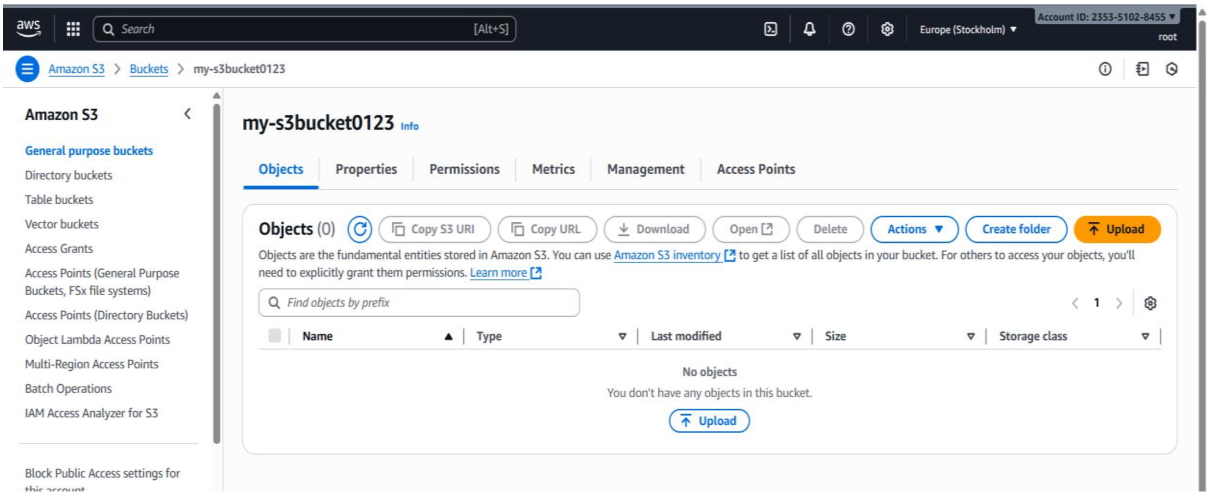
1. Create an S3 bucket and upload some objects to S3.

Open aws console and navigate to S3 and click on create bucket. Give the unique bucket name and give the region where you need to create.



Amazon S3 > Buckets > my-s3bucket0123

my-s3bucket0123 Info

Objects | 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

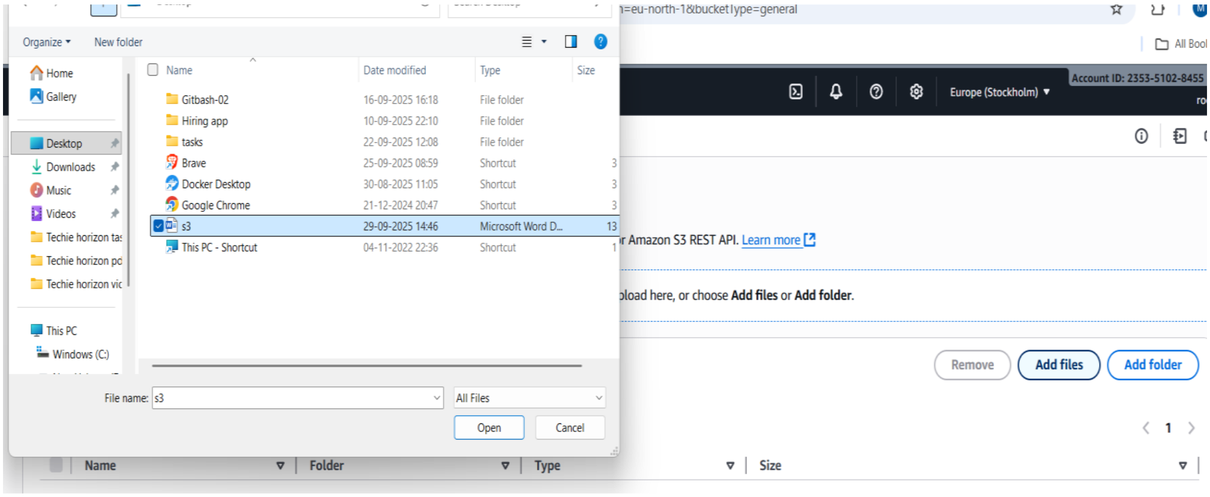
Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.

