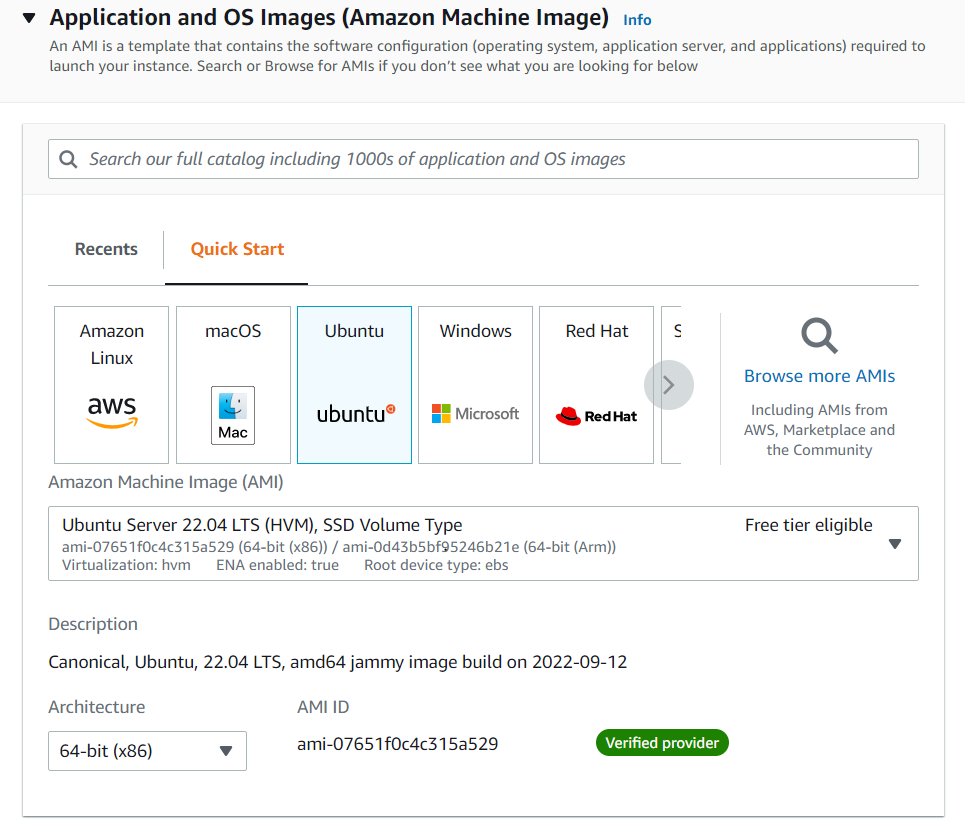
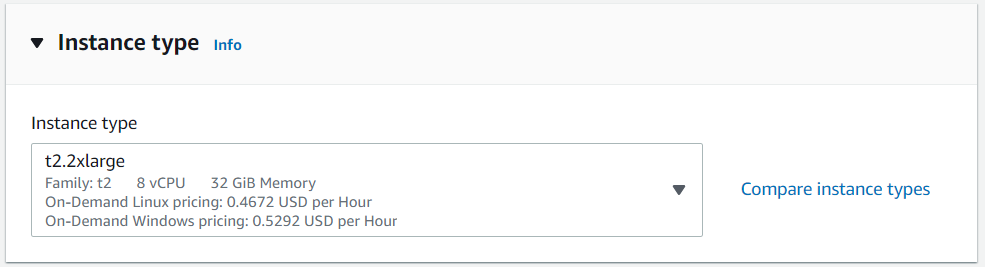
**EFK - SETUP**

**Hello, to display required web server (Nginx, Tomcat, Apache) loggings on Kibana dashboard, follow the document given as below.**

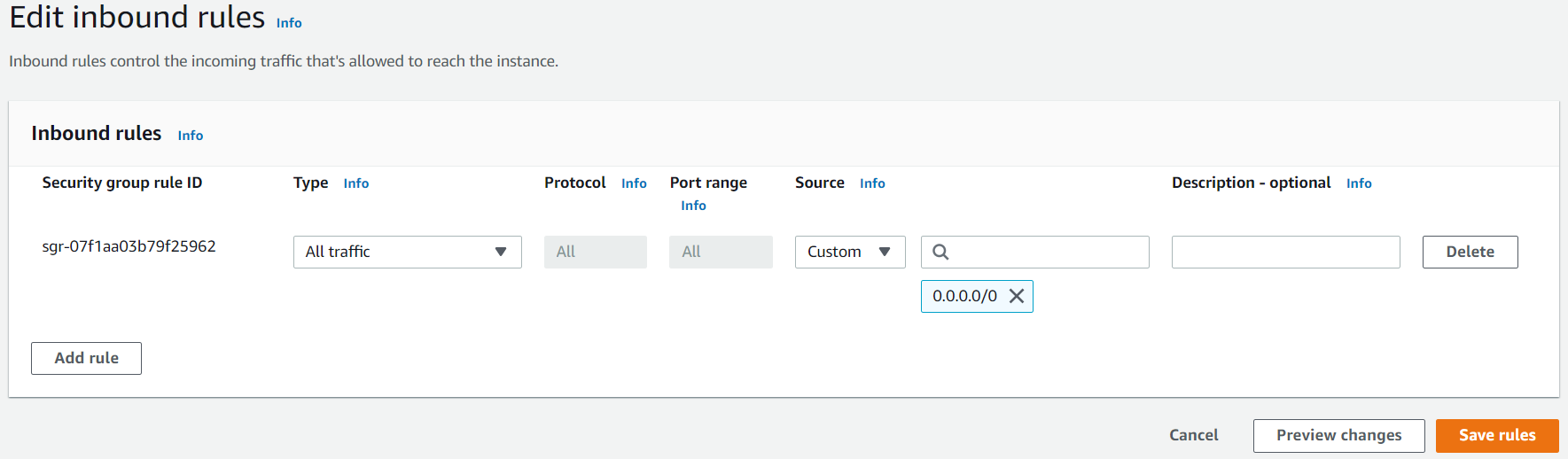
**Launch ec2 instances-1 and choose: Ubuntu (For Elasticsearch & Kibana)**



* Choose instance type which is equals to 8CPU(Pre requisite)

