**Setting Elasticseach , Kibana , Elastic Agent on EC2**

* git clone <https://github.com/Shivamrathi001/elastic-setup.git>
* cd elastic-setup
* chmod +x elastic.sh
* sudo ./elastic.sh

**Note:**

**Save elastic password,**

**Enrollment token and**

**Verification code**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. Launch t3a.medium ,ubuntu 20 , and storage with 16gb

Security Group:

SSH Port:22 MyIp

All TCP Port:0 - 65535 0.0.0.0/0

1. ElasticSearch

* wget -qO -<https://artifacts.elastic.co/GPG-KEY-elasticsearch> | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
* wget<https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.3.0-amd64.deb>
* wget<https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.3.0-amd64.deb.sha512>
* shasum -a 512 -c elasticsearch-8.3.0-amd64.deb.sha512
* sudo dpkg -i elasticsearch-8.3.0-amd64.deb

Save the elastic user password

sudo nano /etc/elasticsearch/elasticsearch.yml

* + sudo systemctl start elasticsearch.service
* sudo curl --cacert /etc/elasticsearch/certs/http\_ca.crt -u elastic<https://localhost:9200>

**Save elasticsearch Password**

1. Install Kibana

* wget -qO -<https://artifacts.elastic.co/GPG-KEY-elasticsearch> | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
* wget<https://artifacts.elastic.co/downloads/kibana/kibana-8.3.0-amd64.deb>
* shasum -a 512 kibana-8.3.0-amd64.deb
* sudo dpkg -i kibana-8.3.0-amd64.deb
* sudo nano /etc/kibana/kibana.yml

server.port: 5601

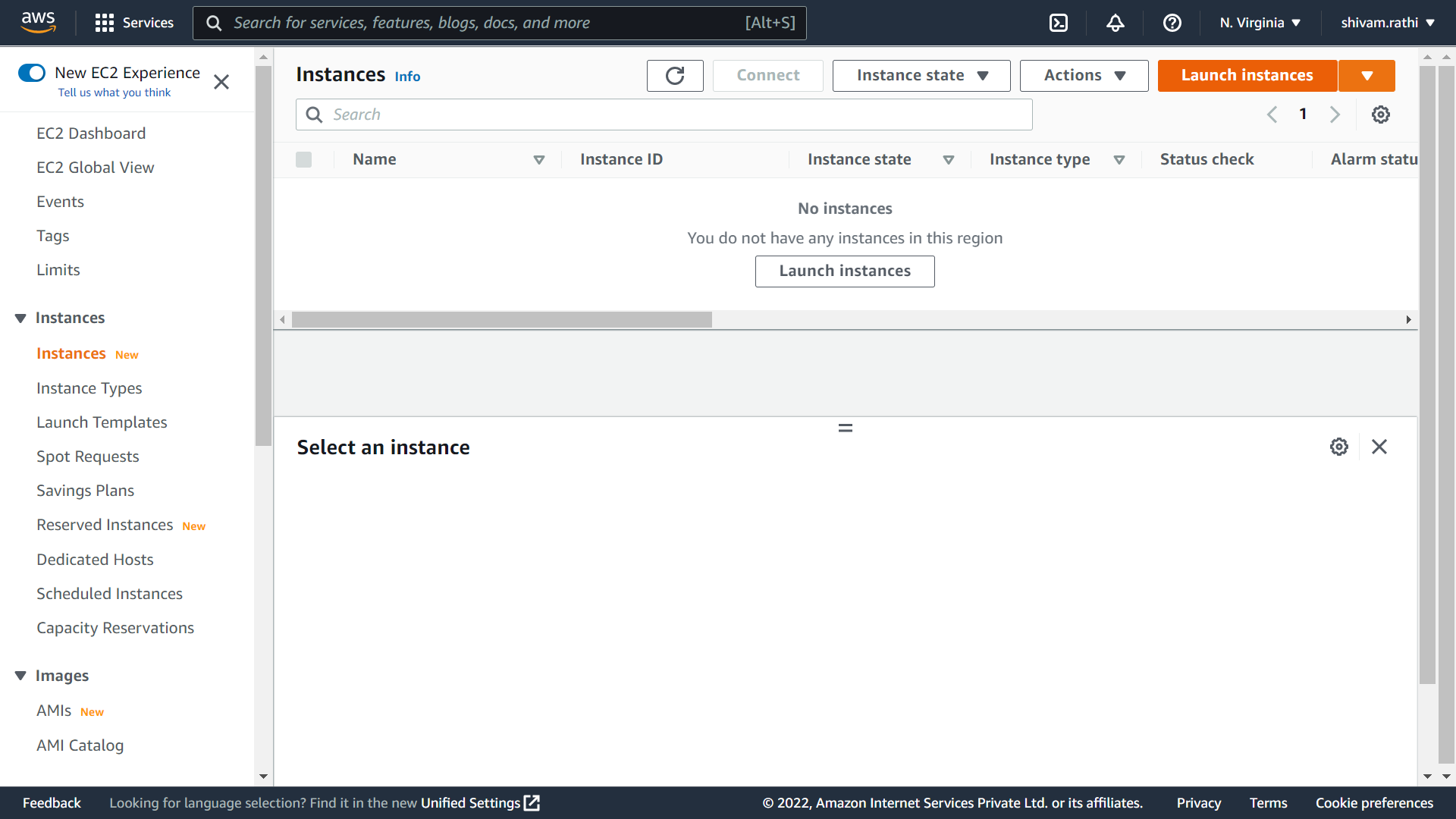
server.host: "0.0.0.0"

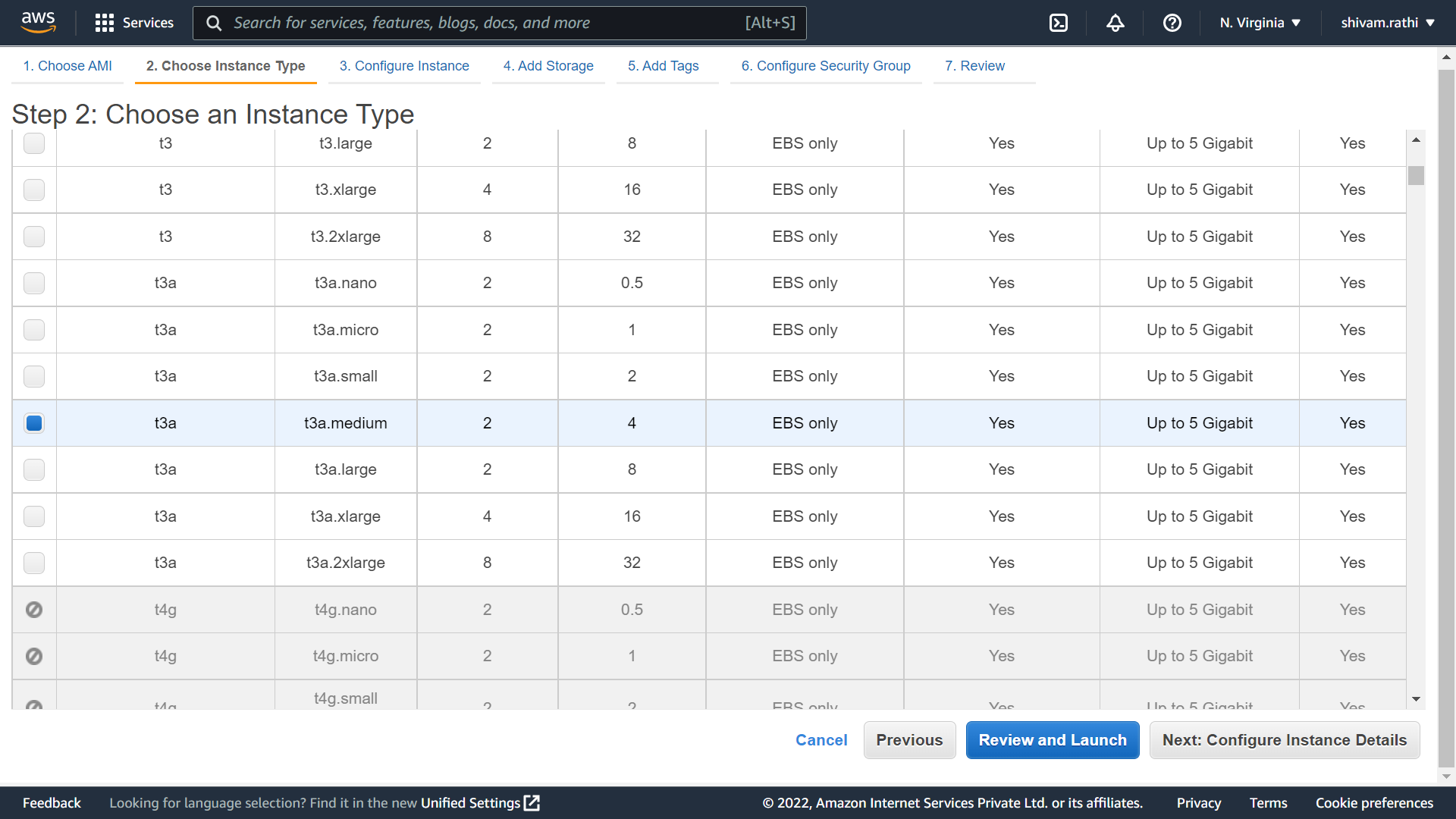
* sudo systemctl start kibana.service
* cd /usr/share/elasticsearch

