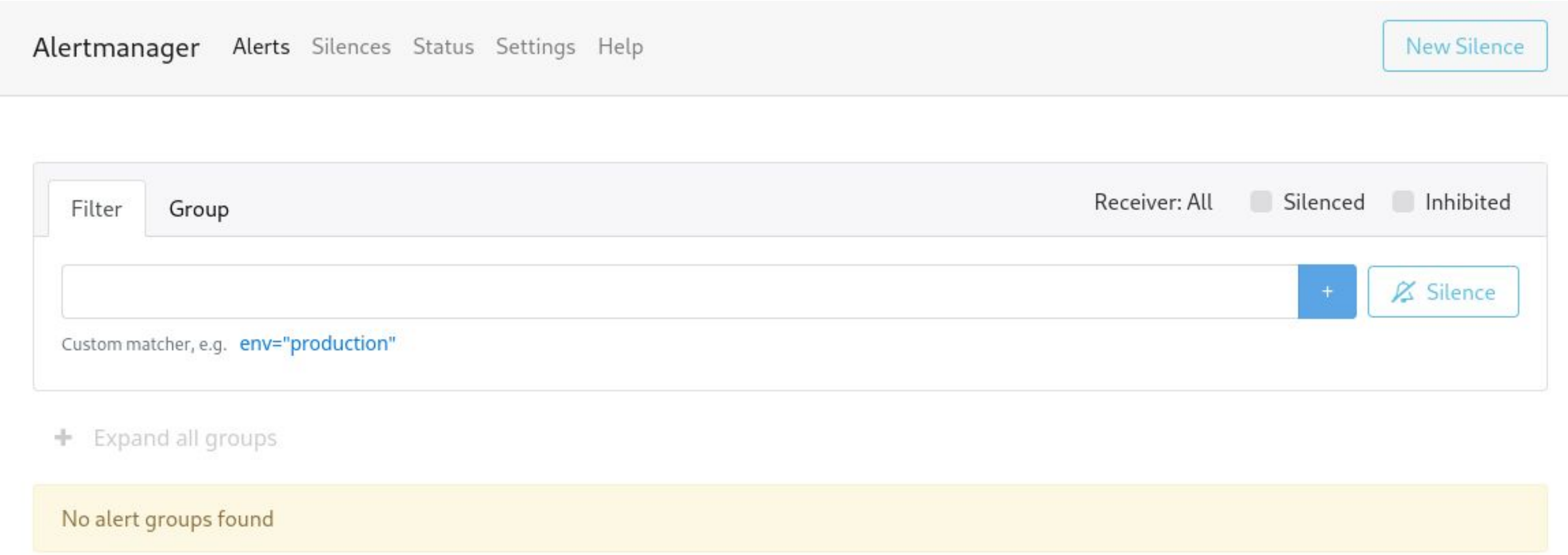
Kiora: A less opinionated Alertmanager

Colin Douch, Observability @ Cloudflare



No alert groups found

Alertmanager is **hard**

Let’s talk about that

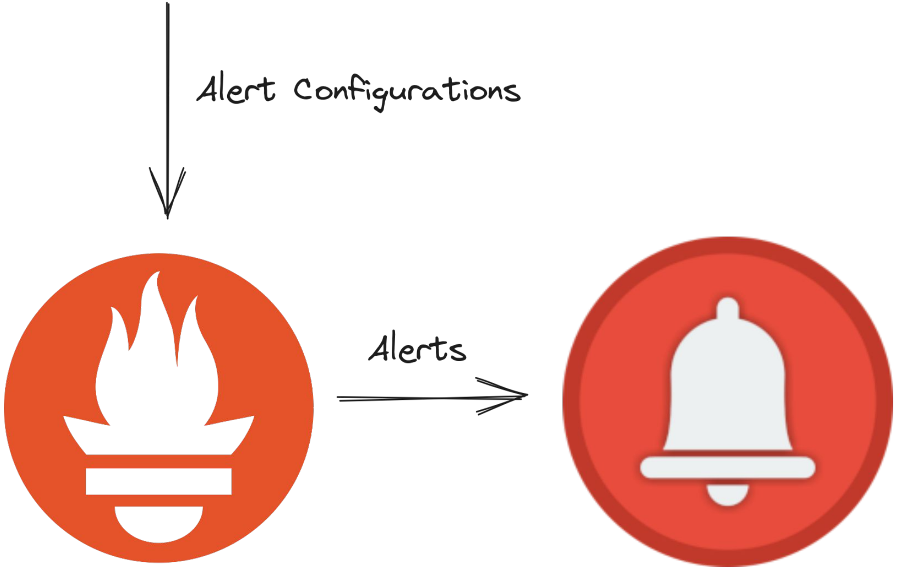
A Quick Introduction

Hi! I’m Colin

Observability Lead @ Cloudflare

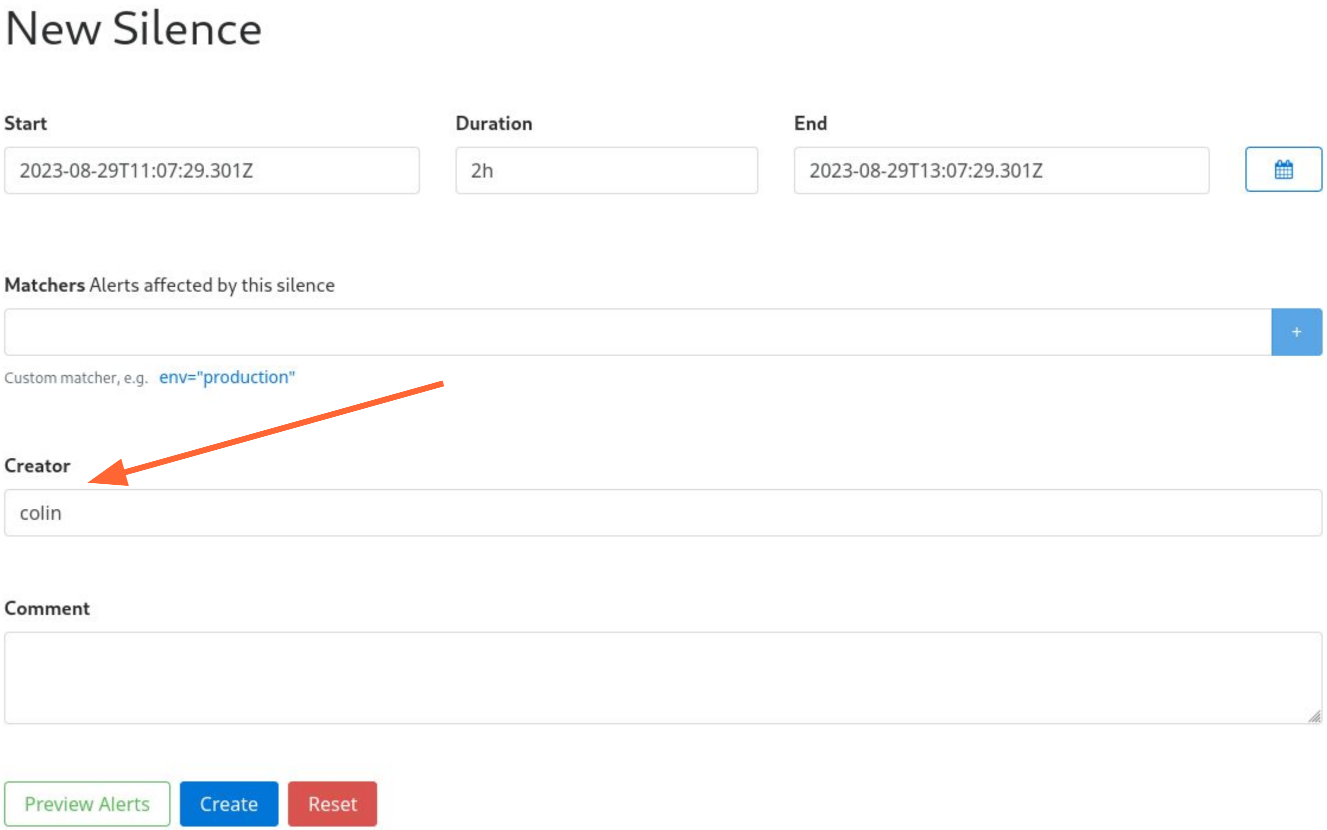
Has bad opinions

Not British



Alertmanager is **simple,** ***right?***

