

School of Computer Science, Engineering and Applications (SCSEA)

B.C.A. TY (CCSA)

Subject: Advanced Cloud Computing (P)

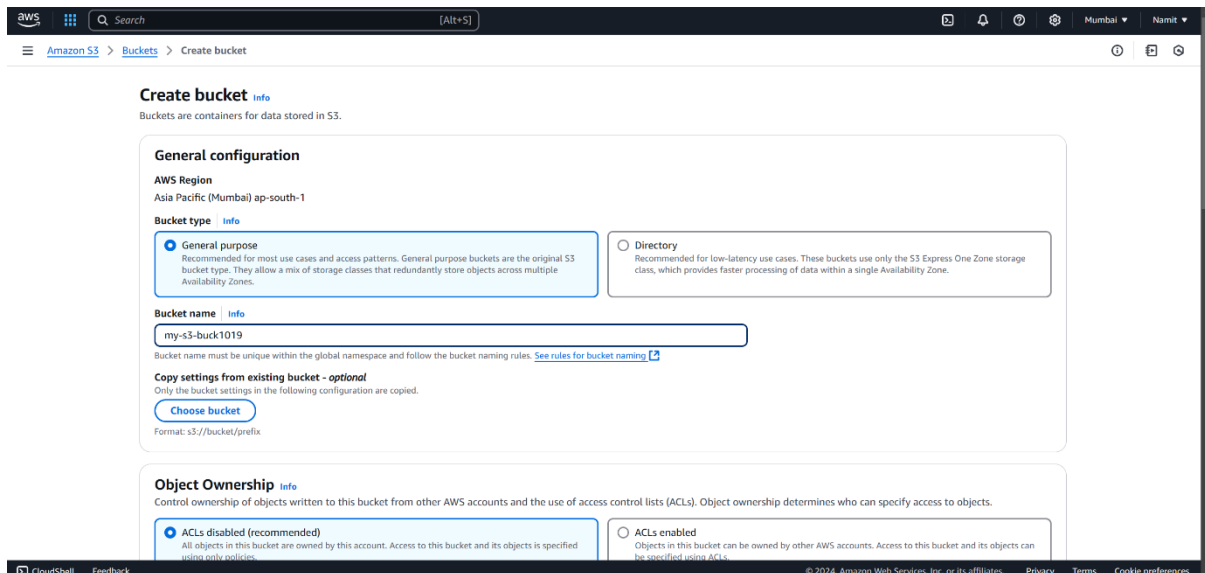
Name of the Student: Namit Agarwal

PRN: 20220801019

Title of Practical: IAM role Custom Policy to access S3

Step 1: Create an S3 Bucket

1. Go to the **S3** service in the AWS Console.
2. Click on **Create bucket**.
3. Enter a unique name for the bucket.



4. Click on **Create bucket** to finalize.
5. Once created, navigate to the bucket and copy the ARN of the S3 bucket. You'll need it in a later step.

School of Computer Science, Engineering and Applications (SCSEA)

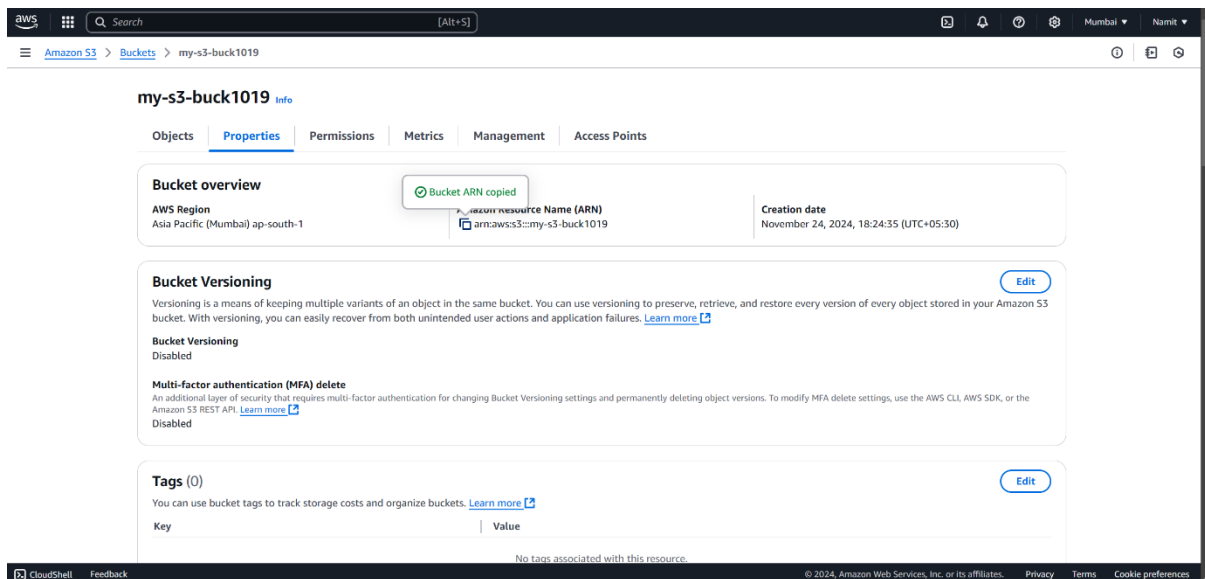
B.C.A. TY (CCSA)

