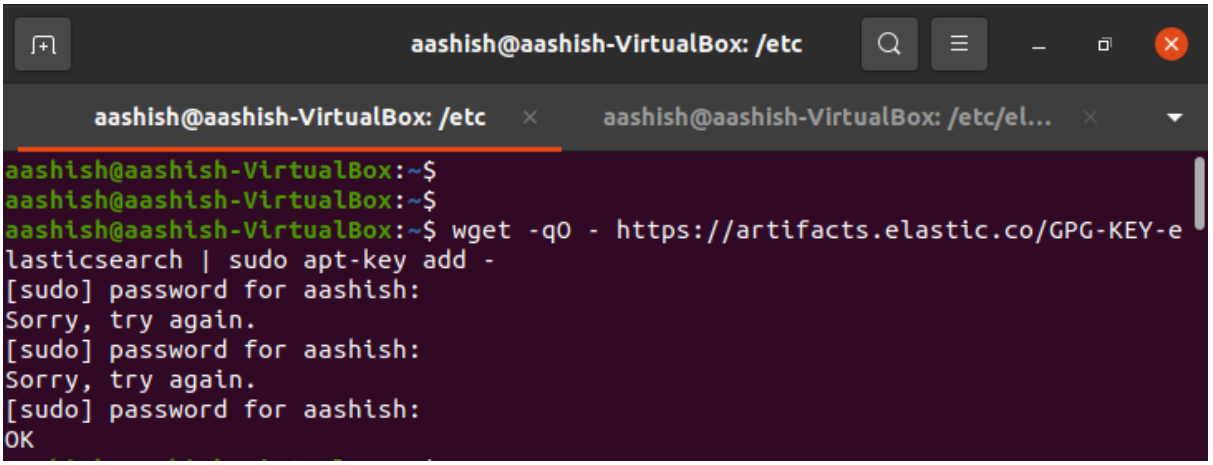
A.
Create two linux servers, server1 => install and configure kibana and elasticsearch with basic username and password authentication server2 => install and configure metricbeat.

Answer:

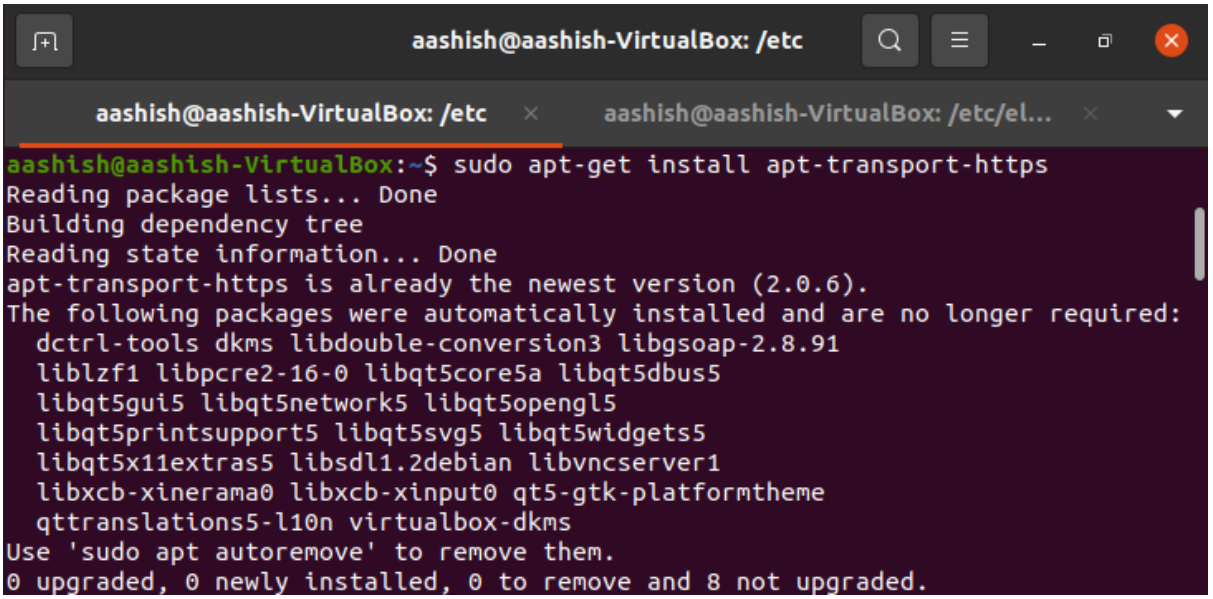
To install **ElasticSearch**, we first need to install the public signing key using the following commands;

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



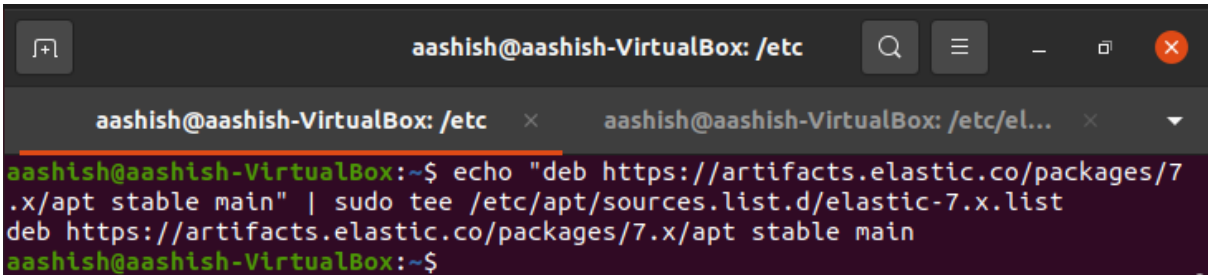
Next, we install apt-transport-https using the following command;

- **sudo apt-get install apt-transport-https**



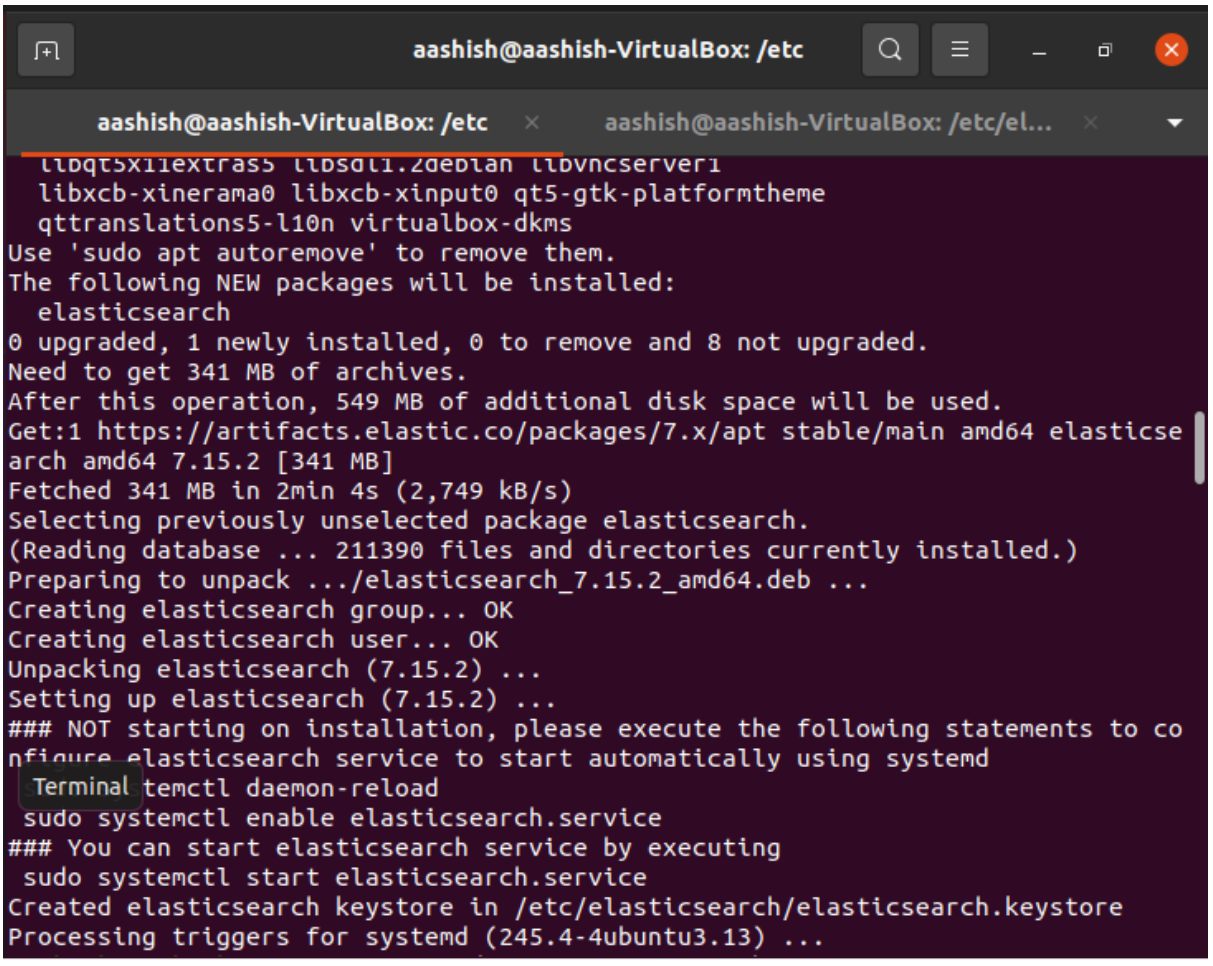
Next we save the repository definition using following command;

