Cloud Computing

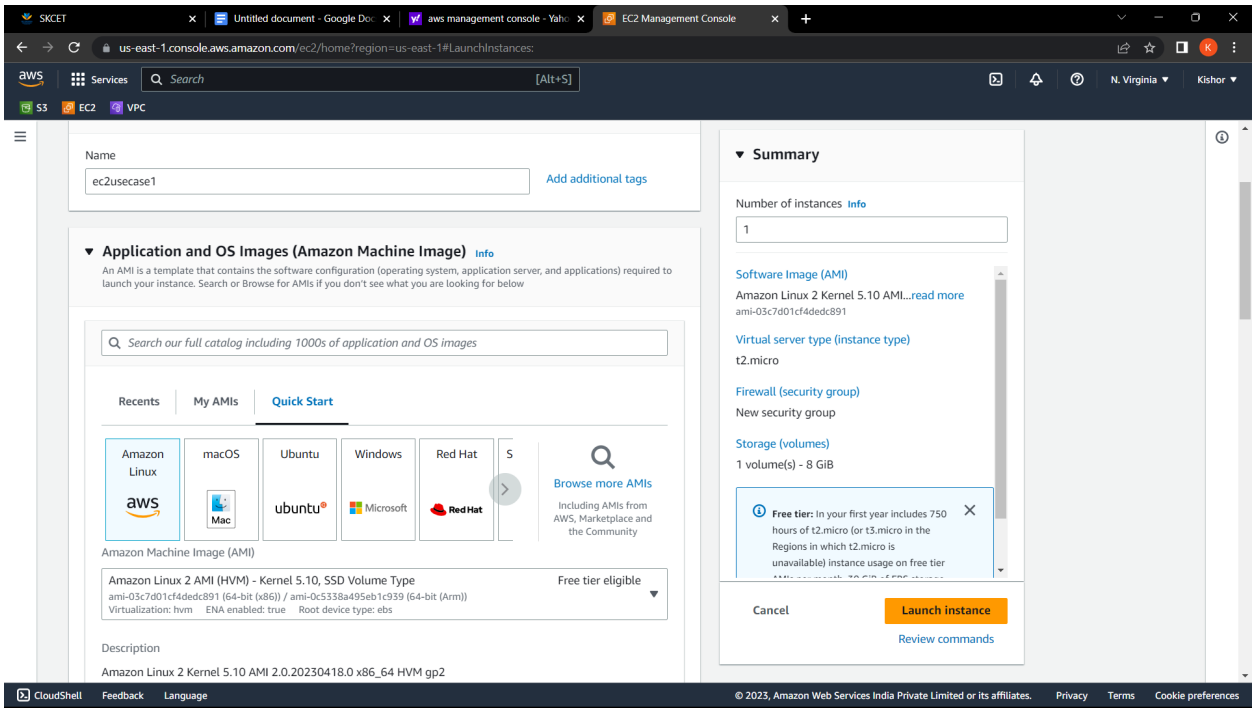
1.

Q1.

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

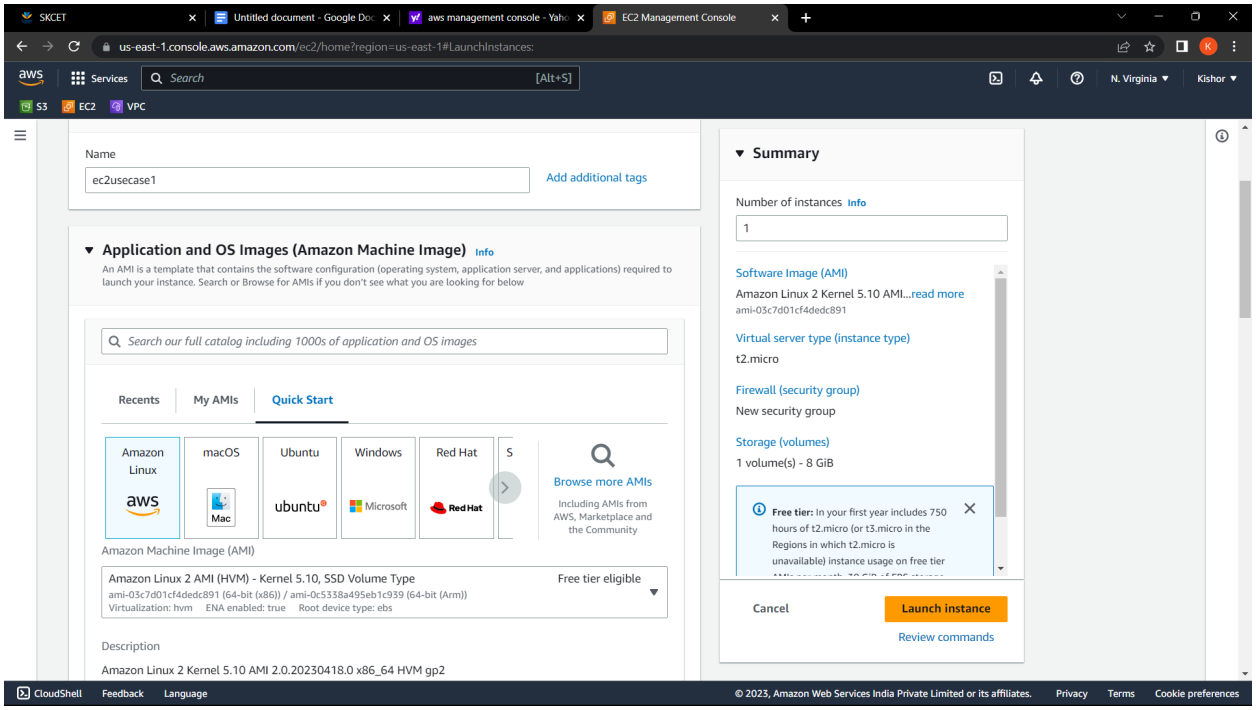
Give the Name tag of both EC2 instance & keypair as "ec2usecase1"(Name).

