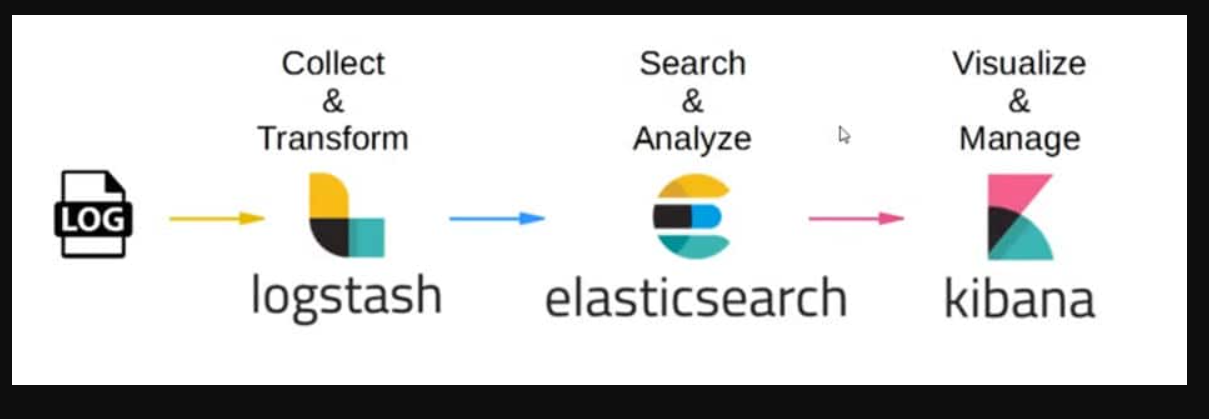
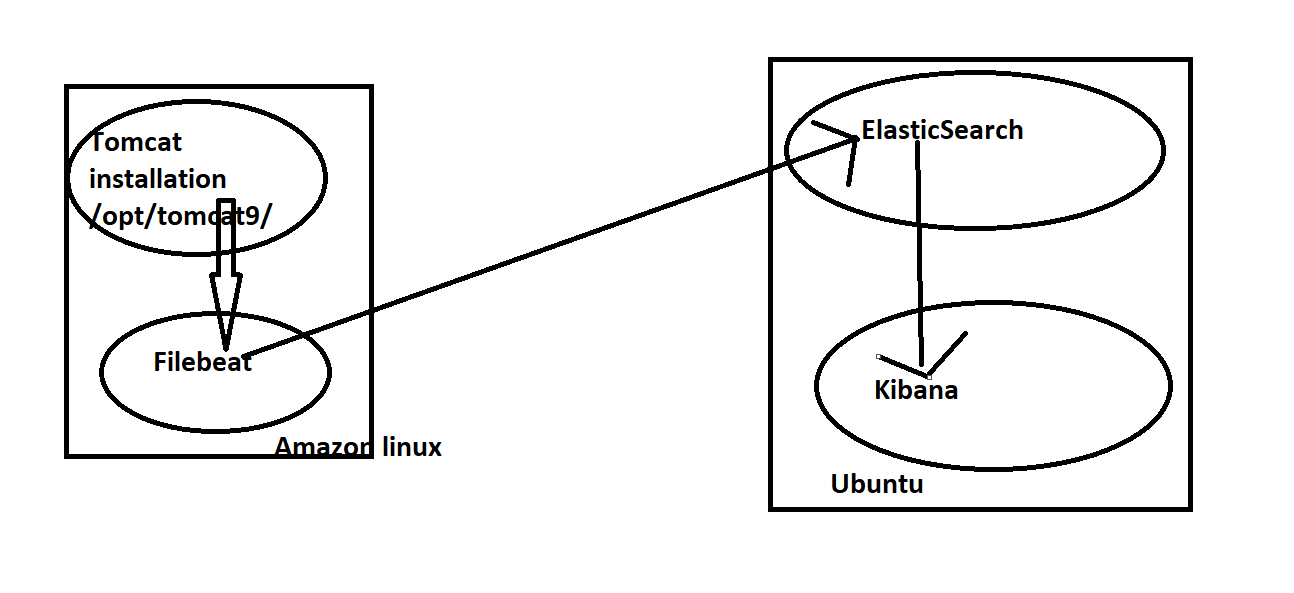
Note :

we have taken Ubuntu based instance for installation ELK components

For application layer we can take any of our choice.





**App Layer** : Tomcat

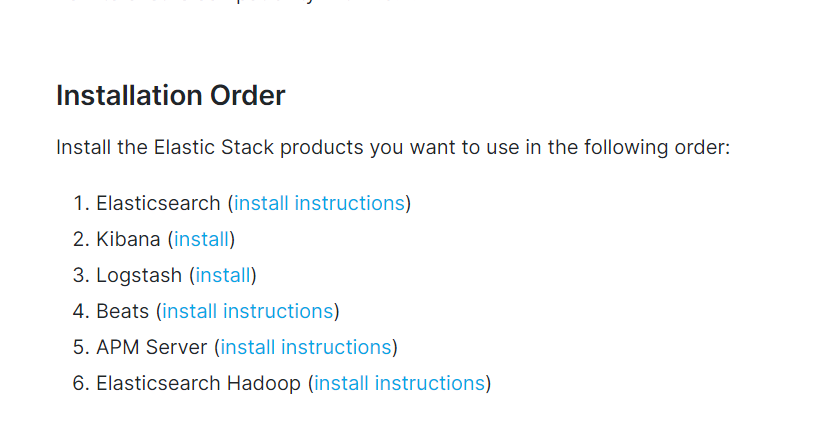
**App Layer logs** : /opt/tomcat9/logs/\*.logs

ELK : <https://www.elastic.co/guide/en/elastic-stack/current/installing-elastic-stack.html>

Goto the <https://www.elastic.co/guide/en/elastic-stack/current/installing-elastic-stack.html>

**Important: Version matching**

When installing the Elastic Stack, you must use the same version across the entire stack. For example, if you are using Elasticsearch 7.9.2, you install Beats 7.9.2, APM Server 7.9.2, Elasticsearch Hadoop 7.9.2, Kibana 7.9.2, and Logstash 7.9.2

