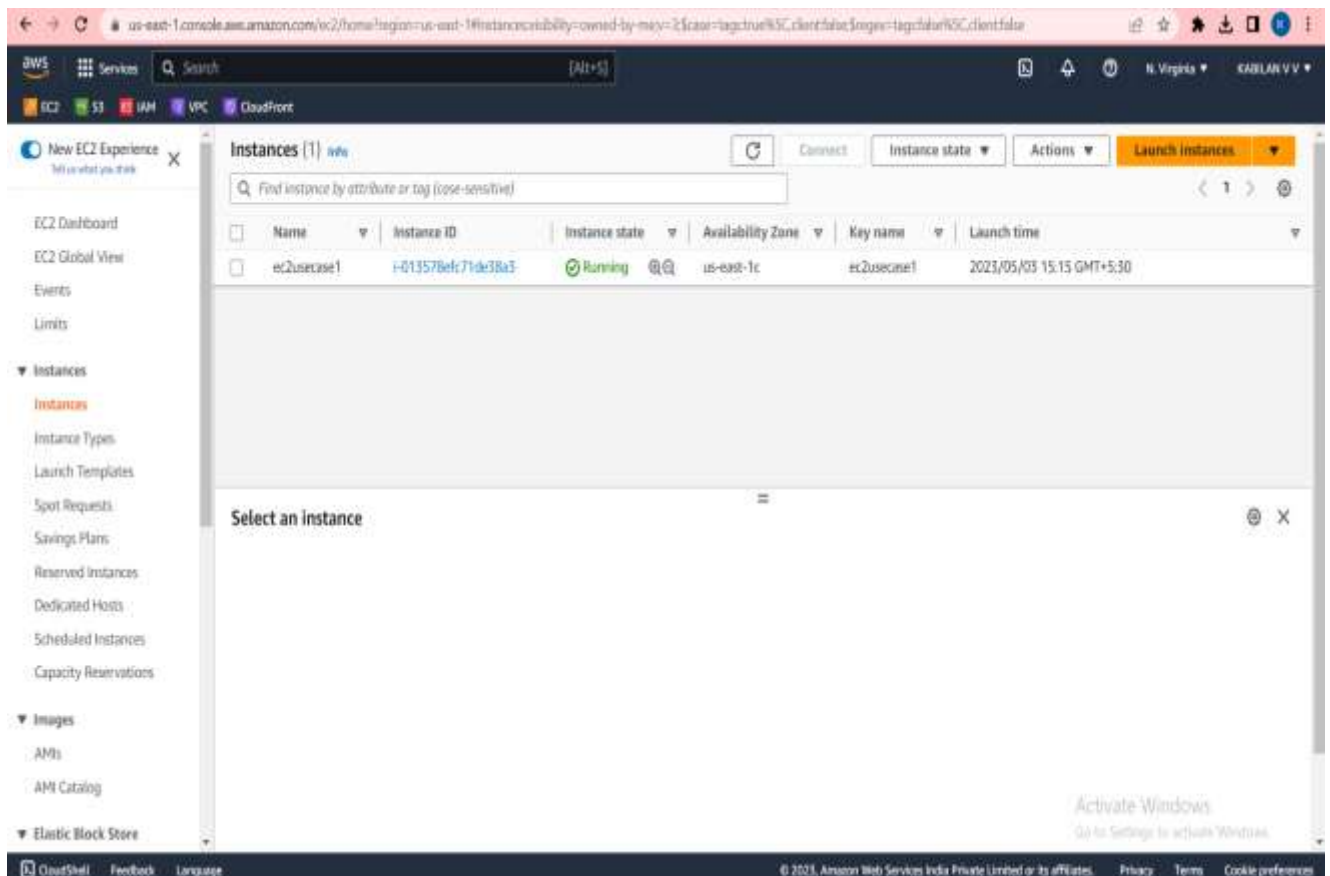


2023 SKCET Cloud CC1 QN-1

Time:30 minutes

Marks: 16

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)

The screenshot displays the AWS Management Console interface for an Amazon Machine Image (AMI). The browser address bar shows the URL: `us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ImageDetails:imageId=ami-07338c31862368efe`. The console header includes the AWS logo, a search bar, and navigation links for EC2, S3, IAM, VPC, and CloudFront. The left sidebar shows the 'New EC2 Experience' button and a navigation menu with categories like EC2 Dashboard, Instances, Images, and Elastic Block Store. The main content area is titled 'Image summary for ami-07338c31862368efe' and contains a table of image details.