Subject: Advanced Cloud Computing (P)

Name of the Student: Namit Agarwal

PRN: 20220801019

Title of Practical: IAM role Custom Policy to access S3



Step 2: Go to IAM Policies

1. Navigate to the **IAM** service in the AWS Console.
2. Click on **Policies** in the left-hand menu.

Step 3: Create a New Policy

1. Click on **Create policy**.
2. In the policy creation interface, select **Service** as **S3**, since we are creating a policy for S3.
3. Under the **List** section, check **List buckets**.
4. Under the **Read** section, check the boxes for the necessary read permissions (e.g., **GetObject**).
5. Under the **Resource** section, click on **Add ARN** and specify the ARN of the bucket:
 - Copy the ARN from the S3 bucket list if you haven't done so already.

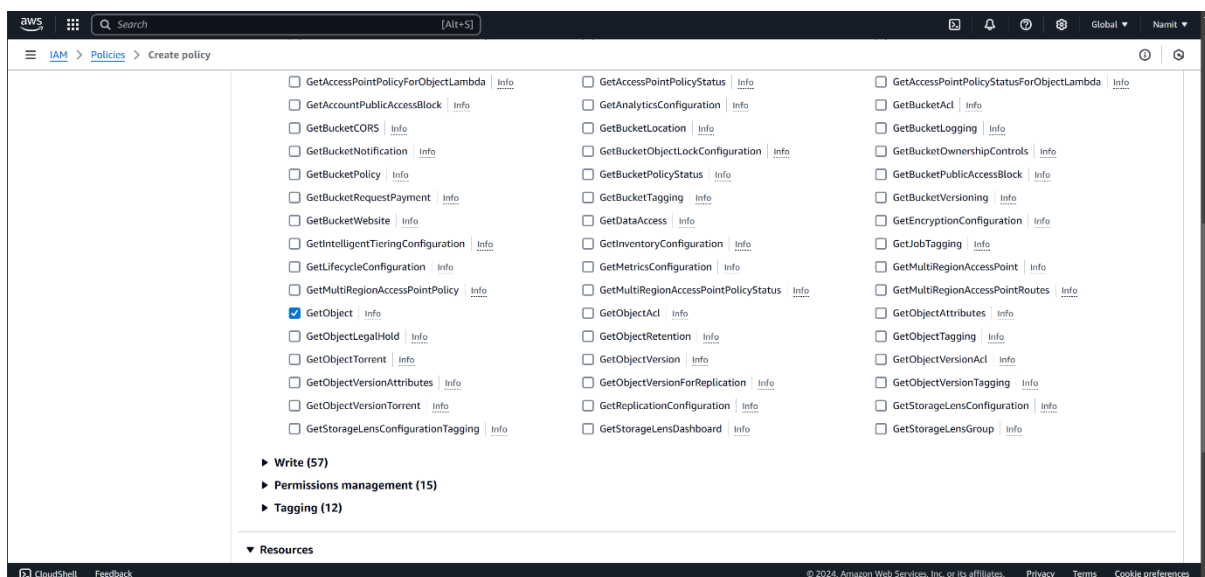
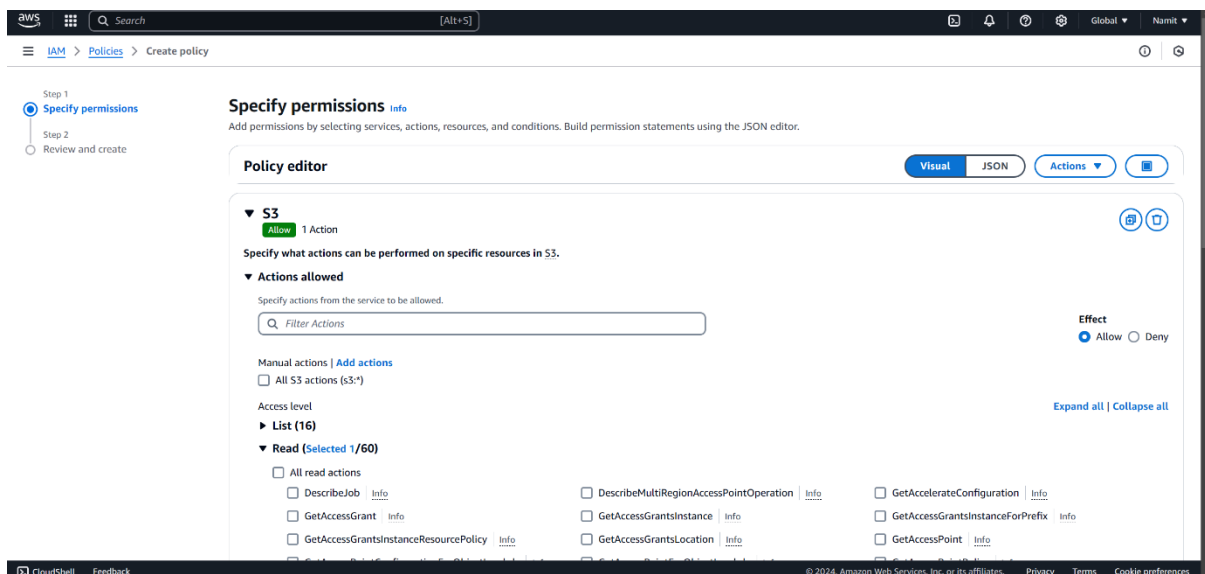
School of Computer Science, Engineering and Applications (SCSEA)
B.C.A. TY (CCSA)
Subject: Advanced Cloud Computing (P)

Name of the Student: Namit Agarwal

PRN: 20220801019

Title of Practical: IAM role Custom Policy to access S3

- Paste it in the Add ARN section under Resources.

