

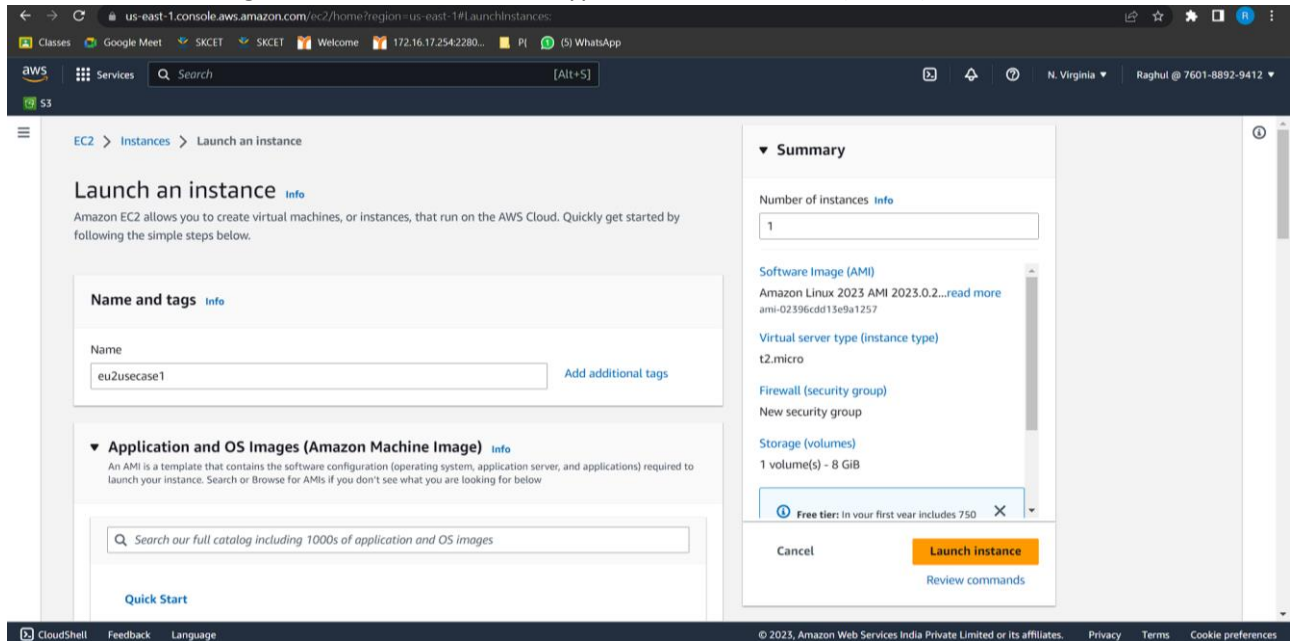
727721euit122

Raghul M

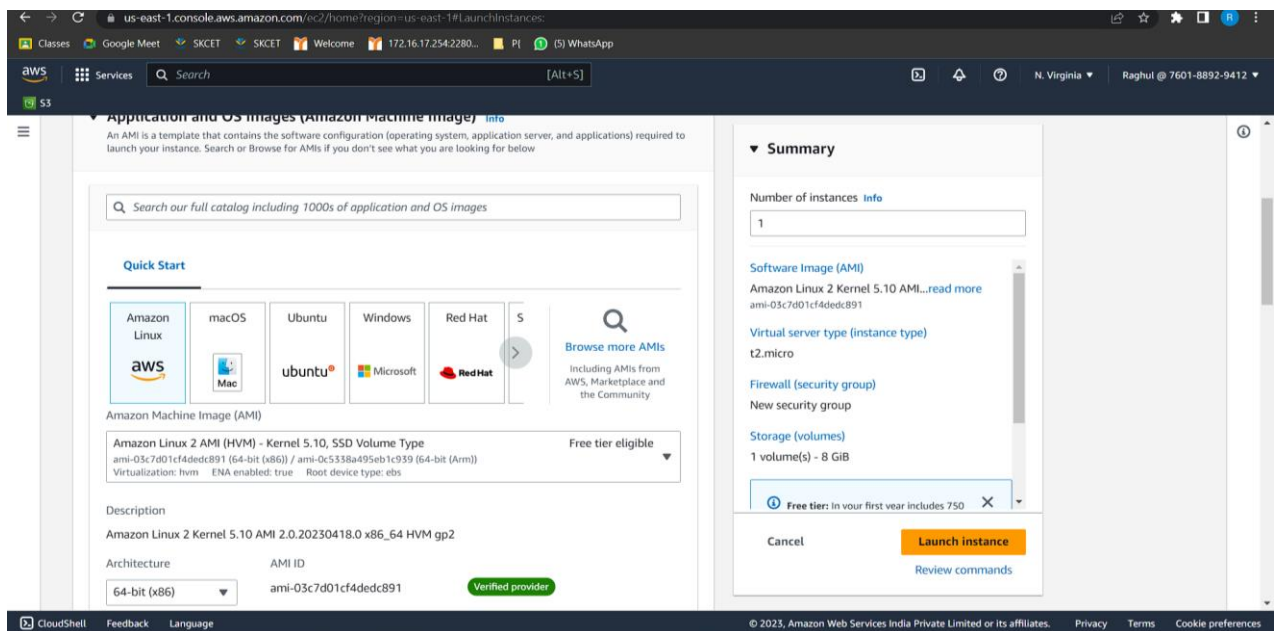
## Question 1:

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

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



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



c. Allow SSH traffic for taking puttyremote connection.

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

Classes Google Meet SKCET SKCET Welcome 172.16.17.254.2280... P( (S) WhatsApp

aws Services Search [Alt+S]

53

▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

eu2usecase1 Create new key pair

▼ Network settings Info Edit

Network Info

vpc-08fa2cdd7c773a802

Subnet Info

No preference (Default subnet in any availability zone)

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

