

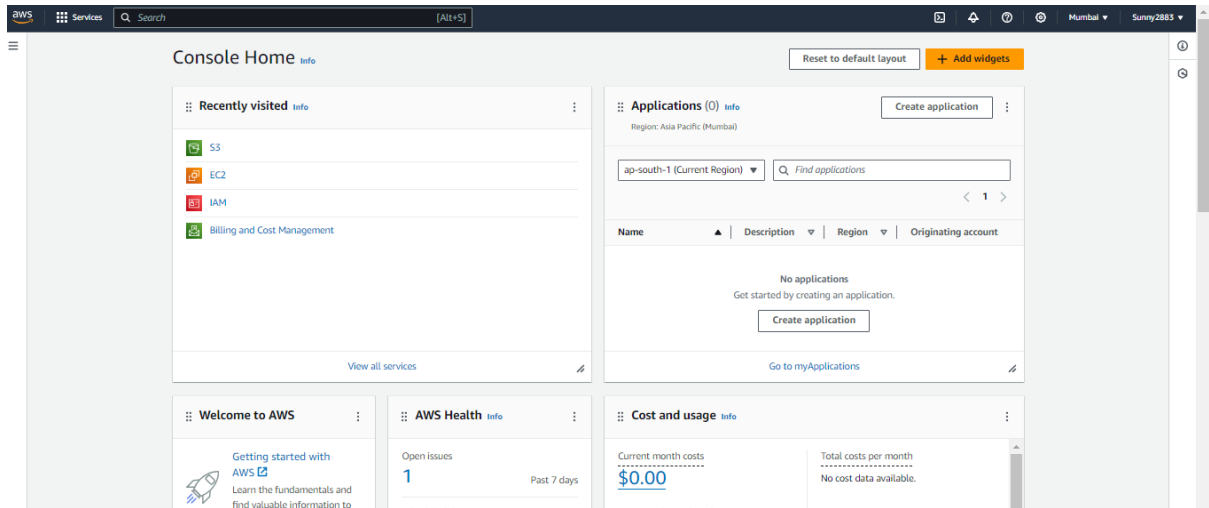
# Assignment:3

## Task:1

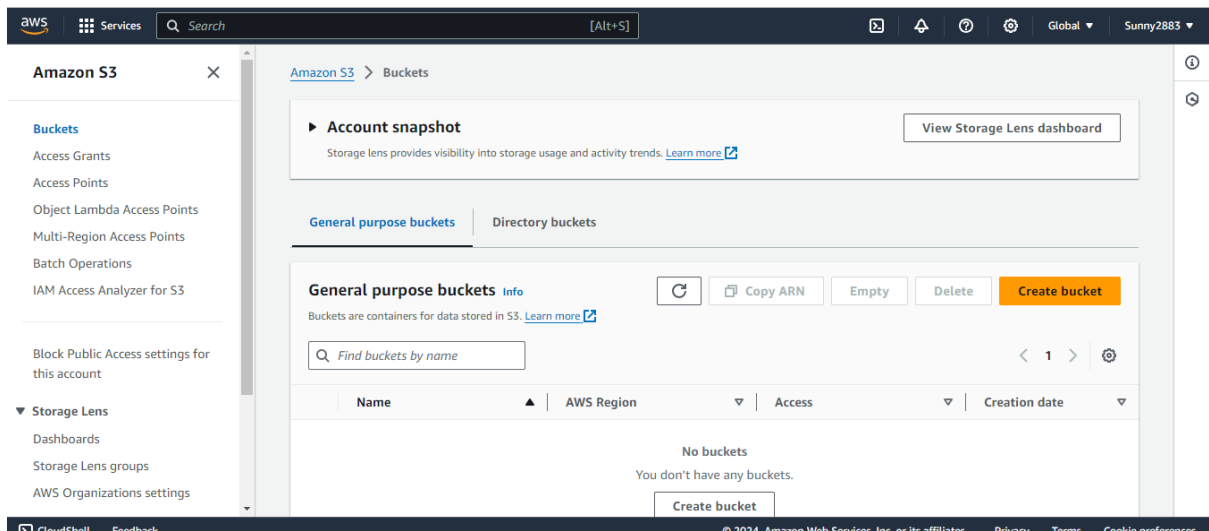
### Create an S3 Bucket:

Create a new S3 bucket with a globally unique name.

Step1: Sign in AWS console.



Step2: Navigate to s3:



### Step3: Create a new bucket and specify bucket name.

Amazon S3 > Buckets > Create bucket

## Create bucket Info

Buckets are containers for data stored in S3. [Learn more](#)

### General configuration

AWS Region  
Asia Pacific (Mumbai) ap-south-1

Bucket name Info  
sunny2883-bucket

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - *optional*  
Only the bucket settings in the following configuration are copied.

