Environmental

Ubuntu 20.04

Grafana List

1. Promtail
2. Loki
3. Grafana

ELK List

1. Filebeat
2. Logstash
3. Kibana

**自行安裝:**

1. Promtail 安裝

指定promtail 版本

PROMTAIL\_VERSION=$(curl -s "https://api.github.com/repos/grafana/loki/releases/latest" | grep -Po '"tag\_name": "v\K[0-9.]+')

sudo mkdir /opt/promtail

sudo wget -qO /opt/promtail/promtail.gz [https://github.com/grafana/loki/releases/download/v${PROMTAIL\_VERSION}/promtail-linux-amd64.zip](https://github.com/grafana/loki/releases/download/v$%7bPROMTAIL_VERSION%7d/promtail-linux-amd64.zip)

sudo gunzip /opt/promtail/promtail.gz

sudo chmod a+x /opt/promtail/promtail

sudo ln -s /opt/promtail/promtail /usr/local/bin/promtail

sudo wget -qO /opt/promtail/promtail-local-config.yaml "https://raw.githubusercontent.com/grafana/loki/v${PROMTAIL\_VERSION}/clients/cmd/promtail/promtail-local-config.yaml"

promtail -version

sudo nano /etc/systemd/system/promtail.service

[Unit]

Description=Promtail client for sending logs to Loki

After=network.target

[Service]

ExecStart=/opt/promtail/promtail -config.file=/opt/promtail/promtail-local-config.yaml

Restart=always

TimeoutStopSec=3

[Install]

WantedBy=multi-user.target

sudo service promtail start

sudo systemctl enable promtail

**Promtail config:**

**(**promtail-local-config.yaml**)**

**clients:**

**- url: http://54.251.35.239:3100/loki/api/v1/push**

**server:**

**disable: true**

**scrape\_configs:**

**- job\_name: app**

**pipeline\_stages:**

**static\_configs:**

**- labels:**

**job: app # A `job` label is fairly standard in prometheus and useful for linking metrics and logs.**

**host: local # A `host` label will help identify logs from this machine vs others**

**\_\_path\_\_: /home/ubuntu/.pm2/logs/\*.log**

1. Install logstash

sudo apt-get install default-jre

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add –

sudo apt-get update

sudo apt-get install logstash

sudo systemctl status logstash

修改 Logstash config如下

input {

beats {

port => 5044

}

}

output {

elasticsearch {

hosts => ["http://elasticsearch:9200"] // used in docker

index => "%{[@metadata][beat]}-%{[@metadata][version]}"

action => "create"

}

}

安裝ElasticSearch

curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elastic.gpg

echo "deb [signed-by=/usr/share/keyrings/elastic.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

sudo apt update

sudo apt install elasticsearch

sudo nano /etc/elasticsearch/elasticsearch.yml

network.host: localhost

sudo systemctl start elasticsearch

network.host: localhost

安裝BY DOCKER

一張含有 文字, 螢幕擷取畫面, 數字, 軟體 的圖片

自動產生的描述

Docker-compose for ELK

version: "3.8"

services:

elasticsearch:

image: elasticsearch:7.16.2

environment:

- discovery.type=single-node

ports:

- 9200:9200

- 9300:9300

filebeat:

image: elastic/filebeat:8.10.1

volumes:

- 'C:/Users/b2badmin/Documents:/data/db' # <- extra space here

logstash:

image: logstash:8.9.2

ports:

- 5044:5044

- 9600:9600

kibana:

image: kibana:7.16.2

ports:

- 5601:5601

version: "3.8"

services:

loki:

image: grafana/loki

ports:

- 3100:3100

promtail:

image: grafana/promtail

volumes:

- 'C:/Users/b2badmin/Documents:/data/db' # <- extra space here

grafana:

image: grafana/grafana

ports:

- 3000:3000