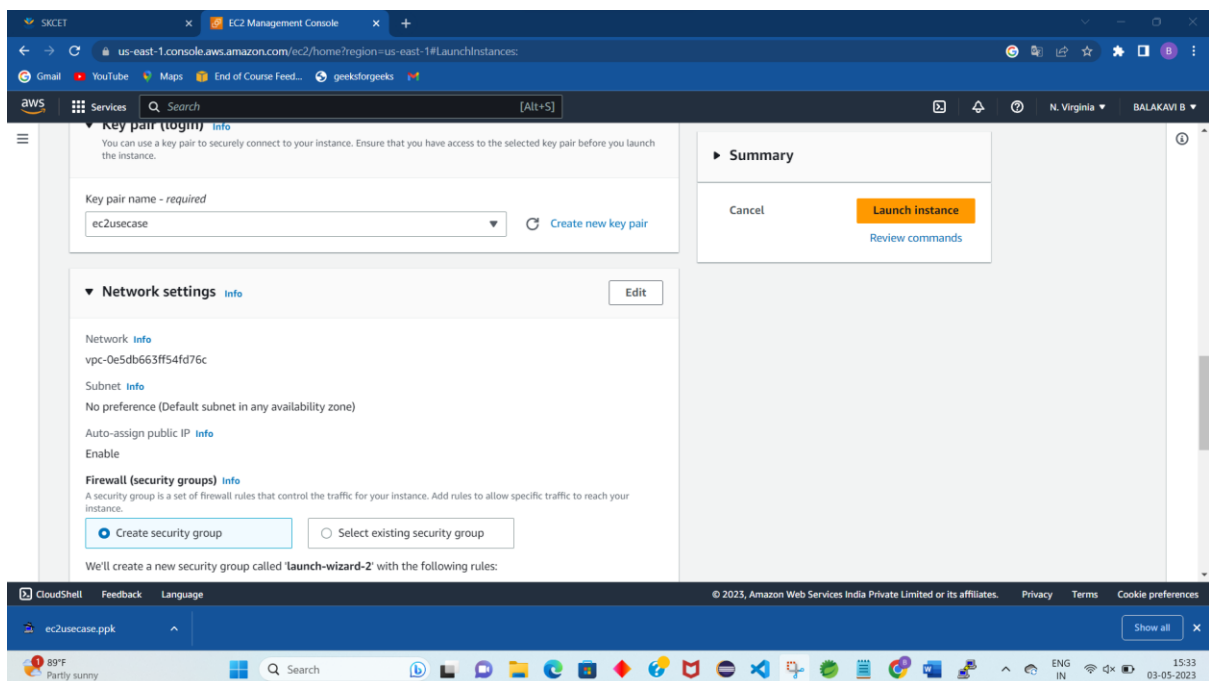
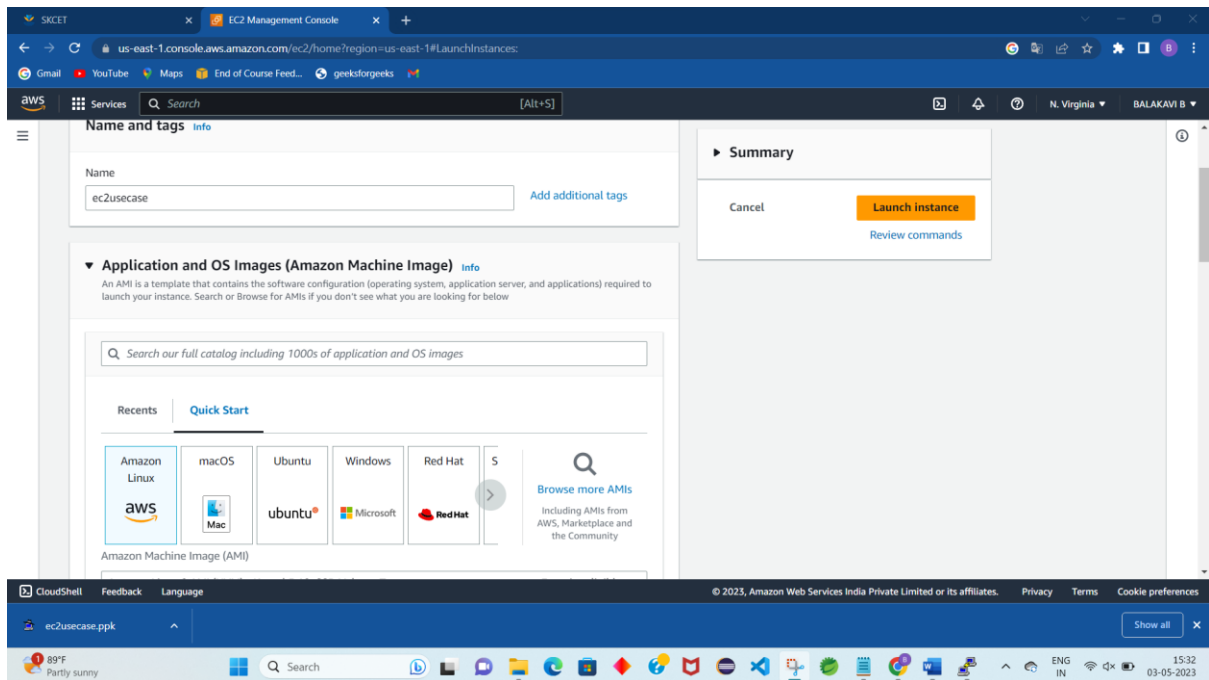


