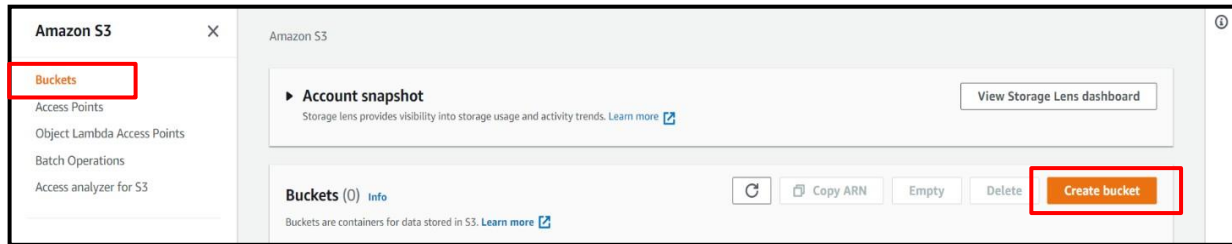


## Enable cross-region replication.

Objectives:

1. Learn to enable cross-region replication of an S3 Bucket.

Step 1: In AWS console go to **S3** services. Select **Buckets** and click on **Create bucket**

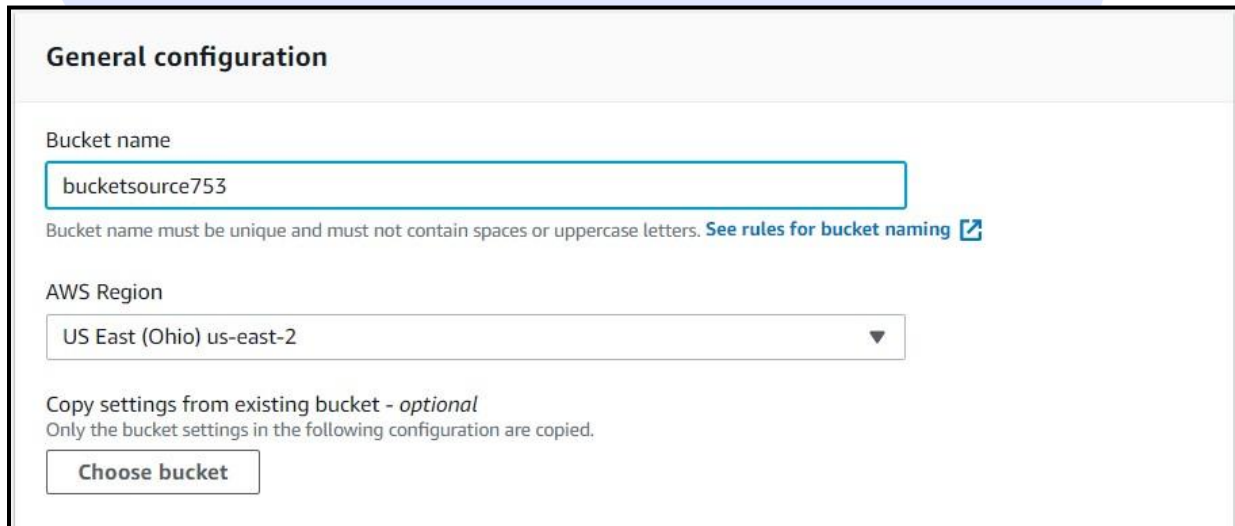


Step 2: Give a **Bucket name** to this **source bucket**.

Here **bucketsource753** is a random name chosen for your bucket.

You may have to try giving a different name if your required bucket name is already being used by some other AWS user.

**Note the region.** Here it is **US East (Ohio)**



**General configuration**

Bucket name  
bucketsource753  
Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region  
US East (Ohio) us-east-2

Copy settings from existing bucket - *optional*  
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Uncheck the checkbox which says **Block Public Access settings for this bucket** and check the acknowledge it by checking the box below.

## 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

Make sure you **Enable** the **Bucket Versioning** option.

Scroll Down and click on **Create Bucket**

# Cloud Plus Plus Services



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

Cancel

Create bucket

Step 3: Create a **destination bucket**, follow Step 2 up to this point. Select a **different region**. Here the name is **bucketdestination7531** and region is selected as Asia Pacific (Mumbai).

