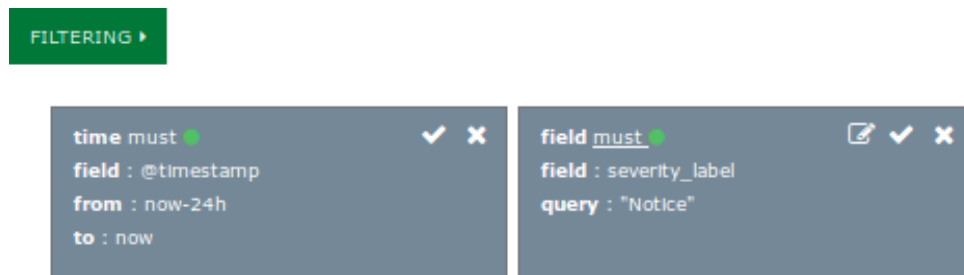


However, adding a filter can be much simpler by using the data in the **ALL EVENTS** table. To view the data about a specific event, click on a log entry in the **ALL EVENTS** table. The left column shows all available fields for this specific log entry. Clicking the spyglass icon (**Add filter to match this value**) for the **severity_label** field will create a **MUST** filter for the value **Notice**.

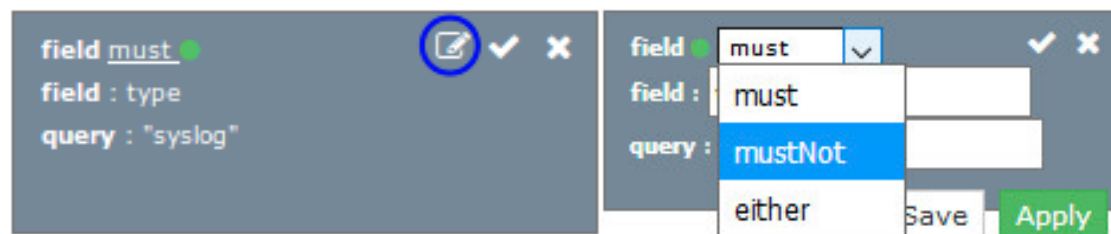
@timestamp >	< host >	< type >	< message >	Actions
2017-10-27T17:14:16.000+11:00	0:0:0:0:0:0:1	syslog	nagios : TTY=unknown ; PWD=/var/www/html /nagioslogserver/www ; USER=root ; COMMAND=/etc/init.d/logstash status	<input type="text" value="Q"/>
View: Table / JSON / Raw				
Field	Action	Value	Search	
<input checked="" type="checkbox"/> @timestamp	<input type="text" value="Q"/> <input type="text" value="X"/>	2017-10-27T06:14:16.000Z	<input type="text" value="Q"/>	
<input type="checkbox"/> @version	<input type="text" value="Q"/> <input type="text" value="X"/>	1	<input type="text" value="Q"/>	
<input type="checkbox"/> _id	<input type="text" value="Q"/> <input type="text" value="X"/>	AV9cd4SUpIMWNT2xD65g	<input type="text" value="Q"/>	
<input type="checkbox"/> _index	<input type="text" value="Q"/> <input type="text" value="X"/>	logstash-2017.10.27	<input type="text" value="Q"/>	
<input type="checkbox"/> _type	<input type="text" value="Q"/> <input type="text" value="X"/>	syslog	<input type="text" value="Q"/>	
<input type="checkbox"/> facility	<input type="text" value="Q"/> <input type="text" value="X"/>	10	<input type="text" value="Q"/>	
<input type="checkbox"/> facility_label	<input type="text" value="Q"/> <input type="text" value="X"/>	security/authorization	<input type="text" value="Q"/>	
<input checked="" type="checkbox"/> host	<input type="text" value="Q"/> <input type="text" value="X"/>	0:0:0:0:0:0:1	<input type="text" value="Q"/>	
<input type="checkbox"/> logsource	<input type="text" value="Q"/> <input type="text" value="X"/>	nls-c6x-x86	<input type="text" value="Q"/>	
<input checked="" type="checkbox"/> message	<input type="text" value="Q"/> <input type="text" value="X"/>	nagios : TTY=unknown ; PWD=/var/www/html/nagioslogserver/www ; USER=root ; COMMAND=/etc/init.d/logstash status	<input type="text" value="Q"/>	
<input type="checkbox"/> priority	<input type="text" value="Q"/> <input type="text" value="X"/>	85	<input type="text" value="Q"/>	
<input type="checkbox"/> program	<input type="text" value="Q"/> <input type="text" value="X"/>	sudo	<input type="text" value="Q"/>	
<input type="checkbox"/> severity	<input type="text" value="Q"/> <input type="text" value="X"/>	5	<input type="text" value="Q"/>	
<input type="checkbox"/> severity_label	<input checked="" type="text" value="Q"/> <input type="text" value="X"/>	Notice	<input type="text" value="Q"/>	
<input type="checkbox"/> timestamp	<input type="text" value="Q"/> <input type="text" value="X"/>	Oct 27 17:14:16	<input type="text" value="Q"/>	
<input checked="" type="checkbox"/> type	<input type="text" value="Q"/> <input type="text" value="X"/>	syslog	<input type="text" value="Q"/>	

