**SET UP EFK ON EC2**

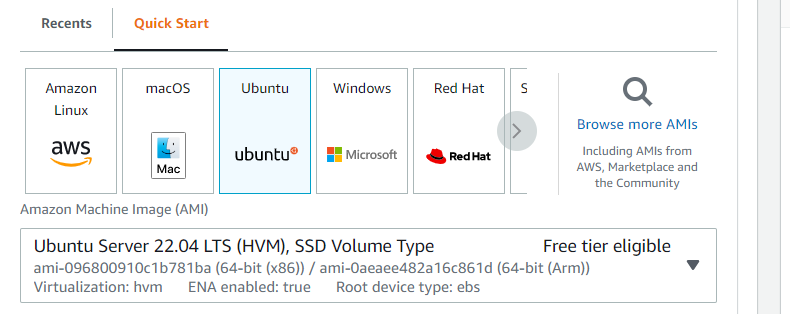
**Efk**

Efk stands for Elasticsearch Fluentd and kibana. Efk is a popular and the best open-source choice for the kubernetes logs aggregation and analysis.  Elasticsearch is a distributed and scalable search engine commonly used to sift through large volumes of log data.

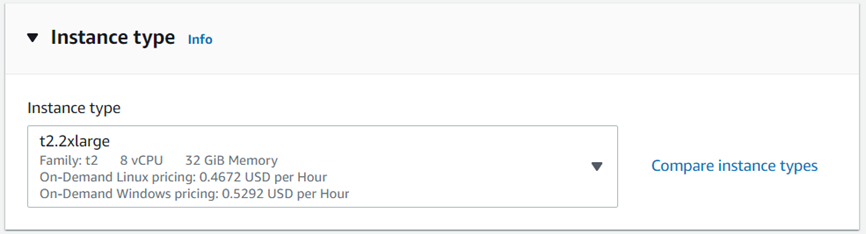
**Ec2**

* Ec2  stands for Amazon elastic compute cloud
* Amazon ec2 is a web service that provides resizable compute capacity in the cloud
* To run the application security group zones. user data applications  installation it's nothing but remote server
* You can scale the computer capacity up and down as per computer requirement changes

**Launch ec2 instances-1 and choose: Ubuntu For Elasticsearch & Kibana**

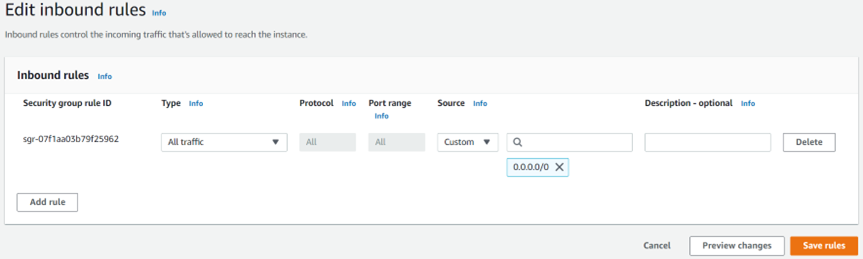


Choose instance type which is equals to 8CPU(Prerequisite)



·

   Set Security group inbound rules as below and attach to ec2



·        Login to ec2 instance-1 in Git Bash : ssh -i pem ubuntu@18.143.159.72

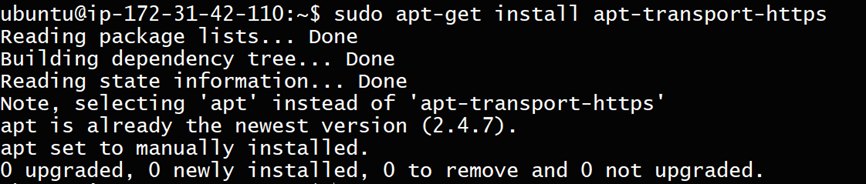
·         Run following commands as ubuntu user

**Installing Elasticsearch and Kibana on ec2 instance-1:**

1.       W get -qO -<https://artifacts.elastic.co/GPG-KEY-elasticsearch> | sudo apt-key add -



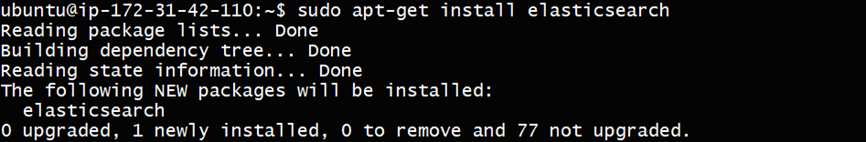
2.       sudo apt-get install apt-transport-https