Search
[Alt+S]
Europe (Stockholm)
Account ID: 2353-5102-8455
root
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
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
1
Upload

To upload the file click on add file and select a file from local.

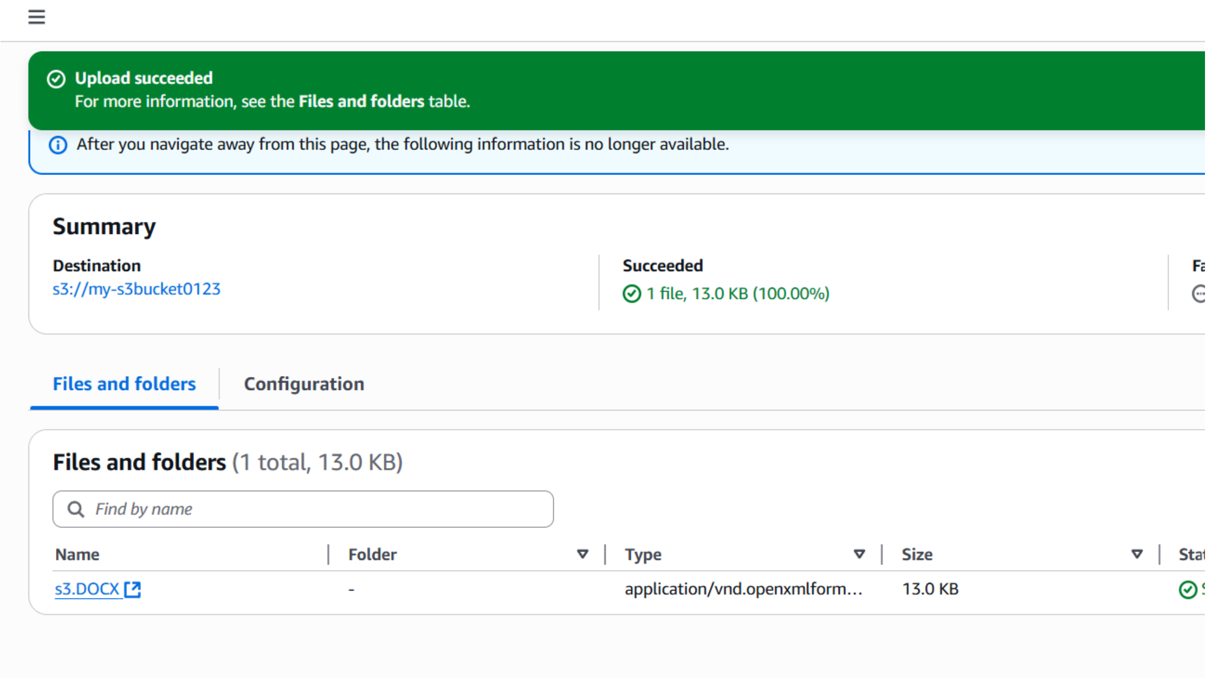


Name	Date modified	Type	Size
Gitbash-02	16-09-2025 16:18	File folder	
Hiring app	10-09-2025 22:10	File folder	
tasks	22-09-2025 12:08	File folder	
Brave	25-09-2025 08:59	Shortcut	3
Docker Desktop	30-08-2025 11:05	Shortcut	3
Google Chrome	21-12-2024 20:47	Shortcut	3
s3	29-09-2025 14:46	Microsoft Word D...	13
This PC - Shortcut	04-11-2022 22:36	Shortcut	1

File name: s3

r Amazon S3 REST API. Learn more

pload here, or choose **Add files** or **Add folder**.



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://my-s3bucket0123

Succeeded
1 file, 13.0 KB (100.00%)

