ELK SETUP

Install Elasticsearch Ubuntu 24

## **#Import the Elasticsearch PGP Key**

Download and install the public signing key:

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg

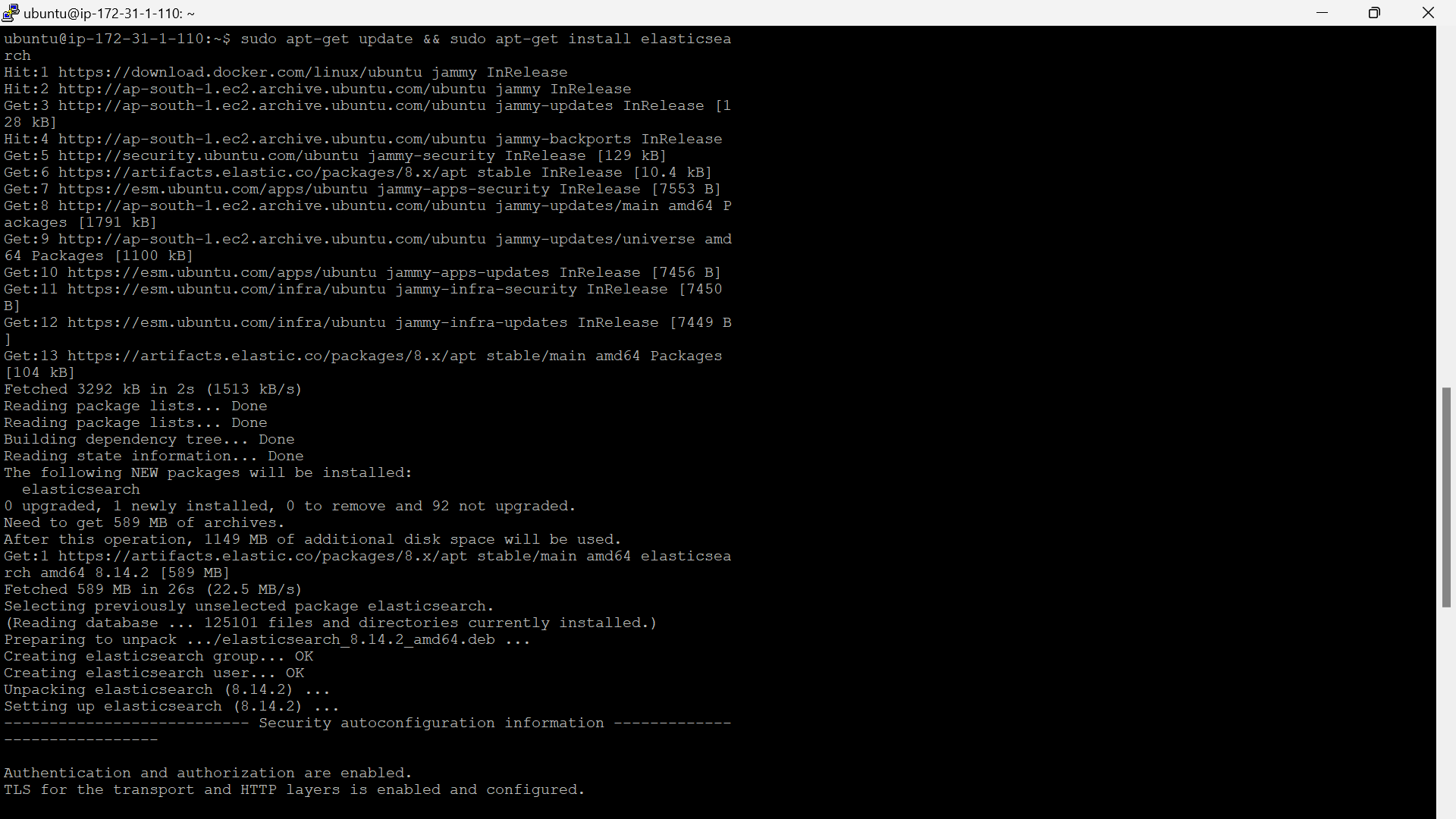
## **#Installing from the APT repository**

sudo apt-get install apt-transport-https

echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list

You can install the Elasticsearch Debian package with:

sudo apt-get update && sudo apt-get install elasticsearch



\*Make sure you save the Security autoconfiguration information

--------------------------- Security autoconfiguration information ------------- -----------------

Authentication and authorization are enabled.

