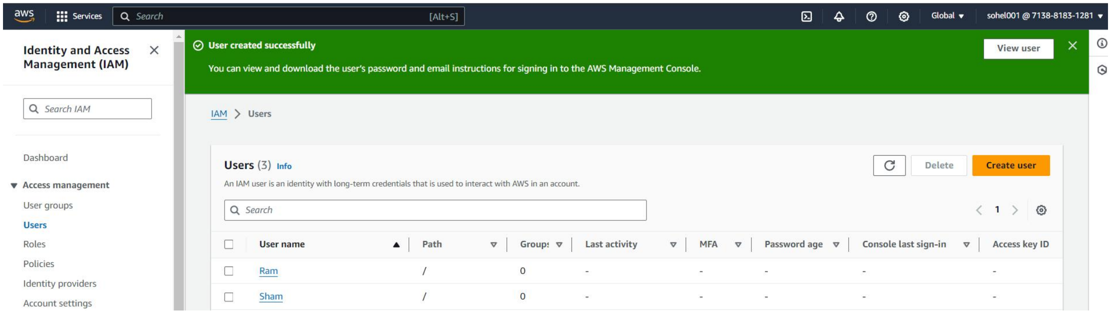
S3 Practical 22 Aug 2024

1. Create two user having S3Readonly access



User created successfully

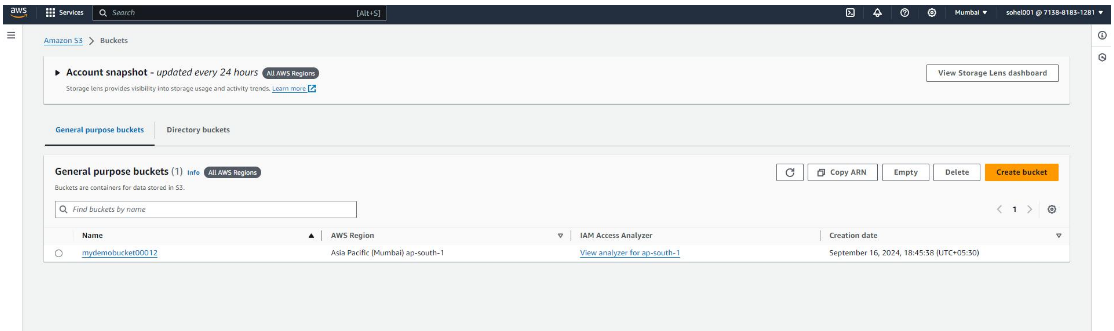
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Users (3) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID
Ram	/	0	-	-	-	-	-
Sham	/	0	-	-	-	-	-

2. Created one bucket



Account snapshot - *updated every 24 hours* All AWS Regions

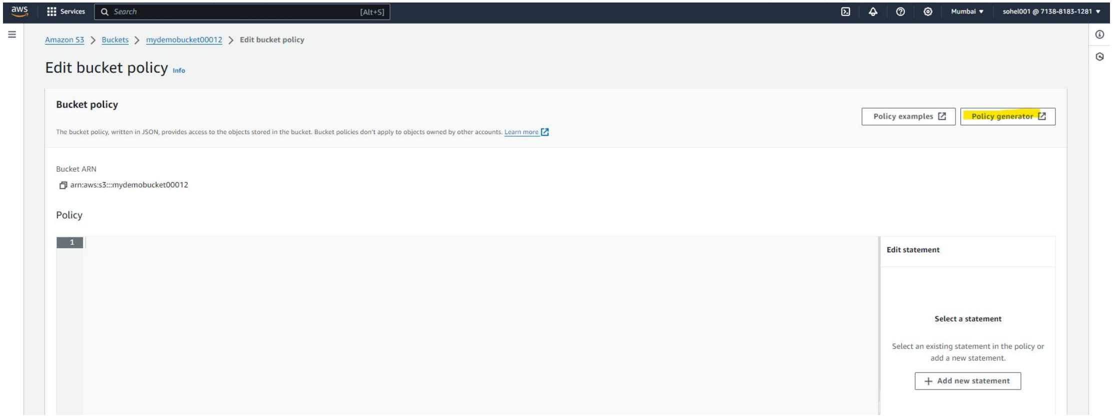
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1) Info All AWS Regions

