

# AWS CLOUD COMPUTING

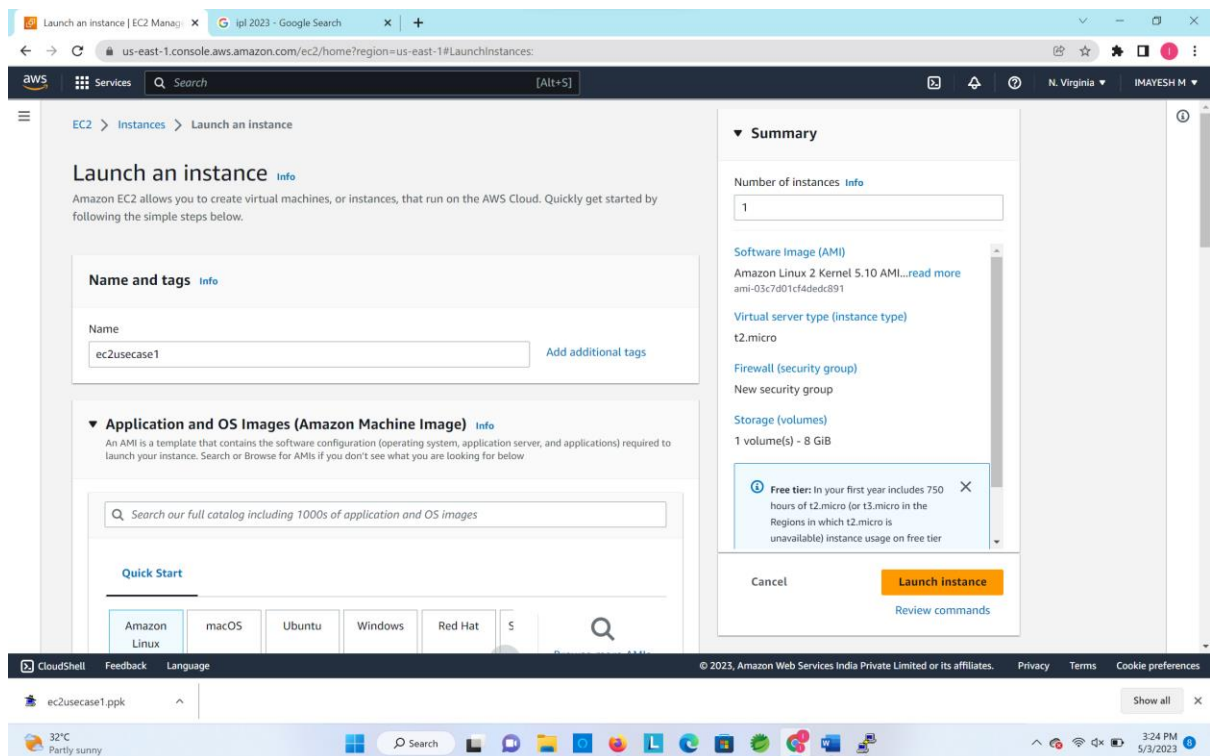
## CODING CONTEST – I

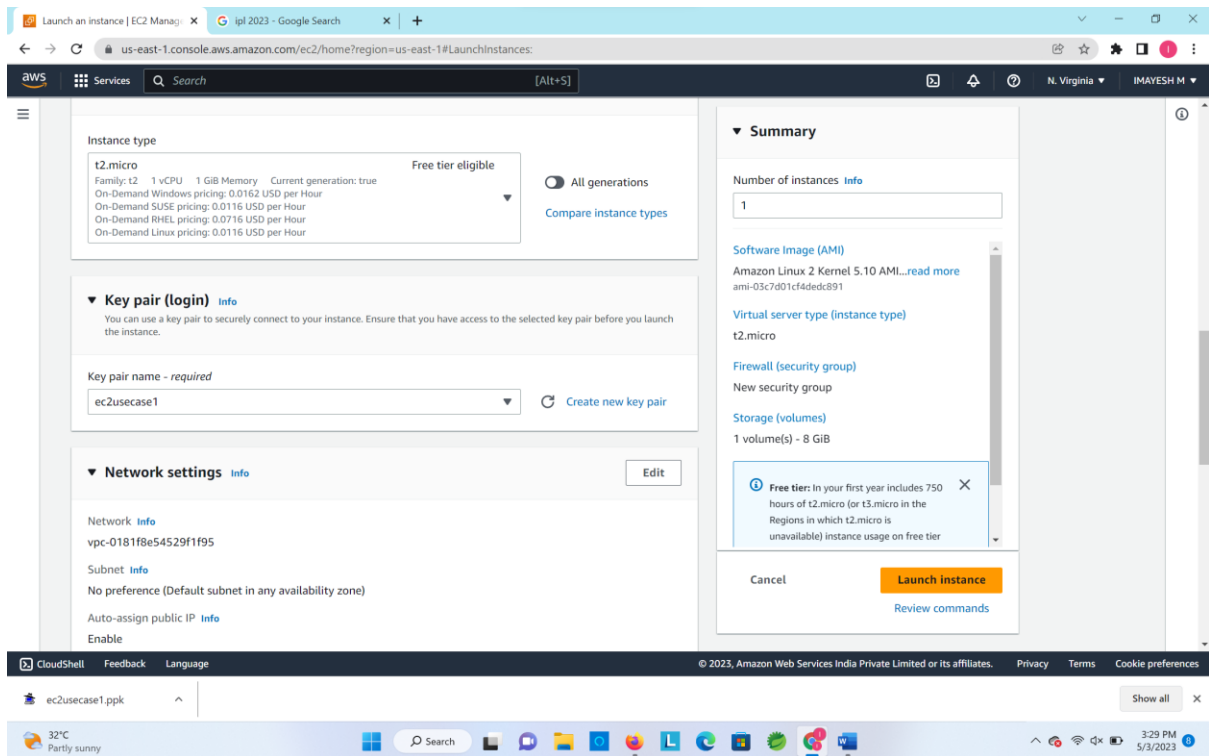
727721EUIT055

M.IMAYESH

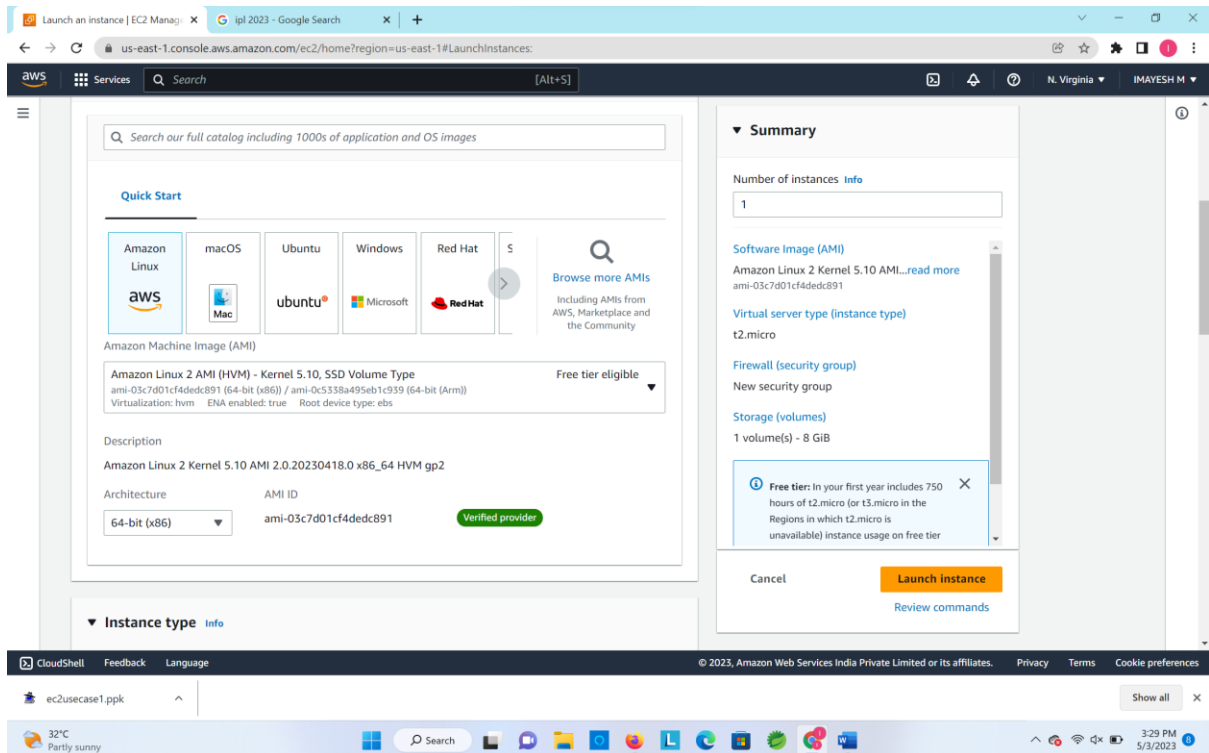
Q1:

1.

