

Steps for Amazon S3 Cross-Region Replication (CRR) to Another AWS Account

1. Create Source and Destination Buckets

- Source Bucket: Create in your account (e.g., "ogbuc1" in US East, N. Virginia).
 - Destination Bucket: Create in the other AWS account (e.g., "repbuc404" in Asia Pacific, Singapore).
 - Go to Amazon S3 console → "Create bucket".
 - Source Bucket:
 - Region: US East (N. Virginia)
 - Name: `ogbuc1`
 - Leave Object Ownership: Bucket owner enforced.
 - Leave Block All Public Access setting ON.
 - Enable Versioning under Bucket Versioning.
 - Leave encryption (SSE-S3) as default.
 - Click Create bucket.
 - Destination Bucket:
 - Log into the other AWS account.
 - Region: Asia Pacific (Singapore)
 - Name: `repbuc404`
 - Same settings: Owner enforced, block public access, enable versioning, default encryption.
 - Click Create bucket.
-

2. Enable Versioning

- Enable bucket versioning on both source and destination buckets. Versioning must be enabled for replication to work.

Set Google Chrome as your default browser and pin it to your taskbar [Set as default](#)

Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

[Create bucket](#)

Pricing

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.


Estimate your monthly bill using the [AWS Simple Monthly Calculator](#)

[View pricing details](#)

Resources

- [User guide](#)
- [API reference](#)
- [FAQs](#)

How it works



[Amazon S3](#) > [Buckets](#) > Create bucket

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

oghucl

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), hyphens (-), and underscores (_). [Learn More](#)

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

Object 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

[Amazon S3](#) > [Buckets](#) > Create bucket

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.

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

aws

Search

[Alt+S]

United States (N. Virginia)

Account ID: 9959-3823-3352

Harry-404

Amazon S3

Buckets

Create bucket

Tags - optional (0)

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

No tags associated with this bucket.

Add new tag

You can add up to 50 tags.

Default encryption

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

Encryption type

☒ 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.

Cancel

Create bucket

Set Google Chrome as your default browser and pin it to your taskbar

Set as default

aws

Search

[Alt+S]

Asia Pacific (Singapore)

Account ID: 9959-3823-3352

Harry-404

Amazon S3

Buckets

Create bucket

Buckets are containers for data stored in S3.

General configuration

AWS Region

Asia Pacific (Singapore) ap-southeast-1

Bucket type

☒ 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 specialized low-latency use cases supported by AWS Availability Zones or data residency use cases supported by AWS Local Zones.

Bucket name

repbuc404

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

Object Ownership

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.

Amazon S3

Buckets

Create bucket

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 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.

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 new tag

You can add up to 50 tags.

Default encryption

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

Encryption type

☒ 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](#)

Amazon S3 > Buckets > Create bucket

Default encryption

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

Encryption type

☒ 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.

Cancel

Create bucket

Amazon S3 > Buckets

General purpose buckets

All AWS regions

Directory buckets

General purpose buckets (2)

Buckets are containers for data stored in S3.

Find buckets by name

< 1 >

Name	AWS Region	Creation date
ogbuc1	US East (N. Virginia) us-east-1	August 13, 2025, 11:22:10 (UTC+05:30)
rgpbuc404	Asia Pacific (Singapore) ap-southeast-1	August 13, 2025, 11:29:35 (UTC+05:30)

Account snapshot

Updated daily

Storage Lens provides visibility into storage usage and activity trends.

[View dashboard](#)

External access summary - new

Updated daily

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

Amazon S3 > Buckets > ogbuc1

ogbuc1

Objects

Metadata

Properties

Permissions

Metrics

Management

Access Points

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

< 1 >

Name	Type	Version ID	Last modified	Size	Storage class
No objects You don't have any objects in this bucket.					

Upload

3. Upload an Object to Source Bucket

- In S3 console, click `ogbuc1` → Upload.
- Add a file (e.g., `Screenshot 2025-08-04 114432.png`).
- Confirm upload completed.