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

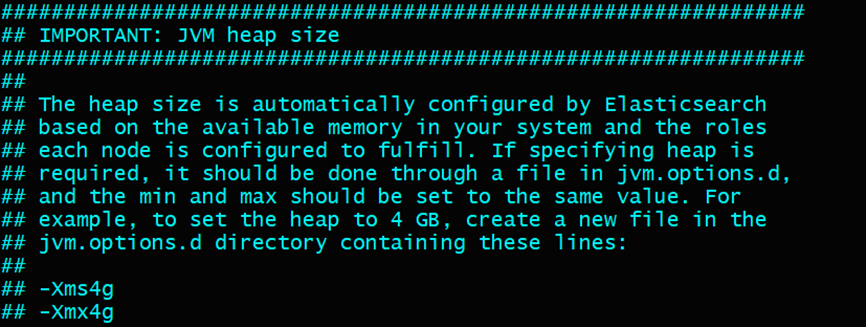
4.       sudo apt-get update

5.       sudo apt-get install elasticsearch

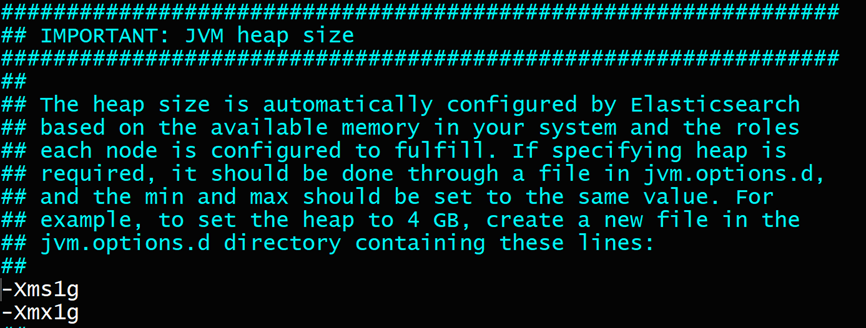


6.       sudo vim /etc/elasticsearch/jvm.options

**Before**



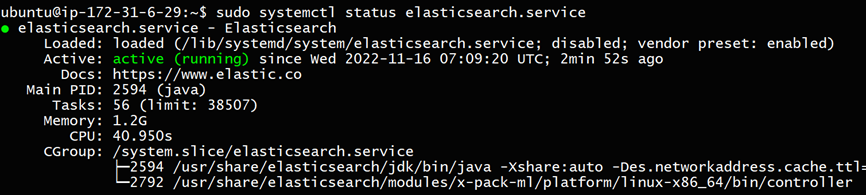
**After**

****

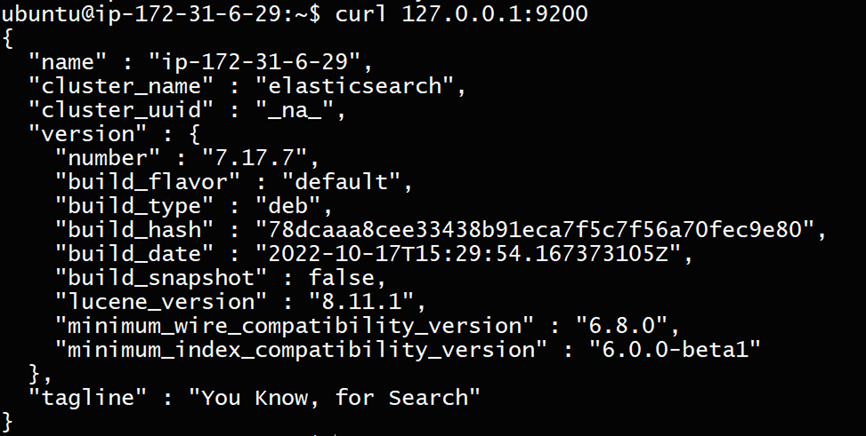
7.       sudo systemctl start elasticsearch.service

