

Alerting in the Prometheus ecosystem

A story of the past, present and future



Josh Abreu

Senior Software Engineer, Grafana Labs



Josue Abreu

Senior Software Engineer

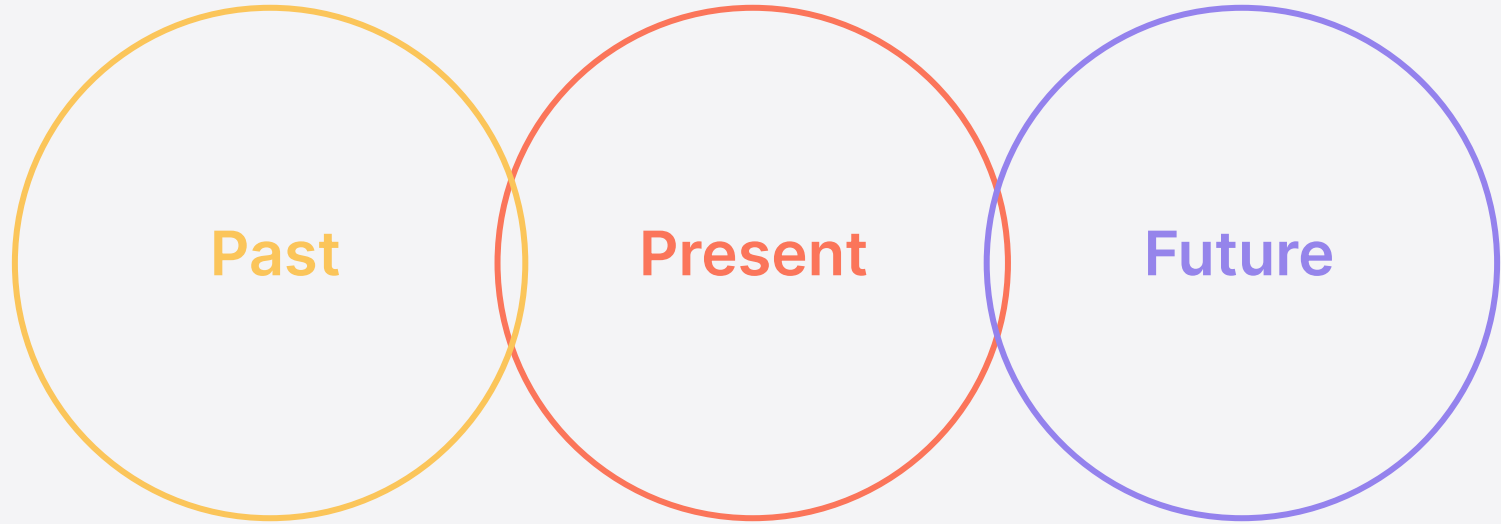
Prometheus/Alertmanager/Cortex contributor