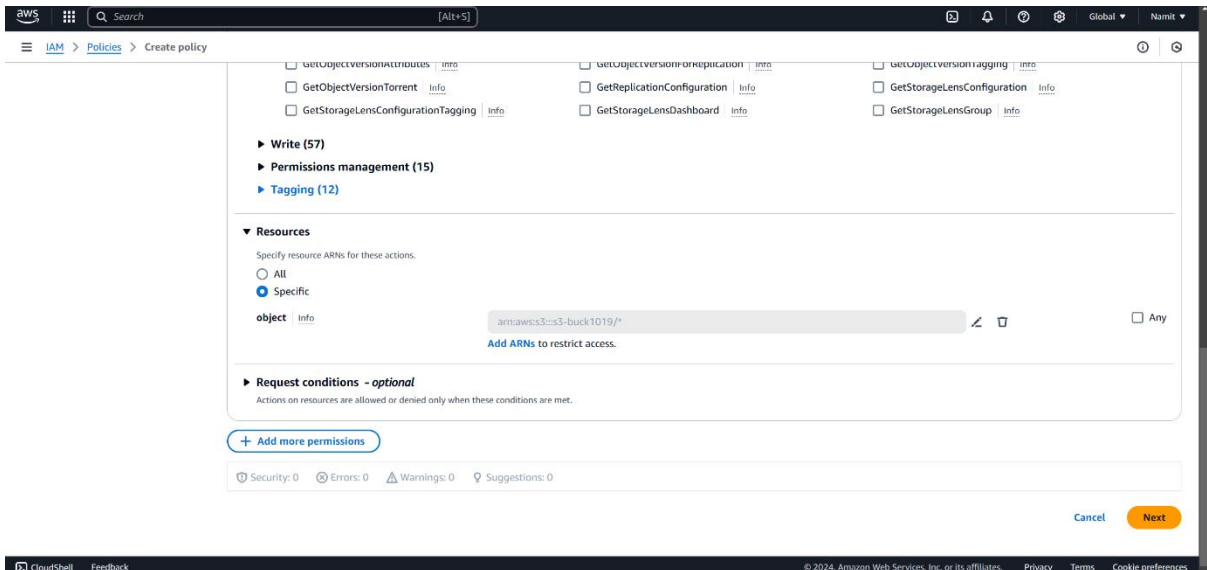


School of Computer Science, Engineering and Applications (SCSEA)
B.C.A. TY (CCSA)
Subject: Advanced Cloud Computing (P)

Name of the Student: Namit Agarwal

PRN: 20220801019

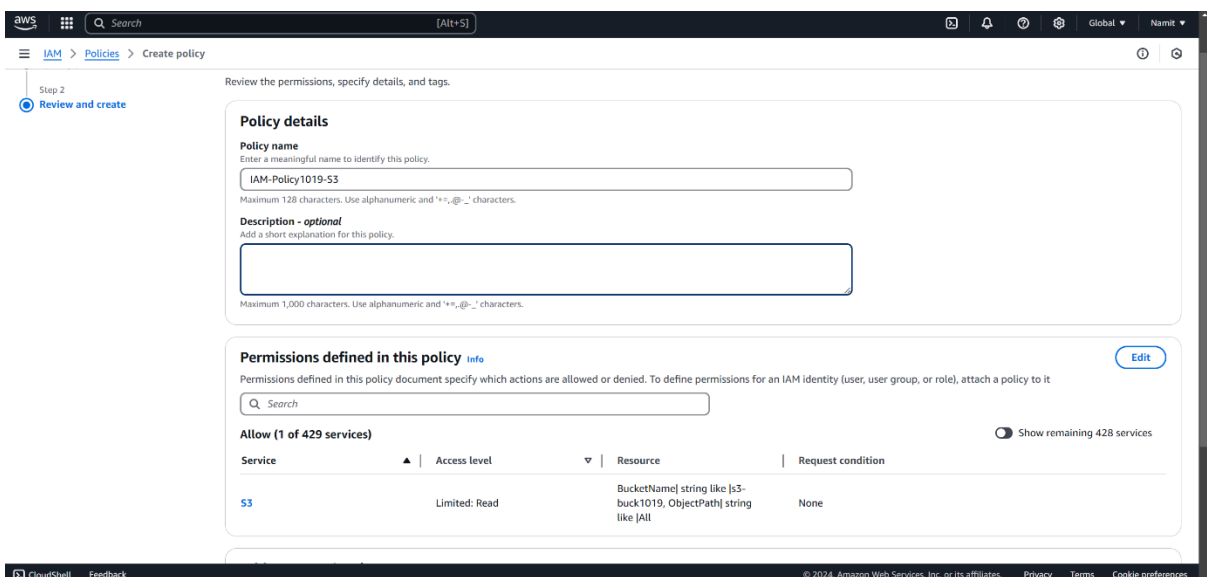
Title of Practical: IAM role Custom Policy to access S3



