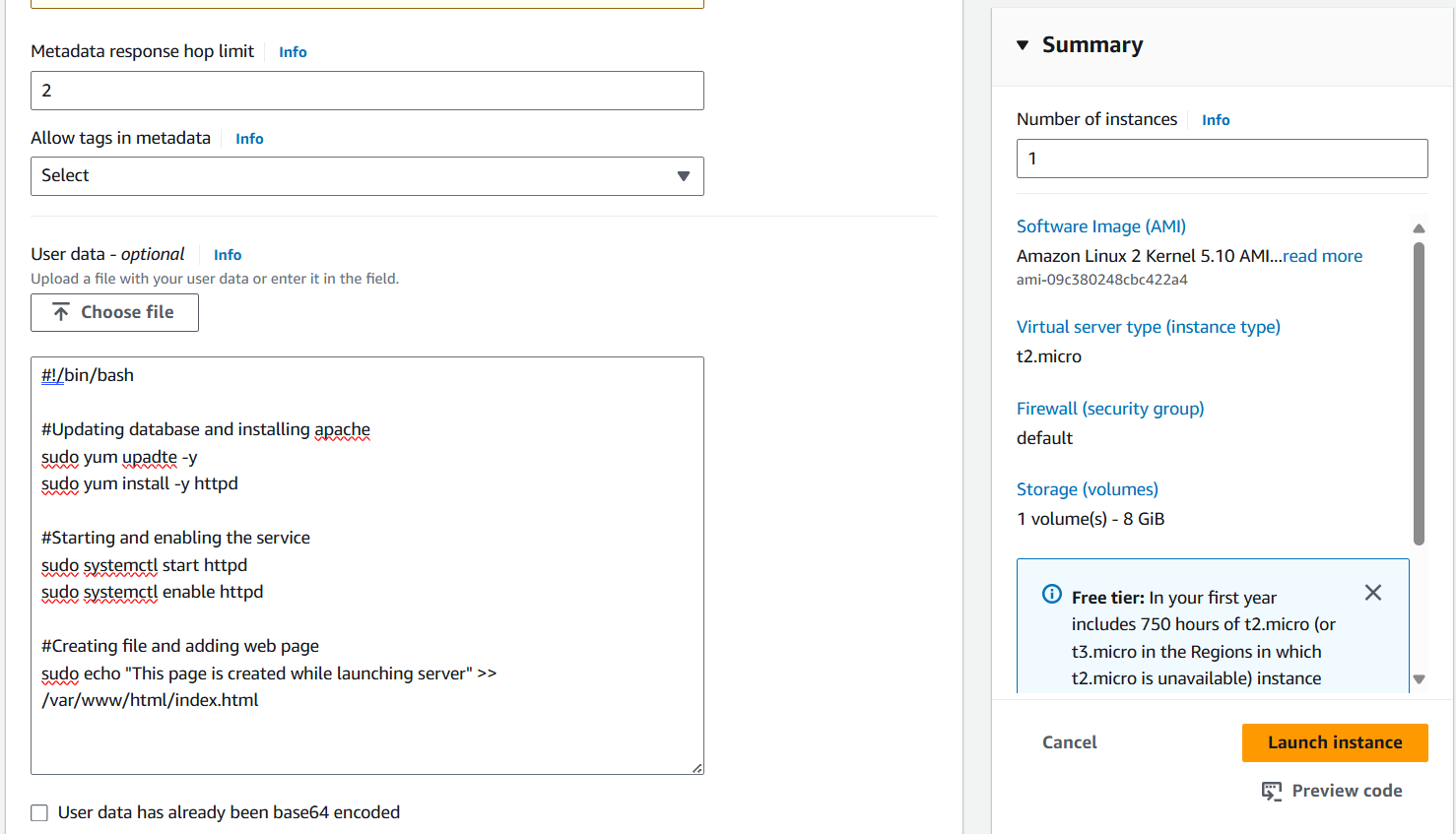
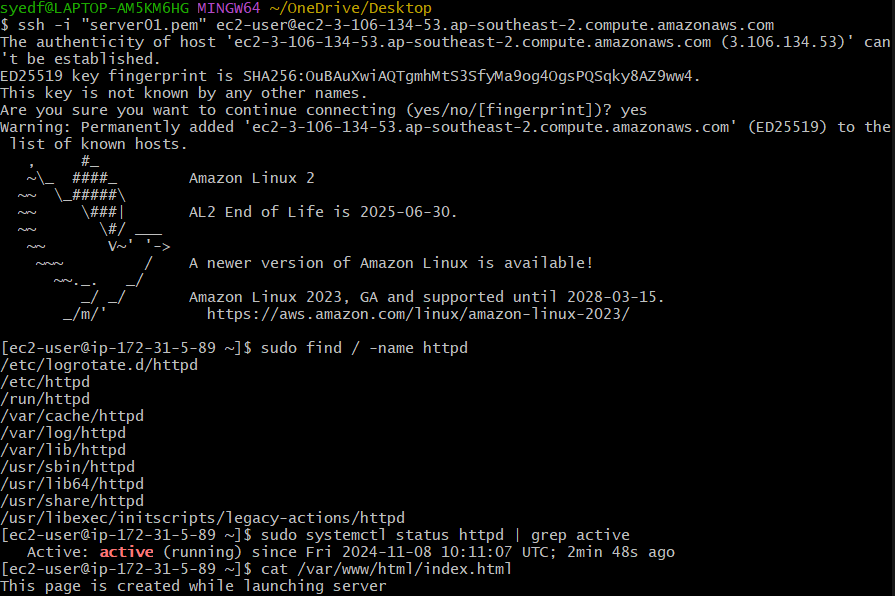
**1) Launch one ec2 using Amazon Linux 2 image and add script in user data to install Apache.**

>>Selecting linux image 2 and adding script in user data in advance option for installing apache