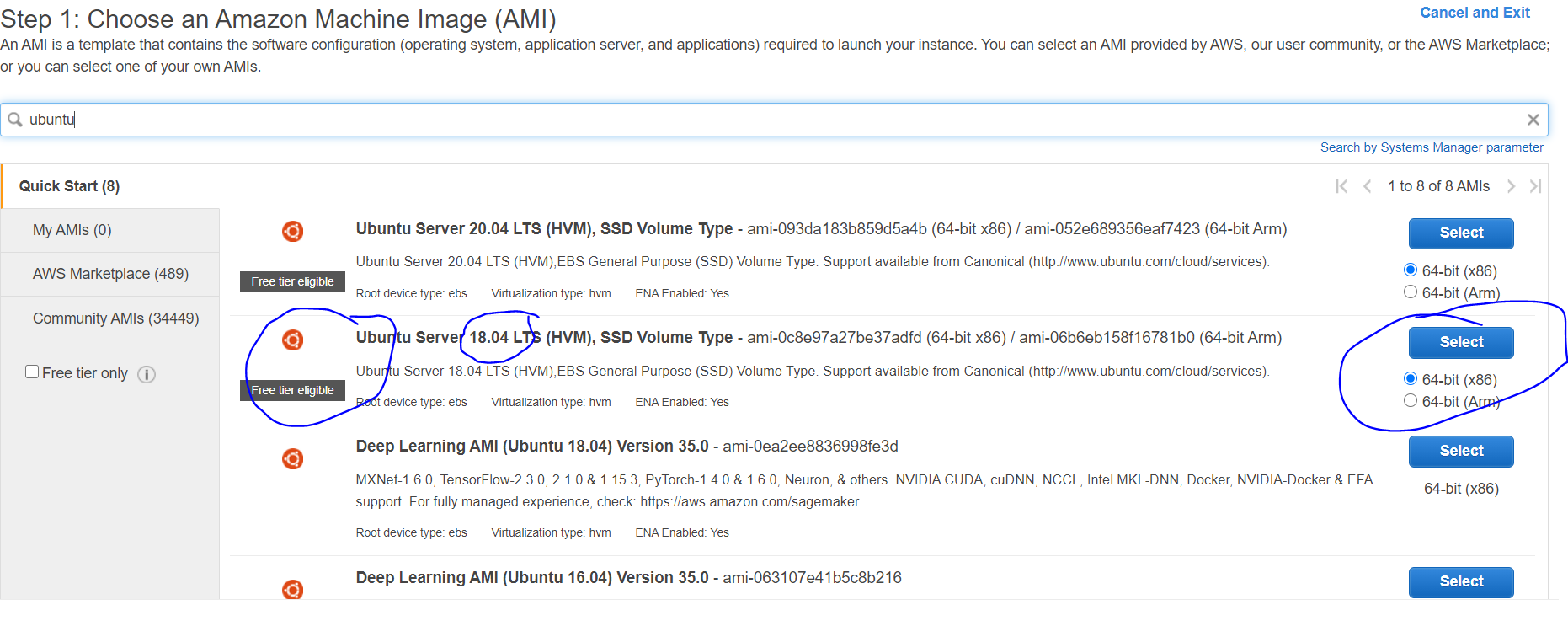


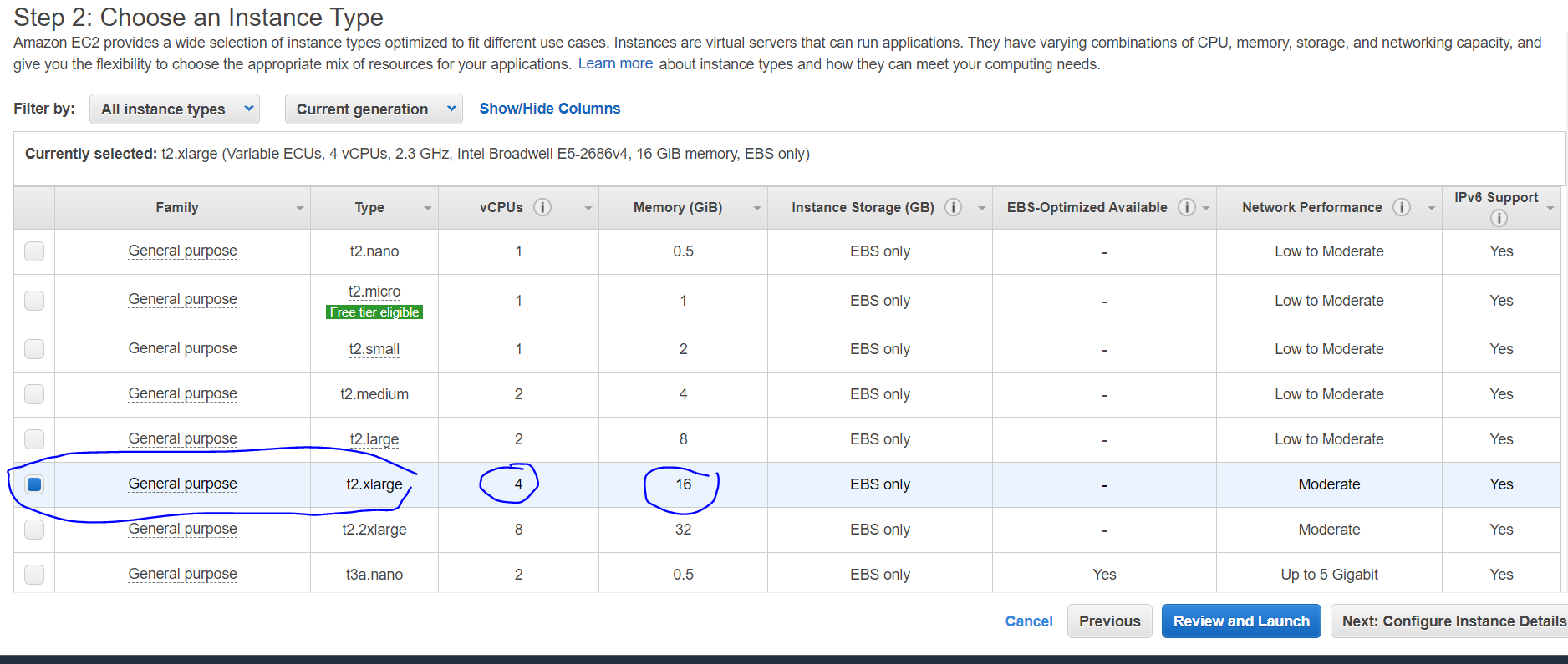
In Above we are choosing 3 components

1. ElasticSearch
2. Kibana
3. Beats(Filebeat)

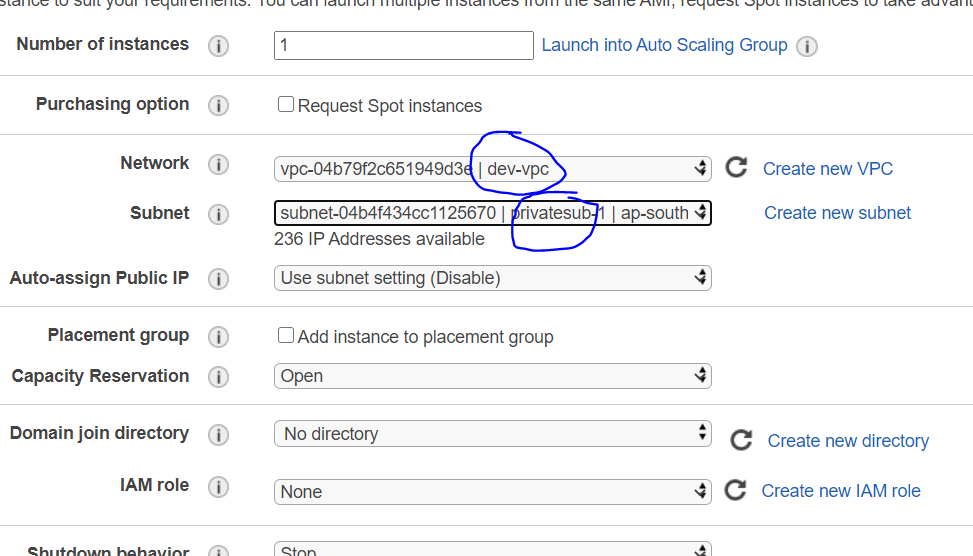
1 . ElasticSearch setup in the ubuntu

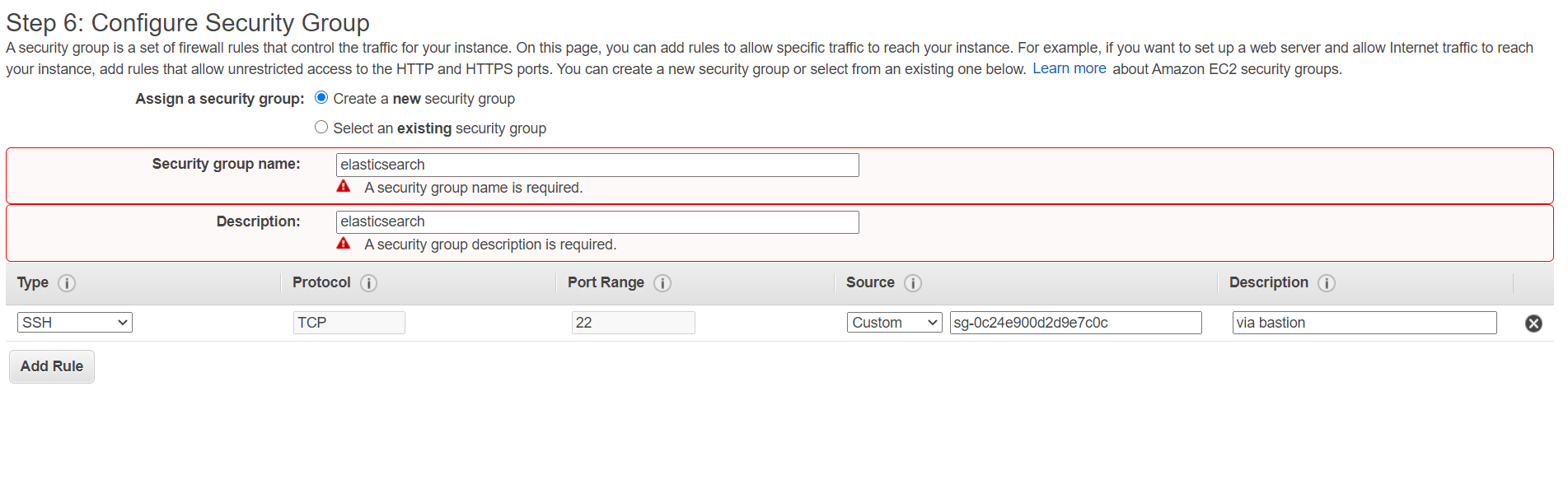
Create the Ubuntu machine in the subnet you choose (we took total in private subnets)





Select the your vpc / default vpc and also subnet

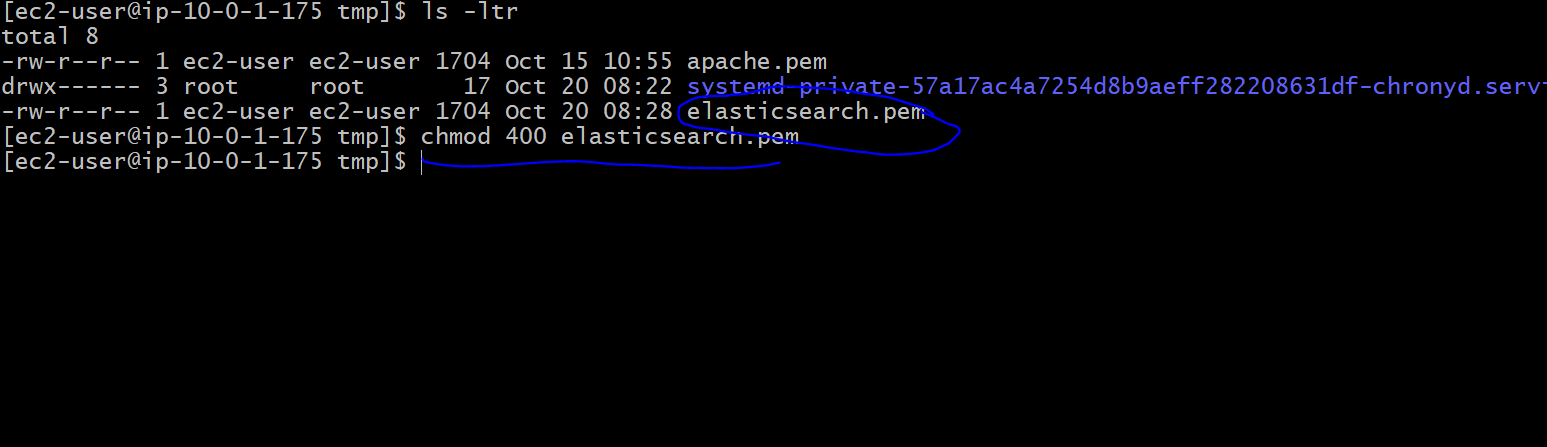


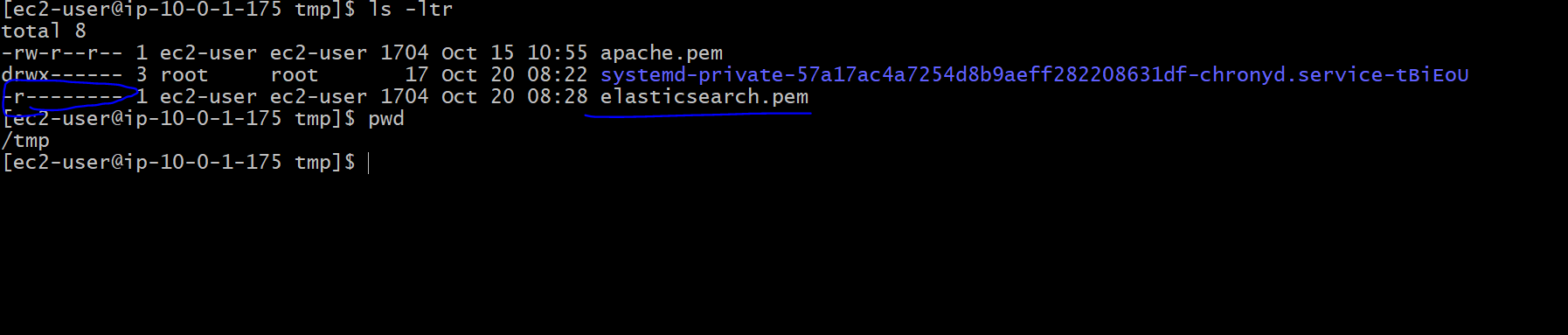


For now only admin security group (22) allowed from bastion.

