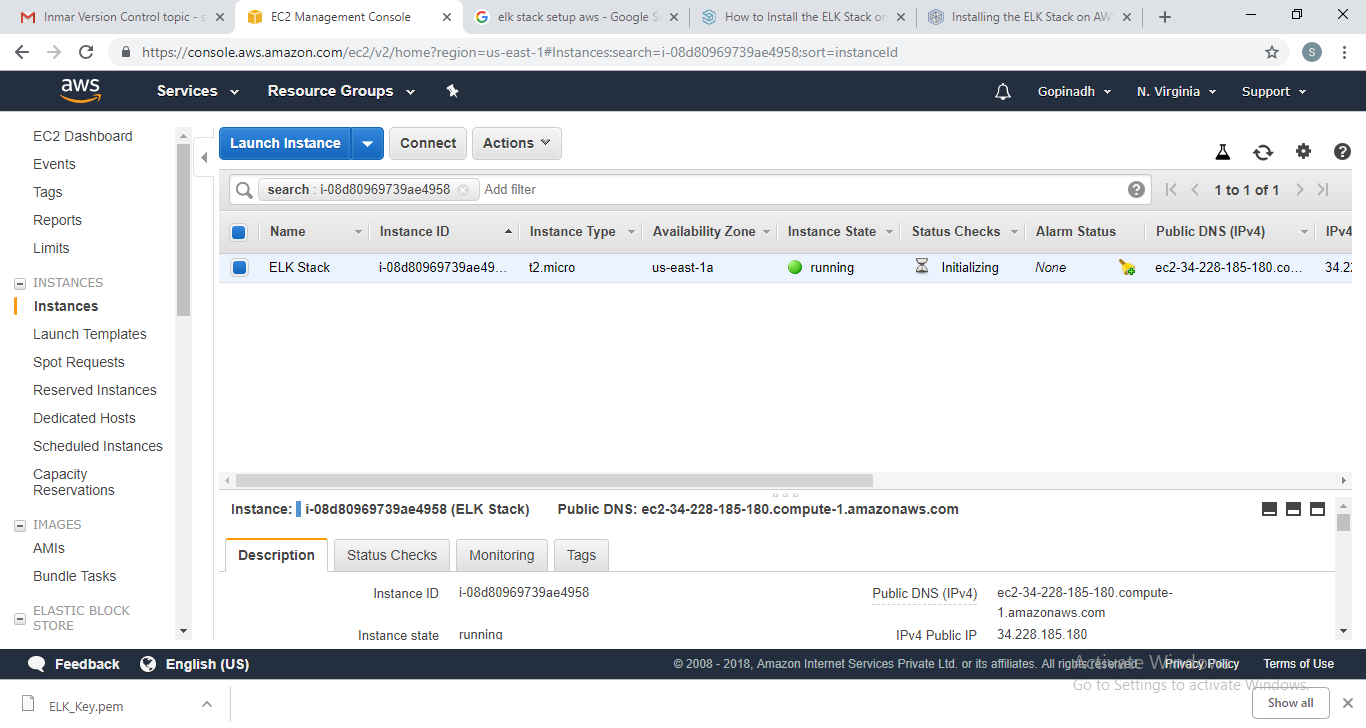
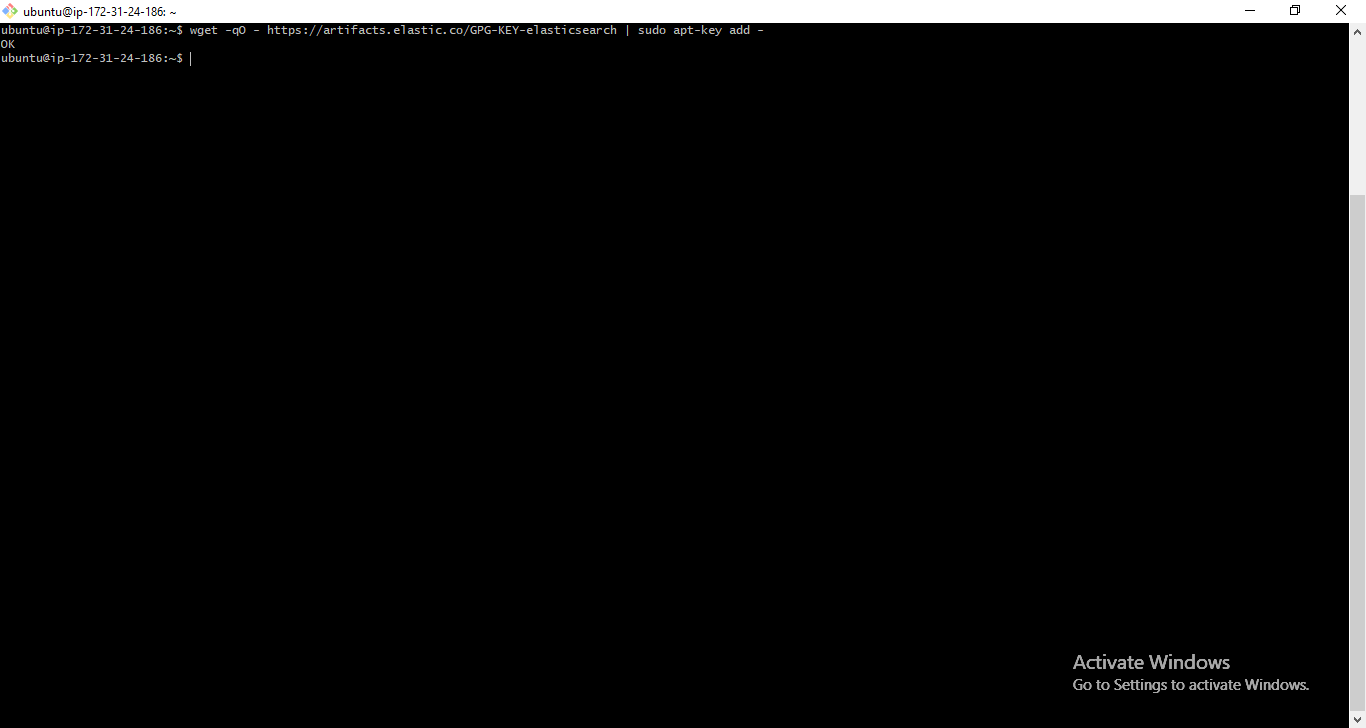
## Step-by-Step ELK Installation

