ElasticSearch – Elastic search is NoSQL database that is based on the Lucene search engine which will helps us to store inputs/logs. The purpose of elastic search is to store the data.

LogStash – Logstash is log pipeline tool that accepts inputs/logs from various sources & export data to various target. Logstash helps us to process the data.

Kibana – Kibana is visualization UI layer, which will helps developer to monitor applications logs. Kibana helps us to view those data.

Elastic Search can be downloaded from below link

<https://www.elastic.co/downloads/elasticsearch>

LogStash can be downloaded from below link

<https://www.elastic.co/downloads/logstash>

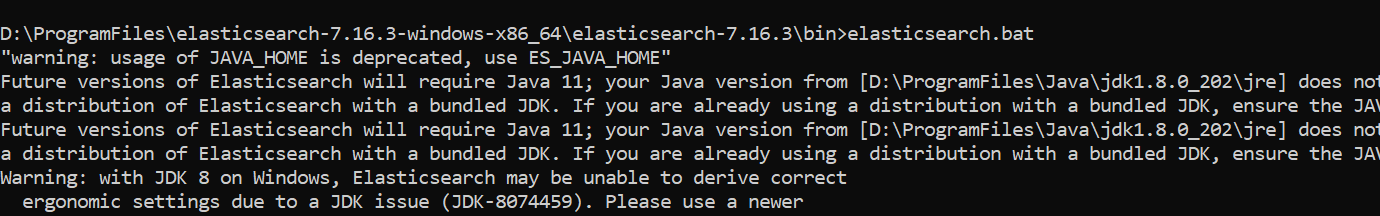
Kibana can be downloaded from below link

<https://www.elastic.co/downloads/kibana>

**How to start Elastic Search** – Download file and extract the same, go to bin folder and execute elasticsearch.batch file

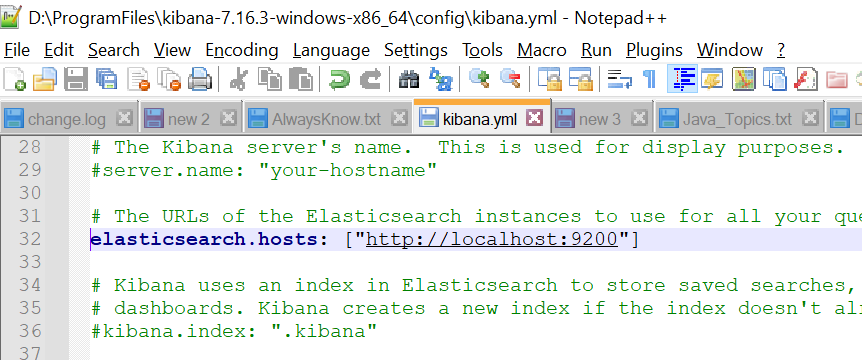
Note – ELK-8.1.3 version is having some issue related to java, I switched backed to ELK-7.16.3 which is working fine. Download the same and proceed with below changes

D:\ProgramFiles\elasticsearch-.1.3\bin\



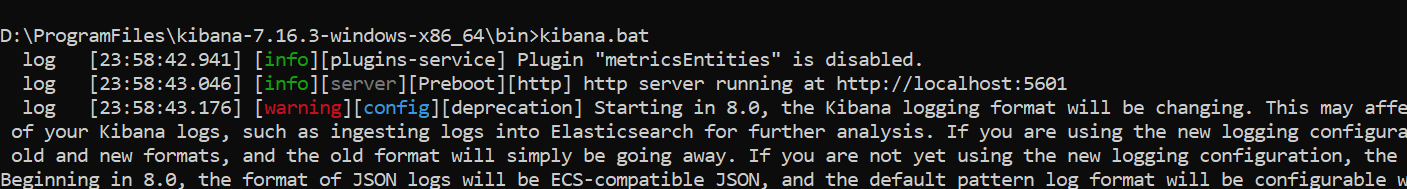
**How to start Kibana**

We need to do change first change in kibana.yml file located under config folder.



Now start kibana as below

Go to bin folder and run kibana.bat file



**How to start Start LogStash**

We need to do some changes to log stash in order to start. First of all we need to create one configuration file for loagstash. Lets assume that file name is logstash.conf file and this file contains log related information like what is the input of logs and what is the output and what is the URL of elasticsearch. Sale code is below

input {

file {

path => "D:/Manish/Projects/Idea/eurodigital/spring.log"

start\_position => "beginning"

}

}

output {

elasticsearch {

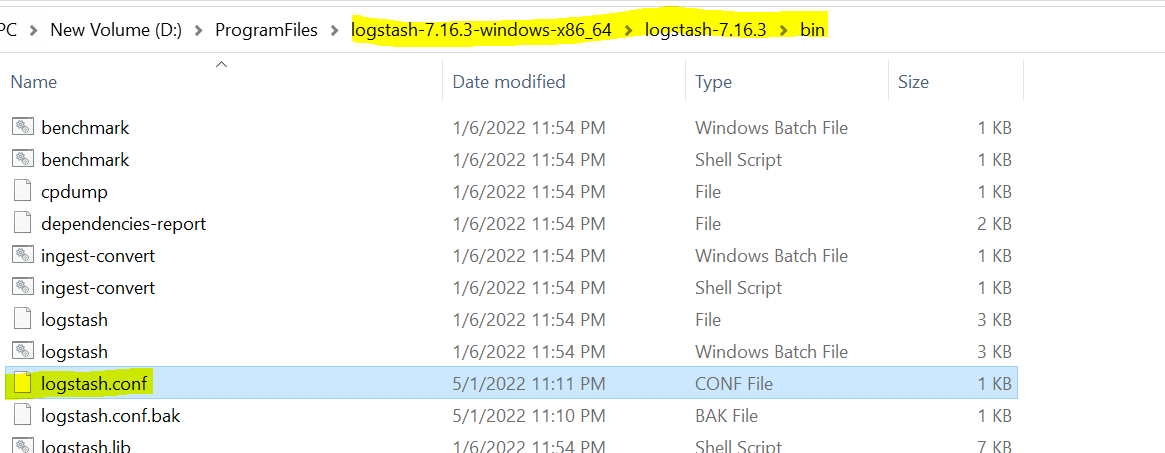
hosts => ["localhost:9200"]

}

stdout { codec => rubydebug }

}

Just copy above code and save the same in one file and rename file as logstash.conf and keep this file un bin folder.