Image summary for ami-07338c31862368efe			
AMI ID	ami-07338c31862368efe	Image type	machine
AMI name	Amazon Linux 2	Owner account ID	540910906034
Root device name	/dev/xvda	Status	Pending
Root mode	-	State reason	-
Block devices	/dev/xvda=snp-027fa6ef3052a3a498:trugp2	Description	-
Deprecation time	-	Last launched time	-
Platform details	Linux/UNIX	Architecture	x86_64
Root device type	EBS	Source	540910906034/Amazon Linux 2
Usage operation	RunInstances	Creation date	Wed May 03 2023 15:16:21 GMT+0530 (India Standard Time)
Virtualization type	hvm	Product codes	-
Kernel ID	-	RAM disk ID	-

Below the table, there are tabs for 'Permissions', 'Storage', and 'Tags'. The 'Permissions' tab is active, showing 'Image share permission' as 'Private' and a note: 'This image is only shared with account IDs, organizations, or OUs that you have specified.' At the bottom right, there is an 'Activate Windows' watermark and a link to 'Go to Settings to activate Windows'.

Allow SSH traffic for taking puttyremote connection.(4 Marks)

The screenshot displays the AWS Management Console for an EC2 instance. The left sidebar shows navigation options like EC2 Dashboard, EC2 Global View, Events, Limits, Instances, Images, and Elastic Block Store. The main content area is the 'Security' tab for the instance, showing 'Security details'. Under 'Inbound rules', there are two rules:

Name	Security group rule ID	Port range	Protocol	Source	Security groups
-	sgr-02124dc656e08fcae	22	TCP	0.0.0.0/0	launch-wizard-1
-	sgr-02647e21a74d2afc3	80	TCP	0.0.0.0/0	launch-wizard-1

Under 'Outbound rules', there is one rule:

Name	Security group rule ID	Port range	Protocol	Destination	Security groups
-	sgr-0a93fa4b275fcd44	All	All	0.0.0.0/0	launch-wizard-1

The bottom of the console shows the footer with '© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences'.

Allow HTTP traffic from the internet for reaching website requests.(4 Marks)

The screenshot displays the AWS Management Console interface for an EC2 instance. The left sidebar shows the navigation menu with categories like Instances, Images, and Elastic Block Store. The main content area is titled 'Security' and shows the 'Inbound rules' table. The table has columns for Name, Security group rule ID, Port range, Protocol, Source, and Security groups. Two rules are listed: one for port 22 (SSH) and one for port 80 (HTTP). The rule for port 80 is highlighted, showing it allows traffic from 0.0.0.0/0. The 'Outbound rules' table is also visible below, showing a single rule for all traffic to 0.0.0.0/0.

Name	Security group rule ID	Port range	Protocol	Source	Security groups
-	sg-0214dc55e08fcae	22	TCP	0.0.0.0/0	launch-wizard-1
-	sg-02647e21e7442afc3	80	TCP	0.0.0.0/0	launch-wizard-1

Name	Security group rule ID	Port range	Protocol	Destination	Security groups
-	sg-0e035a4b275cdk44	All	All	0.0.0.0/0	launch-wizard-1

