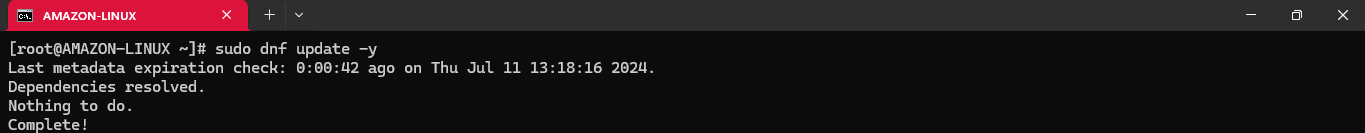
ELK Set-up For Amazon Linux Server

Server Ip : 44.202.205.169

Update the System

sudo dnf update -y

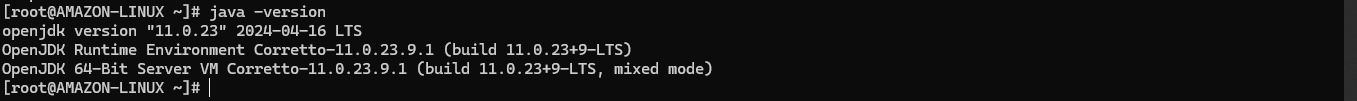


Install Java 11 with development tools (JDK):

sudo yum install java-11 -y

Verifying Installation:

java -version



Configure the Elasticsearch repository:

Create a new repository file for Elasticsearch

sudo nano /etc/yum.repos.d/elasticsearch.repo

[elasticsearch-8.x]

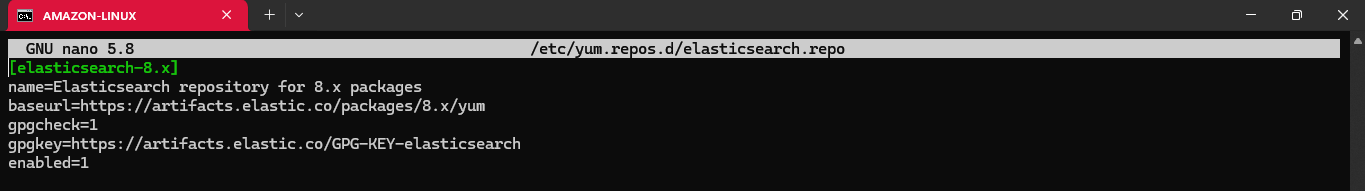
name=Elasticsearch repository for 8.x packages

baseurl=https://artifacts.elastic.co/packages/8.x/yum

gpgcheck=1

gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch

enabled=1



To verify Elasticsearch repository

cat /etc/yum.repos.d/elasticsearch.repo

Import the GPG key:

sudo rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

Update and refresh the repository:

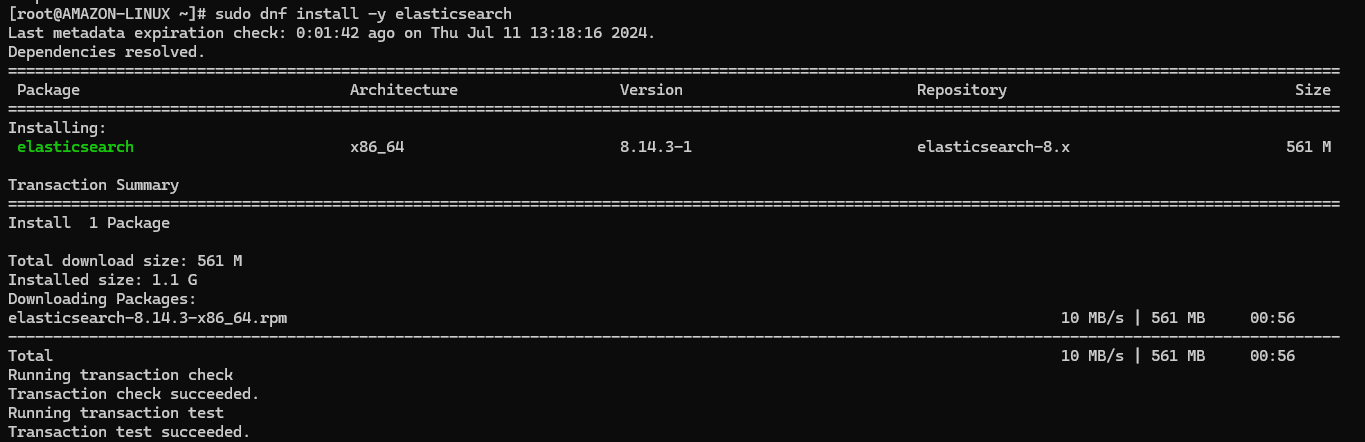
sudo yum clean all

sudo yum makecache

# Install Elasticsearch on Amazon Linux 2023

sudo dnf update -y

sudo dnf install -y elasticsearch



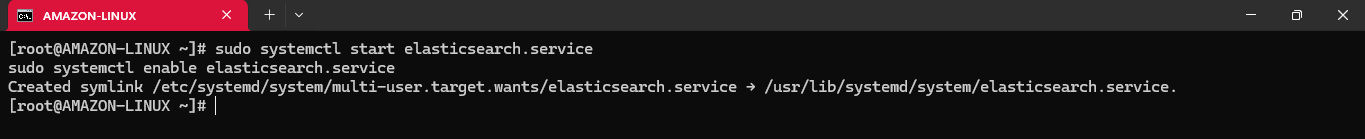
Verify that Elasticsearch has been installed successfully

rpm -qi elasticsearch

Start and enable the Elasticsearch service

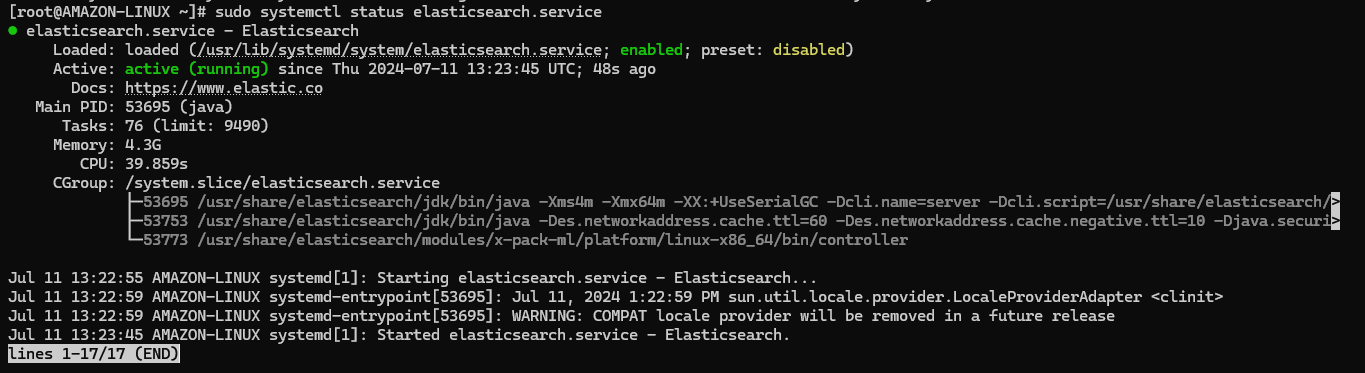
sudo systemctl start elasticsearch.service