>>logging in through ssh and checking for apache and file

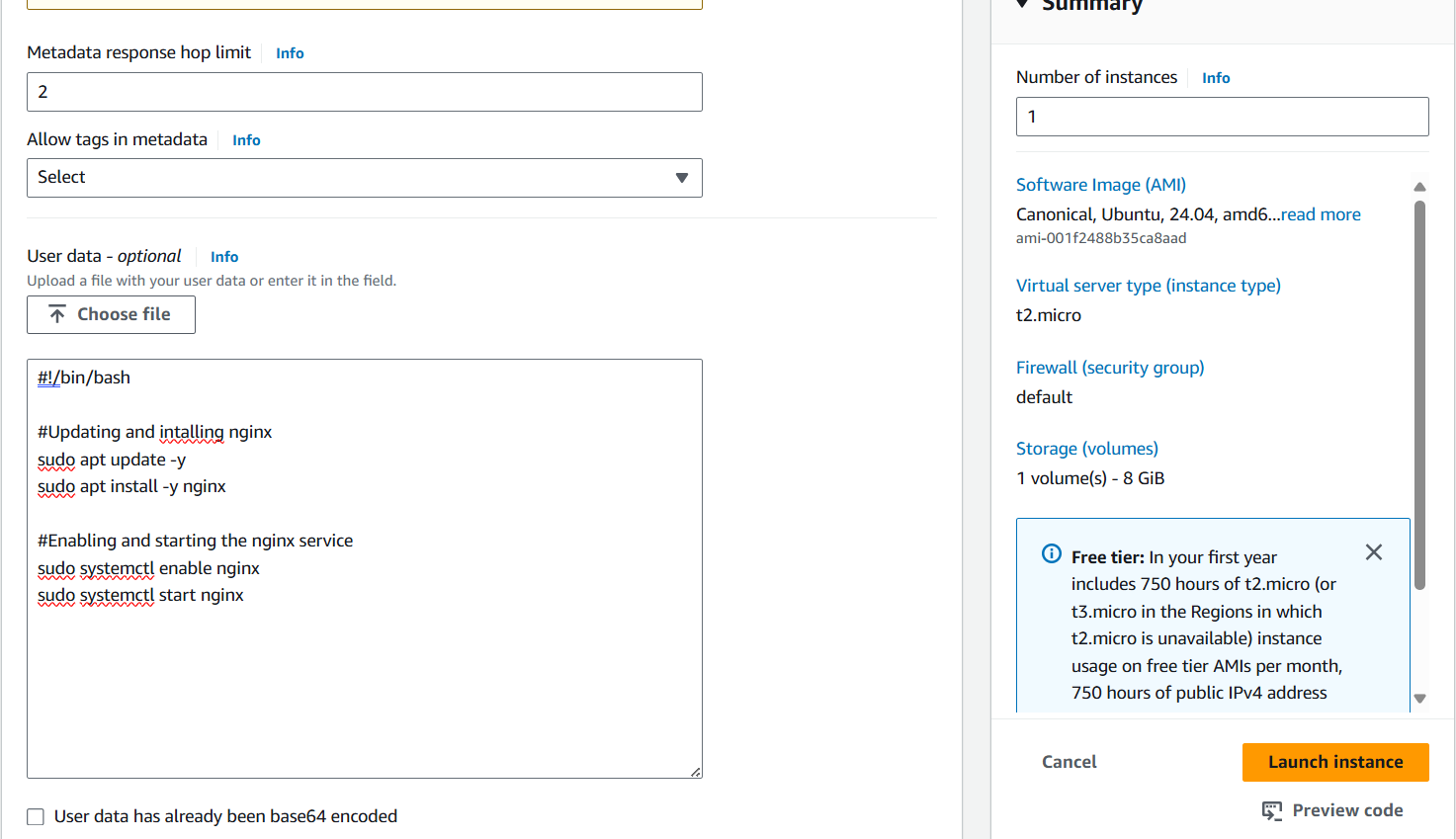


>>searching the ip on web

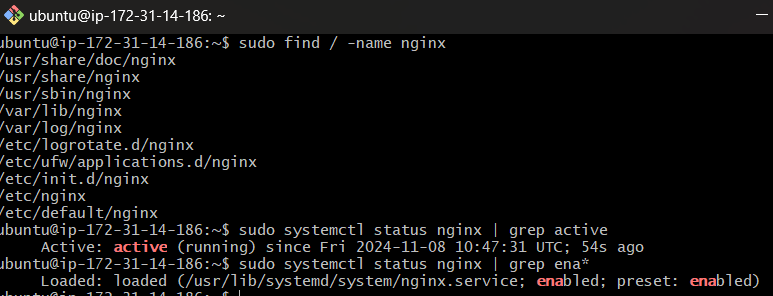


**2) Launch one ec2 using Ubuntu image and add script in user data to install Nginx.**

>> Selecting ubuntu image and adding script in user data in advance option for installing nginx on launch

****

>>checking on CLI for Nginx service



**3) Launch one windows server and install tomcat in windows.**

Create instance with windows image

launch the instance by clicking connect and follow the instrunctions.