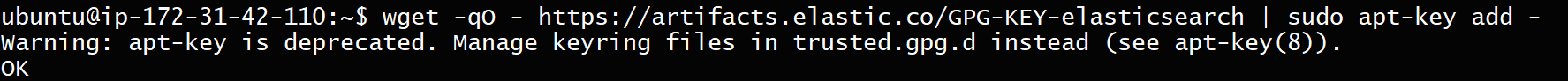
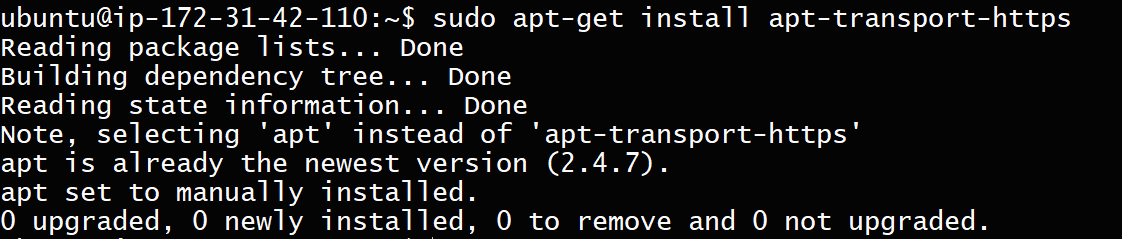
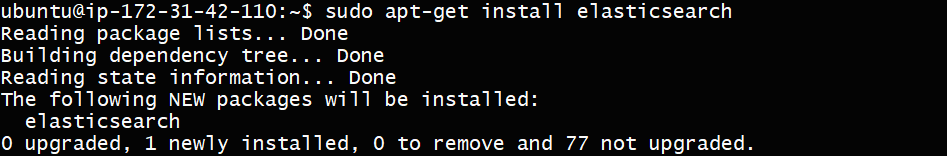
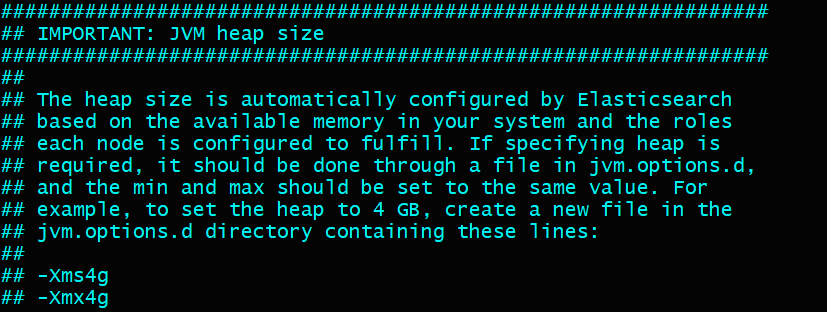
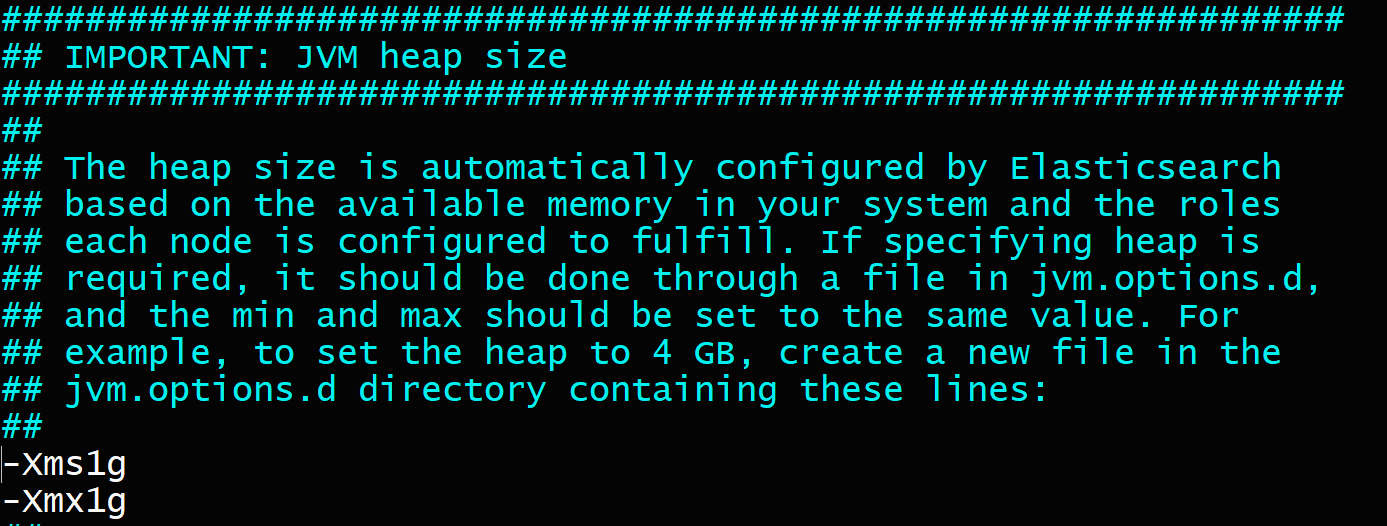
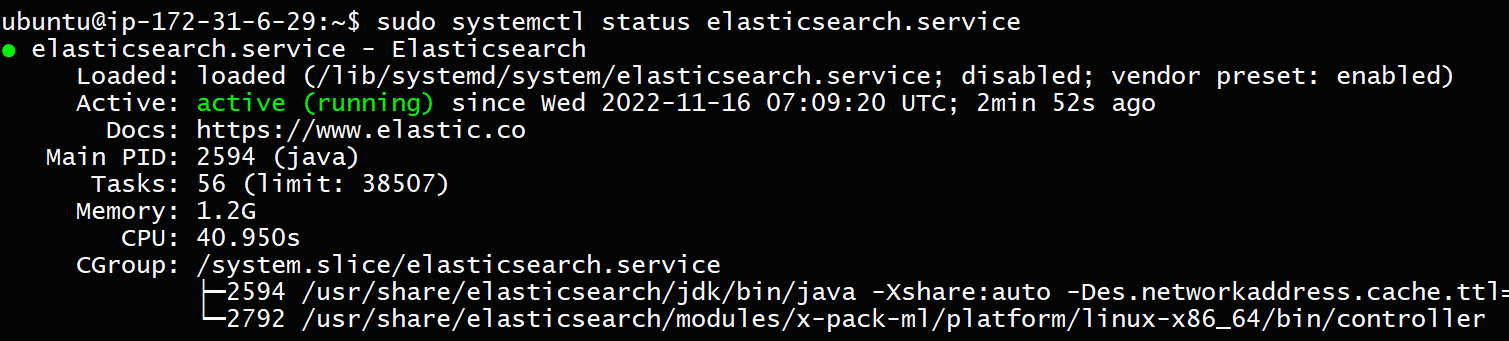
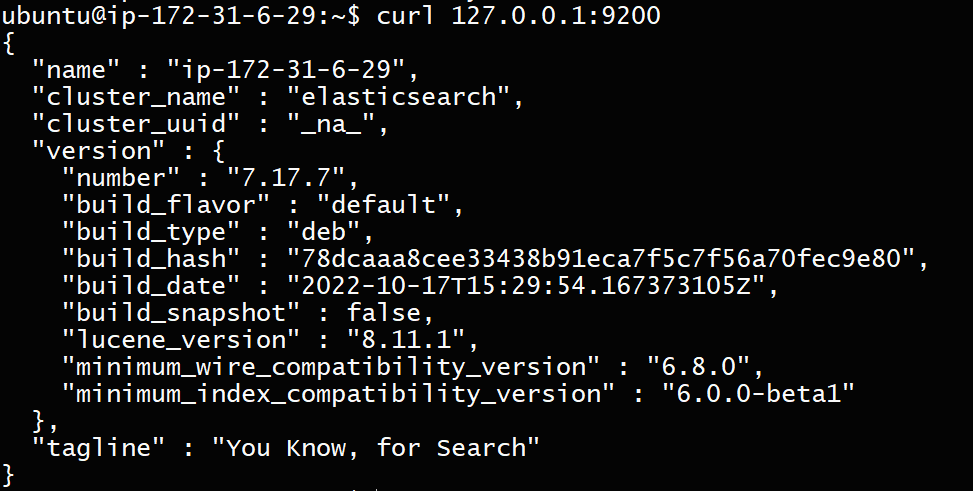
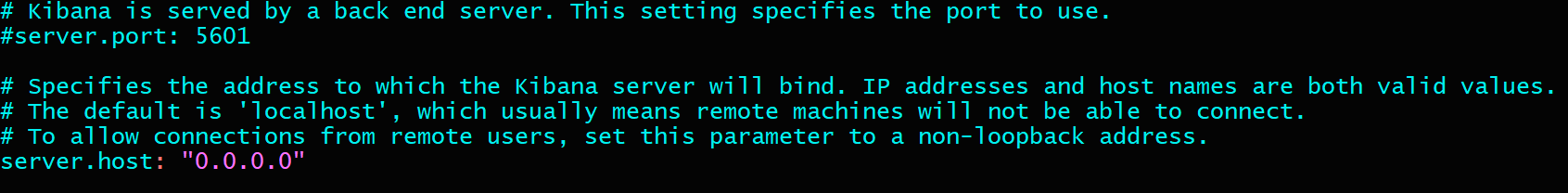
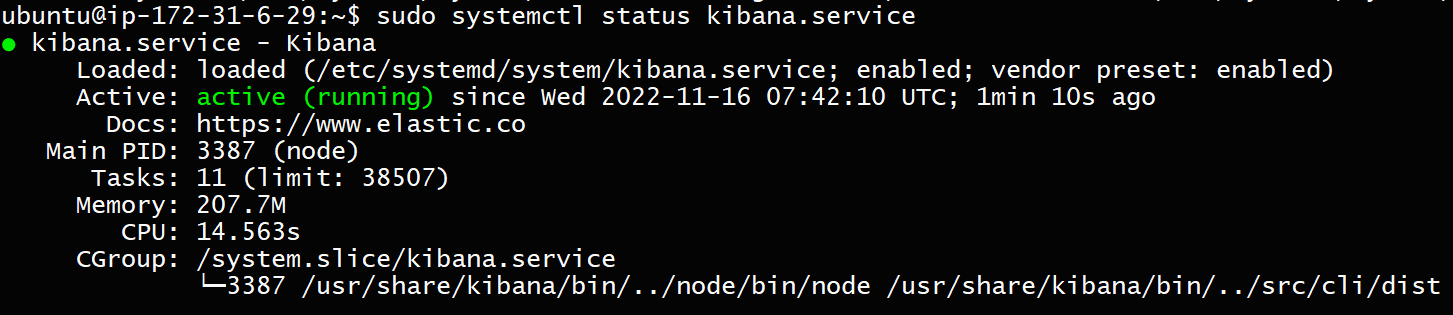
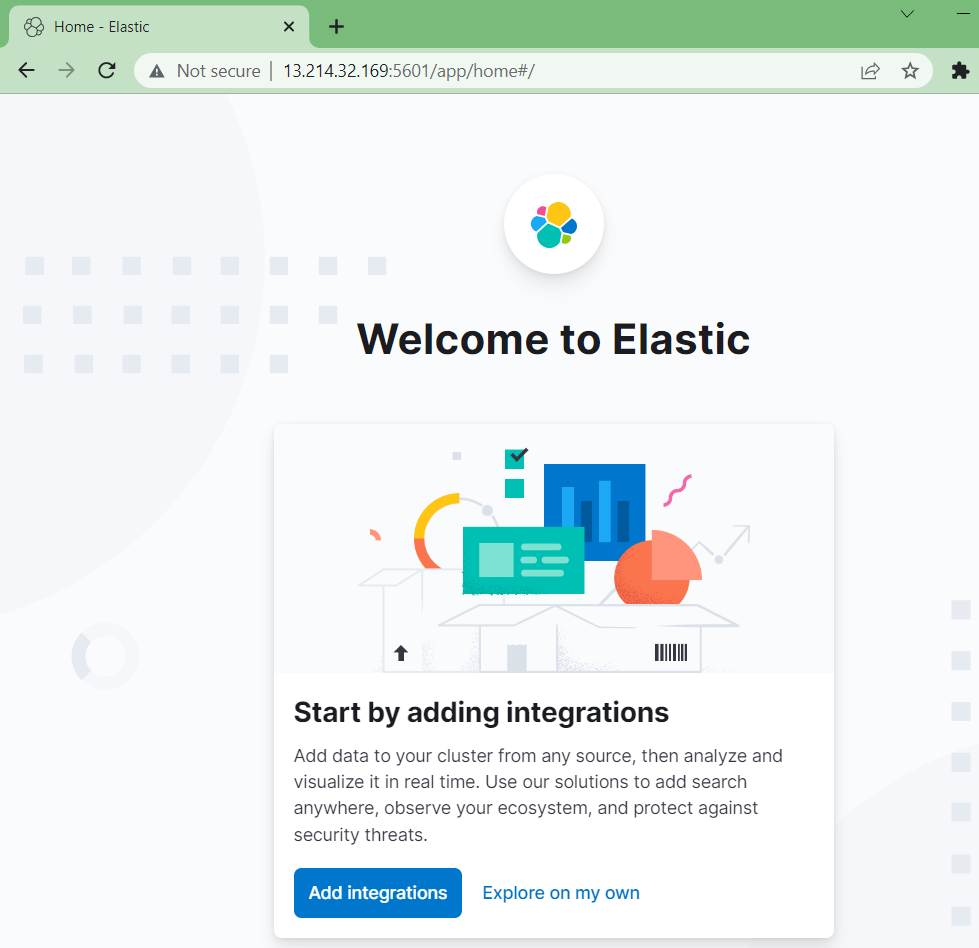
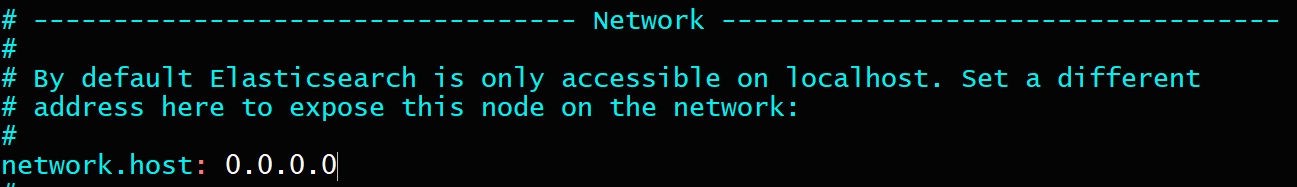
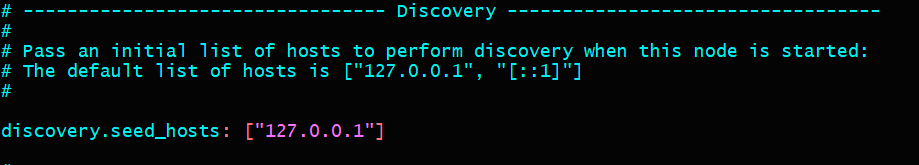
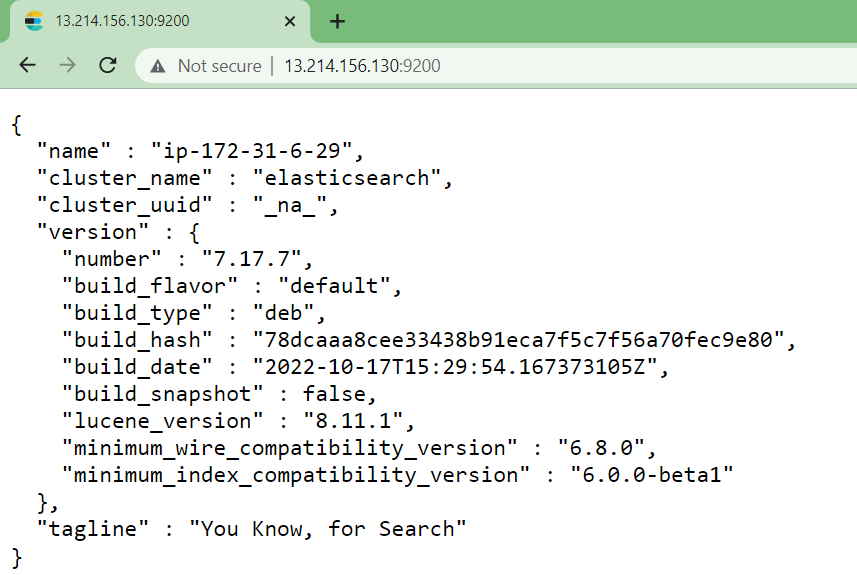