sudo systemctl enable elasticsearch.service



check the status of Elasticsearch

sudo systemctl status elasticsearch.service

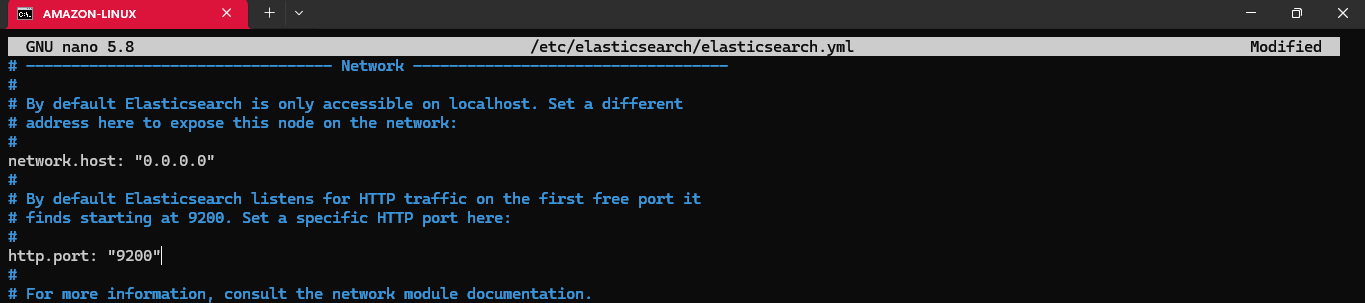


Configure Elasticsearch on Amazon Linux 2023

After the installation, you may need to configure Elasticsearch. Edit the file /etc/elasticsearch/elasticsearch.yml

sudo nano /etc/elasticsearch/elasticsearch.yml

Update the network.host to 0.0.0.0 and http.port to 9200

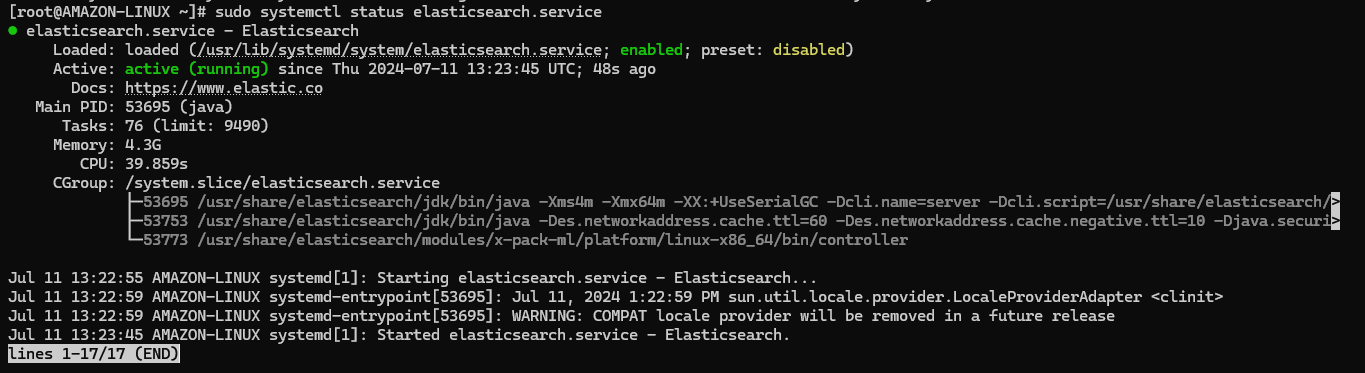


Restart Elasticsearch

sudo systemctl restart elasticsearch.service

Verify service status

sudo systemctl status elasticsearch.service



#Now to integrate Kibana to ElasticSearch You need Tokens

You can then generate an Service Token:

cd /usr/share/elasticsearch/bin/

SERVICE\_TOKEN

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

SERVICE\_TOKEN elastic/kibana/my-token = "AAEAAWVsYXN0aWMva2liYW5hL215LXRva2VuOm5DLWRHQ0pMUVltT2lsU19LeU1pTVE"

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

"eyJ2ZXIiOiI4LjE0LjAiLCJhZHIiOlsiNTUuNTUuMzIuMTIwOjkyMDAiXSwiZmdyIjoiMWQ2MDU5MDAxZGJiNzVmZTBmMDdmYWJkMDE1MDIxOWVmNmE4ZDFmMGZjMWMwNzIwMmY0NmVlOTdiZTJjNzRlMSIsImtleSI6IjlBclBvWkFCb09vaUdyNUNydGl2OjJoRUY2Q1E3UVJpYVAycmNSbF9EV0EifQ=="

sudo nano /etc/elasticsearch/elasticsearch.yml

Update the network.host to 0.0.0.0 and http.port to 9200 and To disable security features, set xpack.security.enabled: false