8.       sudo systemctl enable elasticsearch.service

9.       sudo systemctl status elasticsearch.service



curl 127.0.0.1:9200

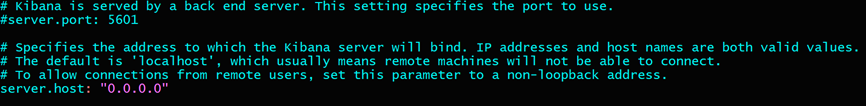


Elastic search installation is completed successfully and running

1.       sudo apt-get install kibana

sudo vi /etc/kibana/kibana.yml

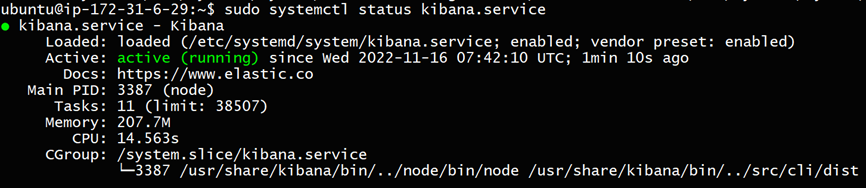
set => server.host: 0.0.0.0



1.       sudo systemctl start kibana.service

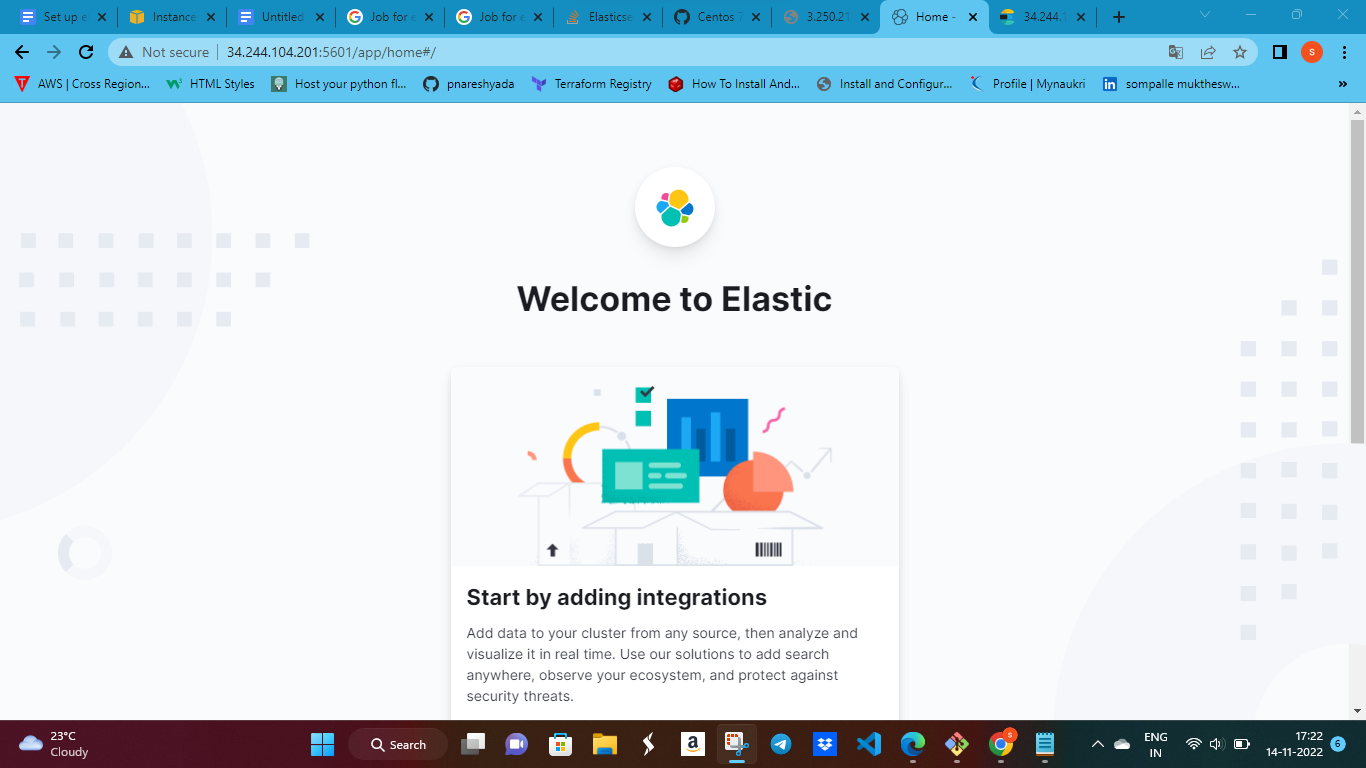
2.       sudo systemctl enable kibana.service

                sudo systemctl status kibana.service



Instance public IP:5601

**Result in Web**

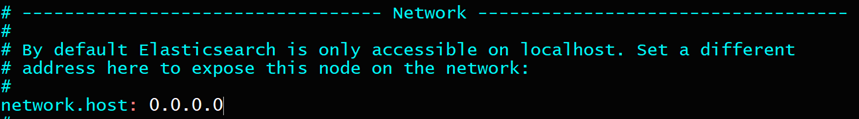
   Kibana installation is completed successfully and running