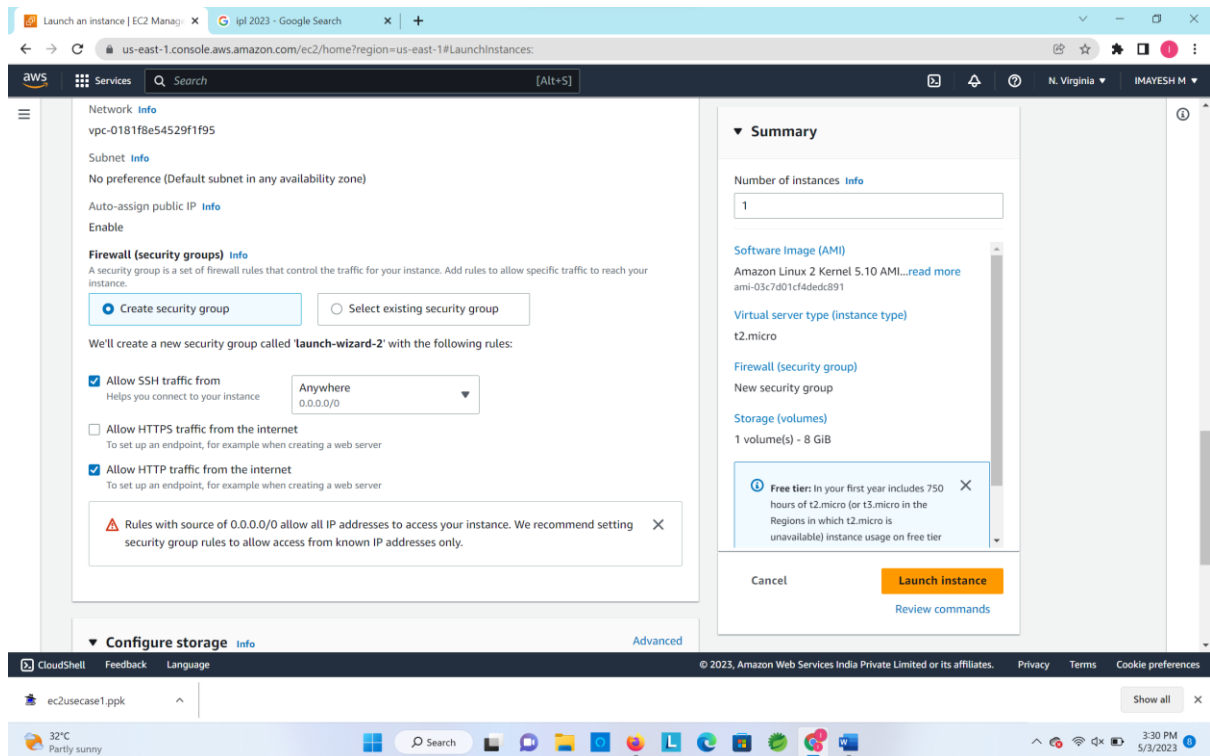




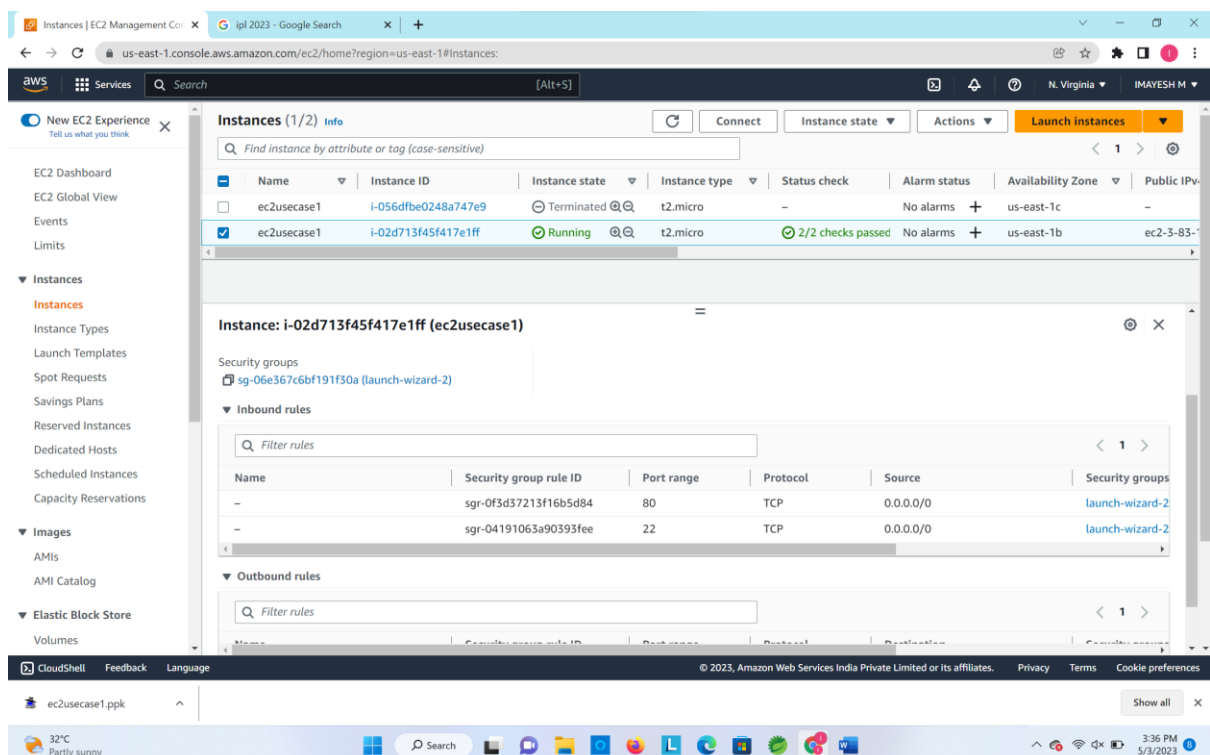
2.



3,4.



## Creation of EC2 Instance:



## Q2:

1.

**Create user group**

**Name the group**

User group name  
Enter a meaningful name to identify this group.  
  
Maximum 128 characters. Use alphanumeric and "+=, @\_-." characters.

**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.

| <input type="checkbox"/> | User name        | Groups | Last activity | Creation time |
|--------------------------|------------------|--------|---------------|---------------|
| <input type="checkbox"/> | Network-L1-User1 | 0      | None          | 4 minutes ago |

**Attach permissions policies - Optional (Selected 2/843) info**

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

2.

**Create user group**

**Name the group**

User group name  
Enter a meaningful name to identify this group.  
  
Maximum 128 characters. Use alphanumeric and "+=, @\_-." characters.