Restart Elasticsearch

sudo systemctl restart elasticsearch.service

Verify service status

sudo systemctl status elasticsearch.service

Testing Elasticsearch

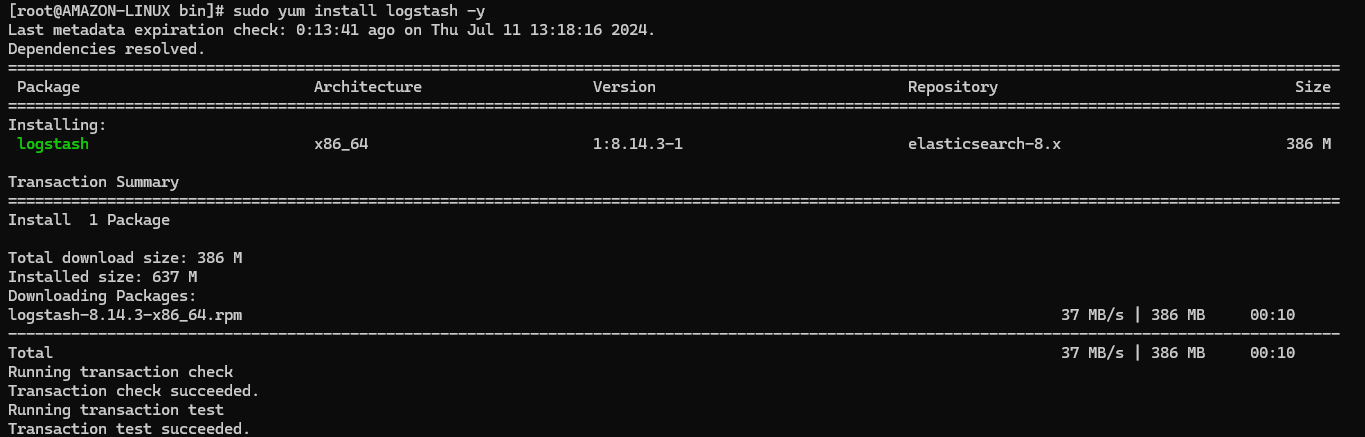
curl -X GET "localhost:9200"

To check browser <Instance publicip>:9200

# Installing and Configuring logstash

Install Logstash

sudo yum install logstash -y



Edit the Logstash configuration file to add the input and output parameters

sudo vi /etc/logstash/conf.d/logstash.conf

paste

input {

beats {

port => 5044

}

}

output {

elasticsearch {

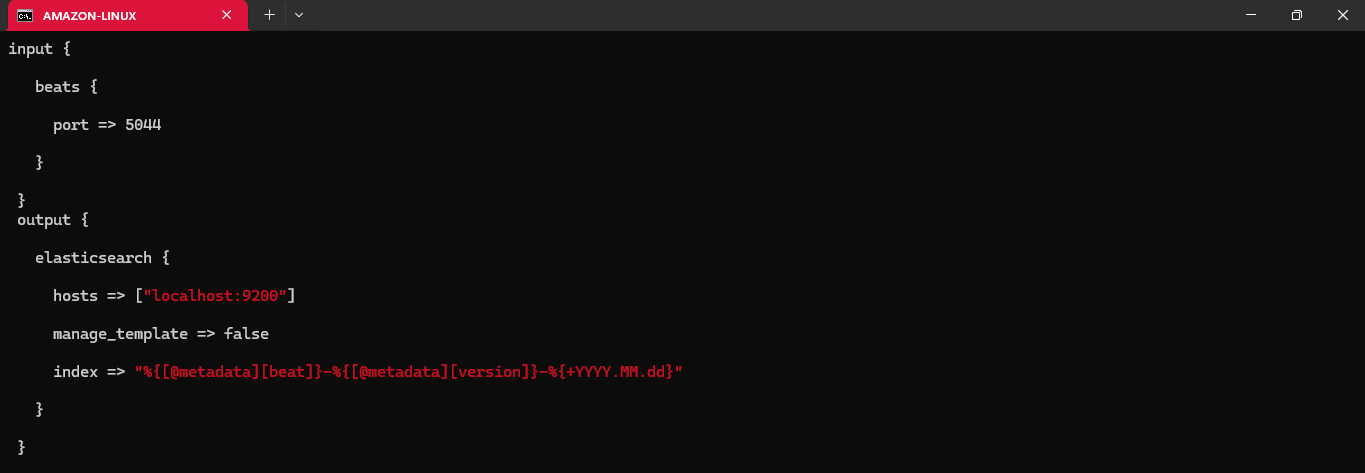
hosts => ["localhost:9200"]

manage\_template => false

index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"

