AWS Day4 (hands on assignment)

In this hands-on assignment, we will perform bucket replication.

Create a bucket in the Mumbai region

Bucket name: manoharbucket007

ACLs Disabled (recommended)

Allow public access

Versioning: enabled

Server side and default encryption: enabled

Click on create a bucket

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.

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 tag

Default encryption Info

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

Encryption type | Info

🔵 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-

Bucket successfully created.

Now I have two buckets

1)manoharbucket209 created in n.virginia region (source bucket)

2)manoharbucket007 created in Mumbai region (destination bucket)

Go to the source bucket and click on management

Note: in the source bucket already I have a file uploaded
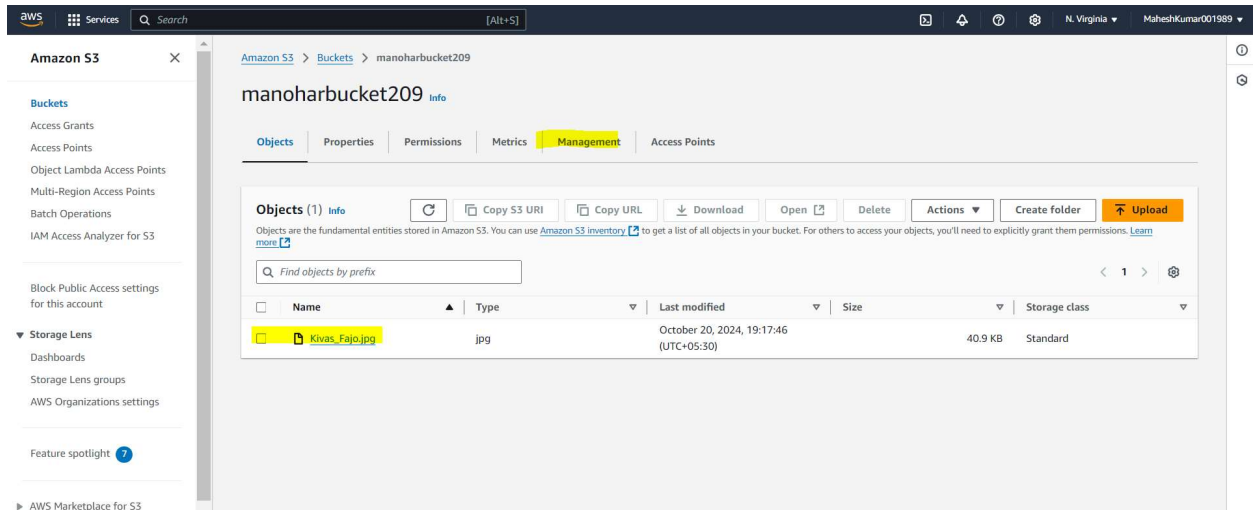
We are going to create replication rule, So click on replication rule.
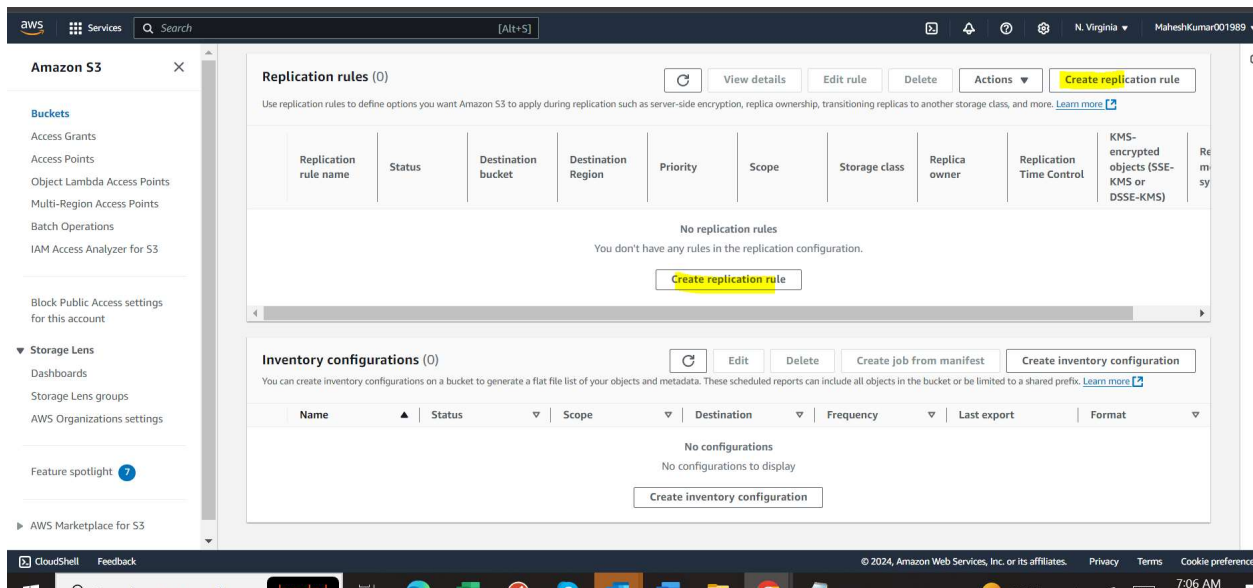
Getting below error so I enabled bucket versioning in the source bucket also.

