Alerting

Alert

A must-have for any time series-based data visualization application is **Alerting**. Alerts allow you to identify problems in your system moments after they occur. By quickly identifying unintended changes in your system, you can minimize disruptions to your services.

Alerts consist of two parts:

1. **Alert rules:** When the alert is triggered. Alert rules are defined by one or more conditions that are regularly evaluated by Grafana.

2. **Notification channel:** How the alert is delivered. When the conditions of an alert rule are met, the Grafana notifies the channels configured for that alert.

Currently, only the graph panel visualization supports alerts.

Alert tasks:

You can perform the following tasks for alerts:

- Add or edit an alert notification channel

- Create an alert rule

- View existing alert rules and their current state

- Test alert rules and troubleshoot

You can also set alert rule notifications along with a detailed message about the alert rule. The message can contain anything: information about how you might solve the issue, link to runbook, and so on.

The actual notifications are configured and shared between multiple alerts.

Alert execution

Alert rules are evaluated in the Grafana backend in a scheduler and query execution engine that is part of core Grafana. Only some data sources are supported right now. They include Graphite, Prometheus, InfluxDB, Elasticsearch, Google Cloud Monitoring, Cloudwatch, Azure Monitor, MySQL, PostgreSQL, MSSQL, OpenTSDB, Oracle, and Azure Data Explorer.

Alert Rules

Alerting rules are the data thresholds that activate an alert. From this tab, you can manage the alerts created in various dashboard panels. Once an alert is triggered, you'll need some form of notification so that you can be made aware of the alert. The process of connecting an alert rule to some form of notification is easy:

1. Establish one or more alerts on your dashboard panel.

2. Configure a notification channel to be activated on an appropriate alert state.

3. Set the alert to use one or more notification channels.

Alert Notifications

When an alert changes state, it sends out notifications. Each alert rule can have multiple notifications. In order to add a notification to an alert rule, you first need to add and configure a notification channel (can be email, PagerDuty, or other integration).

This is done from the **Notification channels** page.

Add a notification channel

- In the Grafana side bar, hover your cursor over the **Alerting** (bell) icon and then click **Notification channels**.

- Click **Add channel**.

- Fill out the fields or select options described below.

New notification channel fields

Default (send on all alerts)

- **Name:** Enter a name for this channel. It will be displayed when users add notifications to alert rules.

- **Type:** Select the channel type. Refer to the List of supported notifiers for details.

- **Default (send on all alerts):** When selected, this option sends a notification on this channel for all alert rules.

- **Include Image:** See Enable images in notifications for details.

- **Disable Resolve Message:** When selected, this option disables the resolve message [OK] that is sent when the alerting state returns to false.

- **Send reminders:** When this option is checked additional notifications (reminders) will be sent for triggered alerts. You can specify how often reminders should be sent using number of seconds (s), minutes (m) or hours (h), for example, `30s`, `3m`, `5m` or `1h`.

Complementary Lesson about Alert on your Loki logs with Grafana