}

}

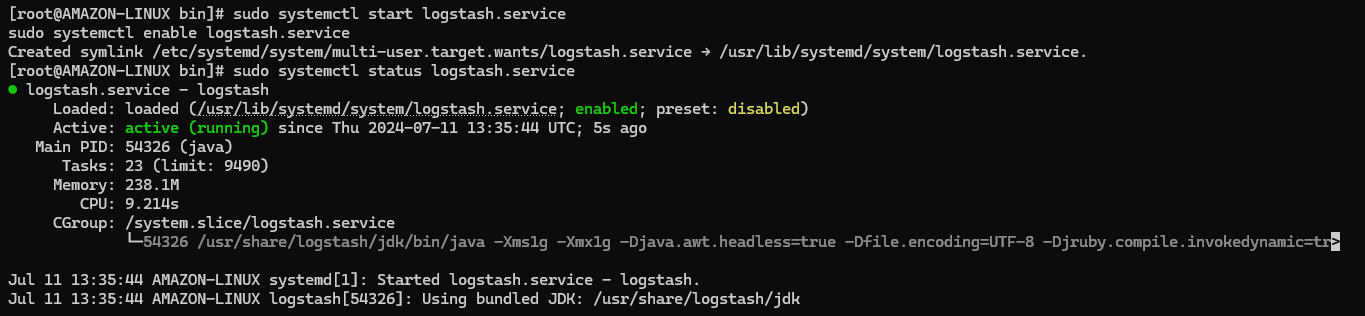


Start and enable the Logstash service

sudo systemctl start logstash.service

sudo systemctl enable logstash.service

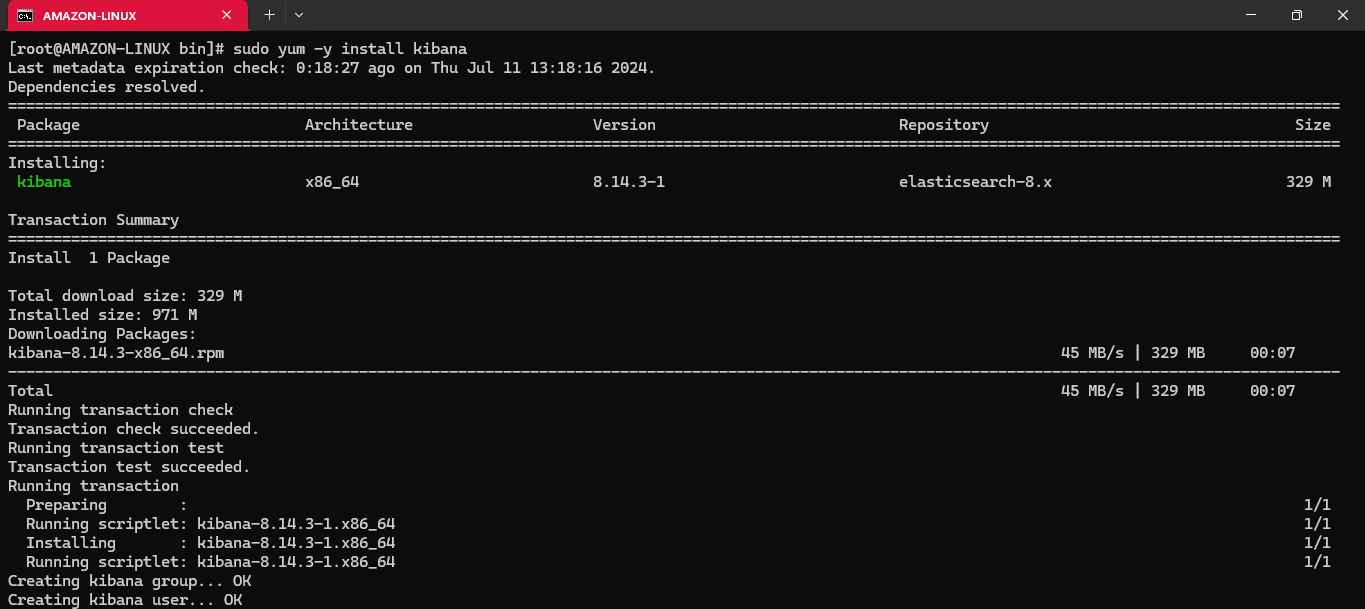
sudo systemctl status logstash.service



# Installing and Configuring Kibana

Install Kibana

