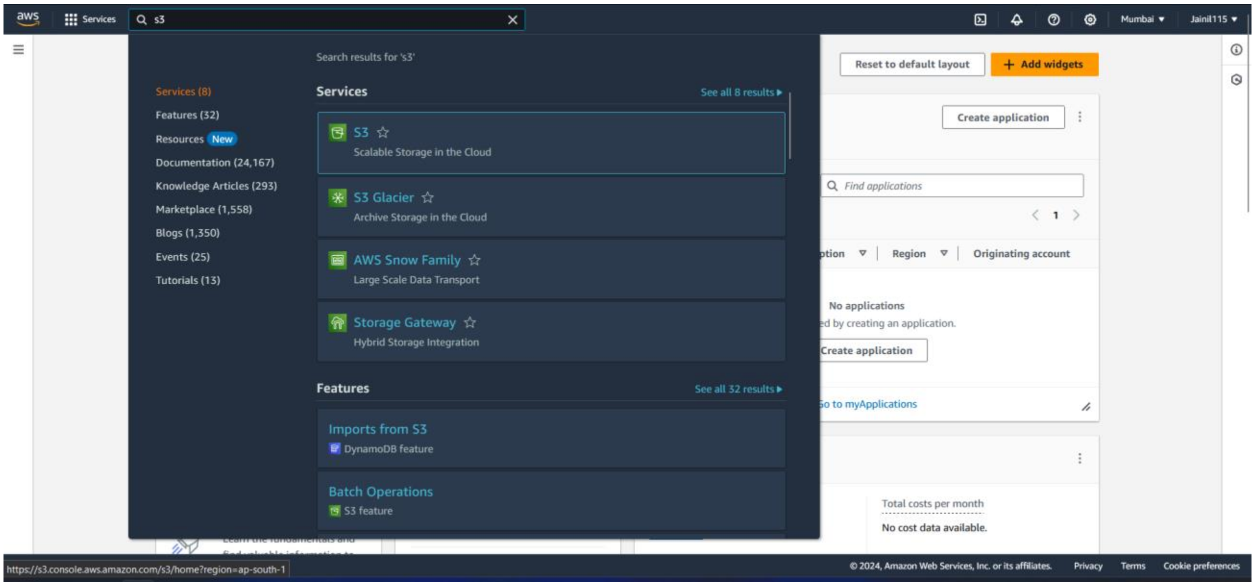
TASK 1: Create an S3 Bucket:

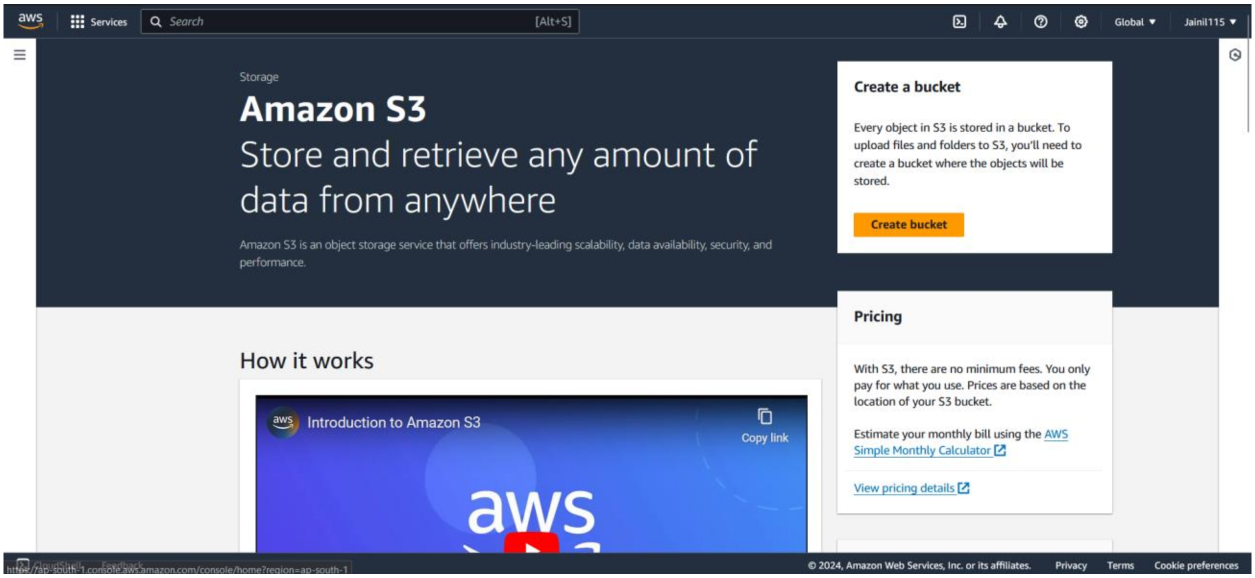
1. **Create a new S3 bucket with a globally unique name.**
2. **Configure bucket policies and access control lists (ACLs) to control permissions.**
3. **Enable versioning for your S3 bucket.**
4. **Upload, modify, and delete objects to observe versioning in action.**

Steps to create S3 Bucket:

1. Search for S3 in AWS Console and select "S3 Scalable Storage in the Cloud".



2. Now click on “Create bucket”.


aws
Services
Search
[Alt+S]
Global ▾
Jainil115 ▾
Storage
Create a bucket
Create bucket
Pricing
How it works
Introduction to Amazon S3
Copy link
aws
https://ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