Fa

Files and folders | **Configuration**

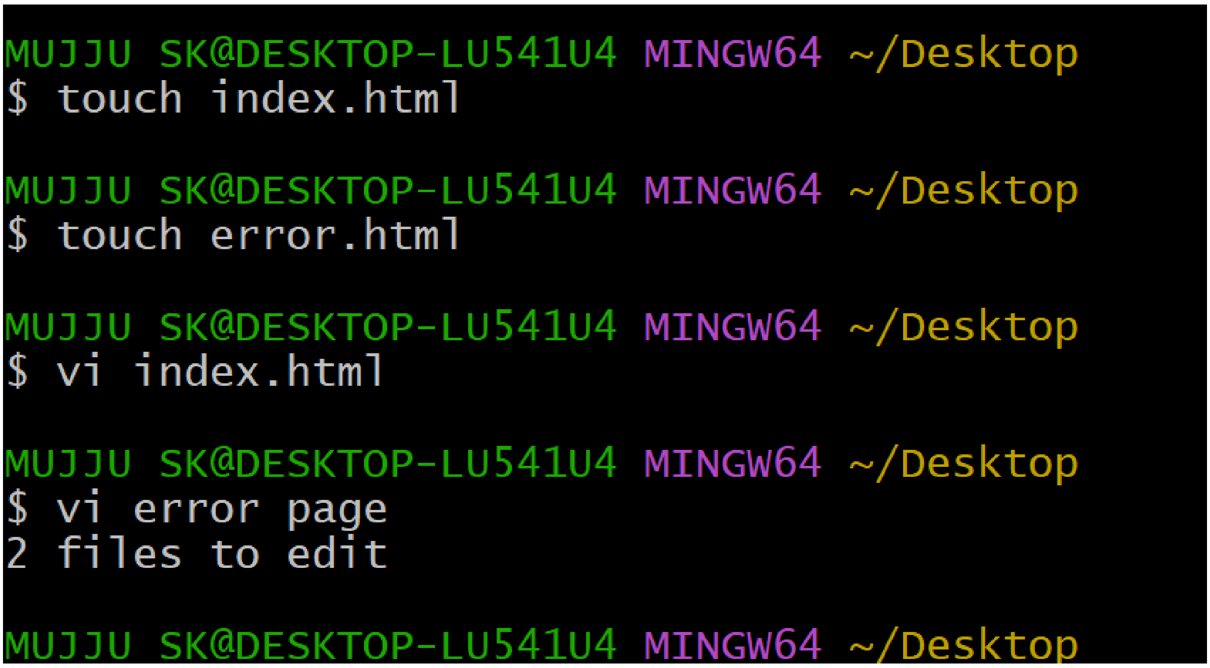
Files and folders (1 total, 13.0 KB)

Find by name

Name	Folder	Type	Size	Stat
s3.DOCX	-	application/vnd.openxmlform...	13.0 KB	✓

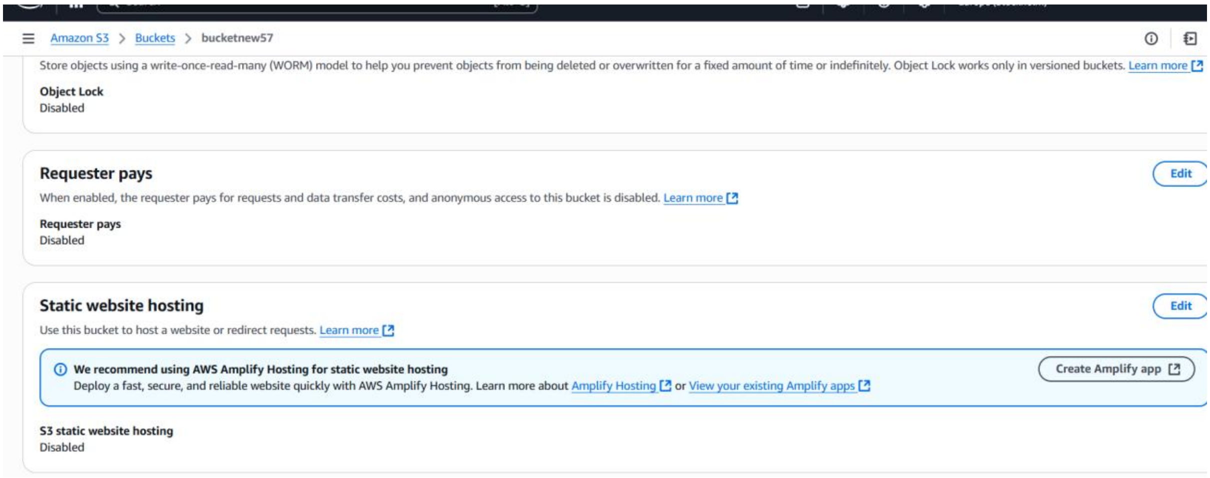
2.Deploy a static website in the S3 bucket.