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



Then, we install the ElasticSearch after updating the apt using following command;

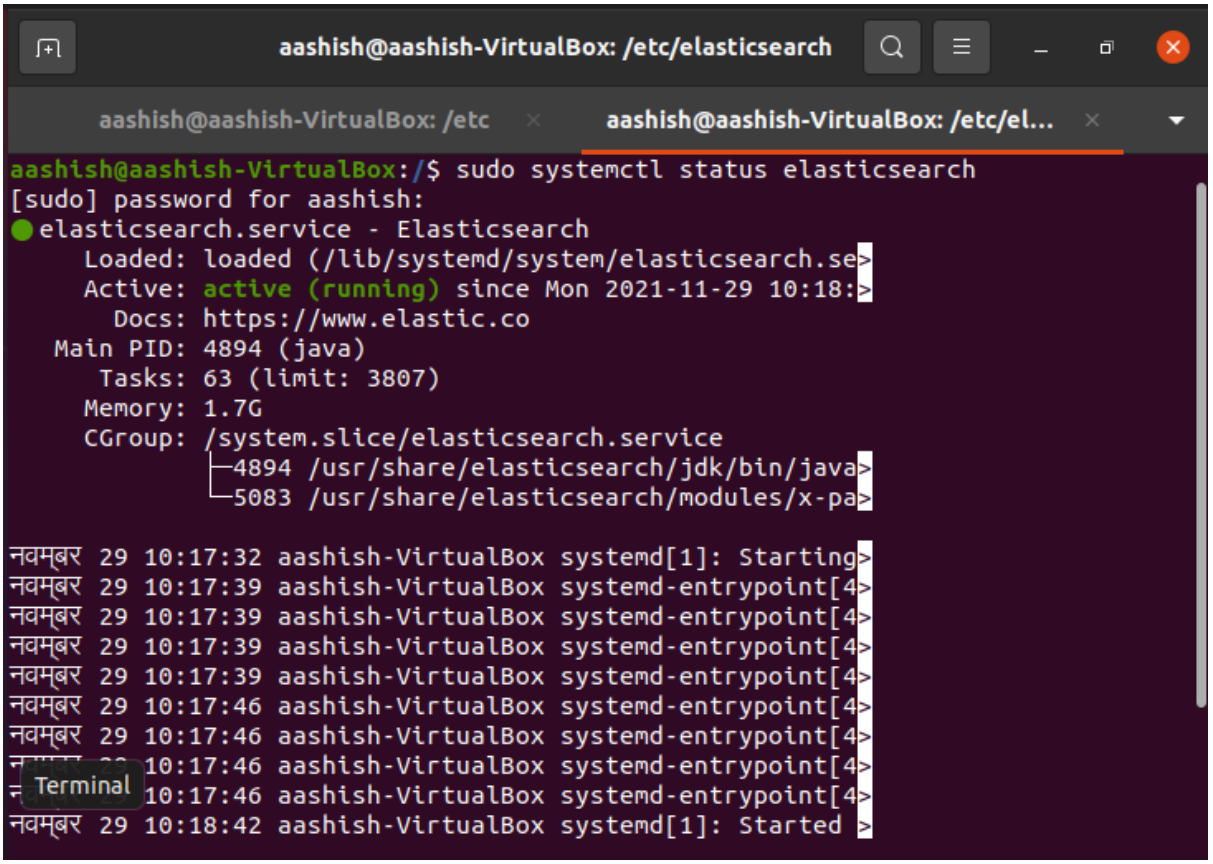
- **sudo apt-get update**
- **sudo apt-get install elasticsearch**



From the above figure, it is clear that elasticsearch has been installed successfully.

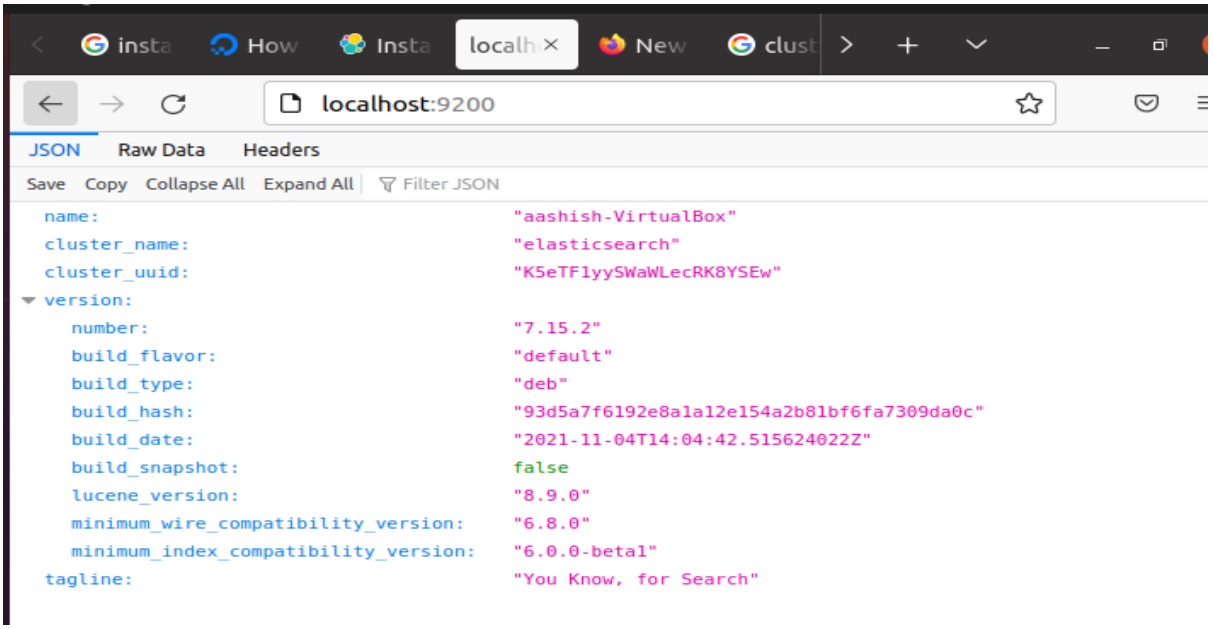
Now, to start, enable and verify the status of elasticsearch, we use following command;

- **sudo systemctl start elasticsearch**
- **sudo systemctl enable elasticsearch**
- **sudo systemctl status elasticsearch**



We can verify the Elastic search via browser also using the url;

