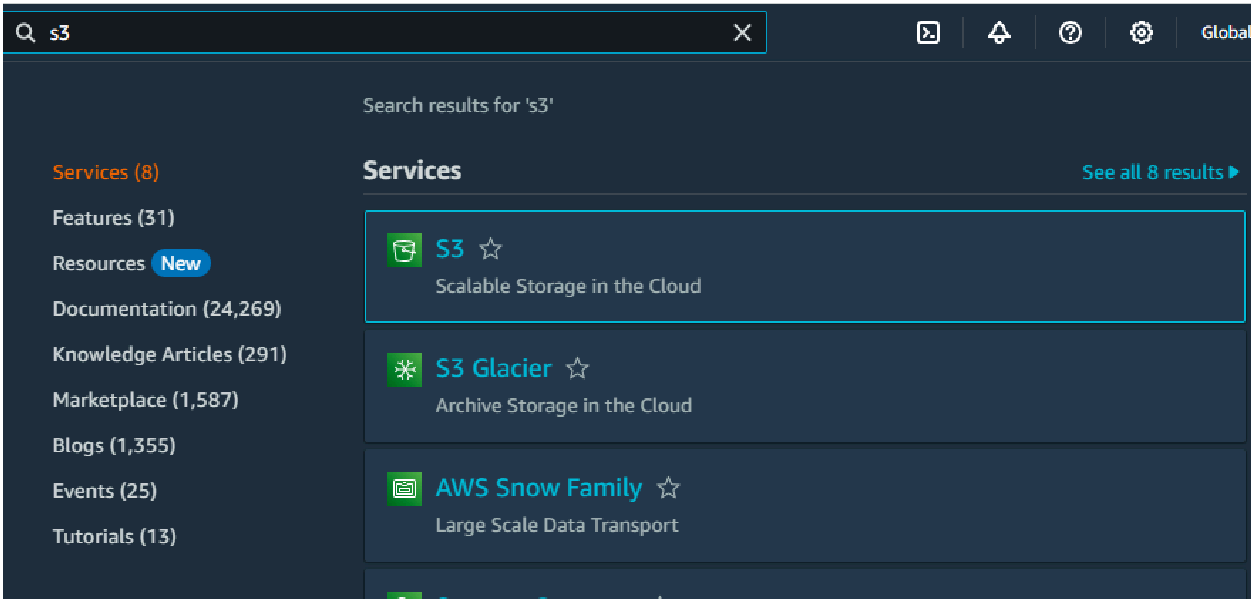
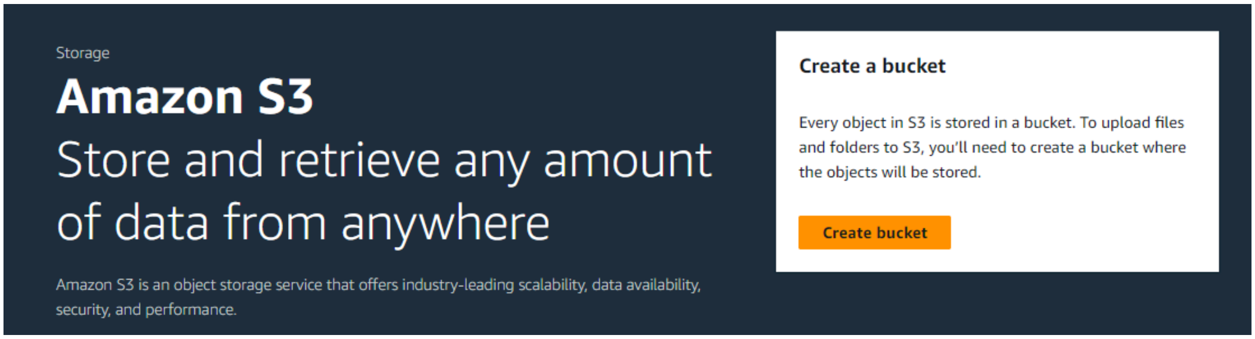
Search for S3 in AWS services.



Click on S3


Storage

Amazon S3

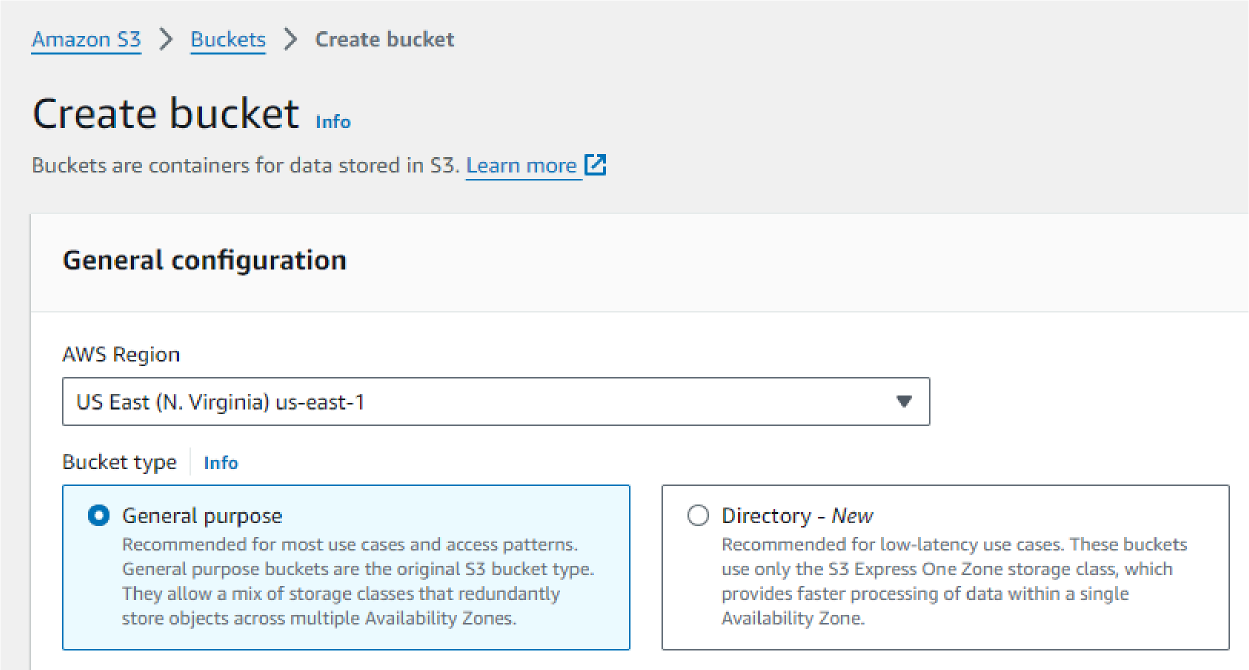
Store and retrieve any amount of data from anywhere

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

Create a bucket

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.

Click on create Bucket



Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

AWS Region

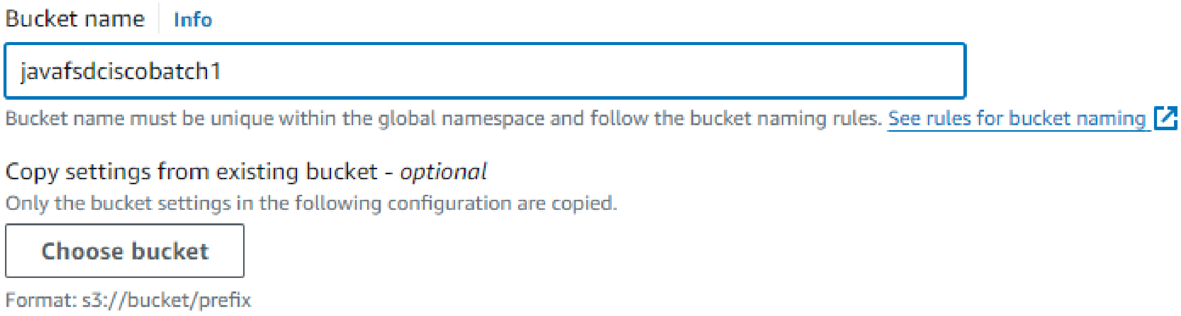
US East (N. Virginia) us-east-1

Bucket type Info

● General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

○ Directory - *New*
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Select us-east-1 region and General purpose bucket type
Give Unique name to your s3 bucket



