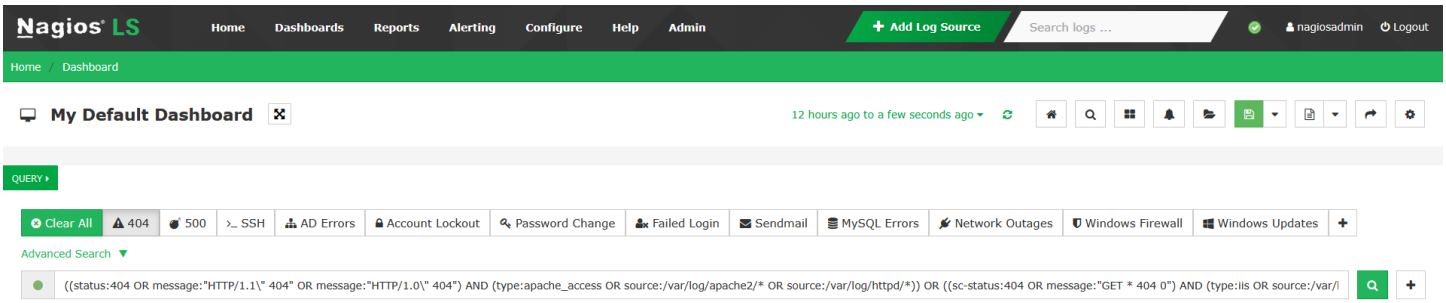
Managing Queries in Nagios Log Server 2024

Purpose

The purpose of this document is intended to provide a description of the default queries in Nagios Log Server as well as how to create and manage queries.

Default Queries (Easy Buttons)

On the **Dashboards** page, there are several default queries available to use. Selecting one or more of these queries will fill out the default dashboard with the selected data. The **404** query is selected in the example below with the **Advanced Search** section expanded to display the query.



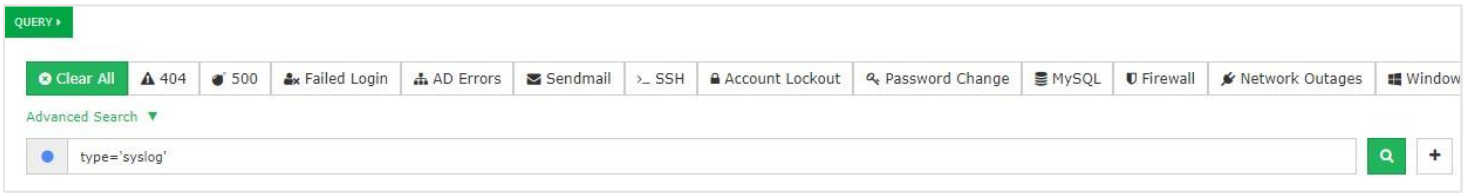
- **404** – Searches Apache and IIS logs for events with a HTTP 404 status.
- **500** – Searches Apache and IIS logs for events with HTTP statuses in the range of 500 to 505.
- **Failed Login** – Searches logs related to failed login attempts.
- **AD Errors** - Searches logs for errors with Active Directory such as replication and DNS issues.
- **Sendmail** – Searches logs associated with the sendmail service, including failed deliveries
- and authentication warnings.
- **SSH** - Searches logs for SSH connection attempts, errors, timeouts, and other related activities.
- **Account Lockout** – Searches logs for account lockouts due to multiple failed login attempts or other security reasons.
- **Password Change** – Searches logs for password change or reset events.
- **MySQL** - Searches logs for MySQL database errors, access denials, syntax errors, and connection issues.
- **Firewall** - Searches for allowed and blocked Windows Firewall events.
- **Network Outages** – Searches logs for network outages, failures, and disconnections.

- **Windows Updates** – Searches for successful and unsuccessful Windows Update events.

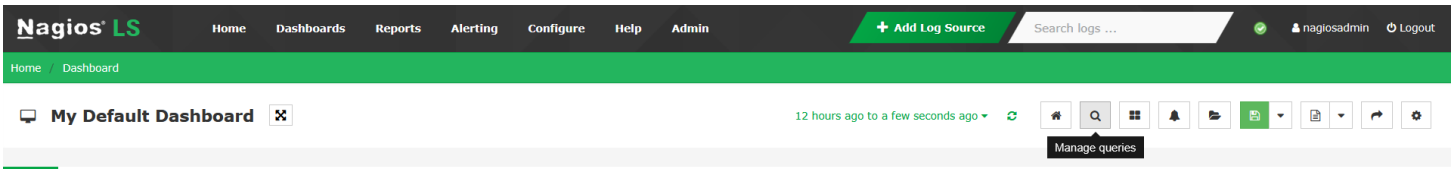
After selecting one or more of these preset queries, you can add to or edit the query. See the following section to create your own queries.

