REVISION HISTORY

Version	Date	Change description	Created by	Updated by	Reviewed by
V 1.0	November, 2022	Release 6.0	Hemanth/Yash	Raksha	Chiranjib

Customizing Alerts using Grafana

Alerts allow to learn about problems in the system moments after they occur. Robust and actionable alerts help identify and resolve issues quickly, minimizing disruption of services.

Grafana alerting has four key components:

- **Alerting rule:** Evaluation criteria that determine whether an alert will fire. It consists of one or more queries and expressions, a condition, the frequency of evaluation, and optionally, the duration over which the condition is met.
- **Contact point:** Channel for sending notifications when the conditions of an alerting rule are met.
- **Notification policy:** Set of matching and grouping criteria used to determine where and how frequently to send notifications.
- **Silences:** Date and matching criteria used to silence notifications.

State and Health of Alerting Rules

The state and health of alerting rules helps understand several key status indicators about the alerts. There are three key components: alert state, alerting rule state and alerting rule health. Although related, each component conveys different information.

Alerting Rule State:

- **Normal**: None of the time series returned by the evaluation engine is in a Pending or Firing state.
- **Pending**: At least one time series returned by the evaluation engine is Pending.
- **Firing**: At least one time series returned by the evaluation engine is Firing.
- **No Data**: The alerting rule has not returned a time series. All values for the time series are null or zero.
- **Error**: Occurrence of error when attempting to evaluate an alerting rule.
- **Ok**: No error when evaluating an alerting rule.

Creation of Grafana Managed Alerting Rule

Grafana allows to create alerting rules that query one or more data sources, reduce or transform the results and compare them to each other or to fix thresholds. When these are executed, Grafana sends notifications to the contact point.

Add Grafana managed rule:

1. In the Grafana menu, click the Alerting (bell) icon to open the Alerting page listing existing alerts.
2. Click New alert rule.
3. **Step 1:** Add the rule name, type and storage location.
   - In Rule name, add a descriptive name. This name is displayed in the alert rule list. It is also the alertname label for every alert instance that is created from this rule.
   - From the Rule type drop-down, select Grafana managed alert.

   - From the Folder drop-down, select the desired folder to store the rule. By default, the rule is stored in the General folder. To create a new folder, click the drop-down and enter the new folder name.

4. **Step 2:** Add queries and expressions to evaluate.
   - Keep the default name or hover over and click the edit icon to change the name.
   - For queries, select a data source from the drop-down.
   - Add one or more queries or expressions.
   - For each expression, select either Classic condition to create a single alert rule or choose from Math, Reduce, Resample options to generate separate alerts for each series. For details on these options, see Single and Multi-dimensional rule.
   - Click Run queries to verify that the query is successful.
5. **Step 3:** Add conditions.
   - From the Condition drop-down, select the query or expression to trigger the alert rule.
   - For Evaluate every, specify the frequency of evaluation. Must be a multiple of 10 seconds. For example, 30s, 1m.
   - For Evaluate for, specify the duration for which the condition must be true before an alert fires.
     Note: Once a condition is breached, the alert goes into the Pending state. If the condition remains breached for the duration specified, the alert transitions to the Firing state, else it reverts back to the Normal state.
   - In Configure no data and error handling, configure alerting behavior in the absence of data. Use the guidelines in No data and error handling.
   - Click Preview alerts to check the result of running the query any particular moment. Preview excludes no data and error handling.
6. **Step 4:** Add additional metadata associated with the rule.
   - Add a description and summary to customize alert messages. Use the guidelines in Annotations and labels for alerting.
   - Add Runbook URL, panel, dashboard and alert IDs.
   - Add custom labels.
7. Click Save to save the rule or Save and exit to save the rule and go back to the Alerting page.

Single and Multi-dimensional rule:

For Grafana managed alerts, a rule can be created with a classic condition or a multi-dimensional rule.

Rule with classic condition:

Use the classic condition expression to create a rule that triggers a single alert when its condition is met. For a query that returns multiple series, Grafana does not track the alert state of each series. As a result, Grafana sends only a single alert even when alert conditions are met for multiple series.

Multi-dimensional rule:

To generate a separate alert for each series, create a multi-dimensional rule. Use Math, Reduce, or Resample expressions to create a multi-dimensional rule. For example:

- Add a Reduce expression for each query to aggregate values in the selected time range into a single value. (Not needed for rules using numeric data).
- Add a Math expression with the condition for the rule. It's not needed in case a query or a reduce expression already returns 0 if the rule should not fire, or a positive number if it should fire. For example: $B > 70. It should fire in case the value of B query/expression is more than 70. $B < $C * 100. It should fire if the value of B is less than the value of C multiplied by 100.
    - If queries being compared have multiple series in their results, series from different queries are matched if they have the same labels or one is a subset of the other.

Annotations and Labels for Alerting Rules

Annotations are key-value pairs that provide additional meta-information about an alert. The following annotations are used: description, summary, runbook_url, alertId, dashboardUid, and panelId.

For example, a description, a summary, and a runbook URL. These are displayed in rule and alert details in the UI and can be used in contact point message templates.

Labels are key-value pairs that contain information about, and are used to uniquely identify an alert. The label set for an alert is generated and added throughout the alerting evaluation and notification process.