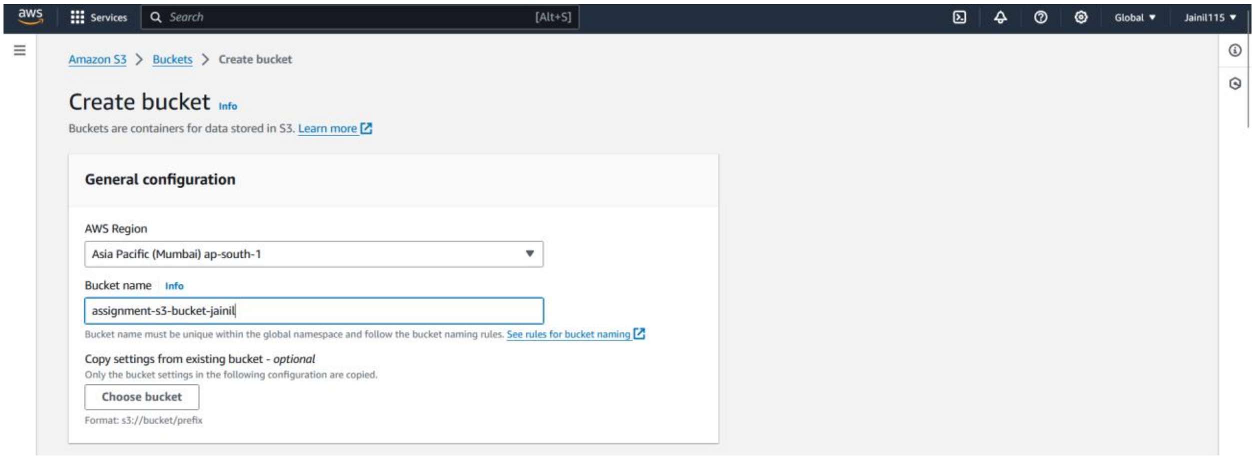
Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

View pricing details

3. Now select region Mumbai and enter a globally unique name “assignment-s3-bucket-jainil”.



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

assignment-s3-bucket-jainil

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

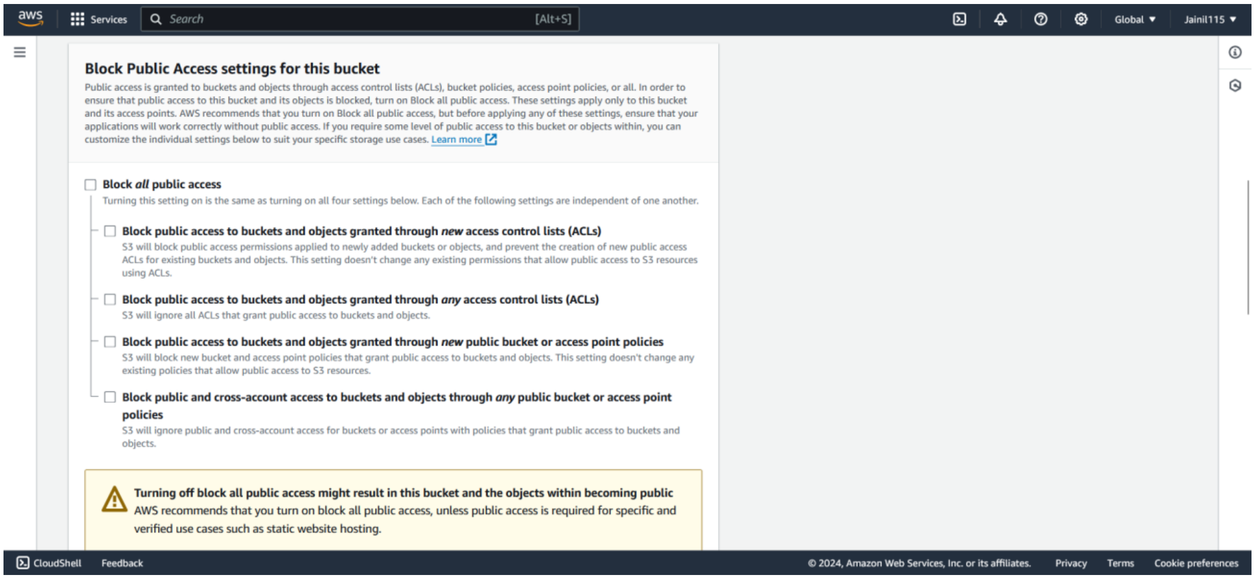
Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

4. Untick Block all public access when creating the bucket to allow accessing files inside s3 bucket publicly, this can be done after the bucket has been created.



Block Public Access settings for this bucket

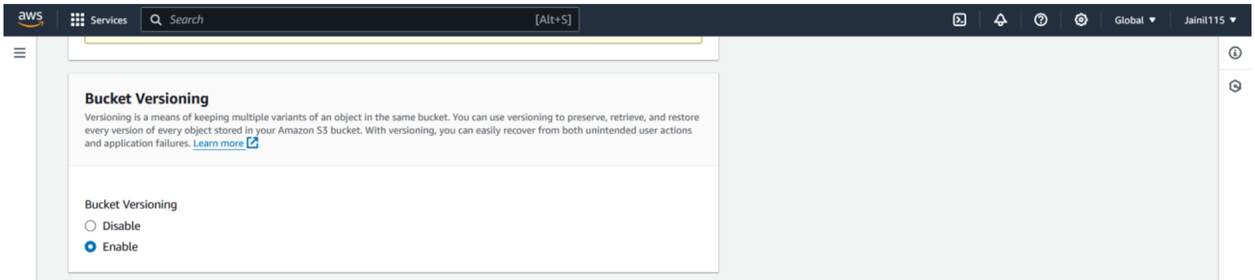
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

☐ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

5. Enable Bucket Versioning:



Bucket Versioning

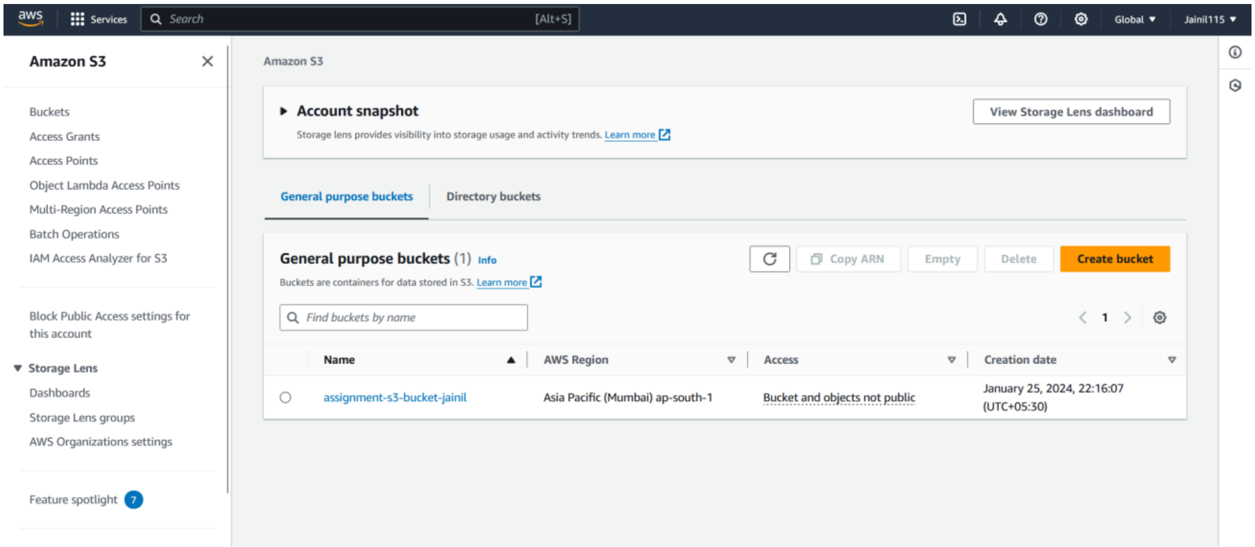
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning

○ Disable

● Enable

S3 Bucket Dashboard:



Amazon S3

▶ Account snapshot

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

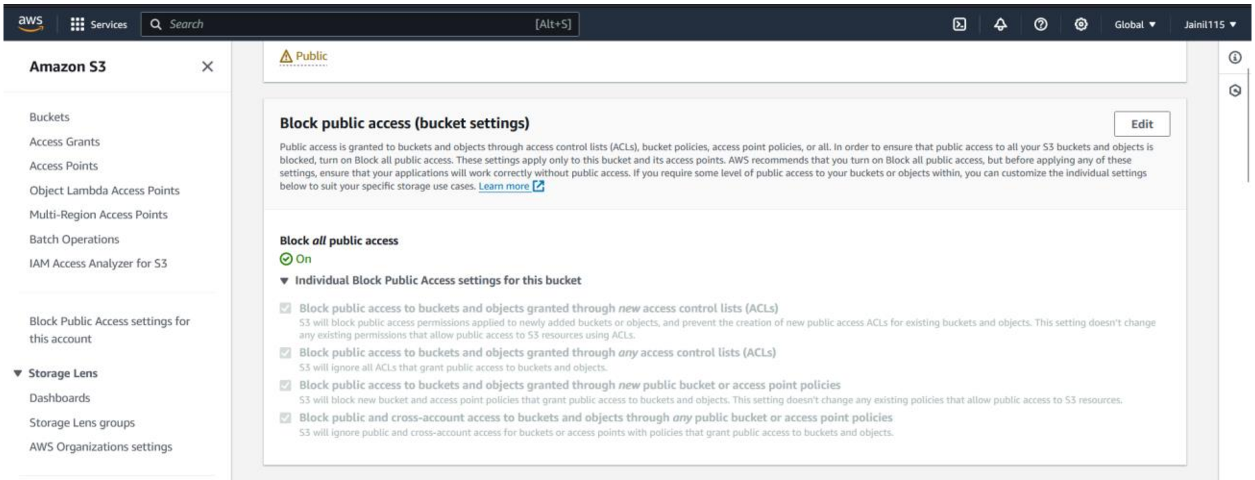
General purpose buckets (1) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	assignment-s3-bucket-jainil	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	January 25, 2024, 22:16:07 (UTC+05:30)

Steps to edit public access:

1. Select the assignment-s3-bucket-jainil then click on permission, inside this tab click on edit on Block public access.


aws
Services
Search
[Alt+S]
Global ▼
Jainil115 ▼
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
▼ Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Edit

⚠ Public

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

Block *all* public access

On

▼ Individual Block Public Access settings for this bucket

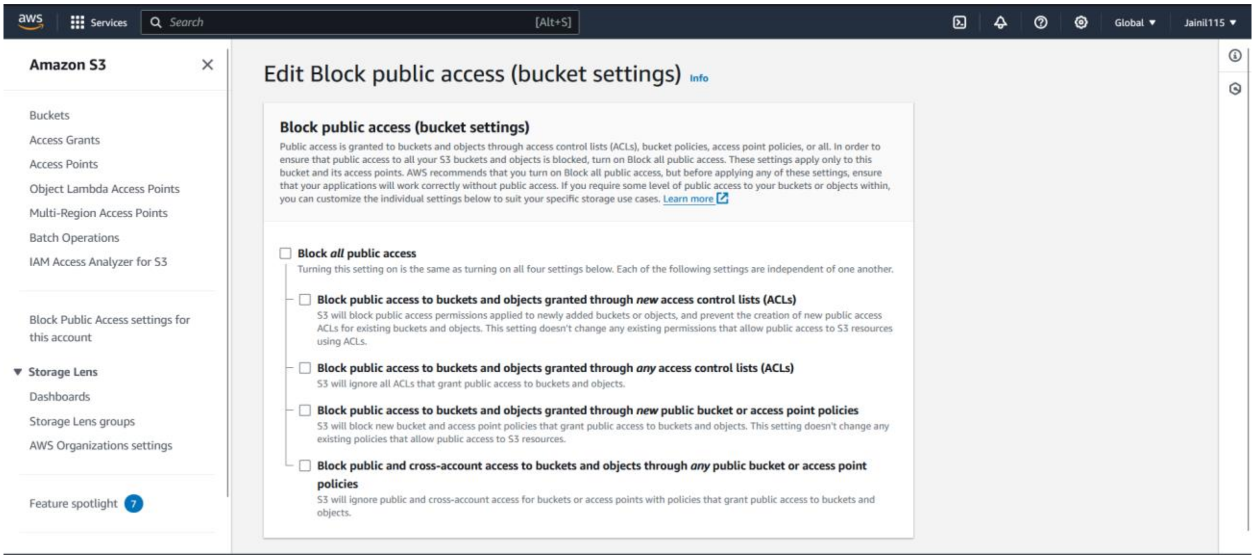
☑ Block public access to buckets and objects granted through *new* access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☑ Block public access to buckets and objects granted through *any* access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.

