## **Logstash and ElasticSearch**

**1934012 - Jayasuriya E**

**1934036 - Sanjay Krishna R**

**Reference Links:**

<https://www.youtube.com/watch?v=3LYP-daiIVU>

<https://phoenixnap.com/kb/how-to-install-elk-stack-on-ubuntu>

<https://www.bmc.com/blogs/elasticsearch-load-csv-logstash/>

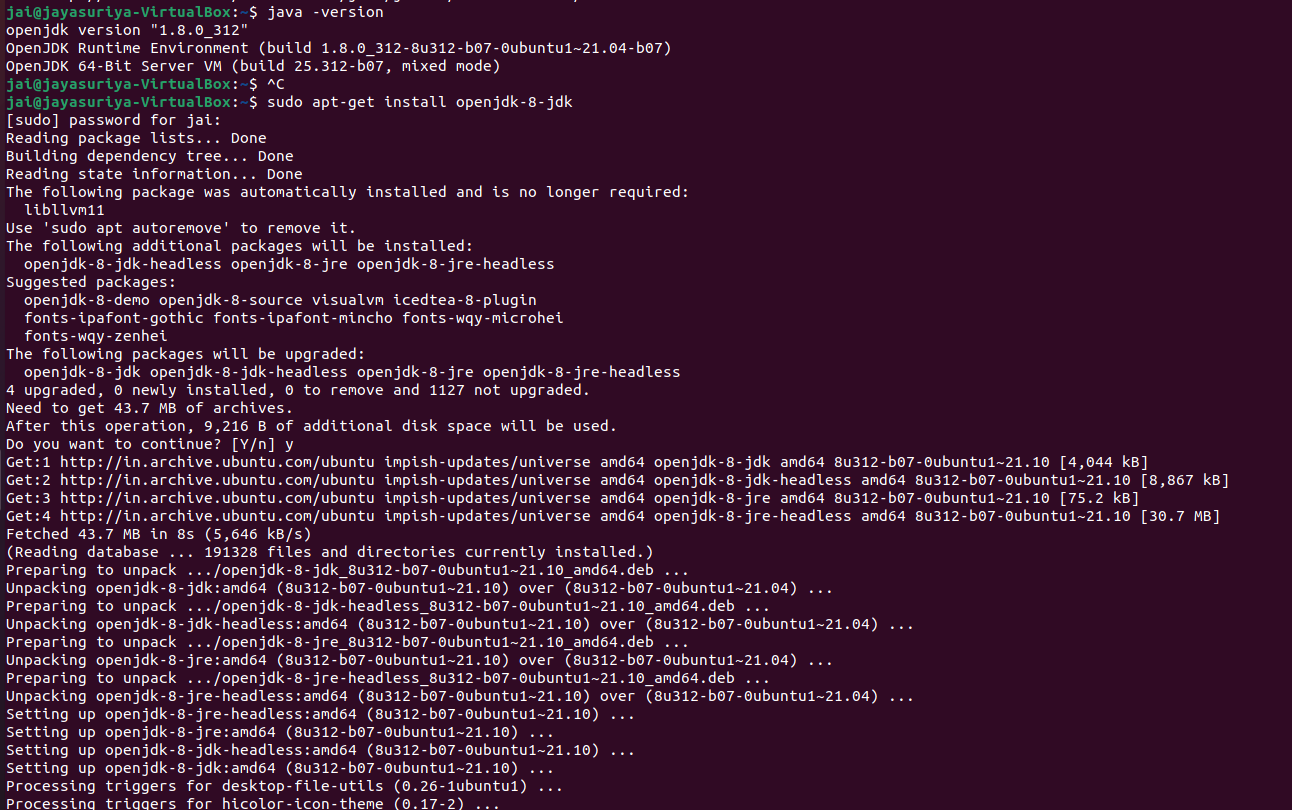
**Prerequisites:**

* java -version

If you don’t have Java 8 installed, install it by opening a terminal window and entering the following:

sudo apt-get install openjdk-8-jdk

If prompted, type y and hit Enter for the process to finish.