* Set Security group inbound rules as below and attach to ec2

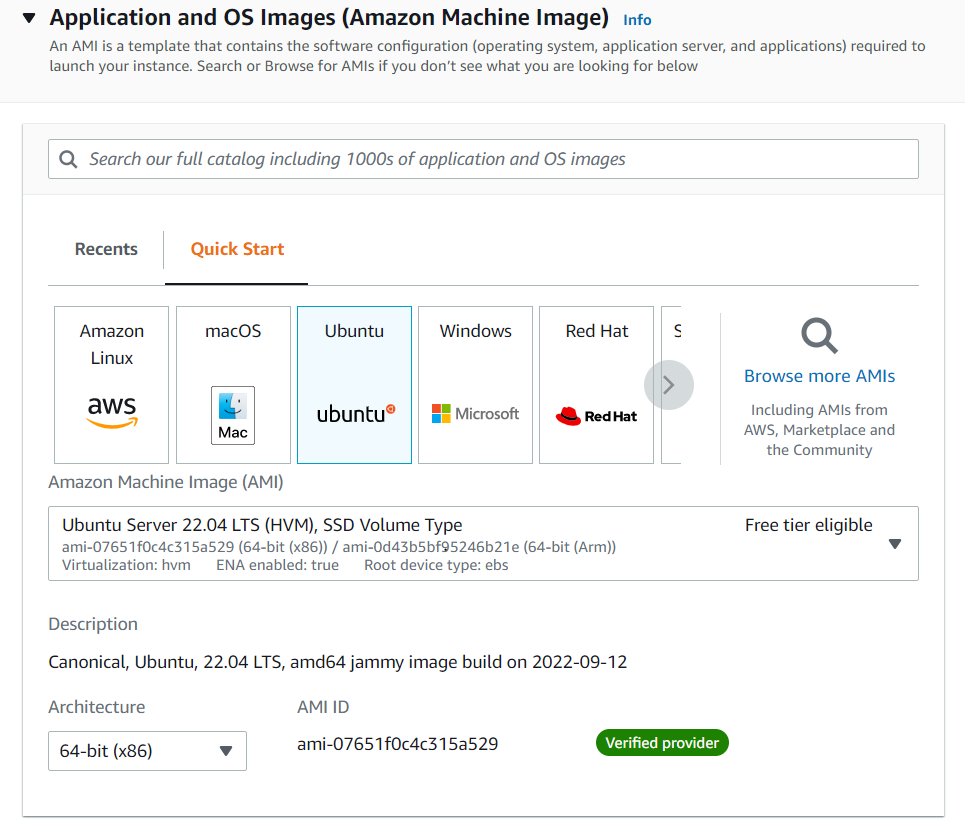


* Login to ec2 instance-1 in Git Bash : ssh -i pem ubuntu@18.143.159.72
* Run following commands as ubuntu user

