**Elasticsearch APM with fleet and elastic-agent**

https://www.youtube.com/watch?v=UHQrOdwUg68&t=857s

https://www.elastic.co/guide/en/elasticsearch/reference/current/rpm.html

<https://www.elastic.co/guide/en/fleet/8.11/add-fleet-server-on-prem.html>

--set on each host almalinux 9

[root@elk ~]# hostnamectl set-hostname elk.kibana.com

[root@elk ~]# hostnamectl set-hostname fleet.elk.com

[root@elk ~]# hostnamectl set-hostname agent.elk.com

#####Elastic\_Kibana#####

--on elk node

[root@elk ~]# cat /etc/hosts

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

192.168.0.103 elk.kibana.com elk

192.168.0.106 fleet.elk.com fleet

192.168.0.107 agent.elk.com agent

[root@elk elk\_stack]# dnf install telnet wget net-tools curl java -y

[root@elk ~]# java -version

[root@elk ~]# mkdir /elk\_stack/

[root@elk ~]# cd /elk\_stack/

[root@elk elk\_stack]# wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.11.1-x86\_64.rpm

[root@elk elk\_stack]# rpm -ivh elasticsearch-8.11.1-x86\_64.rpm

[root@elk elk\_stack]# systemctl daemon-reload

[root@elk elk\_stack]# systemctl enable elasticsearch.service

[root@elk elk\_stack]# systemctl start elasticsearch.service

--kibana download from kibana-8.11.1-x86\_64.rpm https://www.elastic.co/downloads/kibana

[root@elk elk\_stack]# ll

-rw-r--r-- 1 root root 630601103 Nov 13 19:39 elasticsearch-8.11.1-x86\_64.rpm

-rw-r--r-- 1 root root 317639847 Nov 19 16:23 kibana-8.11.1-x86\_64.rpm

[root@elk elk\_stack]# rpm -ivh kibana-8.11.1-x86\_64.rpm

[root@elk elk\_stack]# vi /etc/kibana/kibana.yml

server.port: 5601

server.host: "192.168.0.103"

[root@elk elk\_stack]# systemctl enable kibana

[root@elk elk\_stack]# systemctl start kibana

[root@elk elk\_stack]# /usr/share/elasticsearch/bin/elasticsearch-reset-password -u kibana\_system

This tool will reset the password of the [kibana\_system] user to an autogenerated value.

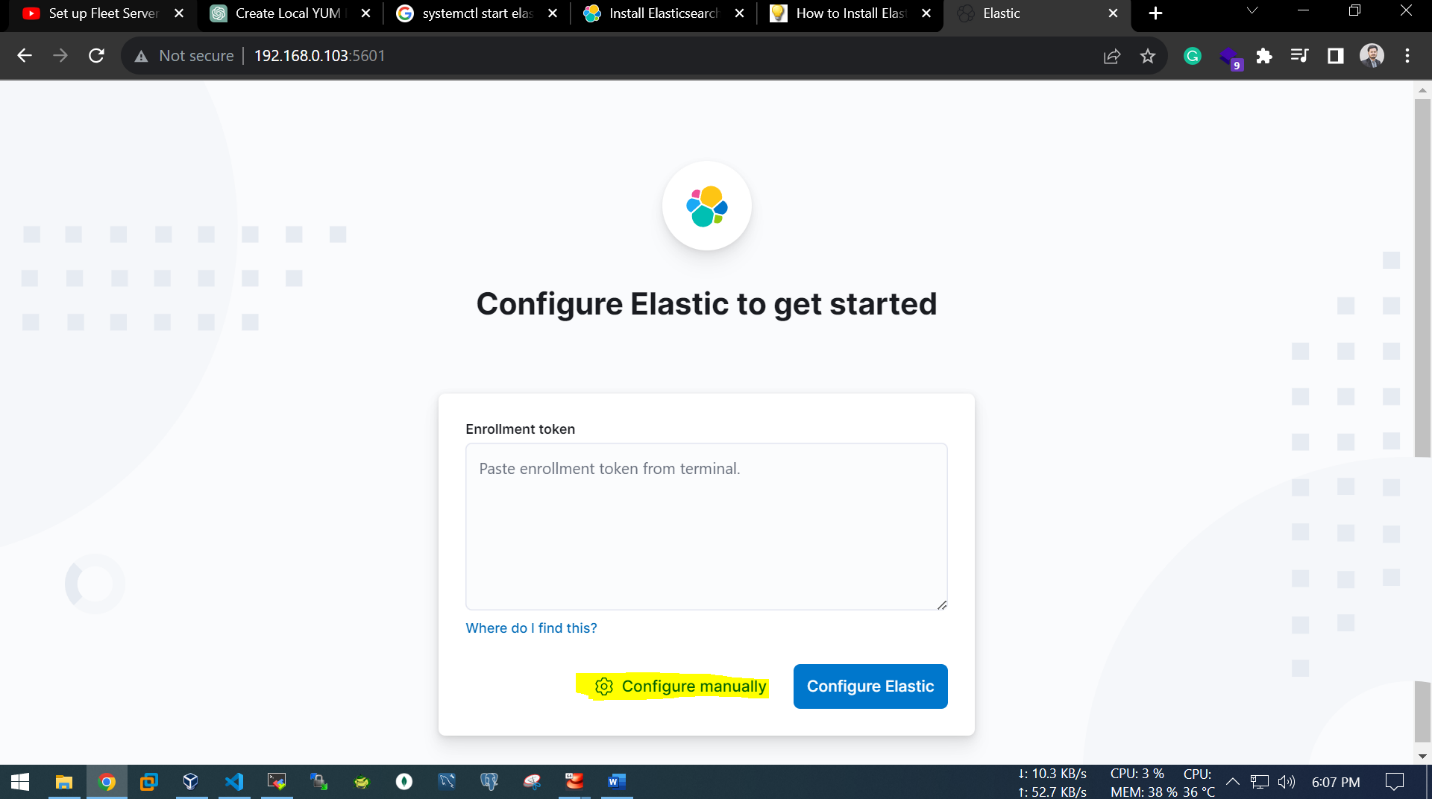
The password will be printed in the console.

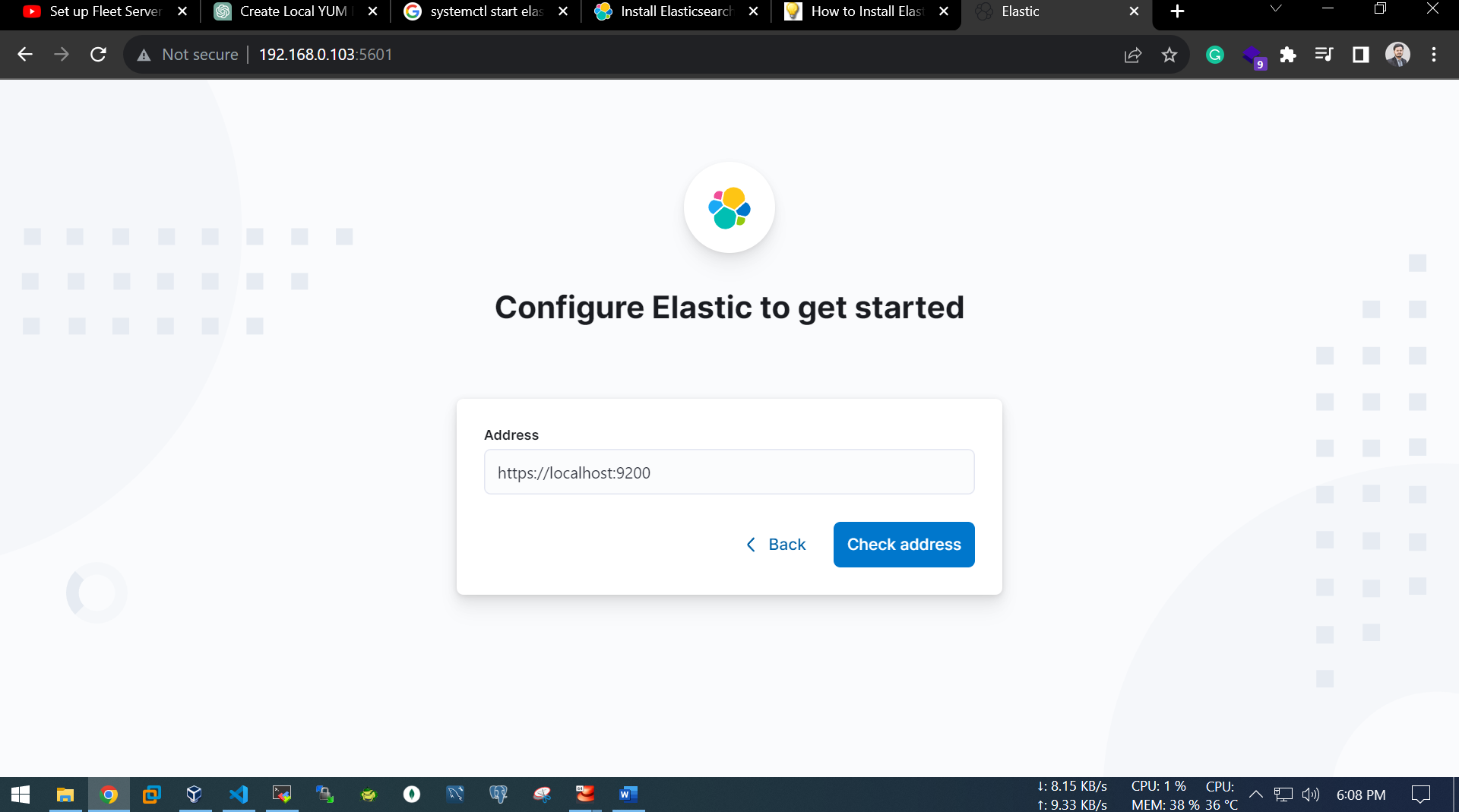
Please confirm that you would like to continue [y/N]y

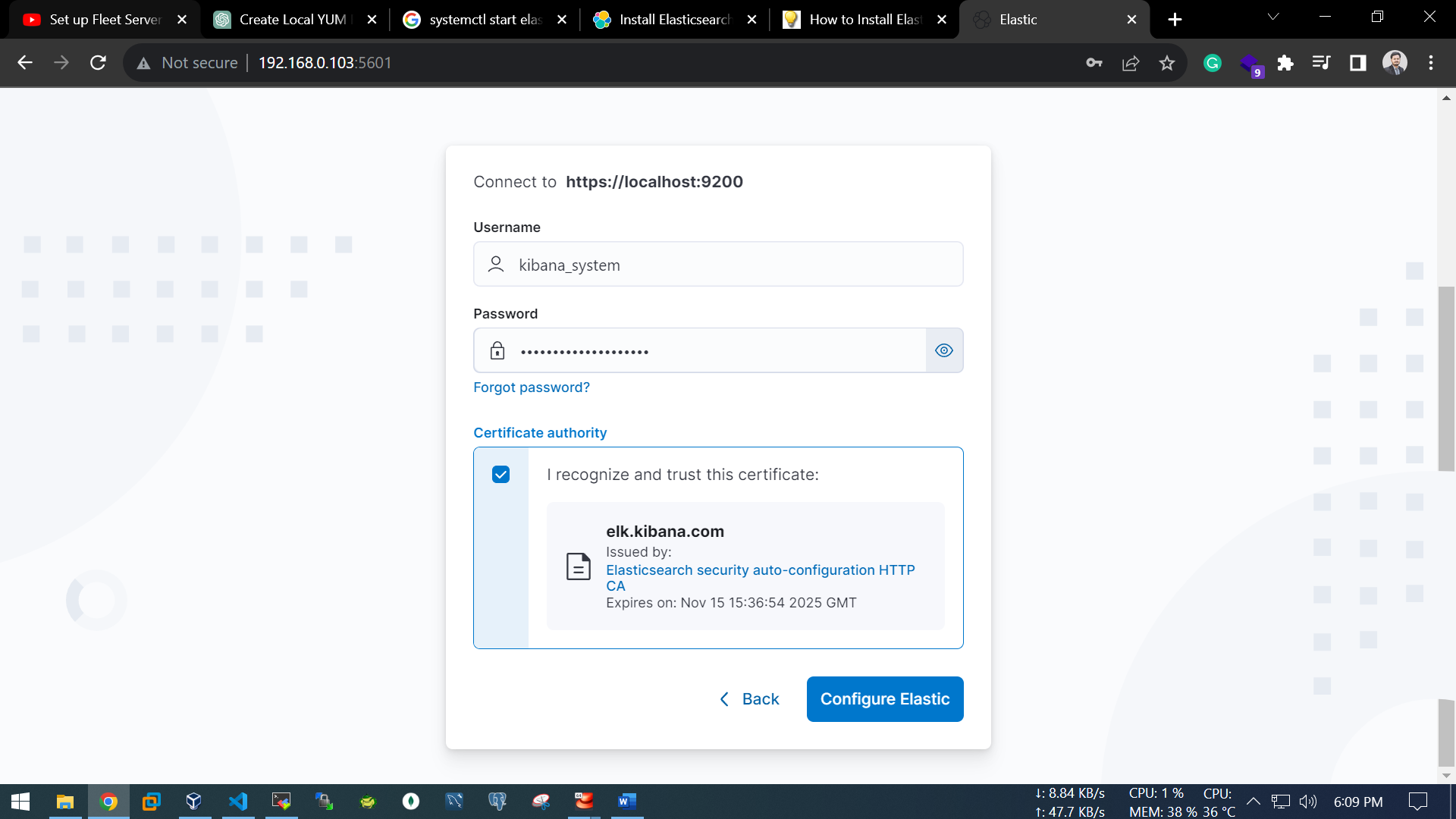
Password for the [kibana\_system] user successfully reset.