☑ Block public access to buckets and objects granted through *new* public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☑ Block public and cross-account access to buckets and objects through *any* public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

2. After clicking on edit, untick Block all public access and click on save changes, Then enter confirm.



Edit Block public access (bucket settings) Info

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

□ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

□ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

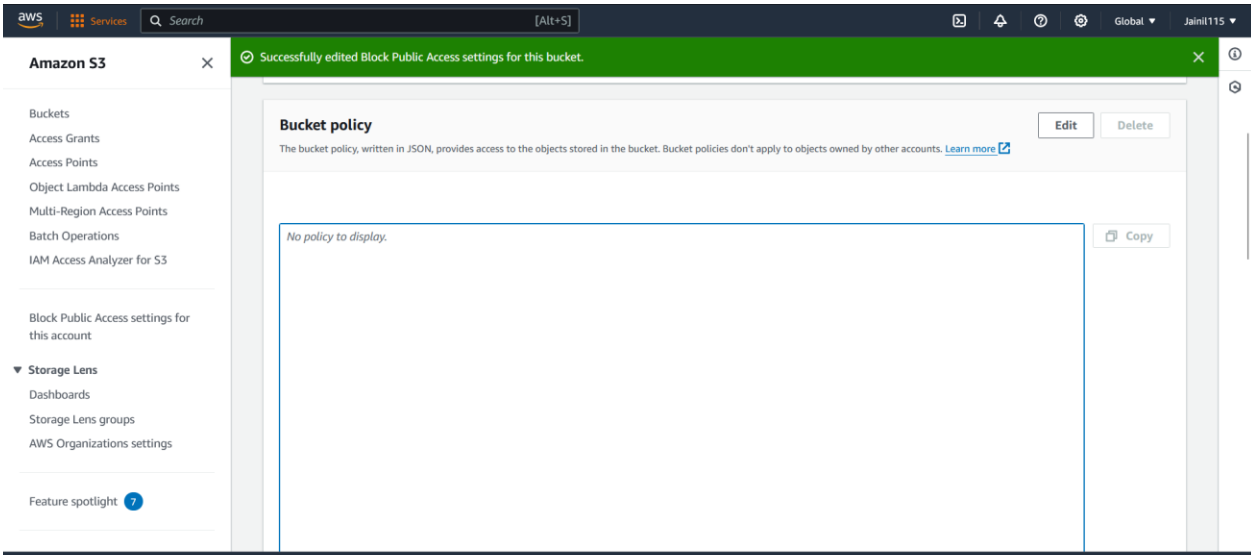
□ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.

□ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

□ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

To configure bucket policies to control permissions:

1. Click on edit inside Bucket policy tab.



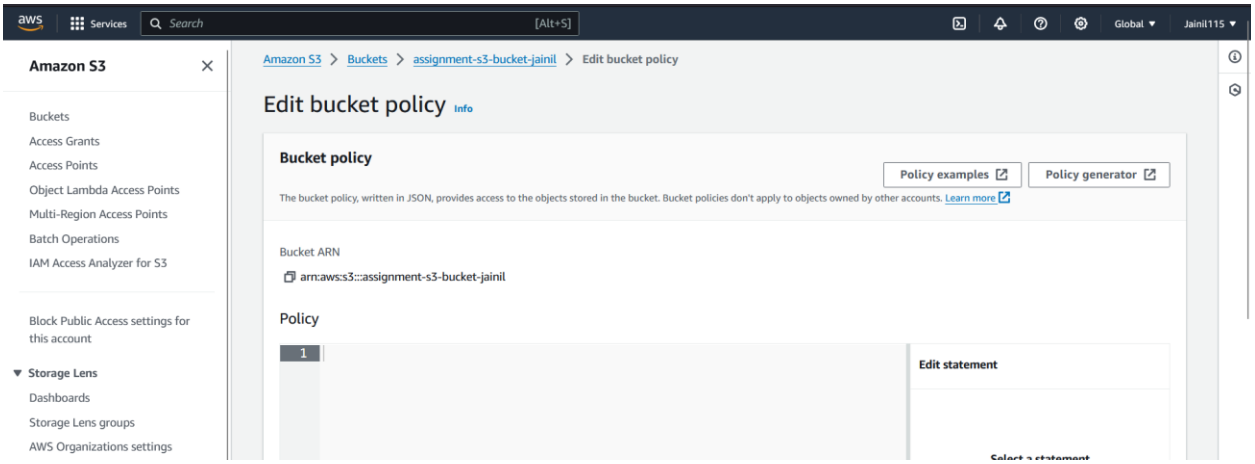
Successfully edited Block Public Access settings for this bucket.

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

No policy to display.

2. Inside edit mode click on policy generator.


aws
Services
Search
[Alt+S]
Global
Jainil115
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Amazon S3 > Buckets > assignment-s3-bucket-jainil > Edit bucket policy
Info
Policy examples
Policy generator
Learn more
1

Edit bucket policy

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

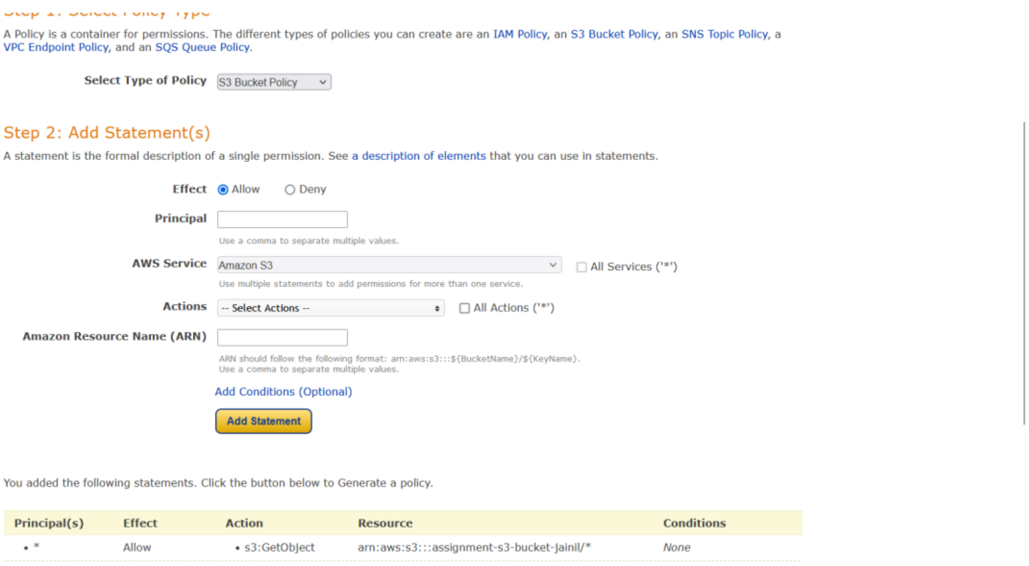
arn:aws:s3:::assignment-s3-bucket-jainil

Policy

Edit statement

Select a statement

3. Policy generator provides gui for creating policies. Now select type of policy "S3 Bucket Policy".
choose effect: "allow", Principal: "*", Actions: "GetObject", Amazon Resource Name (ARN): "arn:aws:s3:::assignment-s3-bucket-jainil/*". Then click on Add Statement and click on generate policy.



