

NAME: KSHITIJ GUPTA
Enrolment Number: 21162101007
Sub: CCE

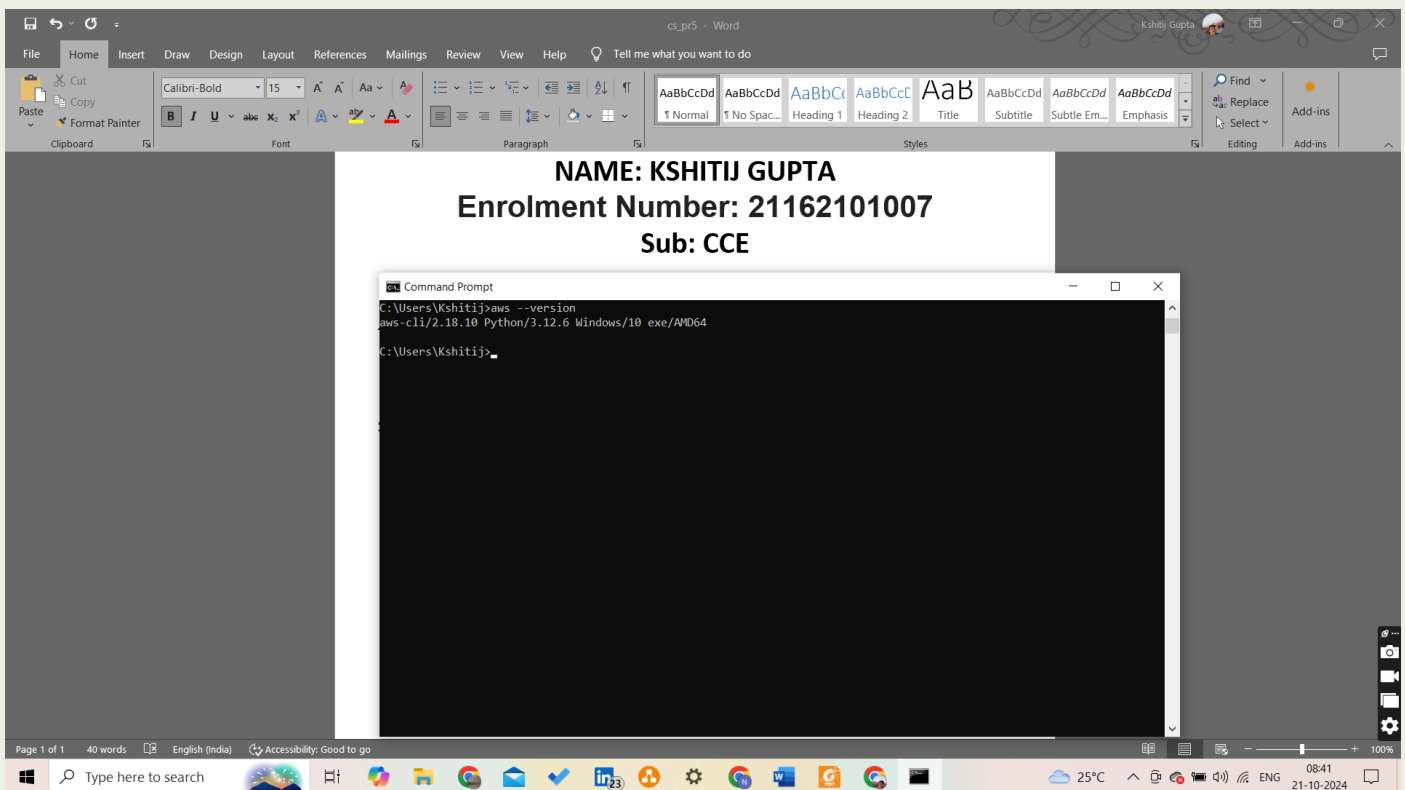
Practical – 13[Batch-71]

Task:

- Use AWS CLI and configure it.
- Services to be configured through CLI: S3, EC2, IAM, VPC

Steps for Practical:

1. First install aws CLI and check the version



Now open secure credentials

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/security_credentials

Services Search [Alt+S]

My security credentials Root user Info

The root user has access to all AWS resources in this account, and we recommend following [best practices](#). To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference

You don't have MFA assigned
As a security best practice, we recommend you assign MFA. Assign MFA

Account details Edit account name, email, and password

Account name KautikGupta	Email address guptakautik@gmail.com
AWS account ID 008971634001	Canonical user ID 020a8e13fe07d92eeb47a0f982608c32a8455e308cd2a438820218e7658a0b41

Multi-factor authentication (MFA) (0) Remove Resync Assign MFA device

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment			

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search

25°C 08:46 21-10-2024

Create access key

us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/security_credentials/access-key-wizard

Services Search [Alt+S]

Alternatives to root user access keys Info

Root user access keys are not recommended
We don't recommend that you create root user access keys. Because you can't specify the root user in a permissions policy, you can't limit its permissions, which is a best practice.
Instead, use alternatives such as an IAM role or a user in IAM Identity Center, which provide temporary rather than long-term credentials. [Learn More](#)
If your use case requires an access key, create an IAM user with an access key and apply least privilege permissions for that user. [Learn More](#)

Continue to create access key?

☒ I understand creating a root access key is not a best practice, but I still want to create one.

