

How To Analyze Logs in Nagios Log Server 2024R2 With Dashboards, Queries, and Reports

Purpose

This document describes how to use queries and filters to drill down to the exact information you need and how to use rows and panels to customize your visualization using Nagios Log Server Dashboards.

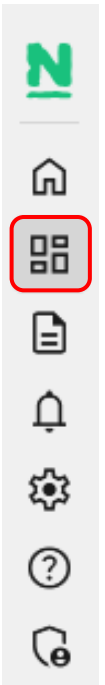
Target Audience

This document is intended for use by Nagios Log Server administrators and users who wish to better understand querying, filtering, and dashboard customization in Nagios Log Server.

Navigate

This documentation explains features that are found in the **Dashboards** menu, located in the left side navigation bar. Dashboards allow you to create custom views of your log data that are based on queries and filters.

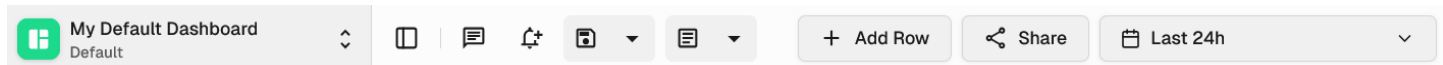
NOTE: When you navigate away from the dashboard's page, any changes you have made will be lost (if you did not click the save button). You can save dashboards, so your customizations are not lost, this is explained in the [Saving Dashboards and Reports](#) section of this document.





How To Analyze Logs in Nagios Log Server 2024R2 With Dashboards, Queries, and Reports


Dashboard Options


At the top of the dashboard are options that apply to the dashboard.




 My Default Dashboard Default - The dashboard dropdown. Click to manage dashboards

 - Full screen toggle. Click to show / hide the left menu

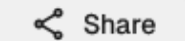
 - Manage queries

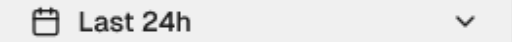
 - Add alerts

 - Save and save as

 - Save and save as report

 - Add a row.

 - Generate a link to the current dashboard

 - Time period dropdown

Many of these options will be referenced or discussed further in upcoming sections.

How To Analyze Logs in Nagios Log Server 2024R2 With Dashboards, Queries, and Reports

Dashboard Dropdown

On the far left of the dashboard options is the dashboard dropdown. Within the dropdown trigger is the dashboard's title, the dashboard's owner (or **Default** if the dashboard is the current user's default dashboard), and the default dashboard button.

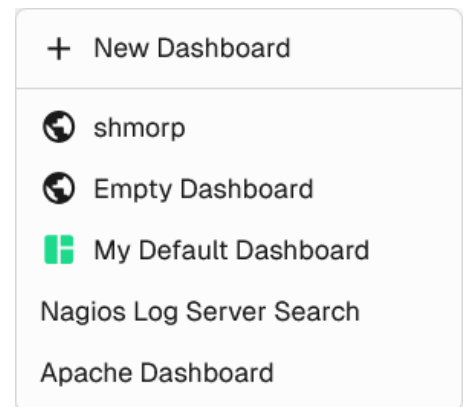
The default dashboard button allows users to change their default dashboard. If the current dashboard is default, the button is filled, otherwise it is empty and can be clicked to change the current dashboard to the user's default dashboard. A user's default dashboard is where they are directed to initially.



When the dashboard dropdown is clicked, a list of the user's dashboards pops up.

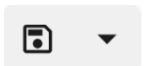
From here, users can add new dashboards, navigate to existing dashboards, and delete dashboards by hovering one of the options and clicking the **X**.

Global dashboards are indicated by the globe icon. These dashboards are accessible by all users.

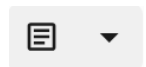


Saving Dashboards and Reports

To keep any changes to dashboards (e.g. a new row or changes to a panel), the dashboard must be saved.



Dashboards can be saved normally (top) or as a report (bottom). The caret to the right of either save icon allows users to save the dashboard as a new dashboard / report with a custom name and with the option to save it globally.



Dashboards saved as reports are added to the user's reports. These are accessible in the **Reports** menu and can be scheduled and downloaded.

