AWS CLOUD COMPUTING (CC1):

R.PRANEISH

727721EUIT111

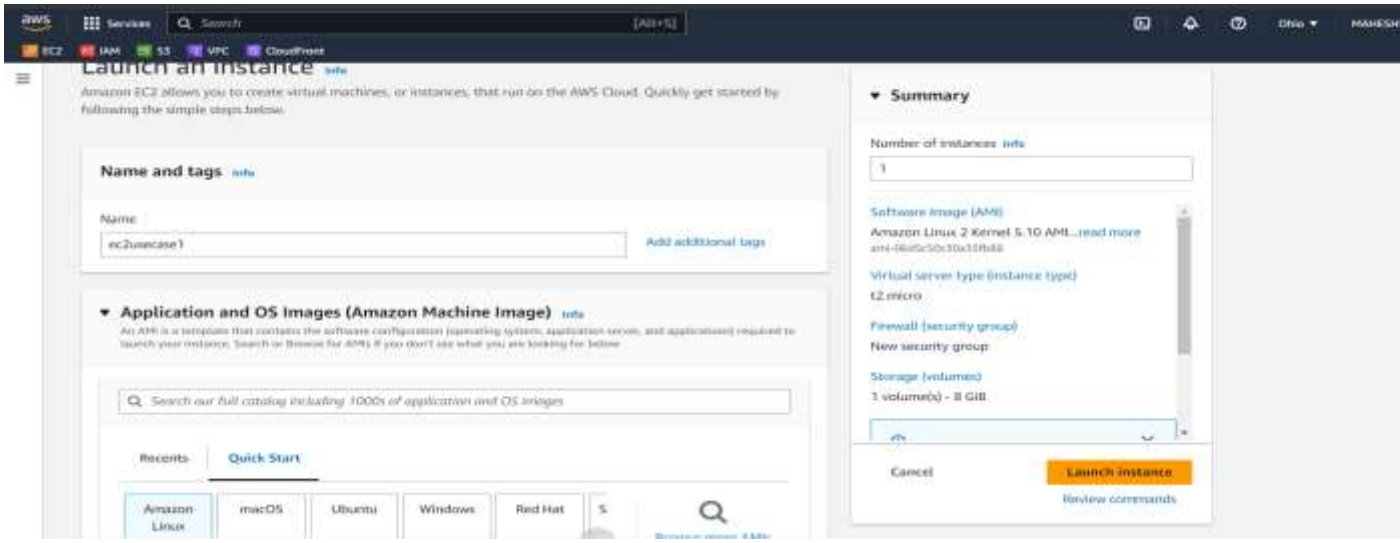
IT-B

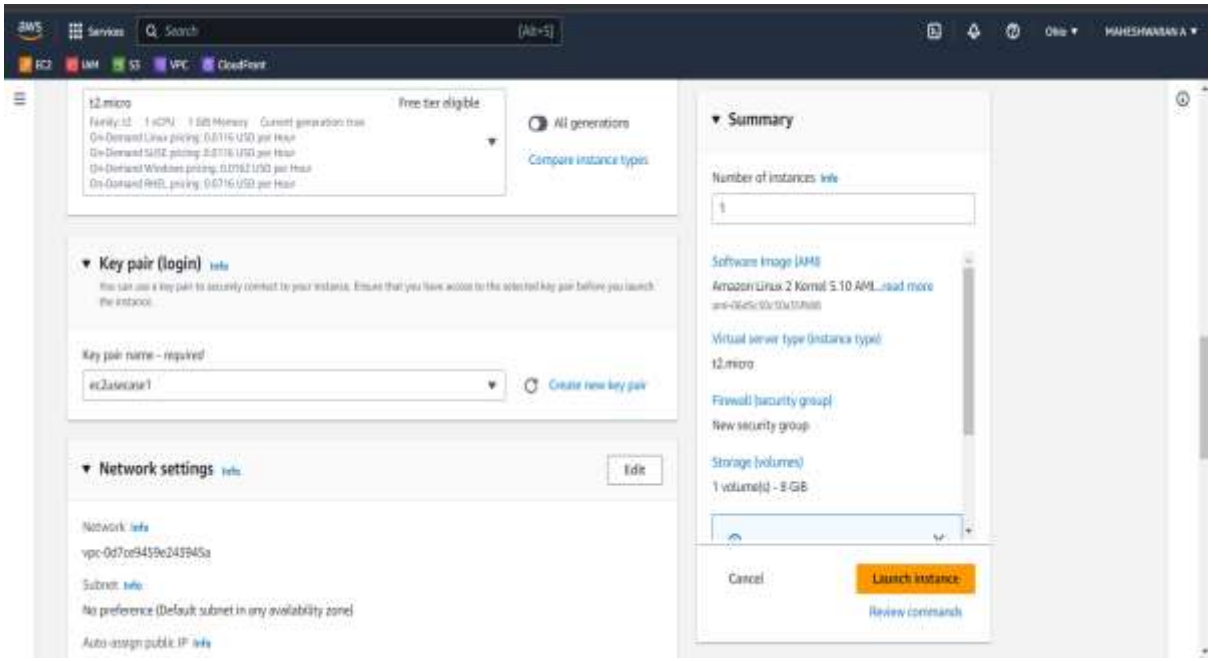
Q1.