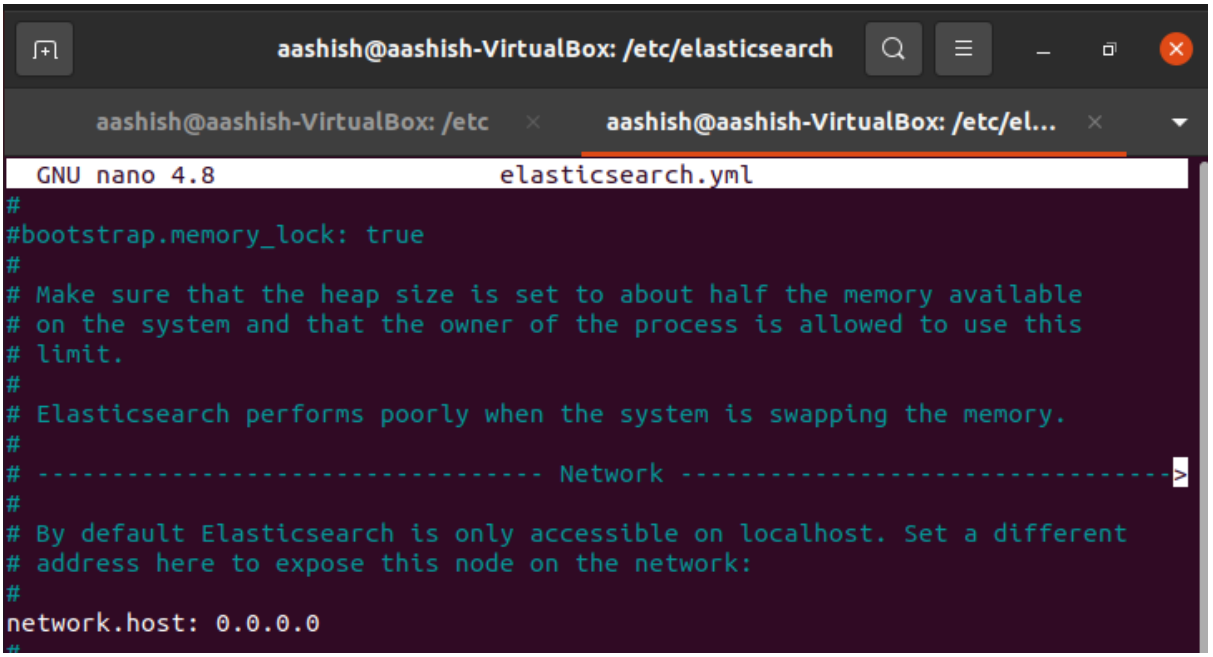
- **http://localhost:9200**



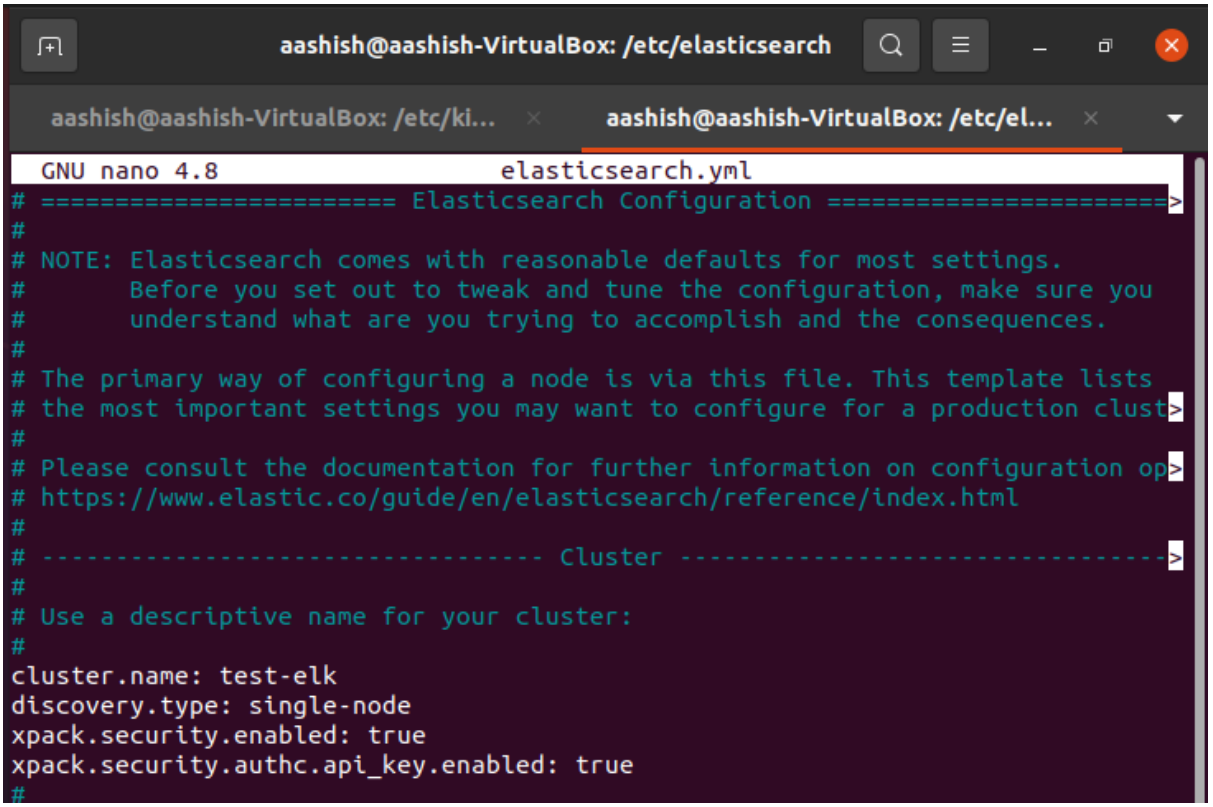
Next, we configure elasticsearch as follows;

- **sudo nano /etc/elasticsearch/elasticsearch.yml**

Then, we change the network host from localhost to 0.0.0.0 to allow all the hosts in **elasticsearch.yml** file.

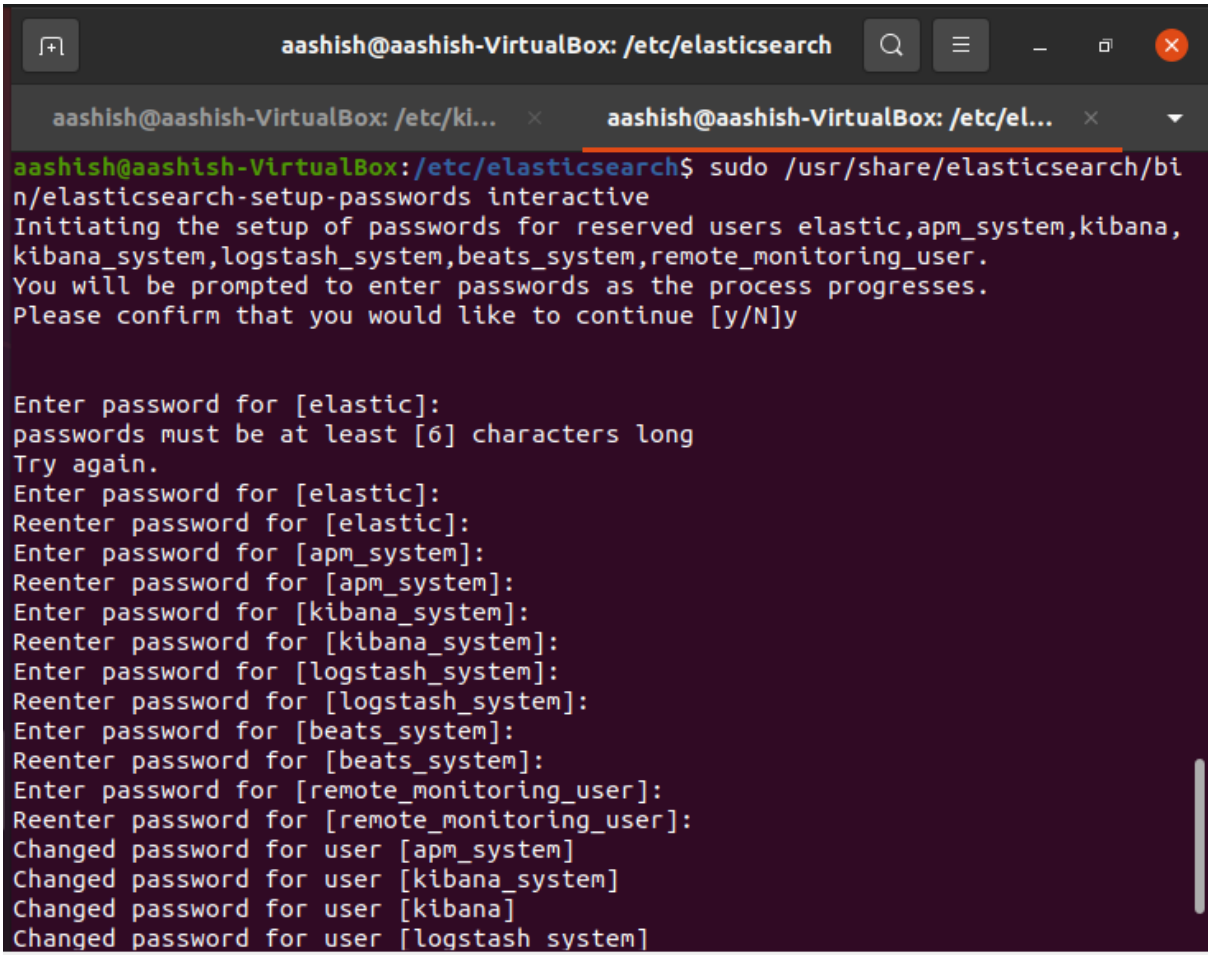


Next, Security was enabled with minimal security as follows;



Then to setup the password for all system,we do following things;

- **sudo /usr/share/elasticsearch/bin/elasticsearch-setup-passwords interactive**