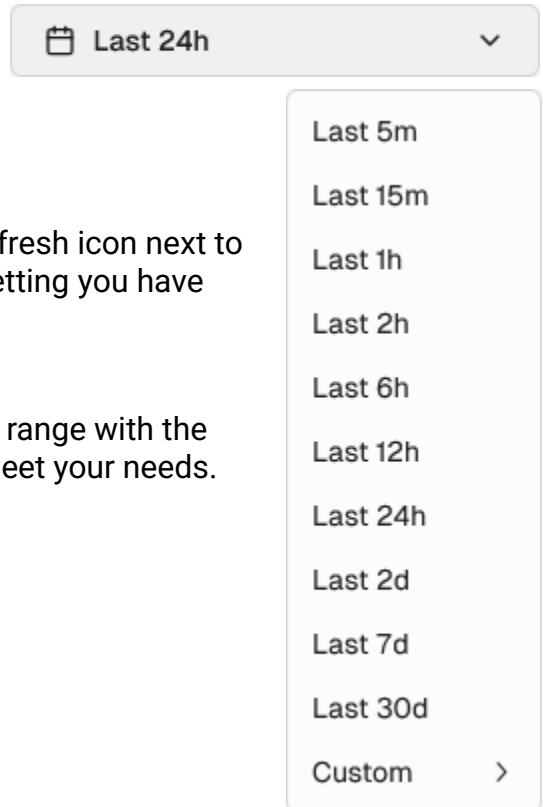
How To Analyze Logs in Nagios Log Server 2024R2 With Dashboards, Queries, and Reports

Time Period

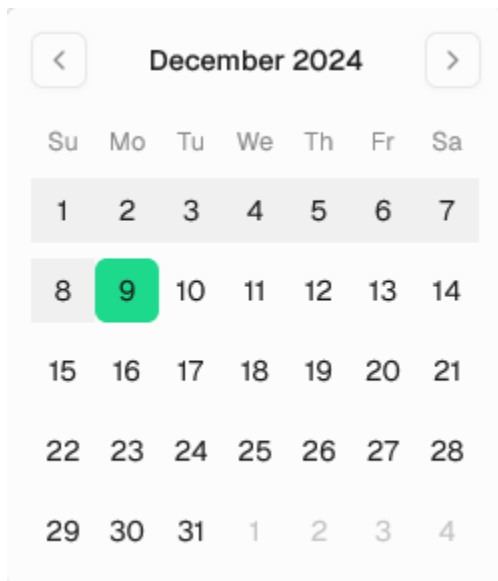
At the top of the screen is a drop-down list that lets you select the period for which you want the dashboard to apply to.

This is by default the past day (**Last 24h**). 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.



The image shows a dropdown menu for selecting a time period. The selected option is 'Last 24h'. The menu is open, showing the following options: Last 5m, Last 15m, Last 1h, Last 2h, Last 6h, Last 12h, Last 24h, Last 2d, Last 7d, Last 30d, and Custom. A refresh icon is visible next to the 'Last 24h' option.



The image shows a calendar for December 2024. The days of the week are listed at the top: Su, Mo, Tu, We, Th, Fr, Sa. The dates are arranged in a grid. The date 9 is highlighted in green, indicating the current date.