**Buckets (2)** [Info](#)

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

Find buckets by name

	Name	AWS Region	Access	Creation date
<input type="radio"/>	bucketdestination7531	Asia Pacific (Mumbai) ap-south-1	Objects can be public	August 17, 2021, 12:17:11 (UTC+05:30)
<input type="radio"/>	bucketsource753	US East (Ohio) us-east-2	Objects can be public	August 17, 2021, 11:54:09 (UTC+05:30)

Step 4: Click on the Hyperlink of **Source Bucket** and in bucket details click on **Management**

[Amazon S3](#) > bucketsource753

## bucketsource753

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

Scroll down and in **Replications Rules**, Click on **Create Replication 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](#)

[View details](#) [Edit rule](#) [Delete](#) [Actions](#) [Create replication rule](#)

Replication rule name	Status	Destination bucket	Destination Region	Priority	Scope	Storage class	Replica owner	Replication Time Control	KMS-encrypted objects	Replica modification sync
No replication rules										
You don't have any rules in the replication configuration.										
<a href="#">Create replication rule</a>										

Step 5: Under **Replication Rule Name**, provide a name for the replication rule. Here, it is given as **ReplicationRuleid1**.

### Replication rule configuration

Replication rule name

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

Under **Source Bucket** select **This rule applies to all objects in the bucket**

### Source bucket

Source bucket name

bucketsource753

Source Region

US East (Ohio) us-east-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

# Cloud Plus Plus Services



For Destination click on **Browse S3** and select your **Destination 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.