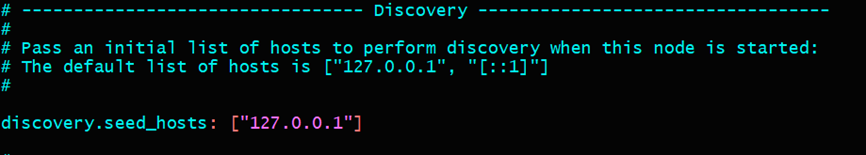
**change elasticsearch configuration**

sudo vi /etc/elasticsearch/elasticsearch.yml

set => network.host: 0.0.0.0

set => discovery.seed\_hosts: ["127.0.0.1"]





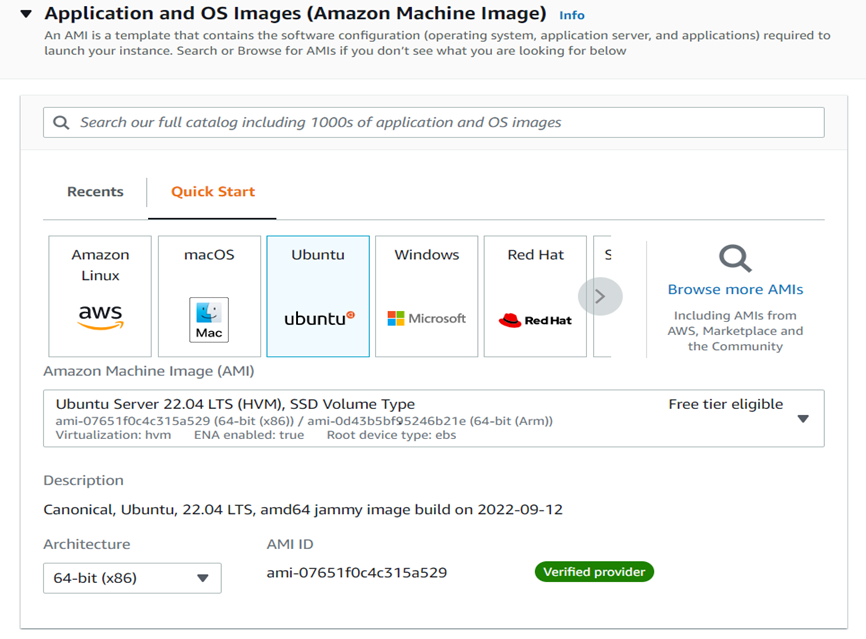
1.       sudo systemctl restart elasticsearch.service

ec2 Instance-1 public IP:9200

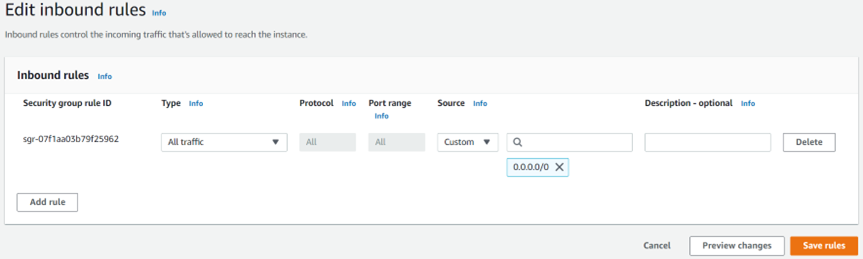
**Result in Web**



**Launch ec2 instance-2 and choose: Ubuntu (For Filebeat & Web server)**



·         Set Security group inbound rules as below and attach to ec2



·         Login to ec2 instance-2 in Git Bash : ssh -i pem ubuntu@18.140.159.77

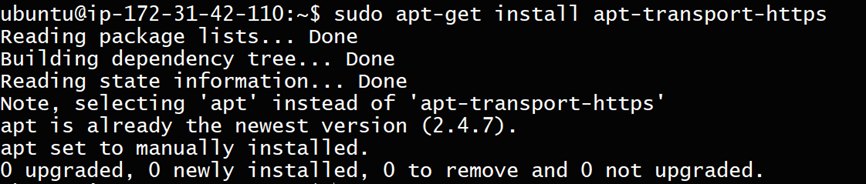
·         Run following commands as ubuntu user

