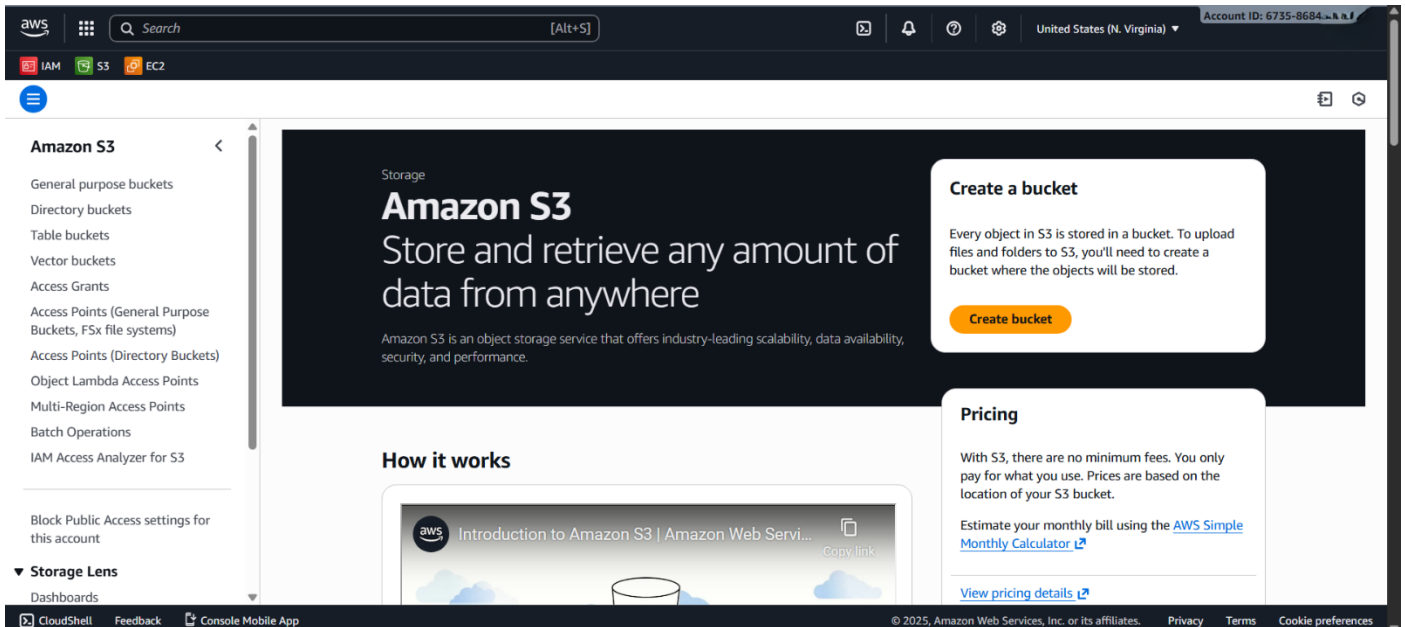


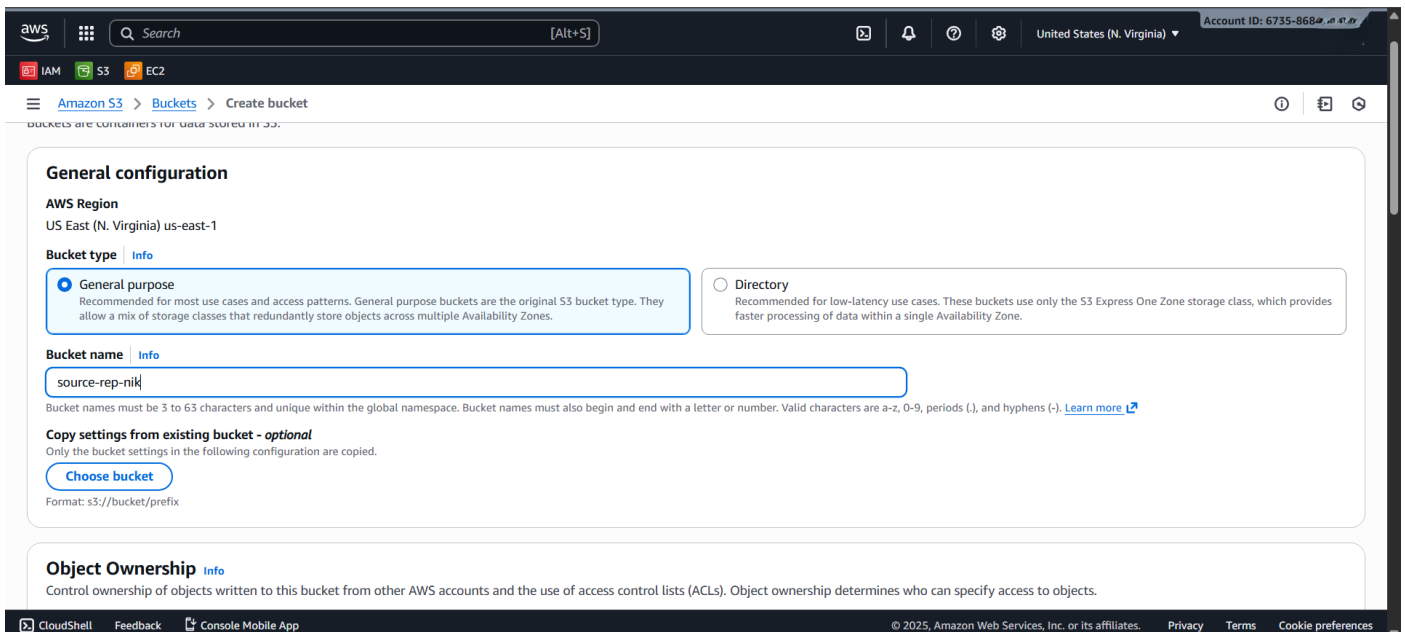
Create a S3 Bucket Replica from one AWS account to another AWS account