New value: xKWz4CnLkUvngQ9n+yPl

[root@elk elk\_stack]#

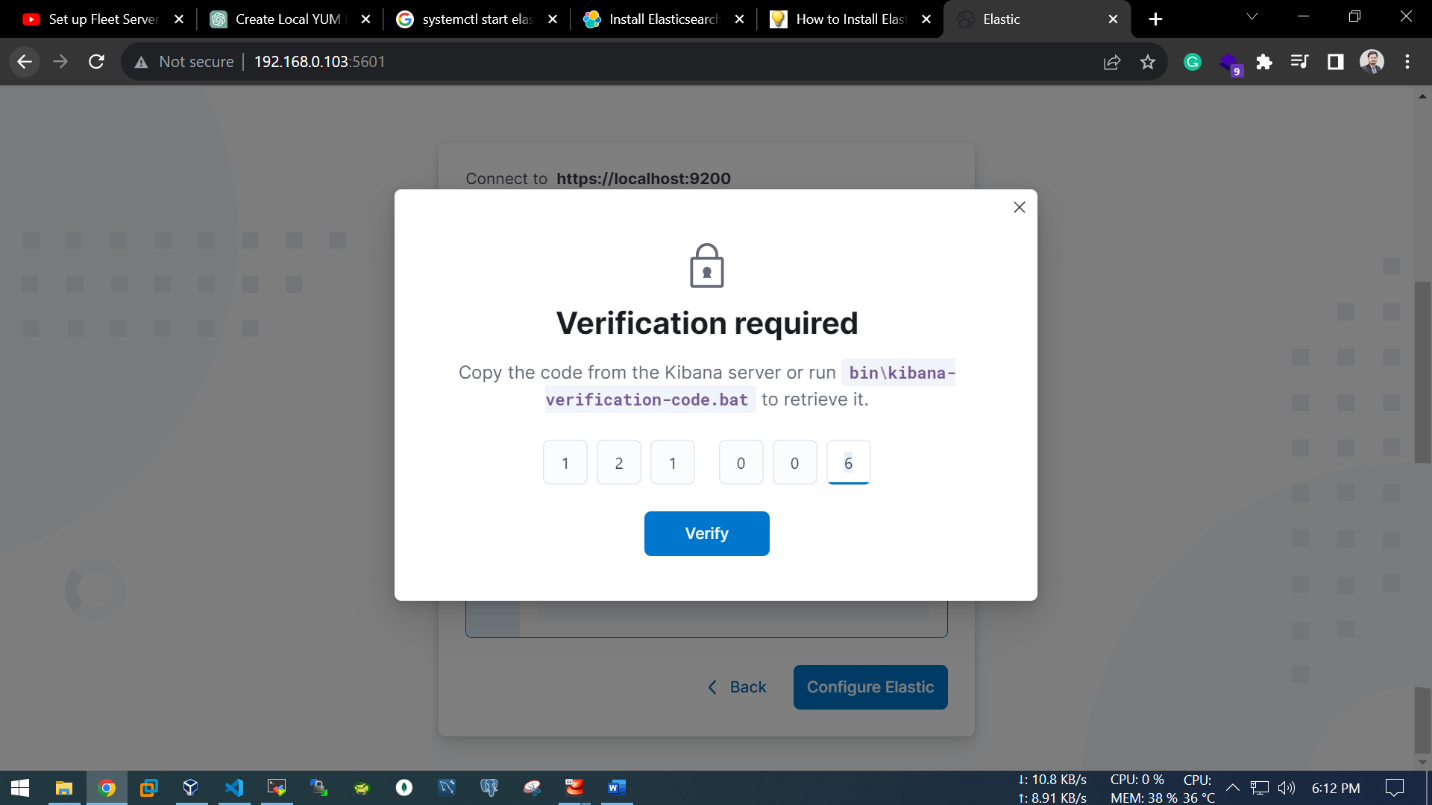






[root@elk elk\_stack]# /usr/share/kibana/bin/kibana-verification-code

Your verification code is: 121 006

[root@elk elk\_stack]#

[root@elk elk\_stack]# /usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic

This tool will reset the password of the [elastic] user to an autogenerated value.

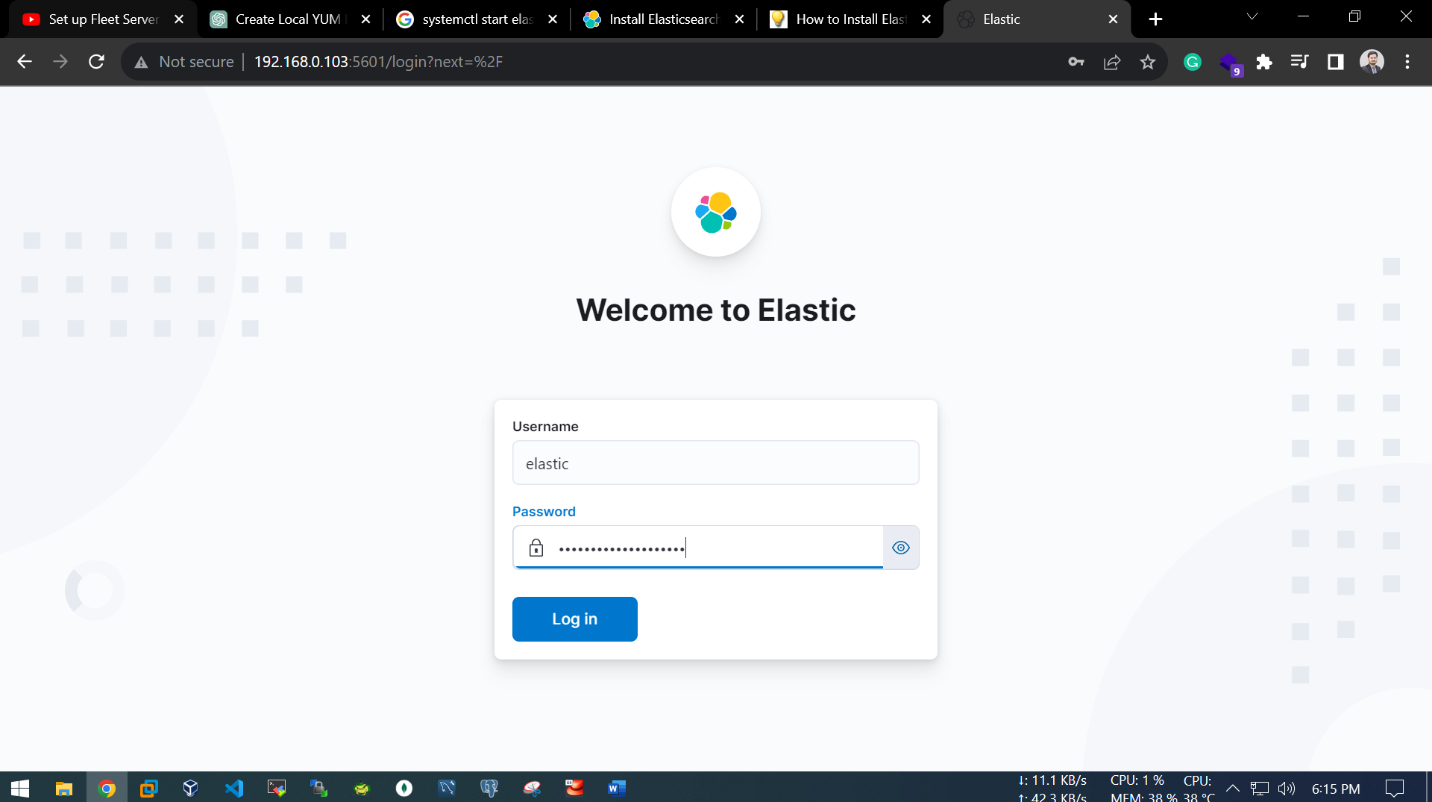
The password will be printed in the console.

Please confirm that you would like to continue [y/N]y

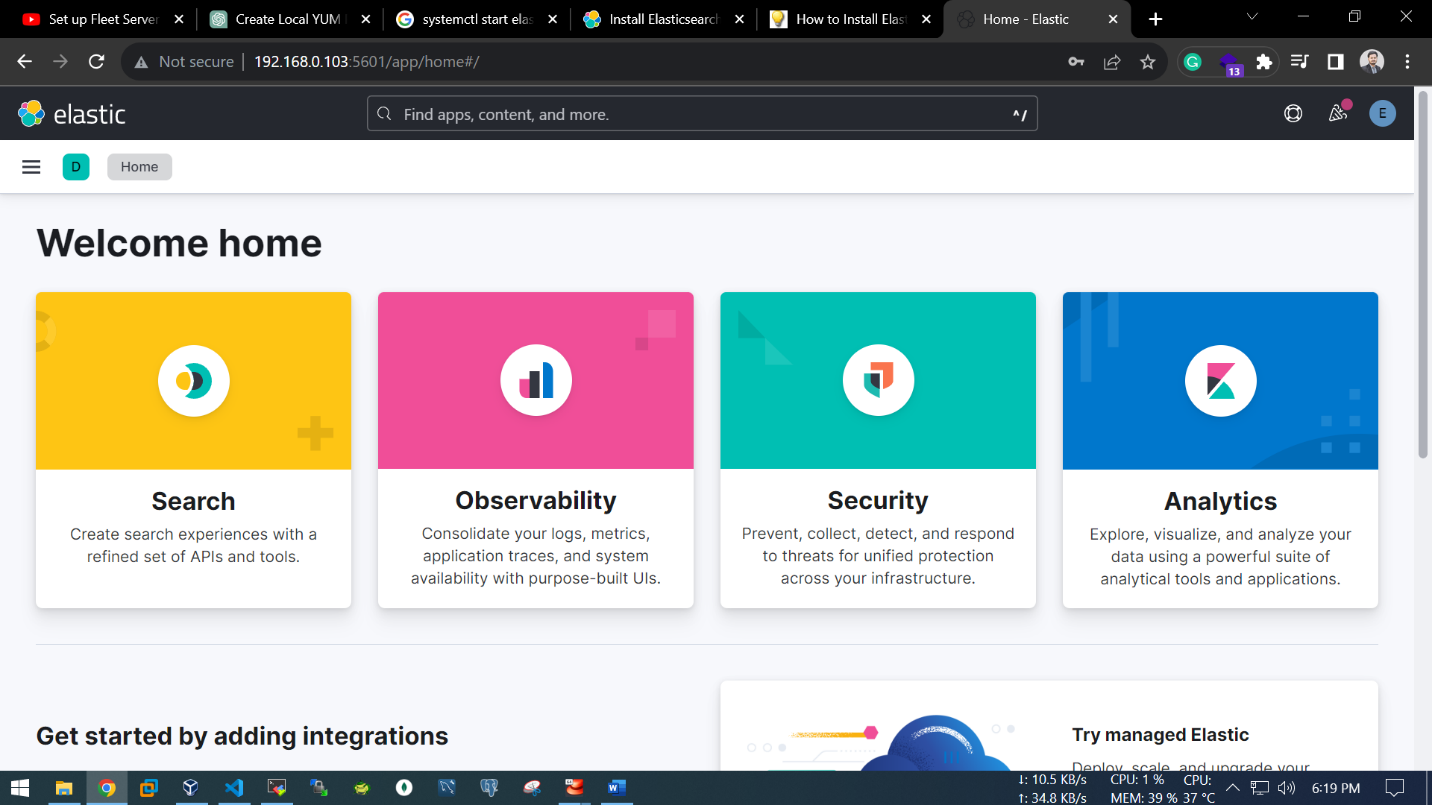
Password for the [elastic] user successfully reset.