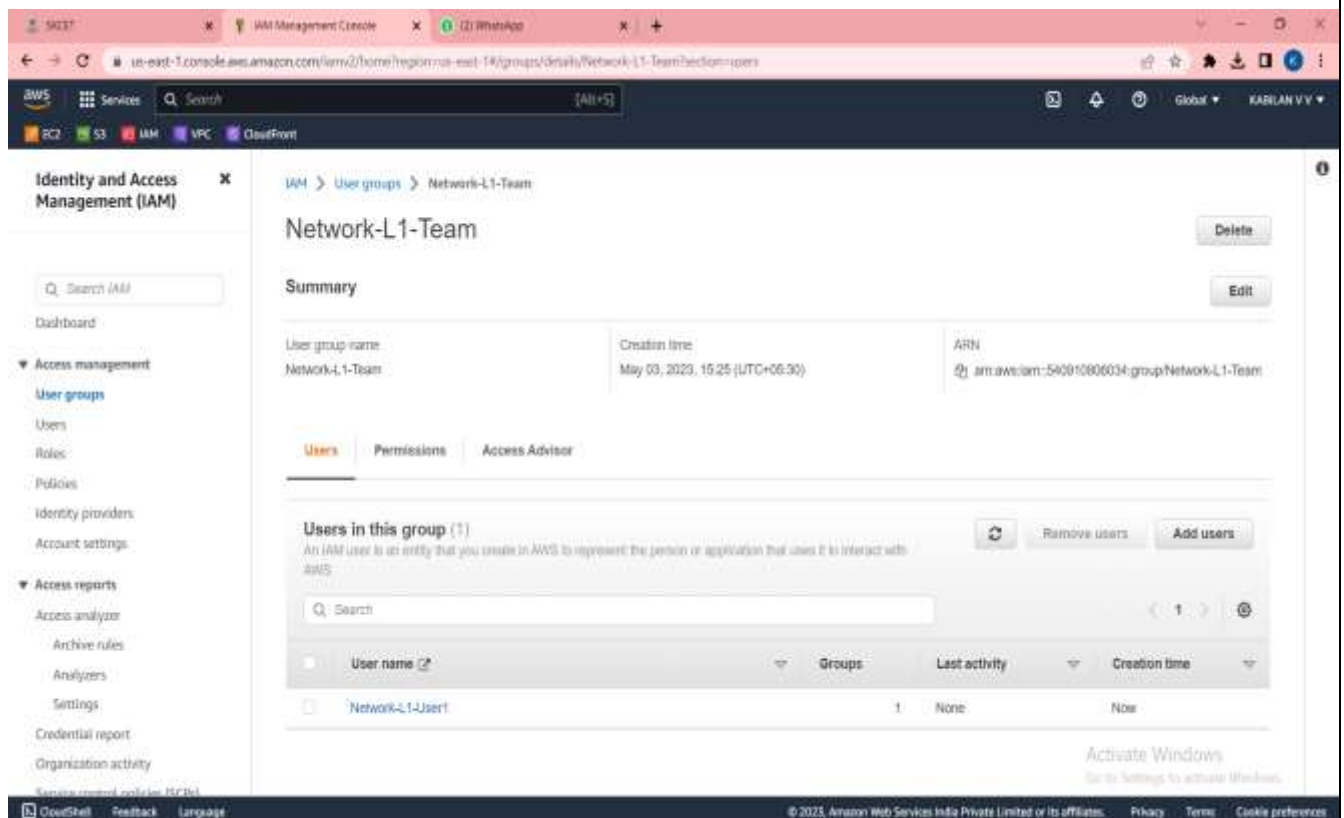
2023 SKCET Cloud CC1 QN-2

Time:30 minutes

Marks: 17

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 screenshot displays the AWS IAM Management Console interface. The left-hand navigation pane shows the 'Identity and Access Management (IAM)' section, with 'User groups' selected. The main content area shows the details for the 'Network-L1-Team' user group. The 'Summary' tab is active, displaying the user group name, creation time (May 05, 2023, 15:25 UTC+05:30), and ARN (arn:aws:iam::540910900334:group/Network-L1-Team). Below the summary, the 'Users' tab is selected, showing a list of users in the group. The list contains one user, 'Network-L1-User1', with a count of 1. The bottom of the screen shows the 'Activate Windows' watermark and the footer with copyright information for Amazon Web Services India Private Limited.

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

Organization activity

Network-L1-Team

Delete

Edit

Summary

User group name: Network-L1-Team

Creation time: May 05, 2023, 15:25 (UTC+05:30)

ARN: arn:aws:iam::540910900334:group/Network-L1-Team

Users

Permissions

Access Advisor

Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

1

User name

Groups

Last activity

Creation time

Network-L1-User1

1

None

Now

Activate Windows

Go to Settings to activate Windows

CloudShell Feedback Language

© 2021 Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

The 'AmazonVPCReadOnlyAccess' policy should be attached.(4 Marks)

The screenshot displays the AWS IAM console interface. The left sidebar shows the 'Identity and Access Management (IAM)' menu with options like 'Dashboard', 'Access management', 'Access reports', and 'Account settings'. The main content area shows the 'Network-L1-Team' user group details. Under the 'Permissions' tab, a table lists the attached policies:

Policy name	Type	Description
AmazonVPCReadOnlyAccess	AWS managed	Provides read only access to Amazon VPC via the AWS Management Console.
AWSNetworkManagerReadOnlyAccess	AWS managed	Provides read only access to Amazon NetworkManager via the AWS Management Console.