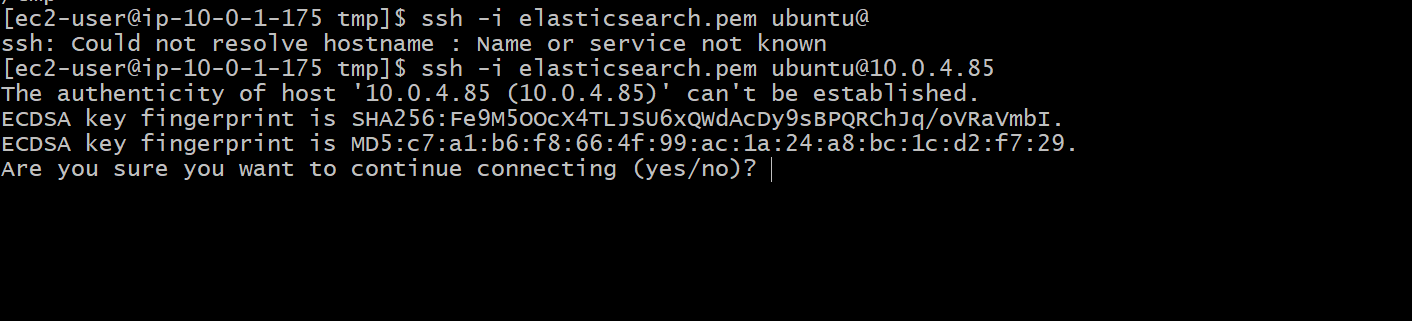
Next we will add few more security groups rules to the elasticsearch security group.

Launch and connect to the Ubuntu(elasticsearch) node via bastion



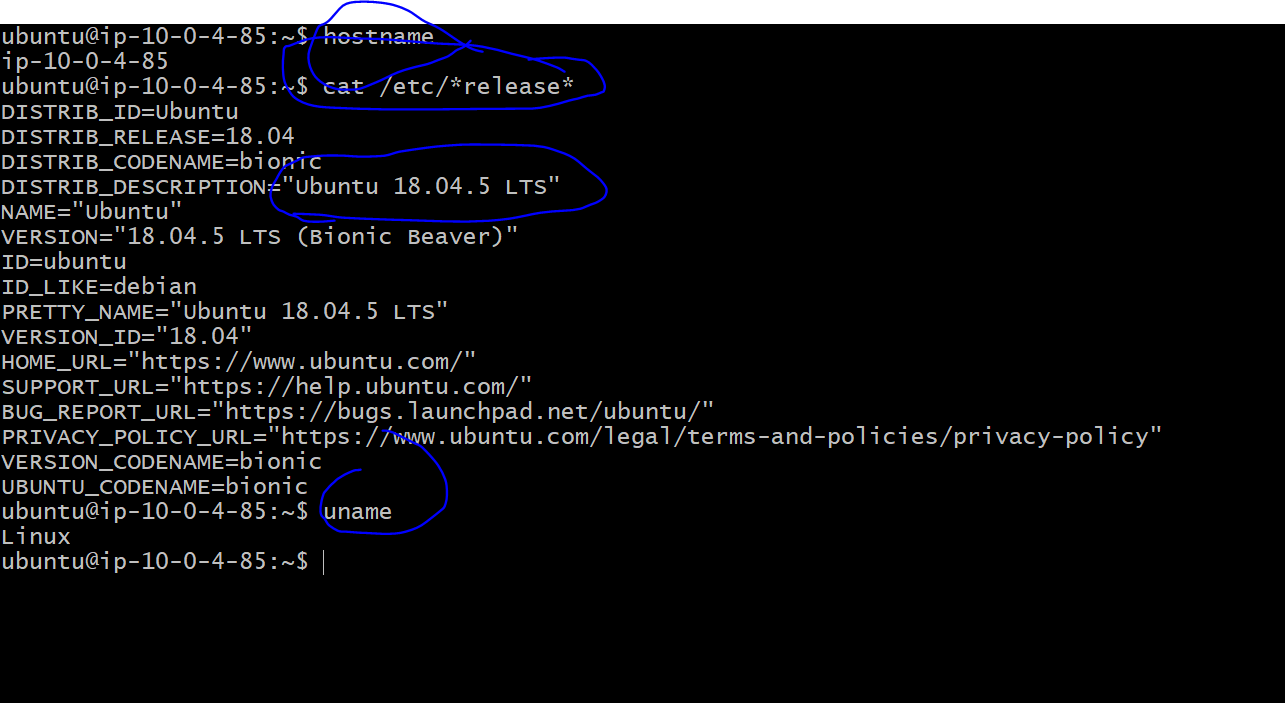


SSH to the elasticsearch node from bastion

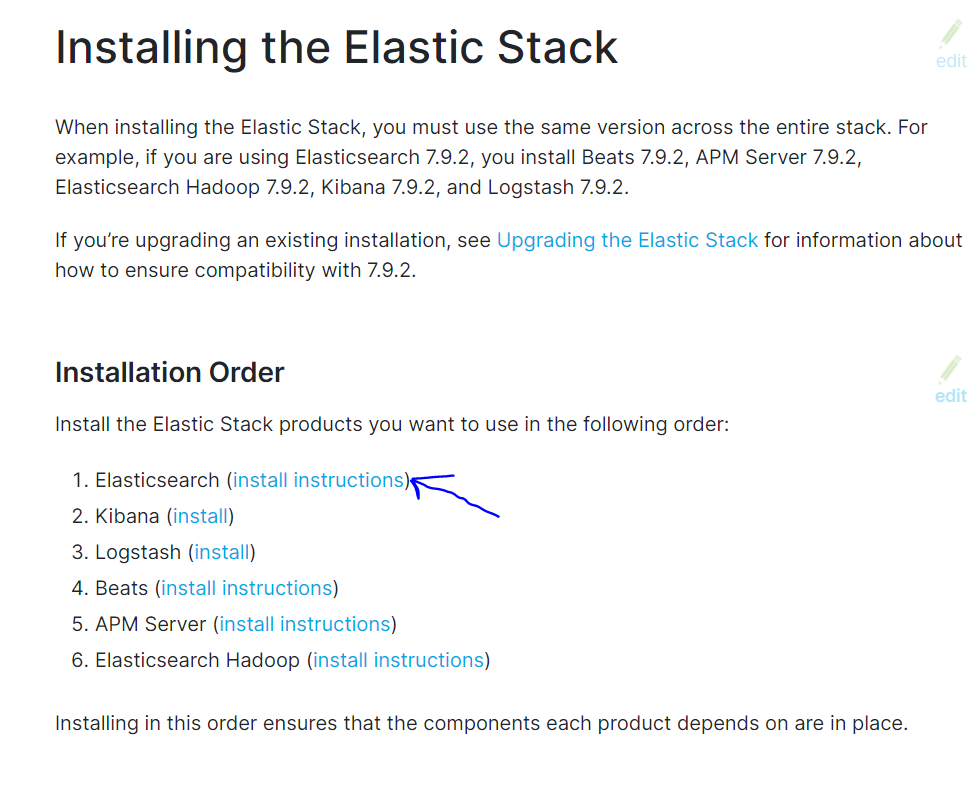


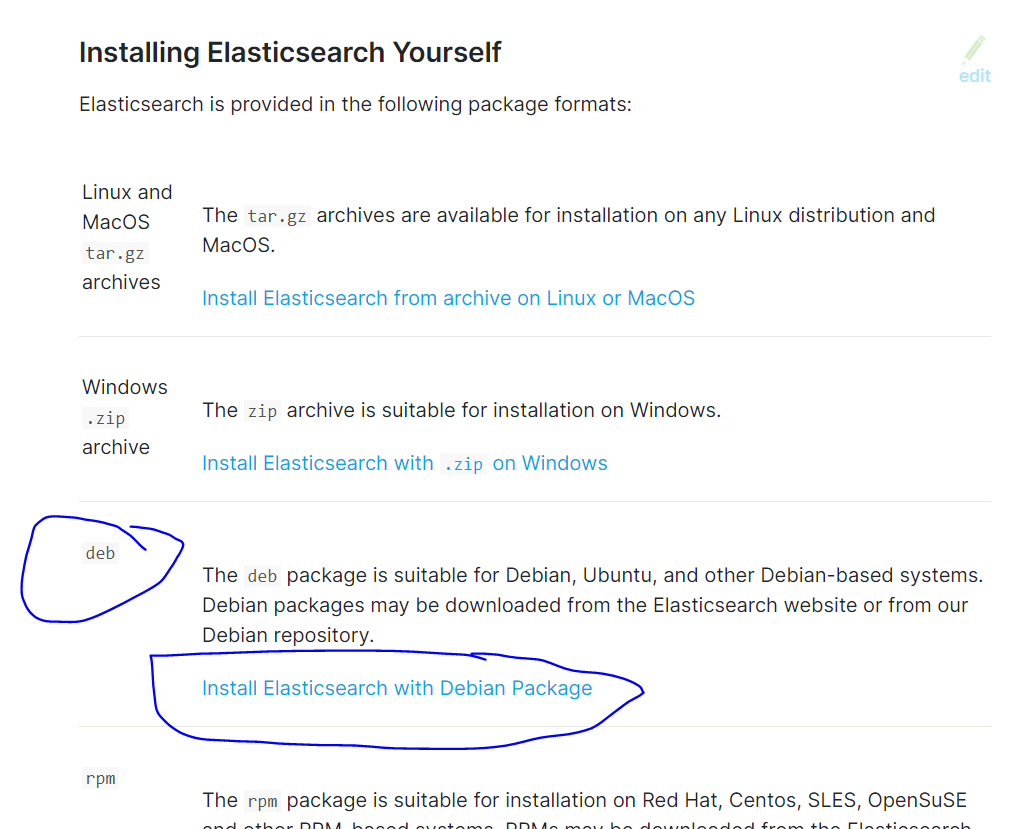
ssh -i elasticsearch.pem [ubuntu@10.0.4.85](mailto:ubuntu@10.0.4.85)