(4 Marks)



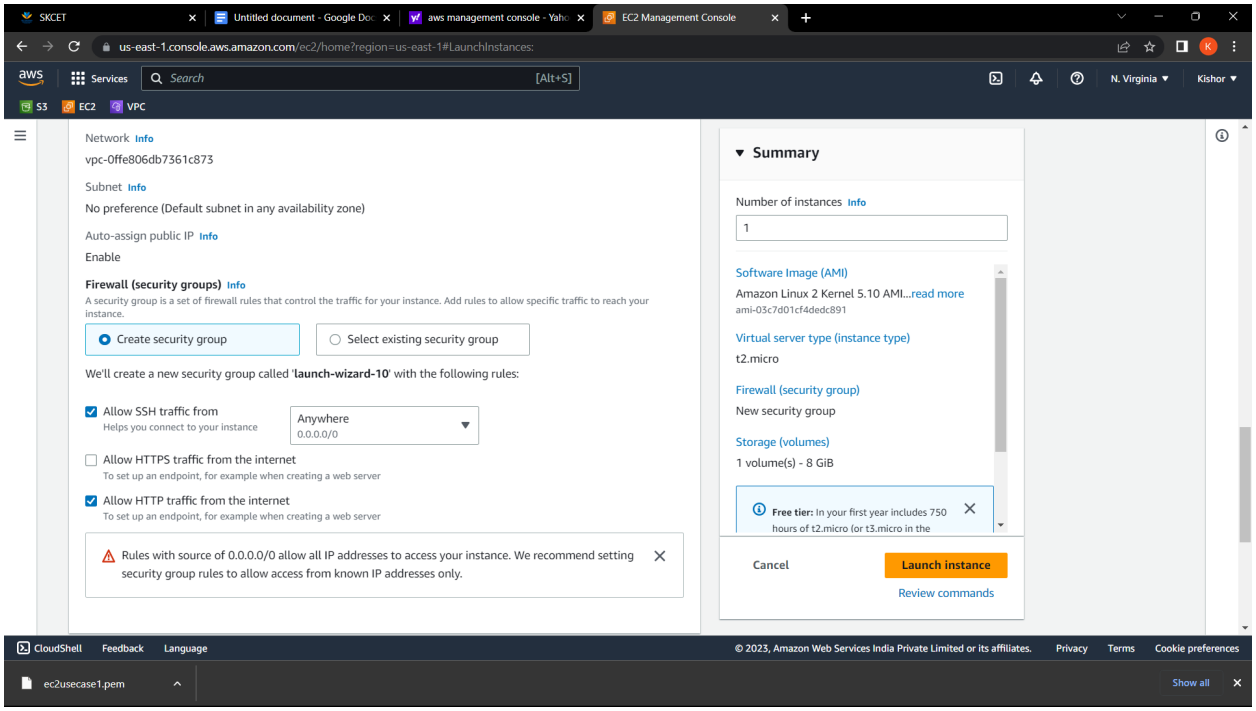
EC2 instance AMI should be "Amazon Linux 2".

(4 Marks)



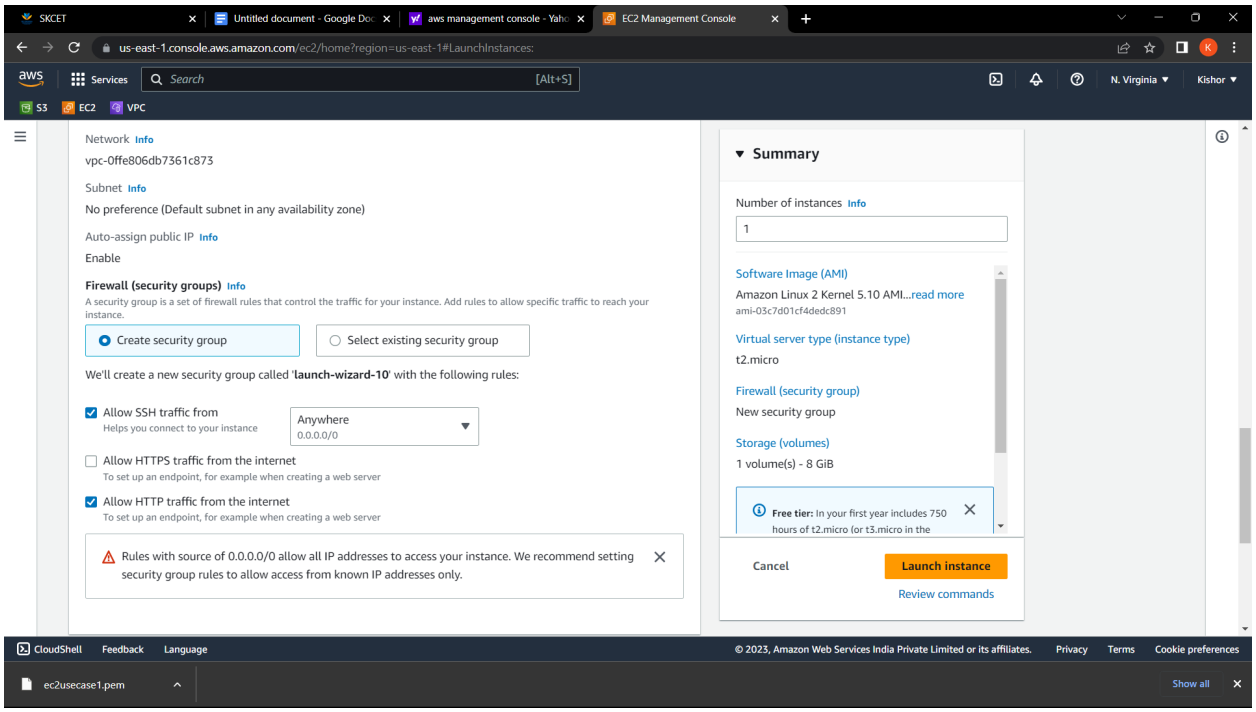
Allow SSH traffic for taking putty remote connection.

