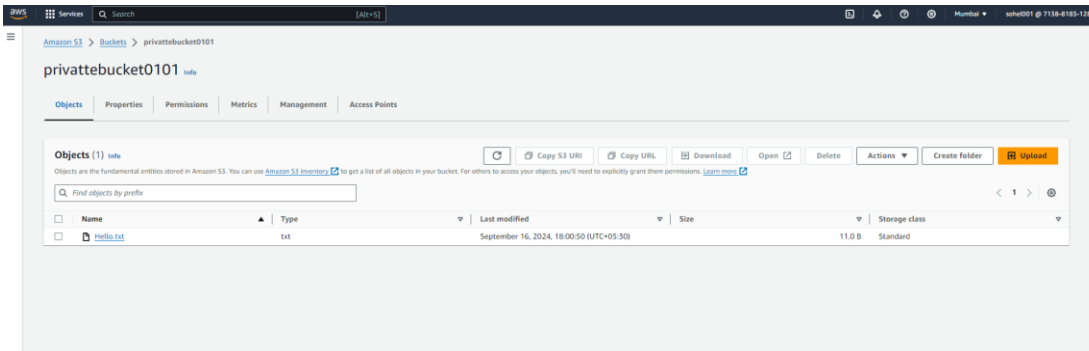
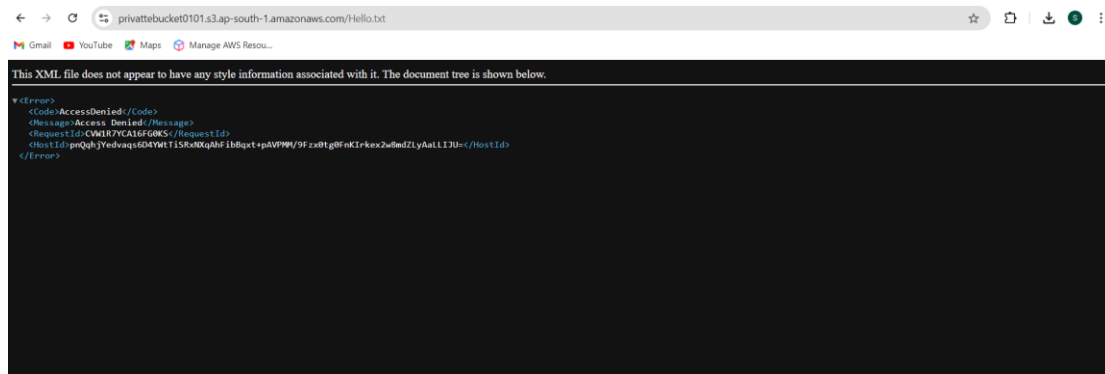