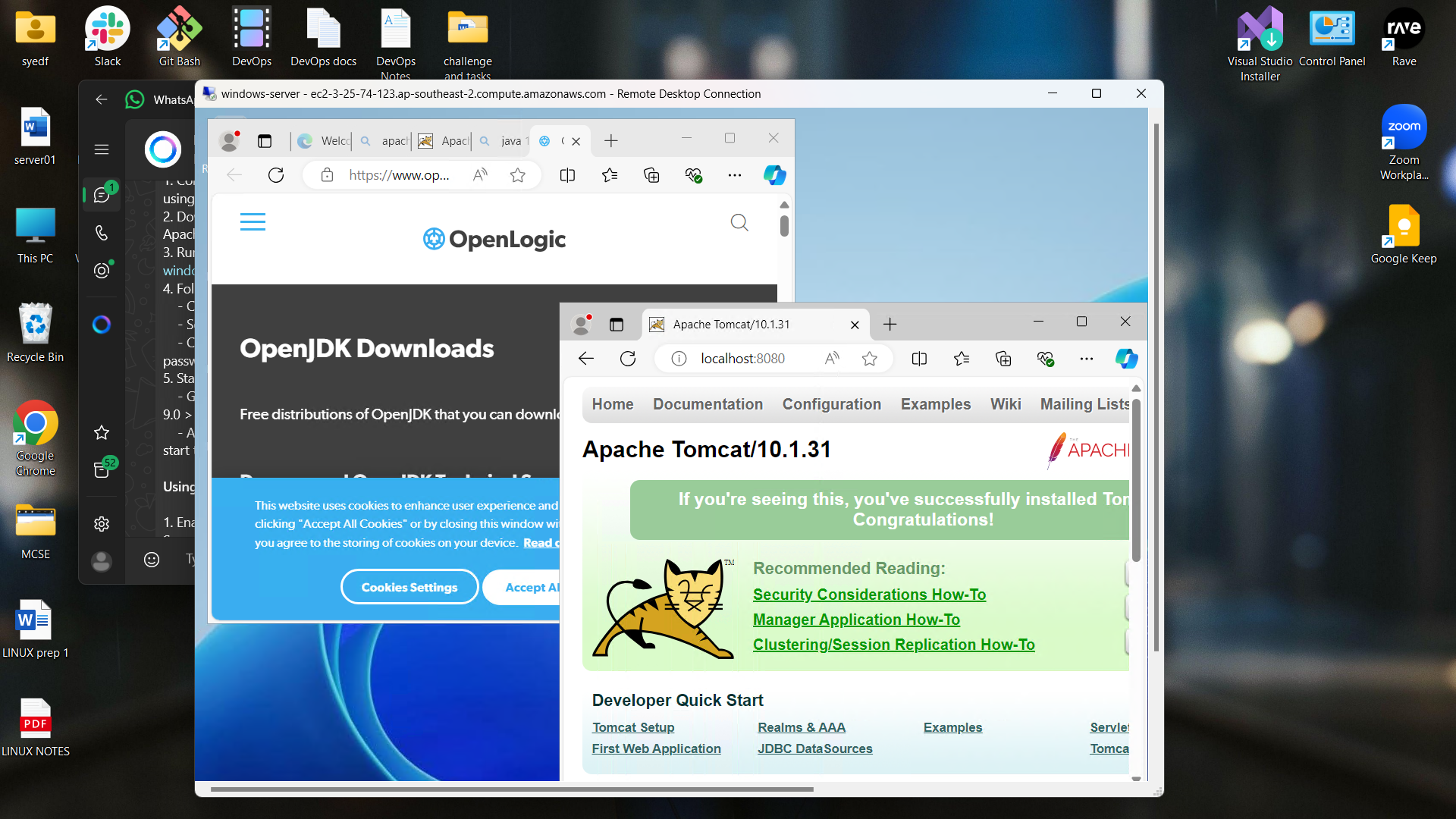
Go to browser and download java jdk from official page

Download tomcat from official page

Install it

Open cmd prompt and run command <net start tomcat\*>

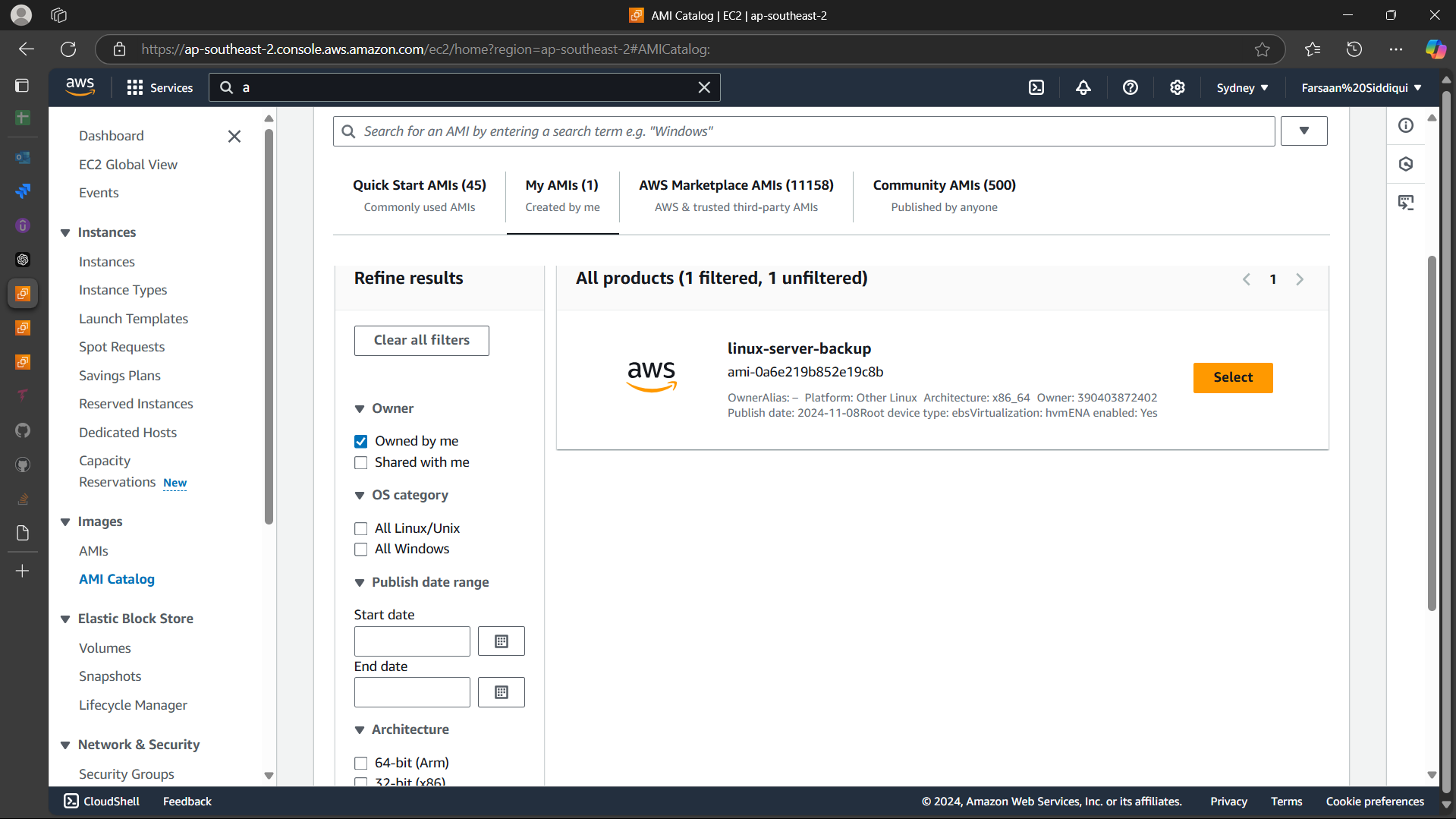
**Go to browser on windows server search locathost:8080**

