School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (SCSEA)
Subject: Advance Cloud Computing(ACC)
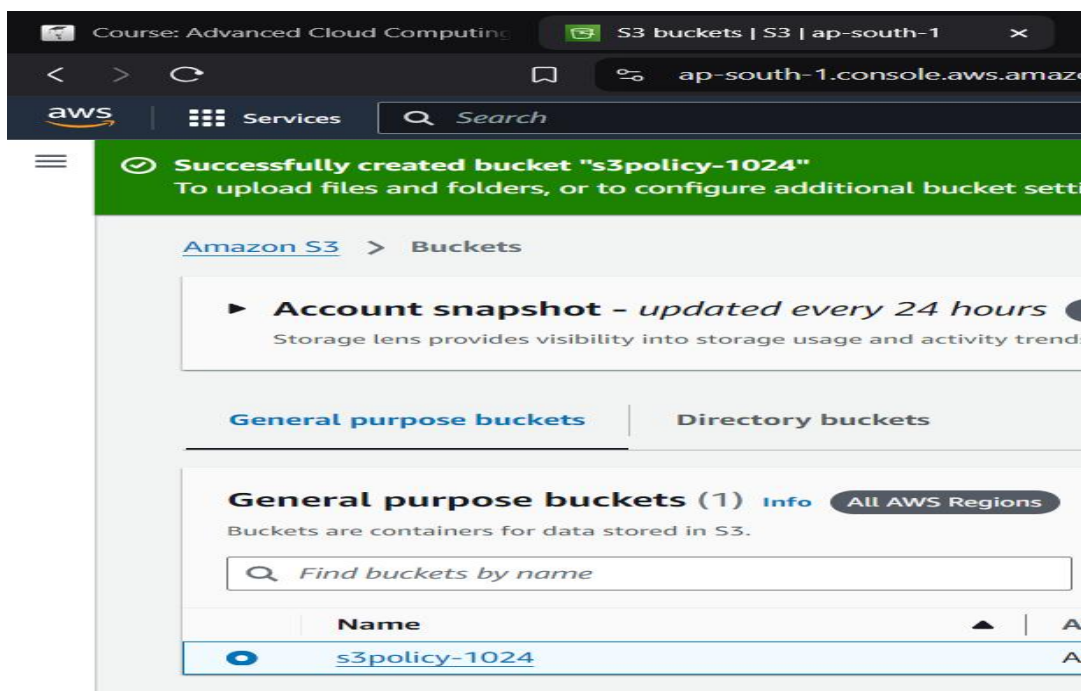
Name of the Student: **Shrushti Krishna Shrivastav**   **PRN:**   **20220801024**