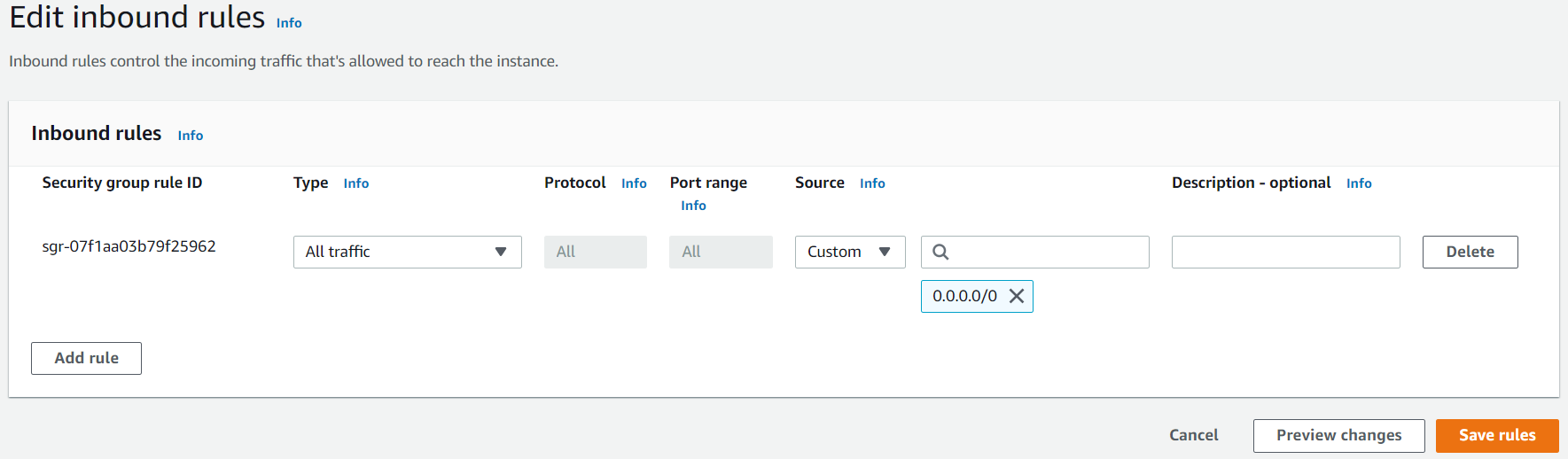
**Installing Elasticsearch and Kibana on ec2 instance-1:**

1. wget -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  
   
10. curl 127.0.0.1:9200  
      
      
    Elastic search installation is completed successfully and running
11. sudo apt-get install kibana
12. sudo vi /etc/kibana/kibana.yml  
    set => server.host: 0.0.0.0  
    
13. sudo systemctl start kibana.service
14. sudo systemctl enable kibana.service
15. sudo systemctl status kibana.service  
    
16. Instance public IP:5601  
    **Result in Web**  
      
      
    Kibana installation is completed successfully and running  
      
    **change elasticsearch configuration**
17. sudo vi /etc/elasticsearch/elasticsearch.yml  
    set => network.host: 0.0.0.0  
    set => discovery.seed\_hosts: ["127.0.0.1"]  
      
    
18. sudo systemctl restart elasticsearch.service
19. ec2 Instance-1 public IP:9200  
    **Result in Web**  
    

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

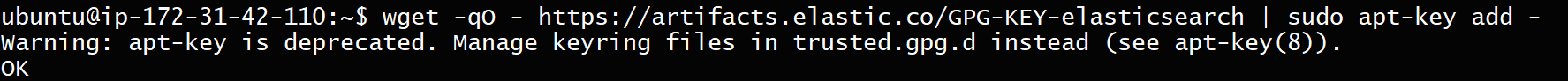
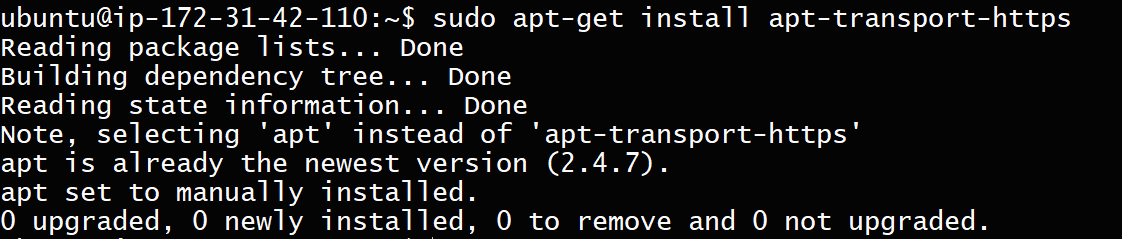
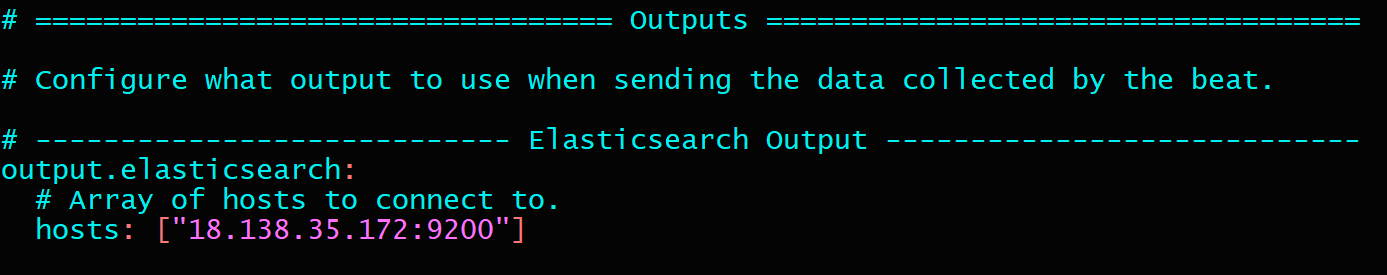
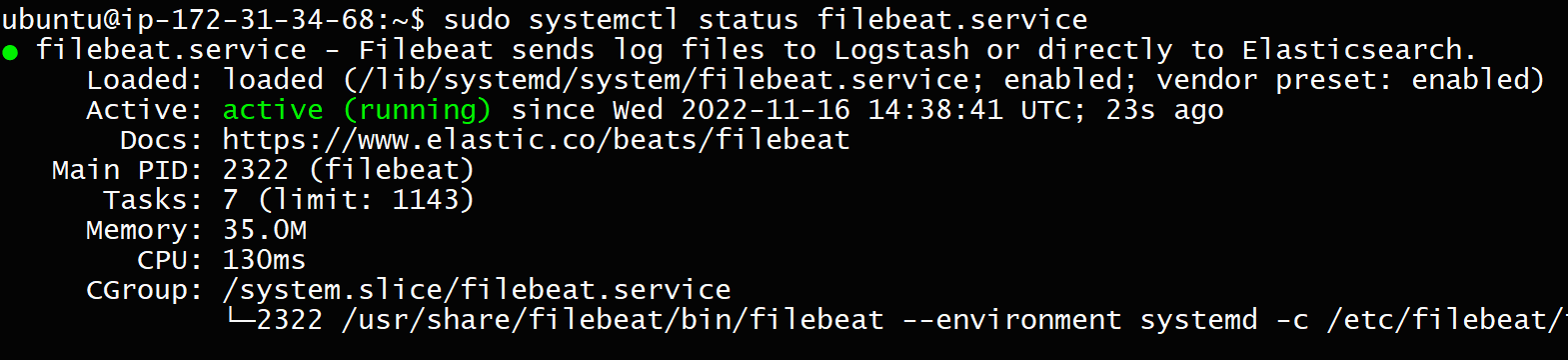