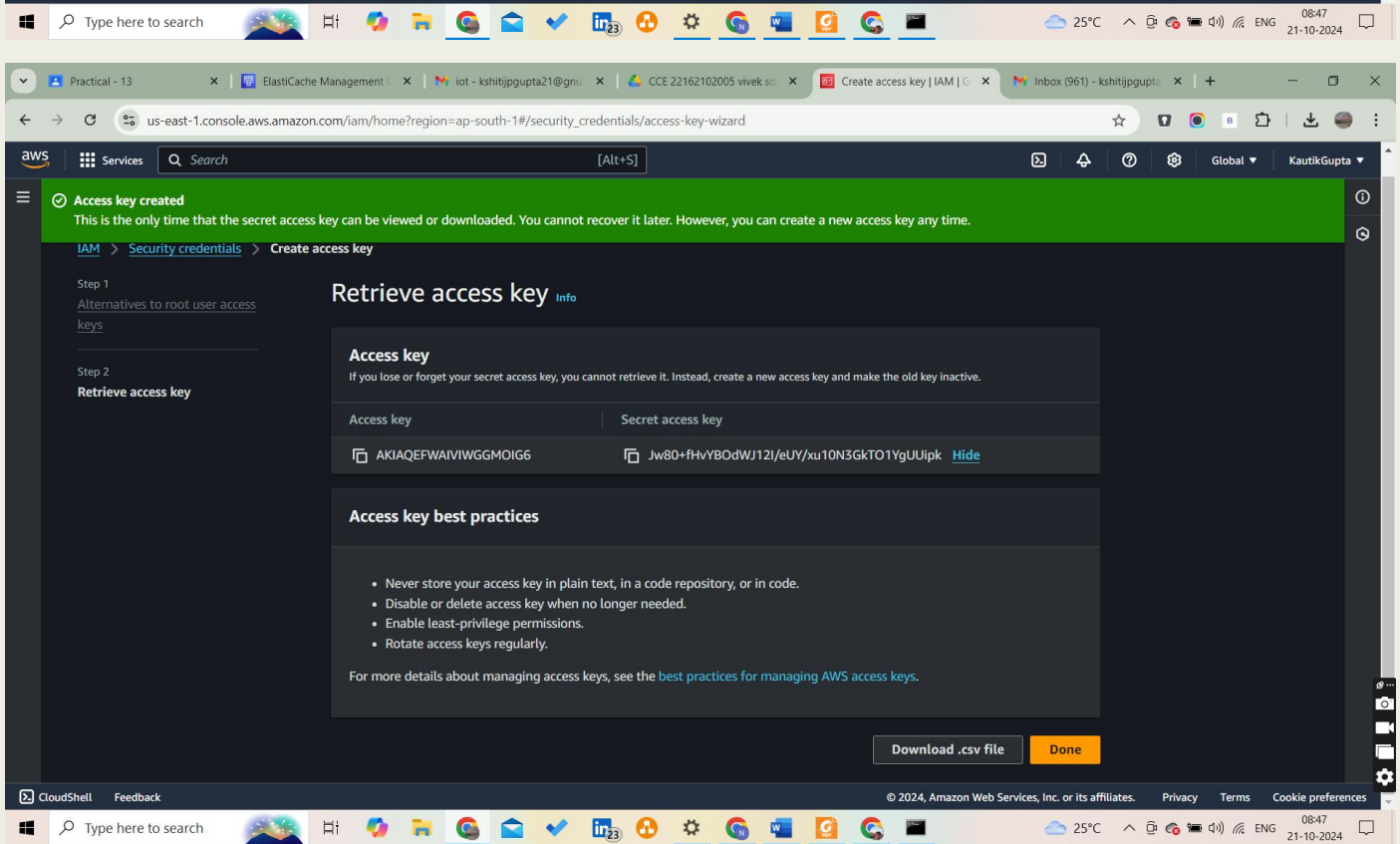
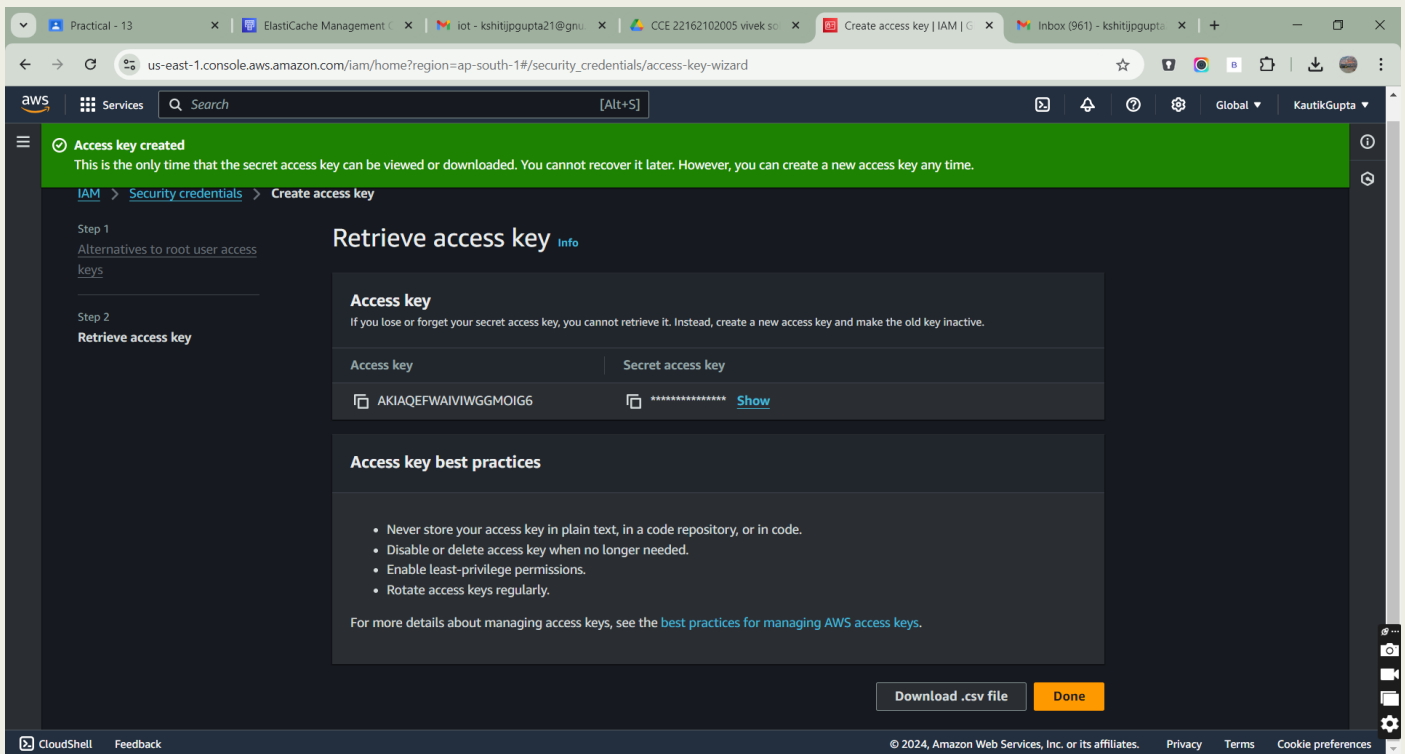
Cancel Create access key

CloudShell Feedback

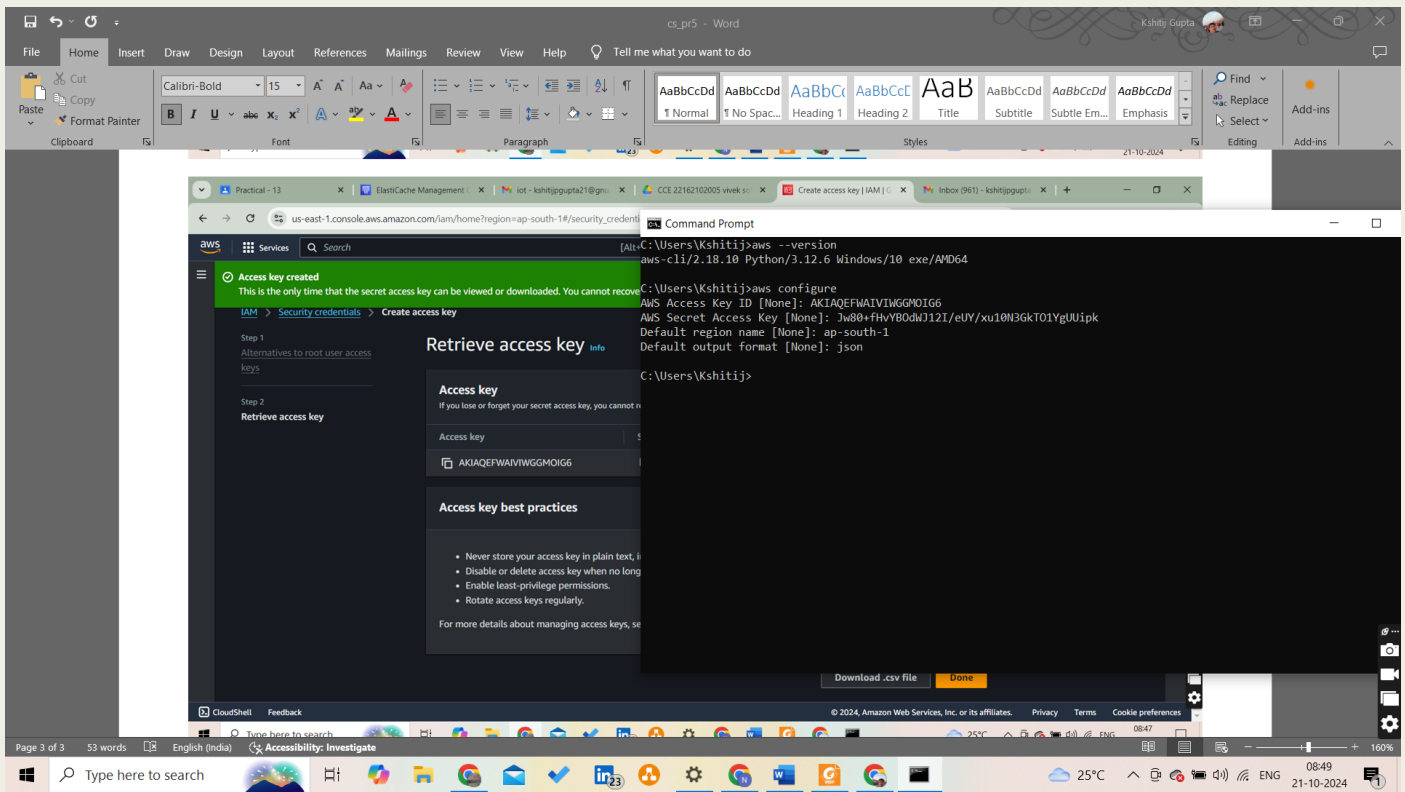
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search