The bottom of the console shows the footer with '© 2023, Amazon Web Services India Private Limited or its affiliates.' and links for 'Privacy', 'Terms', and 'Cookie preferences'.

The 'AWSNetworkManagerReadOnlyAccess' policy should be attached.(5Marks)

The screenshot displays the AWS IAM console interface. The left sidebar shows the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, User groups, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, and Organization activity. The main content area shows the 'Network-L1-Team' user group details. The 'Summary' tab is active, displaying the user group name, creation time (May 03, 2023, 15:25 (UTC+05:30)), and ARN (arn:aws:iam:54091000034:group/Network-L1-Team). The 'Permissions' tab is also visible, showing a list of attached policies. The 'Permissions policies' section indicates that two policies are attached: 'AmazonVPCReadOnlyAccess' and 'AWSNetworkManagerReadOnlyAccess'. The 'AWSNetworkManagerReadOnlyAccess' policy is highlighted, showing its description: 'Provides read only access to Amazon NetworkManager via the AWS Management Console...'. The bottom of the screen shows the footer with '© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences'.

Policy name	Type	Description
AmazonVPCReadOnlyAccess	AWS managed	Provides read only access to Amazon VPC via the AWS Management Console...
AWSNetworkManagerReadOnlyAccess	AWS managed	Provides read only access to Amazon NetworkManager via the AWS Management Console...