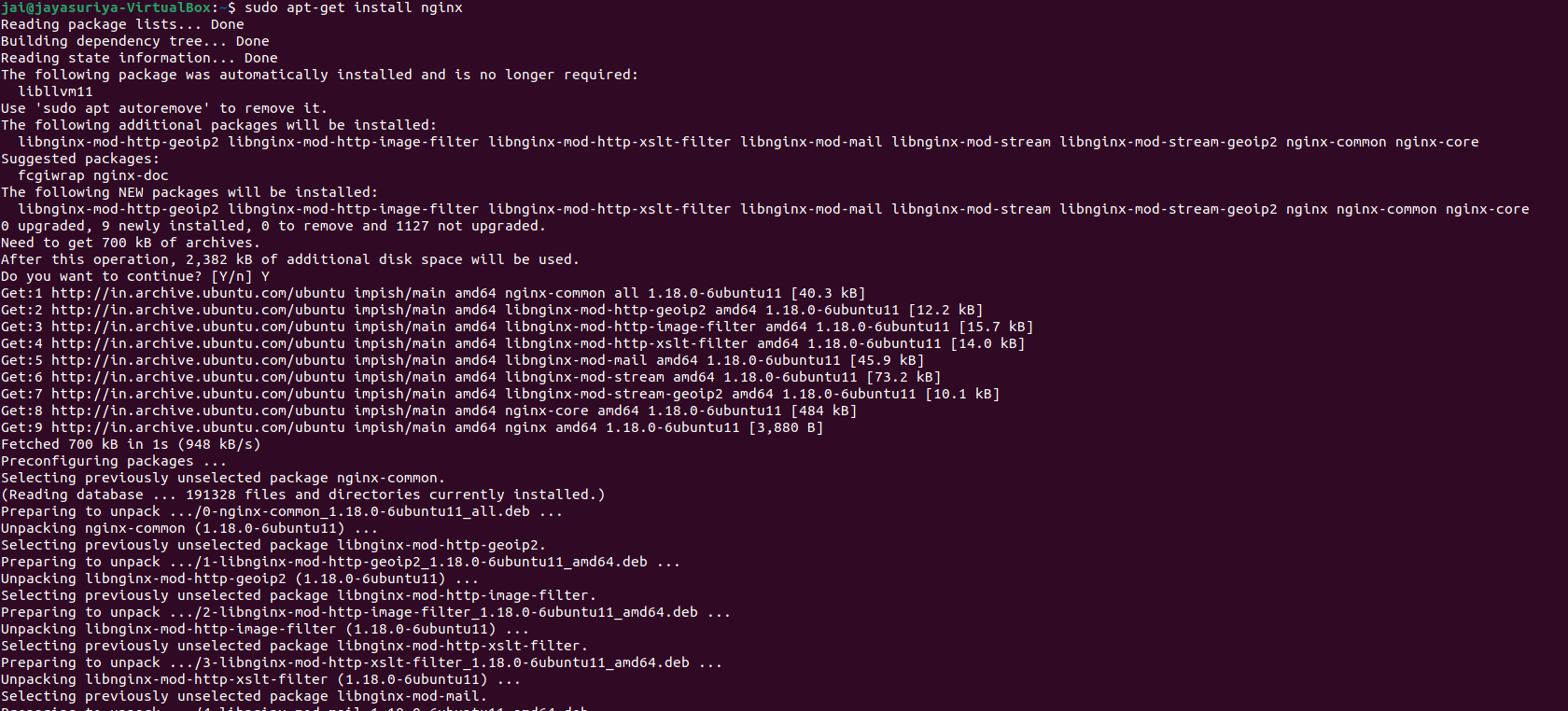
### 

### **Install Nginx**

Nginx works as a web server and proxy server. It’s used to configure password-controlled access to the Kibana dashboard.

Install Nginx by entering the following:

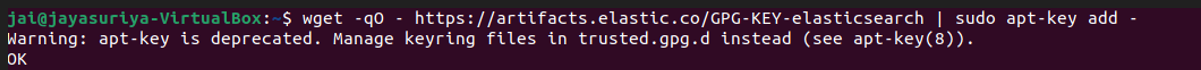
sudo apt-get install nginx



Elastic repositories enable access to all the open-source software in the ELK stack. To add them, start by importing the GPG key.

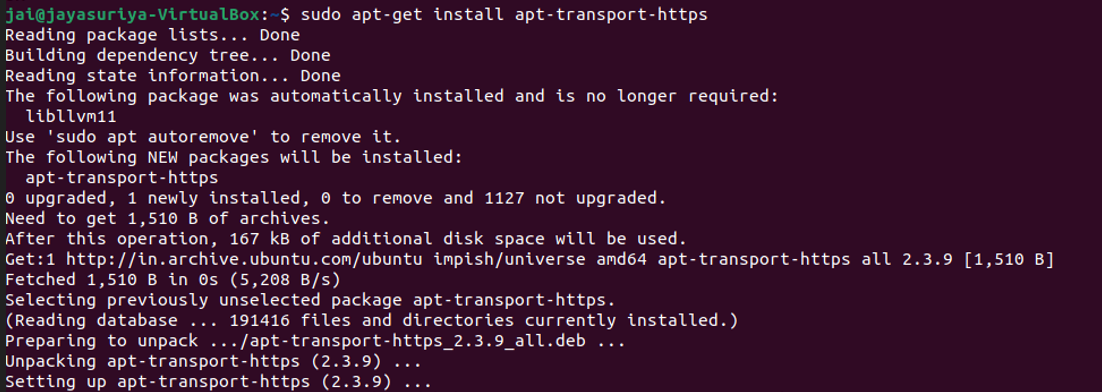
Enter the following into a terminal window to import the PGP key for Elastic:

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



install the apt-transport-https package:

sudo apt-get install apt-transport-https



Add the Elastic repository to your system’s repository list:

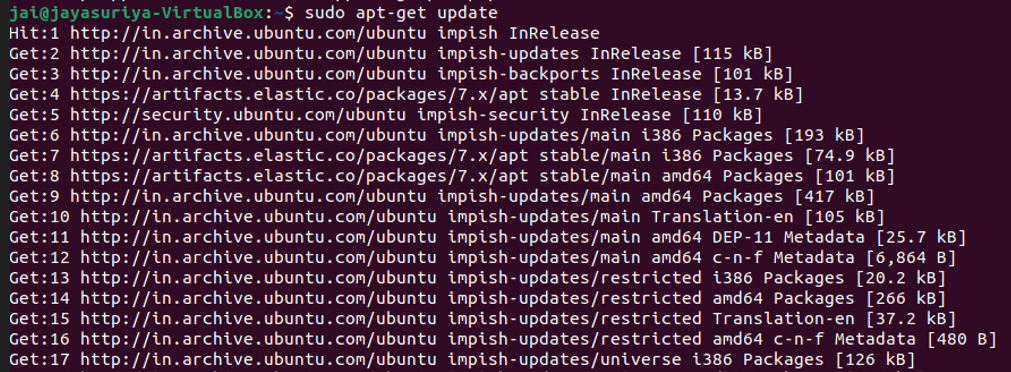
Sudo echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee –a /etc/apt/sources.list.d/elastic-7.x.list



