LogQL in 5 minutes

Cyril Tovena

Grafana Labs

What is LogQL ?

What is LogQL ?

- Language to query logs from Loki.
- Heavily inspired by PromQL.
- Distributed grep.

Selecting time series with PromQL

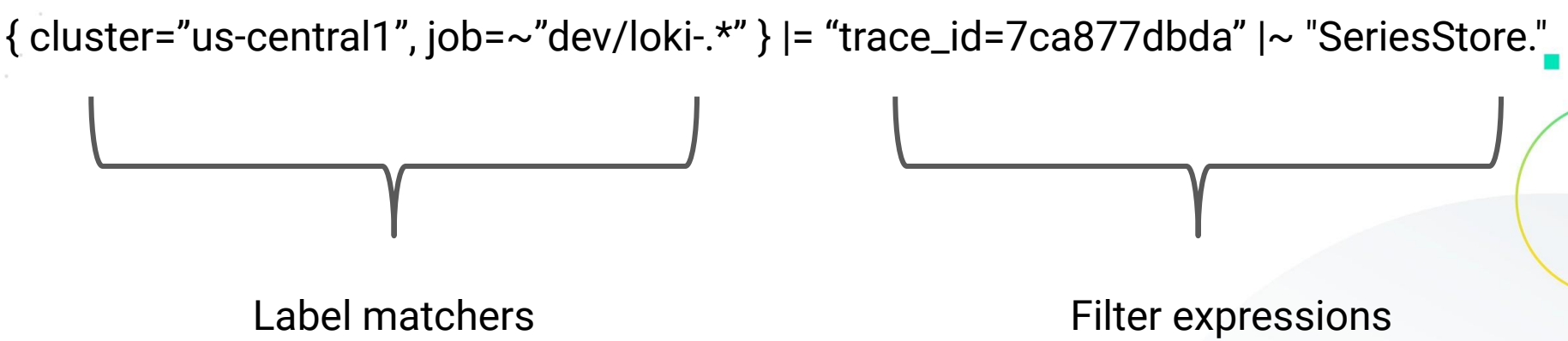
http_request_duration_seconds_count{ cluster=”us-central1”, job=~”dev/loki-.*” }

Metric name

Label matchers

Selecting log streams with LogQL

Log stream selector:



Filter expressions

- |= Log line contains string.
- != Log line does not contain string.
- |~ Log line matches regular expression.
- !~ Log line does not match regular expression.

Counting logs with Range Vectors

rate({ cluster=”us-central1” } |~ “error: .*" **[5m]**)

count_over_time({ cluster=”us-central1” } |= “org_id=5842" **[1m]**)

Vector aggregations

```
sum by(job, instance) ( rate({ cluster=”us-central1” } |= “error" [5m]) )

topk(5, count_over_time({ cluster=”us-central1” } |= “error" [5m]) )
```

sum, min, max, topk, bottomk, avg , etc..

Demo

LogQL Future

- Improve query performance.
- Alert and rules evaluation.
- Extracting metrics.
- Log transformation (JSON, Logfmt, ..).

Thank you !

Questions ?

https://grafana.slack.com/

Range Vec.. what ?

/api/v1/query_range?query=count_over_time({app="foo"}**[10s]**)
&start=**10**
&end=**70**
&step=**20s**