

AWS CLOUD COMPUTING (CC1):

R.PRANEISH

727721EUIT111

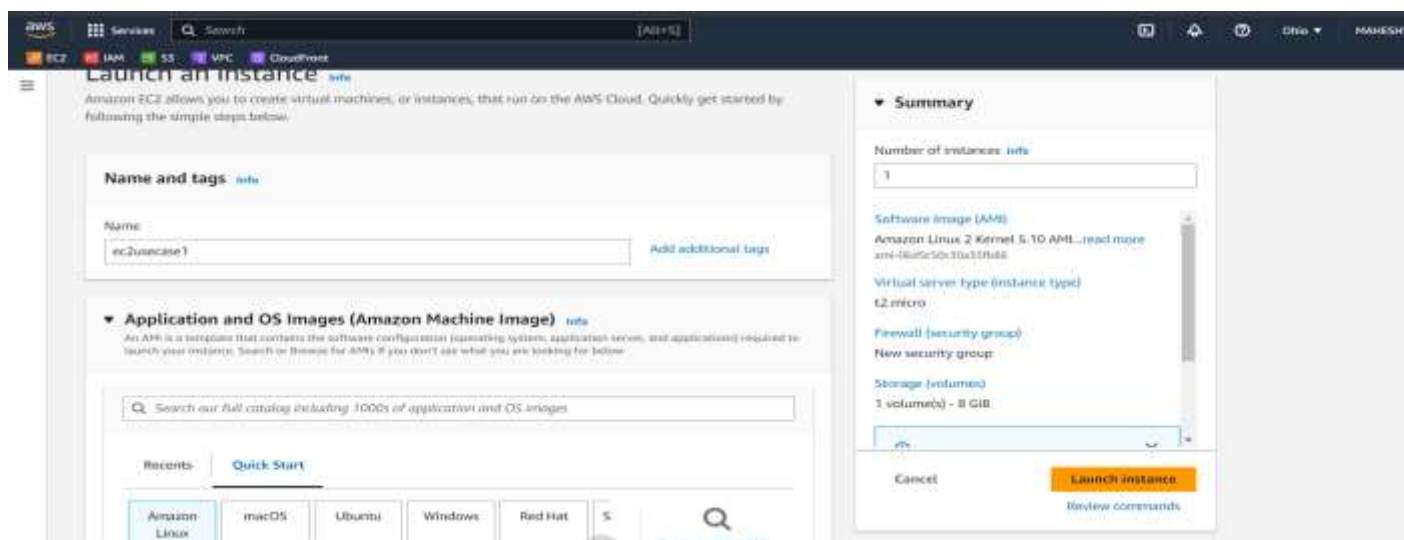
IT-B

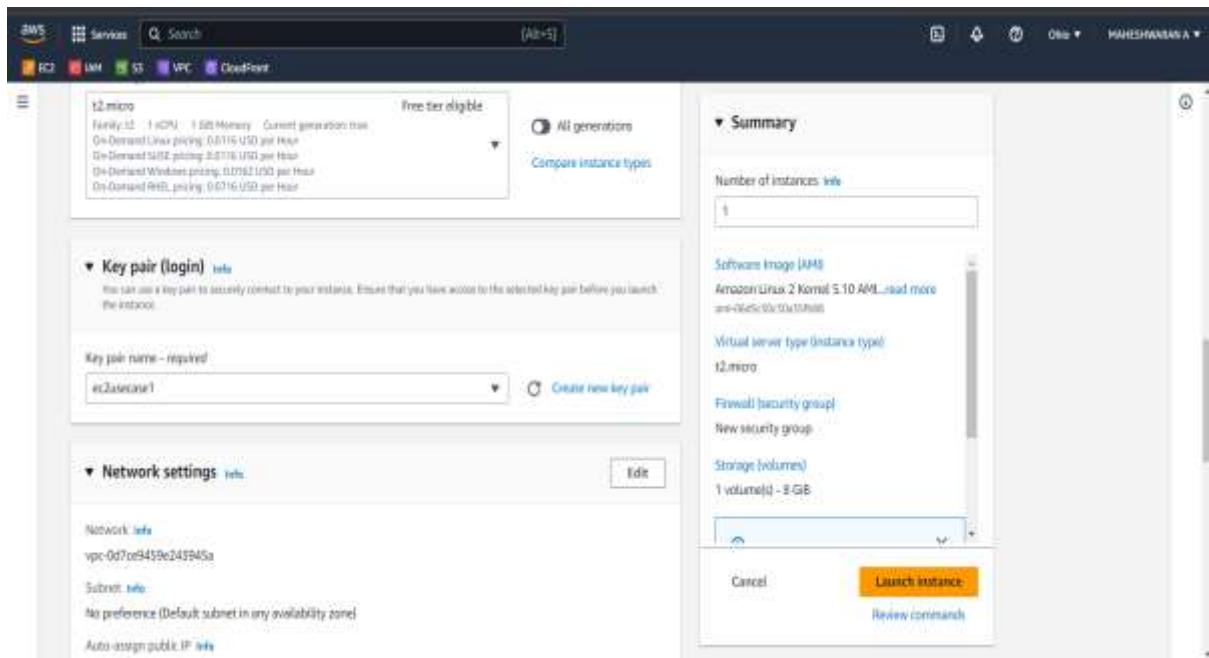
Q1.