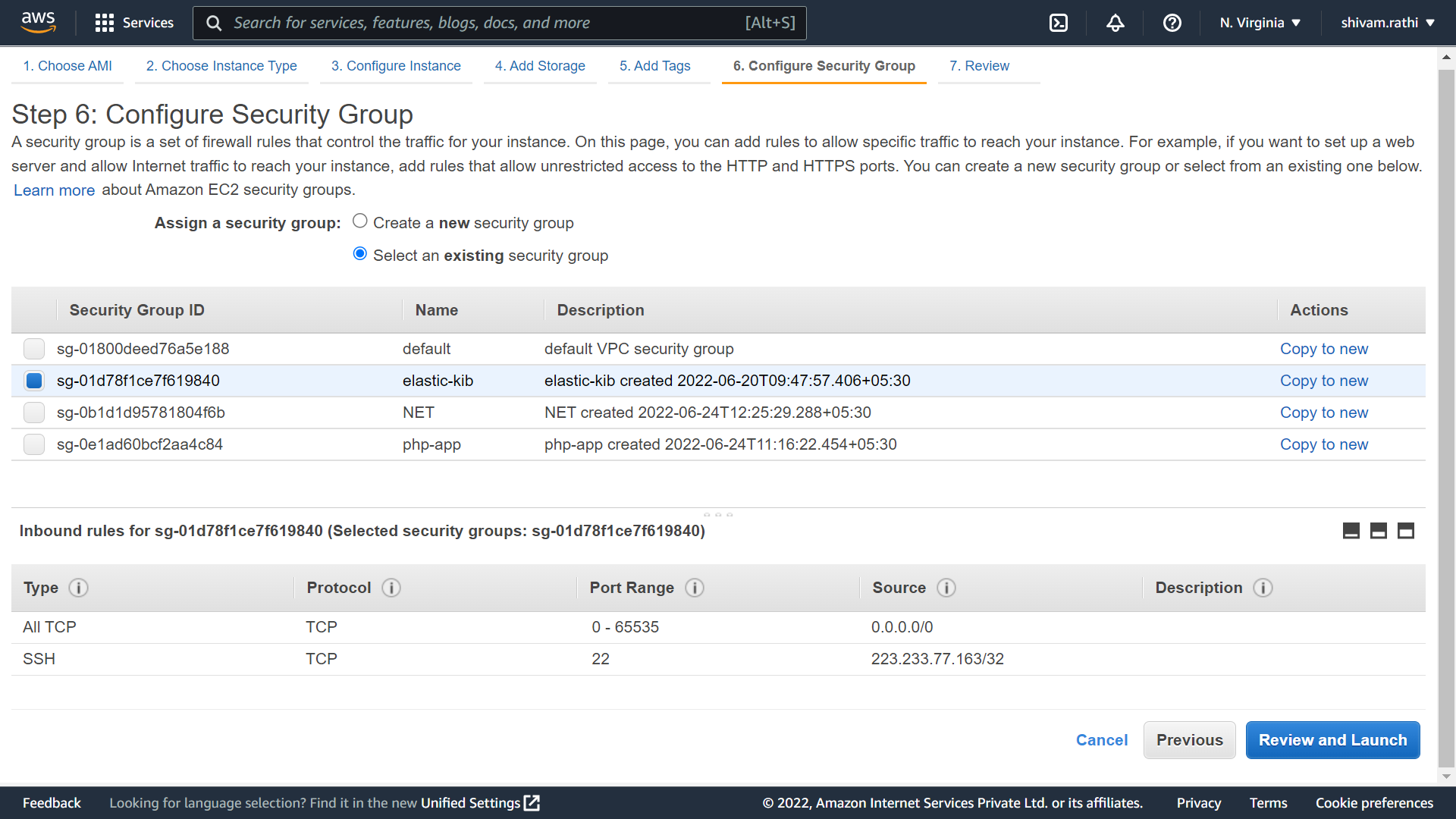
sudo bin/elasticsearch-create-enrollment-token -s kibana