1. Create an EC2 instance.



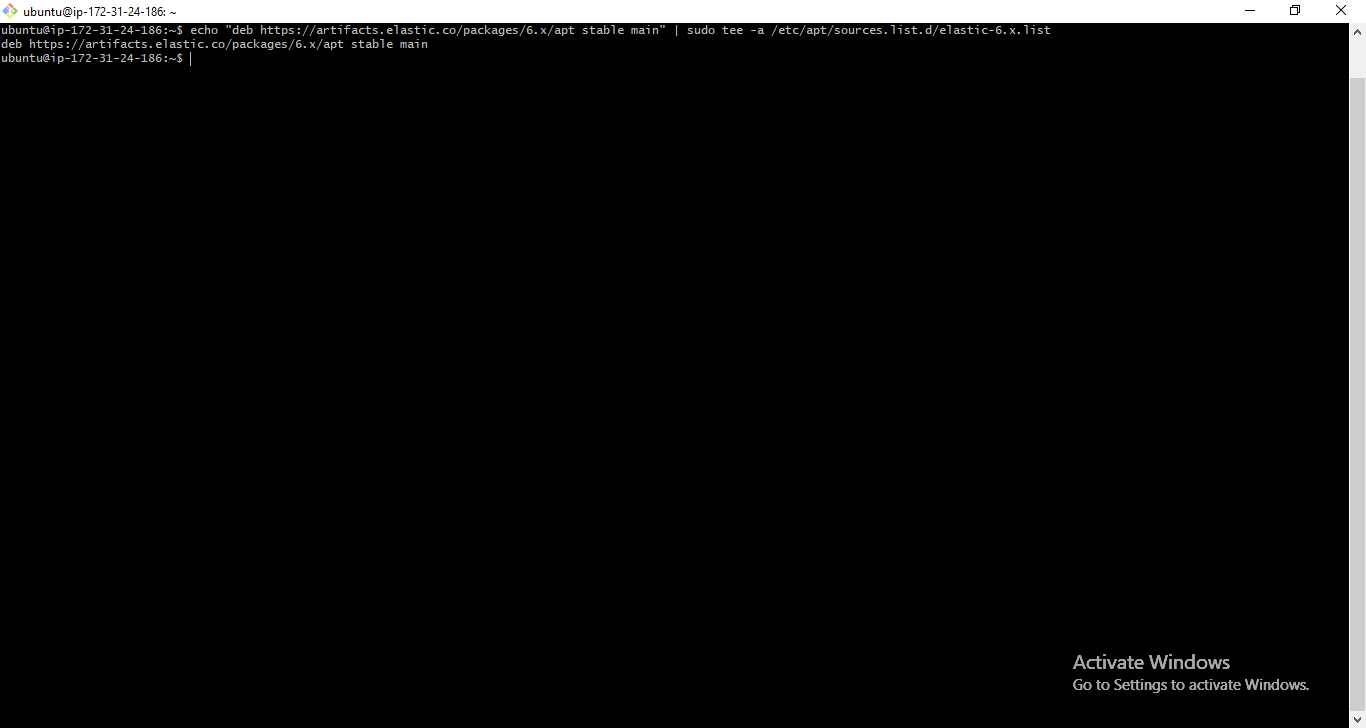
1. To Install ElasticSearch, add the following repository key:
2. $ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