## **Install Elasticsearch**

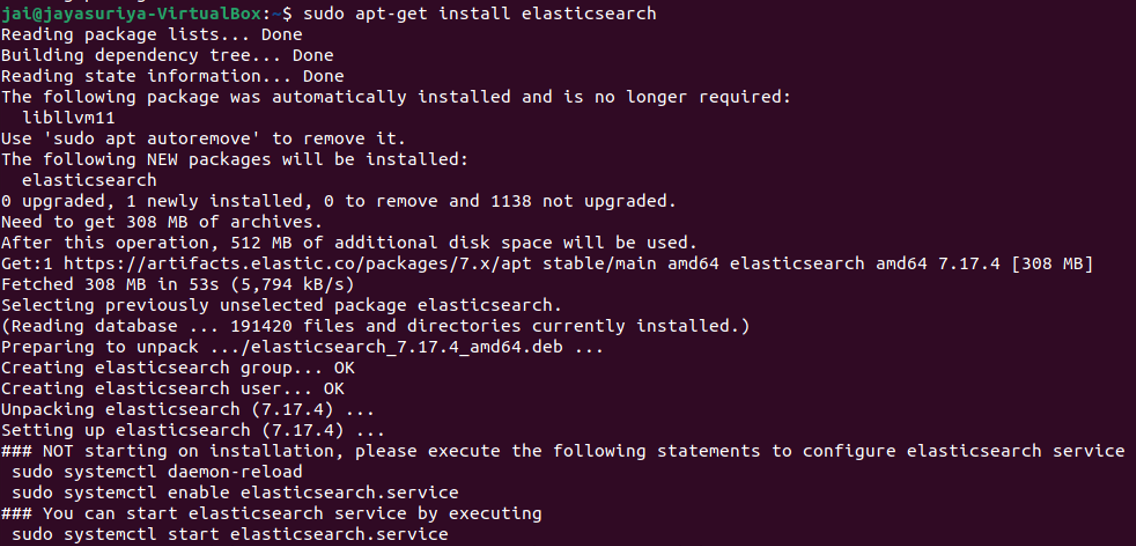
Prior to installing Elasticsearch, update the repositories by entering:

sudo apt-get update



Install Elasticsearch with the following command:

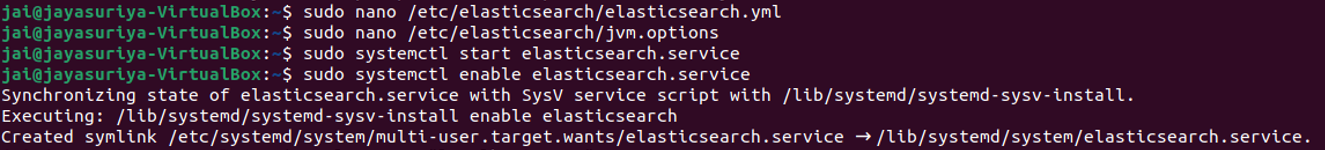
sudo apt-get install elasticsearch



### **Configure Elasticsearch**

Elasticsearch uses a configuration file to control how it behaves. Open the configuration file for [editing in a text editor](https://phoenixnap.com/kb/best-linux-text-editors-for-coding) of your choice. We will be using nano:

sudo nano /etc/elasticsearch/elasticsearch.yml



You should see a configuration file with several different entries and descriptions. Scroll down to find the following entries:

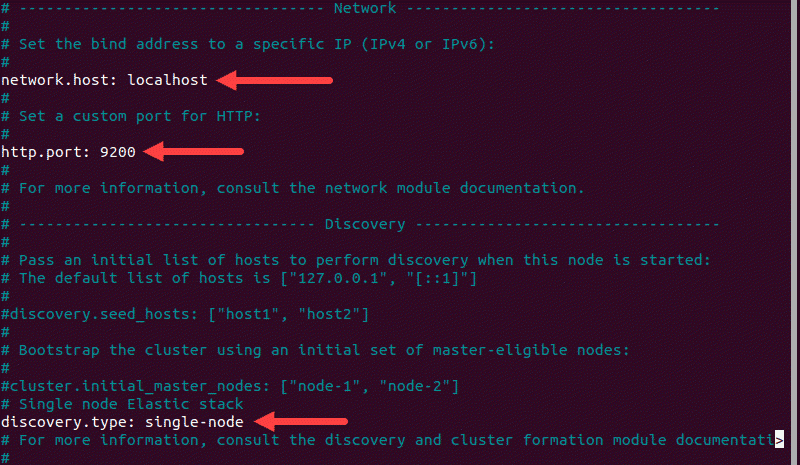
#network.host: 192.168.0.1

#http.port: 9200

Uncomment the lines by deleting the hash (#) sign at the beginning of both lines and replace 192.168.0.1 with localhost.

Just below, find the *Discovery* section. We are adding one more line, as we are configuring a single node cluster:

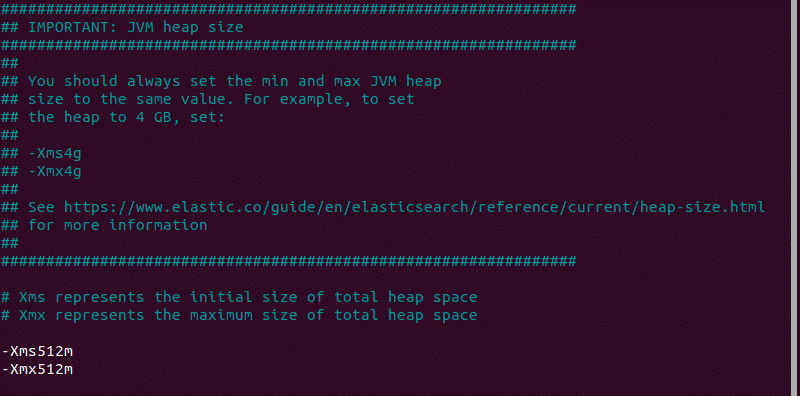
discovery.type: single-node



By default, JVM heap size is set at 1GB. We recommend setting it to no more than half the size of your total memory. Open the following file for editing:

sudo nano /etc/elasticsearch/jvm.options

Find the lines starting with -Xms and -Xmx. In the example below, the maximum (-Xmx) and minimum (-Xms) size is set to 512MB.