Mimir maintainer



Show of hands 🖐

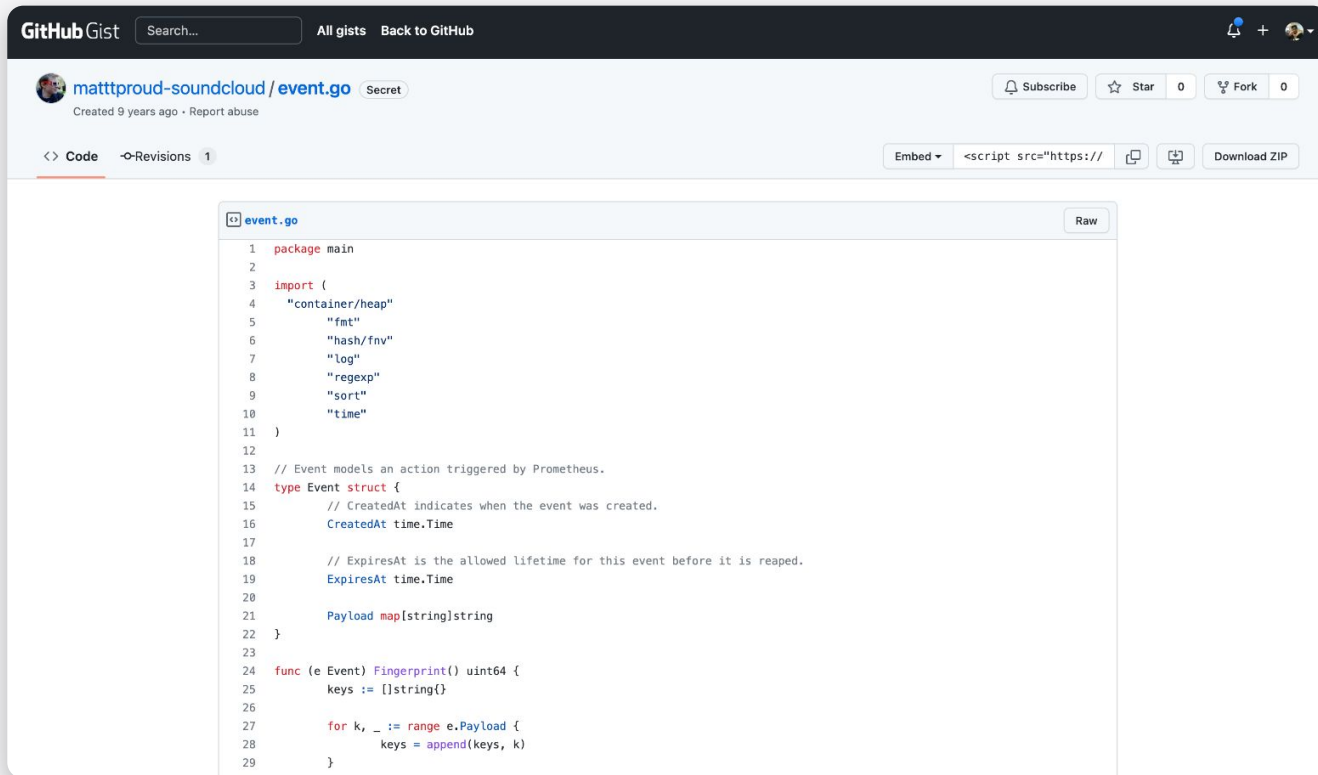






Past

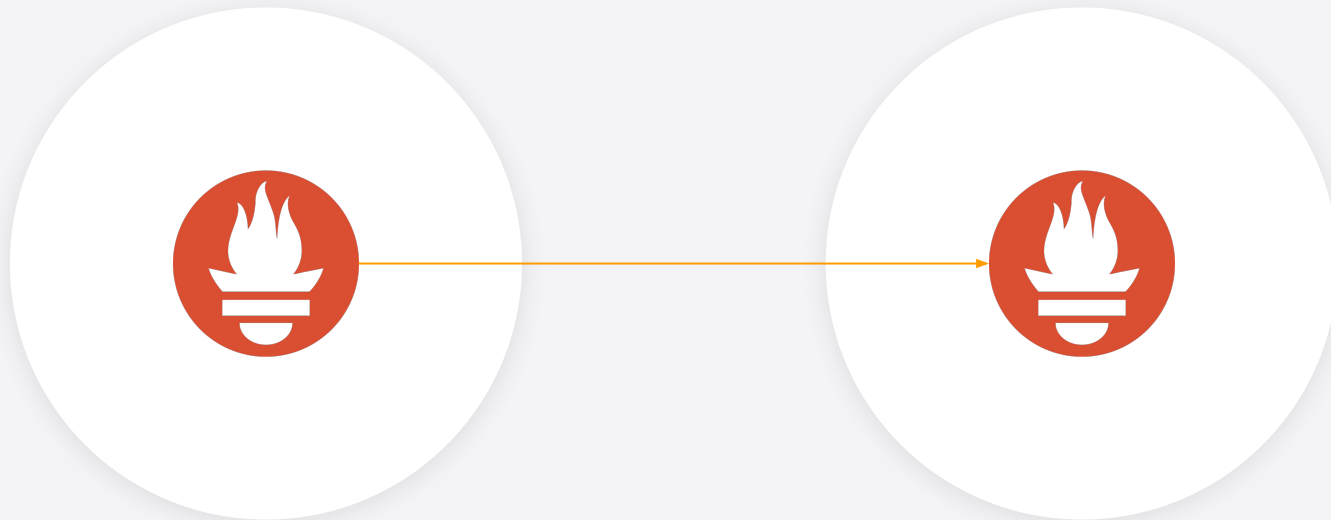
The beginning



The screenshot shows a GitHub Gist page for a file named `event.go`. The page header includes the GitHub Gist logo, a search bar, and navigation links for "All gists" and "Back to GitHub". The user profile for "matttproud-soundcloud" is visible, along with a "Secret" label. The gist was created 9 years ago. Interaction buttons for "Subscribe", "Star" (0), and "Fork" (0) are present. Below the header, there are tabs for "Code" (selected) and "Revisions" (1). On the right, there are buttons for "Embed", a script tag generator, a copy icon, a download icon, and a "Download ZIP" button. The main content area displays the Go code for `event.go` with a "Raw" button in the top right corner. The code defines a `main` package, imports standard libraries, and defines an `Event` struct with fields for `CreatedAt`, `ExpiresAt`, and `Payload`. A `Fingerprint` function is also defined.

```
1 package main
2
3 import (
4     "container/heap"
5     "fmt"
6     "hash/fnv"
7     "log"
8     "regexp"
9     "sort"
10    "time"
11 )
12
13 // Event models an action triggered by Prometheus.
14 type Event struct {
15     // CreatedAt indicates when the event was created.
16     CreatedAt time.Time
17
18     // ExpiresAt is the allowed lifetime for this event before it is reaped.
19     ExpiresAt time.Time
20
21     Payload map[string]string
22 }
23
24 func (e Event) Fingerprint() uint64 {
25     keys := []string{}
26
27     for k, _ := range e.Payload {
28         keys = append(keys, k)
29     }
30 }
```





Prometheus
Alert Generator

Alertmanager
Alert Receiver



Past



Grouping



Deduplication



Routing



Silencing



Templating



Alertmanager Alert

alerts ★ required

array[object]
(body)

The alerts to create

Example Value | Model

```
[
  {
    "startsAt": "2022-05-16T22:38:13.871Z",
    "endsAt": "2022-05-16T22:38:13.871Z",
    "annotations": {
      "additionalProp1": "string",
      "additionalProp2": "string",
      "additionalProp3": "string"
    },
    "labels": {
      "additionalProp1": "string",
      "additionalProp2": "string",
      "additionalProp3": "string"
    },
    "generatorURL": "string"
  }
]
```