New value: +QYvYK5vWZ5g7PJ\_HSzY

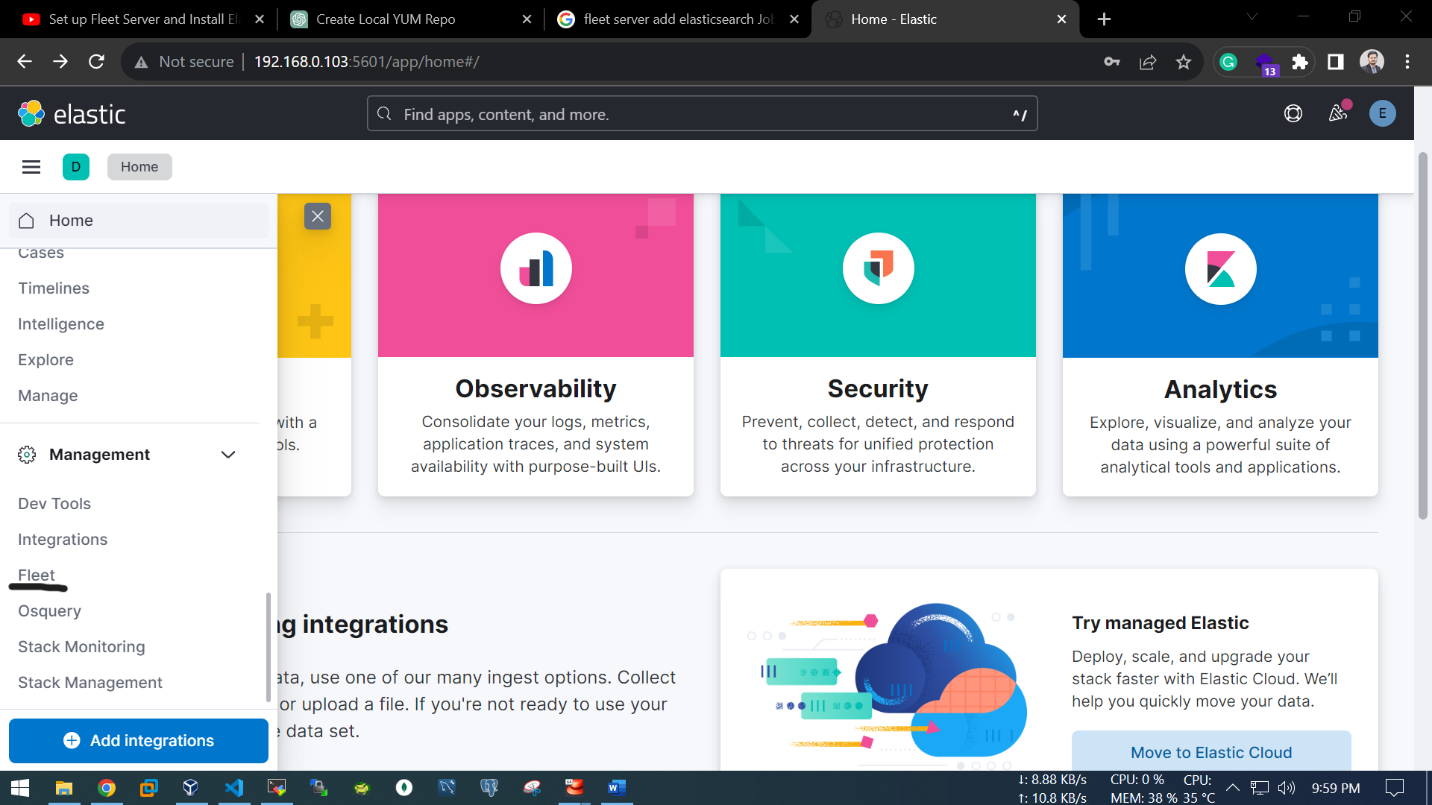
[root@elk elk\_stack]#

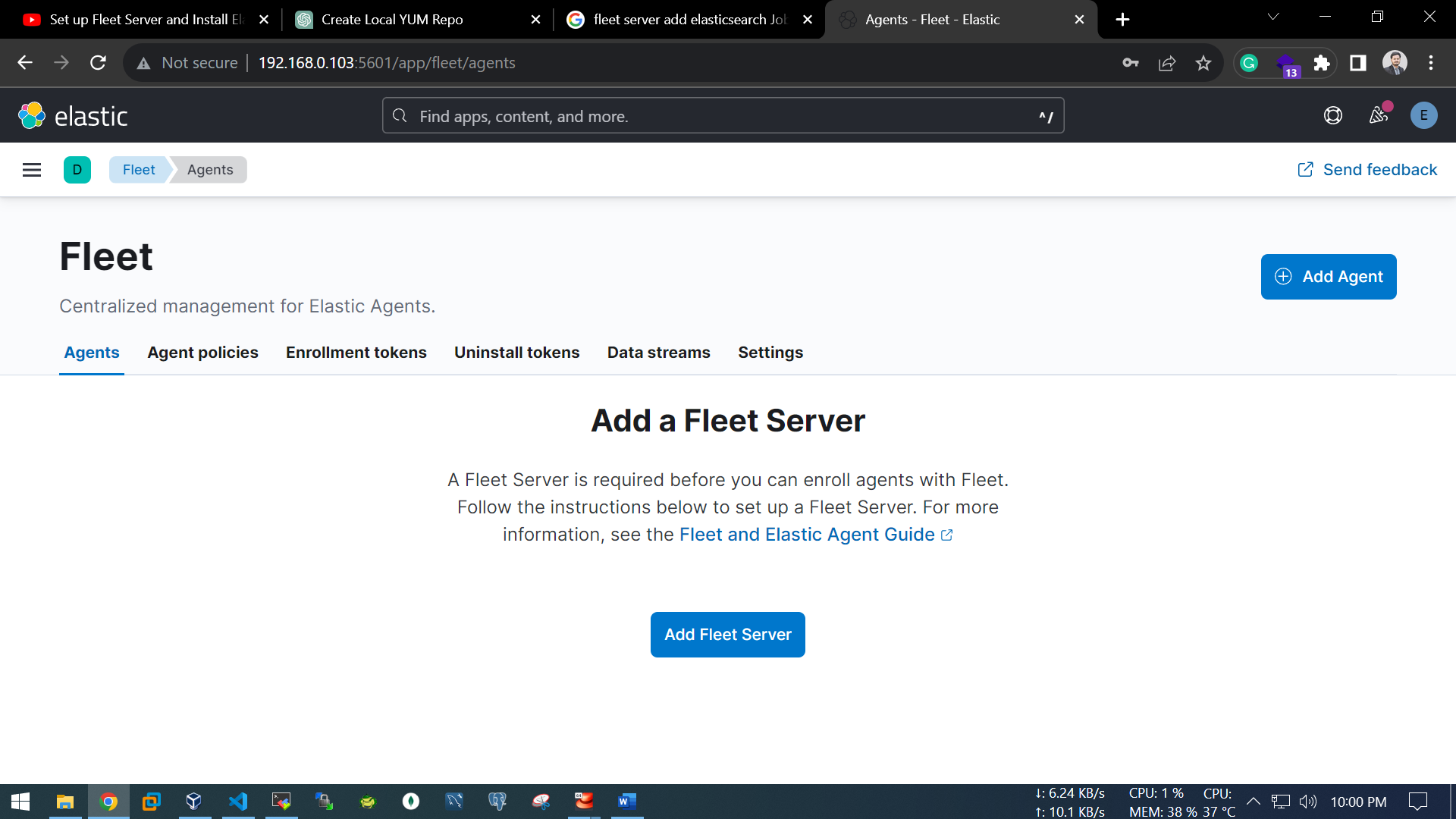


After this, click at “my own”.