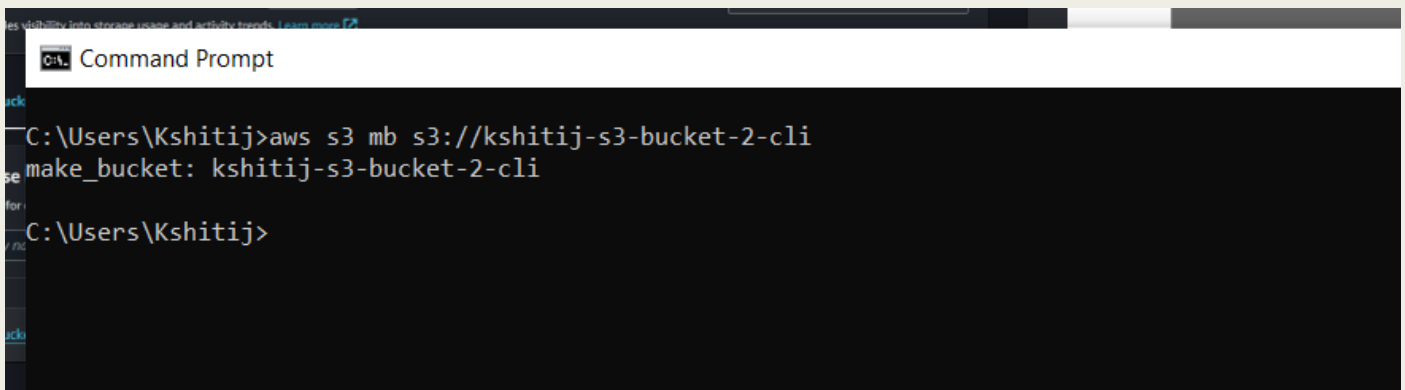
25°C 08:47 21-10-2024

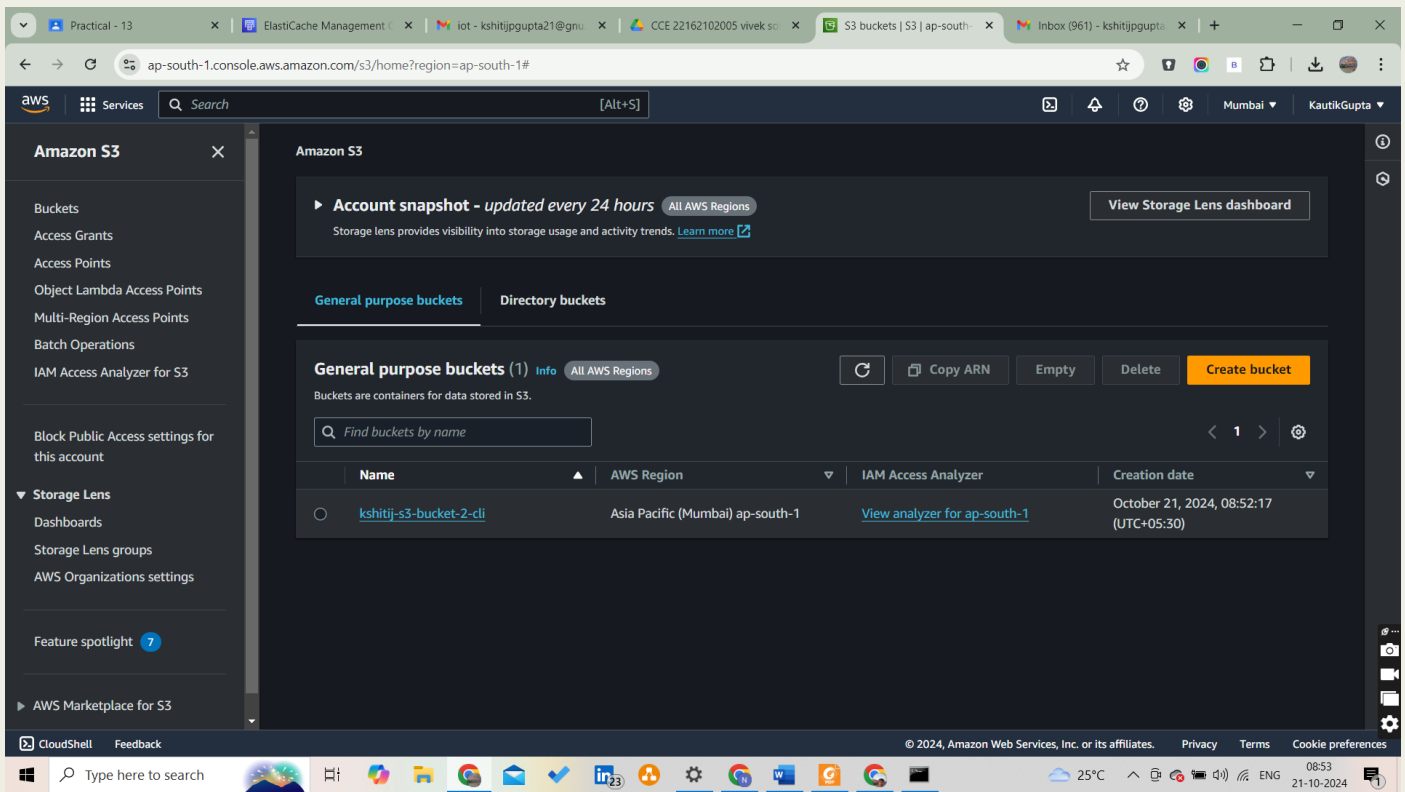


Run “aws configure” to config access

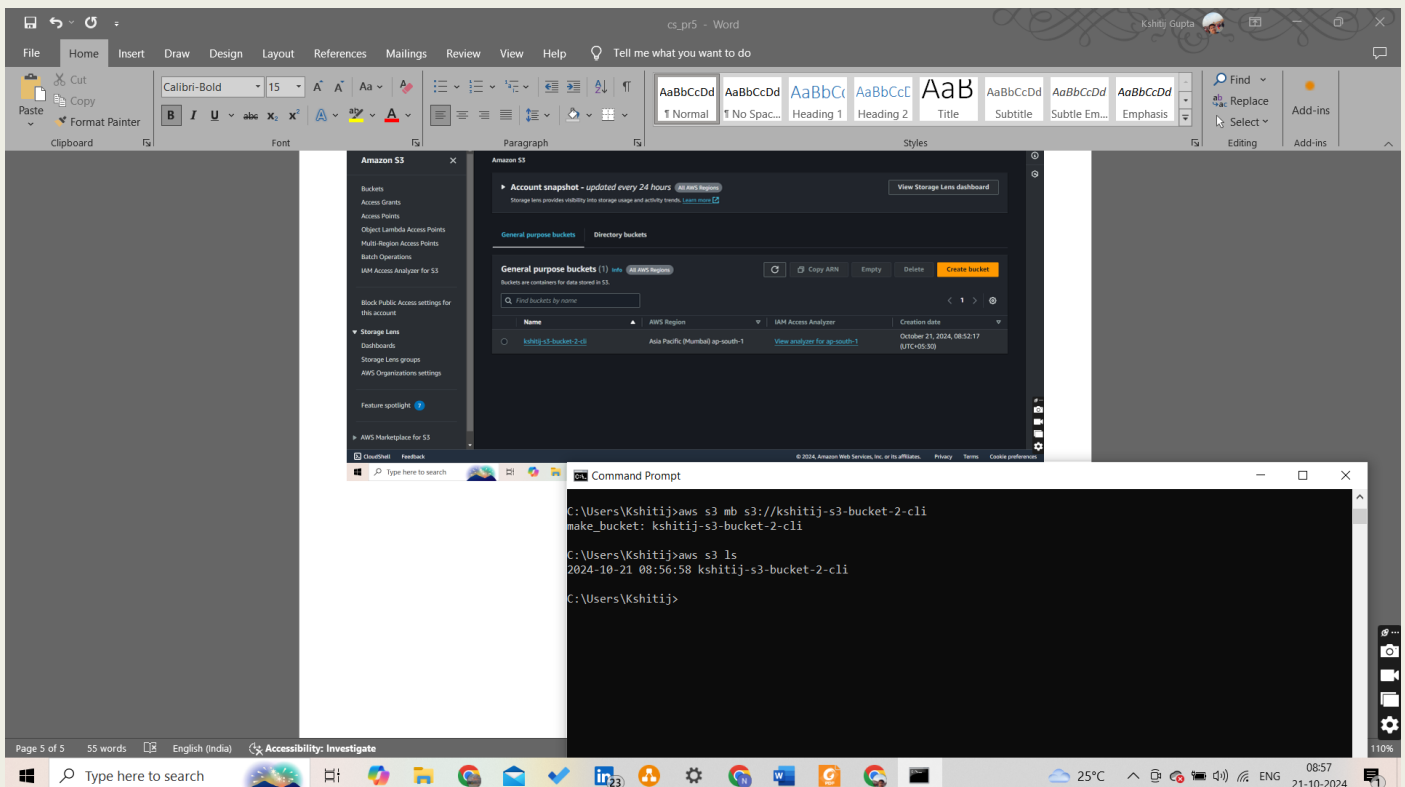


S3 bucket:





List of S3 using Cli:



Now copy the file to your bucket in s3