Creating your own Queries

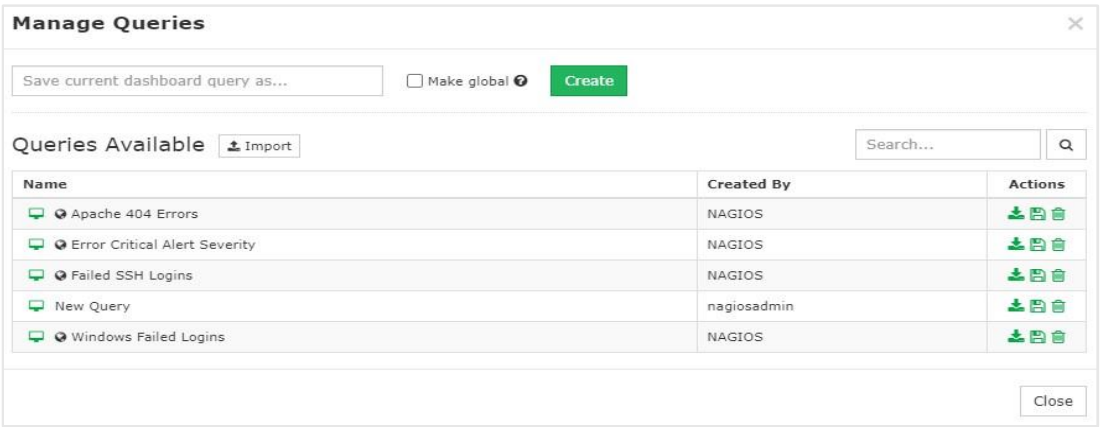
1. To create your own queries, select the **Advanced Search** link to open the query entry fields.
2. Enter your query text. Select the search icon to see the results displayed in the dashboard.



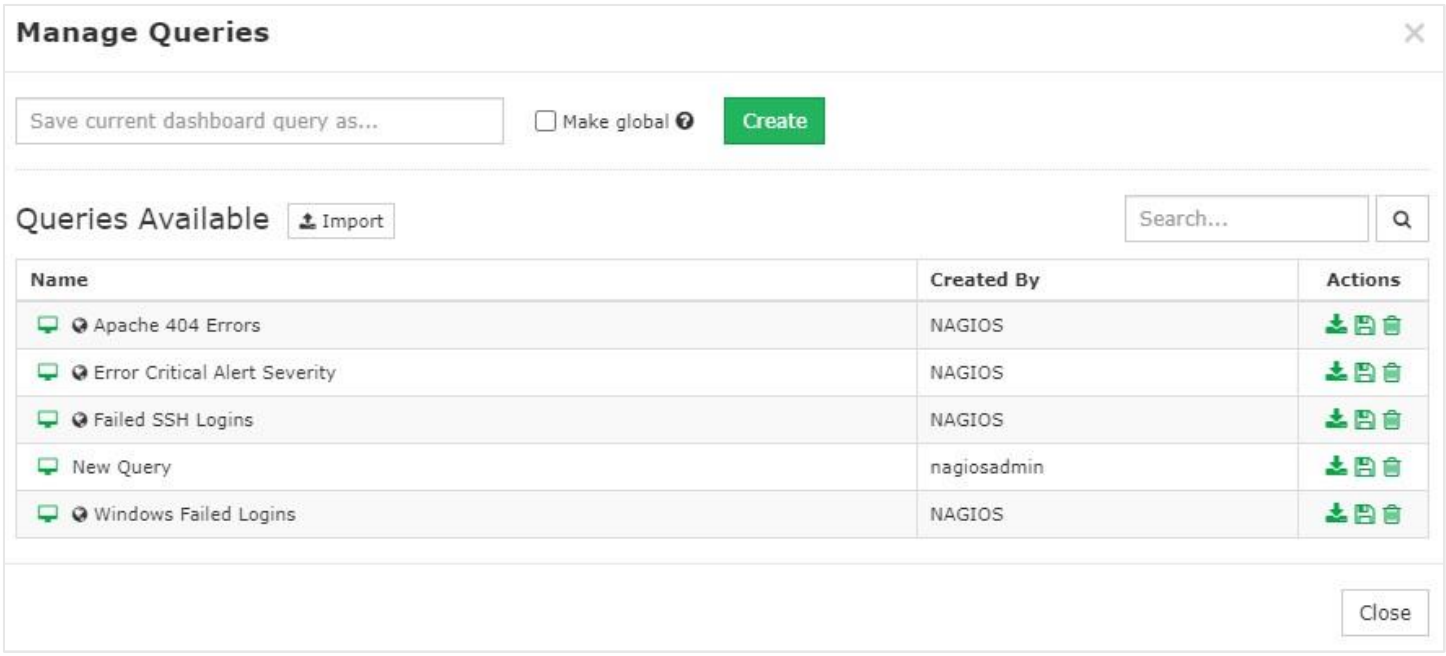
3. You can add more elements to your query by selecting the '**+**' button to add more inclusive queries.
4. Save the new query by selecting the **Manage Queries** button.



5. Enter a name for your query.
6. Select **Create.**



Managing Queries



There are several functions you can perform on your queries in the Manage Queries popup. You can access this from the **Manage Queries** button on the top button navigation on the **Dashboards** page.

- **Import** - You can import an existing query file by selecting the **Import** button.
- **Download** - You can download a query definition file to your local device by selecting the **Download** icon on an existing query.
- **Overwrite** - You can overwrite an existing query definition with the currently defined query by selecting the **Overwrite** icon.
- **Delete** - Delete an existing query.

Finishing Up

This completes the documentation on managing Nagios Log Server queries. 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