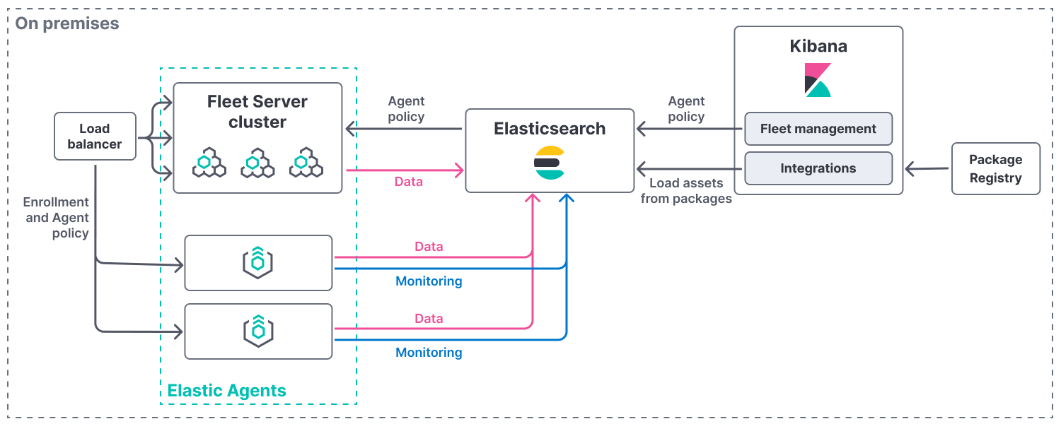


#Fleet Server add

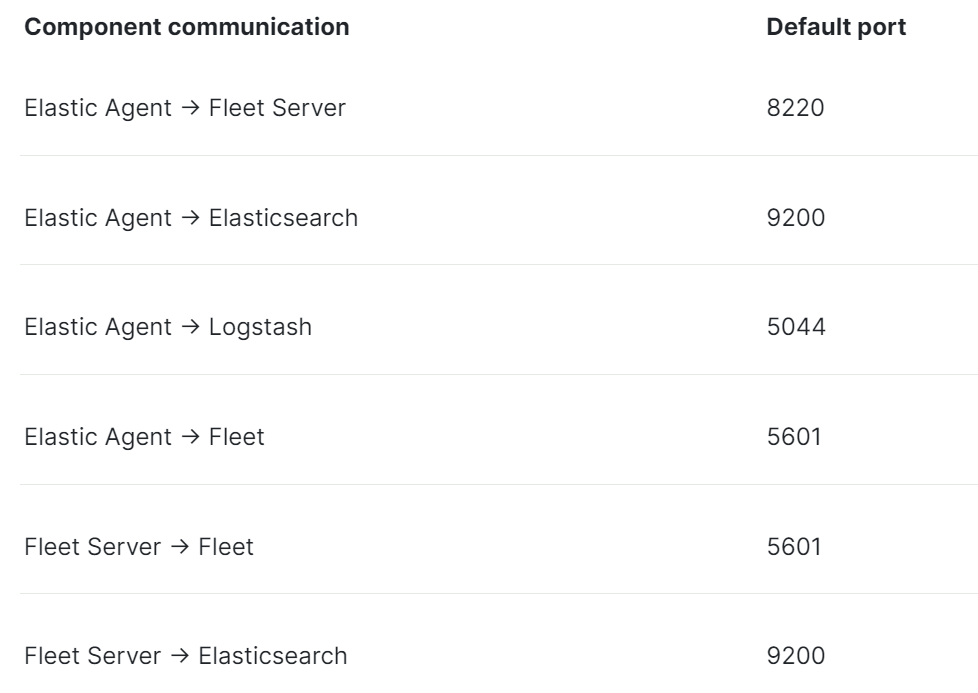


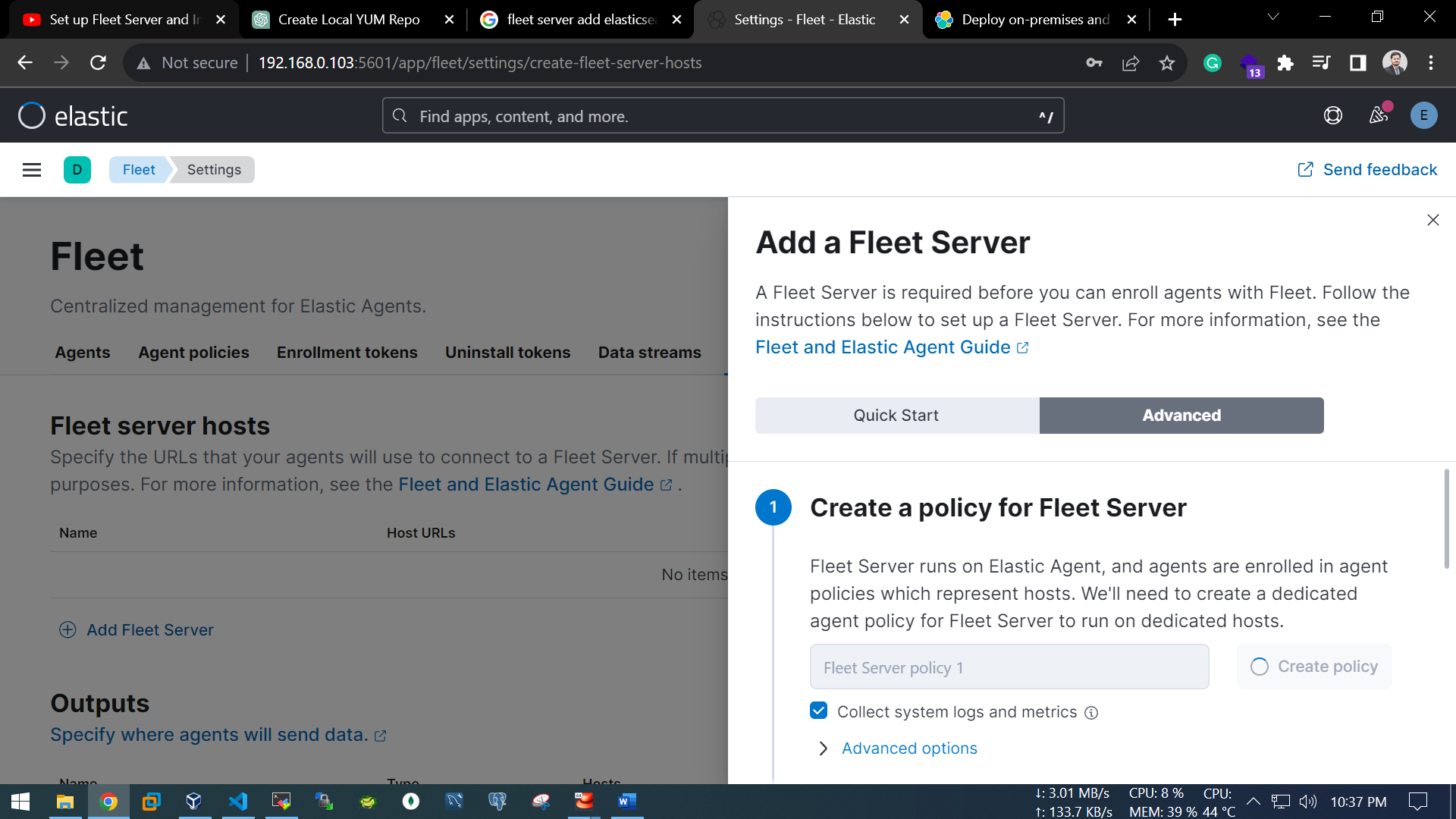
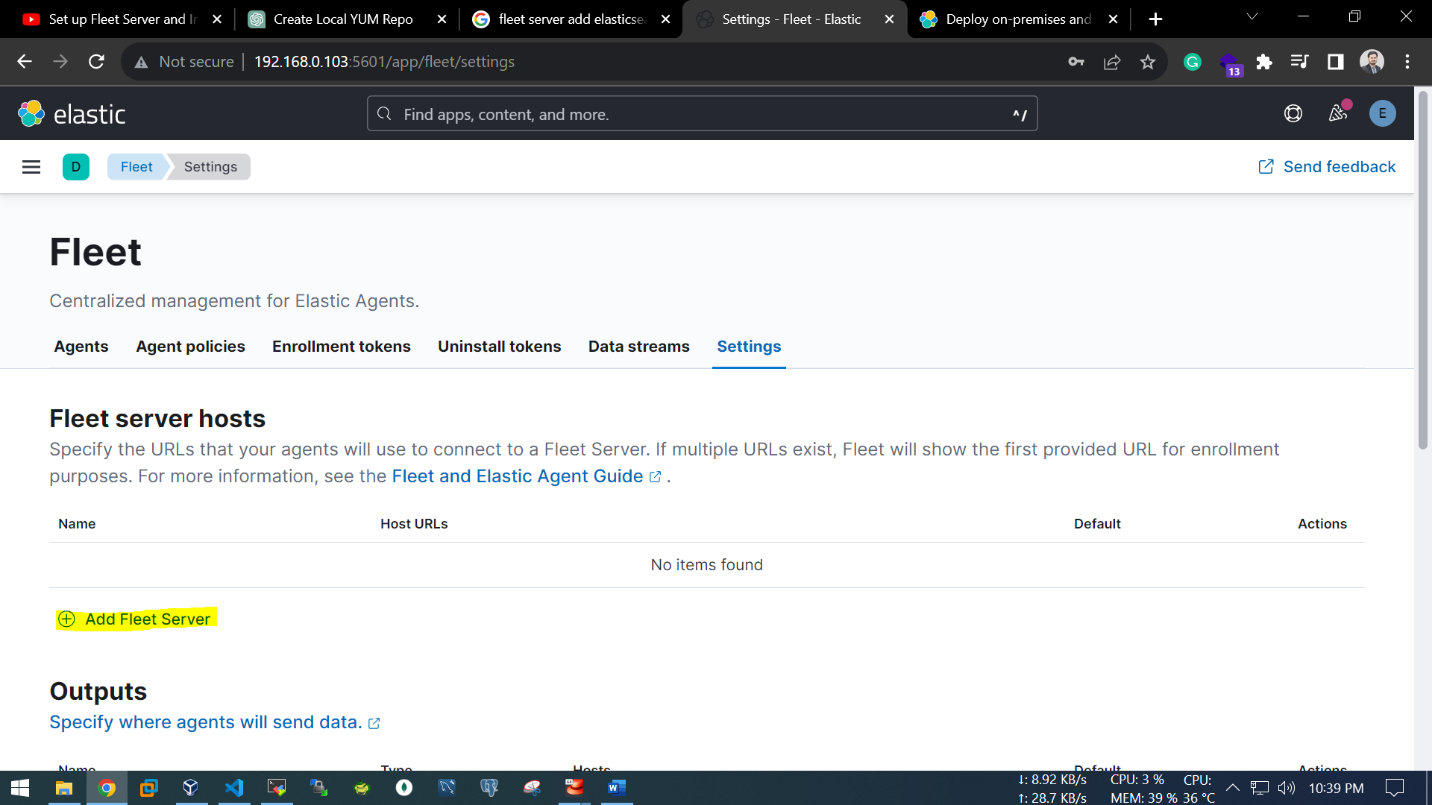


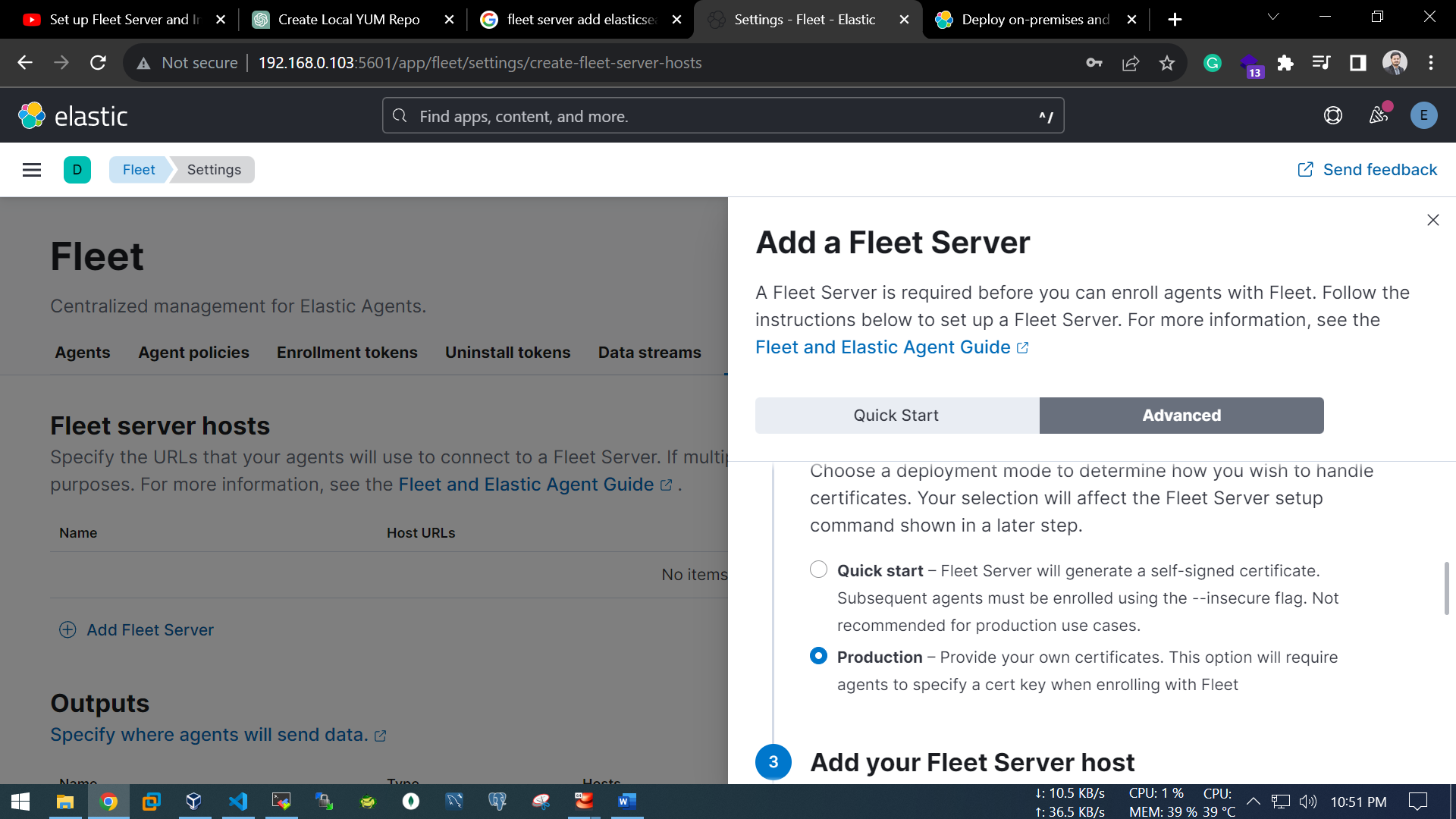
Model of APM:



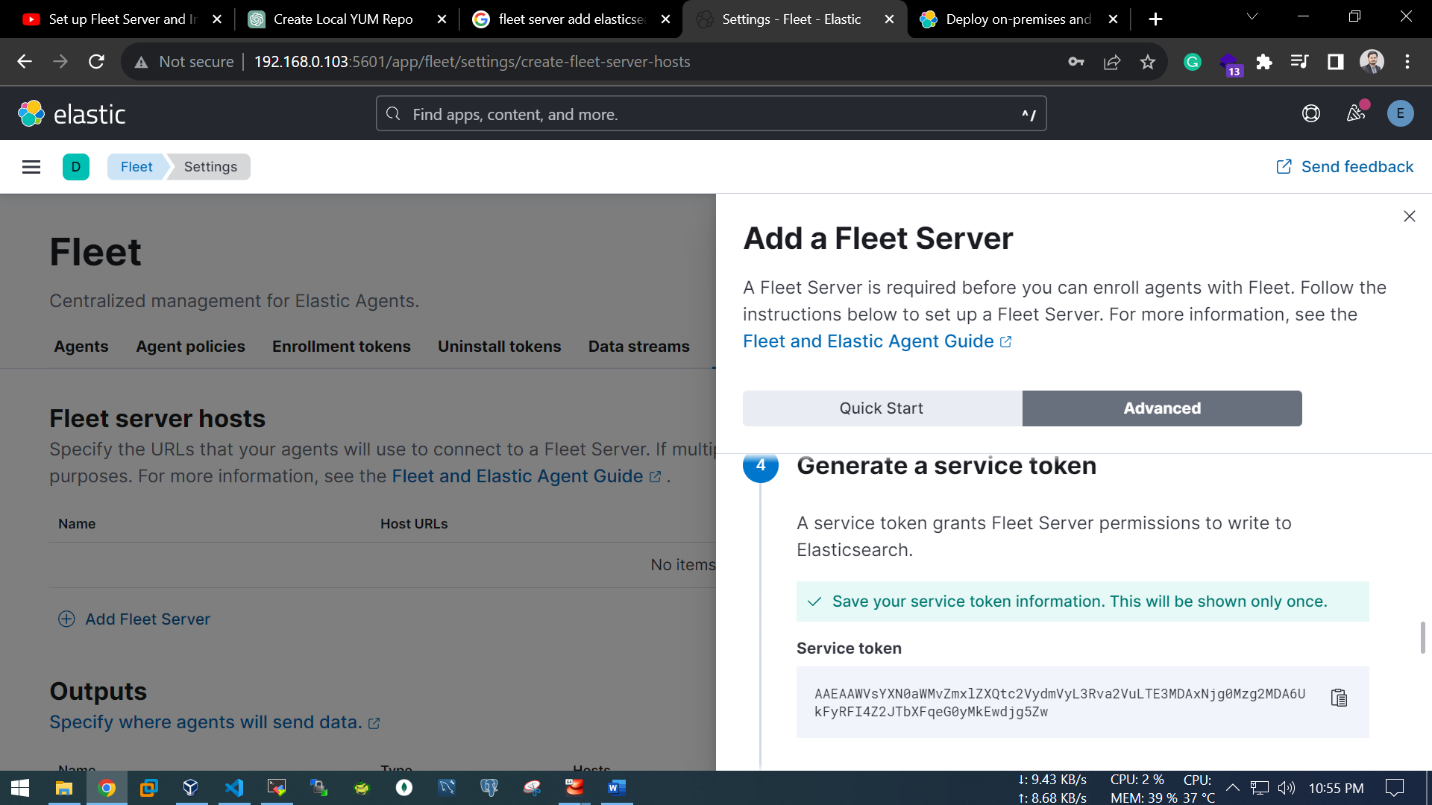
Port Mapping:





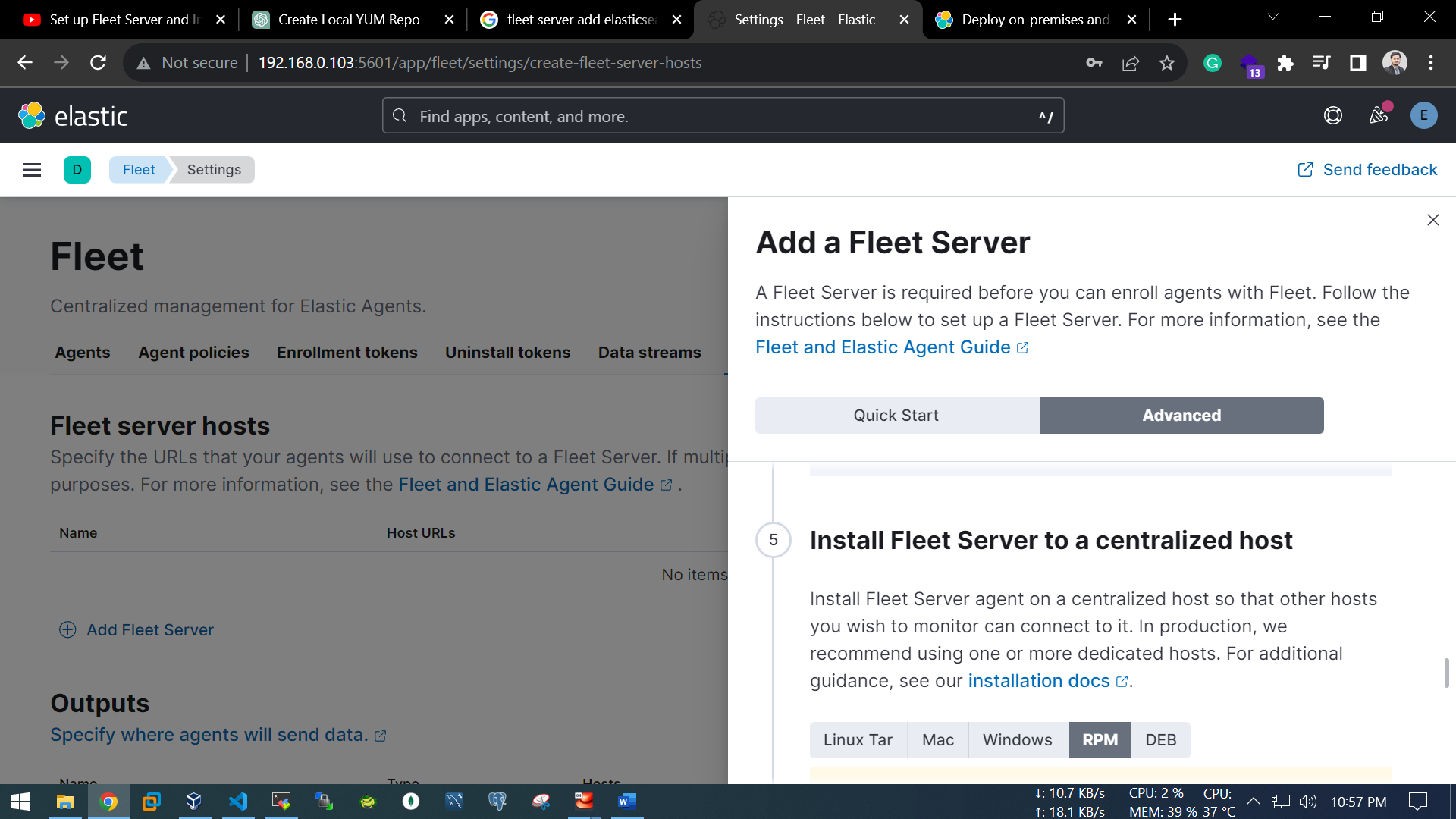


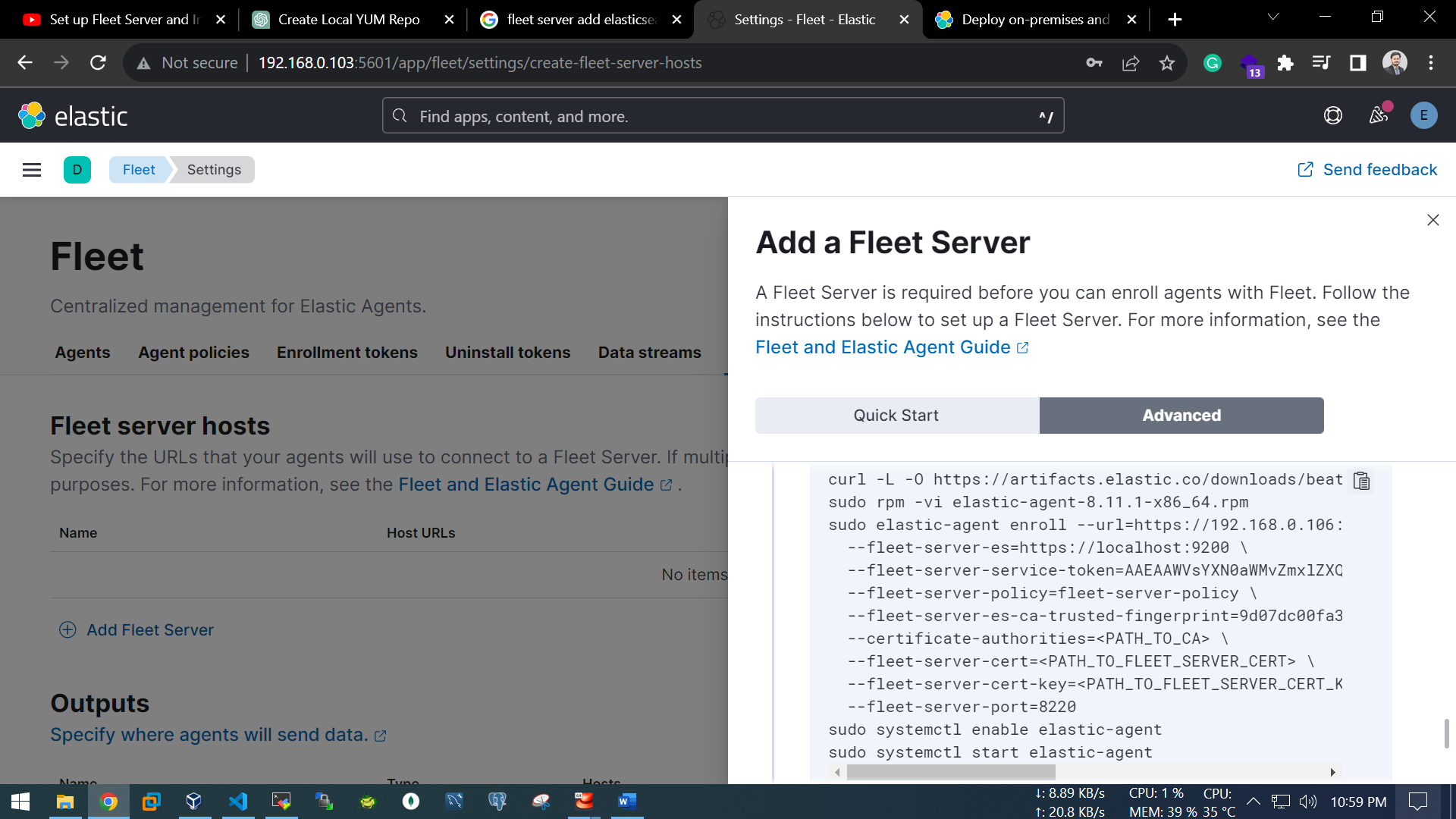




--Generate a service token

AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE3MDA0MTU4ODU1ODg6MWNqNk5rMkVTT0dUMmEwdWQyODRJUQ





--set on fleet OS

[root@fleet ~]# mkdir /root/ca

[root@fleet ~]# cd /root/ca

[root@elk elk\_stack]# mkdir /elk\_stack/ca

[root@elk elk\_stack]# cd /elk\_stack/ca

[root@elk ca]# dnf install openssl -y

[root@elk ca]# openssl genpkey -algorithm RSA -out ca.key

[root@elk ca]# openssl req -x509 -new -key ca.key -out ca.crt -days 36500

Country Name (2 letter code) [XX]:BD

State or Province Name (full name) []:Dhaka

Locality Name (eg, city) [Default City]:Dhaka

Organization Name (eg, company) [Default Company Ltd]:ITCL

Organizational Unit Name (eg, section) []:DevOps

Common Name (eg, your name or your server's hostname) []:elk

Email Address []:ahosan@example.com

[root@elk ca]#

/usr/share/elasticsearch/bin/elasticsearch-certutil cert \

--name fleet-server \

--ca-cert /elk\_stack/ca/ca.crt \

--ca-key /elk\_stack/ca/ca.key \

--dns fleet.elk.com \

--ip 192.168.0.106 \

--pem

[root@elk ca]# ll /usr/share/elasticsearch/certificate-bundle.zip

-rw------- 1 root root 2698 Nov 19 23:55 /usr/share/elasticsearch/certificate-bundle.zip

[root@elk ca]# mv /usr/share/elasticsearch/certificate-bundle.zip .

[root@elk ca]# ll

-rw-r--r-- 1 root root 1403 Nov 19 23:53 ca.crt

-rw------- 1 root root 1704 Nov 19 23:51 ca.key

-rw------- 1 root root 2698 Nov 19 23:55 certificate-bundle.zip

[root@elk ca]# dnf install unzip -y

[root@elk ca]# unzip -q certificate-bundle.zip

[root@elk ca]# cd fleet-server

[root@elk fleet-server]# ll

-rw-r--r-- 1 root root 1298 Nov 19 23:55 fleet-server.crt

-rw-r--r-- 1 root root 1675 Nov 19 23:55 fleet-server.key

[root@elk fleet-server]# pwd

/elk\_stack/ca/fleet-server

[root@elk fleet-server]# cd ..

[root@elk ca]# scp -r . root@192.168.0.106:/root/ca

########Fleet Server########

--Generate a service token

AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE3MDA0MTU4ODU1ODg6MWNqNk5rMkVTT0dUMmEwdWQyODRJUQ

[root@fleet fleet-server]# pwd

/root/ca/fleet-server

[root@fleet fleet-server]# ll

total 8

-rw-r--r-- 1 root root 1298 Nov 20 00:06 fleet-server.crt

-rw-r--r-- 1 root root 1675 Nov 20 00:06 fleet-server.key

[root@fleet fleet-server]#

curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.11.1-x86\_64.rpm

sudo rpm -vi elastic-agent-8.11.1-x86\_64.rpm

sudo elastic-agent enroll --url=https://192.168.0.106:8220 \

--fleet-server-es=https://192.168.0.103:9200 \

--fleet-server-service-token=AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE3MDA0MTU4ODU1ODg6MWNqNk5rMkVTT0dUMmEwdWQyODRJUQ \

--fleet-server-policy=fleet-server-policy \

--fleet-server-es-ca-trusted-fingerprint=9d07dc00fa36c52007e5569d68e27313cdd3a7e54f075b8f32ffed7d54df4c80 \