* Set Security group inbound rules as below and attach to ec2



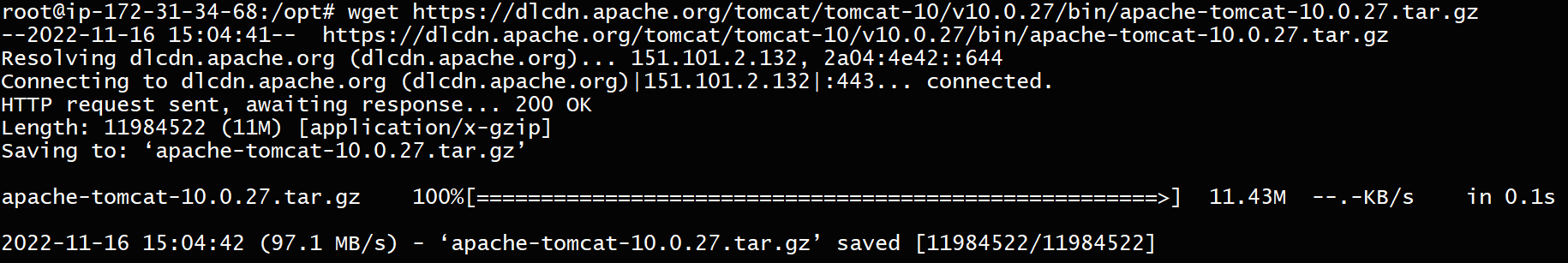
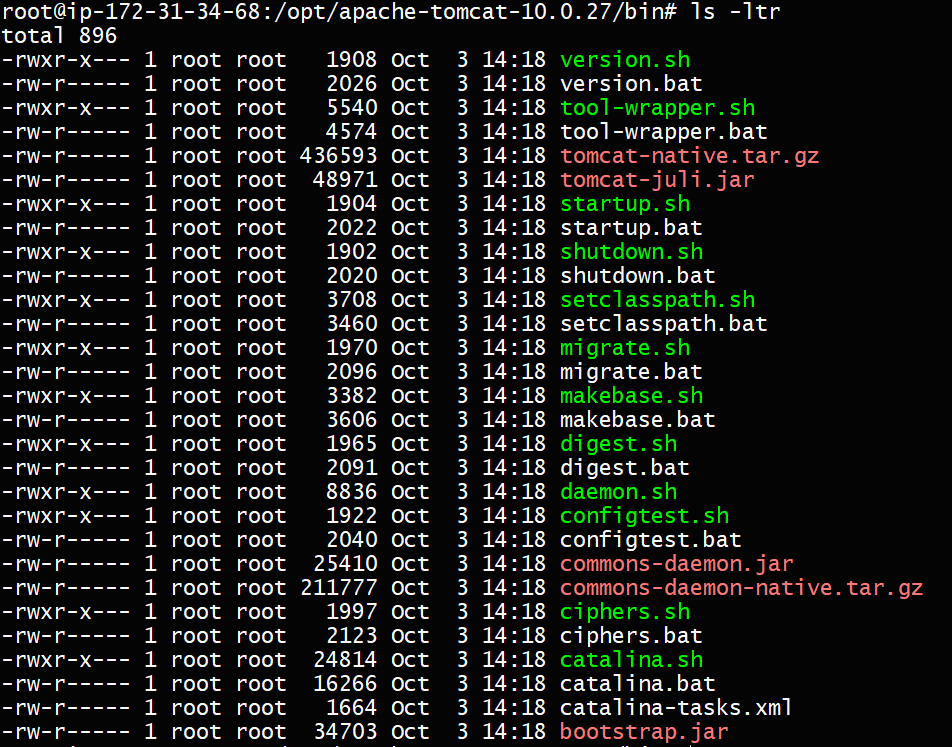
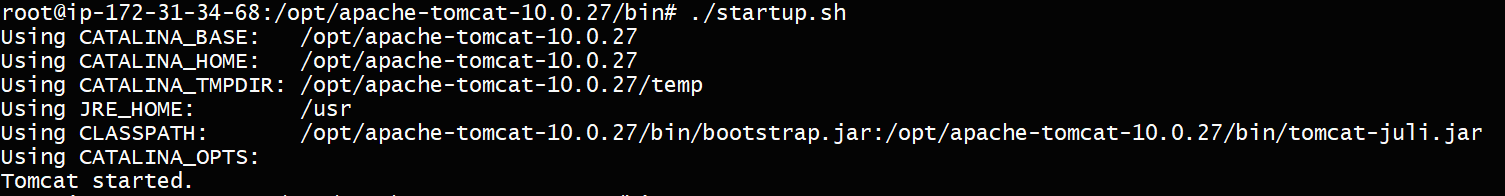
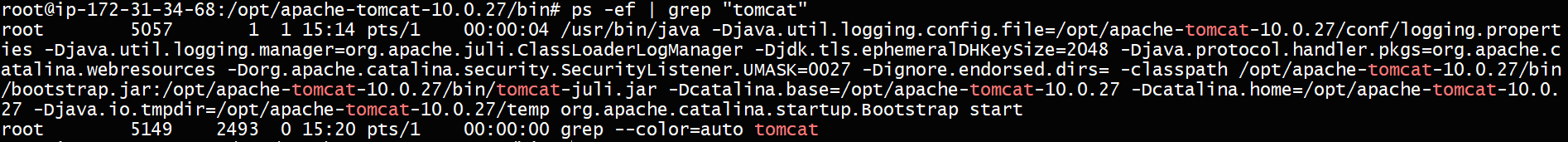
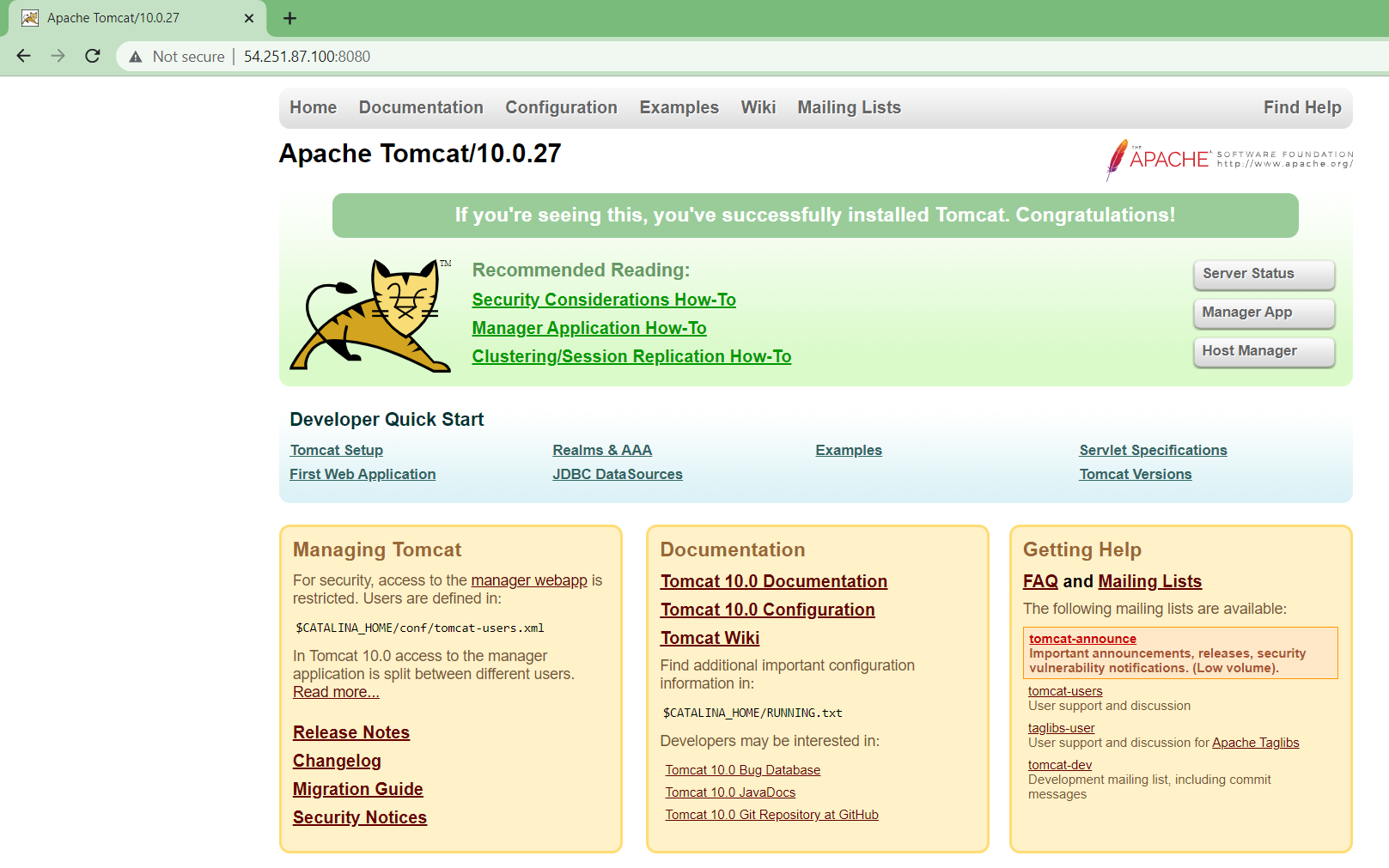
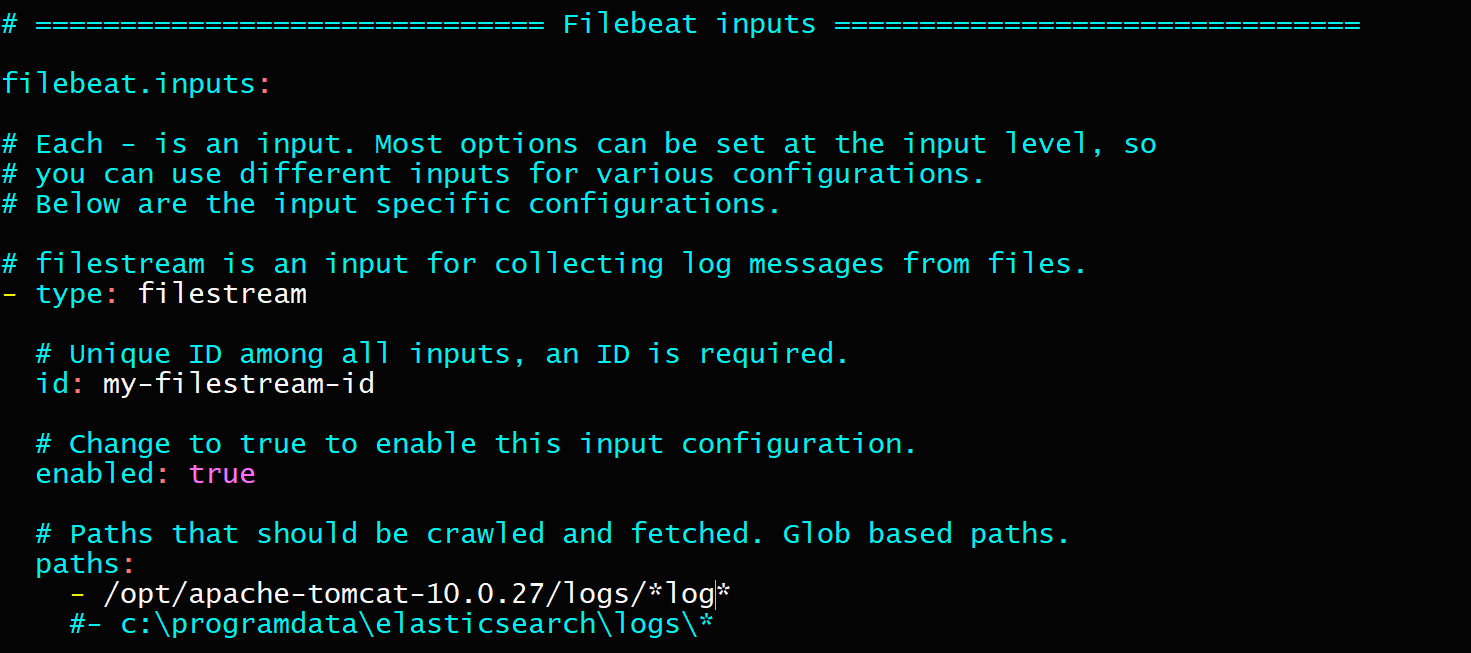
* Login to ec2 instance-2 in Git Bash : ssh -i pem ubuntu@18.140.159.77
* Run following commands as ubuntu user

