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).

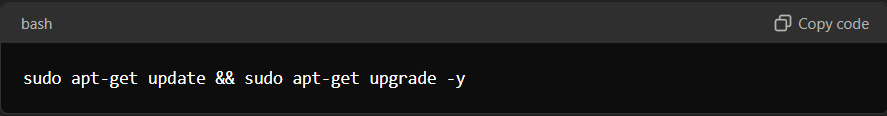
At least 4GB of RAM (8GB recommended).

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:

sudo systemctl start elasticsearch

sudo systemctl enable elasticsearch

Verify Elasticsearch is running:

bash

Copy code

curl -X GET "localhost:9200/"

5.2 Configure Elasticsearch

Open the Elasticsearch configuration file:

bash

Copy code

sudo nano /etc/elasticsearch/elasticsearch.yml

Modify the following settings:

yaml

Copy code

network.host: localhost

Save and close the file, then restart Elasticsearch:

bash

Copy code

sudo systemctl restart elasticsearch

6. Step 4: Install and Configure Logstash

6.1 Install Logstash

Download and install the Logstash package:

bash

Copy code

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

sudo dpkg -i logstash-7.11.0-amd64.deb

Start and enable Logstash:

bash

Copy code

sudo systemctl start logstash

sudo systemctl enable logstash

6.2 Configure Logstash

Create a simple Logstash configuration file:

bash

Copy code

sudo nano /etc/logstash/conf.d/logstash.conf

Add the following basic configuration:

yaml

Copy code

input {

beats {

port => 5044

}

}

output {

elasticsearch {

hosts => ["localhost:9200"]

index => "logstash-%{+YYYY.MM.dd}"

}

}

Save and close the file, then test the configuration:

bash

Copy code

sudo /usr/share/logstash/bin/logstash --path.settings /etc/logstash -t

Restart Logstash:

bash

Copy code

sudo systemctl restart logstash

7. Step 5: Install and Configure Kibana

7.1 Install Kibana

Download and install the Kibana package:

bash

Copy code

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:

bash

Copy code

sudo systemctl start kibana

sudo systemctl enable kibana

7.2 Configure Kibana

Open the Kibana configuration file:

bash

Copy code

sudo nano /etc/kibana/kibana.yml

Modify the following settings:

yaml

Copy code

server.host: "localhost"

Save and close the file, then restart Kibana:

bash

Copy code

sudo systemctl restart kibana

8. Step 6: Access Kibana

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

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

9. Step 7: Configure Filebeat for Log Forwarding

Download and install Filebeat:

bash

Copy code

wget https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-oss-7.11.0-amd64.deb

sudo dpkg -i filebeat-oss-7.11.0-amd64.deb

Configure Filebeat to forward logs to Logstash:

bash

Copy code

sudo nano /etc/filebeat/filebeat.yml

Uncomment and configure the Logstash output section:

yaml

Copy code

output.logstash:

hosts: ["localhost:5044"]

Enable and start Filebeat:

bash

Copy code

sudo systemctl enable filebeat

sudo systemctl start filebeat

10. Step 8: Verify the ELK Stack Setup

In Kibana, navigate to the "Discover" tab to verify that logs are being ingested from Filebeat.

Create visualizations and dashboards in Kibana to display your log data.

11. Troubleshooting

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

Logstash Not Receiving Data: Ensure that the Logstash configuration is correct and that the ports are open.

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

12. 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, Logstash for data ingestion, and Kibana for visualization.