**Destination Region**  
-

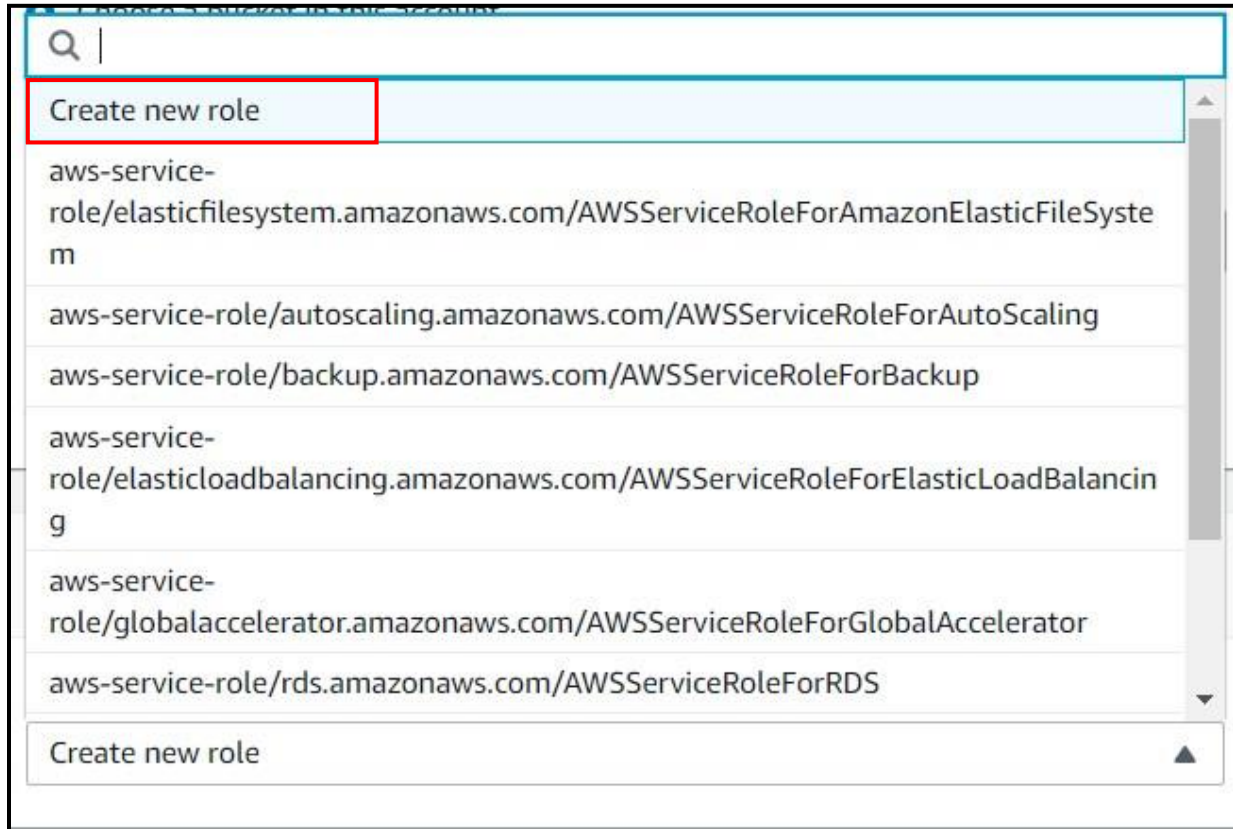
### Choose a bucket

S3 Buckets

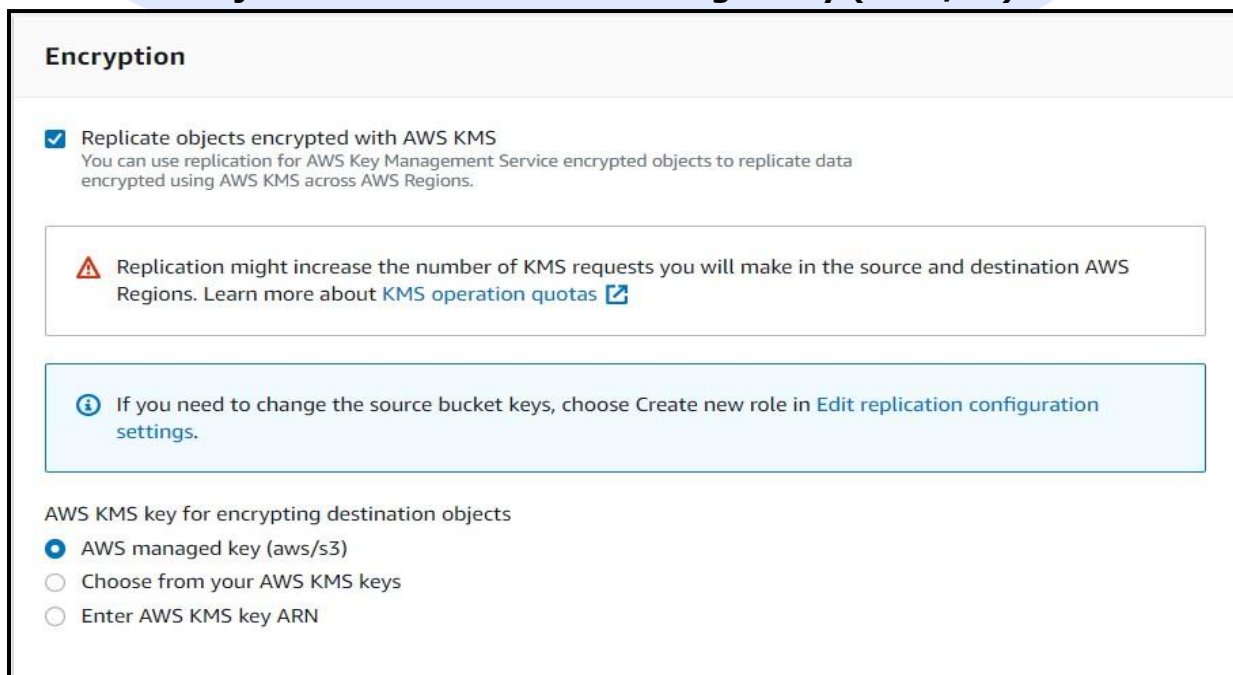
#### Buckets (2)

	Name
<input checked="" type="radio"/>	bucketdestination7531
<input type="radio"/>	bucketsource753

Click on the Dropdown for **IAM Role** and click on **Create new role**



Check the checkbox for bucket replication and make sure **AWS key for encrypting destination objects** is selected as **AWS managed key (AWS/s3)**





Click on the checkbox of **Change the storage class for the replicated objects** and make sure storage class is selected to **Standard**