sudo yum -y install kibana

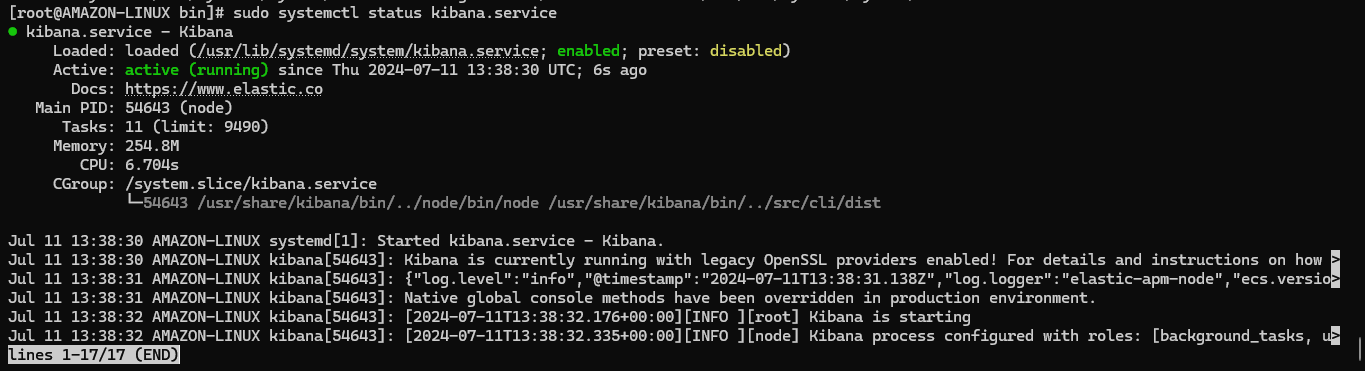


Start and enable the Kibana service

sudo systemctl start kibana.service

sudo systemctl enable kibana.service

sudo systemctl status kibana.service



Configure Kibana by modifying /etc/kibana/kibana.yml.