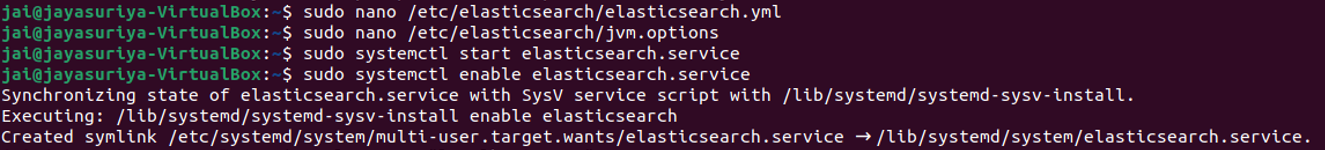


Start the Elasticsearch service by running a systemctl command:

sudo systemctl start elasticsearch.service

Enable Elasticsearch to start on boot:

sudo systemctl enable elasticsearch.service

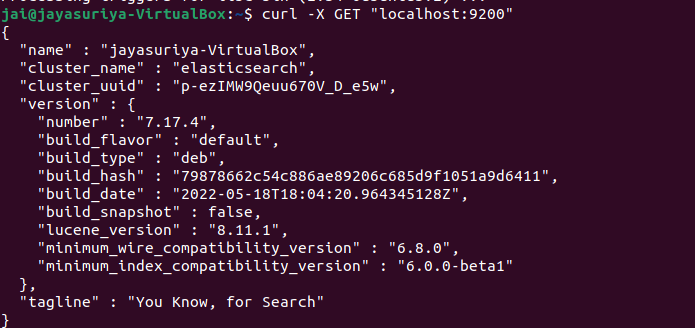


### **Test Elasticsearch**

Use the curl command to test your configuration. Enter the following:

curl -X GET "localhost:9200"

The name of your system should display, and elasticsearch for the cluster name. This indicates that Elasticsearch is functional and is listening on port 9200.\

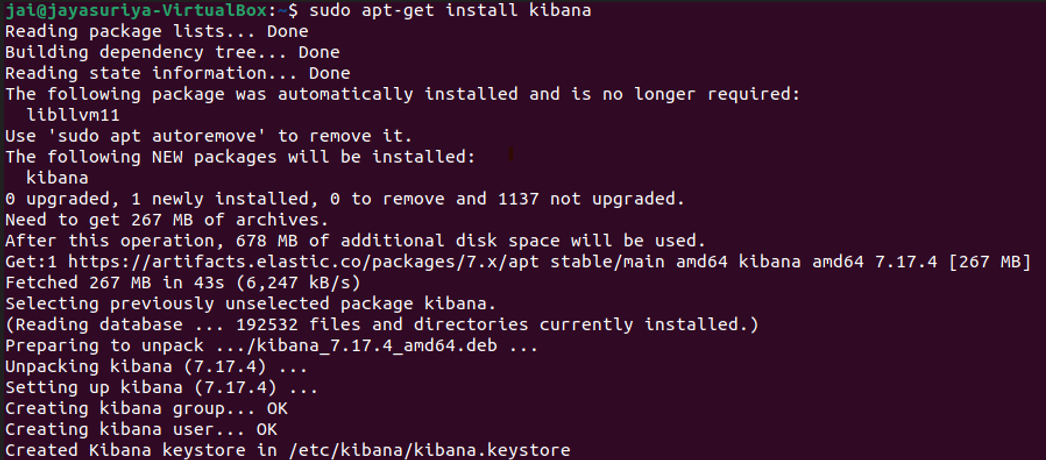


## **Install Kibana**

It is recommended to install Kibana next. Kibana is a graphical user interface for parsing and interpreting collected log files.

Run the following command to install Kibana:

sudo apt-get install kibana



Allow the process to finish. Once finished, it’s time to configure Kibana.

### **Configure Kibana**

open the kibana.yml configuration file for editing:

sudo nano /etc/kibana/kibana.yml

Delete the # sign at the beginning of the following lines to activate them:

#server.port: 5601

#server.host: "your-hostname"

#elasticsearch.hosts: ["<http://localhost:9200>"]

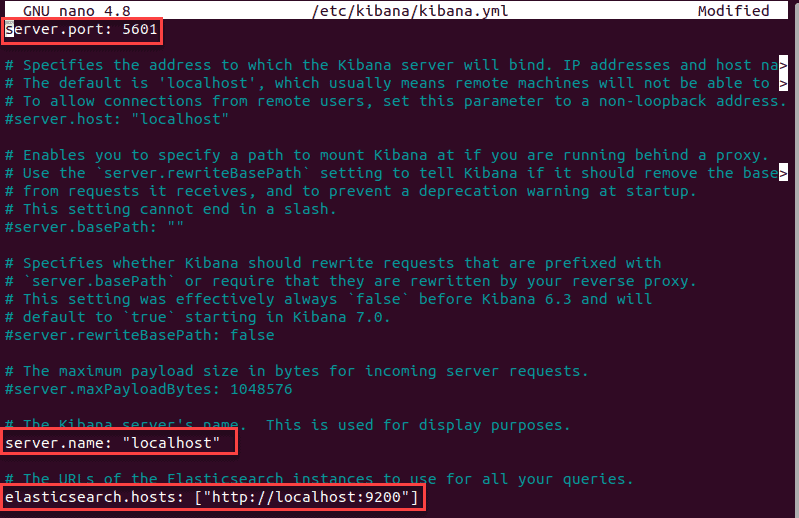
The above-mentioned lines should look as follows:

server.port: 5601

server.host: "localhost"

elasticsearch.hosts: ["http://localhost:9200"]

