**What is Elasticsearch ?**

Elastic search is a open source tool which is used to store logs, Elasticsearch is a NoSQL database based on Lucene search engine, After storing logs we can also search it and indexed it.

In Elasticsearch we can store and analyze large volume data, Management becomes more easier by using Elasticsearch because it offers simple deployment.

**What is Logstash ?**

Logstash is used for collection of data and logs, After collected logs it gets transformed and feeds logs forward to Elasticsearch.

Logstash consists of three components –

* Input
* Filtering
* Output

Logstash can analyze structured as well as unstructured data.

Logstash provides plugins to get connected with different types of input sources to Logstash.

**What is Kibana ?**

Kibana is a visualization tool without which Elastic Stack is incomplete, Kibana provides a web interface on which we can search queries from Elasticsearch DB and then we can visualize it from the results obtained.

Kibana provides various types of dashboards which includes varieties of data diagrams, charts and graphs to visualize data, We can perform real-time search of indexed information.

**Prerequisites**

* Ubuntu Server with 20.04 LTS
* JDK
* 2 CPU and 4 GB RAM
* Open Ports 9200, 5601, 5044
* update the system packages
* sudo apt-get update -y

## Install JDK on Ubuntu:

## ->sudo apt-get install openjdk-11-jdk wget apt-transport-https curl gnupg2 -y

## To check java version

java -version

## **Output:**

## openjdk version "11.0.10" 2021-01-19

## OpenJDK Runtime Environment (build 11.0.10+9-Ubuntu-0ubuntu1.20.04)

## OpenJDK 64-Bit Server VM (build 11.0.10+9-Ubuntu-0ubuntu1.20.04, mixed mode, sharing)

## ****#1: Install and Configure Elasticsearch on Ubuntu****

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch --no-check-certificate | sudo apt-key add -

Next add the repository

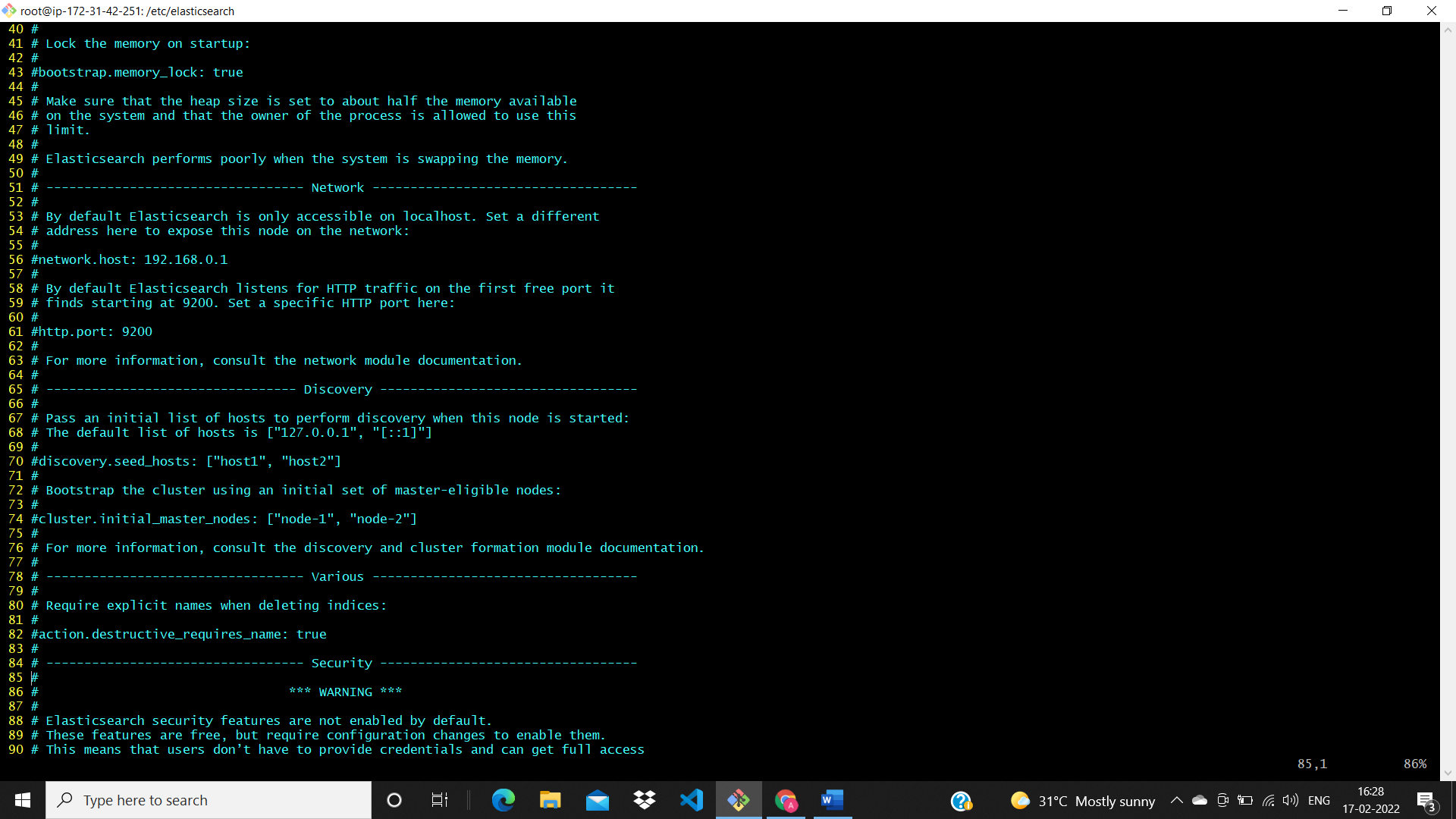
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