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.5011]
(c) Microsoft Corporation. All rights reserved.

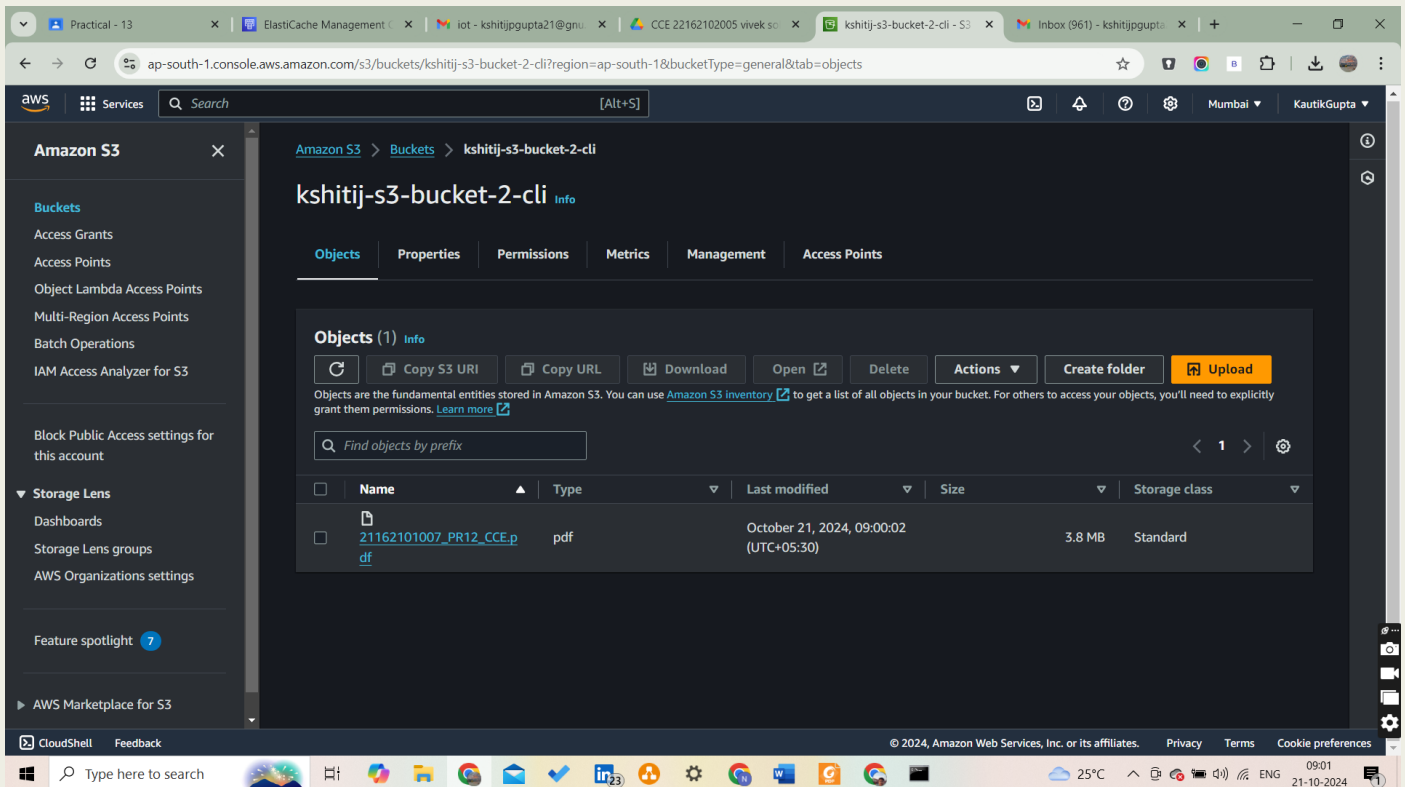
D:\SEM-7\CCE>aws s3 cp 21162101007_PR12_CCE s3://kshitij-s3-bucket-2-cli

The user-provided path 21162101007_PR12_CCE does not exist.

