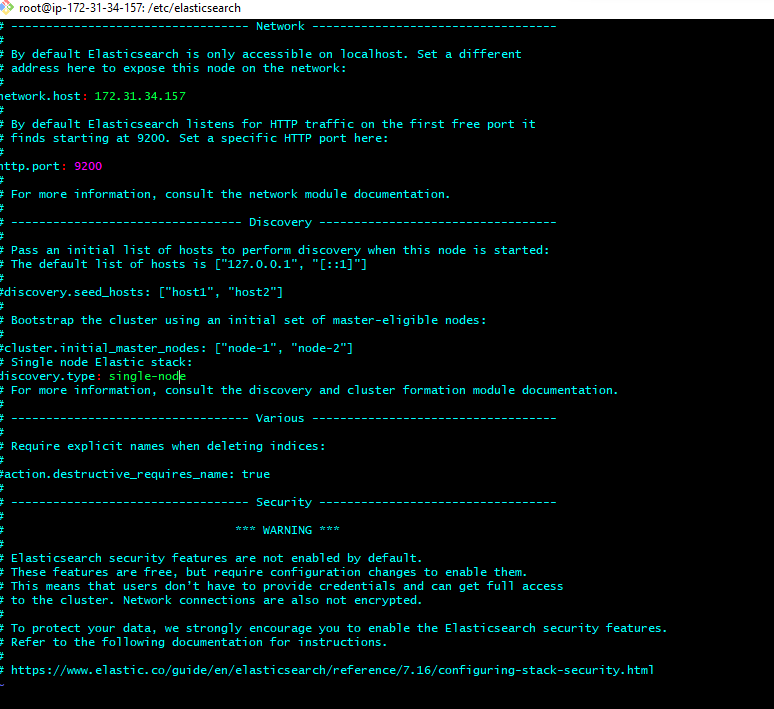
# Installation of ELK (Elasticsearch, Logstash, Kibana)



**Step1:**

sudo su

apt-get install openjdk-8-jdk

**Step2:**

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

**Step3:**

apt-get install apt-transport-https

**Step4:**

echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee –a /etc/apt/sources.list.d/elastic-7.x.list

apt-get update

**Step5:**

apt-get install elasticsearch

**Step6:**

apt-get install vim

vim /etc/elasticsearch/elasticsearch.yml

Edit: Uncomment and put Ur private id: network.host: private Ip (its Ur private Ip) http.port: 9200

discovery.seed\_hosts: private Ip (its Ur private IP)

**Step7:** Go to

vim /etc/elasticsearch/jvm.options(This is to give the size of JVM) edit:

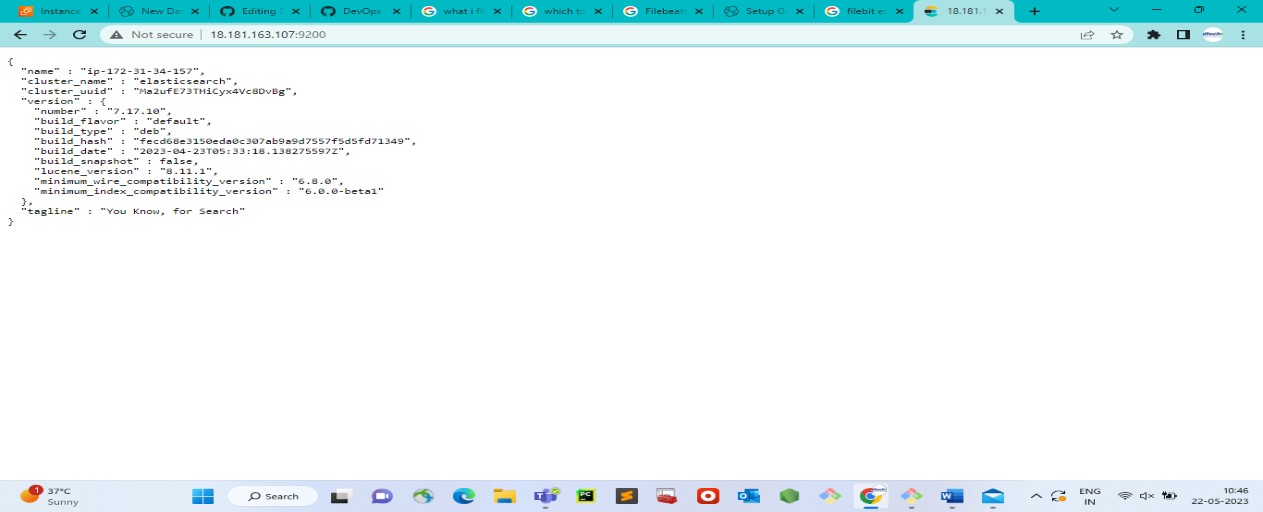
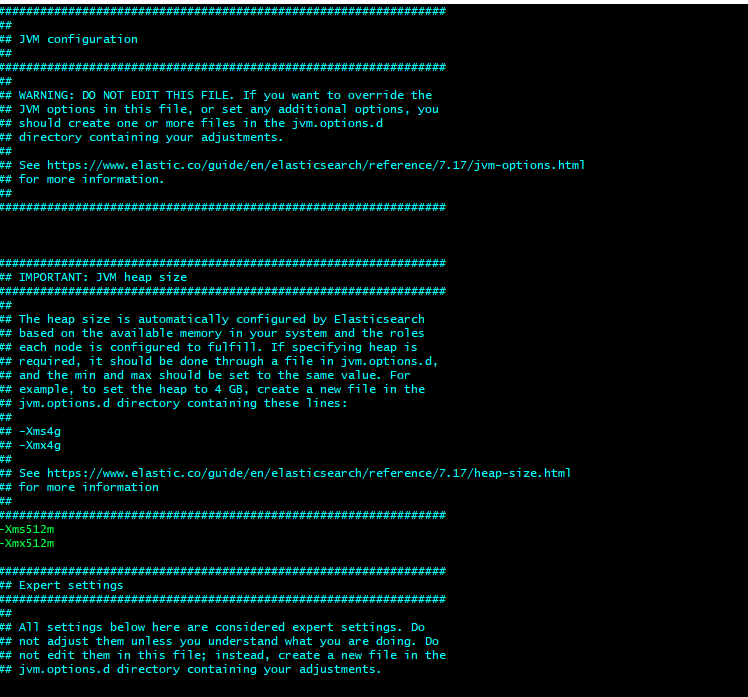
-Xms512m

-Xmx512m

## Step8:

systemctl start elasticsearch.service systemctl enable elasticsearch.service

## Step9:



curl -X GET "172.31.34.157:9200"

(or)

ip:9200 (in web)

### **To run the elastic server automatic whenever server starts**:

go to

cd /systemd/system

touch elastic.service

vim elastic.service

paste below code:

[Unit]

Description=Elasticsearch

Documentation=https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html

Wants=network-online.target

After=network-online.target

[Service]

Type=simple

User=elasticsearch

Group=elasticsearch

ExecStart=/usr/share/elasticsearch/bin/elasticsearch

Restart=always

RestartSec=10

StartLimitInterval=0

LimitMEMLOCK=infinity

[Install]

WantedBy=multi-user.target

# Installation of Kibana on Ubuntu:

Step1:

apt-get install kibana vim /etc/kibana/kibana.yml

Step2:

Edit:

server.port: 5601 server.host: "private ip"