sudo apt-get update -y

i).Install elasticsearch on Ubuntu ec2

sudo apt-get install elasticsearch -y

go to the path: /etc/elasticsearch/elasticsearch.yml

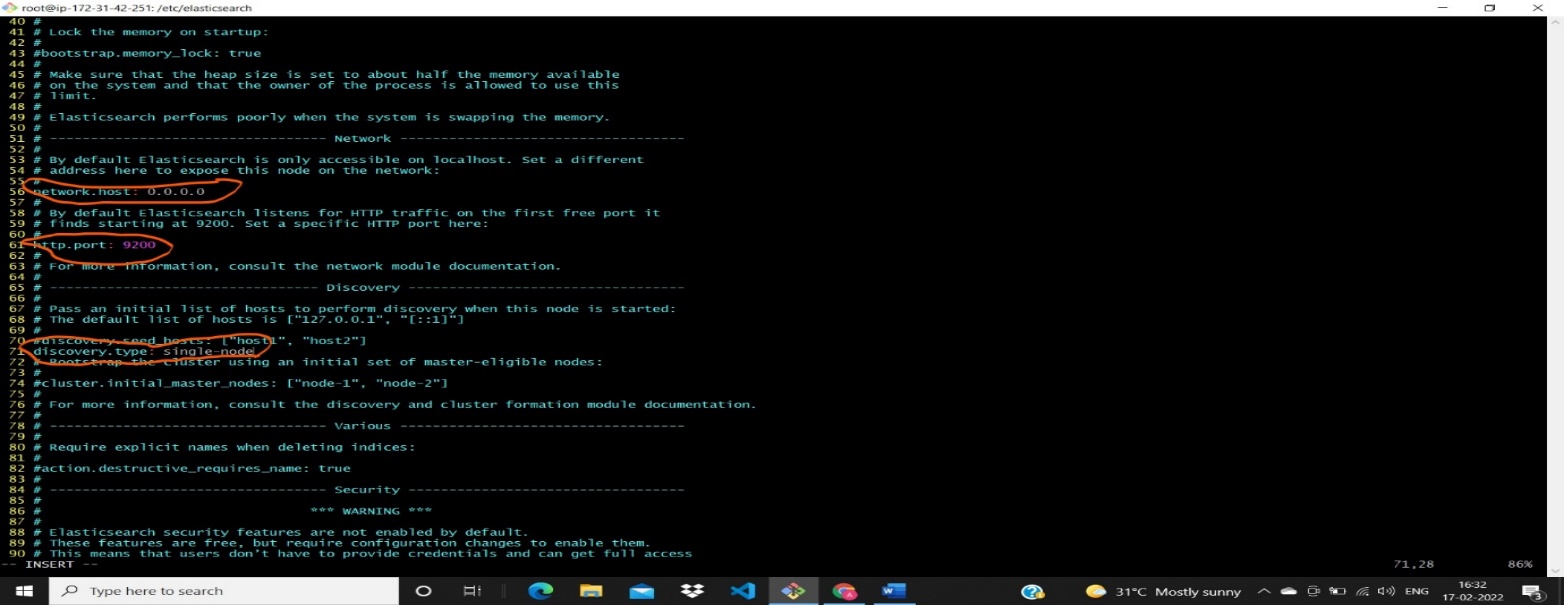


🡪If u can change the line number 56,61 : network.host: 0.0.0.0,61 http.port: 9200