**Choose bucket**

Format: s3://bucket/prefix

### Step4: Configure option and set the permission.

Encryption type Info

- ☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)
- ☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- ☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)  
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key  
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

- ☐ Disable
- ☒ Enable

► Advanced settings

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel **Create bucket**

### Step5: Bucket created successfully.

Successfully created bucket "sunny2883-bucket"  
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Amazon S3 > Buckets

► Account snapshot [View Storage Lens dashboard](#)

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

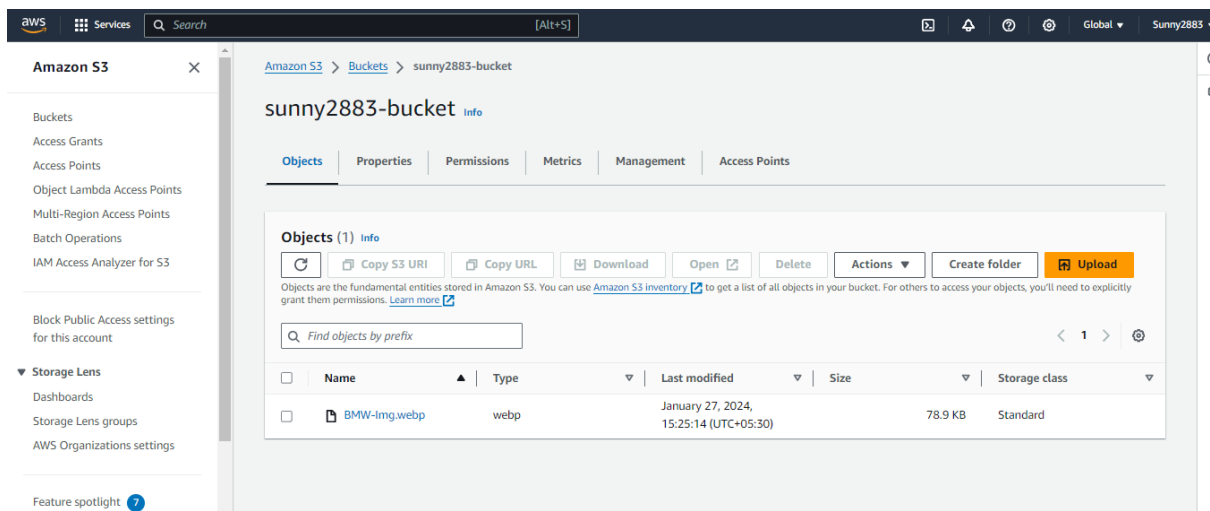
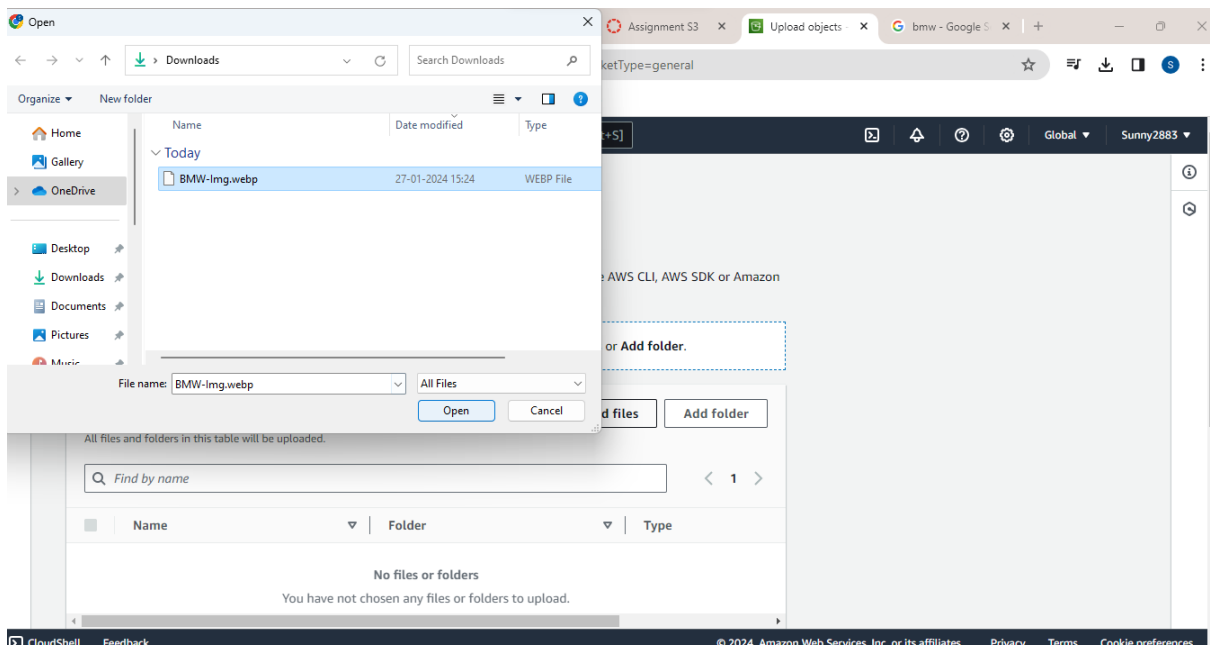
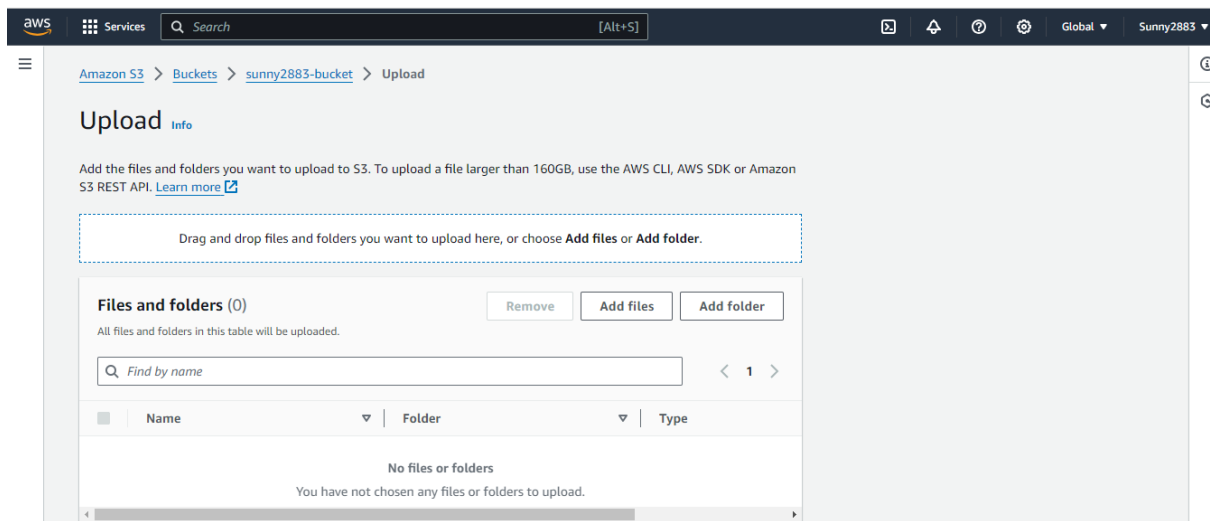
General purpose buckets | Directory buckets