****

**4) Take snapshot of the instane created in Task 1.**

->First stop the instance

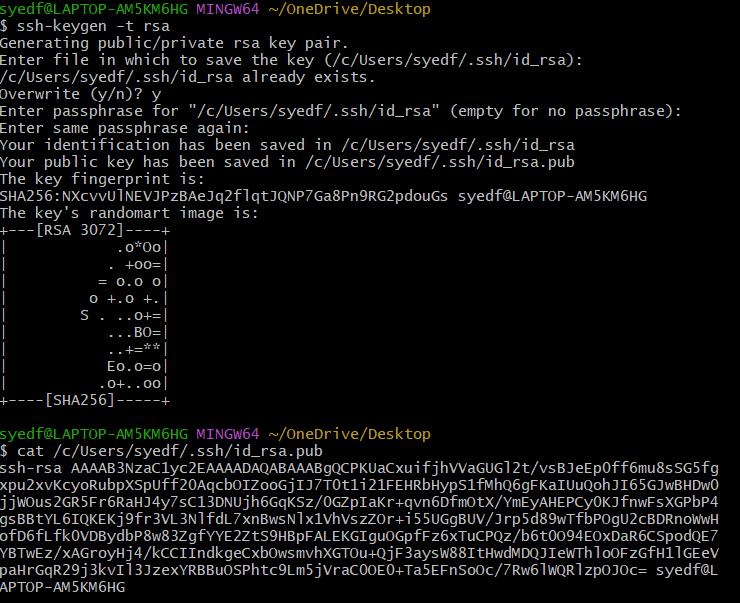
go to Actions > Image and template > Create Image > Give image name > Create Image



