Setting Up ELK Stack on Ubuntu Server

# 1. Introduction

The ELK Stack, composed of Elasticsearch, Logstash, and Kibana, is a powerful open-source tool for managing and analyzing log data. This guide will walk you through the steps to install and configure the ELK Stack on an Ubuntu server.

## 2. Prerequisites

A running instance of Ubuntu Server (20.04 or later).

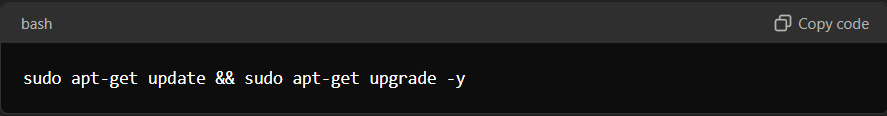
At least 4GB of RAM.

Sudo or root privileges.

# 3. Steps

## Step 1: Update the System

Before installing any packages, update your system to ensure you have the latest software versions.



sudo apt-get update && sudo apt-get upgrade -y

## Step 2: Install Java

Elasticsearch requires Java to run. Install OpenJDK 11:



sudo apt-get install openjdk-11-jdk -y

Verify the installation by running java -version

## Step 3: Install and Configure Elasticsearch

### Install Elasticsearch

Download and install the Elasticsearch package:

A screen shot of a computer

Description automatically generated

wget <https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-7.11.0-amd64.deb>

sudo dpkg -i elasticsearch-7.11.0-amd64.deb

### Start and enable Elasticsearch to start on boot:

A black and white screen

Description automatically generated with medium confidence

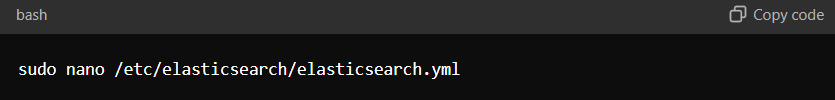
sudo systemctl start elasticsearch

sudo systemctl enable elasticsearch

Verify Elasticsearch is running by running curl -X GET "localhost:9200/"

### Configure Elasticsearch

Open the Elasticsearch configuration file:



sudo nano /etc/elasticsearch/elasticsearch.yml

Modify the settings network.host: localhost under the Network section

**Use the relevant ip address of the server in place of localhost**

Save and close the file, then restart Elasticsearch using sudo systemctl restart elasticsearch

## Step 4: Install and Configure Kibana

### Install Kibana

Download and install the Kibana package:

A screen shot of a computer

Description automatically generated

wget https://artifacts.elastic.co/downloads/kibana/kibana-7.11.0-amd64.deb

sudo dpkg -i kibana-7.11.0-amd64.deb

### Start and enable Kibana

A black and grey rectangular object

Description automatically generated

sudo systemctl start kibana

sudo systemctl enable kibana

### Configure Kibana

Open the Kibana configuration file:

A black and grey rectangular object

Description automatically generated

sudo nano /etc/kibana/kibana.yml

Modify the settings server.host: "localhost" and server.port: "5601"

**Use the relevant ip address of the server in place of localhost**

Save and close the file, then restart Kibana using sudo systemctl restart kibana

## Step 5: Access Kibana

Open a web browser and navigate to <http://localhost:5601>.

**Use the relevant ip address of the server in place of localhost**

You should see the Kibana web interface where you can start setting up visualizations and dashboards.

# 4. Troubleshooting

Elasticsearch Not Running: Check the Elasticsearch logs at /var/log/elasticsearch/ for any errors.

Kibana Not Loading: Verify that Kibana is running and that you can access it from the correct IP address.

# 5. Conclusion

By following these steps, you've successfully installed and configured the ELK Stack on an Ubuntu server. You can now use Elasticsearch for searching and indexing and Kibana for visualization.