Bucket name Info

javafsdciscobatch1

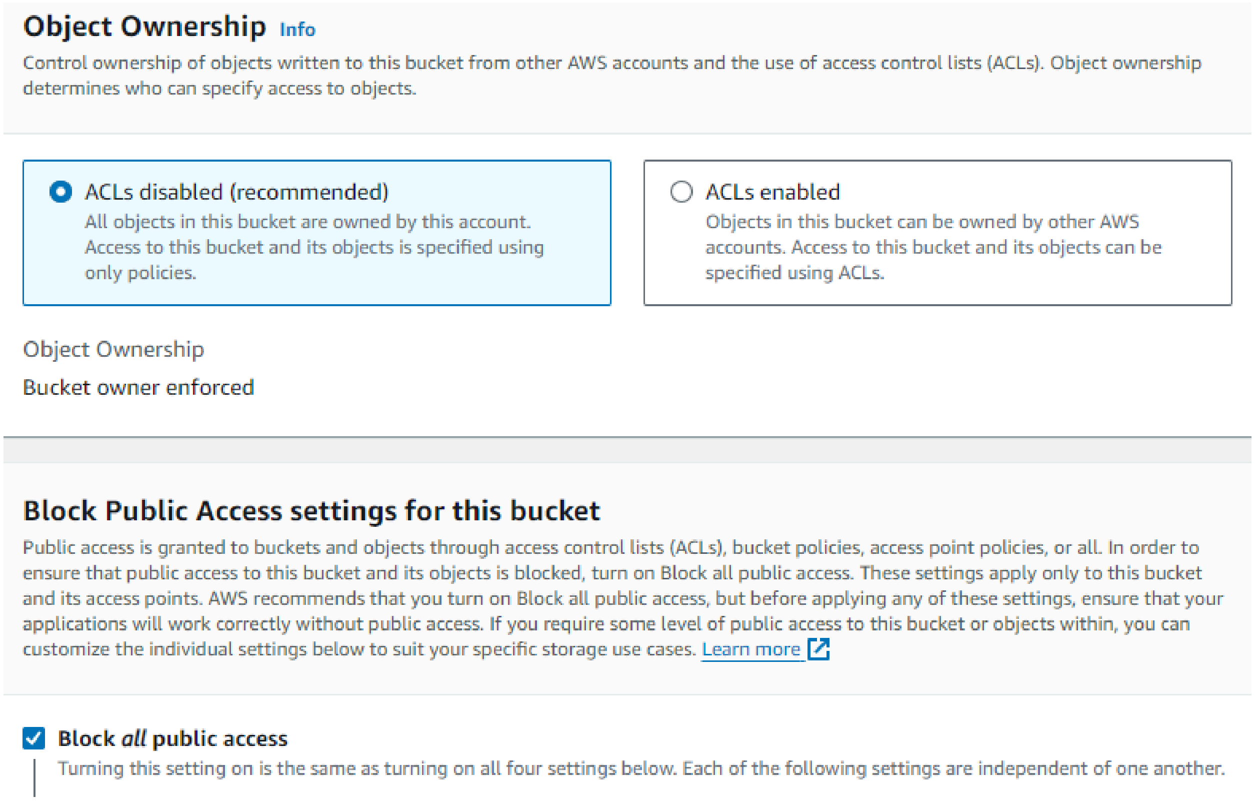
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

If you want to copy some existing bucket to this bucket then from that dropdown select the existing bucket.



Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

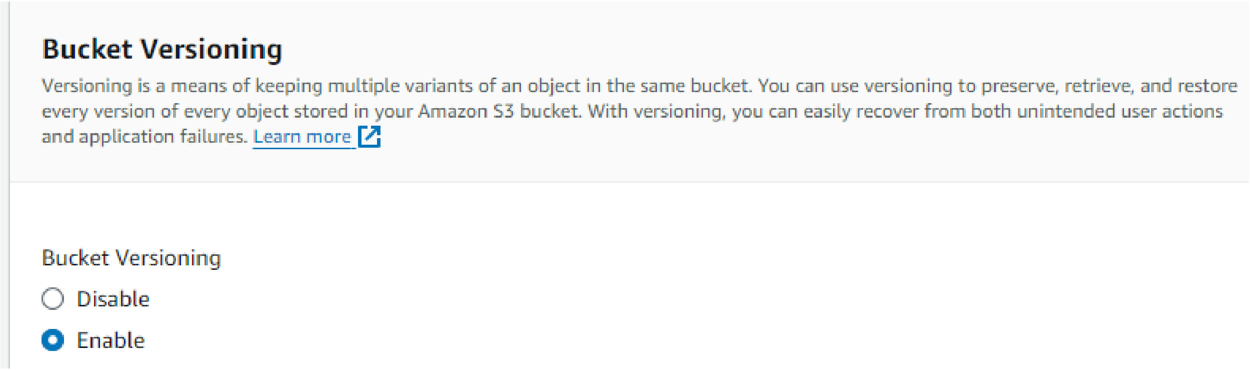
Object Ownership
Bucket owner enforced

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.

ACL - Access control list disabled and , block all public access.
Enable Bucket versioning

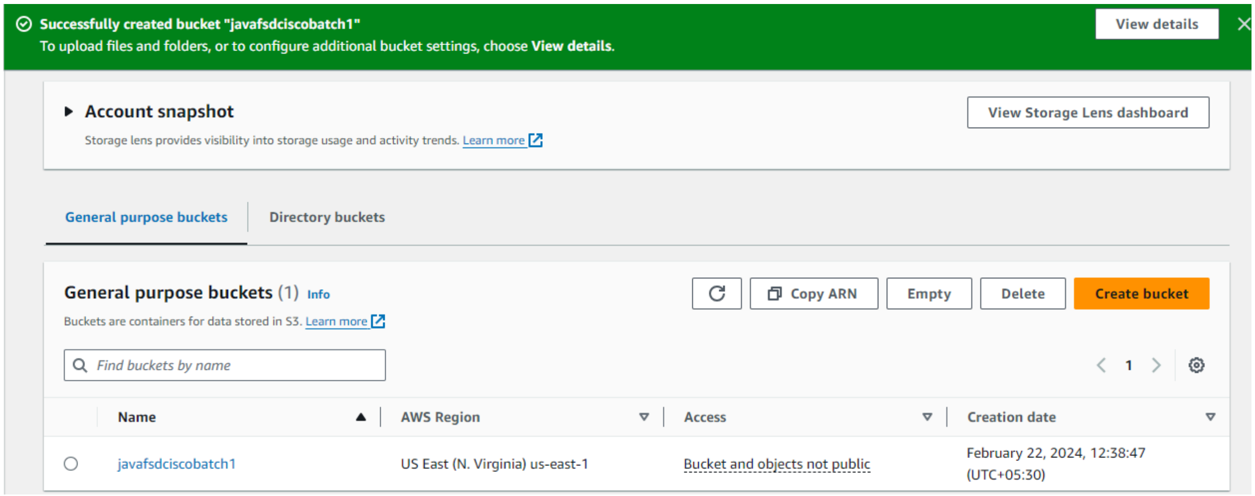


Bucket Versioning

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

Tags are optional so you can leave it and also Continue with this default encryption.
Click on create bucket button.



Successfully created bucket "javafsdciscobatch1"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

▸ **Account snapshot**

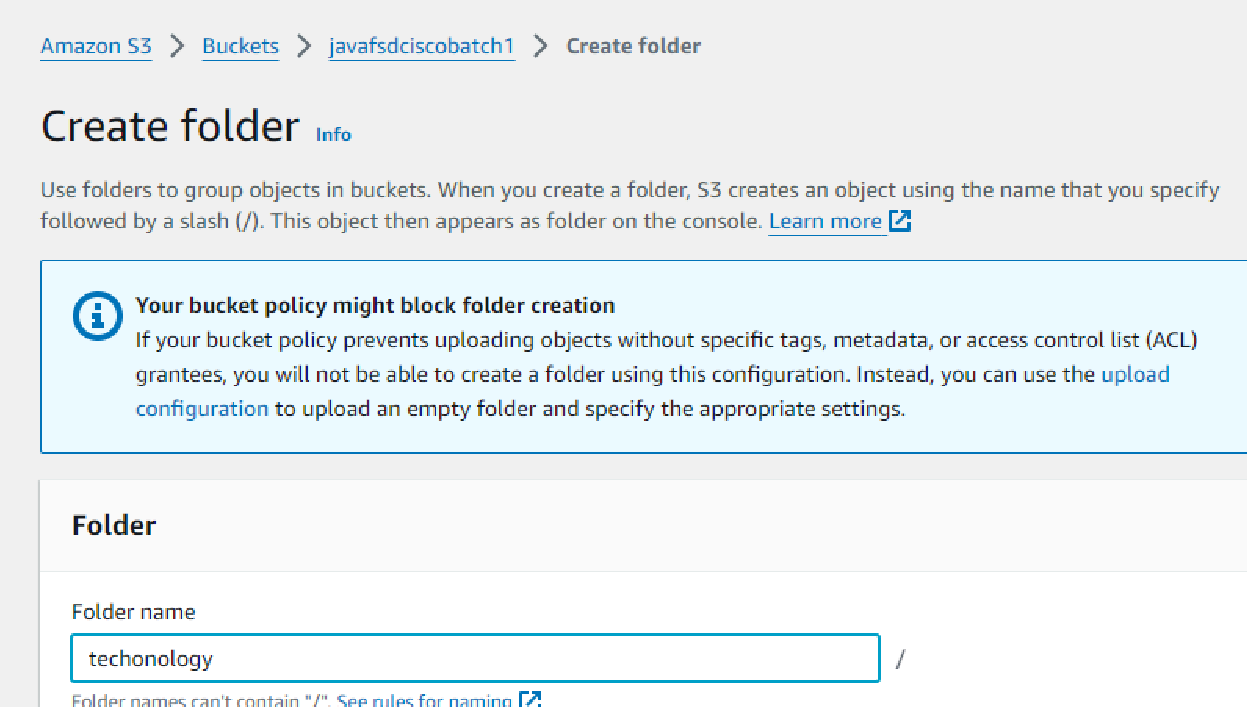
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1) Info

Buckets are containers for data stored in S3. Learn more

	Name ▲	AWS Region ▽	Access ▽	Creation date ▽
○	javafsdciscobatch1	US East (N. Virginia) us-east-1	Bucket and objects not public	February 22, 2024, 12:38:47 (UTC+05:30)

Click on the bucket and see the bucket security, details and objects etc..
Click on create folder and create folder named technologies.