Create an EC2 Instance in the us-east-1 region with the following requirements.

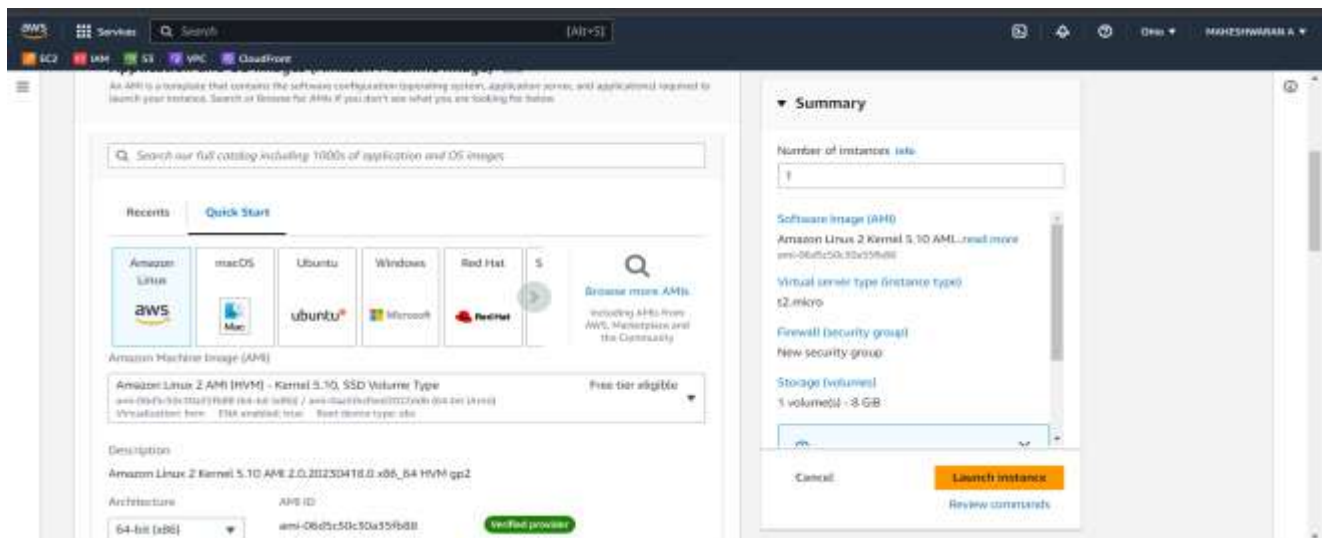
Give the Name tag of both EC2 instance & keypair as "ec2usecase1"(Name).

OUTPUT:



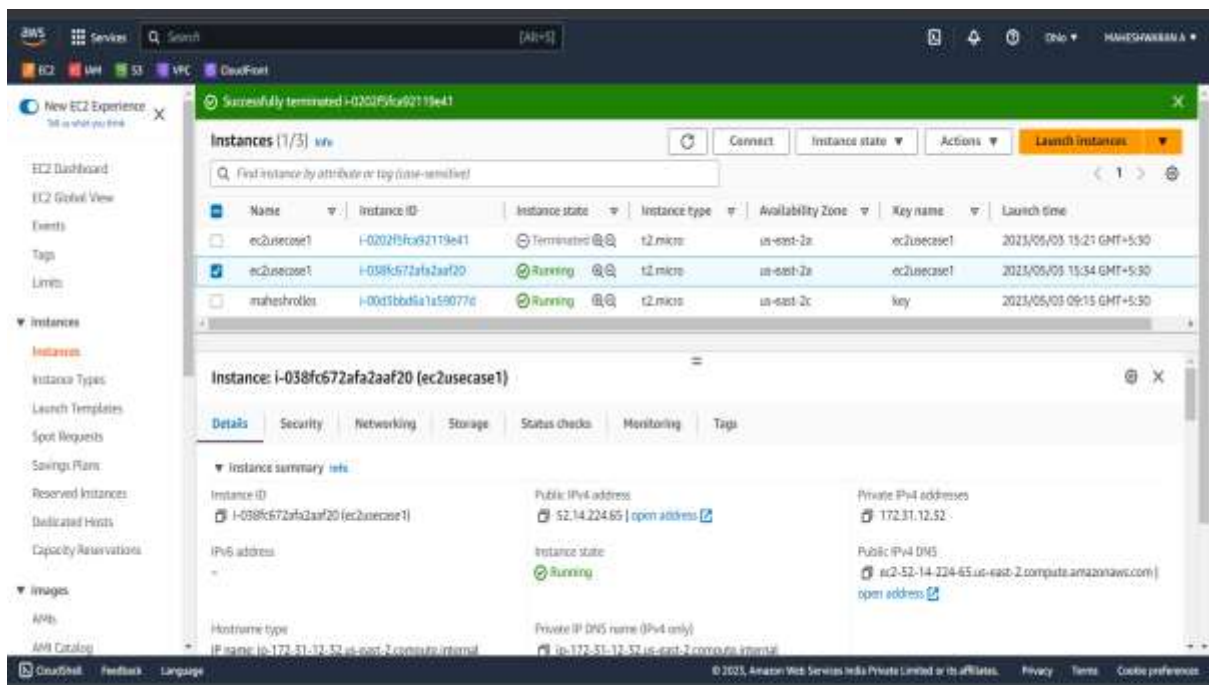
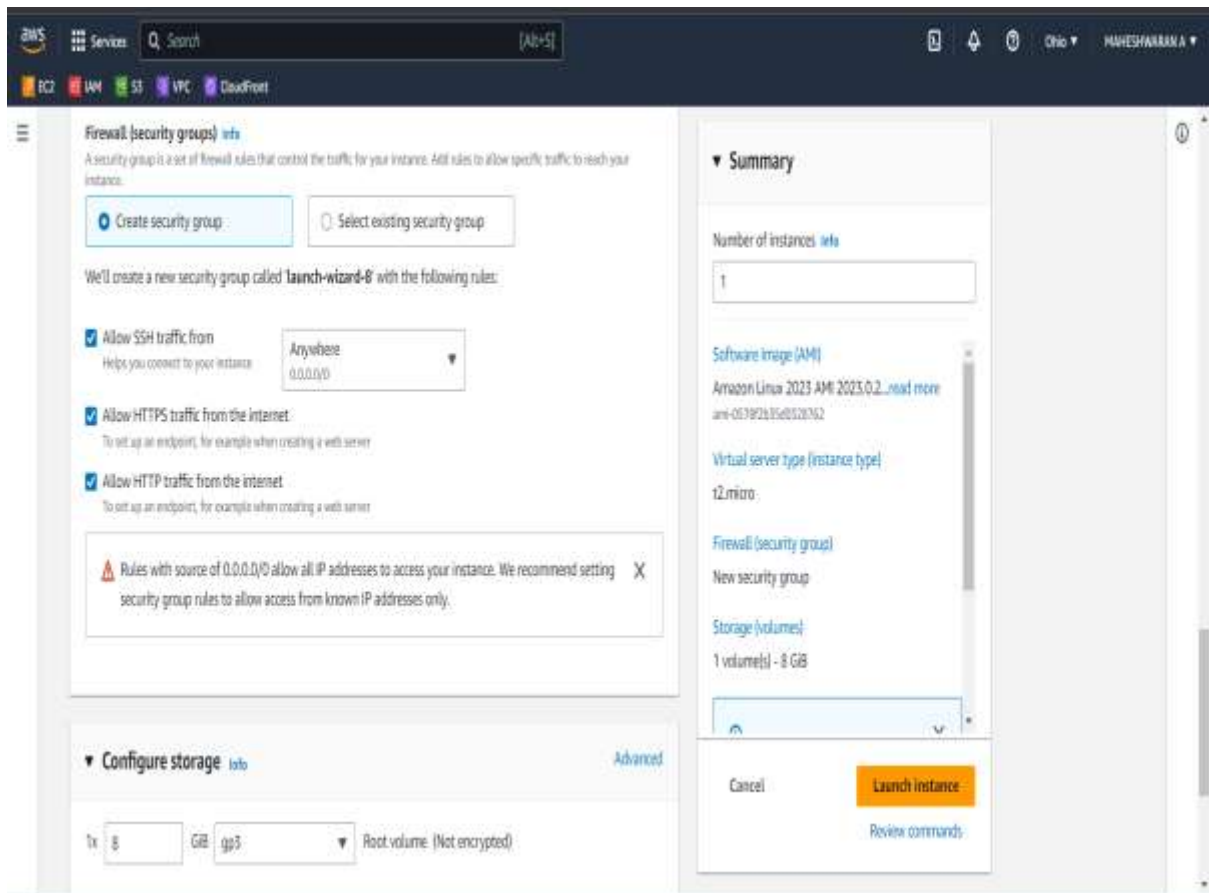


2) EC2 instance AMI should be "Amazon Linux 2".