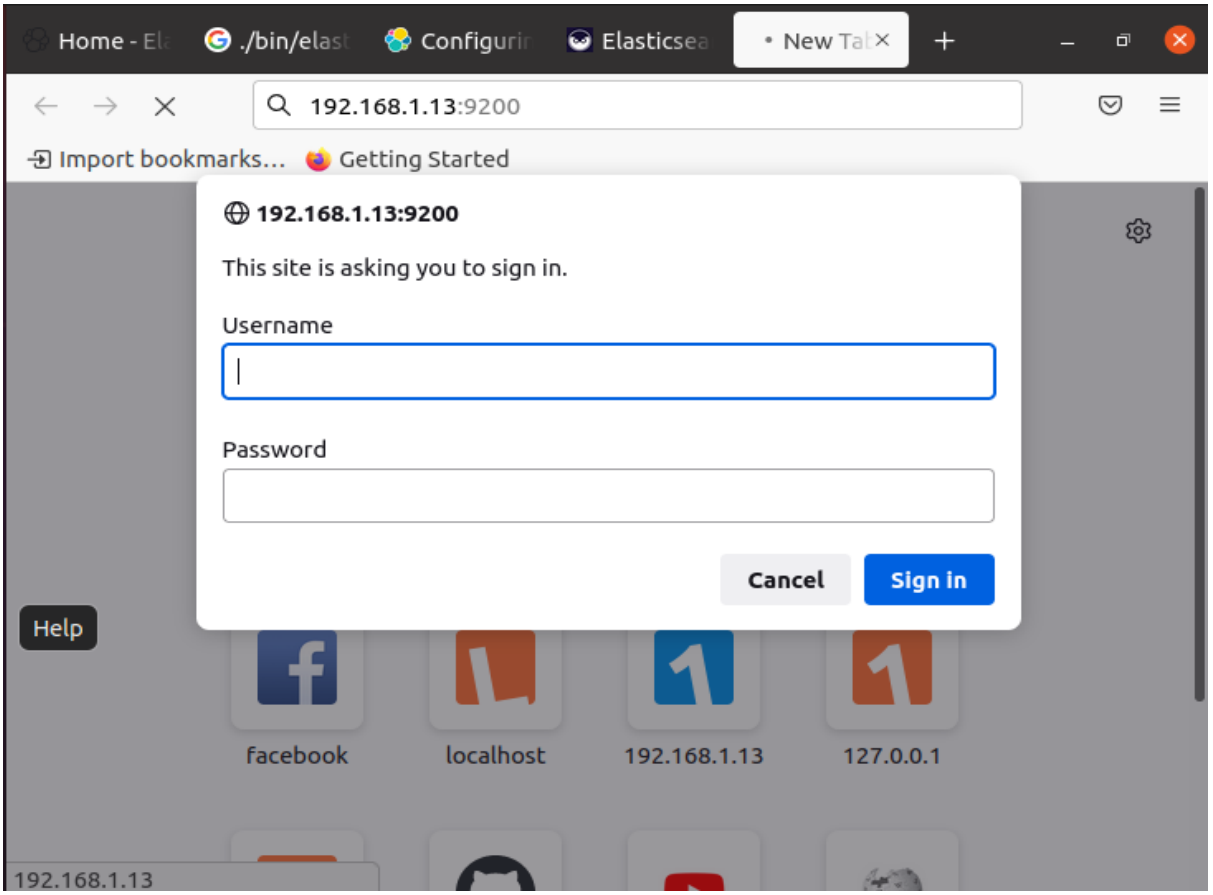


We save and exit. Then we restart the elasticsearch using command;

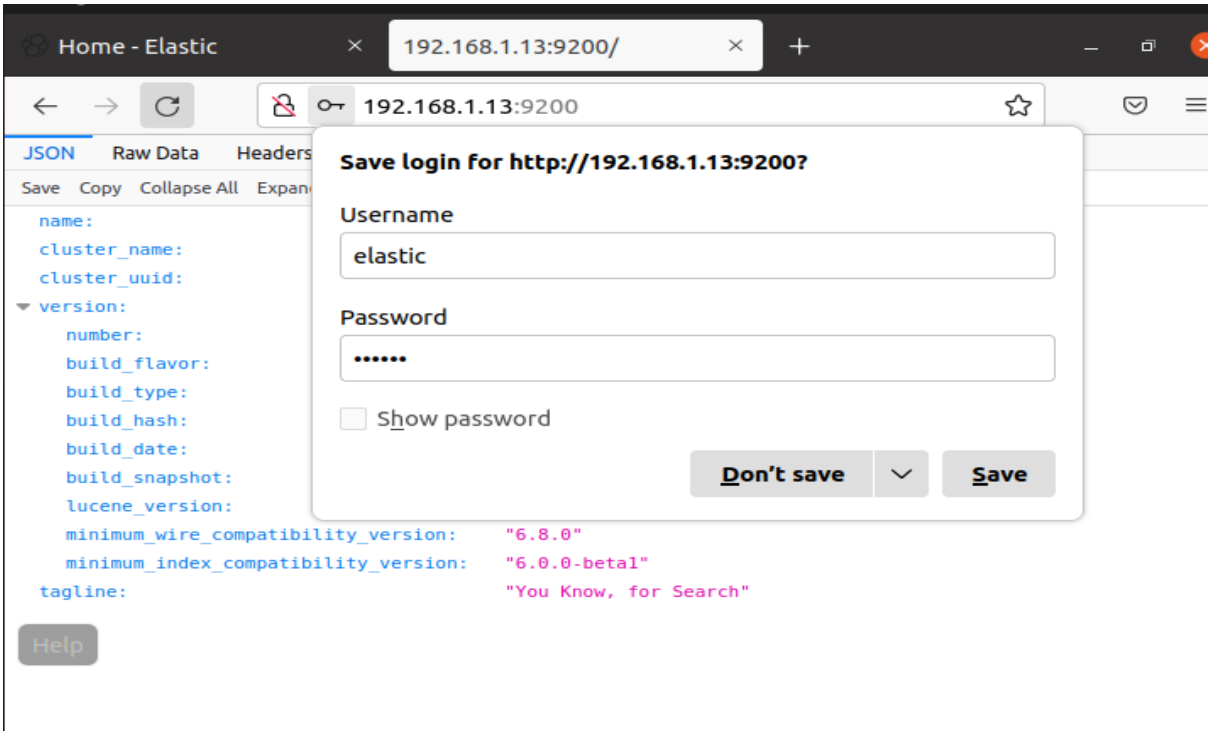
- **sudo systemctl restart elasticsearch**

After configuring the elasticsearch, now we can easily access the elasticsearch using our host ip as follows;

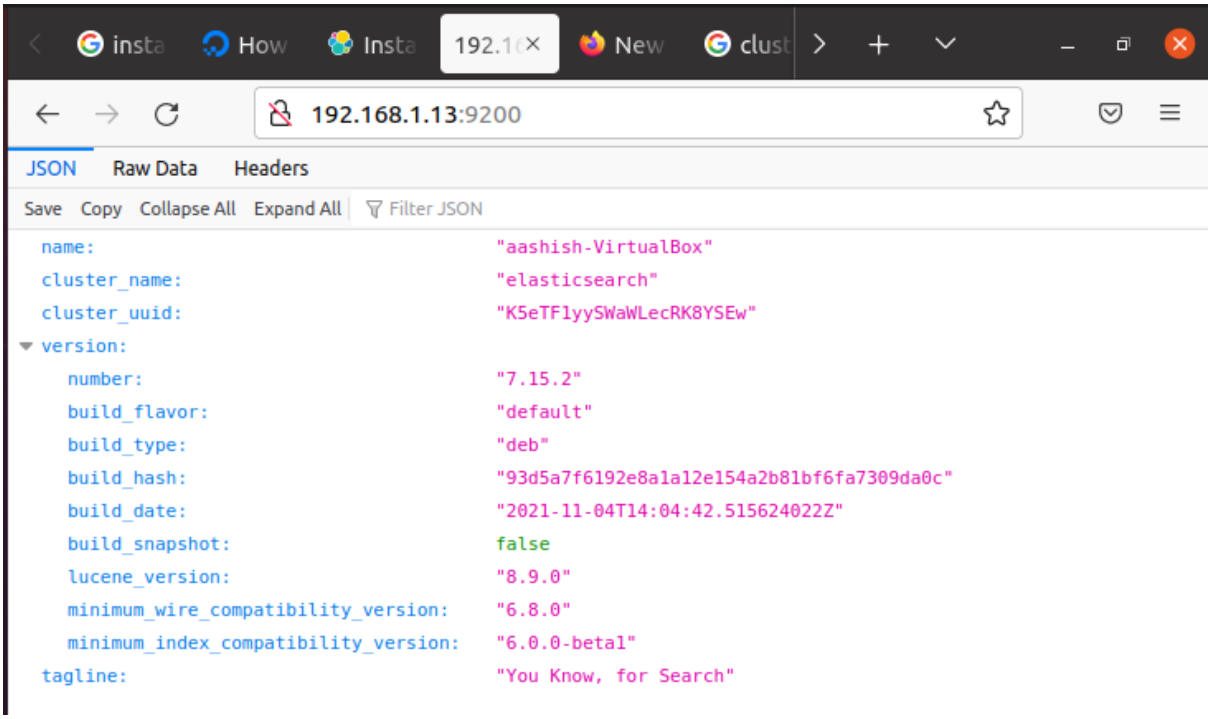
Now, to verify the security we browsing the url as follows;



We use username and password as follows to login to the elasticsearch.



