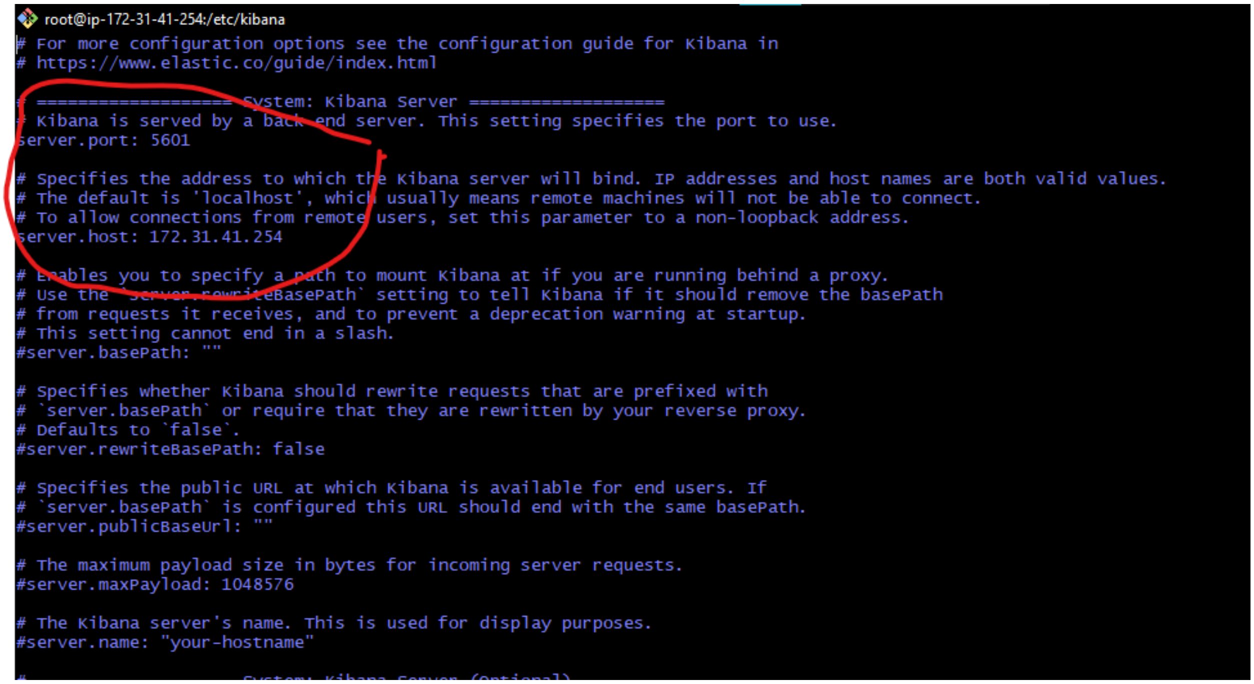
How to install and configure Elasticsearch, Logstash, Kibana (ELK):

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

Step 1:

