



Log Monitoring with Grafana/Loki



Didiet A. Pambudiono
DevOps Engineer



OICNDI

November 7th 2020

vmware®

boer
technology

onf



About Me

- 
- **DevOps Engineer PT. Gits Indonesia**
 - **Member of openSUSE Project**
 - **Cloud Enthusiast**
 - **Just another linux user**
 - **Addicted to Coffee**
 - **Contact me :**
 - **didiet@gits.id**
 - **pambudiono@opensuse.org**
 - **More about me :**
 - **<https://www.linkedin.com/in/didiet-a-pambudiono/>**
 - **<https://medium.com/@sitidy>**

Background

Log monitoring system

Alternate for Elasticsearch Logstash and Kibana Stack



Last Year's Event

- Simple Log Monitoring with Prometheus and Grafana
 - [Presentation Link](#)

Let's talk about Loki

Sponsored by:




OICNDI

November 7th 2020





About Loki

- 
- **Loki is a horizontally scalable, highly available, multi-tenant log aggregation system inspired by Prometheus.**
 - **It is designed to be very cost-effective and easy to operate. It does not index the contents of the logs, but rather a set of labels for each log stream.**
 - **The Loki project was started at Grafana Labs in 2018 and announced at KubeCon Seattle.**
 - **Loki, which is released under the Apache 2.0 License, reached GA with v1.0.0 in November 2019.**



Traditional log management tools

Hard to operate at scale

Expensive

Doesn't correlate well with Prometheus metrics

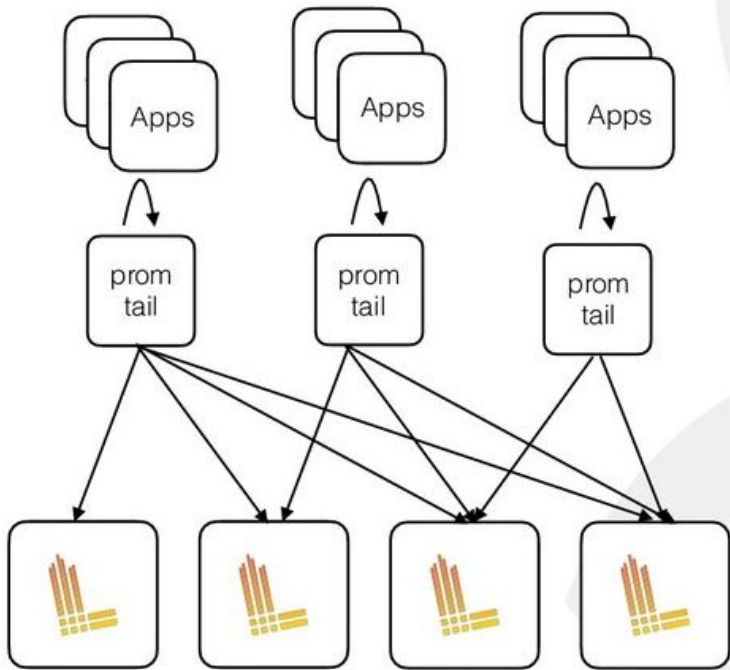




Loki

- does not do full-text indexing on logs. By storing compressed, unstructured logs and only indexing metadata, Loki is simpler to operate and cheaper to run.
- indexes and groups log streams using the same labels you're already using with Prometheus, enabling you to seamlessly switch between metrics and logs using the same labels that you're already using with Prometheus.
- is an especially good fit for storing [Kubernetes](#) Pod logs. Metadata such as Pod labels is automatically scraped and indexed.
- has native support in Grafana (needs Grafana v6.0).

How Loki work





Promtail



November 7th 2020

vmware®


boer
technology

onf






Promtail

- 
- Promtail is an agent which ships the contents of local logs to a private Loki instance or **Grafana Cloud**. It is usually deployed to every machine that has applications needed to be monitored.
 - It primarily:
 - Discovers targets
 - Attaches labels to log streams
 - Pushes them to the Loki instance.
 - Currently, Promtail can tail logs from two sources: local log files and the systemd journal (on AMD64 machines only).



How Promtail work

- 
- Log file discovery
 - Loki push API
 - Receiving logs from syslog
 - Labeling and parsing
 - Shipping
 - API
 - Promtail web server config



More Promtail information :



<https://grafana.com/docs/loki/latest/clients/promtail/>

Demo

Reference :

<https://medium.com/grafana-tutorials/setup-grafana-logs-panel-with-loki-and-promtail-3bd89cf40c31>

Terima kasih

Please visit :
<https://gits.id>

gits.id

Sponsored by:

vmware[®]

 **boer**
technology

 **ONF**



OICNDI

November 7th 2020