### 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

### Storage class

	Storage class	Designed for	Availability Zones	Min storage duration	
<input checked="" type="radio"/>	Standard	Frequently accessed data	≥ 3	-	-
<input type="radio"/>	Intelligent-Tiering	Long-lived data with changing or unknown access patterns	≥ 3	30 days	-
<input type="radio"/>	Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	1
<input type="radio"/>	One Zone-IA	Long-lived, infrequently accessed, non-critical data	1	30 days	1
<input type="radio"/>	Glacier	Long-term data archiving with retrieval times ranging from minutes to hours	≥ 3	90 days	-
<input type="radio"/>	Glacier Deep Archive	Long-term data archiving with retrieval times within 12 hours	≥ 3	180 days	-
<input type="radio"/>	Reduced redundancy	Frequently accessed, non-critical data	≥ 3	-	-

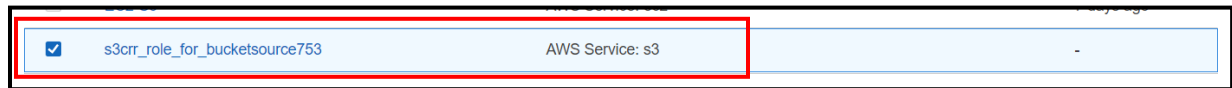
You can see the Replication Rule has been created on the S3 Bucket management section

	Replication rule name	Status	Destination bucket
<input type="radio"/>	ReplicationRule123	Enabled	s3://bucketdestination7531