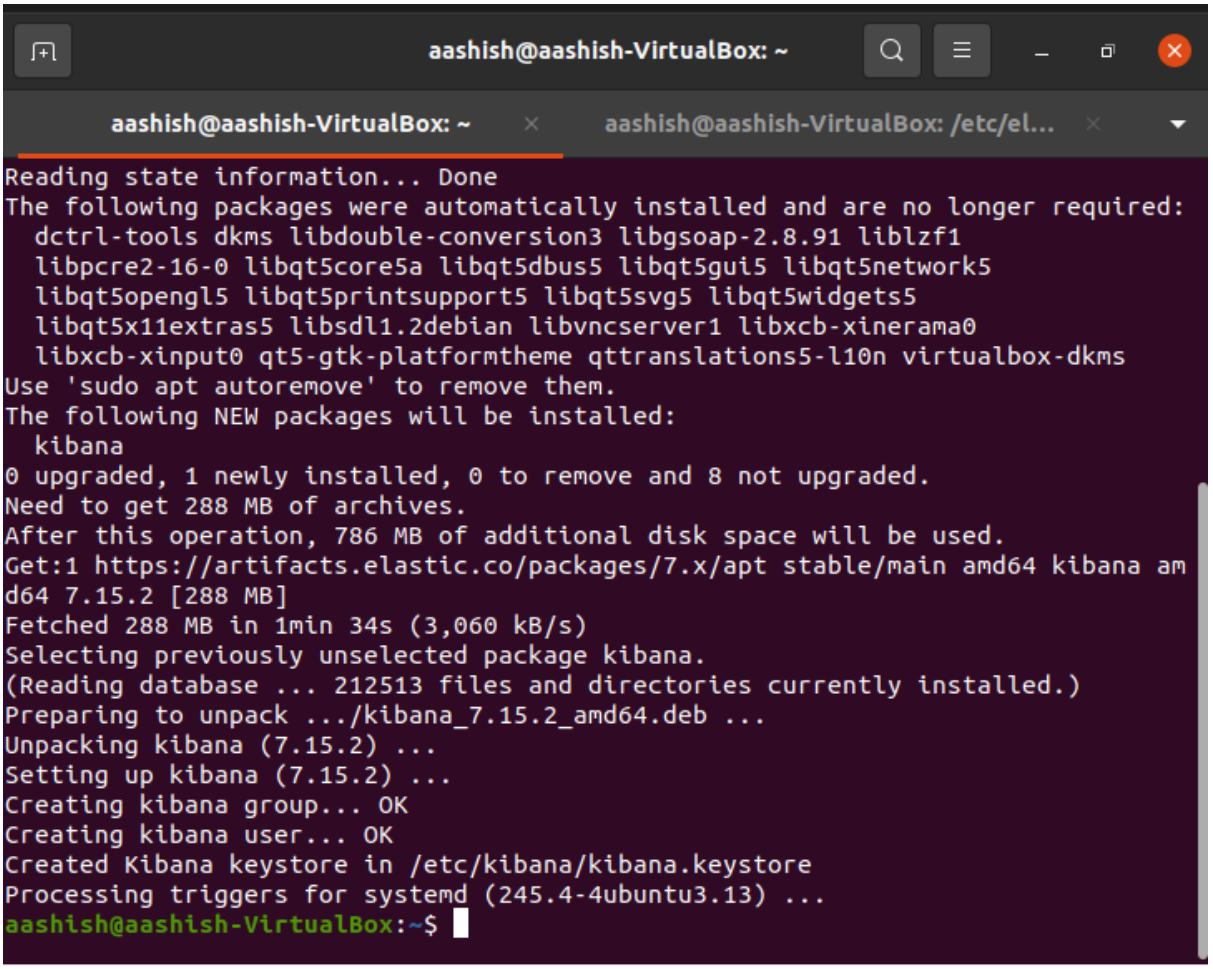
Hence, we are logged in to the elastic search successfully.



Next, we install **Kibana**.

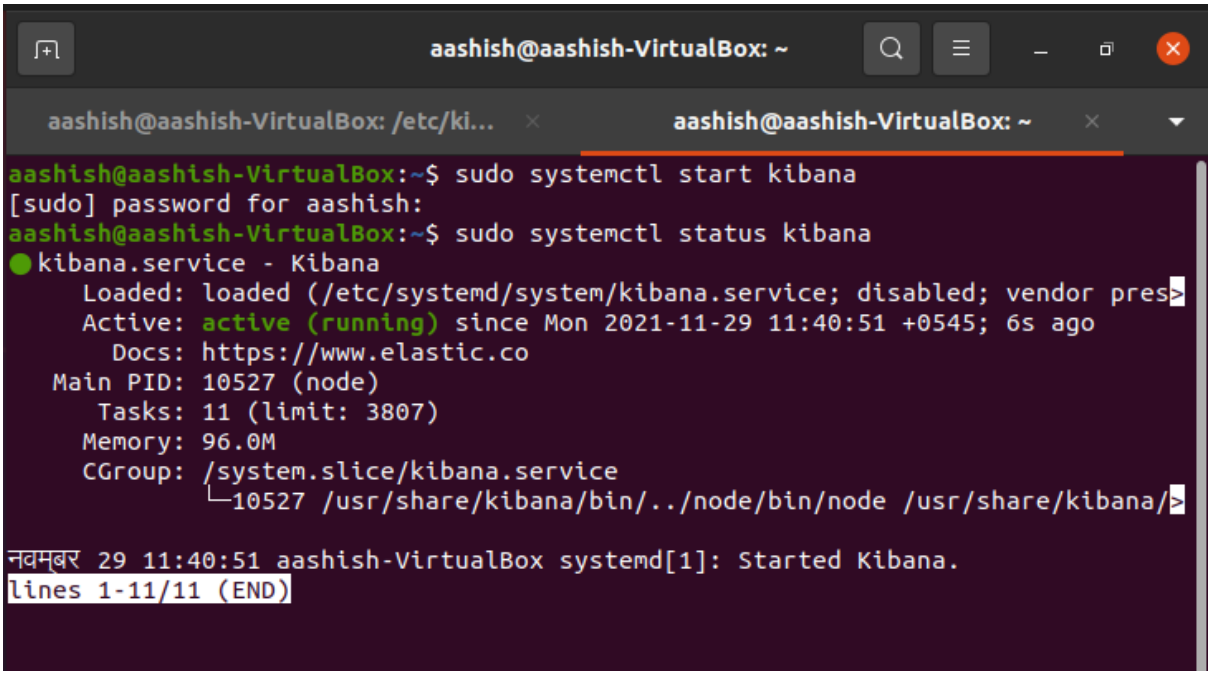
To install kibana, we need the public signing key, apt-transport-https package and save the repo definition. Since we have already done it for elastic search, we don't need to do it again. We can simply run the command;

- **sudo apt-get update**
- **sudo apt-get install kibana**



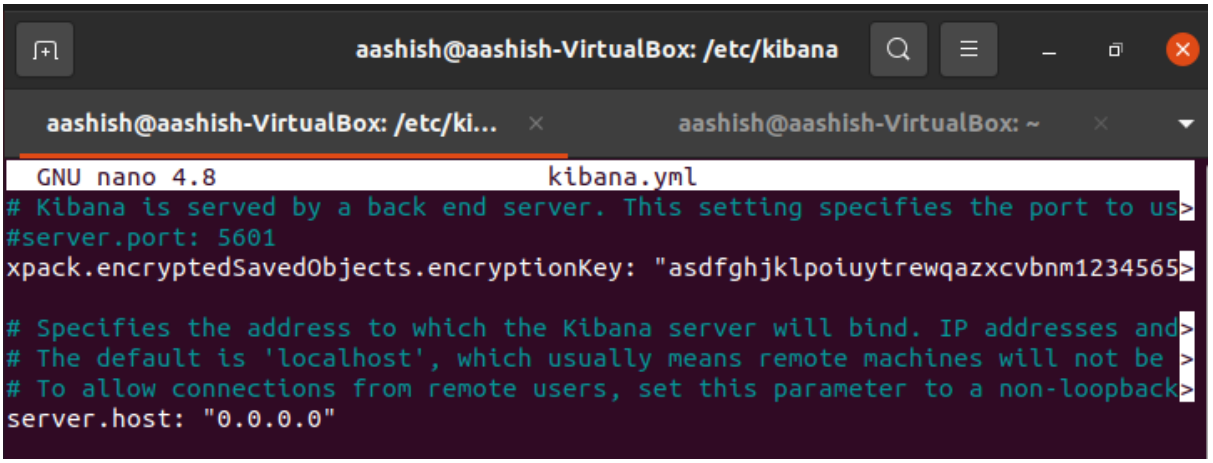
Next, we check start, enable and check the status of kibana using the following commands;

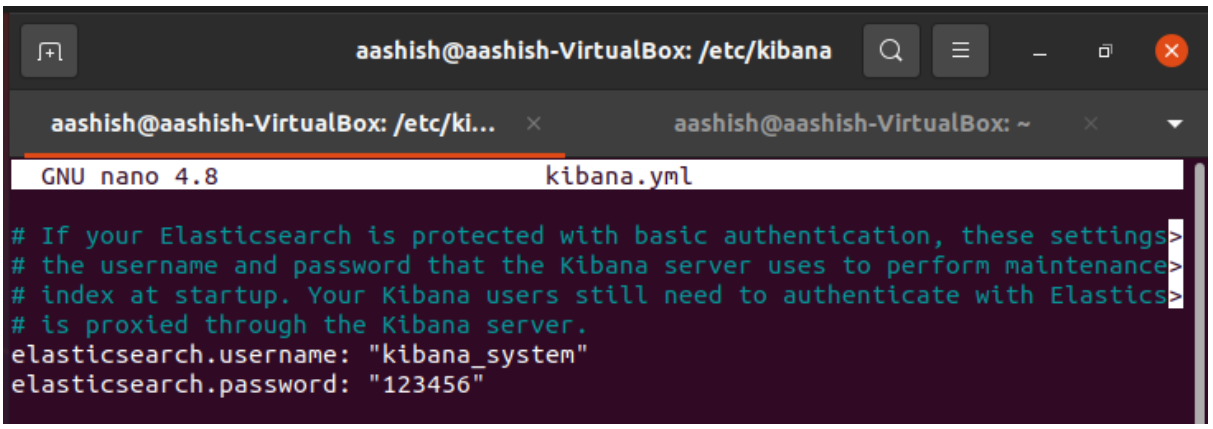
- **sudo systemctl start kibana**
- **sudo systemctl enable kibana**
- **sudo systemctl status kibana**



Next, we configure Kibana by editing the kibana.yml file as follows;

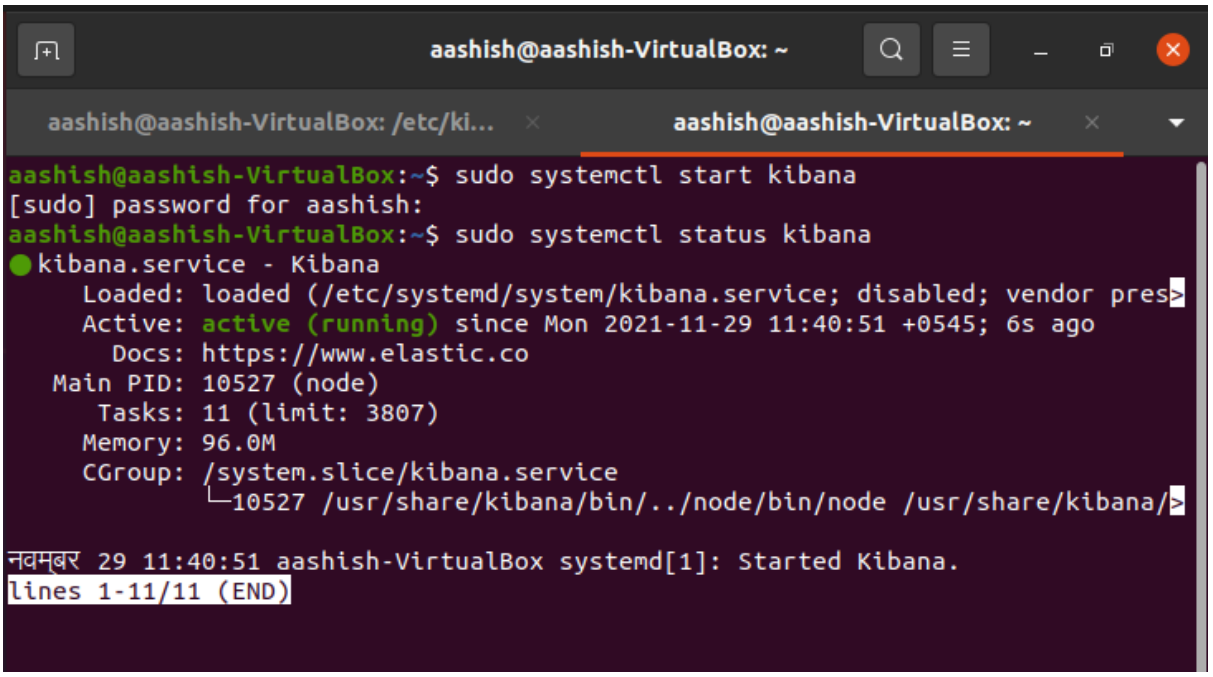
- **sudo nano /etc/kibana/kibana.yml**





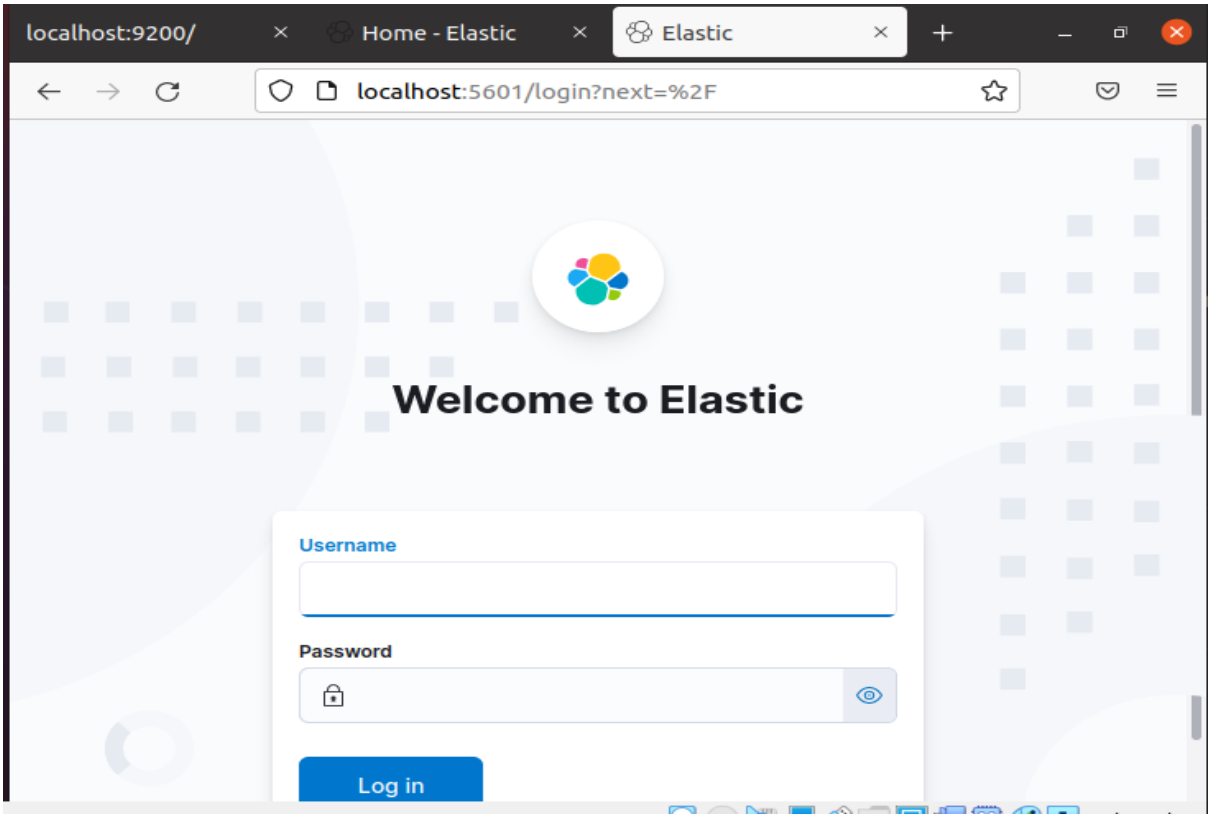
Then, we restart the kibana using;

- **sudo systemctl restart kibana**

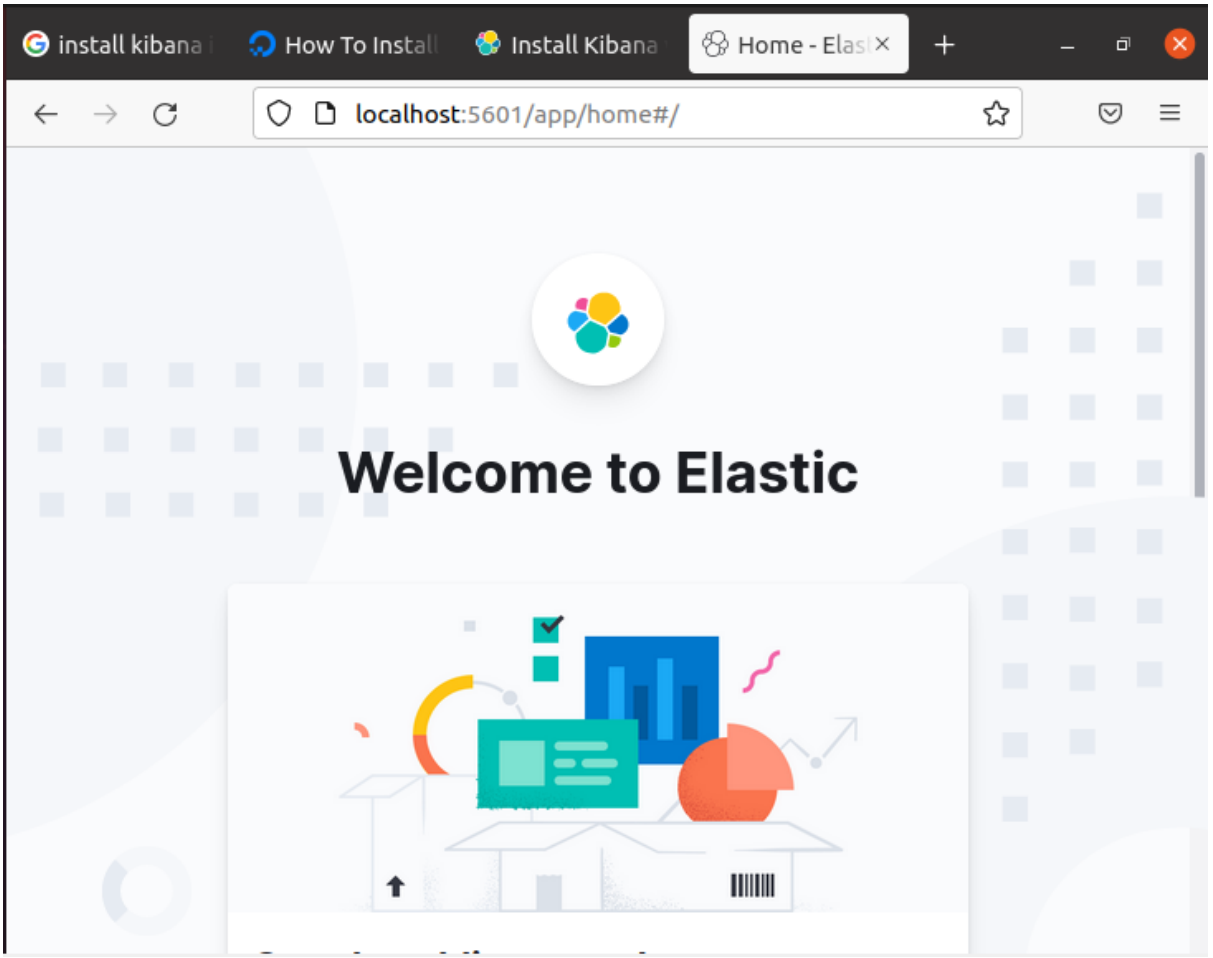


Then, we verify the Kibana via our web browser with url;

