Cross-Region-Replication in Amazon S3

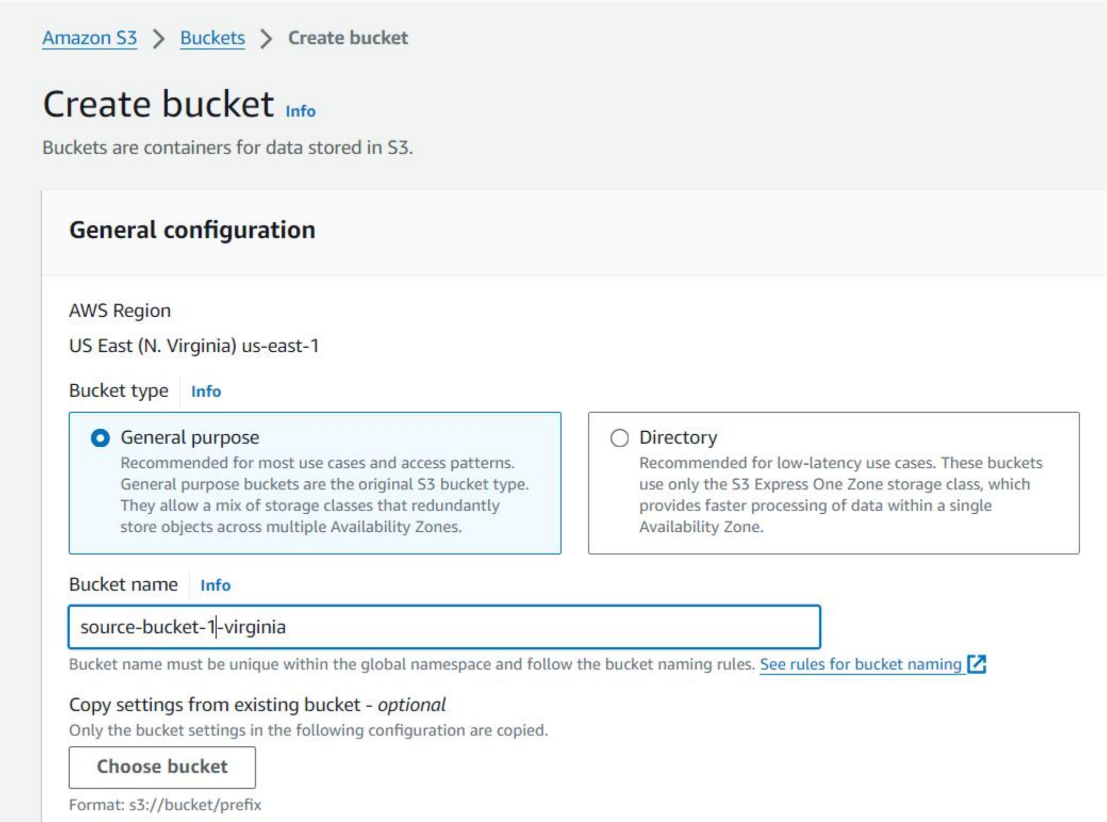
➢ What is cross region replication?

The AWS S3 – Cross-region replica on (CRR) allows you to replicate or copy your data in two different regions.

Setting up CRR:

Follow the below steps to set up the CRR:

- Go to the **AWS S3** – console and **create two buckets**.
- Let's name our source bucket as "source-bucket-1-virginia" and destination bucket as "destination-bucket-1-ohio". Do not forget to **enable versioning**. Also, note that the S3 bucket name needs to be globally unique and hence try adding random numbers a er bucket name.



Create bucket Info

Buckets are containers for data stored in S3.

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
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.

Bucket name Info

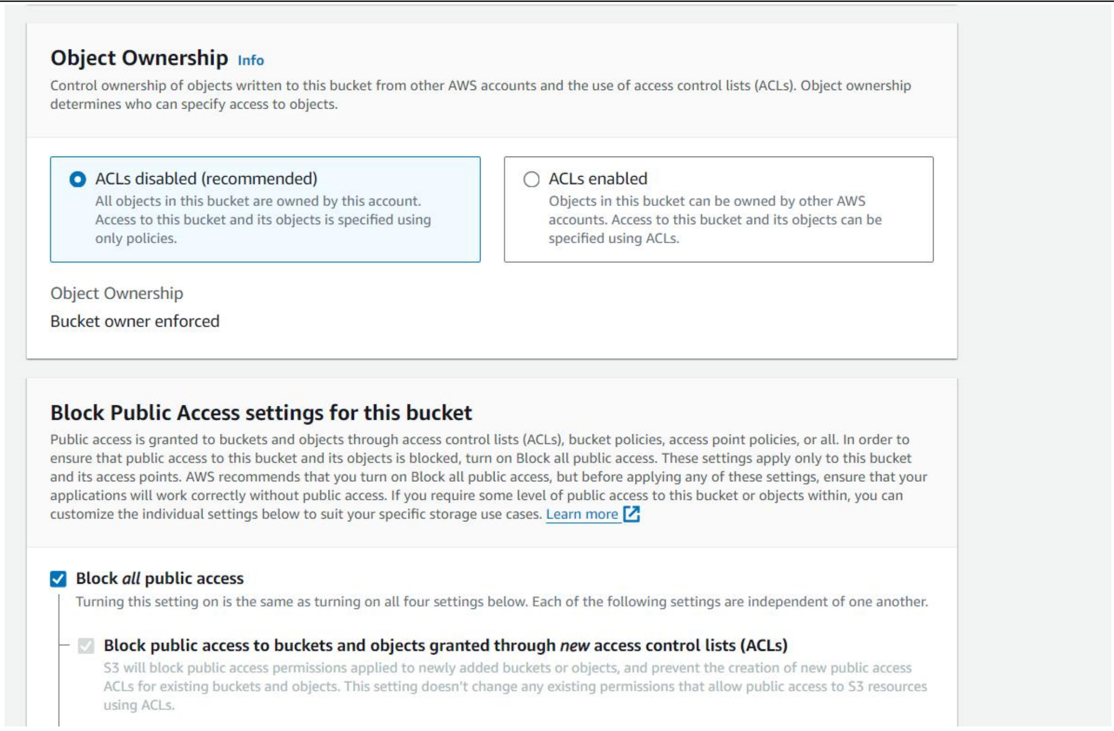
source-bucket-1-virginia

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



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.