**5) Assign password less authentication for ec2 created on Task 2.**

>create a key-gen in local server

>cat the key and copy it

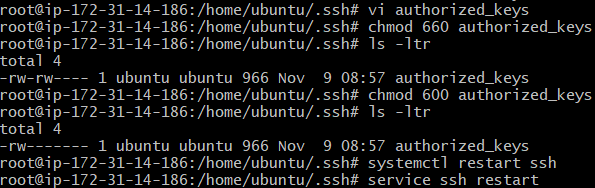


>login to ubuntu server

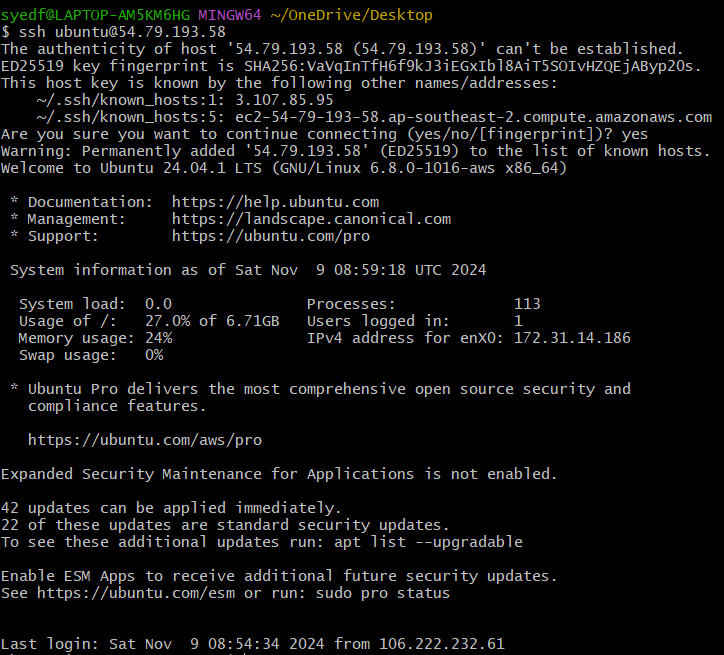
>got to .ssh directory

>edit the file authorized keys

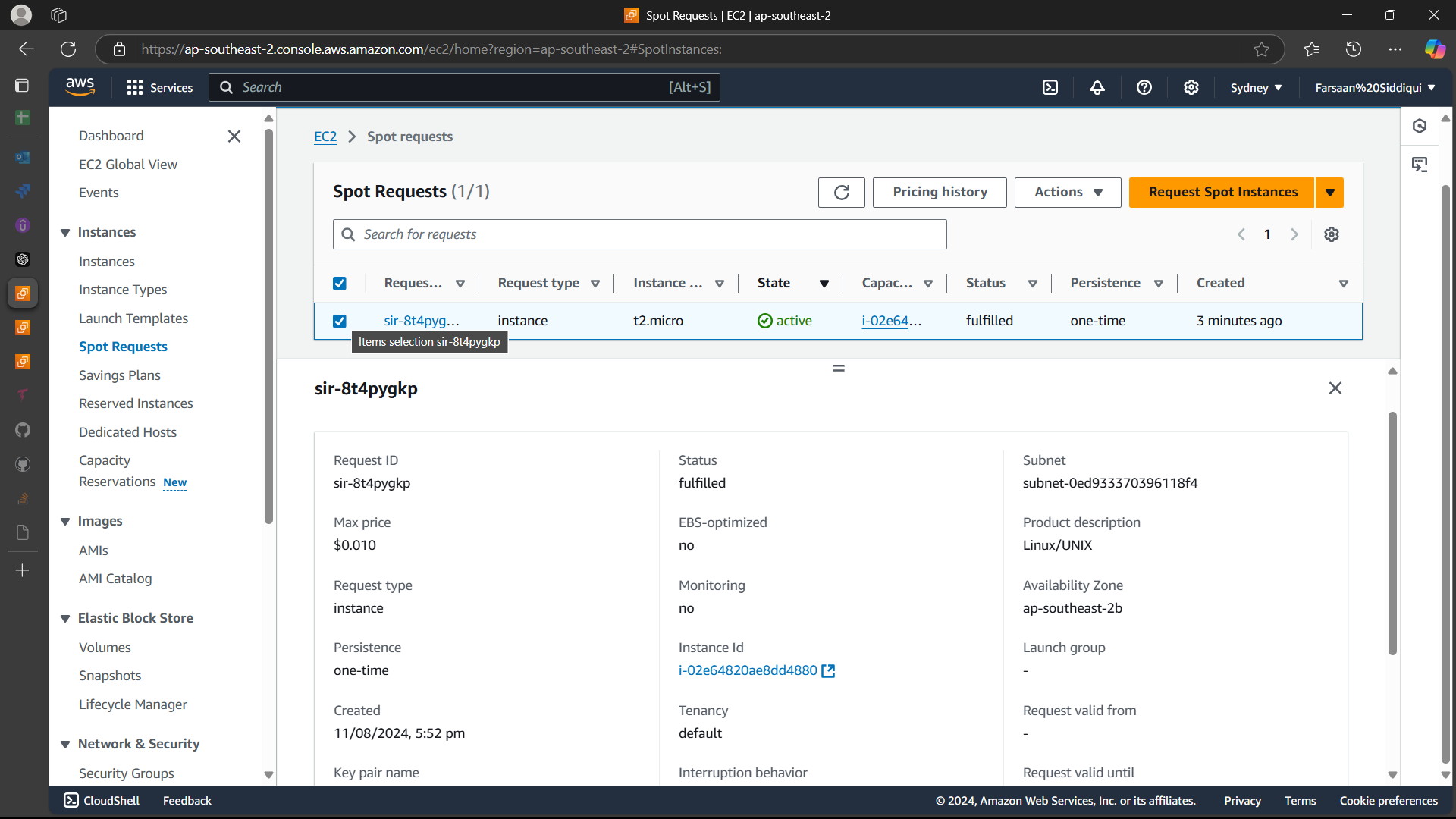
>add the copied key in that file and save the file then restart the ssh service



>Login with ssh username@hostname

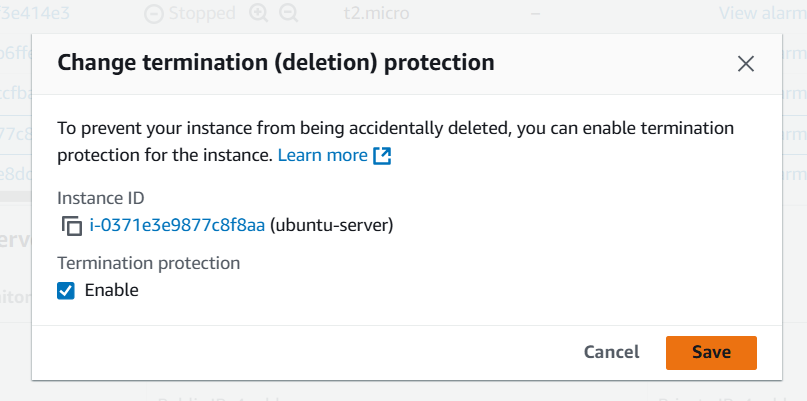


**6) Launch any ec2 using spot purchasing option**.



**7) Enable Termination policy on ec2 created in Task 2.**

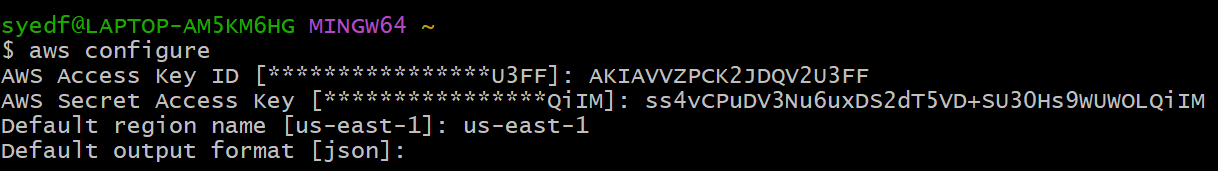
select\_instance > Actions > Instance\_settings > Change\_termination\_protection > Enable



**8) Launch one ec2 using Aws CLI.**

Download AWSCLIV2 from browser > setup the application > open gitbash CLI > check version > configure > add requirements > Done