The screenshot shows the AWS IAM console 'Create policy' page. The 'Permissions' section is expanded, showing a list of actions under 'Write (57)', 'Permissions management (15)', and 'Tagging (12)'. The 'Resources' section is set to 'Specific' with the ARN 'arn:aws:s3::s3-bucket1019/*'. The 'Request conditions' section is optional. The 'Next' button is visible at the bottom right.

Step 4: Review and Create the Policy

1. Click **Next** to proceed.
2. Give a name to the policy.



The screenshot shows the AWS IAM console 'Review and create' page. The 'Policy details' section shows the policy name 'IAM-Policy1019-S3' and a description. The 'Permissions defined in this policy' section shows a table with one permission: 'S3' with 'Limited: Read' access level, 'BucketName| string like [s3-bucket1019, ObjectPath| string like [All]' resource, and 'None' request condition. The 'Next' button is visible at the bottom right.

Service	Access level	Resource	Request condition
S3	Limited: Read	BucketName string like [s3-bucket1019, ObjectPath string like [All]	None

School of Computer Science, Engineering and Applications (SCSEA)

B.C.A. TY (CCSA)

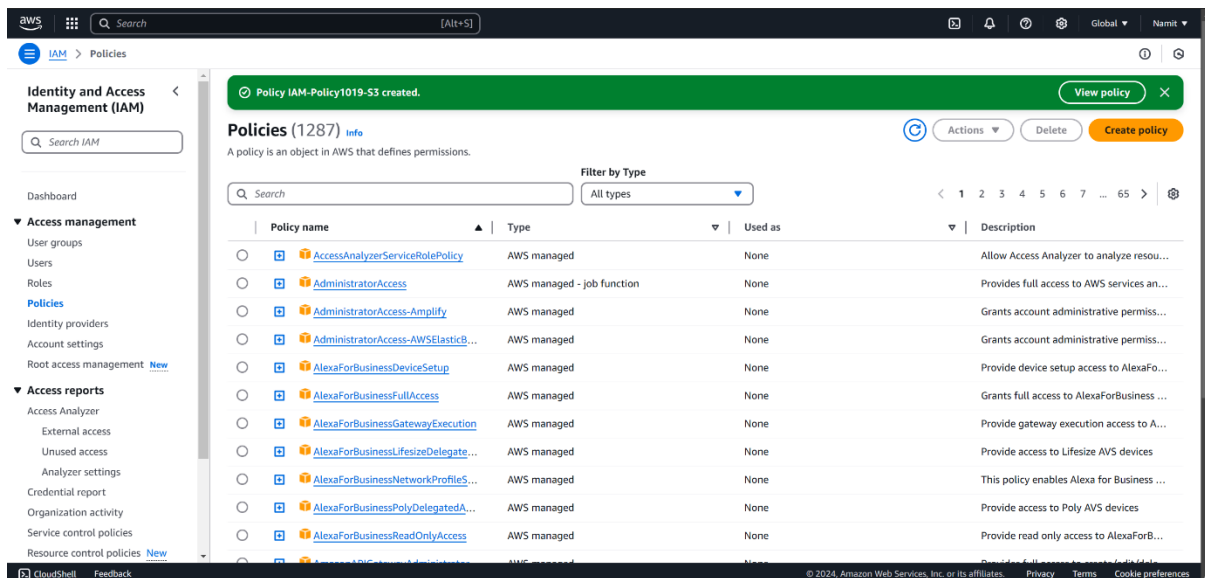
Subject: Advanced Cloud Computing (P)

Name of the Student: Namit Agarwal

PRN: 20220801019

Title of Practical: IAM role Custom Policy to access S3

3. Review the policy settings.
4. Click on **Create policy** to finalize the policy creation.



Step 5: Create an IAM User and Attach the Policy

1. Go to the **Users** section in the IAM service.
2. Click on **Create user**.
3. Enter a name for the IAM user.

School of Computer Science, Engineering and Applications (SCSEA)