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.



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.



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

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 - 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](#)

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.

Amazon S3

General purpose buckets

Directory buckets

Table buckets

Vector buckets

Access Grants

Access Points (General Purpose Buckets, FSx file systems)

Access Points (Directory Buckets)

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

General purpose buckets (1)

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

Buckets are containers for data stored in S3.

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

Account snapshot

Updated daily

[View dashboard](#)

Storage Lens provides visibility into storage usage and activity trends.

External access summary - new

Updated daily

[Info](#)

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

- 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 Management Console for the 'source-rep-nik' bucket. The left sidebar shows the navigation menu with 'Amazon S3' selected. The main content area is divided into three sections: 'Lifecycle configuration', 'Replication rules (0)', and 'Inventory configurations (0)'. Each section has a 'Create' button and a 'Learn more' link. The 'Replication rules' section is the focus of the task.

source-rep-nik

Objects | Metadata | Properties | Permissions | Metrics | **Management** | Access Points

Lifecycle configuration

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.

Lifecycle rules

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 na...	Status	Scope	Current version ...	Noncurrent versi...	Expired object d...	Incomplete mul...
No lifecycle rules						
There are no lifecycle rules for this bucket.						

[Create lifecycle rule](#)

Replication rules (0)

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 (KMS or DSSE-KM)
No replication rules									
You don't have any rules in the replication configuration.									

[Create replication rule](#)

Inventory configurations (0)

You can create inventory configurations on a bucket to generate a flat file list of your objects and metadata. These scheduled reports can include all objects in the bucket or be limited to a shared prefix. [Learn more](#)

[Create inventory configuration](#)

- 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 in the AWS Management Console. The 'Replication rule configuration' section is visible, showing the 'Replication rule name' field with the value 'different-account'. The 'Status' section shows the 'Enabled' radio button selected. The 'Priority' section shows the value '0'.

Create replication rule [Info](#)

Replication rule configuration

Replication rule name

different-account

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

- 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

CloudShell Feedback Console Mobile App

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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.

The screenshot shows the AWS IAM console's 'Replication rules' page for the bucket 'source-rep-nik'. The source bucket is 'source-rep-nik' in the 'US East (N. Virginia) us-east-1' region. The IAM role is 's3crr_role_for_source-rep-nik'. Below, a table lists one replication rule named 'different-account', which is 'Enabled'. It replicates from 's3://dist-rep-nik' in 'US East (N. Virginia) us-east-1' with a priority of 0, scope of 'Entire bucket', storage class 'Same as source', replica owner 'Destination bucket owner', replication time control 'Disabled', KMS-encrypted objects 'Do not replicate', and replica modification sync 'Disabled'.

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:

The screenshot shows the AWS Policy Generator tool. In 'Step 1: Select policy type', 'S3 Bucket Policy' is selected. In 'Step 2: Add statement(s)', the 'Effect' is 'Allow'. The 'Principal' is 'arn:aws:iam::673586847111:role/service-role/s3crr_role_for_source-rep-nik'. Under 'Actions', 'ReplicateDelete', 'ReplicateObject', 'GetObject', and 'PutObject' are selected. The 'Amazon Resource Name (ARN)' is 'arn:aws:s3:::dist-rep-nik'. The 'Add Statement' button is at the bottom.