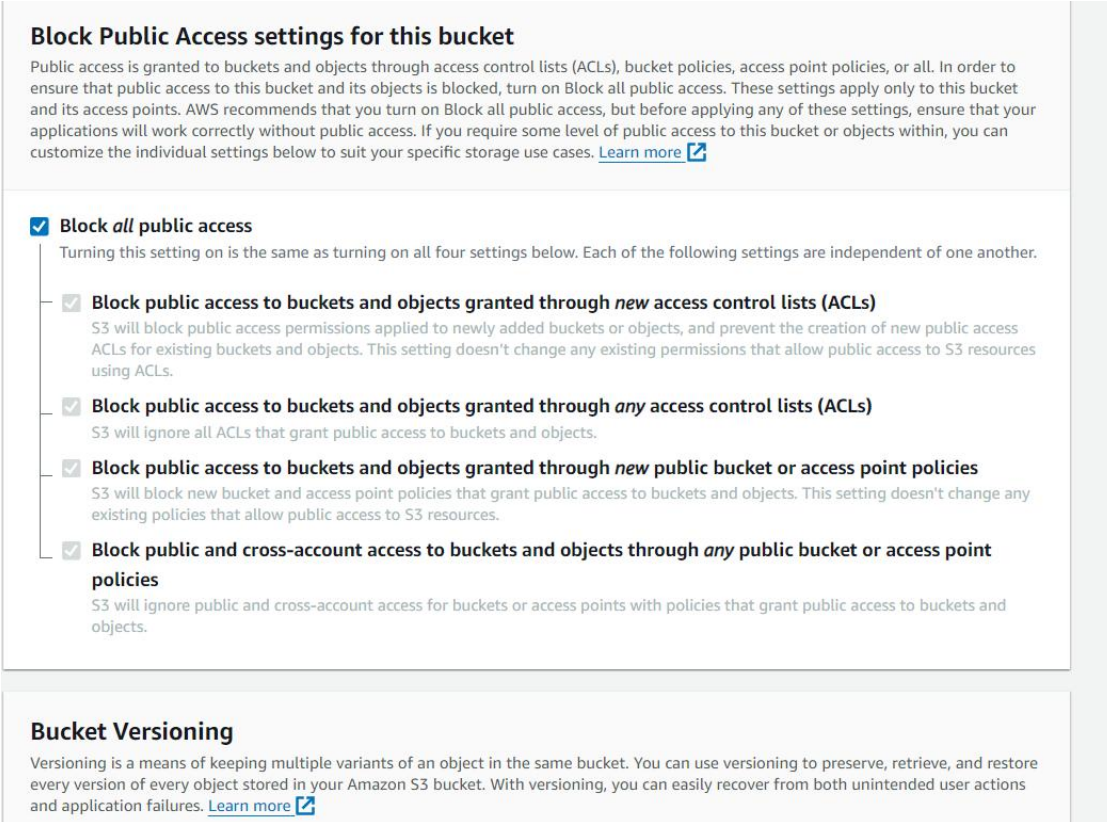
Object Ownership
Bucket owner enforced

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.

- ☑ **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 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

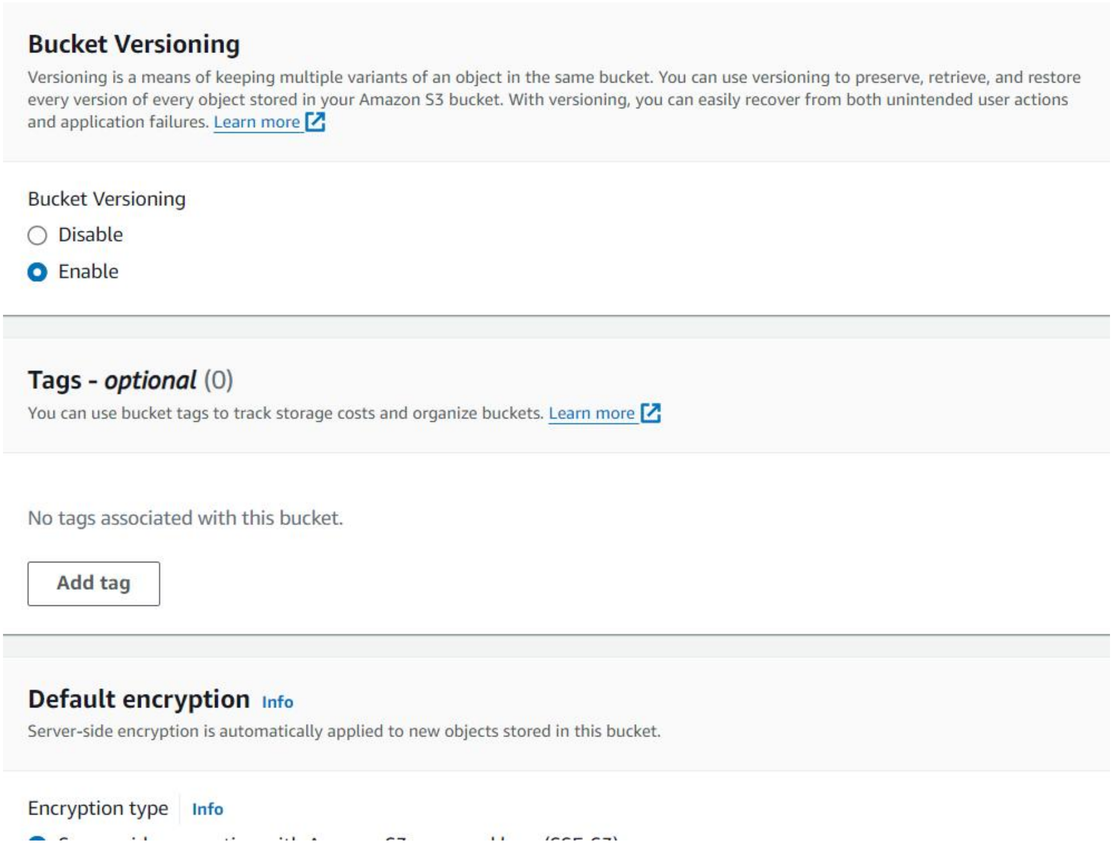
☑ Block *all* public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☑ **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.