How To Analyze Logs In Nagios Log Server 2024

Here you can see the newly added filter.



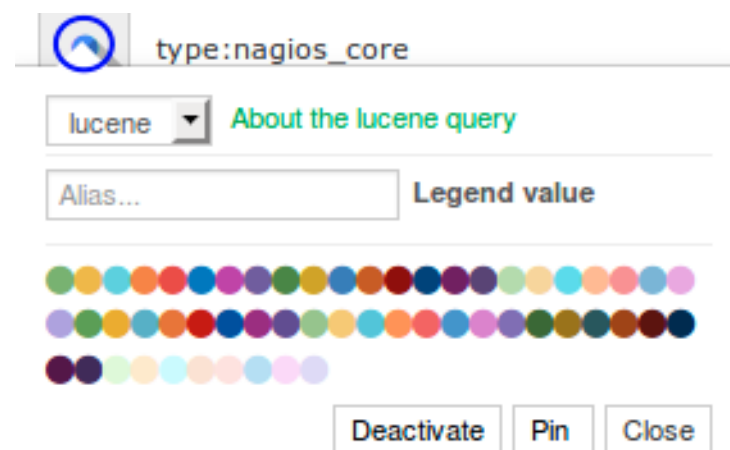
Here is another example. A filter was created by clicking the spyglass icon where the **type** is **syslog**. Click the **Edit** icon and the filter will change to edit mode. Use the **field** drop down list, select **mustNot** and then click **Apply**. The screen will refresh and the **EVENTS OVER TIME** and **ALL EVENTS** panels will apply the updated filters.



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.



How To Analyze Logs In Nagios Log Server 2024

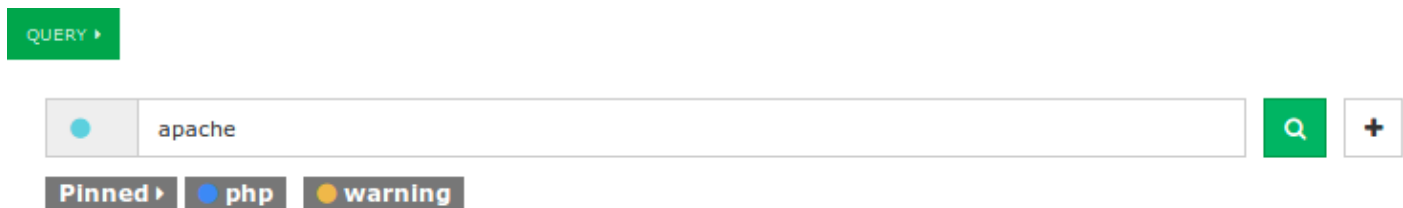
The first option is the query type. There are three types of queries available: **lucene**, **regex** and **topN**. Each query type has a link next to it that provides a modal with more information (**About the xxx query**). This will not be discussed here, as this is an advanced topic, but the help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

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

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

Clicking the **Deactivate** button removes the query from the results in the other rows and panels. Deactivating a query allows you to temporarily stop using it without having to delete and re-add it.