### General purpose buckets (1) Info

Buckets are containers for data stored in S3. [Learn more](#)

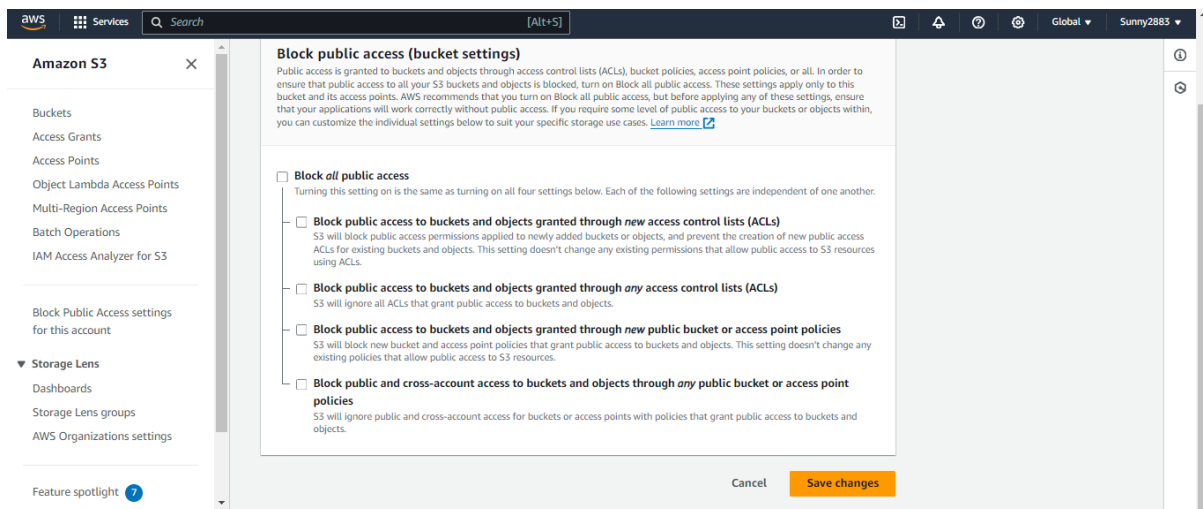
Name	AWS Region	Access	Creation date
sunny2883-bucket	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	January 27, 2024, 15:22:31 (UTC+05:30)