D:\SEM-7\CCE>aws s3 cp 21162101007_PR12_CCE.pdf s3://kshitij-s3-bucket-2-cli
upload: .\21162101007_PR12_CCE.pdf to s3://kshitij-s3-bucket-2-cli/21162101007_PR12_CCE.pdf

D:\SEM-7\CCE>
```

It's copied

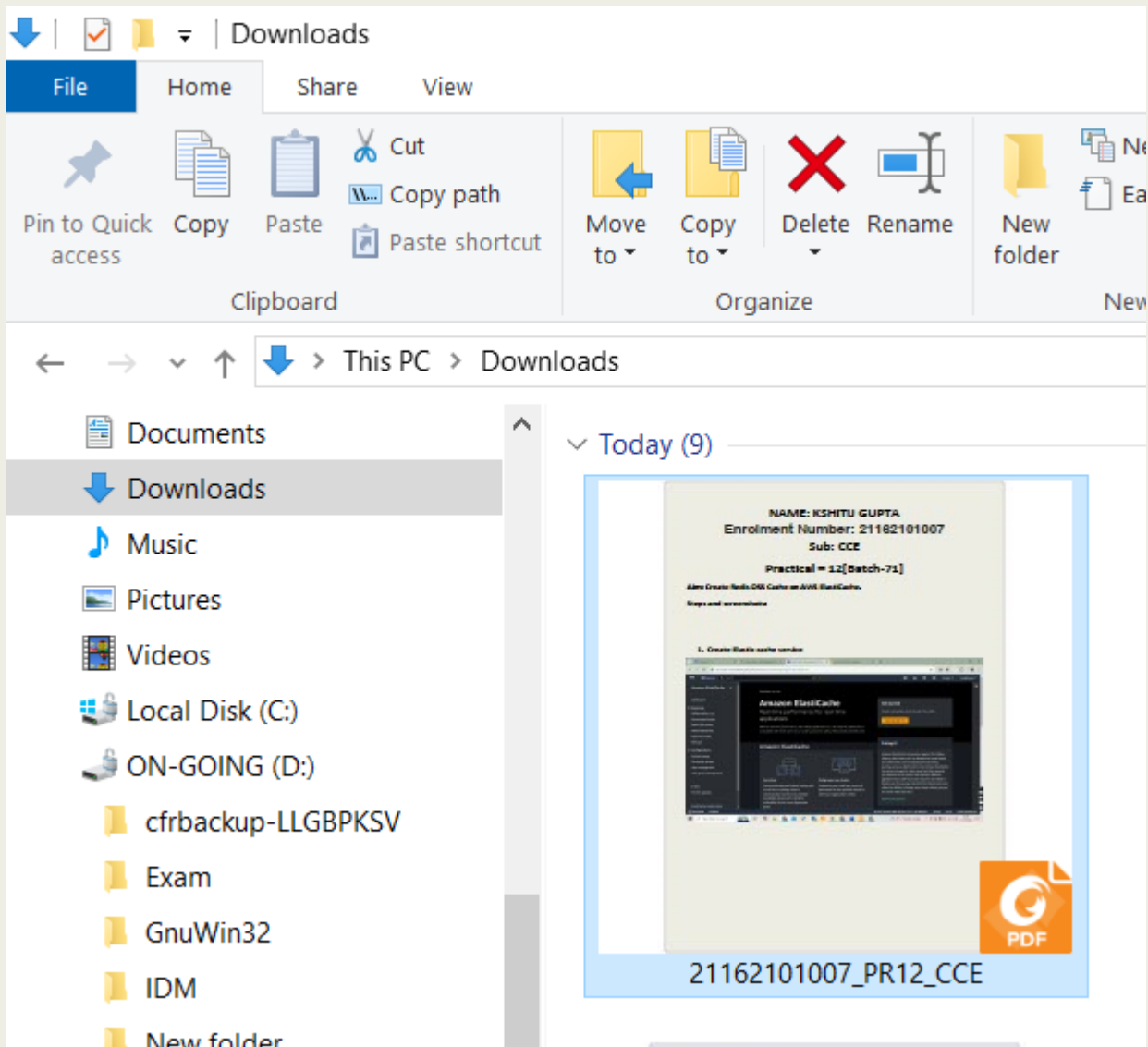


Now download this file to your folder

```
C:\Users\Kshitij>aws s3 cp s3://kshitij-s3-bucket-2-cli/21162101007_PR12_CCE.pdf C:\Users\Kshitij\Downloads\
download: s3://kshitij-s3-bucket-2-cli/21162101007_PR12_CCE.pdf to Downloads\21162101007_PR12_CCE.pdf

C:\Users\Kshitij>
C:\Users\Kshitij>
```

Here we can see that it's downloaded



We can it folder by with following command

```
Command Prompt
C:\Users\Kshitij>aws s3 ls s3://kshitij-s3-bucket-2-cli/21162101007_PR12_CCE.pdf
2024-10-21 09:00:02    3966335 21162101007_PR12_CCE.pdf
C:\Users\Kshitij>_
```

We can delete the file with this following command

```
Command Prompt

C:\Users\Kshitij>aws s3 rm s3://kshitij-s3-bucket-2-cli/21162101007_PR12_CCE.pdf
delete: s3://kshitij-s3-bucket-2-cli/21162101007_PR12_CCE.pdf

C:\Users\Kshitij>
```

Now delete the command by using command “Aws s3 rb bucketname”

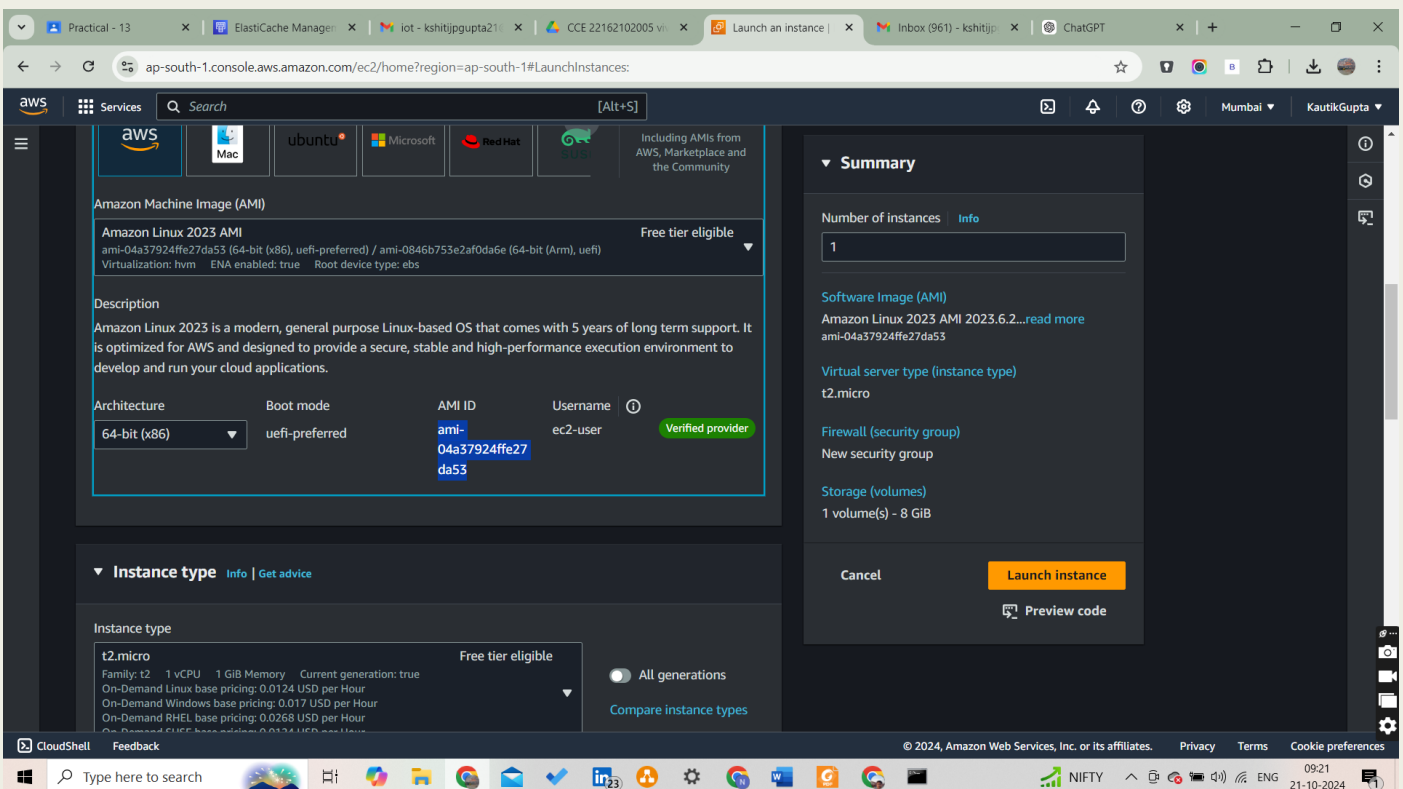
```
Command Prompt