The screenshot displays the AWS S3 console's 'Upload' interface. At the top, the breadcrumb navigation shows 'Amazon S3' > 'Buckets' > 'ogbuc1' > 'Upload'. The main heading is 'Upload' with an 'info' link. Below this, a message states: '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](#).' A dashed box contains the instruction: 'Drag and drop files and folders you want to upload here, or choose [Add files](#) or [Add folder](#).' Below this is a section titled 'Files and folders (1 total, 151.1 KB)' with a 'Remove' button and 'Add files' and 'Add folder' buttons. A search bar labeled 'Find by name' is present. A table lists the upload: one file named 'Screenshot 2025-08-04 114432.png' of type 'image/png' and size '151.1 KB'. Below the table is the 'Destination' section, showing the path 's3://ogbuc1' and expandable details for 'Permissions' and 'Properties'. At the bottom right are 'Cancel' and 'Upload' buttons.

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 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, 151.1 KB)

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	Screenshot 2025-08-04 114432.png	-	image/png	151.1 KB

Destination info

Destination
[s3://ogbuc1](#)

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](#)

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.

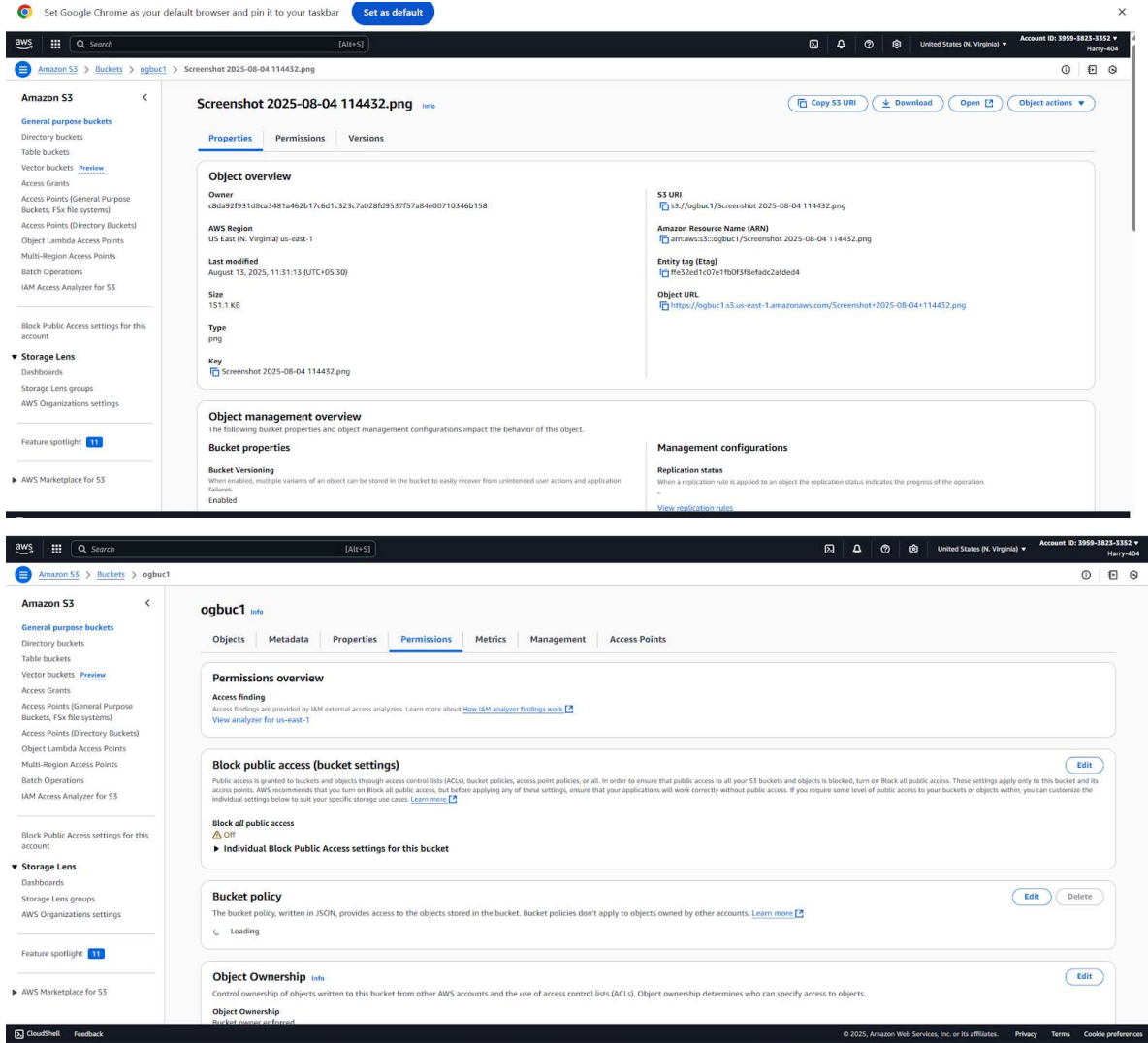
Summary

Destination s3://ogbuc1	Succeeded 1 File, 151.1 KB (100.00%)	Failed 0 Files, 0 B (0%)
---	--	------------------------------------

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

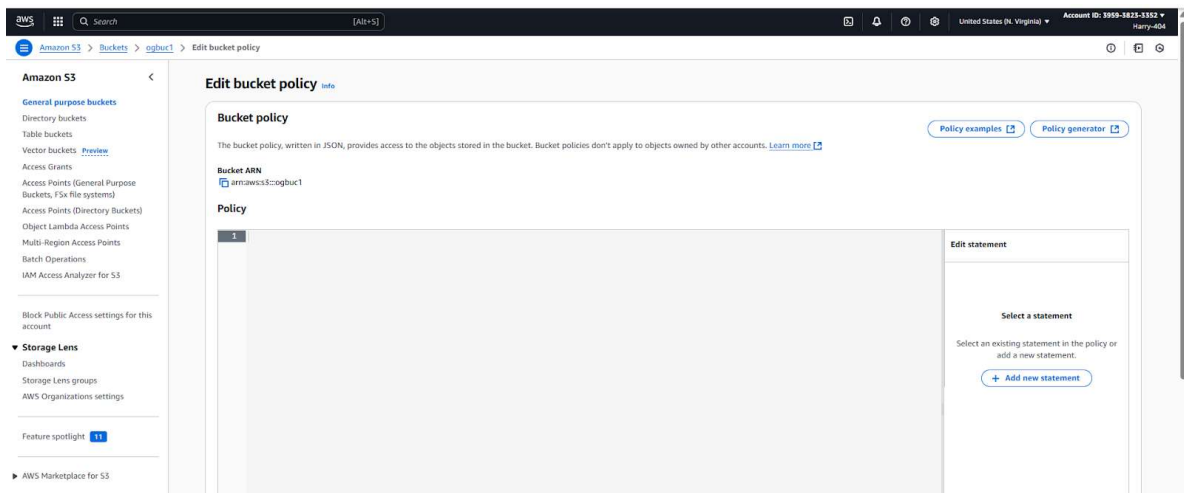
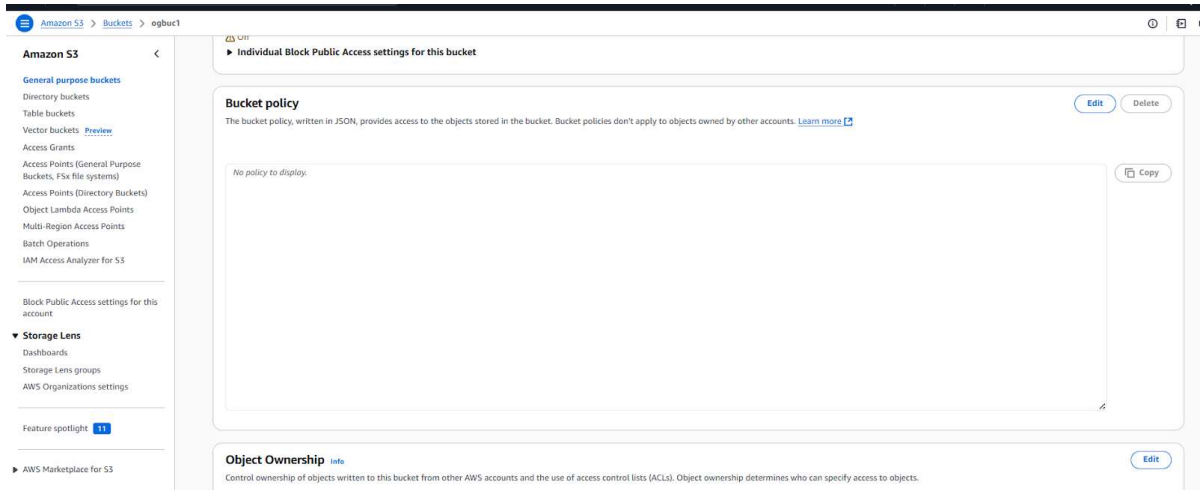
Files and folders (1 total, 151.1 KB)