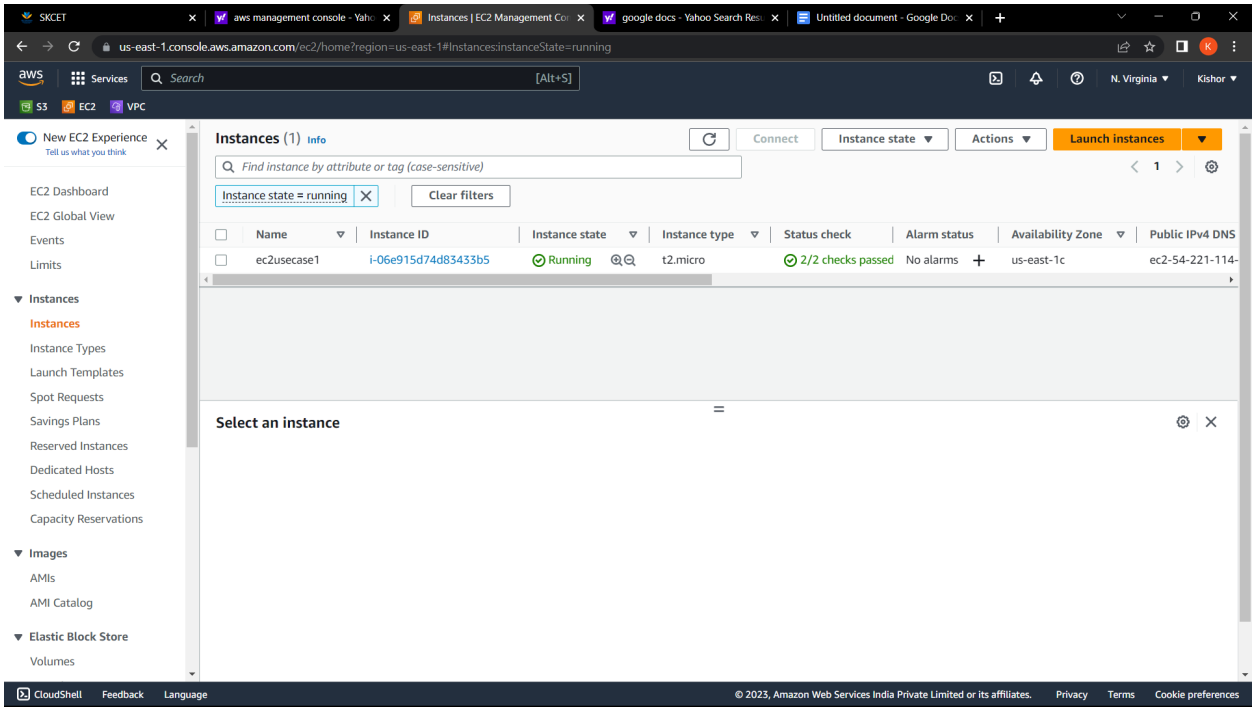
(4 Marks)



Allow HTTP traffic from the internet for reaching website requests.

(4 Marks)