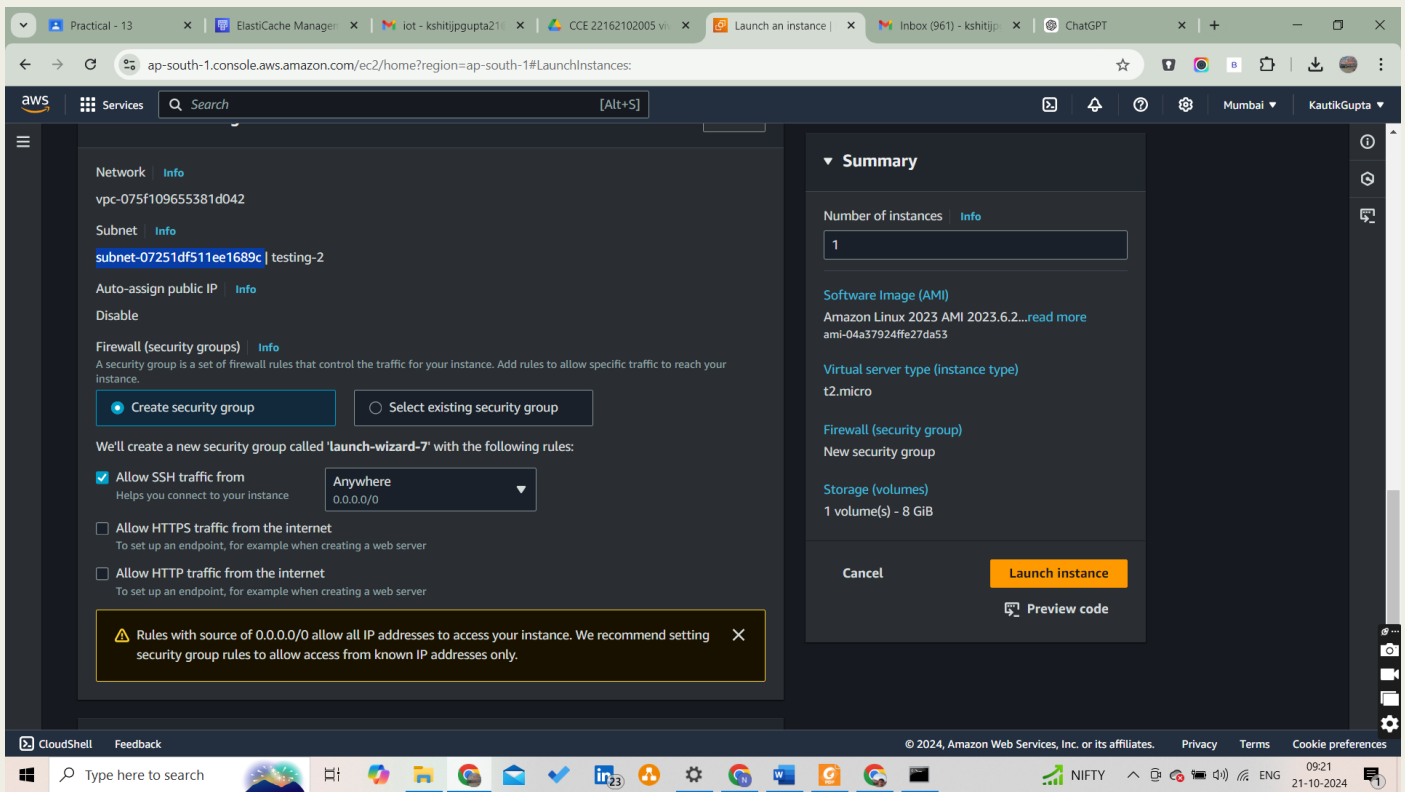
C:\Users\Kshitij>aws s3 rm s3://kshitij-s3-bucket-2-cli/21162101007_PR12_CCE.pdf
delete: s3://kshitij-s3-bucket-2-cli/21162101007_PR12_CCE.pdf

C:\Users\Kshitij>aws s3 rb s3://kshitij-s3-bucket-2-cli
remove_bucket: kshitij-s3-bucket-2-cli