**Configure AWS CLI**: Once installed, configure the AWS CLI with your credentials by running:

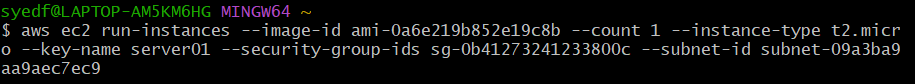


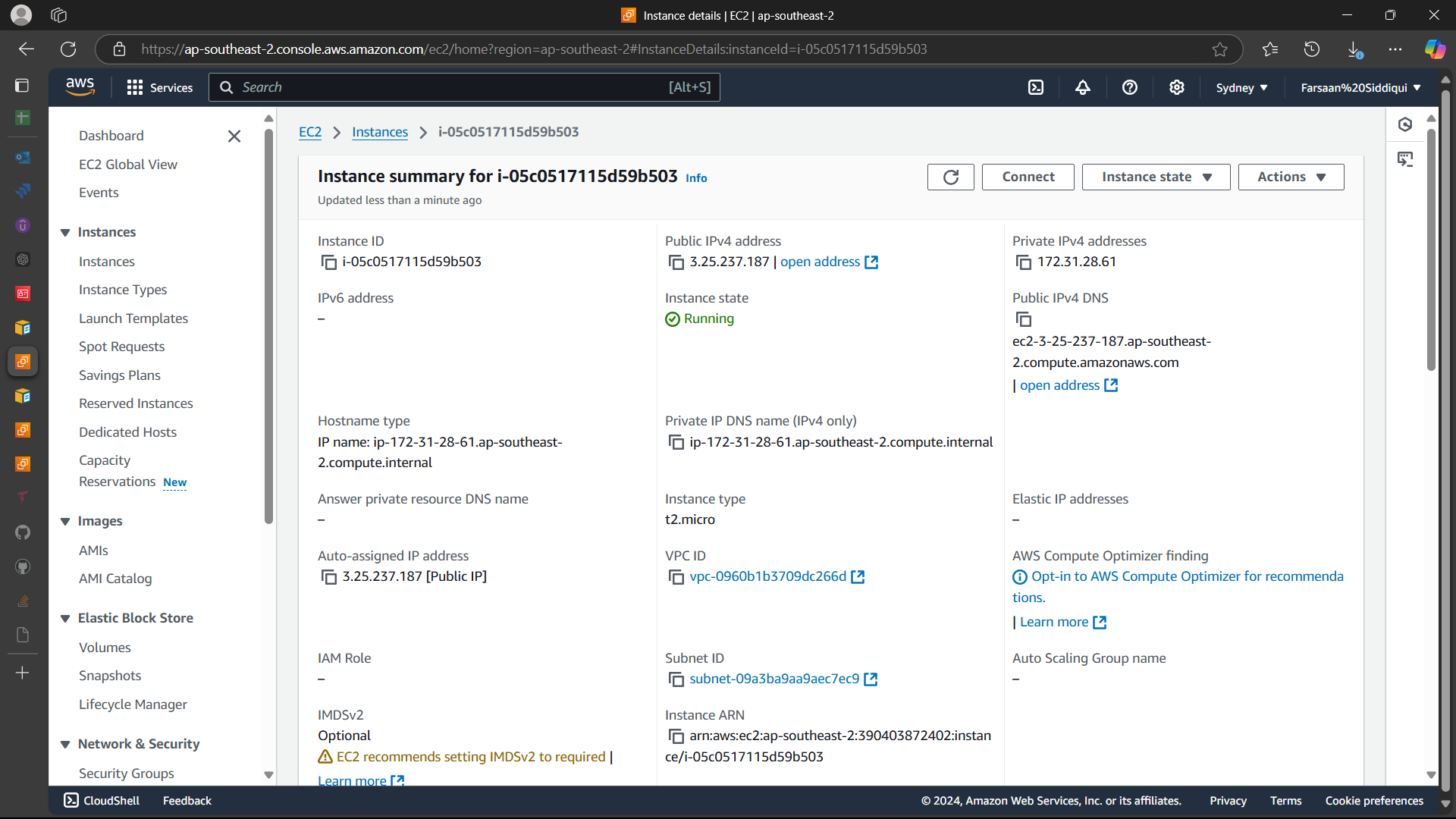
**Follow this to get your access key and secret key**

**Log in to the AWS Management Console** > **Navigate to the IAM (Identity and Access Management service** > **Select Users** from the left-hand menu > **Click on the user** for whom you want to find the access keys > **Go to the Security credentials tab. > Scroll down to the Access keys section**