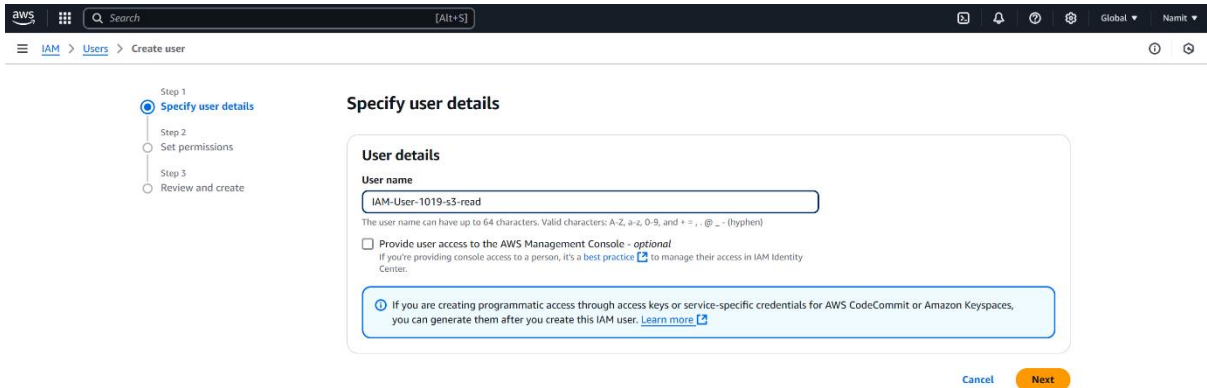
B.C.A. TY (CCSA)

Subject: Advanced Cloud Computing (P)

Name of the Student: Namit Agarwal

PRN: 20220801019

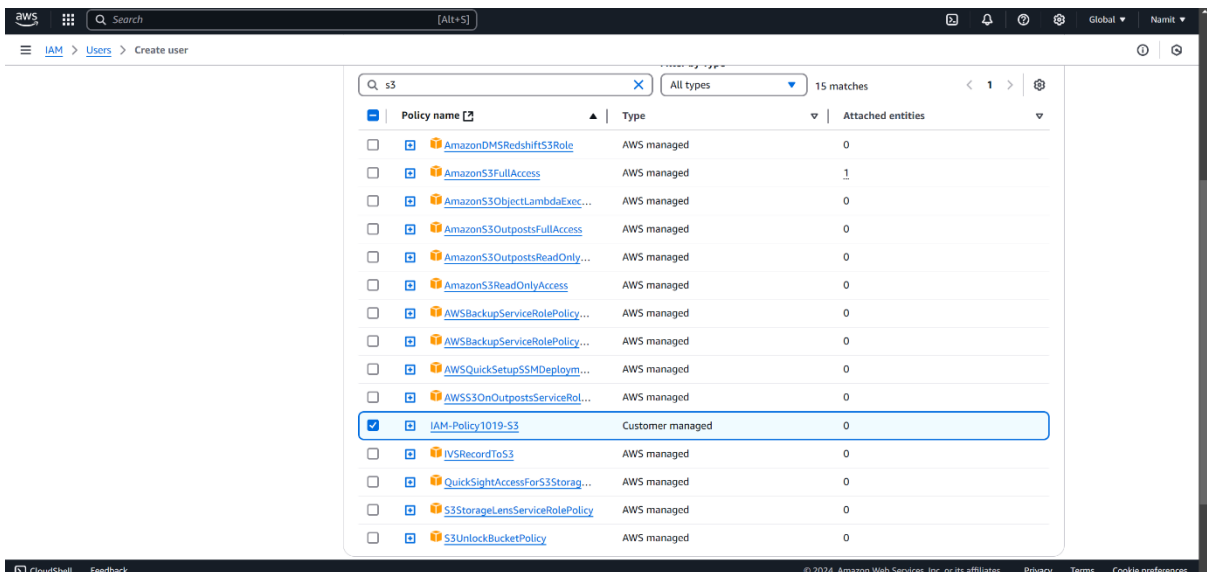
Title of Practical: IAM role Custom Policy to access S3



The screenshot shows the AWS IAM console 'Create user' wizard, Step 1: Specify user details. The 'User name' field is populated with 'IAM-User-1019-s3-read'. Below the field, a note states: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , @ _ - (hyphen)'. There is an unchecked checkbox for 'Provide user access to the AWS Management Console - optional' with a sub-note: 'If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.' A blue information box at the bottom states: 'If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more'. 'Cancel' and 'Next' buttons are at the bottom right.

4. Click **Next**.

5. In the **Permissions options** section, select **Attach policies directly**.



The screenshot shows the AWS IAM console 'Create user' wizard, Step 2: Set permissions. The 'Attach policies directly' tab is selected. A search bar at the top contains 's3' and shows '15 matches'. Below is a table of policies:

Policy name	Type	Attached entities
<input type="checkbox"/> AmazonDMSRedshiftS3Role	AWS managed	0
<input type="checkbox"/> AmazonS3FullAccess	AWS managed	1
<input type="checkbox"/> AmazonS3ObjectLambdaExec...	AWS managed	0
<input type="checkbox"/> AmazonS3OutpostsFullAccess	AWS managed	0
<input type="checkbox"/> AmazonS3OutpostsReadOnly...	AWS managed	0
<input type="checkbox"/> AmazonS3ReadOnlyAccess	AWS managed	0
<input type="checkbox"/> AWSBackupServiceRolePolicy...	AWS managed	0
<input type="checkbox"/> AWSBackupServiceRolePolicy...	AWS managed	0
<input type="checkbox"/> AWSQuickSetupSSMDeploym...	AWS managed	0
<input type="checkbox"/> AWSS3OnOutpostsServiceRol...	AWS managed	0
<input checked="" type="checkbox"/> IAM-Policy1019-S3	Customer managed	0
<input type="checkbox"/> IVSRecordToS3	AWS managed	0
<input type="checkbox"/> QuickSightAccessForS3Storag...	AWS managed	0
<input type="checkbox"/> S3StorageLensServiceRolePolicy	AWS managed	0
<input type="checkbox"/> S3UnlockBucketPolicy	AWS managed	0