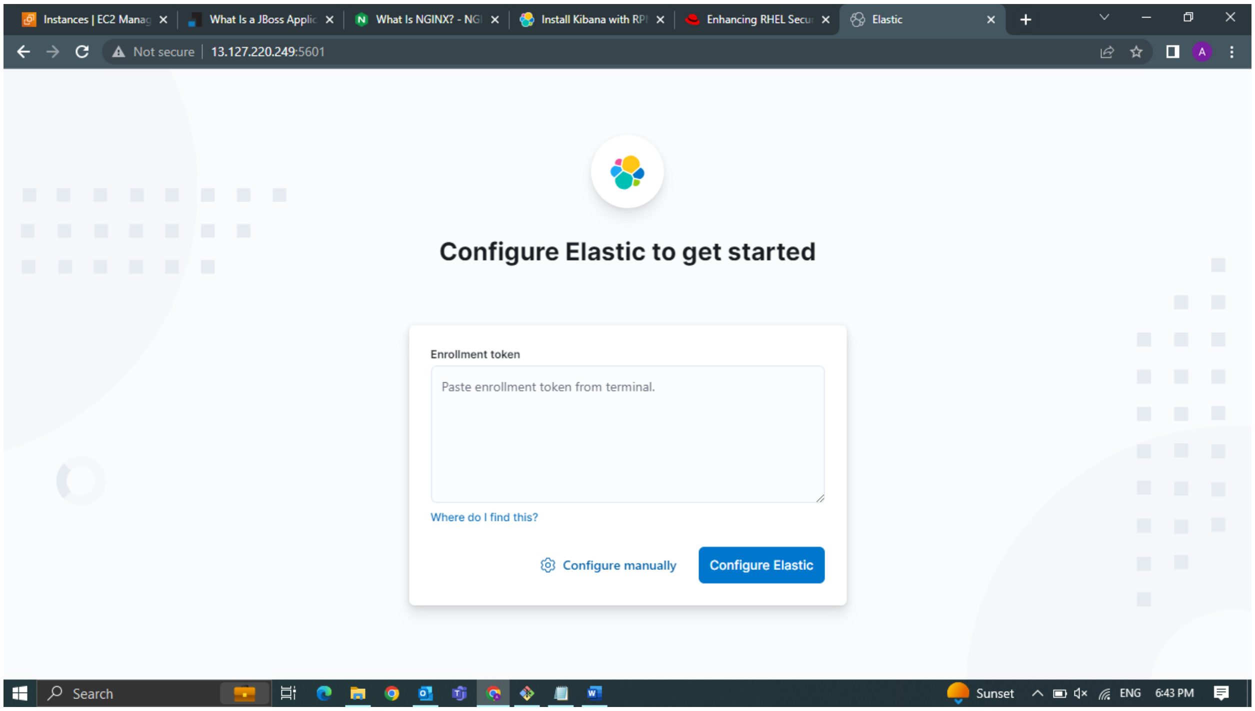
1. Firstly I created a instance for kibana
2. Then install the kibana by using the rpm method from the ELK documentation.
3. When you first enter the rpm command it will say SHAI1 signature is not found.
4. Search for it and you will a following command for that.
   update-crypto-policies --set DEFAULT:SHA1
5. After installation start and enable the
   kibana systemctl start & enable kibana
6. Then go to /etc/kibana/kibana.yml
7. Enable the port number and server host and give private Ip address of kibana instance ,save and exit



root@ip-172-31-41-254:/etc/kibana

```
# For more configuration options see the configuration guide for Kibana in
# https://www.elastic.co/guide/index.html

# =================== System: Kibana Server ===================
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: 172.31.41.254

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.
# Defaults to `false`.
#server.rewriteBasePath: false

# Specifies the public URL at which Kibana is available for end users. If
# `server.basePath` is configured this URL should end with the same basePath.
#server.publicBaseUrl: ""

# The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576

# The Kibana server's name. This is used for display purposes.
#server.name: "your-hostname"
```

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



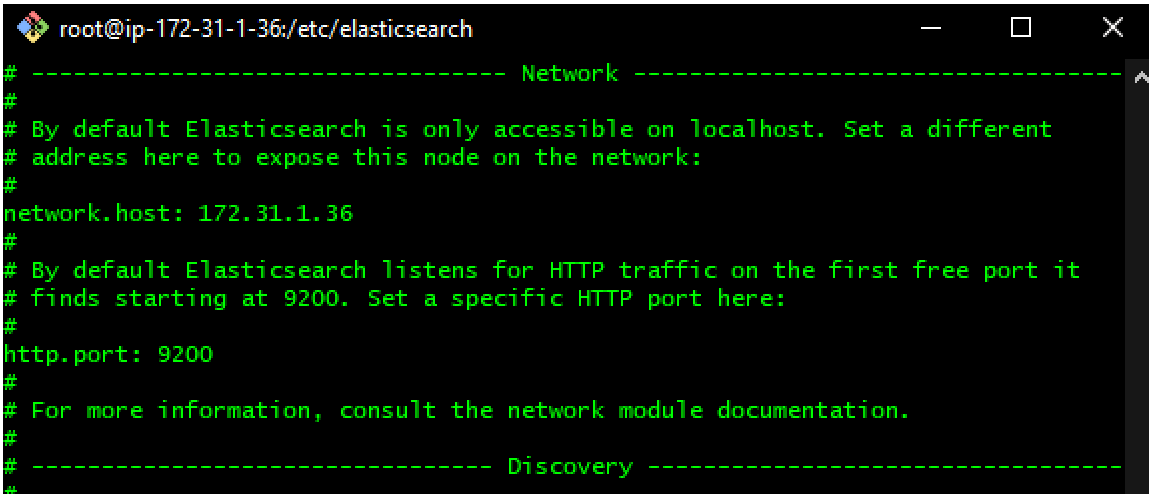
Configure Elastic to get started

Enrollment token

Paste enrollment token from terminal.