## QUESTION NO 1:



EC2 Management Console

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:

Search [Alt+S]

New EC2 Experience

EC2 Dashboard

EC2 Global View

Events

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

Instances (1/1) Info

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
ec2usecase	i-0db94612f9033d7e0	Running	t2.micro	-	No alarms	us-east-1a	ec2-54-91-100-159

Instance: i-0db94612f9033d7e0 (cclinux1)

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

ec2usecase.ppk Show all

89°F Partly sunny

Search

ENG IN

15:24 03-05-2023

EC2 Management Console

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

Search [Alt+S]

Firewall (security groups) info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

We'll create a new security group called 'launch-wizard-2' with the following rules:

☒ Allow SSH traffic from

☐ Allow HTTPS traffic from the internet

☐ Allow HTTP traffic from the internet

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Configure storage info Advanced

1x 8 GiB gp2 Root volume (Not encrypted)

Summary

Cancel Launch instance Review commands

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

ec2usecase.ppk Show all

89°F Partly sunny

Search

ENG IN

15:35 03-05-2023

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:visibility=owned-by-me

Instances (1/2) Info

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
ec2usecase	i-0c70af2176d4bd58c	Running	t2.micro	Initializing	No alarms	us-east-1a	ec2-54-164-162-
ec2usecase	i-0db94612f9033d7e0	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-54-91-100-1

Instance: i-0c70af2176d4bd58c (ec2usecase)

Details Security Networking Storage Status checks Monitoring Tags

Security details

IAM Role: -

Owner ID: 411708117514

Launch time: Wed May 03 2023 15:36:24 GMT+0530 (India Standard Time)

Security groups: sg-05b947e4c992bc63c (launch-wizard-2)

Inbound rules

Filter rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups
------	------------------------	------------	----------	--------	-----------------

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

Auto-assign public IP info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

We'll create a new security group called 'launch-wizard-3' with the following rules:

☒ Allow SSH traffic from   
Helps you connect to your instance   
Anywhere   
0.0.0.0/0

☐ Allow HTTPS traffic from the internet   
To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet   
To set up an endpoint, for example when creating a web server

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Configure storage Info Advanced

1x 8 GIB gp3 Root volume (Not encrypted)

Summary

Number of instances Info   
1

Software Image (AMI)   
Amazon Linux 2023 AMI 2023.0.2...read more   
ami-02396cdd13e9a1257