Amazon S3 > Buckets > javafsdciscobatch1 > Create folder

Create folder Info

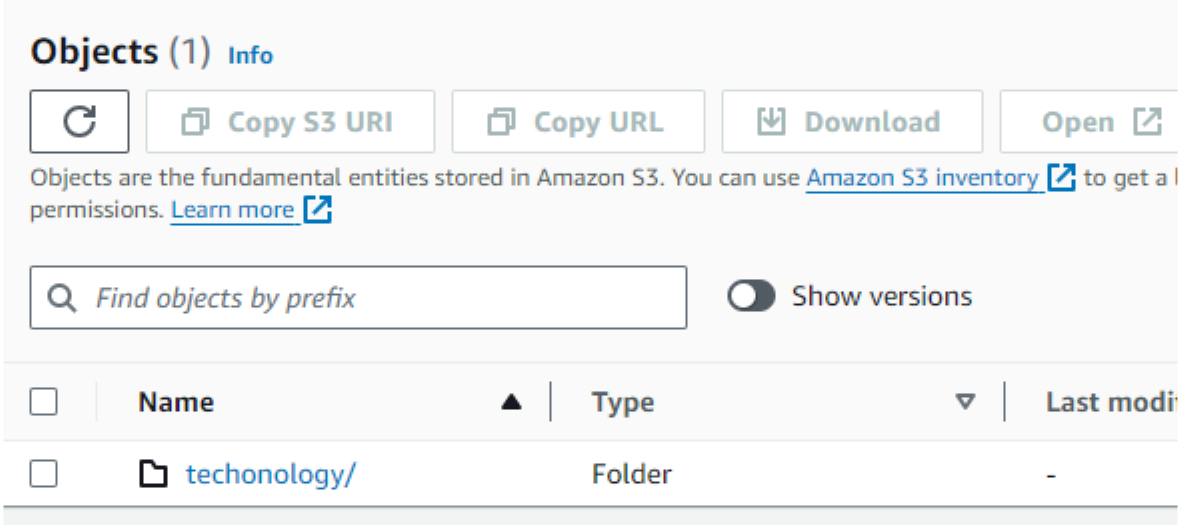
Use folders to group objects in buckets. When you create a folder, S3 creates an object using the name that you specify followed by a slash (/). This object then appears as folder on the console. Learn more

Your bucket policy might block folder creation
If your bucket policy prevents uploading objects without specific tags, metadata, or access control list (ACL) grantees, you will not be able to create a folder using this configuration. Instead, you can use the upload configuration to upload an empty folder and specify the appropriate settings.

Folder

Folder name: techonology /

Folder names can't contain "/". See rules for naming

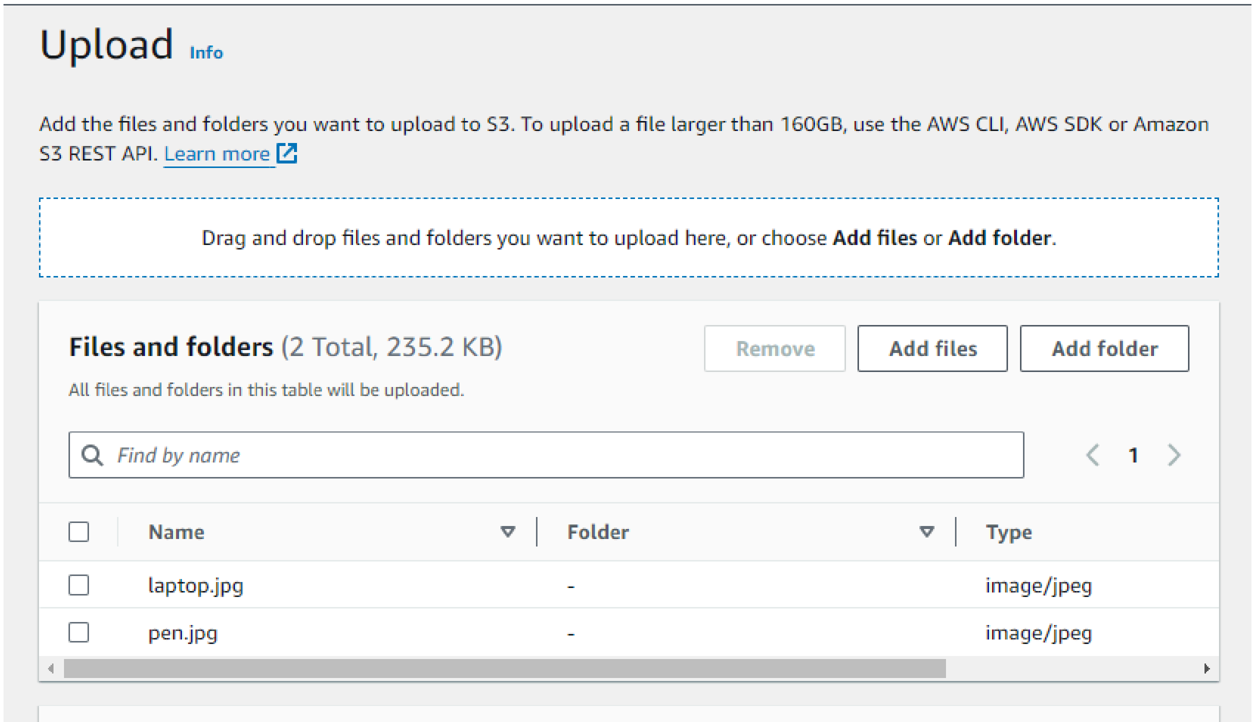


Objects (1) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a l
permissions. Learn more

□	Name	Type	Last modi
□	techonology/	Folder	-

Click on technology and add some files to it.
Click on upload and select multiple files or folder as per requirement.



Upload Info

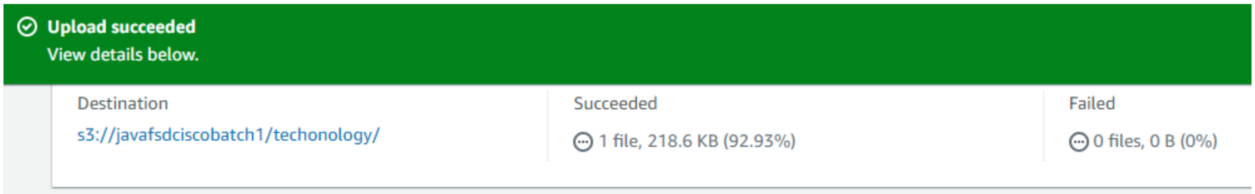
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (2 Total, 235.2 KB)

All files and folders in this table will be uploaded.

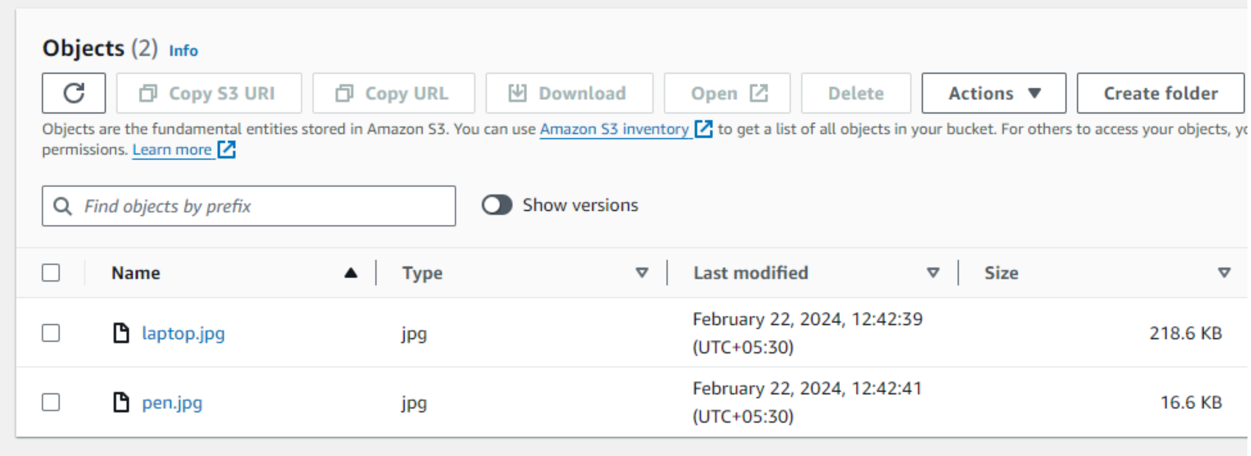
□	Name	Folder	Type
□	laptop.jpg	-	image/jpeg
□	pen.jpg	-	image/jpeg



Upload succeeded
View details below.