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

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 - *optional* (0)

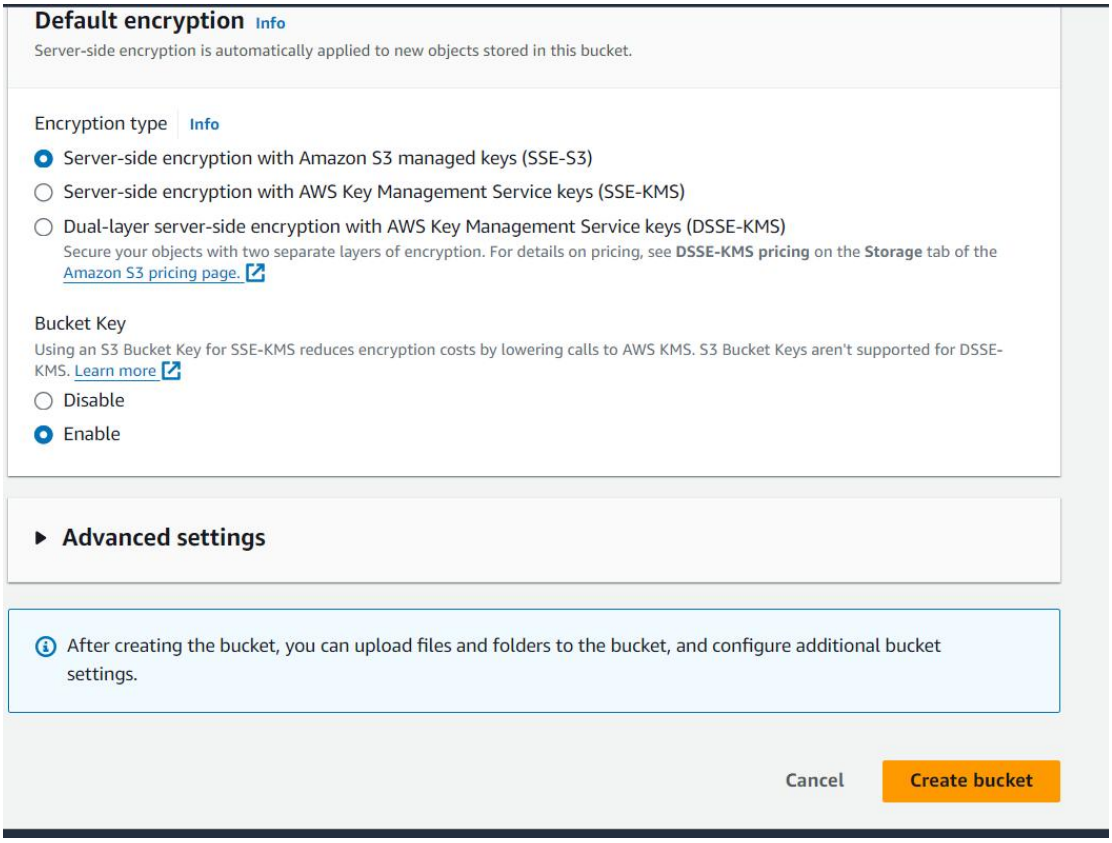
You can use bucket tags to track storage costs and organize buckets. Learn more

No tags associated with this bucket.

Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info



Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

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

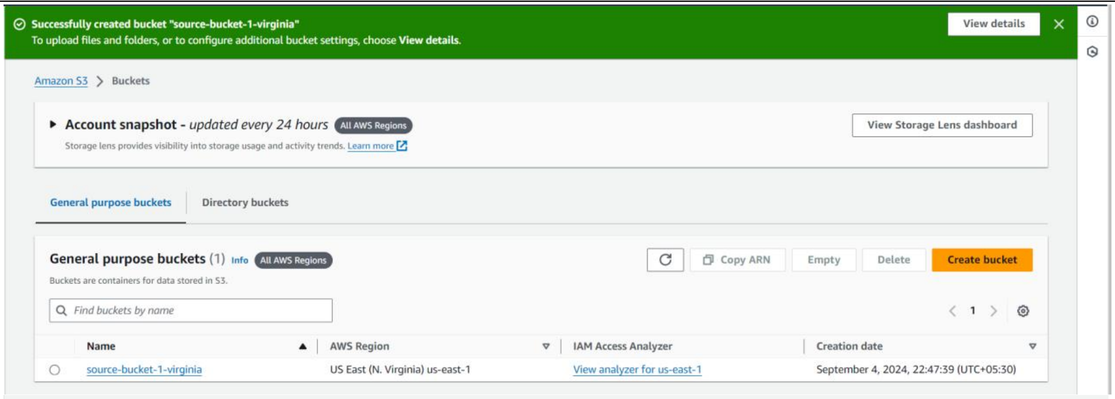
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

○ Disable

● Enable

▸ **Advanced settings**

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



Successfully created bucket "source-bucket-1-virginia"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

Amazon S3 > Buckets

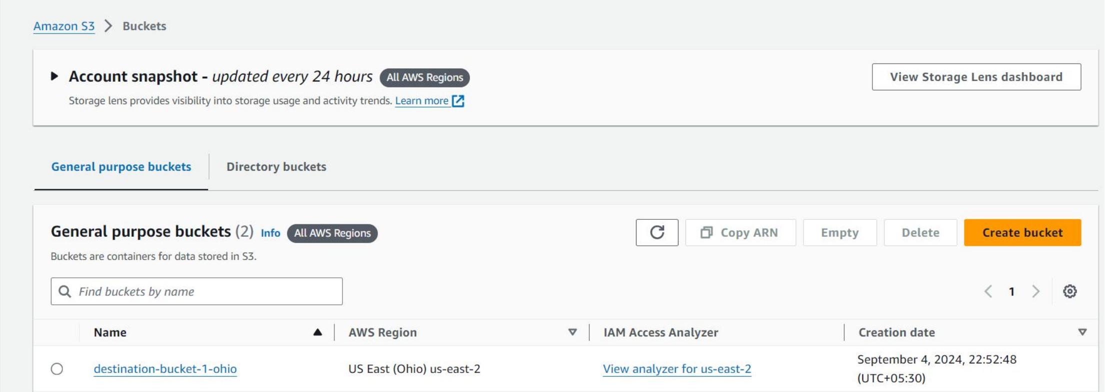
Account snapshot - *updated every 24 hours* All AWS Regions