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

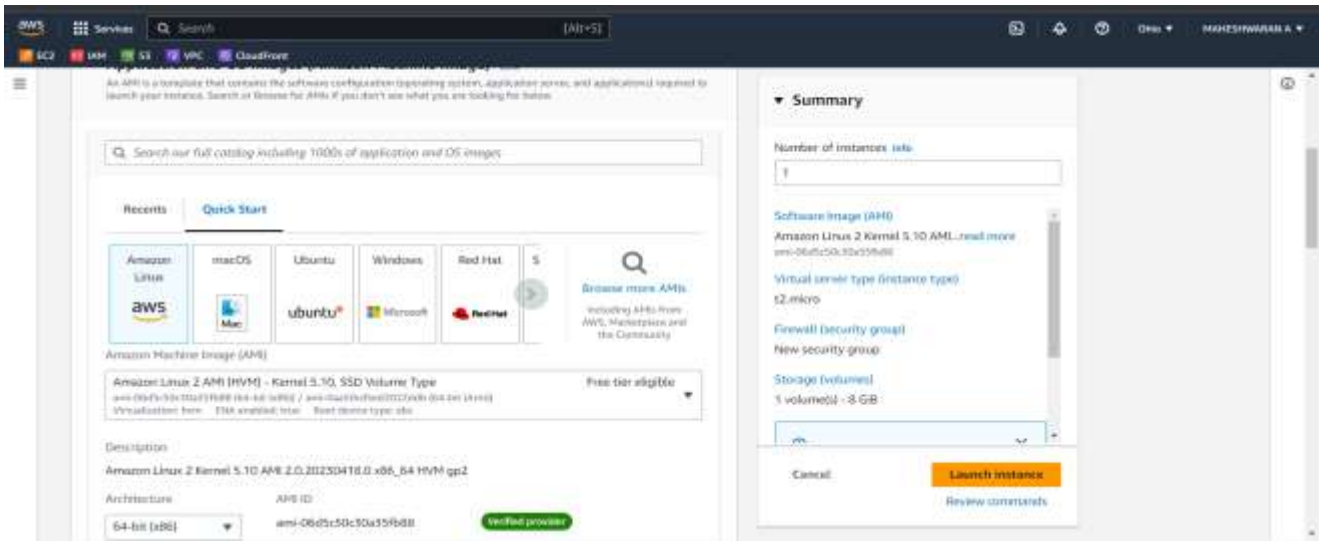
Give the Name tag of both EC2 instance & keypair as "ec2usecase1"(Name).

OUTPUT:



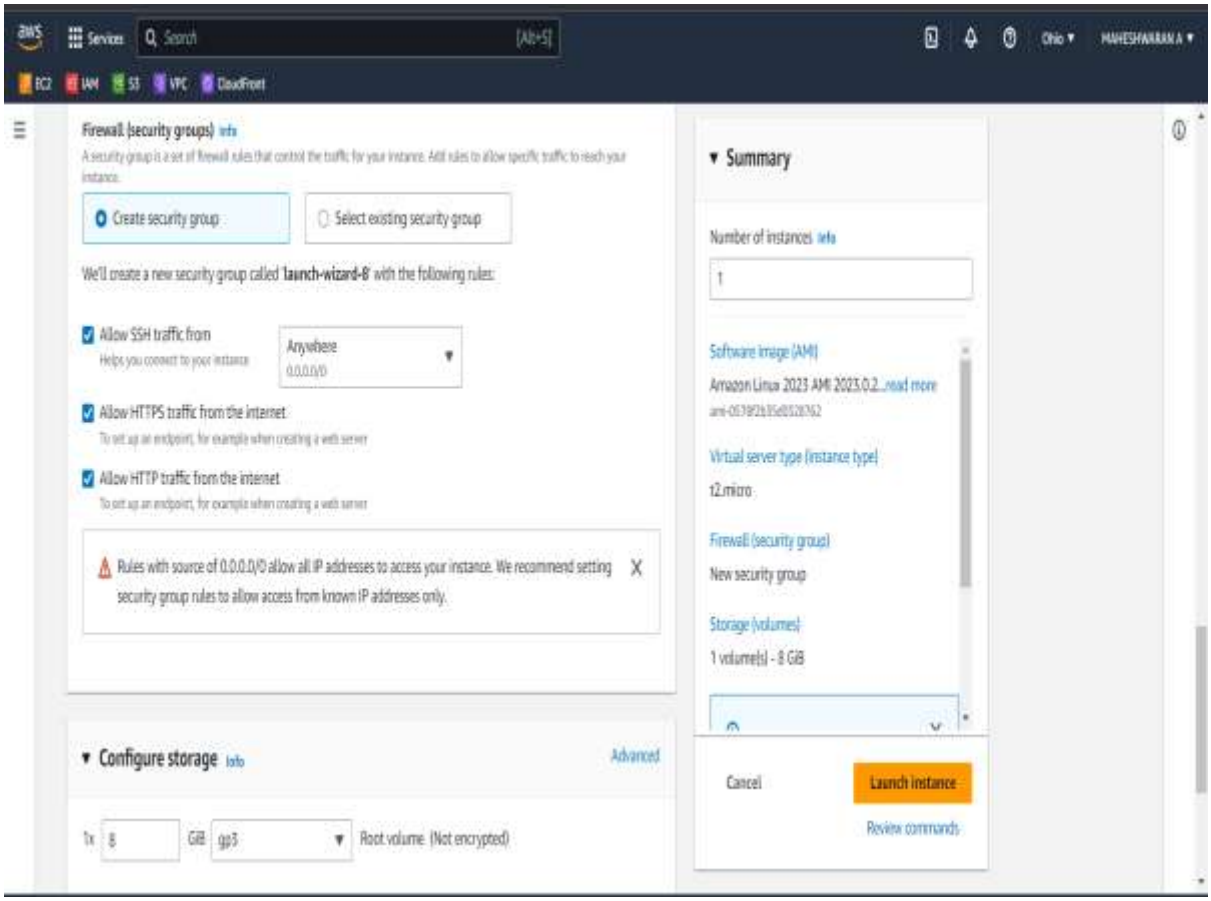


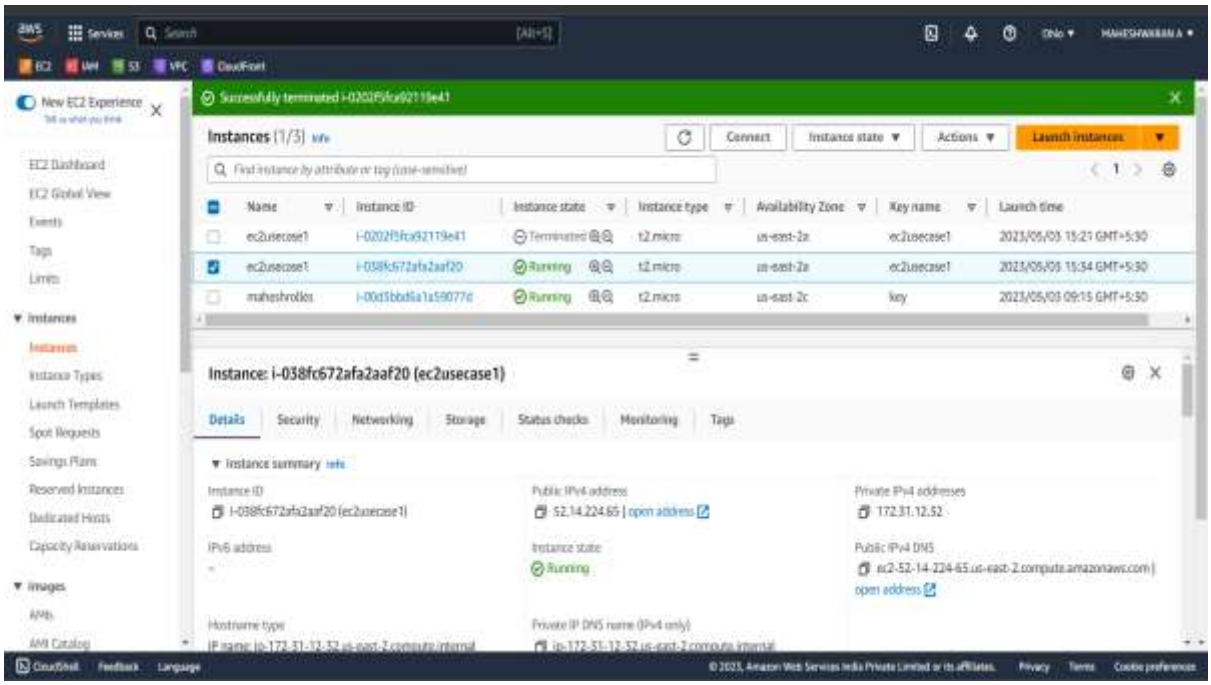
2) EC2 instance AMI should be "Amazon Linux 2".



Allow SSH traffic for taking putty remote connection.

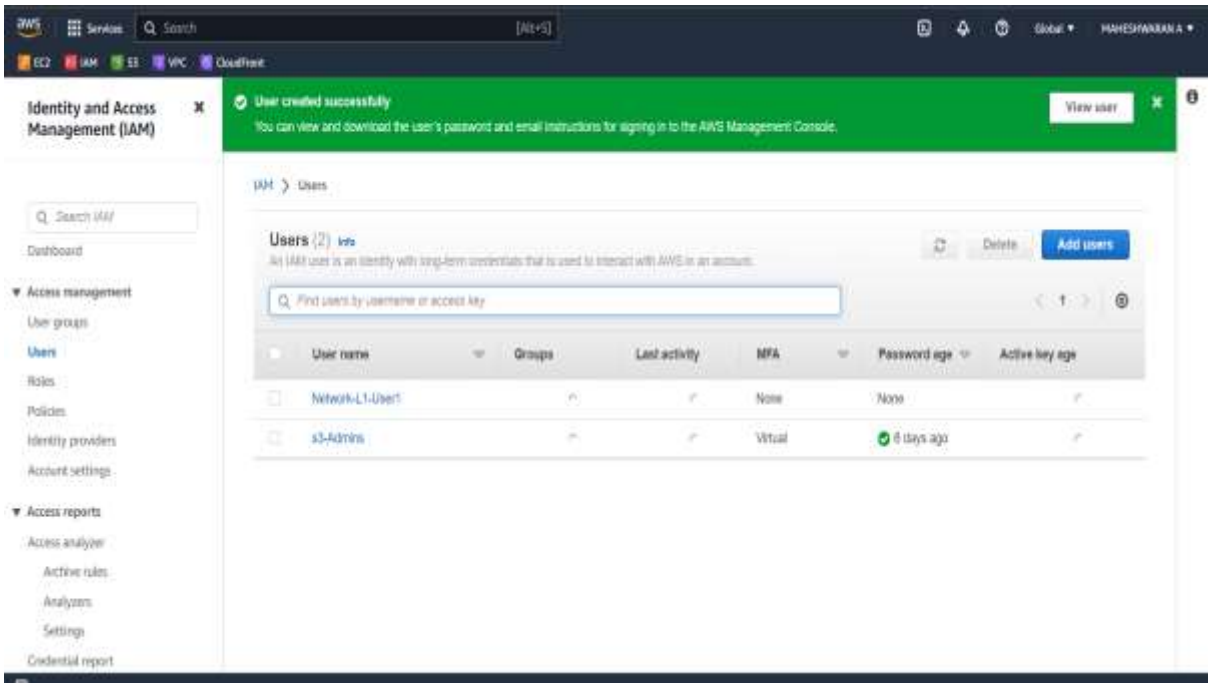
Allow HTTP traffic from the internet for reaching website requests.