S3 practical

- Create a private bucket and add object in it

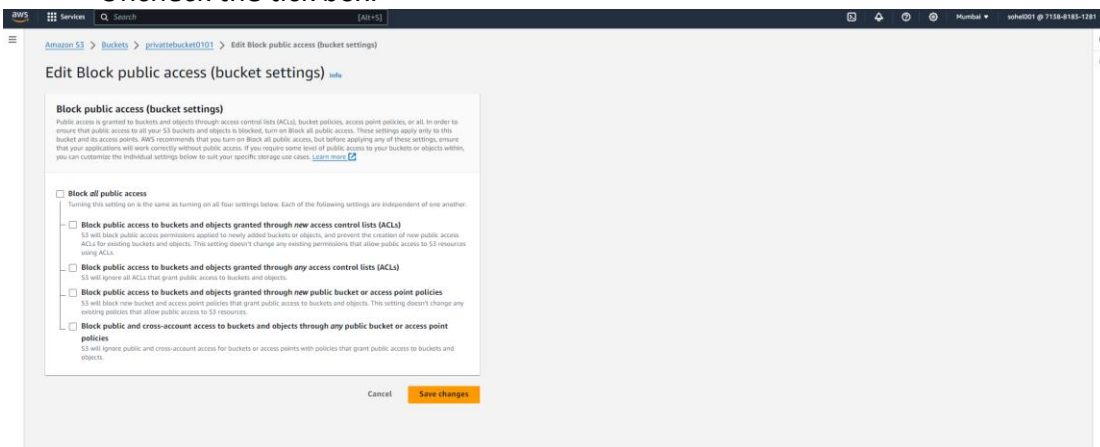


- The Object is private and not able to access

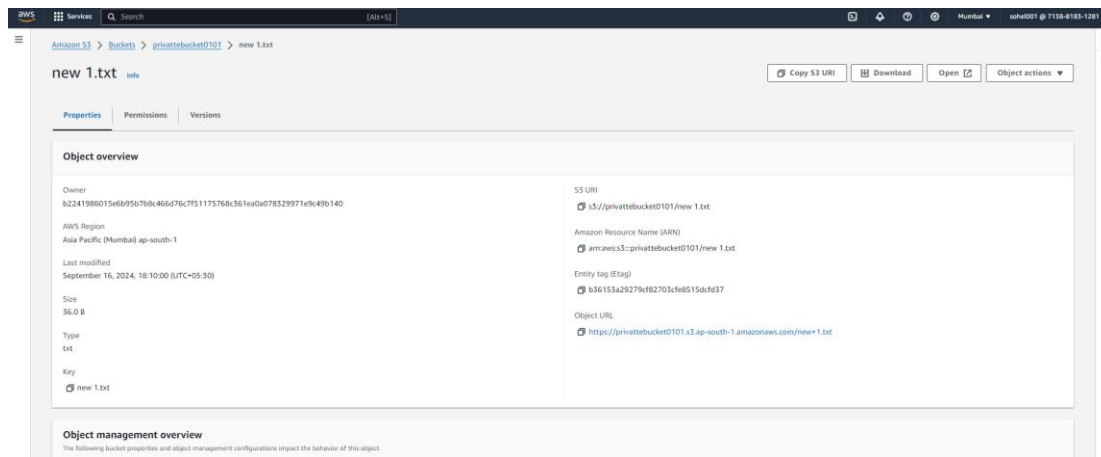


Making existing bucket as public

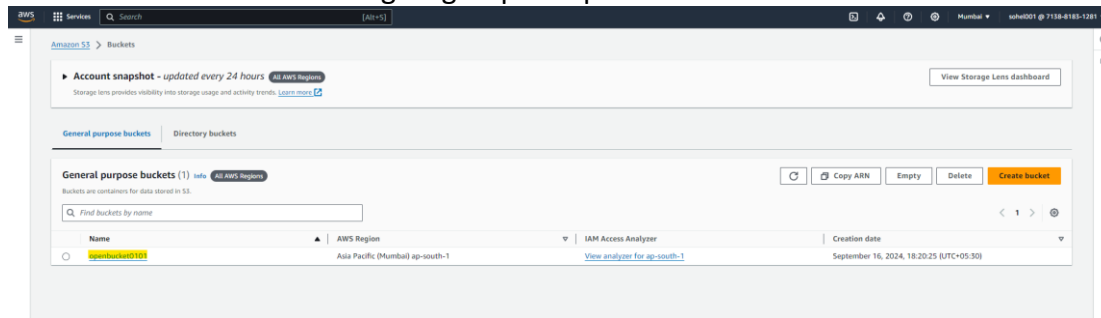
- Uncheck the tick box.



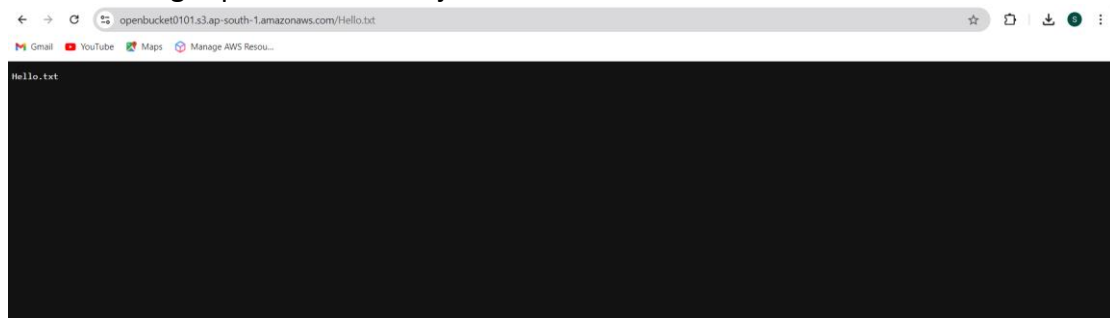
- When we upload any object in bucket, the bucket is private by default