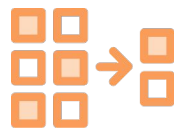
Parameter content type

application/json

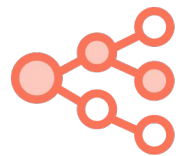




Grouping



Deduplication



Routing



Silencing



Templating

Past



Grouping



Deduplication



Routing



Silencing



Templating



Horizontally Scaling the Alertmanager

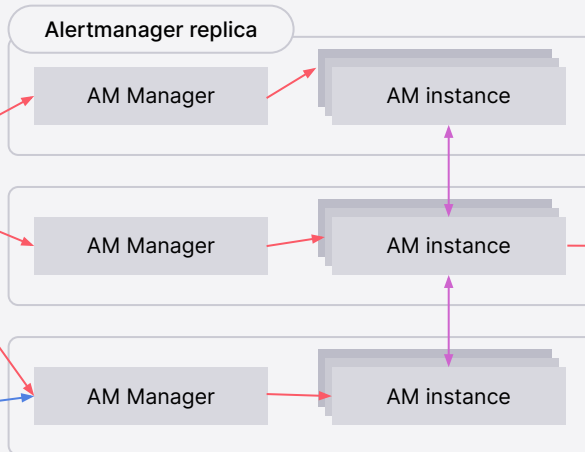


- 1 Ruler sends alerts to all Alertmanager.



User sends requests to any alertmanager

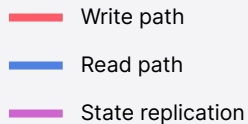
- 2 Alerts are handled by each alertmanager

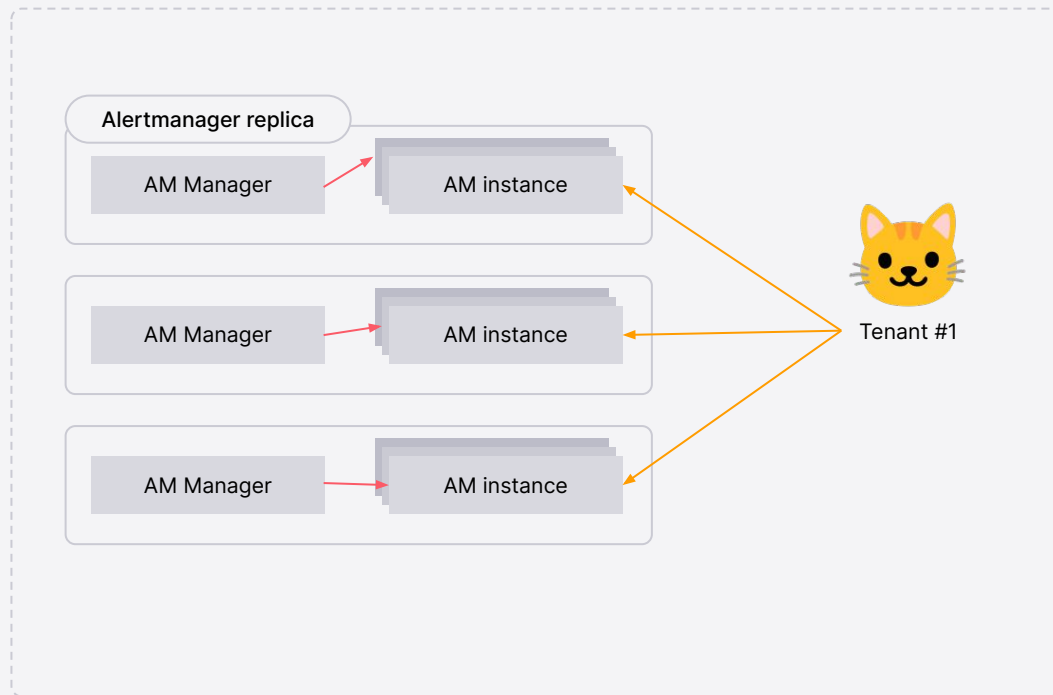


- 3 Store alerts in-memory. Persist to disk and gossip notifications and silences.



- 4 When an alerts notifies it is communicated back to all other peers. Each peer waits their position x 15 seconds.





Past

Scaling the Alertmanager

Survive single
machine failure

Eventual consistency
for reads and writes

Zero downtime
deployments

Scaling of the Cortex Alertmanager

Author: Josh Abreu, Tom Wilkie
Stakeholders: Marco Pracucci, Ganesh Vernekar, Goutham Veeramachaneni
Date: November 2020
Status: Completed

[Background](#)

[Problem & Requirements](#)

[Design Discussion](#)

[Routing & Sharding](#)

[Persistence & State](#)

[Replication & Consistency](#)





Routing & Sharding



Persistence & State

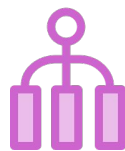


Replication & Consistency



Service Architecture





Routing & Sharding



Persistence & State

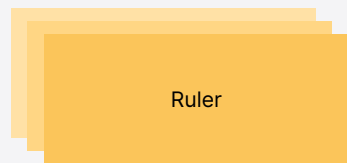


**Replication &
Consistency**



Service Architecture

- 1 Ruler sends alerts to **any** Alertmanager. Rate-limited and validated by the distributor.