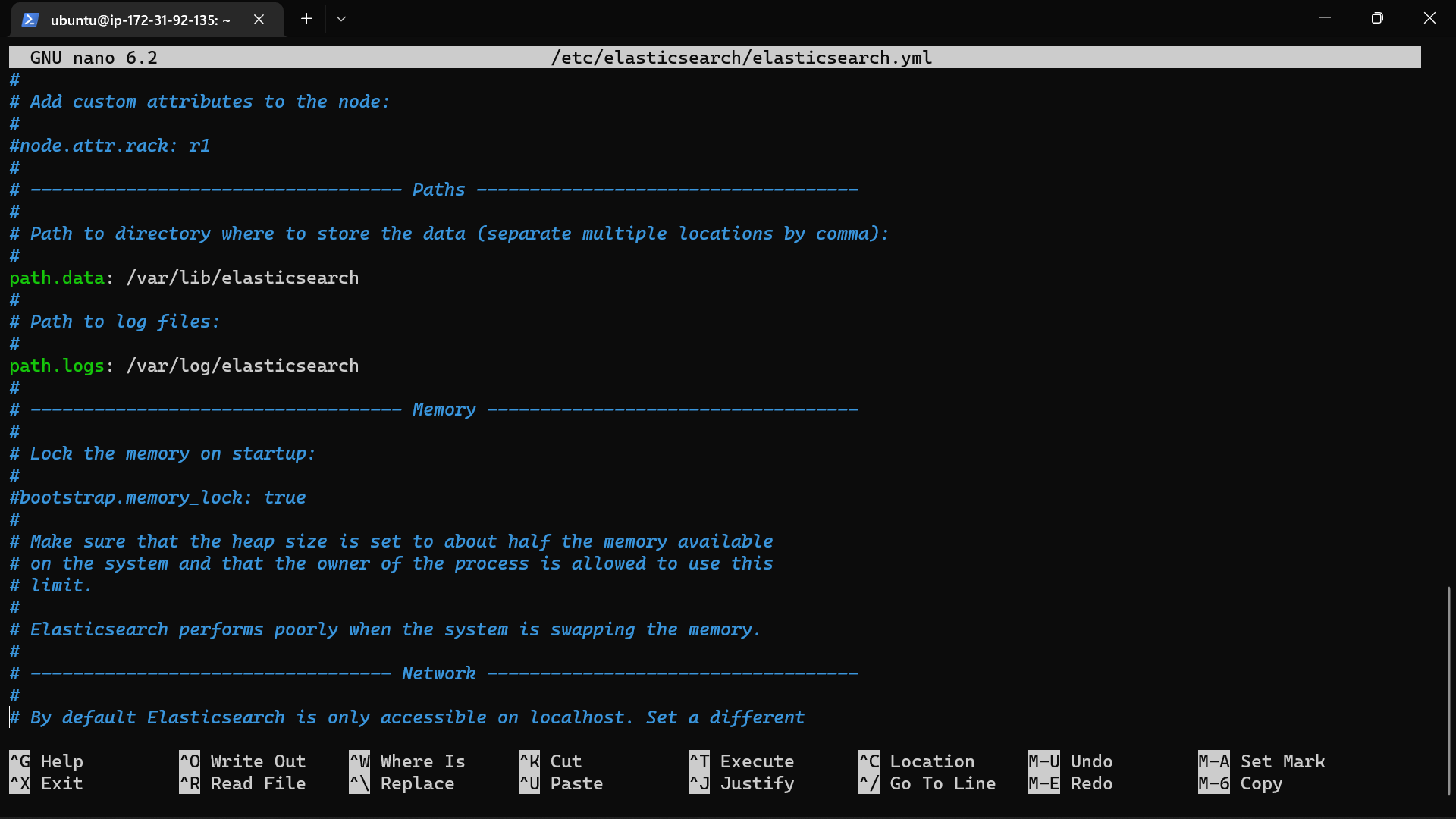
* cd /usr/share/kibana

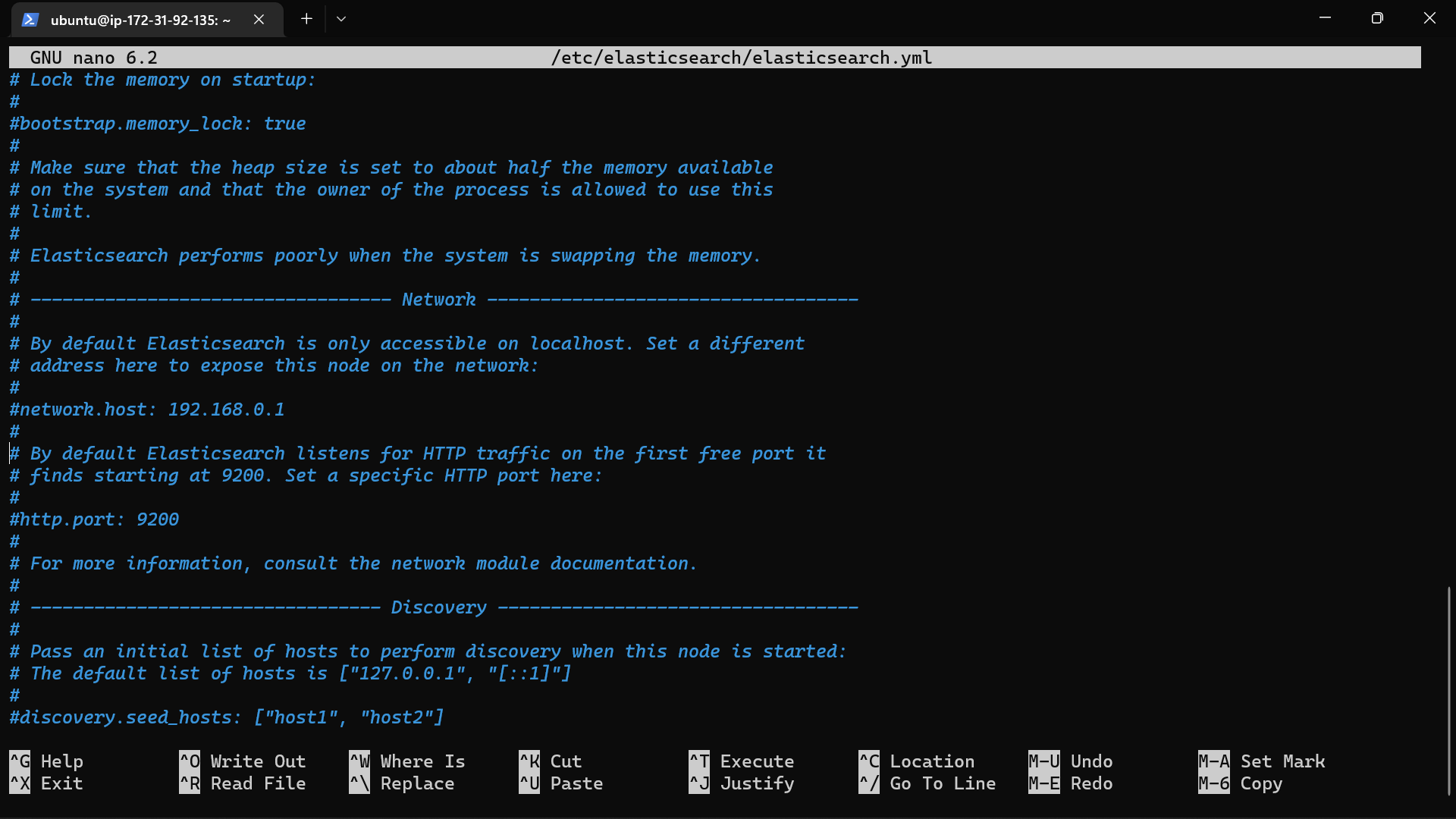
sudo bin/kibana-verification-code

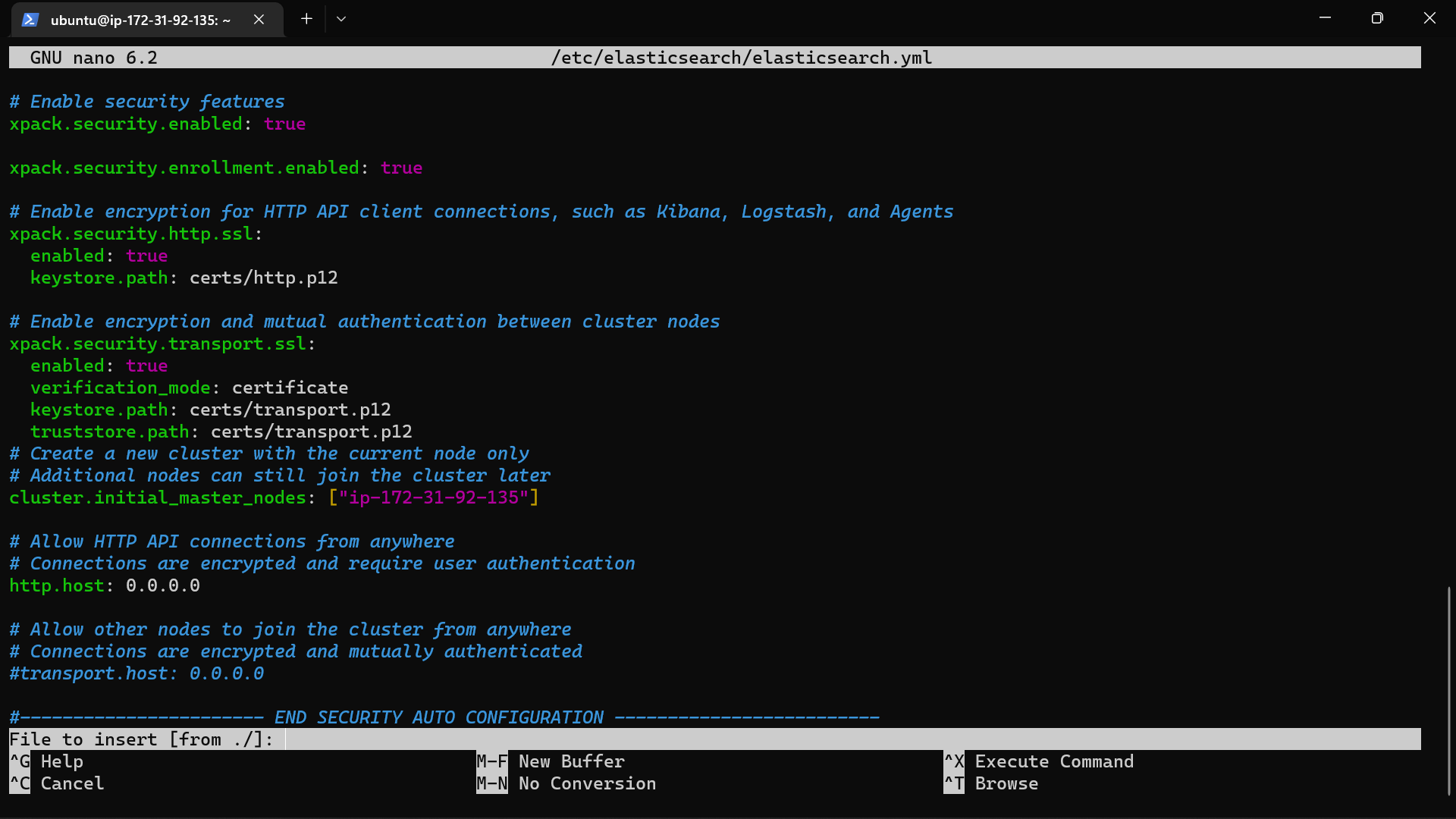


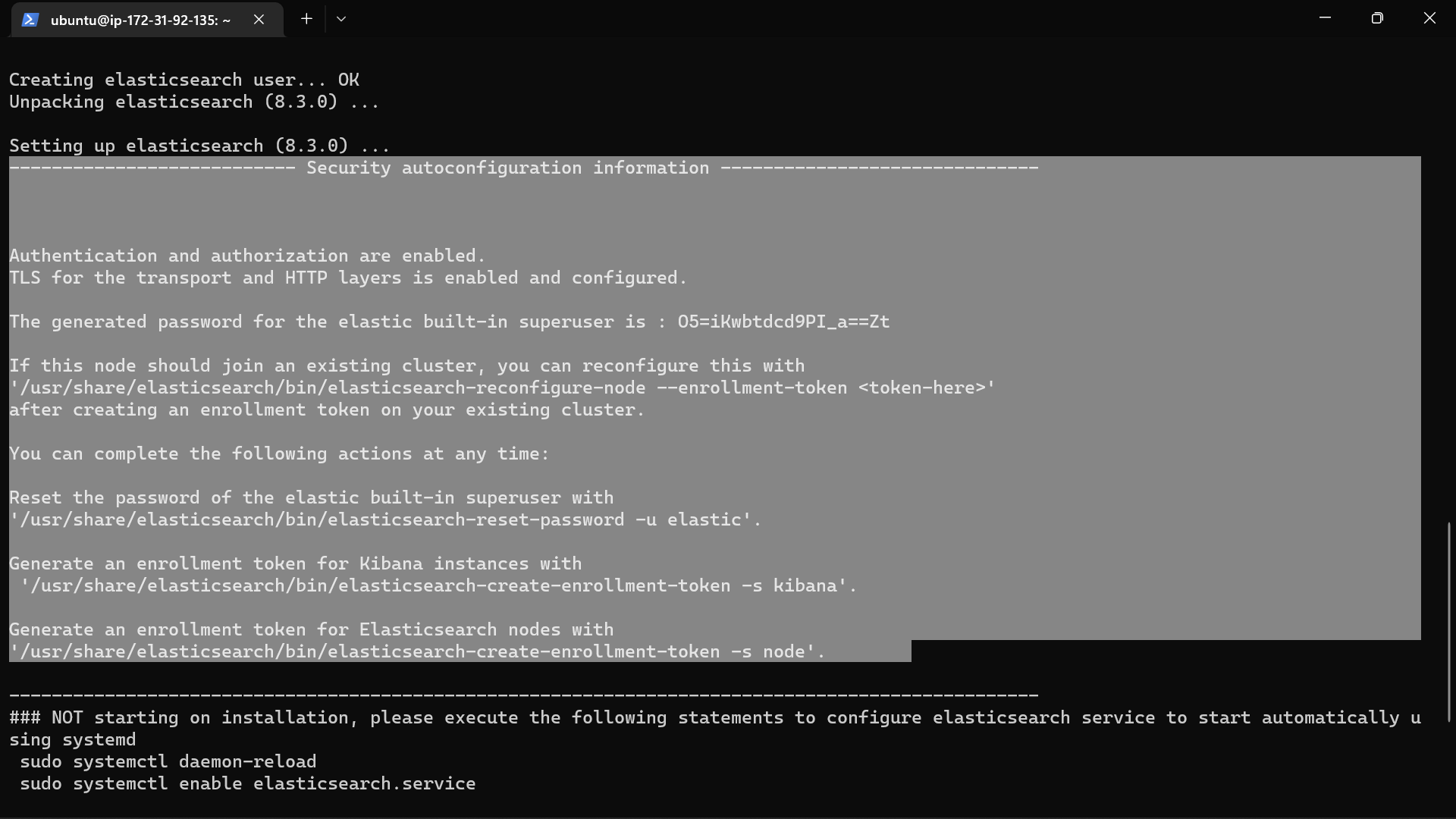


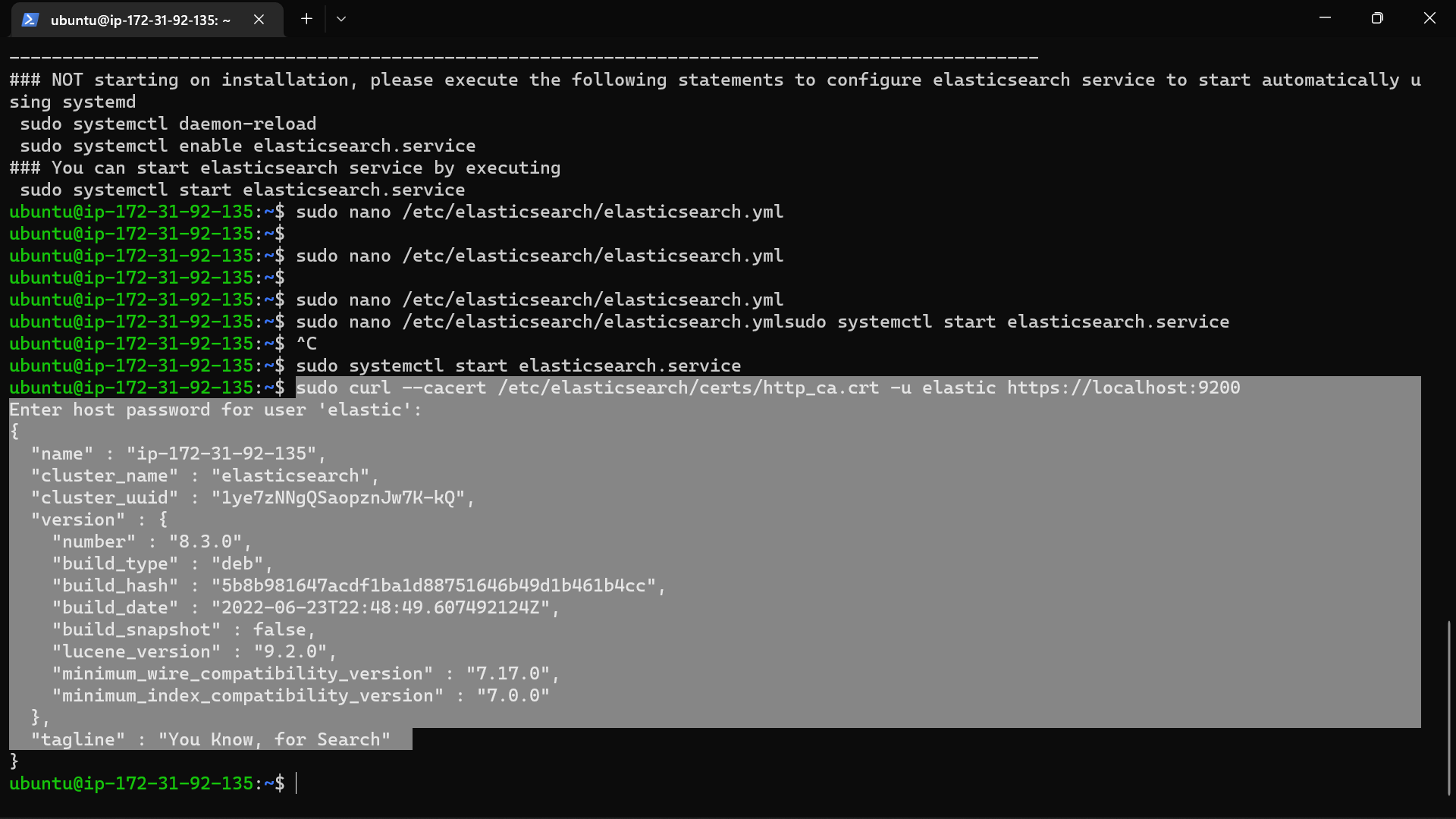