Create 2 files and give the data to it.



```
MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Desktop
$ touch index.html

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Desktop
$ touch error.html

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Desktop
$ vi index.html

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Desktop
$ vi error page
2 files to edit

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Desktop
```

Go to buckets select the bucket and go to permissions, click on website hosting.



Amazon S3 > Buckets > bucketnew57

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. Learn more

Object Lock
Disabled

Requester pays

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. Learn more

Requester pays
Disabled

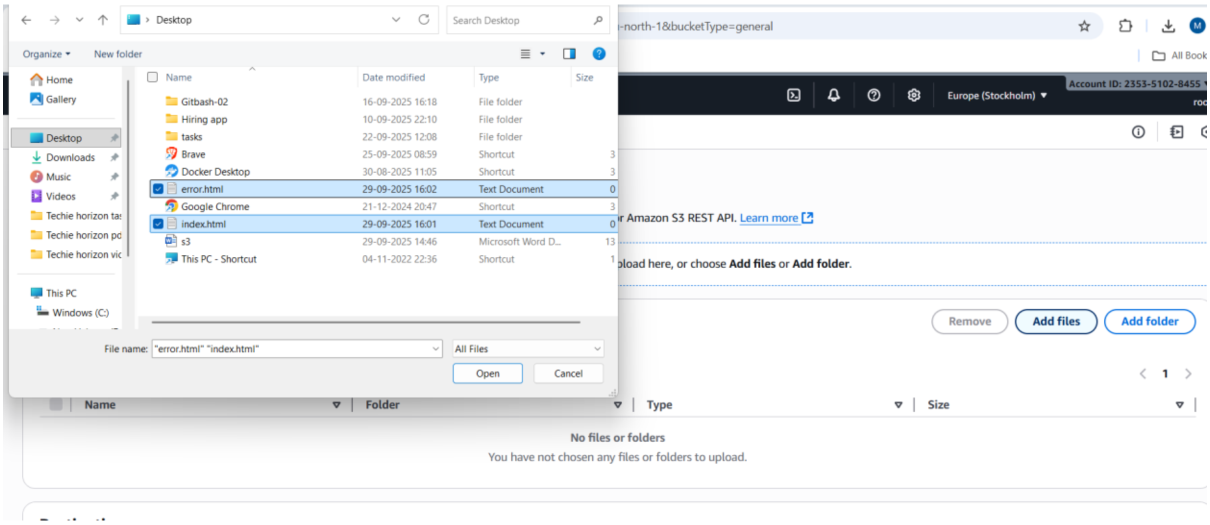
Static website hosting

Use this bucket to host a website or redirect requests. Learn more

We recommend using AWS Amplify Hosting for static website hosting
Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about Amplify Hosting or View your existing Amplify apps

S3 static website hosting
Disabled

Select website hosting and give the two files names .



Desktop

Name	Date modified	Type	Size
Gitbash-02	16-09-2025 16:18	File folder	
Hiring app	10-09-2025 22:10	File folder	
tasks	22-09-2025 12:08	File folder	
Brave	25-09-2025 08:59	Shortcut	3
Docker Desktop	30-08-2025 11:05	Shortcut	3
☑ error.html	29-09-2025 16:02	Text Document	0
Google Chrome	21-12-2024 20:47	Shortcut	3
☑ index.html	29-09-2025 16:01	Text Document	0
s3	29-09-2025 14:46	Microsoft Word D...	13
This PC - Shortcut	04-11-2022 22:36	Shortcut	1