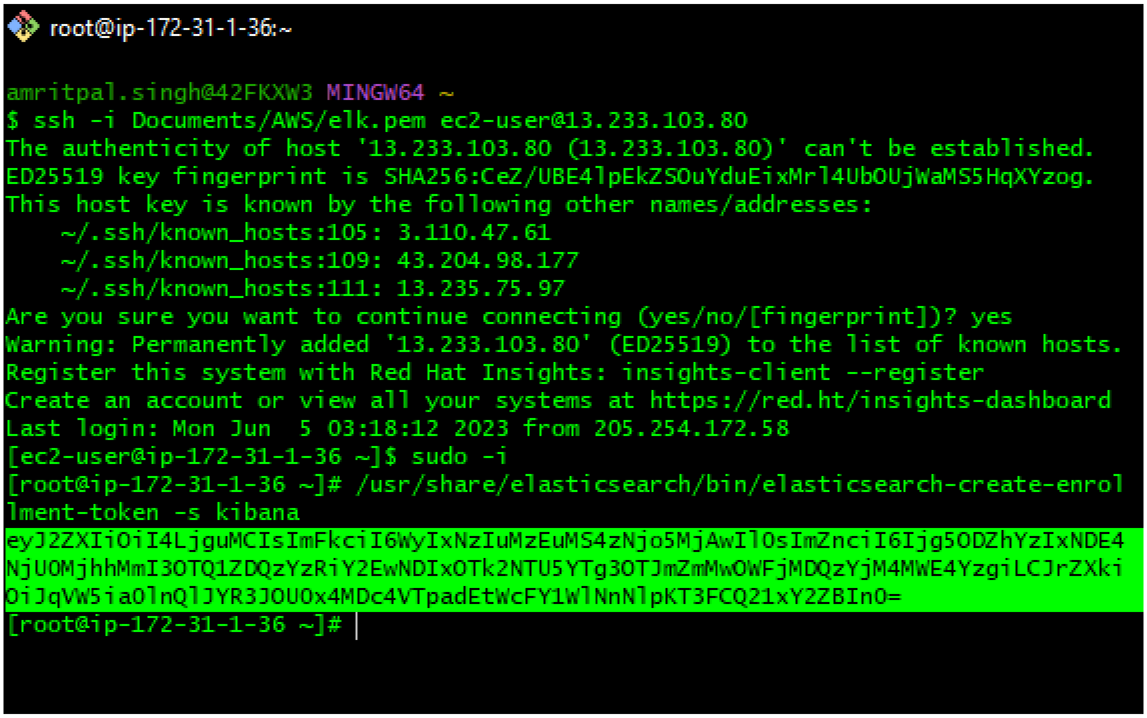
Step 2:

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



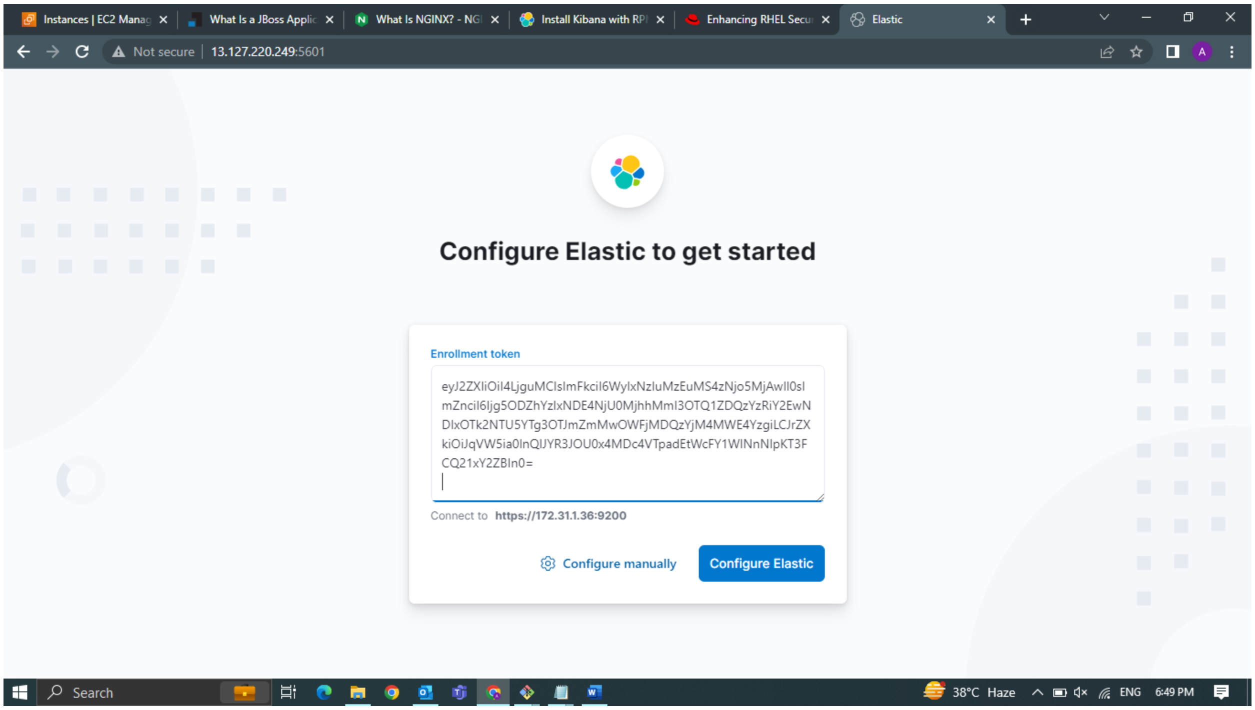
```
# ---------------------------------- Network -----------------------------------
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: 172.31.1.36
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
# --------------------------------- Discovery ----------------------------------
#
```

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



```
amritpal.singh@42FKXW3 MINGW64 ~
$ ssh -i Documents/AWS/elk.pem ec2-user@13.233.103.80
The authenticity of host '13.233.103.80 (13.233.103.80)' can't be established.
ED25519 key fingerprint is SHA256:CeZ/UBE4lpEkZSOuYduEixMrl4UbOUjWaMS5HqXYzog.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:105: 3.110.47.61
    ~/.ssh/known_hosts:109: 43.204.98.177
    ~/.ssh/known_hosts:111: 13.235.75.97
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.233.103.80' (ED25519) to the list of known hosts.
Register this system with Red Hat Insights: insights-client --register
Create an account or view all your systems at https://red.ht/insights-dashboard
Last login: Mon Jun  5 03:18:12 2023 from 205.254.172.58
[ec2-user@ip-172-31-1-36 ~]$ sudo -i
[root@ip-172-31-1-36 ~]# /usr/share/elasticsearch/bin/elasticsearch-create-enrol
lment-token -s kibana
eyJ2ZXIiOiI4LjguMCIsImFkciI6WyIxNzIuMzEuMS4zNjo5MjAwIl0sImZnciI6Ijg5ODZhYzIxNDE4
NjU0MjhhMmI3OTQ1ZDQzYzRiY2EwNDIxOTk2NTU5YTg3OTJmZmMwOWFjMDQzYjM4MWE4YzgiLCJrZXki
OiJqVW5ia0lnQlJYR3JOU0x4MDc4VTpadEtWcFY1WlNnNlpKT3FCQ21xY2ZBIn0=
[root@ip-172-31-1-36 ~]# |
```