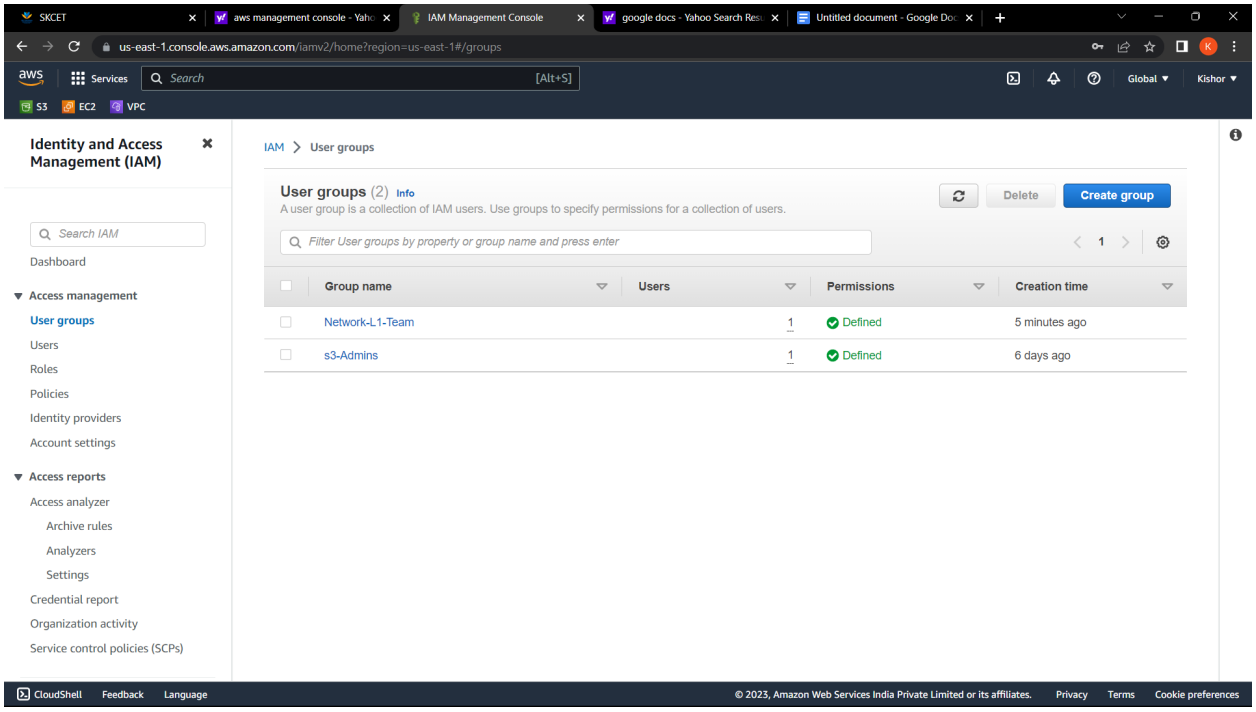
2.

Q2.

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.

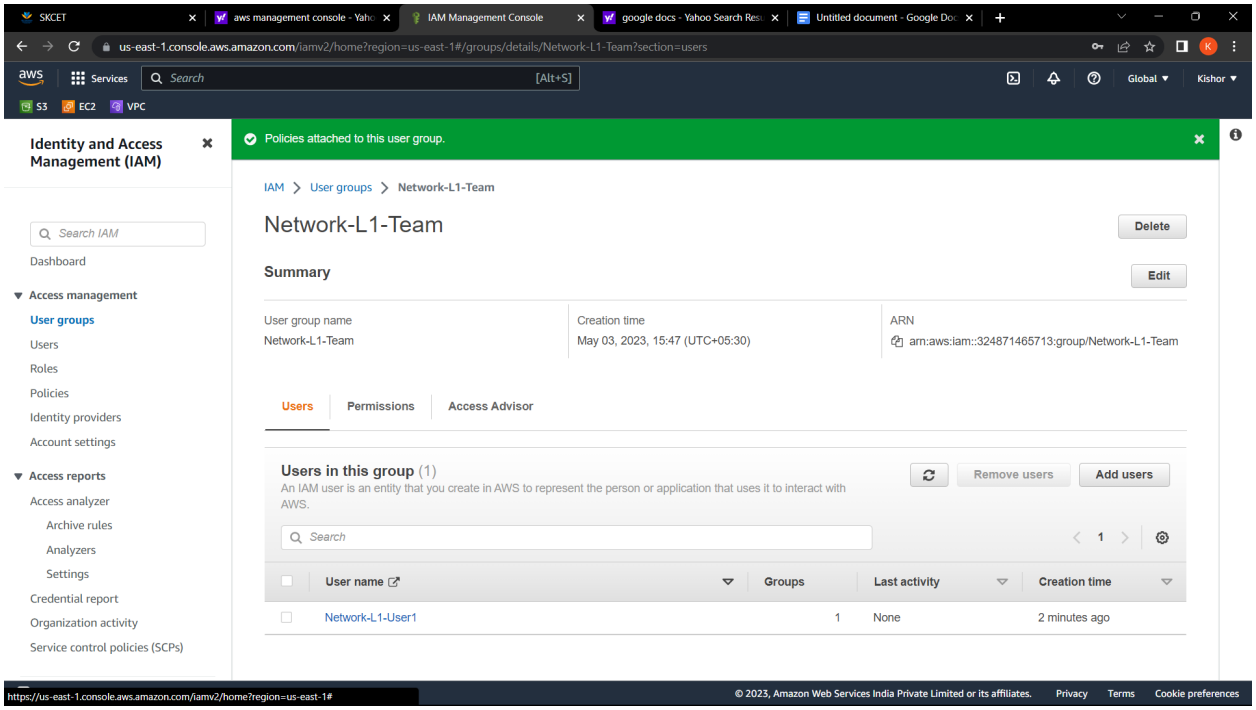
The name of the IAM group should be 'Network-L1-Team'.