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

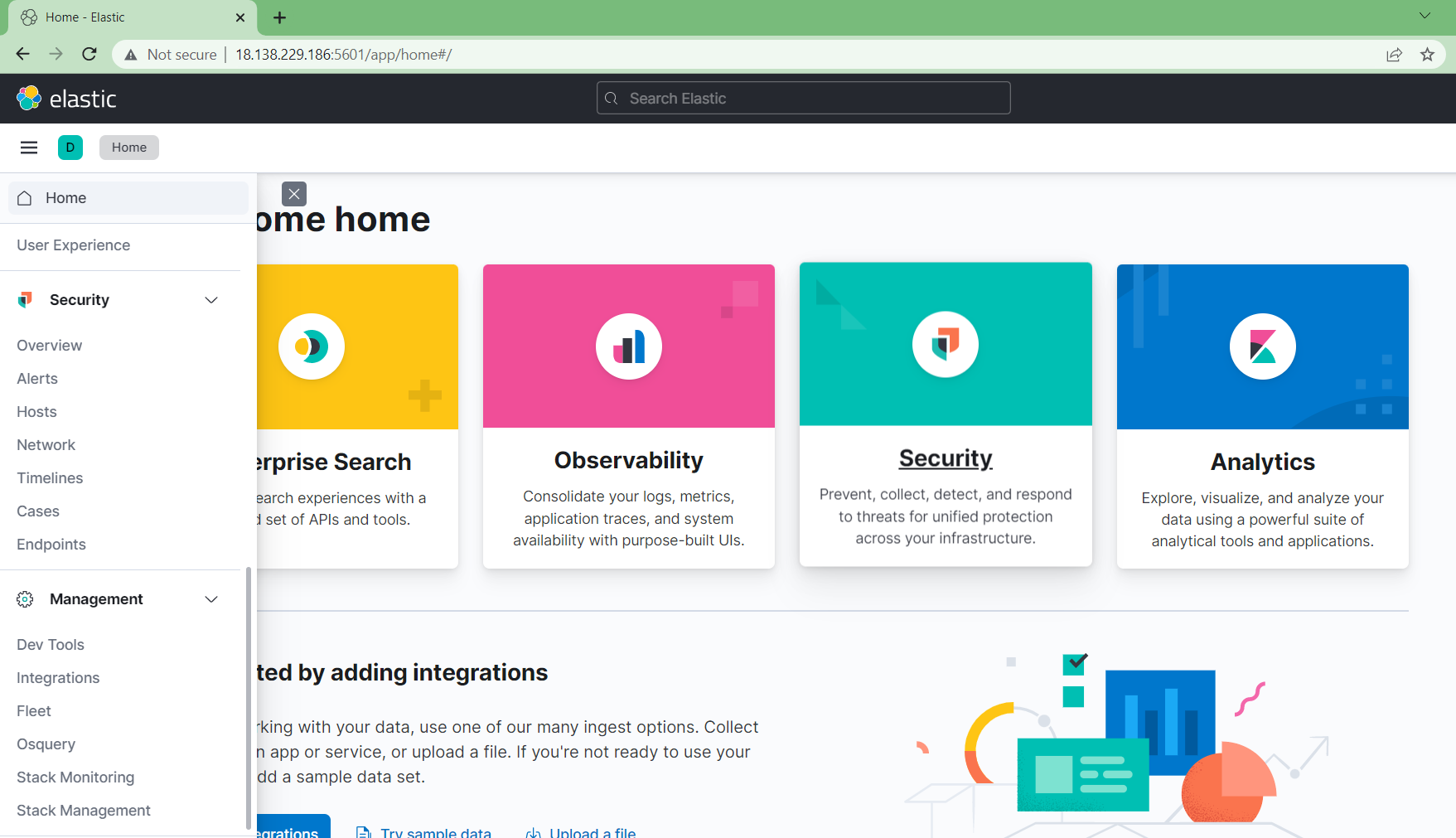
1. wget -qO - <https://artifacts.elastic.co/GPG-KEY-elasticsearch> | sudo apt-key add -  
   