TLS for the transport and HTTP layers is enabled and configured.

The generated password for the elastic built-in superuser is : WGZNC\_Z9uZl\_=4i54 ziJ

If this node should join an existing cluster, you can reconfigure this with

'/usr/share/elasticsearch/bin/elasticsearch-reconfigure-node --enrollment-token <token-here>'

after creating an enrollment token on your existing cluster.

You can complete the following actions at any time:

Reset the password of the elastic built-in superuser with

'/usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic'.

Generate an enrollment token for Kibana instances with

'/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana'.

Generate an enrollment token for Elasticsearch nodes with

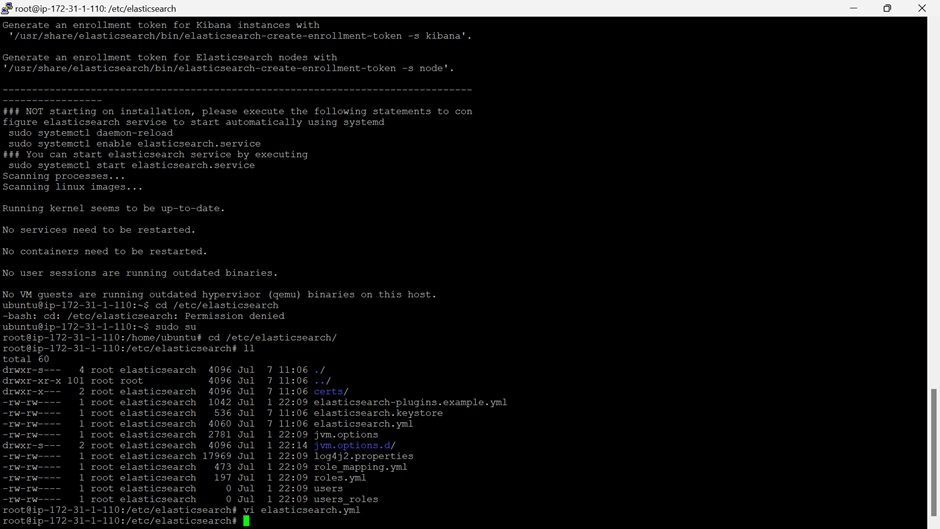
'/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s node'.

-------------------------------------------------------------------------------- -----------------

## **#Configuring the Elasticsearch**

Navigate to Elasticsearch configuration directory:  
cd /etc/elasticsearch

vi elasticsearch.yml



Update the elasticsearch.yml with following network host and port configurations:

network.host: 0.0.0.0

http.port: 9200

# Enable security features

xpack.security.enabled: true

xpack.security.enrollment.enabled: true

# Enable encryption for HTTP API client connections, such as Kibana, Logstash, and Agents

xpack.security.http.ssl:

enabled: true

keystore.path: certs/http.p12

# Enable encryption and mutual authentication between cluster nodes

xpack.security.transport.ssl:

enabled: true

verification\_mode: certificate

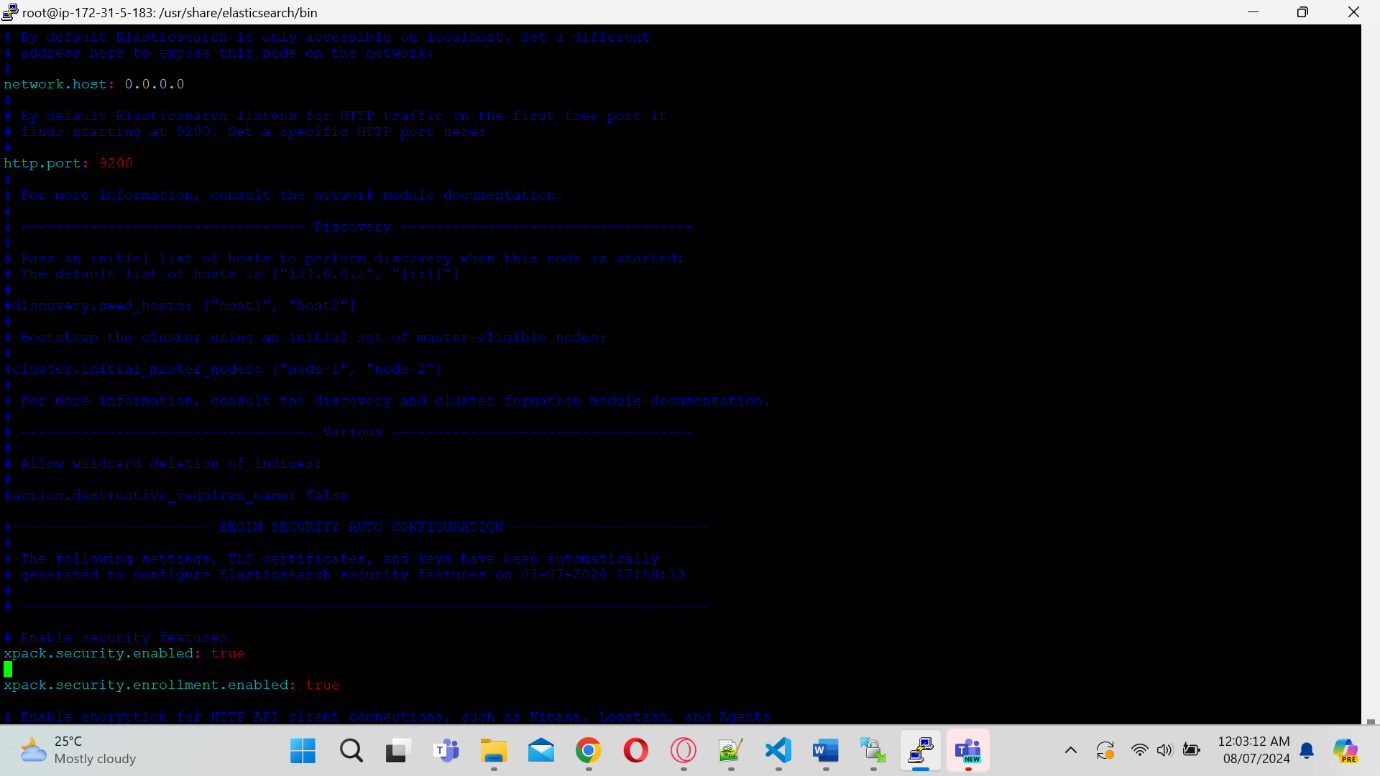
keystore.path: certs/transport.p12

truststore.path: certs/transport.p12

# Allow HTTP API connections from anywhere

# Connections are encrypted and require user authentication

http.host: 0.0.0.0



## **#Running Elasticsearch**

Elasticsearch can be started and stopped as follows:

sudo systemctl start elasticsearch.service

sudo systemctl stop elasticsearch.service

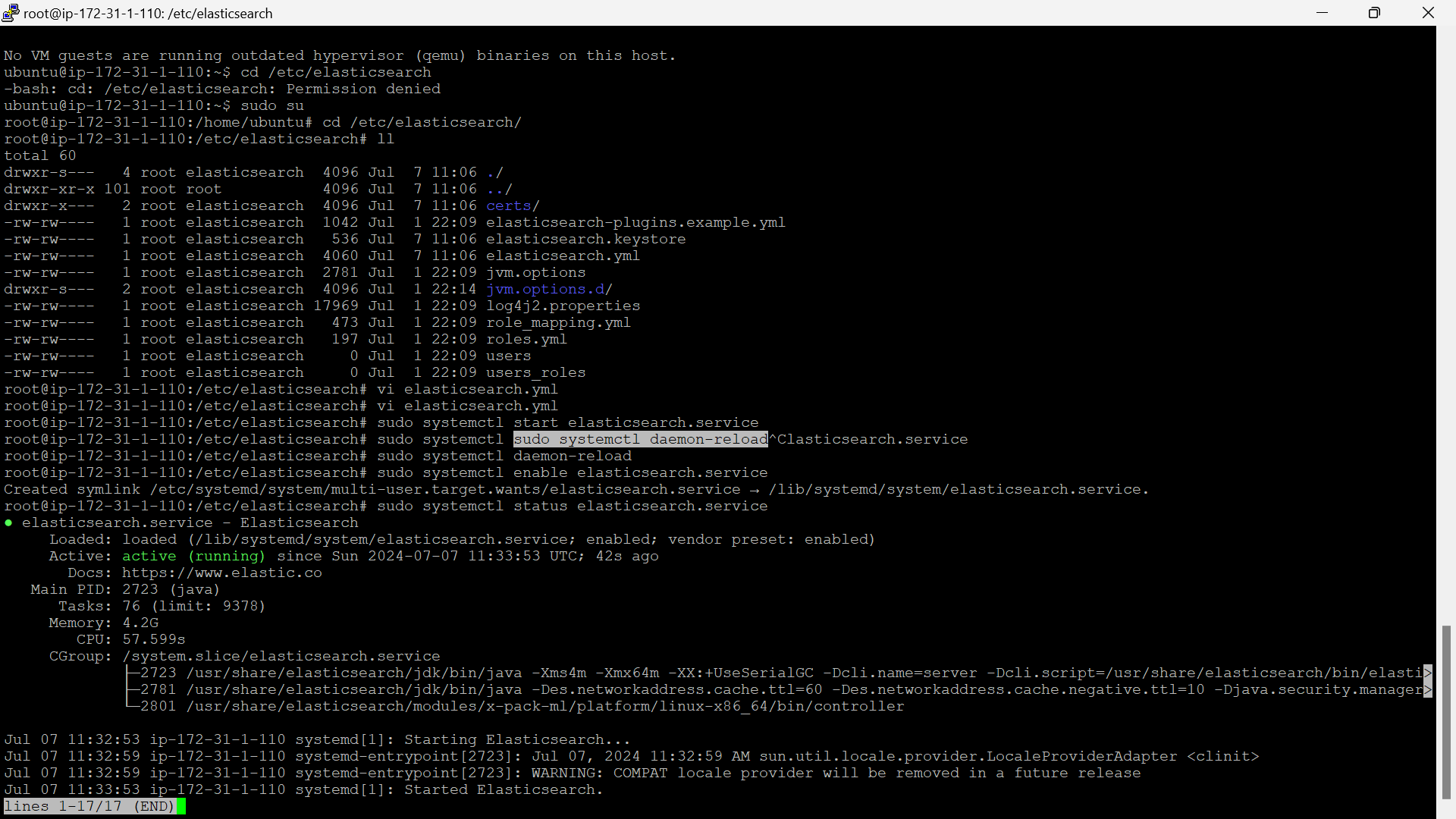
To configure Elasticsearch to start automatically when the system boots up, run the following commands:

sudo systemctl daemon-reload

sudo systemctl enable elasticsearch.service

To check status:

sudo systemctl status elasticsearch.service



Try to access the Elasticsearch URL (i.e http://<server-ip:9200>) from your browser and check the health of the Elasticsearch. An example screenshot is given below for your reference.

# Install Kibana

## **#Import the Elastic PGP key**

Download and install the public signing key:

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg

## **#Install from the APT repository**

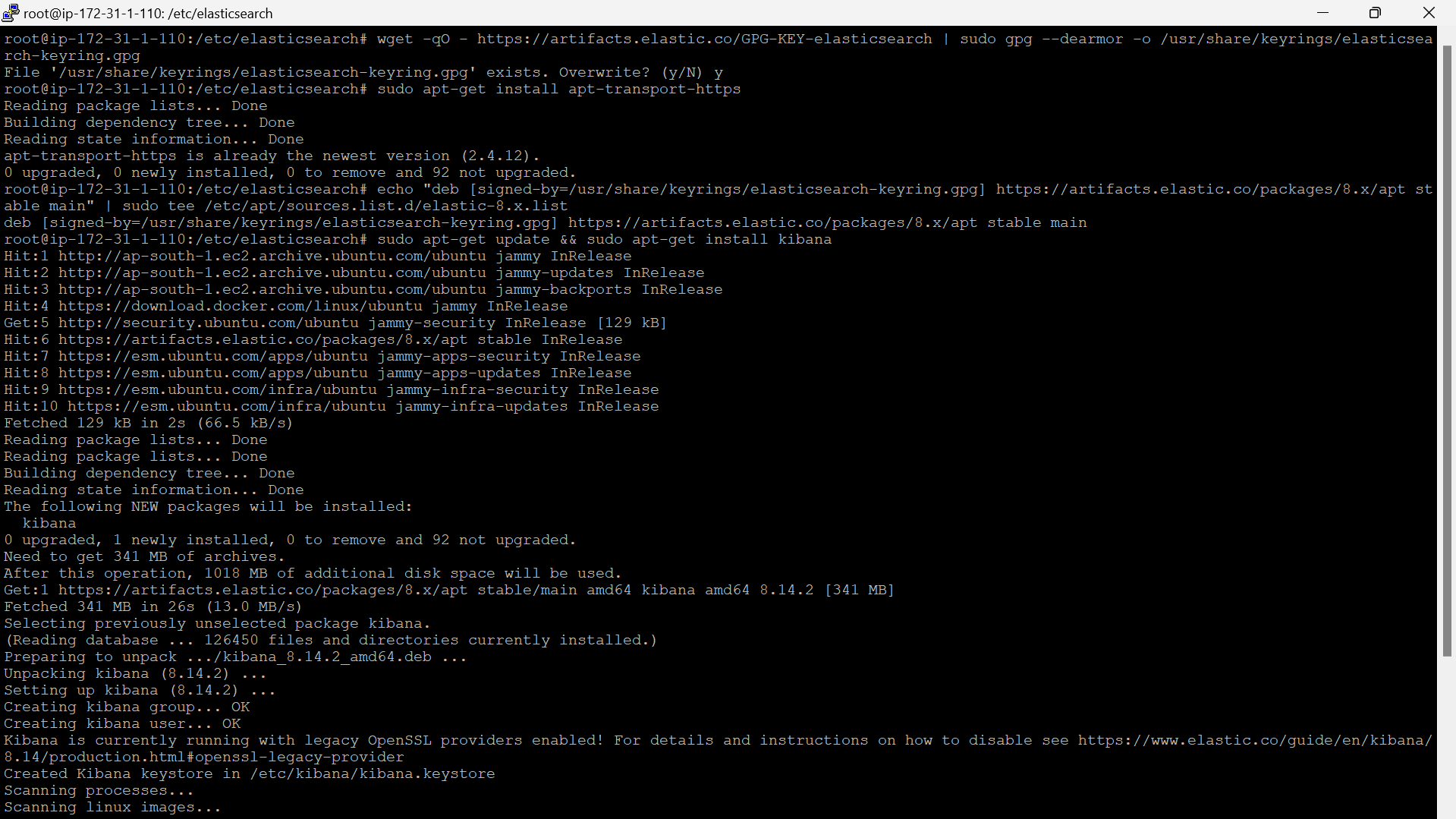
You can install the Kibana Debian package with:

sudo apt-get install apt-transport-https

echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list

You can install the Kibana Debian package with:

sudo apt-get update && sudo apt-get install kibana



## **#Now to integrate Kibana to ElasticSearch You need Tokens**

You can then generate an Service Token:

cd /usr/share/elasticsearch/bin/

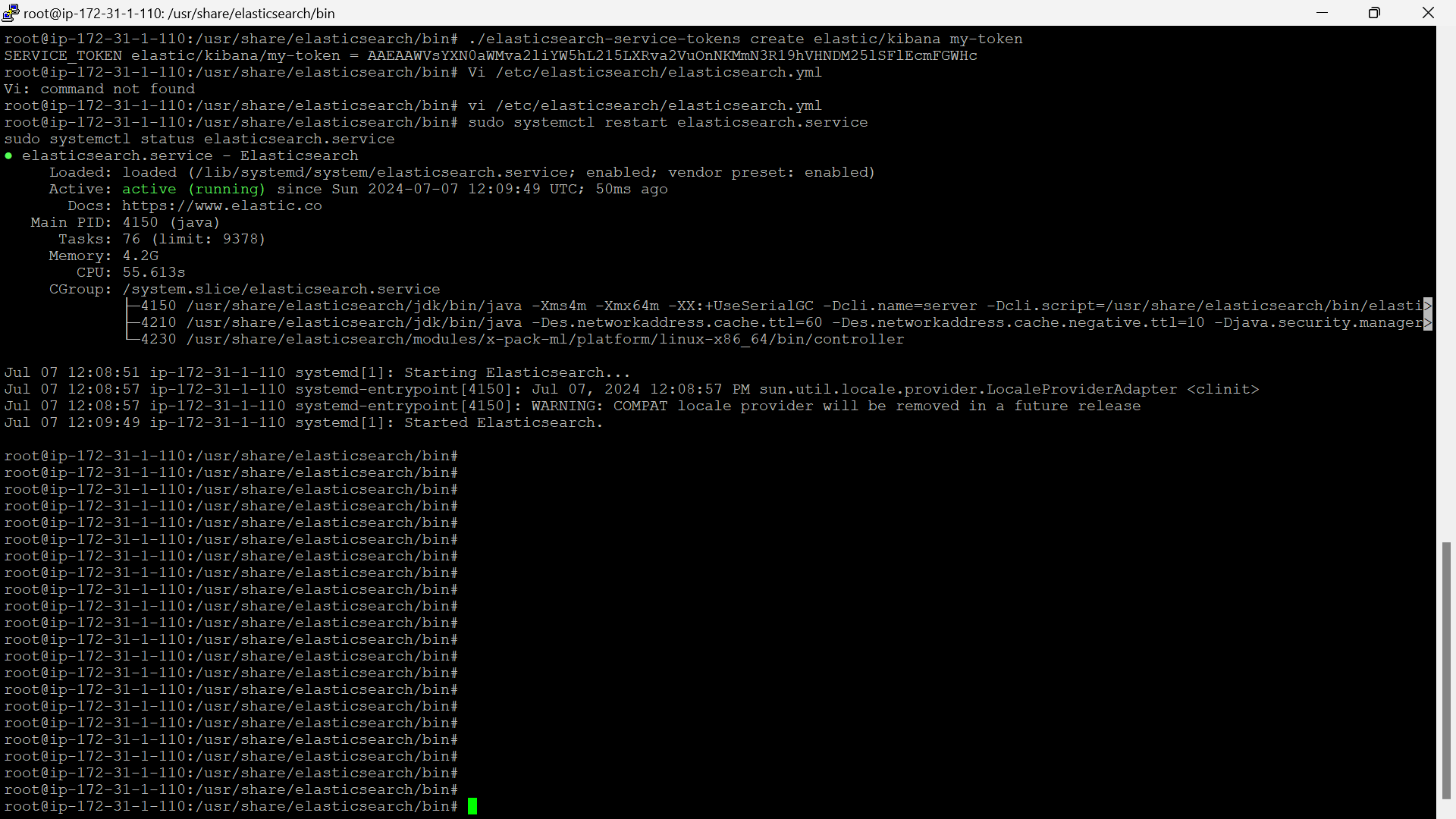
./elasticsearch-service-tokens create elastic/kibana my-token

SERVICE\_TOKEN elastic/kibana/my-token = AAEAAWVsYXN0aWMva2liYW5hL215LXRva2VuOmIyUEI0bkdKUm82SFBMbHZ6NmlScGc

You can then generate an enrollment token for Kibana with the elasticsearch-create-enrollment-token tool:

./elasticsearch-create-enrollment-token --scope kibana

elasticsearch-create-enrollment-token=



### **#Configuring the Kibana**

Navigate to Kibana configuration directory:

cd /etc/kibana

vi kibana.yml

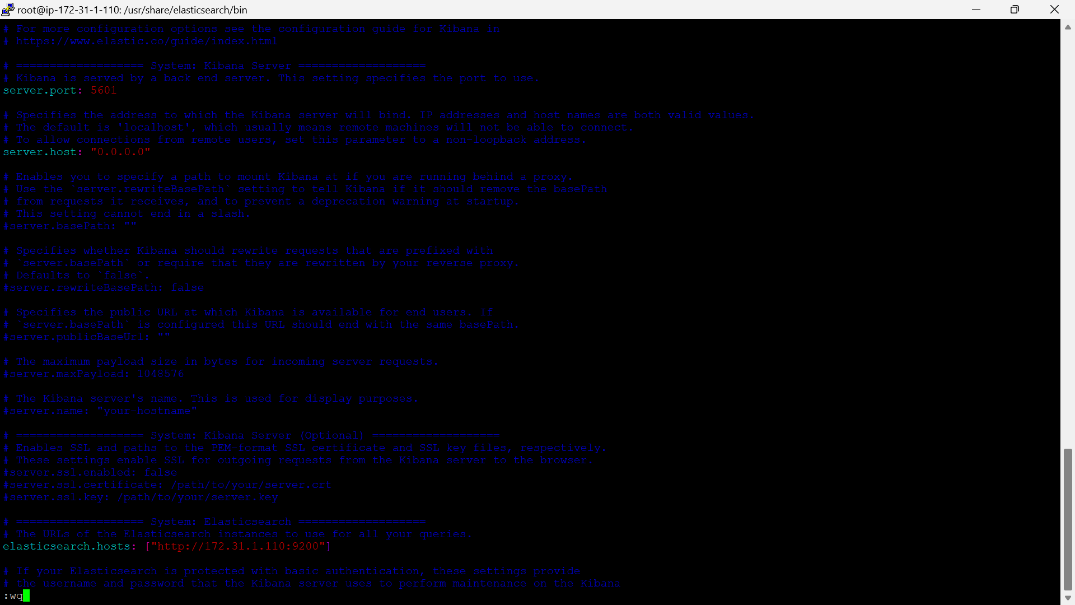
Update the kibana.yml with following server host and port configurations:

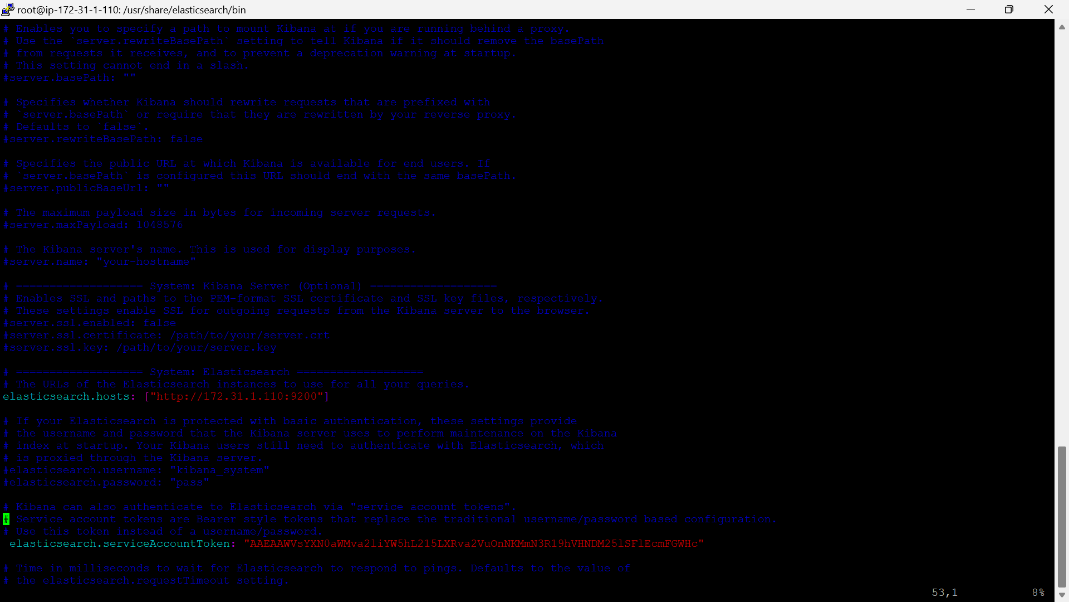
server.port: 5601

server.host: "0.0.0.0"

elasticsearch.hosts: ["http://172.31.5.183:9200"]

elasticsearch.serviceAccountToken: "AAEAAWVsYXN0aWMva2liYW5hL215LXRva2VuOmIyUEI0bkdKUm82SFBMbHZ6NmlScGc"





