



# Grafana Loki: *Like Prometheus, but for logs.*

Tom Wilkie, May 2019



## **Tom Wilkie** *VP Product, Grafana Labs*

Previously: *Kausal, Weaveworks, Google, Acunu, Xensource Prometheus & Cortex maintainer, mixins authors etc*

Twitter: [@tom\\_wilkie](https://twitter.com/tom_wilkie) Email: [tom@grafana.com](mailto:tom@grafana.com)

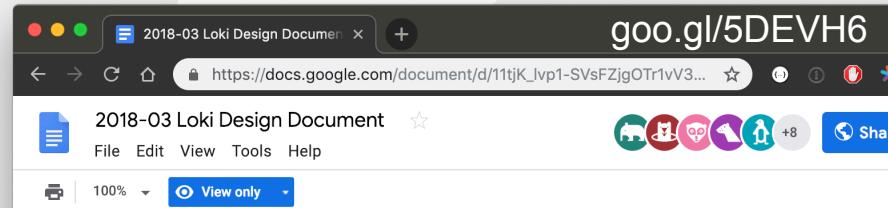




*Loki is a horizontally-scalable, highly-available, multi-tenant log aggregation system inspired by Prometheus.*

- 03/18 Project started
- 12/18 Launched at KubeCon US
- 12/18 #1 on HN for ~12hrs!
- 02/19 FOSDEM talk
- 03/19 Labels from logs
- 04/19 Lazy Queries; LogQL filtering
- 05/19 KubeCon EU: context, live tailing

<https://github.com/grafana/loki>



## Loki: like Prometheus, but for logs.

*Design Document*

Tom Wilkie & David Kaltschmidt, March 2018

This document aims to explain the motivations for, and design of, the Grafana Loki service. This document does not attempt to describe in depth every possible detail of the design, but hopefully explains the key points and should allow us to spot any obvious mistakes ahead of time.

This document aims to answer questions not only about how we're going to build this, but also why we're building it, what it will be used for, and who will be using it.