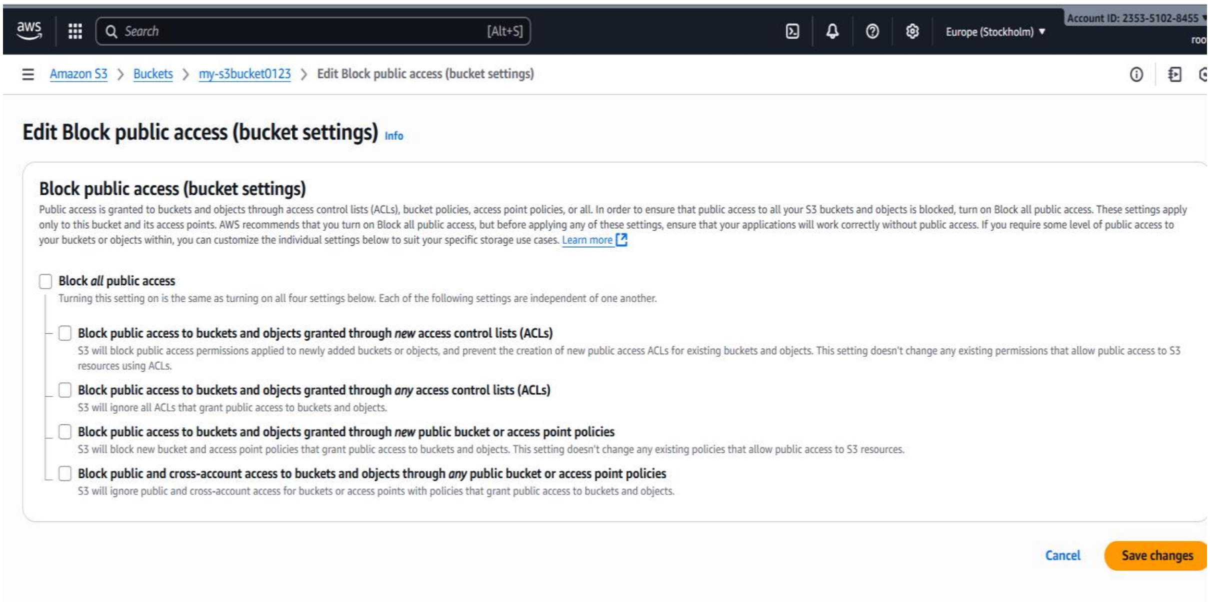
File name: "error.html" "index.html"
All Files

r Amazon S3 REST API. Learn more

pload here, or choose **Add files** or **Add folder**.

No files or folders
You have not chosen any files or folders to upload.

Make sure that your bucket will be accessible for public.



Amazon S3 > Buckets > my-s3bucket0123 > Edit Block public access (bucket settings)

Edit Block public access (bucket settings) Info

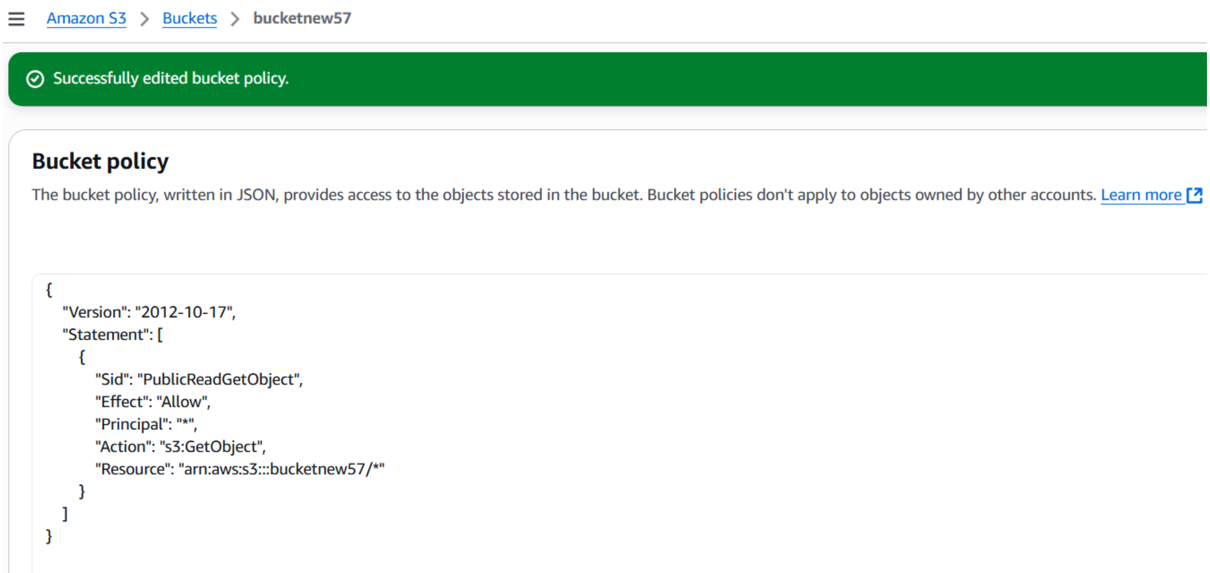
Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets 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.

Attach the poilicies for the bucket if any files added into that getting same access.



