

# 2. Set Cross-Region Replication (CRR) for S3

Cross-Region Replication (CRR) ensures automatic copying of objects between AWS regions.

aws

Search

[Alt+S]

United States (N. Virginia)

vociabz/user1723836~vishhru2005@gmail.com @ 0123-3431-8258

Amazon S3

Buckets

exp2-cc-bucket

Edit Bucket Versioning

0

+

o

Edit Bucket Versioning

Info

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

☐ Suspend

This suspends the creation of object versions for all operations but preserves any existing object versions.

☒ Enable

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Cancel

Save changes

aws

Search

[Alt+S]

United States (N. Virginia)

vociabz/user1723836~vishhru2005@gmail.com @ 0123-3431-8258

Amazon S3

Buckets

exp2-cc-bucket

0

+

o

exp2-cc-bucket

Info

Objects

Metadata

Properties

Permissions

Metrics

Management

Access Points

Bucket overview

AWS Region

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

Amazon Resource Name (ARN)

arn:aws:s3::exp2-cc-bucket

Creation date

February 17, 2025, 10:07:27 (UTC+05:30)

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

Enabled

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Edit

Tags (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

Key

Value

No tags associated with this resource.

Edit

## 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](#)

exp2-cc-test-bucket

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

### 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.

**We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.**

**Object Ownership**

☒ **Bucket owner preferred**

**We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.**

**Object Ownership**

☒ **Bucket owner preferred**  
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

☐ **Object writer**  
The object writer remains the object owner.

**If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)**

### 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.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

# Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

US West (Oregon) us-west-2

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

exp2-cc-source-bucket

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

## Create a source bucket

aws

Search

[Alt+S]

United States (N. Virginia) | vocilabs/user3723836~vishhnu2005@gmail.com @ 0123-3431-8258

Amazon S3

Buckets

Create bucket

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.

Add tag

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 [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

aws

Search

[Alt+S]

United States (N. Virginia)voctabrs/Asser3723836~vshhnu2005@gmail.com @ 0123-3451-8238

Amazon S3 > Buckets > Create bucket

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.

Add tag

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

- Click on the bucket you want to replicate.

- **Set Up Replication:**
- Click on **Replication rules** → **Create replication rule.**
-

Search

[Alt+S]

United States (Oregon) | vociaibz/user3723836~vishnu2005@gmail.com @ 0123-3431-8256

Amazon S3

Buckets

exp2-cc-source-bucket1

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

| Lifecycle rule name   | Status | Scope | Current version actions | Noncurrent versions actions | Expired object delete mar... | Incomplete multipart upl... |
|---|--------|-------|-------------------------|-----------------------------|------------------------------|-----------------------------|
| No lifecycle rules<br>There are no lifecycle rules for this bucket. |        |       |                         |                             |                              |                             |

Create lifecycle rule

Replication rules (0)

View details

Edit rule

Delete

Actions

Create replication rule

Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. [Learn more](#)

| Replication rule name  | Status | Destination bucket | Destination Region | Priority | Scope | Storage class | Replica owner | Replication Time Control | KMS-encrypted objects (SSE-KMS or DSSE-KMS) | Replica modification sync |
|--|--------|--------------------|--------------------|----------|-------|---------------|---------------|--------------------------|---|---------------------------|
| No replication rules<br>You don't have any rules in the replication configuration. |        |                    |                    |          |       |               |               |                          |   |                           |

Create replication rule

Name the replication rule.

Search

[Alt+S]

United States (Oregon) | vociaibz/user3723836~vishnu2005@gmail.com @ 0123-3431-8256

Amazon S3

Buckets

exp2-cc-source-bucket1

Replication rules

Create replication rule

Create replication rule

info

Replication rule configuration

Replication rule name

replicate-all

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

Source bucket name

exp2-cc-source-bucket1

Source Region

US West (Oregon) us-west-2

Choose a rule scope

☐ Limit the scope of this rule using one or more filters

☒ Apply to all objects in the bucket

Click on Save

Amazon S3 > Buckets > exp2-cc-source-bucket1 > Replication rules > Create replication rule

IAM role

LabRole

View

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

Additional replication options

☐ Replication Time Control (RTC)  
Replication Time Control replicates 99.99% of new objects within 15 minutes and includes replication metrics. Additional fees will apply. [Learn more](#)

☐ Replication metrics  
With replication metrics, you can monitor the total number and size of objects that are pending replication, and the maximum replication time to the destination Region. You can also view and diagnose replication failures. CloudWatch metrics fees apply. [Learn more](#) or see [Amazon CloudWatch pricing](#)

☐ Delete marker replication  
Delete markers created by S3 delete operations will be replicated. Delete markers created by lifecycle rules are not replicated. [Learn more](#)

☐ Replica modification sync  
Replicate metadata changes made to replicas from the destination bucket to the source bucket. [Learn more](#)

Cancel

Save

Replication configuration successfully updated  
If changes to the configuration aren't displayed, choose the refresh button. Changes apply only to new objects. To replicate existing objects with this configuration, choose Create replication job.

## Replication rules

Replication enables automatic and asynchronous copying of objects across buckets in the same or different AWS Regions. A replication configuration is a set of rules that define what options should be applied to a group of objects during replication.

**Replication configuration settings**  
Configuration settings affect all replication rules in the bucket.

**Source bucket**  
exp2-cc-source-bucket1

**Source Region**  
US West (Oregon) us-west-2

**Replication rules (1)**  
Use replication rules to define options you want Amazon S3 to apply during replication.

**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.

Cancel Submit

| Replication rule name         | Status  | Destination bucket                       | Destination Region              | Priority | Scope         | Storage class  | Replica owner  | Replication Time Control | KMS-encrypted objects (SSE-KMS or OSSE-KMS) | Replica modification sync |
|-------------------------------|---------|--|---------------------------------|----------|---------------|----------------|----------------|--------------------------|---|---------------------------|
| <a href="#">replicate-all</a> | Enabled | <a href="#">s3://exp2-cc-dest-bucket</a> | US East (N. Virginia) us-east-1 | 0        | Entire bucket | Same as source | Same as source | Disabled                 | Do not replicate                            | Disabled                  |

## Upload

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs 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, 3.3 KB)**  
All files and folders in this table will be uploaded.

| <input type="checkbox"/> | Name     | Folder | Type       | Size   |
|--------------------------|----------|--------|------------|--------|
| <input type="checkbox"/> | kmit.jpg | -      | Image/jpeg | 3.3 KB |

**Destination**  
[s3://exp2-cc-source-bucket1](#)

**Destination details**  
Bucket settings that impact new objects stored in the specified destination.

**Permissions**  
Grant public access and access to other AWS accounts.

**Properties**  
Specify storage class, encryption settings, tags, and more.

Cancel Upload

Now upload a object in source bucket it should display in destination bucket

**Upload succeeded**  
For more information, see the [Files and folders](#) table.

**Upload: status** Close

After you navigate away from this page, the following information is no longer available.

**Summary**

|   |  |                                    |
|---|--|------------------------------------|
| <b>Destination</b><br>s3://exp2-cc-source-bucket1 | <b>Succeeded</b><br>1 file, 3.3 KB (100.00%) | <b>Failed</b><br>0 files, 0 B (0%) |
|---|--|------------------------------------|

[Files and folders](#) | [Configuration](#)

**Files and folders** (1 total, 3.3 KB)

Find by name

| Name                     | Folder | Type       | Size   | Status    | Error |
|--------------------------|--------|------------|--------|-----------|-------|
| <a href="#">kmit.jpg</a> | -      | image/jpeg | 3.3 KB | Succeeded | -     |

Now we got kmit.jpg in destination bucket

**Amazon S3** [exp2-cc-dest-bucket](#)

[General purpose buckets](#)  
Directory buckets  
Table 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

Feature spotlight

**exp2-cc-dest-bucket**

[Objects](#) | [Metadata](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)

**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](#)

Find objects by prefix

☐ **Name** | ☐ **Type** | ☐ **Last modified** | ☐ **Size** | ☐ **Storage class**

|                          |                          |     |   |        |          |
|--------------------------|--------------------------|-----|---|--------|----------|
| <input type="checkbox"/> | <a href="#">kmit.jpg</a> | jpg | February 17, 2025, 10:56:22 (UTC+05:30) | 3.3 KB | Standard |
|--------------------------|--------------------------|-----|---|--------|----------|



Access control list (ACL)

Grant basic read/write permissions to AWS accounts. [Learn more](#)

| Grantee   | Objects                                  | Object ACL  |
|---|--|---|
| <b>Object owner (your AWS account)</b><br>Canonical ID: <a href="#">f43f7c3d8388bd45d3660c7960125d3d2f381a5799c8bb8d35aeddd22b2f704</a>           | <input checked="" type="checkbox"/> Read | <input checked="" type="checkbox"/> Read<br><input checked="" type="checkbox"/> Write |
| <b>Everyone (public access)</b><br>Group: <a href="#">http://acs.amazonaws.com/groups/global/AllUsers</a>   | <input checked="" type="checkbox"/> Read | <input checked="" type="checkbox"/> Read<br><input type="checkbox"/> Write            |
| <b>Authenticated users group (anyone with an AWS account)</b><br>Group: <a href="#">http://acs.amazonaws.com/groups/global/AuthenticatedUsers</a> | <input type="checkbox"/> Read            | <input type="checkbox"/> Read<br><input type="checkbox"/> Write                       |

When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.  
[Learn more](#)

☒ I understand the effects of these changes on this object.

**Access for other AWS accounts**  
No other AWS accounts associated with the resource.

[Add grantee](#)

**Specified objects**

| Name                     | Type | Version ID | Last modified                           | Size   |
|--------------------------|------|------------|---|--------|
| <a href="#">kmit.jpg</a> | jpg  | -          | February 17, 2025, 10:56:22 (UTC+05:30) | 3.3 KB |

[Cancel](#) [Save changes](#)

Kmit logo:- <https://exp2-cc-dest-bucket.s3.us-east-1.amazonaws.com/kmit.jpg>

