

Create a S3 Bucket Replica from one AWS account to another AWS account

By: Nikhilesh Sakhare

1. Sign in to the AWS Management Console with credentials for the source AWS account (Account A) and open the Amazon S3 service home page.

The screenshot shows the AWS Management Console with the S3 service selected in the top navigation bar. The main content area displays the Amazon S3 homepage with the heading "Amazon S3" and the sub-headline "Store and retrieve any amount of data from anywhere". It includes a brief description of the service's features and a prominent "Create a bucket" button. On the left, a sidebar menu for "Amazon S3" lists various options like General purpose buckets, Directory buckets, Table buckets, Vector buckets, Access Grants, etc. At the bottom of the sidebar, there is a "Storage Lens" section and links for CloudShell, Feedback, and Console Mobile App.

2. Click Create bucket, select General purpose as the bucket type, choose region US East (N. Virginia) us-east-1, and enter a unique bucket name such as source-rep-nik, then leave block public access enabled and complete the creation.

The screenshot shows the "Create bucket" wizard in the AWS Management Console. The first step, "General configuration", is displayed. Under "Bucket type", the "General purpose" option is selected. The "Bucket name" field contains "source-rep-nik". Below the form, a note states that bucket names must be 3 to 63 characters and unique within the global namespace. A "Copy settings from existing bucket - optional" section is present, with a "Choose bucket" button and a note about copied settings. At the bottom, an "Object Ownership" section notes that object ownership is determined by ACLs. The footer of the page includes links for CloudShell, Feedback, and Console Mobile App, along with copyright information for 2025 and links for Privacy, Terms, and Cookie preferences.

3. Scroll down in the bucket-creation form and enable Bucket Versioning, which is required for replication, then create the 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

You can use bucket tags to analyze, manage and specify permissions for a bucket. [Learn more](#)

You can use s3>ListTagsForResource, s3:TagResource, and s3:UntagResource APIs to manage tags on S3 general purpose buckets for access control in addition to cost allocation and resource organization. To ensure a seamless transition, please provide permissions to s3>ListTagsForResource, s3:TagResource, and s3:UntagResource actions. [Learn more](#)

No tags associated with this bucket.

[Add new tag](#)

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

On the S3 console in Account A, the new source-rep-nik bucket now appears in the buckets list.

4. Switch to the source AWS account (Account B), open Amazon S3, and again click Create bucket. Use region US East (N. Virginia) us-east-1 and specify a bucket name such as dist-rep-nik; keep the type as General purpose.

Name	AWS Region	Creation date
dist-rep-nik	US East (N. Virginia) us-east-1	November 23, 2025, 12:15:44 (UTC+05:30)

General purpose buckets (1) [Info](#)

[Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Buckets are containers for data stored in S3.

Account snapshot [Info](#)

Updated daily [View dashboard](#)

Storage Lens provides visibility into storage usage and activity trends.

External access summary - new [Info](#)

Updated daily

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

Amazon S3 General purpose buckets All AWS Regions Directory buckets

General purpose buckets

Find buckets by name

Name AWS Region Creation date

dist-rep-nik US East (N. Virginia) us-east-1 November 23, 2025, 12:15:44 (UTC+05:30)

Block Public Access settings for this account

Storage Lens Dashboards

CloudShell Feedback Console Mobile App © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

5. Open the source-rep-nik bucket in Account A and choose the Management tab, where the Replication rules section initially shows “No replication rules”. Click Create replication rule to start configuring cross-account replication for this bucket.

The screenshot shows the AWS S3 Management console for the 'source-rep-nik' bucket. The 'Management' tab is selected. Under 'Lifecycle configuration', it says 'No lifecycle rules'. Under 'Replication rules (0)', it says 'No replication rules'. Both sections have a 'Create replication rule' button at the bottom.

6. On the Create replication rule page, enter a rule name such as different-account, set Status to Enabled, and leave Priority at 0.