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
mydemobucket00012	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	September 16, 2024, 18:45:38 (UTC+05:30)

3. Goto the bucket policy and click edit button it will open and click on policy generatior.



Edit bucket policy Info

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

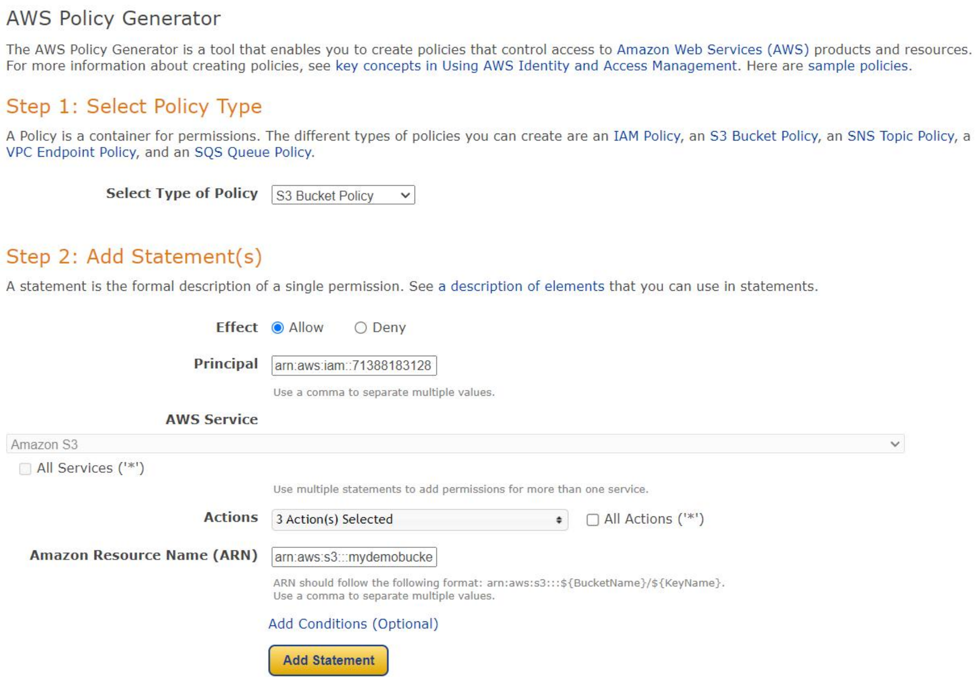
Bucket ARN

arn:aws:s3:::mydemobucket00012

Policy

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

4. We have given policy for Ram 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: arn:aws:iam::71388183128

Use a comma to separate multiple values.

AWS Service: Amazon S3

□ All Services ('*')

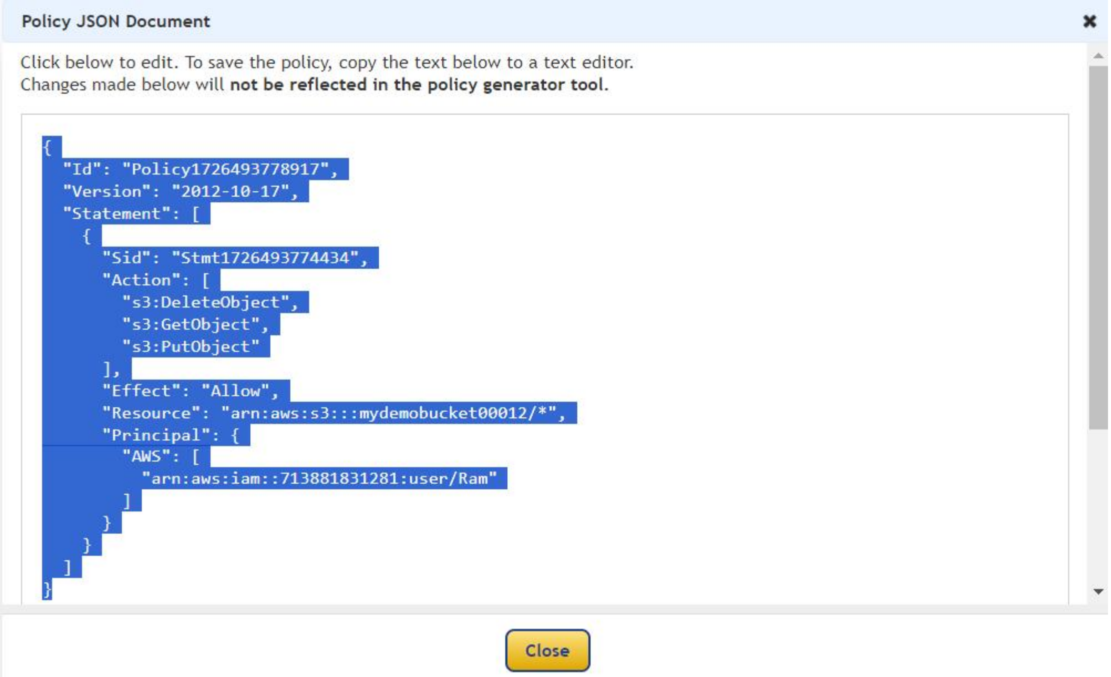
Use multiple statements to add permissions for more than one service.