**Add users to the group - Optional (Selected 1/1) 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.

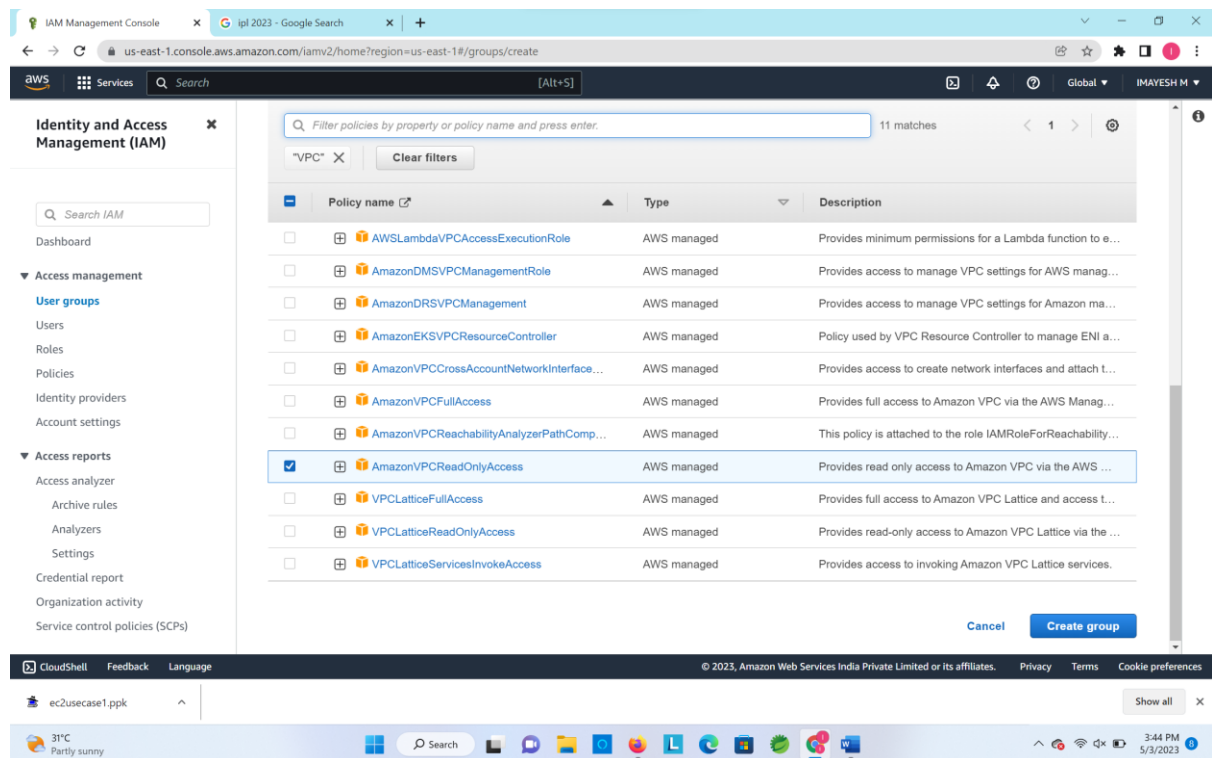
| <input checked="" type="checkbox"/> | User name        | Groups | Last activity | Creation time |
|-------------------------------------|------------------|--------|---------------|---------------|
| <input checked="" type="checkbox"/> | Network-L1-User1 | 0      | None          | 4 minutes ago |

**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.

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

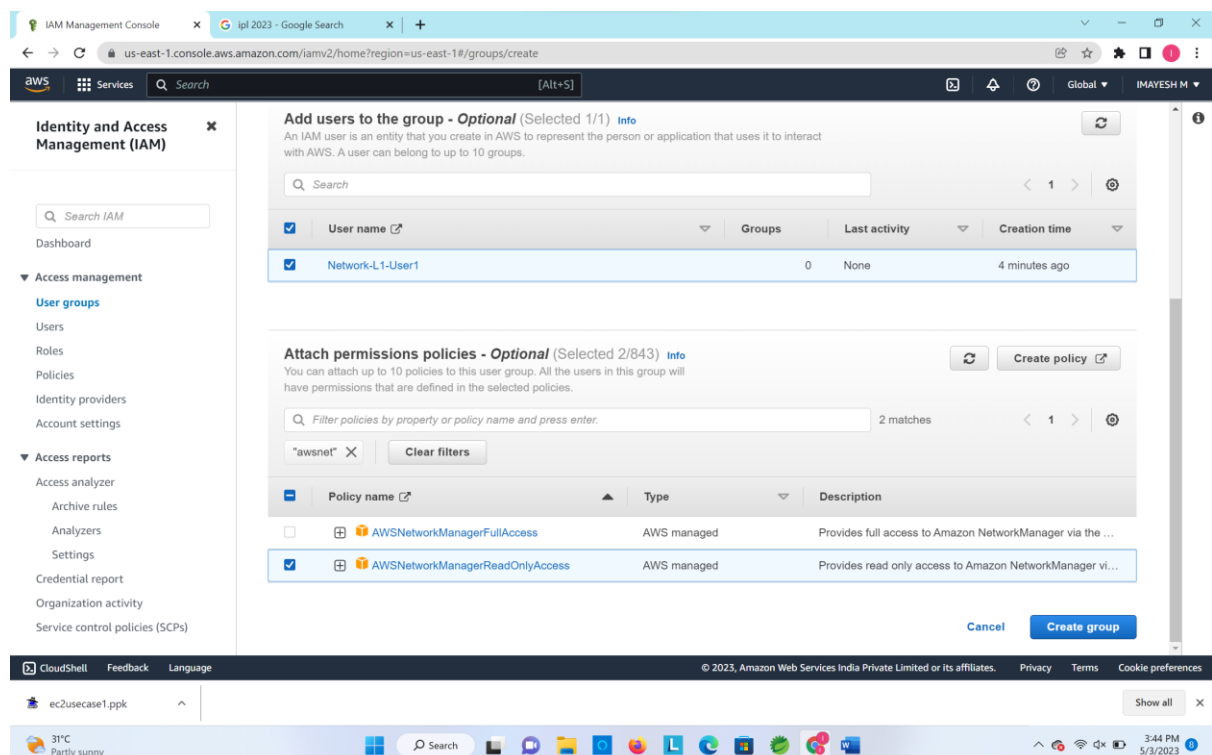
3.