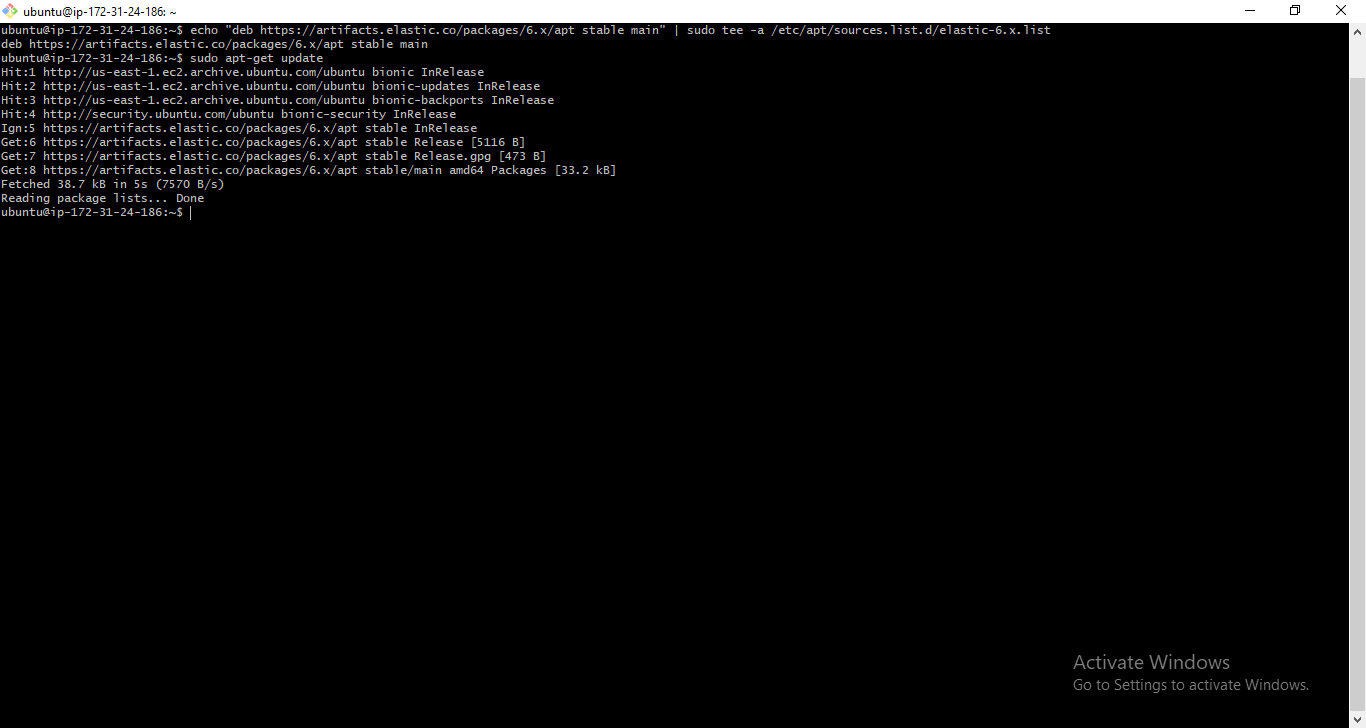


1. Add the following Elasticsearch list to the key:

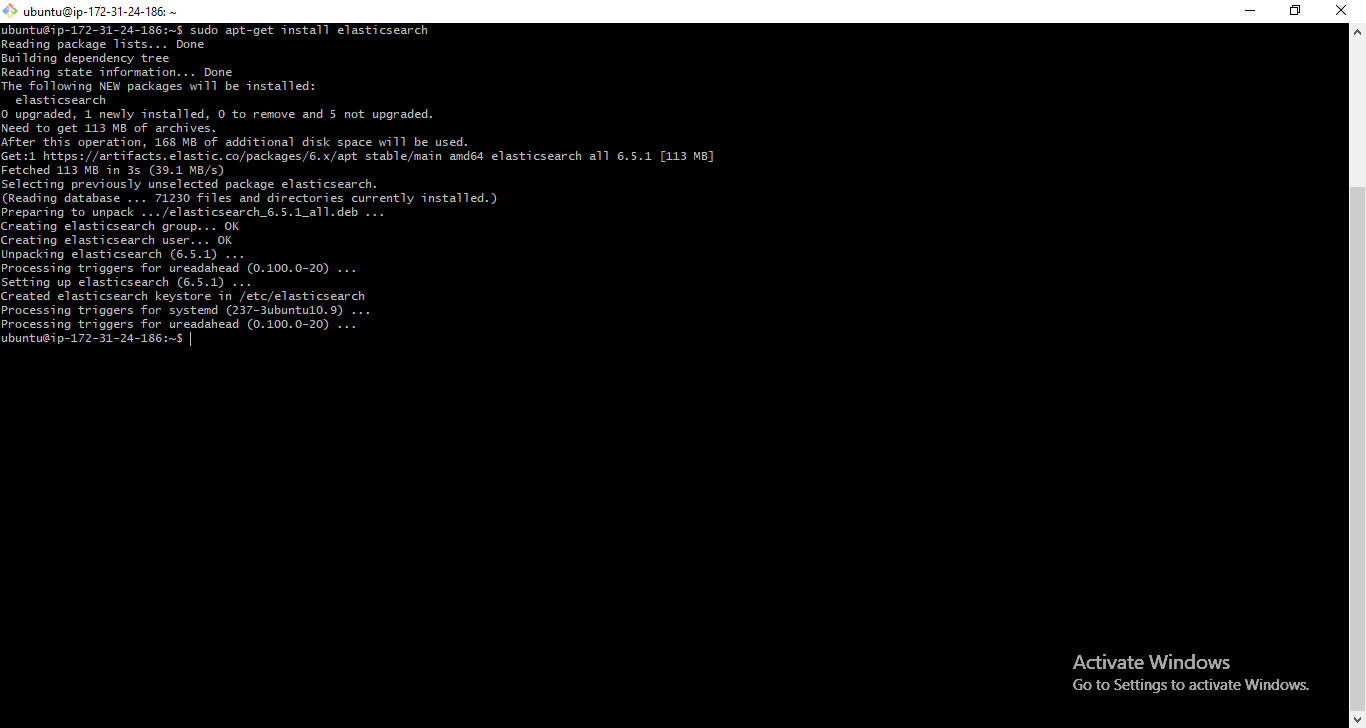
$ echo "deb https://artifacts.elastic.co/packages/6.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-6.x.list

$ sudo apt-get update





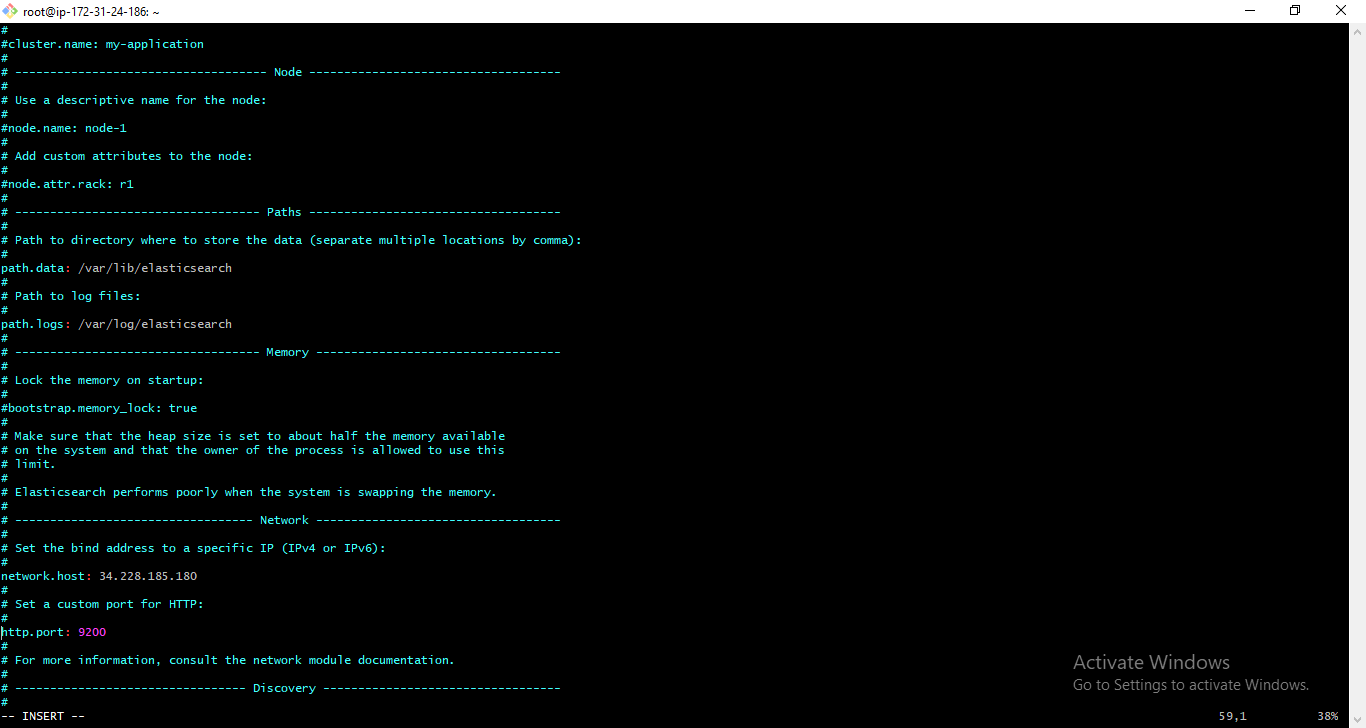
1. Installation: sudo apt-get install elasticsearch