Destination	Succeeded	Failed
s3://javafsdciscobatch1/techonology/	1 file, 218.6 KB (92.93%)	0 files, 0 B (0%)

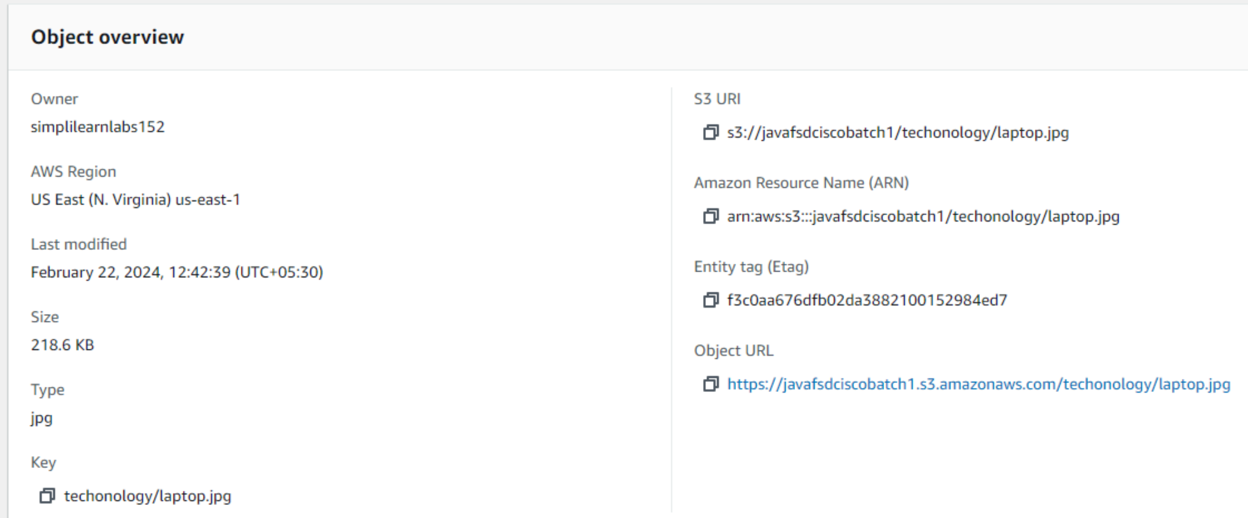
See uploaded objects.



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, yo
permissions. Learn more

□	Name	Type	Last modified	Size
□	laptop.jpg	jpg	February 22, 2024, 12:42:39 (UTC+05:30)	218.6 KB
□	pen.jpg	jpg	February 22, 2024, 12:42:41 (UTC+05:30)	16.6 KB

Click on any object and check object details.



Owner
simplilearnlabs152

AWS Region
US East (N. Virginia) us-east-1

Last modified
February 22, 2024, 12:42:39 (UTC+05:30)

Size
218.6 KB

Type
jpg

Key
techonology/laptop.jpg

S3 URI
s3://javafsdciscobatch1/techonology/laptop.jpg

Amazon Resource Name (ARN)
arn:aws:s3:::javafsdciscobatch1/techonology/laptop.jpg

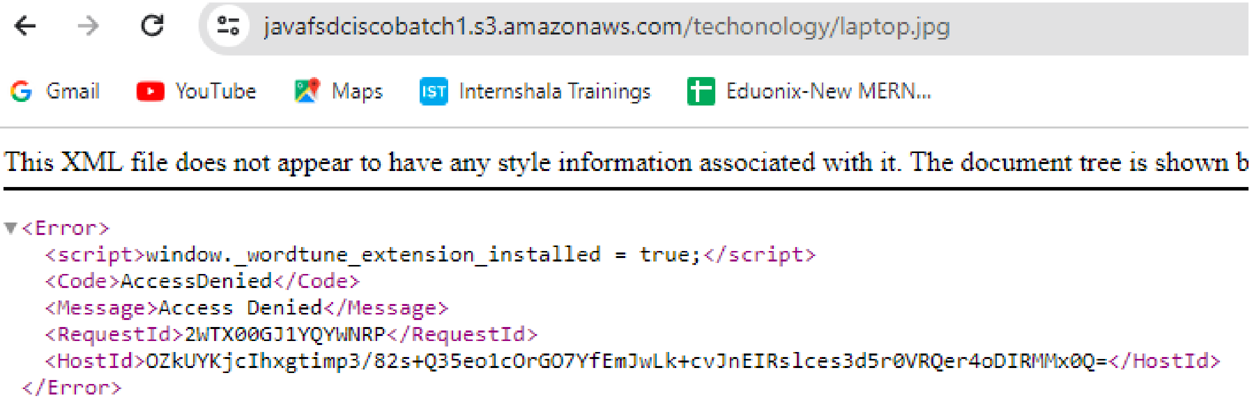
Entity tag (Etag)
f3c0aa676dfb02da3882100152984ed7

Object URL
https://javafsdciscobatch1.s3.amazonaws.com/techonology/laptop.jpg

You can see the link generated for Object in Object URL
https://javafsdciscobatch1.s3.amazonaws.com/techonology/laptop.jpg

Here javafsdciscobatch1 is bucket name
/tochnology/laptop.jpg is the folder name and filename

If you try to access that link the access denied error you can see in browser.



This XML file does not appear to have any style information associated with it. The document tree is shown b

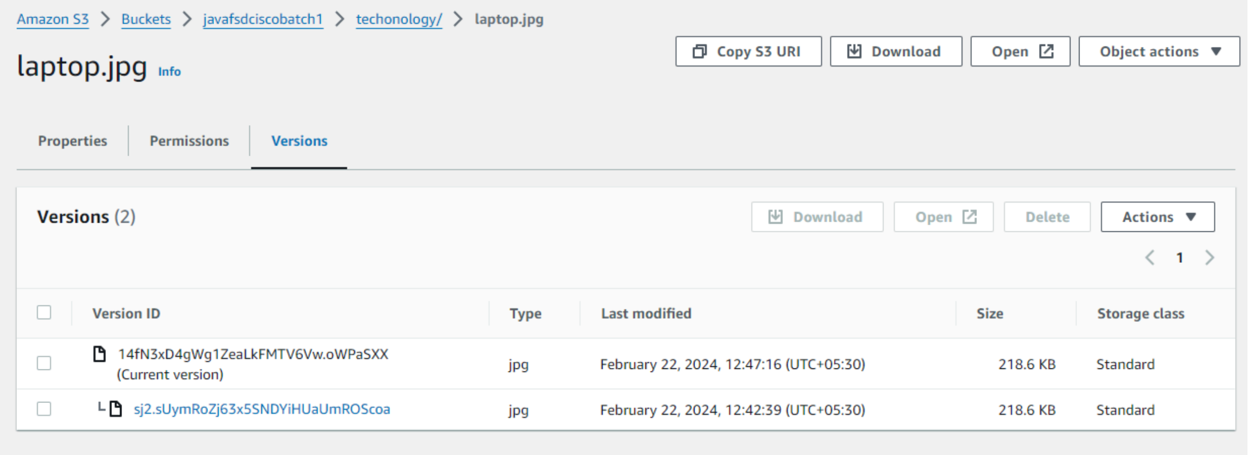
```
▼<Error>
   <script>window._wordtune_extension_installed = true;</script>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>2WTX00GJ1YQYWNRP</RequestId>
   <HostId>OZkUYKjcIhxgtimp3/82s+Q35eo1cOrGO7YfEmJwLk+cvJnEIRslces3d5r0VRQer4oDIRMMx0Q=</HostId>
 </Error>
```

Let’s understand Versioning.

In your technology folder upload the same laptop image again, its not going give you any error like the same file existing but it’s just uploaded.

.

Click on image uploaded and click on version tab and you can see 2 versions of your file.

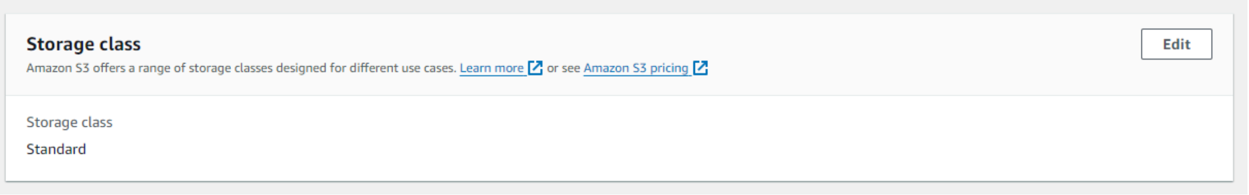


Versions (2)

□	Version ID	Type	Last modified	Size	Storage class
□	14fN3xD4gWg1ZeaLkFMTV6Vw.oWPaSXX (Current version)	jpg	February 22, 2024, 12:47:16 (UTC+05:30)	218.6 KB	Standard
□	sj2.sUymRoZj63x5SNDYiHUaUmROScoa	jpg	February 22, 2024, 12:42:39 (UTC+05:30)	218.6 KB	Standard

If you want use old version file or download old version file is possible here.

To See or change Storage Object Type use below options.
Click on object in properties scroll down.

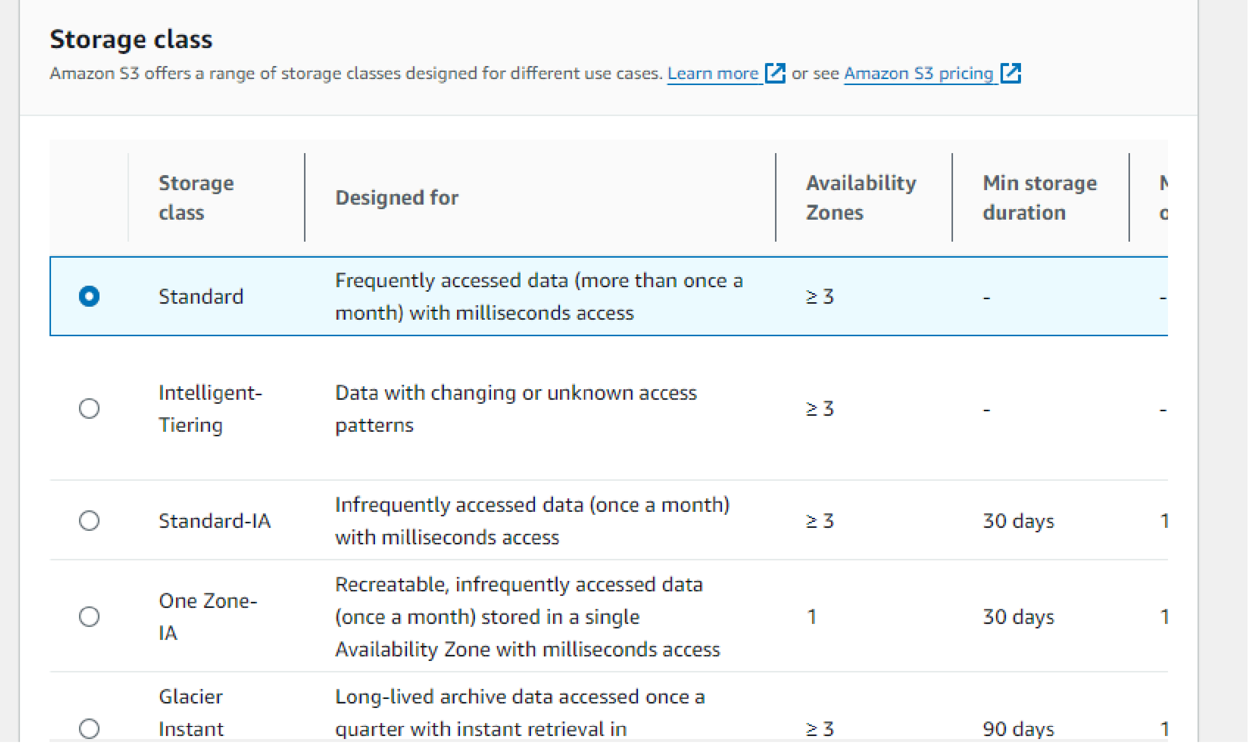


Storage class

Amazon S3 offers a range of storage classes designed for different use cases. Learn more or see Amazon S3 pricing

Storage class
Standard

Click on edit.
Check different storages.

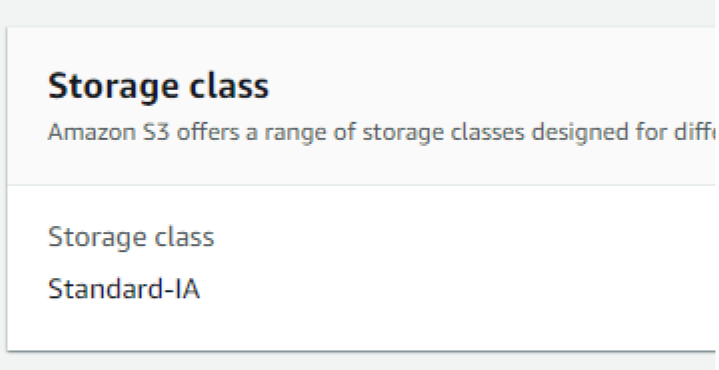


Storage class

Amazon S3 offers a range of storage classes designed for different use cases. Learn more or see Amazon S3 pricing

	Storage class	Designed for	Availability Zones	Min storage duration	N c
●	Standard	Frequently accessed data (more than once a month) with milliseconds access	≥ 3	-	-
○	Intelligent-Tiering	Data with changing or unknown access patterns	≥ 3	-	-
○	Standard-IA	Infrequently accessed data (once a month) with milliseconds access	≥ 3	30 days	1
○	One Zone-IA	Recreatable, infrequently accessed data (once a month) stored in a single Availability Zone with milliseconds access	1	30 days	1
○	Glacier Instant	Long-lived archive data accessed once a quarter with instant retrieval in	≥ 3	90 days	1

Select which you want to apply.



Storage class

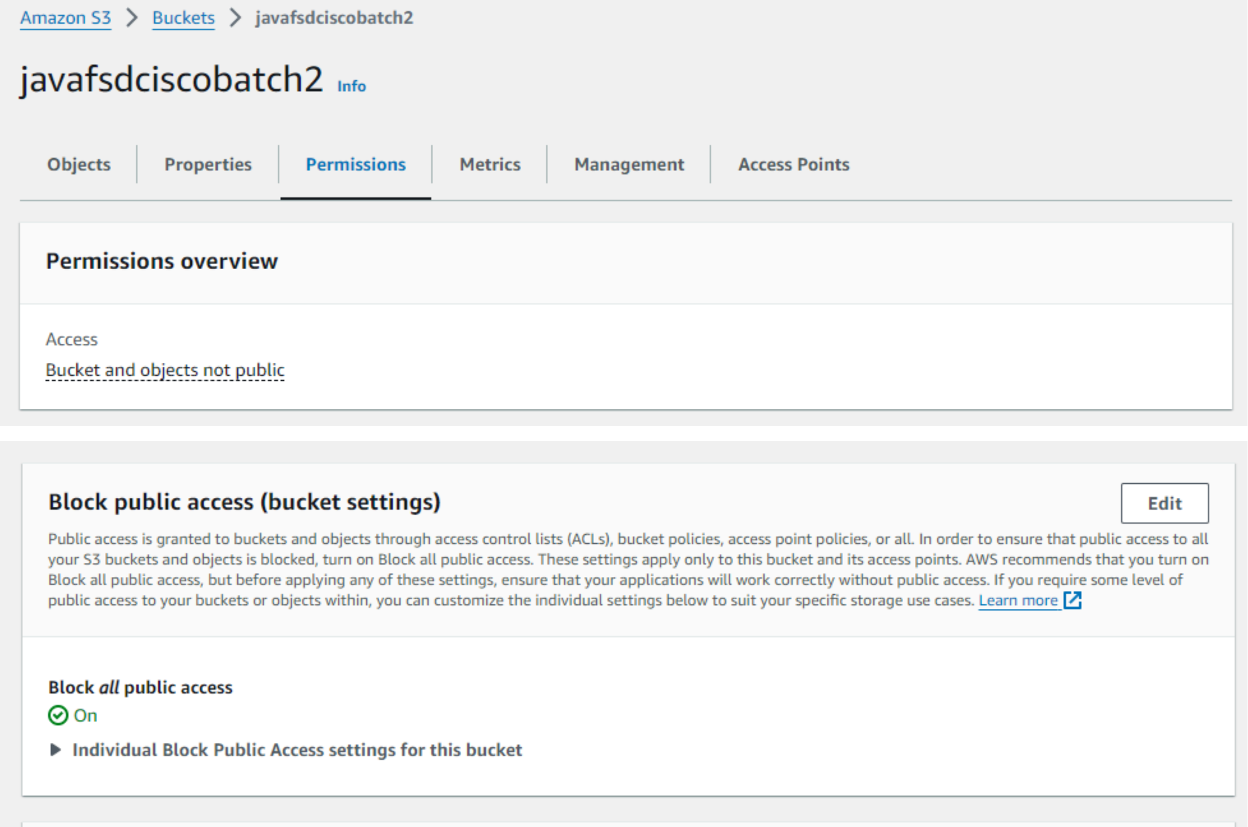
Amazon S3 offers a range of storage classes designed for diff

Storage class
Standard-IA

Storage class is updated.

To Access the objects Let’s Write the Policy: Bucket Policy

Step 1:



Amazon S3 > Buckets > javafsdciscobatch2

javafsdciscobatch2 Info

Permissions overview

Access
Bucket and objects not public

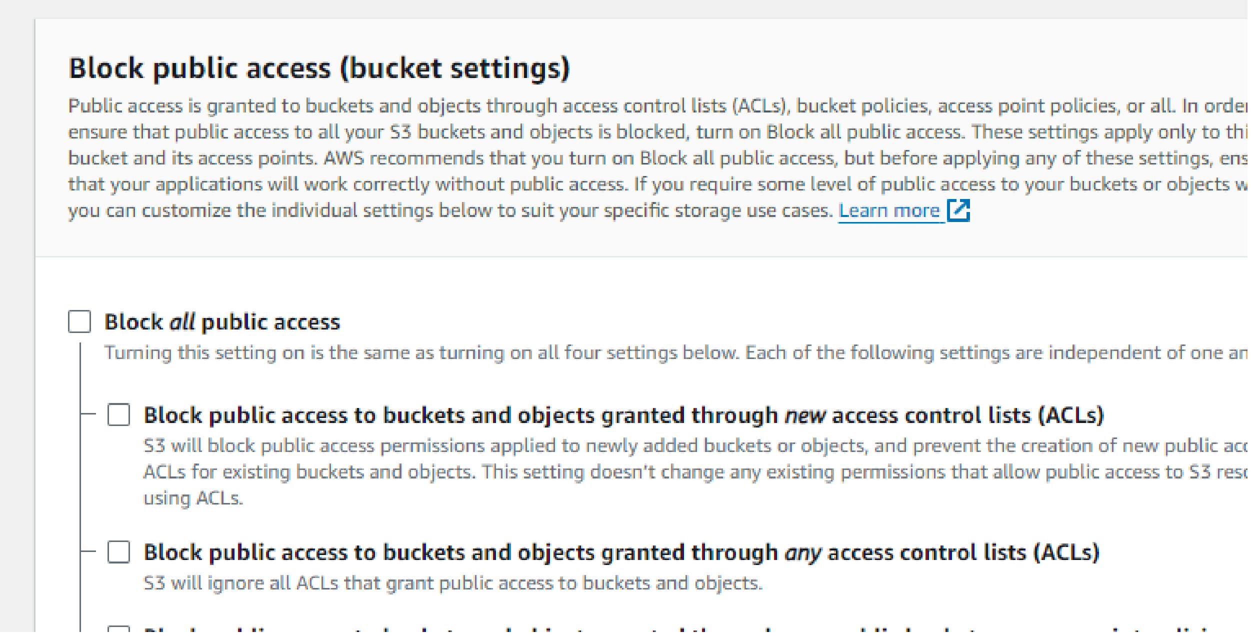
Block public access (bucket settings)

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

Click on edit



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 orde ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to thi bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ens that your applications will work correctly without public access. If you require some level of public access to your buckets or objects w you can customize the individual settings below to suit your specific storage use cases. Learn more

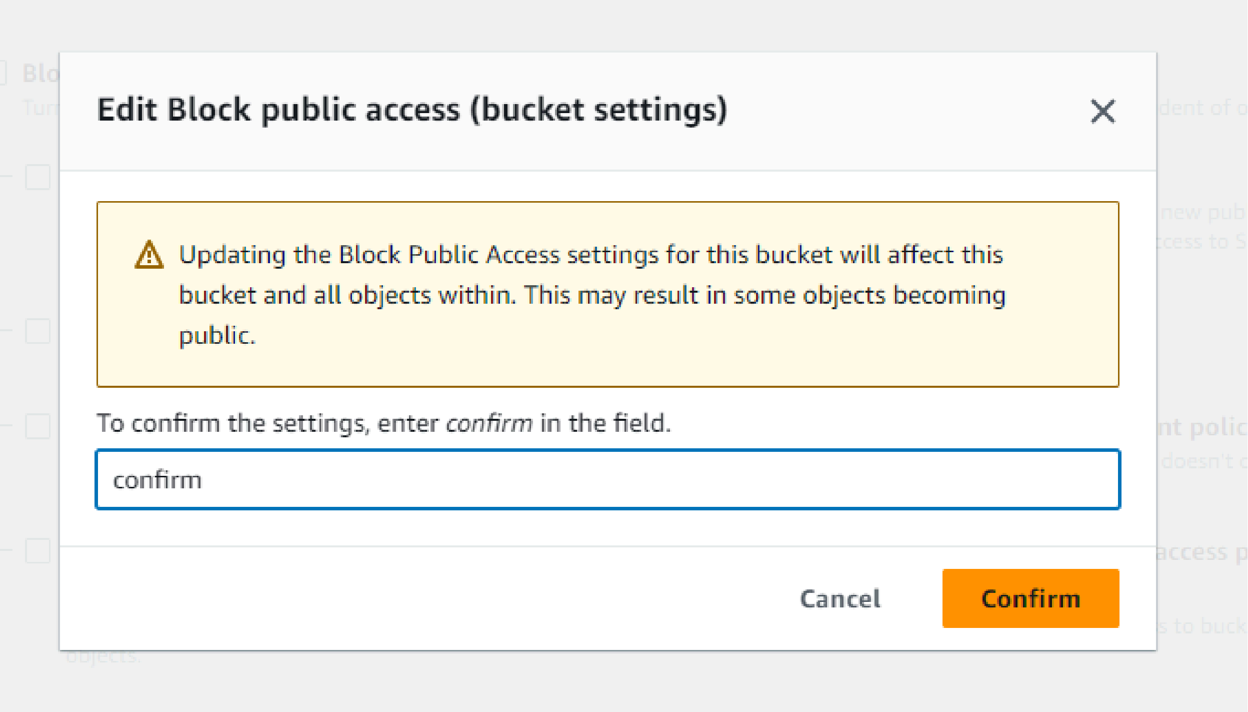
□ Block *all* public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one an

□ 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 acc ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 reso 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.

Uncheck block public access.

Click on save changes and type confirm in the box as shown below.



Edit Block public access (bucket settings)

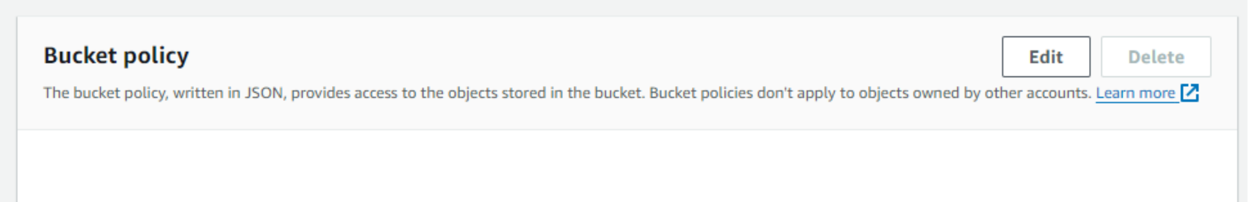
Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter *confirm* in the field.

confirm

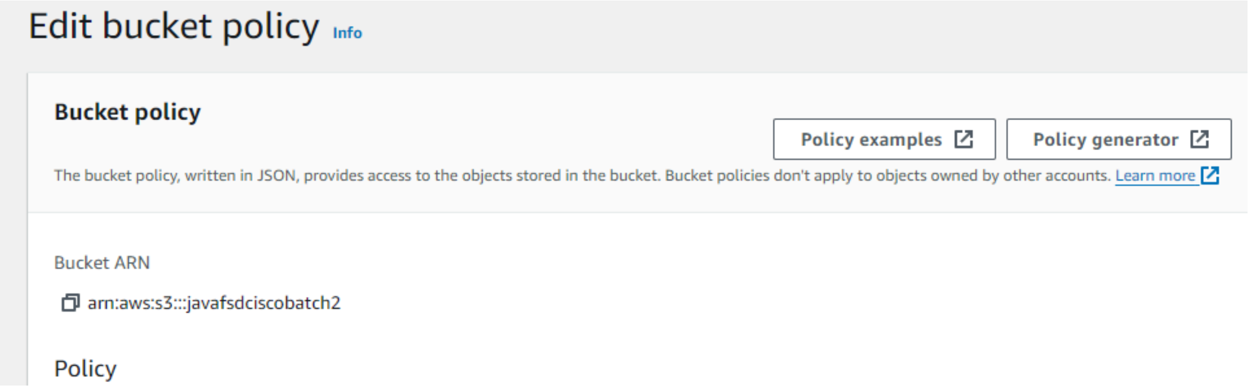
Click on confirm.

Let’s create policy by click on edit.



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



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

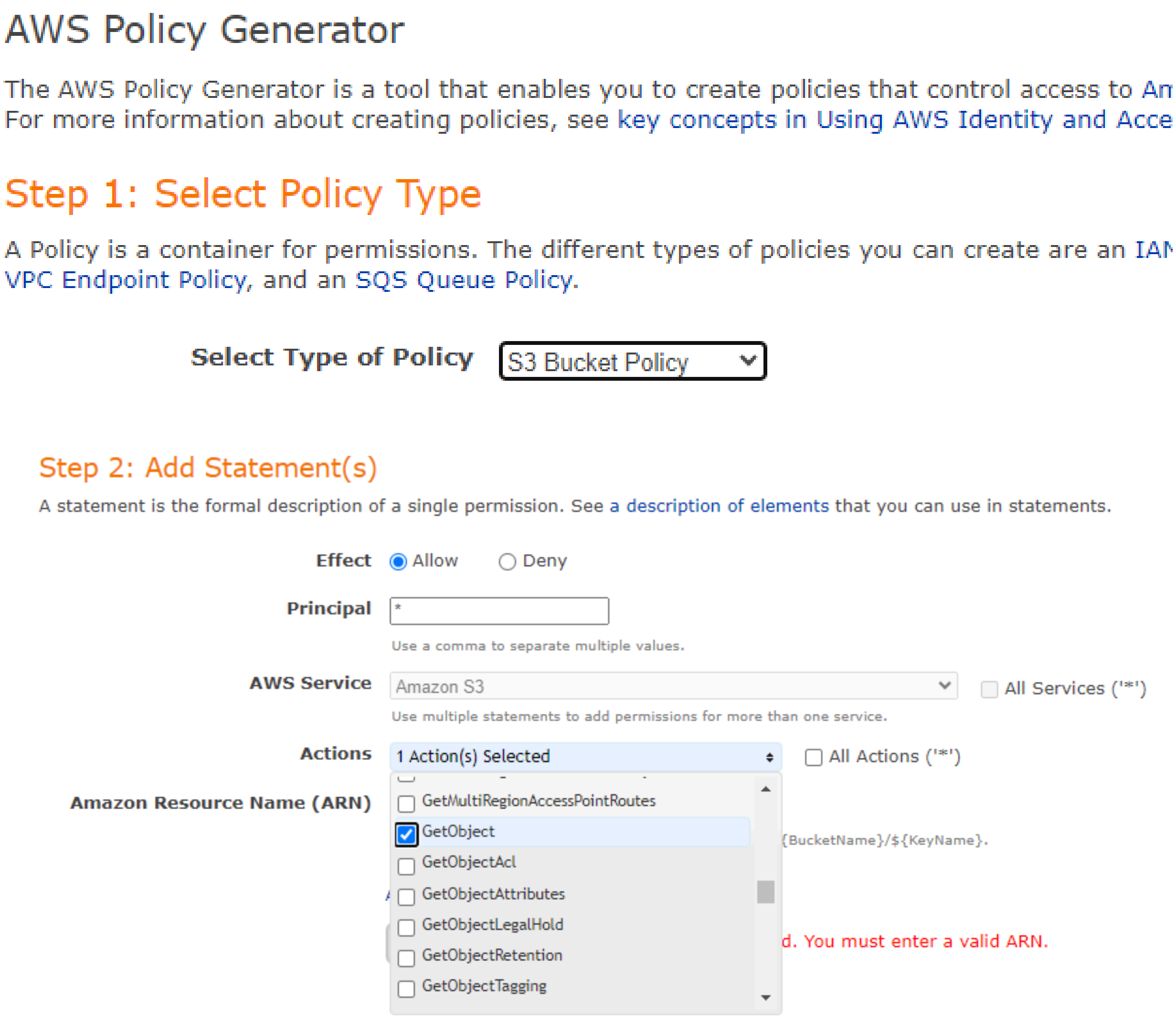
Bucket ARN

arn:aws:s3:::javafsdciscobatch2

Policy

Click on policy generator.

On Policy Generator page select policy type to s3 bucket.



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to An
For more information about creating policies, see key concepts in Using AWS Identity and Acce

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM
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 1 Action(s) Selected □ All Actions ('*')

- □ GetMultiRegionAccessPointRoutes
- ☑ GetObject
- □ GetObjectAcl
- □ GetObjectAttributes
- □ GetObjectLegalHold
- □ GetObjectRetention
- □ GetObjectTagging

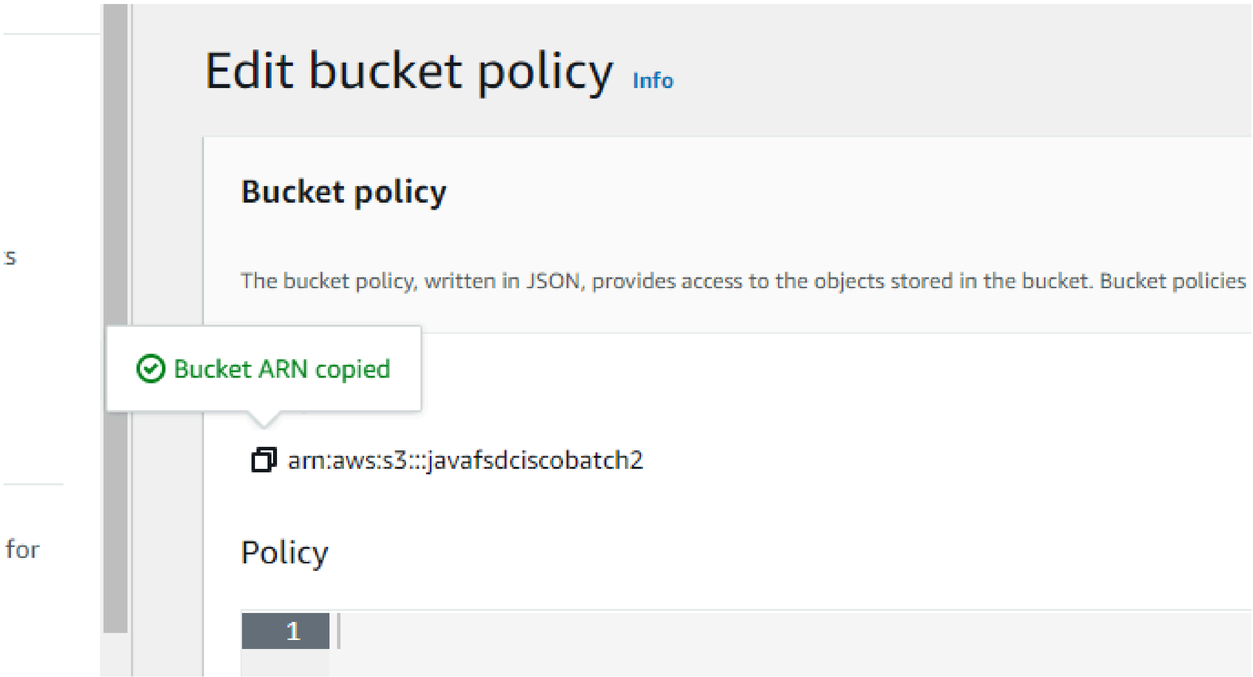
Amazon Resource Name (ARN)

{BucketName}/${KeyName}.

d. You must enter a valid ARN.

In principle type * and in actions search for getObject

.



Edit bucket policy

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies

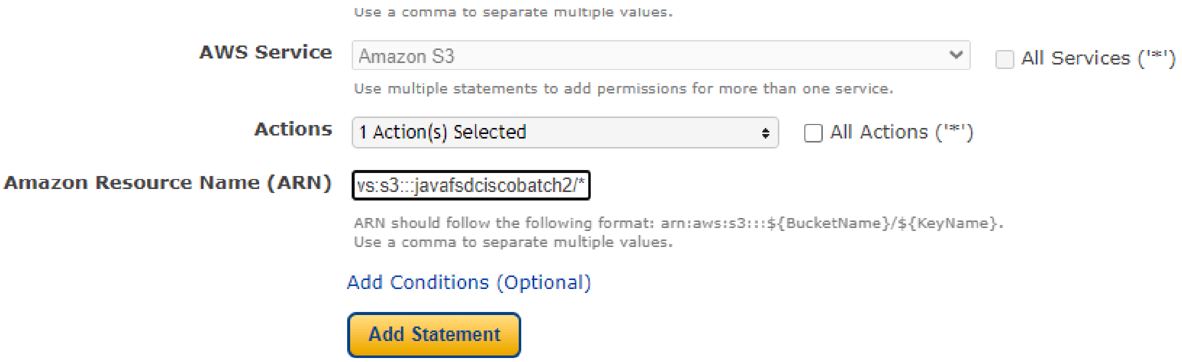
Bucket ARN copied

arn:aws:s3:::javafsdciscobatch2

Policy

1

Copy ARN number from here and paste it with /* in policy generator page



Use a comma to separate multiple values.