**Installing Filebeat on Ec2 instance-2:**

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



sudo apt-get install apt-transport-https



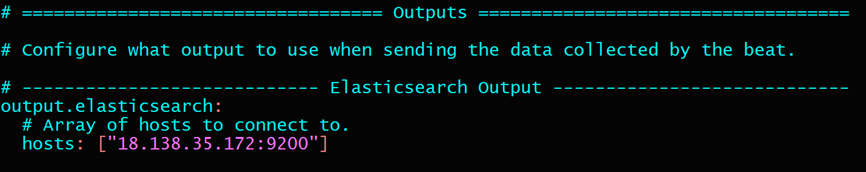
1.       echo "deb<https://artifacts.elastic.co/packages/7.x/apt> stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list

2.       sudo apt-get update

3.       sudo apt-get install filebeat

sudo vi /etc/filebeat/filebeat.yml

set => outputs hosts: ["18.138.35.172:9200"] (ec2 instance-1 public IP:9200)



1.       sudo systemctl start filebeat.service

2.       sudo systemctl enable filebeat.service

sudo systemctl status filebeat.service

Filebeat installation is completed successfully and running

**Installing tomcat on Ec2 instance-2:**

1.       sudo su -

run following commands as root user

2.       cd /opt

3.       apt install openjdk-11-jdk

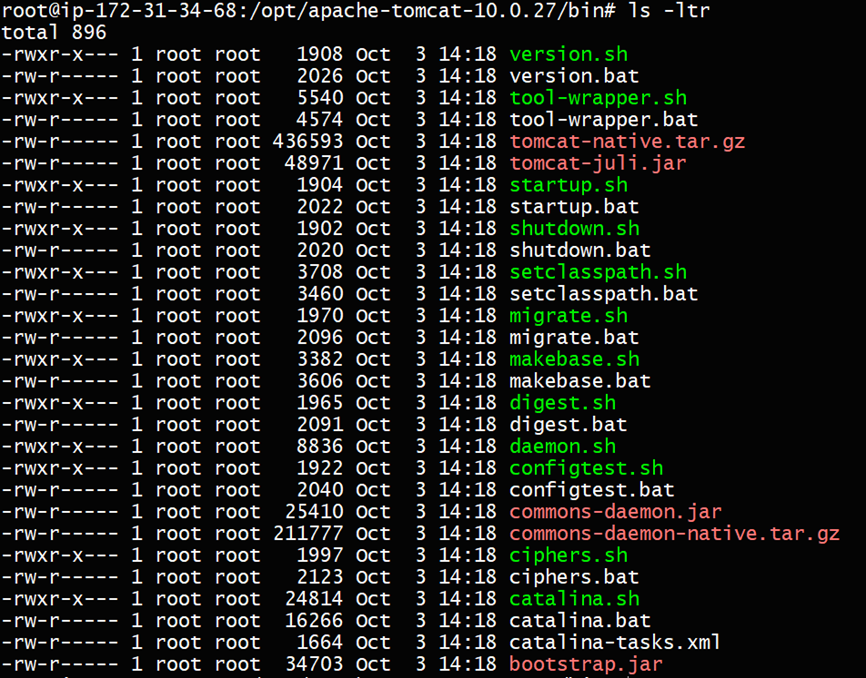
wget<https://dlcdn.apache.org/tomcat/tomcat-10/v10.0.27/bin/apache-tomcat-10.0.27.tar.gz>



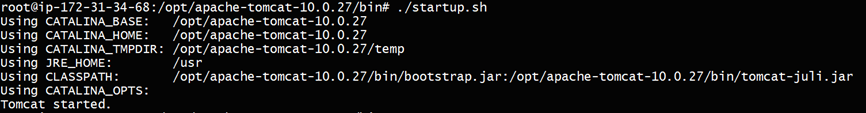
1.       tar -zvxf apache-tomcat-10.0.27.tar.gz