Name	Folder	Type	Size	Status	Error
Screenshot 2025-08-04 114432.png	-	image/png	151.1 KB	Succeeded	-



4. Set Up Permissions for Replication

- **IAM Role:** Create an IAM role in the source account with permissions to read objects from the source bucket and write objects to the destination bucket.
 - The destination bucket policy in the other account must allow the replication role to write objects (put object) and update object tags.



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
☐ Deny

Principal

*

Use a comma to separate multiple values.

Actions

☐ All Actions (***)

--Select Actions--

GetObject

Amazon Resource Name (ARN)

☐ All Resources (***)

arn:aws:s3:::ogbuc1/*

ARN should follow the following format: arn:aws:s3:::(BucketName)/(Key/Name). Use a comma to separate multiple values.

(Add Statement)

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
*	Allow	s3:GetObject	arn:aws:s3:::ogbuc1/*	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.

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       "Action": [  
9         "s3:GetObject"  
10      ],  
11      "Resource": "arn:aws:s3:::ogbuc1/*"  
12    }  
13  ]  
14 }
```

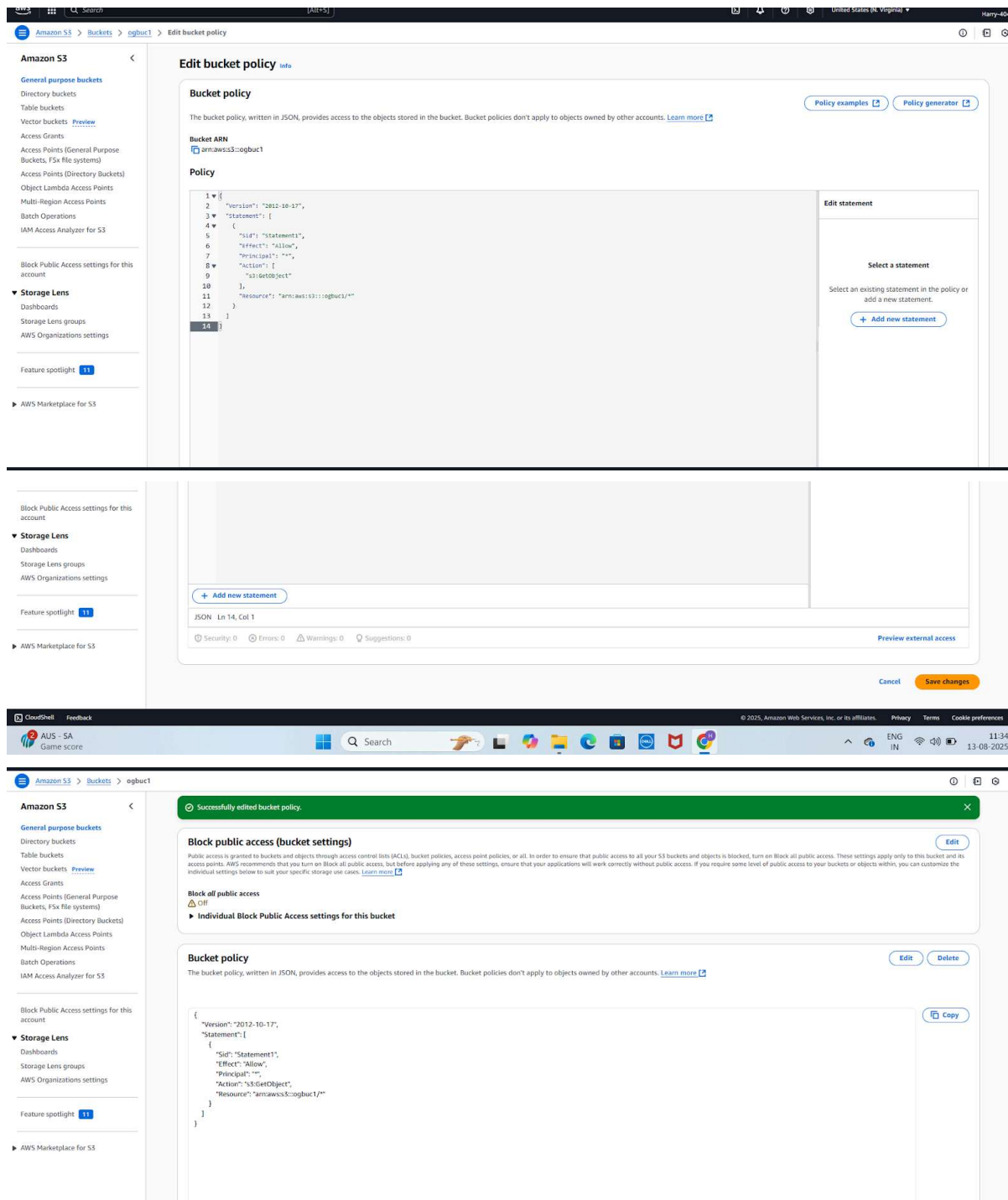
1:1 JSON

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](#)

of Amazon Web Services technologies.



5. Create the Replication Rule in Source Bucket

1. Go to S3 → Buckets → **ogbuc1** → Management → Replication rules → Create replication rule.
2. Rule name: **demo**

3. Enable rule.
4. Scope: "Apply to all objects in the bucket" (or set a prefix if only certain objects).
5. Destination bucket:
 - Enter "Account number" → 883915072455 → enter the destination bucket name `replica-tejas`
6. IAM Role: Select `s3crr_role_for_ogbuc1`.
7. Leave Storage class, Replica owner, Encryption as in your PDF (Same as source, Replica ownership same as source, etc.).
8. Save.