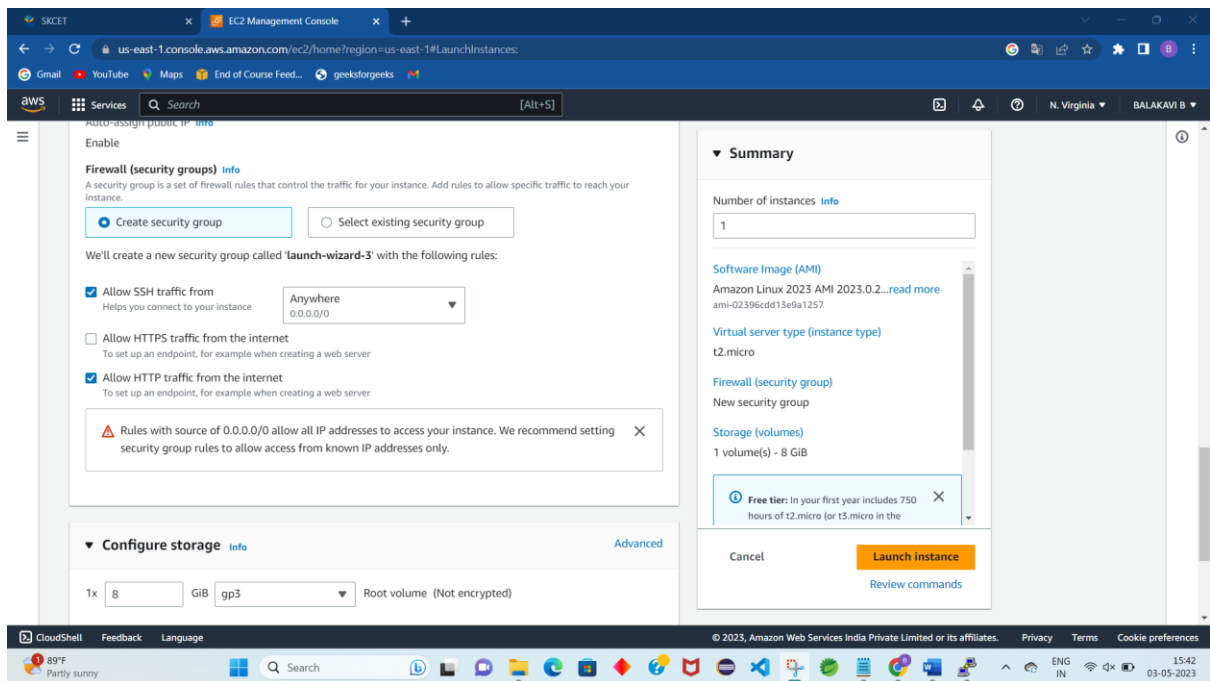
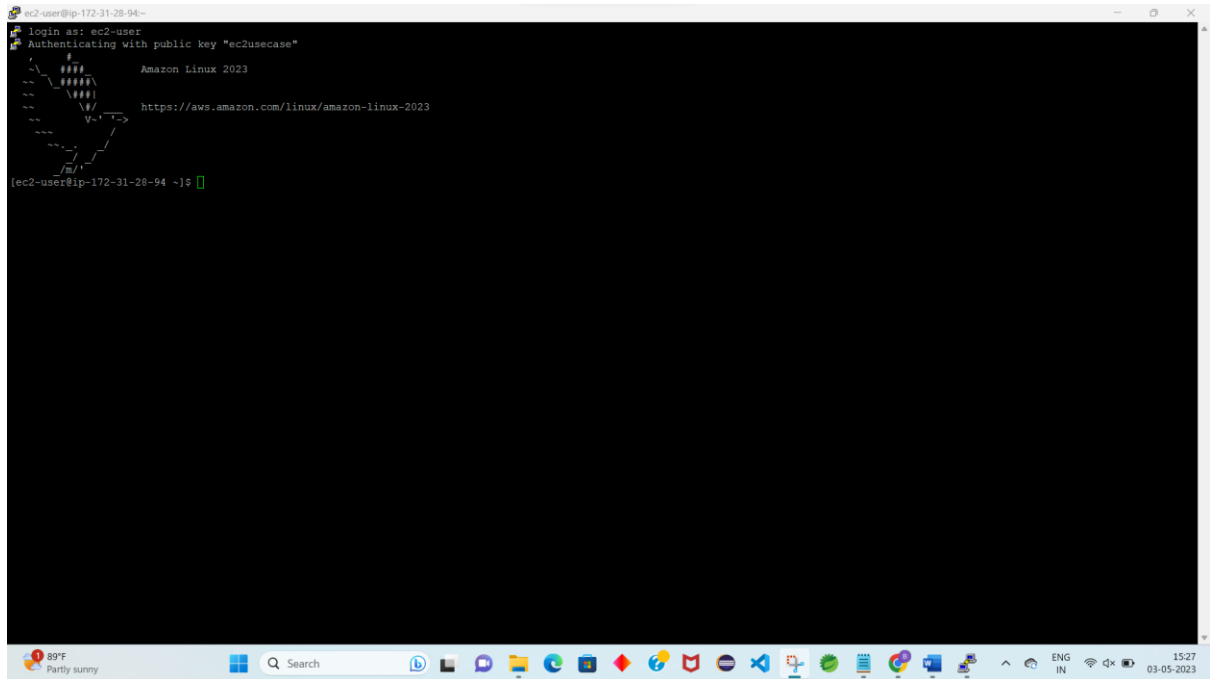
Virtual server type (instance type)   
t2.micro

Firewall (security group)   
New security group

Storage (volumes)   
1 volume(s) - 8 GIB

Free tier: In your first year includes 750 hours of t2.micro for t3.micro in the

Cancel Launch instance   
Review commands



## QUESTION NO:2

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity

Network-L1-Team user group created. View group

IAM > User groups

User groups (1) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	Network-L1-Team	Loading	Defined	Now

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

88°F Partly sunny

Search

ENG IN 15:55 03-05-2023

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity

User created successfully View user

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

IAM > Users

Users (1) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	Network-L1-User1	None	Never	None	None	-

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

88°F Partly sunny

Search

ENG IN 15:47 03-05-2023

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/groups/create

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analysers

Settings

Credential report

Organization activity

Add users to the group - Optional (1) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

Search

User name	Groups	Last activity	Creation time
Network-L1-User1	0	None	3 minutes ago

Attach permissions policies - Optional (Selected 1/843) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter policies by property or policy name and press enter. 1 match

\*AmazonVPCReadOnlyAccess X Clear filters

Policy name	Type	Description
AmazonVPCReadOnlyAccess	AWS managed	Provides read only access to Amazon VPC via the AWS Manage...