## Step6: Upload the Objects.

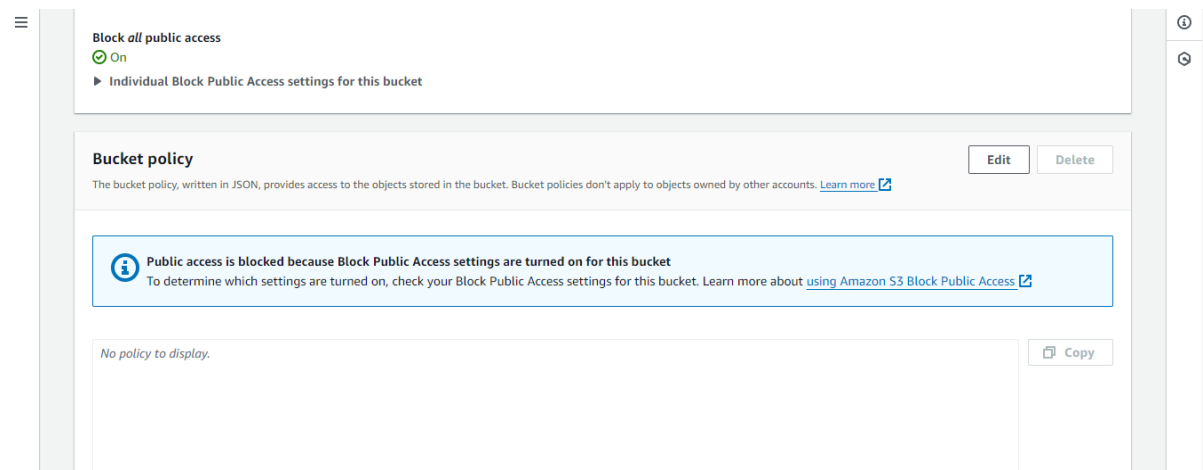


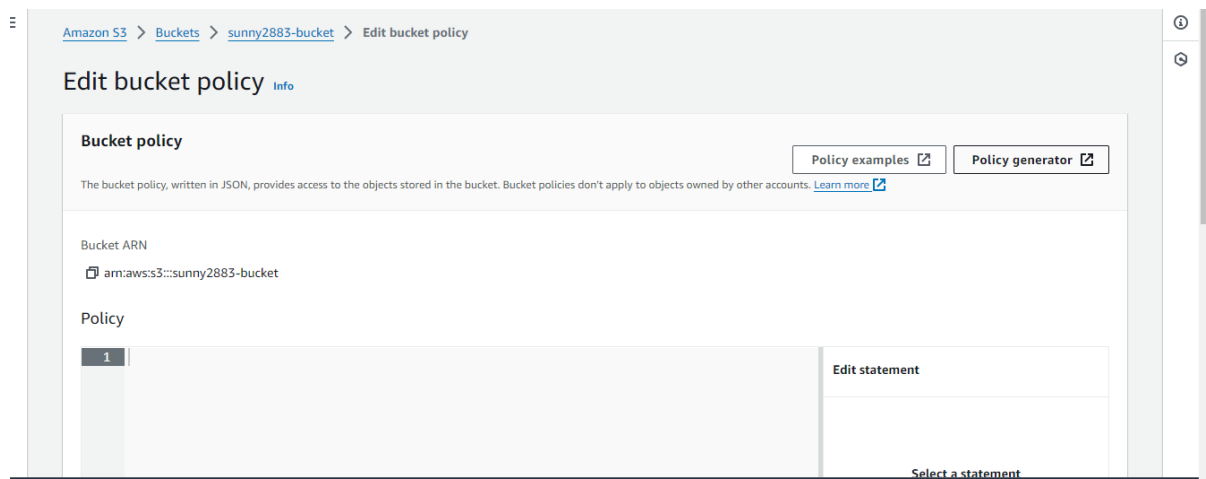
## Configure bucket policies and access control lists (ACLs) to control permissions.

Step1: Disable public access start by unchecking all options for public access in the s3 bucket setting to ensure a secure environment.



Step2: Access bucket policy, navigate to the bucket click on the permissions tab and select Bucket policy to define access controls at the bucket level.





Step3: Define Policy type Such as “Identity-based” or “Resource-based” and proceed to add specific statements for desired permissions. Craft Policy statement’s specified allowed or denied actions for different AWS identities or conditions.

### Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy S3 Bucket Policy

### Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a [description of elements](#) that you can use in statements.

Effect ☒ Allow ☐ Deny

Principal

Use a comma to separate multiple values.

AWS Service Amazon S3 ☐ All Services ("\*")

Use multiple statements to add permissions for more than one service.

Actions 3 Action(s) Selected ☐ All Actions ("\*")

Amazon Resource Name (ARN) arn:s3::sunny2883-bucket/\*

ARN should follow the following format: arn:aws:s3:::{BucketName}/{KeyPrefix}.

Use a comma to separate multiple values.

[Add Conditions \(Optional\)](#)

[Add Statement](#)

You added the following statement(s). Click the button below to generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
* *	Allow	<ul style="list-style-type: none"> <li>s3:DeleteObject</li> <li>s3:GetObject</li> <li>s3:PutObject</li> </ul>	arn:aws:s3::sunny2883-bucket/*	None

### Step 3: Generate Policy

## Step5: Create Policy JSON document Within the policy editor.

Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor.  
Changes made below will **not** be reflected in the policy generator tool.

```
{
  "Id": "Policy1706349587832",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1706349567329",
      "Action": [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::sunny2883-bucket/*",
      "Principal": "*"
    }
  ]
}
```

Close

## Step6: Copy generated policy JSON into policy editor.

aws Services Search [Alt+S]