Check basic details after login

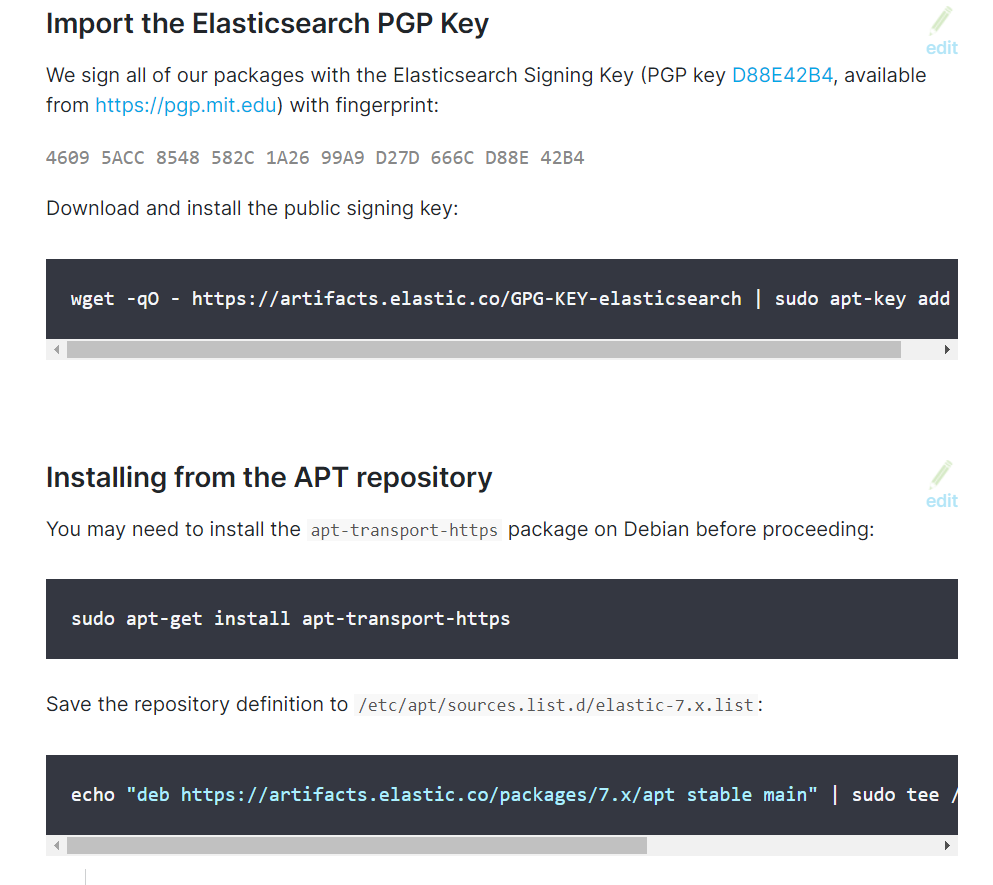


After login install the packages of elasticsearch on the Ubuntu





Click on the above link



Run one by one on Ubuntu node

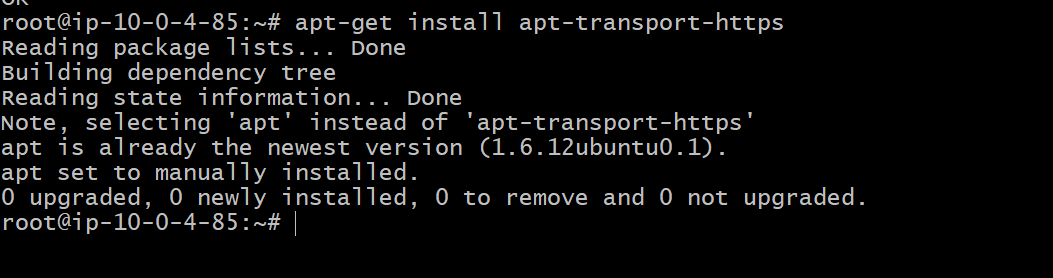
Switch to the root user from Ubuntu

Run all the commands with the root user

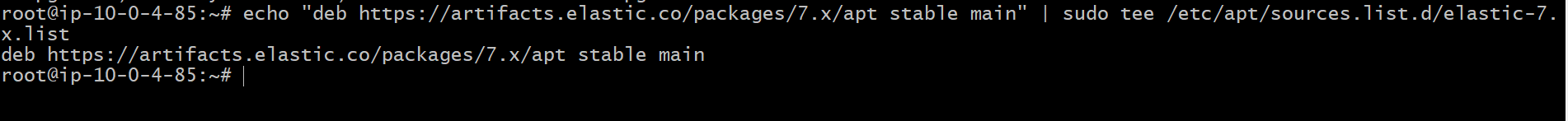
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -



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



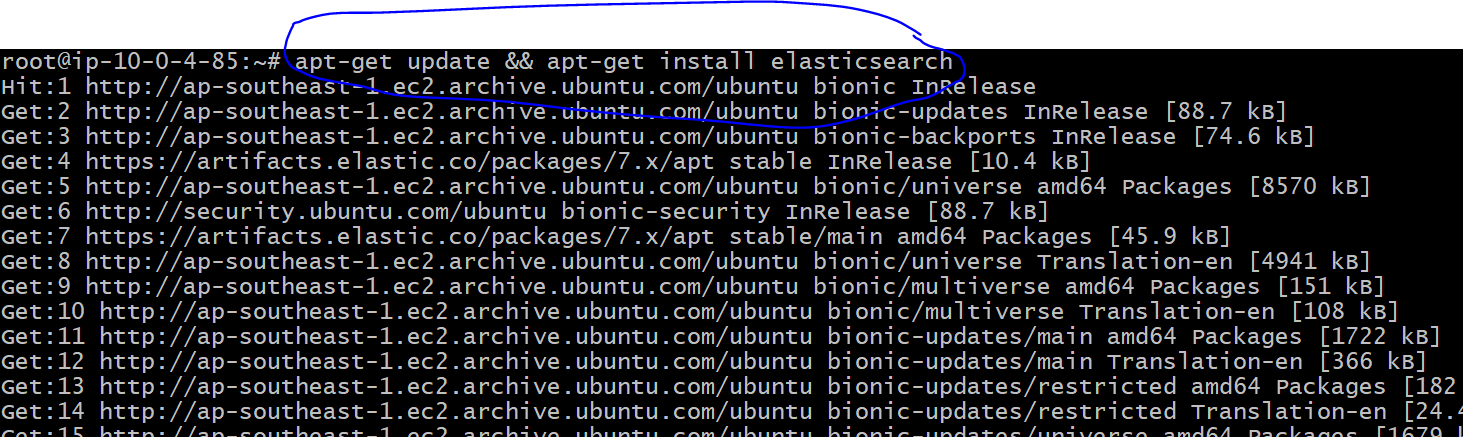
**echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list**



After enabling the EPEL repos

Install the elasticsearch

**apt-get update && apt-get install elasicsearch**

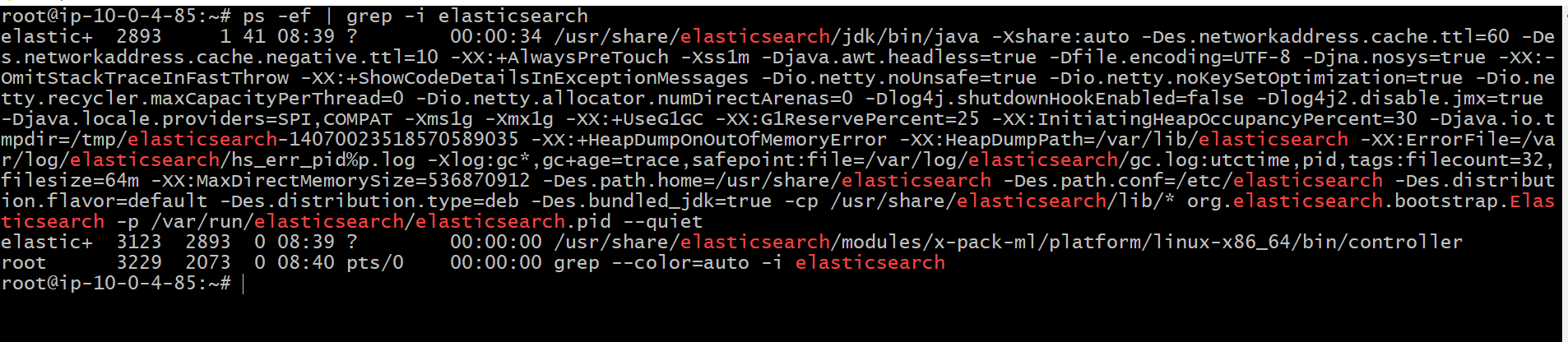


Start elasticsearch

**systemctl start elasticsearch**

check elasticsearch running or not

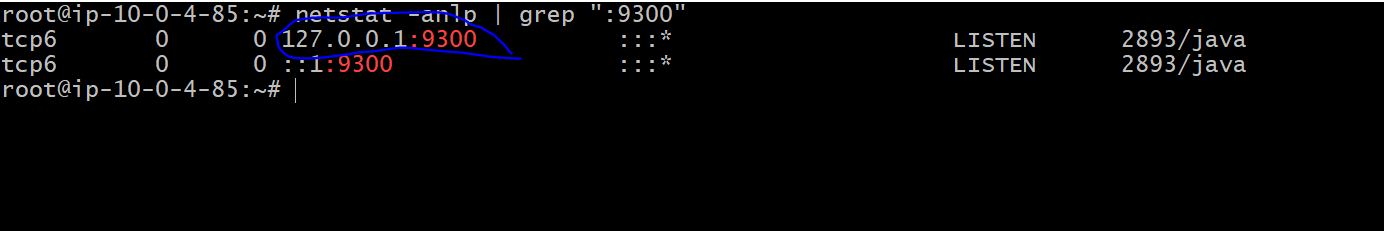
**ps –ef | grep –I elasticsearch**



**Important tip:**

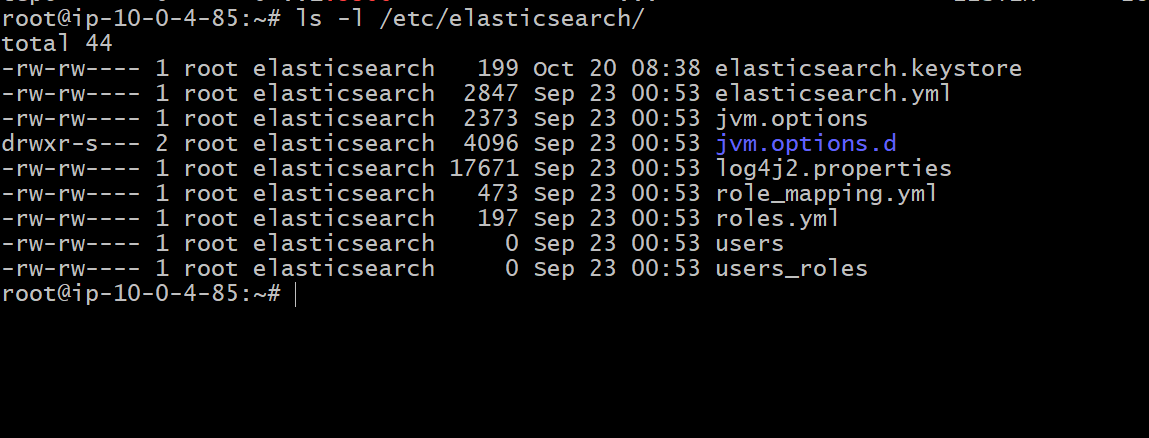
Elastic search will starts listens on 9300, but it only accepts connections on 127.0.0.1

Check with : netstat –anlp | grep “:9300”



If any process listens on 127.0.0.1 , you cant connect from outside, so we have make it allow to 0.0.0.0 in elasticsearch config file.