Line number:71 u can add discovery.type: single-node

Then save and exit

***o/p:***



i).start the elacticsearch service🡪 sudo systemctl start elasticsearch

ii).To enable elacticsearch at system startup🡪 sudo systemctl enable elasticsearch

iii).To check the status of elasticsearch🡪 sudo systemctl status elasticsearch

iv).To restart elasticsearch service🡪 sudo systemctl restart elasticsearch

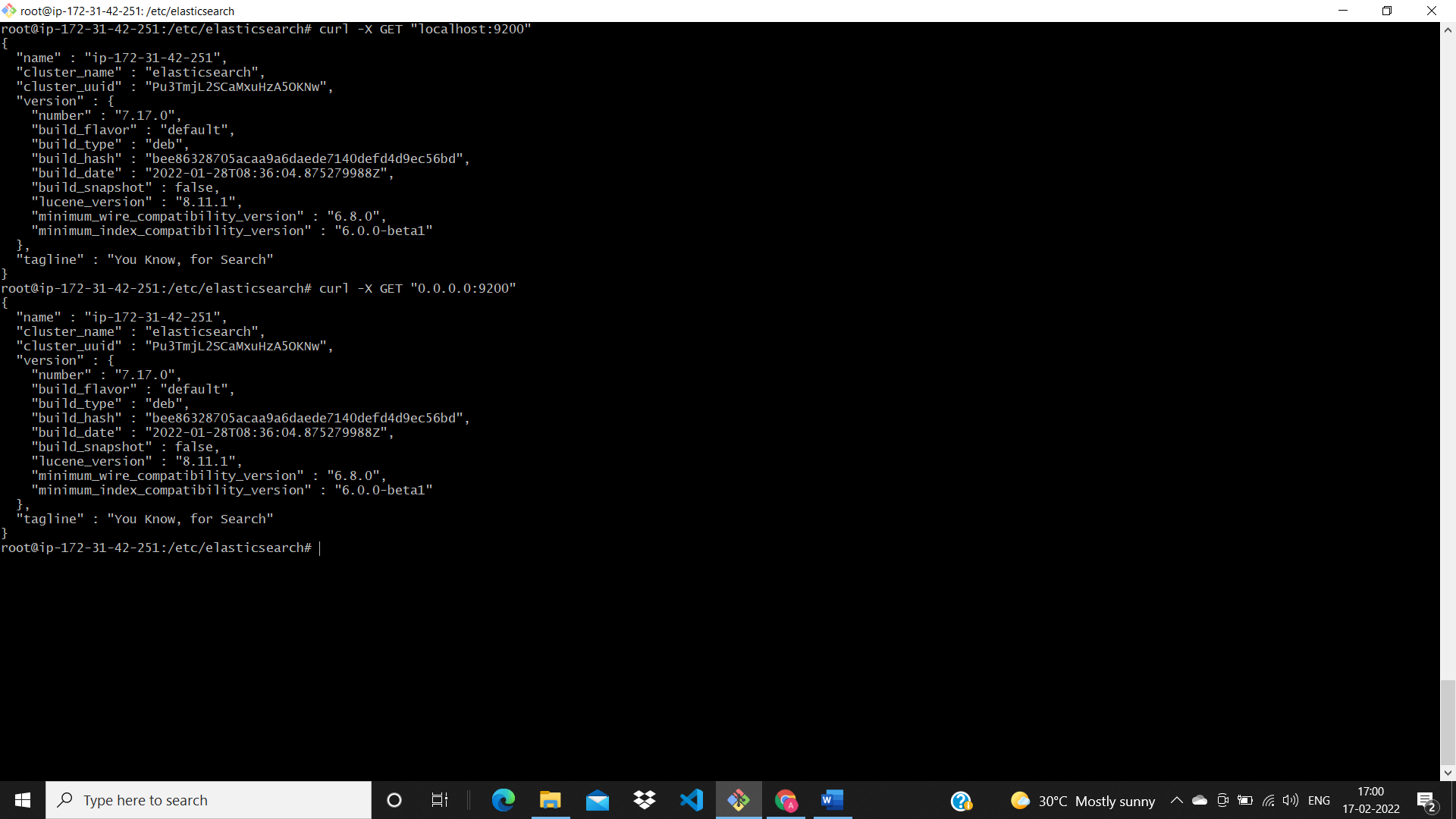
v).ps -ef | grep -i elasticsearch

vi).netstat -anlp | grep -i "3007"