The screenshot shows the AWS IAM Management Console interface. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and CloudShell. The main content area is titled 'Create group' and shows a search bar with the filter 'VPC'. Below the search bar, a table lists 11 AWS managed policies. The 'AmazonVPCReadOnlyAccess' policy is selected, highlighted in blue. The table columns are Policy name, Type, and Description.

| Policy name                              | Type        | Description   |
|--|-------------|---|
| AWSLambdaVPCAccessExecutionRole          | AWS managed | Provides minimum permissions for a Lambda function to e...    |
| AmazonDMSVPCManagementRole               | AWS managed | Provides access to manage VPC settings for AWS manag...       |
| AmazonDRSVPCManagement                   | AWS managed | Provides access to manage VPC settings for Amazon ma...       |
| AmazonEKSVPCResourceController           | AWS managed | Policy used by VPC Resource Controller to manage ENI a...     |
| AmazonVPCCrossAccountNetworkInterface... | AWS managed | Provides access to create network interfaces and attach t...  |
| AmazonVPCFullAccess                      | AWS managed | Provides full access to Amazon VPC via the AWS Manag...       |
| AmazonVPCReachabilityAnalyzerPathComp... | AWS managed | This policy is attached to the role IAMRoleForReachability... |
| <b>AmazonVPCReadOnlyAccess</b>           | AWS managed | Provides read only access to Amazon VPC via the AWS ...       |
| VPC_Lattice_FullAccess                   | AWS managed | Provides full access to Amazon VPC Lattice and access t...    |
| VPC_Lattice_ReadOnlyAccess               | AWS managed | Provides read-only access to Amazon VPC Lattice via the ...   |
| VPC_Lattice_Services_InvokeAccess        | AWS managed | Provides access to invoking Amazon VPC Lattice services.      |

4.



The screenshot shows the AWS IAM Management Console interface. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and CloudShell. The main content area is titled 'Add users to the group - Optional' and shows a search bar with the filter 'awsnet'. Below the search bar, a table lists 2 AWS managed policies. The 'AWSNetworkManagerReadOnlyAccess' policy is selected, highlighted in blue. The table columns are Policy name, Type, and Description.

| Policy name                            | Type        | Description   |
|--|-------------|---|
| AWSNetworkManagerFullAccess            | AWS managed | Provides full access to Amazon NetworkManager via the ... |
| <b>AWSNetworkManagerReadOnlyAccess</b> | AWS managed | Provides read only access to Amazon NetworkManager vi...  |

## Creation of User:

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

Service control policies (SCPs)

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 a... | 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

ec2usecase1.ppk

31°C Partly sunny

Search

3:46 PM 5/3/2023

## Creation of User Groups:

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

Service control policies (SCPs)

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 | 1     | Defined     | Now           |