The screenshot shows the 'Create replication rule' page. The 'Replication rule configuration' section includes fields for 'Replication rule name' (set to 'different-account'), 'Status' (radio button selected for 'Enabled'), and 'Priority' (set to '0').

- Under Source bucket, confirm the bucket name source-rep-nik and choose Apply to all objects in the bucket so every object will be replicated.

Source bucket

Source bucket name
source-rep-nik

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

Choose a rule scope
 Limit the scope of this rule using one or more filters
 Apply to all objects in the bucket

- In the Destination section of the same rule wizard, select Specify a bucket in another account. Enter the Account ID of the destination account (e.g., 346871994407) and type the previously created destination bucket name dist-rep-nik; the Destination Region remains US East (N. Virginia) us-east-1.

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

Account ID
346871994407

Bucket name
Choose the bucket that will receive replicated objects.
dist-rep-nik

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

Change object ownership to destination bucket owner
Objects in the source bucket not owned by the source bucket owner will be replaced with access policy that grants full permission to the destination bucket owner

Check the option Change object ownership to destination bucket owner so that replicated objects are owned and fully manageable by Account B's bucket owner.

- In the IAM role section of the replication rule, choose Create new role so Amazon S3 automatically creates a role that it will assume to perform replication.

IAM role

Permission to access the specified resources
 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

Additional replication options

After the rule is saved, S3 creates a service role with a name like s3crr_role_for_source-rep-nik that has permission to read from the source bucket and write to the destination bucket.

- Once all settings are reviewed, scroll to the bottom and click Save to create and enable the replication rule. Verify that the rule different-account is listed with Status: Enabled, destination bucket s3://dist-rep-nik, region us-east-1, scope Entire bucket, and replica owner set to Destination bucket owner. The IAM role column links to the auto-created role s3crr_role_for_source-rep-nik, confirming that S3 has everything required to perform replication.

Screenshot of the AWS S3 Replication rules configuration page.

Source bucket: source-rep-nik

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

IAM role: s3crr_role_for_source-rep-nik

Replication rules (1)

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
different-account	Enabled	s3://dist-rep-nik	US East (N. Virginia) us-east-1	0	Entire bucket	Same as source	Destination bucket owner	Disabled	Do not replicate	Disabled

11. To allow the S3 replication role from Account A to write into dist-rep-nik, open a new browser tab with the AWS Policy Generator set to S3 Bucket Policy.

Configure the statement with:

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, [key concepts in Using AWS Identity and Access Management](#).

Step 1: Select policy type
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.

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

Principal: arn:aws:iam::673586847111:role/service-role/s3crr_role_for_source-rep-nik

Actions: All Actions ("")
-Select Actions-
ReplicateDelete X | ReplicateObject X | GetObject X | PutObject X

Amazon Resource Name (ARN): All Resources ("")
arn:aws:s3:::dist-rep-nik

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

Add conditions (optional)

Add Statement

12. Click Add Statement and then Generate Policy to view the JSON document, which looks like this in the Policy Generator preview.

Statements added (1)
You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource(s)	Condition(s)	Remove
arn:aws:iam::673586849368:role/service-role/s3crr_role_for_source-rep-nik	Allow	s3:ReplicateDelete s3:ReplicateObject s3:GetObject s3:PutObject	arn:aws:s3:::dist-rep-nik	None	Remove

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.

[Generate Policy](#)

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 your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2025, Amazon Web Services or its affiliates. All rights reserved.

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

[Add conditions \(optional\)](#)

[Add Statement](#)

Statements added (1)
You added the following statements. Click the button below to Generate a policy.

Principal(s)
arn:aws:iam::673586849368:role/service-role/s3crr_role_for_source-rep-nik

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.

[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.

```
1 * []
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Allow",
7       "Principal": {
8         "AWS": "arn:aws:iam::673586849368:role/service-role/s3crr_role_for_source-rep-nik"
9       },
10      "Action": [
11        "s3:ReplicateDelete",
12        "s3:ReplicateObject",
13        "s3:GetObject",
14        "s3:PutObject"
15      ],
16      "Resource": "arn:aws:s3:::dist-rep-nik"
17    }
18  ]
19 }
```

Condition(s) | Remove
None | [Remove](#)

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 your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2025, Amazon Web Services or its affiliates. All rights reserved.

