Loki alerting

- Before you begin
- Supported queries for alerting
- Create a Grafana-managed alert rule
- Example: alert on error log rate
- Manage data source-managed alert rules
- Best practices
  - Test queries before alerting
  - Reduce a time series to a single value
  - Set a pending period to avoid false positives
  - Handle no data versus zero results
- Troubleshoot alerting
  - Alerts don't fire
  - Alert enters No Data unexpectedly
  - Alert fires on brief spikes
  - Data source-managed rules don't appear
- Related resources

The Loki data source supports Grafana Alerting. You can alert on your logs so Grafana notifies you when a LogQL metric query crosses a threshold, for example when the rate of error logs spikes.

Loki works with two kinds of alert rules:

- **Grafana-managed alert rules:** Grafana evaluates the rule against a LogQL metric query. This is the most common approach and works with any Loki data source.
- **Data source-managed alert rules:** The Loki ruler stores and evaluates the rule. Use these when you want alert rules to live alongside your Loki deployment. Enable **Manage alert rules in Alerting UI** on the data source to create and edit them from Grafana.

Before you begin

Before you create alert rules with Loki data, ensure you have:

- A configured Loki data source.
- Permissions to create alert rules in Grafana.
- Familiarity with Grafana Alerting concepts.
- For data source-managed rules, a Loki deployment with the ruler enabled, and the **Manage alert rules in Alerting UI** setting turned on in the data source configuration.

  To route the resulting alerts, add a separate Alertmanager data source.

Supported queries for alerting

Alert rules require queries that return numeric data that Grafana can evaluate against a threshold. Wrap a Loki log query in a LogQL metric function, such as `rate` or `count_over_time`, to produce numeric time series.

{{< admonition type="note" >}} Use a metric query for alerting, not a plain log query. A log query returns log lines, which Grafana can't evaluate against a threshold. {{< /admonition >}}

The following queries are common starting points for alerting. Replace the label matchers with values from your own logs.

Rate of error lines per second:

```
sum(rate({app="my-app"} |= `error` [5m]))
```

Error rate broken down by status code, to alert per endpoint or service:

```
sum by (status) (rate({app="nginx"} | logfmt | status=~`5..` [5m]))
```

Count of slow requests, for a latency alert:

```
sum(count_over_time({app="my-app"} | logfmt | duration > 1s [5m]))
```

Detect a service that stopped logging by alerting when the count drops to zero:

```
sum(count_over_time({app="my-app"} [10m]))
```

Create a Grafana-managed alert rule

To create a Grafana-managed alert rule using Loki data:

1. Go to **Alerting** > **Alert rules**.
2. Click **New alert rule**.
3. Enter a name for your alert rule.
4. In the **Define query and alert condition** section:
   - Select your Loki data source.
   - Enter a LogQL metric query.
   - Add a **Reduce** expression if your query returns multiple series.
   - Add a **Threshold** expression to define the alert condition.
5. Configure the **Set evaluation behavior** section:
   - Select or create a folder and evaluation group.
   - Set the evaluation interval and pending period.
6. Add labels and annotations to provide context for notifications.
7. Click **Save rule**.

For detailed instructions, refer to Create a Grafana-managed alert rule.

Example: alert on error log rate

This example fires when the rate of log lines that contain `error` exceeds a threshold:

1. Create a new alert rule.
2. Configure the query, replacing the label matcher with your own:

   ```
   sum(rate({app="my-app"} |= `error` [5m]))
   ```

3. Add expressions:
   - **Reduce**: Last, to get the most recent value.
   - **Threshold**: Is above `10`.
4. Set evaluation to run every 1 minute with a 5-minute pending period.
5. Save the rule.

Manage data source-managed alert rules

When you turn on **Manage alert rules in Alerting UI** for the Loki data source, you can create and edit alert and recording rules that the Loki ruler stores and evaluates. These rules appear in the Grafana Alerting UI alongside your Grafana-managed rules, grouped under the Loki data source.

The Loki data source configuration doesn't include Alertmanager routing. To route the resulting alerts, add a separate Alertmanager data source. For more information, refer to Configure the Loki data source and Data source-managed alert rules.

Best practices

Follow these recommendations to create reliable alerts with Loki data.

Test queries before alerting

Verify your query returns numeric data before you create an alert:

1. Go to **Explore**.
2. Select your Loki data source.
3. Run the LogQL metric query you plan to use for alerting.
4. Confirm the result is numeric and suitable for threshold evaluation.

Reduce a time series to a single value

A Grafana-managed rule evaluates a single number against the threshold. A `range` query returns a time series with many points, which the rule can't evaluate directly. Either set the query **Type** to `instant`, or add a **Reduce** expression, such as **Last** or **Mean**, between the query and the **Threshold** expression. Without one of these, the rule can evaluate incorrectly.

Set a pending period to avoid false positives

A transient condition, such as a brief network blip or a momentary spike in errors, can cross the threshold for a single evaluation. Set a pending period so the rule fires only after the condition holds for a sustained duration. A pending period of a few evaluation intervals reduces false positives from short-lived conditions.

Handle no data versus zero results

A LogQL metric query returns *no series* when no log lines match, rather than returning a value of `0`. Grafana evaluates a rule that receives no series as **No Data**, not **Normal**, which can cause an alert to enter the No Data state instead of resolving.

To avoid unexpected No Data states:

- Apply the threshold in the alert condition rather than writing a query so restrictive that it returns nothing. For example, query the error rate and compare it in a **Threshold** expression, instead of writing a query that only returns lines above the threshold.
- Set the No Data behavior under **Configure no data and error handling** to the state you want. The options are **No Data**, **Alerting**, **Normal**, and **Keep Last State**. Choose **Normal** if the absence of matching logs isn't a problem.

{{< admonition type="note" >}} Editing and saving an alert rule resets its state to **Normal**. The rule re-enters **Pending** or **Alerting** on the next evaluation if the condition is still met. This is standard Grafana Alerting behavior and isn't specific to the Loki data source. {{< /admonition >}}

Troubleshoot alerting

If your Loki alerts don't work as expected, use the following sections to diagnose common issues.

Alerts don't fire

- Confirm the query is a LogQL metric query that returns numeric data in Explore.
- Ensure the evaluation interval allows enough time for data to be available.
- Review the alert rule's health and any error messages in the Alerting UI.

Alert enters No Data unexpectedly

- The query returned no series because no log lines matched. A LogQL metric query returns no series rather than `0` when nothing matches. Set the No Data behavior under **Configure no data and error handling**, or restructure the query so it returns a value that you compare with a threshold.

- Confirm logs exist for the query and time range in Explore.

Alert fires on brief spikes

- Add or increase the pending period so the rule fires only when the condition holds over several evaluations.
- Widen the range in the metric query, for example from `[1m]` to `[5m]`, so short-lived spikes have less effect.

Data source-managed rules don't appear

- Confirm **Manage alert rules in Alerting UI** is enabled in the Loki data source configuration.
- Verify the Loki ruler is enabled and reachable from Grafana.

For more help, refer to Troubleshoot Loki issues.

Related resources

- Grafana Alerting
- Create a Grafana-managed alert rule
- Loki query editor

□□□ #2
□ □□□ □□□ 2026-10-31 15:58:02 UTC
□ □□□ □□□ 2026-10-31 15:58:04 UTC