(4 Marks)



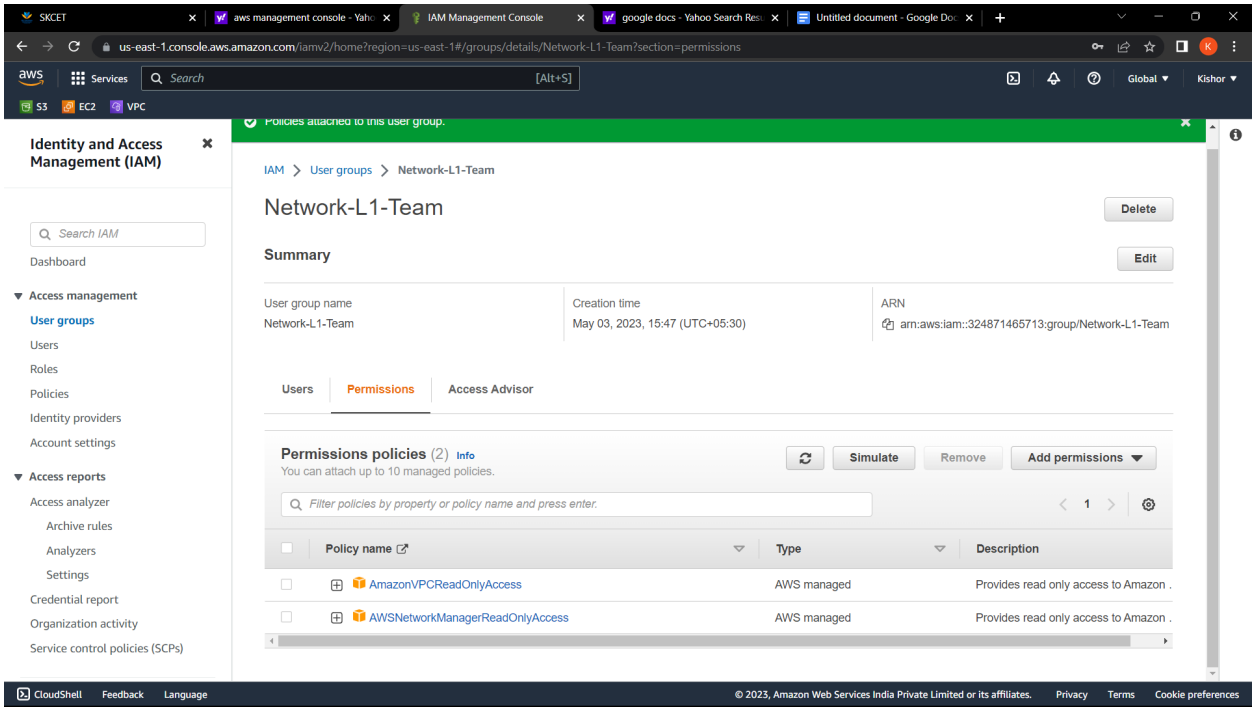
The name of the IAM user should be 'Network-L1-User1'.

(4 Marks)



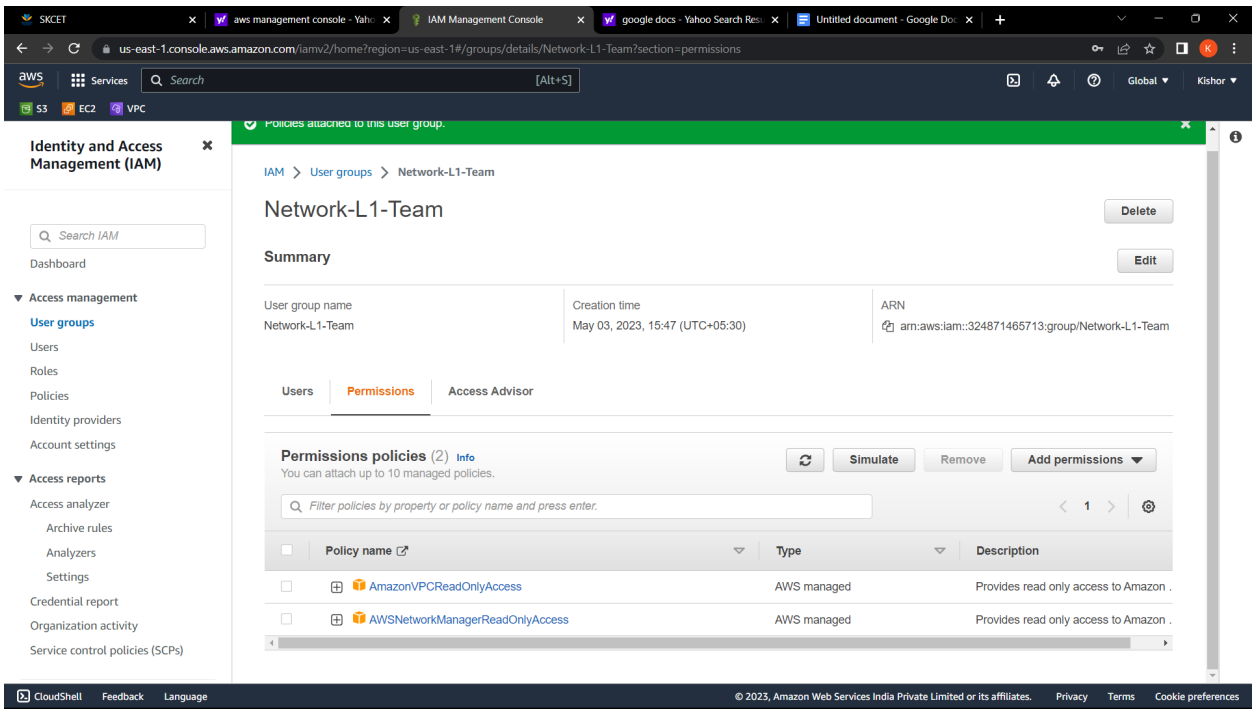
The 'AmazonVPCReadOnlyAccess' policy should be attached.