Elasticsearch will get installs in /etc/elasticsearch directory

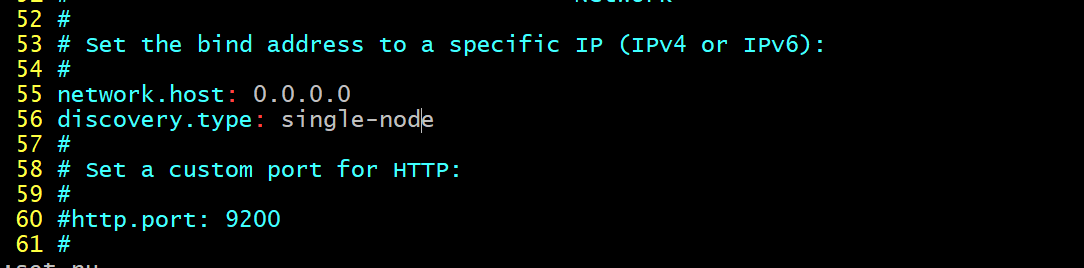


Important file : elasticsearch.yml

We will edit elasticsearch.yml to accept connections on any IP address( we will update 0.0.0.0)

vi /etc/elasticsearch/elasticsearch.yml

Add the lines



network.host : 0.0.0.0

discovery.type: single-node

Above changes for single node elasticsearch, if you are following for the production, we have other setup lines.

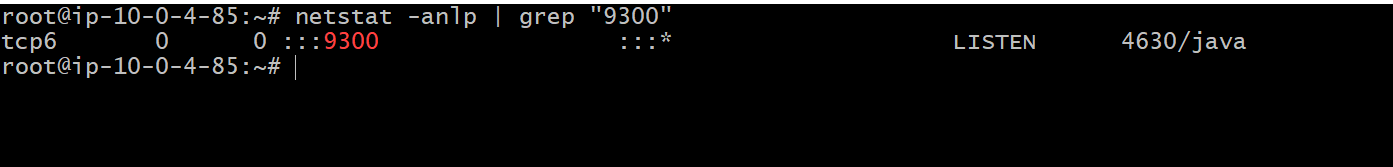
Restart the elasticsearch after updating the yaml file

**systemctl restart elasticsearch**

check again port and processID

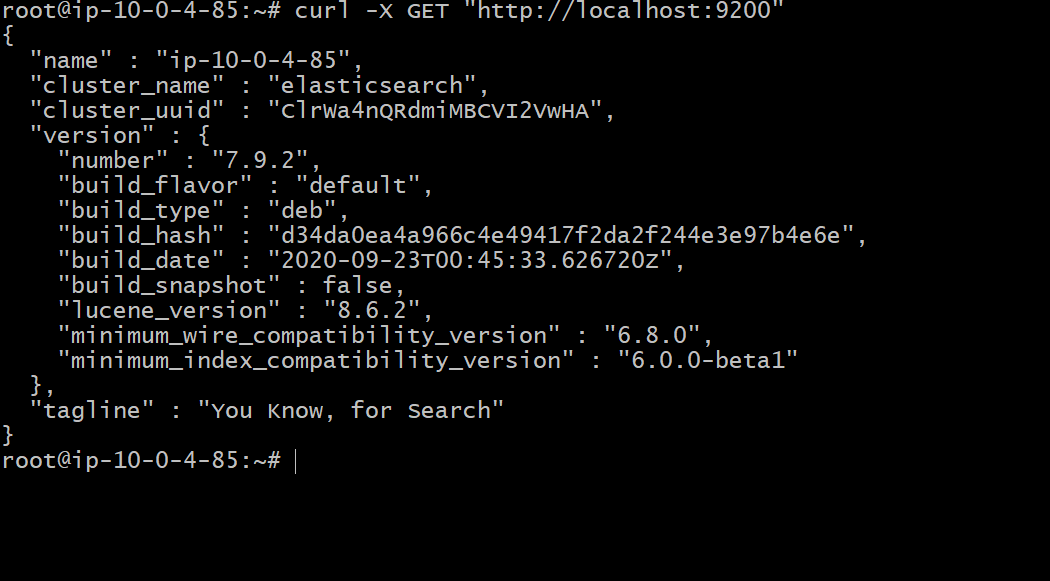
ps –ef | grep –I elasticsearch

netstat –anlp | grep “:9300”



You can observe 127.0.0.1 has been cleared.

You can do the curl test for the elasticsearch status check on 9300 port number.

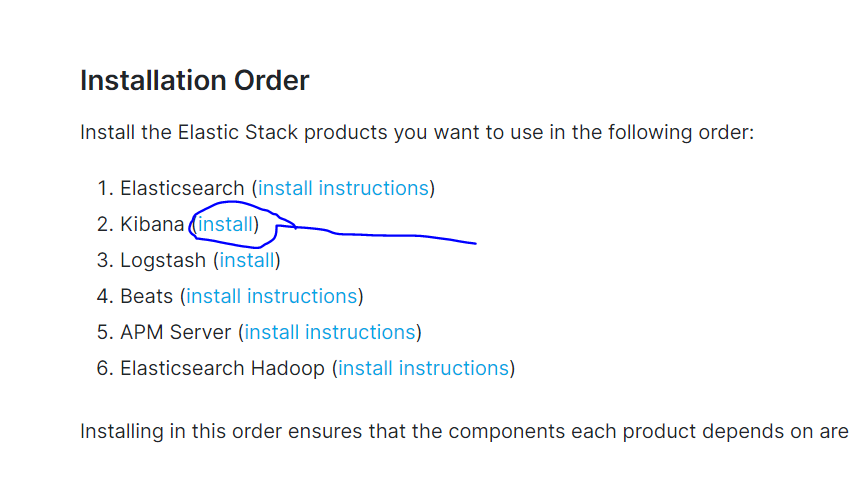


curl -X GET <http://localhost:9200>

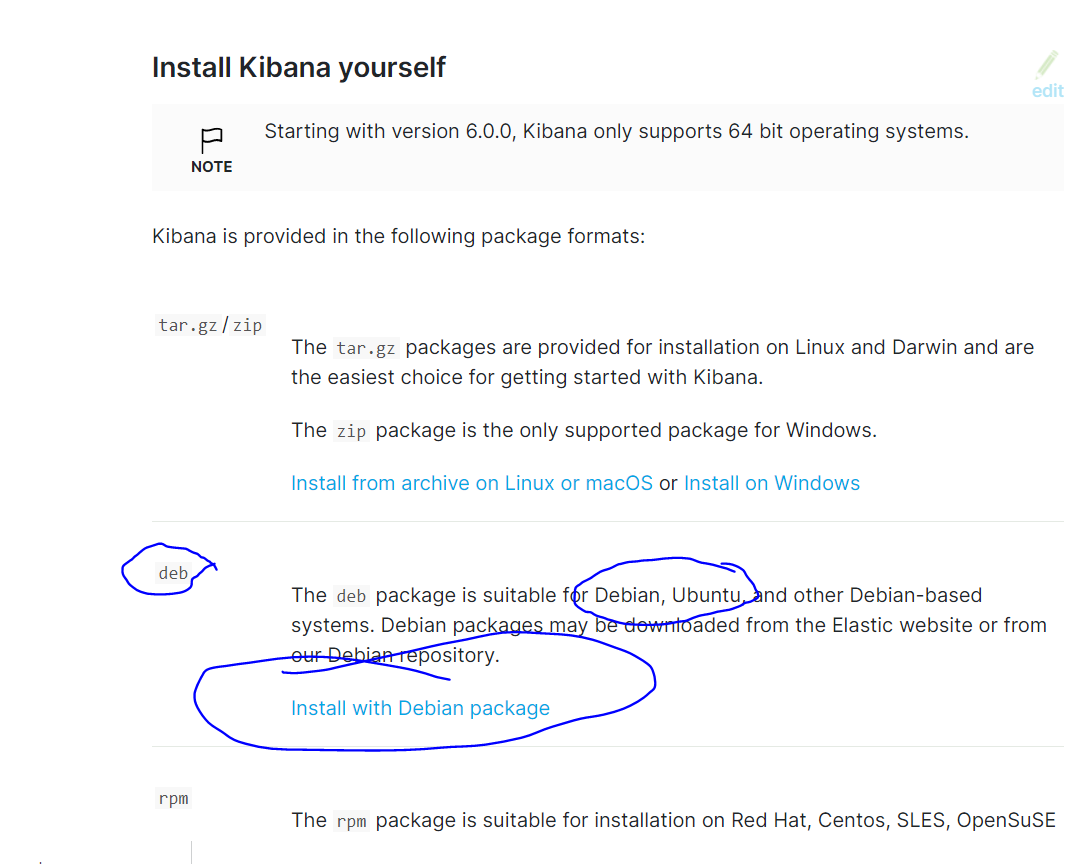
We are good if we get above results for the elastic search curl command.

We will configure now the kibana in the same machine and will connect to the elastic search

2. Kibana setup



Click on install for the Ubuntu setup/deb packages.

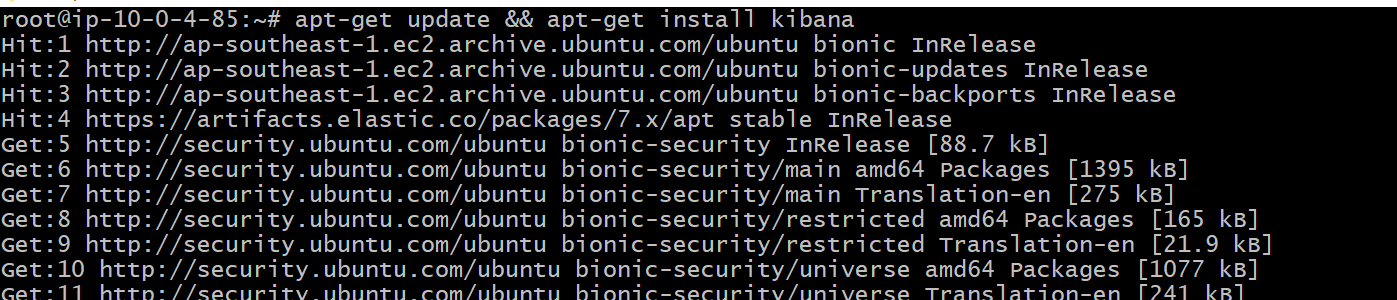


We already enabled the gpg key and epel repo , so we can go directly installation of kibana on the same machine.

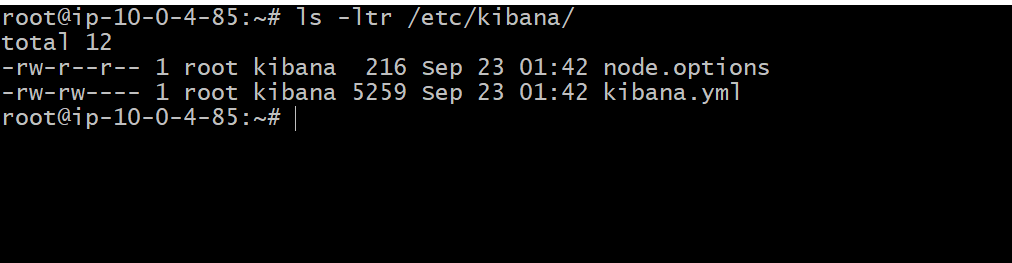
If we have kibana on diff then again we have to confiugure the key and epel.

