

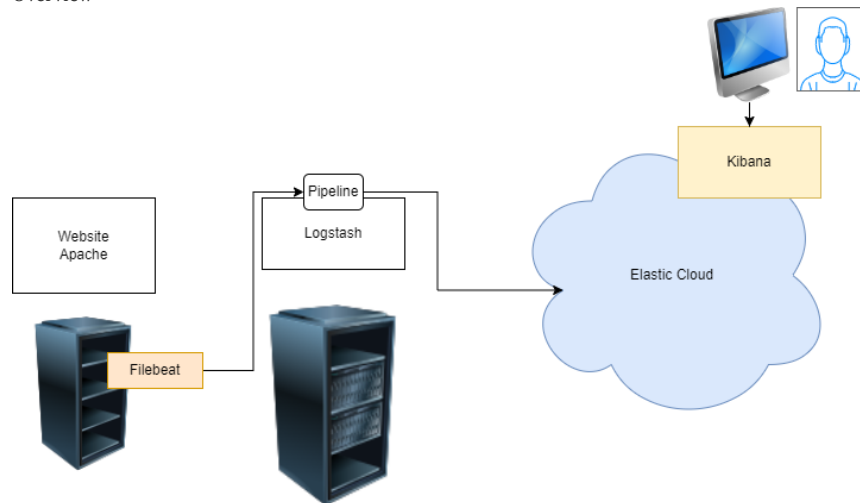


MAY 19, 2023

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:dXmTY2VudHJhbDEuZ2NwLmNsY3VkbWVzLm1vOjQ0MyQxMDg1YTJVJ0"
    cloud_auth => "elastic:h22owprNjqqbEGTKPSvHHpqS"
  }
}
```

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

- Enable and start logstash service

```
ubuntu@ip-172-31-11-65:/etc/logstash/conf.d$ ls -al
total 8
drwxr-xr-x 2 root root 4096 Apr 20 10:52 .
drwxr-xr-x 3 root root 4096 May 19 03:16 ..
ubuntu@ip-172-31-11-65:/etc/logstash/conf.d$ sudo vi apache.conf
ubuntu@ip-172-31-11-65:/etc/logstash/conf.d$ sudo systemctl enable logstash.service
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /lib/systemd/system/logstash.service.
ubuntu@ip-172-31-11-65:/etc/logstash/conf.d$ sudo systemctl start logstash.service
ubuntu@ip-172-31-11-65:/etc/logstash/conf.d$ sudo systemctl status logstash.service
● logstash.service - logstash
   Loaded: loaded (/lib/systemd/system/logstash.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2023-05-19 03:20:14 UTC; 6s ago
     Main PID: 2236 (java)
       Tasks: 22 (limit: 4686)
      Memory: 247.9M
         CPU: 12.358s
    CGroup: /system.slice/logstash.service
            └─2236 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.headless=true -Dfile.encoding=UTF-8

May 19 03:20:14 ip-172-31-11-65 systemd[1]: Started logstash.
May 19 03:20:14 ip-172-31-11-65 logstash[2236]: Using bundled JDK: /usr/share/logstash/jdk
lines 1-12/12 (END)
```

- Now configure filebeat to send logs from /var/log/apache2/access.log to logstash
- To generate artificial 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.1
```

Leave a Reply

Enter your comment here...

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)



About continuous learner

devops & cloud enthusiastic learner

[VIEW ALL POSTS](#)

◀ [PREVIOUS POST](#)

[Azure Classroomnotes 19/May/2023](#)

[NEXT POST](#)

[AWS Classroomnotes 19/May/2023](#)