[Close](#) | [Copy Policy](#)

13. Copy this JSON and go back to Account B's S3 console, open the dist-rep-nik bucket Permissions tab, and edit the Bucket policy.

Block public access (bucket settings)

Block all public access On

► Individual 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](#)

ⓘ Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [using Amazon S3 Block Public Access](#)

No policy to display.

14. Paste the generated policy and save; the editor now shows the full bucket policy granting the replication role permissions on the destination bucket.

```

arn:aws:s3:::dist-rep-nik
1 Version: "2012-10-17",
2 Statement: [
3   {
4     Sid: "Statement1",
5     Effect: "Allow",
6     Principal: [
7       "arn:aws:iam::673586841111:role/service-role/s3crr_role_for_source-rep-nik"
8     ],
9     Action: [
10       "s3:ReplicateDelete",
11       "s3:ReplicateObject",
12       "s3:GetObject",
13       "s3:PutObject"
14     ],
15     Resource: "arn:aws:s3:::dist-rep-nik/*"
16   }
17 ]
18
19

```

Edit statement

Select a statement

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

+ Add new statement

15. In the source-rep-nik bucket's Objects tab, click Upload, add a test file such as nik_accessKeys.csv, and start the upload.

The screenshot shows the AWS S3 console with the 'source-rep-nik' bucket selected. The 'Objects' tab is active. At the top right, there are several buttons: 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and a large orange 'Upload' button. Below these are search and filter fields for 'Name', 'Type', 'Last modified', 'Size', and 'Storage class'. A message states 'No objects' and 'You don't have any objects in this bucket.' A blue 'Upload' button is located at the bottom right of the object list area.

The screenshot shows the 'Upload' wizard for the 'source-rep-nik' bucket. The 'Files and folders' section lists one item: 'nik_accessKeys.csv' (text/csv, 99.0 B). There are buttons for 'Remove', 'Add files', and 'Add folder'. Below this is the 'Destination' section, which shows the destination as 's3://source-rep-nik'. The 'Destination details' section contains a note about bucket settings. At the bottom, there are sections for 'Permissions' and 'Properties'. The footer includes links for CloudShell, Feedback, and Console Mobile App, along with copyright information for 2025 and links for Privacy, Terms, and Cookie preferences.

16. The upload page shows the file listed under Files and folders with the destination s3://source-rep-nik, and once the upload completes the object appears in the source bucket.

The screenshot shows the AWS S3 console interface. At the top, there's a green success message: "Upload succeeded" with a link to "Files and folders table". Below it, a note says "After you navigate away from this page, the following information is no longer available." The main area is titled "Summary" and shows the destination "s3://source-rep-nik". It indicates 1 file was uploaded successfully (Succeeded) and 0 files failed (Failed). Under "Files and folders", there's a table showing one file: "nik_accessKeys.csv" (text/csv, 99.0 B, Status: Succeeded). The bottom of the screen includes standard AWS navigation links like CloudShell, Feedback, and Console Mobile App, along with copyright and legal information.

17. After a short delay, open the dist-rep-nik bucket in Account B and confirm that the same object now appears there, proving that cross-account replication from Account A to Account B is working.

The screenshot shows the AWS S3 console for the "dist-rep-nik" bucket in Account B. The left sidebar shows the "General purpose buckets" section with various options like Directory buckets, Table buckets, Vector buckets, Access Grants, etc. The main content area is titled "dist-rep-nik" and shows the "Objects" tab selected. It displays one object: "nik_accessKeys.csv" (csv, 99.0 B, Last modified: November 23, 2025, 12:34:45 UTC+05:30, Storage class: Standard). There are buttons for Actions, Create folder, and Upload. The bottom of the screen includes standard AWS navigation links like CloudShell, Feedback, and Console Mobile App, along with copyright and legal information.