



JJ Tech

S3 Cross Region Replication

Replication enables automatic, asynchronous copying of objects across Amazon S3 buckets. Buckets that are configured for object replication can be owned by the same AWS account or by different accounts. Objects may be replicated to a single destination bucket or multiple destination buckets. Destination buckets can be in different AWS Regions or within the same Region as the source bucket.

By default, replication only supports copying new Amazon S3 objects after it is enabled. You can use replication to copy existing objects and clone them to a different bucket, but in order to do so, you must contact [AWS Support Center](#). When you contact support, give your AWS Support case the subject “Replication for Existing Objects” and include the following information:

- Source bucket
- Destination bucket or buckets
- Estimated storage volume to replicate (in terabytes)
- Estimated storage object count to replicate

To enable object replication, you add a replication configuration to your source bucket. The minimum configuration must provide the following:

- The destination bucket or buckets where you want Amazon S3 to replicate objects
- An AWS Identity and Access Management (IAM) role that Amazon S3 can assume to replicate objects on your behalf

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720





JJ Tech

Why use Replication:

Replication can help you do the following:

- **Replicate objects while retaining metadata** — You can use replication to make copies of your objects that retain all metadata, such as the original object creation time and version IDs. This capability is important if you need to ensure that your replica is identical to the source object.
- **Replicate objects into different storage classes** — You can use replication to directly put objects into S3 Glacier, S3 Glacier Deep Archive, or another storage class in the destination buckets. You can also replicate your data to the same storage class and use lifecycle policies on the destination buckets to move your objects to a colder storage class as it ages.
- **Maintain object copies under different ownership** — Regardless of who owns the source object, you can tell Amazon S3 to change replica ownership to the AWS account that owns the destination bucket. This is referred to as the *owner override* option. You can use this option to restrict access to object replicas.
- **Keep objects stored over multiple AWS Regions** — You can set multiple destination buckets across different AWS Regions to ensure geographic differences in where your data is kept. This could be useful in meeting certain compliance requirements.
- **Replicate objects within 15 minutes** — You can use S3 Replication Time Control (S3 RTC) to replicate your data in the same AWS Region or across different Regions in a predictable time frame. S3 RTC replicates 99.99 percent of new objects stored in Amazon S3 within 15 minutes (backed by a service level agreement).

+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermill Field Dr Bowie MD 20720





JJ Tech

When to use Cross-Region Replication:

S3 Cross-Region Replication (CRR) is used to copy objects across Amazon S3 buckets in different AWS Regions. CRR can help you do the following:

- **Meet compliance requirements** — Although Amazon S3 stores your data across multiple geographically distant Availability Zones by default, compliance requirements might dictate that you store data at even greater distances. Cross-Region Replication allows you to replicate data between distant AWS Regions to satisfy these requirements.
- **Minimize latency** — If your customers are in two geographic locations, you can minimize latency in accessing objects by maintaining object copies in AWS Regions that are geographically closer to your users.
- **Increase operational efficiency** — If you have compute clusters in two different AWS Regions that analyze the same set of objects, you might choose to maintain object copies in those Regions

Replication requires the following:

- The source bucket owner must have the source and destination AWS Regions enabled for their account. The destination bucket owner must have the destination Region-enabled for their account.

For more information about enabling or disabling an AWS Region, see [AWS Service Endpoints](#) in the *AWS General Reference*.

- Both source and destination buckets must have versioning enabled. For more information about versioning, see [Using versioning in S3 buckets](#).
- Amazon S3 must have permissions to replicate objects from the source bucket to the destination bucket or buckets on your behalf.

+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720





JJ Tech

- If the owner of the source bucket doesn't own the object in the bucket, the object owner must grant the bucket owner READ and READ_ACP permissions with the object access control list (ACL). For more information, see [Access control list \(ACL\) overview](#).
- If the source bucket has S3 Object Lock enabled, the destination buckets must also have S3 Object Lock enabled.

Demo:

For this demo we are going to create two new buckets in different regions and do the replication. FYI, you can follow the same process for existing buckets as well.

Create two buckets with versioning enabled.

You can anytime enable versioning after the bucket creation as well in the bucket properties.

JJ Tech

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermill Field Dr Bowie MD 20720



Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

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

- ☐ Disable
- ☒ Enable

Tags (0) - optional

Track storage cost or other criteria by tagging your bucket. [Learn more](#)

No tags associated with this bucket.

Default encryption

Automatically encrypt new objects stored in this bucket. [Learn more](#)

Server-side encryption

- ☒ Disable
- ☐ Enable

► Advanced settings

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

+1 (410) 8887049

contact@jjtechinc.co

www.jjtechinc.co

ermil Field Dr Bowie MD 20720





JJ Tech

- Once you create two buckets with versioning enabled, You have to navigate to the management tab on bucket 1.
- Then click create Replication rule.

The screenshot shows the Amazon S3 console interface. On the left is a navigation sidebar with options like Buckets, Access Points, and Storage Lens. The main content area is for the bucket 'jjtech-source-test-1'. The 'Management' tab is selected, indicated by a red arrow. Below the tabs, there are two sections: 'Lifecycle rules (0)' and 'Replication rules (0)'. The 'Replication rules' section shows a message 'No replication rules' and a 'Create replication rule' button, which is pointed to by another red arrow.

JJ Tech

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720



Services

Search for services, features, marketplace products, and

Amazon S3

jjtech-source-test-1

Replication rules

Create replication rule

Create replication rule

Replication rule configuration

Replication rule name

replication

Up to 255 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

jjtech-source-test-1

Source Region

US West (Oregon) us-west-2

Choose a rule scope

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

☒ This rule applies to *all* objects in the bucket

Destination

Destination

You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Same-Region Replication). You can also specify a different bucket for each rule in the configuration. [Learn more](#) or see [Amazon S3 pricing](#)

☒ Choose a bucket in this account

☐ Specify a bucket in another account

Bucket name

Choose the bucket that will receive replicated objects.

Enter bucket name

Browse S3

Destination Region

-

IAM role

IAM role

Create new role

View

Encryption

☐ Replicate objects encrypted with AWS KMS

You can use replication for AWS Key Management Service encrypted objects to replicate data encrypted using AWS KMS across AWS Regions.

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 provides replication metrics and notifications. Additional fees will apply. [Learn more](#)

☐ Replication metrics and notifications

Monitor the progress of your replication rule through Cloudwatch Metrics. 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 in this bucket to the destination bucket. [Learn more](#)

Cancel

Save

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

Ammermil Field Dr Bowie MD 20720





JJ Tech

- Once you click save, one replication rule is saved on bucket one.
- Test the replication rule by adding any objects to bucket one, you can see the same objects in bucket two in some time automatically.

Enable versioning on existing buckets:

Amazon S3 > jjtech-source-test-1

jjtech-source-test-1 [Info](#)

Objects **Properties** Permissions Metrics Management Access Points

Bucket overview

AWS Region US West (Oregon) us-west-2	Amazon Resource Name (ARN) arn:aws:s3::jjtech-source-test-1	Creation date August 20, 2021, 02:35:02 (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](#)

[Edit](#)

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

JJ Tech

+1 (410) 8887049
contact@jjtechinc.co

www.jjtechinc.co

14103 Hammermil Field Dr Bowie MD 20720