1. Open the Elasticsearch configuration file at: vi /etc/elasticsearch/elasticsearch.yml, and apply the following configurations:

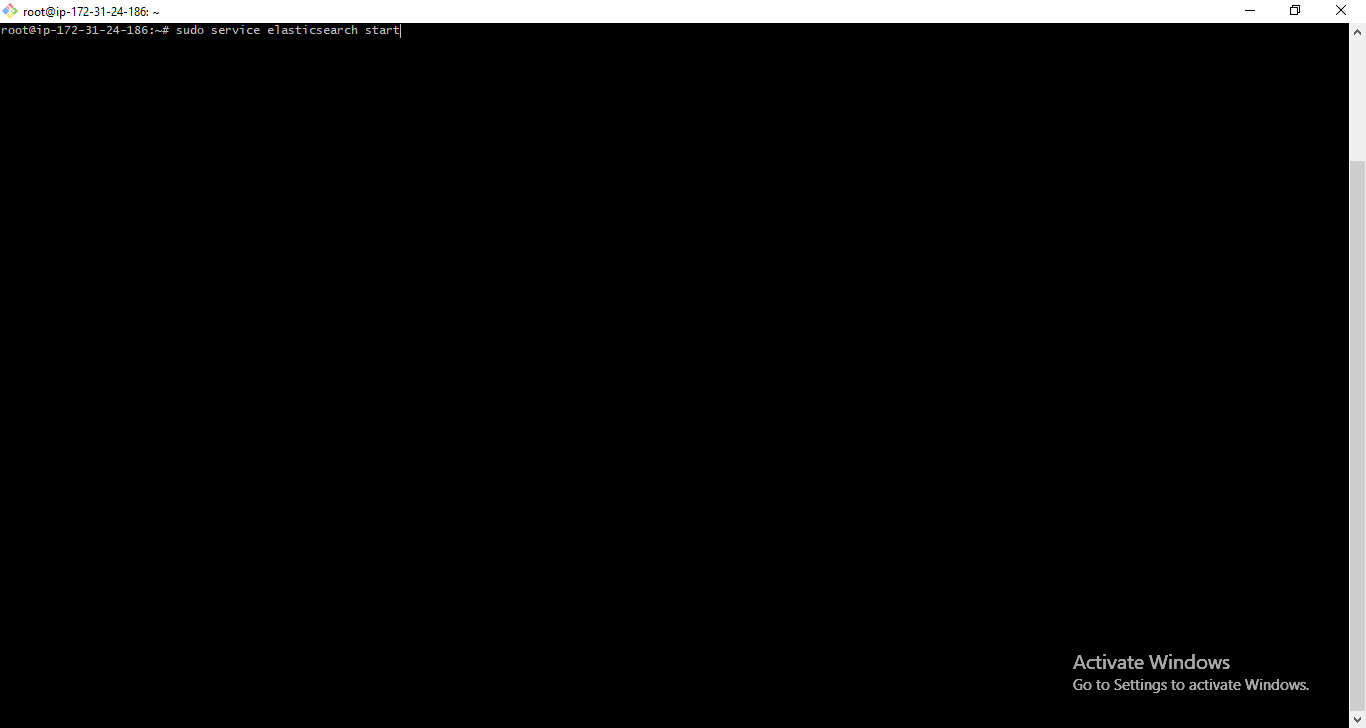