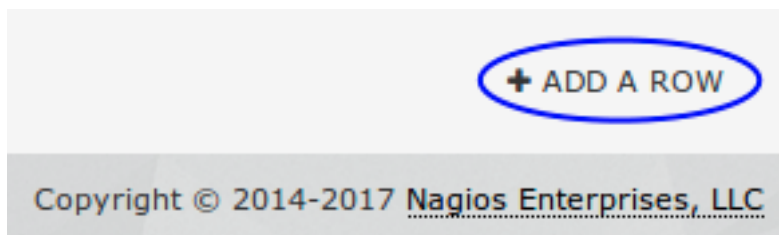
The **Pin** button allows a query to collapse, which is useful when managing multiple queries. Pinned queries appear next to the **Pinned** button. Clicking the **Pinned** button hides the list of pinned queries, helping to conserve screen space.



Row And Panel Customization

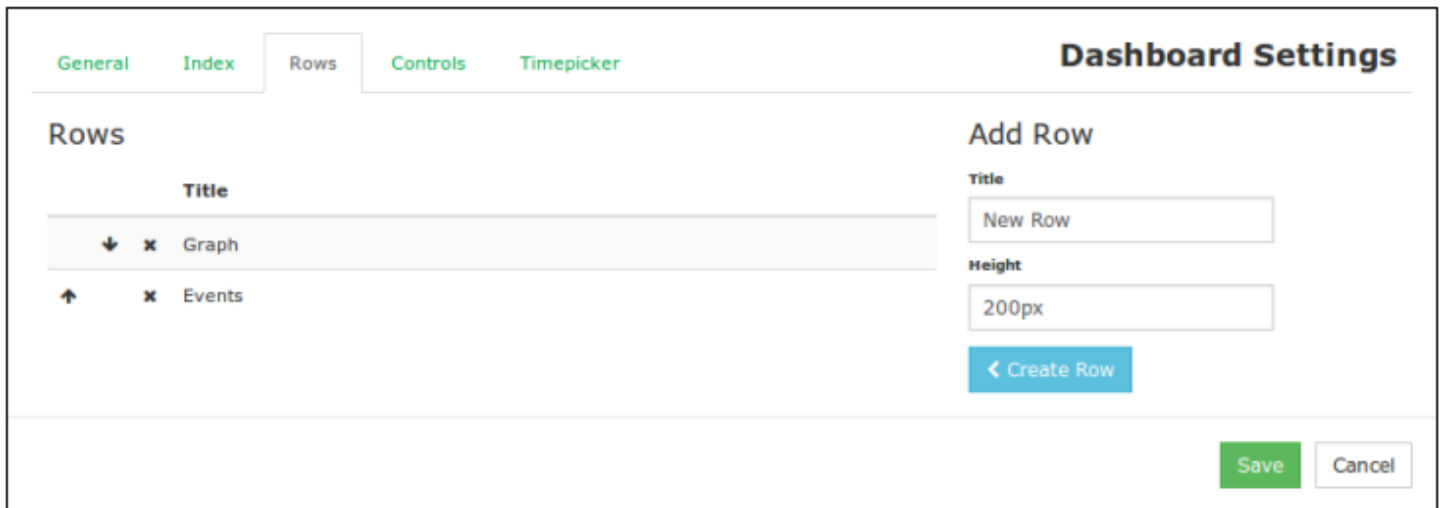
As explained earlier, rows and panels are the building blocks for creating dashboards comprised of graphs and tables. Now that the basic concepts of queries have been explained you will see how these queries can be used to visualize your log data.