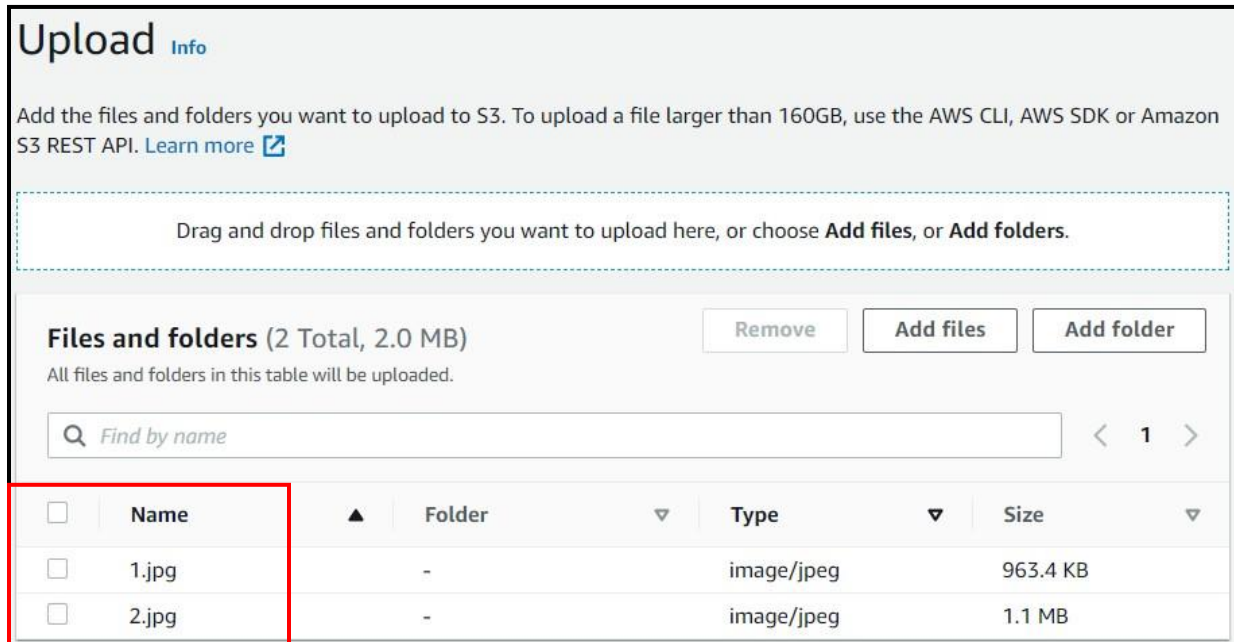
# Cloud Plus Plus Services



Even in IAM Role you can see IAM Role for S3 service role has been created

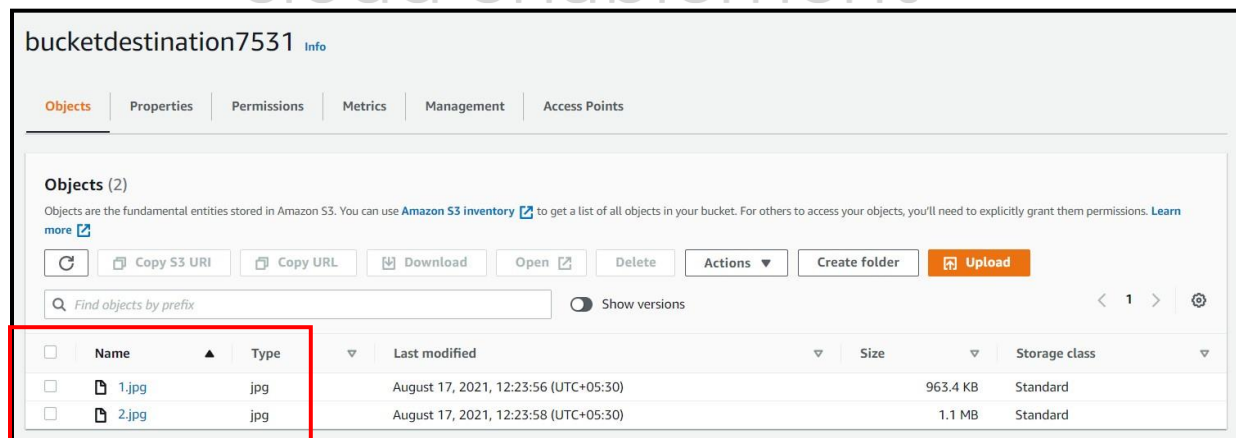


Step 6: Open the S3 Source Bucket and Upload 2 images.



Step 7: Go to Destination bucket check that the files have been replicated. A copy of these files has been created in this bucket.

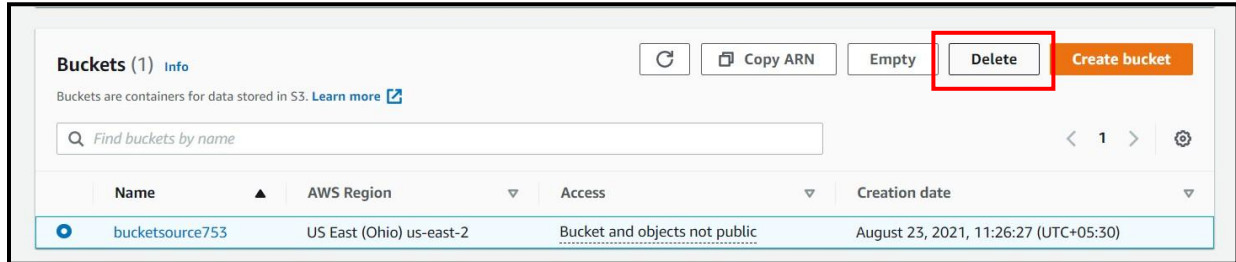
Note: It takes a little while for the Source Bucket Item to replicate on the destination bucket so wait for a few minutes and then refresh the destination bucket page