;
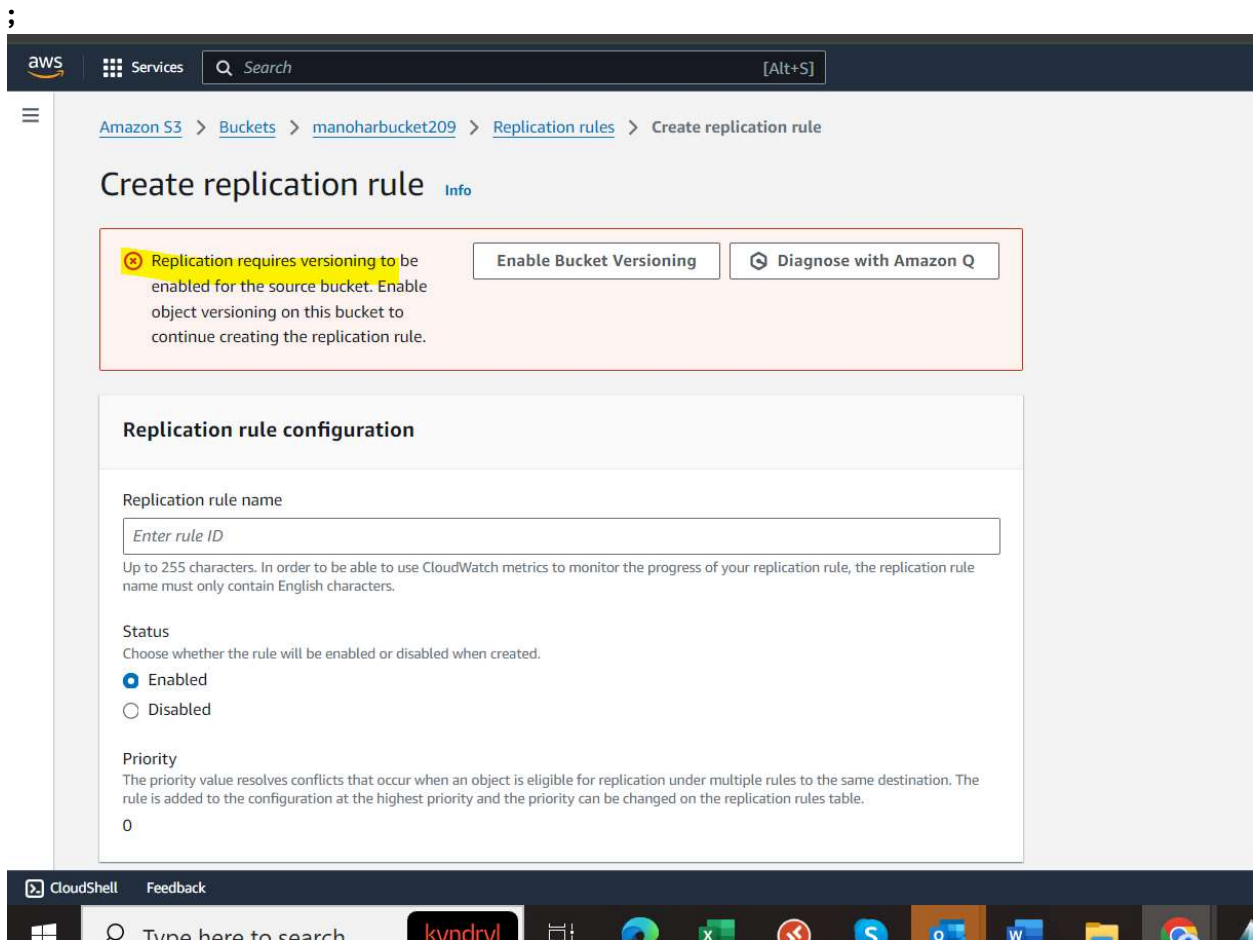
Versioning enabled in the source bucket