ELK Stack

links:

[**https://elk-docker.readthedocs.io/**](https://elk-docker.readthedocs.io/)

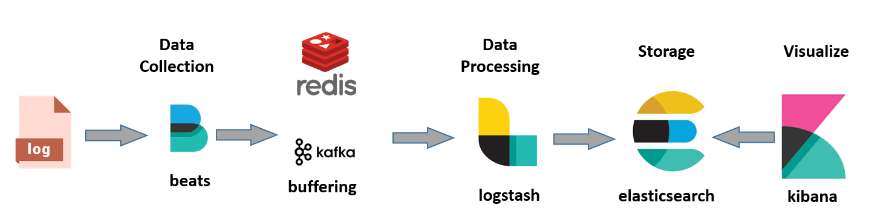
[**https://www.elastic.co/guide/en/beats/filebeat/current/index.html**](https://www.elastic.co/guide/en/beats/filebeat/current/index.html)

[**https://www.elastic.co/guide/en/logstash/current/index.html**](https://www.elastic.co/guide/en/logstash/current/index.html)

<https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html>

**https://www.elastic.co/guide/en/kibana/current/index.html**

**What is ELK or ELK stack??**

****

The **ELK Stack** is a collection of three open-source products — Elasticsearch, Logstash, and Kibana. ELK stack provides centralized logging in order to identify problems with servers or applications. It allows you to search all the logs in a single place. It also helps to find issues in multiple servers by connecting logs during a specific time frame.

* **E** stands for ElasticSearch: used for storing logs
* **L** stands for LogStash : used for both shipping as well as processing and storing logs
* **K** stands for Kibana: is a [visualization tool](https://www.guru99.com/best-data-visualization-tools.html) (a web interface) which is hosted through Nginx or Apache

ElasticSearch, LogStash and Kibana are all developed, managed ,and maintained by the company named Elastic.

ELK Stack is designed to allow users to take data from any source, in any format, and to search, analyze, and visualize that data in real time.

1) install docker

refer to the following page for detail and commands to install docker in linux

https://github.com/nandeesh-kumar/docker

2) pull ELK docker image from docker hub

docker pull sebp/elk

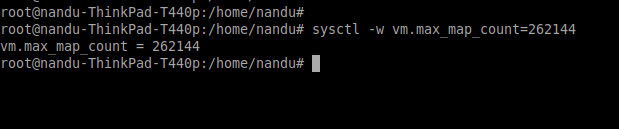
3) run the docker image

before start the elk docker image, may need to set the parameter

sysctl -w vm.max\_map\_count=262144

to avoid the error.

[Elasticsearch: Max virtual memory areas vm.max\_map\_count [65530] is too low, increase to at least [262144]](https://stackoverflow.com/questions/51445846/elasticsearch-max-virtual-memory-areas-vm-max-map-count-65530-is-too-low-inc)

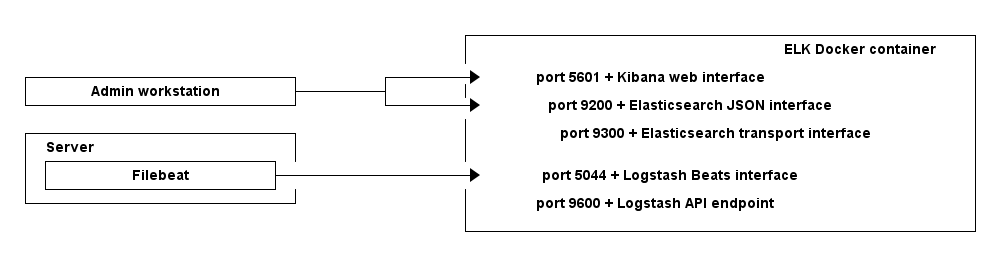
****

docker run -p 5601:5601 -p 9200:9200 -p 9300:9300 -p 9600:9600 -p 5044:5044 -it --name elk sebp/elk