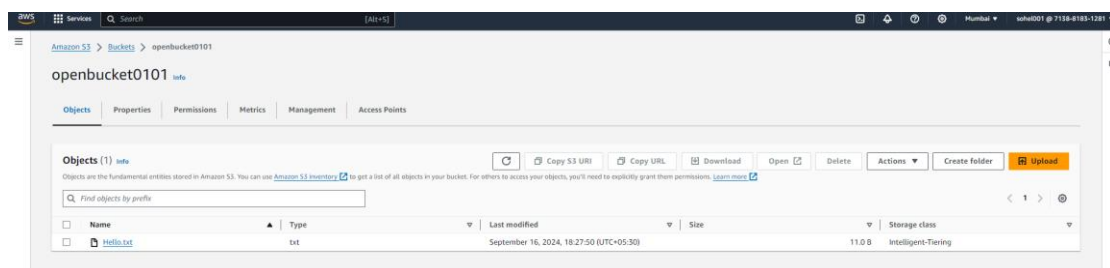
- Create a bucket with giving required permission.



- Changes permission of object

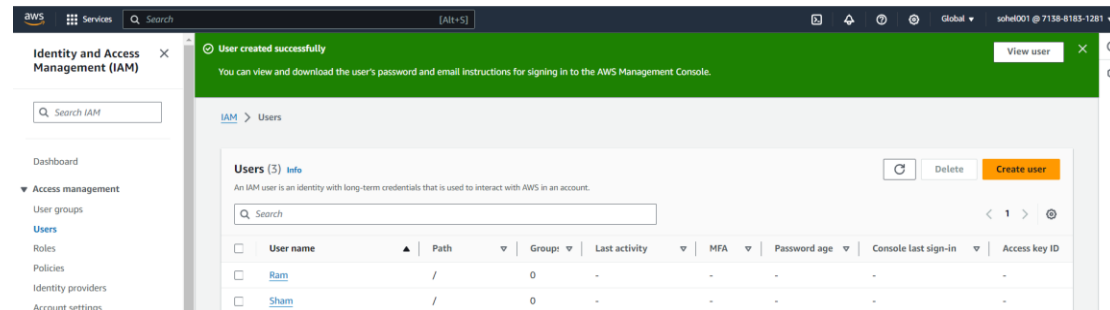


- Change storage class of bucket to Intelligent-Tiering

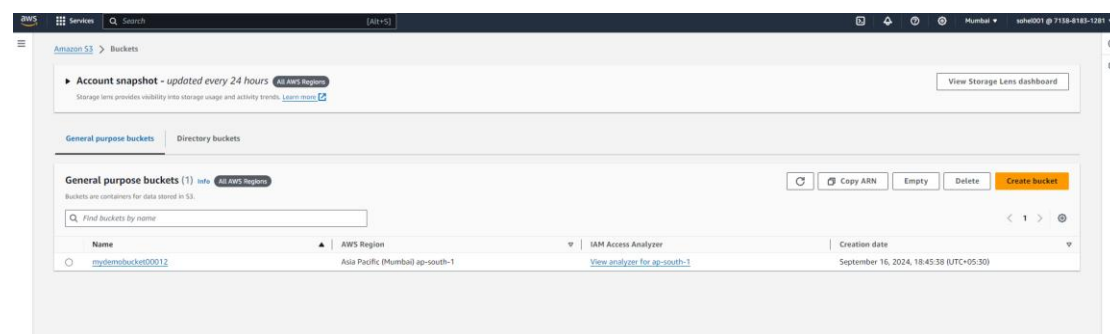


S3 Practical : 2

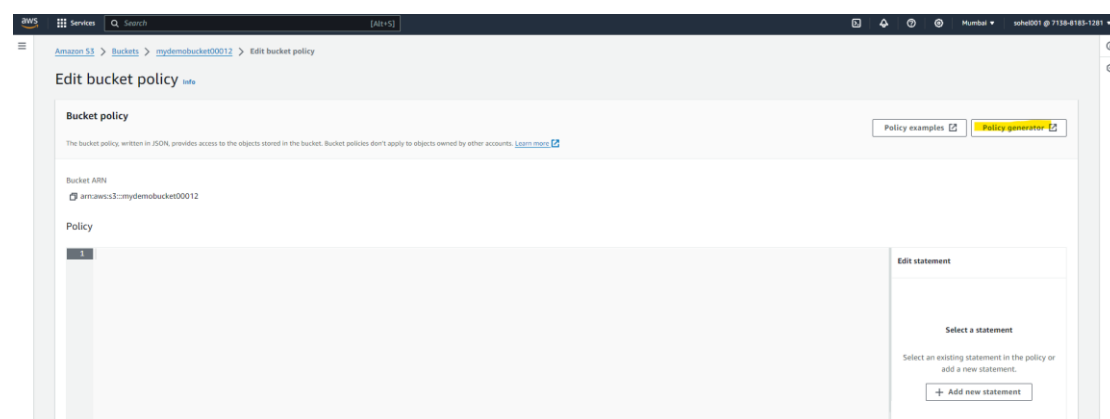
1. Create two users having S3Readonly access