2.       cd apache-tomcat-10.0.27/bin/

ls -ltr



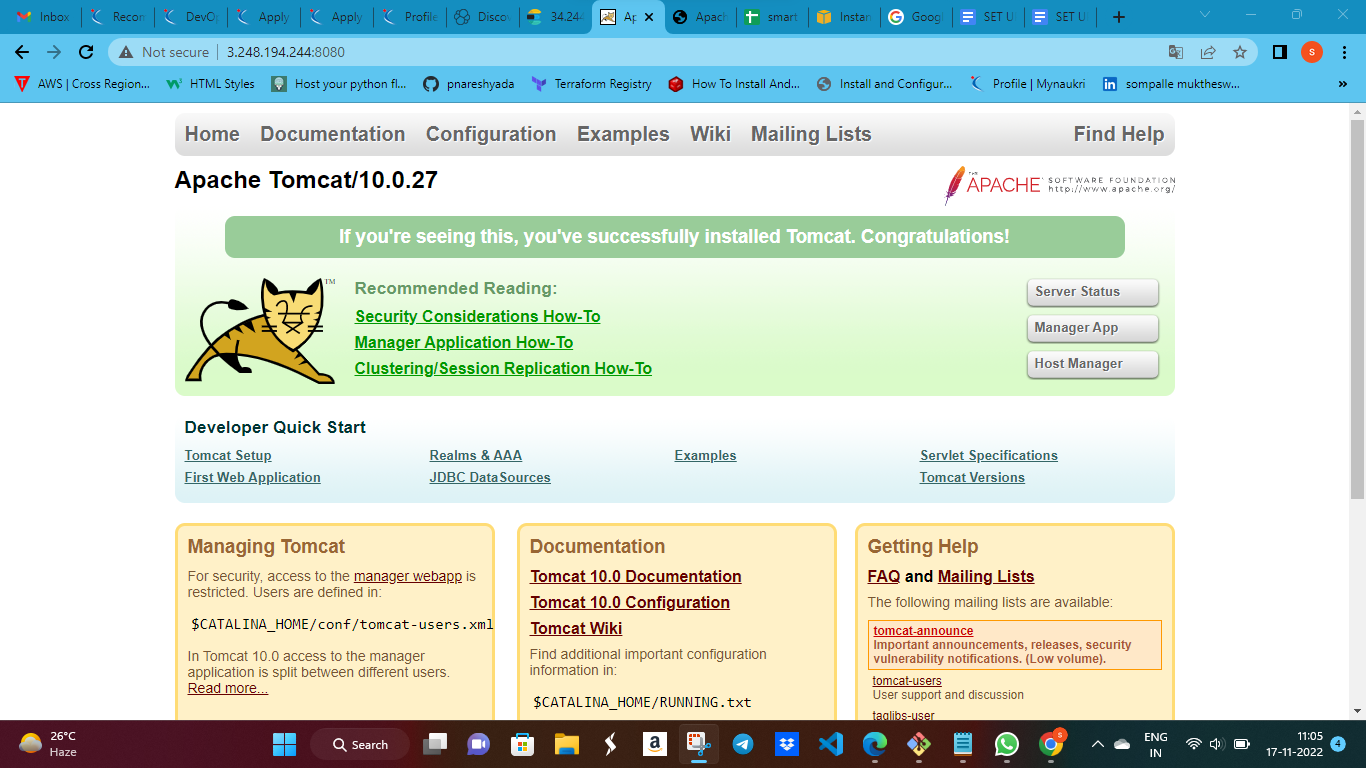
./startup.sh



ps -ef | grep "tomcat"



create logs by accessing to Ec2 instance-2 public IP:8080



1.       check logs in /opt/apache-tomcat-10.0.27/logs/\*.log

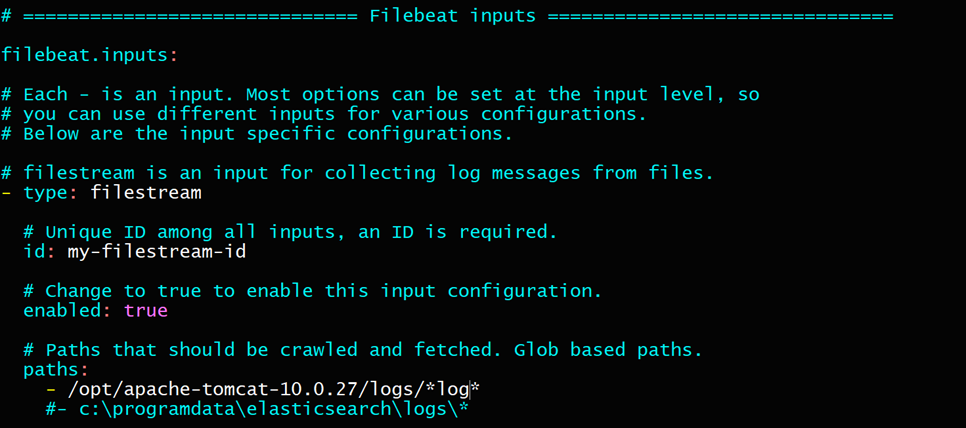
Tomcat installation is completed successfully and running