Background & Motivations

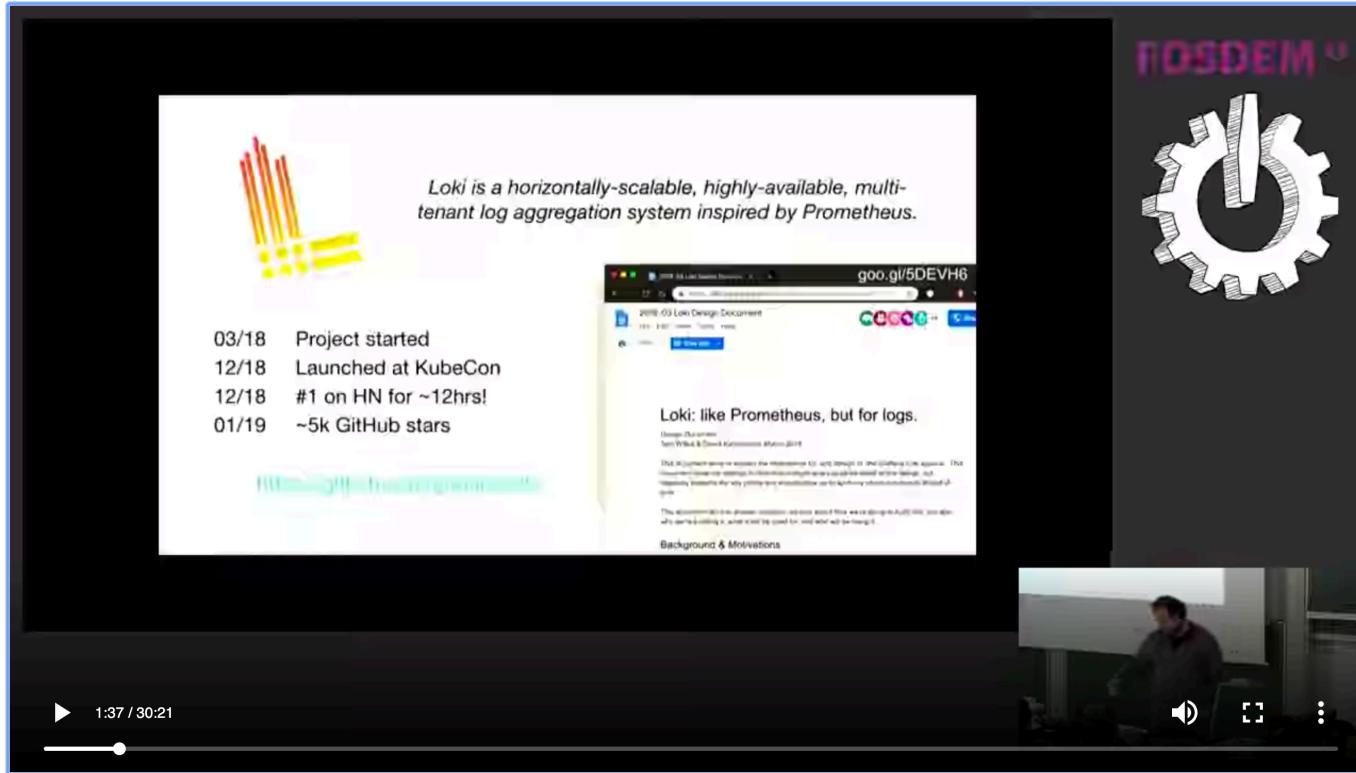
Intro

FOSDEM summary

What's New...

What's Next?

Demo



[https://fosdem.org/2019/schedule/event/loki\\_prometheus\\_for\\_logs/](https://fosdem.org/2019/schedule/event/loki_prometheus_for_logs/)

- #0 Simple and cost effective to operate
- #1 Integrated with existing observability tools
- #2 Cloud Native and Airplane Mode

*Loki doesn't index the text of the logs, instead grouping entries into "streams" and indexing those with labels.*

```
{job="frontend", env="dev"} => {  
    time: "2018-01-31 15:41:04",  
    line: "POST /api/prom/push HTTP/1.1 502 0"  
}
```

#0 Simple to scale



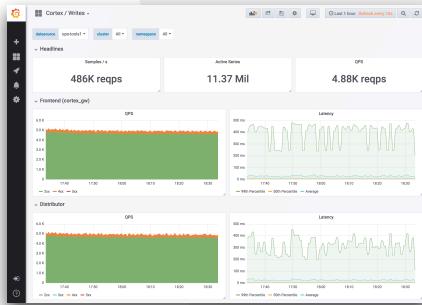
## 1. Alert

 The Watchmen APP 5:48 PM  
[FIRING:3] **CFRoutesTooLow** (cf router pcf-dev  
10.130.7.229:9186 pcf-dev-firehose codelab-monitor  
gorouter)  
The number of routes in the router's routing table is  
dangerously low: 113

---

 The Watchmen APP 5:54 PM  
[RESOLVED] **CFRoutesTooLow** (cf router pcf-dev  
10.130.7.229:9186 pcf-dev-firehose codelab-monitor  
gorouter)  
The number of routes in the router's routing table is  
dangerously low: 113

## 2. Dashboard

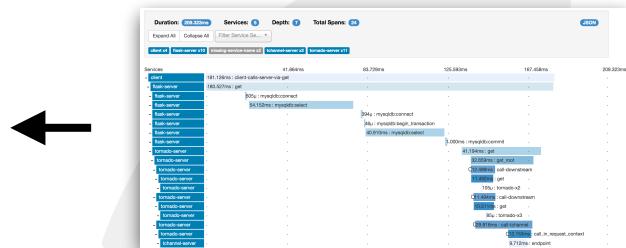


### 3. Adhoc Query

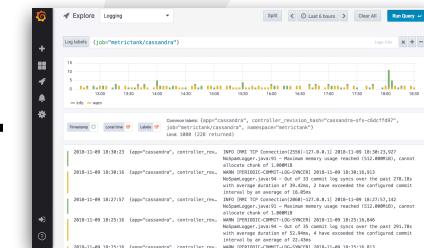


Fix!