To create a new row, click the **+ADD A ROW** link at the bottom right of the **Dashboards** page.



How To Analyze Logs In Nagios Log Server 2024

This will open the **Dashboard Settings** with the **Rows** tab selected. On the right, provide a **Title** for the row, define the **Height**, and click the **Create Row** button.

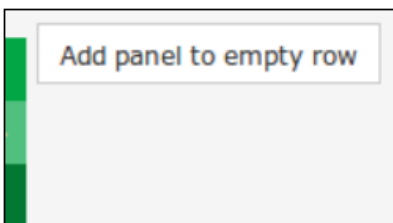


The screenshot shows the 'Dashboard Settings' window with the 'Rows' tab selected. On the left, under the 'Rows' heading, there is a list of existing rows: 'Graph' and 'Events'. Each row has a down arrow icon to its left and an 'x' icon to its right. On the right side, the 'Add Row' section contains a 'Title' input field with the text 'New Row', a 'Height' input field with the text '200px', and a blue 'Create Row' button. At the bottom right of the window are green 'Save' and 'Cancel' buttons.

A newly created row is placed at the bottom of the **Rows** list. Use the **arrow** icons to change the order in which the rows are displayed on the dashboard. Click the **Save** button to apply these changes to the dashboards page.

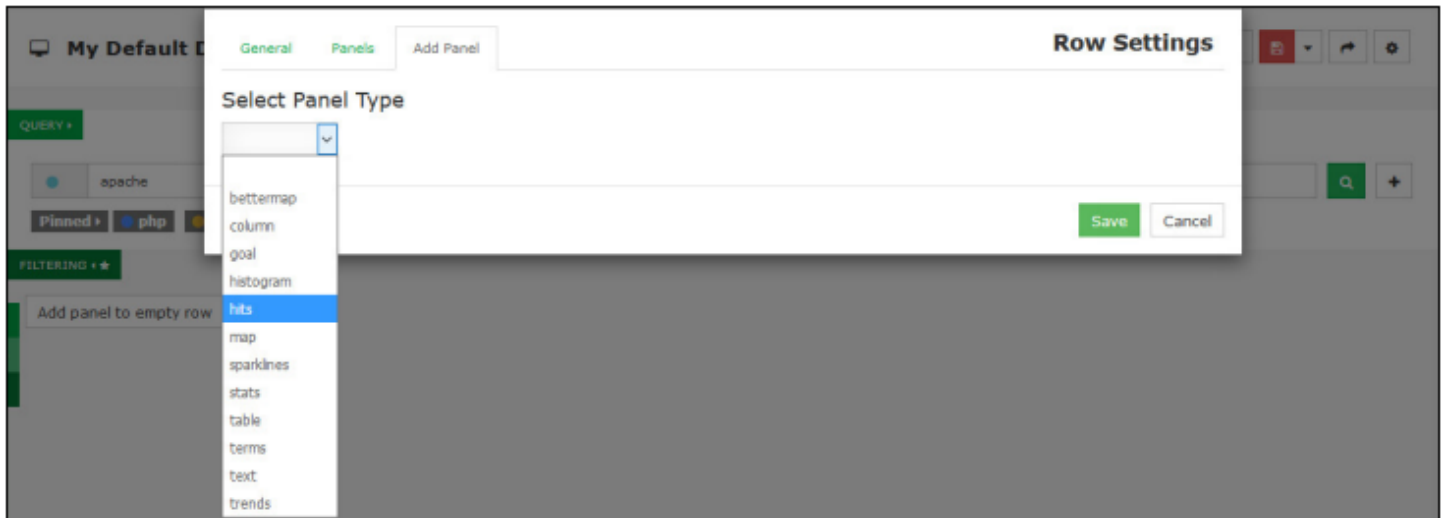
Rows			Rows		
Title			Title		
↓	x	Graph	↓	x	New Row
↑	↓	Events	↑	↓	Graph
⬆	x	New Row	↑	x	Events

When the dashboard is refreshed, the new row will be added but will be empty. To add content, click the **Add panel to empty row** button.