2. Created one bucket



3. Go to the bucket policy and click edit button it will open the tab and click on policy generation button.



4. We have given policy for User it will generate

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to [Amazon Web Services \(AWS\)](#) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

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 should follow the following format: arn:aws:s3:::\${BucketName}/\${KeyName}.
Use a comma to separate multiple values.

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

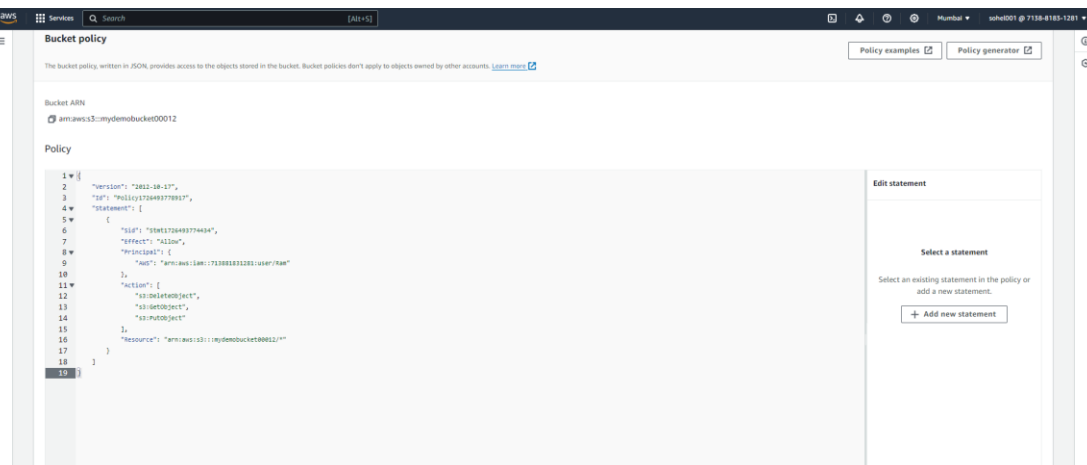
5. The Policy is ready

Policy JSON Document

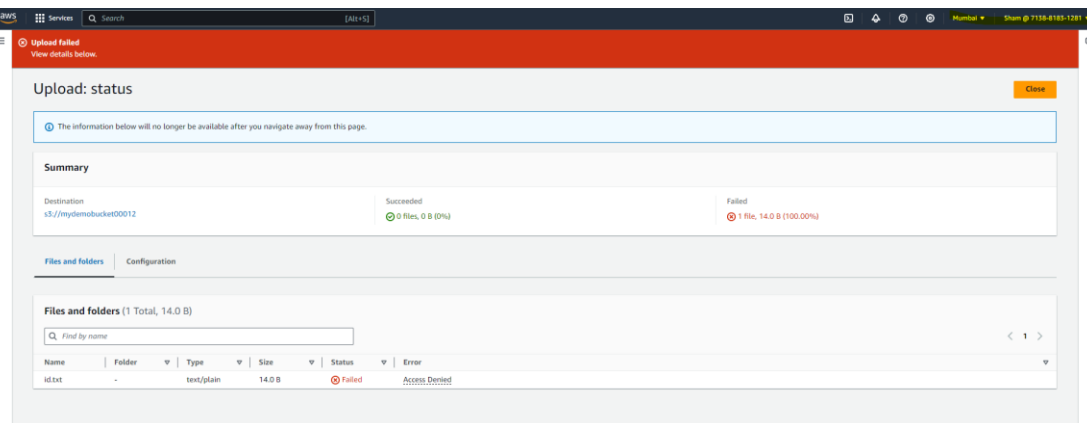
Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected in the policy generator tool**.

```
{
  "Id": "Policy1726493778917",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1726493774434",
      "Action": [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::mydemobucket00012/*",
      "Principal": {
        "AWS": [
          "arn:aws:iam::713881831281:user/Ram"
        ]
      }
    }
  ]
}
```