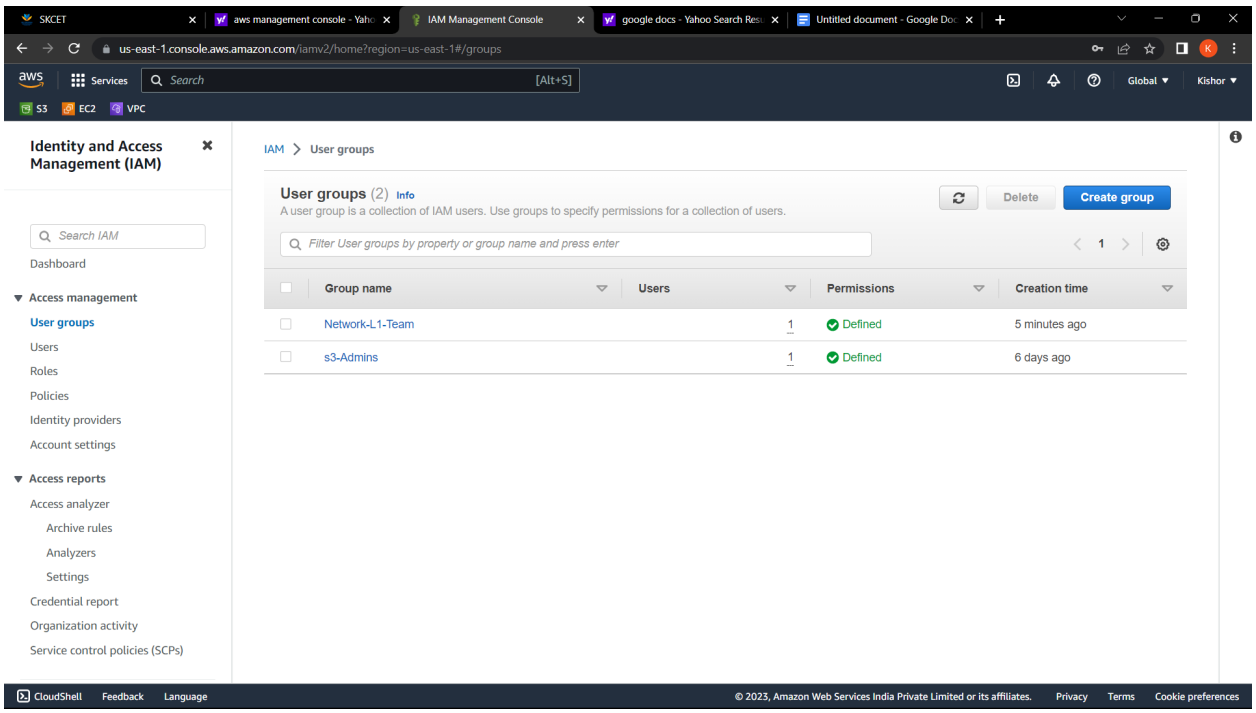
(4 Marks)



The 'AWSNetworkManagerReadOnlyAccess' policy should be attached.

(5 Marks)





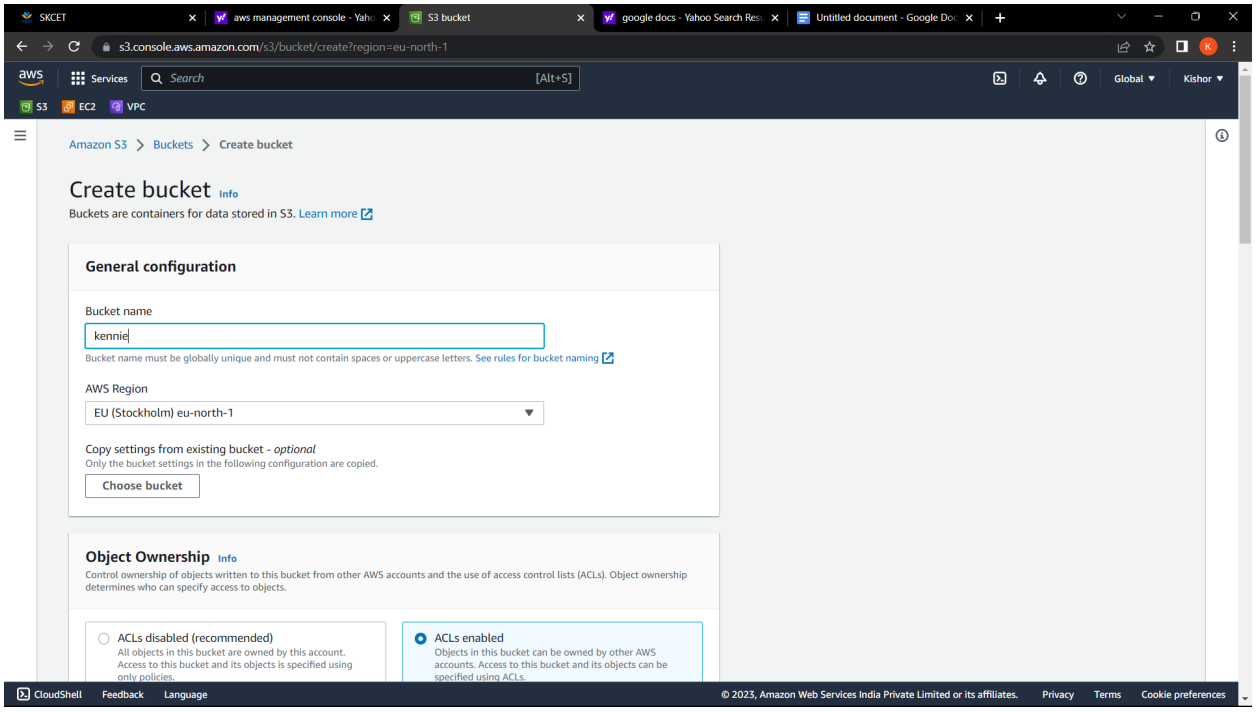
3.