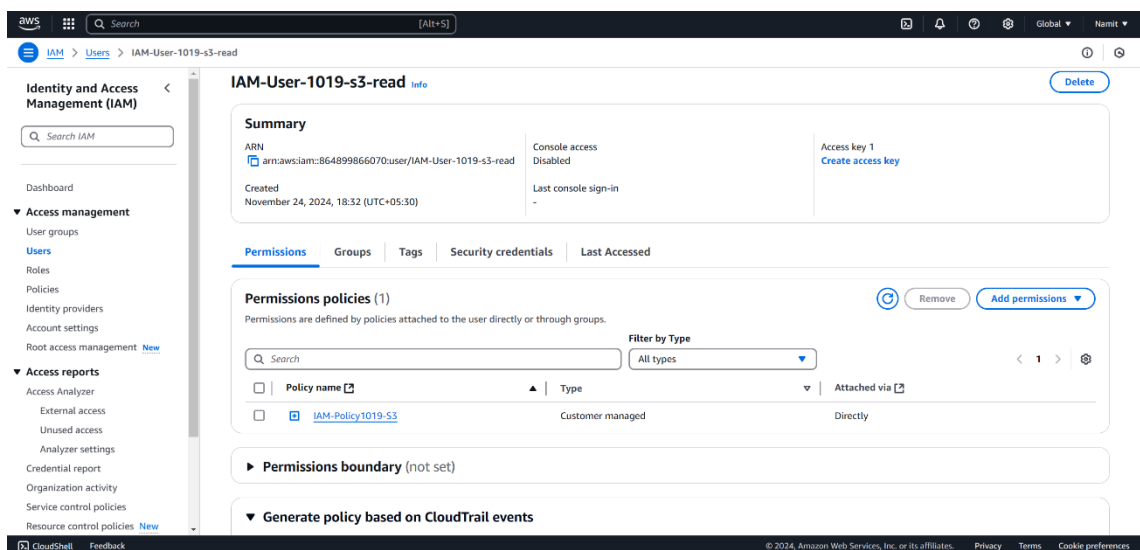
School of Computer Science, Engineering and Applications (SCSEA)
B.C.A. TY (CCSA)
Subject: Advanced Cloud Computing (P)

Name of the Student: Namit Agarwal

PRN: 20220801019

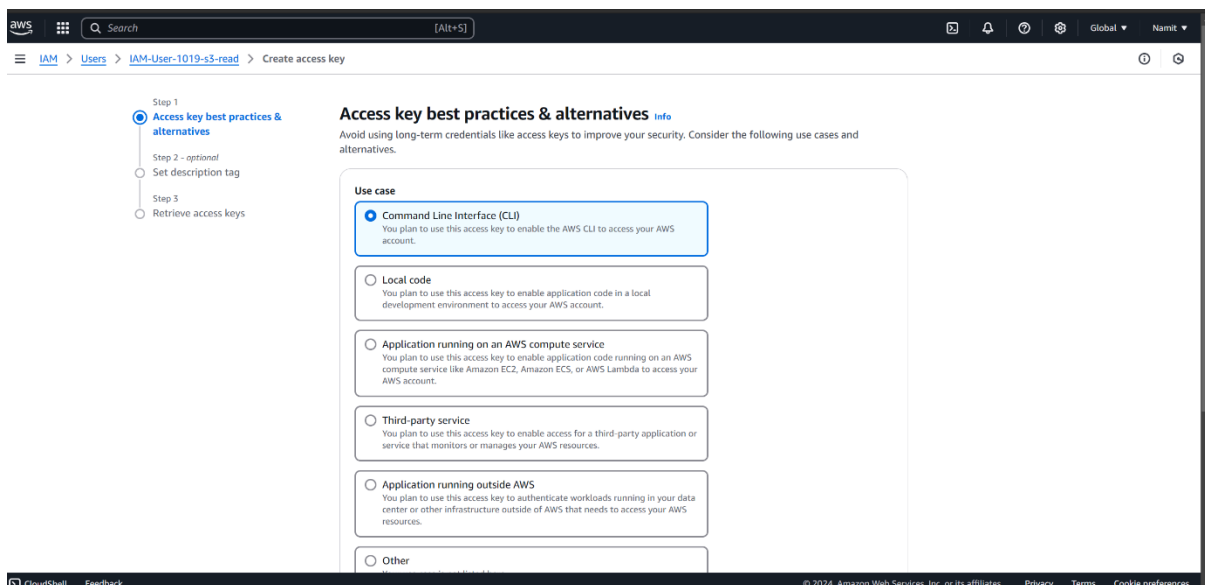
Title of Practical: IAM role Custom Policy to access S3

6. In the **Permissions policies** section, search for the policy you just created and select it.
7. Click Next and then Create user.