How To Analyze Logs In Nagios Log Server 2024

This will open the **Row Settings** with the **Add Panel** tab selected. Select a panel type from the drop-down list. This example is going to use the **hits** panel type.

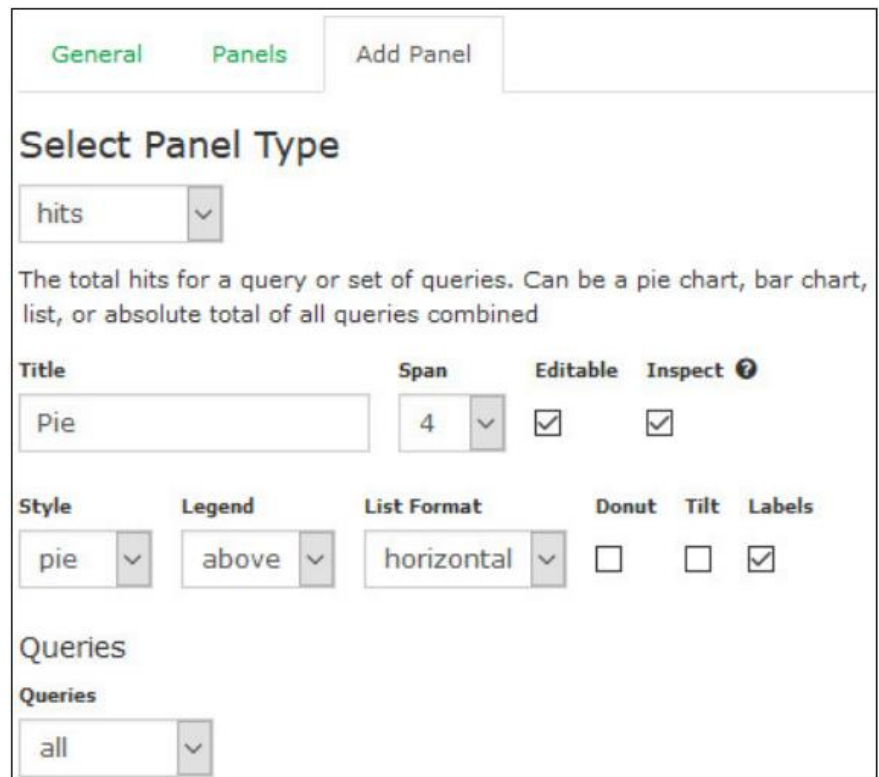


You will be presented with all the options available for the panel type selected.