6. Post the code in bucket and save it



A. trying to get console for the user and creating bucket it won't be able to create.



B. Trying to delete the existing bucket but it won't delete

aws Services Search [Alt+S]

Amazon S3 > Buckets > mydemobucket00012 > Delete bucket

Delete bucket [Info](#)

- ⚠ Deleting a bucket cannot be undone.
- Bucket names are unique. If you delete a bucket, another AWS user can use the name.
- If this bucket is used with a Multi-Region Access Point in an external account, initiate failover before deleting the bucket.
- If this bucket is used with an access point in an external account, the requests made through those access points will fail after you delete this bucket.

[Learn more](#)

Delete bucket "mydemobucket00012"?

To confirm deletion, enter the name of the bucket in the text input field.

mydemobucket00012

❌ **You don't have permission to delete bucket "mydemobucket00012"**

After you or your AWS admin has updated your IAM permissions to allow `s3:DeleteBucket`, choose **delete bucket**. [Learn more about Identity and Access Management in Amazon S3](#)

If you have the `s3:DeleteBucket` permission in your IAM user policy and you cannot delete a bucket, the bucket policy might include a deny statement for `s3:DeleteBucket`. Before you can delete the bucket, you must delete the deny `s3:DeleteBucket` statement or delete the bucket policy.

▶ API response

Hence, that means we cannot add or delete the object in bucket when user having S3Read only access.

7. Now login with the user which we provide policy.

A. We can add the object

aws Services Search [Alt+S]

Upload: status [Close](#)

The information below will no longer be available after you navigate away from this page.

Summary

Destination	s3://mydemobucket00012
Succeeded	1 file, 14.0 B (100.00%)
Failed	0 files, 0 B (0%)

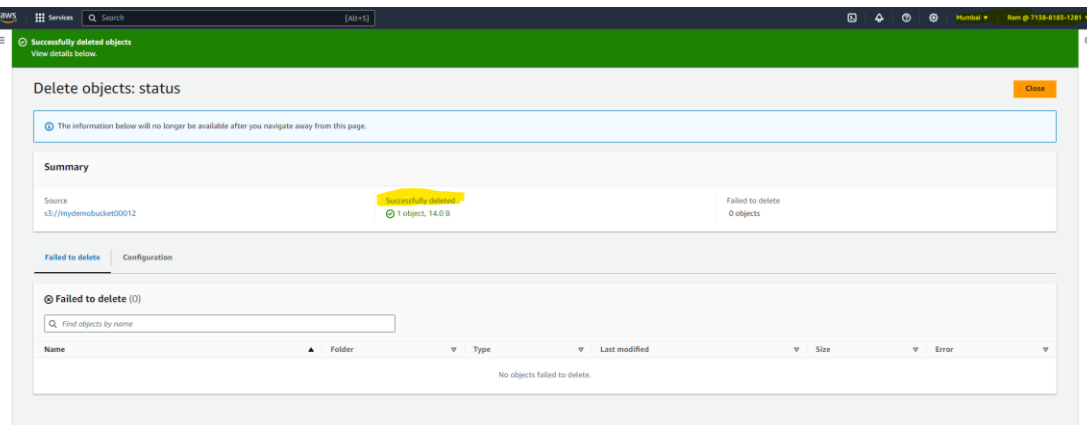
Files and folders

Files and folders (1 Total, 14.0 B)

Find by name

Name	Folder	Type	Size	Status	Error
id.txt	-	text/plain	14.0 B	Succeeded	-

B. We can delete the object.



- Amazon S3 (Simple Storage Service) supports a wide range of use cases, including data backups, content delivery, web hosting, and big data analytics. Key features like versioning, cross-region replication, encryption, and lifecycle management enable users to control and manage their data effectively. With a pay-as-you-go pricing model, Amazon S3 provides an affordable, flexible, and scalable storage solution suitable for businesses of all sizes, from startups to large enterprises.
- In conclusion, Amazon S3 offers a powerful combination of scalability, security, and flexibility, making it a go-to solution for storing and managing data in the cloud.