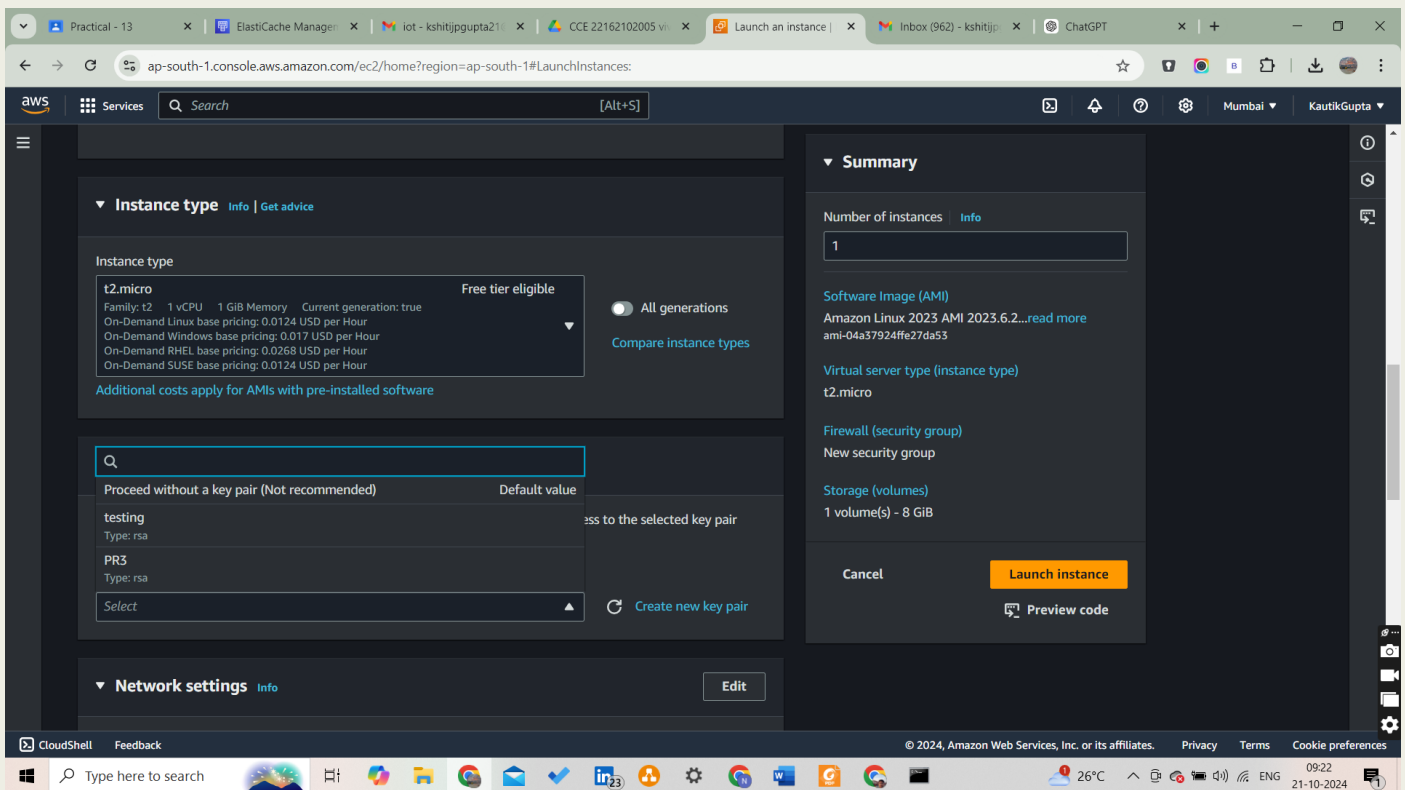
C:\Users\Kshitij>
```

Copy this AWS AMI-id and Subnet-id

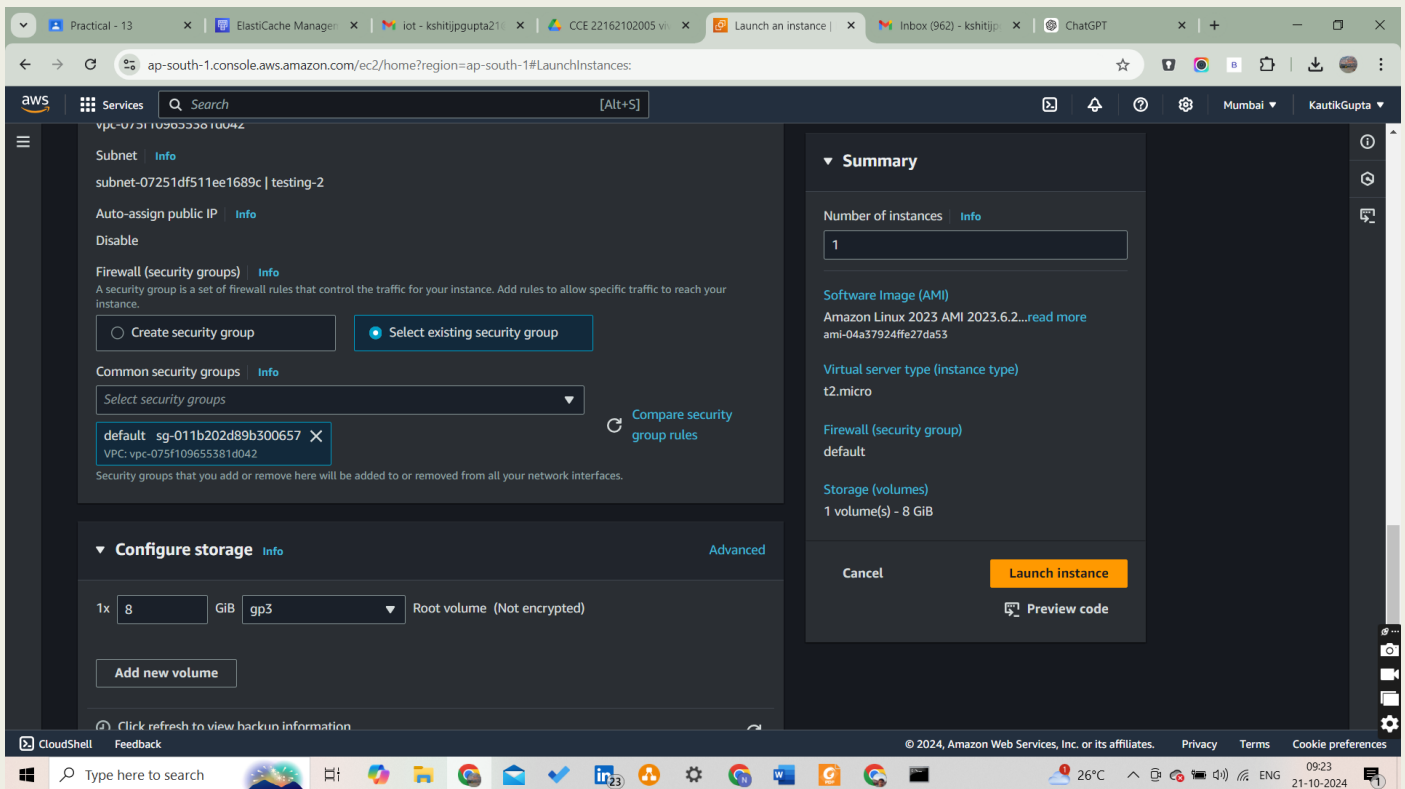




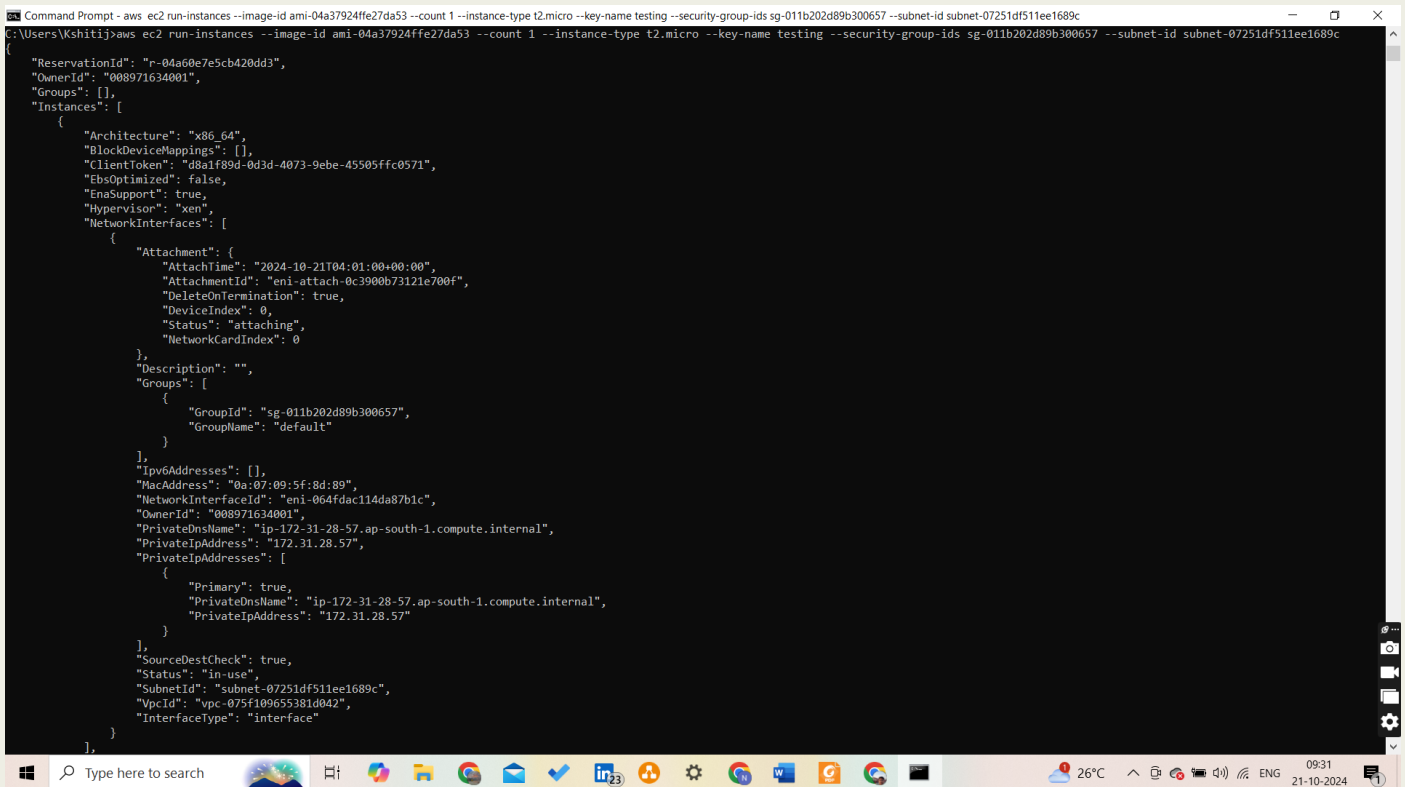
key pair name:



Security group ID



Now run the command and add that all id in this command by below screenshot



Se we can see in below screenshot that instance is running

The screenshot shows the AWS Management Console for the 'ap-south-1' region. The 'Instances' page is active, displaying a list of instances. The instance 'CLI' (i-018fa65cb7b09c18c) is selected, and its details are shown in the 'Details' tab. The instance is in the 'Running' state. The 'Instance summary' section shows the instance ID, public IPv4 address, private IPv4 addresses, instance state, public IPv4 DNS, and private IP DNS name.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
testing	i-00056131a6dad5818	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b	-
CLI	i-018fa65cb7b09c18c	Running	t2.micro	Initializing	View alarms +	ap-south-1b	-

i-018fa65cb7b09c18c (CLI)

Instance summary

Instance ID	Public IPv4 address	Private IPv4 addresses
i-018fa65cb7b09c18c (CLI)	-	172.31.28.57
IPv6 address	Instance state	Public IPv4 DNS
-	Running	-
Hostname type	Private IP DNS name (IPv4 only)	
IP name: ip-172-31-28-57.ap-south-1.compute.internal	ip-172-31-28-57.ap-south-1.compute.internal	

Now run this following command to stop the instance