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: -- Select Actions -- □ All Actions ('*')

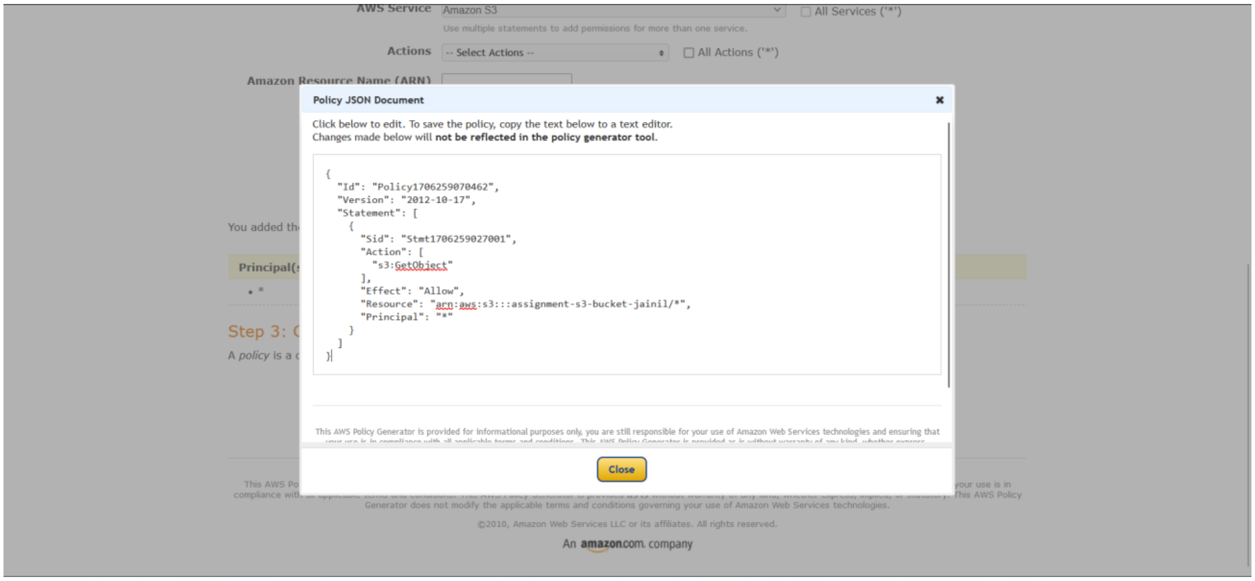
Amazon Resource Name (ARN):

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

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• *	Allow	• s3:GetObject	arn:aws:s3:::assignment-s3-bucket-jainil/*	None

4. Then Copy the json text and paste it in the Edit bucket policy page, then click on Save Changes.



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.**

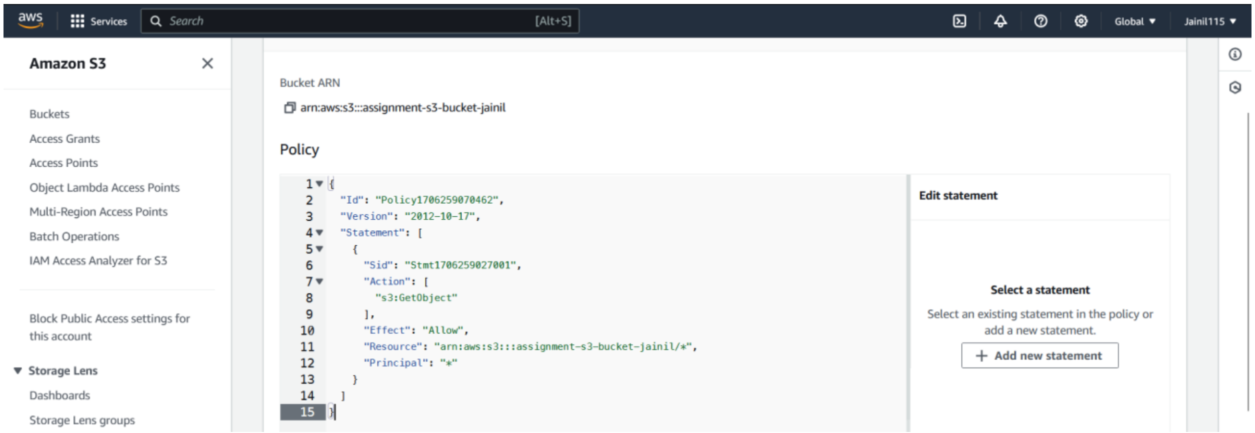
```
{
  "Id": "Policy1706259070462",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1706259027001",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::assignment-s3-bucket-jainil/*",
      "Principal": "*"
    }
  ]
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that

Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.

An amazon.com company



Bucket ARN

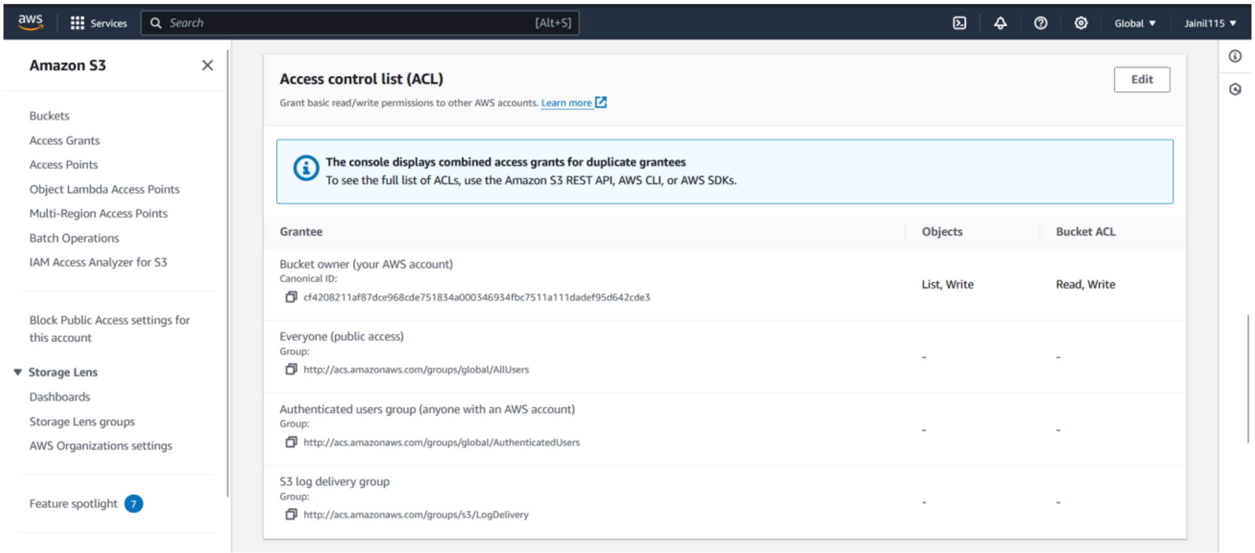
arn:aws:s3:::assignment-s3-bucket-jainil

Policy