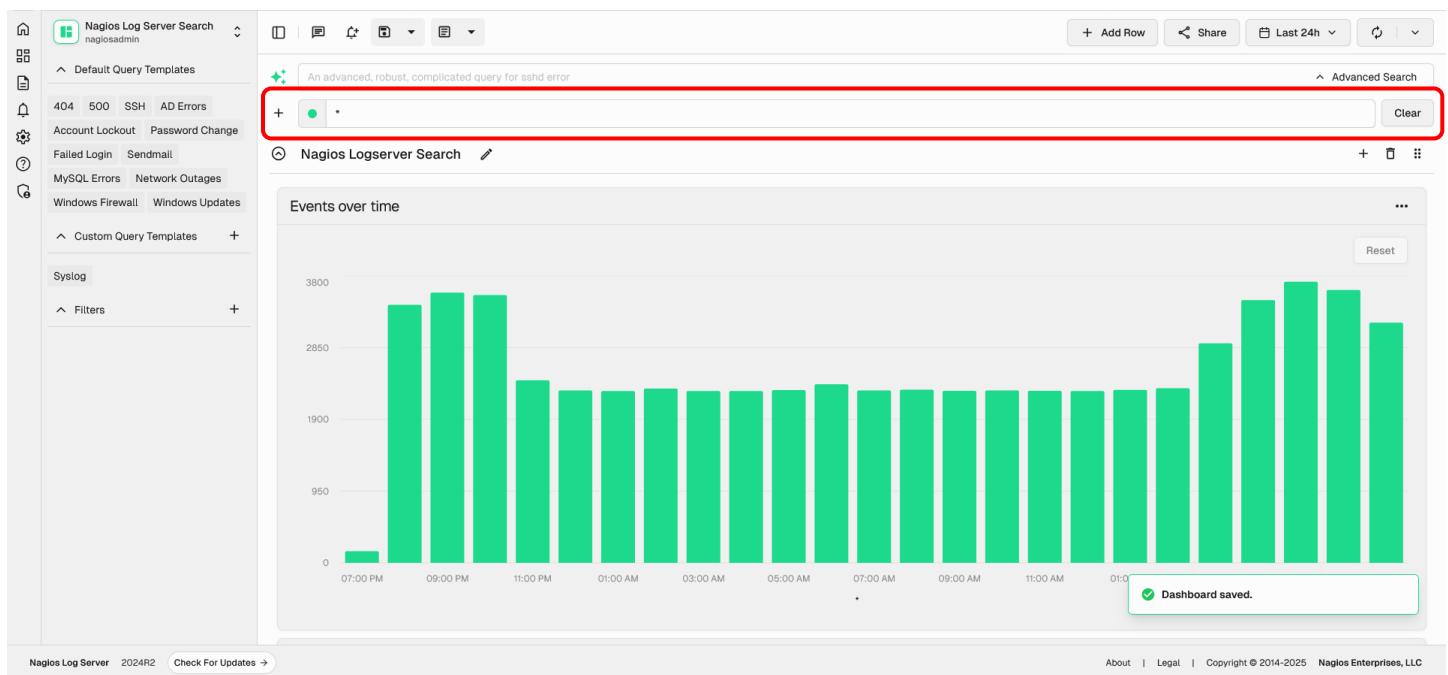
How To Analyze Logs in Nagios Log Server 2024R2 With Dashboards, Queries, and Reports

Dashboard Queries, Queries, and Filters

In Nagios Log Server, dashboards correspond to dashboard queries. Each dashboard has one dashboard query which consists of queries and filters. Managing and using dashboard queries, queries, and filters effectively will be discussed further in their own sections.

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. Queries are automatically applied to the data shown in the dashboard. The query toolbar is located at the top of the dashboard.



This graph view (**Events over time**) shows us all the log data the server receives. 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.

How To Analyze Logs in Nagios Log Server 2024R2 With Dashboards, Queries, and Reports

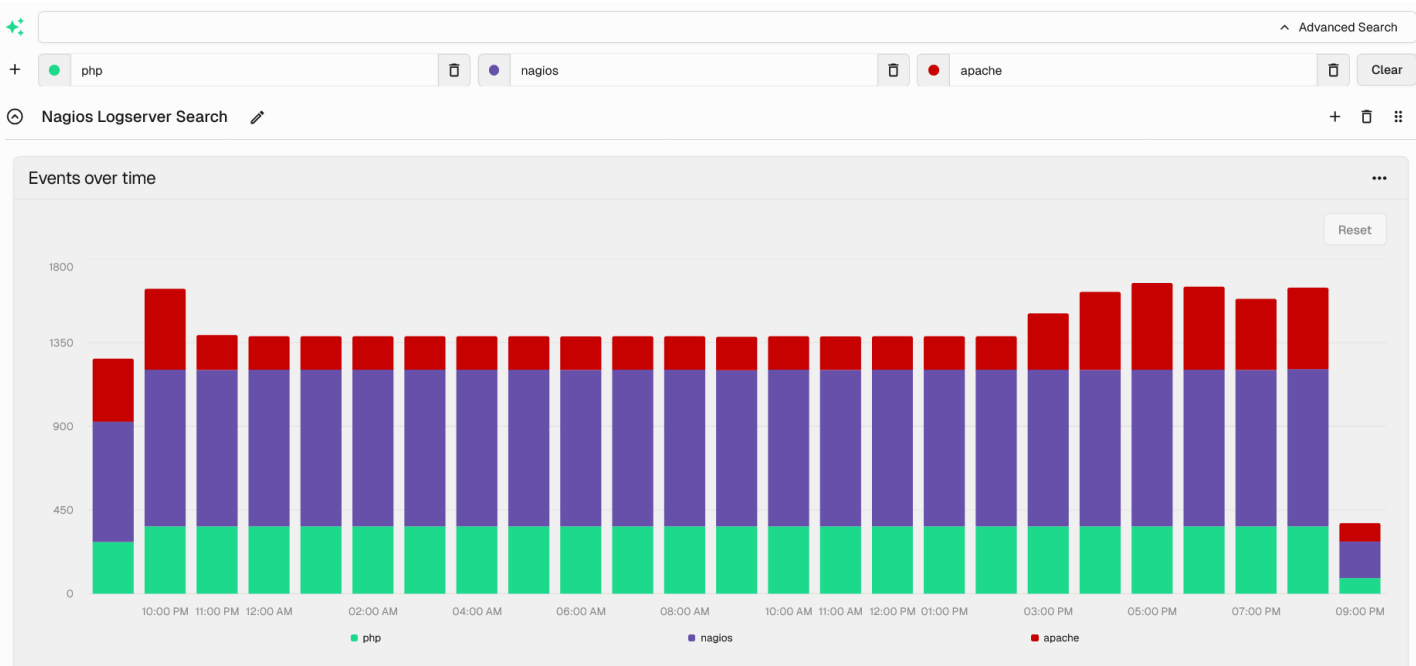
Performing a query is as simple as typing the word you want to search for.

