INDONESIA
OpenInfra Days

02.11.2019 | Surabaya, Indonesia

Simple Log Monitoring with Prometheus and Grafana

Didiet A. Pambudiono – DevOps Engineer

didiet@gits.id

gits Indonesia

Biznet GioCloud Biznet Mellanox TECHNOLOGIES BANK BRI OSF OpenStack Foundation

About Me

- DevOps engineer of PT. Gits Indonesia (https://www.gits.id)
- Cloud Explorer
- FOSS Community member : opensuse, opensuse-id, KLaS, etc
- Fortune Teller
- Contact me :
  - didiet@gits.id
  - pambudiono@opensuse.org
- Blog :
  - https://medium.com/@sitidy

Background

Log monitoring system

Light resource

Rich content of Dashboard

Alternate for Elasticsearch Logstash and Kibana Stack

How About Grafana Loki?

Nope, we will not talk about it in this class

<> What is Prometheus?

Open-source systems monitoring and alerting toolkit originally built at SoundCloud.

Since its inception in 2012, many companies and organizations have adopted Prometheus.

The project has a very active developer and user community.

It is now a standalone open source project and maintained independently of any company.

Prometheus joined the Cloud Native Computing Foundation in 2016 as the second hosted project, after Kubernetes.

<> Grok Exporter

- Grok is a tool to parse crappy unstructured log data into something structured and queryable.
- Heavily used in Logstash to provide log data as input for ElasticSearch.
- Grok ships with about 120 predefined patterns for syslog logs, apache and other webserver logs, mysql logs, etc.

<> Grok Exporter

- https://github.com/fstab/grok_exporter
- Log → grok_exporter → prometheus?

<> Unstructured to Structured

- Unstructured :
  - ERROR 30.07.2016 14:37:03 alice 1.5
  - WARNING 30.07.2016 14:37:33 alice 2.5
  - ERROR 30.07.2016 14:43:02 bob 2.5
  - ERROR 30.07.2016 14:45:59 alice 2.5

<> Unstructured to Structured

- Structured :
  - LOGLEVEL: ERROR
  - DATE: 30.07.2016
  - TIME: 14:37:03
  - USER: alice
  - NUMBER: 1.5

<> grok_exporter config file

- Input:
  - type: file
    path: ./example.log
- grok:
  - patterns_dir: ./logstash-patterns
- metrics:

Lorem ipsum doloret is amet

✓ **One article**
Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

✓ **Two article**
Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

✓ **Three article**
Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

✓ **Four article**
Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

Lorem ipsum doloret is amet

✓

One article

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

✗

Two article

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

✗

Three article

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

DEMO

DEMO

Tools:

- grok_exporter
- http://grokconstructor.appspot.com/do/match

Thank you!

We Are Hiring
https://gits.id/career