**change Filebeat configuration**

sudo vi /etc/filebeat/filebeat.yml

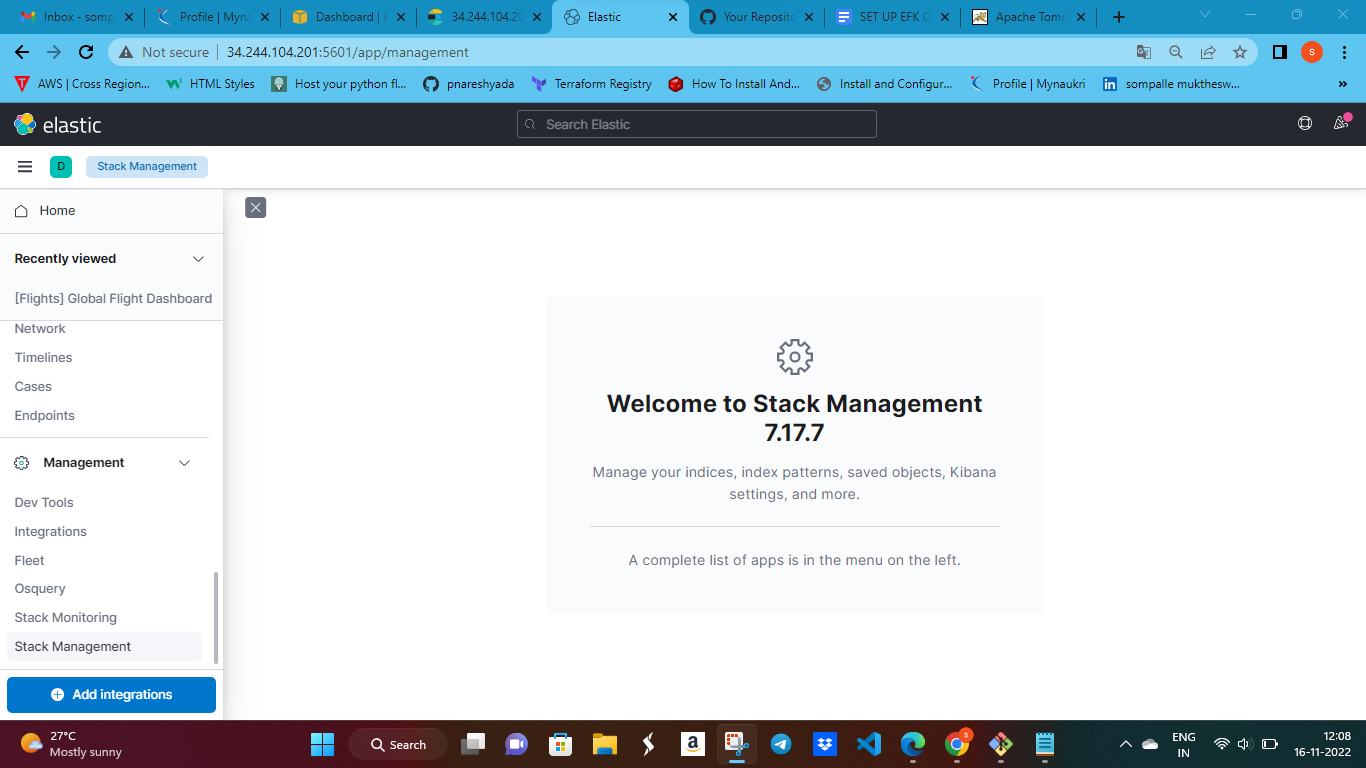
set => enabled: true

set => - /opt/apache-tomcat-10.0.27/logs/\*log\*

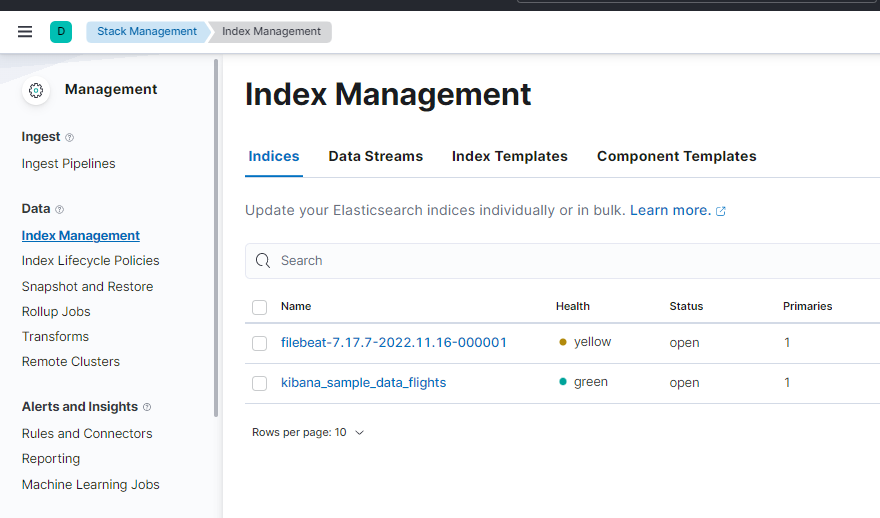


1.       sudo systemctl restart filebeat.service

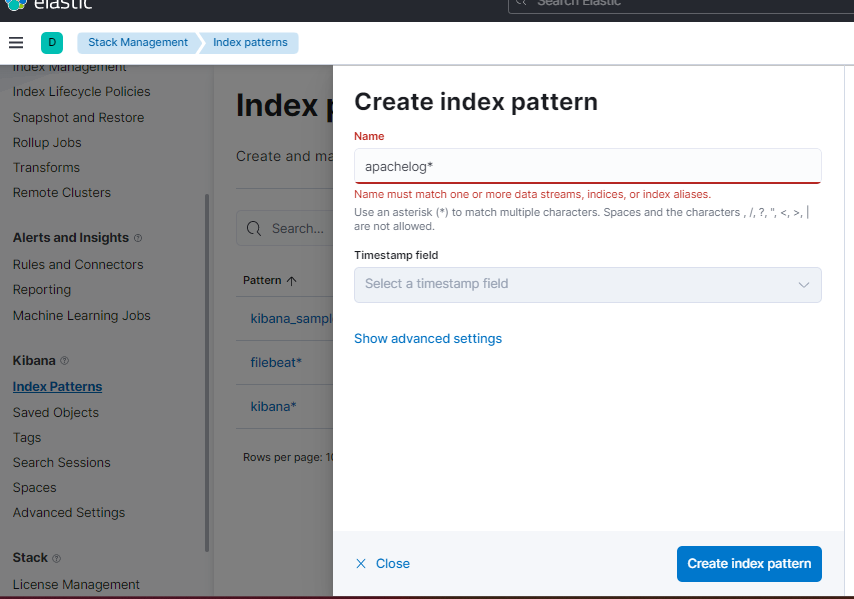