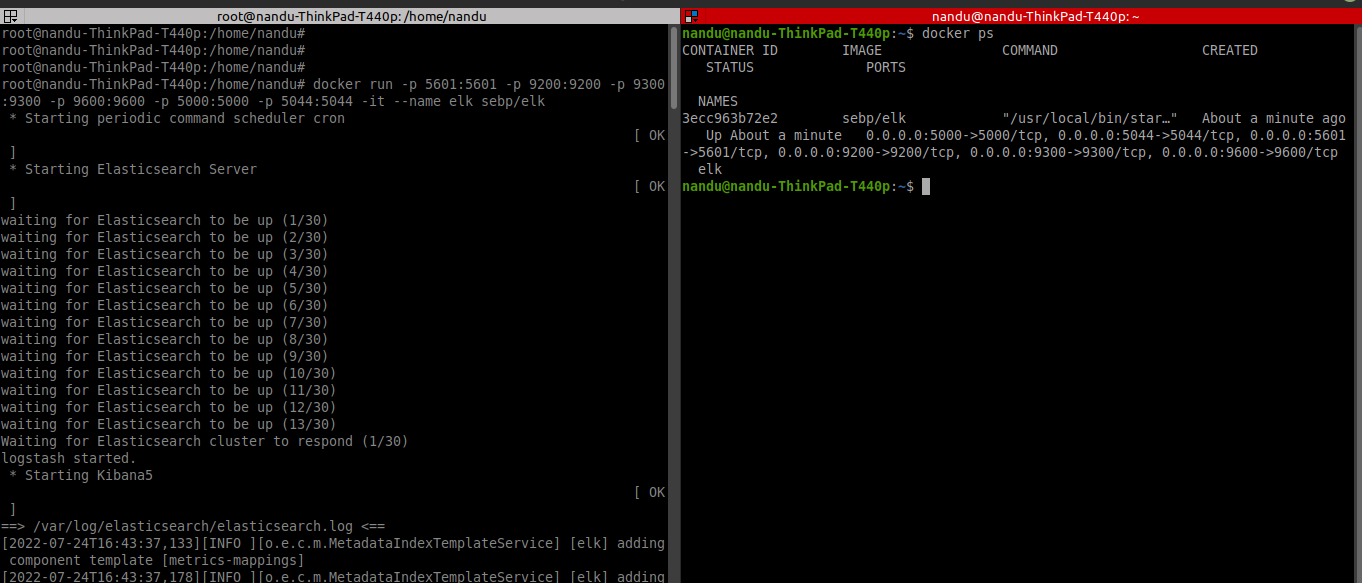
docker run -p 5601:5601 -p 9200:9200 -p 9300:9300 -p 9600:9600 -p 5044:5044 -it \

-e ES\_HEAP\_SIZE="2g" -e LS\_HEAP\_SIZE="1g" --name elk sebp/elk

**the port details are as followoing**

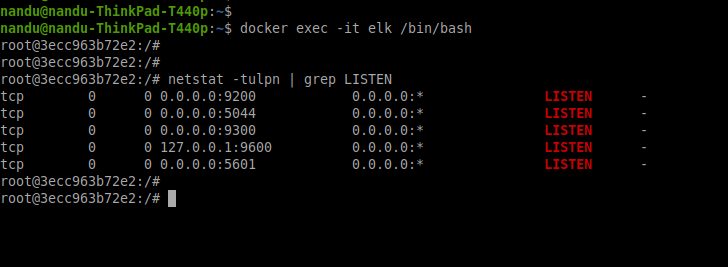
****

**docker process is started successfully.**

****

4) connecting to docker container

docker exec -it elk /bin/bash

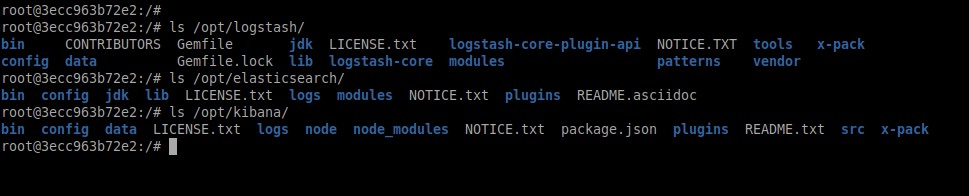


note: may need to install netstat command in docker container.

apt update

apt install net-tools

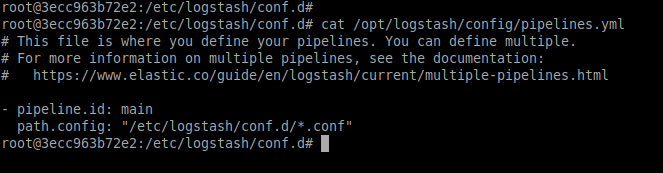
the logstash, elastisearch and kibana are present in following location in docker container