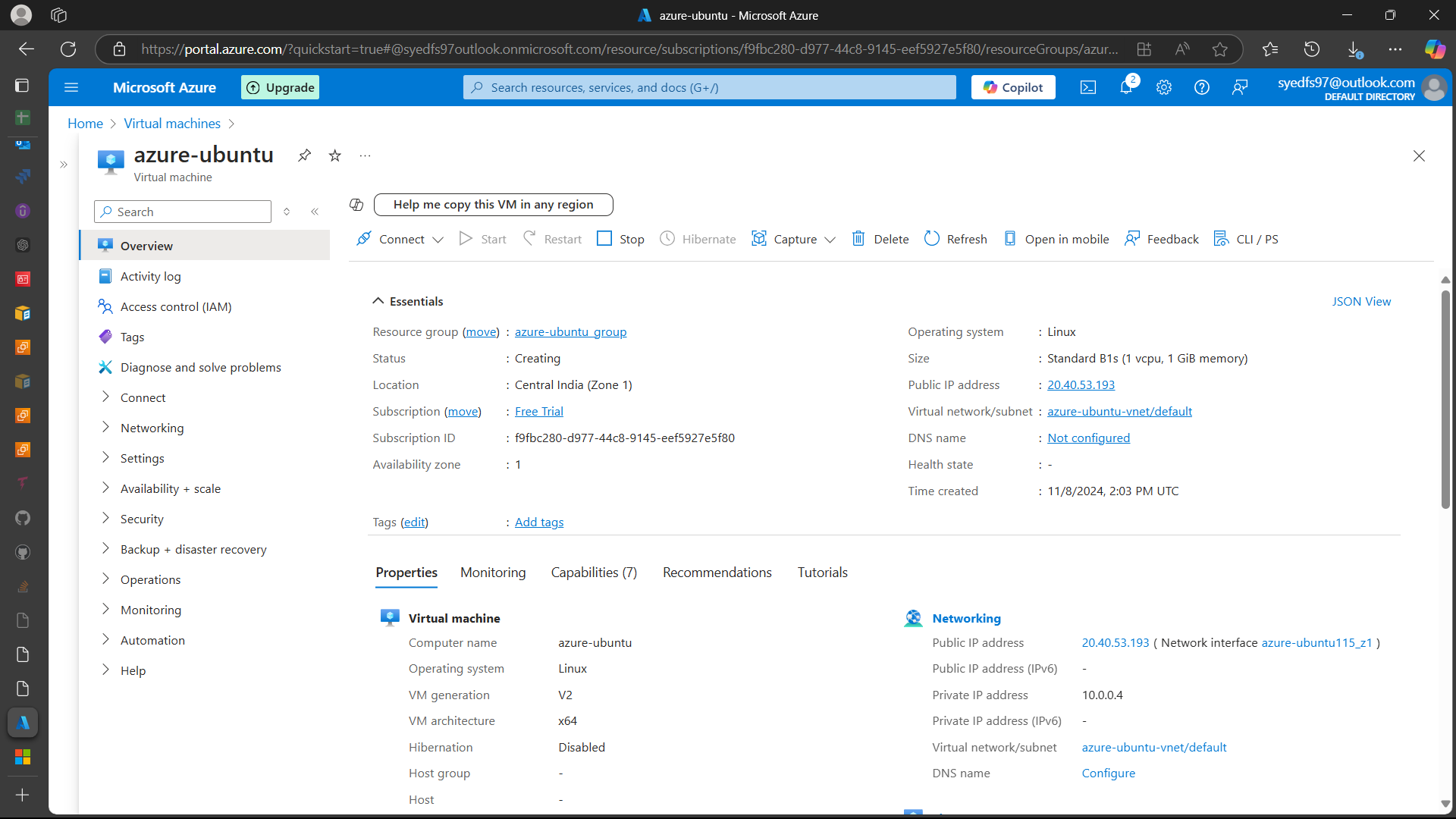
**Run command**

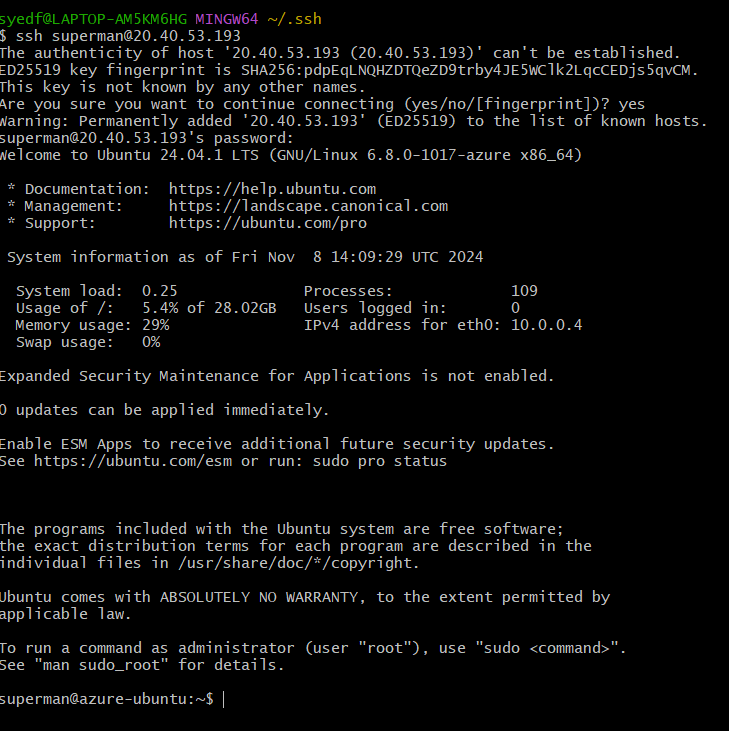
~$ **aws ec2 run-instances --image-id <ami-0abcdef1234567890> --count <1> --instance-type <t2.micro> --key-name <your\_key> --security-group-ids <sg-0123456789abcdef0> --subnet-id <subnet-6e7f829e>**