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 Opensearch 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 left of the query field. The screenshot below shows three queries: **php**, **warning**, and **nagios**.

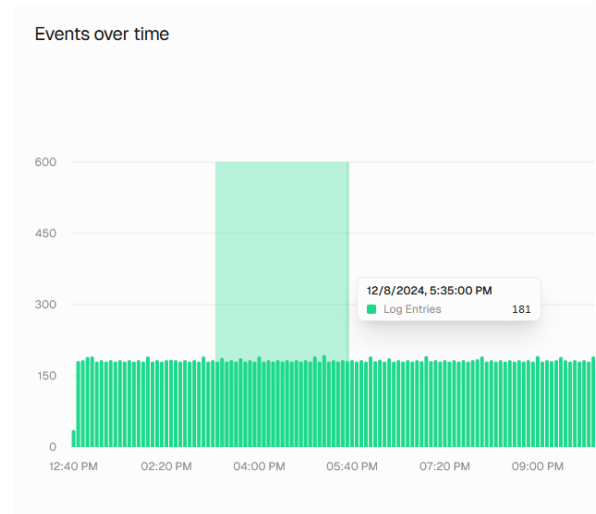
Queries have colors that can be customized by clicking on the colored dot in the query box.



How To Analyze Logs in Nagios Log Server 2024R2 With Dashboards, Queries, and Reports

With the **Events over time** graph, you can also drag your mouse across a period to zoom in for a closer look at those log events. This will set your period to the selected range.

Up until now, queries have been searching all the fields in the Opensearch database for the period you are currently viewing. You can also perform the queries on specific fields. For example, the All Events panel shows data organized into the **Type**, **Message**, and **@timestamp** fields by default.



All Events ...

Filter messages... Export as CSV Columns ▾

Type ↑↓	Message ↑↓	@timestamp ↑↓
syslog	Started Session c18665 of User root.	2024-12-09T19:00:36.000Z
syslog	pam_unix(sudo:session): session closed for user root	2024-12-09T19:00:36.000Z
syslog	pam_unix(sudo:session): session closed for user root	2024-12-09T19:00:36.000Z
syslog	session-c18665.scope: Deactivated successfully.	2024-12-09T19:00:36.000Z

