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:

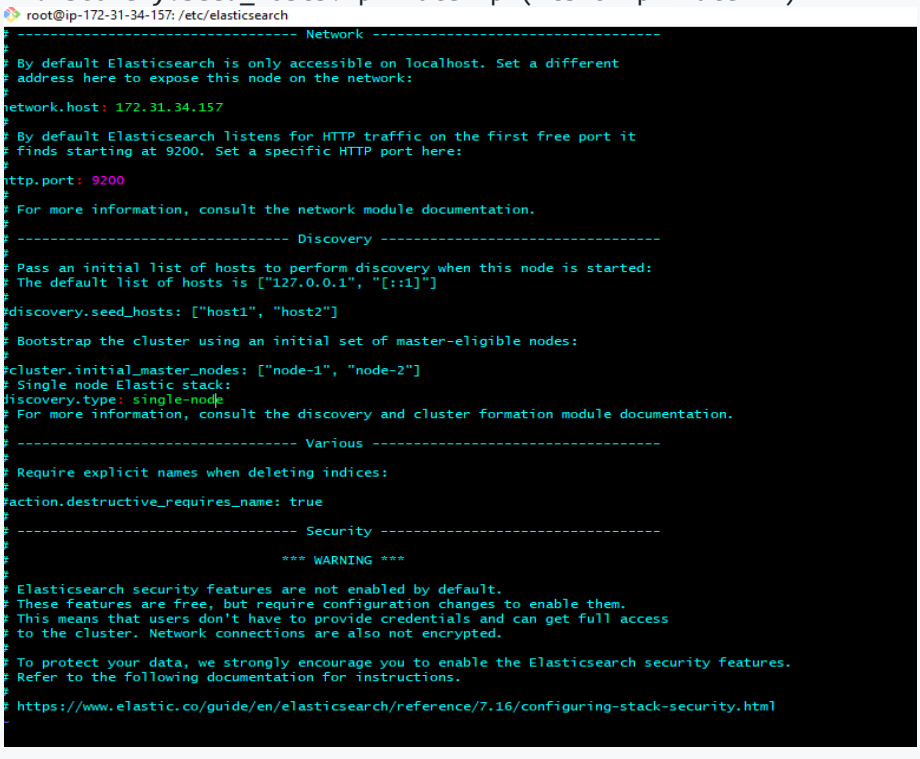
```
apt-get install vim
vim /etc/elasticsearch/elasticsearch.yml
```

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

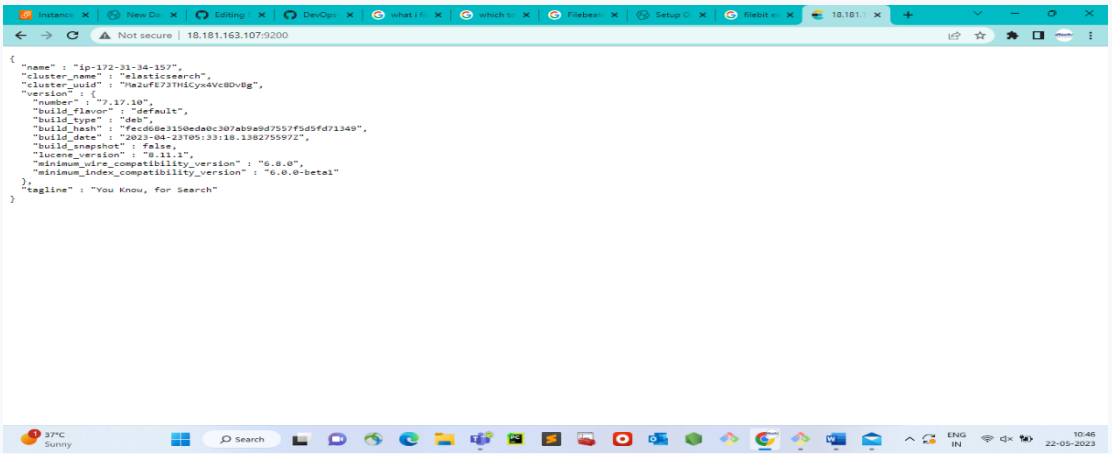
```
################################################################
##
## JVM configuration
##
################################################################
##
## WARNING: DO NOT EDIT THIS FILE. If you want to override the
## JVM options in this file, or set any additional options, you
## should create one or more files in the jvm.options.d
## directory containing your adjustments.
##
## See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/jvm-options.html
## for more information.
##
################################################################



################################################################
## IMPORTANT: JVM heap size
################################################################
##
## The heap size is automatically configured by Elasticsearch
## based on the available memory in your system and the roles
## each node is configured to fulfill. If specifying heap is
## required, it should be done through a file in jvm.options.d,
## and the min and max should be set to the same value. For
## example, to set the heap to 4 GB, create a new file in the
## jvm.options.d directory containing these lines:
##
## -Xms4g
## -Xmx4g
##
## See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/heap-size.html
## for more information
##
################################################################
-Xms512m
-Xmx512m

################################################################
## Expert settings
################################################################
##
## All settings below here are considered expert settings. Do
## not adjust them unless you understand what you are doing. Do
## not edit them in this file; instead, create a new file in the
## jvm.options.d directory containing your adjustments.
```