**Log in to Kibana dashboard with ec2 instance-1 public IP:5601**



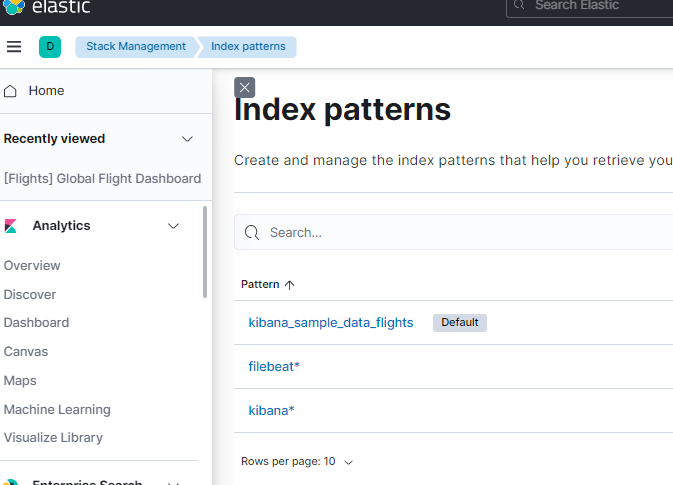
·         open Stack Management > Index Management ,check for filebeat logs file availability



·         create Index Pattern



·         open Discover



·         Choose the created index pattern and time to display logs