CloudShell Feedback Language

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

ec2usecase1.ppk

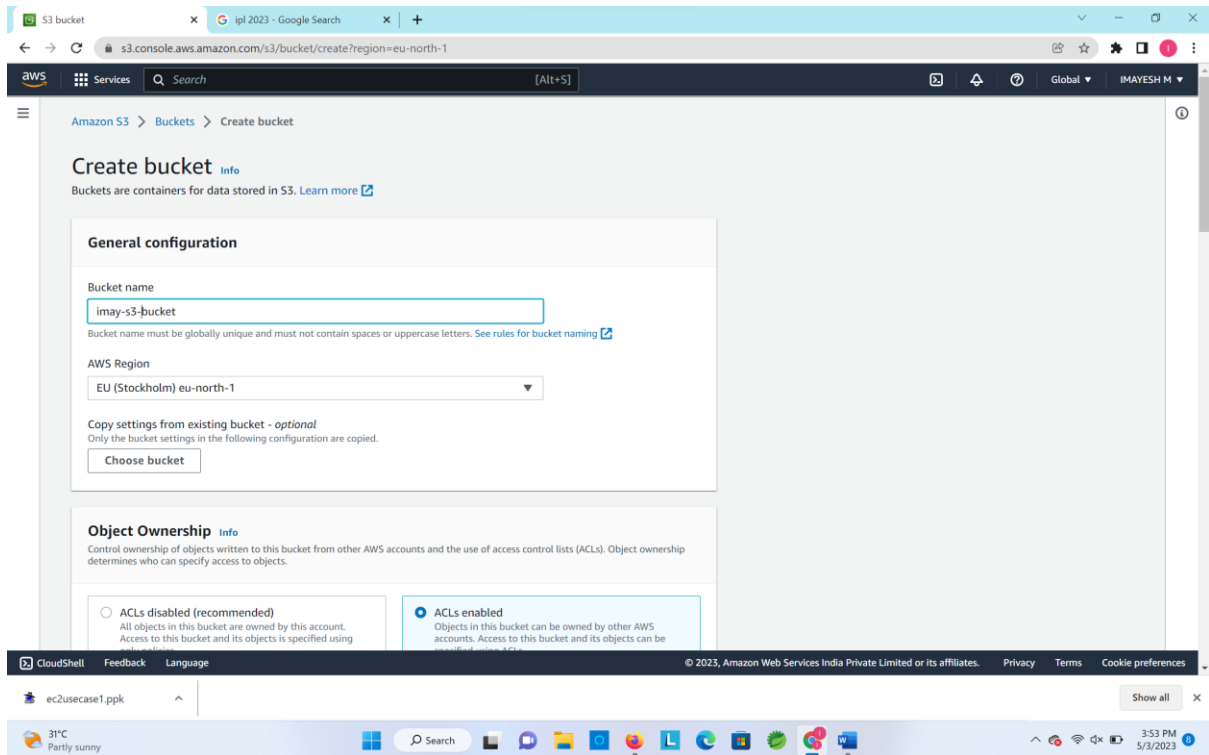
31°C Partly sunny

Search

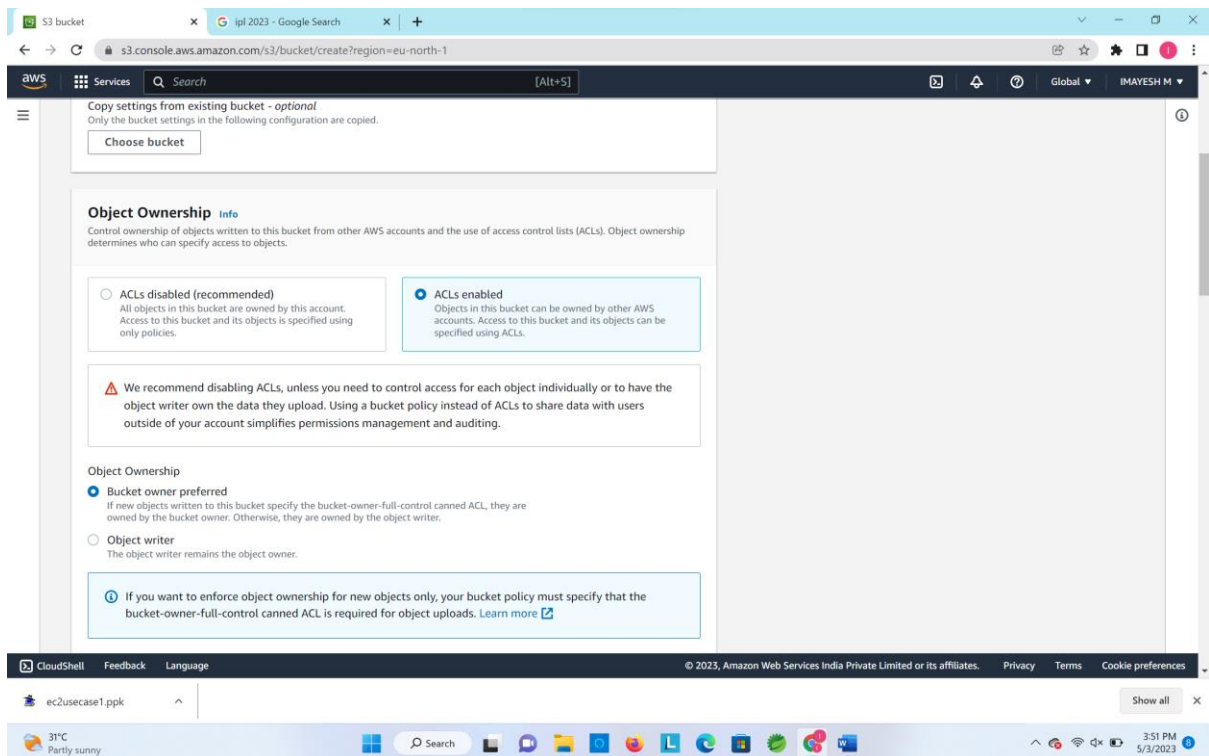
3:45 PM 5/3/2023

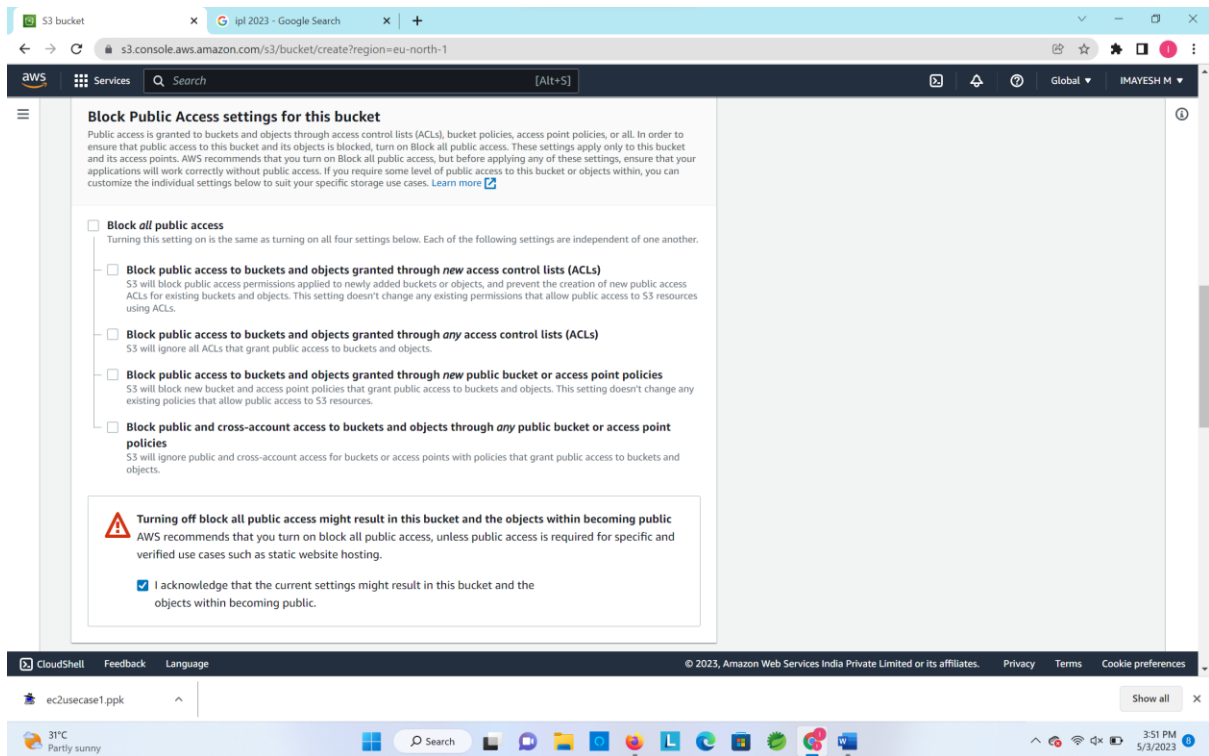
Q3:

1.

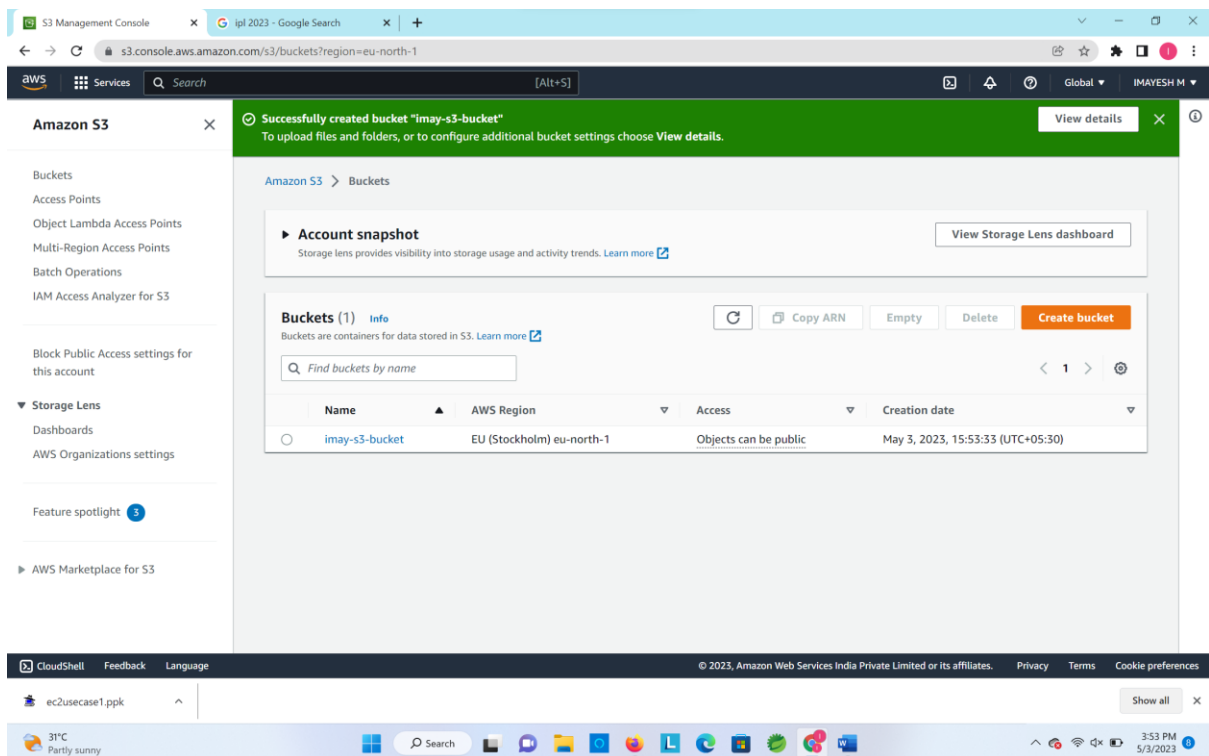


2.



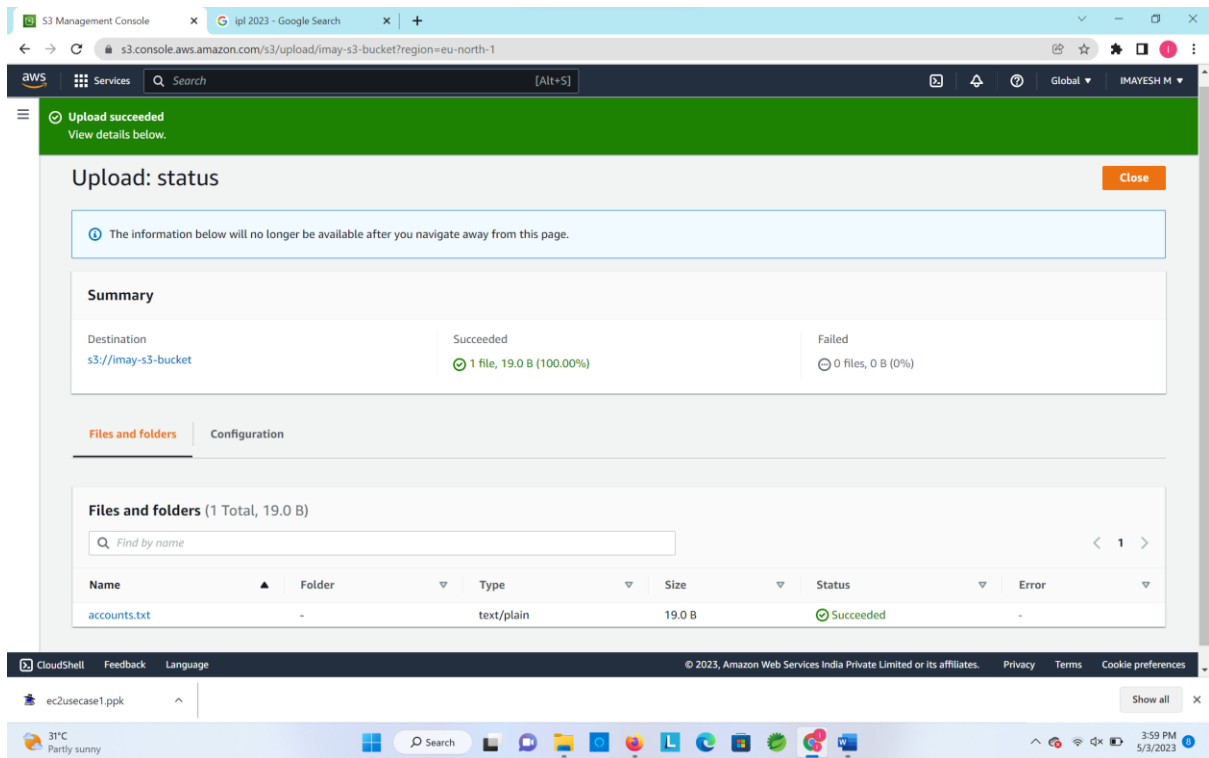


## Creation of S3 bucket:





3.



S3 Management Console

Upload succeeded  
View details below.

### Upload: status

The information below will no longer be available after you navigate away from this page.

**Summary**

|                                    |                                       |                             |
|------------------------------------|---------------------------------------|-----------------------------|
| Destination<br>s3://imay-s3-bucket | Succeeded<br>1 file, 19.0 B (100.00%) | Failed<br>0 files, 0 B (0%) |
|------------------------------------|---------------------------------------|-----------------------------|

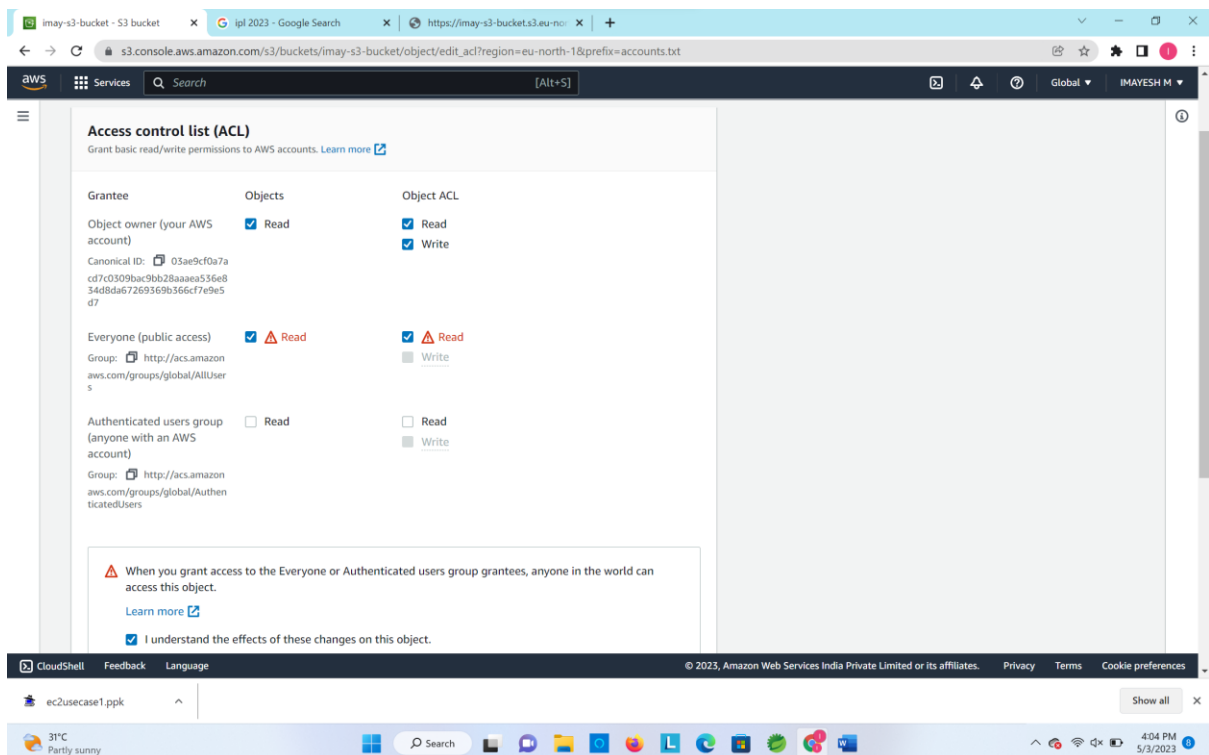
**Files and folders** | Configuration

Files and folders (1 Total, 19.0 B)

Find by name

| Name         | Folder | Type       | Size   | Status    | Error |
|--------------|--------|------------|--------|-----------|-------|
| accounts.txt | -      | text/plain | 19.0 B | Succeeded | -     |

4.



imay-s3-bucket - S3 bucket

Access control list (ACL)  
Grant basic read/write permissions to AWS accounts. [Learn more](#)

| Grantee  | Objects   | Object ACL  |
|--|---|---|
| Object owner (your AWS account)<br>Canonical ID: 03ae9cf0a7acd7c0309bac9bb28aaae536e834d8da67269369b366cf7e9e5d7           | <input checked="" type="checkbox"/> Read                                  | <input checked="" type="checkbox"/> Read<br><input checked="" type="checkbox"/> Write                       |
| Everyone (public access)<br>Group: http://acs.amazonaws.com/groups/global/AllUsers   | <input checked="" type="checkbox"/> <span style="color: red;">Read</span> | <input checked="" type="checkbox"/> <span style="color: red;">Read</span><br><input type="checkbox"/> Write |
| Authenticated users group (anyone with an AWS account)<br>Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers | <input type="checkbox"/> Read   | <input type="checkbox"/> Read<br><input type="checkbox"/> Write   |

⚠ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.  
[Learn more](#)

☒ I understand the effects of these changes on this object.

## Accounts.txt (publicly accessible):