Step8:

```
systemctl start elasticsearch.service
systemctl enable elasticsearch.service
```

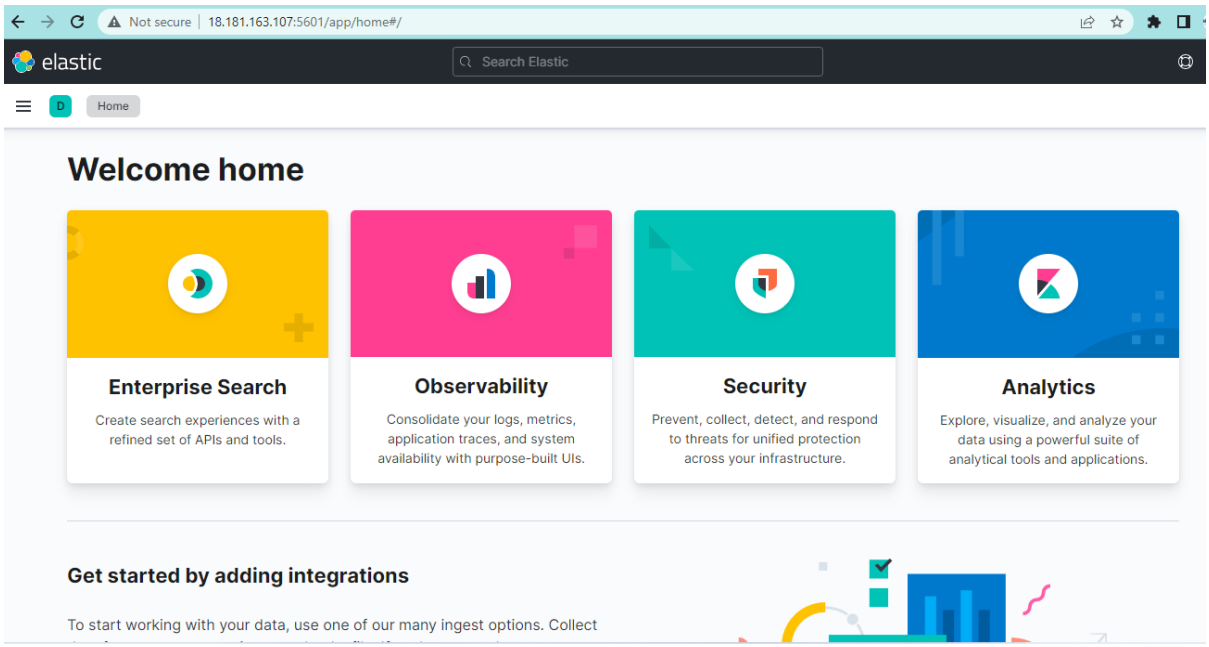
Step9:

```
curl -X GET "172.31.34.157:9200"
(or)
ip:9200 (in web)
```



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