successfully.
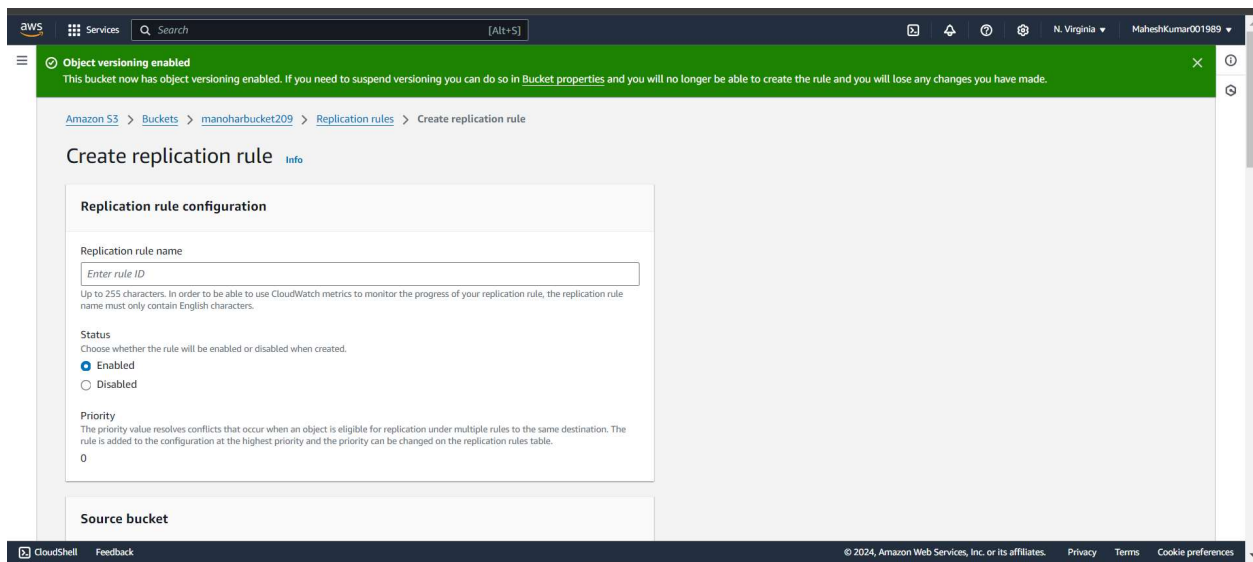
Create replication rule:

Rule name: mybucketreplicationrule

Status: enabled

Source bucket rule scope : apply to all objects in the bucket

Destination bucket: manoharbucket007

IAM Role: create a new role

⊘ Object versioning enabled
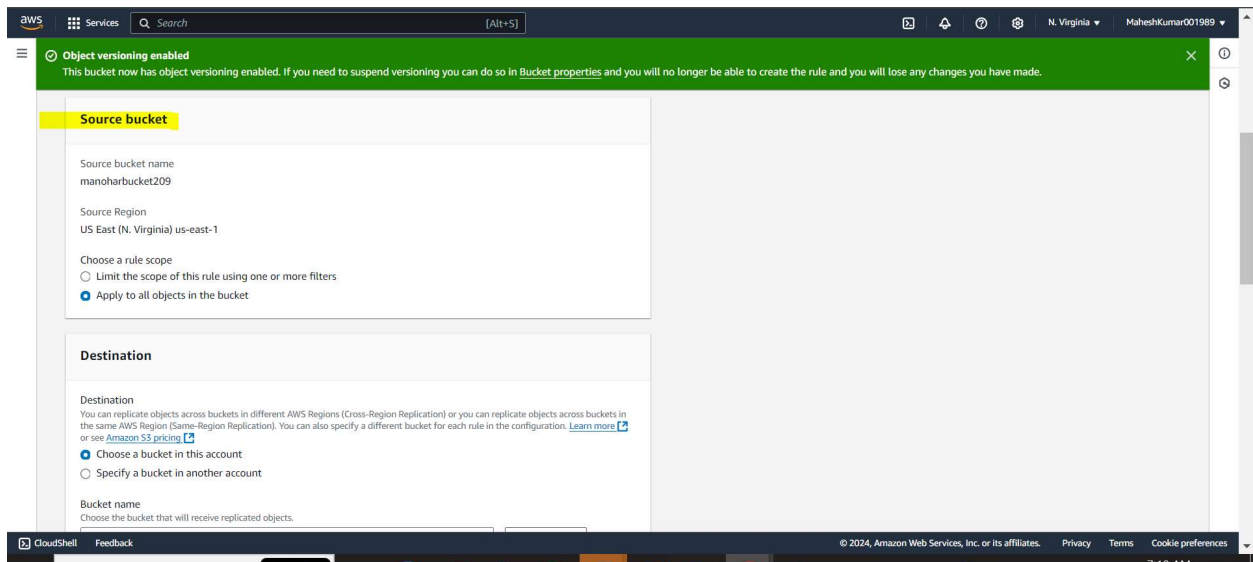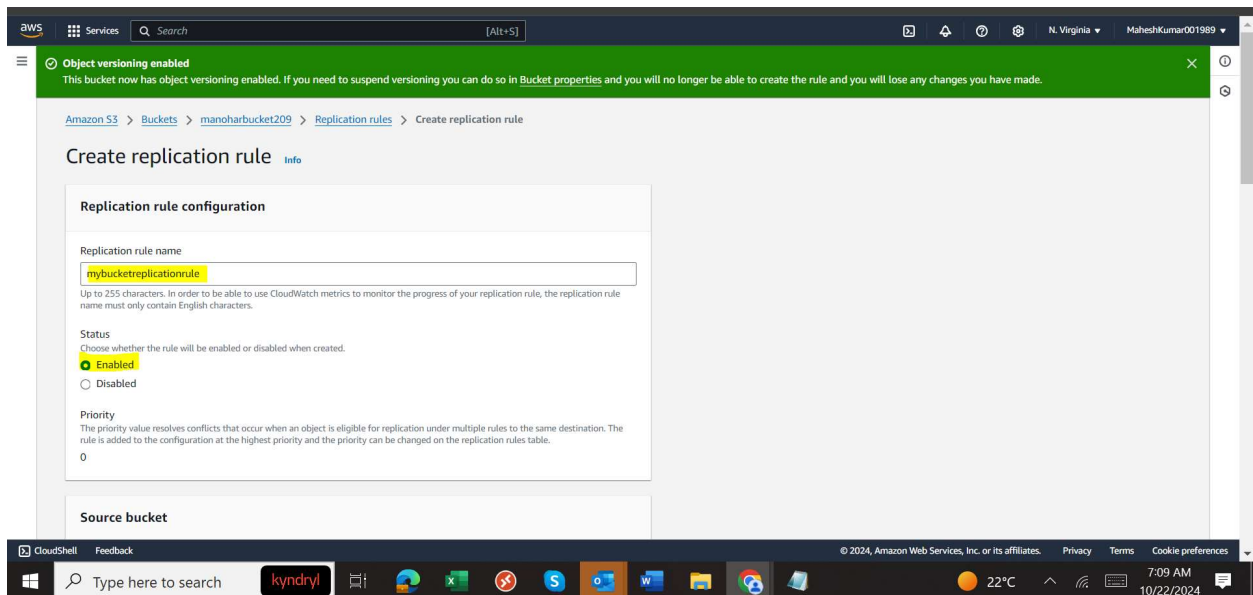This bucket now has object versioning enabled. If you need to suspend versioning you can do so in Bucket properties and you will no longer be able to create the rule and you will lose any changes you have made. ✕