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

Condition(s)

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.

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 {}
```

1:1 JSON

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.

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.

The screenshot shows the AWS S3 console interface. On the left, the navigation pane is open, showing the 'Amazon S3' section with 'General purpose buckets' selected. The main content area is titled 'dist-rep-nik' and has tabs for 'Objects', 'Metadata', 'Properties', 'Permissions' (selected), 'Metrics', 'Management', and 'Access Points'. Under the 'Permissions' tab, there is a 'Permissions overview' section with an 'Access finding' link. Below that is the 'Block public access (bucket settings)' section, which shows 'Block all public access' is turned on. A 'Bucket policy' section follows, indicating that public access is blocked because Block Public Access settings are turned on. The policy editor shows '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.

The screenshot shows the 'Edit bucket policy' page in the AWS S3 console. The navigation pane is the same as in the previous screenshot. The main content area is titled 'arn:aws:s3:::dist-rep-nik' and has a 'Policy' tab. The policy editor shows a JSON policy with the following content:

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Allow",
7       "Principal": {
8         "AWS": "arn:aws:iam::673586801000: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 }
```

On the right side of the policy editor, there is a section titled 'Edit statement' with a 'Select a statement' button and a 'Select an existing statement in the policy or add a new statement.' message. Below this is a '+ Add new statement' button.

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 Management Console interface for the 'source-rep-nik' bucket. The 'Objects' tab is selected, displaying a list of objects (currently empty). The 'Upload' button is highlighted in orange. The console header shows the AWS logo, search bar, and account information (United States (N. Virginia), Account ID: 6735-8684).

source-rep-nik Info

Objects (0)

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

Show versions

No objects
You don't have any objects in this bucket.

Upload

The screenshot shows the AWS Management Console interface for the 'source-rep-nik' bucket's Upload page. The 'Add files' button is highlighted in blue. The console header shows the AWS logo, search bar, and account information (United States (N. Virginia), Account ID: 6735-8684).

Files and folders (1 total, 99.0 B)

All files and folders in this table will be uploaded.

Find by name

Name	Folder	Type	Size
nik_accessKeys.csv	-	text/csv	99.0 B

Destination Info

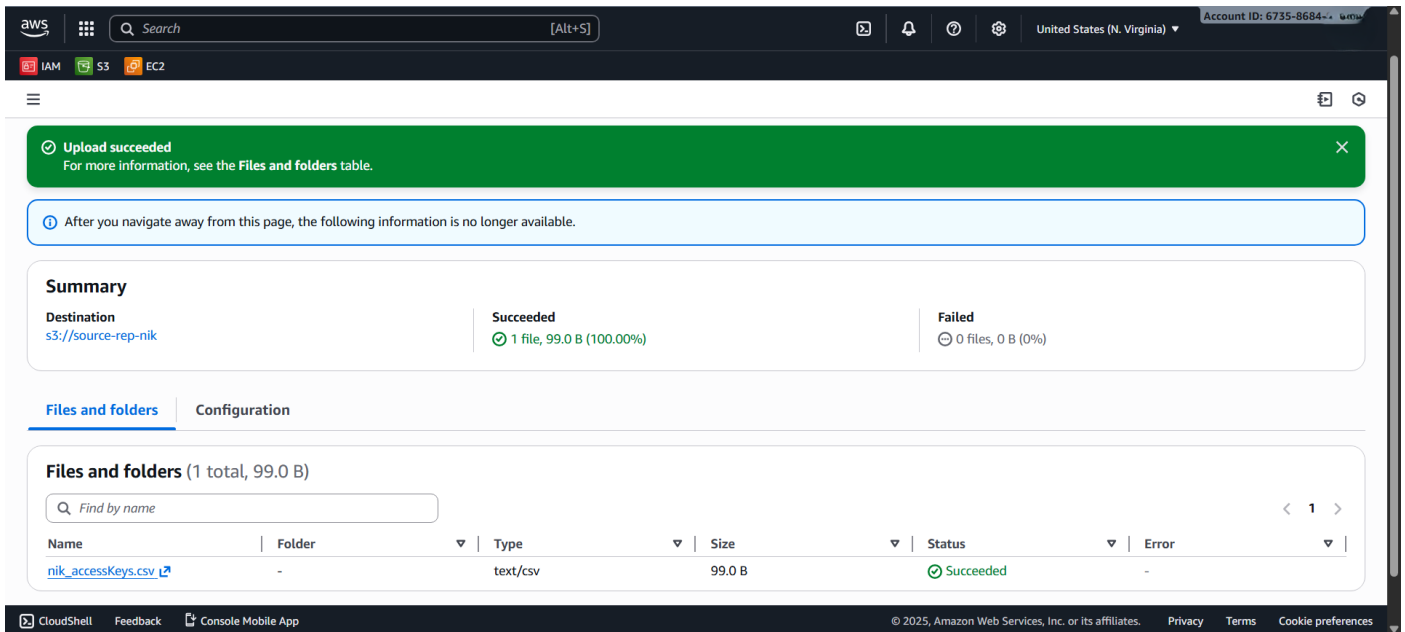
Destination
[s3://source-rep-nik](#)