Cancel Create group

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

88°F Partly sunny

Search

ENG IN 15:52 03-05-2023

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/groups/create

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analysers

Settings

Credential report

Organization activity

Add users to the group - Optional (1) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

Search

User name	Groups	Last activity	Creation time
Network-L1-User1	0	None	3 minutes ago

Attach permissions policies - Optional (Selected 2/843) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter policies by property or policy name and press enter. 1 match

\*AWSNetworkManagerReadOnlyAccess X Clear filters

Policy name	Type	Description
AWSNetworkManagerReadOnlyAccess	AWS managed	Provides read only access to Amazon NetworkManager via the A...

Cancel Create group

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

88°F Partly sunny

Search

ENG IN 15:53 03-05-2023

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/groups/details/Network-L1-Team?section=permissions

Services

Search

[Alt+S]

GlobalBALAKAVI B

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Credential report

Organization activity

IAM > User groups > Network-L1-Team

Network-L1-Team

Delete

Summary

Edit

User group name

Creation time

ARN

Network-L1-Team

May 03, 2023, 15:55 (UTC+05:30)

arn:aws:iam::411708117514:group/Network-L1-Team

Users

Permissions

Access Advisor

Permissions policies (2) Info

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

Policy name

Type

Description

☐

AmazonVPCReadOnlyAccess

AWS managed

Provides read only access to Amazon VPC via the AWS Management Console.

☐

AWSNetworkManagerReadOnlyAccess

AWS managed

Provides read only access to Amazon NetworkManager via the AWS Management Co...

CloudShell

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates.

Privacy

Terms

Cookie preferences

88°F

Partly sunny

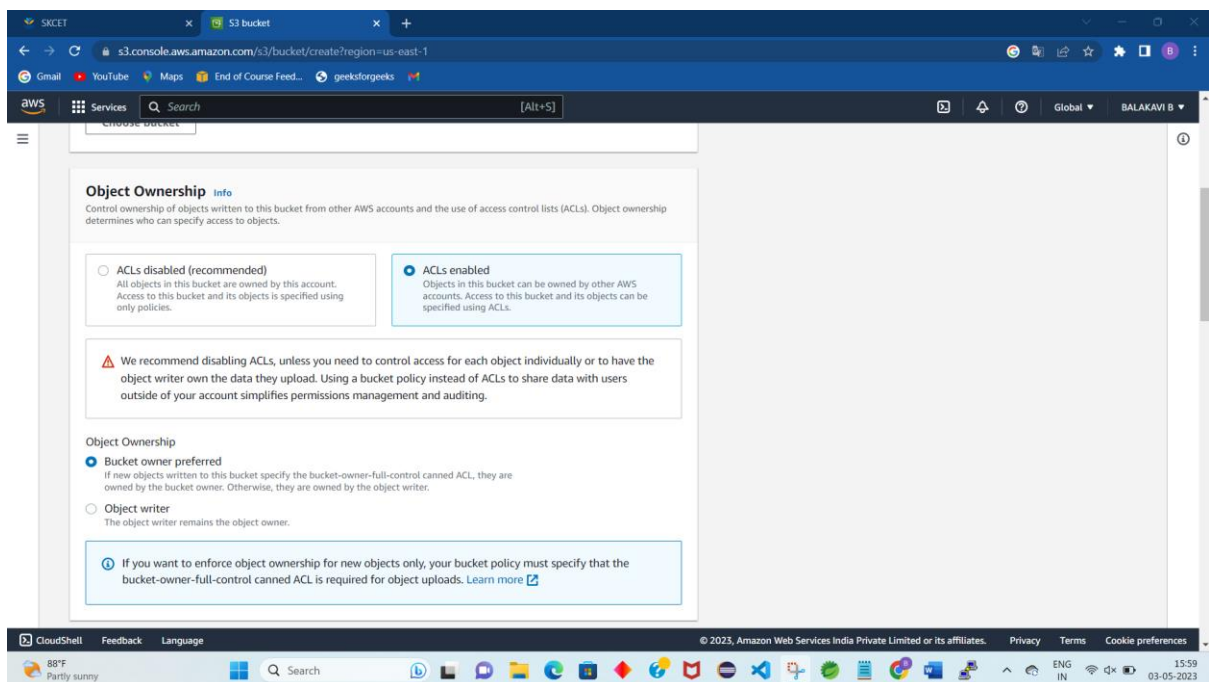
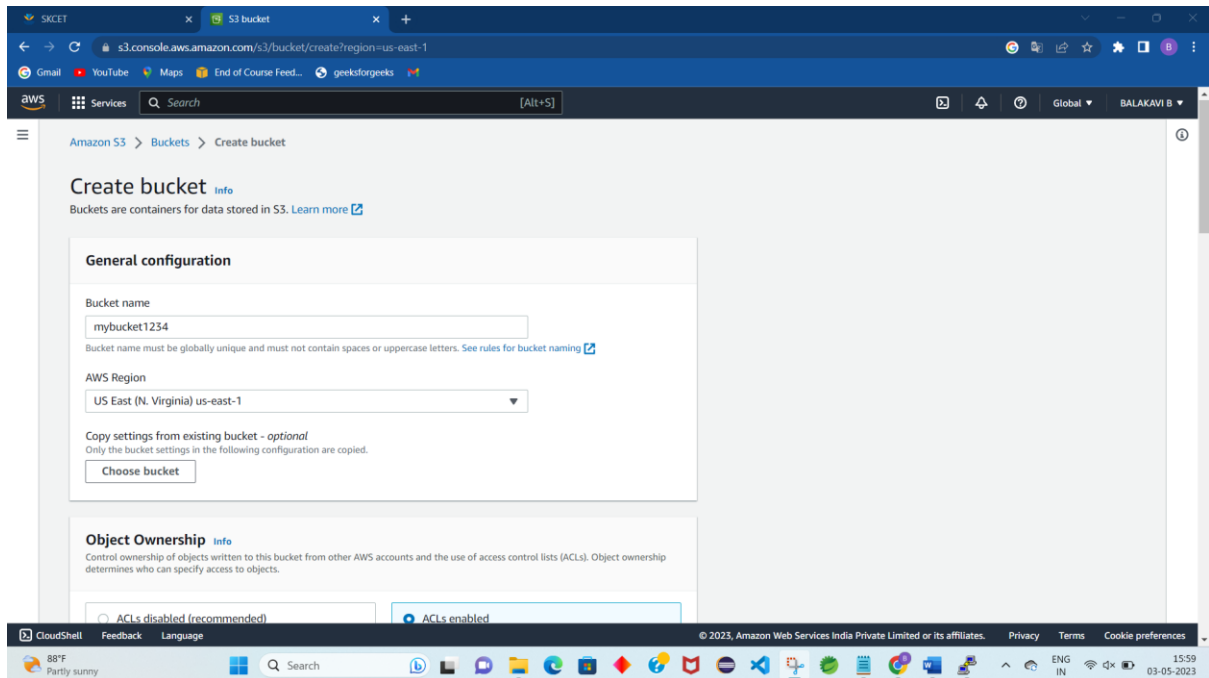
Search