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

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
-

Choose a bucket ✕

S3 Buckets

Buckets (1/5)   ⟳

[Q Find buckets by name]   ‹ 1 ›

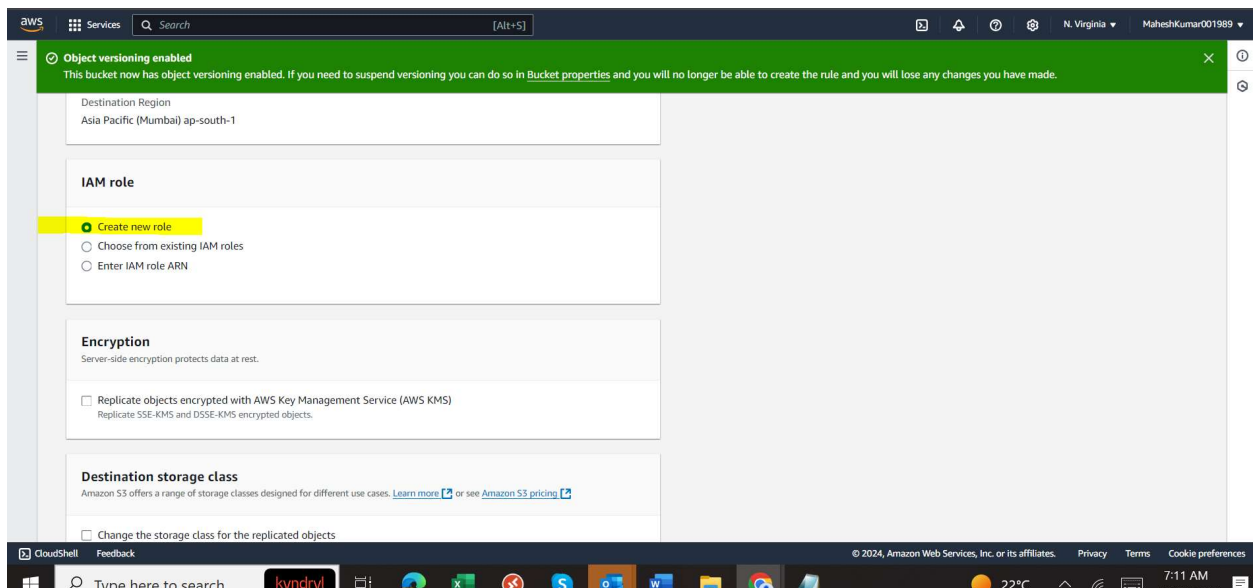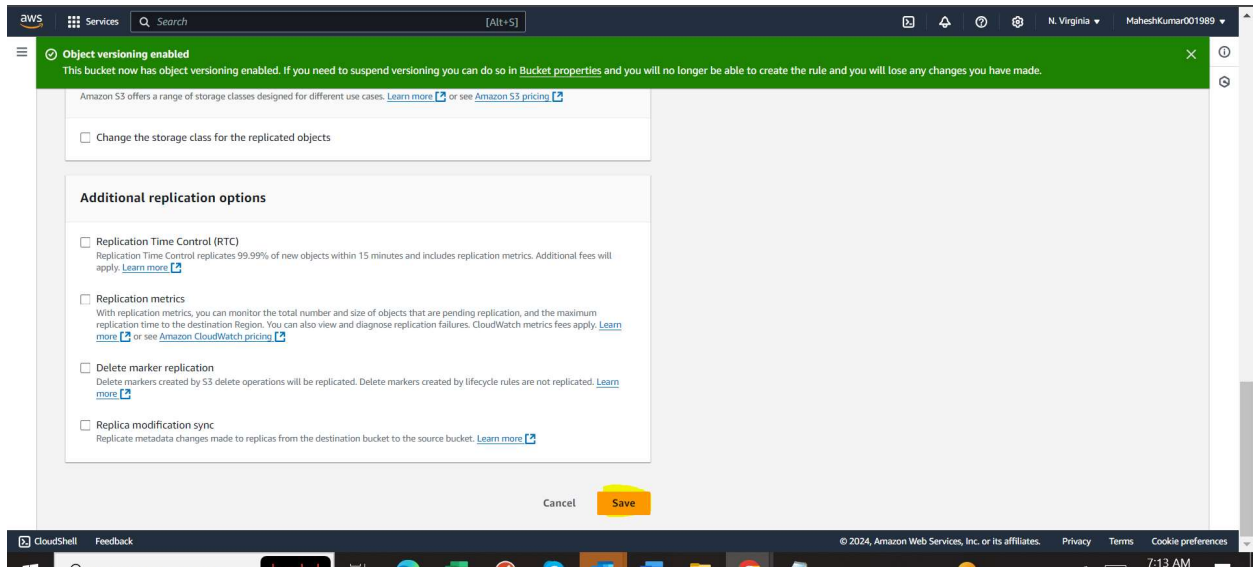|	Name ▽	AWS Region ▽
○	cf-templates-87xgs0s4mysr-us-east-1	US East (N. Virginia) us-east-1
○	elasticbeanstalk-ap-southeast-1-637423404772	Asia Pacific (Singapore) ap-southeast-1
○	elasticbeanstalk-us-east-1-637423404772	US East (N. Virginia) us-east-1
◉	manoharbucket007	Asia Pacific (Mumbai) ap-south-1
○	manoharbucket209	US East (N. Virginia) us-east-1

