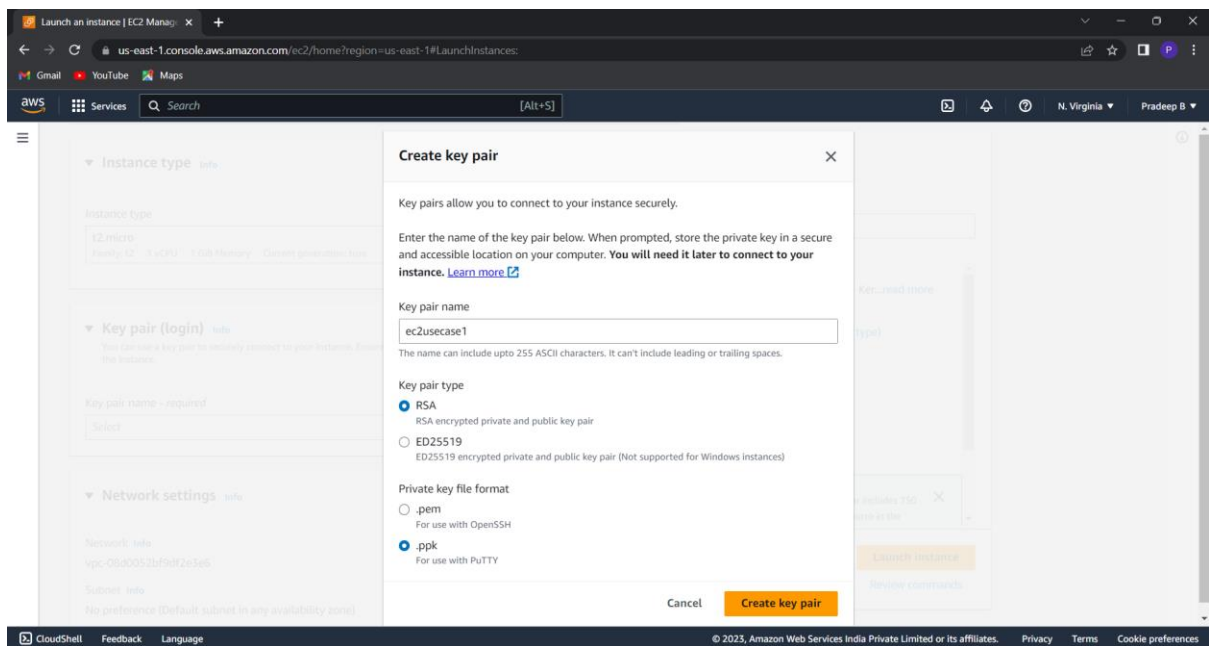
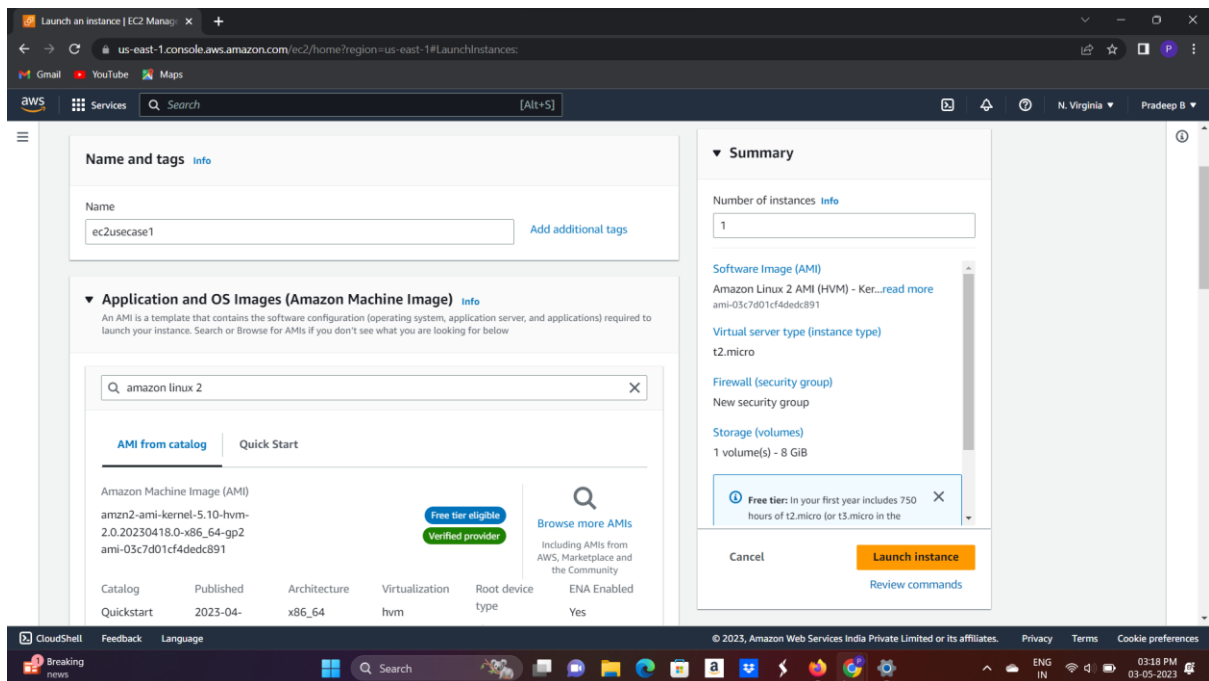
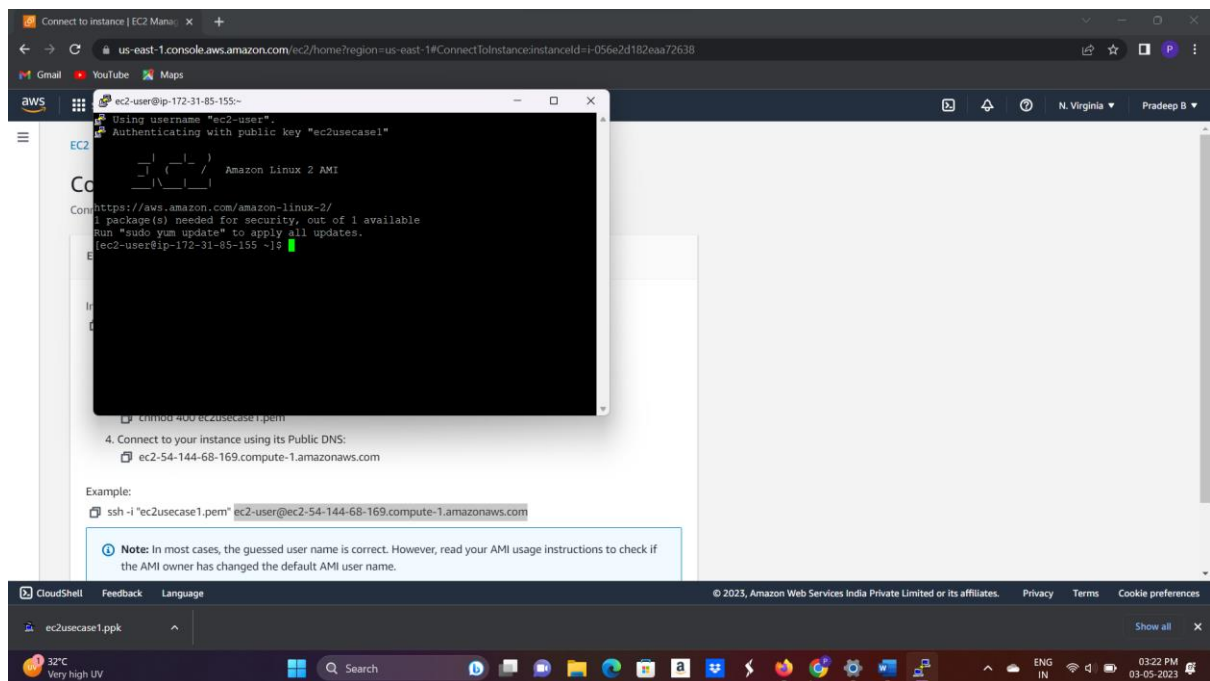
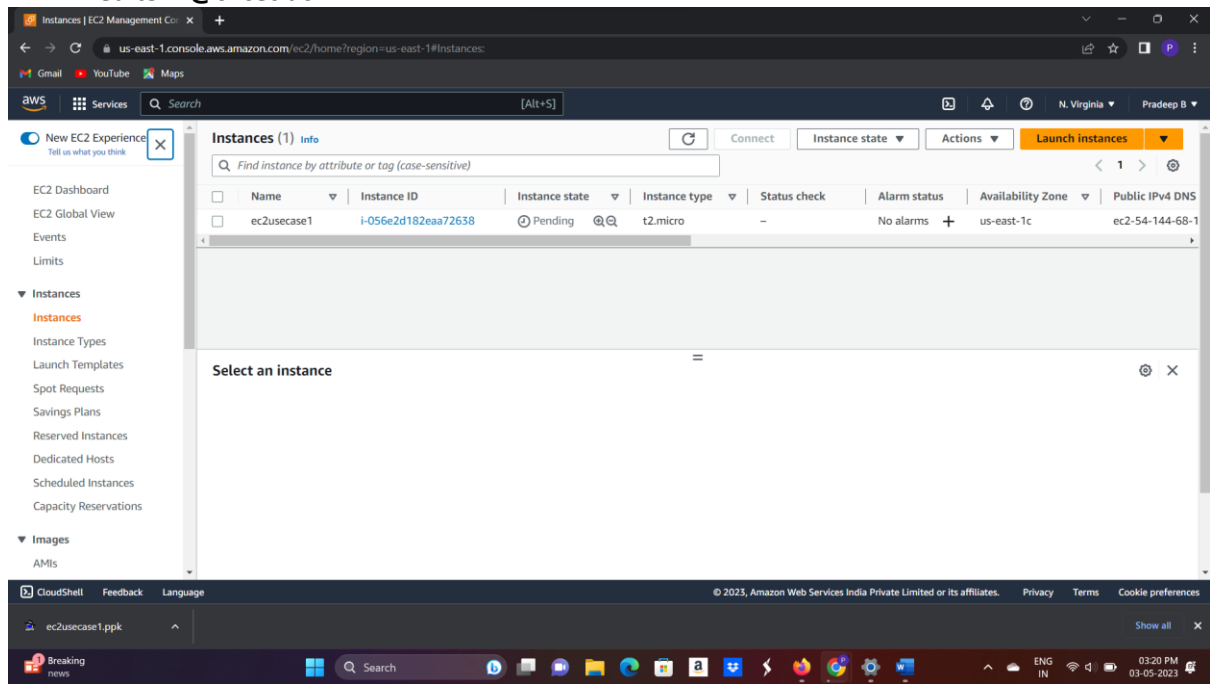


Pradeep B
727722EUIT514
727722euit514@skcet.ac.in
Q1.



Pradeep B
727722EUIT514
727722euit514@skcet.ac.in



Pradeep B
727722EUIT514
727722euit514@skcet.ac.in

The screenshot displays the AWS Management Console interface for a security group. The top navigation bar shows the user is logged in as 'Pradeep B' in the 'us-east-1' region. The left sidebar contains navigation links for various AWS services, including EC2 Dashboard, Instances, Images, and Elastic Block Store.

The main content area shows the details of a security group named 'launch-wizard-1'. The details are organized into a grid:

- Security group name:** launch-wizard-1
- Security group ID:** sg-0f0bfda0f0373fdd7
- Description:** launch-wizard-1 created 2023-05-03T09:48:32.572Z
- VPC ID:** vpc-08d0052bf9df2e3e6
- Owner:** 244123390764
- Inbound rules count:** 2 Permission entries
- Outbound rules count:** 1 Permission entry

Below the details grid, there are tabs for 'Inbound rules', 'Outbound rules', and 'Tags'. The 'Inbound rules' tab is selected, showing a list of inbound rules. A notification banner at the top of the rules section states: 'You can now check network connectivity with Reachability Analyzer' with a 'Run Reachability Analyzer' button.

The 'Inbound rules (2)' section contains a table with the following data:

Name	Security group rule...	IP version	Type	Protocol	Port range
-	sgr-00c2e2e1fec18c3d9	IPv4	SSH	TCP	22
-	sgr-05af1076f340f3dd9	IPv4	HTTP	TCP	80

The bottom of the screenshot shows the Windows taskbar with the date and time as 03:32 PM on 03-05-2023.

Pradeep B
727722EUIT514
727722euit514@skcet.ac.in
Q2.

The screenshot shows the 'Create user' page in the AWS IAM Management Console. The user name is 'Network-L1-User1'. The 'Provide user access to the AWS Management Console - optional' checkbox is checked. A message box asks 'Are you providing console access to a person?' with two options: 'Specify a user in Identity Center - Recommended' and 'I want to create an IAM user' (selected). The 'Console password' section has 'Custom password' selected, with a password field containing '*****'. The password requirements are listed: must be at least 8 characters long, and must include at least three of uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * { } _ + - (hyphen) =.

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

User details

User name
Network-L1-User1
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , @ _ - (hyphen)

☒ Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice [to manage their access in IAM Identity Center](#).

Are you providing console access to a person?

☐ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☐ Autogenerated password
You can view the password after you create the user.

☒ Custom password
Enter a custom password for the user.

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * { } _ + - (hyphen) =

CloudShell Feedback Language

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

32°C Partly sunny

Search

ENG IN

03:39 PM 03-05-2023

The screenshot shows the 'Users' page in the AWS IAM Management Console. A green banner at the top says 'User created successfully' with a 'View user' button. The 'Users (2)' section shows a table with two users: 'Network-L1-User1' and 'S3Admin1'. The 'Network-L1-User1' user has no groups, no MFA, and no password age. The 'S3Admin1' user is in the 'S3-Admins' group, has no MFA, and a password age of 7 days ago.

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
- Analyzers
- Settings

User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console. [View user](#)

IAM > Users

Users (2) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	Network-L1-User1	None	⌚	None	None	⌚
<input type="checkbox"/>	S3Admin1	S3-Admins	⌚	None	7 days ago	⌚

CloudShell Feedback Language

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

Network-L1-User1...csv

32°C Partly sunny

Search

ENG IN

03:40 PM 03-05-2023

Pradeep B
727722EUIT514
727722euit514@skcet.ac.in

The screenshot shows the AWS IAM Management Console in the 'us-east-1' region, specifically the 'Create user group' page. The left sidebar contains navigation links for Identity and Access Management (IAM), including Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity), and CloudShell. The main content area is titled 'Create user group' and has a sub-header 'Name the group'. Below this, there is a text input field for 'User group name' with the value 'Network-L1-Team'. A note states: 'Maximum 128 characters. Use alphanumeric and '+', '@', '_' characters.' Below the name field, there is a section 'Add users to the group - Optional (Selected 1/2)' with an 'Info' icon. It explains that an IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS, and a user can belong to up to 10 groups. Below this explanation is a search bar and a table of users. The table has columns for 'User name', 'Groups', 'Last activity', and 'Creation time'. Two users are listed: 'Network-L1-User1' (selected with a checkbox) and 'S3Admin1'. The 'Network-L1-User1' row shows 0 groups, no last activity, and was created 2 minutes ago. The 'S3Admin1' row shows 1 group, last activity 7 days ago, and was created 7 days ago. The bottom of the screenshot shows a Windows taskbar with a search bar, several application icons, and a system tray showing the date and time as 03:43 PM on 03-05-2023.

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
- Analyzers
- Settings
- Credential report
- Organization activity

Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

Network-L1-Team

Maximum 128 characters. Use alphanumeric and '+', '@', '_' characters.

Add users to the group - Optional (Selected 1/2) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

Search

	User name	Groups	Last activity	Creation time
<input checked="" type="checkbox"/>	Network-L1-User1	0	None	2 minutes ago
<input type="checkbox"/>	S3Admin1	1	7 days ago	7 days ago

CloudShell Feedback Language

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

32°C Partly sunny

Search

ENG IN 03:43 PM 03-05-2023

The screenshot shows the AWS IAM Management Console in the 'us-east-1' region, specifically the 'User groups' page. The left sidebar is identical to the previous screenshot. The main content area has a green banner at the top stating 'Network-L1-Team user group created.' with a 'View group' button. Below the banner, the page title is 'User groups (2)' with an 'Info' icon. It explains that a user group is a collection of IAM users and is used to specify permissions. Below this is a search bar with the placeholder text 'Filter User groups by property or group name and press enter'. Below the search bar is a table of user groups. The table has columns for 'Group name', 'Users', 'Permissions', and 'Creation time'. Two groups are listed: 'Network-L1-Team' and 'S3-Admins'. The 'Network-L1-Team' row shows 1 user, permissions are 'Loading', and it was created 'Now'. The 'S3-Admins' row shows 1 user, permissions are 'Loading', and it was created '7 days ago'. The bottom of the screenshot shows a Windows taskbar with a search bar, several application icons, and a system tray showing the date and time as 03:46 PM on 03-05-2023.

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
- Analyzers
- Settings
- Credential report
- Organization activity

CloudShell Feedback Language

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

32°C Partly sunny

Search

ENG IN 03:46 PM 03-05-2023

Pradeep B
727722EUIT514
727722euit514@skcet.ac.in

The screenshot shows the AWS IAM Management Console for the user group 'Network-L1-Team'. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Access Advisor. The main content area displays the 'Network-L1-Team' user group details, including its creation time (May 03, 2023, 15:46 UTC+05:30) and ARN (arn:aws:iam::244123390764:group/Network-L1-Team). The 'Permissions' tab is active, showing a table of attached policies. One policy, 'AmazonVPCReadOnlyAccess', is listed with the description 'Provides read only access to Amazon ...'. The bottom of the screen shows a Windows taskbar with the date and time as 03:52 PM on 03-05-2023.

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

Analizers

Settings

Credential report

Organization activity

Network-L1-Team

Summary

User group name: Network-L1-Team

Creation time: May 03, 2023, 15:46 (UTC+05:30)

ARN: arn:aws:iam::244123390764:group/Network-L1-Team

Permissions policies (1)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

Policy name	Type	Description
AmazonVPCReadOnlyAccess	AWS managed	Provides read only access to Amazon ...

03:52 PM 03-05-2023

This screenshot is similar to the one above but shows two permission policies attached to the 'Network-L1-Team' user group. The 'Permissions policies (2)' section now includes 'AmazonVPCReadOnlyAccess' and 'AWSNetworkManagerReadOnlyAccess', both with the description 'Provides read only access to Amazon ...'. The Windows taskbar at the bottom shows the date and time as 03:54 PM on 03-05-2023.

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

Analizers

Settings

Credential report

Organization activity

Network-L1-Team

Summary

User group name: Network-L1-Team

Creation time: May 03, 2023, 15:46 (UTC+05:30)

ARN: arn:aws:iam::244123390764:group/Network-L1-Team

Permissions policies (2)

You can attach up to 10 managed policies.

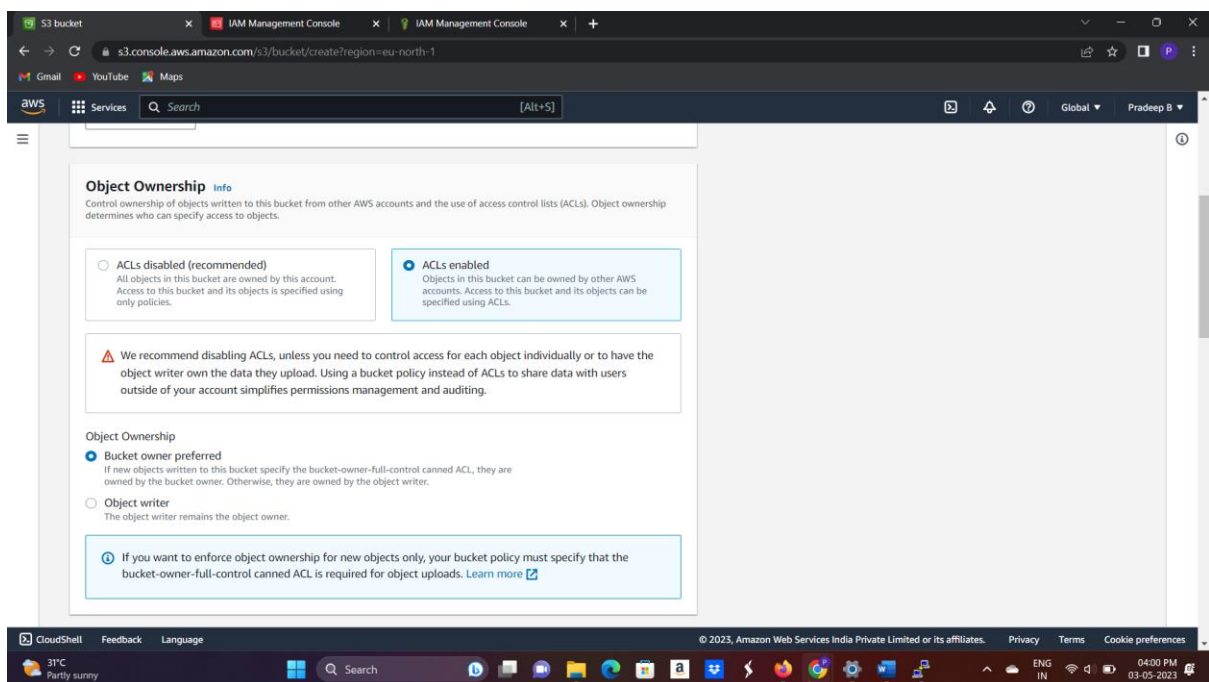
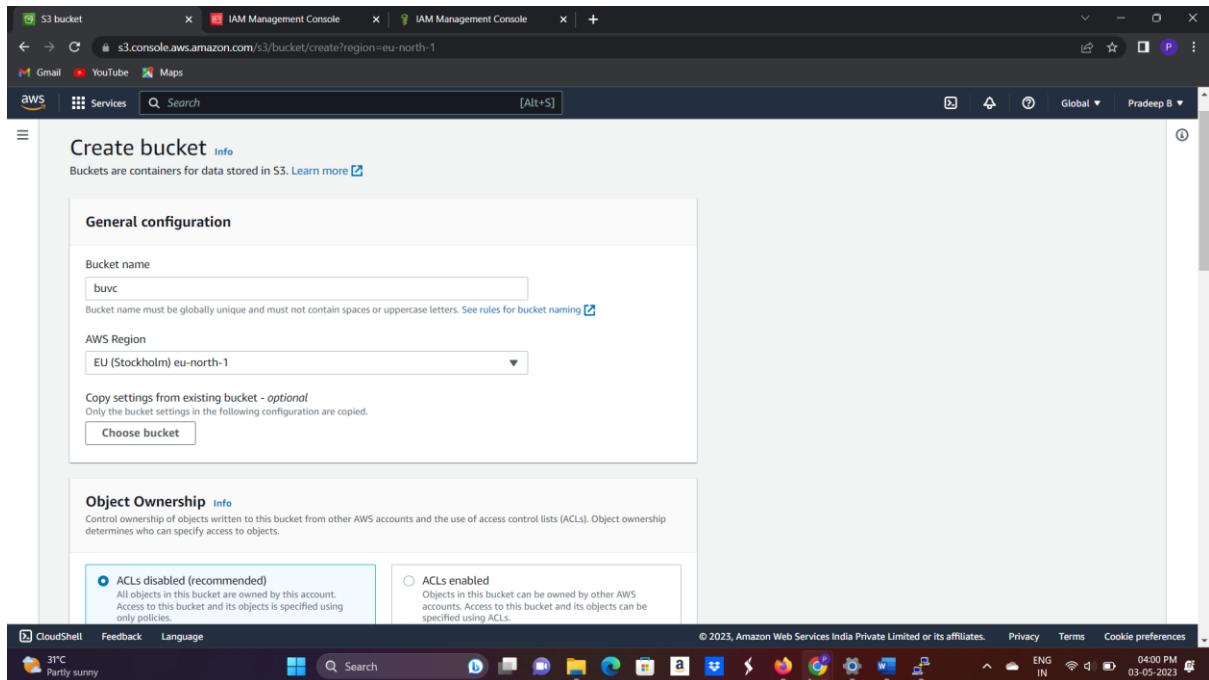
Filter policies by property or policy name and press enter.

Policy name	Type	Description
AmazonVPCReadOnlyAccess	AWS managed	Provides read only access to Amazon ...
AWSNetworkManagerReadOnlyAccess	AWS managed	Provides read only access to Amazon ...

03:54 PM 03-05-2023

Pradeep B
727722EUIT514
727722euit514@skcet.ac.in

Q3.



Pradeep B
727722EUIT514
727722euit514@skcet.ac.in

The screenshot shows the 'Block Public Access' settings for an S3 bucket in the AWS Management Console. The page title is 'Block Public Access Settings for this bucket'. It explains that public access is granted through ACLs, bucket policies, access point policies, or all. It lists five settings, all of which are currently unchecked:

- ☐ **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.

A warning message states: '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.' Below this, a checkbox 'I acknowledge that the current settings might result in this bucket and the objects within becoming public.' is checked.

The screenshot shows the 'Upload succeeded' confirmation page in the AWS S3 console. A green banner at the top says 'Upload succeeded' and 'View details below.' Below this, a blue box contains the text: 'The information below will no longer be available after you navigate away from this page.'

The 'Summary' section shows the upload details:

Destination	Succeeded	Failed
s3://buvc	1 file, 27.0 B (100.00%)	0 files, 0 B (0%)

The 'Files and folders' section shows a table with one file uploaded:

Name	Folder	Type	Size	Status	Error
accounts.txt	-	text/plain	27.0 B	Succeeded	-

Pradeep B
727722EUIT514
727722euit514@skcet.ac.in

The screenshot shows the AWS IAM Management Console interface. The browser address bar displays the URL: `s3.console.aws.amazon.com/s3/bucket/buvvc/property/acl/edit?region=eu-north-1`. The page title is "Edit access control list (ACL)". Below the title, there is a section titled "Access control list (ACL)" with a subtitle "Grant basic read/write permissions to other AWS accounts. [Learn more](#)".

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: <code>ad82e2c365969e760d74405944f63ee36189b0405a99efdc778fa5e6051519</code>	<input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) Group: <code>http://acs.amazonaws.com/groups/global/AllUsers</code>	<input checked="" type="checkbox"/> List <input type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account) Group: <code>http://acs.amazonaws.com/groups/global/AuthenticatedUsers</code>	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write
S3 log delivery group Group: <code>http://acs.amazonaws.com/groups/global/S3LogDeliveryGroup</code>	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write

The screenshot shows the AWS IAM Management Console interface for the "accounts.txt" object. The browser address bar displays the URL: `https://buvvc.s3.eu-north-1.amazonaws.com/s3/object/buvvc?region=eu-north-1&prefix=accounts.txt&tab=permissions`. The page title is "accounts.txt".

Properties | **Permissions** | Versions

Access control list (ACL) [Edit](#)

Grant basic read/write permissions to AWS accounts. [Learn more](#)

Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: <code>ad82e2c365969e760d74405944f63ee36189b0405a99efdc778fa5e6051519</code>	Read	Read, Write
Everyone (public access) Group: <code>http://acs.amazonaws.com/groups/global/AllUsers</code>	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Read
Authenticated users group (anyone with an AWS account) Group: <code>http://acs.amazonaws.com/groups/global/AuthenticatedUsers</code>	-	-

727722euit514@skcet.ac.in