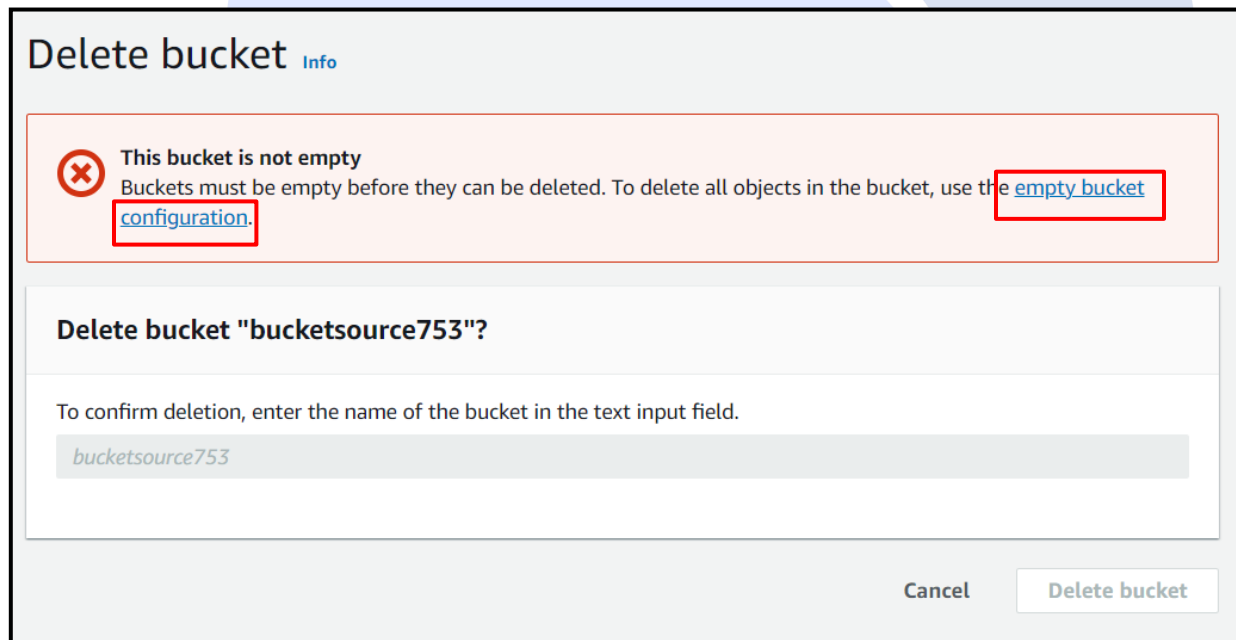
Note: Follow the next step only if you do not require the bucket for later use.

Step 8: Select the bucket and click on **delete**

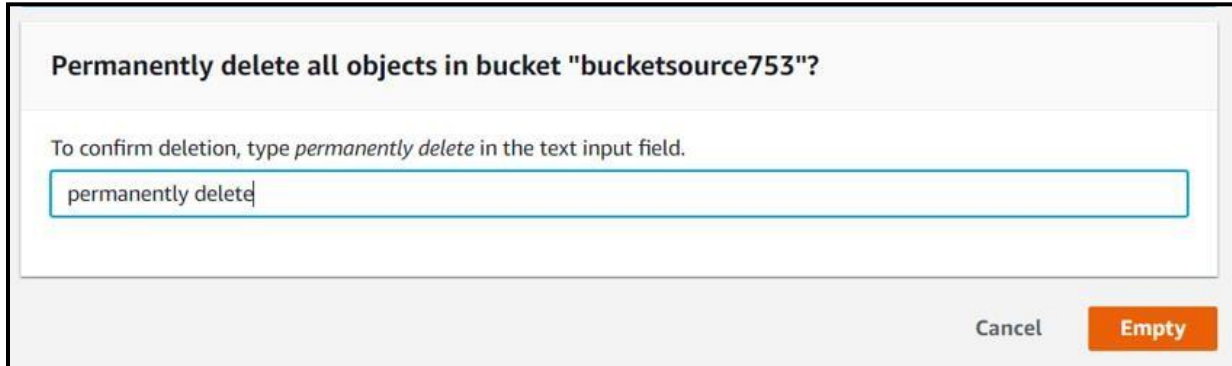


Since our bucket has objects in it we need to empty the bucket first before deleting.

Click on **empty bucket configuration**



Type **permanently delete** in the text field and click on **Empty**. Now all the objects in your bucket are emptied. And the bucket can be deleted.