Q3.

Create a S3 bucket for the following requirements

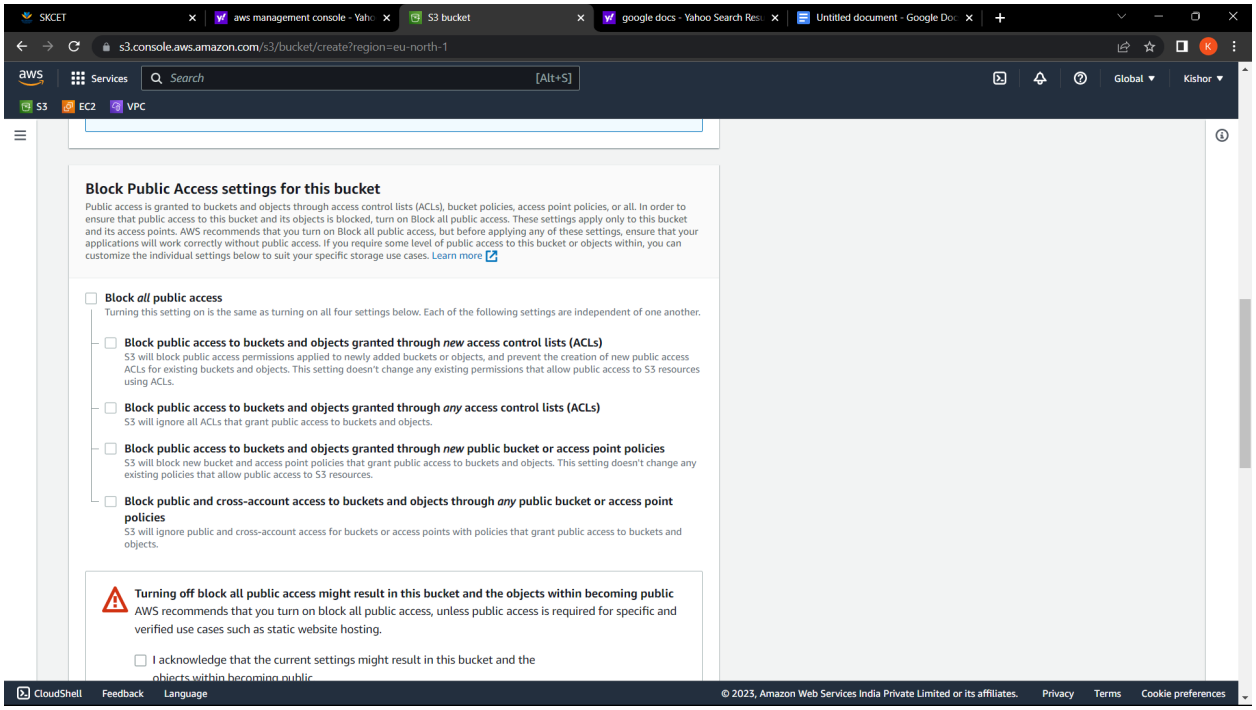
Create a new S3 bucket in the region of "Stockholm".

(4 Marks)