Actions: 3 Action(s) Selected □ All Actions ('*')

Amazon Resource Name (ARN): arn:aws:s3:::mydemobucke

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

5. Policy is ready



Policy JSON Document

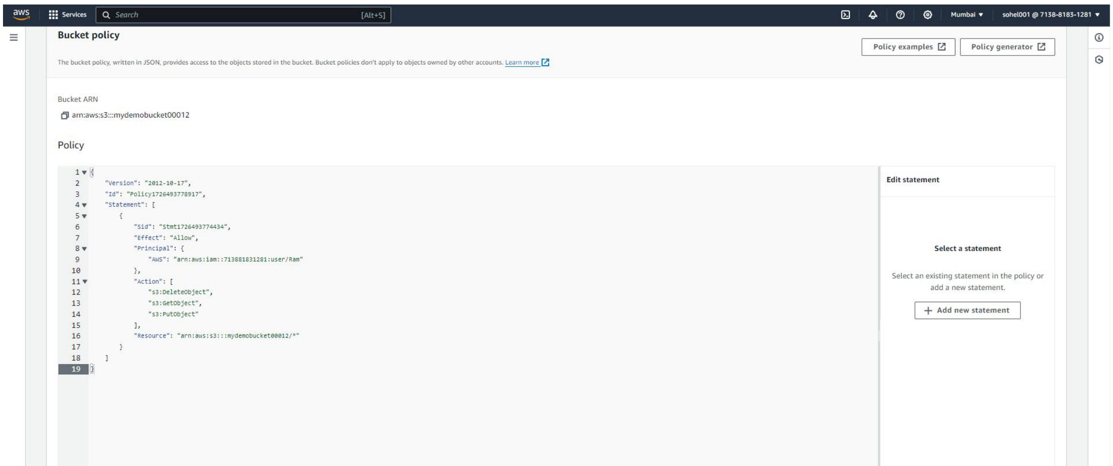
Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected in the policy generator tool.**

```
{
  "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.

7.

8. Post the code in bucket and save it



Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Bucket ARN

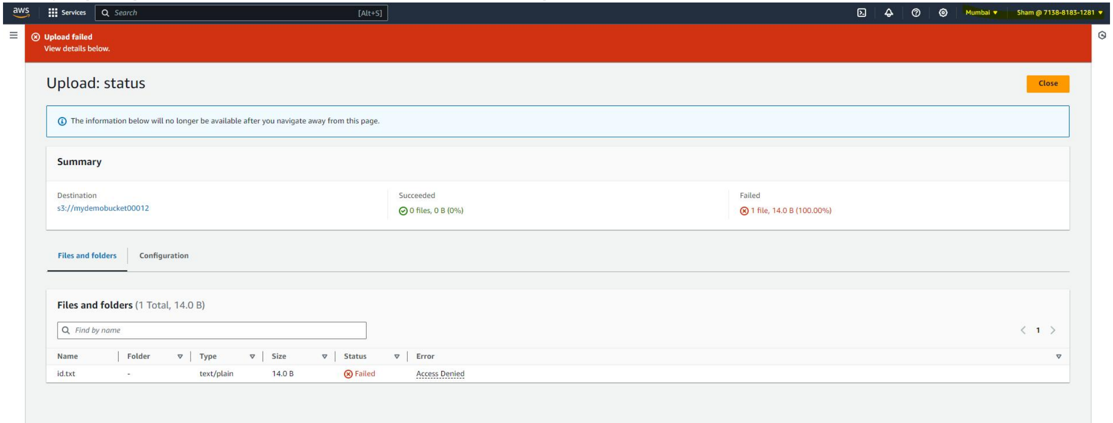
arn:aws:s3:::mydemobucket00012

Policy

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

9. Now,

A. trying to get console for Sham user and creating bucket it wont able to create.