▼ Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...read more

ami-03c7d01cf4dedc891

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 X

Cancel Launch instance Review commands

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

d. Allow HTTP traffic from the internet for reaching website requests.

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

Classes Google Meet SKCET SKCET Welcome 172.16.17.254.2280... P( (S) WhatsApp

aws Services Search [Alt+S]

53

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 gp2 Root volume (Not encrypted)

▼ Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...read more

ami-03c7d01cf4dedc891

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

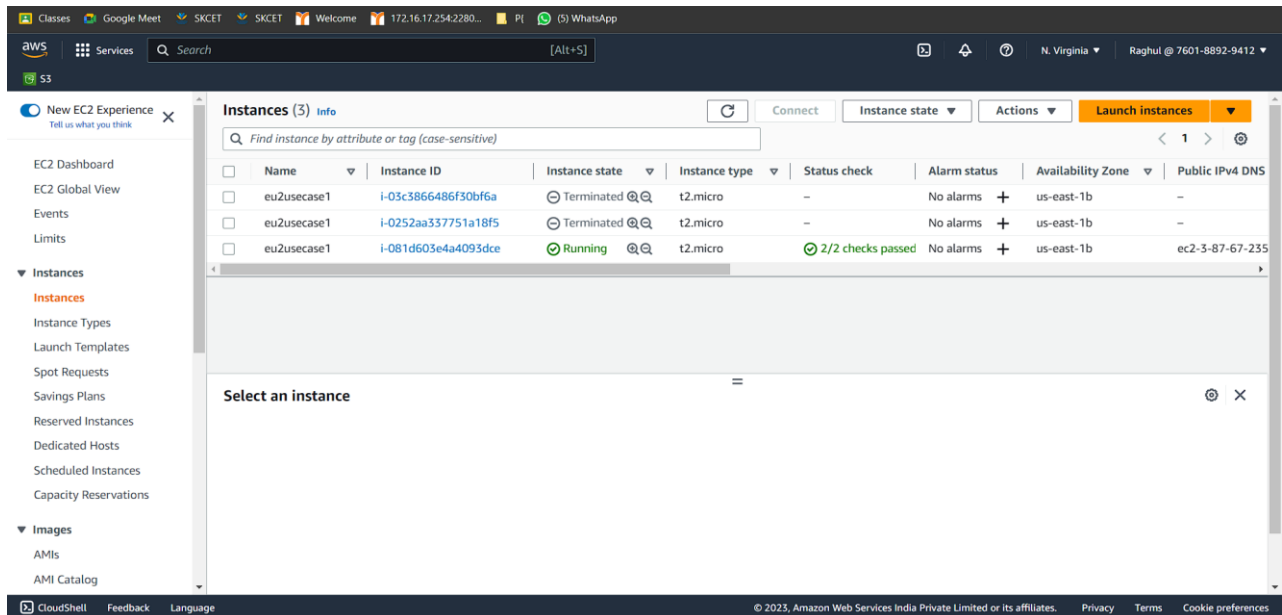
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 X