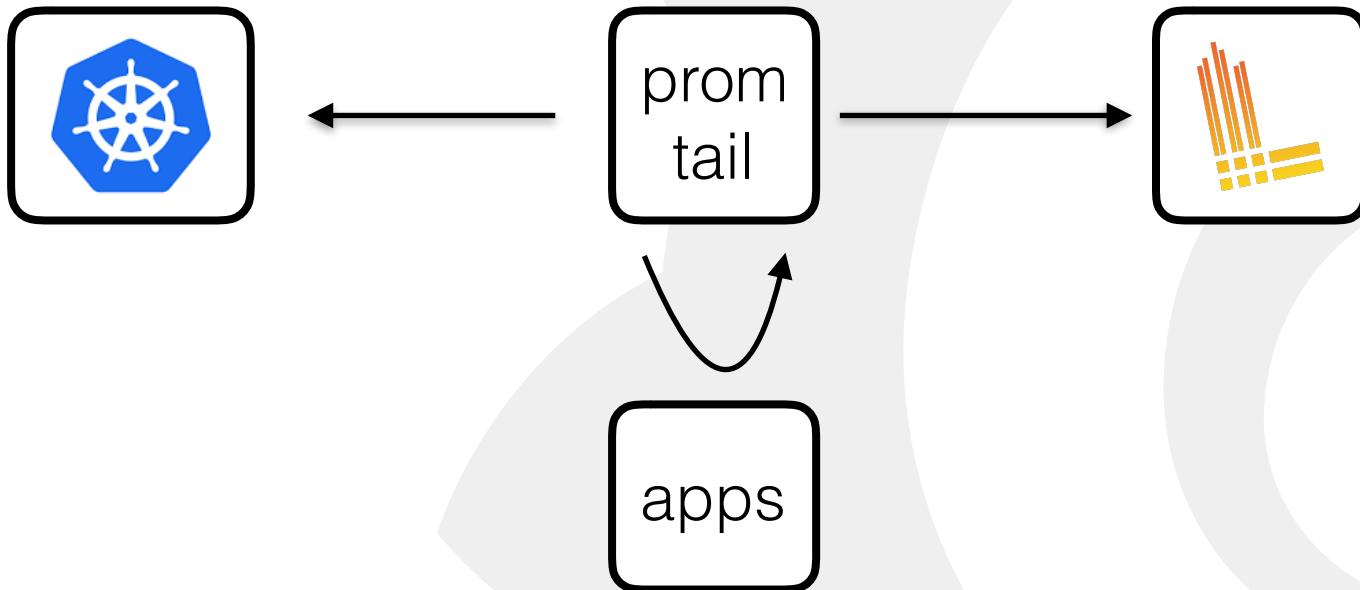
## 5. Distributed Tracing



## 4. Log Aggregation

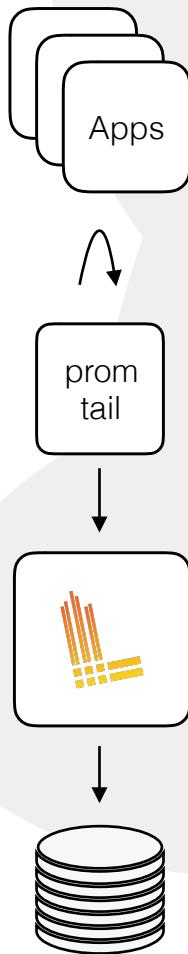


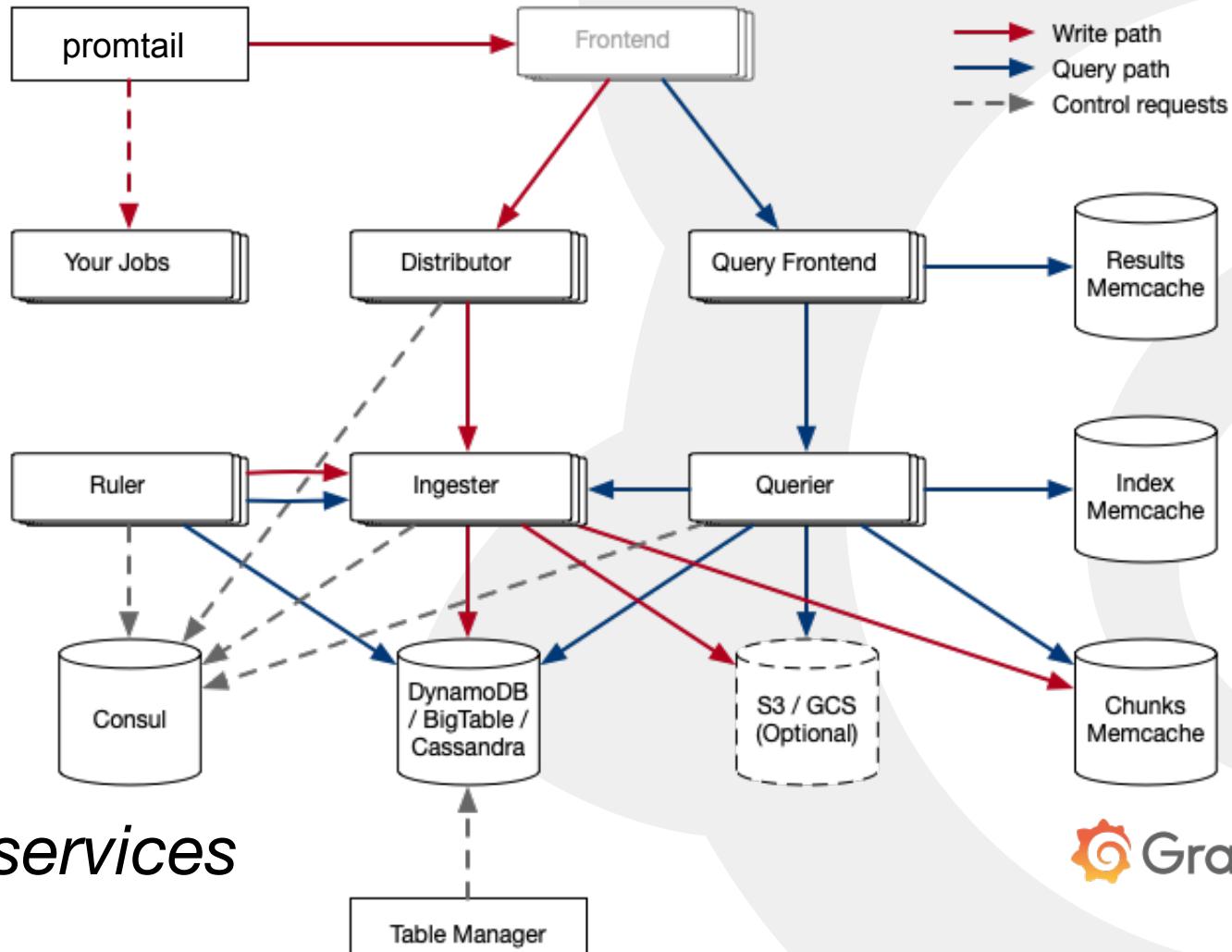
## #1 *Integrated*



#1 Integrated

## #3 Airplane Mode





# Microservices

Grafana Labs

- #0 Simple and cost effective to operate
- #1 Integrated with existing observability tools
- #2 Airplane Mode and Cloud Native

# *Whats new?*

## LogQL Filter Chaining:

```
{job="app"} |= "/foo" !~ "/foo/bar"
```

## Extracting Labels from Logs

## Live Tailing, Context

## Much more

# *Demo*

# *Whats next?*

```
rate(({"job="app"} |= "/foo" !~ "/foo/bar") [1m])  
extract_label({job="default/nginx"}, "code=(\d+)"  
  |> {code ~= "5.."})  
sum(extract_value({job="app"}, "code=(\d+)", "$1"))
```

## *LogQL Aggregations*

*Add alerts & rules using aggregations*

*Signature chaining for verifiability*

*Removing dependancy on NOSQL*

*Launch first beta in ~now*

# *Thanks! Questions?*