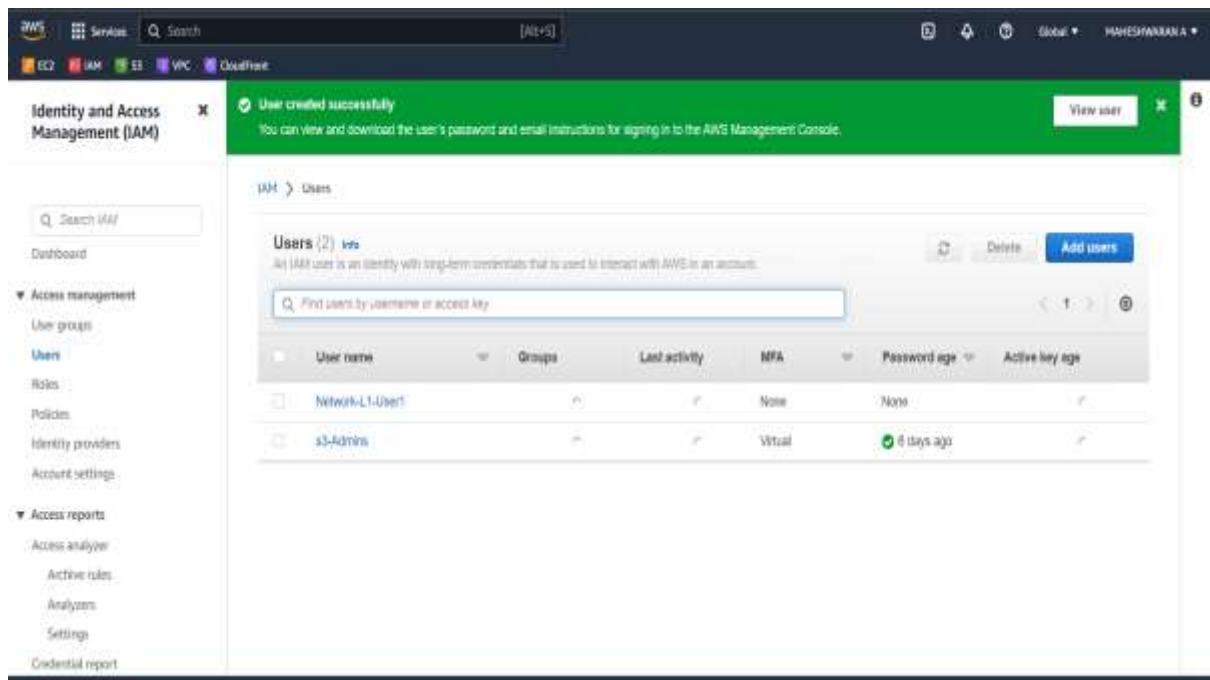
Allow SSH traffic for taking putty remote connection.

Allow HTTP traffic from the internet for reaching website requests.