Now directly install the kibana

**apt-get update && apt-get install kibana**



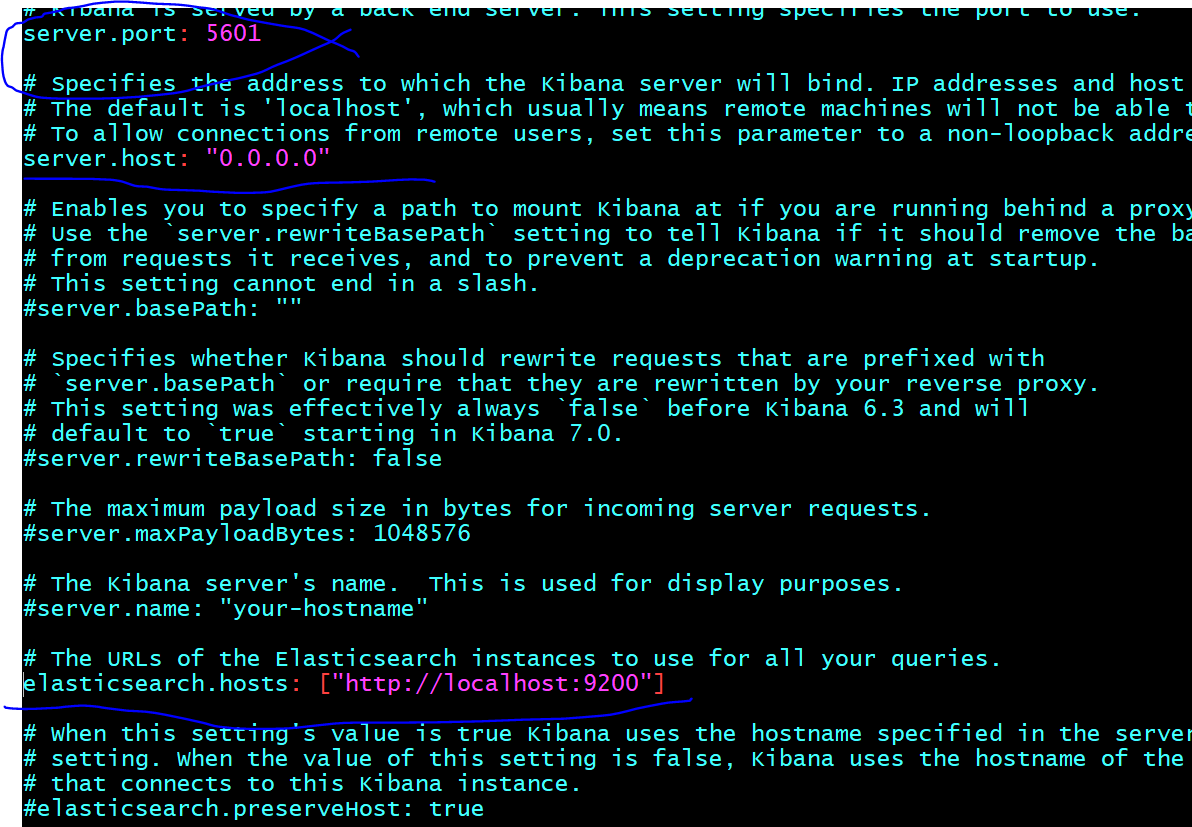
**Kibana also will get installs at the /etc/kibana/**



WE will configure kibana port and kibana to connect elasticsearch.

For those changes , update the /etc/kibana/kibana.yml

vi /etc/kibana/kibana.yml



Update the above 3 lines as

Server port : kibana listens port

Server.host : kibana can access any ip

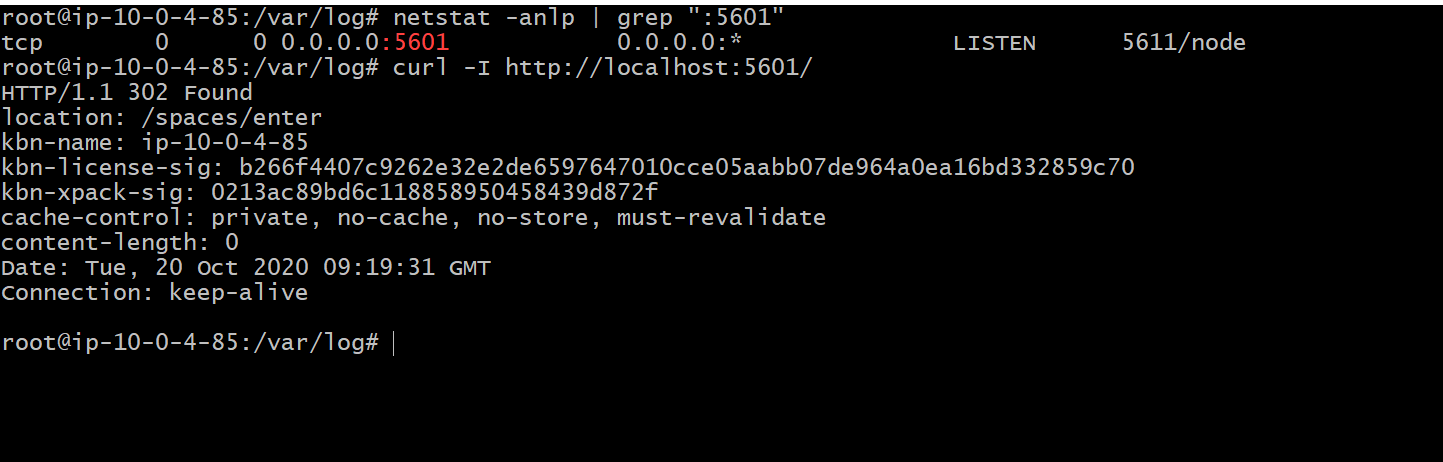
Elasticsearc.hosts: kiaban connecting to the elasticsearch

Start kibana:

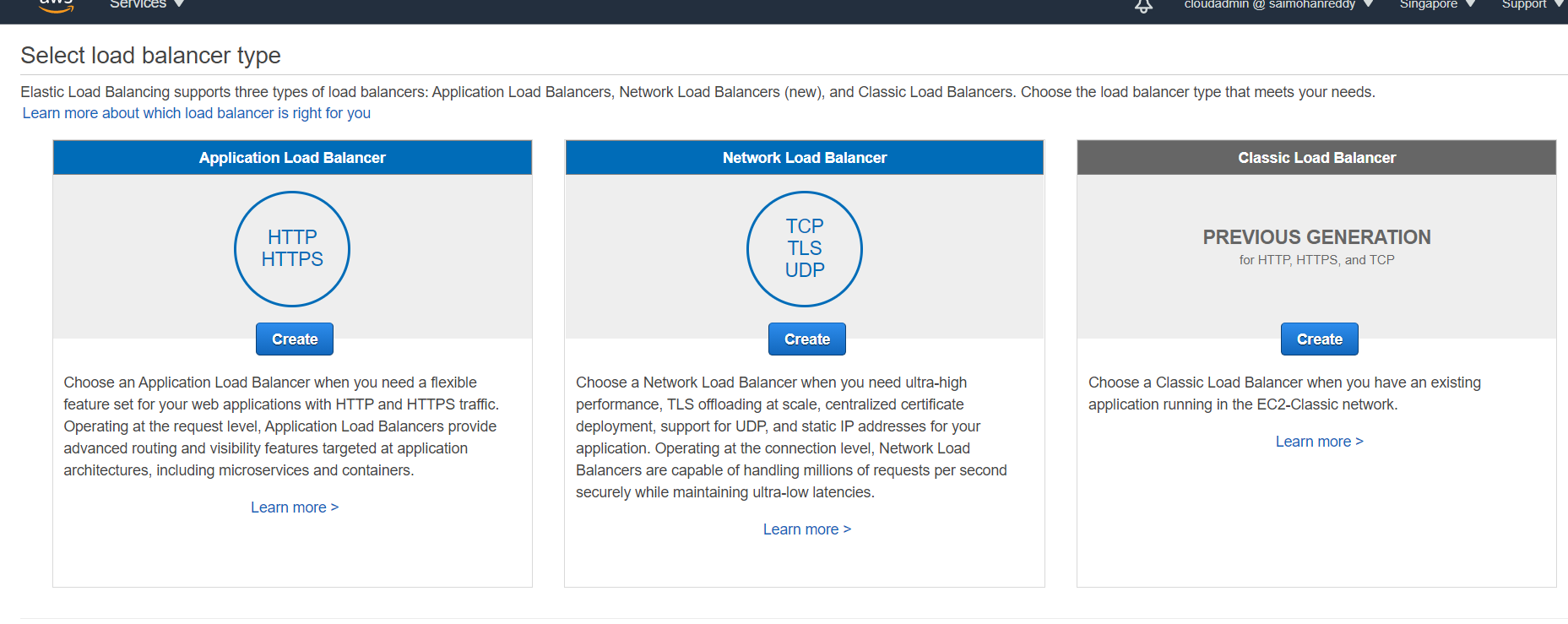
Systemctl start kibana

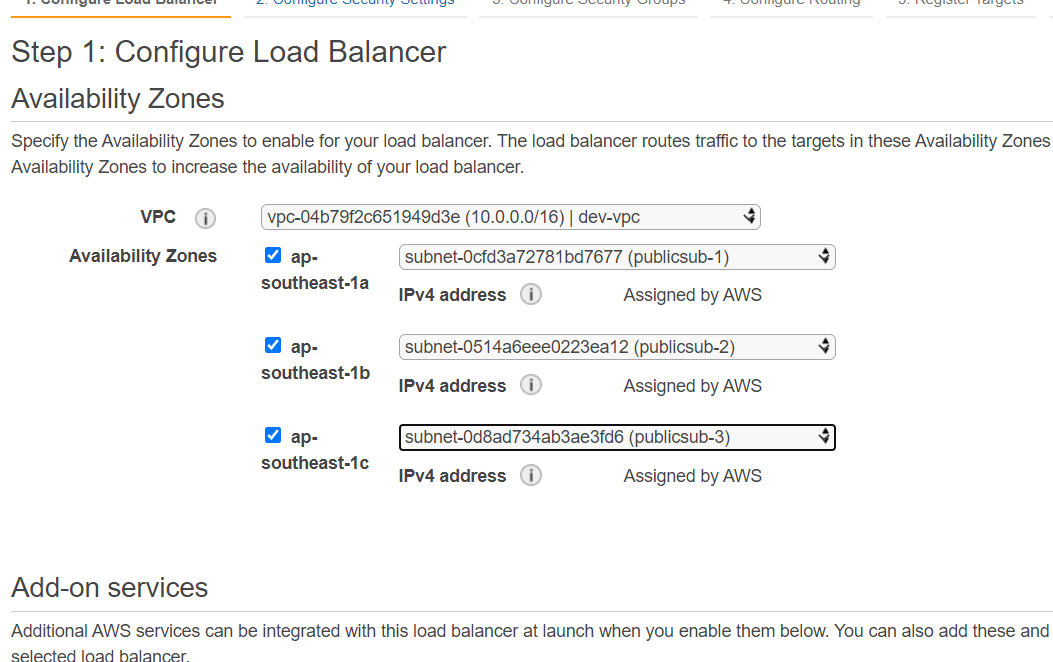
If you have launched kibana in the private subnet , you can’t access outside without load balancer