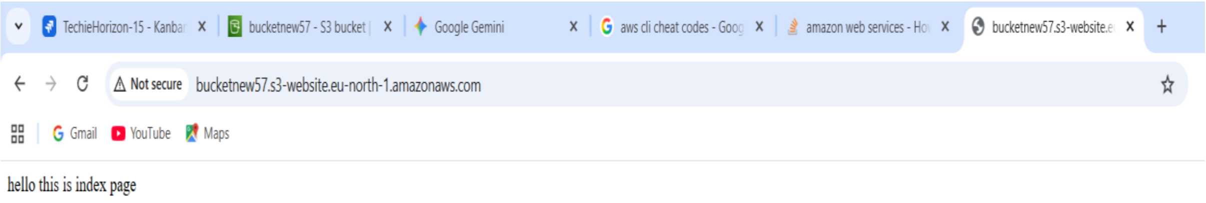
Successfully edited bucket policy.

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::bucketnew57/*"
    }
  ]
}
```

With the created bucket endpoint check it in browser.



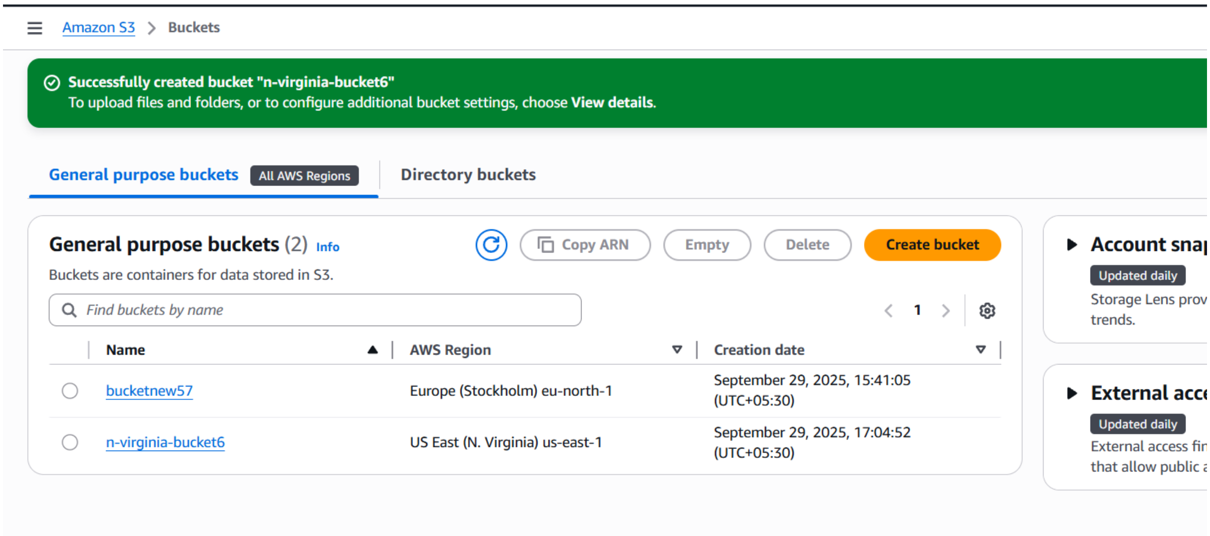
bucketnew57.s3-website.eu-north-1.amazonaws.com

hello this is index page

If incase the index.html file will be deleted then it will take to the error.html file.

3. Enable cross-region replication on S3 buckets.

Make sure that you have created your buckets in 2 different region.



Amazon S3 > Buckets

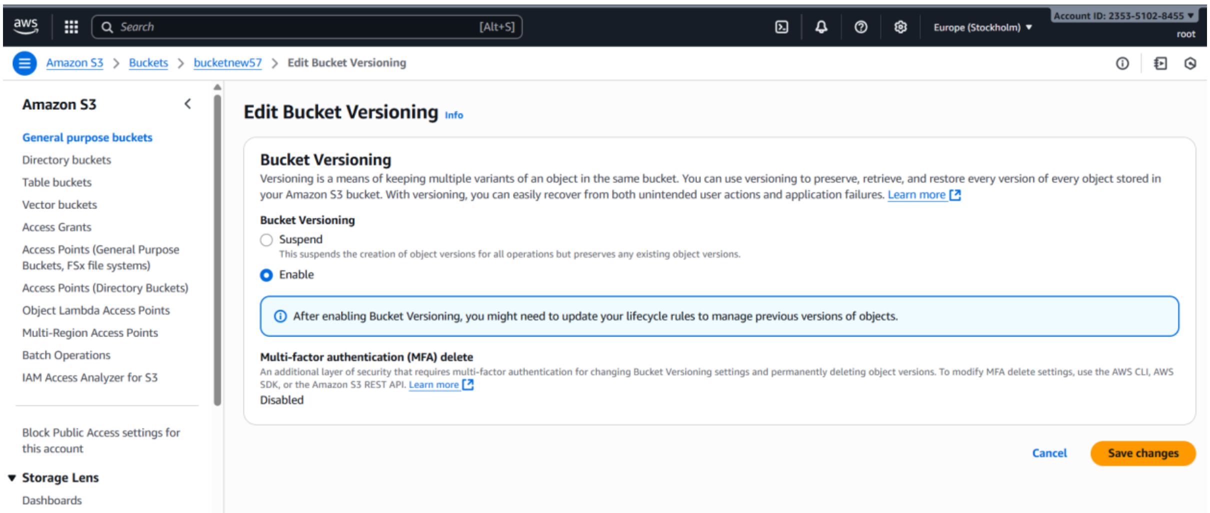
Successfully created bucket "n-virginia-bucket6"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

General purpose buckets (2) Info

Buckets are containers for data stored in S3.

Name	AWS Region	Creation date
○ bucketnew57	Europe (Stockholm) eu-north-1	September 29, 2025, 15:41:05 (UTC+05:30)
○ n-virginia-bucket6	US East (N. Virginia) us-east-1	September 29, 2025, 17:04:52 (UTC+05:30)