```
{
  "Id": "Policy1706259070462",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1706259027001",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::assignment-s3-bucket-jainil/*",
      "Principal": "*"
    }
  ]
}
```

To configure access control lists (ACLs) to control permissions:

1. Scroll Down in Permission of s3 bucket find Access Control List and click on edit.



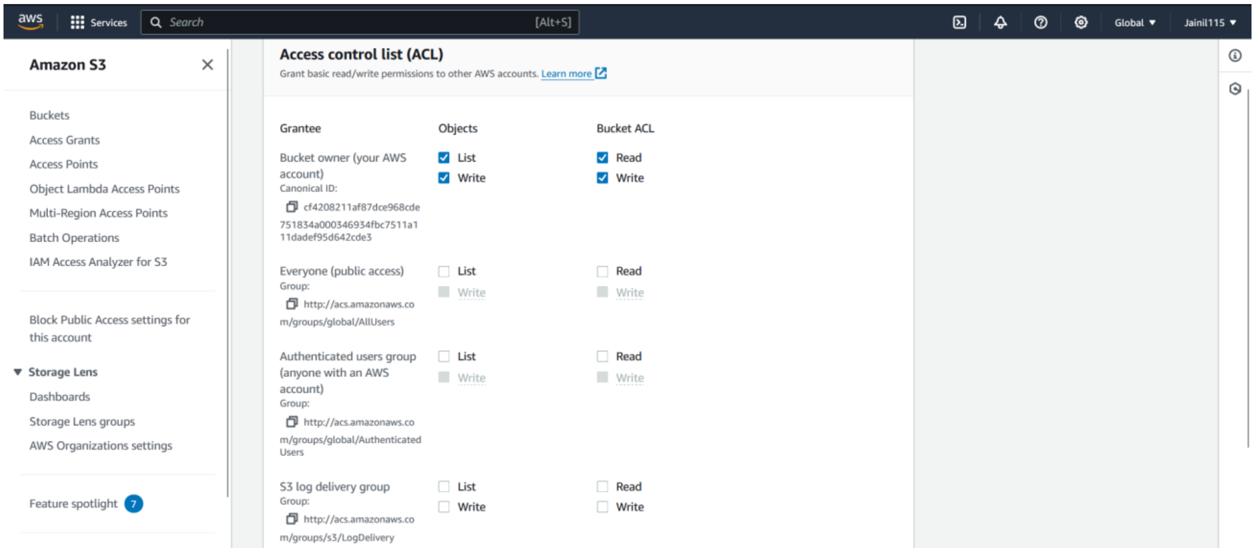
Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. Learn more

The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: cf4208211af87dce968cde751834a000346934fbc7511a111dadef95d642cde3	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	-	-

2. Now configure access control list to control list, read, write permission about objects and Bucket ACL. After configuring ACL click on “Save changes”.

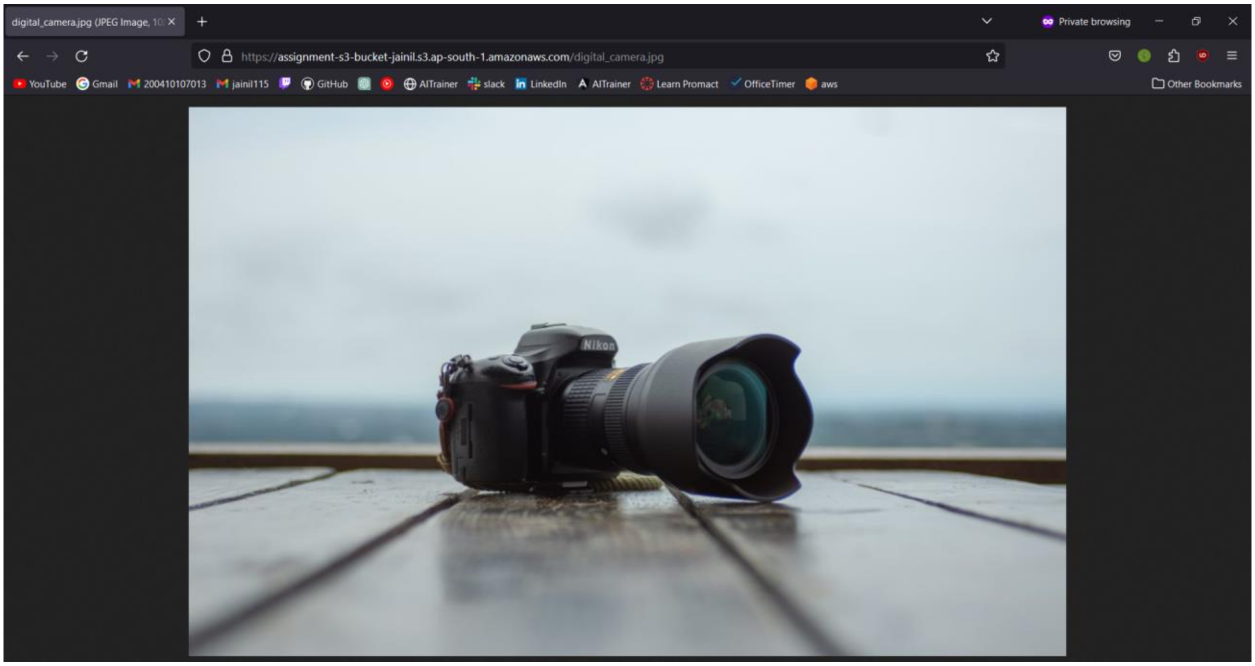


Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. Learn more

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: cf4208211af87dce968cde751834a000346934fbc7511a111dadef95d642cde3	☑ List ☑ Write	☑ Read ☑ Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	□ List □ Write	□ Read □ Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	□ List □ Write	□ Read □ Write