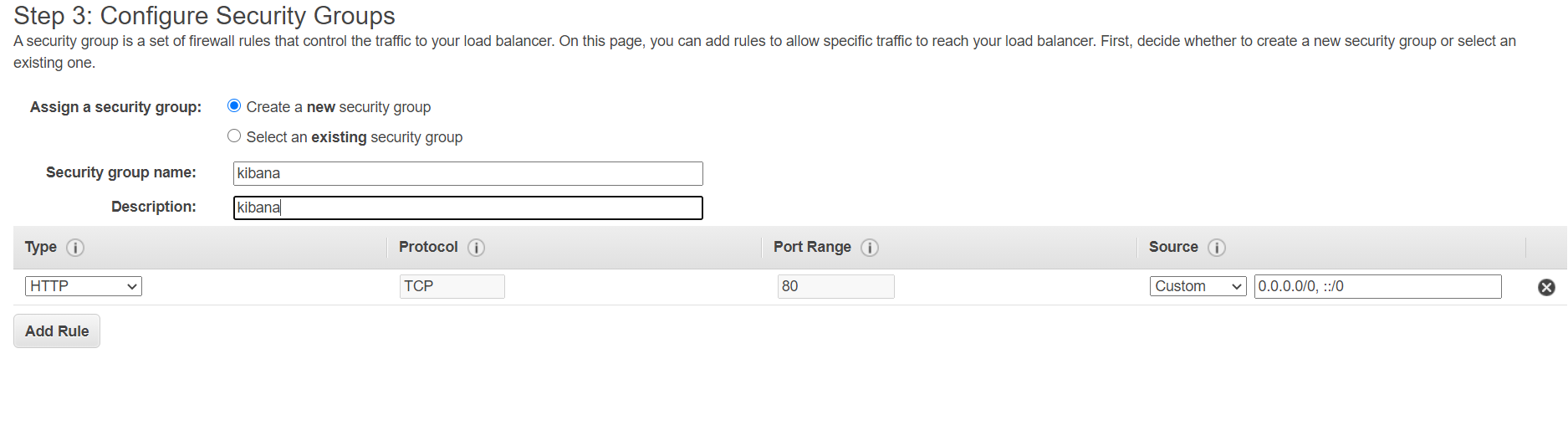
You can test local with the curl.

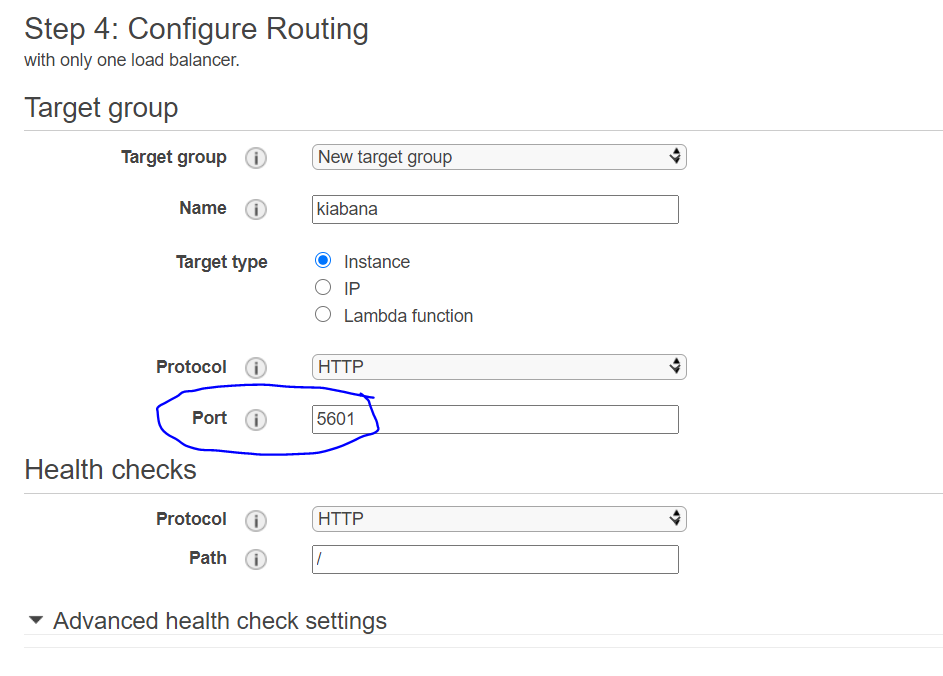


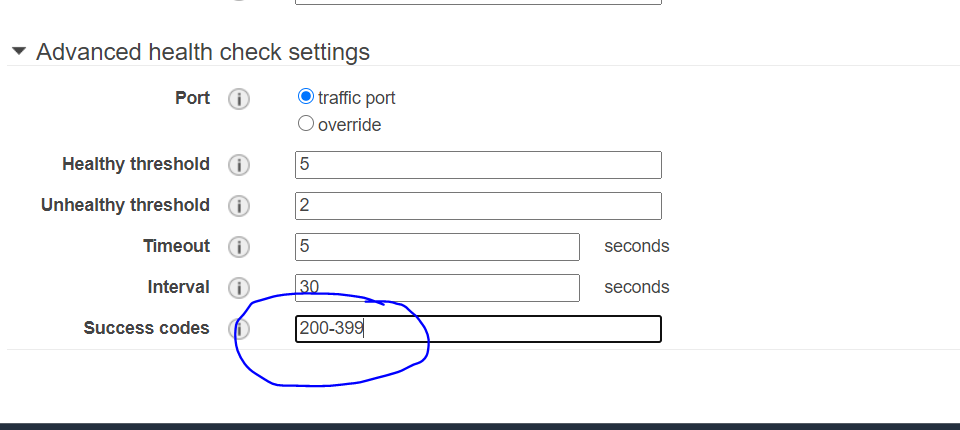
Create the alb and target group with the 5601 port number to access kibana