Title of Practicle :   IAM role Custom Policy to access S3

STEP1: Create bucket

Go to S3 service and create one bucket

School of Computer Science, Engineering and Applications(SCSEA)
B.C.A. TY (SCSEA)
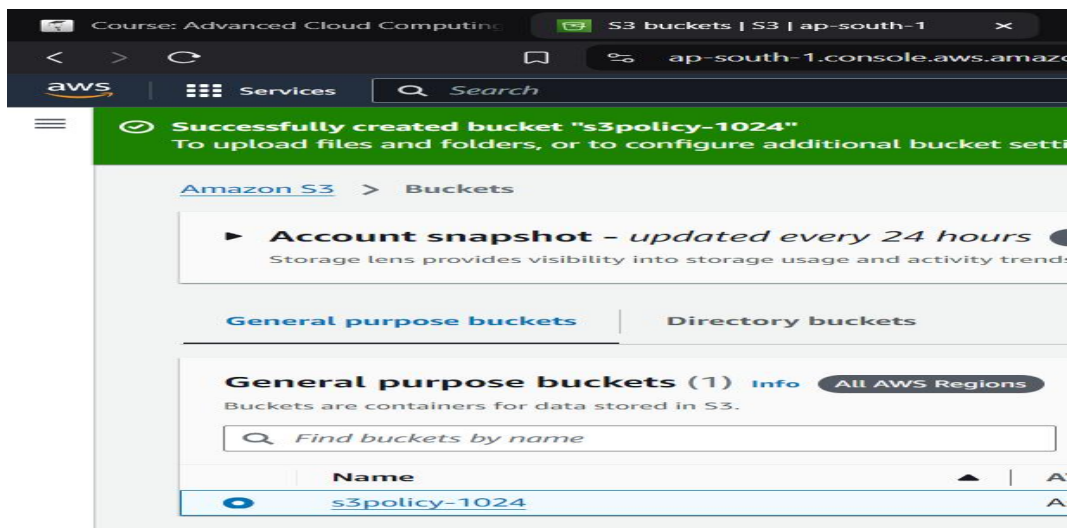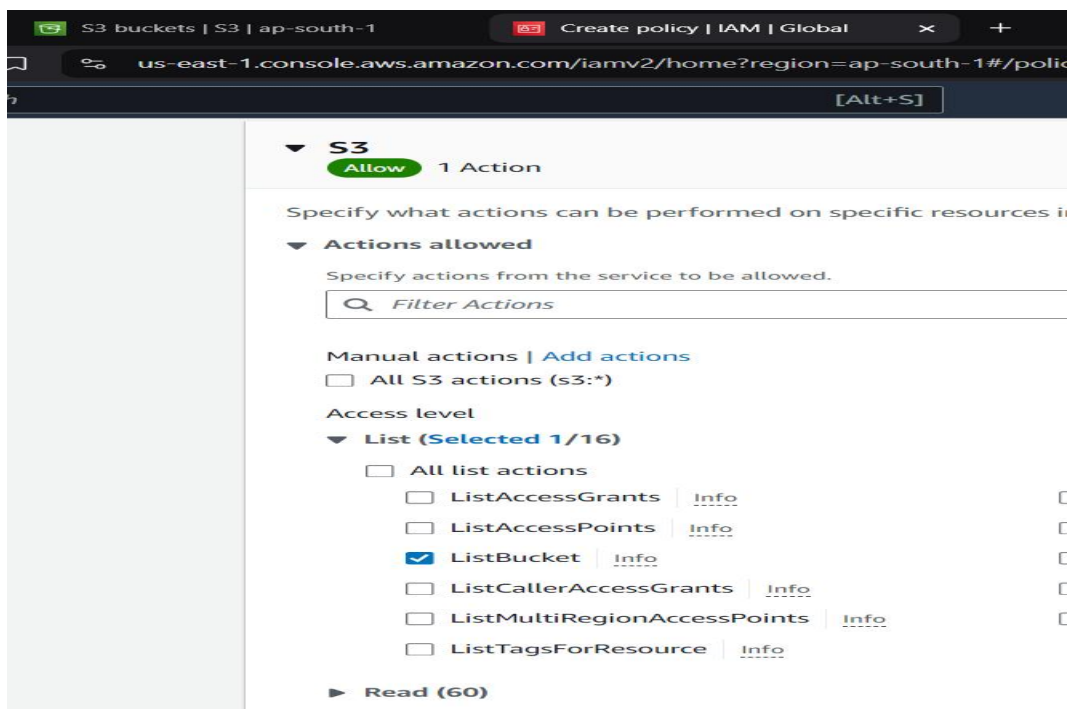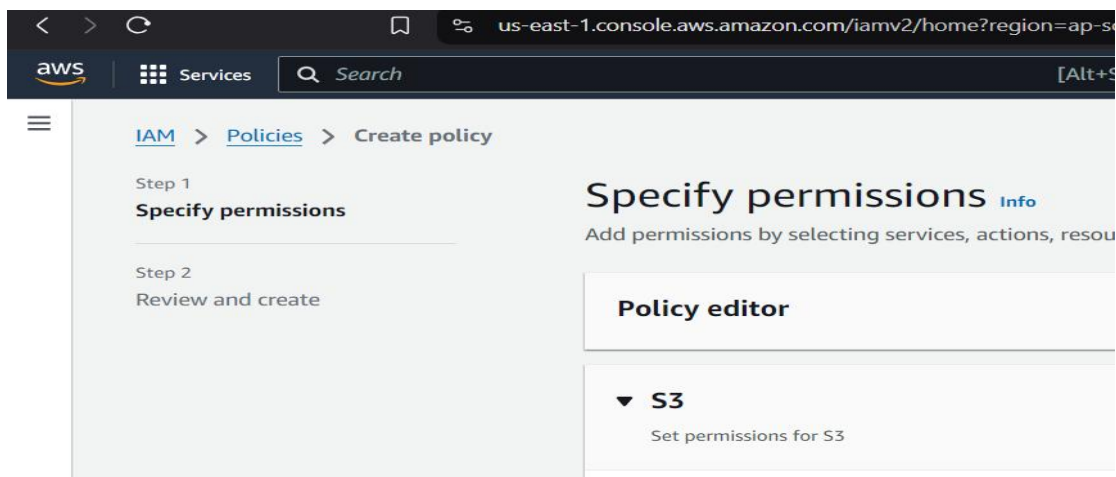## Subject: Advance Cloud Computing(ACC)