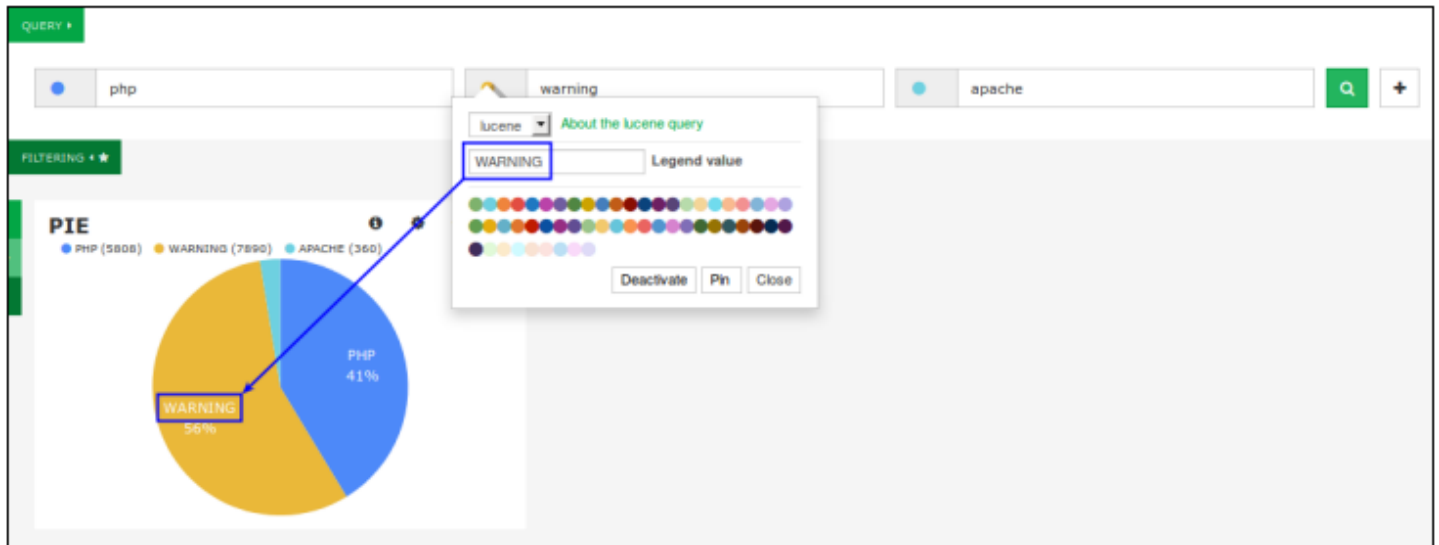
In this example:

- 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.

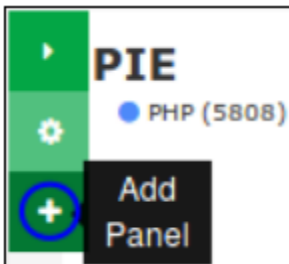
A screenshot of the 'Select Panel Type' dialog box for the 'hits' panel type. The 'hits' option is selected in the dropdown. Below the dropdown, a description reads: 'The total hits for a query or set of queries. Can be a pie chart, bar chart, list, or absolute total of all queries combined'. The 'Title' field is 'Pie', 'Span' is '4', 'Editable' and 'Inspect' are checked. The 'Style' is 'pie', 'Legend' is 'above', 'List Format' is 'horizontal', 'Donut', 'Tilt', and 'Labels' are unchecked. The 'Queries' dropdown is set to 'all'.

How To Analyze Logs In Nagios Log Server 2024



In the screenshot above, the **Legend value** assigned to the query is displayed on the pie chart, making it easy to customize the visualization. This can also be turned off. In the **Panel Settings** on the previous page, there is a **Labels** checkbox that allows you to enable or disable this feature.

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 **+ Add Panel** option.



How To Analyze Logs In Nagios Log Server 2024

In this example, the **terms** panel type is selected. It is used to provide information about the fields in the log data. The **Field host** has been defined.

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

GeneralPanelsAdd Panel

Select Panel Type

terms

Displays the results of an elasticsearch facet as a pie chart, bar chart, or a table

Title

Addresses

Span

4

Editable

☒

Inspect

☒

Parameters

Terms mode

terms

Field

host

Length

10

Order

count

Exclude Terms(s) (comma separated)