Save the file and exit



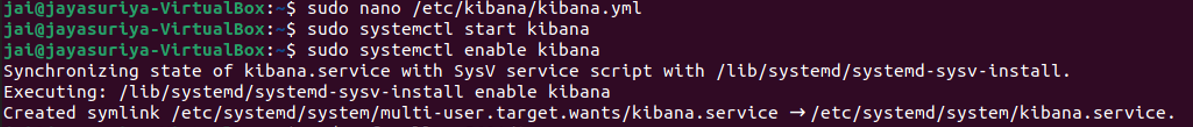
Start and Enable Kibana

Start the Kibana service:

sudo systemctl start kibana

configure Kibana to launch at boot:

sudo systemctl enable kibana

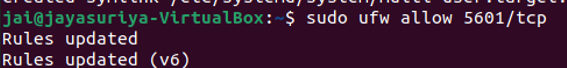


### **Allow Traffic on Port 5601**

If the [UFW firewall](https://phoenixnap.com/kb/configure-firewall-with-ufw-on-ubuntu) is enabled on your Ubuntu system, you need to allow traffic on port 5601 to access the Kibana dashboard.

In a terminal window, run the following command:

sudo ufw allow 5601/tcp



### **Test Kibana**

To access Kibana, open a web browser and browse to the following address:

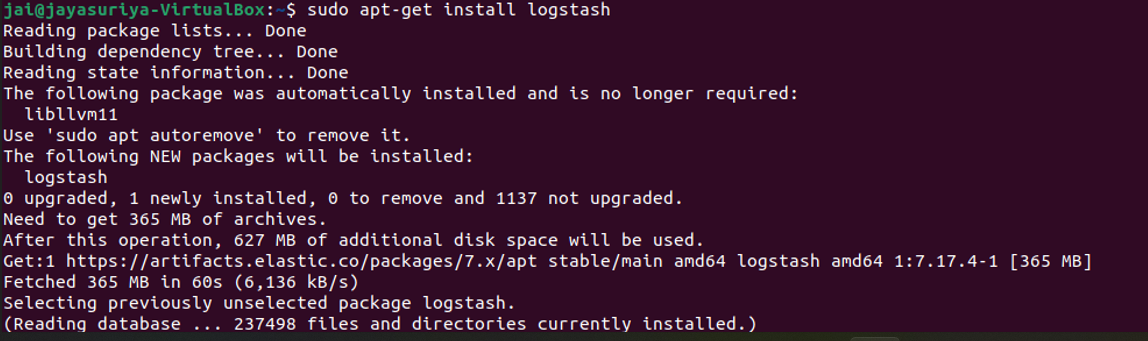
http://localhost:5601

## **Install Logstash**

Logstash is a tool that collects data from different sources. The data it collects is parsed by Kibana and stored in Elasticsearch.

Install Logstash by running the following command:

sudo apt-get install logstash



### **Start and Enable Logstash**

Start the Logstash service:

sudo systemctl start logstash

Enable the Logstash service:

sudo systemctl enable logstash

To check the status of the service, run the following command:

sudo systemctl status logstash

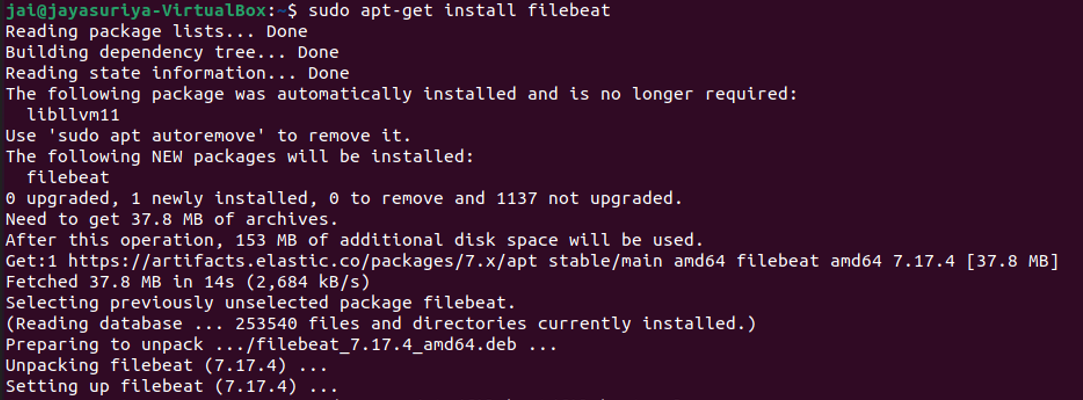


## **Install Filebeat**

Filebeat is a lightweight plugin used to collect and ship log files. It is the most commonly used Beats module. One of Filebeat’s major advantages is that it slows down its pace if the Logstash service is overwhelmed with data.

Install Filebeat by running the following command:

sudo apt-get install filebeat



### **Configure Filebeat**

Filebeat, by default, sends data to Elasticsearch. Filebeat can also be configured to send event data to Logstash.