Cancel Launch instance Review commands

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

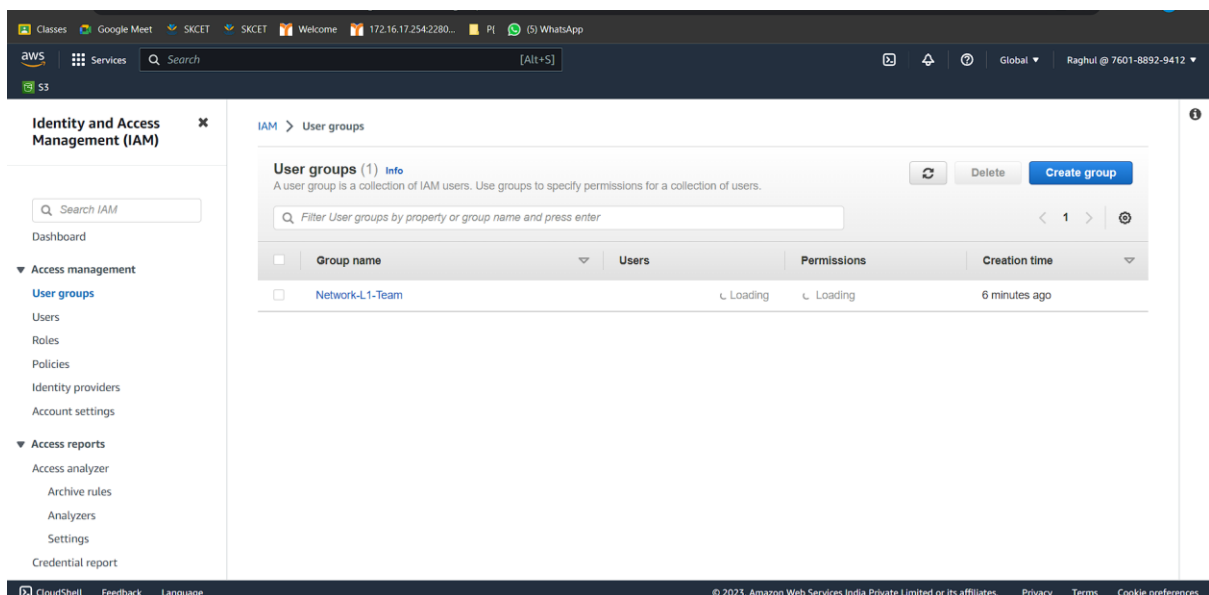
Result:



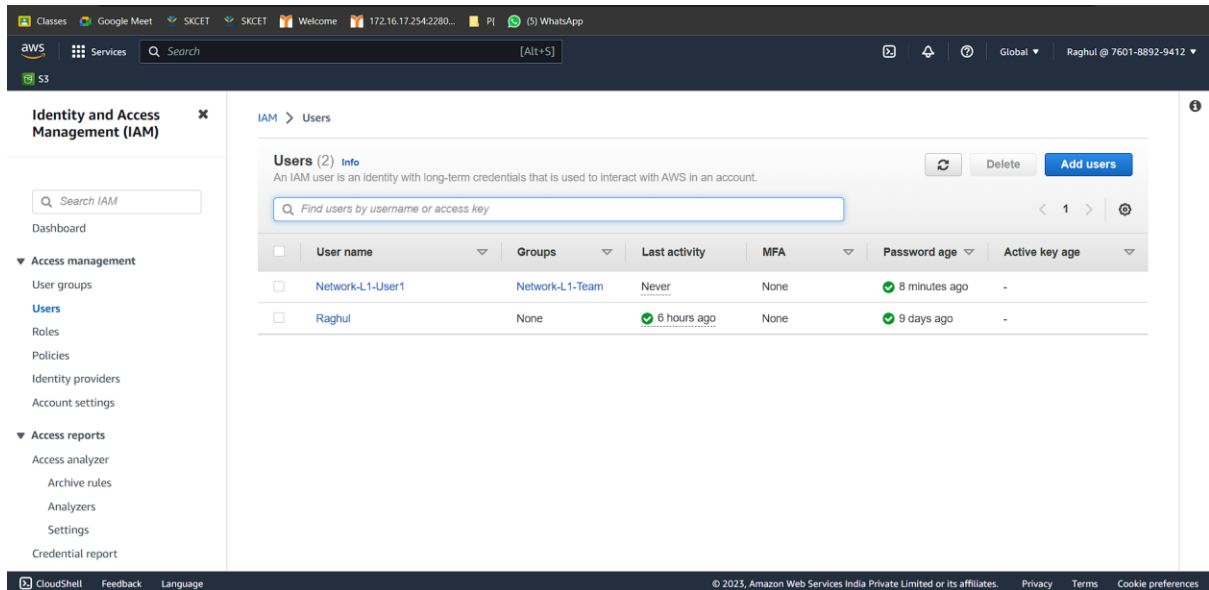
## Question 2:

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.

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



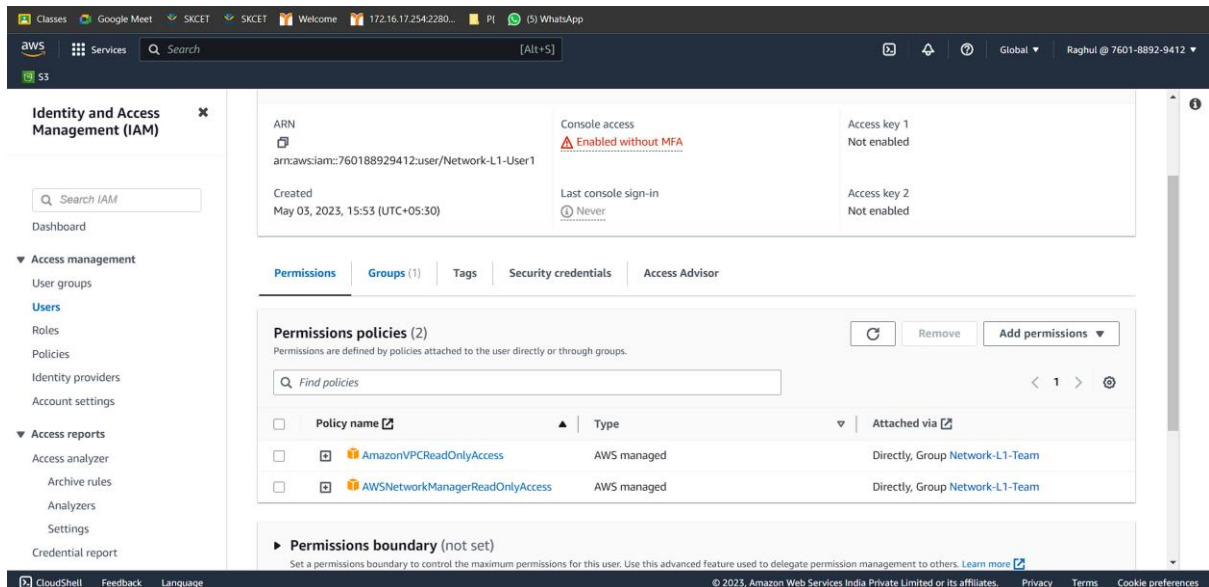
b. The name of the IAM user should be 'Network-L1-User1'.