- http://192.168.1.13:5601 **or,**
- **http://localhost:5601**



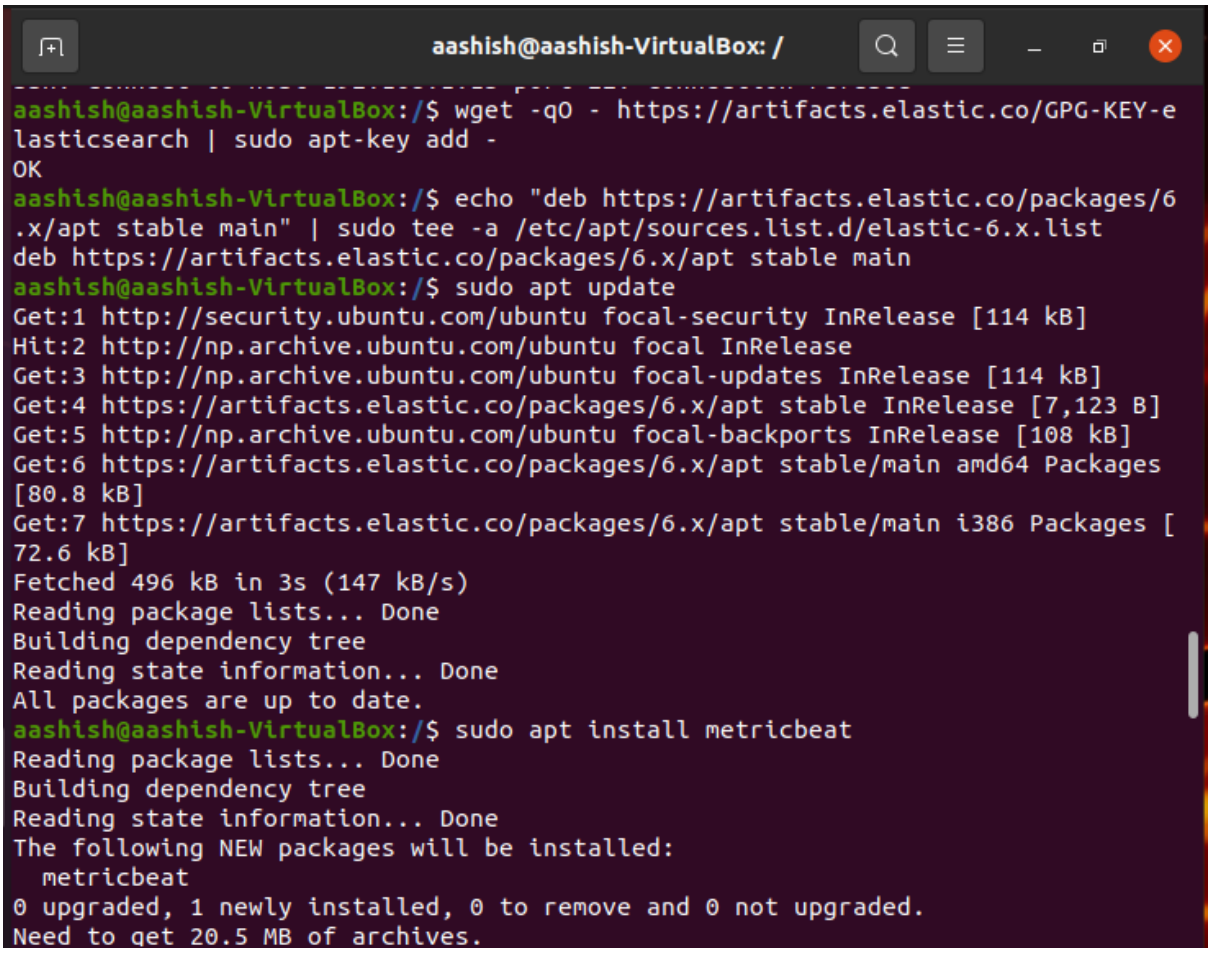
Next, we login to Kibana using the login credentials and get started with Kibana as follows;



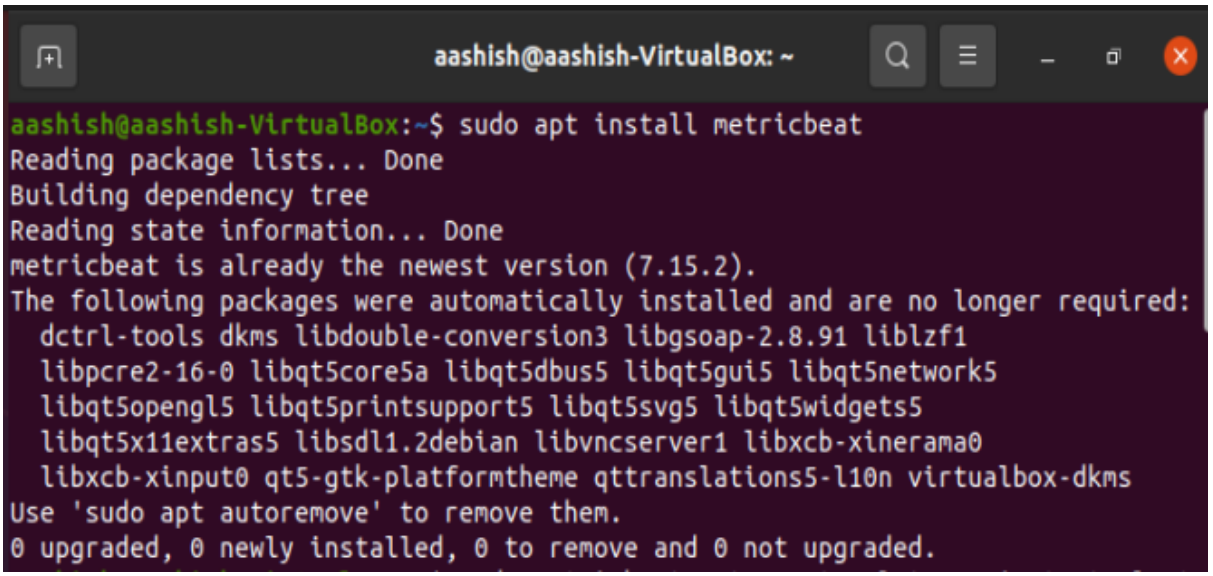
Next, we install **Metricbeat**.

We have another server or vm to install the metricbeat. To install metricbeat, we need the public signing key, apt-transport-https package and save the repo definition using the following commands on server2 as follows;

- **wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -**
- **sudo apt-get install apt-transport-https**
- **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 update**
- **sudo apt install metricbeat**

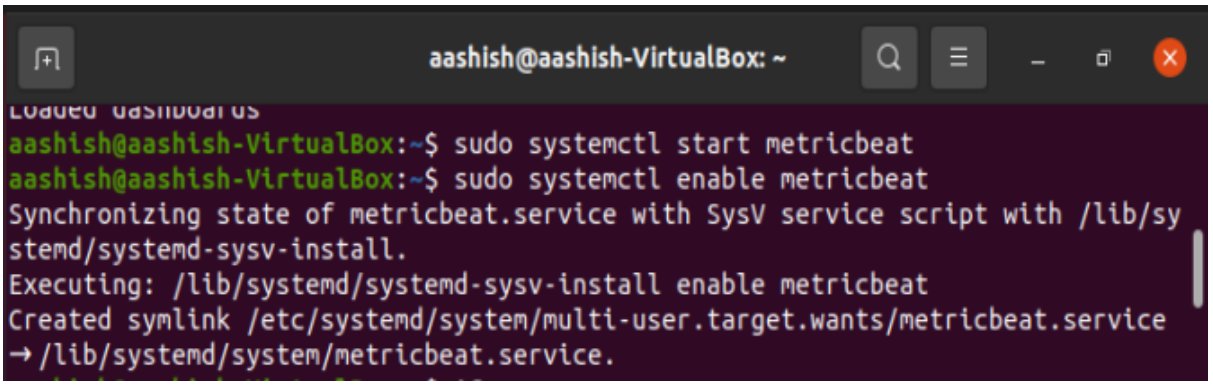


Metricbeat was installed successfully.



