+++ title = “Notification policies” description = “Notification policies” keywords = [“grafana”, “alerting”, “guide”, “notification policies”, “routes”] weight = 450 +++

Notification policies

Notification policies determine how alerts are routed to contact points. Policies have a tree structure, where each policy can have one or more child policies. Each policy, except for the root policy, can also match specific alert labels. Each alert is evaluated by the root policy and subsequently by each child policy. If you enable the `Continue matching subsequent sibling nodes` option is enabled for a specific policy, then evaluation continues even after one or more matches. A parent policy's configuration settings and contact point information govern the behavior of an alert that does not match any of the child policies. A root policy governs any alert that does not match a specific policy.

You can configure Grafana managed notification policies as well as notification policies for an [external Alertmanager data source]({{< relref “../../../data-sources/alertmanager.md” >}}). For more information, see [Alertmanager]({{< relref “../fundamentals/alertmanager.md” >}}).

Grouping

{{< figure max-width=“40%” src=“/static/img/docs/alerting/unified/notification-policies-grouping.png” max-width=“650px” caption=“Notification policies grouping” >}}

Grouping is a new and key concept of Grafana alerting that categorizes alert notifications of similar nature into a single funnel. This allows you to properly route alert notifications during larger outages when many parts of a system fail at once causing a high number of alerts to fire simultaneously.

For example, suppose you have 100 services connected to a database in different environments. These services are differentiated by the label `env=environmentname`. An alert rule is in place to monitor whether your services can reach the database named `alertname=DatabaseUnreachable`.

When a network partition occurs, half of your services can no longer reach the database. As a result, 50 different alerts (assuming half of your services) are fired. For this situation, you want to receive a single-page notification (as opposed to 50) with a list of the environments that are affected.

You can configure grouping to be `group_by: [alertname]` (take note that the `env` label is omitted). With this configuration in place, Grafana sends a single compact notification that has all the affected environments for this alert rule.

> **Note:** Grafana also has a special label named `...` that you can use to group all alerts by all labels (effectively disabling grouping),

therefore each alert will go into its own group. It is different from the default of `group_by: null` where **all** alerts go into a single group.

Edit root notification policy

Note: Before Grafana v8.2, the configuration of the embedded Alertmanager was shared across organisations. Users of Grafana 8.0 and 8.1 are advised to use the new Grafana 8 Alerts only if they have one organisation. Otherwise, silences for the Grafana managed alerts will be visible by all organizations.

1. In the Grafana menu, click the **Alerting** (bell) icon to open the Alerting page listing existing alerts.
2. Click **Notification policies**.
3. From the **Alertmanager** dropdown, select an external Alertmanager. By default, the Grafana Alertmanager is selected.
4. In the Root policy section, click **Edit** (pen icon).
5. In **Default contact point**, update the [contact point]({{< relref "../contact-points.md" >}}) to whom notifications should be sent for rules when alert rules do not match any specific policy.
6. In **Group by**, choose labels to group alerts by. If multiple alerts are matched for this policy, then they are grouped by these labels. A notification is sent per group. If the field is empty (default), then all notifications are sent in a single group. Use a special label `...` to group alerts by all labels (which effectively disables grouping).
7. In **Timing options**, select from the following options:
   - **Group wait** Time to wait to buffer alerts of the same group before sending an initial notification. Default is 30 seconds.
   - **Group interval** Minimum time interval between two notifications for a group. Default is 5 minutes.
   - **Repeat interval** Minimum time interval for re-sending a notification if no new alerts were added to the group. Default is 4 hours.
8. Click **Save** to save your changes.

Add new specific policy

1. In the Grafana menu, click the **Alerting** (bell) icon to open the Alerting page listing existing alerts.
2. Click **Notification policies**.
3. From the **Alertmanager** dropdown, select an Alertmanager. By default, the Grafana Alertmanager is selected.
4. To add a top level specific policy, go to the **Specific routing** section and click **New specific policy**.
5. In **Matching labels** section, add one or more rules for matching alert labels. For more information, see "How label matching works".
6. In **Contact point**, add the [contact point]({{< relref "../contact-

points.md" >}}) to send notification to if alert matches only this specific policy and not any of the nested policies.
7. Optionally, enable **Continue matching subsequent sibling nodes** to continue matching nested policies even after the alert matched the parent policy. When this option is enabled, you can get more than one notification. Use it to send notification to a catch-all contact point as well as to one of more specific contact points handled by nested policies.
8. Optionally, enable **Override grouping** to specify the same grouping as the root policy. If this option is not enabled, the root policy grouping is used.
9. Optionally, enable **Override general timings** to override the timing options configured in the group notification policy.
10. Click **Save policy** to save your changes.

Add nested policy

1. Expand the specific policy you want to update.
2. Click **Add nested policy**, then add the details using information in Add new specific policy.
3. Click **Save policy** to save your changes.

Edit specific policy

1. In the Alerting page, click **Notification policies** to open the page listing existing policies.
2. Find the policy you want to edit, then click **Edit** (pen icon).
3. Make any changes using instructions in Add new specific policy.
4. Click **Save policy**.

How label matching works

A policy will match an alert if the alert's labels match all the "Matching Labels" specified on the policy.

- The **Label** field is the name of the label to match. It must exactly match the label name.
- The **Operator** field is the operator to match against the label value. The available operators are:
  - `=`: Select labels that are exactly equal to the provided string.
  - `!=`: Select labels that are not equal to the provided string.
  - `=~`: Select labels that regex-match the provided string.
  - `!~`: Select labels that do not regex-match the provided string.
- The **Value** field matches against the corresponding value for the specified **Label** name. How it matches depends on the **Operator** value.

Example

An example of an alert configuration.

- Create a “default” contact point for slack notifications, and set it on root policy.
- Edit the root policy grouping to group alerts by `cluster`, `namespace` and `severity` so that you get a notification per alert rule and specific kubernetes cluster and namespace.
- Create specific route for alerts coming from the development cluster with an appropriate contact point.
- Create a specific route for alerts with “critical” severity with a more invasive contact point type, like pager duty notification.
- Create specific routes for particular teams that handle their own onduty rotations.

{{< figure max-width=“40%” src=“/static/img/docs/alerting/unified/notification-policies-8-0.png” max-width=“650px” caption=“Notification policies” >}}