Cancel   **Choose path**

Click on save

Click on : yes, replicate existing objects

Replication configuration successfully updated
If changes to the configuration aren't displayed, choose the refresh button. Changes apply only to new objects. To replicate existing objects with this configuration, choose Create replication job.

Amazon S3 > Buckets > manoharbucket209 > Replication rules

Replication rules Info

Replication enables automatic and 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. You can define what options should be applied to a group of objects during replication.

Replication configuration settings

Configuration settings affect all replication rules in the bucket.

Source bucket
manoharbucket209

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

Create replication job   Edit

Replicate existing objects?   ✕

You can enable a one-time Batch Operations job from this replication configuration to replicate objects that already exist in the bucket and to synchronize the source and destination buckets. Learn more ⧉ or see pricing ⧉

Existing objects
○ No, do not replicate existing objects.
● Yes, replicate existing objects.

Cancel   Submit

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 ⧉

View details   Edit rule   Delete   Actions ▾   Create replication rule

1

CloudShell Feedback

Amazon S3 > Buckets > manoharbucket209 > Replication rules > Create Batch Operations job

Create Batch Operations job

Job settings
A job is used to execute batch operations on a list of S3 objects. The list of objects is contained in a replication manifest object generated by S3.

Job run 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

CloudShell Feedback

© 2024 Amazon Web

Complete report destination: click on browse s3

Choose destination bucket: manoharbucket007

Permissions:

Create a new IAM Role

Click on save

Replication rule created successfully.

After waiting for few mins my file is available in the destination bucket.

Amazon S3 ✕

Buckets

Access Grants
Access Points
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
Storage Lens groups
AWS Organizations settings

Feature spotlight 7

▶ AWS Marketplace for S3

Amazon S3 > Buckets > manoharbucket007

manoharbucket007 Info

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

Objects (2) Info

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 ↗

[C] [Copy S3 URI] [Copy URL] [Download] [Open ↗] [Delete] [Actions ▾] [Create folder] [Upload]

🔍 Find objects by prefix   ⬤ Show versions   ‹ 1 › ⚙

☐	Name ▲	Type ▽	Last modified ▽	Size ▽	Storage class ▽
☐	📄 job-f10c15fe-cdbf-488d-a706-e3dd3cd8c338/	Folder	-	-	-
☐	📄 Kivas_Fajo.jpg	jpg	October 20, 2024, 19:17:46 (UTC+05:30)	40.9 KB	Standard