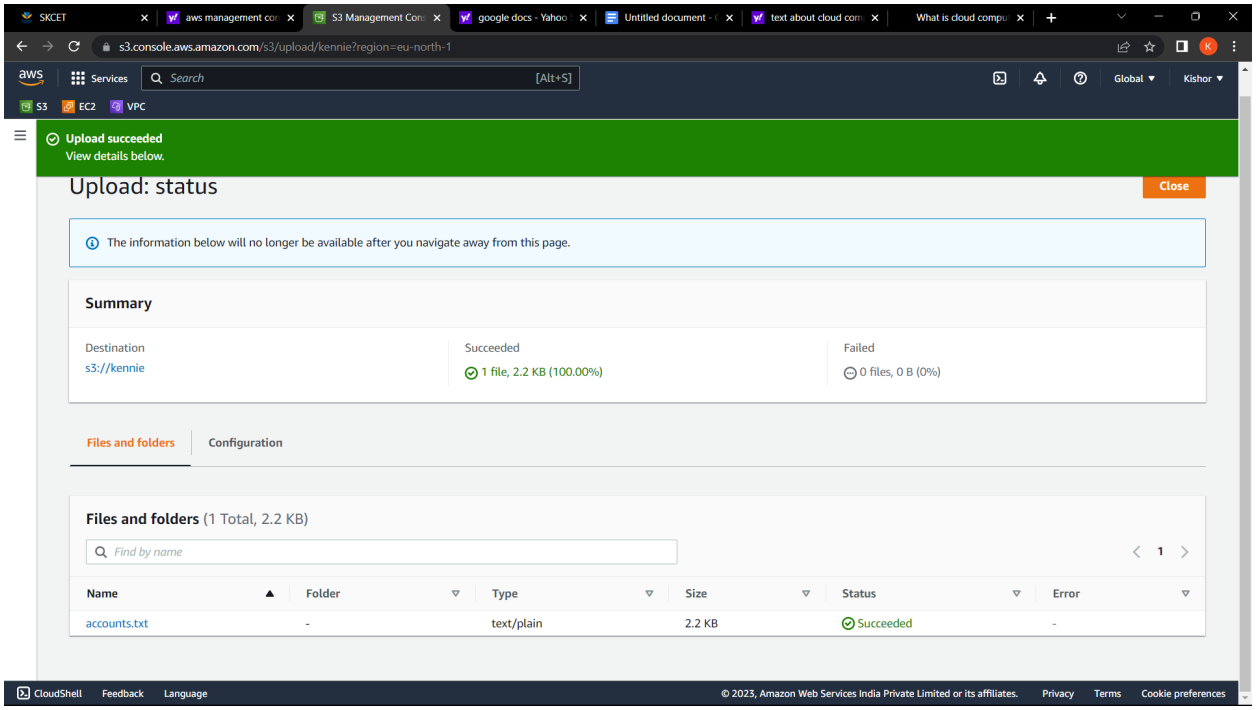
Make the bucket accessible to everyone(publicly) via Bucket ACL.

(4 Marks)



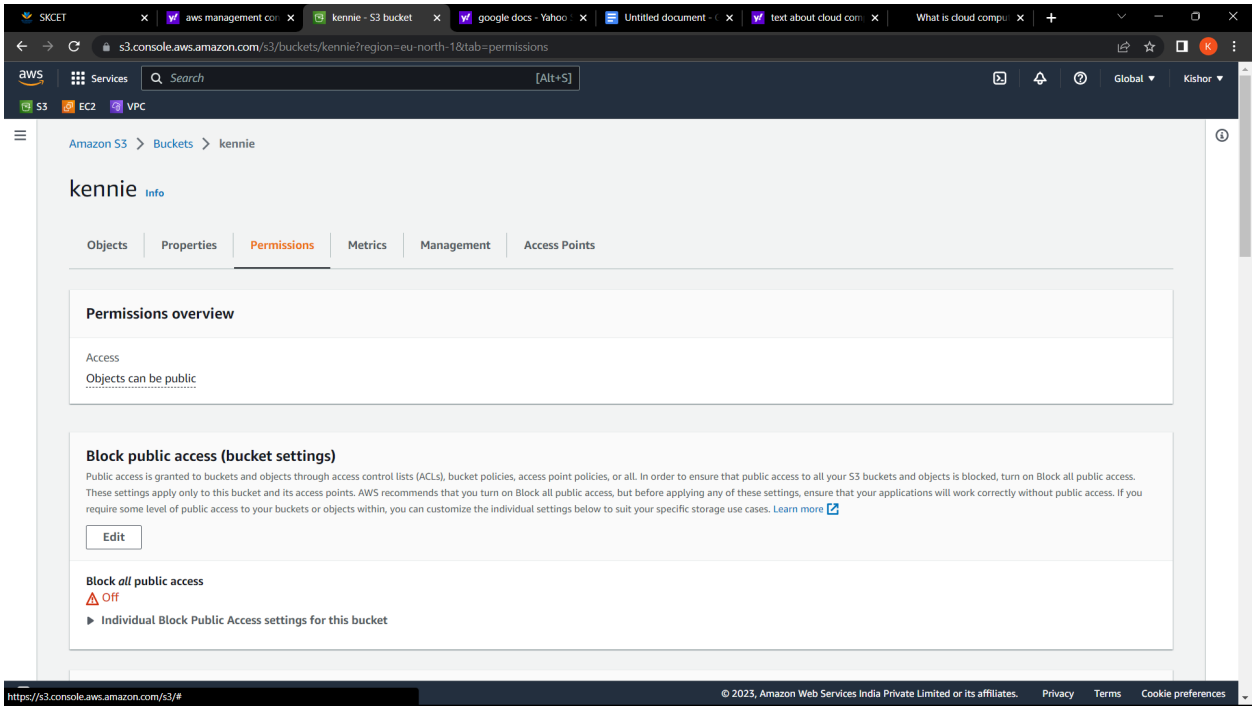
Upload a text file in the name of 'accounts.txt'.

(5 Marks)



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

(4 Marks)


SKCET
aws management con
kennie - S3 bucket
google docs - Yahoo
Untitled document -
text about cloud com
What is cloud compu
s3.console.aws.amazon.com/s3/buckets/kennie?region=eu-north-1&tab=permissions
aws
Services
Search
[Alt+S]
Global
Kishor
S3
EC2
VPC
Amazon S3 > Buckets > kennie
kennie Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Permissions overview
Access
Objects can be public
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Edit
Block all public access
Off
Individual Block Public Access settings for this bucket
https://s3.console.aws.amazon.com/s3/#
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences