

CC Lab manual 2025

Experiment 1: Demonstrate steps for creating and setting up a S3 bucket.

Step 1: Sign into AWS Management console.

Step 2: Creating Bucket

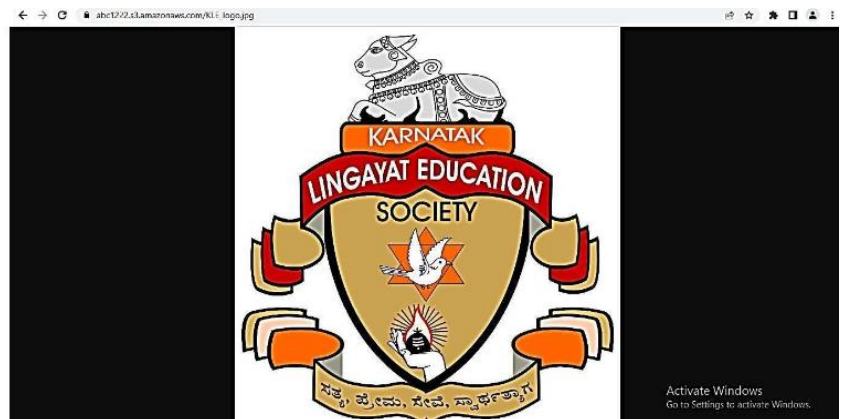
- From the navigation bar click on to the services menu, under the
- Storage and Content Delivery, choose the S3(Simple Storage Service).
- From the Amazon S3 console dashboard, choose Create Bucket.
- In Create a Bucket, type a bucket name in Bucket Name.
- The bucket name you choose must be globally unique across all existing bucket names in Amazon S3
- In the AWS Region select the US East (N. Virginia) us-east-1
- Under Object Ownership, enable ACLs and control ownership of objects uploaded in your bucket, choose one of the following settings:
- Under Block Public Access settings for this bucket, choose the Block Public Access settings that you want to apply to the bucket. By un checking the check box.
- Click on create bucket button.

Step 3: for uploading objects

- In the Buckets list, choose the name of the bucket that you want to upload your object to.
- On the Objects tab for your bucket, choose Upload.
- Under Files and folders, choose Add files.
- Choose a file to upload, and then choose Open.
- Choose Upload.
- Operations or Settings
- Select the object, which has been uploaded
- Click on to the Permission
- Under permissions select the Access Control click on to the Edit option and enable the read and write access permission for public access and
- save the changes.

Step 4: Steps for execution

- Open the object
- Copy the Object URL
- Paste it in the new tab



Experiment 2:

Demonstrate Creating bucket, uploading files and creating Versioning on S3 bucket.

Step 1. Sign into AWS Management console.

- Steps for creating bucket
- Create bucket.
- Once the bucket is created select the Properties, under the properties click on to the Bucket Versioning.
- Select the edit option and enable the bucket versioning and save the changes.

Step 2 for uploading objects

- In the Buckets list, choose the name of the bucket that you want to upload your object to.
- On the Objects tab for your bucket, choose Upload.
- Under Files and folders, choose Add files.
- Choose a file to upload, and then choose Open.
- Choose Upload.
- Upload the same file again by performing the same steps.

Step 3 Operations or Settings

- Select the object, which has been uploaded
- Click on to the Permission
- Under permissions select the Access Control click on to the Edit option and enable the read and write access permission for public access and save the changes.
- Go back to the bucket where the objects which are uploaded are present,
- enable the Show Version option to make visible the versions of the object

The screenshot shows the AWS Management Console interface for an S3 bucket named 'demoversion2025'. The 'Objects' tab is selected, displaying a list of two object versions. The interface includes a top navigation bar with the AWS logo, a search bar, and account information. The bucket's breadcrumb path is 'Amazon S3 > Buckets > demoversion2025'. Below the bucket name, there are tabs for 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab shows a list of objects with columns for Name, Type, Version ID, Last modified, Size, and Storage class. Two versions of a file named 'Screenshot 2025-09-25 103506.png' are listed, both with a size of 182.7 KB and 'Standard' storage class. The first version has a Version ID of '.uNQAKDUfOHZc5awxGKIhDFsM4cqvg5U' and was last modified on September 25, 2025, at 10:54:16 (UTC+05:30). The second version has a Version ID of 'N8SQxFNZZCw_Nu5imZMLJ1k2whRQe6t' and was last modified on September 25, 2025, at 10:46:10 (UTC+05:30). The 'Show versions' toggle is turned on. The bottom of the console shows a footer with 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc. or its affiliates, along with links for 'Privacy', 'Terms', and 'Cookie preferences'.

<input type="checkbox"/>	Name	Type	Version ID	Last modified	Size	Storage class
<input type="checkbox"/>	Screenshot 2025-09-25 103506.png	png	.uNQAKDUfOHZc5awxGKIhDFsM4cqvg5U	September 25, 2025, 10:54:16 (UTC+05:30)	182.7 KB	Standard
<input type="checkbox"/>	Screenshot 2025-09-25 103506.png	png	N8SQxFNZZCw_Nu5imZMLJ1k2whRQe6t	September 25, 2025, 10:46:10 (UTC+05:30)	182.7 KB	Standard

Experiment 3:

Create a Cross Region Replication for objects in S3 buckets

1. Create Bucket 1.
2. Enable versioning for the created bucket.
3. Create another Bucket 2(Source Bucket) in different region.
4. Enable versioning for the newly created bucket 2.
5. Go to Bucket 2, under Management, choose 2nd option Replication Rules
6. Click on Create Replication rule.
7. Enter Replication Rule name.
8. Under Source Bucket, choose a rule scope to apply to all objects.
9. Under Destination bucket section, choose the Bucket which has been already created in different region (Bucket 1).
10. In IAM Role, click on the drop down menu and choose create new role.
11. Click on Save.
12. Replication rules have been defined.
13. Upload objects into Bucket 2 (Source Bucket)
14. Check Bucket 1 to confirm the replication in different region.

The object uploaded in Bucket 2 will be replicated in Bucket 1

This screenshot shows the 'Replication rules' page for the bucket 'source.bucket25' in the 'Europe (London)' region. A single rule named 'rule25' is listed, which is 'Enabled'. It replicates from 'source.bucket25' in the 'Asia Pacific (Mumbai) ap-south-1' region to the same bucket in the same region. The rule scope is 'Entire bucket' and it uses the 'Same as source' storage class. The 'Replica owner' is 'Same as source', 'Replication Time Control' is 'Disabled', and 'KMS-encrypted objects' are 'Do not replicate'.

Replication rule name	Status	Destination bucket	Destination Region	Priority	Scope	Storage class	Replica owner	Replication Time Control	KMS-encrypted objects (SSE-KMS or DSSE-KMS)	Replica modification sync
rule25	Enabled	s3://destination.bucket-25	Asia Pacific (Mumbai) ap-south-1	0	Entire bucket	Same as source	Same as source	Disabled	Do not replicate	Disabled

This screenshot shows the 'Objects' page for 'source.bucket25' in the 'Europe (London)' region. It displays a list of objects with columns for Name, Type, Version ID, Last modified, Size, and Storage class. One object is listed: 'Screenshot 2025-05-11 155232.png' with a version ID of 'szfwAtcwl9XxXf423N7j.ntgYM RTbzW_'. It was last modified on September 25, 2025, at 22:39:54 (UTC+05:30) and has a size of 142.1 KB, stored in the 'Standard' storage class.

Name	Type	Version ID	Last modified	Size	Storage class
Screenshot 2025-05-11 155232.png	png	szfwAtcwl9XxXf423N7j.ntgYM RTbzW_	September 25, 2025, 22:39:54 (UTC+05:30)	142.1 KB	Standard

This screenshot shows the 'Objects' page for 'destination.bucket-25' in the 'Asia Pacific (Mumbai)' region. It displays a list of objects with columns for Name, Type, Last modified, Size, and Storage class. One object is listed: 'Screenshot 2025-05-11 155232.png' with a version ID of 'szfwAtcwl9XxXf423N7j.ntgYM RTbzW_'. It was last modified on September 25, 2025, at 22:39:54 (UTC+05:30) and has a size of 142.1 KB, stored in the 'Standard' storage class.

Name	Type	Last modified	Size	Storage class
Screenshot 2025-05-11 155232.png	png	September 25, 2025, 22:39:54 (UTC+05:30)	142.1 KB	Standard

Experiment 4:

Demonstrate how to set up static website hosting by using Amazon S3

Step 1. Sign into AWS Management console.

Step 2 for creating bucket

- Create bucket.
- Once the bucket is created, Select the Properties option under the bucket
- Select server access logging and enable server access logging
- and save the changes
- Select the Static website hosting and click on edit, Enable the static website hosting, below that enter html file name in index document and save the changes

Step 3 to upload the html file

- In the Buckets list, choose the name of the bucket that you want to
- upload your object to.
- On the Objects tab for your bucket, choose Upload.
- Under Files and folders, choose Add files.
- Choose a html file to upload, and then choose Open.
- Choose Upload.
- Operations or Settings
- Select the object i.e. html file , which has been uploaded
- Click on to the Permission
- Under permissions select the Access Control click on to the Edit option and enable the read and write access permission for public access and save the changes.

Example for html file

```
<Html>
```

```
<head>
```

```
<title>
```

```
Registration Page
```

```
</title>
```

```
</head>
```

```
<body bgcolor="Lightskyblue">
```

```
<br>
```

```
<br>
```

```
<form>
```

```
<label> Firstname </label>
```

```
<input type="text" name="firstname" size="15"/> <br> <br>
```

```
<label> Middlename: </label>
```

```
<input type="text" name="middlename" size="15"/> <br> <br>
```

```
<label> Lastname: </label>
```

```
<input type="text" name="lastname" size="15"/> <br> <br>
```

```
<label>
```

```
Course :
```

```
</label>
```

```
<select>
```

```
<option value="Course">Course</option>
```

```
<option value="BCA">BCA</option>
```

```
<option value="BBA">BBA</option>
```

```
<option value="B.Tech">B.Tech</option>
```

```
<option value="MBA">MBA</option>
```

```

<option value="MCA">MCA</option>
<option value="M.Tech">M.Tech</option>
</select>
<br>
<br>
<label>
Gender :
</label><br>
<input type="radio" name="male"/> Male <br>
<input type="radio" name="female"/> Female <br>
<input type="radio" name="other"/> Other
<br>
<br>
<label>
Phone :
</label>
<input type="text" name="country code" value="+91" size="2"/>
<input type="text" name="phone" size="10"/> <br> <br>
Address
<br>
<textarea cols="80" rows="5" value="address">
</textarea>
<br> <br>
Email:
<input type="email" id="email" name="email"/> <br>
<br> <br>
Password:
<input type="Password" id="pass" name="pass"> <br>
<br> <br>
Re-type password:
<input type="Password" id="repass" name="repass"> <br> <br>
<input type="button" value="Submit"/>
</form>
</body>
</html>

```

Steps for execution:-

- ☐ Open the Static website hosting page
- ☐ Copy the below link (eg:awsamazon.com)
- ☐ Paste it in the new tab

Note: HTML Page has to be written as per the question

Firstname:

Middlename:

Lastname:

Course :

Gender :

☐ Male

☐ Female

☐ Other

Phone :

Address

Email:

Password:

Re-type password:

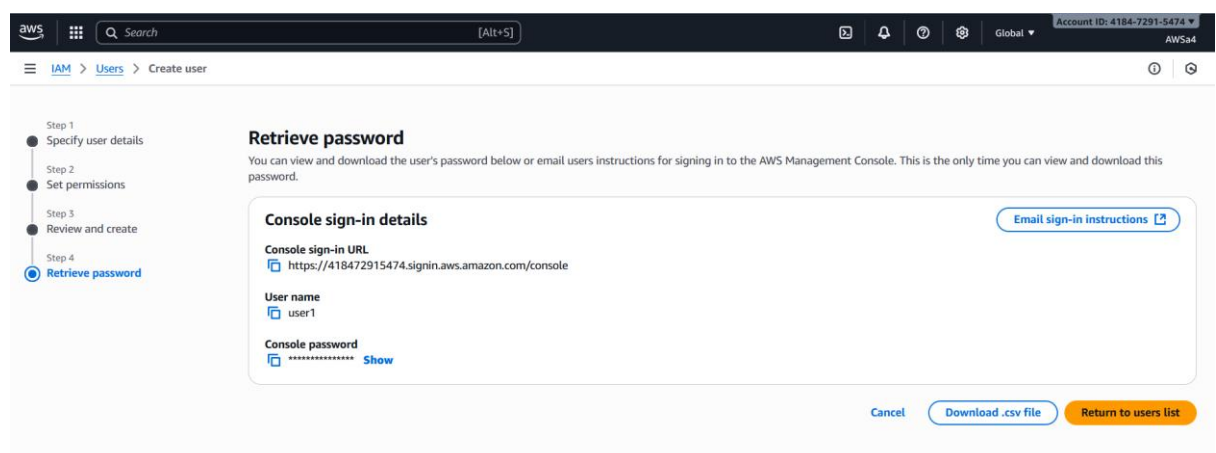
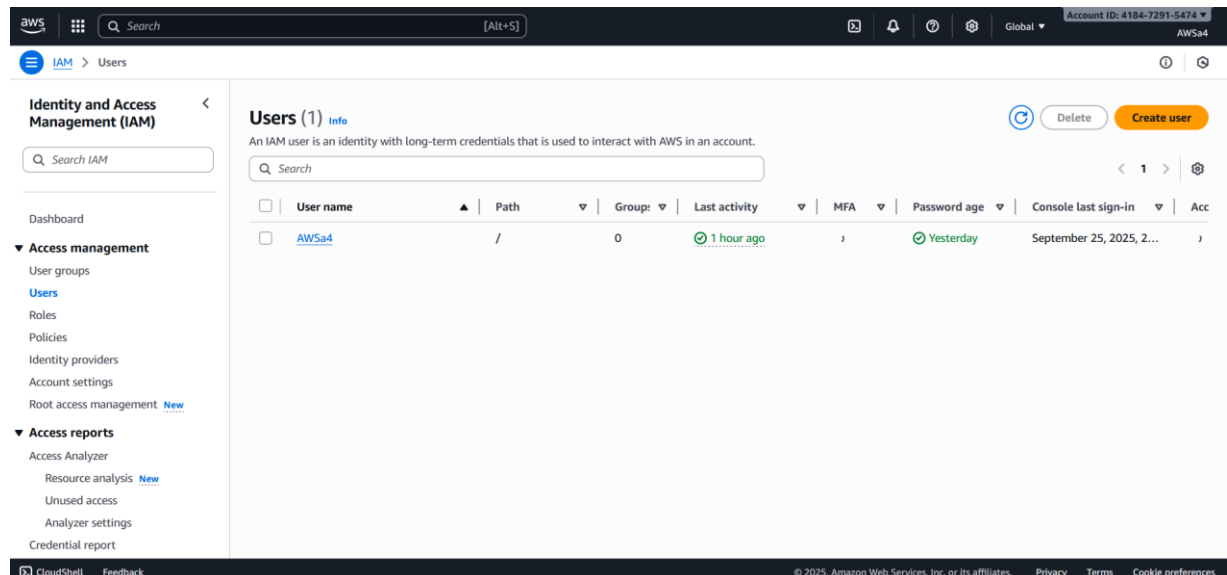
Activate Windows
Go to Settings to activate Windows.