ENG IN

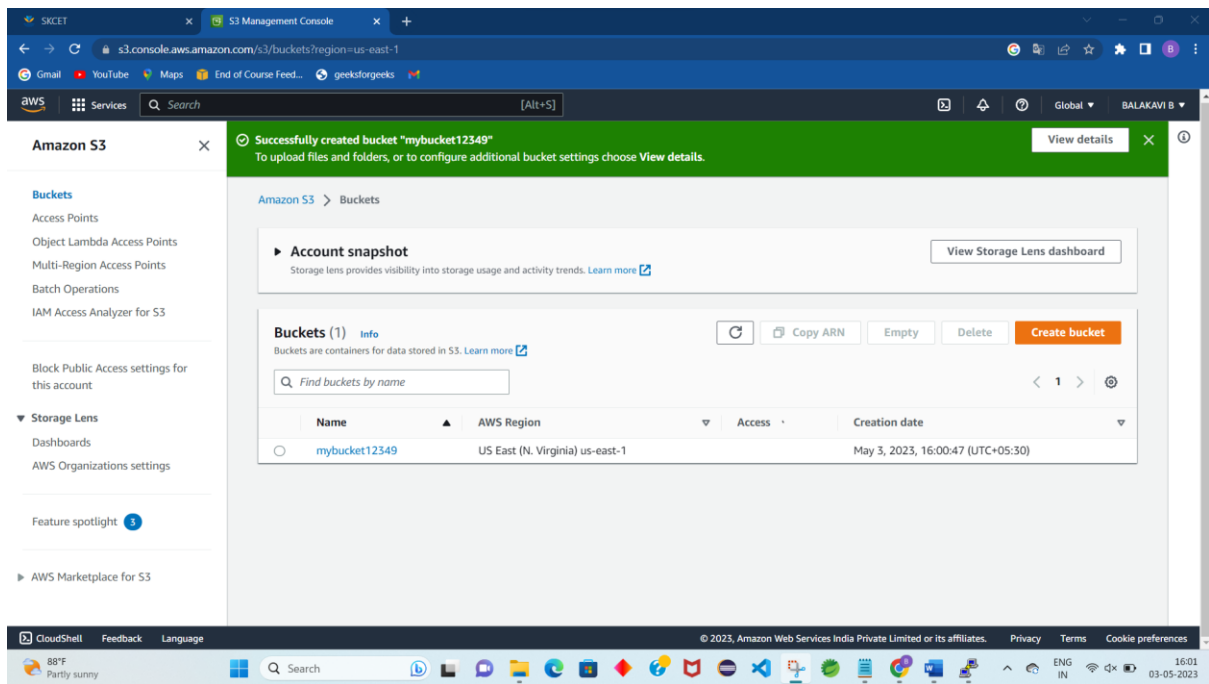
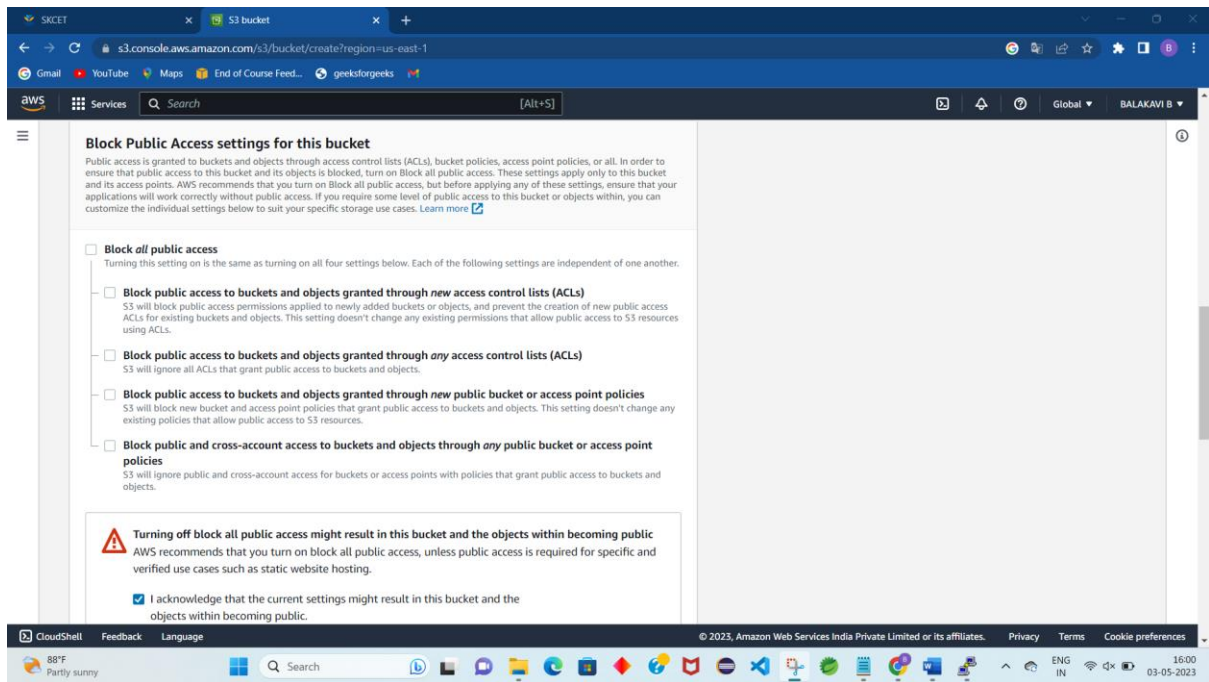
15:56