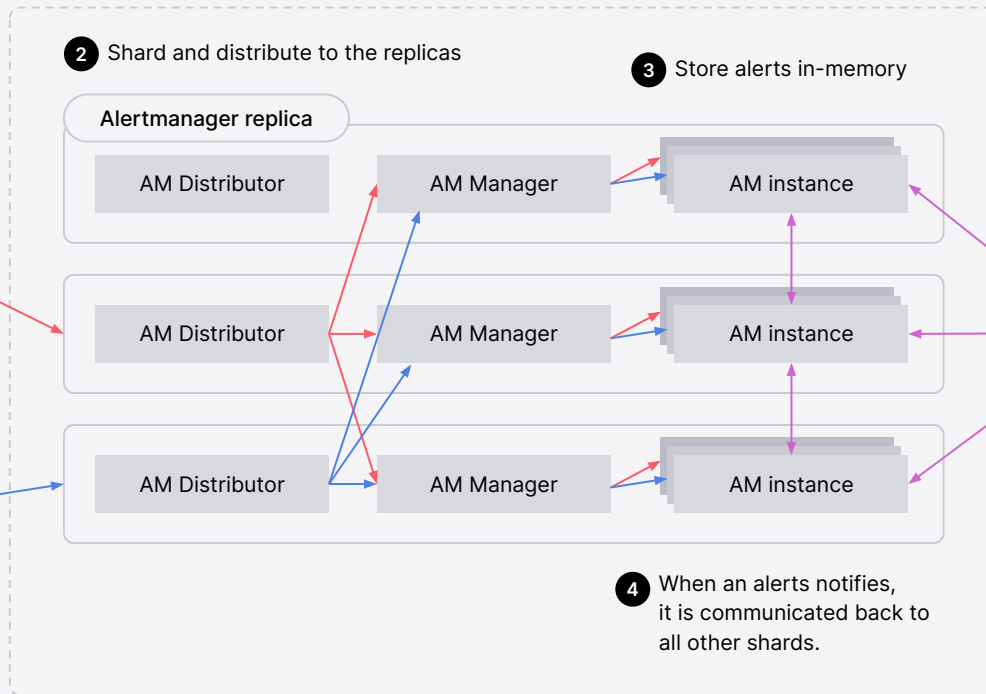
POST /api/v1/alerts

User sends requests to any alertmanager

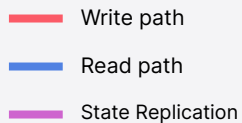
- 2 Shard and distribute to the replicas

- 3 Store alerts in-memory

- 5 State is periodically persisted to object store.



- 4 When an alerts notifies, it is communicated back to all other shards.





Present

grafana / grafana Public

Code Issues 2.2k Pull requests 245 Discussions Actions

Alerting support for queries using templates

Closed calind opened this issue on 12 Nov 2016 · 137 comments



calind commented on 12 Nov 2016

It would be pretty useful if grafana would support alerting for queries using templates as follows:

1. Generate queries for each template variable combination (discarding template variable for which the value is empty)
2. When generating queries, consider the frozen list if the template variable is set to never refresh
3. Allow filtering (through regex or by providing a static value) for each template variable

The current workaround is to use an invisible wildcard metric, but the problem I see with this is context.



593



128

https://github.com/grafana/grafana/issues/6557

grafana / grafana Public

Code Issues 2.2k Pull requests 245 Discussions Actions Projects 9 Security 18 Insights

Alerting: Time of day restrictions #6592

Closed torkelo opened this issue on 16 Nov 2016 · 122 comments



torkelo commented on 16 Nov 2016

Member

Time of day restrictions.

See two ways this could be implemented.

1. As an alert condition
2. As a filter on notifications



525



16



59



29



27



sanchitraizada commented on 14 Mar 2017 · edited

Contributor

As per <http://docs.grafana.org/alerting/rules/>, Grafana plans to track state per series in future releases.

- "If a query returns multiple series then the aggregation function and threshold check will be evaluated for each series. What Grafana does not do currently is track alert rule state per series." and
- "To improve support for queries that return multiple series we plan to track state per series in a future release"

But it seems like there can be use cases where we have graphs containing set of metrics for which different sets of alerts are required. This is slightly different from "Support per series state change" (#6041) because

1. The action (notifications) can be different.
2. Also, tracking separate states of an alert is not always preferred (as the end-user would need to know the details behind

https://github.com/grafana/grafana/issues/7832



grafana / grafana Public

Code Issues 2.2k Pull requests 245 Discussions Actions Projects 9 Security 18

Alerting support for queries using template variables #6557

Closed calind opened this issue on 12 Nov 2016 · 137 comments

calind commented on 12 Nov 2016

It would be pretty useful if grafana would support alerting for queries using template variables be as follows:

1. Generate queries foreach template variable combination (discarding template variable for
2. When generating queries, consider the frozen list if the template variable is set to never re
3. Allow filtering (trough regex or by providing a static value) for each template variable

The current workaround is to use an invisible wildcard metric, but the problem I see with this a context.