network.host: 34.228.185.180

http.port: 9200



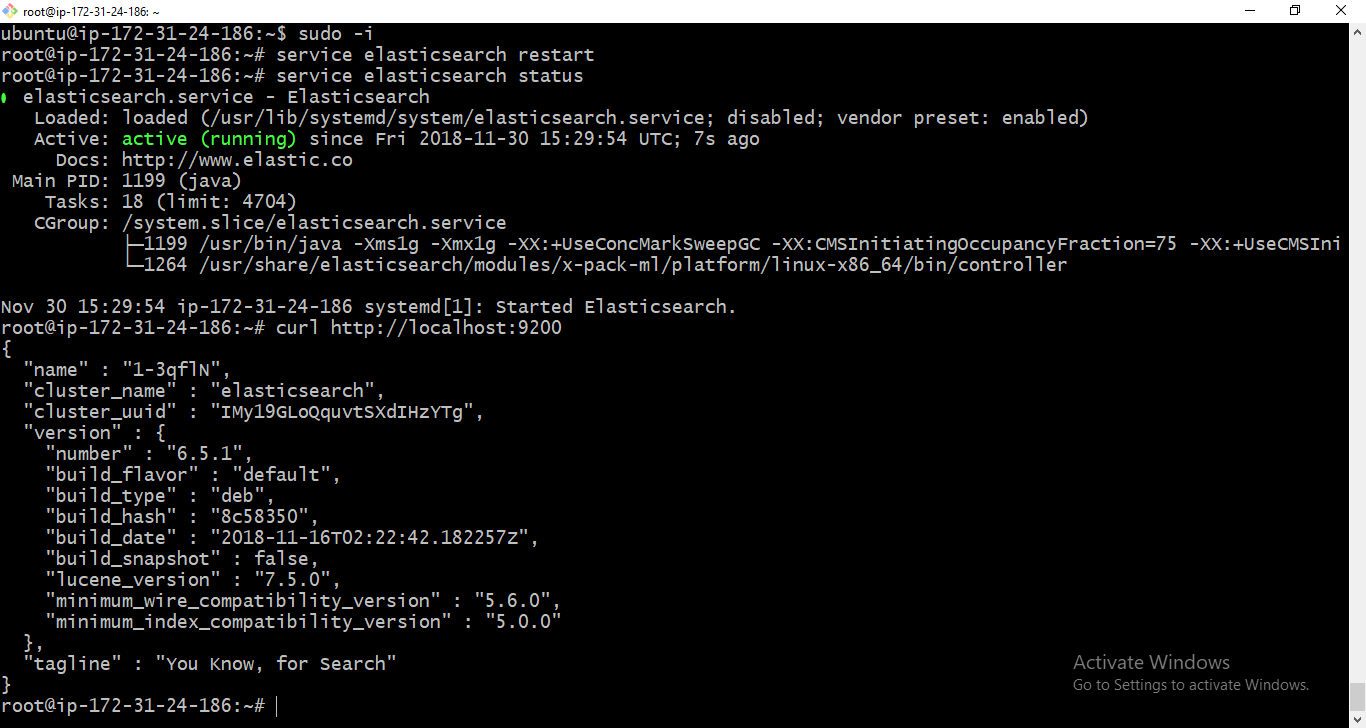
1. Start service:

sudo service elasticsearch start



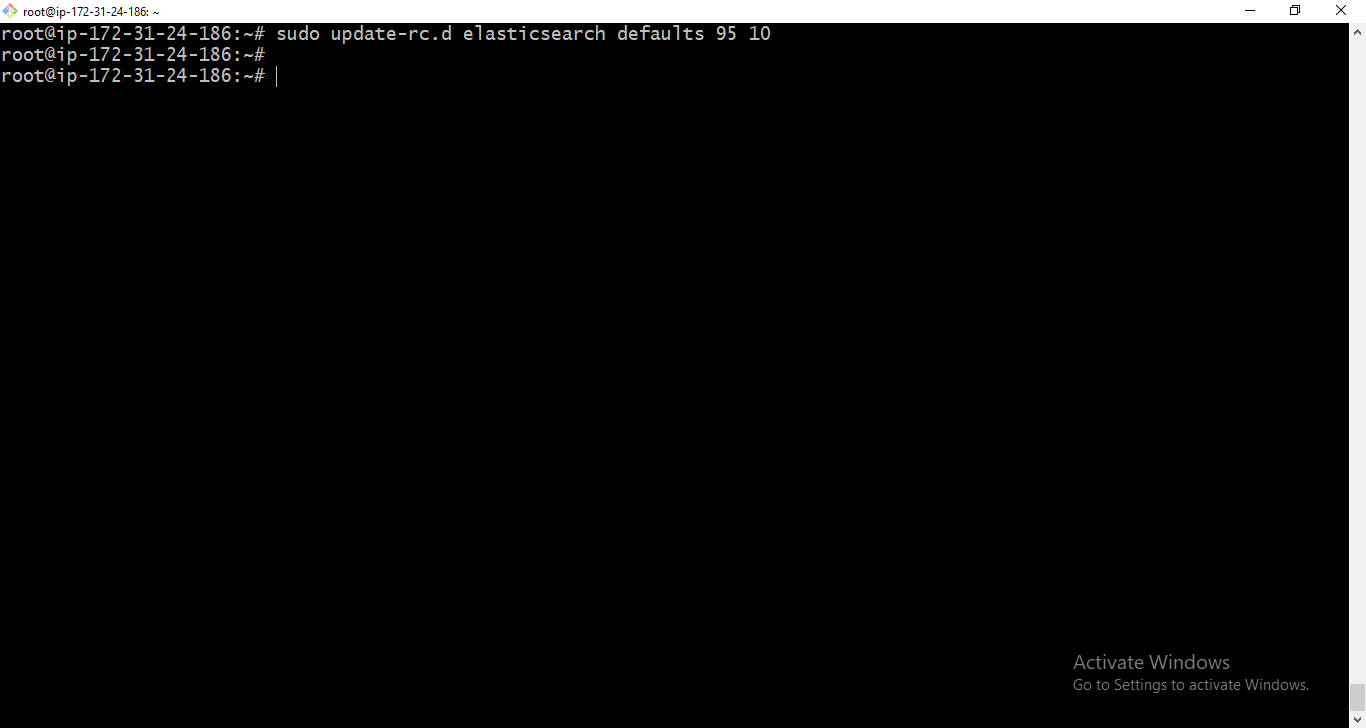
1. Test:

sudo curl http://localhost:9200



1. In order to make the service start on boot run:

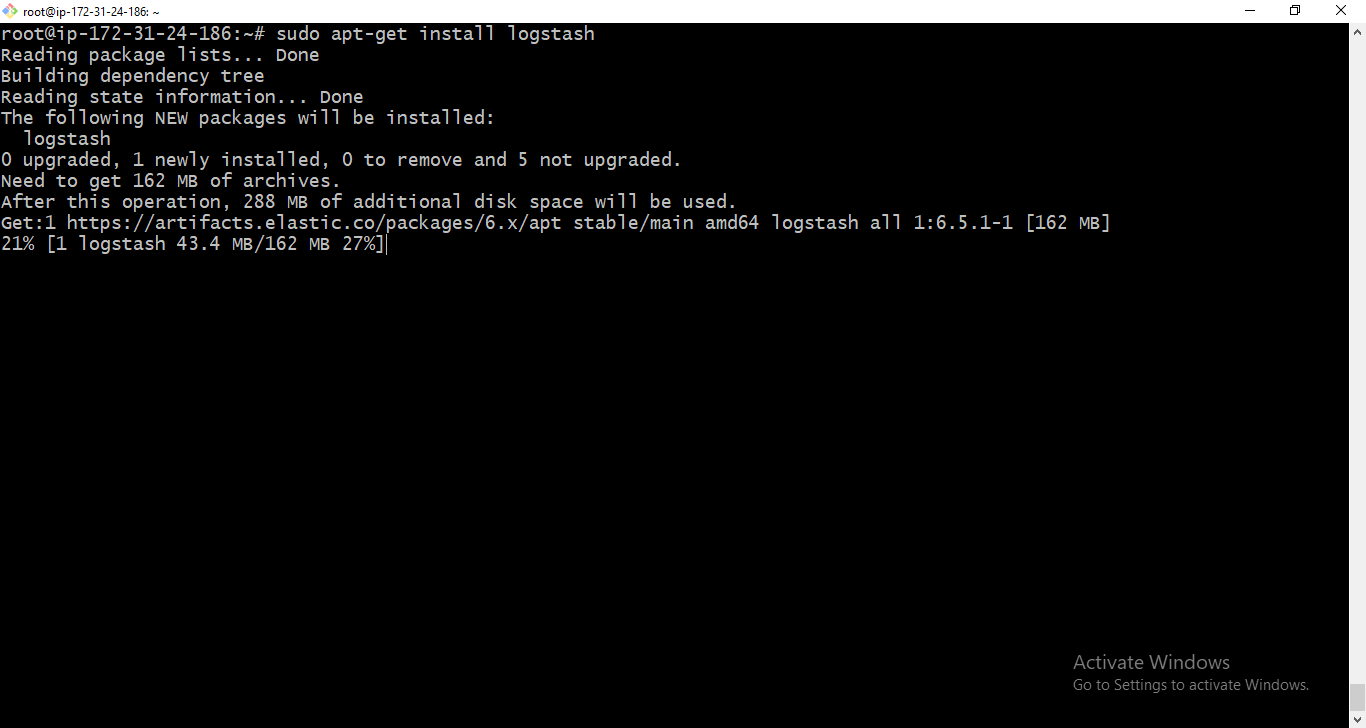
sudo update-rc.d elasticsearch defaults 95 10



## Logstash Installation

1. Install Logstash with:

sudo apt-get install logstash



1. Collect System Logs with Logstash - Create a Logstash configuration file:

sudo vim /etc/logstash/conf.d/10-syslog.conf

1. Enter the following configuration:

input {

file {

type => "syslog"

path => [ "/var/log/messages", "/var/log/\*.log" ]

}

}

output {

stdout {

codec => rubydebug

}

elasticsearch {

hosts => "52.91.183.106" # Use the internal IP of your Elasticsearch server

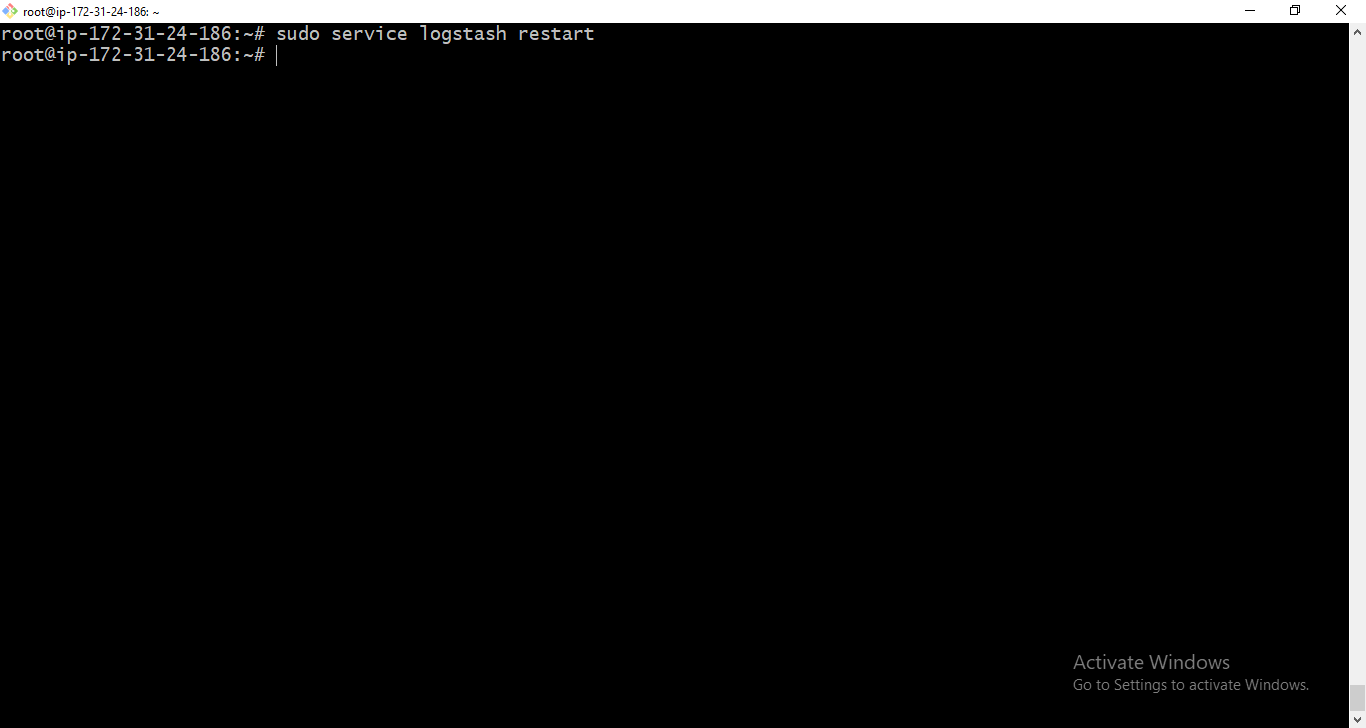
}

}

Note: This file tells Logstash to store the local syslog ‘/var/log/syslog’ and all the files under ‘/var/log\*.log’ inside the Elasticsearch database in a structured way. The input section specifies which files to collect (path) and what format to expect (syslog). The output section uses two outputs – stdout and elasticsearch. The stdout output is used to debug Logstash – you should find nicely-formatted log messages under ‘/var/log/logstash/logstash.stdout’. The elasticsearch output is what actually stores the logs in Elasticsearch.

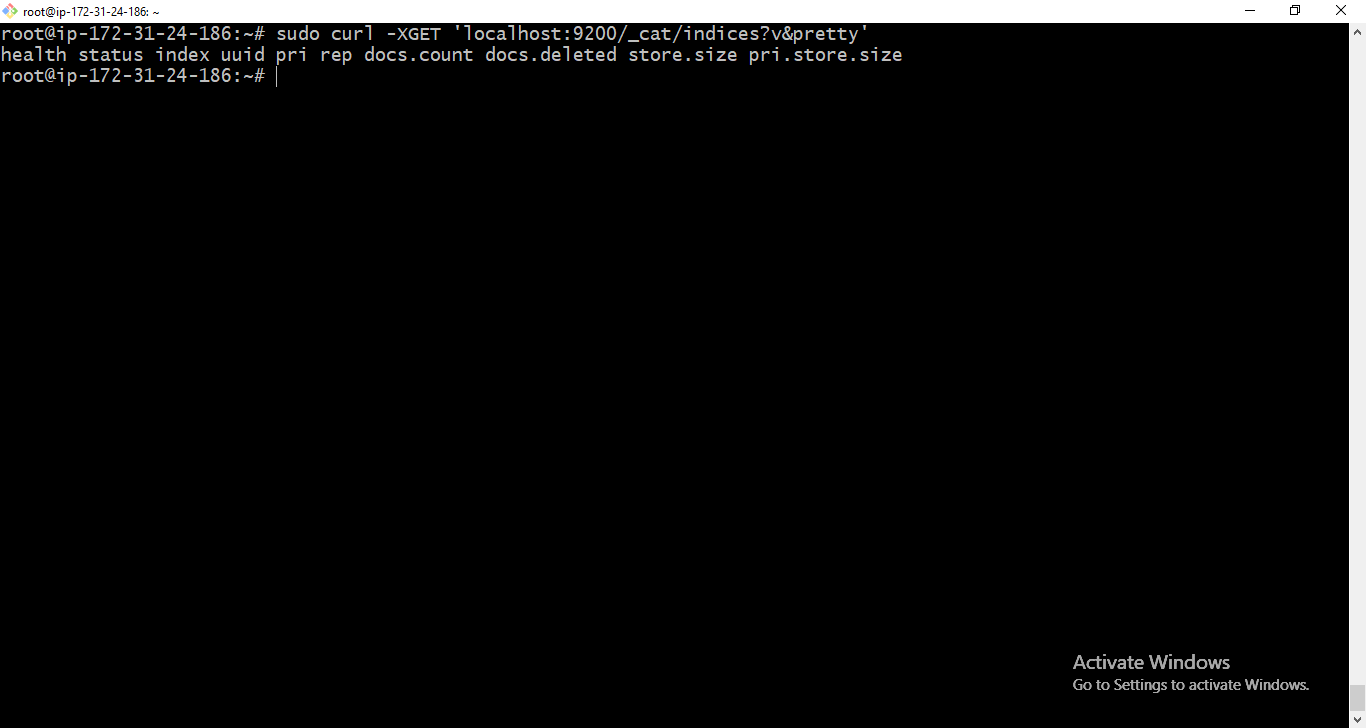
1. Finally, start Logstash to read the configuration:

sudo service logstash restart



1. To make sure the data is being indexed, use:

sudo curl -XGET 'localhost:9200/\_cat/indices?v&pretty'



1. You should see your new Logstash index created:

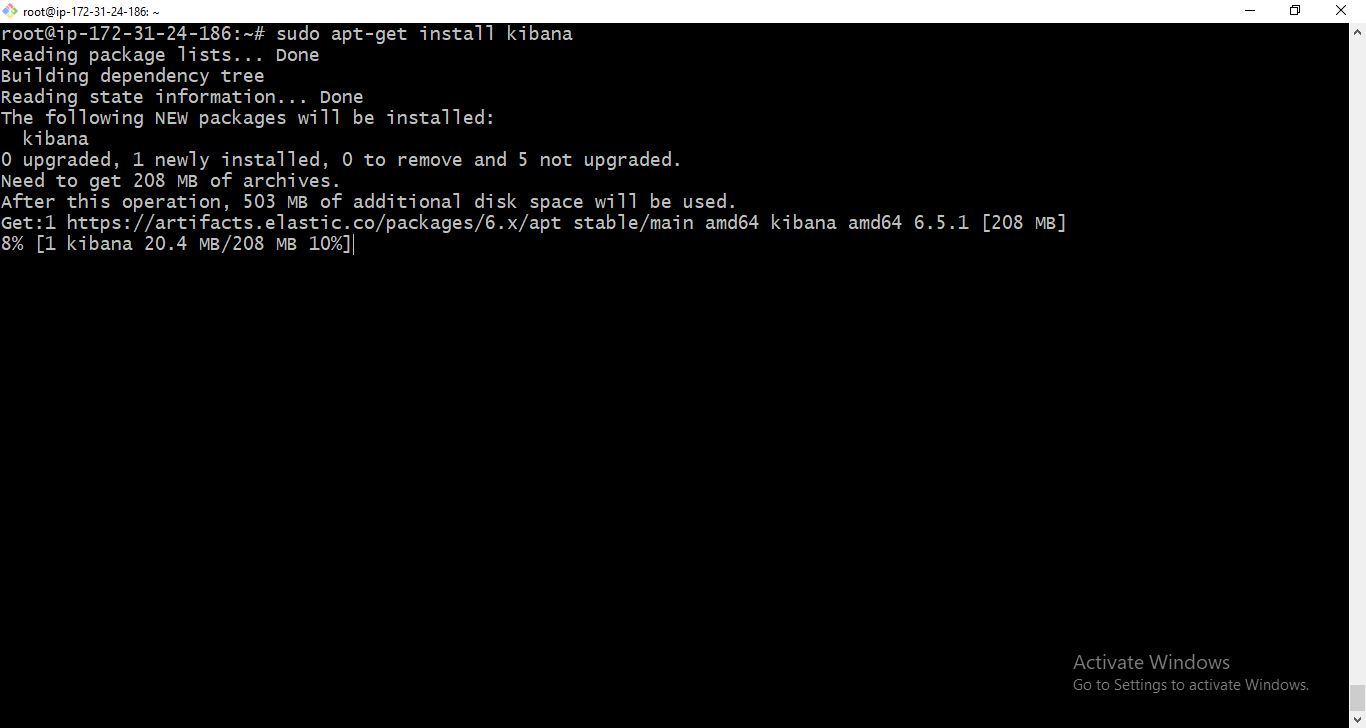
health status index uuid pri rep docs.count docs.deleted store.size pri.store.size

yellow open logstash-2017.12.12 sCf9FxPETImc6pyZMFYacw 5 1 31 0 55.5kb 55.5kb

## Kibana Installation

1. To install Kibana, use this command:

sudo apt-get install kibana



1. Open the Kibana configuration file and enter the following configurations:

sudo vim /etc/kibana/kibana.yml

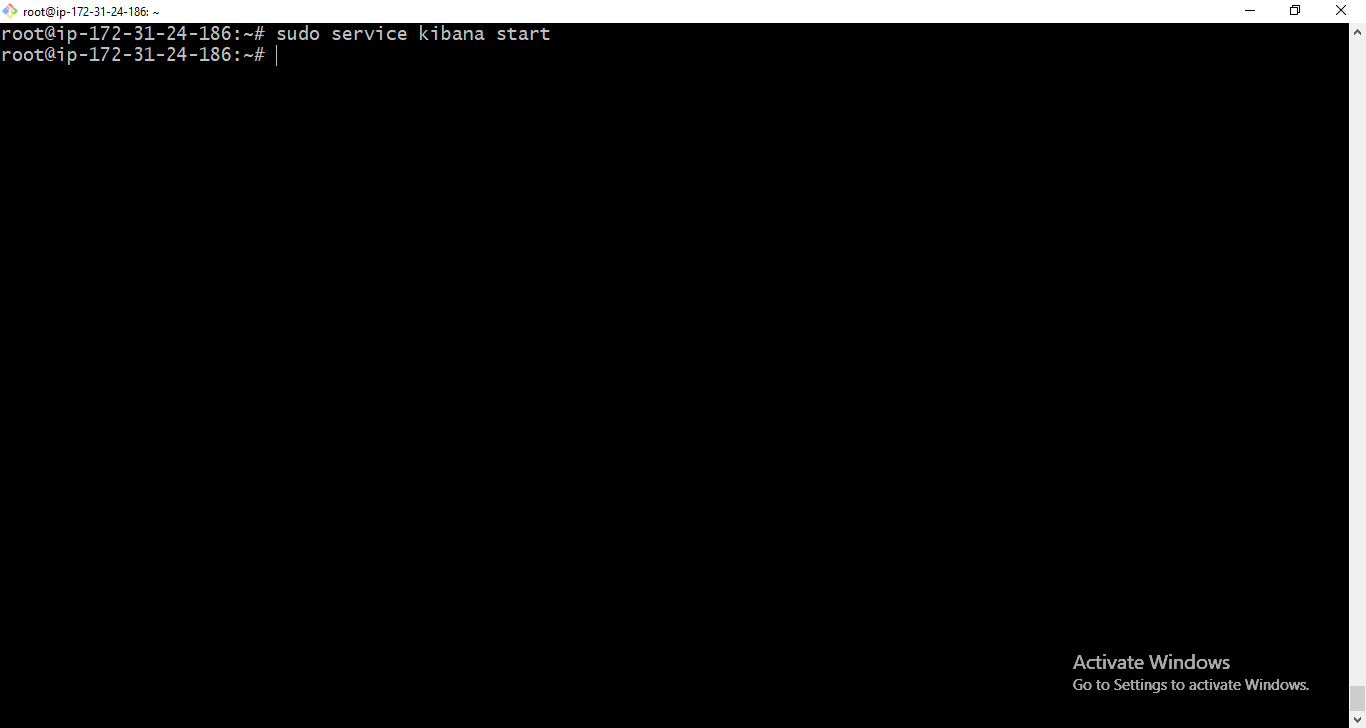
and update the below data:

server.port: 5601

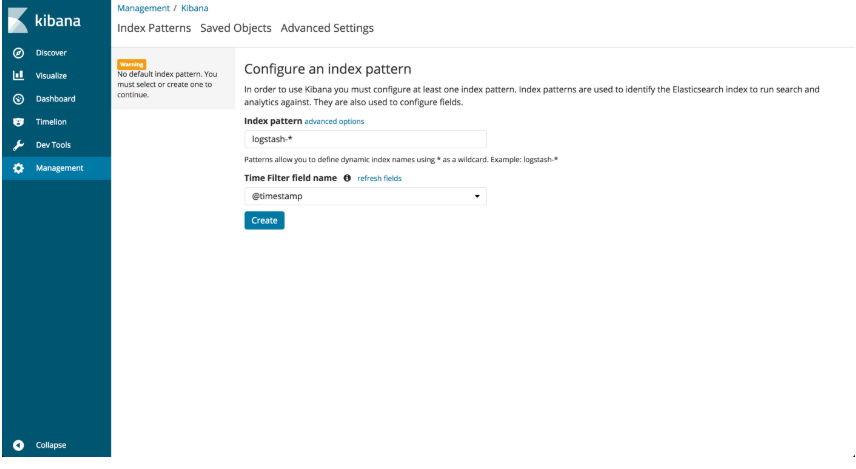
server.host: "localhost"

elasticsearch.url: "http://localhost:9200"

1. Start Kibana: sudo service kibana start



1. Test: Point your browser to ‘http://52.91.183.106:5601’ after Kibana is started.



1. Note: We are accessing Kibana directly through its application server on port 5601, but in a production environment you might want to put a reverse proxy server, like Nginx, in front of it.