**#Running Kibana**

Kibana can be started and stopped as follows:

sudo systemctl start kibana.service

sudo systemctl stop kibana.service

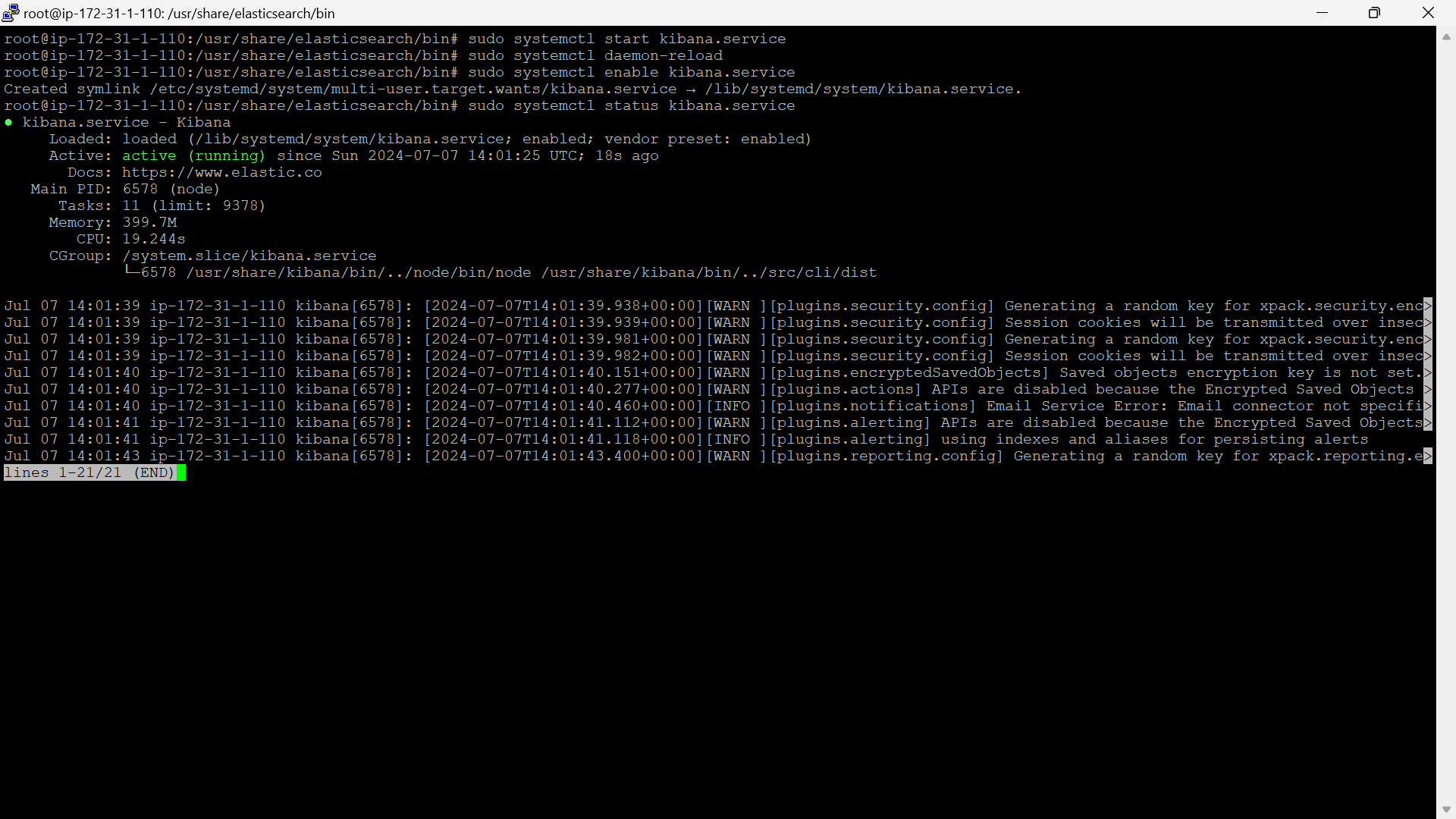
To configure Kibana to start automatically when the system starts, run the following commands:

sudo systemctl daemon-reload

sudo systemctl enable kibana.service

To check status:

sudo systemctl status kibana.service



**Register/Enrolling Kibana with Elasticsearch**

Navigate to kibana-setup:

cd /usr/share/kibana/bin

./kibana-setup --enrollment-token (token)

./kibana

\*If Required.

For verificationcode Navigate to kibana-verification-code:

cd /usr/share/kibana/bin

./kibana-verification-code

( verification code- \*\*\* \*\*\* )