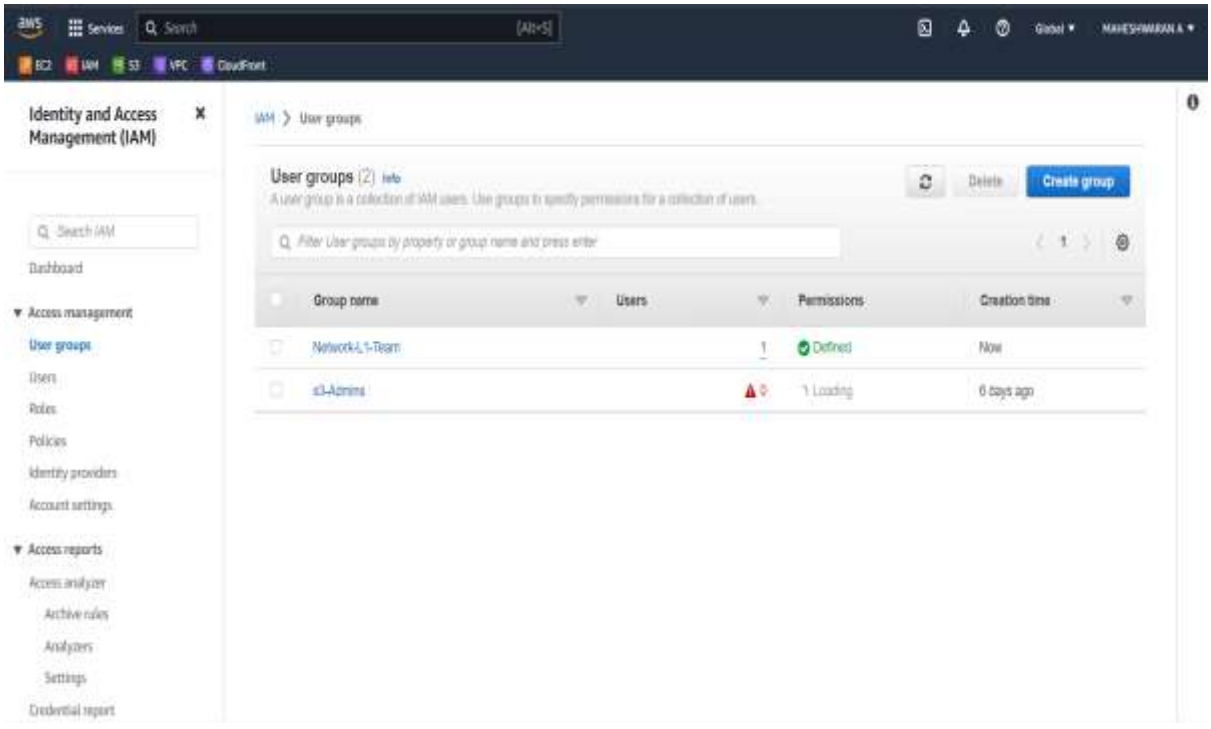


Create an IAM group called 'Network-L1-Team' with 'AmazonVPCReadOnlyAccess' and 'AWSNetworkManagerReadOnlyAccess' policies, then add an IAM user called 'Network-L1-User1' to the group.

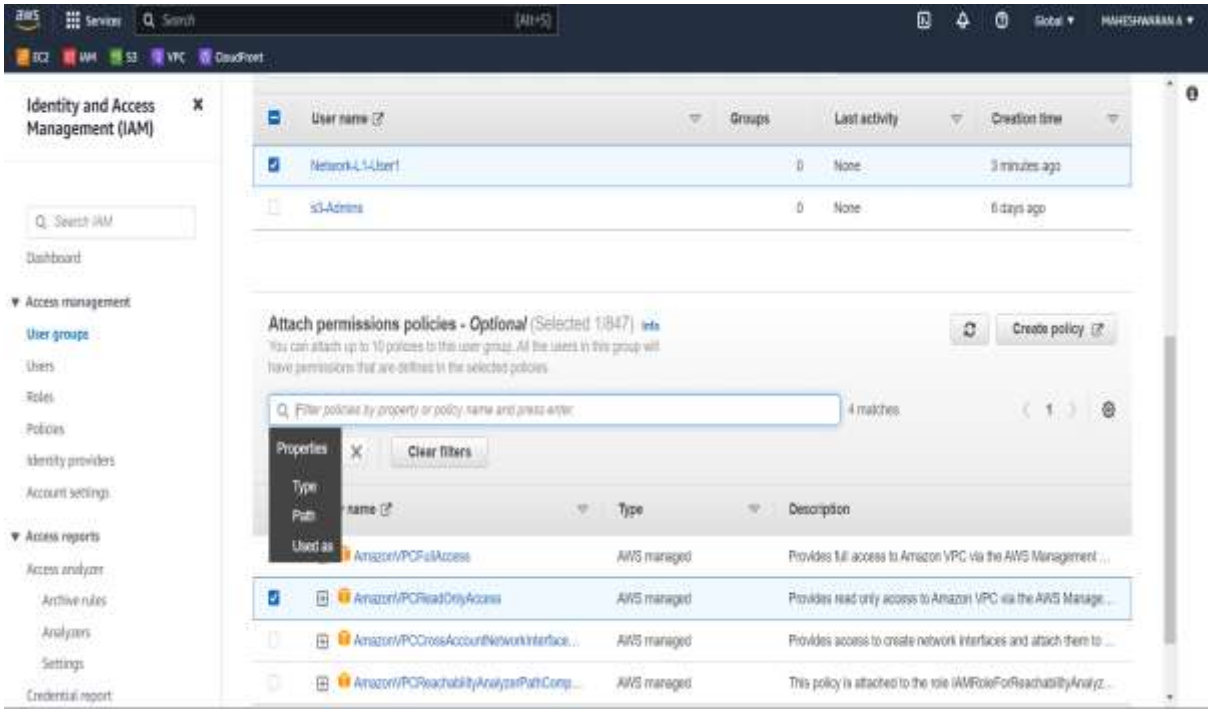
The name of the IAM user should be 'Network-L1-User1'.