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



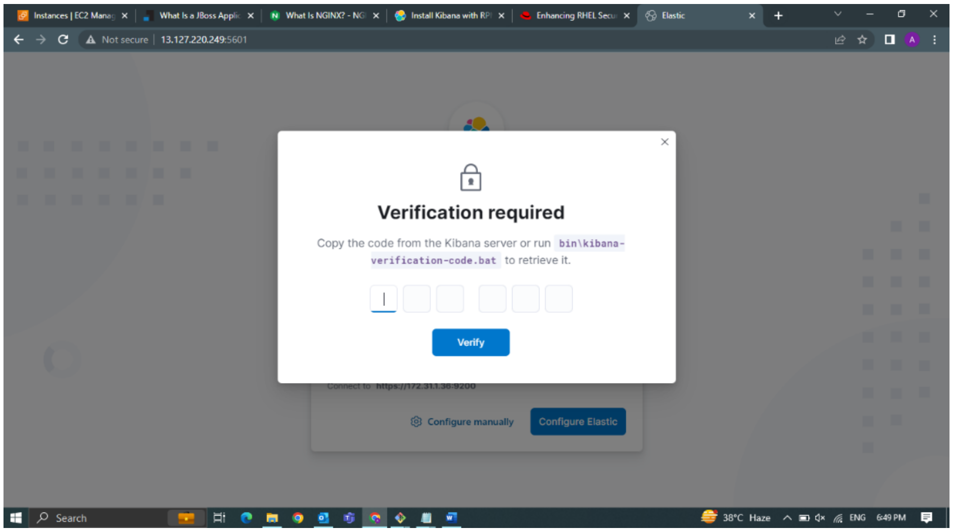
Configure Elastic to get started

Enrollment token

eyJ2ZXIiOiI4LjguMCIsImFkciI6WyIxNzIuMzEuMS4zNjo5MjAwIl0sImZnciI6Ijg5ODZhYzIxNDE4NjU0MjhhMmI3OTQ1ZDQzYzRiY2EwNDIxOTk2NTU5YTg3OTJmZmMwOWFjMDQzYjM4MWE4YzgiLCJrZXkiOiJqVW5ia0lnQlJYR3JOU0x4MDc4VTpadEtWcFY1WlNnNlpKT3FCQ21xY2ZBIn0=