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

`<field_name>:<query>`

For example,

`message:nagios`

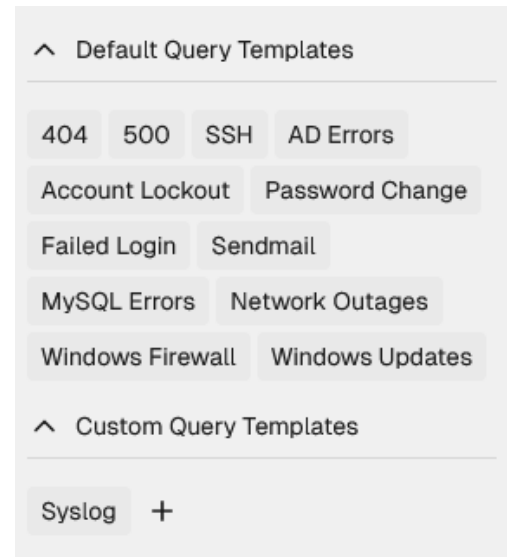


How To Analyze Logs in Nagios Log Server 2024R2 With Dashboards, Queries, and Reports

Query Templates

Query templates are used to save individual queries to Nagios Log Server, allowing queries to be toggled and instantly applied to any dashboard. Located in the left menu of the dashboard, query templates are categorized into collapsible **Default** and **Custom** query template sections.

Any user can create their own custom query templates to use across their dashboards or global query templates for anyone to use by clicking the **+** icon. Every custom query template must also have a display name and a query that is applied when the template is toggled.



Add Query Template

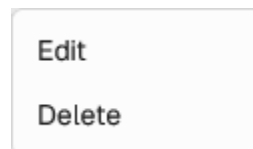
Use this to add a new query template!

Name

Query

Global

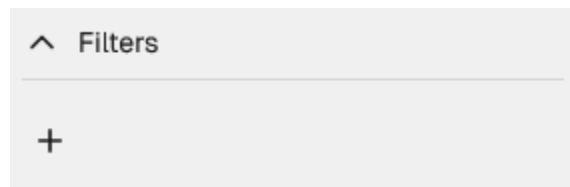
To **edit** or **delete** a custom query template, right click an existing query template toggle. This will bring up a context menu with the available options.



How To Analyze Logs in Nagios Log Server 2024R2 With Dashboards, Queries, and Reports

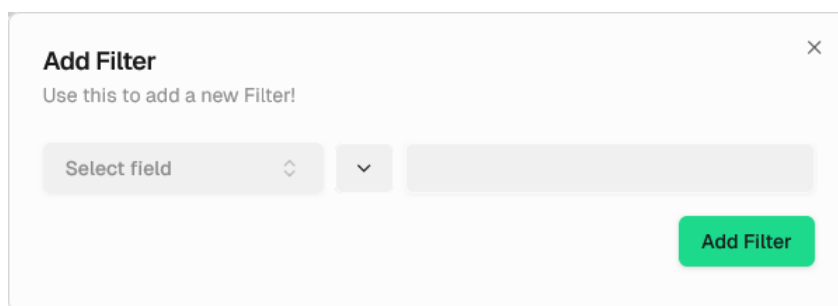
Filters

A filter is like a query, but its purpose is to reduce the amount of data a query is performed against. Filters are located just below query templates in the dashboard's left menu in their own collapsible section.

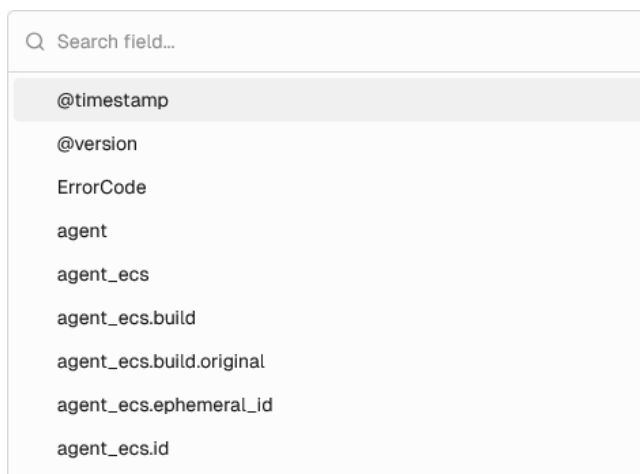



New filters can be added by clicking the + icon in the collapsible menu.

When adding filters, you must choose a field, a match, and a value. Filters operate by reducing the data to entries in which the chosen field matches the chosen value under the selected case.



Choose the field by clicking **Select field** and selecting one of the options from the searchable dropdown menu that contains the available fields in the current data.



Choose the match case by clicking . The options are **must**, **must not**, and **should**. Filters that must match the chosen value filter out data in which that is not the case. Filters that must not match the chosen value do the opposite. Filters that should match the chosen value prioritize these results if they exist.