Experiment 5:

Create an IAM users, groups and roles

To create one or more IAM users (console)

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the navigation pane, choose Users and then choose Add user.
3. Type the user name for the new user. This is the sign-in name for AWS.
4. Select the type of access this set of users will have. You can select programmatic access, access to the AWS Management Console,
5. Select I want to create an IAM user
6. For Console password, choose one of the following:
Autogenerated password or Custom password.
7. Choose Next: Permissions.
8. On the Set permissions page, specify how you want to assign permissions to this set of new users.
Choose Attach existing policies to user directly and add policies in below given list
9. Choose Next: Tags.
10. To view the users' access keys (access key IDs and secret access keys), choose Show next to each password and access key that you want to see. To save the access keys, choose Download .csv and then save the file to a safe location.



Experiment 6:

Enabling a Virtual Multi-Factor Authentication (MFA) Device

To enable a virtual MFA device for an IAM user (console)

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the navigation pane, choose Users.
3. In the User Name list, choose the name of the intended MFA user.
4. Choose the Security credentials tab. Next to Assigned MFA device, choose Manage.
5. In the Manage MFA Device wizard, choose Virtual MFA device, and then choose Continue. IAM generates and displays configuration information for the virtual MFA device, including a QR code graphic.

Open your virtual MFA app. For a list of apps that you can use for hosting virtual MFA devices.

6. Determine whether the MFA app supports QR codes, and then do one of the following:
 - From the wizard, choose Show QR code, and then use the app to scan the QR code. For example, you might choose the camera icon or choose an option similar to Scan code, and then use the device's camera to scan the code. In the Manage MFA Device wizard, choose Show secret key, and then type the secret key into your MFA app.
 - When you are finished, the virtual MFA device starts generating one-time passwords.
7. In the Manage MFA Device wizard, in the MFA code 1 box, type the one-time

password that currently appears in the virtual MFA device. Wait up to 30 seconds for the device to generate a new one-time password. Then type the second one- time password into the MFA code 2 box.


Choose Assign MFA.

The virtual MFA device is now ready for use with AWS

Select MFA device [Info](#)


Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.

☒




Authenticator app
Authenticate using a code generated by an app installed on your mobile device or computer.

☐



Security Key
Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.

☐




Hardware TOTP token
Authenticate using a code displayed on a hardware Time-based one-time password (TOTP) token.

Set up virtual MFA device

1. Install a compatible app on your mobile device or computer
[See a list of compatible applications](#)

2. Use your virtual MFA app and your device's camera to scan the QR code



Alternatively, you can type the secret key. [Show secret key](#)

3. Type two consecutive MFA codes below

MFA code 1

MFA code 2

[Cancel](#) [Previous](#) [Assign MFA](#)

2FA authenticator
by typingdata

928699 LinkedIn (john.doe@myemail.com)
077834 Google (john.doe@myemail.com)
658488 Amazon Web Services (john.doe...)
[Grab QR code](#) [Add code manually](#)

All secret keys are stored exclusively on this PC/Chrome user. Also keep in mind that some websites ask you to repeatedly type in your code (inject/copy/paste will not work). [Dismiss](#)

© typingdata.com | How it works | Feedback | Logout

Multi-factor Authentication

Enter an MFA code to complete sign-in.

MFA Code:

Submit

[Cancel](#)

Experiment 7:

Demonstrate how to secure a bucket using bucket policy.

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the left navigation pane, choose Buckets.
3. In the Buckets list, choose the name of the bucket that you want to create a bucket policy for or whose bucket policy you want to edit.
4. Choose the Permissions tab
5. Under Bucket policy, choose Edit. The Edit bucket policy page appears
6. On the Edit bucket policy page, do the following:
 - edit the JSON same as below JSON policy elements

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::trail123456djhsb",
        "arn:aws:s3:::trail123456djhsb/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "YOUR_AWS_ACCOUNT_ID"
        }
      }
    }
  ]
}
```

Note:

For your convenience, the Edit bucket policy page displays the Bucket ARN (Amazon Resource Name) of the current bucket above the Policy text field. You can copy this ARN for use in the statements on the AWS Policy Generator page

7. Choose Save changes, which returns you to the Permissions tab.
8. Now we can't delete or modify the object.