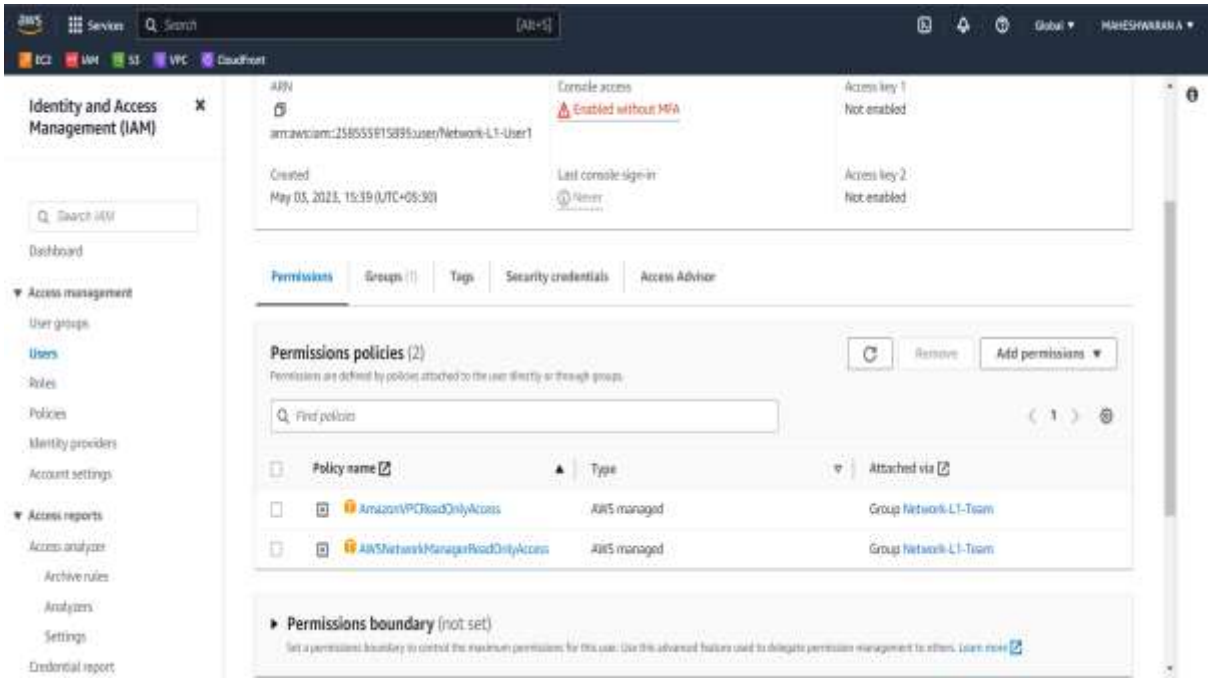
The name of the IAM group should be 'Network-L1-Team'.

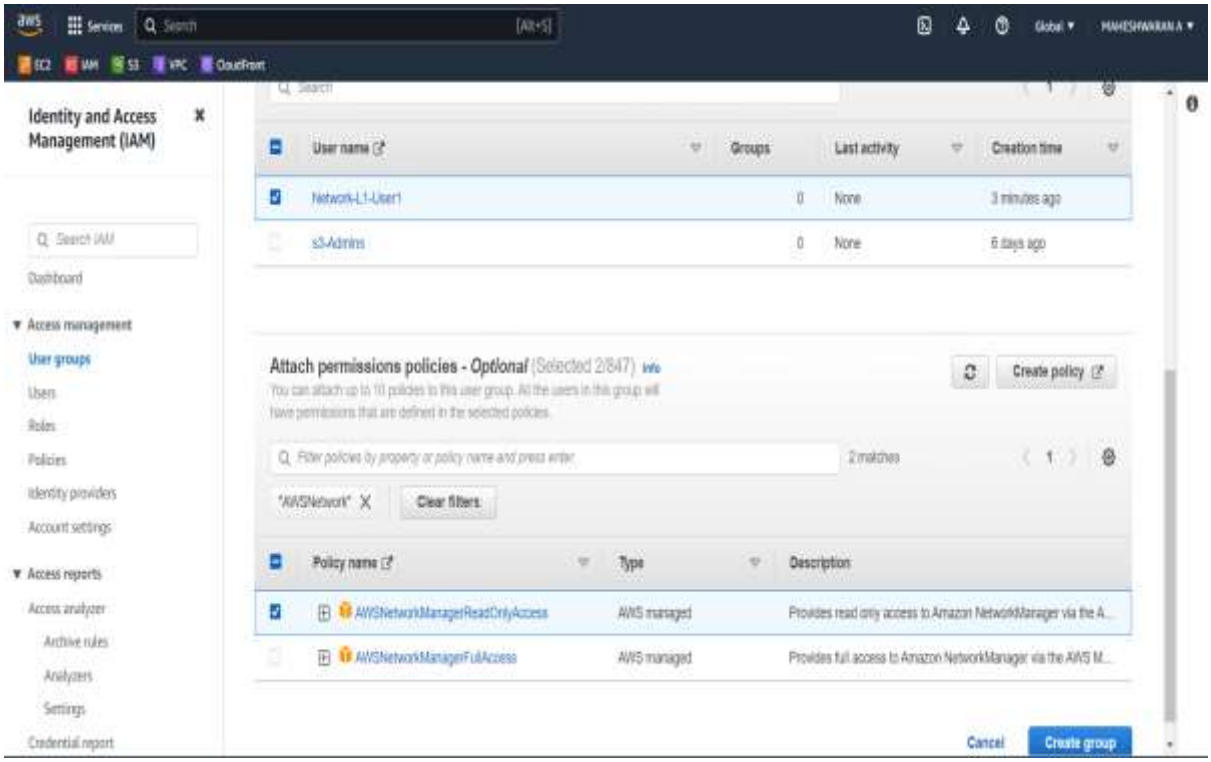


The 'AmazonVPCReadOnlyAccess' policy should be attached.



The 'AWSNetworkManagerReadOnlyAccess' policy should be attached.