Name of the Student: **Shrushti Krishna Shrivastav**   **PRN: 20220801024**

Title of Practicle :   IAM role Custom Policy to access S3

STEP2: Create POLICY

Go to IAM and create on policy

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

Name of the Student: **Shrushti Krishna Shrivastav**   **PRN: 20220801024**

Title of Practicle :   IAM role Custom Policy to access S3

Copy the arn of the bucket

D Y PATIL INTERNATIONAL UNIVERSITY AKURDI PUNE

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

Name of the Student: **Shrushti Krishna Shrivastav**   **PRN: 20220801024**

Title of Practicle :   IAM role Custom Policy to access S3

![D Y Patil International University, Akurdi Pune logo]

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

Name of the Student:	Shrushti Krishna Shrivastav	PRN: 20220801024

Title of Practicle :   IAM role Custom Policy to access S3

Policy is created

STEP3: Create USER

Create one user and attach the policy to that user

School of Computer Science, Engineering and Applications(SCSEA)
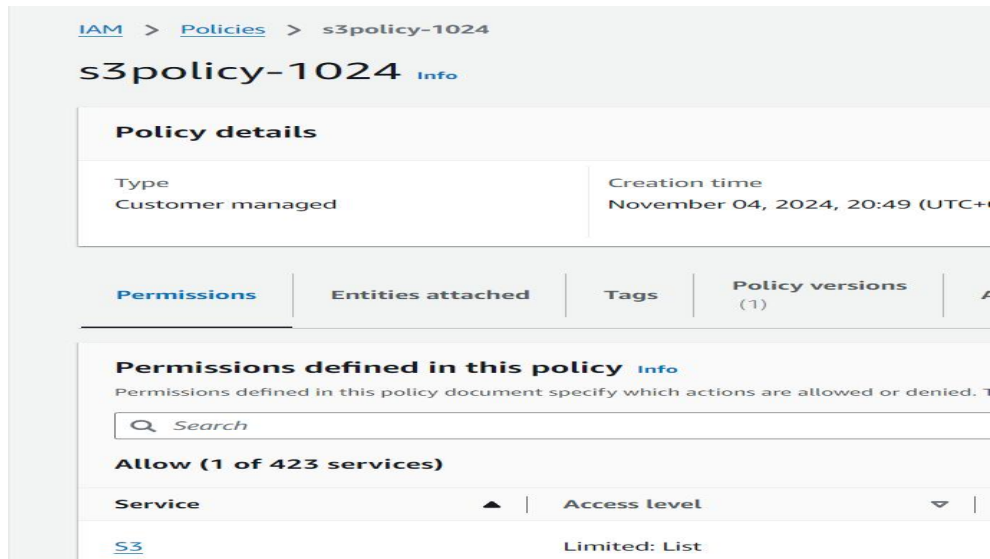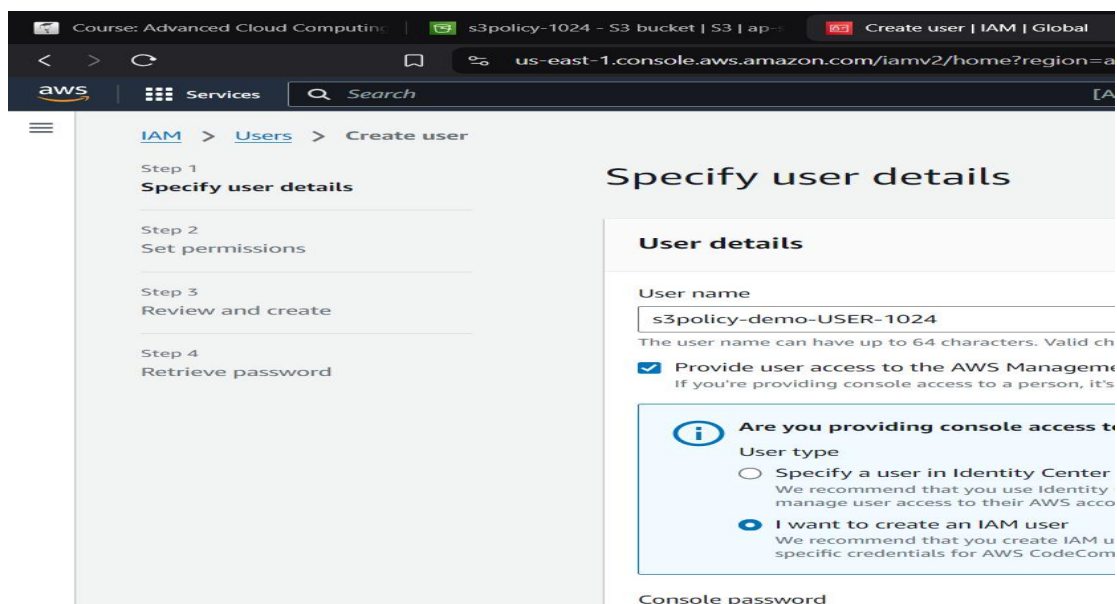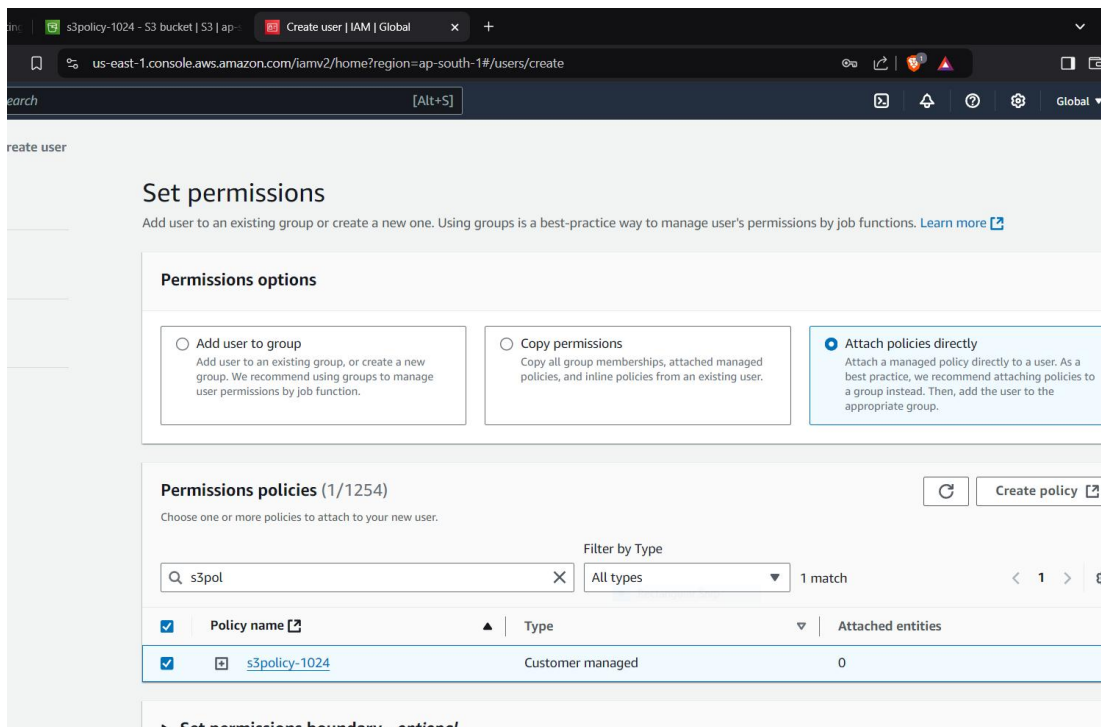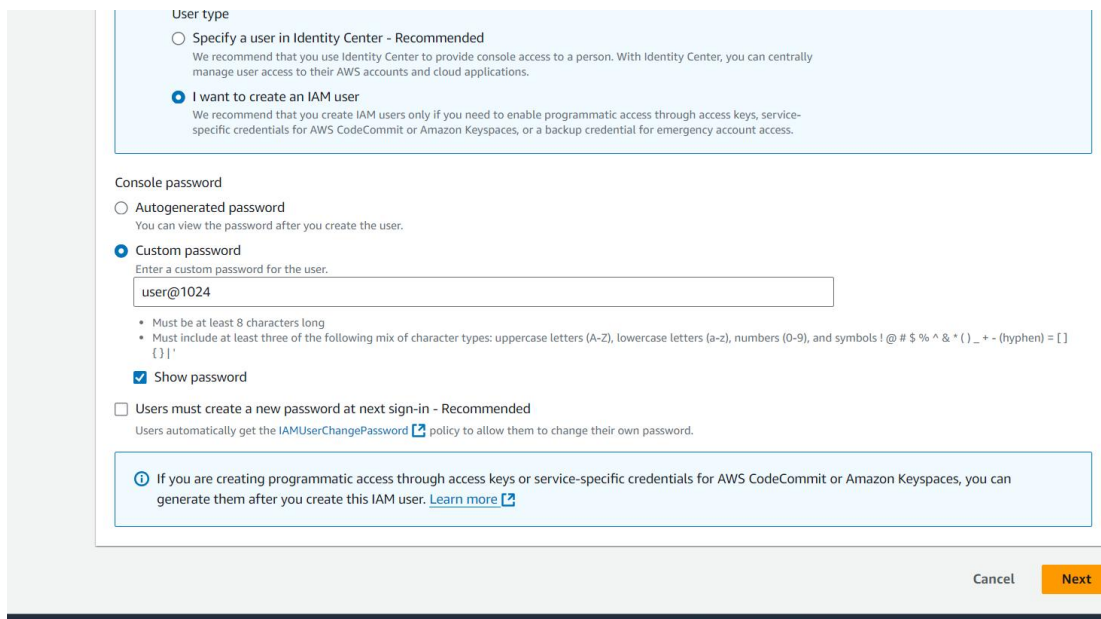## B.C.A. TY (SCSEA)
Subject: Advance Cloud Computing(ACC)