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
○	source-bucket-1-virginia	US East (N. Virginia) us-east-1	View analyzer for us-east-1	September 4, 2024, 22:47:39 (UTC+05:30)



Amazon S3 > Buckets

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

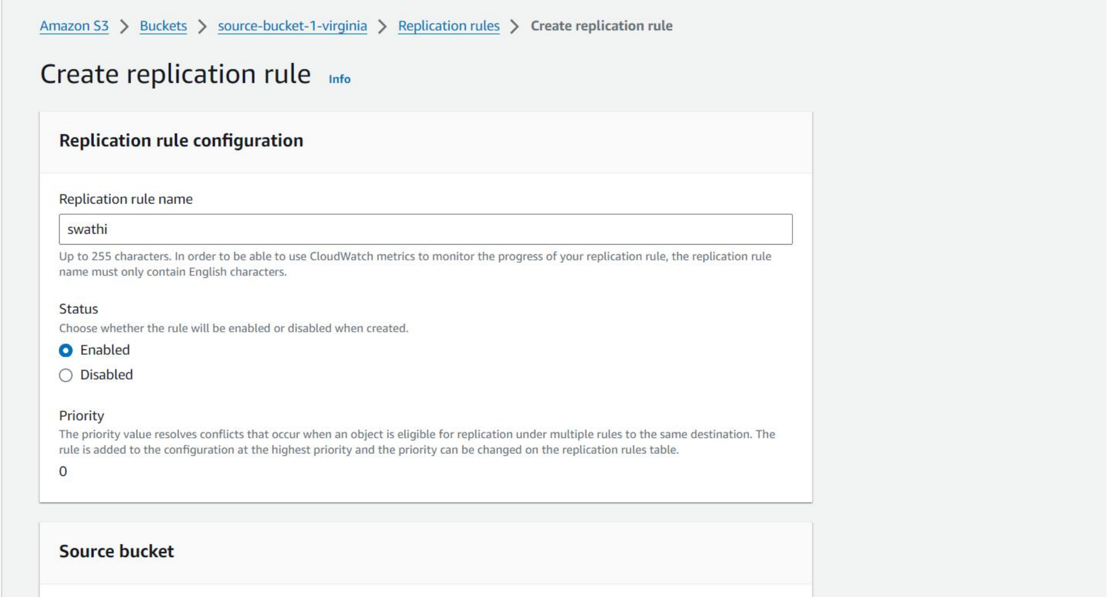
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (2) Info All AWS Regions

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	destination-bucket-1-ohio	US East (Ohio) us-east-2	View analyzer for us-east-2	September 4, 2024, 22:52:48 (UTC+05:30)

- Now click on your **source bucket** and head over to the **management tab** & click on "**Create a replica on rule**" and give your replica on rule name as "swathi"



Amazon S3 > Buckets > source-bucket-1-virginia > Replication rules > Create replication rule

Create replication rule Info

Replication rule configuration

Replication rule name

swathi

Up to 255 characters. In order to be able to use CloudWatch metrics to monitor the progress of your replication rule, the replication rule name must only contain English characters.

Status

Choose whether the rule will be enabled or disabled when created.

● Enabled

○ Disabled

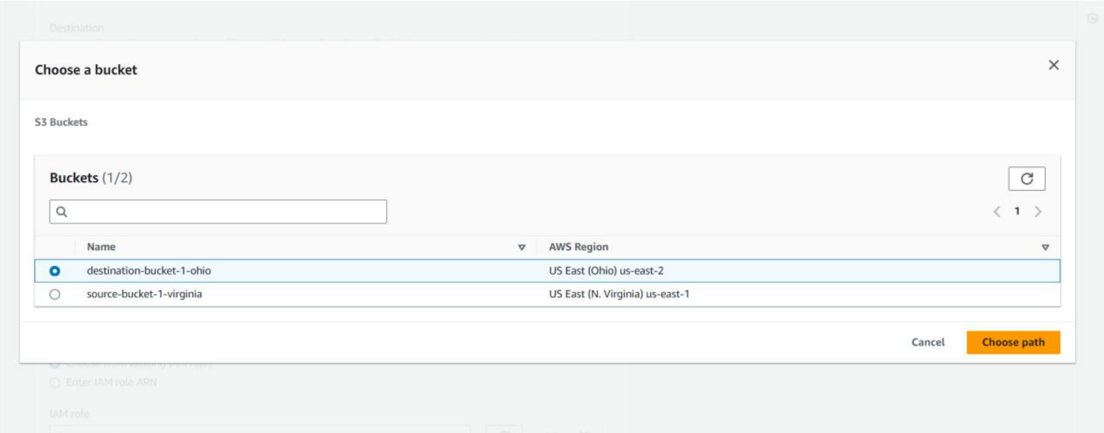
Priority

The priority value resolves conflicts that occur when an object is eligible for replication under multiple rules to the same destination. The rule is added to the configuration at the highest priority and the priority can be changed on the replication rules table.

0

Source bucket

- Choose the **destination on bucket** as "destination-bucket-1-ohio".
- Notice that you have an op on to choose a destination bucket in another account.
- In order to replicate objects from the source bucket to the destination bucket, you need to create an **IAM role**. So just create one by clicking on "**create a new role**".