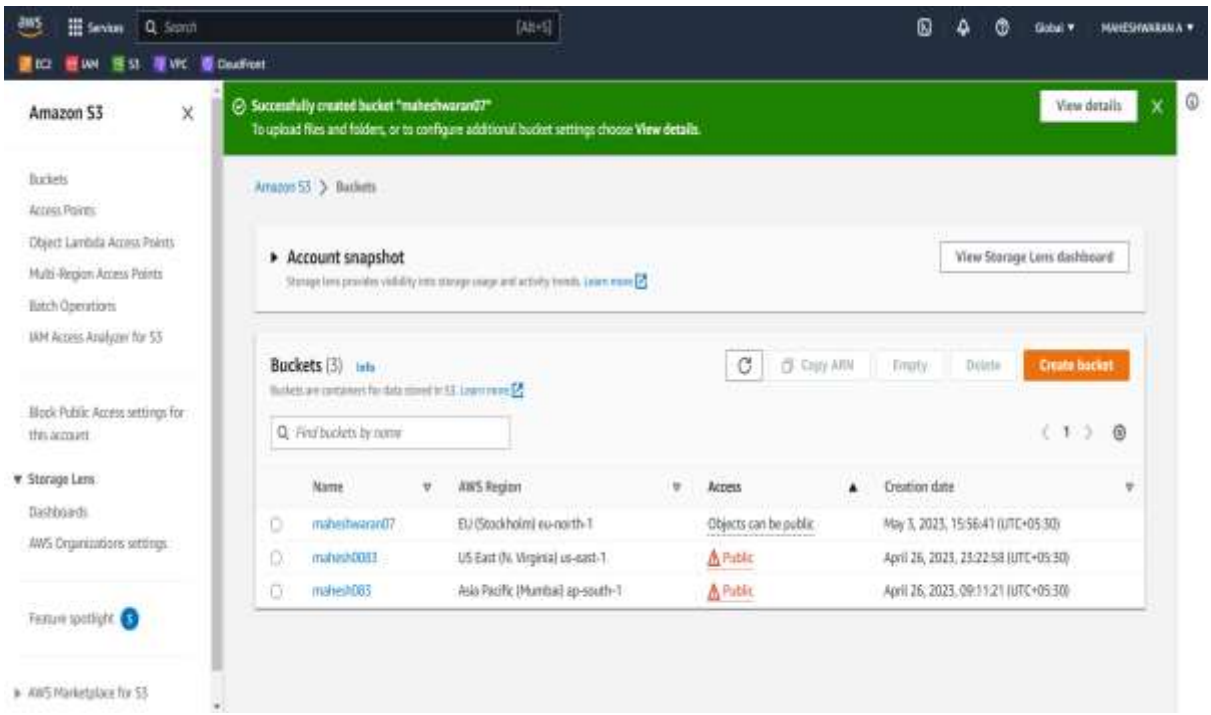




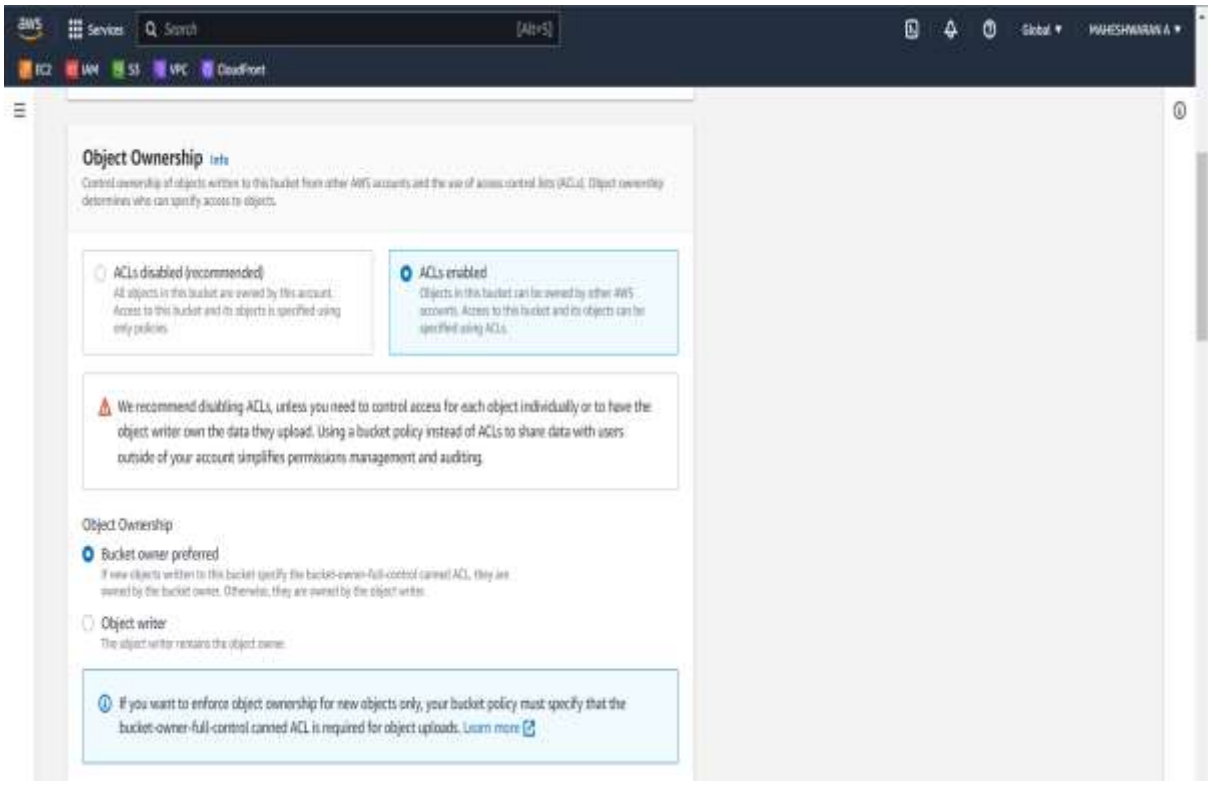
Q3.