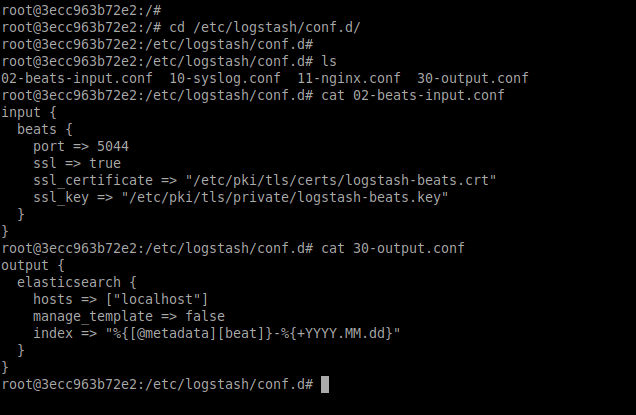


5) elk configuration

**logstash:**

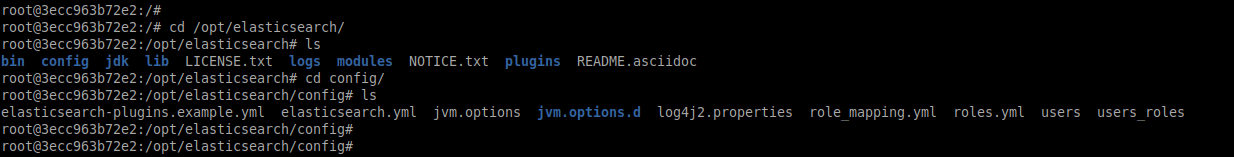
pipeline configuarion

configuraiton files

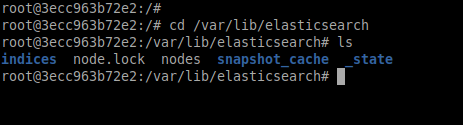


**elastisearch:**

elastisearch config path



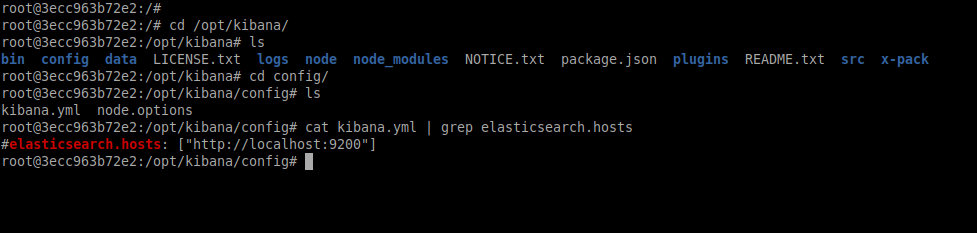
data file in elastisearch present in following location



**kibana:**

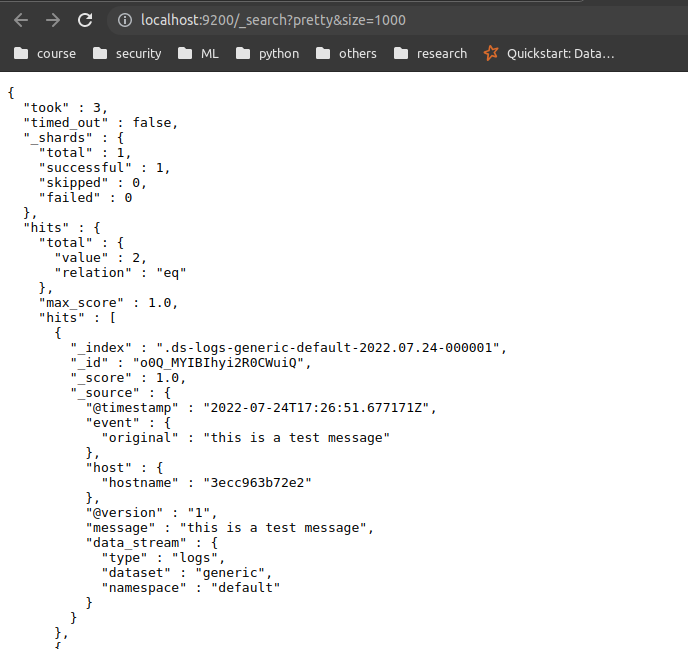
kibana to elastisearch configuraiton presenr in kibana.yml file

the default value is elasticsearch.hosts: ["http://localhost:9200"]



6) Testing the connection and flow

the test data sent to logstash are stored in elastisearch



select the index to query in kibana

and check the message