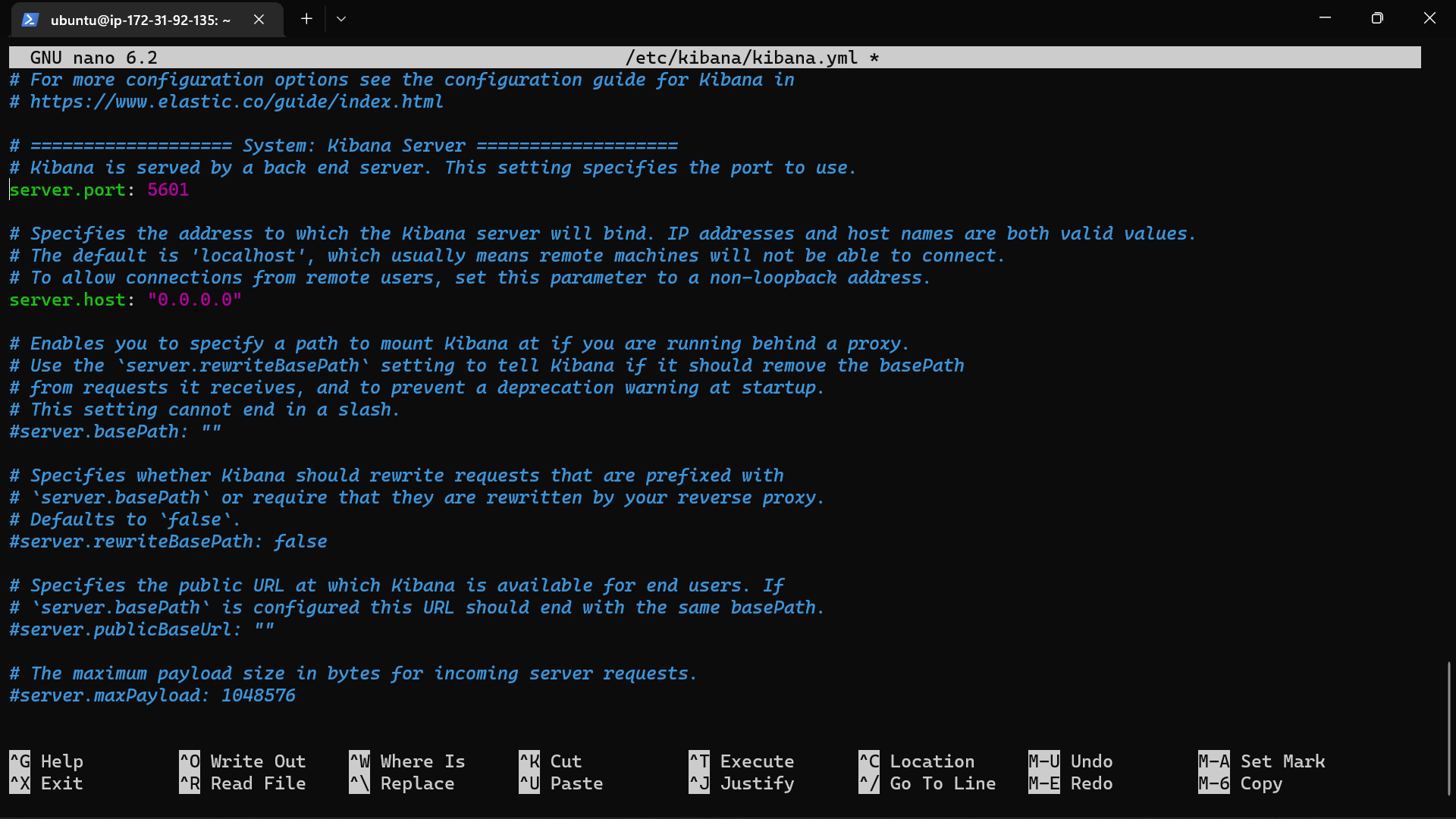


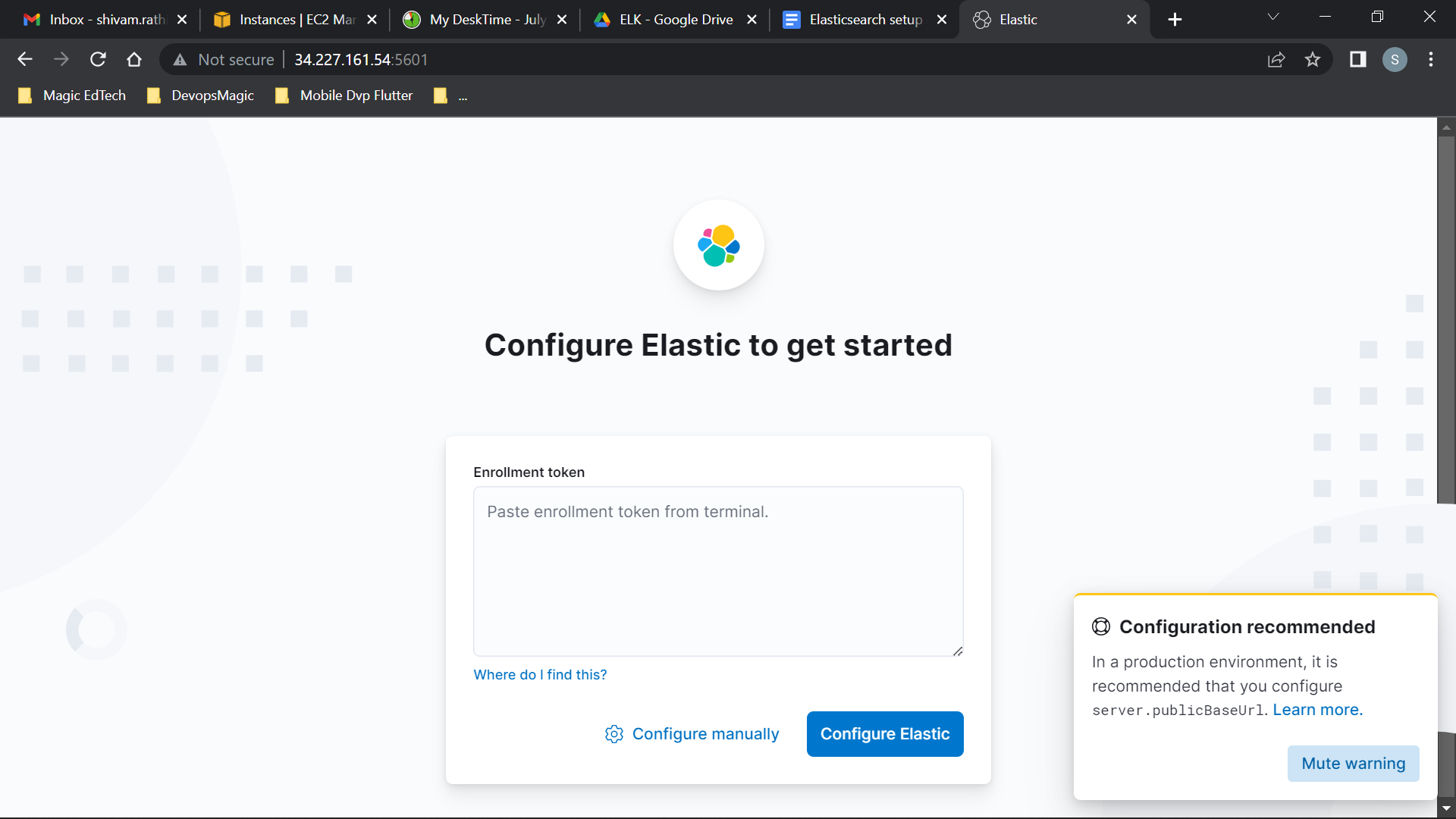


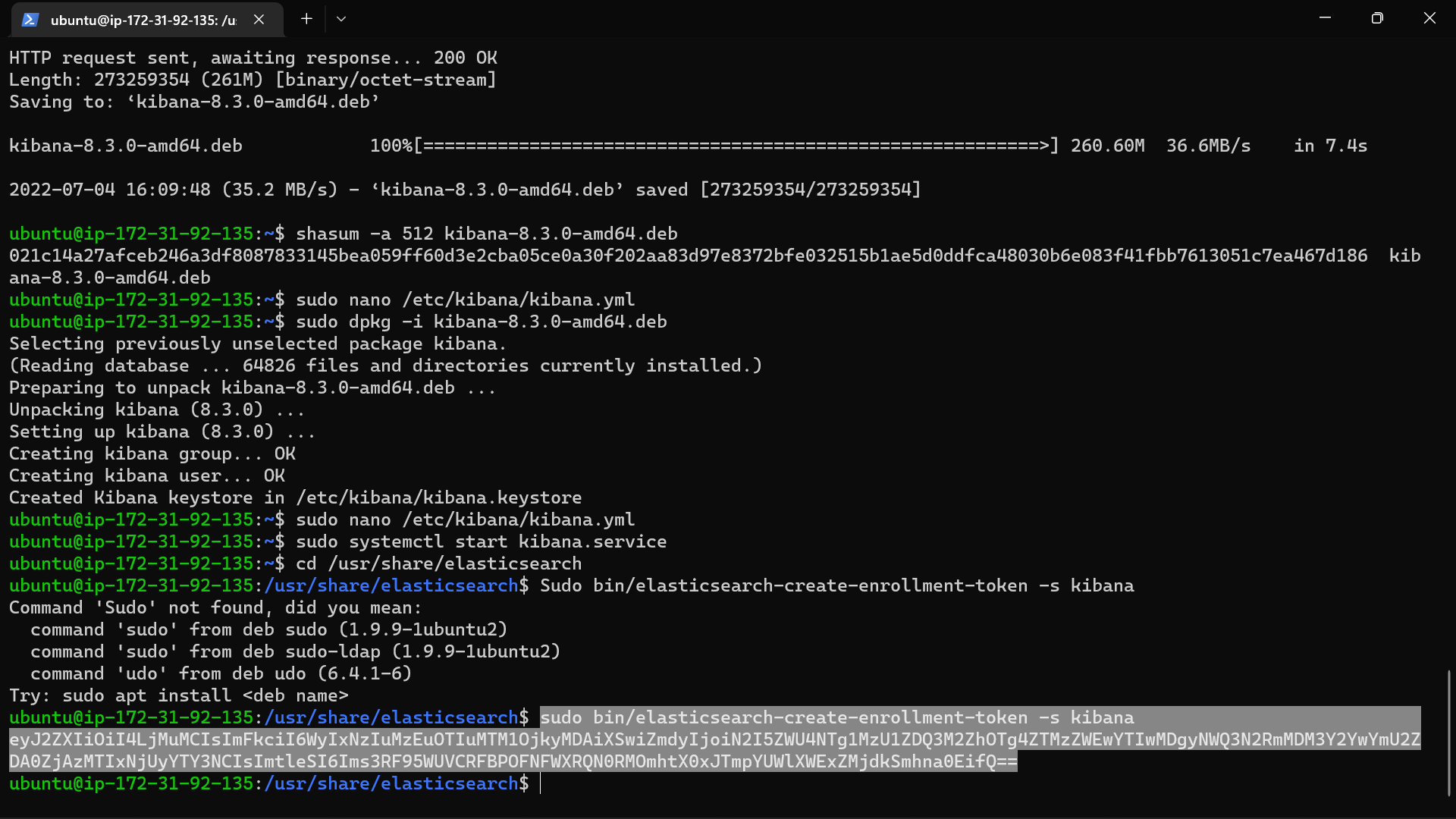


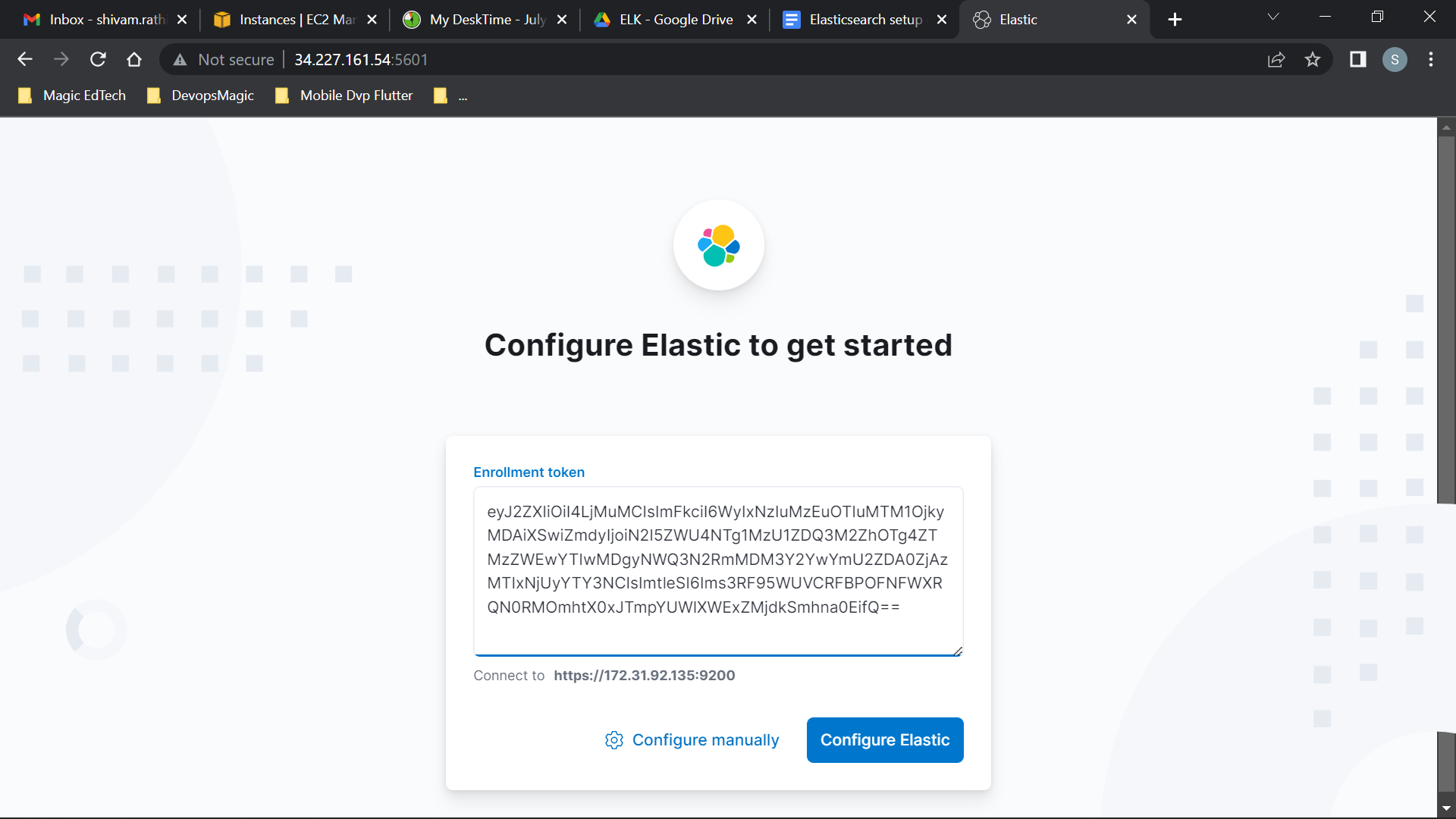


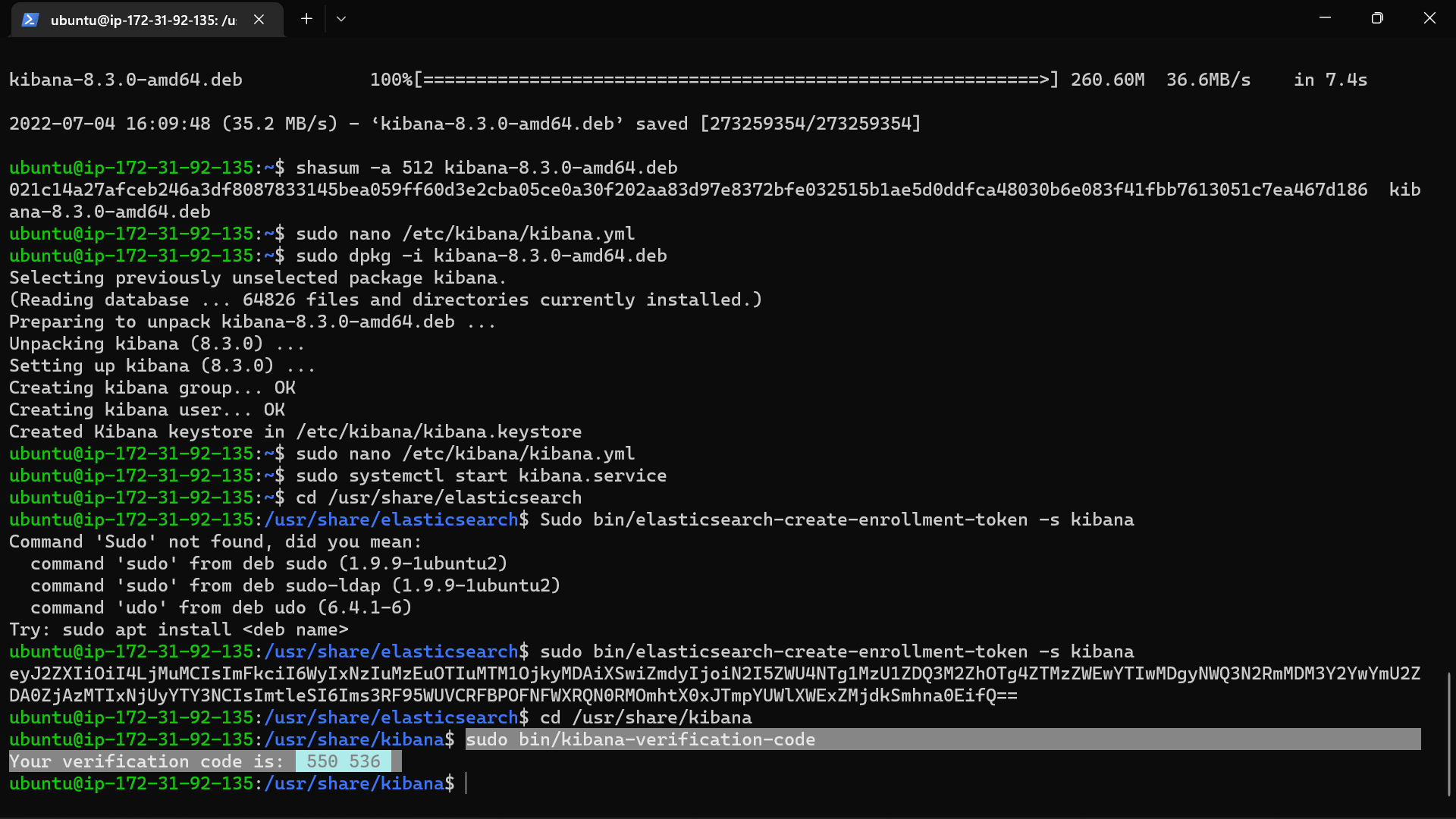


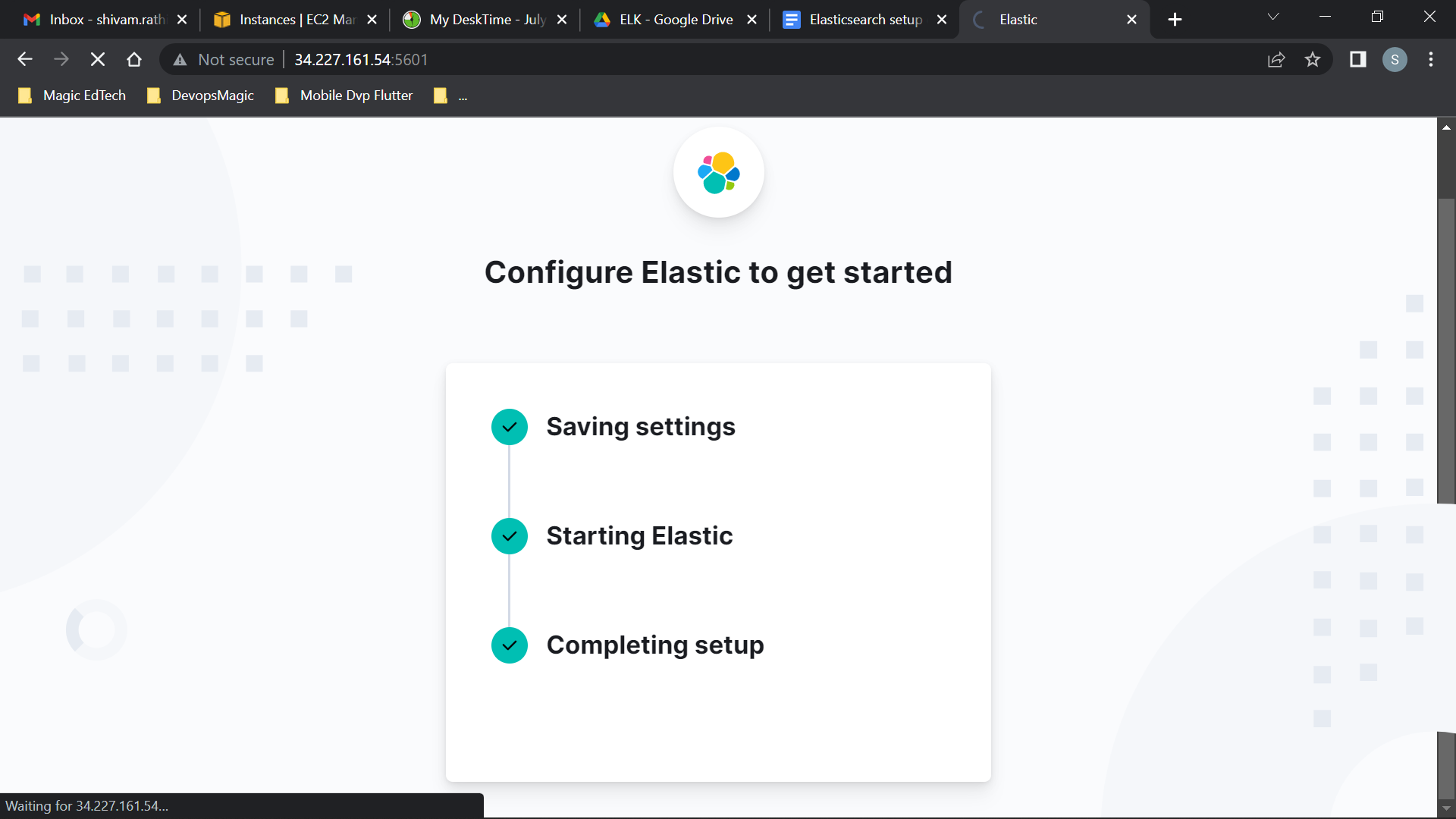