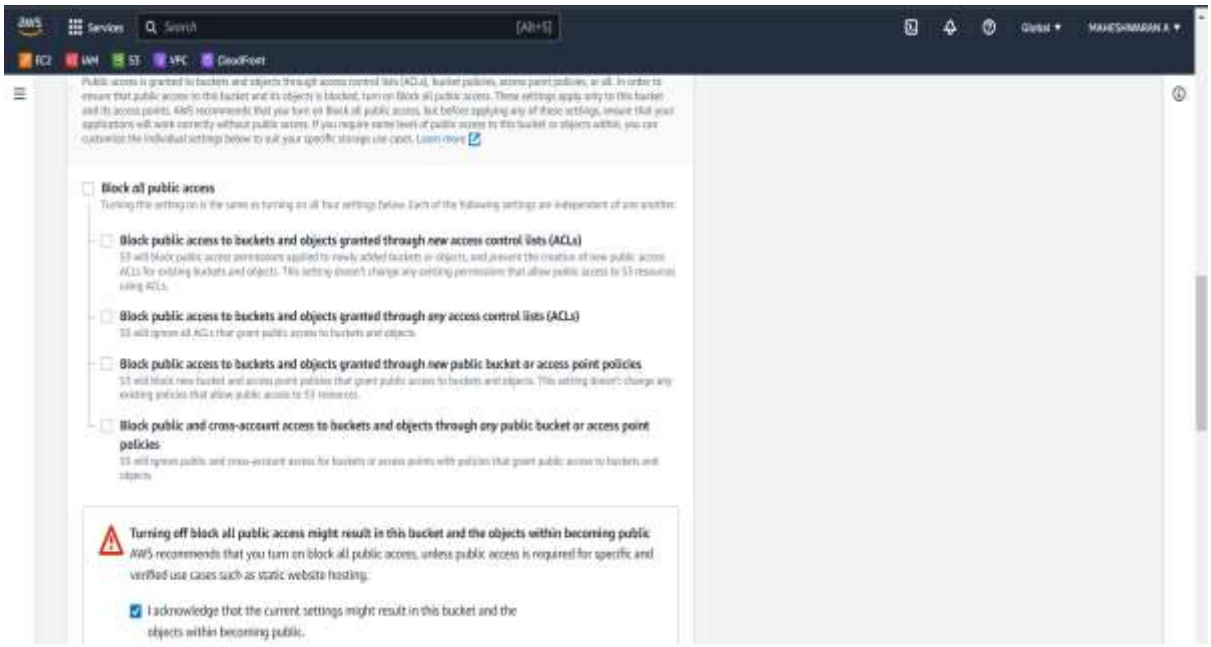
Create a S3 bucket for the following requirements

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

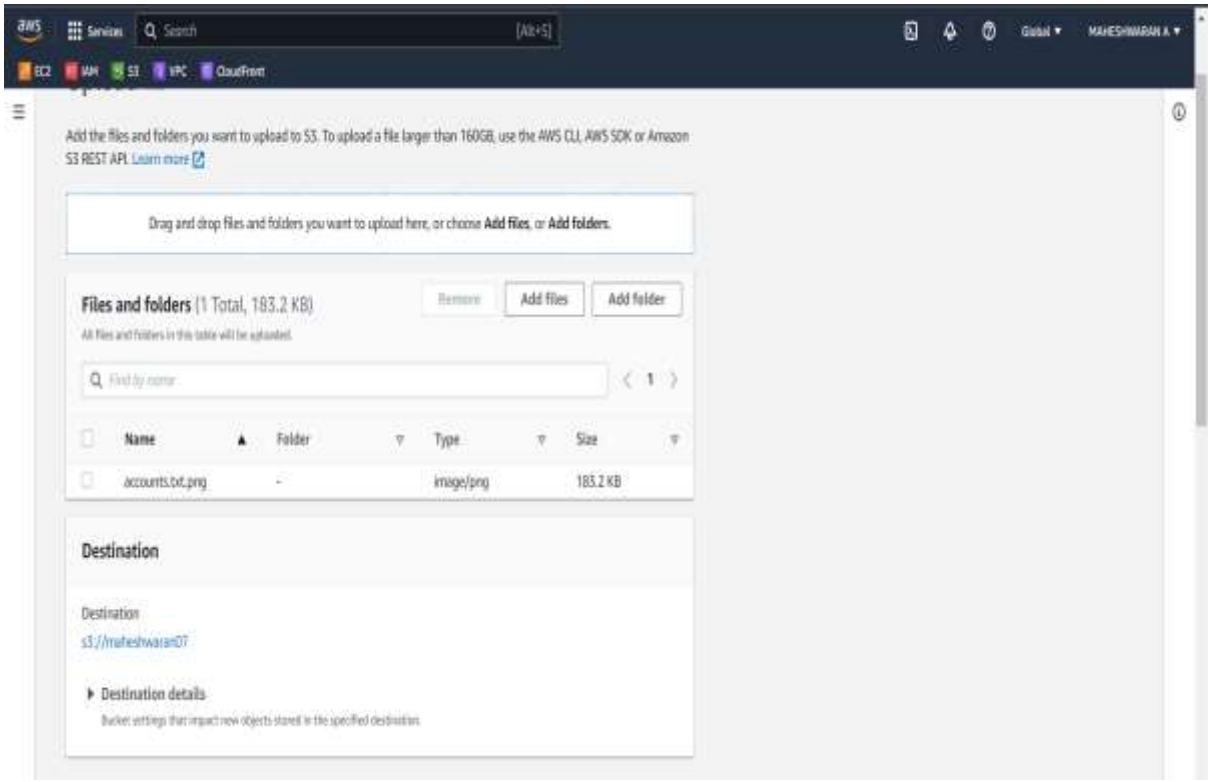


Make the bucket accessible to everyone(publicly) via Bucket ACL.