Name of the Student: **Shrushti Krishna Shrivastav**   **PRN:** **20220801024**

Title of Practicle : IAM role Custom Policy to access S3

User type

○ 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.

    user@1024

• 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) = [ ] { } | '

☑ Show password

☐ Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword 🔗 policy to allow them to change their own password.

ⓘ 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   **Next**

us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/create

Create user

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more 🔗

Permissions options

○ **Add user to group**
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ **Copy permissions**
Copy all group memberships, attached managed policies, and inline policies from an existing user.

◉ **Attach policies directly**
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1254)   ↻   Create policy 🔗

Choose one or more policies to attach to your new user.

                                    Filter by Type
Q s3pol   ✕ | All types   ▽ | 1 match   ‹ 1 › ⚙

☑	Policy name 🔗 ▲	Type	▽	Attached entities	▽
☑	⊞ s3policy-1024	Customer managed		0	

▶ **Set permissions boundary** - *optional*
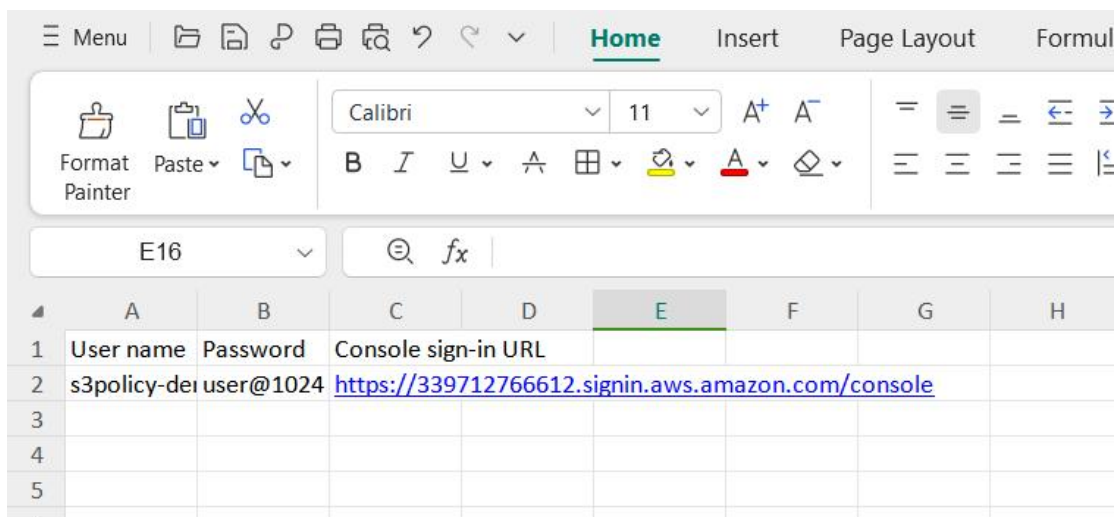
Download the csv file