Upload failed
View details below.

Upload: status

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

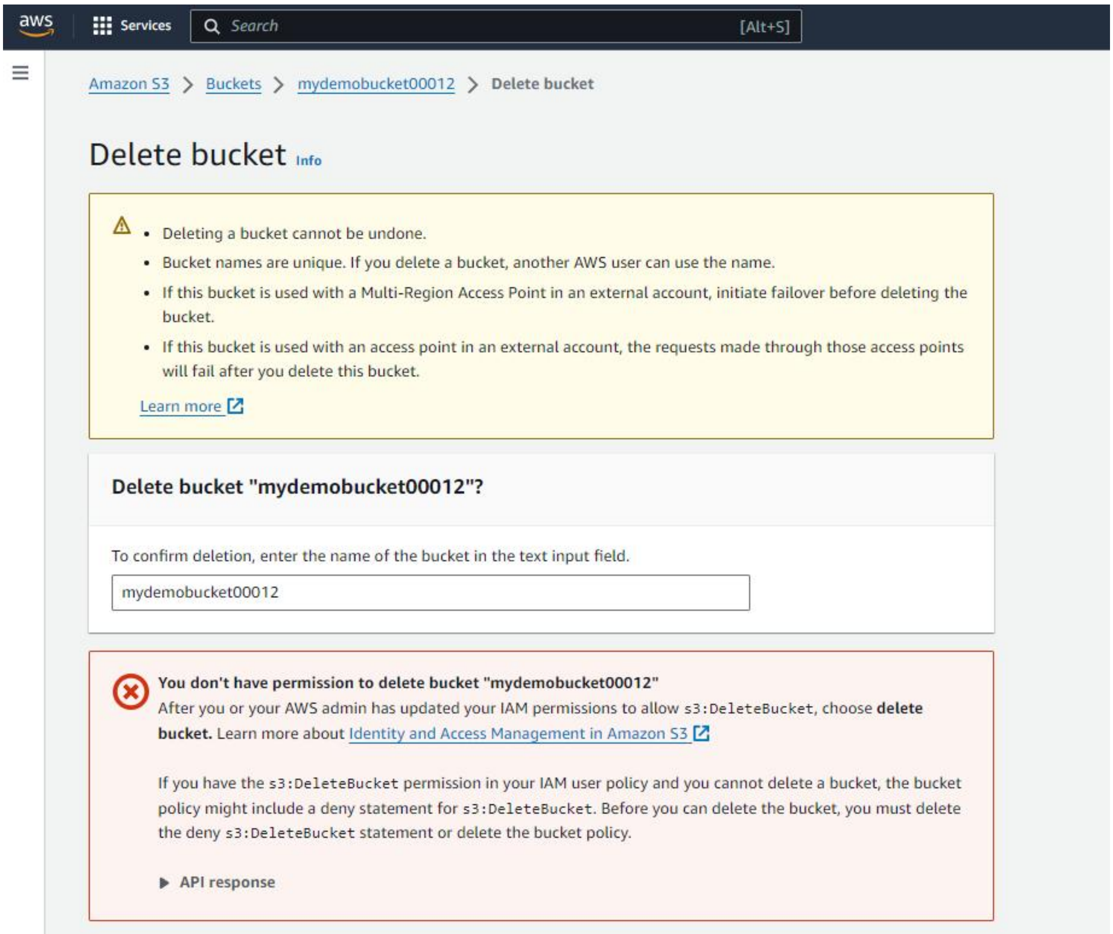
Summary

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

Files and folders (1 Total, 14.0 B)

Name	Folder	Type	Size	Status	Error
id.txt	-	text/plain	14.0 B	Failed	Access Denied

B. Trying to deleted the existing bucket it wont



Delete bucket

- 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

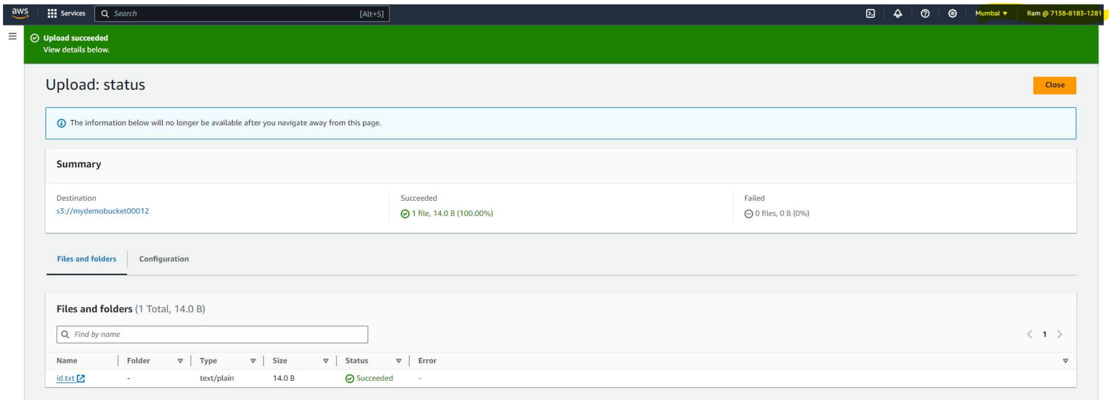
You don't have permission to delete bucket "mydemobucket00012"

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.

C.That means we can not add or delete the object in bucket when user having S3Read only access.