```
Command Prompt

C:\Users\Kshitij>
C:\Users\Kshitij>aws ec2 stop-instances --instance-ids i-018fa65cb7b09c18c
{
  "StoppingInstances": [
    {
      "InstanceId": "i-018fa65cb7b09c18c",
      "CurrentState": {
        "Code": 64,
        "Name": "stopping"
      },
      "PreviousState": {
        "Code": 16,
        "Name": "running"
      }
    }
  ]
}
```

C:\Users\Kshitij>i-018fa65cb7b09c18c

Also we can terminate with that command

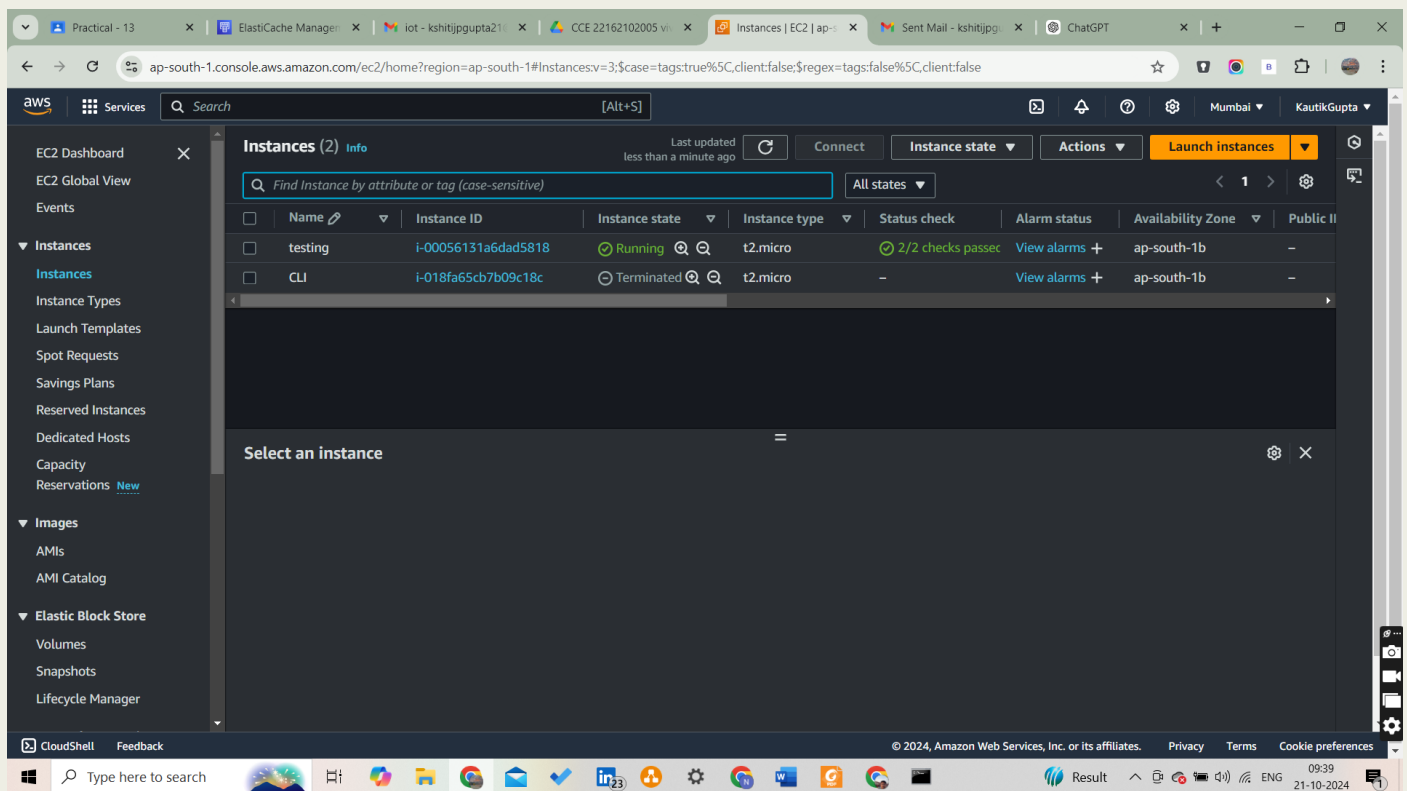
```
Command Prompt

C:\Users\Kshitij>aws ec2 terminate-instances --instance-ids i-018fa65cb7b09c18c

{
  "TerminatingInstances": [
    {
      "InstanceId": "i-018fa65cb7b09c18c",
      "CurrentState": {
        "Code": 48,
        "Name": "terminated"
      },
      "PreviousState": {
        "Code": 80,
        "Name": "stopped"
      }
    }
  ]
}
```

C:\Users\Kshitij>

Termination screen short:



Now run command to create user

```
C:\Users\Kshitij>aws iam create-user --user-name kshitijgupta505
```

```
{  
  "User": {  
    "Path": "/",  
    "UserName": "kshitijgupta505",  
    "UserId": "AIDAQEFWAIVI7I267LF2C",  
    "Arn": "arn:aws:iam::008971634001:user/kshitijgupta505",  
    "CreateDate": "2024-10-21T04:10:42+00:00"  
  }  
}
```

```
C:\Users\Kshitij>
```