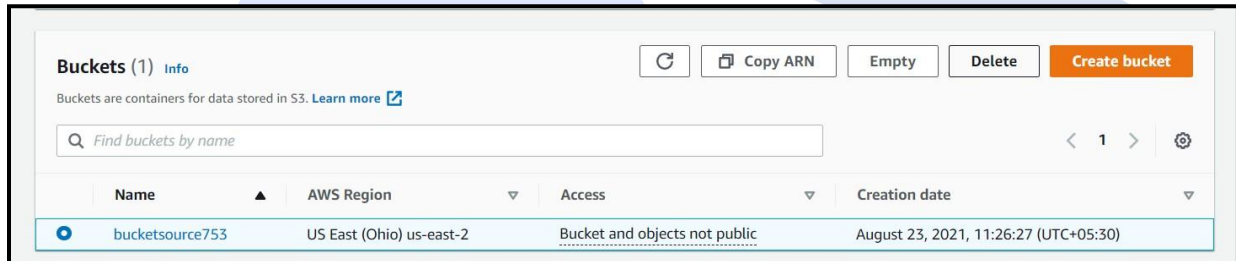


**Permanently delete all objects in bucket "bucketsource753"?**

To confirm deletion, type *permanently delete* in the text input field.

Cancel **Empty**

Now go to S3 buckets page again and click on delete



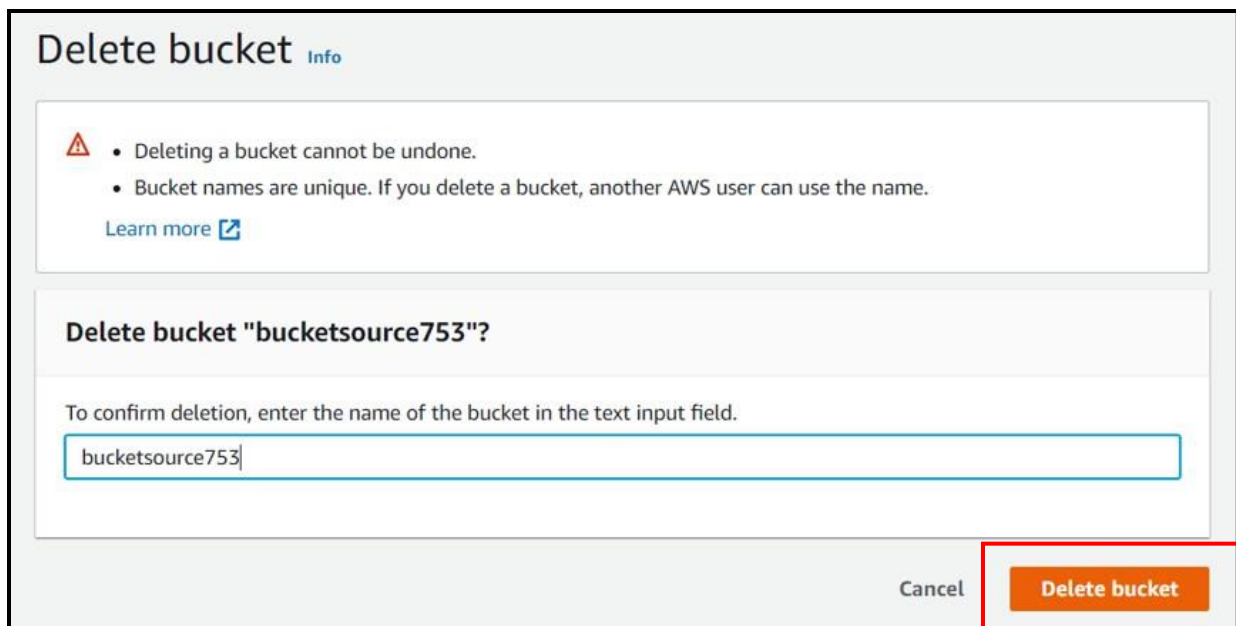
**Buckets (1)** [Info](#)

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

Find buckets by name

Name	AWS Region	Access	Creation date
<a href="#">bucketsource753</a>	US East (Ohio) us-east-2	Bucket and objects not public	August 23, 2021, 11:26:27 (UTC+05:30)

This time enter the bucket name in this case **bucketsource753** in the text field and click on **Delete Bucket**



**Delete bucket** [Info](#)

⚠ • Deleting a bucket cannot be undone.  
• Bucket names are unique. If you delete a bucket, another AWS user can use the name.  
[Learn more](#)

**Delete bucket "bucketsource753"?**

To confirm deletion, enter the name of the bucket in the text input field.

Cancel **Delete bucket**

Was this document helpful? YES / NO

**CLOUD ++**

Document Created by	Version
Soham Pingat	23-Aug-2021
Bavyaa R	25-Jan-2022