vii).apt install net-tools -y

viii). Enter below command to check elasticsearch is running by sending HTTP request: curl -X GET "0.0.0.0:9200"

**o/p**



2. **Install and Configure Logstash on Ubuntu:**

🡪 sudo apt-get install logstash

i). To load logstash beat create the below config file and insert below lines.

🡪 sudo vi /etc/logstash/conf.d/02-beats-input.conf

input {

beats {

port => 5044

}

}

Then save and apply

ii). To start logstash service

🡪 sudo systemctl start logstash

🡪 sudo systemctl status logstash

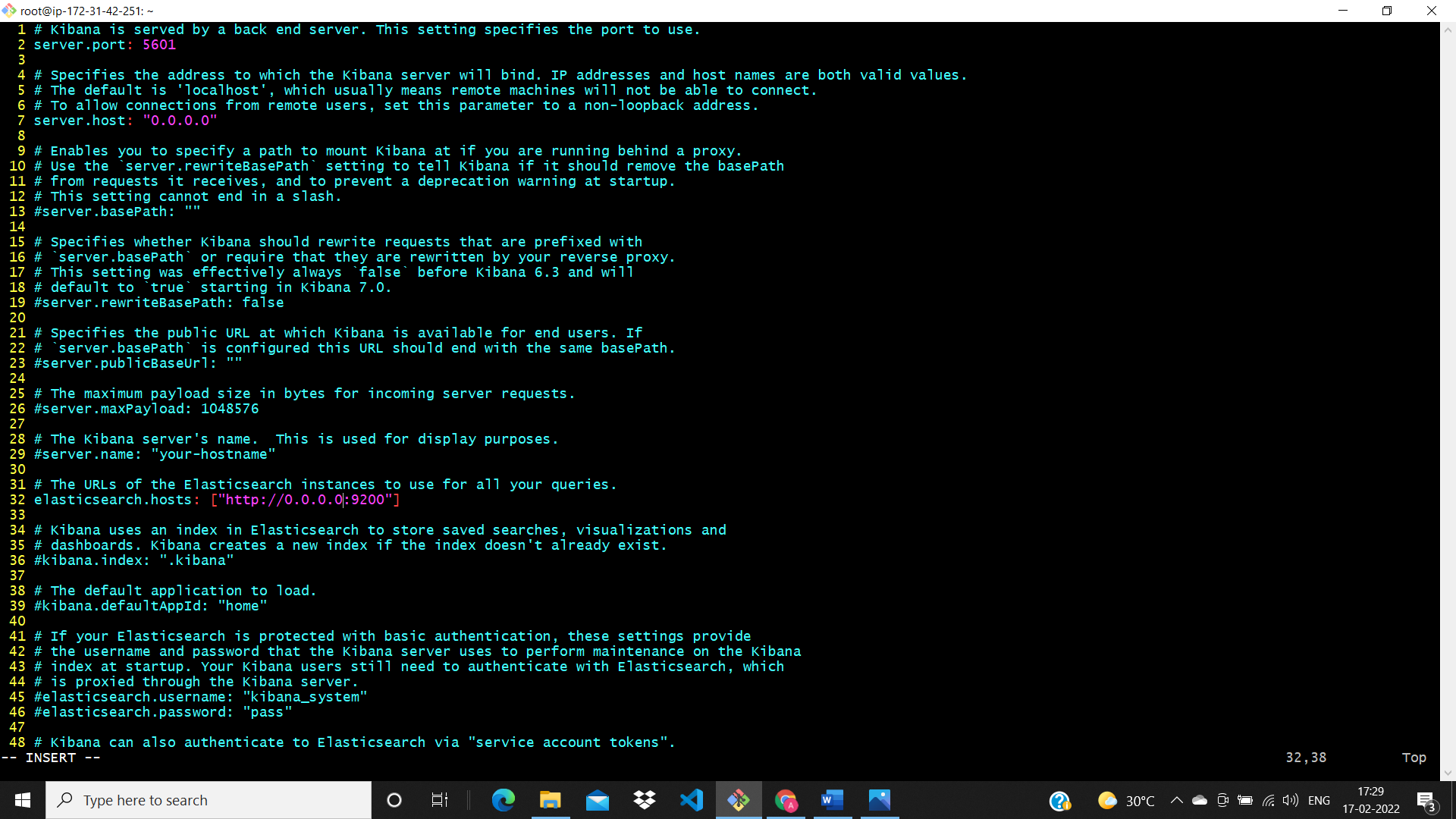
* sudo systemctl enable logstash
* sudo systemctl restart logstash

## ****3. Install and Configure Kibana on Ubuntu****

🡪 sudo apt-get install kibana

i).sudo apt-get install kibana

🡪🡪 sudo vi /etc/kibana/kibana.yml



## To start kibana service

sudo systemctl start kibana

sudo systemctl enable kibana

sudo systemctl status kibana

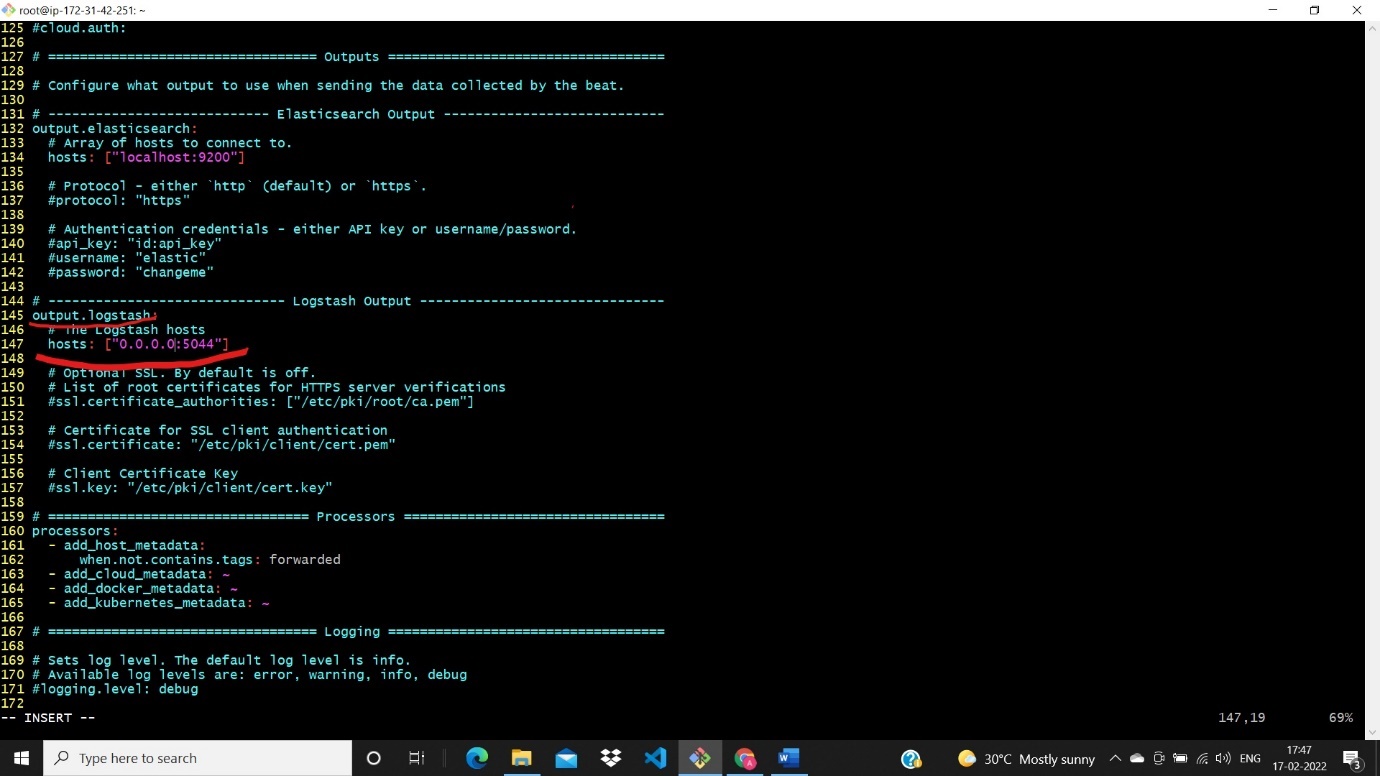
sudo systemctl restart kibana

## ****4. Install and Configure Filebeat on Ubuntu****

**sudo apt-get install