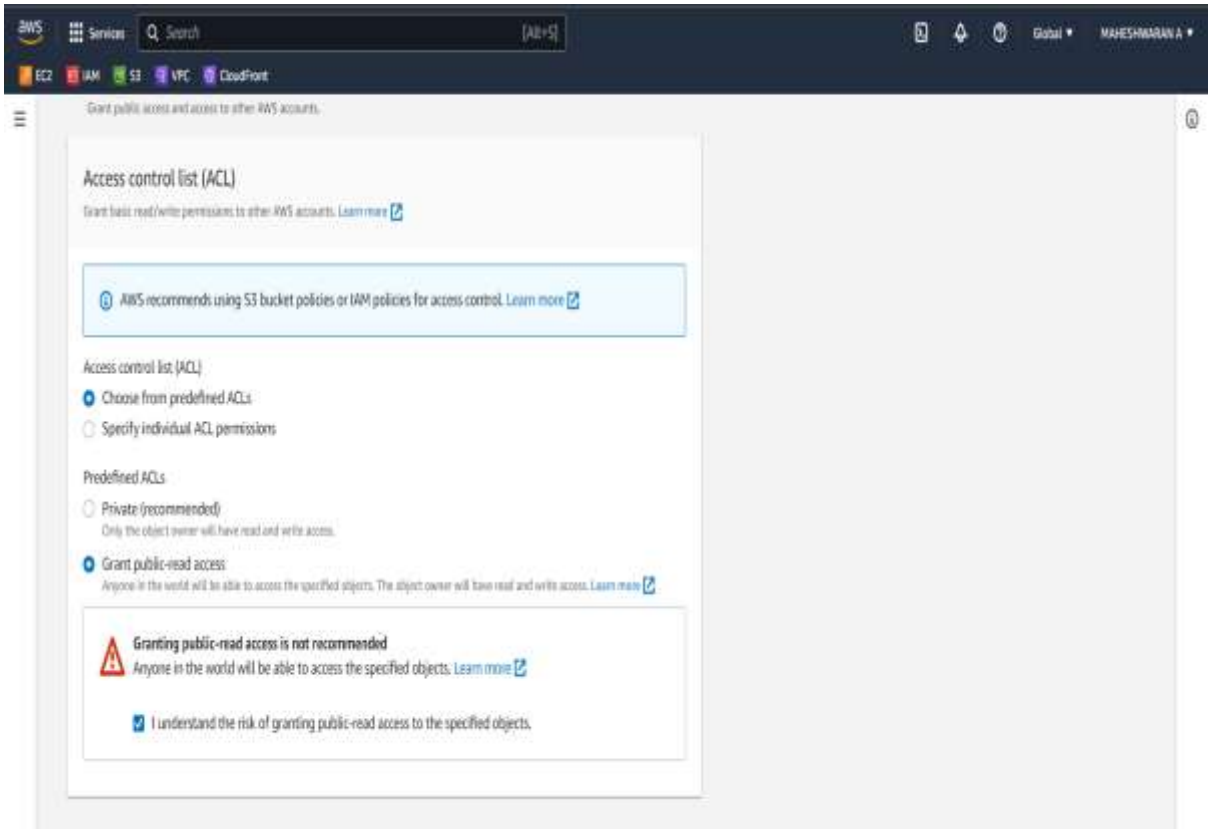


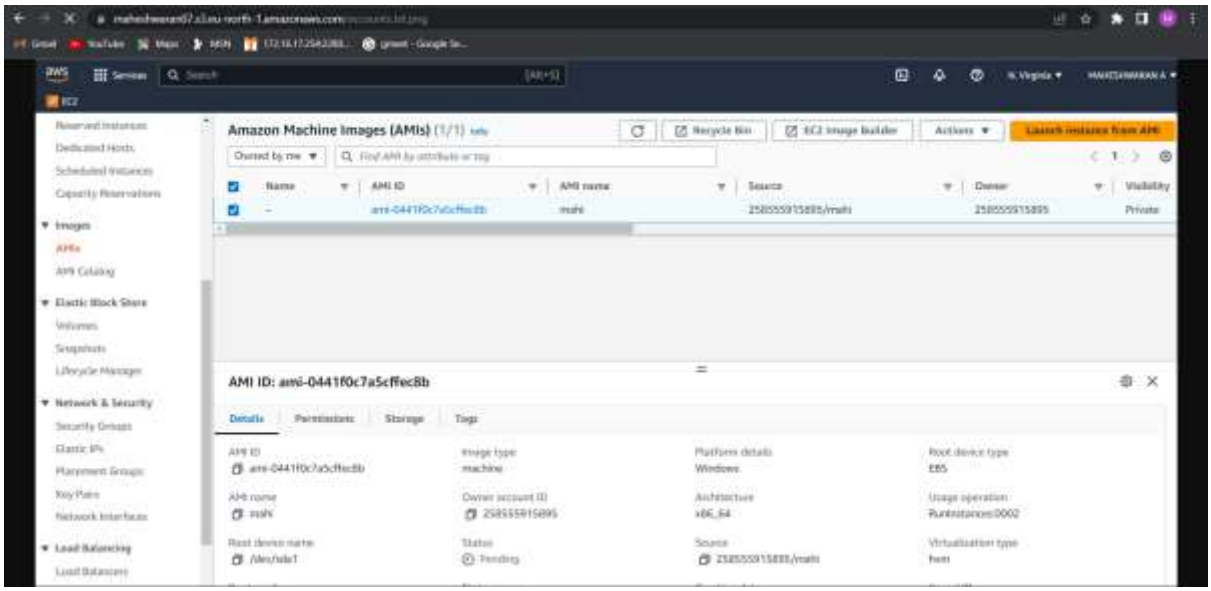


Upload a text file in the name of 'accounts.txt'.



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


Grant public access and access to other AWS accounts.
Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. Learn more
AWS recommends using S3 bucket policies or IAM policies for access control. Learn more
Access control list (ACL)
Choose from predefined ACLs
Specify individual ACL permissions
Predefined ACLs
Private (recommended)
Only the object owner will have read and write access.
Grant public-read access
Anyone in the world will be able to access the specified objects. The object owner will have read and write access. Learn more
Granting public-read access is not recommended
Anyone in the world will be able to access the specified objects. Learn more
I understand the risk of granting public-read access to the specified objects.


Amazon Machine Images (AMIs) (1/1)
AMI ID: ami-0441f0c7a5cffec8b
Details
Permissions
Storage
Tags