2. sudo apt-get install apt-transport-https  
   
3. echo "deb <https://artifacts.elastic.co/packages/7.x/apt> stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
4. sudo apt-get update
5. sudo apt-get install filebeat
6. sudo vi /etc/filebeat/filebeat.yml  
   set => outputs hosts: ["18.138.35.172:9200"] (ec2 instance-1 public IP:9200)  
   
7. sudo systemctl start filebeat.service
8. sudo systemctl enable filebeat.service
9. sudo systemctl status filebeat.service  
   

Filebeat installation is completed successfully and running

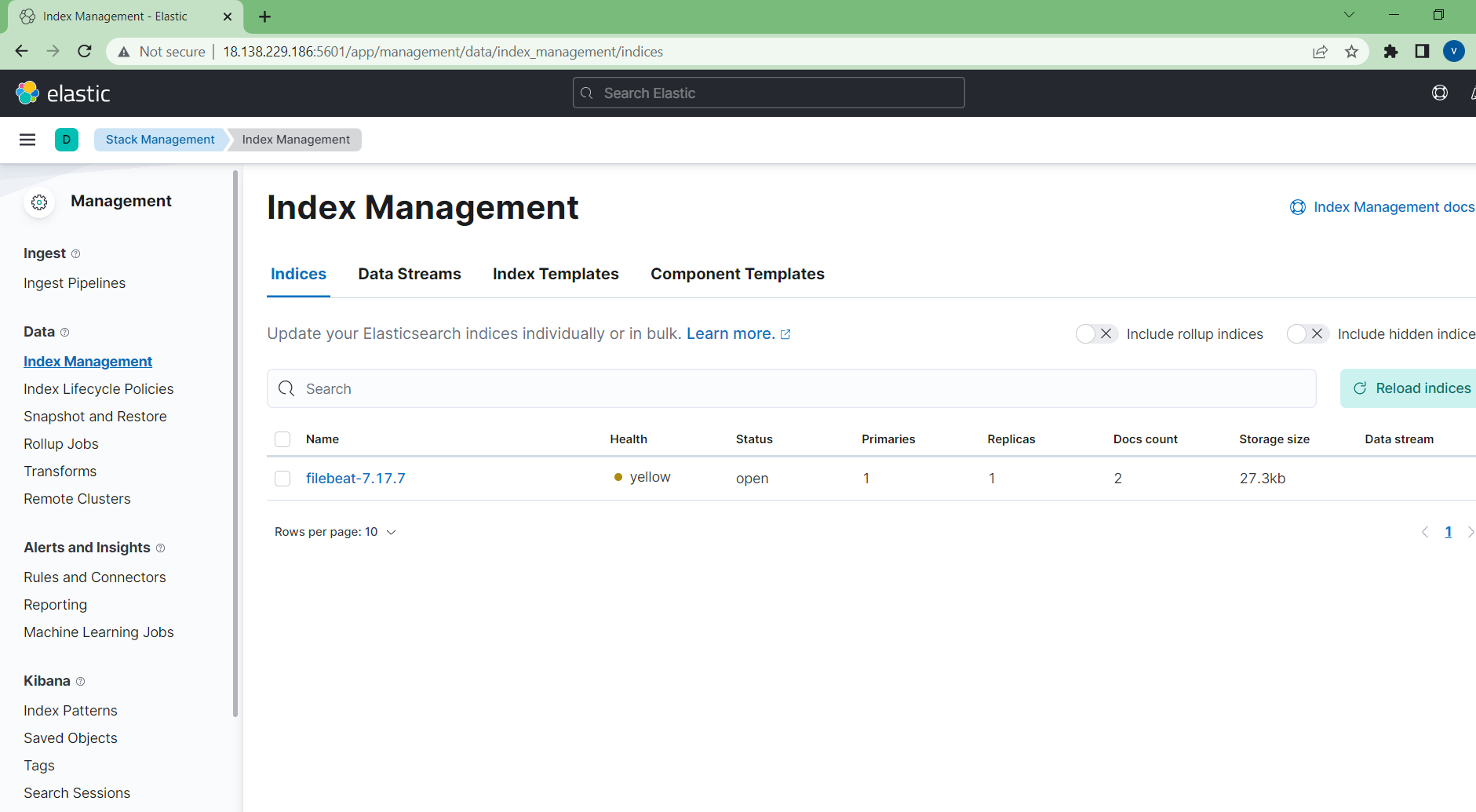
**Installing tomcat on Ec2 instance-2:**

1. sudo su -  
   run following commands as root user
2. cd /opt
3. apt install openjdk-11-jdk
4. wget <https://dlcdn.apache.org/tomcat/tomcat-10/v10.0.27/bin/apache-tomcat-10.0.27.tar.gz>  
   
5. tar -zvxf apache-tomcat-10.0.27.tar.gz
6. cd apache-tomcat-10.0.27/bin/
7. ls -ltr  
   
8. ./startup.sh  
   
9. ps -ef | grep "tomcat"  
   
10. create logs by accessing to Ec2 instance-2 public IP:8080  
    
11. check logs in /opt/apache-tomcat-10.0.27/logs/\*.log  
      
    Tomcat installation is completed successfully and running  
      
    **change Filebeat configuration**
12. sudo vi /etc/filebeat/filebeat.yml  
    set => enabled: true  
    set => - /opt/apache-tomcat-10.0.27/logs/\*log\*  
    
13. sudo systemctl restart filebeat.service

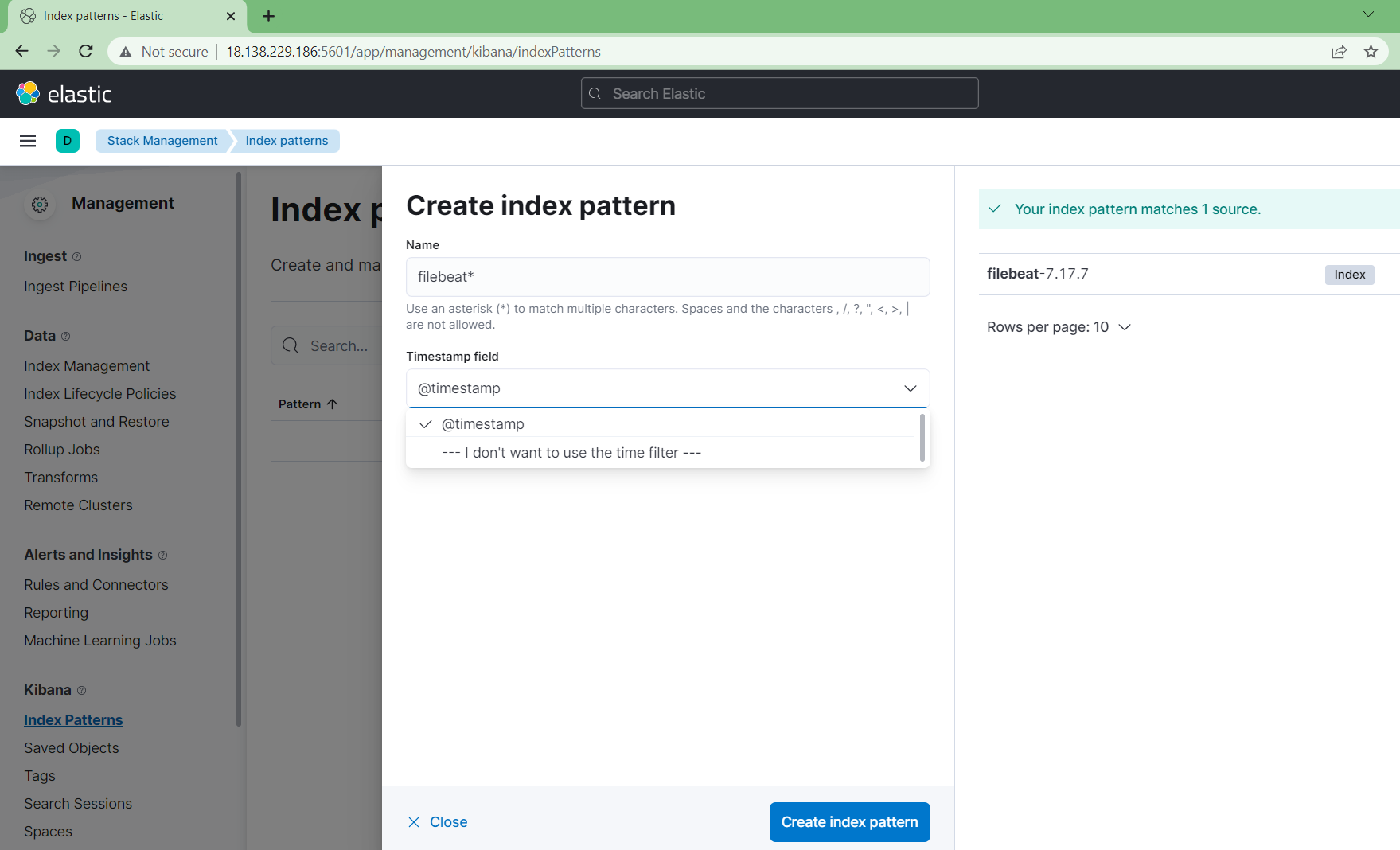
**Log in to Kibana dashboard with ec2 instance-1 public IP:5601**