593 128

<https://github.com/grafana/grafana/issues/6557>

grafana / grafana Public

Code Issues 2.2k Pull requests 245 Discussions Actions Projects 9 Security 18 Insights

[Feature request] Multiple alerts per graph #7832

Closed sanchitraizada opened this issue on 14 Mar 2017 · 148 comments

sanchitraizada commented on 14 Mar 2017 · edited Contributor

As per <http://docs.grafana.org/alerting/rules/>, Grafana plans to track state per series in future releases.

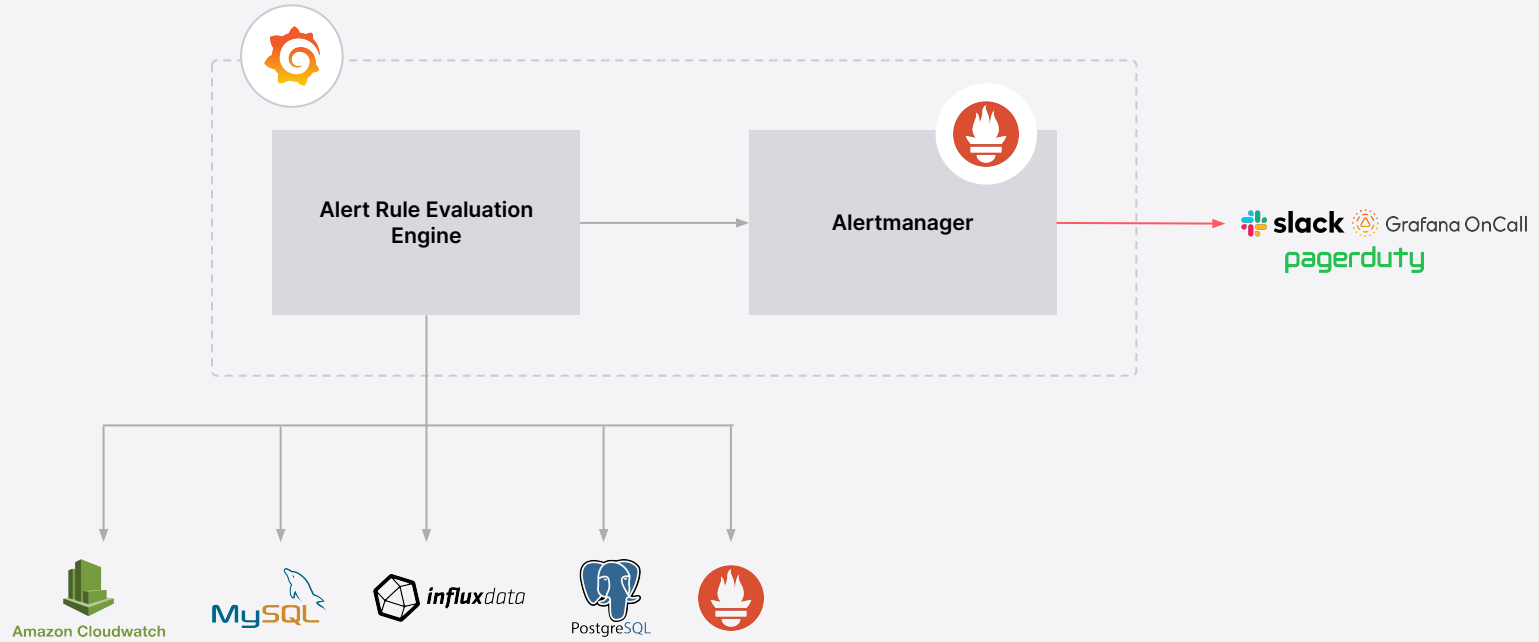
- "If a query returns multiple series then the aggregation function and threshold check will be evaluated for each series. What Grafana does not do currently is track alert rule state per series." and
- "To improve support for queries that return multiple series we plan to track state per series in a future release"

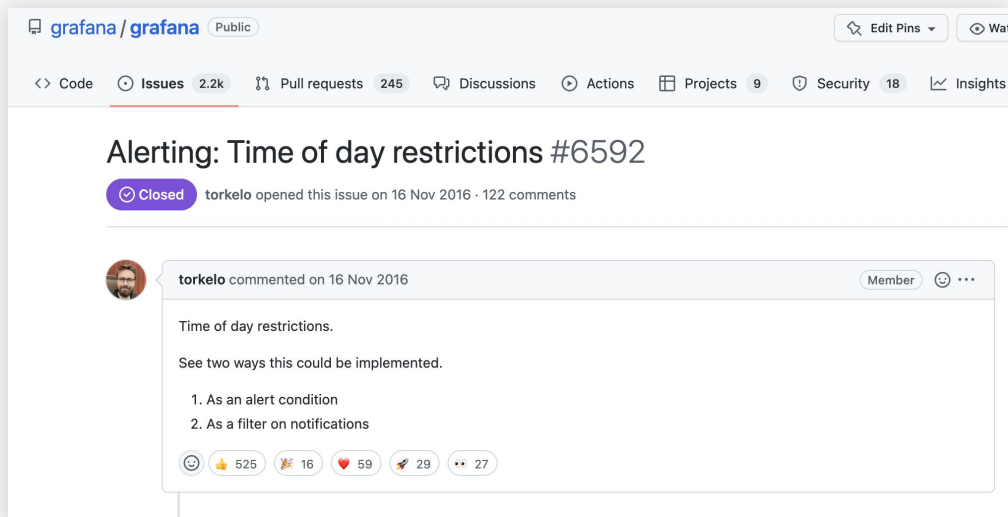
But it seems like there can be use cases where we have graphs containing set of metrics for which different sets of alerts are required. This is slightly different from "Support per series state change" (#6041) because