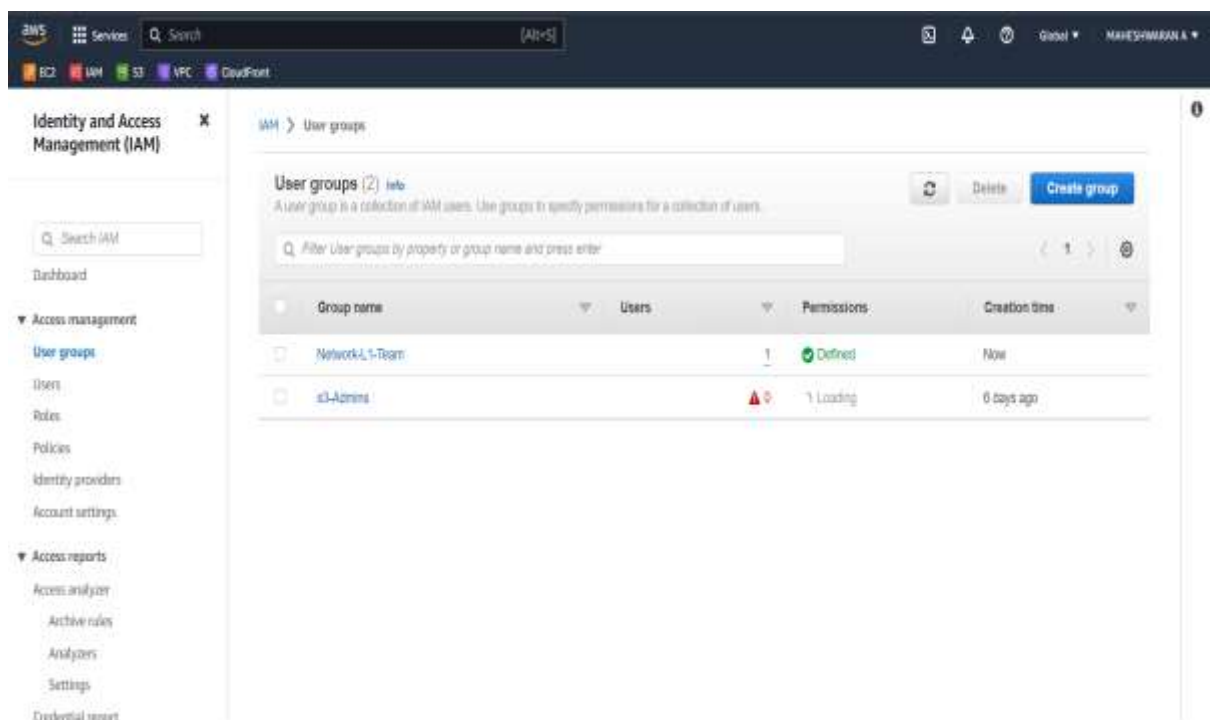


Create an IAM group called 'Network-L1-Team' with 'AmazonVPCReadOnlyAccess' and 'AWSNetworkManagerReadOnlyAccess' policies, then add an IAM user called 'Network-L1-User1' to the group.

The name of the IAM user should be 'Network-L1-User1'.



The name of the IAM group should be 'Network-L1-Team'.



The 'AmazonVPCReadOnlyAccess' policy should be attached.

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

Analysts

Settings

Credential report

Attach permissions policies - Optional (Selected: 1/847) [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 4 matches

Properties

Type

Path

Used as

Policy name	Type	Description
AmazonVPCFullAccess	AWS managed	Provides full access to Amazon VPC via the AWS Management Console...
AmazonVPCReadOnlyAccess	AWS managed	Provides read-only access to Amazon VPC via the AWS Management Console...
AmazonVPCCrossAccountNetworkInterface...	AWS managed	Provides access to create network interfaces and attach them to...
AmazonVPCReachabilityAnalyzerPathComp...	AWS managed	This policy is attached to the role IAMRoleForReachabilityAnalyz...

The 'AWSNetworkManagerReadOnlyAccess' policy should be attached.

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

Analysts

Settings

Credential report

Network-L1-User1

arn:aws:iam::258555815895:user/Network-L1-User1

Created: May 05, 2023, 15:39 (UTC+05:30)

Console access: **Enabled without MFA**

Last console sign-in: Never

Access key 1: Not enabled

Access key 2: Not enabled

Permissions

Groups (1)

Tags

Security credentials

Access Advisor

Permissions policies (2)