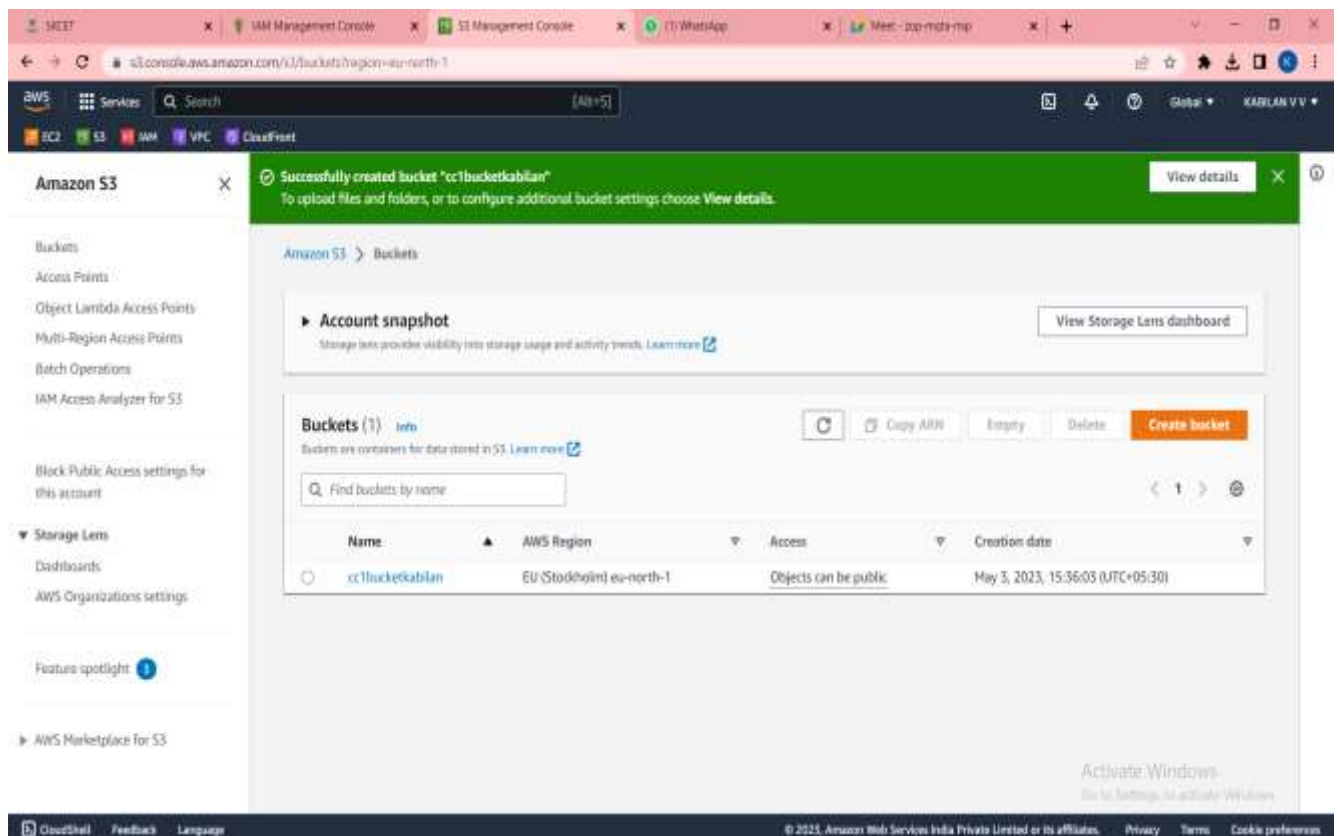
023 SKCET Cloud CC1 QN-3

Time : 30 minutes

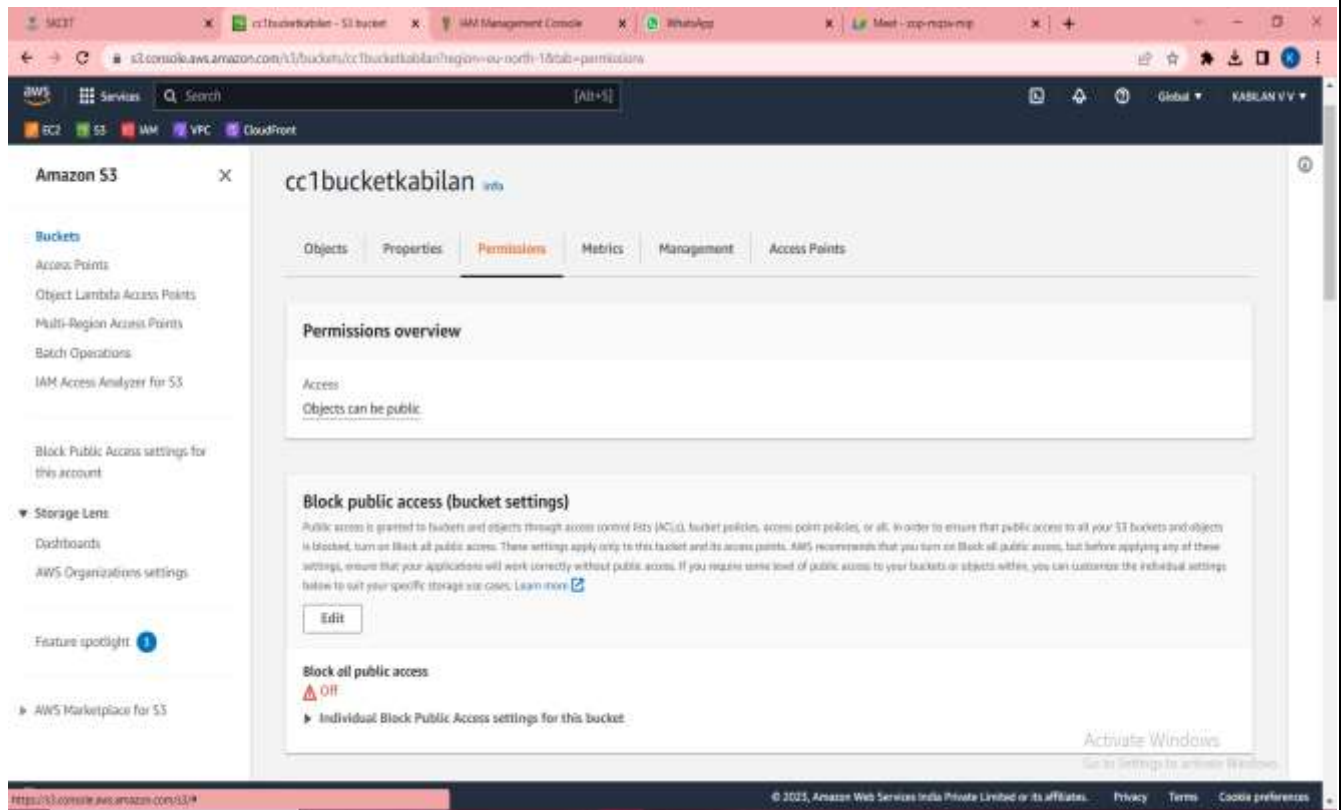
Marks: 17

Q3. Create a S3 bucket for the following requirements

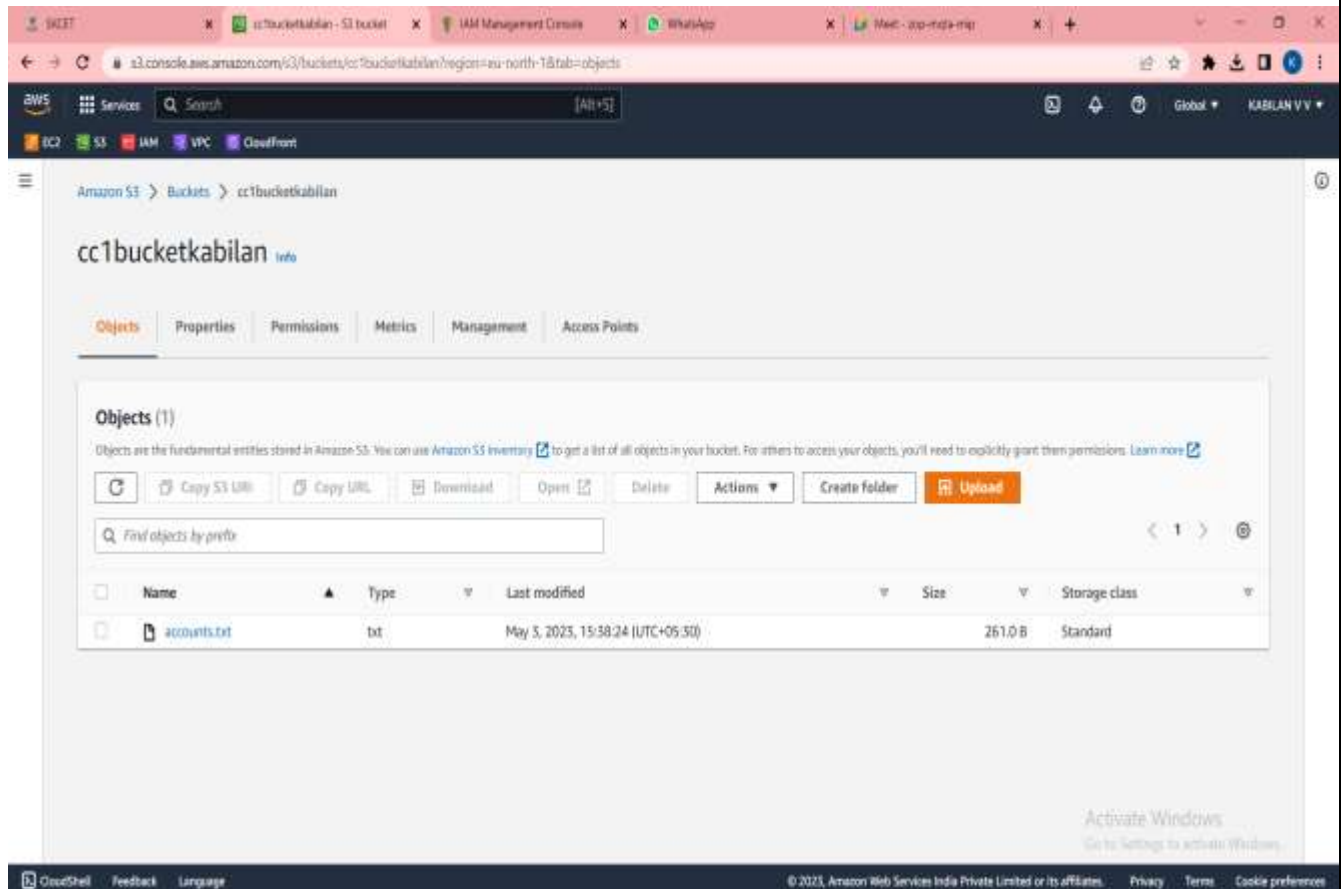
Create a new S3 bucket in the region of "Stockholm". (4 Marks)



Make the bucket accessible to everyone(publicly) via Bucket ACL.(4 Marks)



Upload a text file in the name of 'accounts.txt'. (5Marks)



Make the object 'accounts.txt' file accessible to everyone (publicly).(4 Marks)