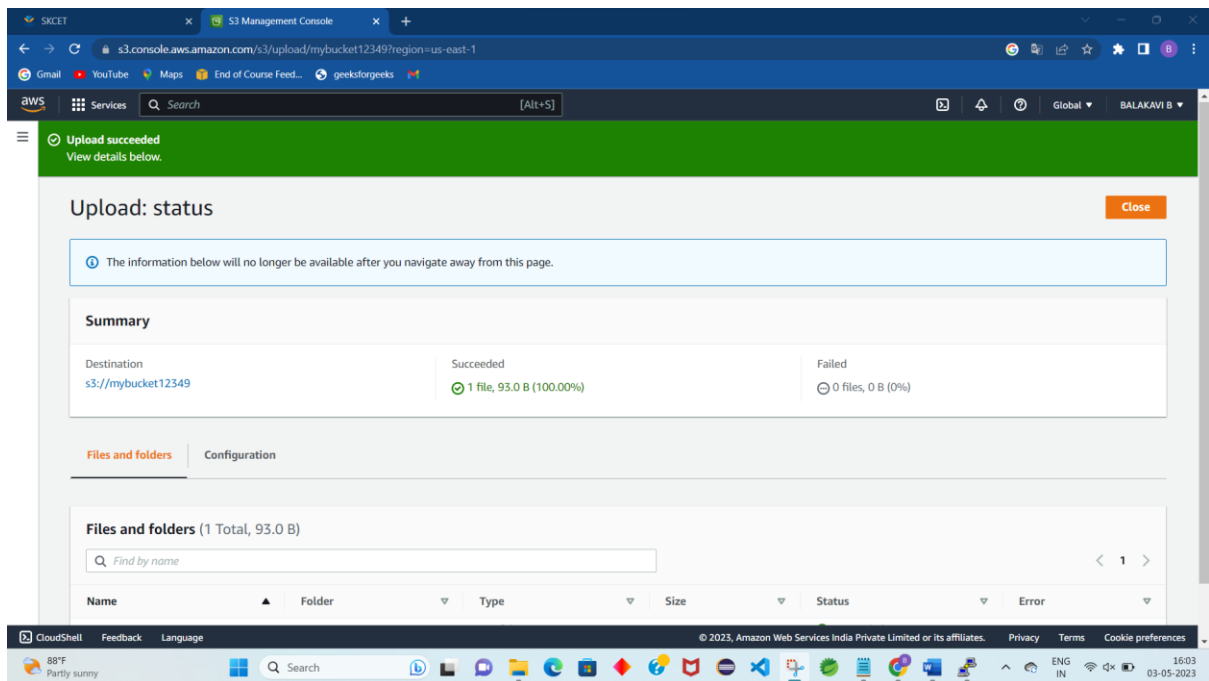
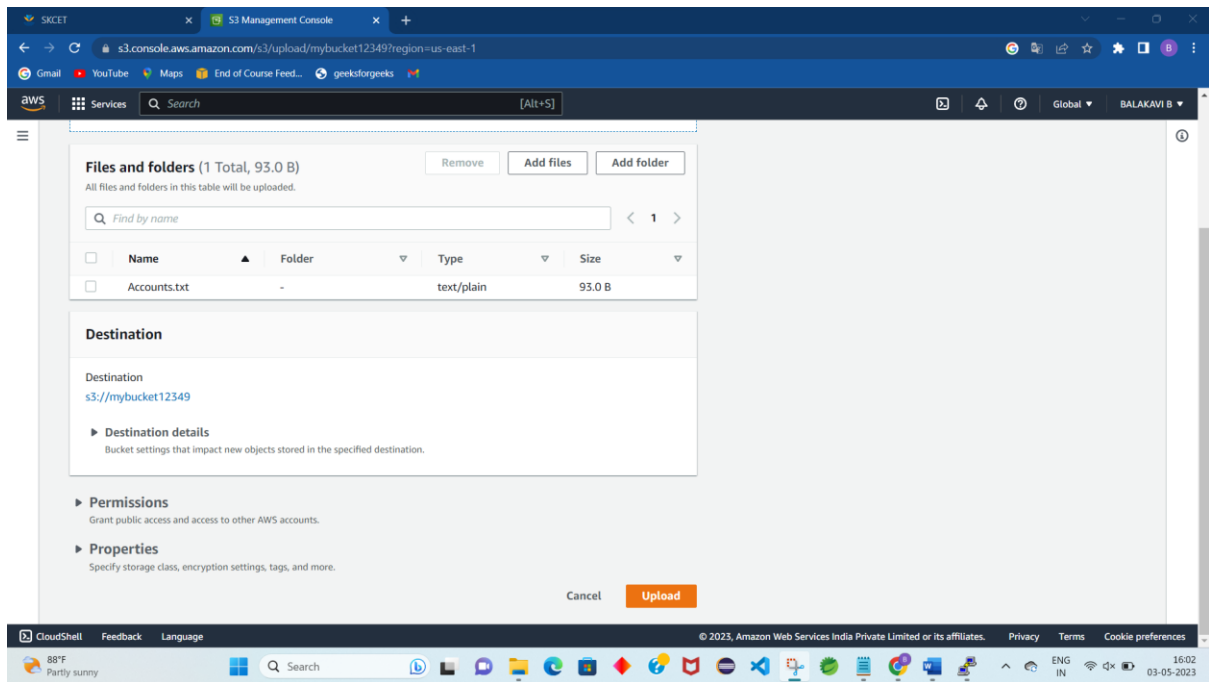
03-05-2023