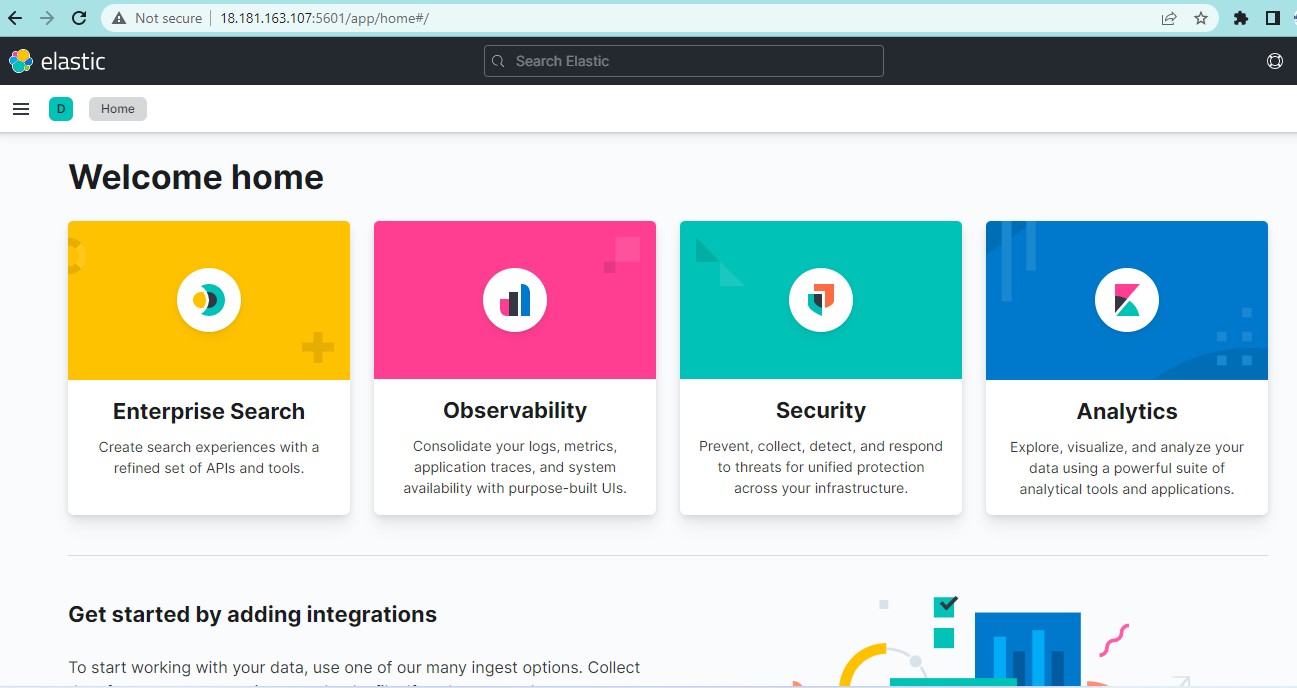
elasticsearch.hosts: ["http://privateip:9200"]

Step3:

systemctl start kibana systemctl enable kibana

Step4:

allow traffic on port 5601 to access the Kibana dashboard. ufw allow 5601/tcp



**Installation of Logstash on Ubuntu:**

## Installation of Logstash on Ubuntu:

Step1:

apt-get install logstash systemctl start logstash systemctl enable logstash systemctl status logstash

Step2:

Logstash is a highly customizable part of the ELK stack.

Once installed, configure its INPUT, FILTERS, and OUTPUT pipelines according to your own individual use case.

* All logstash files will be stored in:

/etc/logstash/conf.d/.

* Logstash Process:

input-->filter-->output

* apt-get install filebeat

Step3:

vim /etc/filebeat/filebeat.yml Edit:

output.logstash

hosts: ["privateip:5044"]

Step4:

\* What is Filebeat?

filebeat modules enable system

one cmd: [ filebeat setup --index-management -E output.logstash.enabled=false

-E 'output.elasticsearch.hosts= ["172.31.34.157:9200"]' ]

systemctl start filebeat systemctl enable filebeat

Step5:

curl -XGET <http://172.31.34.157:9200/_cat/indices?v>

## Install Connecting the nginx to apache tomcat:

* apt install nginx
* cd /etc/nignx
* vim nginx.conf

* then comment 404 all that files

server {

listen 80;

server\_name 18.216.96.3;(tomcat public id)

location / {

proxy\_pass http://18.216.96.3:8080/;((tomcat public link)

}

}

then save & systemctl start nginx