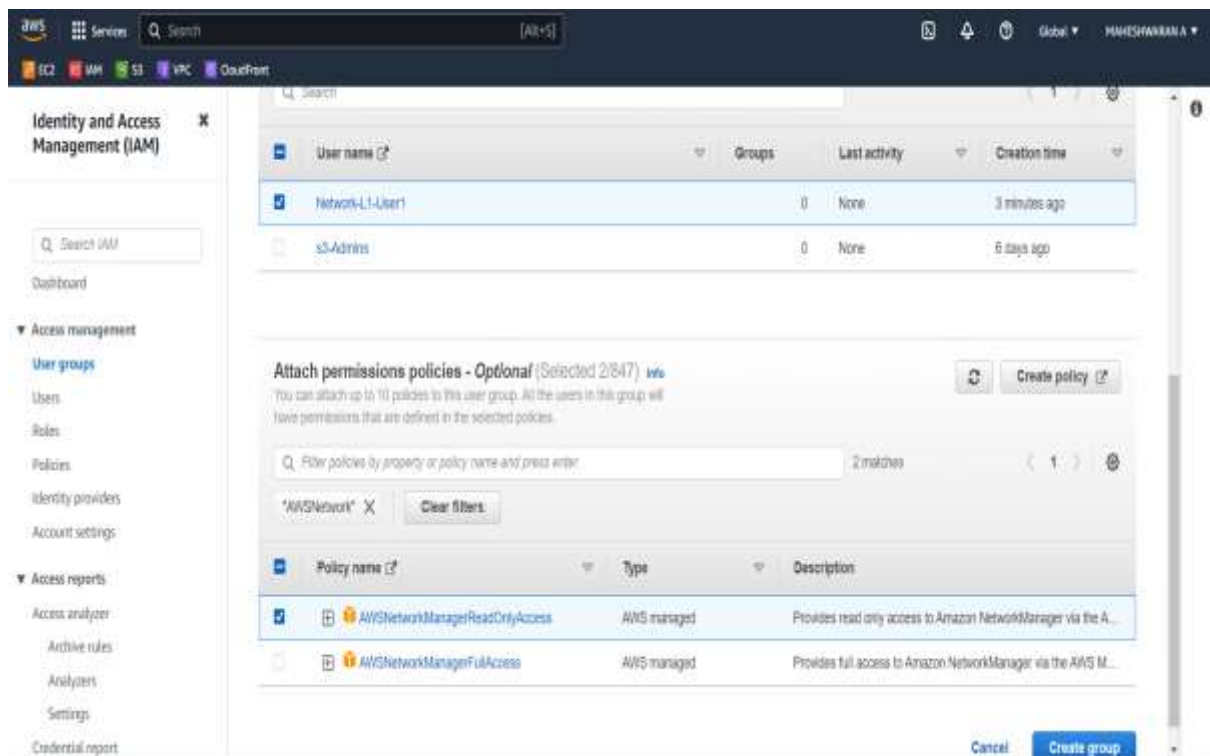
Permissions are defined by policies attached to the user directly or through groups.

Find policies

Policy name	Type	Attached via
AmazonVPCReadOnlyAccess	AWS managed	Group Network-L1-Team
AWSNetworkManagerReadOnlyAccess	AWS managed	Group Network-L1-Team

Permissions boundary (not set)

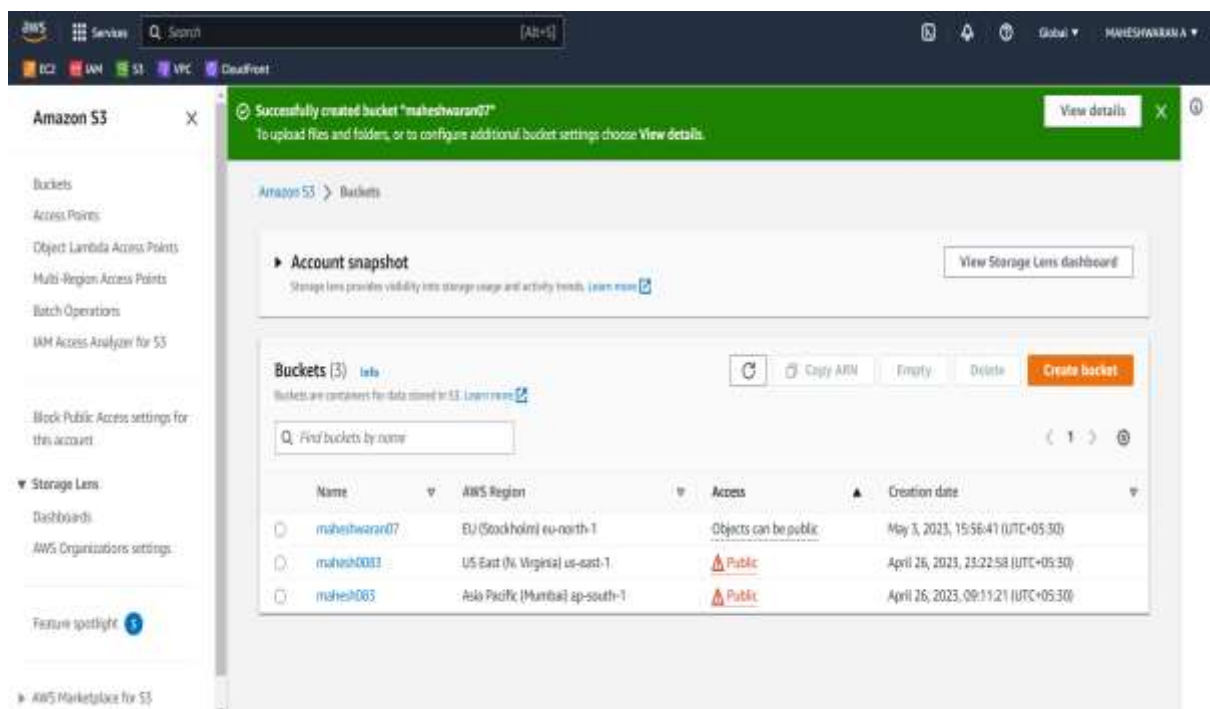
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)



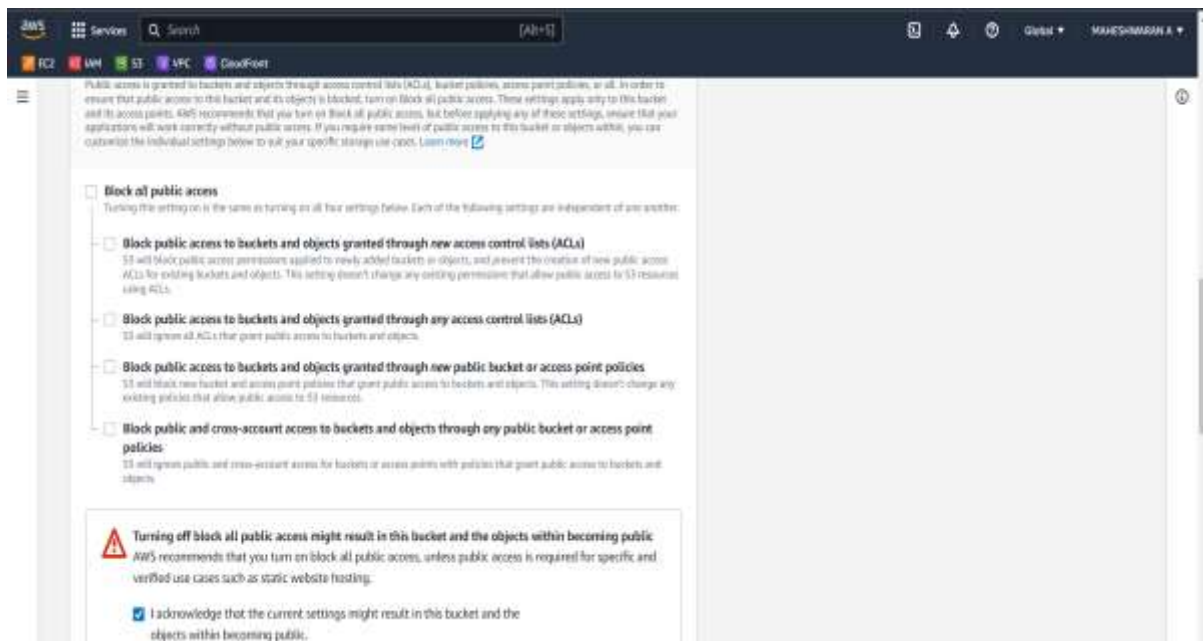
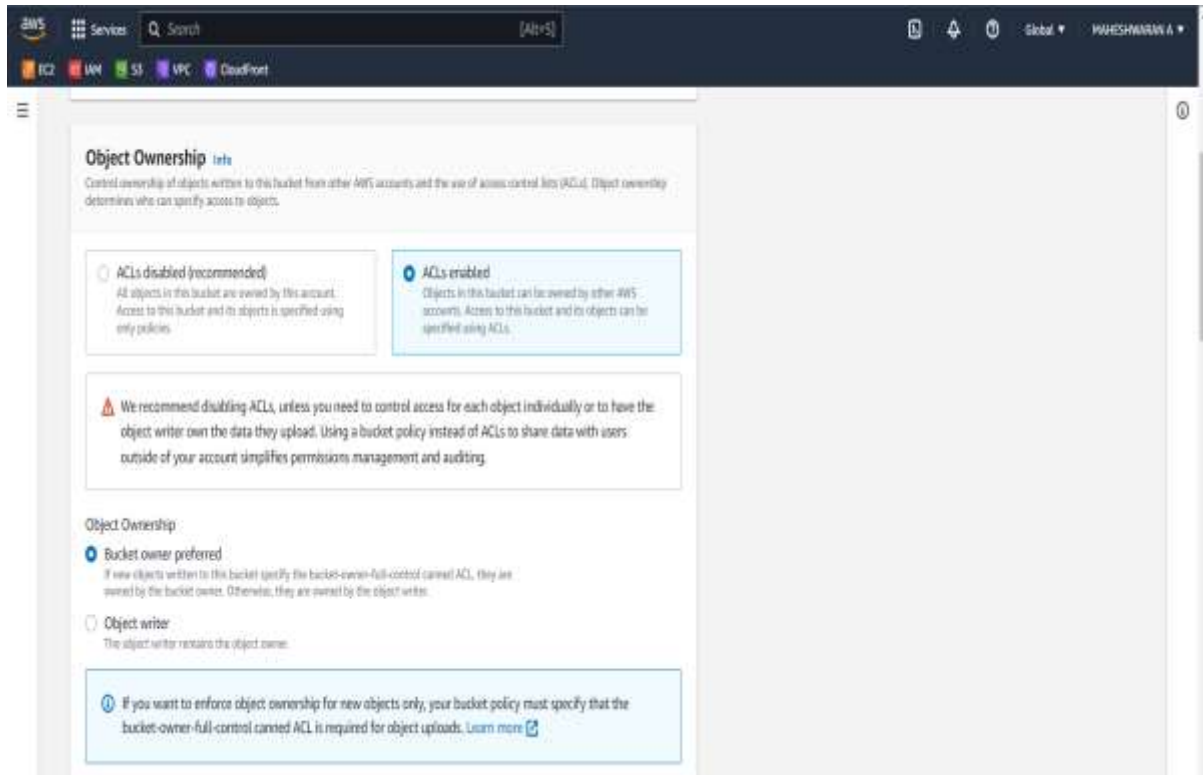
Q3.

Create a S3 bucket for the following requirements

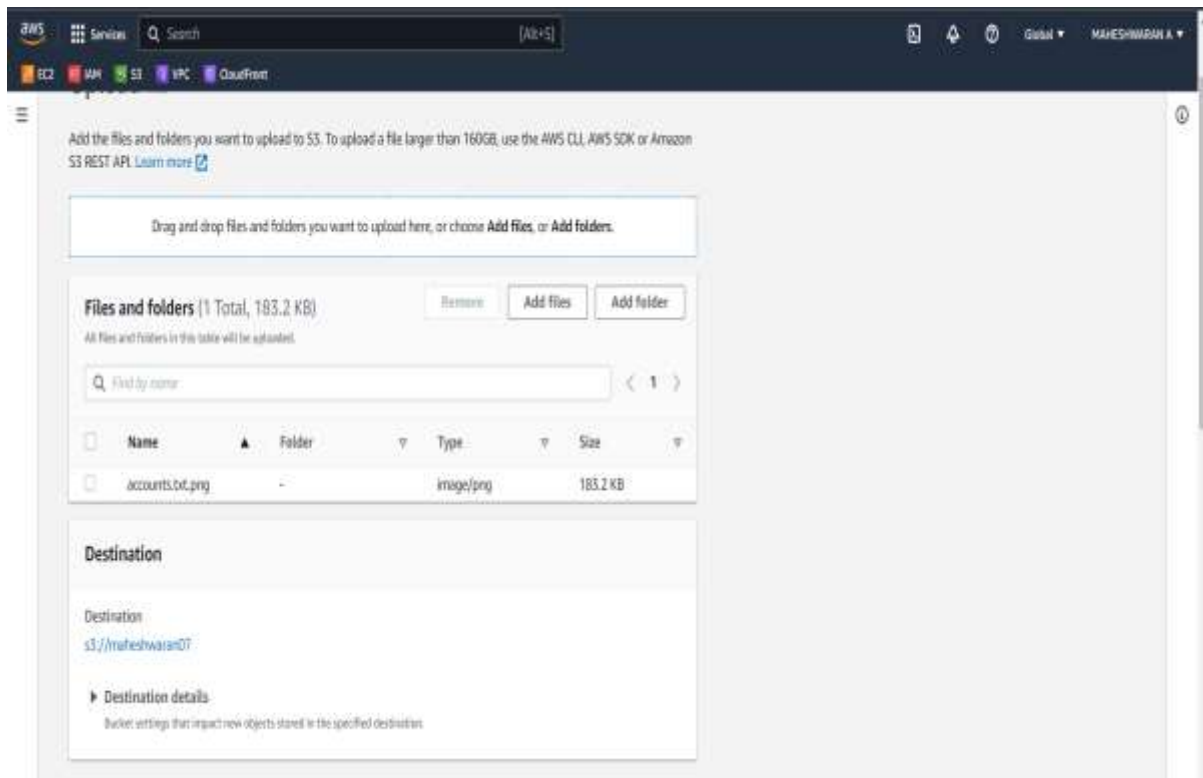
Create a new S3 bucket in the region of "Stockholm".



Make the bucket accessible to everyone(publicly) via Bucket ACL.



Upload a text file in the name of 'accounts.txt'.



Make the object 'accounts.txt' file accessible to everyone(publicly).