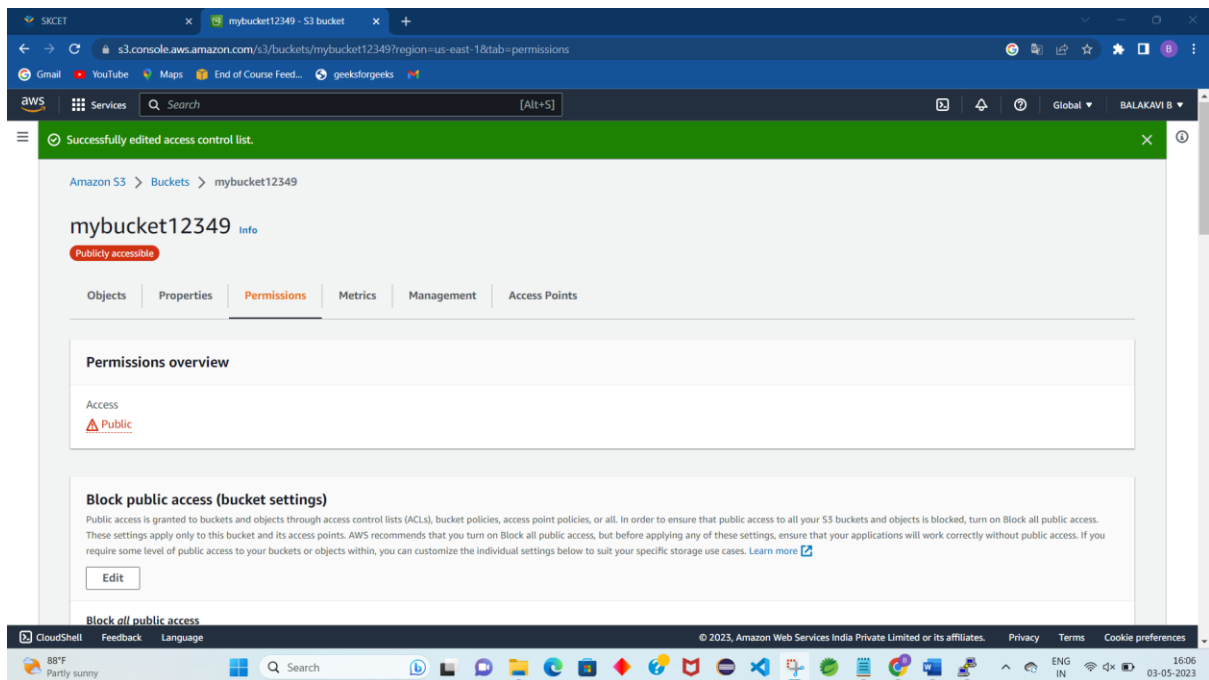
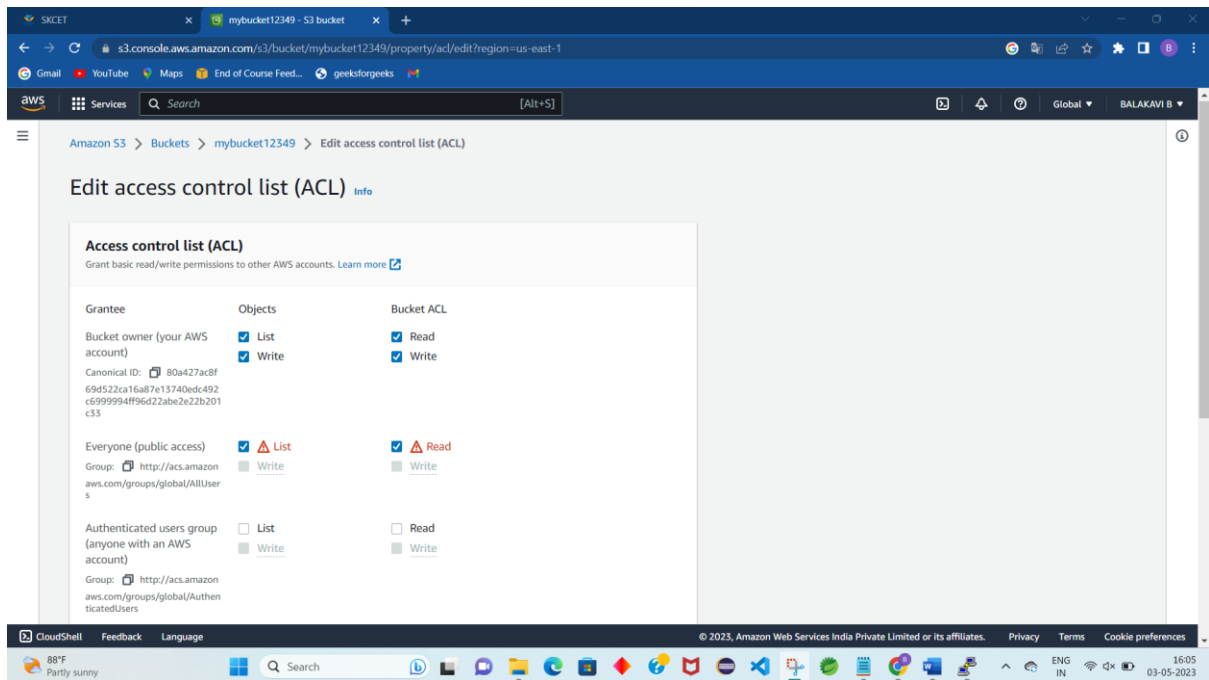
## QUESTION NO: 3











SKCET mybucket12349 - S3 bucket https://mybucket12349.s3.amazonaws.com/

s3.console.aws.amazon.com/s3/buckets/mybucket12349/object/edit\_public\_read\_access?region=us-east-1&showversions=false

Amazon S3 > Buckets > mybucket12349 > Make public

## Make public info

The make public action enables public read access in the object access control list (ACL) settings. [Learn more](#)

⚠ When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.

### Specified objects

Find objects by name

< 1 >

Name	Type	Last modified	Size
Accounts.txt	txt	May 3, 2023, 16:03:24 (UTC+05:30)	93.0 B

Cancel **Make public**

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

88°F Partly sunny Search 16:08 03-05-2023

SKCET S3 Management Console https://mybucket12349.s3.amazonaws.com/

mybucket12349.s3.amazonaws.com/Accounts.txt

Network-L1-User1  
Network-L1-Team  
AmazonVPCReadOnlyAccess  
AWSNetworkManagerReadOnlyAccess

88°F Partly sunny Search 16:08 03-05-2023