Name of the Student: **Shrushti Krishna Shrivastav**   **PRN: 20220801024**
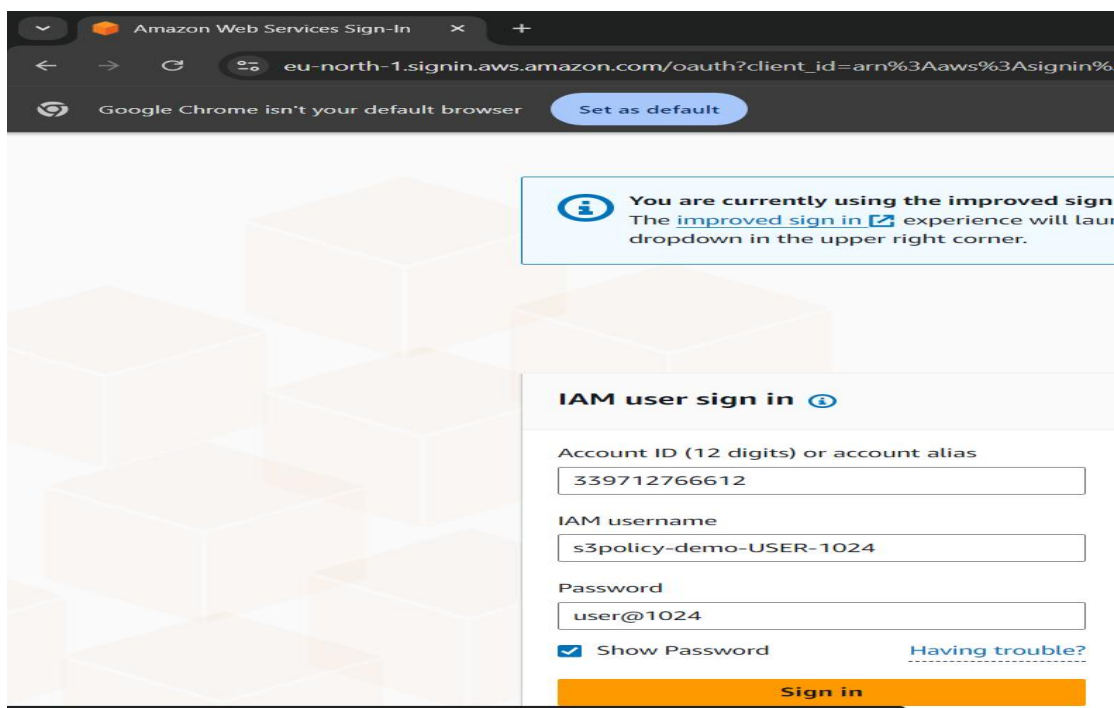
Title of Practicle :   IAM role Custom Policy to access S3