The final required selection is a value. This can be any string of characters intended to match the field according to the chosen match case.

Once added, filters can be edited or deleted by selecting the vertical ellipse at the end of the filter.



How To Analyze Logs in Nagios Log Server 2024R2 With Dashboards, Queries, and Reports

Row And Panel Customization

Rows and panels are the building blocks for creating dashboards. A dashboard consists of rows and each row consists of panels. Panels are responsible for the actual data visualization. The **Events over time** graph used to demonstrate queries is an example of one of the available panels.

Rows

To add a row, click the Add Row button in the top right corner of the dashboard.

This will bring up a dialog with a single input field for the row name. Once submitted, the row is appended to the dashboard.

Rows have five options.

⌵ Test Row ✎

- ⌵ - Hide / show the row
- ✎ - Edit the row's title
- +
- 🗑 - Delete the row
- ⋮ - Move the row

To save any changes to rows, the dashboard must be saved.

+ Add Row

Add Row ×

Use this to add a new row to your dashboard

Name

+ 🗑 ⋮

How To Analyze Logs in Nagios Log Server 2024R2 With Dashboards, Queries, and Reports

Panels

Once a row is added to the dashboard, panels can be added to the row. The row acts as a fully reactive, customizable grid, allowing panels to be freely moved around within their row. The dimensions of the row change depending on the size and positions of the inner panels.

To add a panel, click the **+** in the row header. A menu will appear with the panel options:

- **Panel Type:** choose the type of visualization to add. The panel options will change for different types.
- **Title:** every type of panel requires a title. This will show in the top left corner of the panel in the dashboard.
- **Queries:** choose whether this panel displays data for all queries or for specifically selected queries.
- **Other:** the rest of the panel options depend on the panel type. For example, the screenshot to the right shows the histogram panel options.

Add Panel ×

Configure your new panel here.

Panel Type

Title

Queries

Chart Options Bar
 Lines
 Points
 Zoomable

Multi Series Stack
 Cumulative
 Percent

Once the panel options are selected, click **Save** to add the panel to the row.

Panels within rows can be adjusted at will. The row will adjust to the panels.

asd	⋮
	Count 60159
Minimum	1733779067000
Maximum	1733865451000
Mean	1733822761943.4675
Total	104305043535757060
Sum of Squares	1.8084645870984216e+29
Variance	698852434478340.9
Standard Deviation	26435817.265186656

To edit or delete added panels, click the **more** icon in the top right corner of the added panel. This will open a dropdown menu with the options to delete the panel or to open the panel's settings.

Clicking **Settings** will open the same menu that opens when panels are added without the **Panel Type** option. Clicking **Delete** will remove the panel from the row.

Certain panels will have buttons and options when within a row, but they depend on the panel type. For instance, the **Table** panel can be exported as a CSV and log entries can be selected and further investigated.

How To Analyze Logs in Nagios Log Server 2024R2 With Dashboards, Queries, and Reports

Manage Dashboard Queries

From the dashboard, users can manage dashboard queries.

- Dashboard queries contain both queries and 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 **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 a file.
- The **more** icon at the end of each dashboard query table row has additional options, including:
 - **Run**: load the chosen query into the current dashboard. This will populate the dashboard with the dashboard query's filters and queries.
 - **Export**: export the dashboard query to a file.
 - **Overwrite**: Overwrite the chosen dashboard query with the current dashboard query.
 - **Delete**: delete the chosen dashboard query. Deleted dashboard queries cannot be recovered.

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

Create Alerts

Alerts can be created from the dashboard as well. Clicking the **Add Alert** button from the dashboard options will open a dialog with several options.

- **Alert Name**
- **Check Interval**: the frequency at which to run the alert.
- **Lookback period**: how far back to look at log data when the alert runs.
- **Thresholds**: the warning and critical thresholds to compare the alert against.
- **Notification Method**: how to notify when the alert runs.

When created, the alert will be added to the user's list of alerts which can be managed on the **Alerting** page.

Check Interval	Lookback Period

Thresholds
Warning Critical

How To Analyze Logs in Nagios Log Server 2024R2 With Dashboards, Queries, and Reports

Finishing Up

This completes the documentation on How To Analyze Logs in Nagios Log Server 2024R2. 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](#)