Variables available to alerting rule labels and annotations:

The following template variables are available when expanding annotations and labels.

Name	Description
$labels	The labels from the query or condition. For example, {{ $labels.instance }} and {{ $labels.job }}. This is unavailable when the rule uses a classic condition.
$values	The values of all reduce and math expressions that were evaluated for this alert rule. For example, {{ $values.A }}, {{ $values.A.Labels }} and {{ $values.A.Value }} where A is the refID of the expression. If the rule uses classic conditions, then a combination of the refID and position of the condition is used. For example, {{ $values.A0.Value }} or {{ $values.A1.Value }}
$value	The value string of the alert instance. For example, [var='A' labels={instance=foo} value=10].

Alert Groups

Alert groups show grouped alerts from an Alertmanager instance. By default, the alerts are grouped by the label keys for the root policy in notification policies. Grouping common alerts into a single alert group prevents duplicate alerts from being fired.

View alert groupings:

1. In the Grafana menu, click the Alerting (bell) icon to open the Alerting page listing existing alerts.
2. Click Alert grouping to open the page listing existing groups.
3. From the Alertmanager drop-down, select an external Alertmanager as your data source. By default, the Grafana Alertmanager is selected.
4. From custom group by drop-down, select a combination of labels to view a grouping other than the default. This is useful to debug and verify the grouping of notification policies.

If an alert does not contain labels specified either in the grouping of the root policy or the custom grouping, then the alert is added to a catch all group with a header as No grouping.

Filter alerts:

Use the following filters to view alerts that match specific criteria:

- **Search by label:** In Search, enter an existing label to view alerts matching the label. For example, environment=production,region=~US|EU,severity!=warning
- **Filter alerts by state:** In States, select from Active, Suppressed, or Unprocessed states to view alerts matching the selected state. All other alerts are hidden.

Contact Points

Contact points define how contacts are notified when an alert fires. A contact point can have one or more contact point types. For example, email, slack, webhook, and so on. When an alert fires, a notification is sent to all contact point types listed for a contact point.

Addition of contact point:

1. In the Grafana menu, click the Alerting (bell) icon to open the Alerting page listing existing alerts.
2. Click Contact points to open the page listing existing contact points.
3. Click New contact point.
4. From the Alertmanager dropdown, select an Alertmanager. By default, Grafana Alertmanager is selected.
5. Under Name field, enter a descriptive name for the contact point.
6. From Contact point type, select a type and fill out mandatory fields. For example, if email is selected, enter the email addresses. Or if Slack is selected, enter the Slack channel(s) and the users to be contacted.
7. Some contact point types, like email or webhook, have optional settings. In Optional settings, specify additional information for the selected contact point type.
8. In Notification settings, select Disable resolved message to stop notifying when an alert is resolved. This is an optional setting.

9. To add another contact point type, click New contact point type and repeat steps 6 through 8.
10. Click Save contact point to save the changes.

Testing a contact point:

Before testing a contact point add a mail configuration in grafana.yaml file as follows:

Open kubernetes_resources/softwares/istio-1.13.2/samples/addons/grafana.yaml file

Check whether the below snippet is present in grafana.ini section:

```
[smtp]
  enabled = true
  host = "<your-host>:587"
  user = "username"
  password = "password"
  skip_verify = false
  from_address = "username"
```

Restart Grafana for the configuration changes to take effect.

Sending a test notification:

1. In the Grafana side bar, hover cursor over the Alerting (bell) icon and click Contact points.
2. Find the contact point to test. Click Edit (pen icon). A new contact point can be created if required.
3. Click Test (paper airplane icon) to open the contact point testing modal.
4. Choose whether to send a predefined test notification or choose custom to add custom annotations and labels to include in the notification.
5. Click Send test notification to fire the alert.

Deletion of contact point:

1. In the Alerting page, click Contact points to open the page listing existing contact points.
2. Find the contact point to delete. Click Delete (trash icon).
3. In the confirmation dialog, click Yes, delete.

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.

Root notification 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 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 to send the notifications to, when alert rules do not match any specific policy.
6. In Group by, choose labels to group the alerts. 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:** 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 the changes.

Edit a specific policy:

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

Silences

Use silences to stop notifications from one or more alerting rules. Silences do not prevent alert rules from being evaluated. They do not stop alerting instances from being shown in the user interface. Silences only stop notifications from getting created. A silence lasts for only a specified window of time.

Addition of silence:

1. In the Grafana menu, click the Alerting (bell) icon to open the Alerting page listing existing alerts.
2. In the Alerting page, click Silences to open the page listing existing contact points.
3. From Alertmanager drop-down, select an external Alertmanager to create and manage silences for the external data source. Otherwise, keep the default option of Grafana.
4. Click New Silence to open the Create silence page.
5. In Silence start and end, select the start and end date to indicate when the silence should go into effect and expire.
6. Optionally, in Duration, specify how long the silence is enforced. This automatically updates the end time in the Silence start and end field.

7. In the Name and Value fields, enter one or more Matching Labels. Matchers determine which rules the silence will apply to. For more information, see Label matching for alert suppression.
8. In Comment, add details about the silence.
9. In Creator, enter the name of the silence owner or keep the default owner.
10. Click create.

Removal of silences:

1. In the Alerting page, click Silences to view the list of existing silences.
2. Find the silence that needs to end. Click Unsilence.