Step 6: Generate IAM User Access Keys

1. Go to the IAM user you just created.
2. Click on **Create access key**.



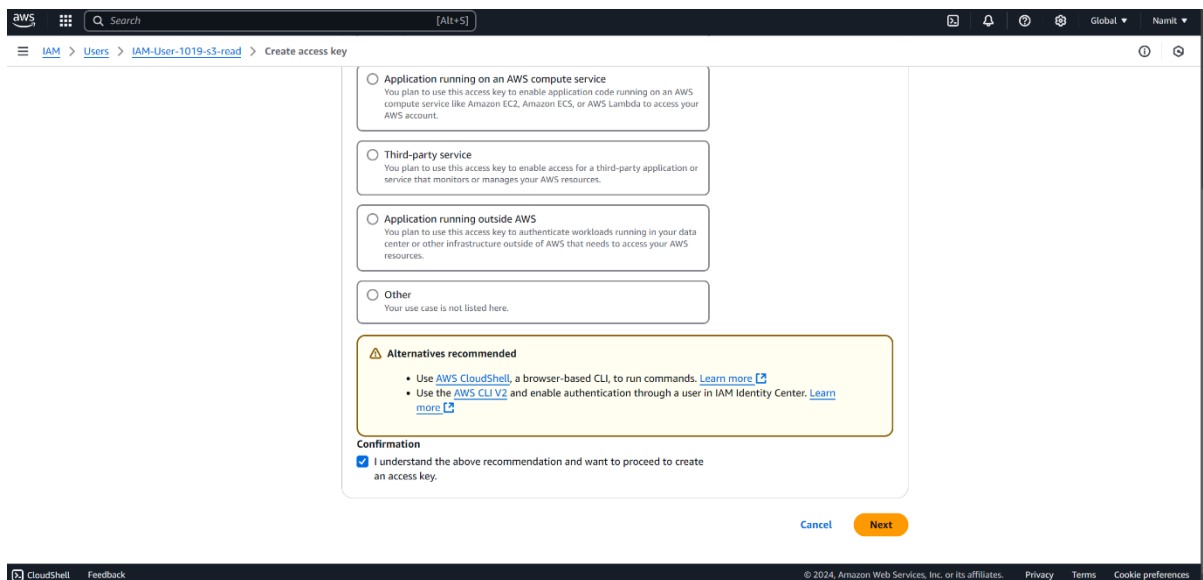
School of Computer Science, Engineering and Applications (SCSEA)
B.C.A. TY (CCSA)
Subject: Advanced Cloud Computing (P)

Name of the Student: Namit Agarwal

PRN: 20220801019

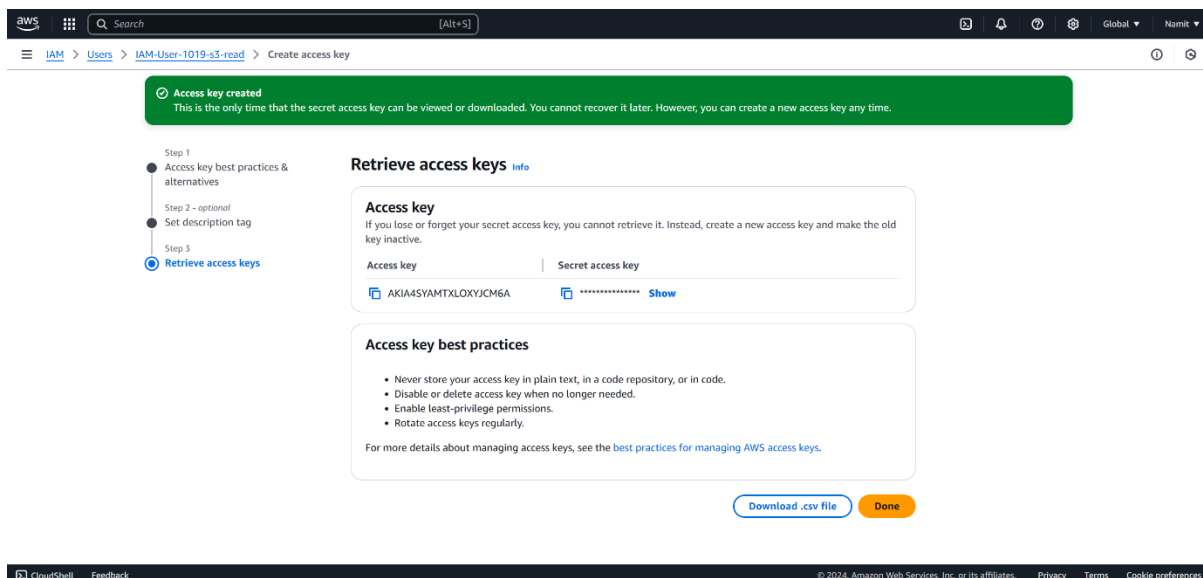
Title of Practical: IAM role Custom Policy to access S3

1. Select **Command Line Interface (CLI)** as the use case.
2. Scroll down, check the confirmation box, and click **Next**.