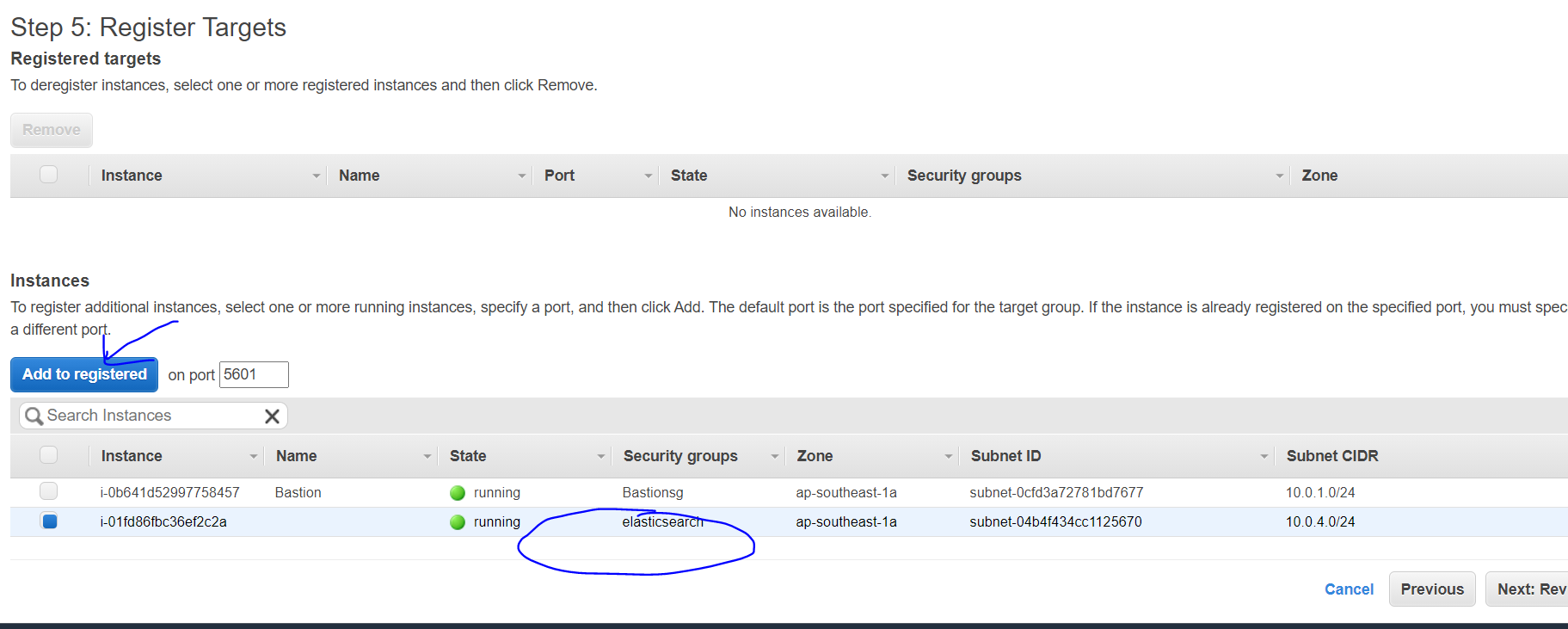




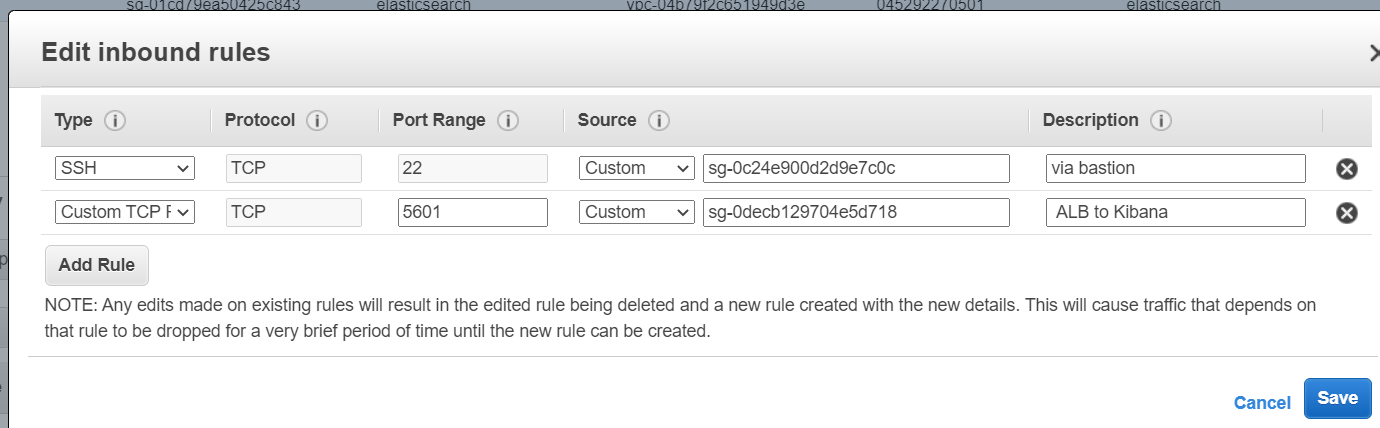




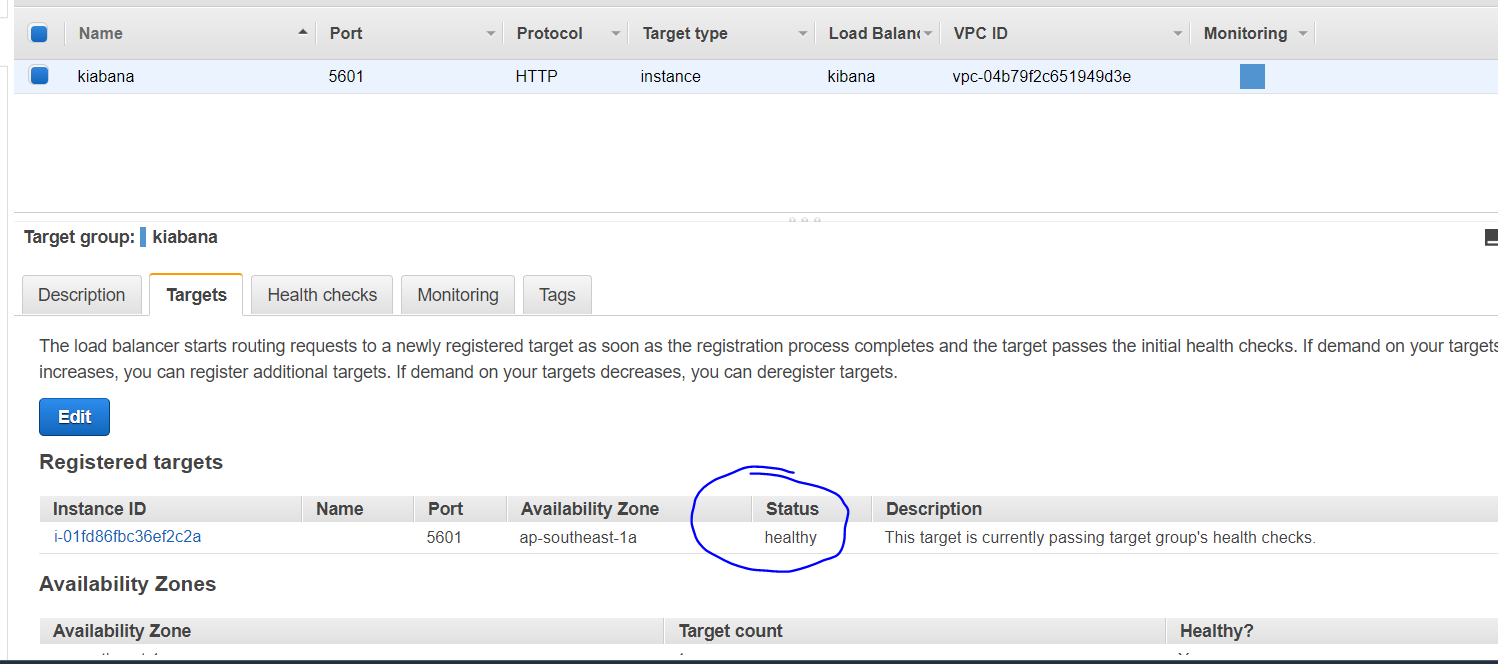




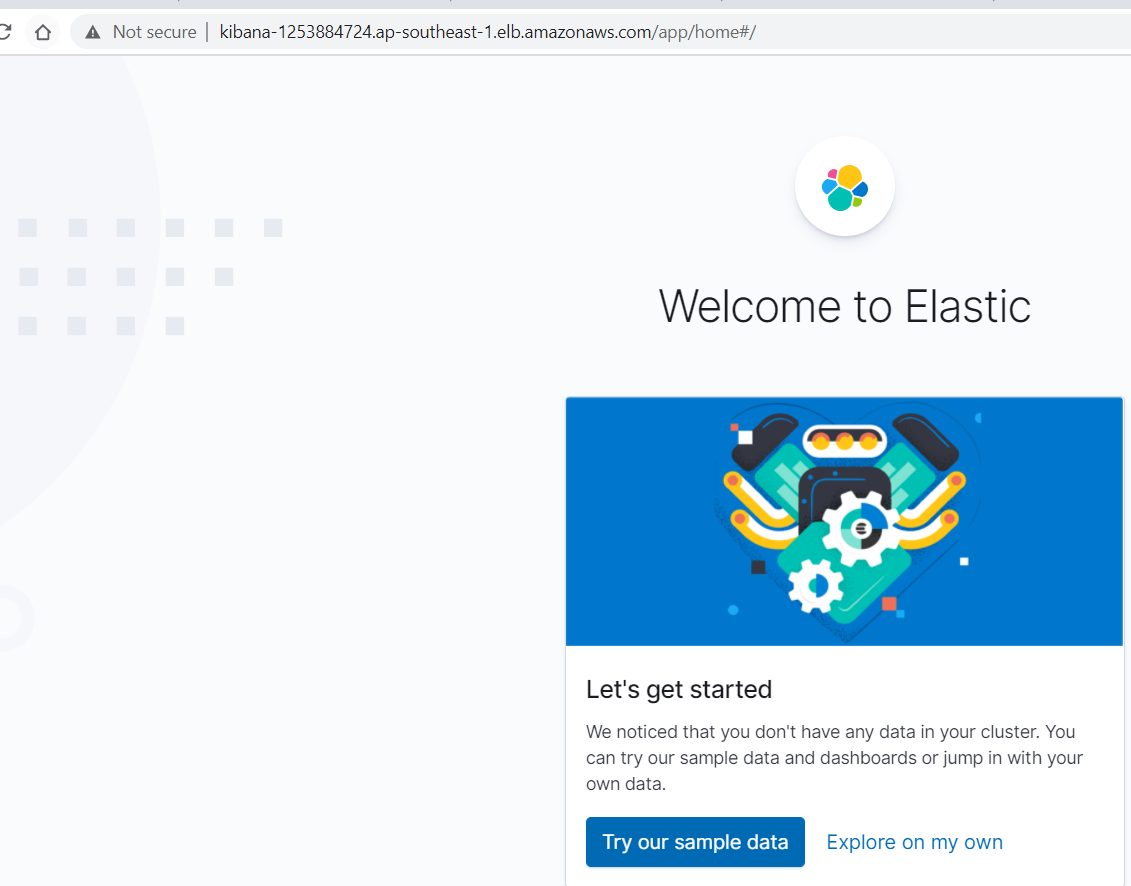
Allow the elasticsearch to connect from alb on the 5601 port number(kibana)



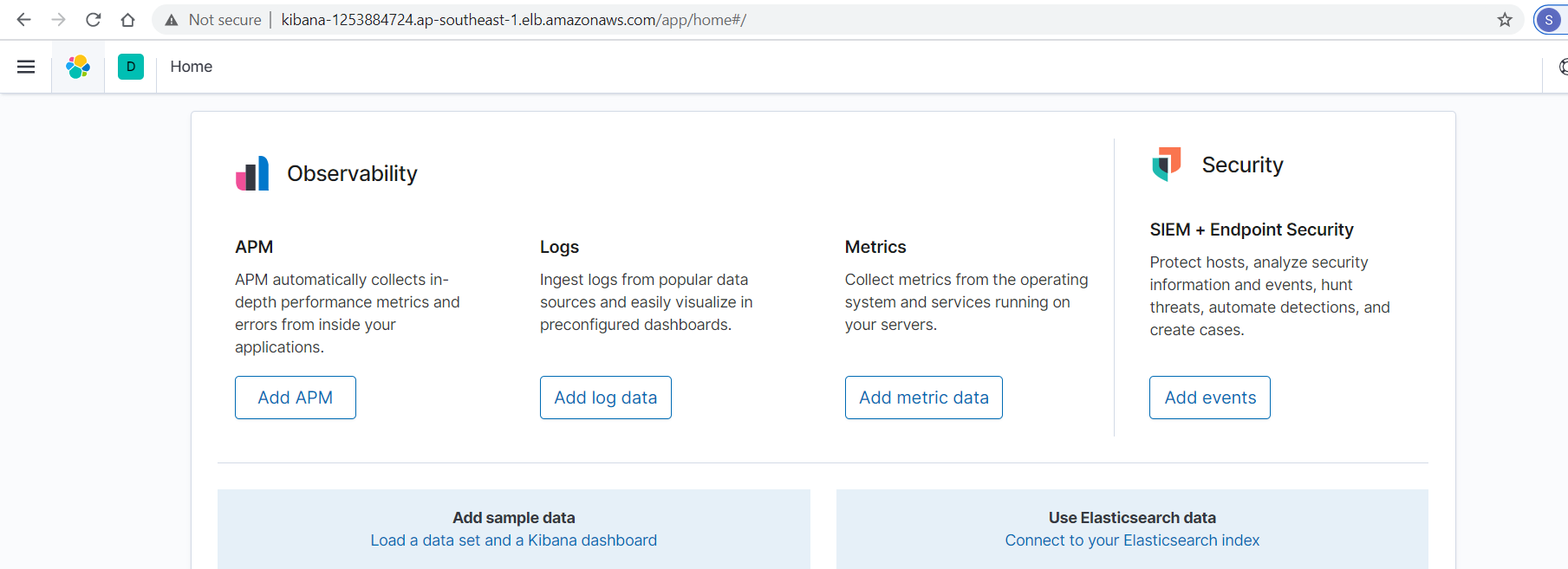
Instance state should be health in the target group



Access the kibana page, with the load balancer endpoint



Click on explore on my own.



Upto now , we have configured elasticsearch and kibana.

We need to send the logs to the elasticsearch from tomcat.

<doc in progress for the agent to the elasticsearch>