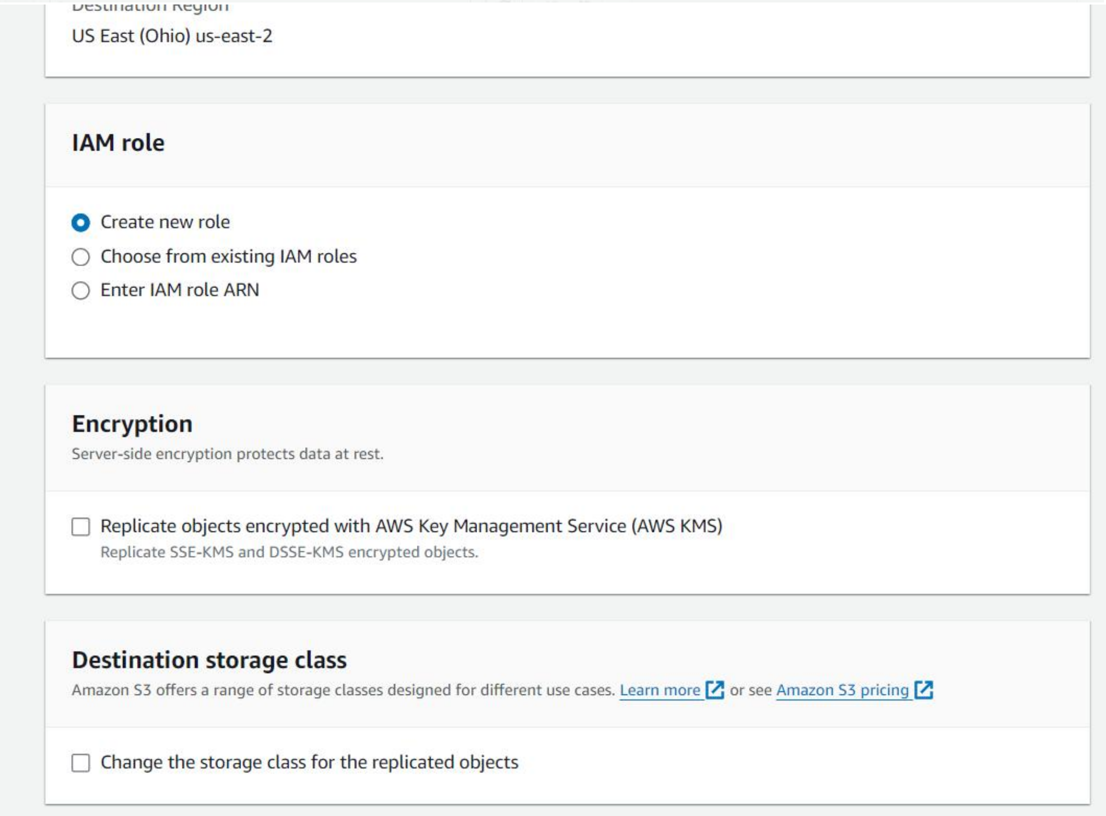


Choose a bucket

S3 Buckets

Buckets (1/2)

	Name	AWS Region
●	destination-bucket-1-ohio	US East (Ohio) us-east-2
○	source-bucket-1-virginia	US East (N. Virginia) us-east-1



Destination Region

US East (Ohio) us-east-2

IAM role

● Create new role
○ Choose from existing IAM roles
○ Enter IAM role ARN

Encryption

Server-side encryption protects data at rest.

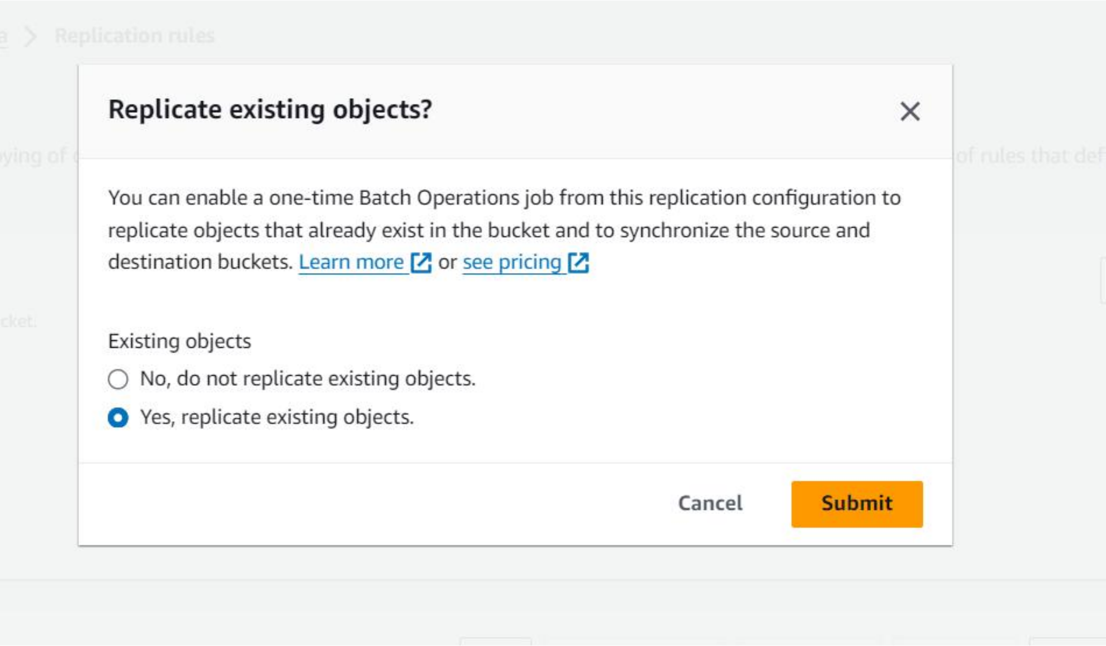
□ Replicate objects encrypted with AWS Key Management Service (AWS KMS)
Replicate SSE-KMS and DSSE-KMS encrypted objects.

Destination storage class

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

□ Change the storage class for the replicated objects

- As soon as you click on save, a screen will pop up asking if you want to replicate existing objects in the S3 bucket, choose yes and click on submit.



Replicate existing objects?

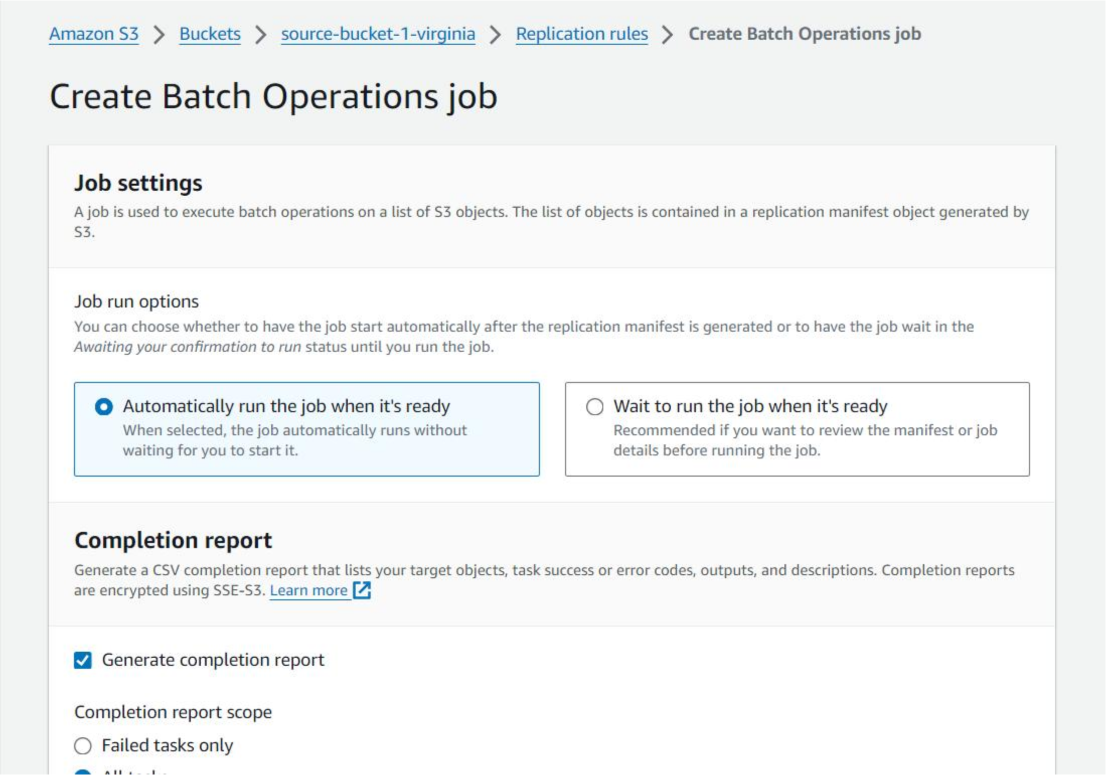
You can enable a one-time Batch Operations job from this replication configuration to replicate objects that already exist in the bucket and to synchronize the source and destination buckets. Learn more or see pricing

Existing objects

○ No, do not replicate existing objects.

● Yes, replicate existing objects.

- Now you will get create batch operations job – go down at **completion report destination**- choose destination bucket that we already created.
- For be er understanding look at below snapshots.



Amazon S3 > Buckets > source-bucket-1-virginia > Replication rules > Create Batch Operations job

Create Batch Operations job

Job settings

A job is used to execute batch operations on a list of S3 objects. The list of objects is contained in a replication manifest object generated by S3.

Job run options

You can choose whether to have the job start automatically after the replication manifest is generated or to have the job wait in the *Awaiting your confirmation to run* status until you run the job.

● Automatically run the job when it's ready
When selected, the job automatically runs without waiting for you to start it.

○ Wait to run the job when it's ready
Recommended if you want to review the manifest or job details before running the job.

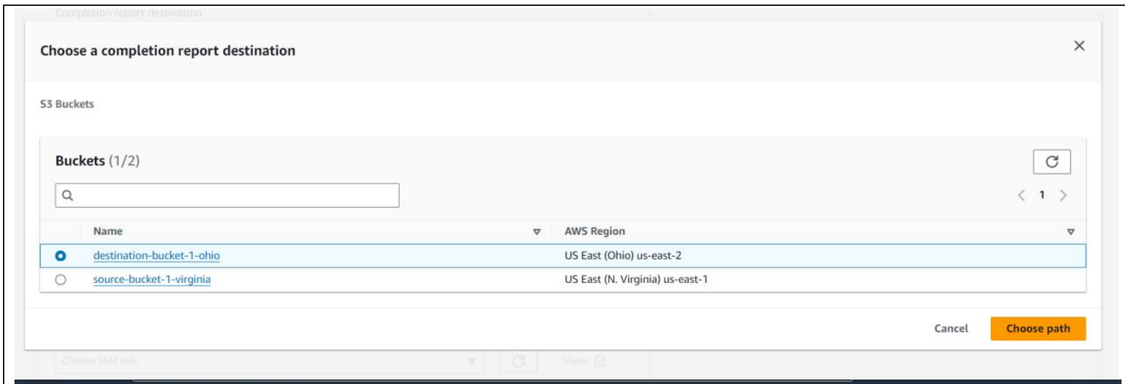
Completion report

Generate a CSV completion report that lists your target objects, task success or error codes, outputs, and descriptions. Completion reports are encrypted using SSE-S3. Learn more