filebeat**

**sudo systemctl start filebeat**

**sudo vi /etc/filebeat/filebeat.yml**



## In the above line number 145,147 # REMOVE

## 

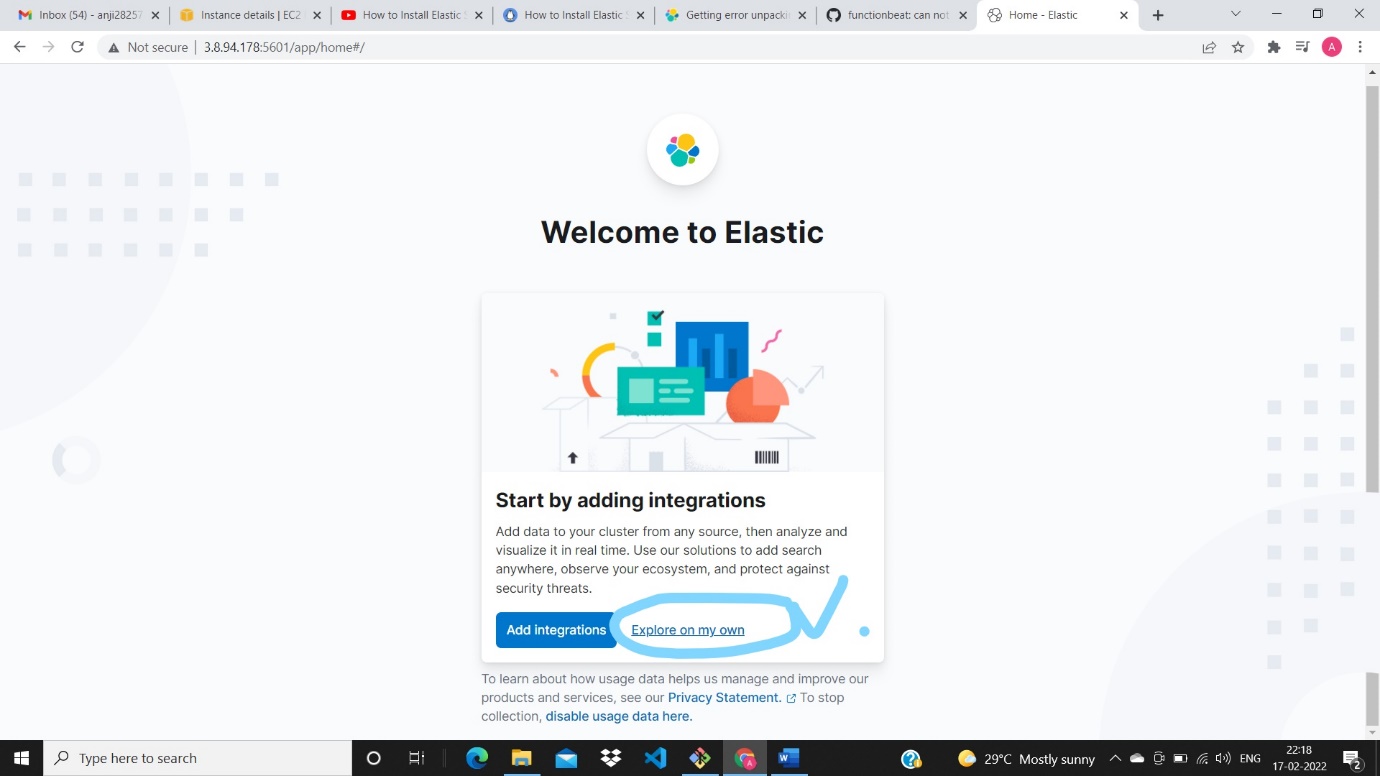
sudo systemctl enable filebeat

sudo systemctl start filebeat

sudo systemctl restart filebeat

sudo filebeat modules enable system

<http://3.8.94.178:5601/app/home#/>

* Check your console o/p
* 

## Fallow on instaragram

## Anjuyadav143