stack-ELK-kafka

This Example is about How Deploy ELK with kafka and filebeat

FileBeat

Essentially, Filebeat is a logging agent installed on the machine generating the log files ,tailing them, and forwarding to kafka ,it has configuration file which has input and output

kafka

Apache Kafka is a distributed event store and stream-processing platform create pipeline between filebeat and logstash

logstash

Logstash is a light-weight, open-source, server-side data processing pipeline that allows you to collect data from a variety of sources in this example input data is kafka and output data is elasticsearch

elasticsearch

Elasticsearch is a search engine

HOW IT WORKS

We have two dokcer-compose file we need to run first docker-compose1.yaml to run nginx as a create log, and save Log into /logs directory which filebeat read log from that file you can change the configuration with your requirements.

Logstash configuration has input kafka and output elasticsearch.

HOW RUN:

docker-compose -f docker-compose1.yaml up

After run the first compose file

Docker-compose up

curl http://<MACHINE-IP>:9200

it takes minute to be ready kibana and elasticsearch

Refresh Nginx page on port 80

http://localhost:5601

Go to database and create index on kibana dashboard.