☑ Generate completion report

Completion report scope

○ Failed tasks only

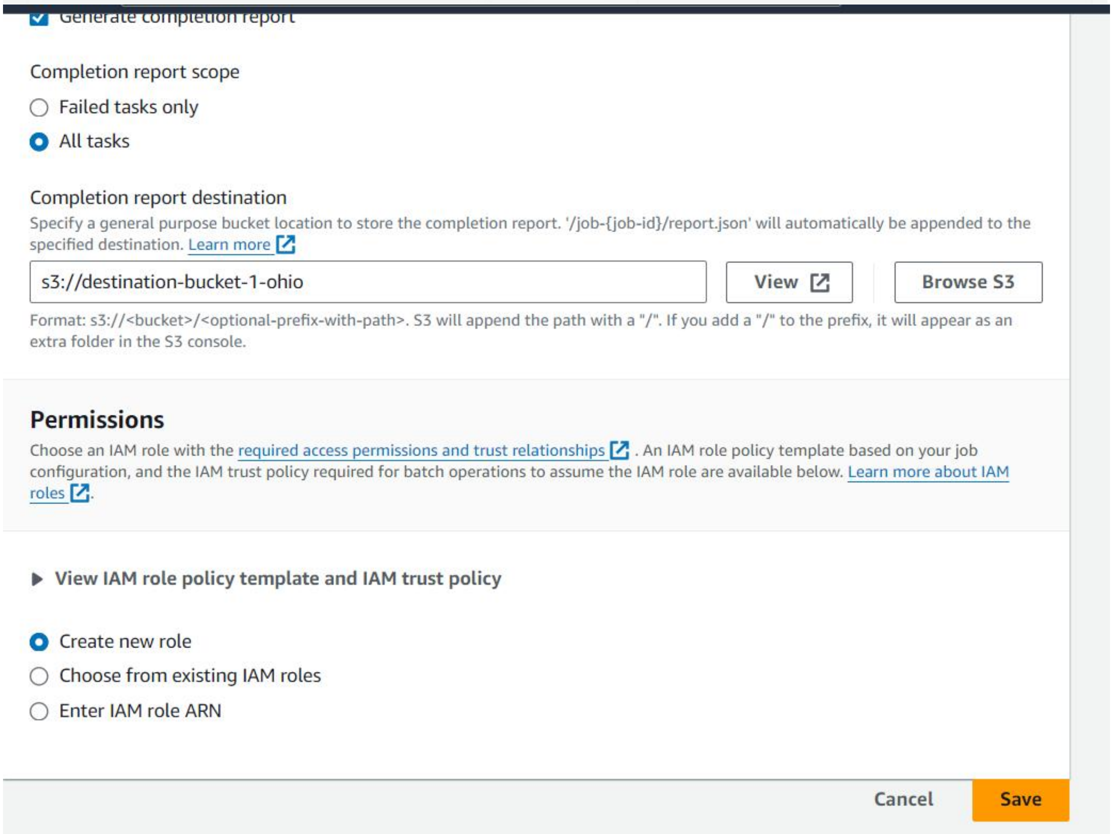


Choose a completion report destination

S3 Buckets

Buckets (1/2)

	Name	AWS Region
●	destination-bucket-1-ohio	US East (Ohio) us-east-2
○	source-bucket-1-virginia	US East (N. Virginia) us-east-1



☑ Generate completion report

Completion report scope

○ Failed tasks only

● All tasks

Completion report destination

Specify a general purpose bucket location to store the completion report. '/job-{job-id}/report.json' will automatically be appended to the specified destination. Learn more

s3://destination-bucket-1-ohio

Format: s3://<bucket>/<optional-prefix-with-path>. S3 will append the path with a "/". If you add a "/" to the prefix, it will appear as an extra folder in the S3 console.

Permissions

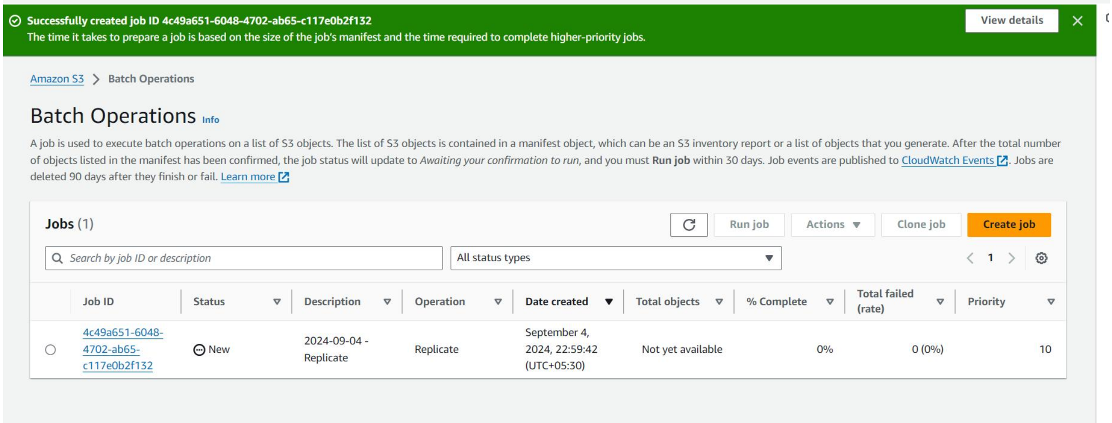
Choose an IAM role with the required access permissions and trust relationships . An IAM role policy template based on your job configuration, and the IAM trust policy required for batch operations to assume the IAM role are available below. Learn more about IAM roles .

▶ View IAM role policy template and IAM trust policy

● Create new role

○ Choose from existing IAM roles

○ Enter IAM role ARN



Successfully created job ID 4c49a651-6048-4702-ab65-c117e0b2f132

The time it takes to prepare a job is based on the size of the job's manifest and the time required to complete higher-priority jobs.