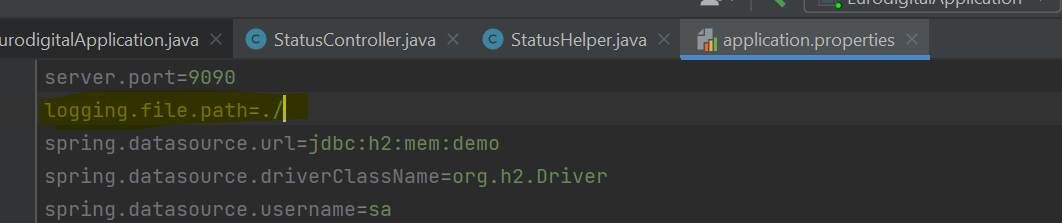


Changes for the log.

Look at above file, log it is reading from below location, it means spring boot application must write log in below file and logstash will read file and get the latest logs

D:/Manish/Projects/Idea/eurodigital/spring.log

I am saving log in the same director where application is located. As below

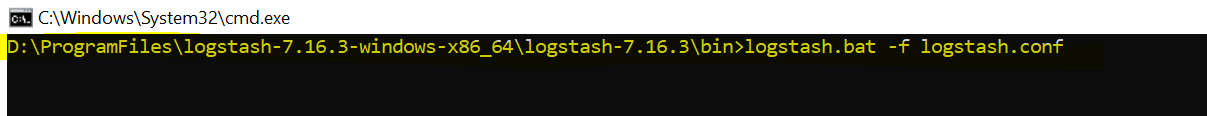


Assume if project is located in D:/Manish/Projects/Idea/eurodigital

Then log will be generated under eurodigital folder and same location is given to the logstash file.

Note: Logstash will accept forward slash so please change accordingly as mention above.

Once this change is done. Go to Bin folder and start logstash as below.



Once it is started successfully. You can see logstash started accepting log as long as log is generating

Check indices

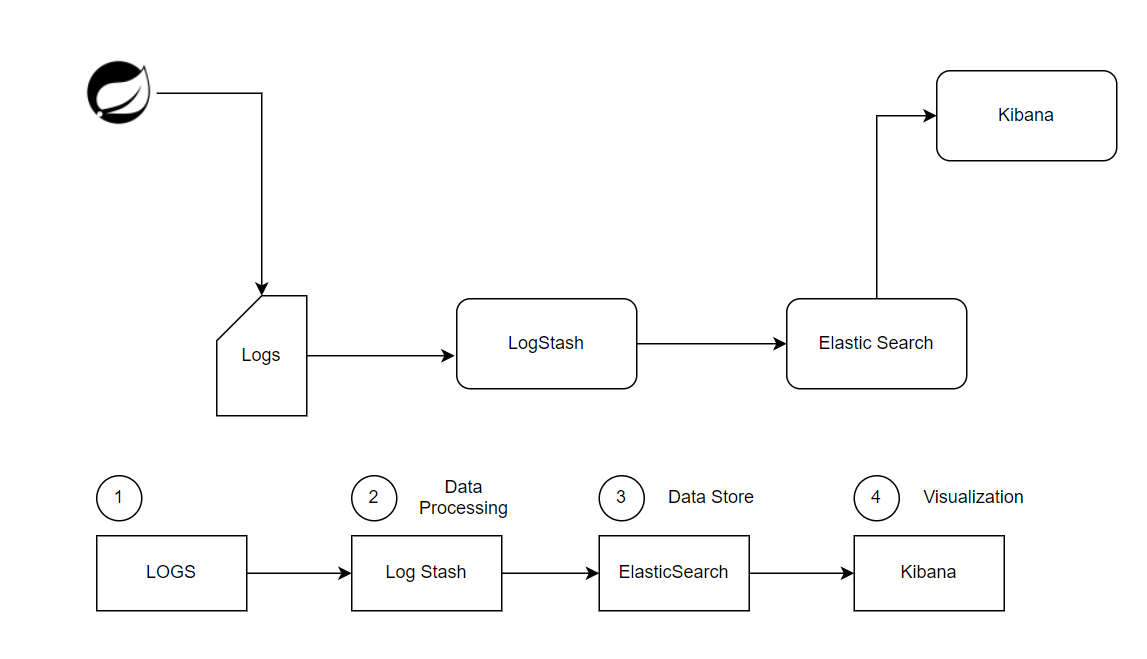
Localhost:9200/\_cat

This command will give all cat generated and if you hit Localhost:9200/\_cat/indicaes then it will give indices generated against log file.

Now open Kibana and go to management and click Stack Management. Now create index pattern ( here you will get option to create index pattern)

While creating index pattern make sure that you select @timestamp. Once this is done go to Kibana discovery and select the index pattern created. This will display all log generated in the elastic search

**Architecture**



Application will generate log, logStah will pull log and process it and push it to the elastic search. Kibana get the log from elastic search and display the same.