**9) Launch one azure VM using ubuntu image.**

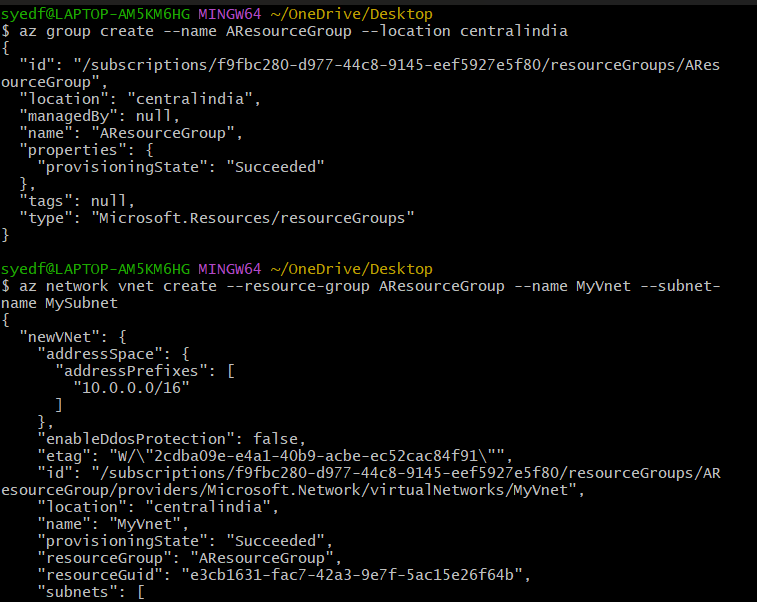
****



**10) Launch one azure VM using Azure CLI.**

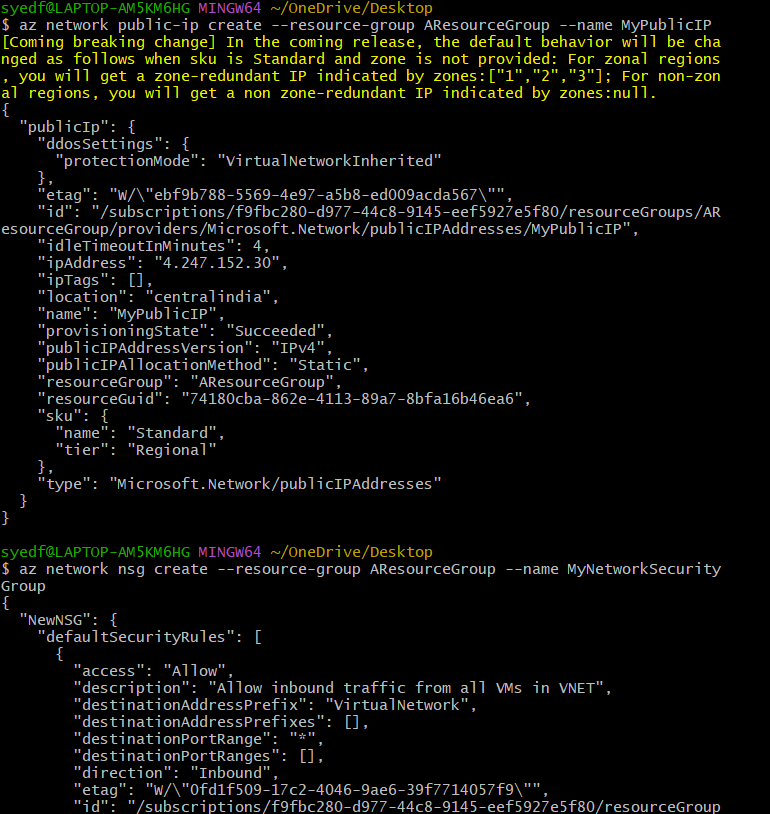
az group create --name AResourceGroup --location eastus

az network vnet create --resource-group AResourceGroup --name MyVnet --subnet-name MySubnet

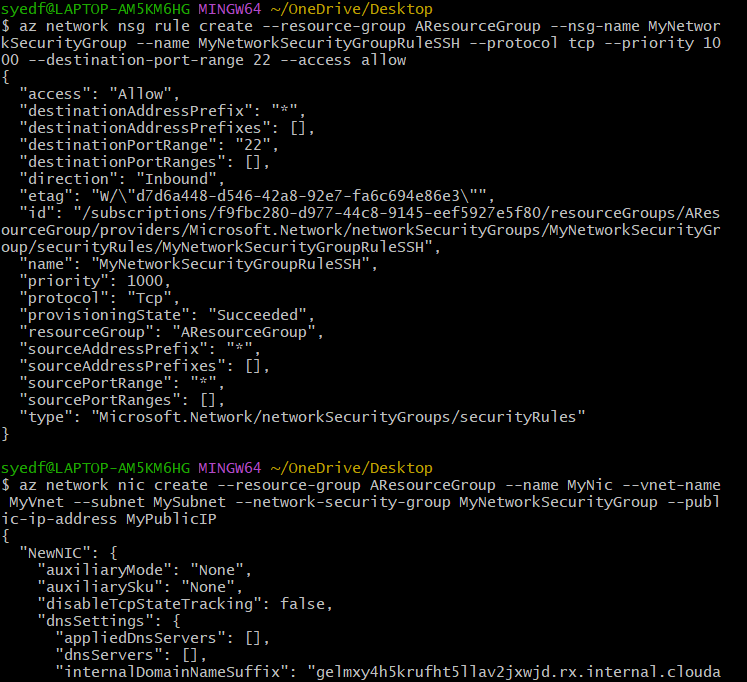


az network public-ip create --resource-group AResourceGroup --name MyPublicIP

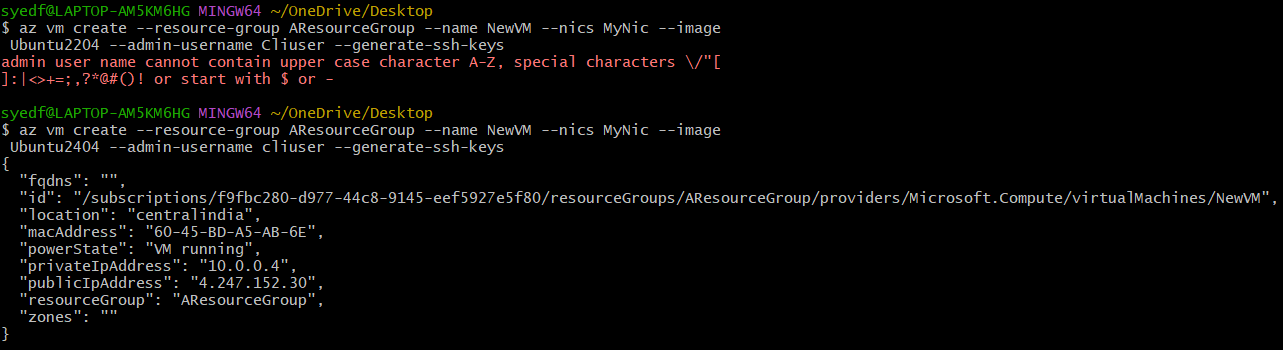
az network nsg create --resource-group AResourceGroup --name MyNetworkSecurityGroup



az network nsg rule create --resource-group AResourceGroup --nsg-name MyNetworkSecurityGroup --name MyNetworkSecurityGroupRuleSSH --protocol tcp --priority 1000 --destination-port-range 22 --access allow

az network nic create --resource-group AResourceGroup --name MyNic --vnet-name MyVnet --subnet MySubnet --network-security-group MyNetworkSecurityGroup --public-ip-address MyPublicIP

az vm create --resource-group MyResourceGroup --name MyVM --nics MyNic --image UbuntuLTS --admin-username azureuser --generate-ssh-keys



Checking the sever on azure website