Amazon S3 > Batch Operations

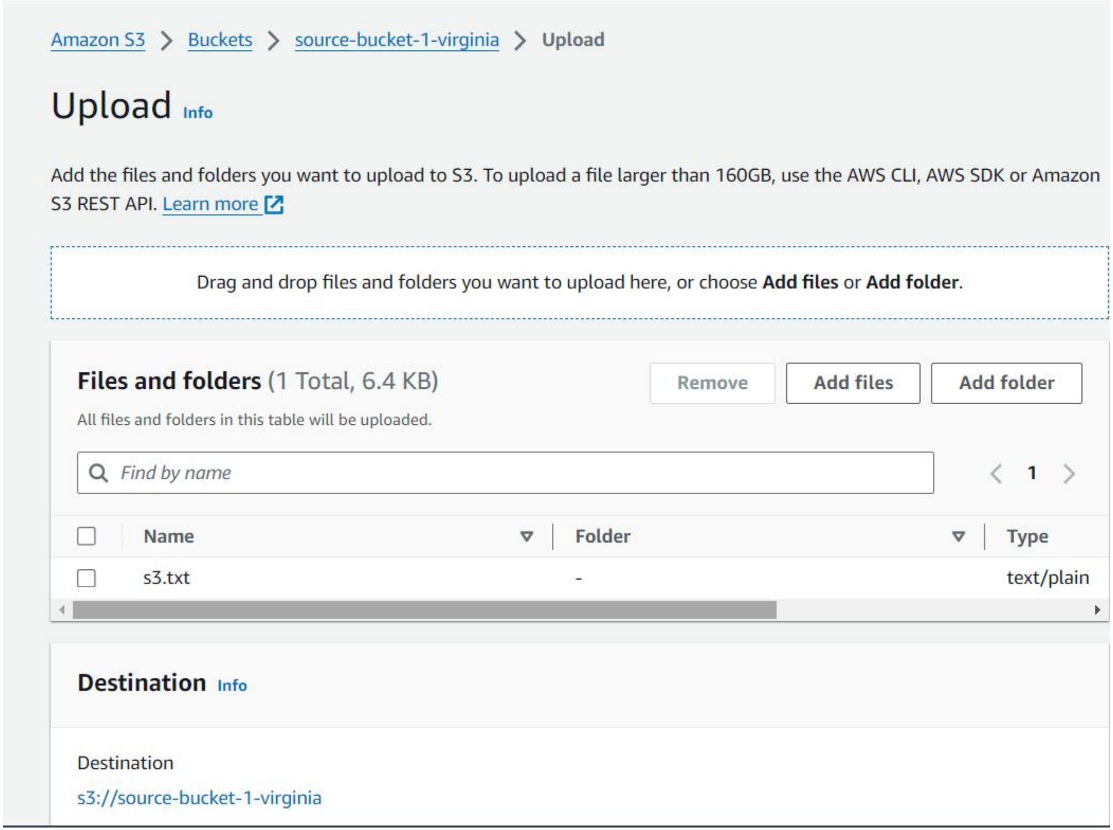
Batch Operations Info

A job is used to execute batch operations on a list of S3 objects. The list of S3 objects is contained in a manifest object, which can be an S3 inventory report or a list of objects that you generate. After the total number of objects listed in the manifest has been confirmed, the job status will update to *Awaiting your confirmation to run*, and you must **Run job** within 30 days. Job events are published to CloudWatch Events. Jobs are deleted 90 days after they finish or fail. Learn more

Jobs (1)

	Job ID	Status	Description	Operation	Date created	Total objects	% Complete	Total failed (rate)	Priority
○	4c49a651-6048-4702-ab65-c117e0b2f132	New	2024-09-04 - Replicate	Replicate	September 4, 2024, 22:59:42 (UTC+05:30)	Not yet available	0%	0 (0%)	10

- Now It’s me to test! Now go to the source bucket: source-bucket-1-virginia and upload a file.



Amazon S3 > Buckets > source-bucket-1-virginia > Upload

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 (1 Total, 6.4 KB)

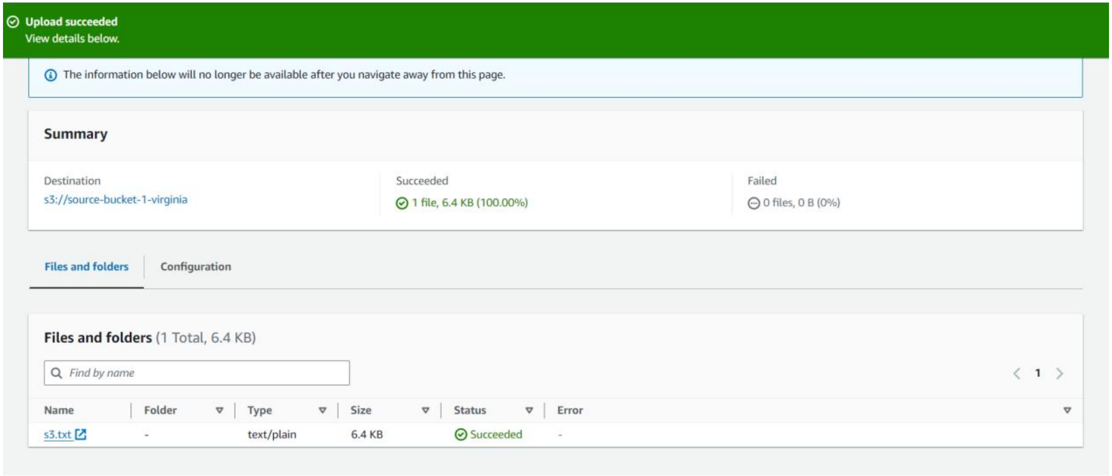
All files and folders in this table will be uploaded.

□	Name	Folder	Type
□	s3.txt	-	text/plain

Destination Info

Destination

s3://source-bucket-1-virginia



Upload succeeded
View details below.

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

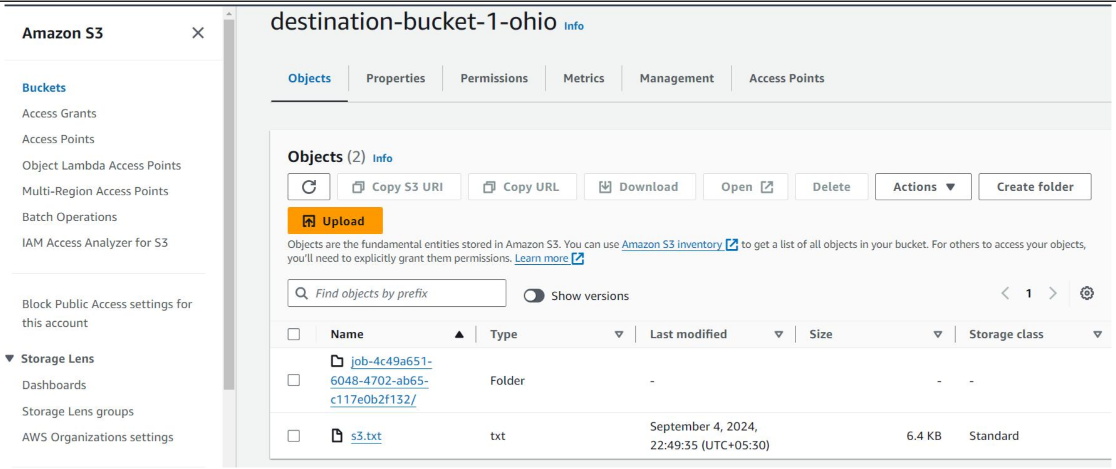
Summary

Destination	Succeeded	Failed
s3://source-bucket-1-virginia	✓ 1 file, 6.4 KB (100.00%)	0 files, 0 B (0%)

Files and folders (1 Total, 6.4 KB)

Name	Folder	Type	Size	Status	Error
s3.txt	-	text/plain	6.4 KB	✓ Succeeded	-

- Now go to the destination bucket: destination-bucket-1-ohio to check if the uploaded file is replicated to our destination bucket. You can see that our uploaded file is successfully copied to the destination bucket.



destination-bucket-1-ohio

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	Last modified	Size	Storage class
□	job-4c49a651-6048-4702-ab65-c117e0b2f132/	Folder	-	-	-
□	s3.txt	txt	September 4, 2024, 22:49:35 (UTC+05:30)	6.4 KB	Standard

Note: While deleting the buckets, do not forget to empty your buckets and then delete them, if you do not have any further use. Also, you cannot delete a bucket if it is not empty.