The screenshot shows the Amazon S3 console interface for the 'ogbuc1' bucket. The 'Management' tab is selected, displaying the 'Lifecycle configuration' section. This section includes 'Lifecycle rules' and 'Replication rules' tables, both of which are currently empty. Below the screenshot, the 'Create replication rule' form is shown, detailing the configuration for a new rule named 'demo'.

Create replication rule configuration

Replication rule name
demo

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: ogbuc1
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

Filter type
You can filter objects by prefix, object tags, or a combination of both.
Prefix
Add a filter to limit the scope of this rule to a single prefix.

Don't include the bucket name in the prefix. Using certain characters in key names can cause problems with some applications and protocols.

Amazon S3

Buckets

ogbuc1

Replication rules

Create replication rule

☐ Apply to all objects in the bucket

Filter type
 You can filter objects by prefix, object tags, or a combination of both.
Prefix
 Add a filter to limit the scope of this rule to a single prefix.

Tags
 You can limit the scope of this rule to the key value pairs added below.

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

Bucket name
 Choose the bucket that will receive replicated objects.

Destination Region
 Asia Pacific (Singapore) ap-southeast-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

☐ 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

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 DSE-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](#)

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Amazon S3

Buckets

ogbuc1

Replication rules

Create replication rule

☒ 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 DSE-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