sudo nano /etc/kibana/kibana.yml

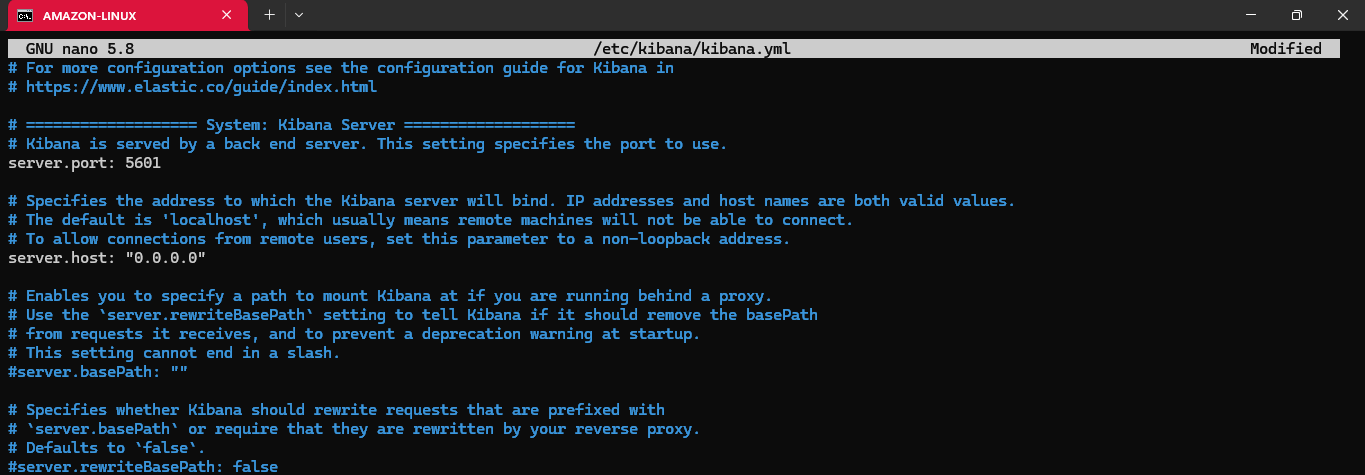
Update and uncomment

server.port to 5601

server.host to "0.0.0.0"

elasticsearch.hosts to ["http://44.202.205.169/:9200"]

elasticsearch.serviceAccountToken: "AAEAAWVsYXN0aWMva2liYW5hL215LXRva2VuOm5DLWRHQ0pMUVltT2lsU19LeU1pTVE"

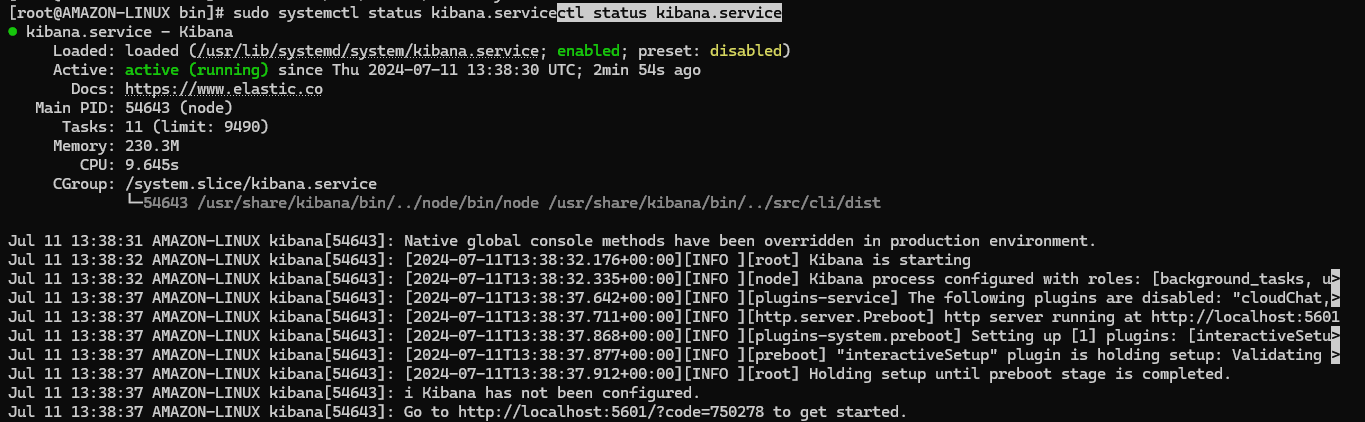


Restart Kibana

sudo systemctl restart kibana.service

Verify service status

sudo systemctl status kibana.service



Register/Enrolling Kibana with Elasticsearch

Navigate to kibana-setup:

cd /usr/share/kibana/bin

./kibana-setup --enrollment-token "eyJ2ZXIiOiI4LjE0LjAiLCJhZHIiOlsiNTUuNTUuMzIuMTIwOjkyMDAiXSwiZmdyIjoiMWQ2MDU5MDAxZGJiNzVmZTBmMDdmYWJkMDE1MDIxOWVmNmE4ZDFmMGZjMWMwNzIwMmY0NmVlOTdiZTJjNzRlMSIsImtleSI6IjlBclBvWkFCb09vaUdyNUNydGl2OjJoRUY2Q1E3UVJpYVAycmNSbF9EV0EifQ=="

./kibana