To configure this, edit the filebeat.yml configuration file:

sudo nano /etc/filebeat/filebeat.yml

Under the *Elasticsearch* o*utput* section, comment out the following lines:

# output.elasticsearch:

# Array of hosts to connect to.

# hosts: ["localhost:9200"]

Under the *Logstash output* section, remove the hash sign (#) in the following two lines:

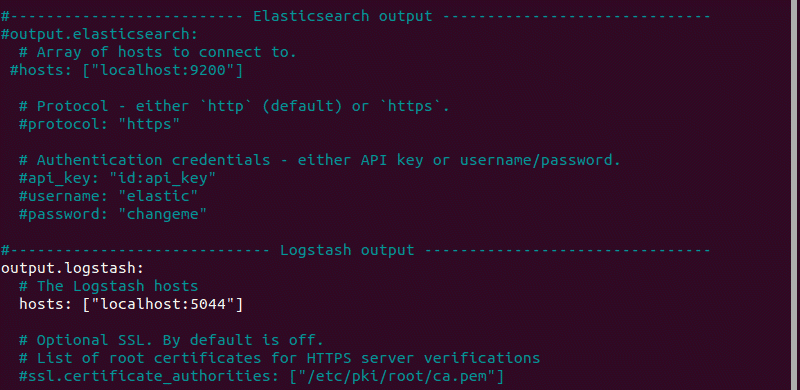
# output.logstash

# hosts: ["localhost:5044"]

It should look like this:

output.logstash

hosts: ["localhost:5044"]



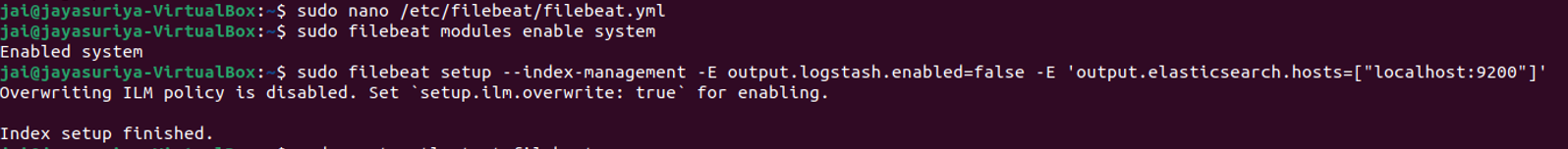
enable the Filebeat system module, which will examine local system logs:

sudo filebeat modules enable system

The output should read Enabled system.

load the index template:

sudo filebeat setup --index-management -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["localhost:9200"]'

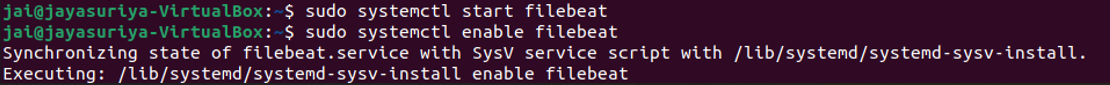


### **Start and Enable Filebeat**

Start and enable the Filebeat service:

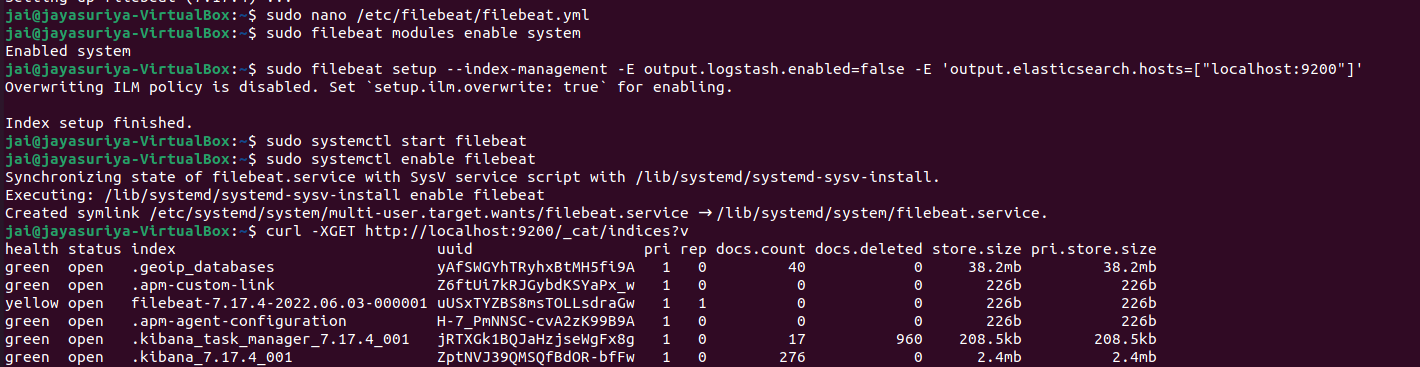
sudo systemctl start filebeat

sudo systemctl enable filebeat

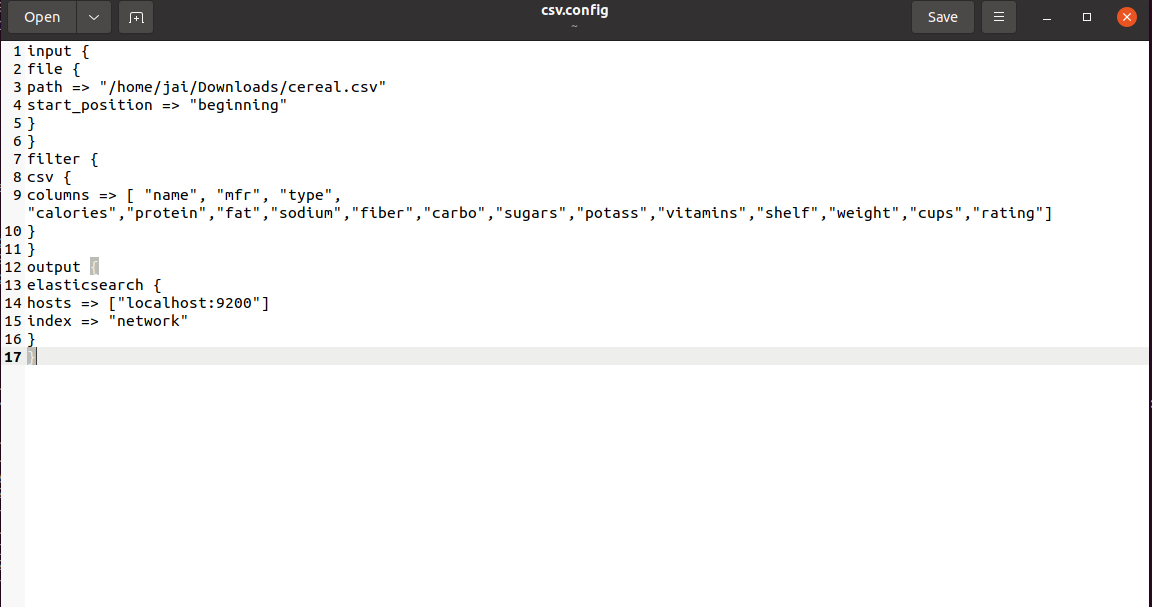


verify if Filebeat is shipping log files to Logstash for processing. Once processed, data is sent to Elasticsearch.

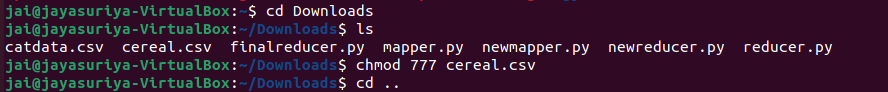
curl -XGET <http://localhost:9200/_cat/indices?v>



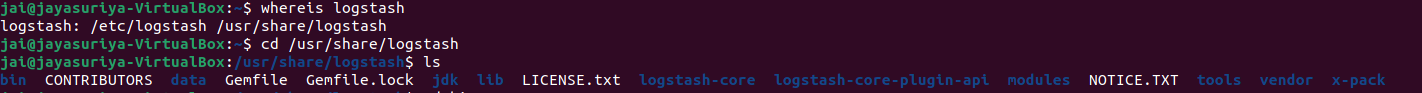
**Running files in logstash:**

First create a config file and save .I have created csv.config file   


Use chmod 777 filename to enable read write access



Find logstash location using whereis logstash and open that folder

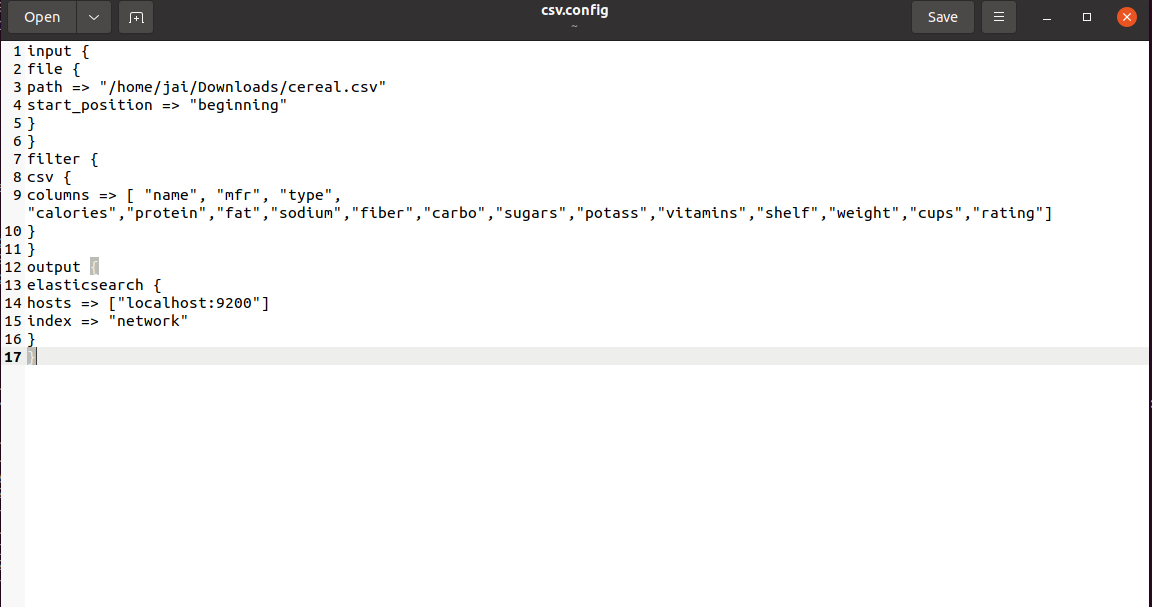


Create a configuration file in /etc/logstash/conf.d

To run configuration files you have to store them in conf.d folder

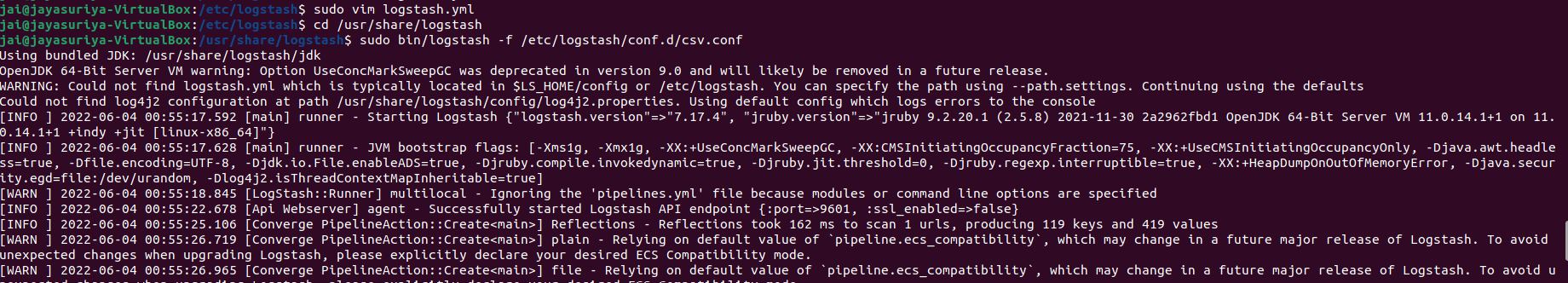


Config file



After creation and storing config file move back to logstash folder /usr/share/logstash