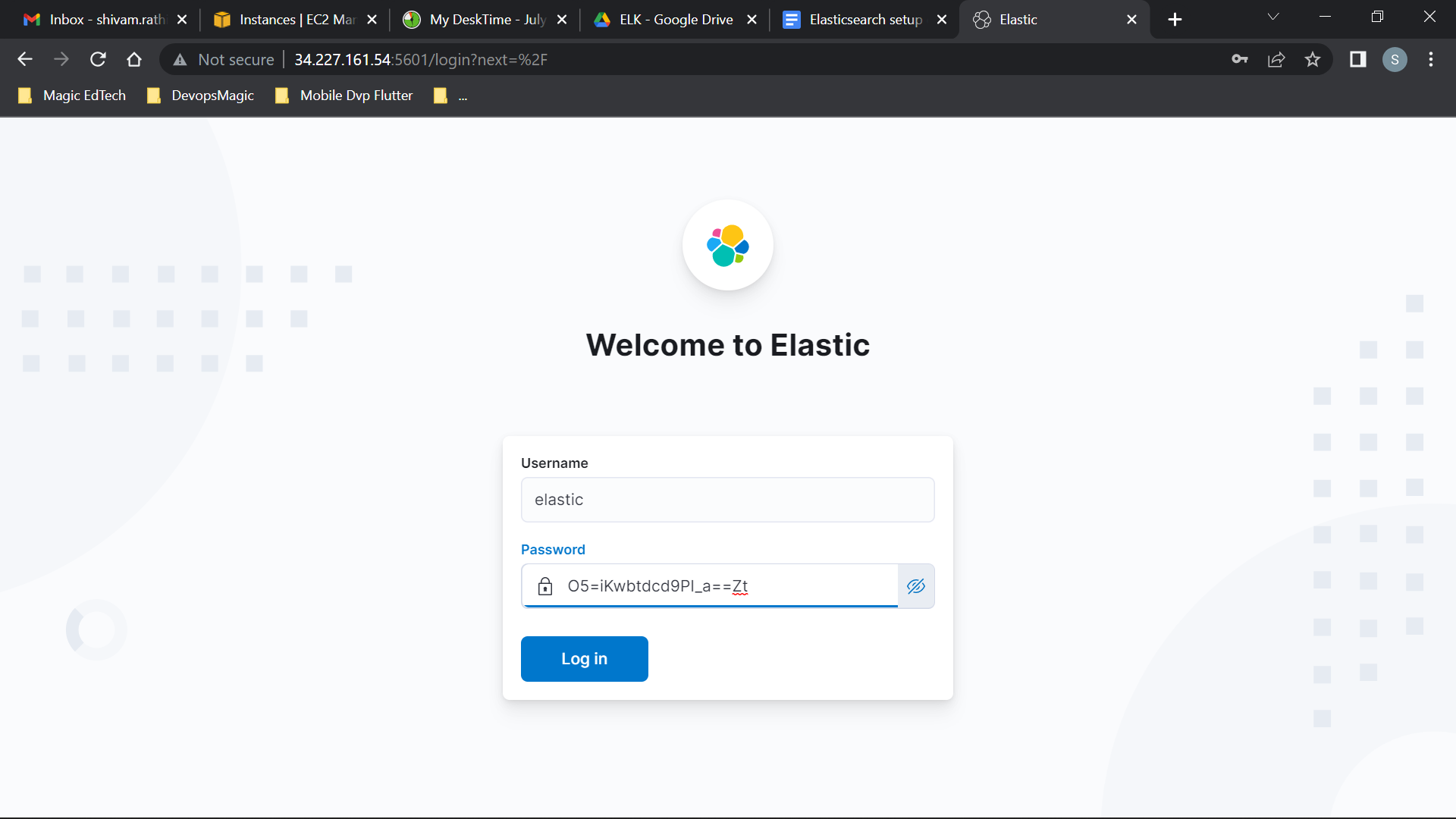












\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* **Install Kibana and Elasticsearch on DOCKER→**

docker network create elastic

docker run -d --name elasticsearch --net elastic -p 9200:9200 -p 9300:9300 -e "discovery.type=single-node" elasticsearch:7.12.1

docker run -d --name kibana --net elastic -p 5601:5601 kibana:7.12.1

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<https://levelup.gitconnected.com/how-to-run-elasticsearch-8-on-docker-for-local-development-401fd3fff829>  
  
version: "3.9"

services:

elasticsearch:

image: elasticsearch:8.2.2

container\_name: elastic

environment:

- discovery.type=single-node

- ES\_JAVA\_OPTS=-Xms1g -Xmx1g

- xpack.security.enabled=false

volumes:

- es\_data:/usr/share/elasticsearch/data

ports:

- target: 9200

published: 9200

networks:

- elastic

kibana:

image: kibana:8.2.2

container\_name: kibana

ports:

- target: 5601

published: 5601

depends\_on:

- elasticsearch

networks:

- elastic

volumes:

es\_data:

driver: local

networks:

elastic:

name: elastic

driver: bridge