***ELK integration with Filebeat via Dockerization.***

Pre-requisite –

1. JDK
2. Maven
3. Docker
4. Docker compose

**Docker compose installation steps-**

sudo apt-get update

sudo apt-get install docker-ce docker-ce-cli containerd.io docker-compose-plugin

<https://www.theserverside.com/blog/Coffee-Talk-Java-News-Stories-and-Opinions/How-to-install-Docker-and-docker-compose-on-Ubuntu>

**Install filebeat on ubuntu-**

#Install Filebeat

curl -fsSL <https://artifacts.elastic.co/GPG-KEY-elasticsearch> | sudo apt-key add -  
sudo add-apt-repository "deb <https://artifacts.elastic.co/packages/7.x/apt> stable main"  
sudo apt-get update  
sudo apt-get install filebeat

Once you installed filebeat then change the configuration in filebeat.yml

Goto - /etc/filebeat

Add –

setup.ilm.enabled: false

setup.template.enabled: false

setup.template.overwrite: true

filebeat.inputs:

- type: filestream

id: my-filestream-2

enabled: true

paths:

- /home/prashantkatiyar01/logs/\*.log - Put directory from where logs needs to be read.

fields\_under\_root: true

fields:

type: logs2

Points-

1. By default Elastic search configs are enabled, just disable them.

#output.elasticsearch

1. Enable logstash configs.

output.logstash:

# The Logstash hosts

hosts: ["localhost:5044"]

**Start and stop the filebeat -**

sudo service filebeat start or sudo filebeat -e -d "publish"  
sudo service filebeat stop

Here logs will be pushed to logstash server.

**Install ELK via Docker –**

https://github.com/lemoncode21/docker-loging-elk

1. Create directory ex - /elk
2. Create a docker compose file
3. Create directory –

cd /elk

mkdir logstash

cd /logstash

mkdir pipeline

mkdir config

1. Create logstash.yml under config folder with below configuration.

cd /config

vi logstash.yml

--------------

http.host: "0.0.0.0"

path.config: /usr/share/logstash/pipeline

xpack.monitoring.elasticsearch.hosts: [ "elasticsearch:9200" ]

------

1. Create logstash.conf under pipeline folder with below configuration.

cd ../pipeline/

vi logstash.conf

----

input {

beats {

port => 5044 - reading from filebeat

}

}

output {

elasticsearch {

hosts => "elasticsearch:9200"

index => "index\_second" - Index name on elastic search

}

}

------------

1. Create docker compose file in parent folder

cd /elk

vi docker-compose.yml

----------

Copy the content from this file - <https://github.com/lemoncode21/docker-loging-elk/blob/master/docker-compose.yml>

or copy below file



1. Run the elk compose file from the parent directory.

docker compose up

Run spring boot dockerized application and mount to log location.

docker build -f Dockerfile -t mylogapp .

docker run -d -v /nagarro/elk/code/logs/LogGenerator:/logs -p 8080:8080 mylogapp

docker run -d -v /nagarro/elk/code/logs/logbeautifier:/logs -p 8090:8090 logbeautifier