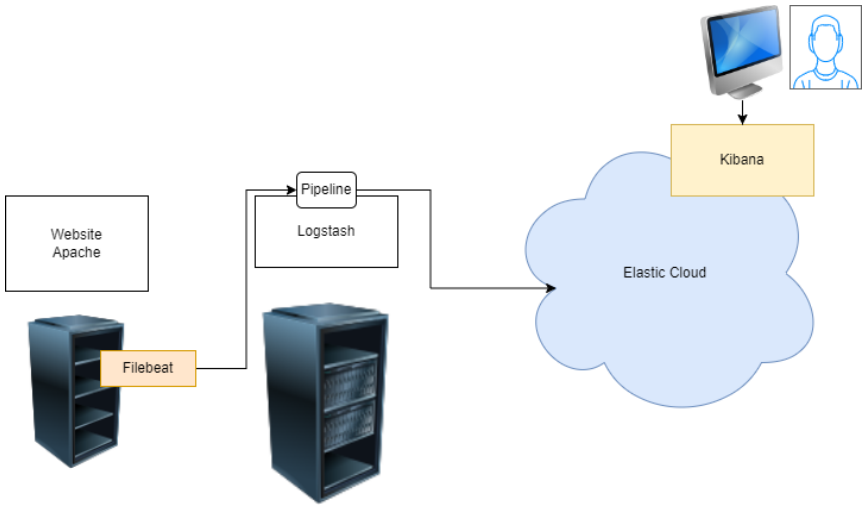
MENU ☰

MAY 19, 2023

DevOps Classroomnotes 19/May/2023

Sending logs to elastic cloud

- Overview



- Install apache and filebeat on one linux instance Refer Here

```
sudo apt update
sudo apt install apache2 -y
```

- Install logstash on other linux instance Refer Here

Configuring filebeats to send apache access logs to logstash

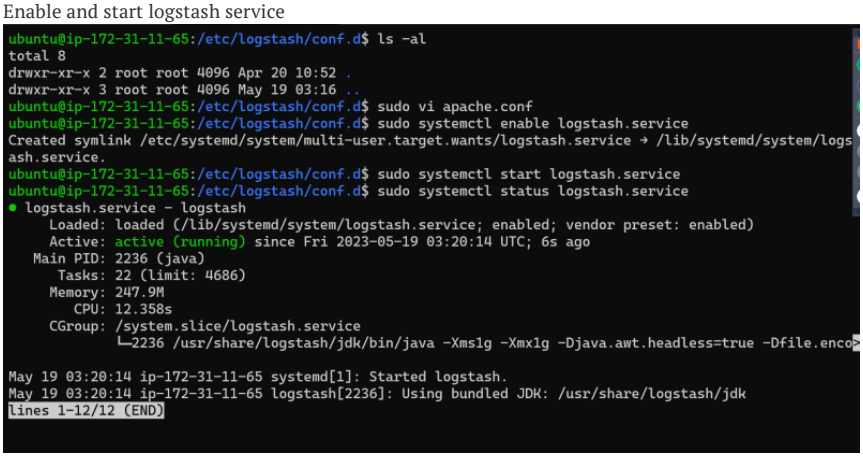
- Refer Here for basic configuration information
- Sending data from logstash to elastic cloud Refer Here
- Logstash pipeline

```
input {
  beats {
    port => 5044
  }
}
filter {
    grok {
        match => { "message" => "%{COMBINEDAPACHELOG}" }
    }

}
output {
    elasticsearch {
        cloud_id => "learningenv:dXMtY2VudHJhbDEuZ2NwLmNsb3VkLmVzLmlvOjQ0MyQxMDg1YTVjO
        cloud_auth => "elastic:h22oWprNjqqbEGTKPSvHHpqS"
```

- Create a file called as apache.conf in `/etc/logstash/conf.d`

- Enable and start logstash service



- Now configure filebeat to send logs from `/var/log/apache2/access.log` to logstash
- To generate artifical traffic we have executed the following script

```
#!/bin/bash
while true; do
        curl 'http://34.219.90.251'
        sleep 2
done
```

- As of now we are getting issue with indexing (storing) in elastic search

```
[WARN ] 2023-05-19 03:52:25.065 [[main]>worker0] elasticsearch - Could not index event to
[INFO ] 2023-05-19 03:52:25.066 [[main]>worker0] file - Opening file {:path=>"/tmp/test.l
```

Leave a Reply

Enter your comment here...

About continuous learner

devops & cloud enthusiastic learner

VIEW ALL POSTS

PREVIOUS POST

Azure Classroomnotes 19/May/2023

NEXT POST

AWS Classroomnotes 19/May/2023