

Commands for ELK stack installation

Install Java

```
sudo apt-get install openjdk-8-jdk
```

Install Nginx

Nginx works as a web server and proxy server.

1. Install Nginx by entering the following:

sudo apt-get install nginx
check your localhost type in URL

Step 2: Add Elastic Repository

1. 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 -
```
2. Next, install the apt-transport-https package:

```
sudo apt-get install apt-transport-https
```
3. Add the Elastic repository to your system's repository list:

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

Step 3: Install Elasticsearch

```
sudo apt-get update
```

2. Install Elasticsearch with the following command:

```
sudo apt-get install elasticsearch
```

Configure Elasticsearch

```
sudo nano /etc/elasticsearch/elasticsearch.yml
```

```
#network.host: 192.168.0.1
```

```
#http.port: 9200
```

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

```
discovery.type: single-node
```
5. 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
```

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

```
-Xms512m  
-Xmx512m
```

It may take some time for the system to start the service.
There will be no output if successful.

2. Enable Elasticsearch to start on boot:

```
sudo systemctl enable elasticsearch.service  
Test Elasticsearch
```

Step 3: Install Kibana

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

1. Run the following command to install Kibana:

```
sudo apt-get install kibana
```
2. Allow the process to finish. Once finished, it's time to configure Kibana.

Configure Kibana

1. Next, open the kibana.yml configuration file for editing:

```
sudo nano /etc/kibana/kibana.yml
```
2. 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"]
```

```
=====
```

Start and Enable Kibana

1. Start the Kibana service:

```
sudo systemctl start kibana
```

There is no output if the service starts successfully.

2. Next, configure Kibana to launch at boot:

```
sudo systemctl enable kibana
```

Allow Traffic on Port 5601

If the UFW firewall 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>

=====

=====

STEP 4: 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

1. Start the Logstash service:

```
sudo systemctl start logstash
```

2. Enable the Logstash service:

```
sudo systemctl enable logstash
```

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

```
sudo systemctl status logstash
```

Configure Logstash

Logstash is a highly customizable part of the ELK stack.

Once installed, configure its INPUT, FILTERS, and OUTPUT pipelines according to your own individual use case.