Configuring X-Pack Security for ELK Stack on Ubuntu

Contents

[1. Introduction 2](#_Toc174537550)

[2. Prerequisites 2](#_Toc174537551)

[3. Steps 2](#_Toc174537552)

[Step 1: Stop Elasticsearch and Kibana 2](#_Toc174537553)

[Step 2: Configure Elasticsearch for X-Pack 2](#_Toc174537554)

[Open the Elasticsearch configuration file: 2](#_Toc174537555)

[Start Elasticsearch: 3](#_Toc174537556)

[Check the status of Elasticsearch to ensure it's running: 3](#_Toc174537557)

[Step 3: Generate X-Pack Usernames and Passwords 3](#_Toc174537558)

[Navigate to the Elasticsearch directory: 3](#_Toc174537559)

[For auto-generation: 3](#_Toc174537560)

[For interactive mode: 4](#_Toc174537561)

[Step 4: Configure Kibana for X-Pack 4](#_Toc174537562)

[Navigate to the Kibana configuration directory: 4](#_Toc174537563)

[Open the Kibana configuration file: 4](#_Toc174537564)

[Start Kibana: 5](#_Toc174537565)

[Check the status of Kibana to ensure it's running: 5](#_Toc174537566)

[Step 5: Access Kibana with X-Pack Security 5](#_Toc174537567)

[8. Conclusion 5](#_Toc174537568)

# 1. Introduction

X-Pack is a powerful extension for the ELK Stack that provides security features, including authentication, authorization, and encryption. This guide will walk you through configuring X-Pack on an Ubuntu server running Elasticsearch, Logstash, and Kibana.

# 2. Prerequisites

A running instance of the ELK Stack (Elasticsearch, Logstash, Kibana) on Ubuntu.

Sudo or root privileges.

# 3. Steps

## Step 1: Stop Elasticsearch and Kibana

Before configuring X-Pack, stop the Elasticsearch and Kibana services.



sudo systemctl stop elasticsearch

sudo systemctl stop kibana

## Step 2: Configure Elasticsearch for X-Pack

### Open the Elasticsearch configuration file:

A black and white text on a black background

Description automatically generated

sudo nano /etc/elasticsearch/elasticsearch.yml

Add the following line to enable X-Pack security, xpack.security.enabled: true under security section.

Save the file and exit the editor (Ctrl + X, then Y, then Enter).

### Start Elasticsearch:

A black rectangular object with a black stripe

Description automatically generated

sudo systemctl start elasticsearch

### Check the status of Elasticsearch to ensure it's running:

A black and grey rectangular object

Description automatically generated

sudo systemctl status elasticsearch

## Step 3: Generate X-Pack Usernames and Passwords

### Navigate to the Elasticsearch directory:

A black and grey rectangular object

Description automatically generated

cd /usr/share/elasticsearch/bin

Run the elasticsearch-setup-passwords script to generate usernames and passwords. You can choose between auto (for automatically generated passwords) or interactive (to set your own passwords):

### For auto-generation:

A black and white text

Description automatically generated

sudo ./elasticsearch-setup-passwords auto

### For interactive mode:

A black and white screen with white text

Description automatically generated

sudo ./elasticsearch-setup-passwords interactive

Save the generated usernames and passwords securely, as you'll need them to configure Kibana and Logstash.

## Step 4: Configure Kibana for X-Pack

### Navigate to the Kibana configuration directory:

A black and grey rectangular object

Description automatically generated

cd /etc/kibana

### Open the Kibana configuration file:

A black and grey rectangular object

Description automatically generated

sudo nano kibana.yml

Locate the lines for elasticsearch.username and elasticsearch.password, and update them with the credentials for the kibana\_system user

A screen shot of a computer

Description automatically generated

elasticsearch.username: "kibana\_system"

elasticsearch.password: "<your-kibana-system-password>"

Save the file and exit the editor.

### Start Kibana:

A black and grey rectangular object

Description automatically generated

sudo systemctl start kibana

### Check the status of Kibana to ensure it's running:

A black and grey rectangular object

Description automatically generated

sudo systemctl status kibana

## Step 5: Access Kibana with X-Pack Security

Open a web browser and navigate to http://<your-server-ip>:5601 (**replace <your-server-ip> with your actual IP address**).

You should now see a login prompt. Use the elastic username and the corresponding password generated in Step 3.

# 8. Conclusion

By following these steps, you've successfully configured X-Pack security for your ELK Stack on Ubuntu. With X-Pack, you can now secure your Elasticsearch data with authentication and authorization, ensuring that only authorized users can access your logs and analytics.