10. Now login with Ram which we provide policy.
A. We can add the object



Upload succeeded
View details below.

Upload: status

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

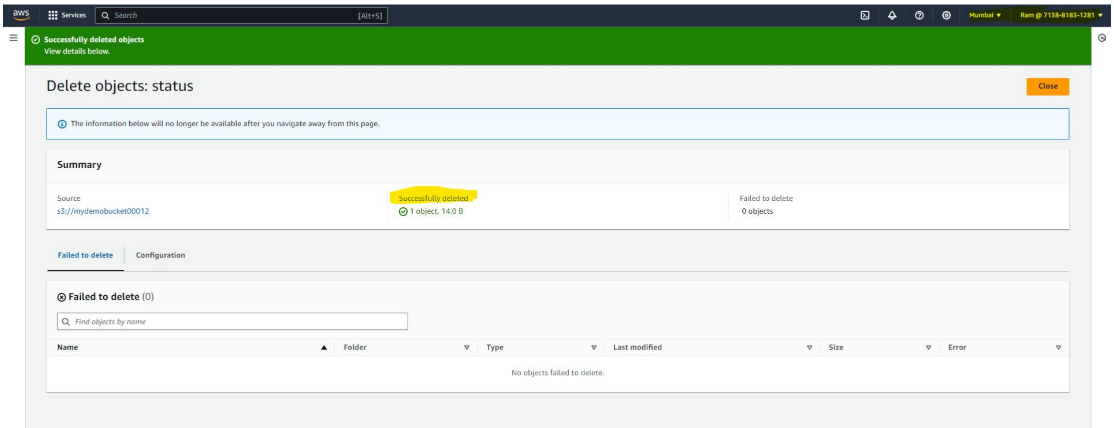
Summary

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

Files and folders (1 Total, 14.0 B)

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

B. We can delete the object.



Successfully deleted objects
View details below.

Delete objects: status

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

Summary

Source	Successfully deleted	Failed to delete
s3://mydemobucket00012	✓ 1 object, 14.0 B	0 objects

Failed to delete (0)

Name ▲	Folder ▽	Type ▽	Last modified ▽	Size ▽	Error ▽

No objects failed to delete.