Bucket ARN  
arn:aws:s3:::sunny2883-bucket

Policy

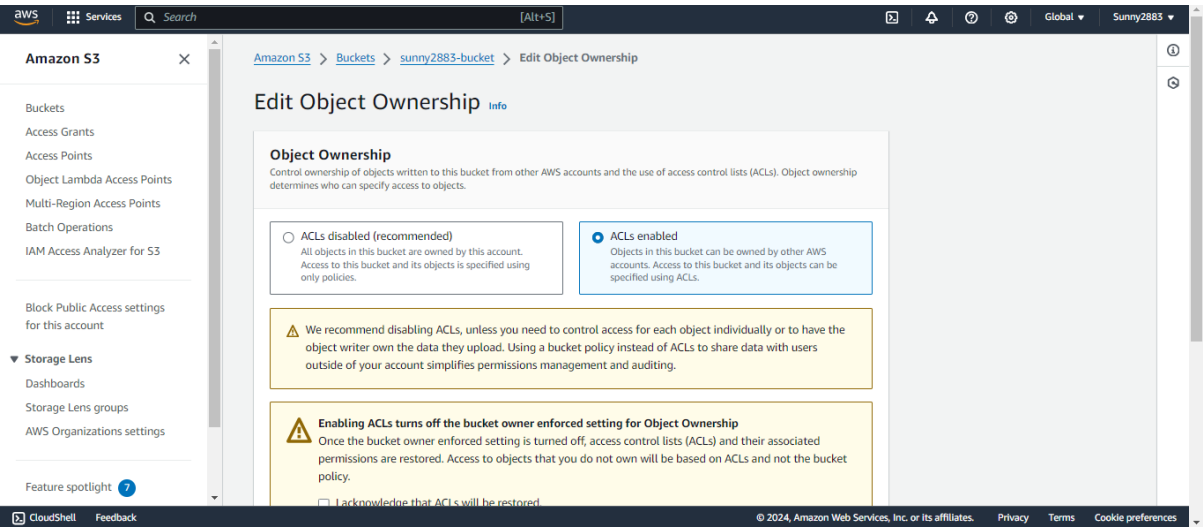
```
1 {
2   "Id": "Policy1706349587832",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "Stmt1706349567329",
7       "Action": [
8         "s3:DeleteObject",
9         "s3:GetObject",
10        "s3:PutObject"
11      ],
12      "Effect": "Allow",
13      "Resource": "arn:aws:s3:::sunny2883-bucket/*",
14      "Principal": "*"
15    }
16  ]
17 }
```

Edit statement

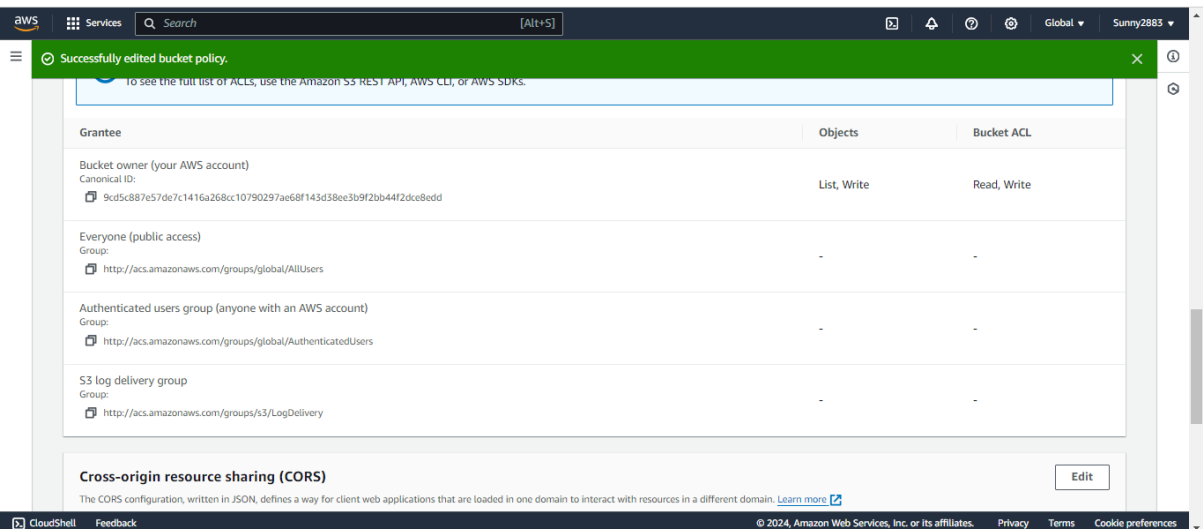
Select a statement  
Select an existing statement in the policy or  
add a new statement.  

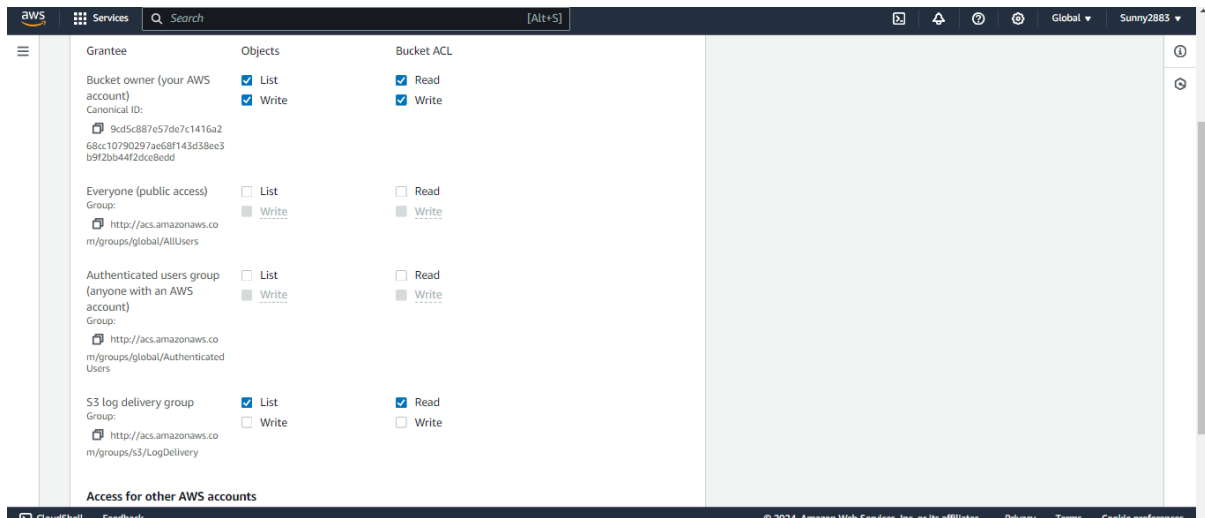
+ Add new statement

## Step7: Edit object ownership and select ACLs enabled



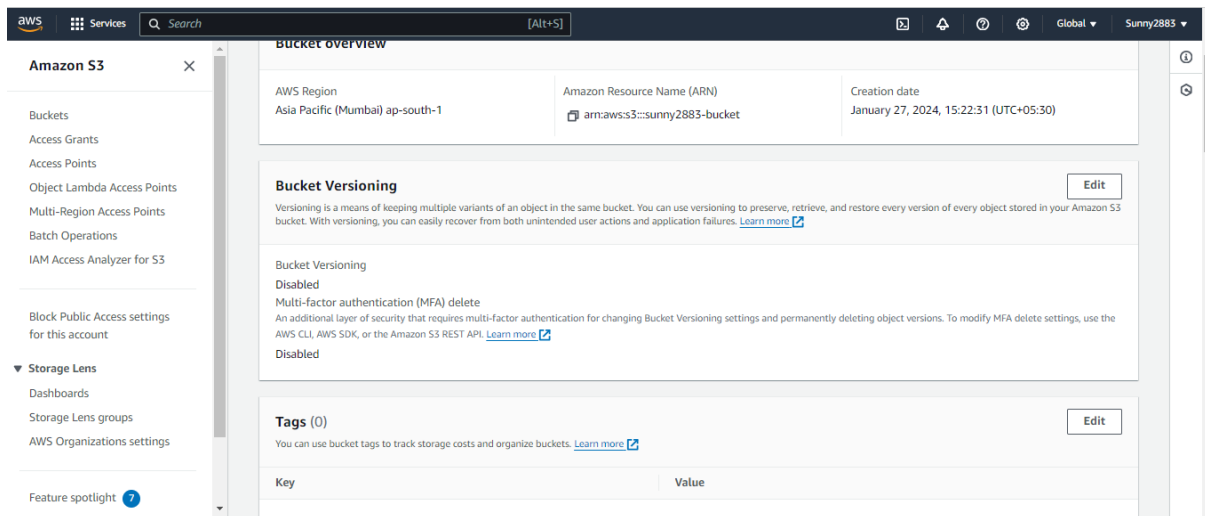
## Step8: Bucket policy edited successfully.





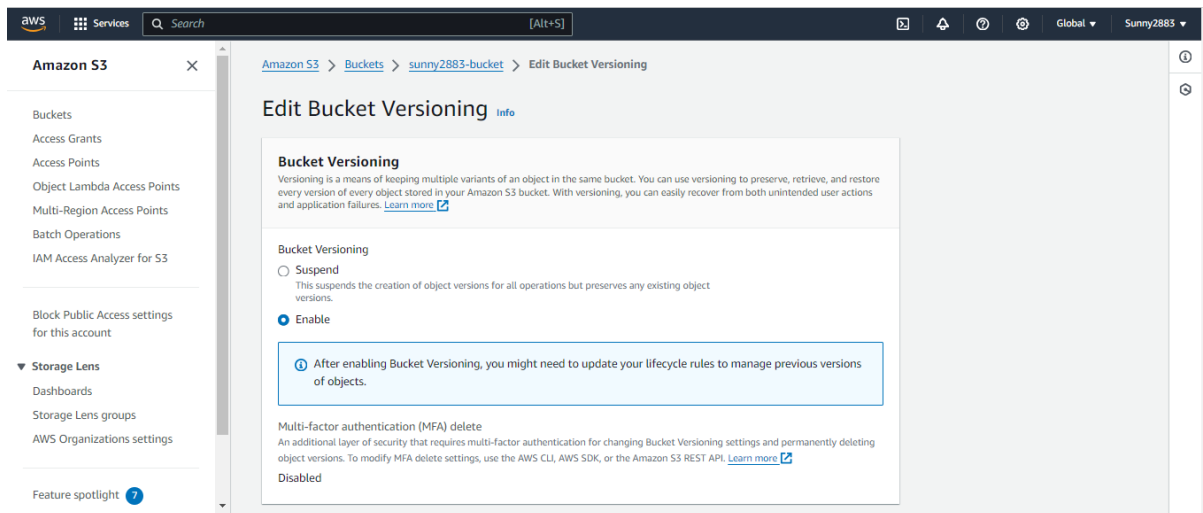
## Enable versioning for your S3 bucket.

Step1: Select your bucket and choose bucket versioning.



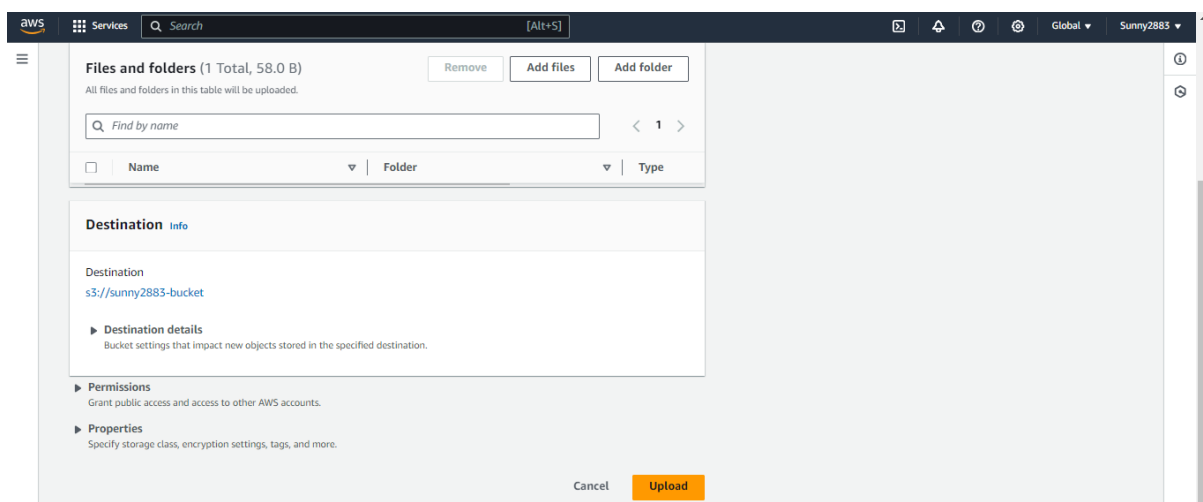
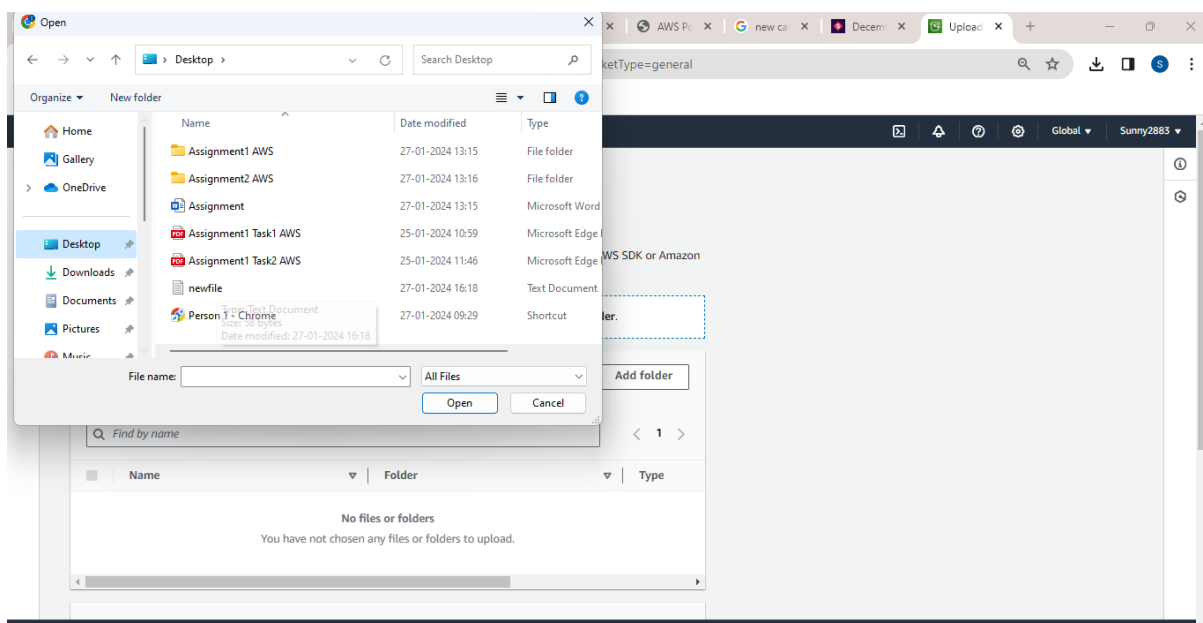
Step2: Toggle the versioning option to “Enable versioning” and confirm your action.