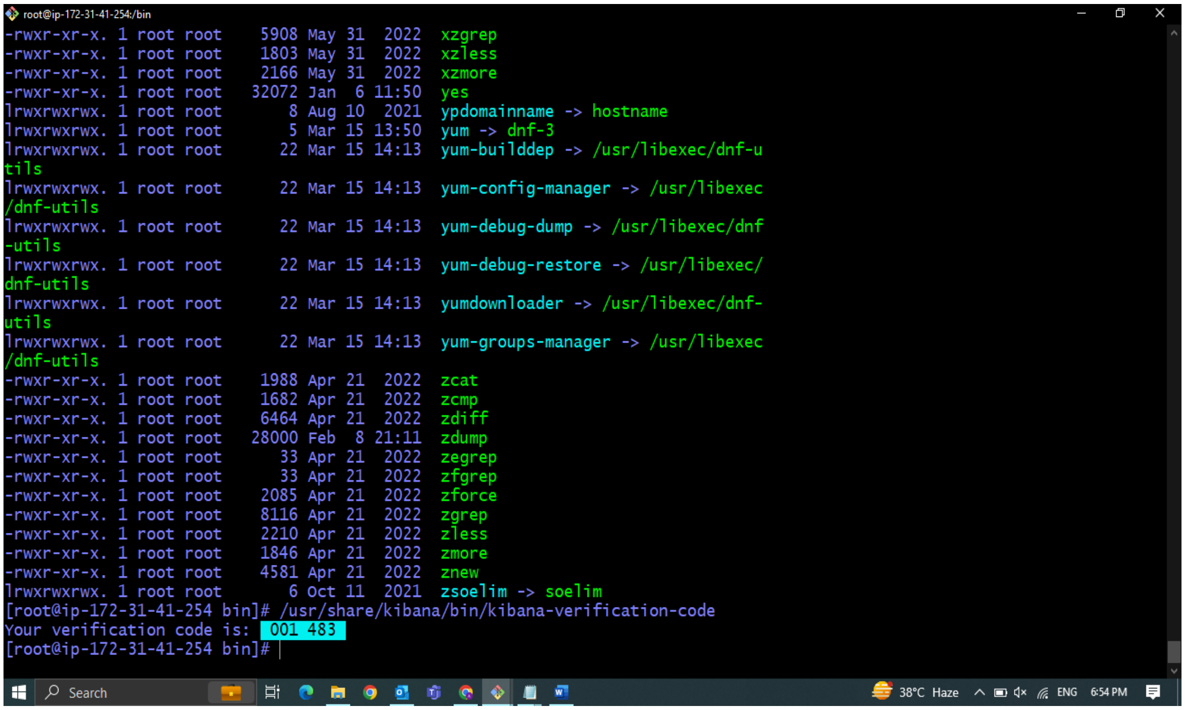
Connect to **https://172.31.1.36:9200**

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



Verification required

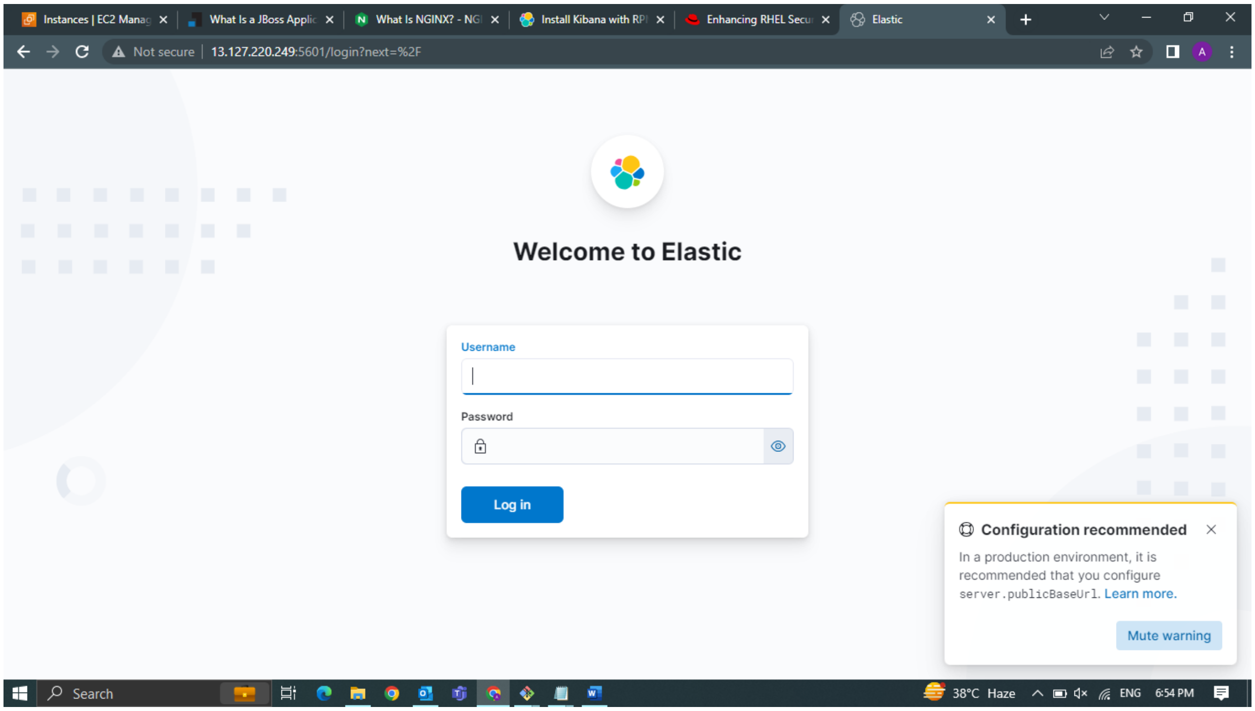
Copy the code from the Kibana server or run `bin\kibana-verification-code.bat` to retrieve it.



```
-rwxr-xr-x. 1 root root    5908 May 31  2022  xzgrep
-rwxr-xr-x. 1 root root    1803 May 31  2022  xzless
-rwxr-xr-x. 1 root root    2166 May 31  2022  xzmore
-rwxr-xr-x. 1 root root   32072 Jan  6 11:50  yes
lrwxrwxrwx. 1 root root       8 Aug 10  2021  ypdomainname -> hostname
lrwxrwxrwx. 1 root root       5 Mar 15 13:50  yum -> dnf-3
lrwxrwxrwx. 1 root root      22 Mar 15 14:13  yum-builddep -> /usr/libexec/dnf-u
tils
lrwxrwxrwx. 1 root root      22 Mar 15 14:13  yum-config-manager -> /usr/libexec
/dnf-utils
lrwxrwxrwx. 1 root root      22 Mar 15 14:13  yum-debug-dump -> /usr/libexec/dnf
-utils
lrwxrwxrwx. 1 root root      22 Mar 15 14:13  yum-debug-restore -> /usr/libexec/
dnf-utils
lrwxrwxrwx. 1 root root      22 Mar 15 14:13  yumdownloader -> /usr/libexec/dnf-
utils
lrwxrwxrwx. 1 root root      22 Mar 15 14:13  yum-groups-manager -> /usr/libexec
/dnf-utils
-rwxr-xr-x. 1 root root    1988 Apr 21  2022  zcat
-rwxr-xr-x. 1 root root    1682 Apr 21  2022  zcmp
-rwxr-xr-x. 1 root root    6464 Apr 21  2022  zdiff
-rwxr-xr-x. 1 root root   28000 Feb  8 21:11  zdump
-rwxr-xr-x. 1 root root      33 Apr 21  2022  zegrep
-rwxr-xr-x. 1 root root      33 Apr 21  2022  zfgrep
-rwxr-xr-x. 1 root root    2085 Apr 21  2022  zforce
-rwxr-xr-x. 1 root root    8116 Apr 21  2022  zgrep
-rwxr-xr-x. 1 root root    2210 Apr 21  2022  zless
-rwxr-xr-x. 1 root root    1846 Apr 21  2022  zmore
-rwxr-xr-x. 1 root root    4581 Apr 21  2022  znew
lrwxrwxrwx. 1 root root       6 Oct 11  2021  zsoelim -> soelim
[root@ip-172-31-41-254 bin]# /usr/share/kibana/bin/kibana-verification-code
Your verification code is:  001 483
[root@ip-172-31-41-254 bin]# 
```