host

host.raw

View Options

Style

table

Font Size

10pt

Missing

☐

Other

☐

Queries

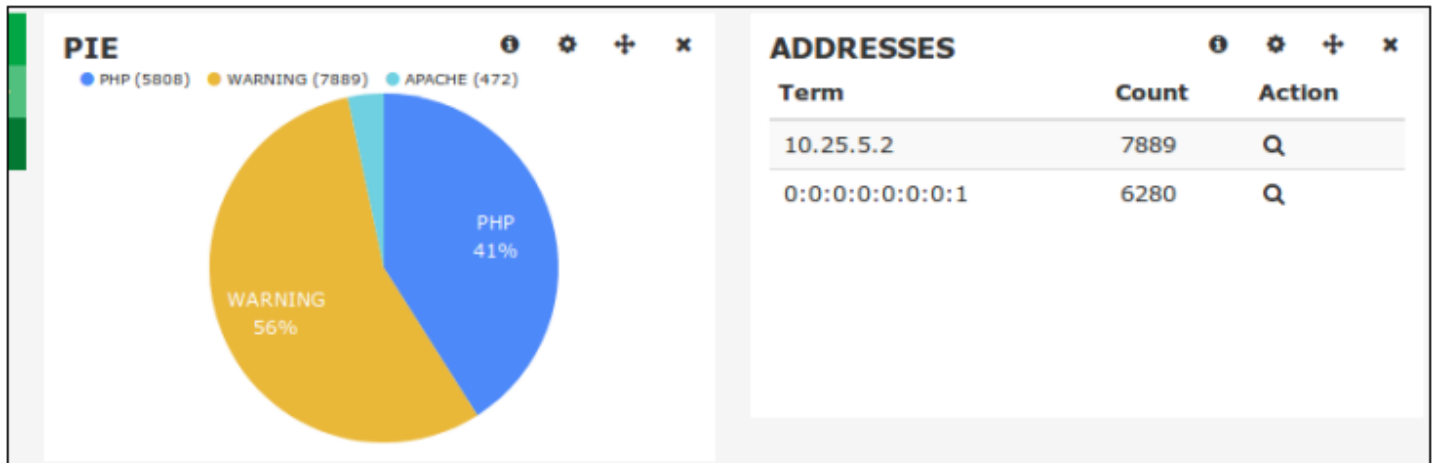
Queries

all

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

How To Analyze Logs In Nagios Log Server 2024

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, **hits** panel type has been selected again. This time the **Style** of **bar** is selected.

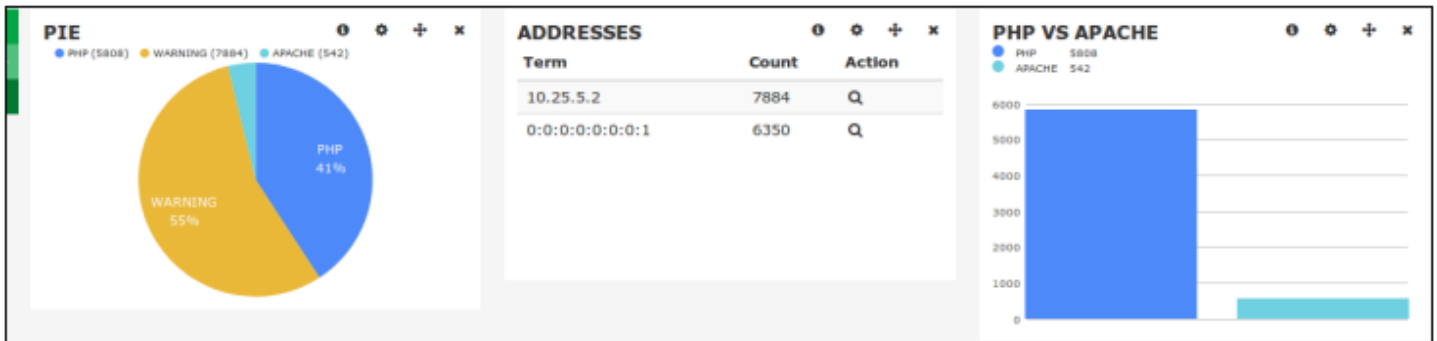
Under **Queries**, **selected** is the chosen option. To the right is the list of queries where **PHP** and **APACHE** are selected. The border surrounding the queries indicate which ones have been chosen.