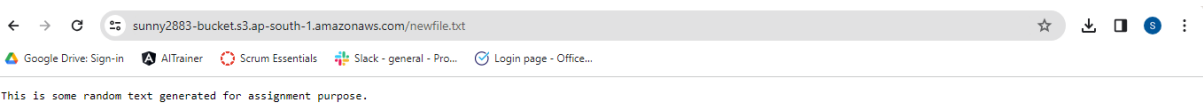


Upload, modify, and delete objects to observe versioning in action.

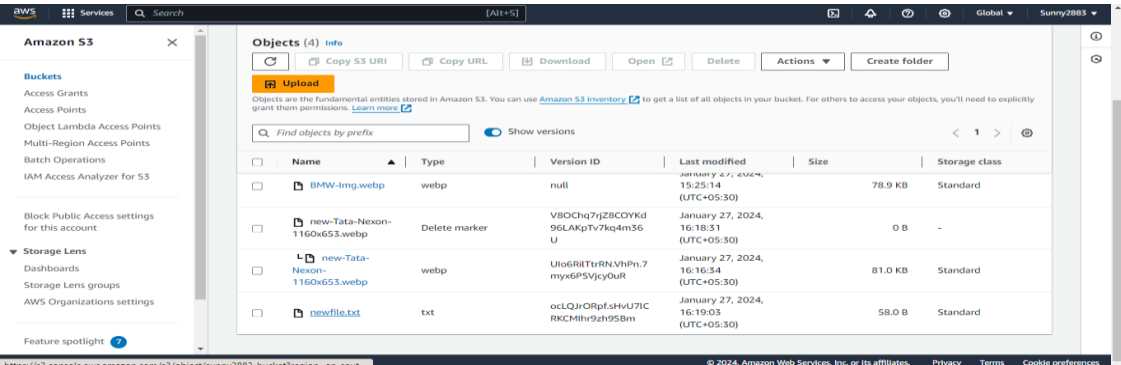
Step1: Upload Initial object to your versioned s3 bucket.



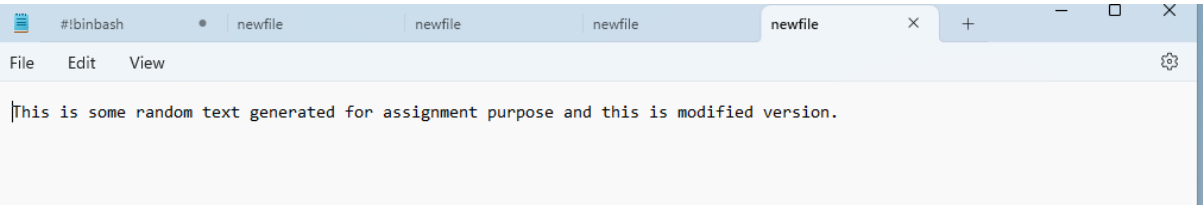
# Content of object.



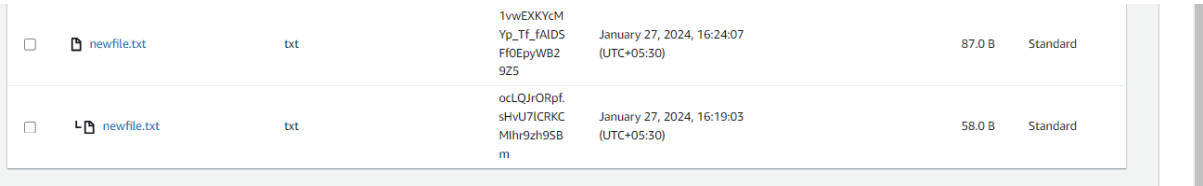
# Version of added objects.



Step2: Modify object make changes to one or more object by either replacing them or updating the content.



Step3; Check version history, select an object and view its version history.



Step4: Delete one or more objects from the bucket. Deleted opbjects are not permanently removed. Instead, a delete marker is added.

aws

Services

Search

[Alt+S]

Global

Sunny2883


• If a folder is selected for deletion, all objects in the folder will be deleted, and any new objects added while the delete action is in progress might also be deleted. If an object is selected for deletion, any new objects with the same name that are uploaded before the delete action is completed will also be deleted.

Deleting the specified objects can't be undone.

[Learn more](#)

Specified objects

Find objects by name

Name	Version ID	Type	Last modified
 newfile.txt	1vwEXKYcMYp_Tf_fAlDSFf0EpyWB29Z5	txt	January 27, 2024, 16:24:07 (UTC+0)

Permanently delete objects?

To confirm deletion, type *permanently delete* in the text input field.

permanently delete

Cancel

Delete objects

Step5: Updated version id.