AWS Service: Amazon S3 — □ All Services ('*')

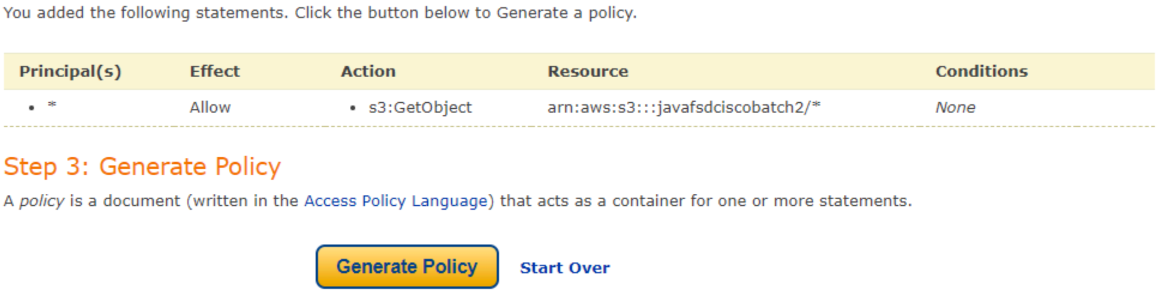
Use multiple statements to add permissions for more than one service.

Actions: 1 Action(s) Selected — □ All Actions ('*')

Amazon Resource Name (ARN): vs:s3:::javafsdciscobatch2/*

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

Click on Add Statement



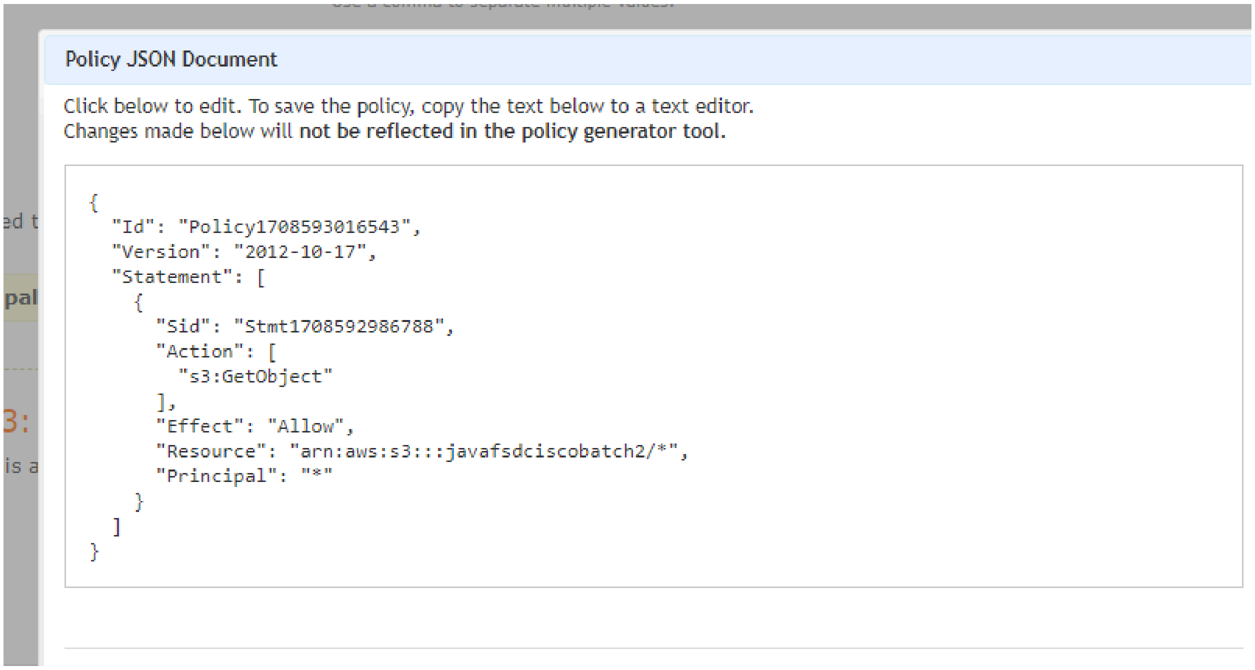
You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• *	Allow	• s3:GetObject	arn:aws:s3:::javafsdciscobatch2/*	*None*

Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.

Click on generate Policy

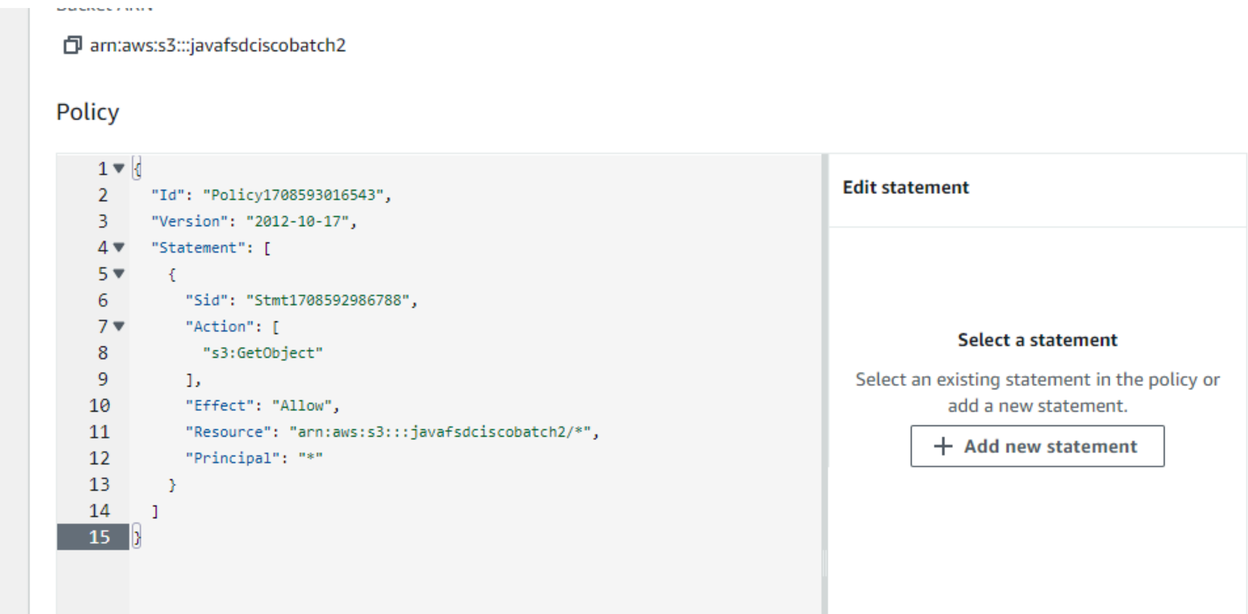


Policy JSON Document

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": "Policy1708593016543",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1708592986788",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::javafsdciscobatch2/*",
      "Principal": "*"
    }
  ]
}
```

Copy that generated code and add it to your policy page.



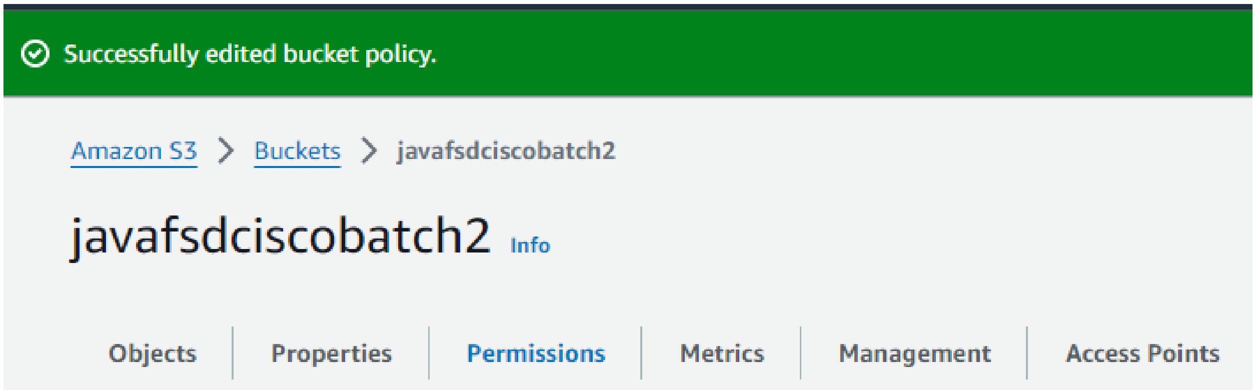
arn:aws:s3:::javafsdciscobatch2

Policy

```
{
  "Id": "Policy1708593016543",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1708592986788",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::javafsdciscobatch2/*",
      "Principal": "*"
    }
  ]
}
```

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

Click on Save Changes.



Successfully edited bucket policy.

Amazon S3 > Buckets > javafsdciscobatch2

javafsdciscobatch2 Info

Now Again try to access that added object in browser.