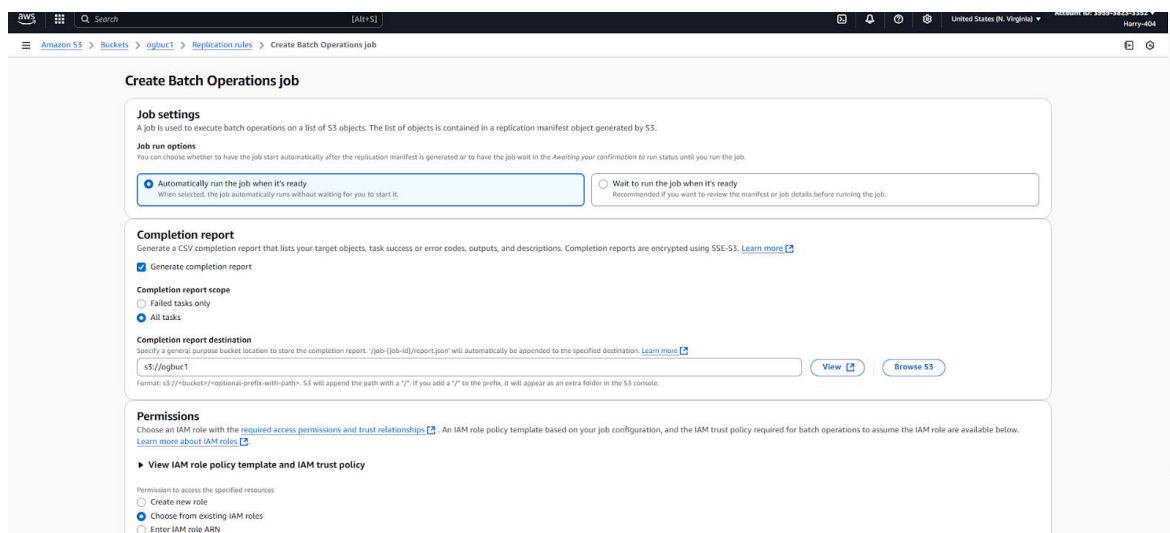
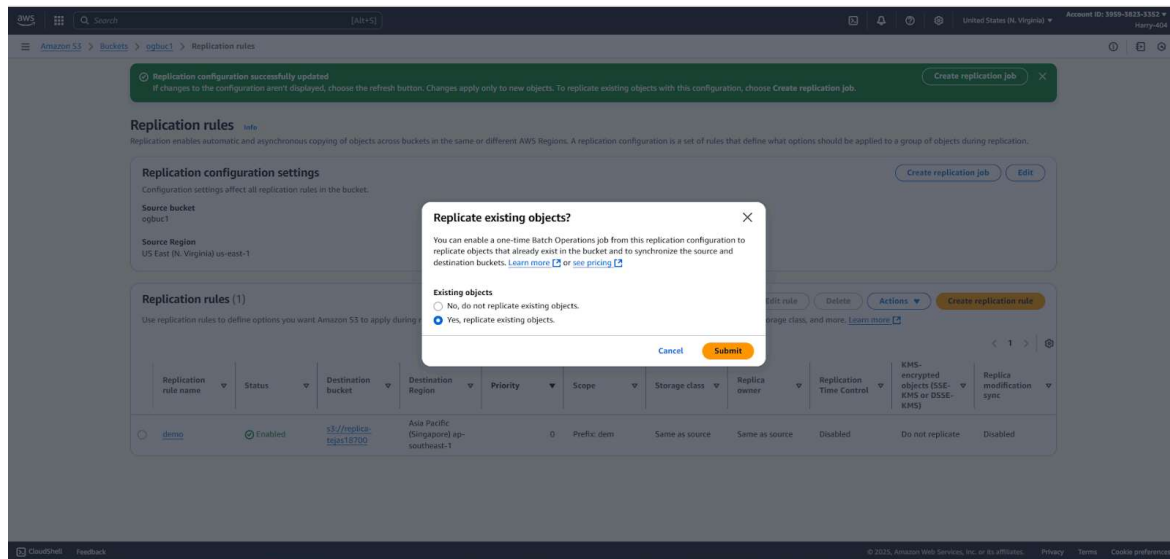
Save

6. Replicate Existing Objects

From your PDF: after creating the rule you got the "Create replication job" option.

If you want existing files moved (not just new ones):

1. Click Create replication job.
2. Use the default “Automatically run the job” or choose “Wait to run the job” for review.
3. Report destination: `s3://ogbuc1` as in PDF.
4. Permissions: Pick the same replication IAM role or a new batch operations role allowing `s3:GetObject` on source + `s3:PutObject` on destination.
5. Run job.



Amazon S3 > Buckets > ogbuc1 > Replication rules > Create Batch Operations job

Run job 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

All tasks

Completion report destination

Specify a general purpose bucket location to store the completion report. `{job-id}/report.json` will automatically be appended to the specified destination. [Learn more](#)

s3://ogbuc1

View

Browse S3

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

Permission to access the specified resources

Create new role

Choose from existing IAM roles

Enter IAM role ARN

IAM role

s3cmr_role_for_ogbuc1

View

Cancel

Save

Amazon S3 > Batch Operations

Successfully created job ID `c121c7db-6590-4805-b974-3d523ba3db44`

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.

View details

Batch Operations

A job is used to execute batch operations on a list of S3 objects. Job events are published to [CloudWatch Events](#).

Jobs (1)

Search by job ID or description

All status types

Run job

Actions

Close job

Create job

Job ID	Status	Description	Operation	Date created	Total objects	% Complete	Total failed (rate)	Priority
c121c7db-6590-4805-b974-3d523ba3db44	Preparing	2025-08-13 - Replicate	Replicate	August 13, 2025, 11:46:59 (UTC+05:30)	0	0%	0 (0%)	10

Amazon S3 > Buckets > ogbuc1

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 name