--certificate-authorities=/root/ca/ca.crt \

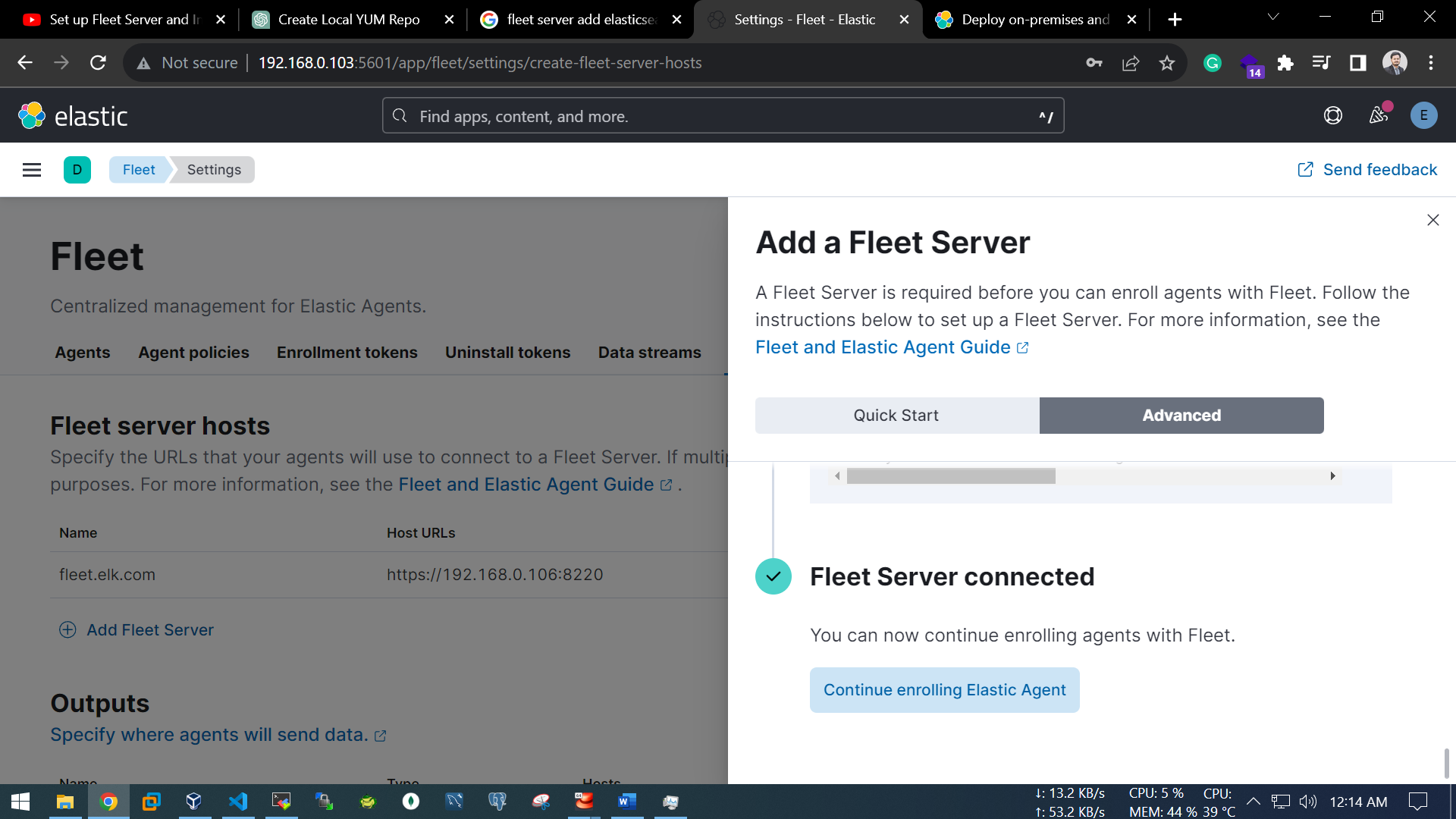
--fleet-server-cert=/root/ca/fleet-server/fleet-server.crt \

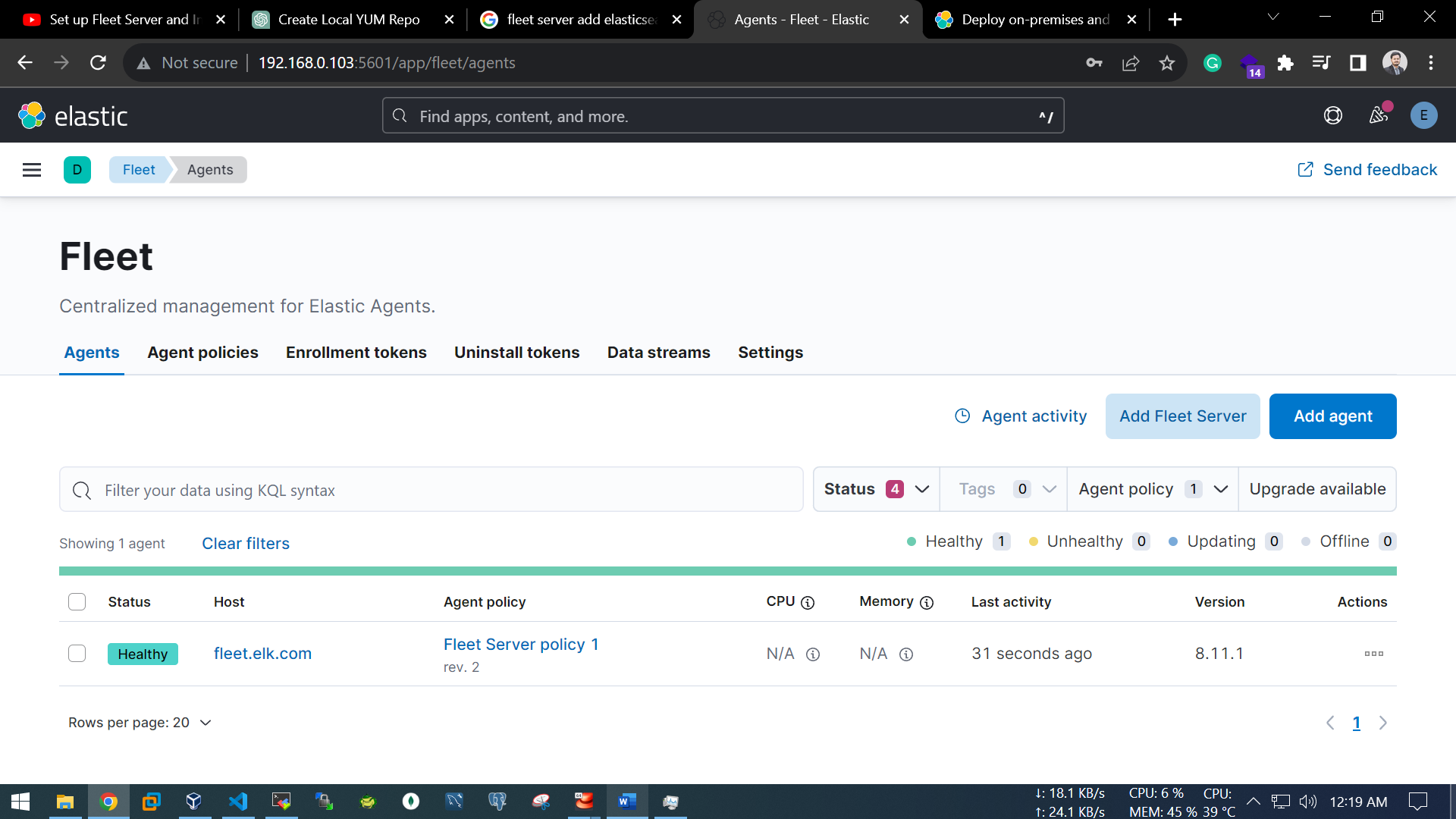
--fleet-server-cert-key=/root/ca/fleet-server/fleet-server.key \