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

Permissions
Grant public access and access to other AWS accounts.

Properties
Grant public access and access to other AWS accounts.

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.



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

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

Summary

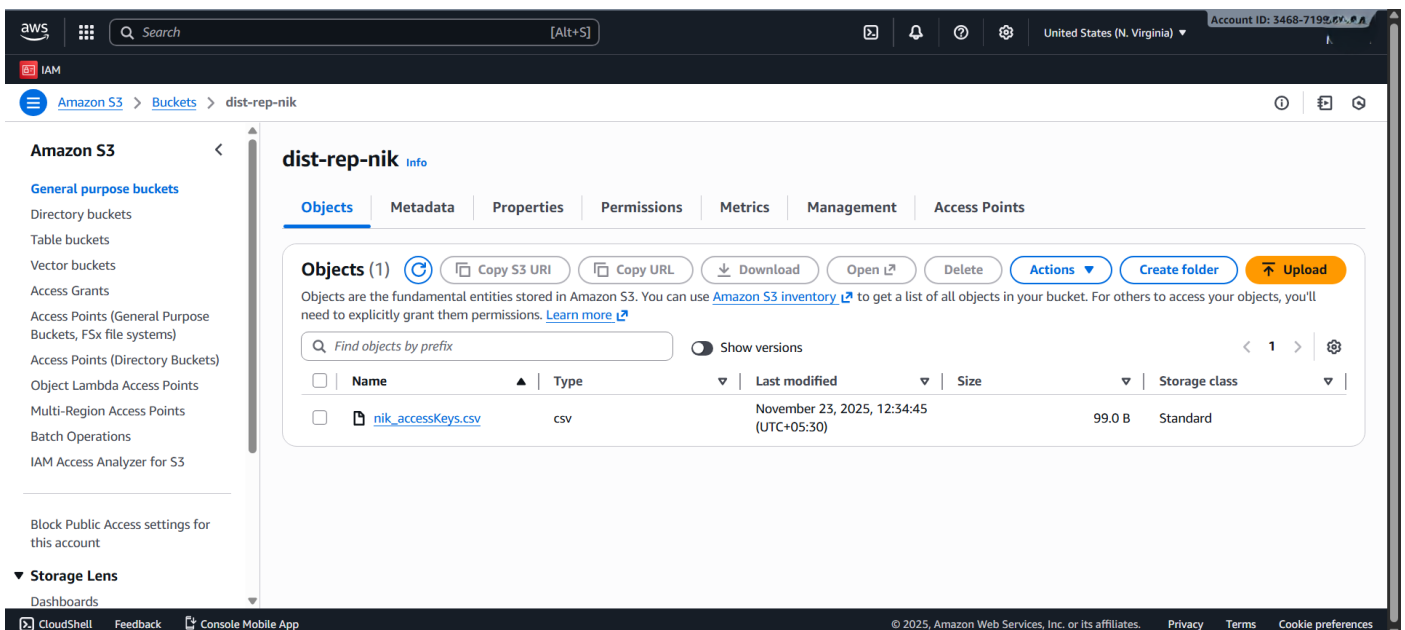
Destination s3://source-rep-nik	Succeeded 1 file, 99.0 B (100.00%)	Failed 0 files, 0 B (0%)
-------------------------------------------	----------------------------------------------	------------------------------------

Files and folders (1 total, 99.0 B)

Find by name

Name	Folder	Type	Size	Status	Error
nik_accessKeys.csv	-	text/csv	99.0 B	Succeeded	-

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.



dist-rep-nik

Info

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

Show versions

Name	Type	Last modified	Size	Storage class
nik_accessKeys.csv	csv	November 23, 2025, 12:34:45 (UTC+05:30)	99.0 B	Standard