The screenshot shows the AWS IAM console 'Create access key' page for user 'IAM-User-1019-s3-read'. It features four radio button options: 'Application running on an AWS compute service', 'Third-party service', 'Application running outside AWS', and 'Other'. Below these is a yellow box titled 'Alternatives recommended' with links to AWS CloudShell and AWS CLI V2. A 'Confirmation' section has a checked checkbox stating 'I understand the above recommendation and want to proceed to create an access key.' At the bottom right are 'Cancel' and 'Next' buttons.

1. Click **Create access key**.
2. Copy the **Access Key** and **Secret Access Key** and save them in a secure location.



The screenshot shows the AWS IAM console 'Retrieve access keys' page. A green banner at the top states 'Access key created' and 'This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.' A progress bar on the left shows 'Step 3 Retrieve access keys' as the current step. The main section, titled 'Retrieve access keys', contains an 'Access key' table with one entry: 'AKIA4SYAMTXLOXYJCM6A' and a 'Secret access key' field with a 'Show' button. Below this is an 'Access key best practices' section with a list of guidelines and a link to 'best practices for managing AWS access keys'. At the bottom right are 'Download .csv file' and 'Done' buttons.

School of Computer Science, Engineering and Applications (SCSEA)

B.C.A. TY (CCSA)

Subject: Advanced Cloud Computing (P)

Name of the Student: Namit Agarwal

PRN: 20220801019

Title of Practical: IAM role Custom Policy to access S3

Step 7: Configure AWS CLI with IAM Credentials

1. Open a terminal on your local machine.
2. Type the following command to configure AWS CLI:

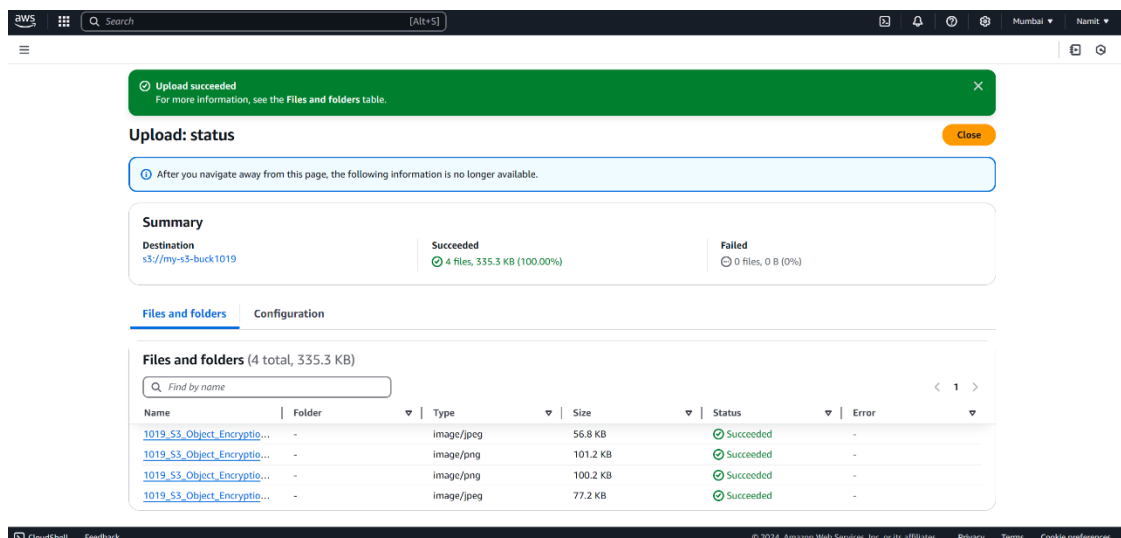
aws configure

3. Enter the **Access Key** and **Secret Access Key** obtained in Step 6, along with your **Default region** and **Default output format**.

```
Windows PowerShell
PS C:\Users\Namit> aws configure
AWS Access Key ID [*****6RFZ]: AKIA4SYAMTXLOXYJCM6A
AWS Secret Access Key [*****yoe5]: aSZhLa823VwsRMxb6UdoPm1FucA/i+CyN0m/Bj1o
Default region name [ap-south-1]:
Default output format [json]:
PS C:\Users\Namit>
```

Step 9: Test Access to the S3 Bucket

1. Go back to the S3 bucket and upload a test file to it.



School of Computer Science, Engineering and Applications (SCSEA)

B.C.A. TY (CCSA)

Subject: Advanced Cloud Computing (P)

Name of the Student: Namit Agarwal

PRN: 20220801019

Title of Practical: IAM role Custom Policy to access S3

In the terminal, run the following command to list the contents of your S3 bucket:

`aws s3 ls s3://<bucket-name>`

```
Windows PowerShell
PS C:\Users\Namit> aws s3 ls
2024-11-24 18:24:36 my-s3-buck1019
PS C:\Users\Namit> aws s3 ls my-s3-buck1019/
2024-11-24 18:37:54      58175 1019_S3_Object_Encryption_KMS.pdf-image-011.jpg
2024-11-24 18:37:54     103630 1019_S3_Object_Encryption_KMS.pdf-image-014.png
2024-11-24 18:37:54     102558 1019_S3_Object_Encryption_KMS.pdf-image-015.png
2024-11-24 18:37:54      79013 1019_S3_Object_Encryption_KMS.pdf-image-018.jpg
PS C:\Users\Namit> _
```