1. The action (notifications) can be different.
2. Also, tracking separate states of an alert is not always preferred (as the end-user would need to know the details behind

<https://github.com/grafana/grafana/issues/7832>








The screenshot shows a GitHub repository for 'grafana/grafana'. The 'Issues' tab is selected, showing 2.2k issues. A specific issue, '#6592', titled 'Alerting: Time of day restrictions', is highlighted. It is marked as 'Closed' and was opened by 'torkelo' on November 16, 2016, with 122 comments. A comment from 'torkelo' is shown, dated November 16, 2016. The comment text is: 'Time of day restrictions. See two ways this could be implemented. 1. As an alert condition 2. As a filter on notifications'. The comment has 525 thumbs up, 16 reactions, 59 hearts, 29 replies, and 27 mentions.

grafana / grafana Public

<> Code Issues 2.2k Pull requests 245 Discussions Actions Projects 9 Security 18 Insights

Alerting: Time of day restrictions #6592

Closed torkelo opened this issue on 16 Nov 2016 · 122 comments

 torkelo commented on 16 Nov 2016 Member ...

Time of day restrictions.

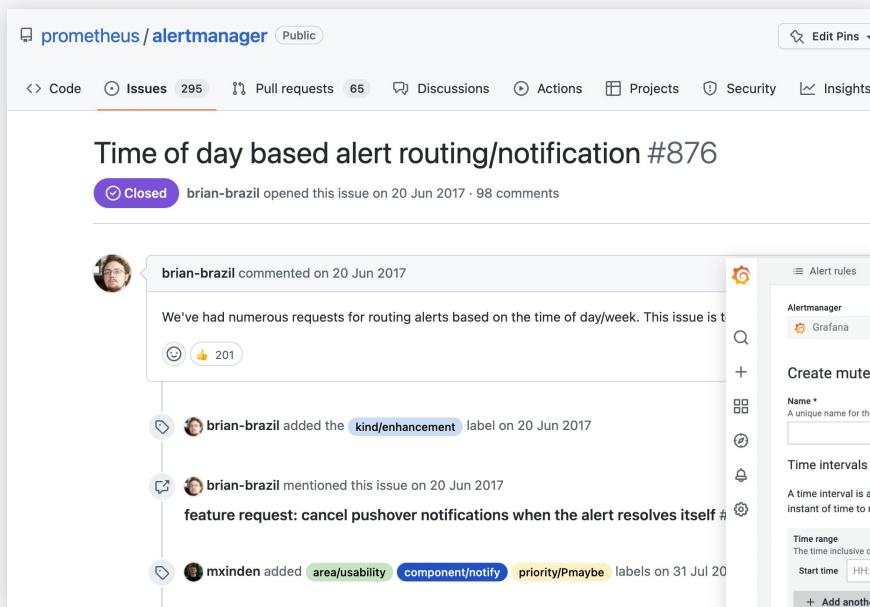
See two ways this could be implemented.

1. As an alert condition
2. As a filter on notifications

👍 525 👏 16 ❤️ 59 💬 29 👤 27

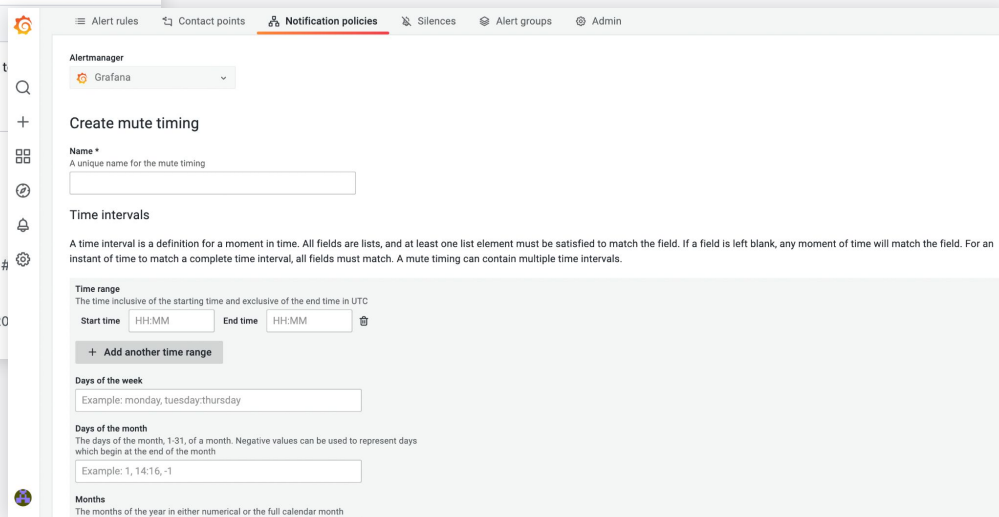
<https://github.com/grafana/grafana/issues/6592>





The screenshot shows a GitHub issue titled "Time of day based alert routing/notification #876" in the Prometheus/alertmanager repository. The issue is marked as "Closed" and was opened by brian-brazil on June 20, 2017, with 98 comments. The issue description states: "We've had numerous requests for routing alerts based on the time of day/week. This issue is t". The comment history shows brian-brazil adding the "kind/enhancement" label, mentioning the issue, and adding the feature request "cancel pushover notifications when the alert resolves itself #". mxinden added labels "area/usability", "component/notify", and "priority/Pmaybe" on July 31, 2017.

<https://github.com/prometheus/alertmanager/issues/876>



The screenshot shows the Grafana Mute Timing interface. The top navigation bar includes "Alert rules", "Contact points", "Notification policies" (which is active), "Silences", "Alert groups", and "Admin". The main content area is titled "Create mute timing" and includes a dropdown for "Alertmanager" (set to "Grafana"). The "Name" field is required and has a placeholder "A unique name for the mute timing". The "Time intervals" section explains that a time interval is a definition for a moment in time, where all fields are lists and at least one list element must be satisfied to match the field. It provides an example: "For an instant of time to match a complete time interval, all fields must match. A mute timing can contain multiple time intervals." The "Time range" section specifies that the time is inclusive of the starting time and exclusive of the end time in UTC, with input fields for "Start time" and "End time" in HH:MM format. Below this is a button to "Add another time range". The "Days of the week" section has a text input with the example "monday,tuesdaythursday". The "Days of the month" section explains that the days are of the month 1-31, with negative values for days before the 1st, and provides an example input "1, 14-16, -1". The "Months" section has a text input for the months of the year in numerical or full calendar month format.

Grafana's Mute Timing interface

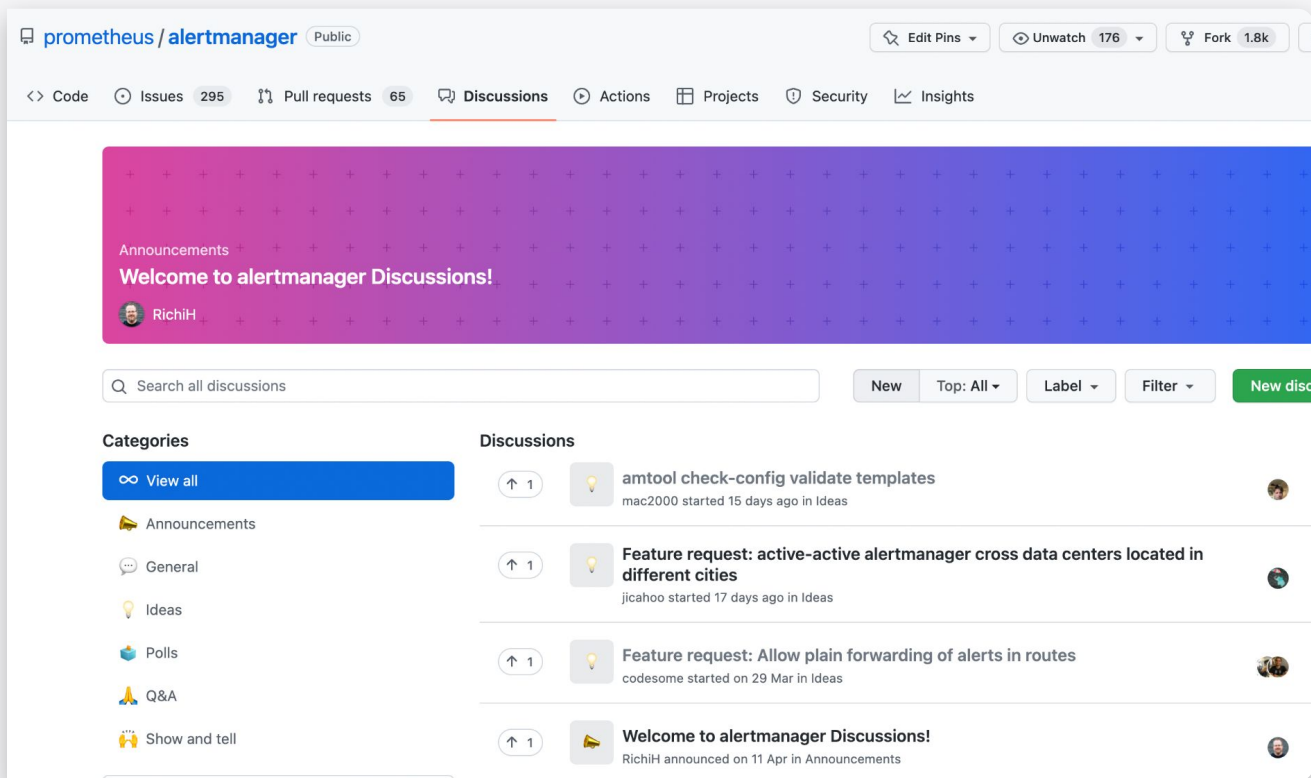






Future

Feedback



The screenshot shows the GitHub Discussions page for the Prometheus/alertmanager repository. The repository is public and has 176 unwatchers and 1.8k forks. The Discussions tab is selected, showing a welcome message from RichiH and a list of discussions.

Repository: prometheus / alertmanager (Public)

Navigation: Code, Issues (295), Pull requests (65), Discussions (selected), Actions, Projects, Security, Insights

Actions: Edit Pins, Unwatch (176), Fork (1.8k)

Welcome to alertmanager Discussions!

Search: Search all discussions

Filters: New, Top: All, Label, Filter, New disc

Categories:

- View all
- Announcements
- General
- Ideas
- Polls
- Q&A
- Show and tell

Discussions:

- amttool check-config validate templates**
mac2000 started 15 days ago in Ideas
- Feature request: active-active alertmanager cross data centers located in different cities**
jicahoo started 17 days ago in Ideas
- Feature request: Allow plain forwarding of alerts in routes**
codesome started on 29 Mar in Ideas
- Welcome to alertmanager Discussions!**
RichiH announced on 11 Apr in Announcements



Testing Receivers

Test contact point [X]

Notification message

You will send a test notification that uses the annotations defined below. This is a good option if you use custom templates and messages.

Summary and annotations

severity	critical	[X]
Summary	An alert that's firing.	[X]

Custom Labels

Labels	namespace	=	us-central1	[X]
--------	-----------	---	-------------	-----



Alert Pipeline Insights

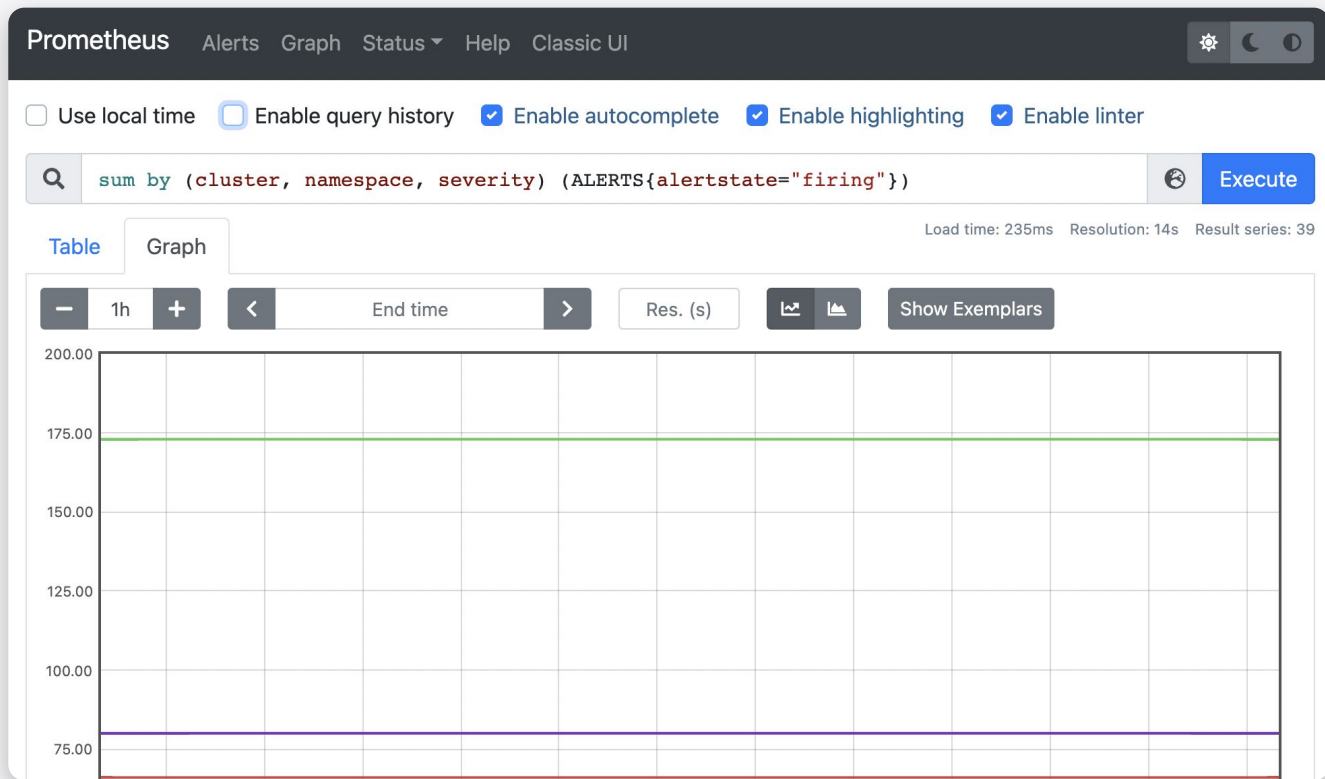
Prometheus Alerts Graph Status ▾ Help Classic UI

Rules

alerts				3.470s ago	1.390ms
Rule	State	Error	Last Evaluation	Evaluation Time	
alert: AlwaysFiring expr: vector(1) > 0 labels: __alert_rule_uid__: 1	OK		3.475s ago	0.668ms	
alert: UpZero expr: up == 0	OK		3.475s ago	0.240ms	
alert: VectorZero expr: vector(0) == 0	OK		3.475s ago	0.128ms	
alert: Oscillating expr: (minute() % 4) * 5 >= 5 labels:	OK		3.475s ago	0.332ms	



Like Prometheus but for Alerts





Thank you  !