**How to install and configure Elasticsearch, Logstash, Kibana (ELK):**

We are going to do this by making two instances one is for elasticsearch and logstash and another is for kibana

**Step 1:**

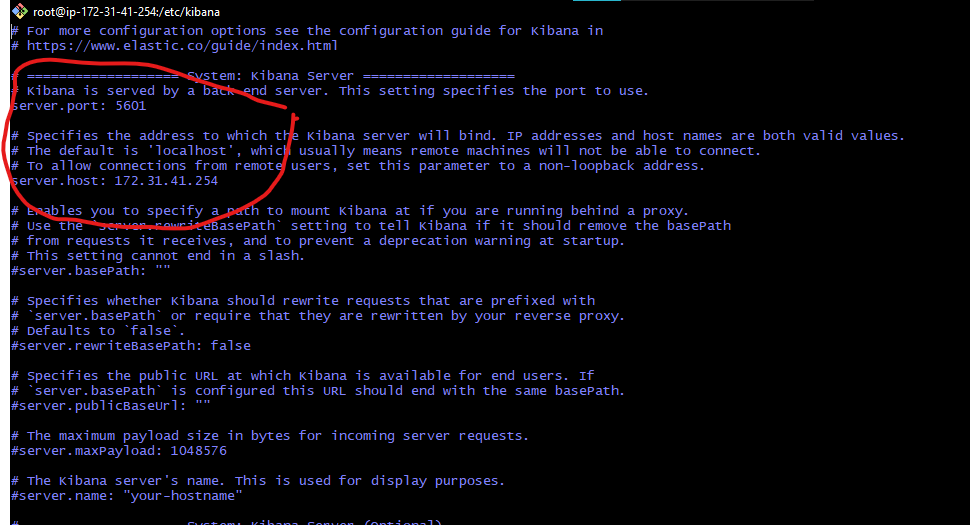
1. Firstly I created a instance for kibana
2. Then install the kibana by using the rpm method from the ELK documentation.
3. When you first enter the rpm command it will say SHAI1 signature is not found.
4. Search for it and you will a following command for that.

update-crypto-policies --set DEFAULT:SHA1

1. After installation start and enable the

kibana systemctl start & enable kibana

1. Then go to /etc/kibana/kibana.yml
2. Enable the port number and server host and give private Ip address of kibana instance ,save and exit



1. Then restart the kibana by systemctl kibana restart
2. When you put the ip of kibana in url ip:5601 it will ask for elasticsearch token.... for that refer the Step 2.

A screenshot of a computer

Description automatically generated

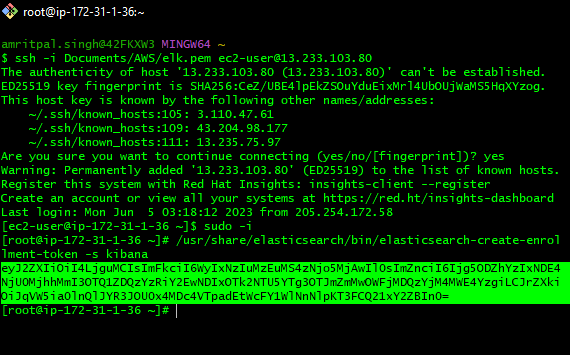
**Step 2:**

1. Firstly install the elasticsearch from the rpm package (from ELK documentation) and note the password after the installation .
2. Or change it from /usr/share/elasticsearch/bin/elasticsearch-reset-password -i -u elastic
3. Then change the server host in vi /etc/elasticsearch/elasticsearch.yml (give private ip) and and enable the port

A screenshot of a computer

Description automatically generated with medium confidence

1. Now find the token by /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana (kibana is username)



1. Now put that enrollment token in the login page of kibana

A screenshot of a computer

Description automatically generated

1. If it ask for the verification of kibana then find the code by usr/share/kibana/bin/kibana-verification-code

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated with medium confidence

The username is elastic

And password is Elastic@...

A screenshot of a computer

Description automatically generated

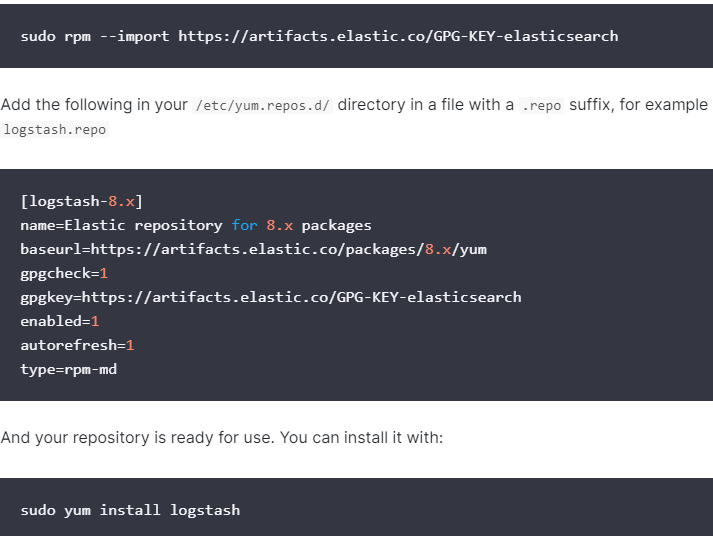
A screenshot of a computer

Description automatically generated

**Step 3:**

Now install the logstash:

1. Install the logstash from the ELK documentation in the elasticsearch instance



Start and enable the logstash