STEP4: Signin as IAM-USER

In new browser or private window copy-paste the url from csv file
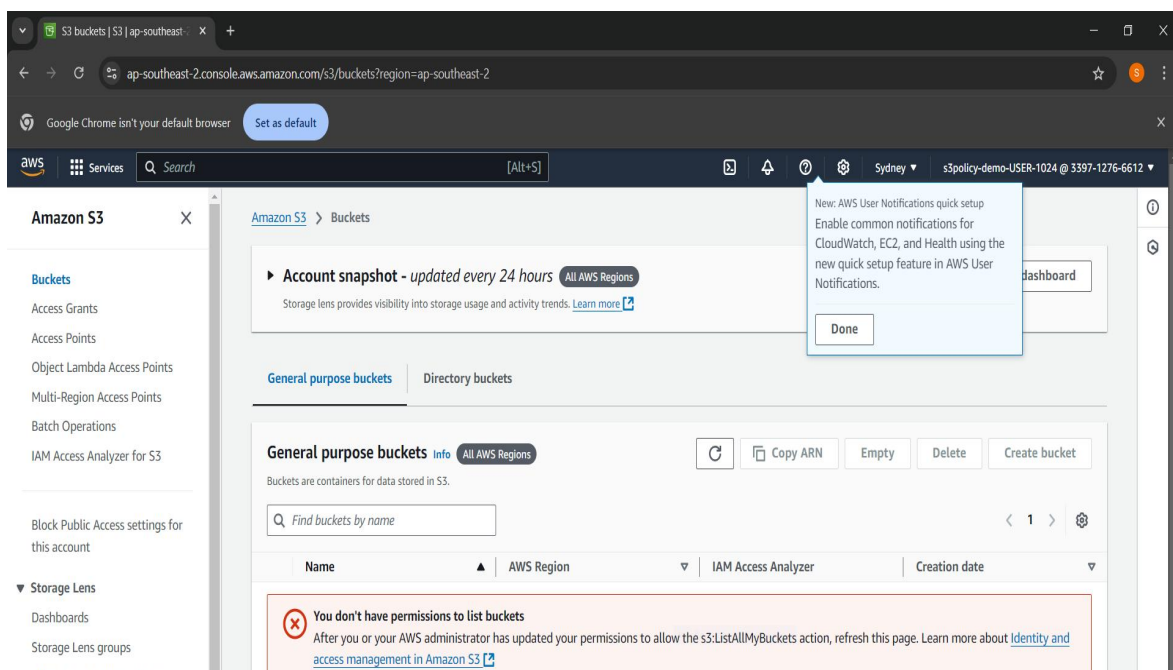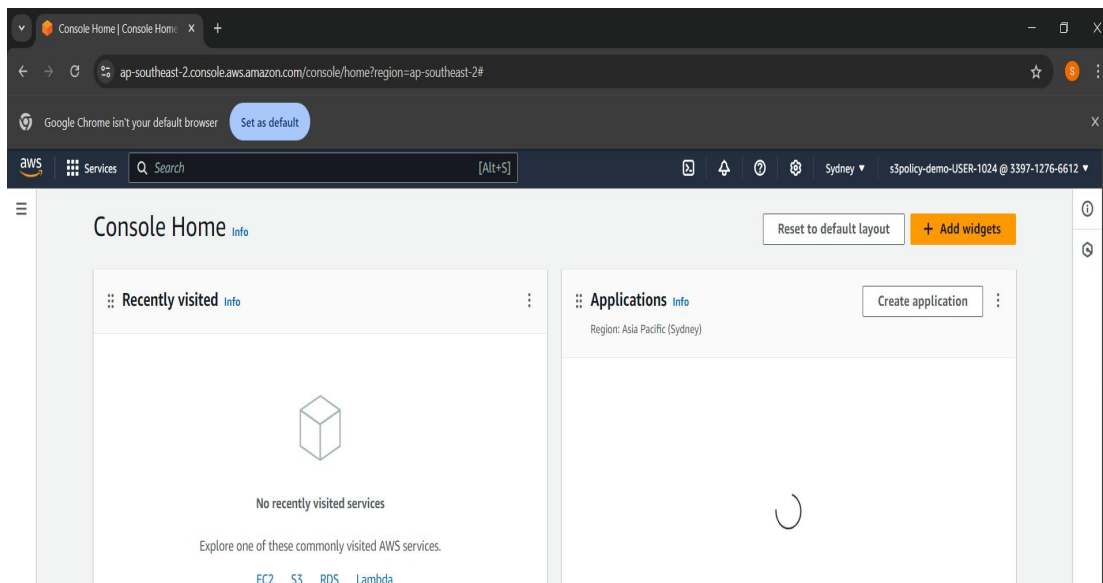
D Y PATIL INTERNATIONAL UNIVERSITY
AKURDI PUNE

School of Computer Science, Engineering and Applications(SCSEA)
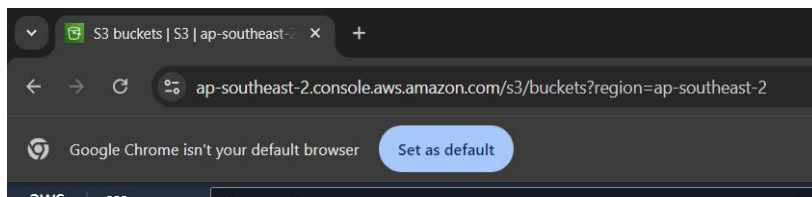# B.C.A. TY (SCSEA)
Subject: Advance Cloud Computing(ACC)