Run the command

sudo bin/logstash -f /etc/logstash/conf.d/csv.config

to send csv to elasticsearch through logstash

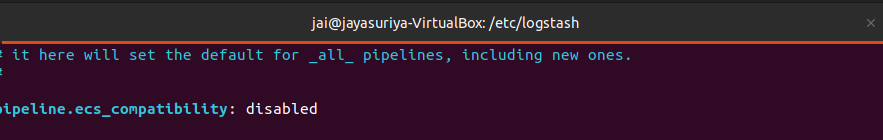
If you get pipeline.ecs\_compatibility warning then

Open path /etc/logstash/

Open logstash.yaml file using

Sudo nano logstash.yml

uncomment the following line



Run the command

sudo bin/logstash -f /etc/logstash/conf.d/csv.config

While this is running open new terminal and run the following

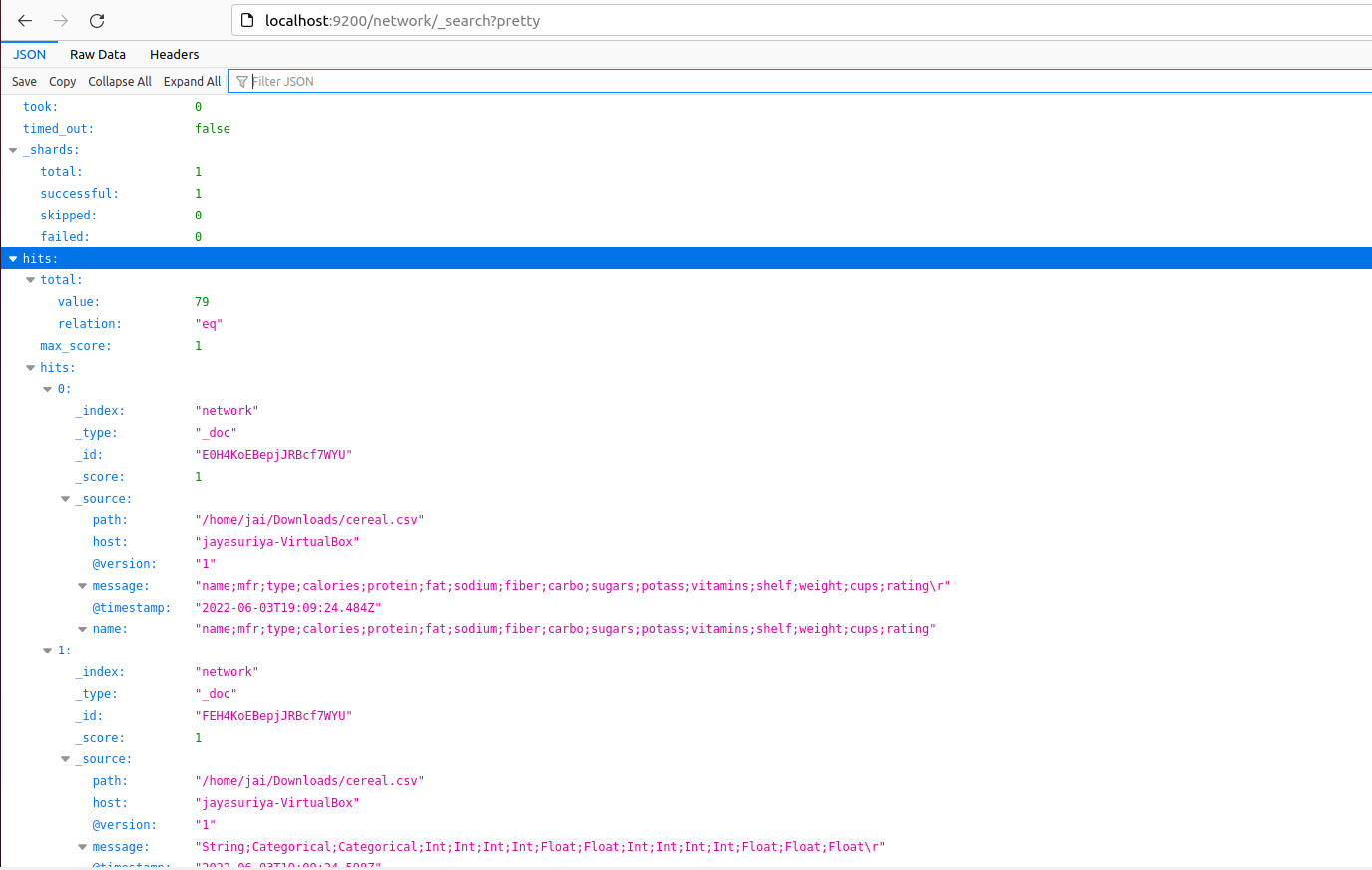
Curl -XGET <http://localhost:9200/_cat/indices?v>

Curl -XGET <http://localhost:9200/network/_search?pretty>

Or using browser try

<http://localhost:9200/_cat/indices?v>

<http://localhost:9200/network/_search?pretty>



**Visualization Using Kibana:**

Network is the created index.