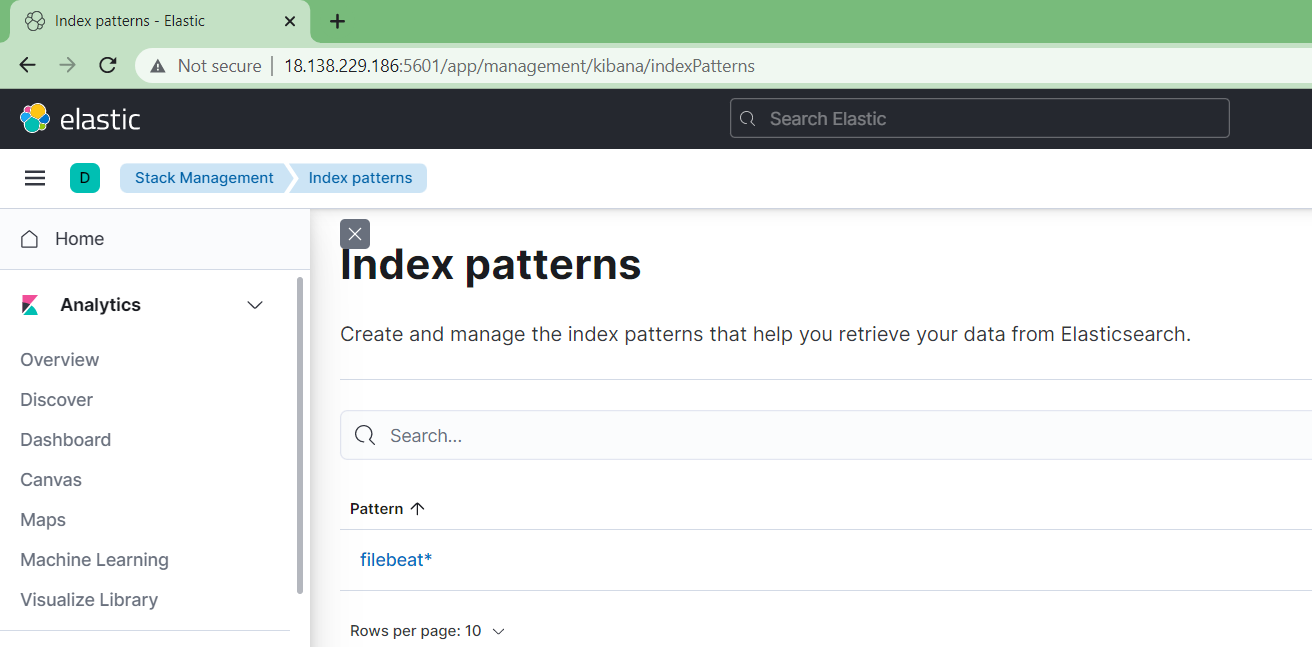
* open Stack Management > Index Management ,check for filebeat logs file availability



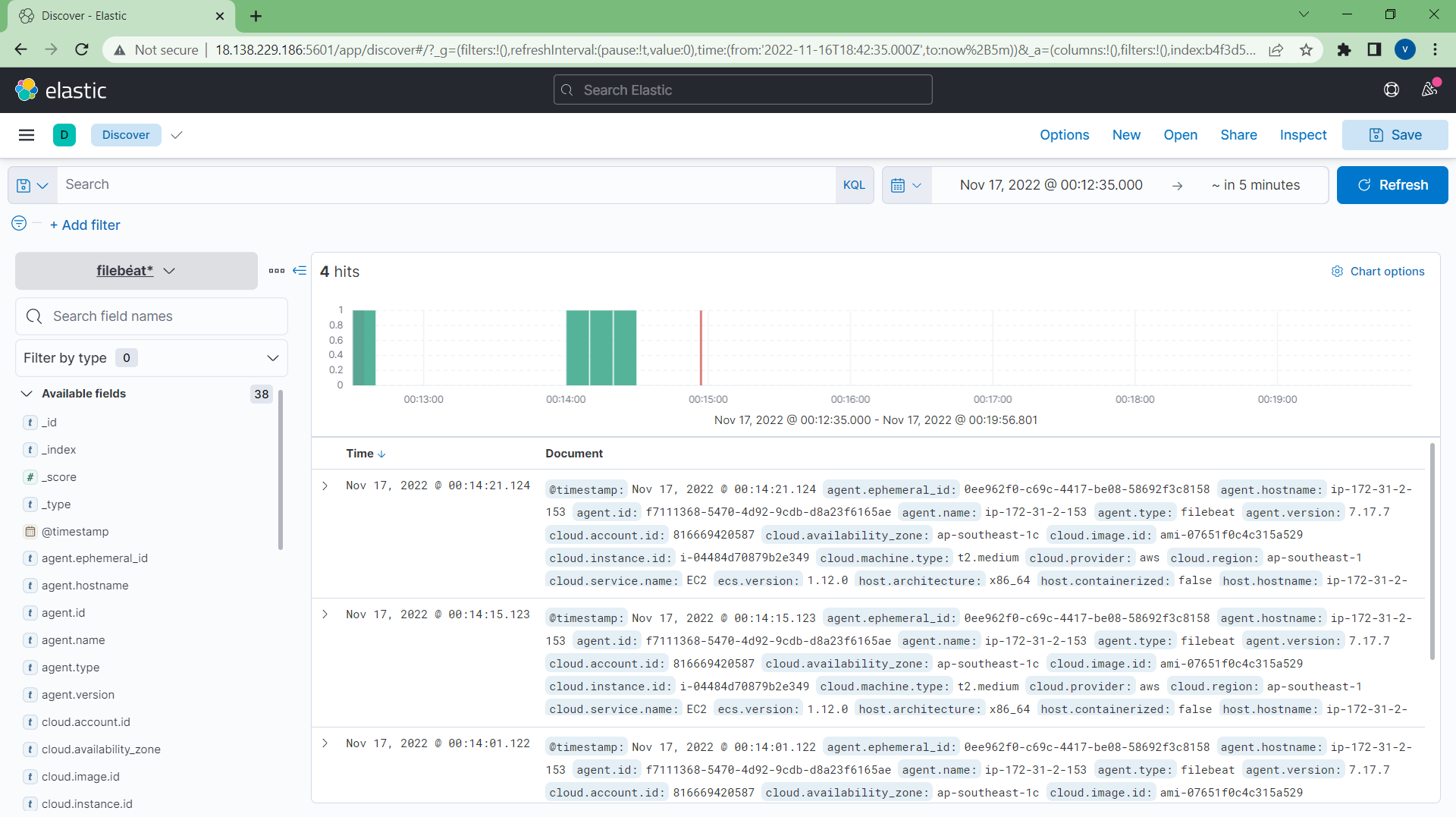
* create Index Pattern



* open Discover



* Choose created index pattern and time to display logs!!!



#you can bring any web servers logs to Kibana by configuring filebeat.yml

**Documented by Vinay**