The username is elastic

And password is Elastic@...



Welcome to Elastic

Username

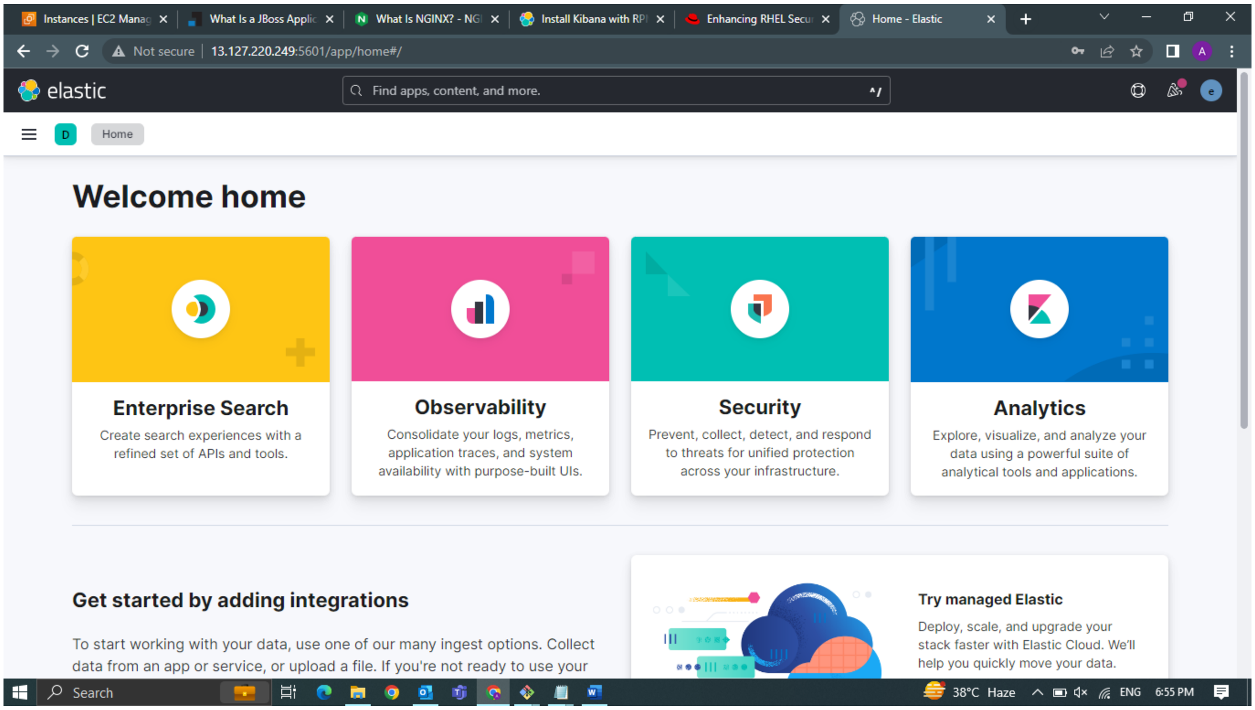
Password

Log in

Configuration recommended

In a production environment, it is recommended that you configure `server.publicBaseUrl`. Learn more.

Mute warning



Welcome home

Enterprise Search

Create search experiences with a refined set of APIs and tools.

Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Analytics

Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your

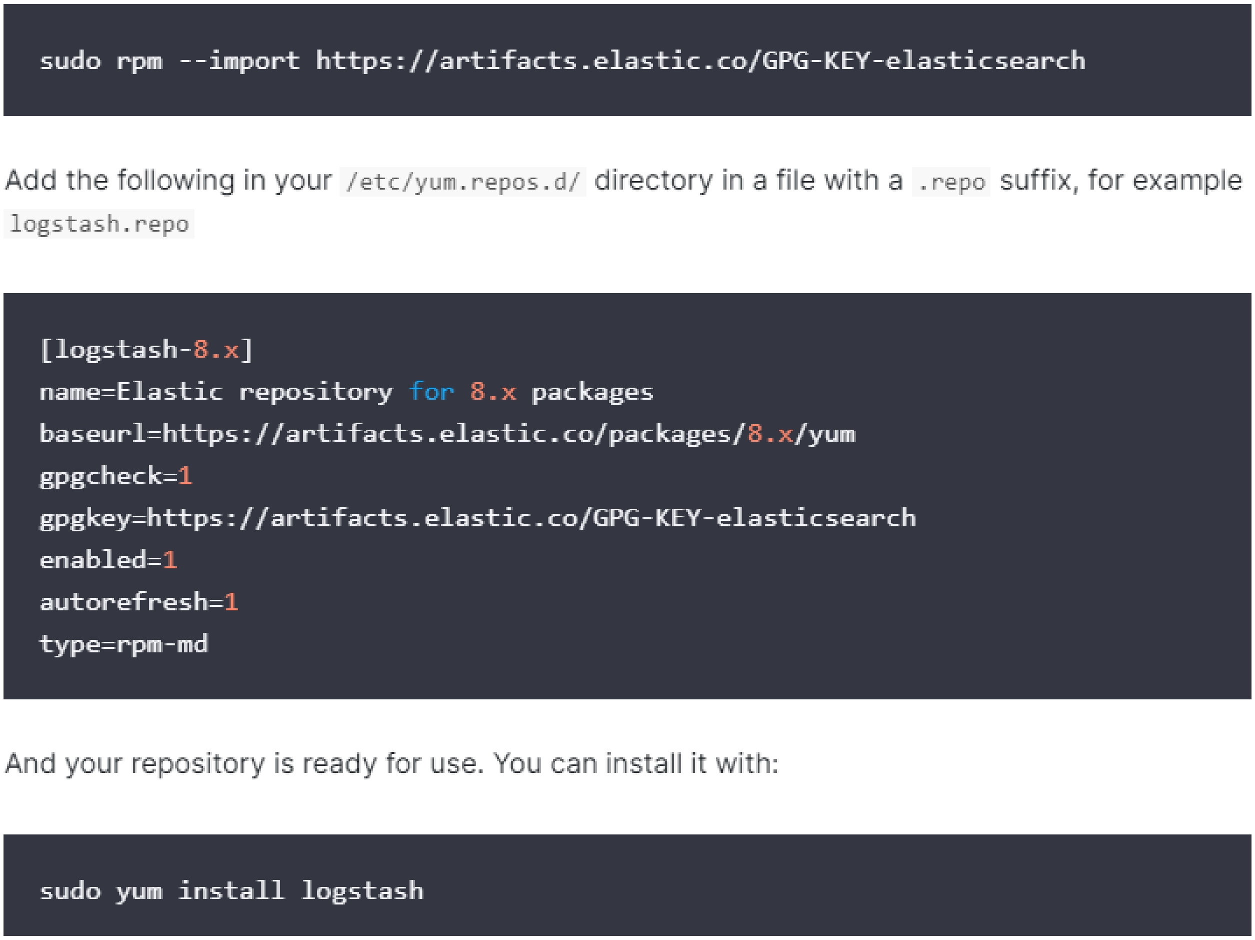
Try managed Elastic

Deploy, scale, and upgrade your stack faster with Elastic Cloud. We'll help you quickly move your data.

Step 3:

Now install the logstash:

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



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

Add the following in your `/etc/yum.repos.d/` directory in a file with a `.repo` suffix, for example `logstash.repo`

```
[logstash-8.x]
name=Elastic 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
autorefresh=1
type=rpm-md
```

And your repository is ready for use. You can install it with:

```
sudo yum install logstash
```

Start and enable the logstash