Status

Scope

Current version actions

Noncurrent versions actions

Expired object delete mar...

Incomplete multipart upl...

No lifecycle rules

There are no lifecycle rules for this bucket.

Create lifecycle rule

Replication rules (1)

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
demo	Enabled	s3://replica-trajax187080	Asia Pacific (Singapore) ap-southeast-1	0	Prefix: dem	Same as source	Same as source	Disabled	Do not replicate	Disabled

View replication configuration

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](#)

Name

Status

Scope

Destination

Frequency

Last export

Format

Create inventory configuration

CloudShell

Feedback

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

28°C Light rain

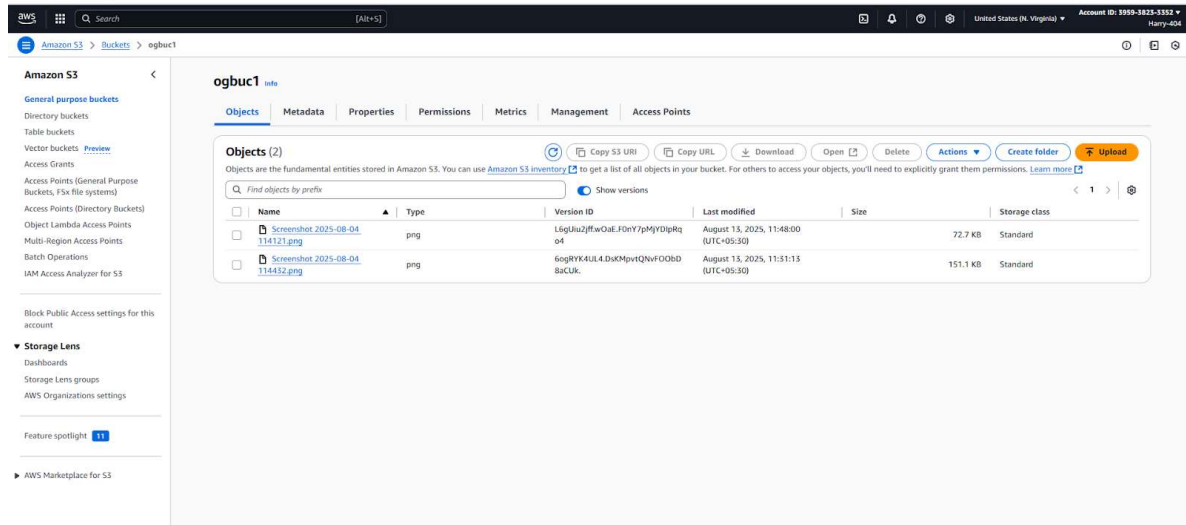
Search

ENG IN

11:49 13-08-2025

6. Test & Verify

- Upload a file to `ogbuc1`.
- Wait a few minutes — in `replica-tejas` it should appear with `Replication status: COMPLETED`.
- Check Object properties in destination bucket for replication status



In the same way this steps will be followed by other user at there end and send me so the file be synced at repbuc404

Once both replications are active:

- Your uploads to `ogbuc1` → go to `replica-tejas`
- Their uploads to `original-tejas` → come to your `repbuc404`

This achieves near-real-time two-way sync (subject to the replication delay) as long as you use separate prefixes to avoid loops.

Quick Reference Table

Step	Source Account Action	Destination Account Action
Create buckets	Create and configure "ogbuc1" (versioning ON)	Create and configure "repbuc404" (versioning ON)
IAM Permissions	Create replication role, assign necessary policies	Set bucket policy to allow role to write
Replication Rule	Set up CRR in S3 console	
Batch Operations	(Optional) Create job for existing objects	
Monitor	Use console for status, reports	