You can see how the **Legend value** defined in the query makes it easy to identify the different queries (**PHP**, **WARNING**, and **APACHE**).

The screenshot shows the configuration interface for the 'hits' panel. The 'General' tab is active, and the 'Add Panel' button is visible. The 'Select Panel Type' dropdown is set to 'hits'. The description states: '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'. The 'Title' is 'PHP vs APACHE', 'Span' is 4, 'Editable' is checked, and 'Inspect' is checked. The 'Style' is 'bar', 'Legend' is 'above', and 'List Format' is 'vertical'. Under 'Queries', the 'selected' option is chosen. The 'Selected Queries' section shows three buttons: 'PHP' (highlighted with a blue border), 'WARNING' (highlighted with a yellow border), and 'APACHE' (highlighted with a cyan border).

How To Analyze Logs In Nagios Log Server 2024

Once you save the panel, it will be added to the row when the dashboard refreshes.



There are many different panel types available allowing you to build a dashboard that visualizes your log data.

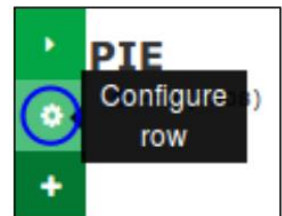
Panel Controls

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

- i** 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 open the **Row Settings**.



How To Analyze Logs In Nagios Log Server 2024

Dashboard Controls

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

 Toggle Fullscreen/  Exit Fullscreen


- The full screen mode removes the top menu bar and the bottom status bar.

 Home

- Loads the dashboard saved as the default. This can be changed by navigating to **Save (drop down arrow) > Advanced > Set as Default Dashboard**.

 Manage Queries

- Opens **Manage Queries** modal, which is explained in detail in the [Manage Queries](#) section.

 Create an alert

- Allows you to create an alert using the current query. Please refer to the [Alerting On Log Events](#) documentation.

 Load

- Allows you to load any dashboard that you previously saved.
- Clicking the icon presents a drop-down menu with all saved dashboards. Select a dashboard to load it.
- Global dashboards are indicated by the globe icon to the left of the dashboard title.
- To delete a dashboard from the load list, click the green X to the right of the dashboard title
 - Use with caution, as deleted dashboards cannot be recovered.
- The **Advanced** link at the bottom of the list allows you to import a dashboard from a file

How To Analyze Logs In Nagios Log Server 2024



Save

- Saves all customizations, including queries, filters, graphs, tables, colors, etc.
- The icon turns red color when there are unsaved changes to your dashboard.
- To save the current dashboard with a name:
 - Click the drop-down arrow.
 - Enter a name for the dashboard.
 - Click the appropriate save button:
 - ➡ **Save as dashboard** - only you can see this dashboard.
 - 🌐 ➡ **Save as global dashboard** - all users can access this dashboard.
 - **Note:** Only Admins can save global dashboards
 - The **Advanced** link underneath allows you to:
 - Set this dashboard as the default when navigating to the Dashboards page via the top menu bar
 - Export the dashboard to a file



Share

- Provides a URL that can be shared with other users to access your dashboard.
- The user will be required to have a Nagios Log Server account to view the URL.



Configure

- Displays the **Dashboard Settings** for the current dashboard.

How To Analyze Logs In Nagios Log Server 2024

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 considered part of a query, so any references here to a query also include filters.
- To save your current dashboard query, type a value in the top field and click the **Create** button. You can optionally check the **Make global** box to save the query for other users to access (**Note:** only Admins can create global queries).
- The **Import** button allows you to import a saved query from a file.
- In the list of queries, clicking the desktop icon in the **Name** column will load the query into your dashboard. Be aware that this will overwrite the existing queries 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 deleted queries cannot be recovered.

How To Analyze Logs In Nagios Log Server 2024

Finishing Up

This completes the documentation on analyzing logs with 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](#)