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	□ List □ Write	□ Read □ Write

Check if s3 object is accessible:

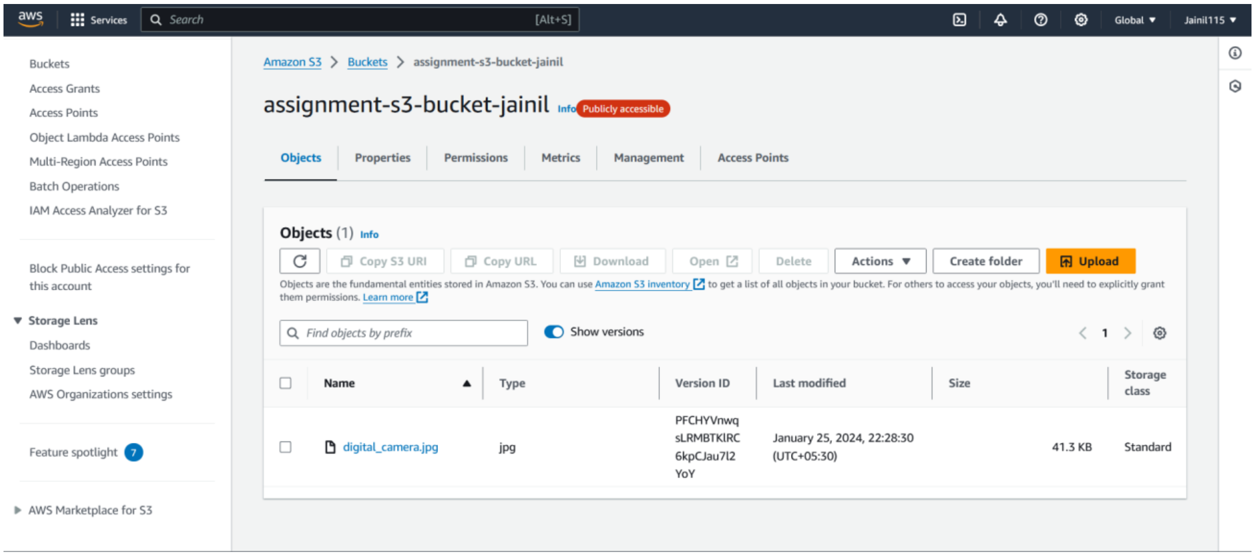


https://assignment-s3-bucket-jainil.s3.ap-south-1.amazonaws.com/digital_camera.jpg

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

Uploading Image:

In assignment-s3-bucket-jainil click on upload and then click on add file and select digital_camera.jpg to upload it to s3 bucket. This created a new version id which is visible in the image.



Amazon S3 > Buckets > assignment-s3-bucket-jainil

assignment-s3-bucket-jainil Info Publicly accessible

Objects (1) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

● Show versions

< 1 >

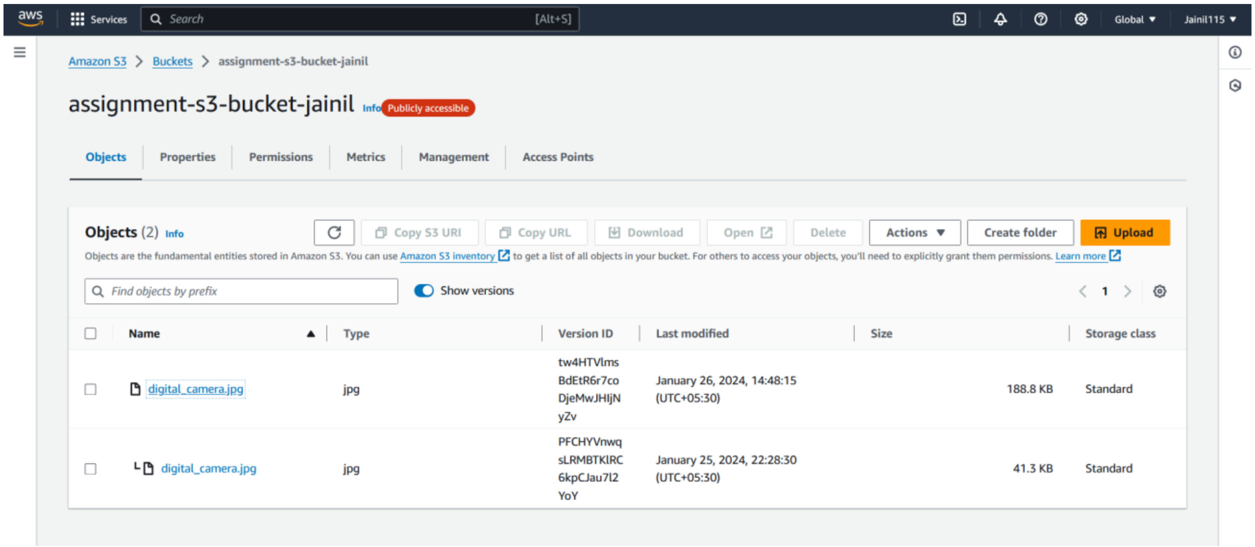
□	Name ▲	Type	Version ID	Last modified	Size	Storage class
□	digital_camera.jpg	jpg	PFCHYVnwq sLRMBTKIRC 6kpCJau7l2 YoY	January 25, 2024, 22:28:30 (UTC+05:30)	41.3 KB	Standard

Modifying Image:

Click on upload in assignment-s3-bucket-jainil and click on add file then select another digital_camera.jpg to replace existing image.

Existing Image:

Modified Image:



assignment-s3-bucket-jainil

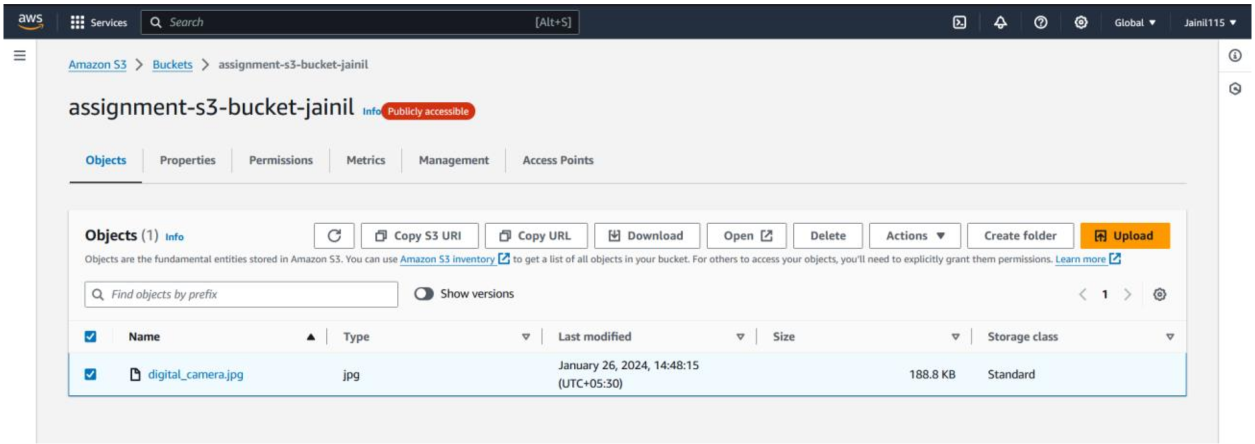
Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

	Name	Type	Version ID	Last modified	Size	Storage class
□	digital_camera.jpg	jpg	tw4HTVlms BdEtR6r7co DjeMwJHIjN yZv	January 26, 2024, 14:48:15 (UTC+05:30)	188.8 KB	Standard
□	└ digital_camera.jpg	jpg	PFCHYVnwq sLRMBTKlRC 6kpCJau7l2 YoY	January 25, 2024, 22:28:30 (UTC+05:30)	41.3 KB	Standard

Delete:

To delete a s3 object select that object and click on delete. Now confirm the deletion by writing delete and click on Delete object.

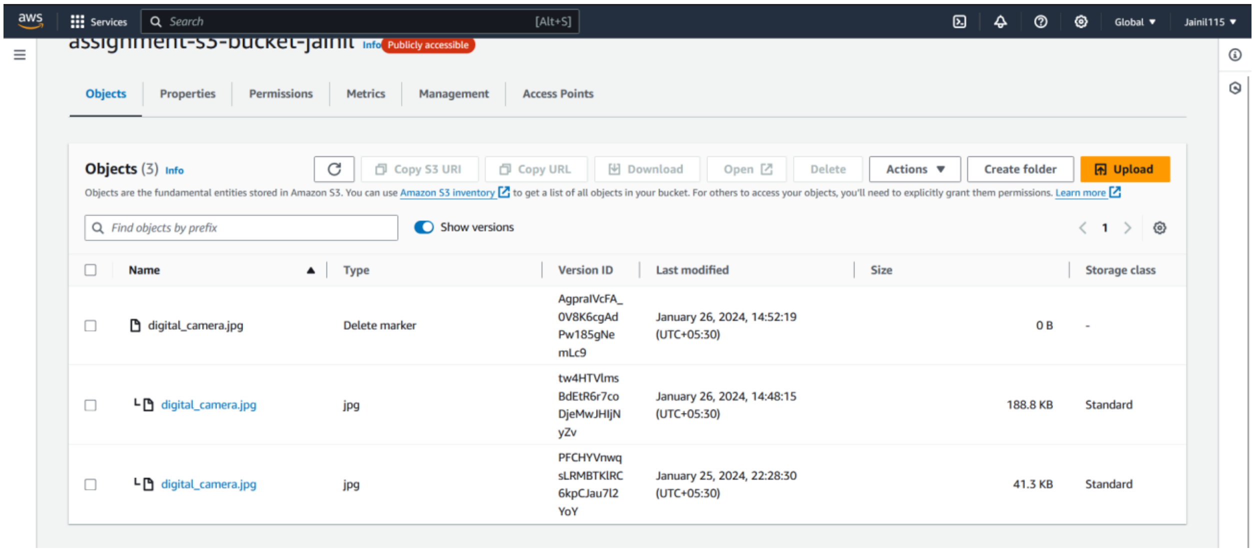


assignment-s3-bucket-jainil

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

☑	Name	Type	Last modified	Size	Storage class
☑	digital_camera.jpg	jpg	January 26, 2024, 14:48:15 (UTC+05:30)	188.8 KB	Standard



assignment-s3-bucket-jainil

Objects (3)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name ▲	Type	Version ID	Last modified	Size	Storage class
□	digital_camera.jpg	Delete marker	AgpraIVcFA_0V8K6cgAdPw185gNemLc9	January 26, 2024, 14:52:19 (UTC+05:30)	0 B	-
□	└ digital_camera.jpg	jpg	tw4HTVlmsBdEtR6r7coDjeMwJHIjNyZv	January 26, 2024, 14:48:15 (UTC+05:30)	188.8 KB	Standard
□	└ digital_camera.jpg	jpg	PFCHYVnwqsLRMBTKlRC6kpCJau7l2YoY	January 25, 2024, 22:28:30 (UTC+05:30)	41.3 KB	Standard