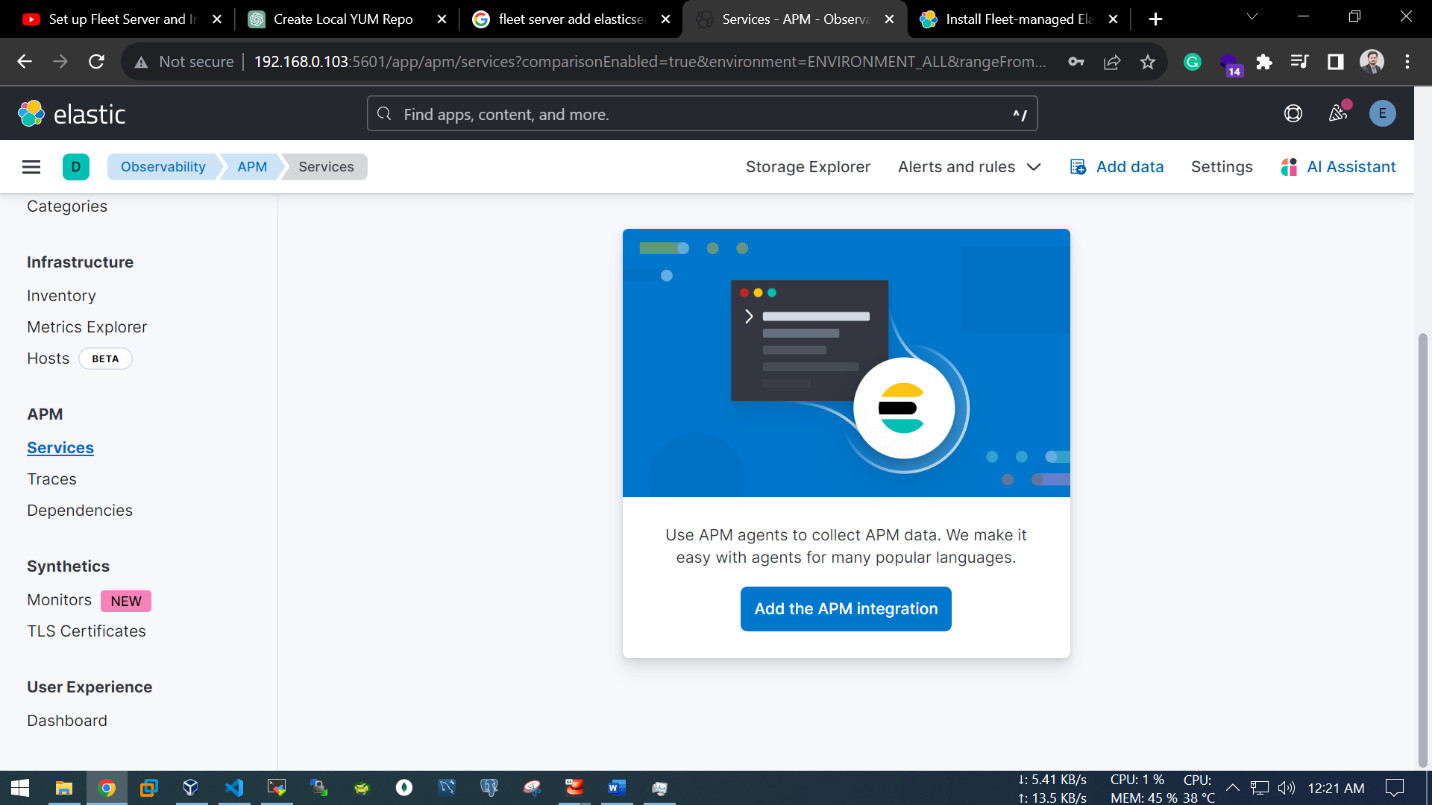
--fleet-server-port=8220

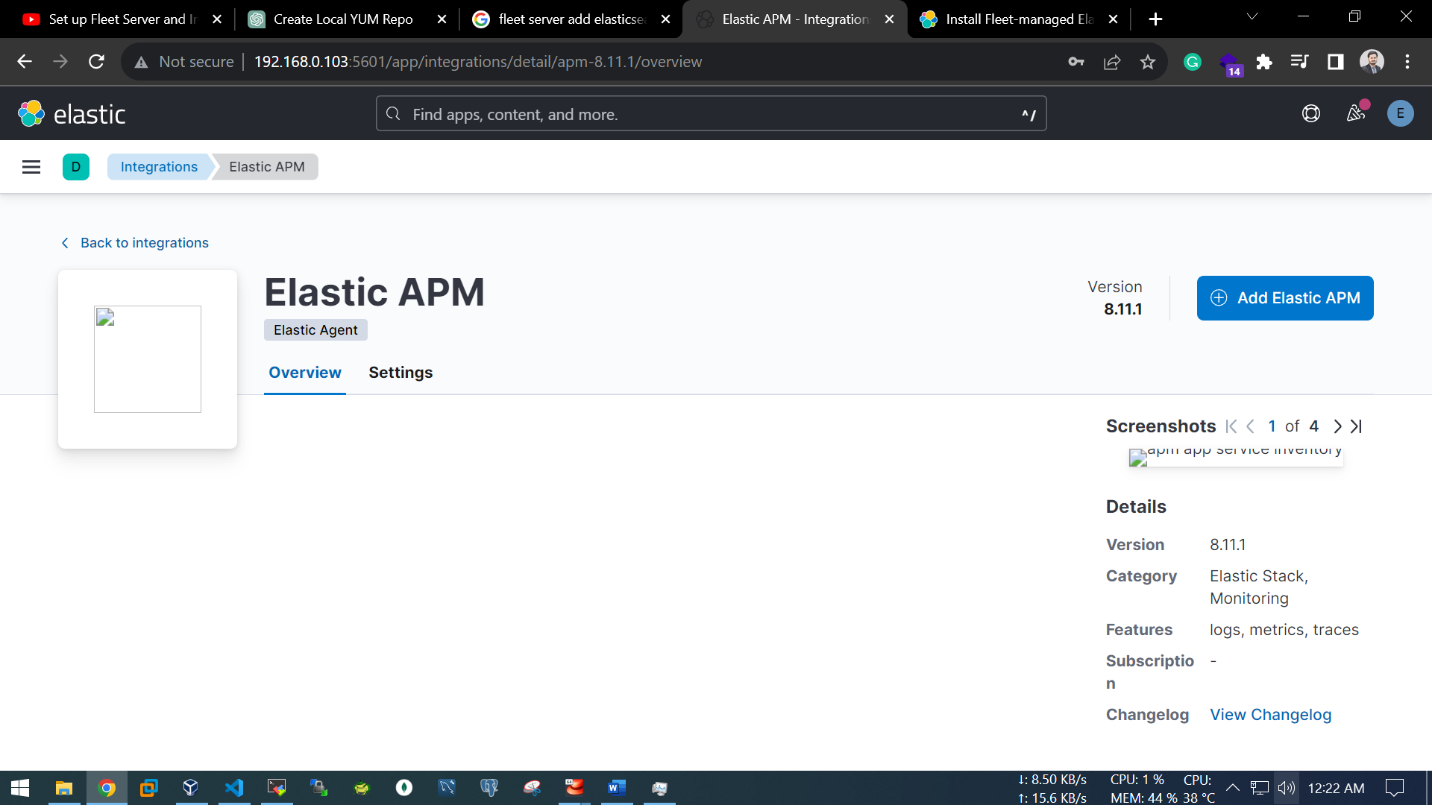
sudo systemctl enable elastic-agent

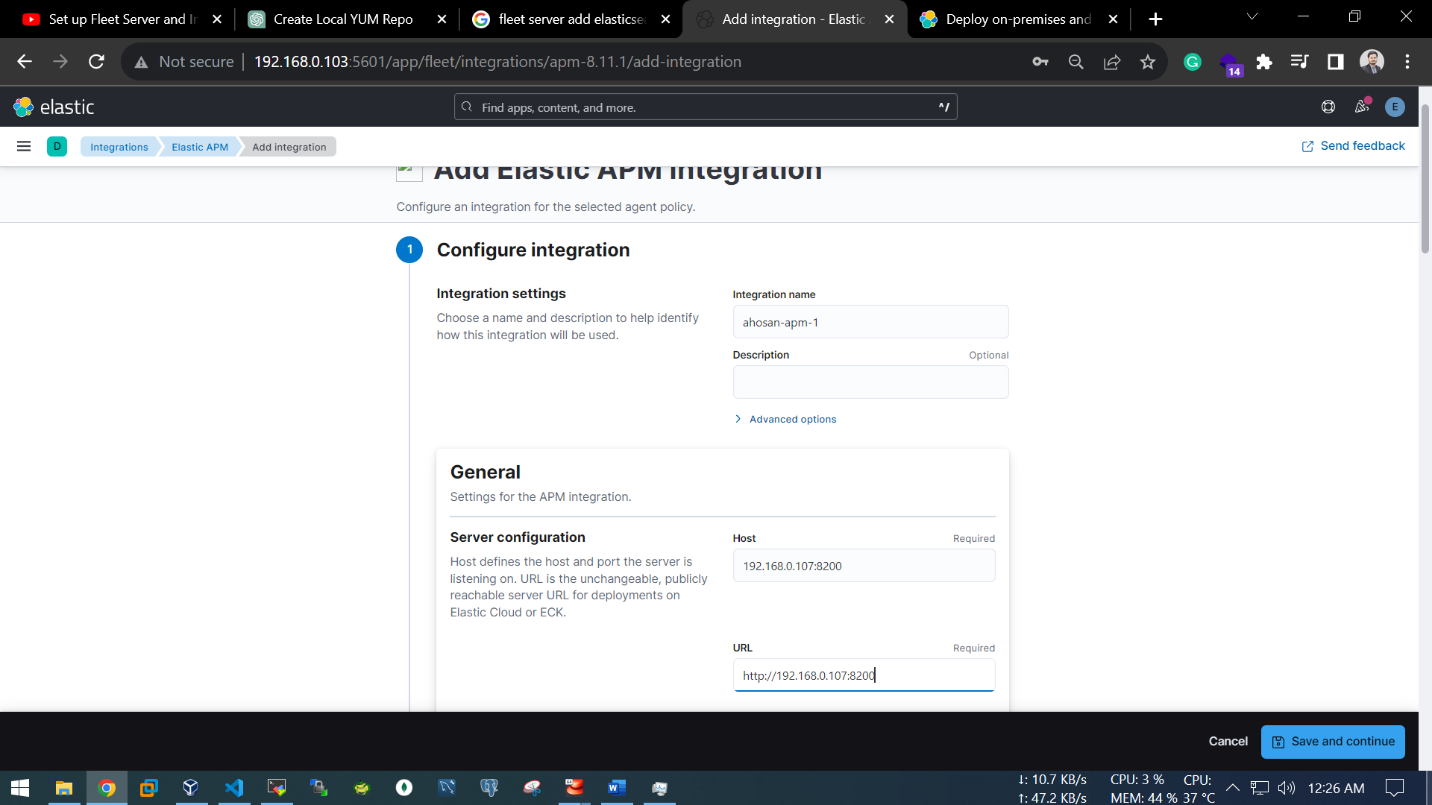
sudo systemctl start elastic-agent

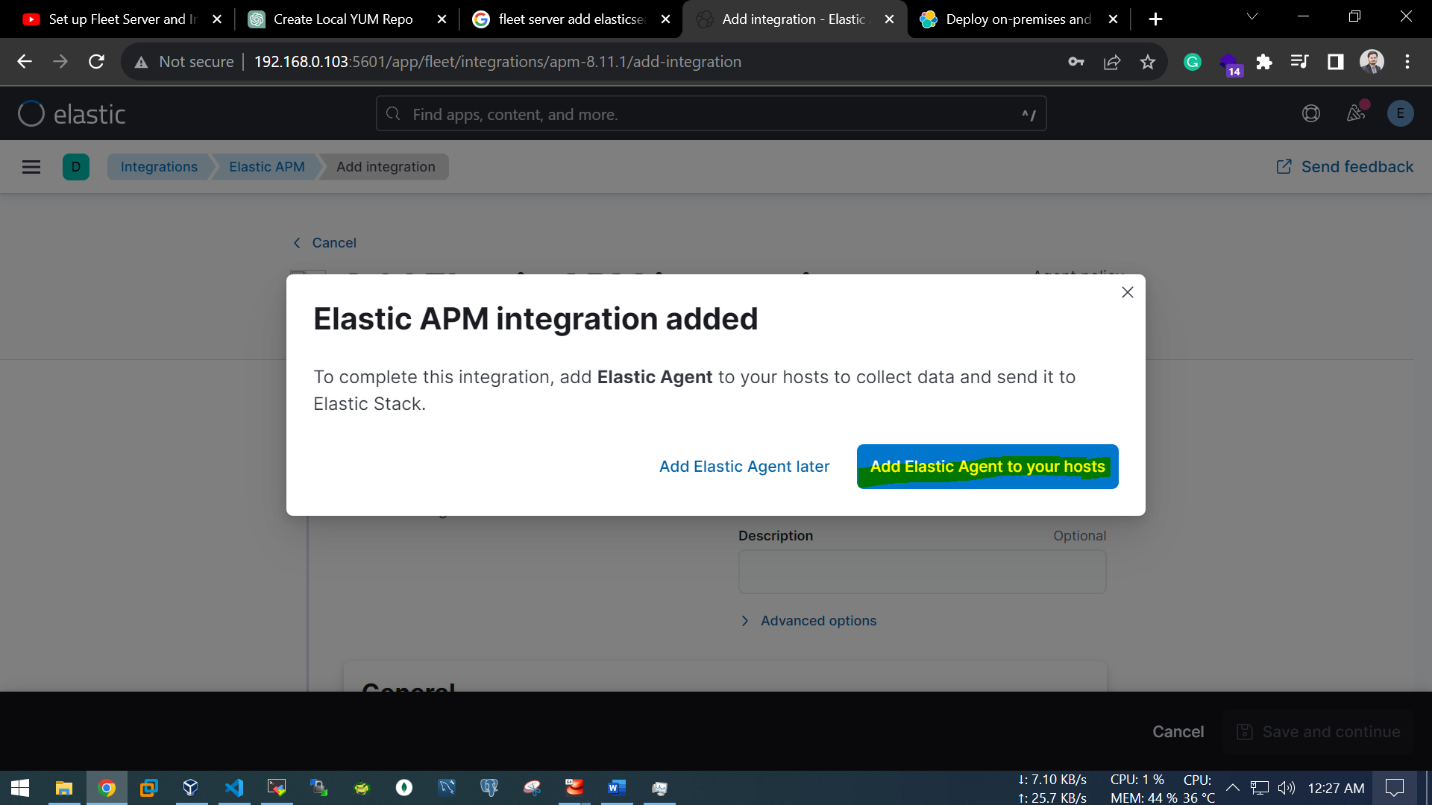


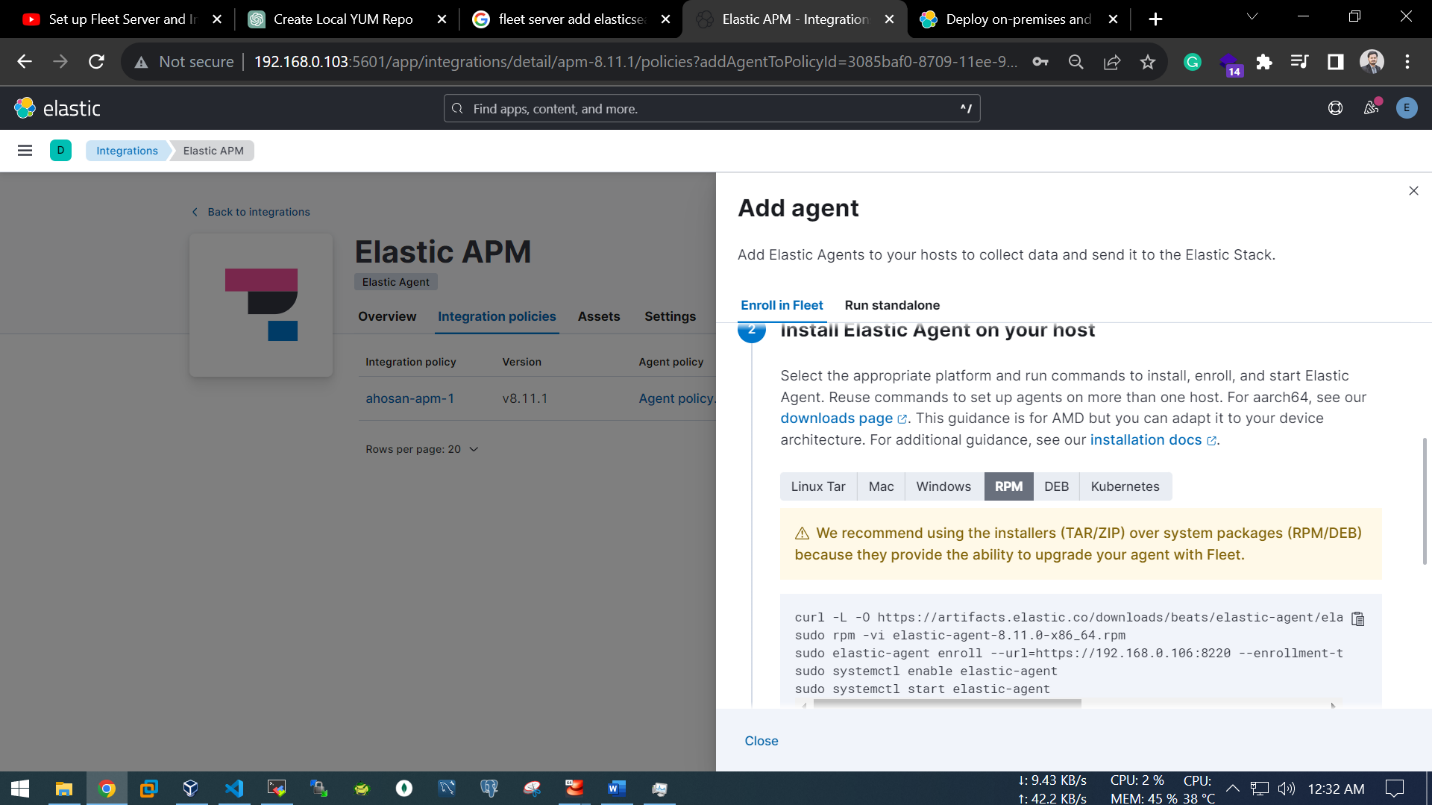












#####On APP host#####

[root@agent ~]# mkdir /root/ca/

[root@agent ~]# cd /root/ca/

--on fleet host

[root@elk ca]# scp -r /root/ca/elastic-agent-8.11.1-x86\_64.rpm root@192.168.0.107:/root/ca/

#curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.11.0-x86\_64.rpm

sudo rpm -vi elastic-agent-8.11.1-x86\_64.rpm

--on elk host

[root@elk ca]# scp -r /elk\_stack/ca root@192.168.0.107:/root/ca

elastic-agent enroll --url=https://192.168.0.106:8220 --enrollment-token=UG13dzY0c0JrOGRQNHhqaFJIeFQ6c2NYOG5tNnZTeXVjUTNJTVB1dXdzZw== \

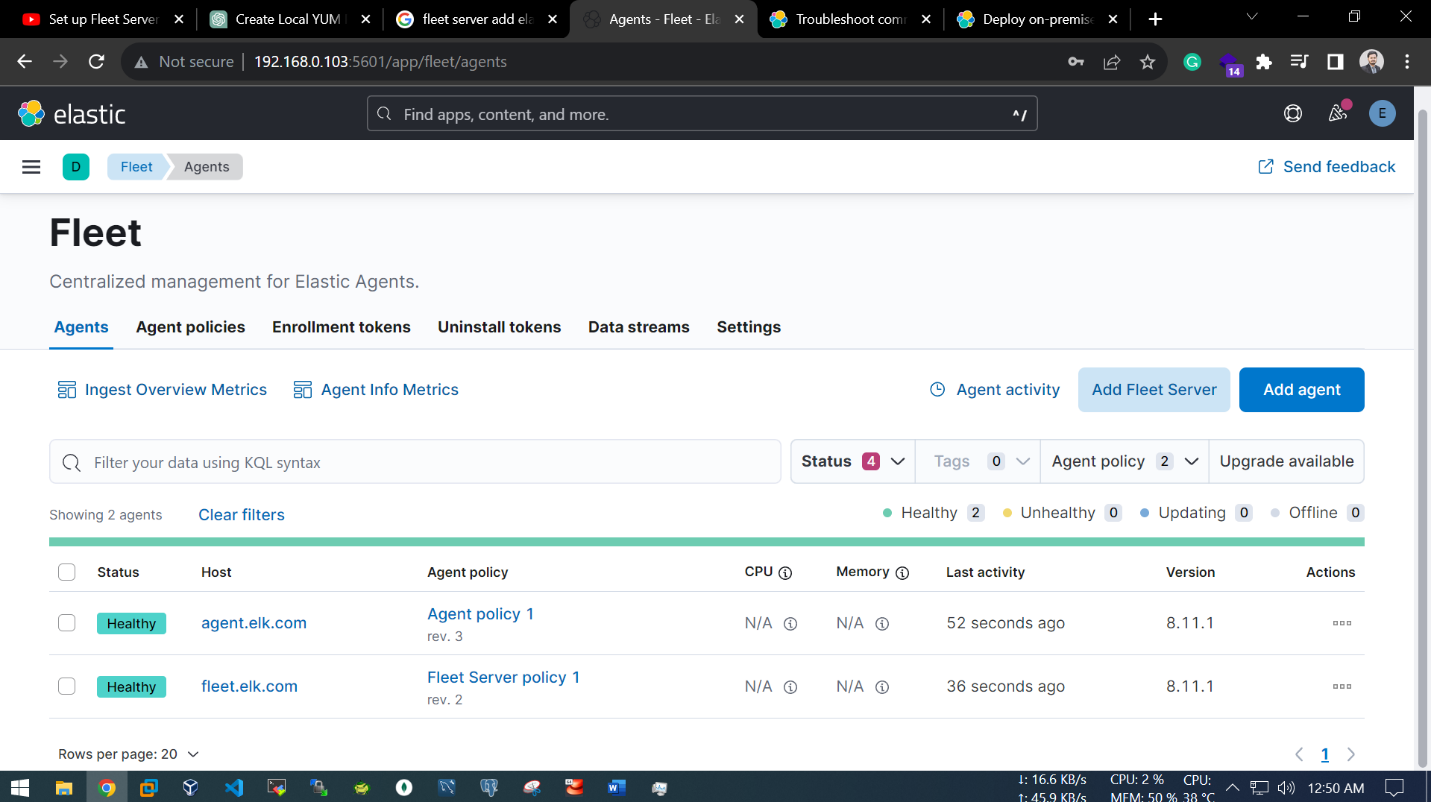
--certificate-authorities=/root/ca/ca/ca.crt \

--fleet-server-cert=/root/ca/ca/fleet-server/fleet-server.crt \

--fleet-server-cert-key=/root/ca/ca/fleet-server/fleet-server.key

sudo systemctl enable elastic-agent

sudo systemctl start elastic-agent



#################Sample Python\_FastAPI app################

[root@agent ca]# cd /root/ca

[root@agent ca]# sudo dnf install python3 -y

[root@agent ca]# dnf install pip

[root@agent ca]# pip3 install fastapi uvicorn

[root@agent ca]# pip install elastic-apm

[root@agent ca]# vi /root/ca/main.py

from fastapi import FastAPI

from elasticapm.contrib.starlette import make\_apm\_client, ElasticAPM

app = FastAPI()

#Configure the Elastic APM client

apm = make\_apm\_client(

app\_name="APMbyPython", # Set your app name

server\_url="http:// 127.0.0.1:8200", # Set your APM server URL

)

#Add the APM middleware to your FastAPI app

app.add\_middleware(ElasticAPM, client=apm)

@app.get("/")

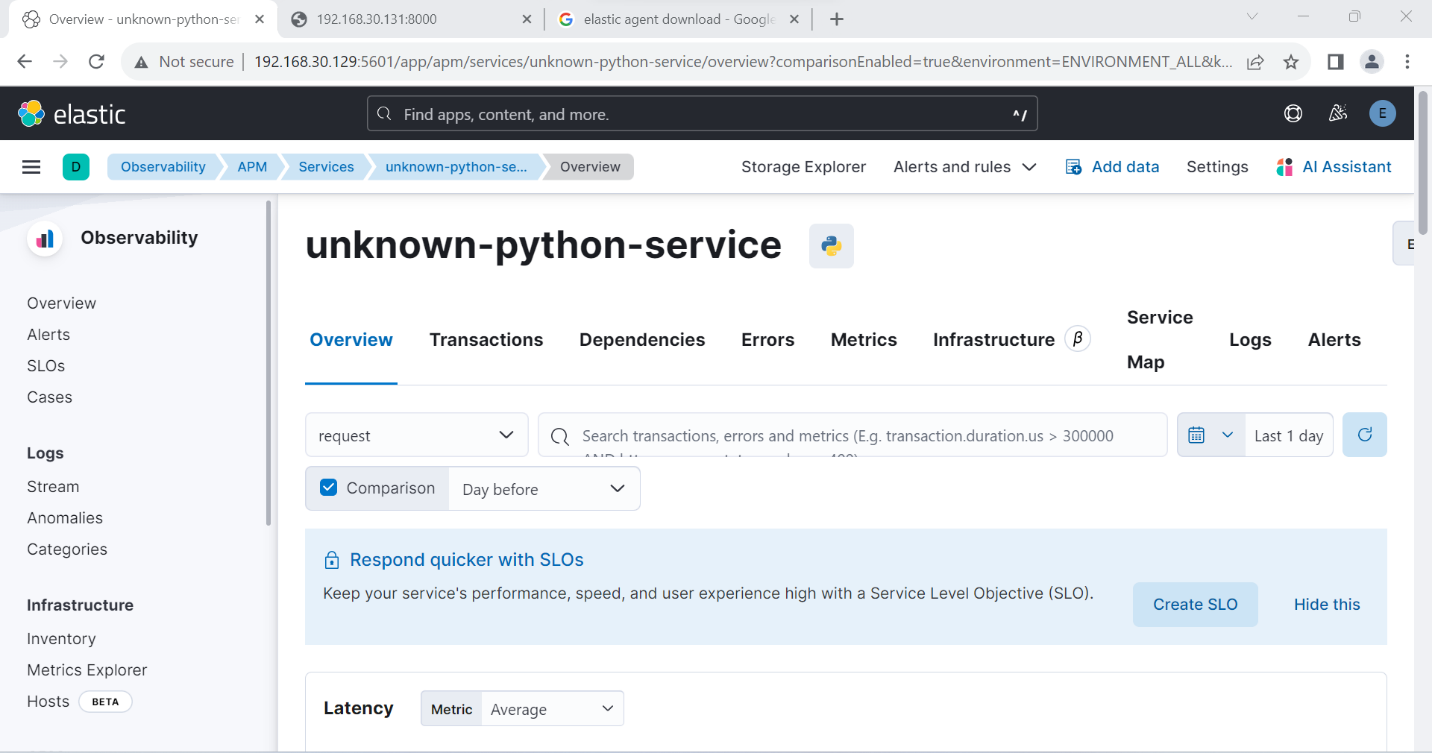
def read\_root():

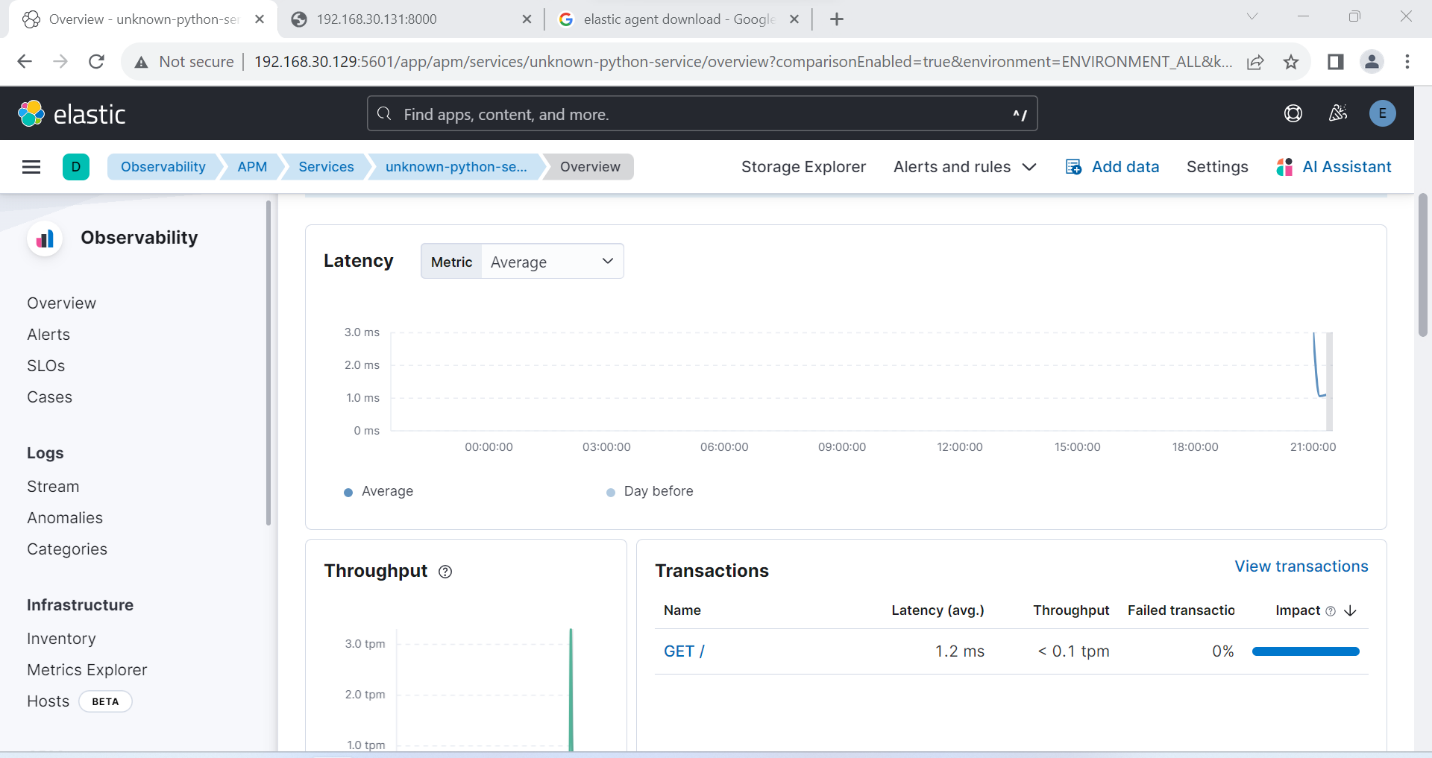
# Your FastAPI route code

return {"ITCL": "APM\_ELK\_TEST"}

[root@agent ~]# cd /root/ca/

[root@agent ca]# uvicorn main:app --reload --host 192.168.0.107 --port 8000





Should more explore in future…