

NAME :KARTHIKEYAN R

REGISTER NO:727721EUIT071

CODING CONTEST

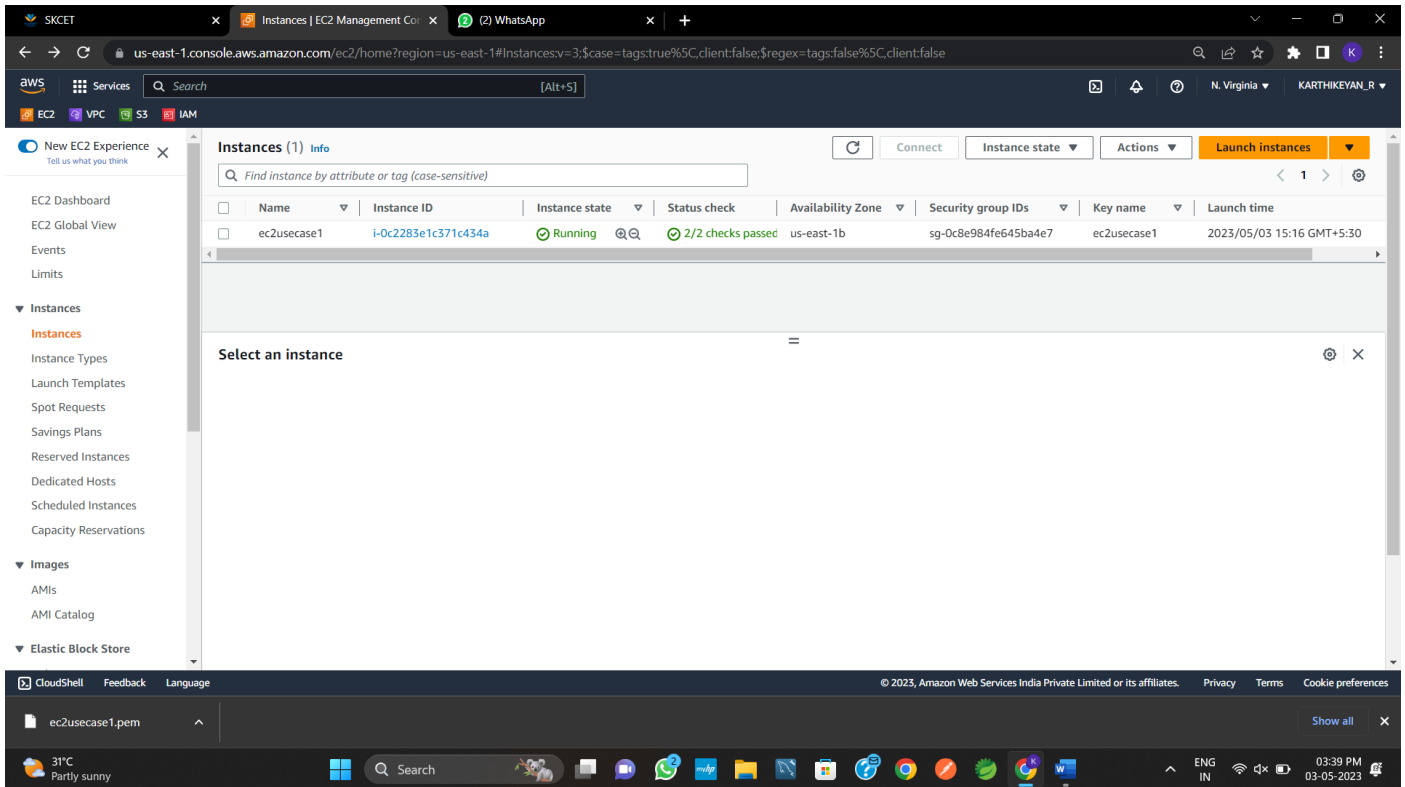
2023_SKCET_Cloud_CC1

Time:30 minutes

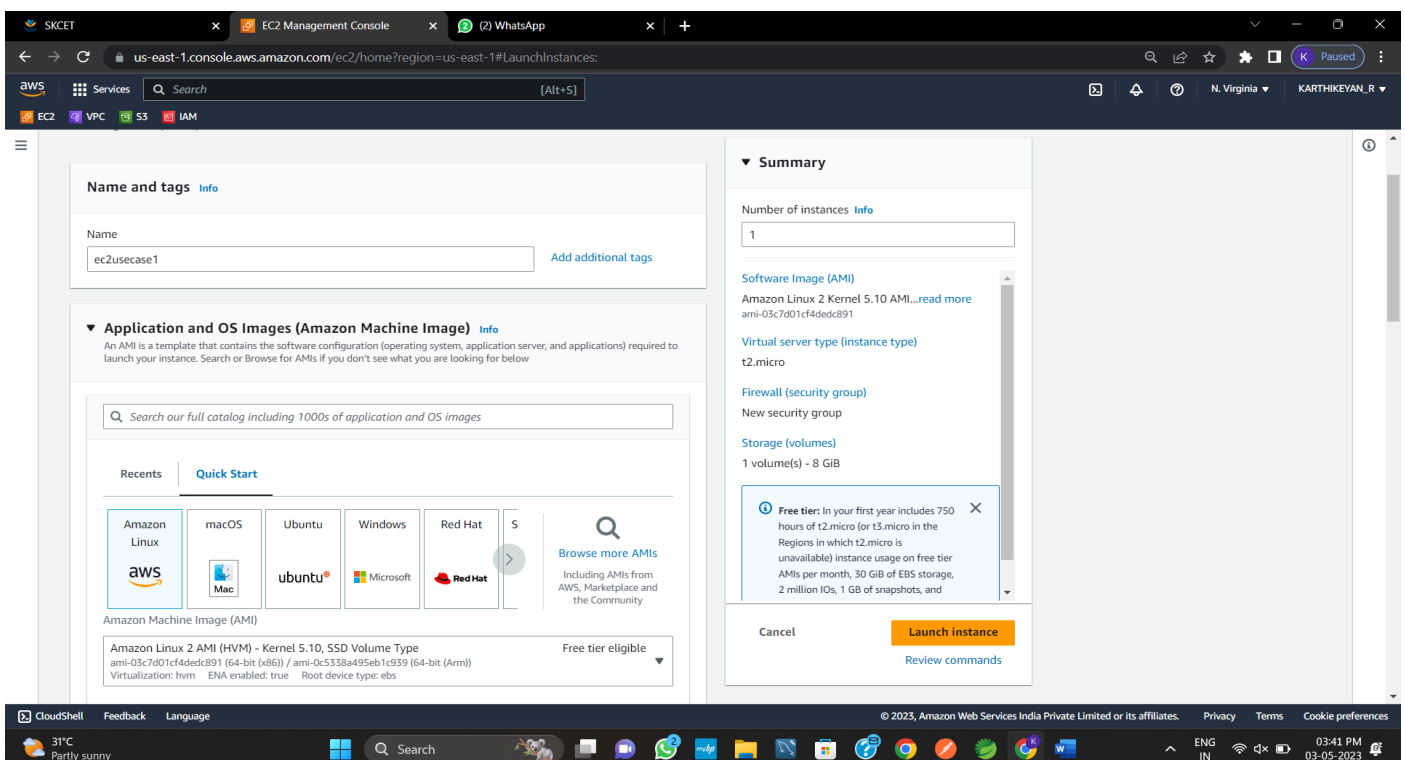
Marks: 16

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)



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

The screenshot shows the AWS Management Console interface for launching an EC2 instance. The 'Firewall (security groups)' step is active, showing the configuration for a new security group named 'launch-wizard-2'. The 'Allow SSH traffic from' rule is selected, and the source is set to 'Anywhere (0.0.0.0/0)'. The 'Summary' panel on the right displays the instance configuration: 1 instance, ami-03c7d01cf4dedc891, t2.micro instance type, and 1 volume of 8 GiB. The 'Launch instance' button is visible.

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

The screenshot shows the AWS Management Console interface for launching an EC2 instance. The 'Firewall (security groups)' step is active, showing the configuration for a new security group named 'launch-wizard-2'. The 'Allow HTTP traffic from the internet' rule is selected, and the source is set to 'Anywhere (0.0.0.0/0)'. The 'Summary' panel on the right displays the instance configuration: 1 instance, ami-03c7d01cf4dedc891, t2.micro instance type, and 1 volume of 8 GiB. The 'Launch instance' button is visible.

NAME :KARTHIKEYAN R

REGISTER NO:727721EUIT071

2023_SKCET_Cloud_CC1

Time:30 minutes

Marks: 17

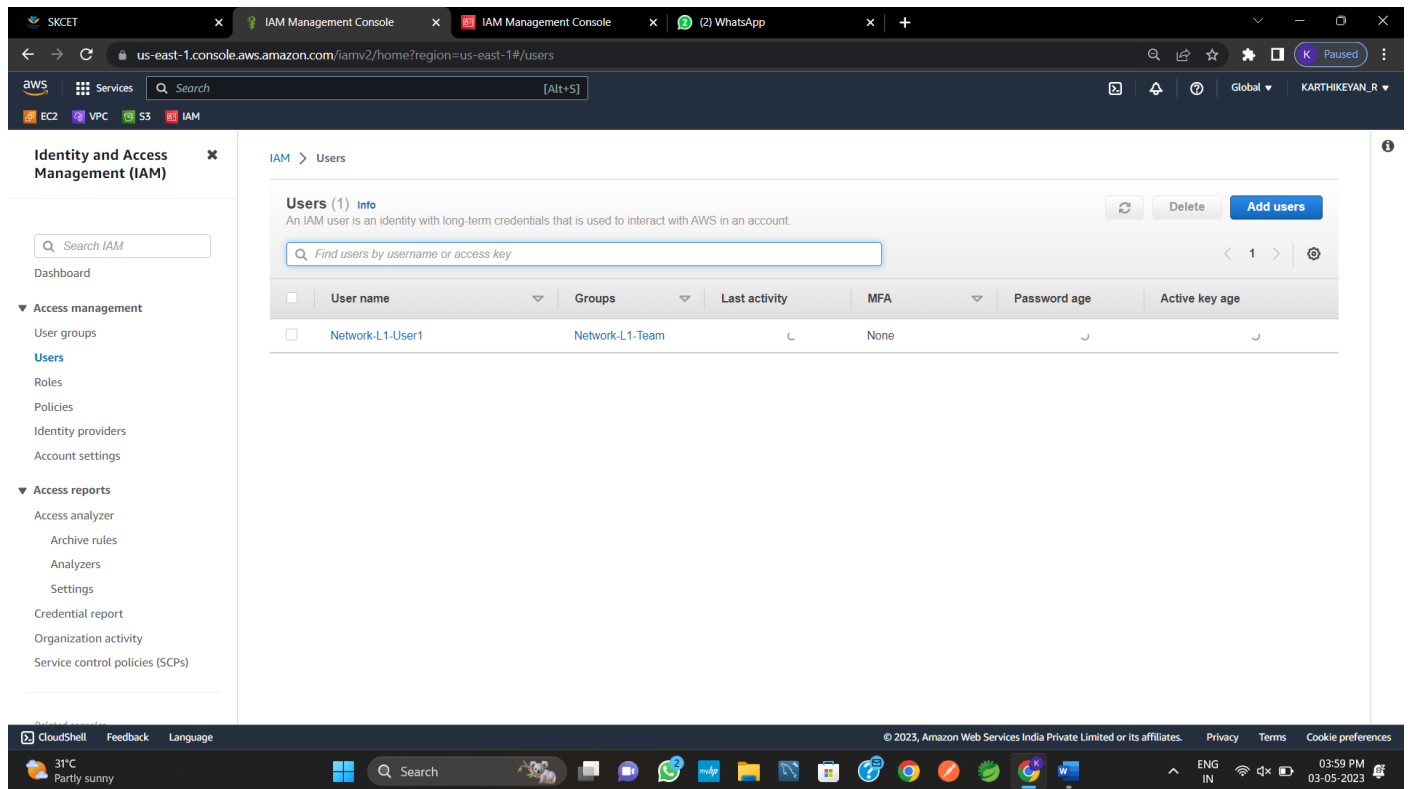
Q2. Create an IAM group called 'Network-L1-Team' with 'AmazonVPCReadOnlyAccess' and 'AWSNetworkManagerReadOnlyAccess' policies, then add an IAM user called 'Network-L1-User1' to the group.

The name of the IAM group should be 'Network-L1-Team'.(4 Marks)

The screenshot shows the AWS IAM console 'User groups' page. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, and Access reports. The main content area shows a list of user groups. One group, 'Network-L1-Team', is listed with 1 user, 'Network-L1-User1', and is defined 5 minutes ago. A tooltip shows the user 'Network-L1-User1' is in this group.

The screenshot shows the AWS IAM console 'Network-L1-Team' details page. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, and Access reports. The main content area shows the 'Summary' tab for the 'Network-L1-Team' group. The 'Users' tab is selected, showing a list of users in the group. One user, 'Network-L1-User1', is listed with 1 group, 'None' last activity, and 'Now' creation time.

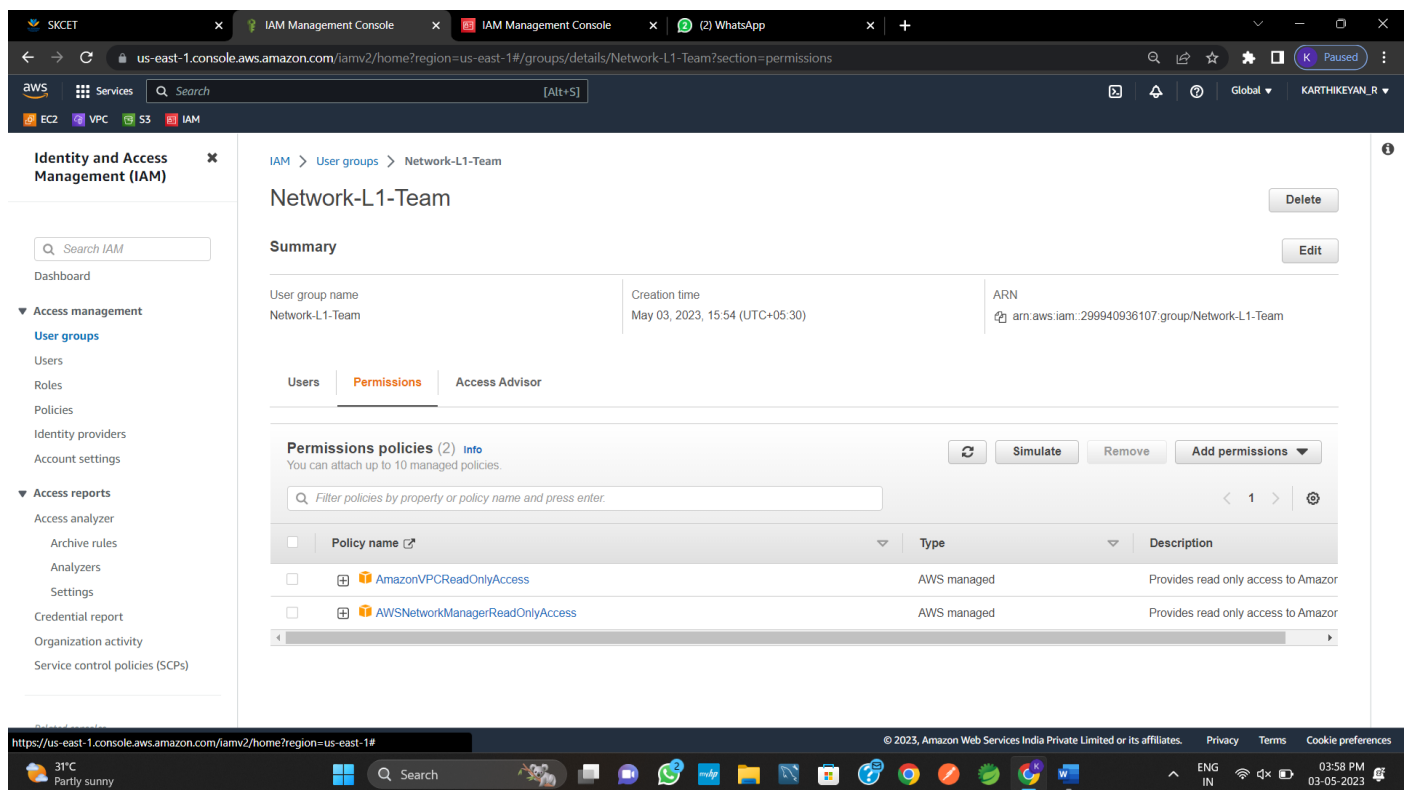
The name of the IAM user should be 'Network-L1-User1'.(4 Marks)



The screenshot shows the AWS IAM Management Console in the 'us-east-1' region. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Access reports, and Access analyzer. The main content area is titled 'Users (1)' and shows a table of IAM users. The table has columns for User name, Groups, Last activity, MFA, Password age, and Active key age. The user 'Network-L1-User1' is listed with the group 'Network-L1-Team'.

User name	Groups	Last activity	MFA	Password age	Active key age
Network-L1-User1	Network-L1-Team		None		

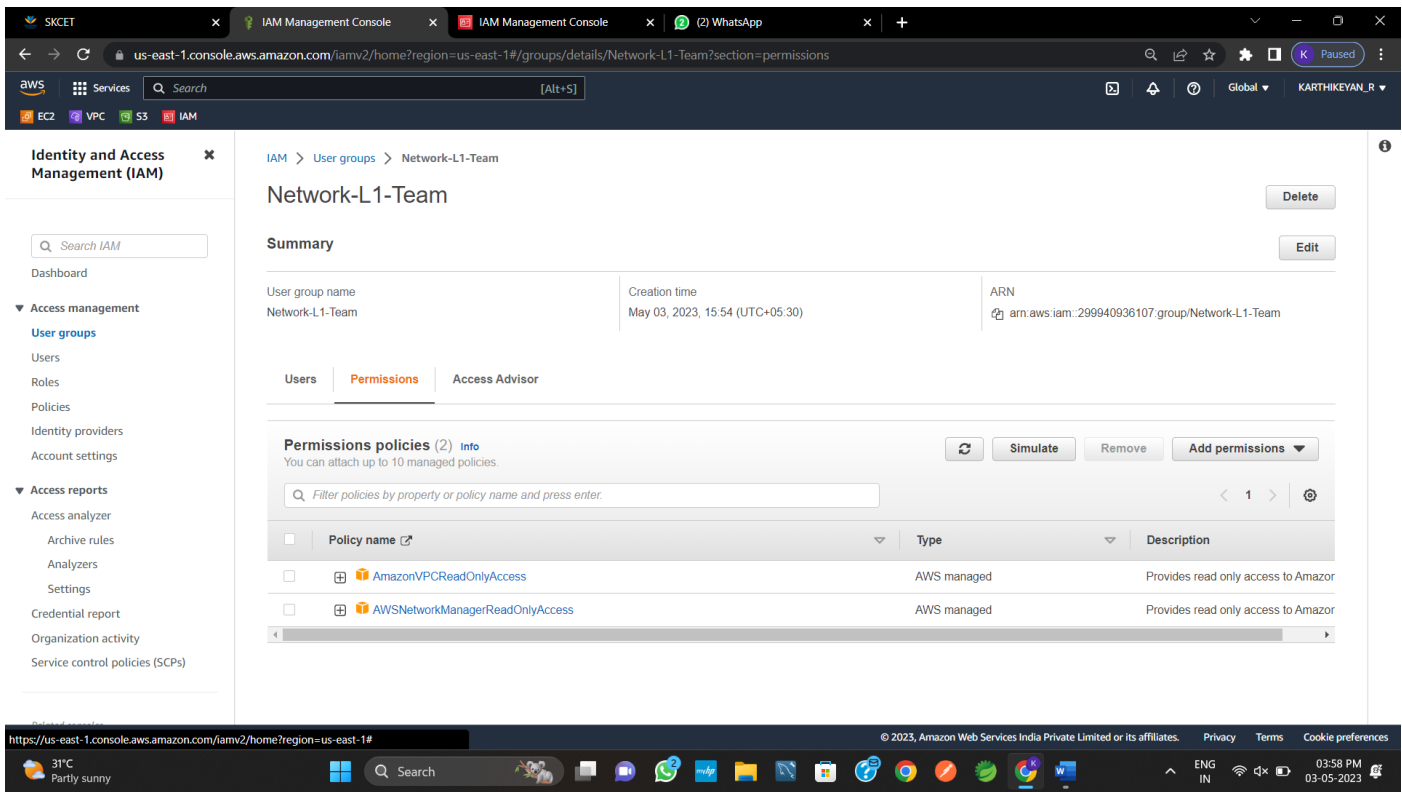
The 'AmazonVPCReadOnlyAccess' policy should be attached.(4 Marks)



The screenshot shows the AWS IAM Management Console in the 'us-east-1' region. The left sidebar contains the 'Identity and Access Management (IAM)' menu. The main content area is titled 'Network-L1-Team' and shows the 'Summary' tab. The 'Permissions' tab is selected, showing a list of attached policies. The policies are 'AmazonVPCReadOnlyAccess' and 'AWSNetworkManagerReadOnlyAccess'.

Policy name	Type	Description
AmazonVPCReadOnlyAccess	AWS managed	Provides read only access to Amazon VPC resources
AWSNetworkManagerReadOnlyAccess	AWS managed	Provides read only access to Amazon Network Manager resources

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



NAME :KARTHIKEYAN R

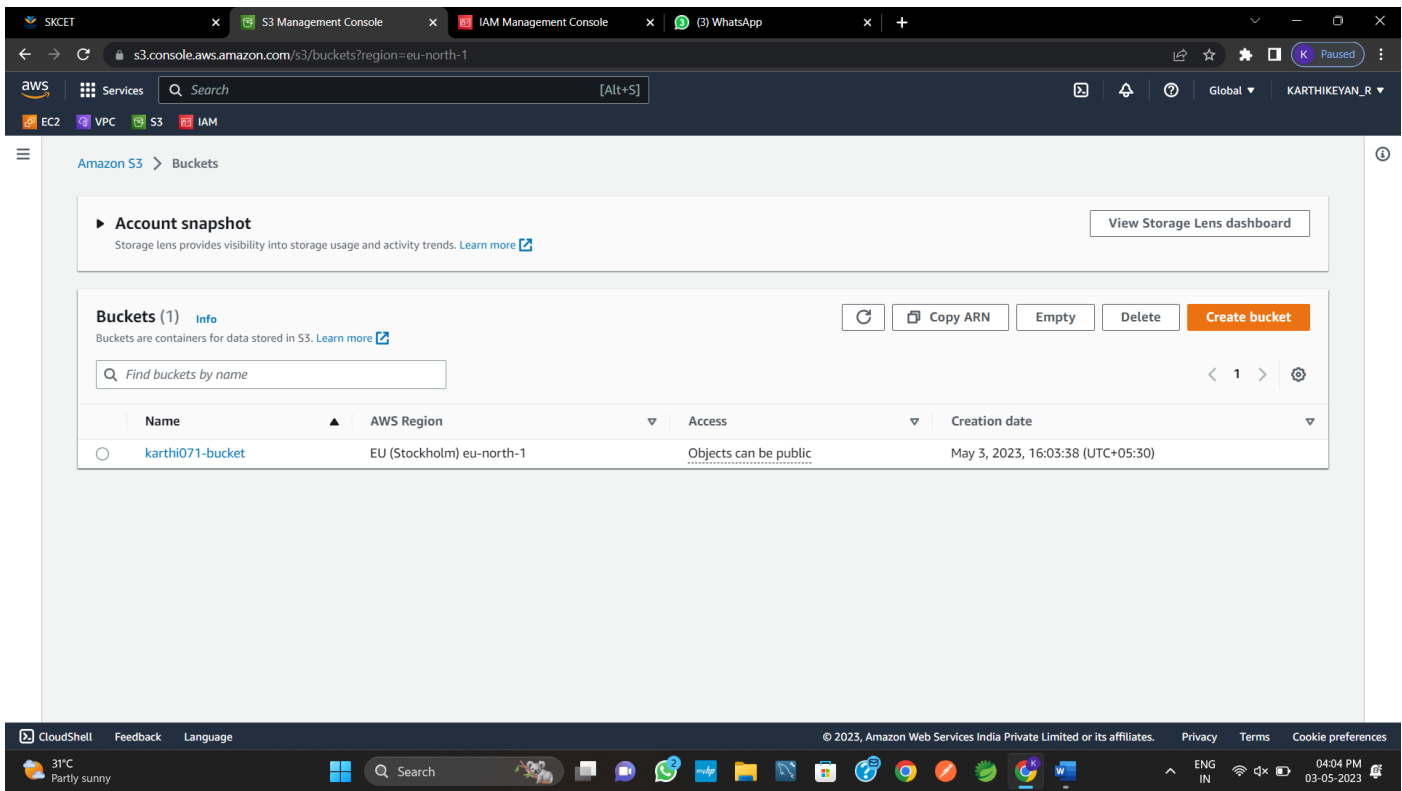
REGISTER NO:727721EUIT071

2023 SKCET Cloud CCI

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)

The screenshot shows the AWS IAM Management Console for the 'karthi071-bucket'. The 'Block public access' settings are displayed, showing that public access is currently blocked. The 'Block all public access' toggle is set to 'Off'. The 'Individual Block Public Access settings for this bucket' are also shown, with all four settings (Block public access to buckets and objects granted through new access control lists (ACLs), Block public access to buckets and objects granted through any access control lists (ACLs), Block public access to buckets and objects granted through new public bucket or access point policies, and Block public and cross-account access to buckets and objects through any public bucket or access point policies) all set to 'Off'.

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](#)

Block all public access

Individual Block Public Access settings for this bucket

- ☐ **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.

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

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

The screenshot shows the AWS S3 Management Console for the 'karthi071-bucket'. A green banner at the top indicates 'Upload succeeded'. The 'Summary' section shows that the upload was successful, with 1 file (2.0 B) uploaded (100.00%). The 'Files and folders' section shows a table with 1 total file, 2.0 B in size, and a status of 'Succeeded'.

Upload succeeded
View details below.

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

Summary

Destination s3://karthi071-bucket	Succeeded 1 file, 2.0 B (100.00%)	Failed 0 files, 0 B (0%)
--------------------------------------	--------------------------------------	-----------------------------

Files and folders (1 Total, 2.0 B)

Name	Folder	Type	Size	Status	Error
accounts.txt	-	text/plain	2.0 B	Succeeded	-

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

SKCET

karthi071-bucket - S3 bucket

IAM Management Console

(4) WhatsApp

s3.console.aws.amazon.com/s3/buckets/karthi071-bucket/object/edit_public_read_access?region=eu-north-1&showversions=false

aws

Services

Search

[Alt+S]

Global

KARTHIKEYAN_R

EC2

VPC

S3

IAM

Amazon S3 > Buckets > karthi071-bucket > Make public

Make public [info](#)

The make public action enables public read access in the object access control list (ACL) settings. [Learn more](#).

⚠ When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.

Specified objects

Find objects by name

< 1 >

Name	Type	Last modified	Size
accounts.txt	txt	May 3, 2023, 16:09:11 (UTC+05:30)	2.0 B

Cancel

Make public

CloudShell

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates.

Privacy

Terms

Cookie preferences

31°C

Partly sunny

Search

ENG IN

04:10 PM

03-05-2023

SKCET

karthi071-bucket - S3 bucket

IAM Management Console

(4) WhatsApp

s3.console.aws.amazon.com/s3/buckets/karthi071-bucket/object/edit_public_read_access?region=eu-north-1&showversions=false

aws

Services

Search

[Alt+S]

Global

KARTHIKEYAN_R

EC2

VPC

S3

IAM

☑ Successfully edited public access

View details below.

Close

Make public: status

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

Summary

Source

s3://karthi071-bucket

Successfully edited public access

🟢 1 object, 2.0 B

Failed to edit public access

0 objects

Failed to edit public access

Configuration

⊗ Failed to edit public access (0)

Find objects by name

< 1 >

Name	Folder	Type	Last modified	Size	Error
------	--------	------	---------------	------	-------

No objects failed to edit.

CloudShell

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates.

Privacy

Terms

Cookie preferences

31°C

Partly sunny

Search

ENG IN

04:10 PM

03-05-2023