Name of the Student: **Shrushti Krishna Shrivastav**   **PRN: 20220801024**

Title of Practicle :   IAM role Custom Policy to access S3

Name of the Student: **Shrushti Krishna Shrivastav**   **PRN: 20220801024**
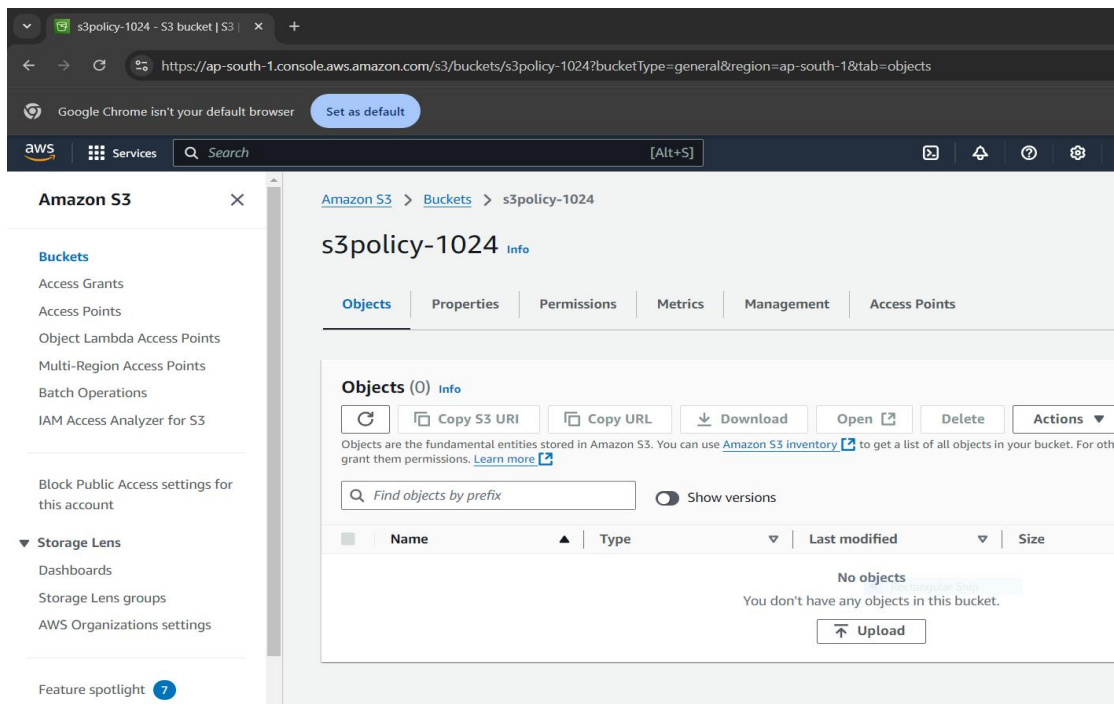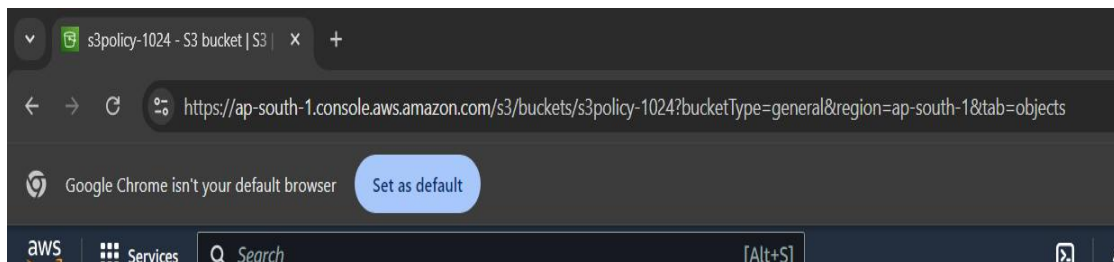
Title of Practicle :   IAM role Custom Policy to access S3

In this url after bucket provide your bucket name and enter

(give bucket name)

Done.