The screenshot shows the AWS IAM console 'Users' page. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Access reports, and Credential report. The main content area shows a list of users. The user 'Network-L1-User1' is highlighted, and its details are shown below the list. The details include the ARN, console access status (Enabled without MFA), last console sign-in (Never), and access key status (Not enabled). The permissions section shows two policies attached: 'AmazonVPCReadOnlyAccess' and 'AWSNetworkManagerReadOnlyAccess', both attached directly to the user.

User name	Groups	Last activity	MFA	Password age	Active key age
Network-L1-User1	Network-L1-Team	Never	None	8 minutes ago	-
Raghul	None	6 hours ago	None	9 days ago	-

c. The 'AmazonVPCReadOnlyAccess' policy should be attached.



The screenshot shows the AWS IAM console 'Permissions' page for the user 'Network-L1-User1'. The left sidebar is the same as in the previous screenshot. The main content area shows the 'Permissions' tab selected. The 'Permissions policies' section lists two policies attached to the user: 'AmazonVPCReadOnlyAccess' and 'AWSNetworkManagerReadOnlyAccess', both attached directly to the user. The 'Permissions boundary' section is also visible, showing that no boundary is set for this user.

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

d. The 'AWSNetworkManagerReadOnlyAccess' policy should be attached.

The screenshot shows the AWS IAM console interface. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, and Access reports. The main content area displays the 'Permissions' tab for a user. The user's ARN is 'arn:aws:iam::760188929412:user/Network-L1-User1'. The console access is 'Enabled without MFA'. The user was created on May 03, 2023, at 15:53 (UTC+05:30). The last console sign-in was 'Never'. The user has two access keys, both of which are 'Not enabled'. The 'Permissions policies (2)' section shows a table with two policies: 'AmazonVPCReadOnlyAccess' and 'AWSNetworkManagerReadOnlyAccess', both of which are 'AWS managed' and attached directly to the 'Network-L1-Team' group. The 'Permissions boundary' section is currently 'not set'.

Q3.

**Create a S3 bucket for the following requirements**

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

The screenshot shows the AWS S3 console 'Create bucket' page. The bucket name is 'mybucketraghu169' and the AWS Region is 'EU (Stockholm) eu-north-1'. The page includes a 'General configuration' section with a 'Bucket name' field, an 'AWS Region' dropdown, and a 'Copy settings from existing bucket - optional' section. The 'Object Ownership' section is also visible, explaining that it controls ownership of objects written to the bucket.

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

applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

- ☐ **Block all public access**  
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
- ☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through new public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

**Turning off block all public access might result in this bucket and the objects within becoming public**  
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

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

Successfully created folder "account.txt".  
Operation successfully completed.

Amazon S3 > Buckets > mybucketraghul69

mybucketraghul69

Objects | Properties | Permissions | Metrics | Management | Access Points

**Objects (1)**  
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

[Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	account.txt/	Folder	-	-	-

d.

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

EC2 S3 IAM

Successfully edited public access  
View details below.

Make public: status Close

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

**Summary**

Source s3://bucket07	Successfully edited public access ✔ 1 object	Failed to edit public access 0 objects
-------------------------	---	---

Failed to edit public access Configuration

Failed to edit public access (0)