Let's start with **Silences**



New Silence

Start: 2023-08-29T11:07:29.301Z

Duration: 2h

End: 2023-08-29T13:07:29.301Z

Matchers Alerts affected by this silence

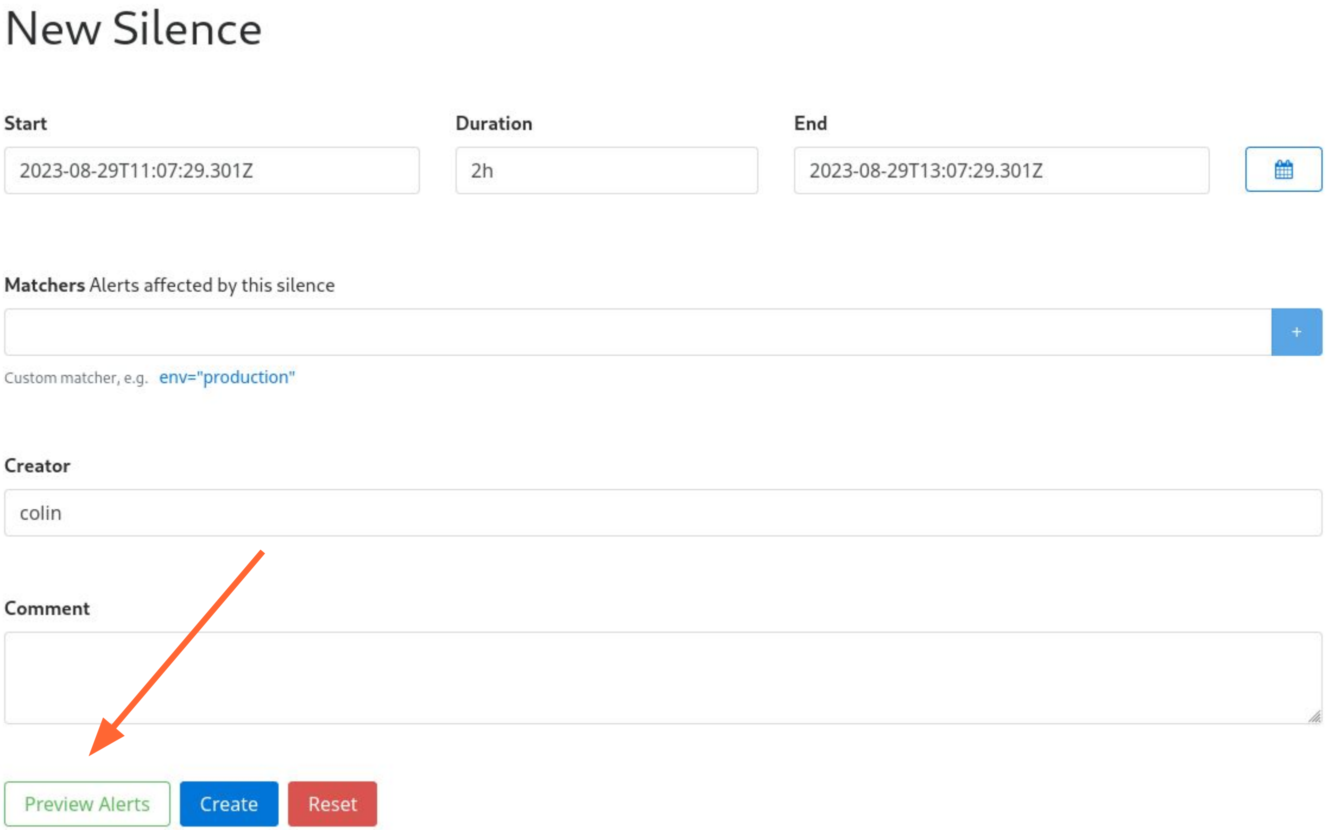
Custom matcher, e.g. env="production"

Creator: colin

Comment:

What if we just *didn’t*

```
amtool silence add -c 'cd@cloudflare.com' -d 8h instance="$instance"
amtool silence add -c 'cd@cloudflare.com' -d 8h instance="$instance"
```



New Silence

Start 2023-08-29T11:07:29.301Z

Duration 2h

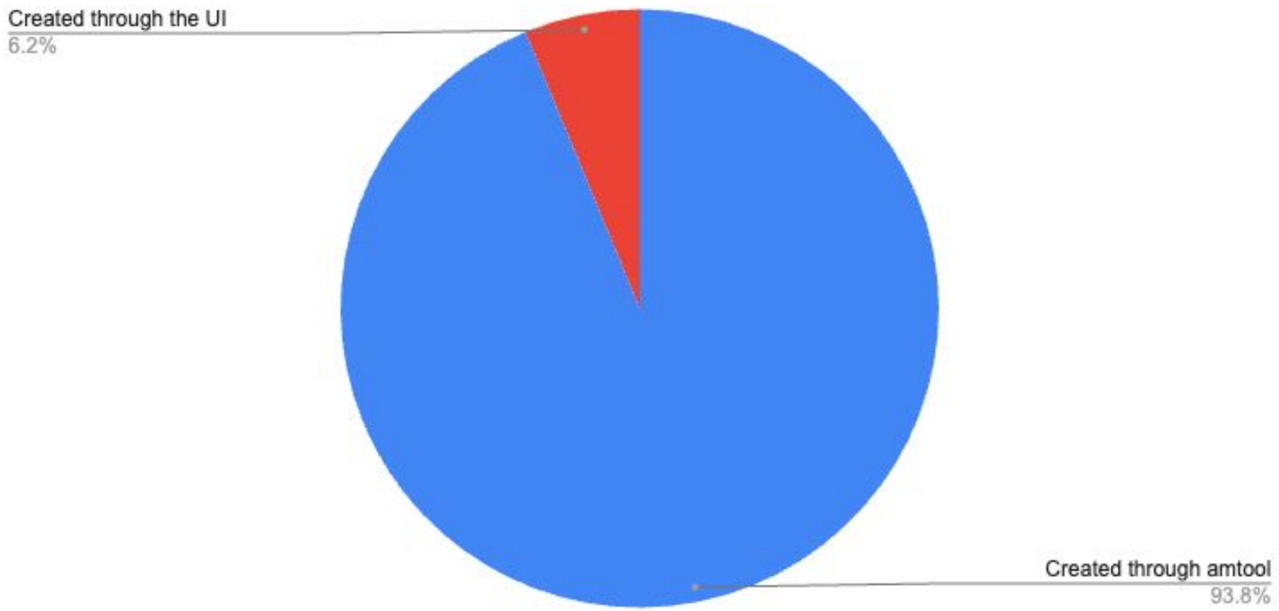
End 2023-08-29T13:07:29.301Z

Matchers Alerts affected by this silence

Custom matcher, e.g. env="production"

Creator colin

Comment

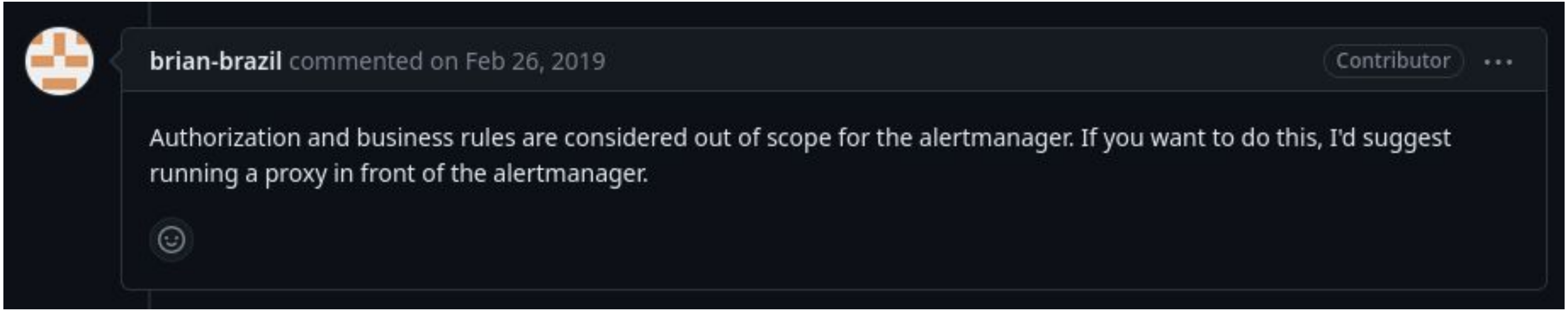

Created through the UI
6.2%
Created through amtool
93.8%

Let’s talk about **alerts**

We lint our alerts:

https://github.com/cloudflare/pint

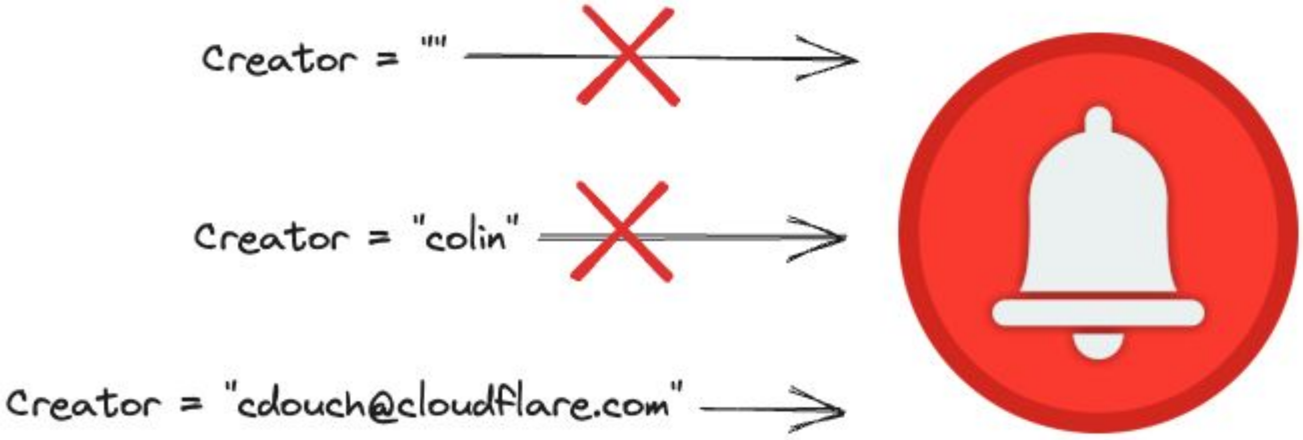
But what does **“Bad”** mean?

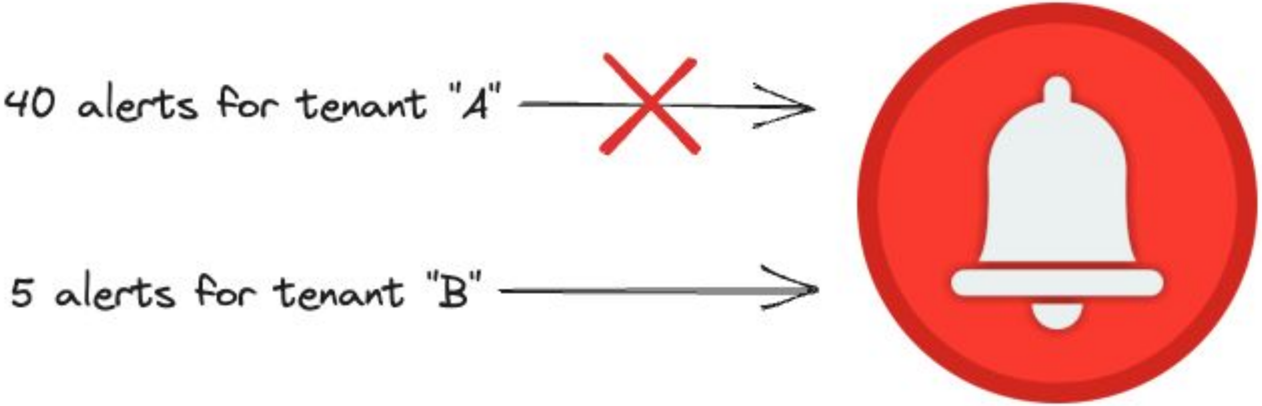


brian-brazil commented on Feb 26, 2019

Authorization and business rules are considered out of scope for the alertmanager. If you want to do this, I'd suggest running a proxy in front of the alertmanager.

https://github.com/prometheus/alertmanager/issues/1769 https://github.com/sinkingpoint/alertmanager_bouncer


Creator = ""
Creator = "colin"
Creator = "cdouch@cloudflare.com"

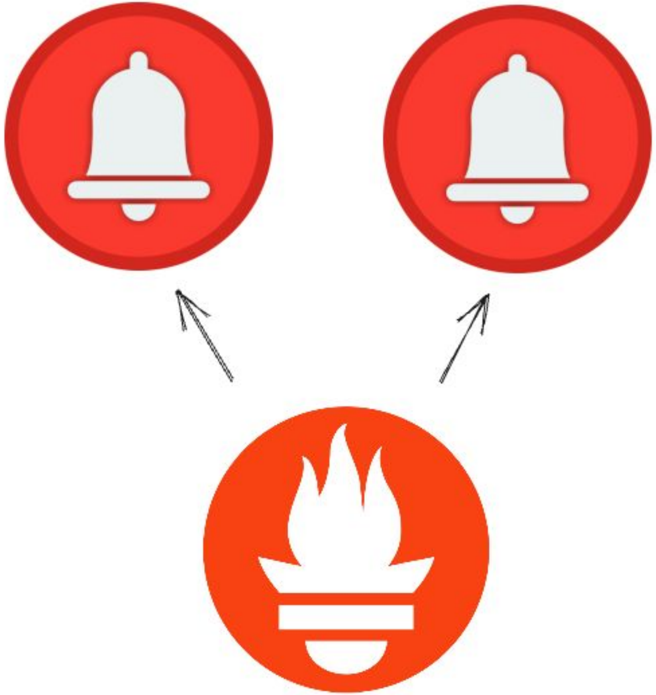

40 alerts for tenant "A"
5 alerts for tenant "B"

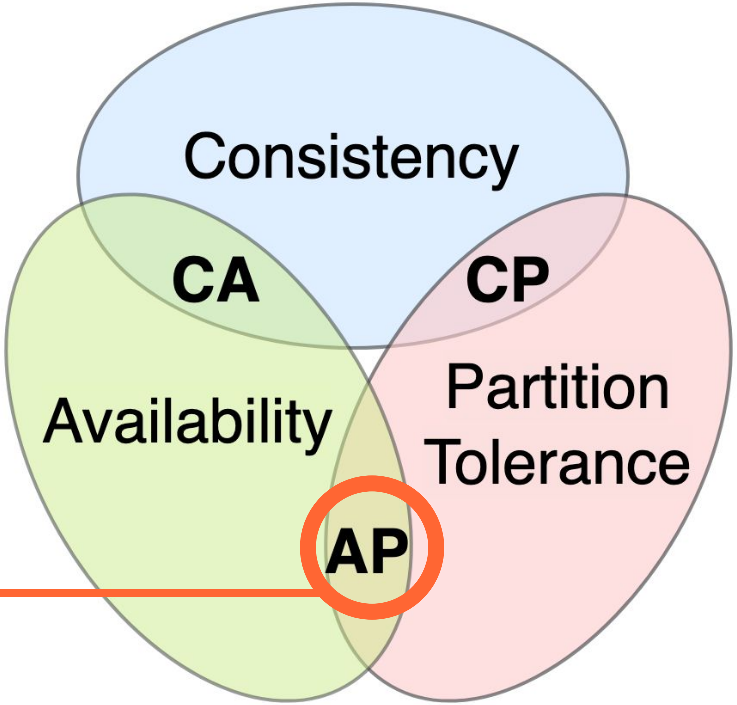
This works quite well!

But ...

1. Send your alerts to two Alertmanagers

2. Done





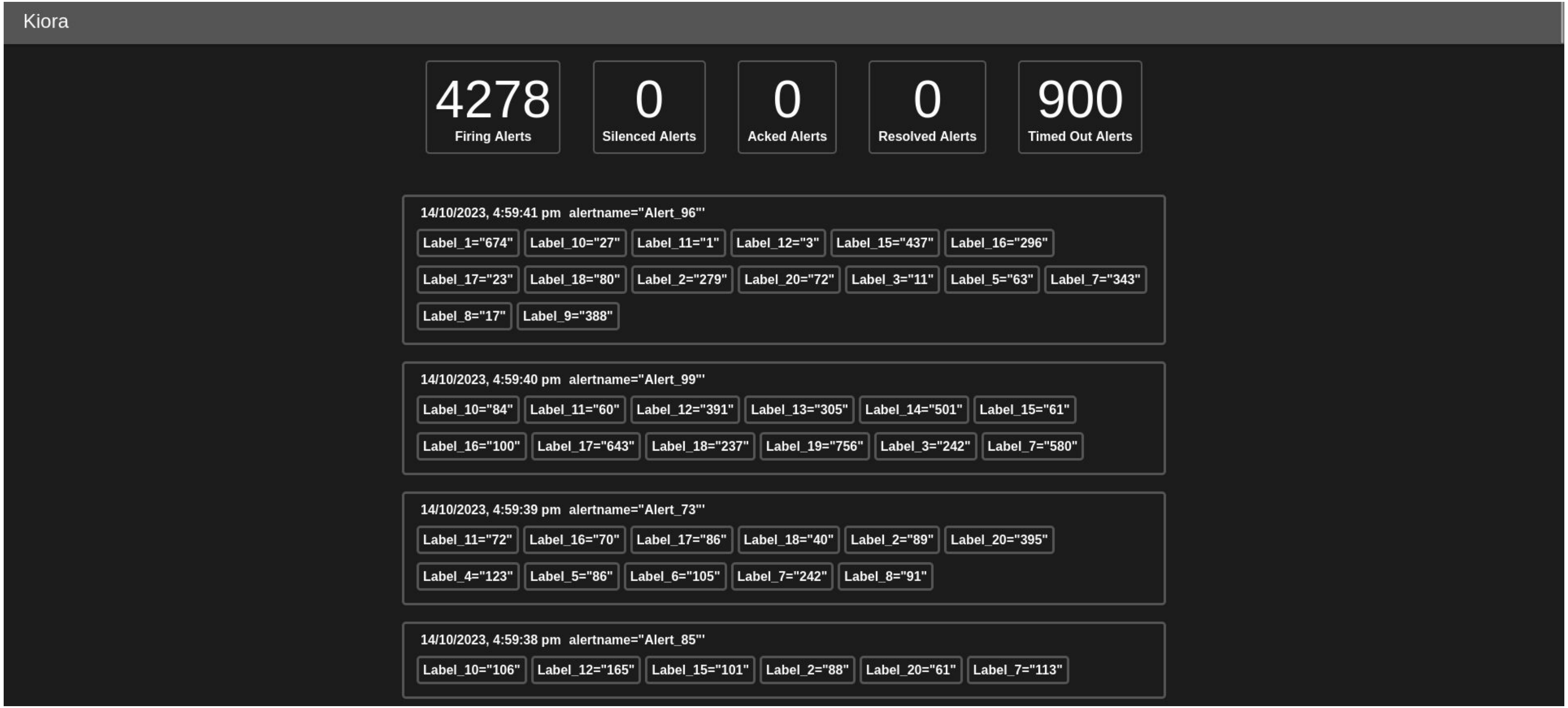
Alertmanager

Why didn’t my alert fire?

Why *did* my alert take so long to fire?

Why *did* my alert fire?

👋 Kiora 👋



Kiora

4278 Firing Alerts

0 Silenced Alerts

0 Acked Alerts

0 Resolved Alerts

900 Timed Out Alerts

14/10/2023, 4:59:41 pm alertname="Alert_96"'

Label_1="674" Label_10="27" Label_11="1" Label_12="3" Label_15="437" Label_16="296"
Label_17="23" Label_18="80" Label_2="279" Label_20="72" Label_3="11" Label_5="63" Label_7="343"
Label_8="17" Label_9="388"

14/10/2023, 4:59:40 pm alertname="Alert_99"'

Label_10="84" Label_11="60" Label_12="391" Label_13="305" Label_14="501" Label_15="61"
Label_16="100" Label_17="643" Label_18="237" Label_19="756" Label_3="242" Label_7="580"

14/10/2023, 4:59:39 pm alertname="Alert_73"'

Label_11="72" Label_16="70" Label_17="86" Label_18="40" Label_2="89" Label_20="395"
Label_4="123" Label_5="86" Label_6="105" Label_7="242" Label_8="91"

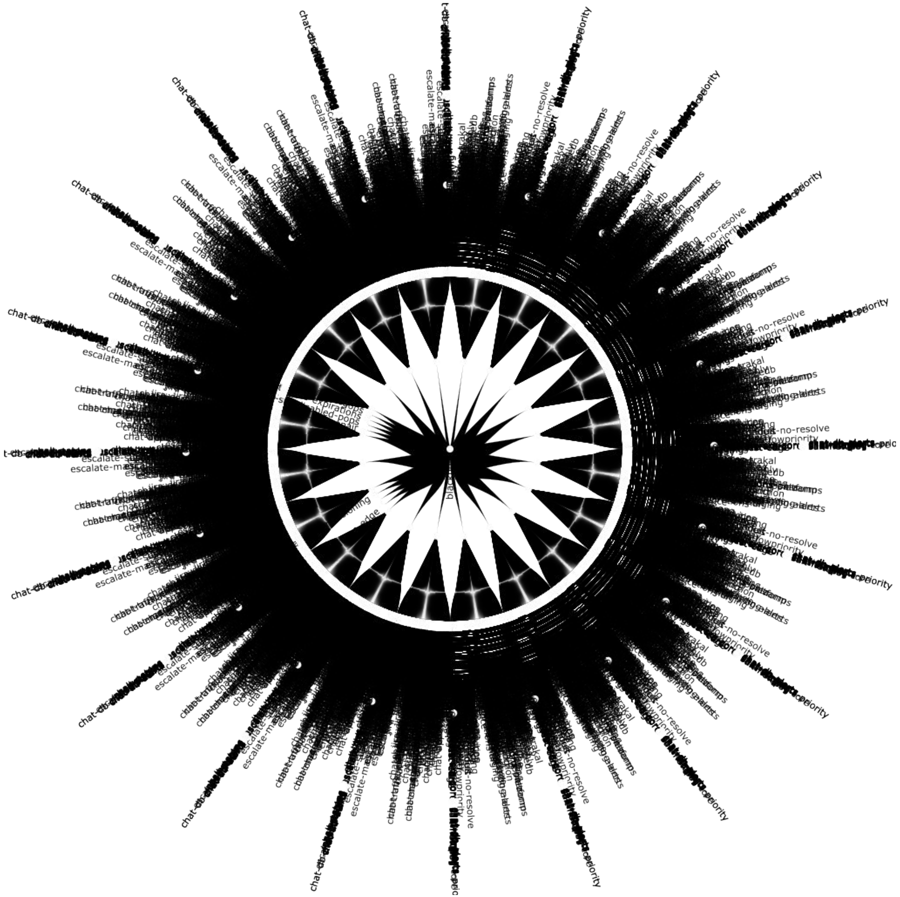
14/10/2023, 4:59:38 pm alertname="Alert_85"'

Label_10="106" Label_12="165" Label_15="101" Label_2="88" Label_20="61" Label_7="113"

⚠️ But: Some Caveats ⚠️

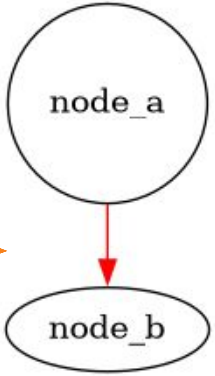
👋

https://github.com/sinkingpoint/kiora/


chat-db
escalate-master
escalate-
chat
-no-resolve
lowpriority
priority
trakal
edb
expirations
blackbox

```
digraph {
  node_a [shape="circle"];
  node_b;

  node_a -> node_b [color=”red”];
}
```

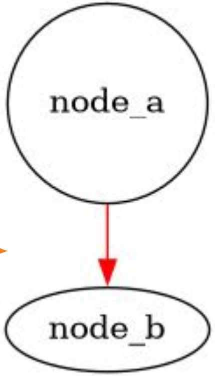
```
dot -Tpng test.dot > out.png
```



Attributes!

```
digraph {
  node_a [shape="circle"];
  node_b;

  node_a -> node_b [color=”red”];
}
```

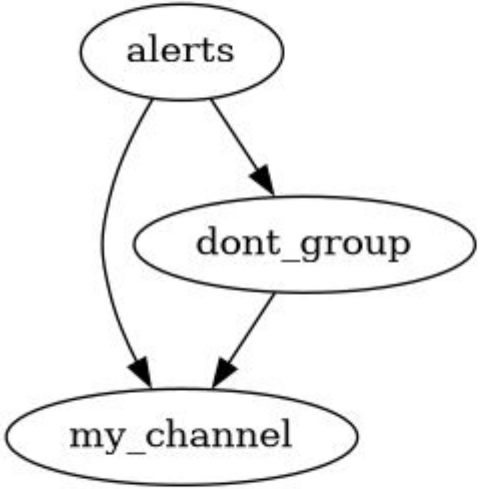
```
dot -Tpng test.dot > out.png
```



```
digraph {
  my_channel [type="slack" api_url="https://hooks.slack.com/services/x/x"];

  alerts -> my_channel;
}
```

```
digraph {
  my_channel [type="slack" api_url="https://hooks.slack.com/services/x/x"];

  alerts -> my_channel [type="regex" field="dest" regex=".*slack.*"];
}
```

```
digraph {
  my_channel [type="slack" api_url="https://hooks.slack.com/services/x/x"];
  dont_group [type="group_wait" duration="0s"];

  alerts -> dont_group [type="regex" field="grouping" regex=".*none.*"];
  dont_group -> my_channel [type="regex" field="dest" regex=".*slack.*"];
  alerts -> my_channel [type="regex" field="dest" regex=".*slack.*"];
}
```


alerts
dont_group
my_channel

```
digraph config {
    longer_than_one_shift -> test_ticket [type="duration" field="duration" min="8h"];

     // If they're longer than 8h, enforce a JIRA ticket.
    test_ticket -> silences [type="regex" field="comment" regex="[A-Z]+-[0-9]+"];

    // Alternatively, if they're a maximum of 8h long, let them through.
    short_silences -> silences [type="duration" field="duration" max="8h"];
}
```

But that’s **not interesting**

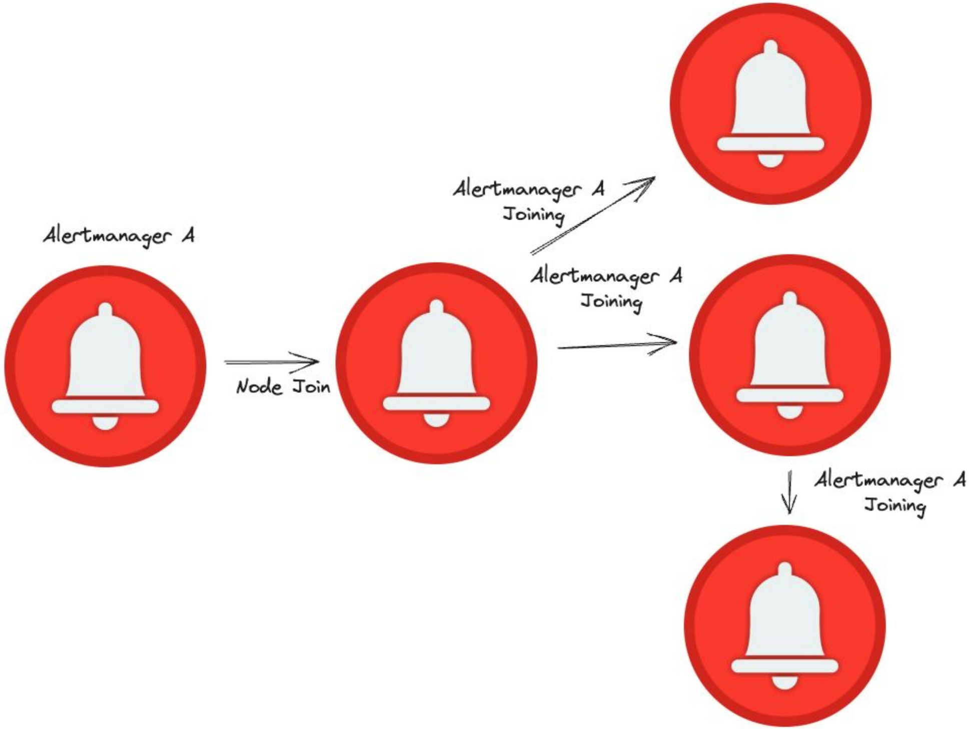
¯\_(ツ)_/¯

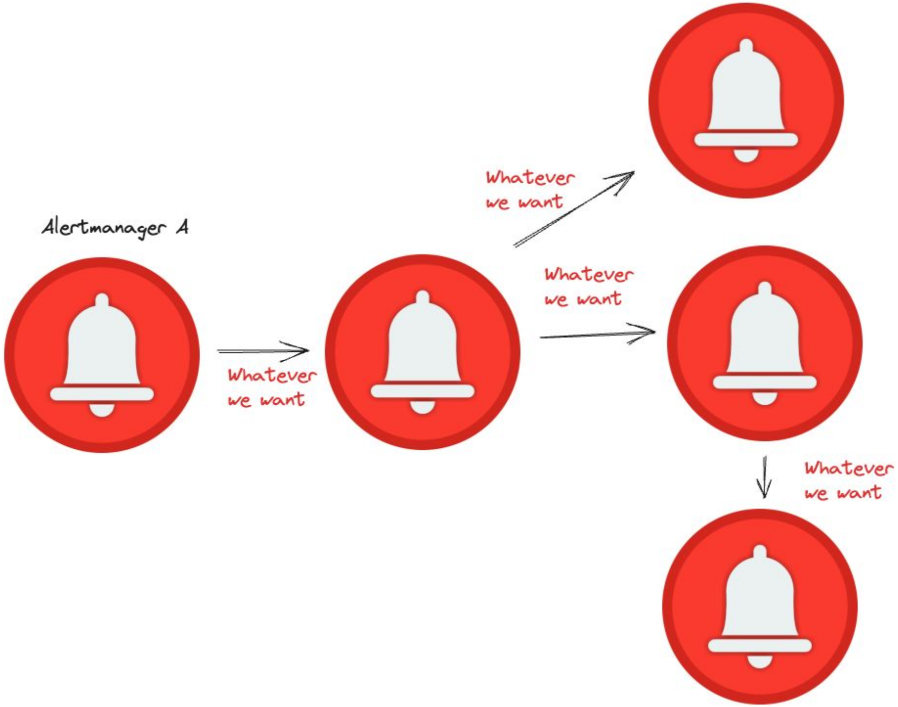
https://github.com/hashicorp/memberlist

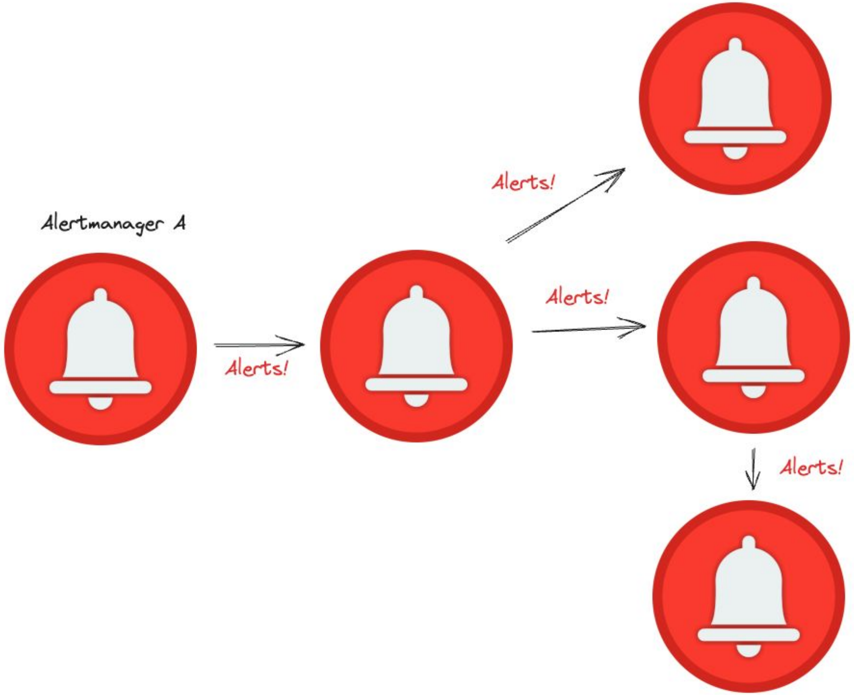
🤝

https://github.com/hashicorp/serf

Serf

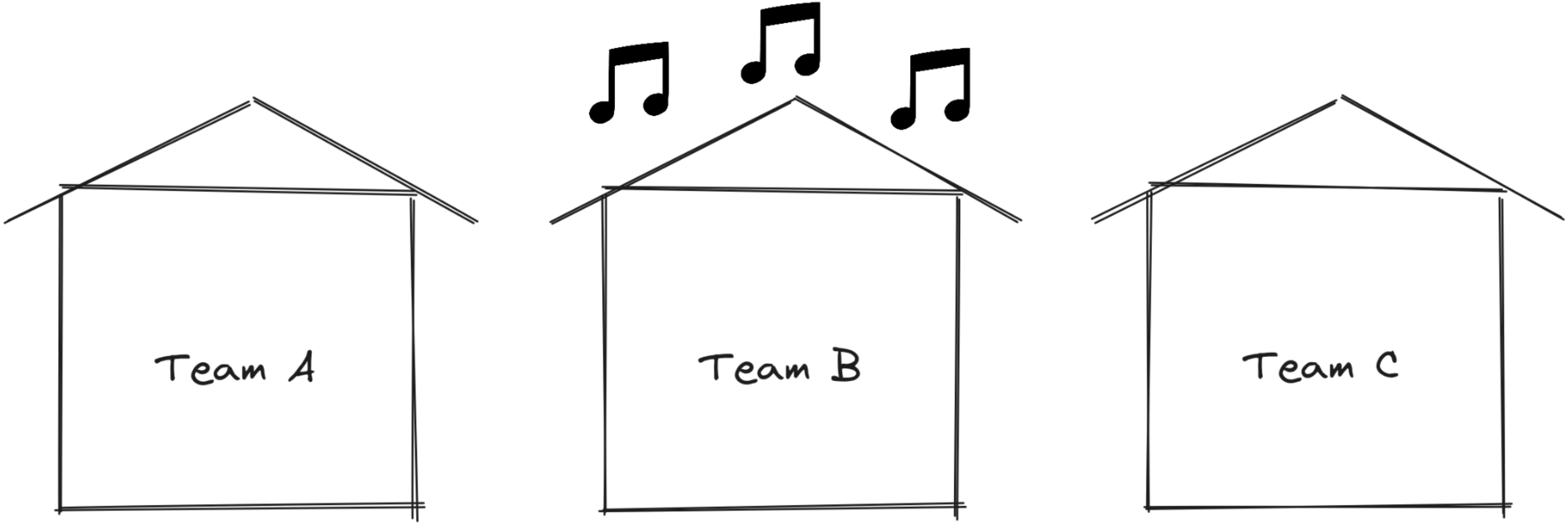

Alertmanager A
Node Join
Alertmanager A
Joining
Alertmanager A
Joining
Alertmanager A
Joining


Alertmanager A
Whatever we want
Whatever we want
Whatever we want
Whatever we want


Alertmanager A
Alerts!
Alerts!
Alerts!
Alerts!

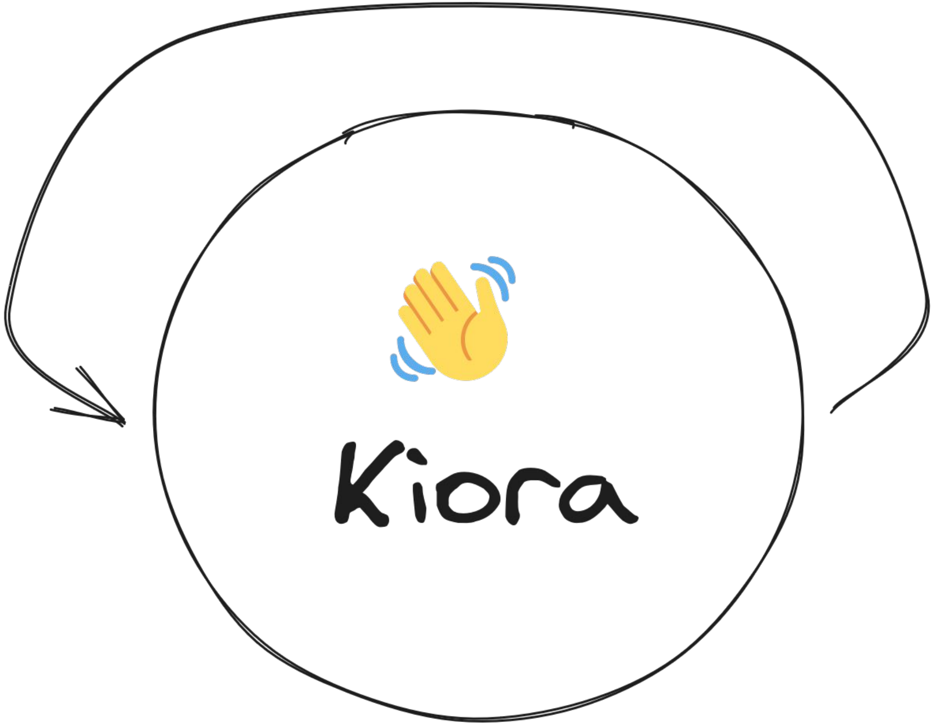
Serf does a full state sync over TCP periodically.

https://www.serf.io/docs/internals/gossip.html


Team A
Team B
Team C

```
digraph {
    tenant_key = "{{ .team }}";
    // Ratelimit alerts to 300 per 30 seconds per tenant.
    ratelimit -> alerts [type="ratelimit" rate="300" interval="30s"];
}
```

Kiora acts as its own Client



Which brings us back to

✨ **Meta Observability** ✨

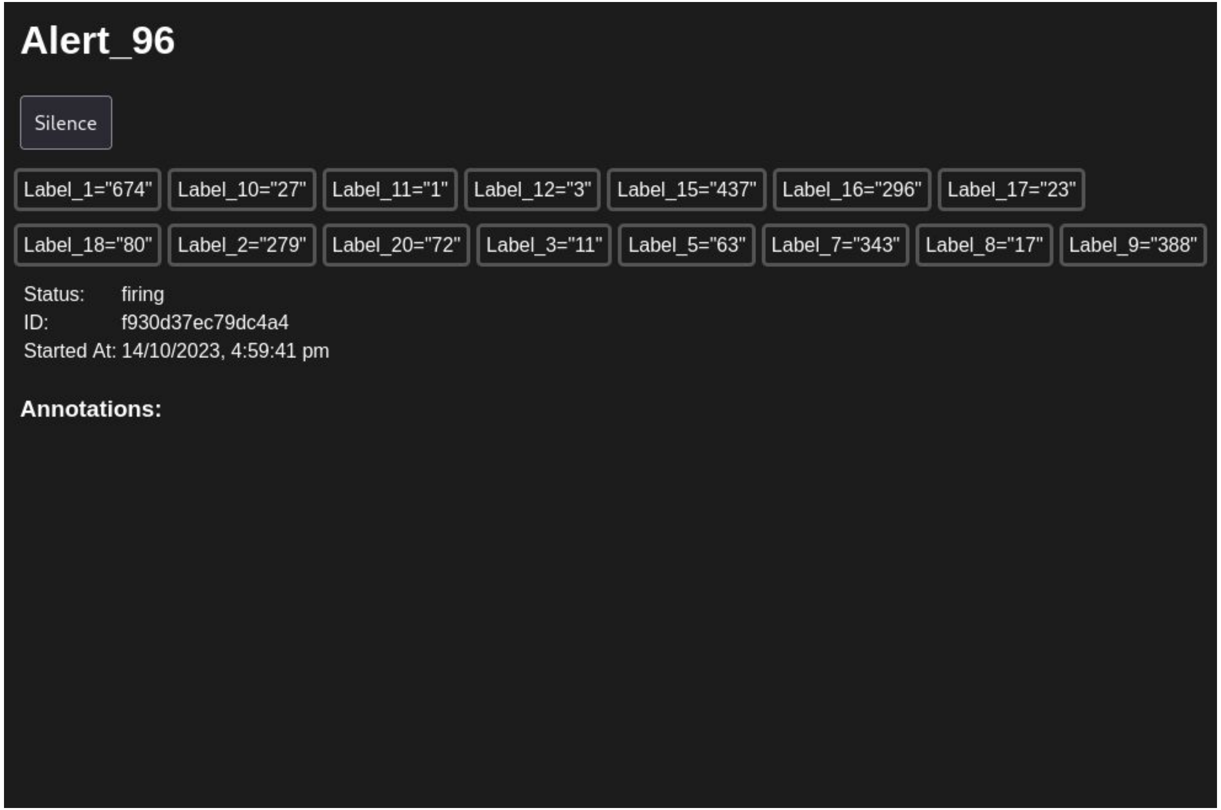
Is anyone actually working on this alert?

```
digraph config {
  test_email -> acks [type="regex" field="creator" regex=".+@cloudflare.com"];
}
```

Why didn’t my alert fire?

Why *did* my alert take so long to fire?

Why *did* my alert fire?



Alert_96

Label_1="674" Label_10="27" Label_11="1" Label_12="3" Label_15="437" Label_16="296" Label_17="23"

Label_18="80" Label_2="279" Label_20="72" Label_3="11" Label_5="63" Label_7="343" Label_8="17" Label_9="388"

Status: firing
ID: f930d37ec79dc4a4
Started At: 14/10/2023, 4:59:41 pm

Annotations:

Thanks!

Slides ^