Then, metricbeat was started and enabled using the following command;

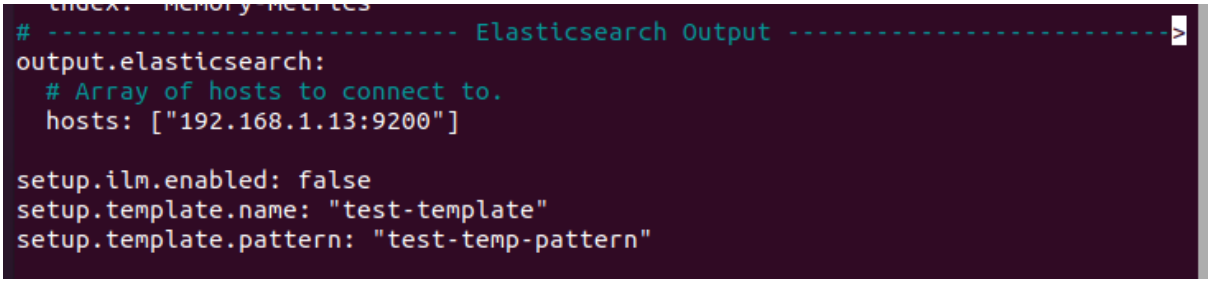
- **sudo systemctl start metricbeat**
- **sudo systemctl enable metricbeat**



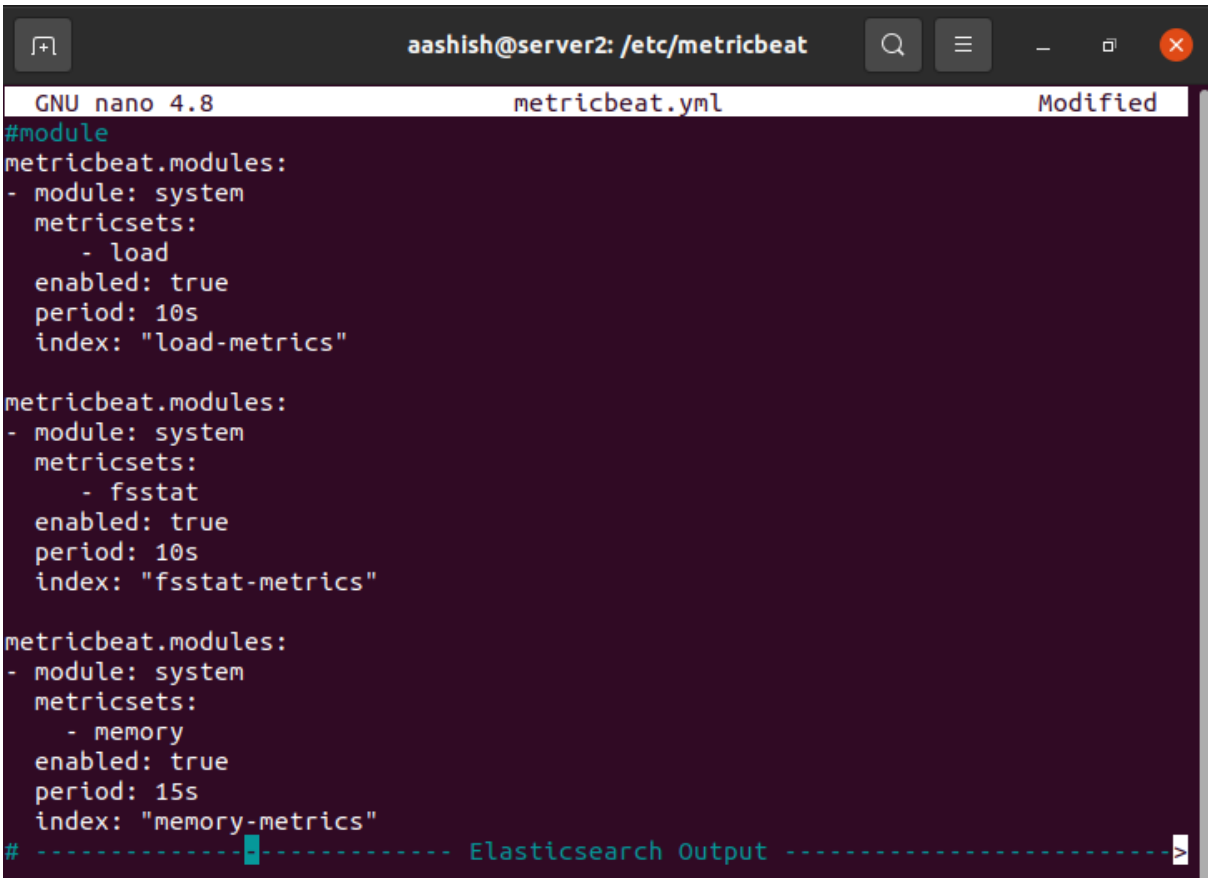
We used sudo hostnamectl set-hostname server2 to change the hostname.

Next, we edit the **metricbeat.yml** file to configure metric beat as follows;

- **sudo nano /etc/metricbeat/metricbeat.yml**

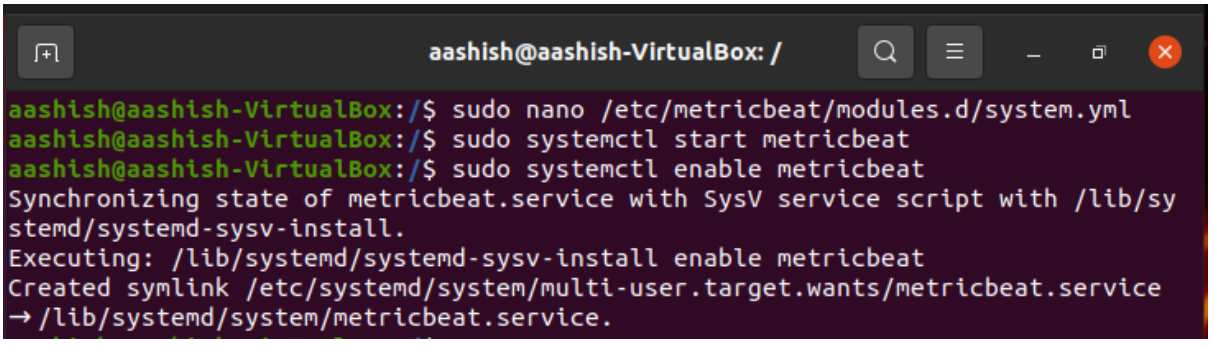


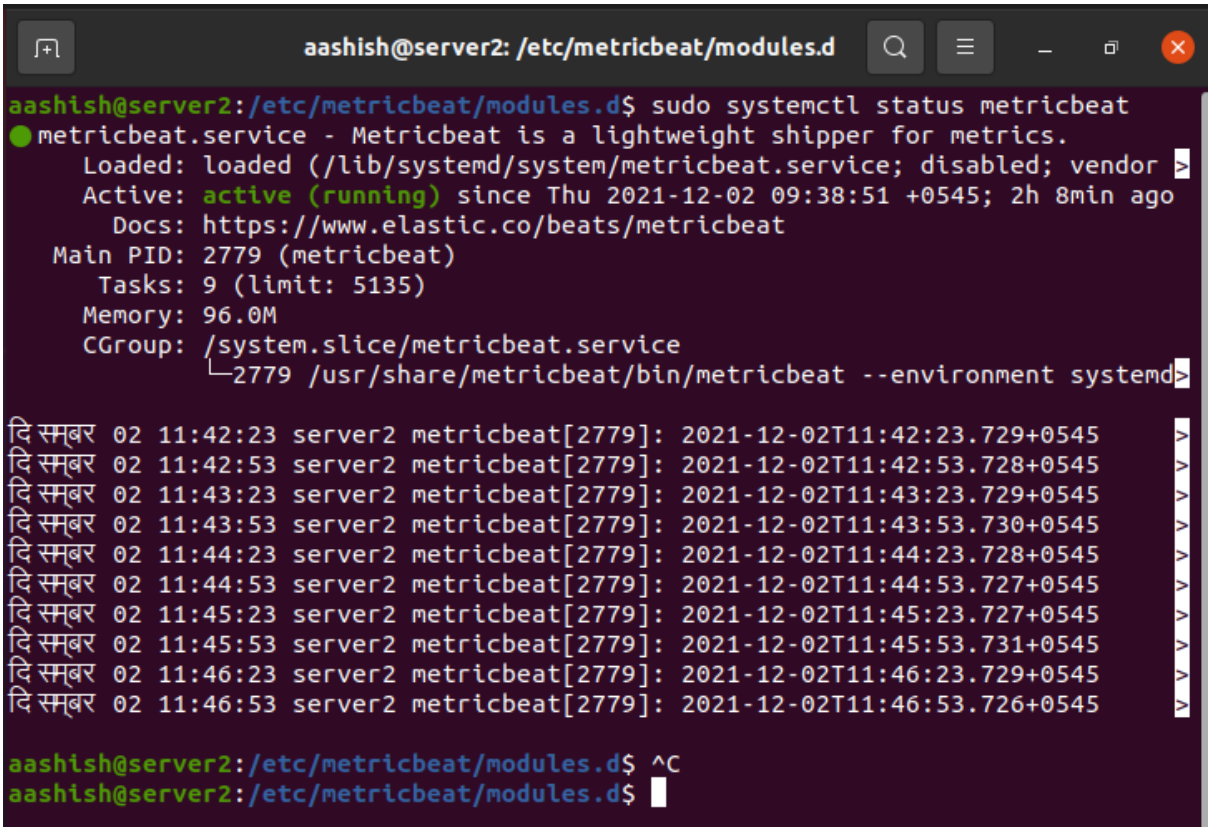
Then, we add metrics as follows;



We save and exit the file. Then we restart the metricbeat using command;

- **sudo systemctl restart metricbeat**
- **sudo systemctl enable metricbeat**
- **sudo systemctl status metricbeat**





Hence, metricbeat is also installed successfully on the server 2.