Select your bucket and go to permissions and make edit bucket versioning as enable.



Amazon S3 > Buckets > bucketnew57 > Edit Bucket Versioning

Edit Bucket Versioning Info

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

○ Suspend
This suspends the creation of object versions for all operations but preserves any existing object versions.

● Enable

After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.

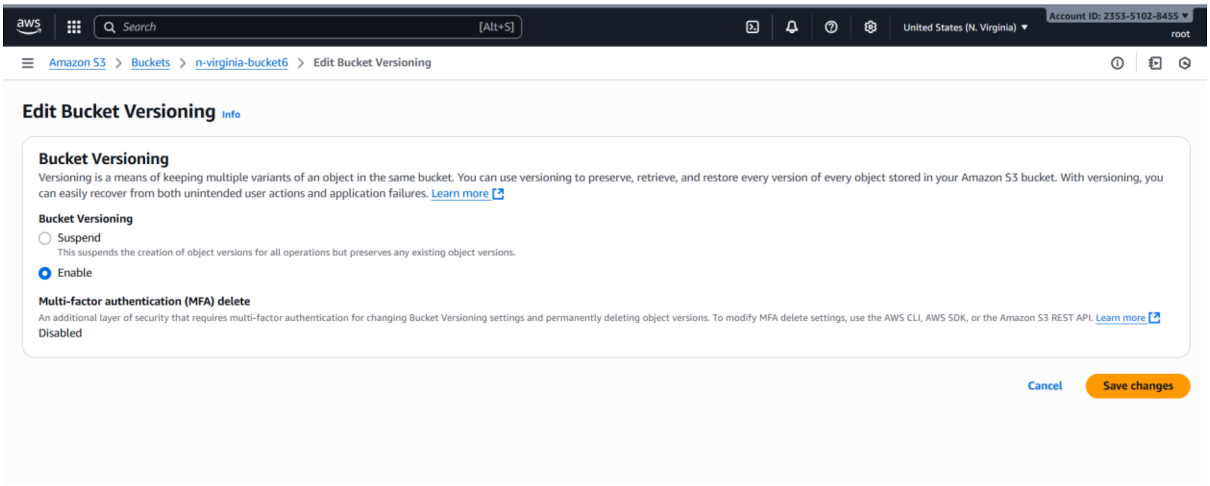
Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more

Disabled

aws
Search
[Alt+S]
Europe (Stockholm)
Account ID: 2353-5102-8455
root
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
Cancel
Save changes

Enable bucket versioning for another region also.



Amazon S3 > Buckets > n-virginia-bucket6 > Edit Bucket Versioning

Edit Bucket Versioning Info

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

○ Suspend
This suspends the creation of object versions for all operations but preserves any existing object versions.

● Enable

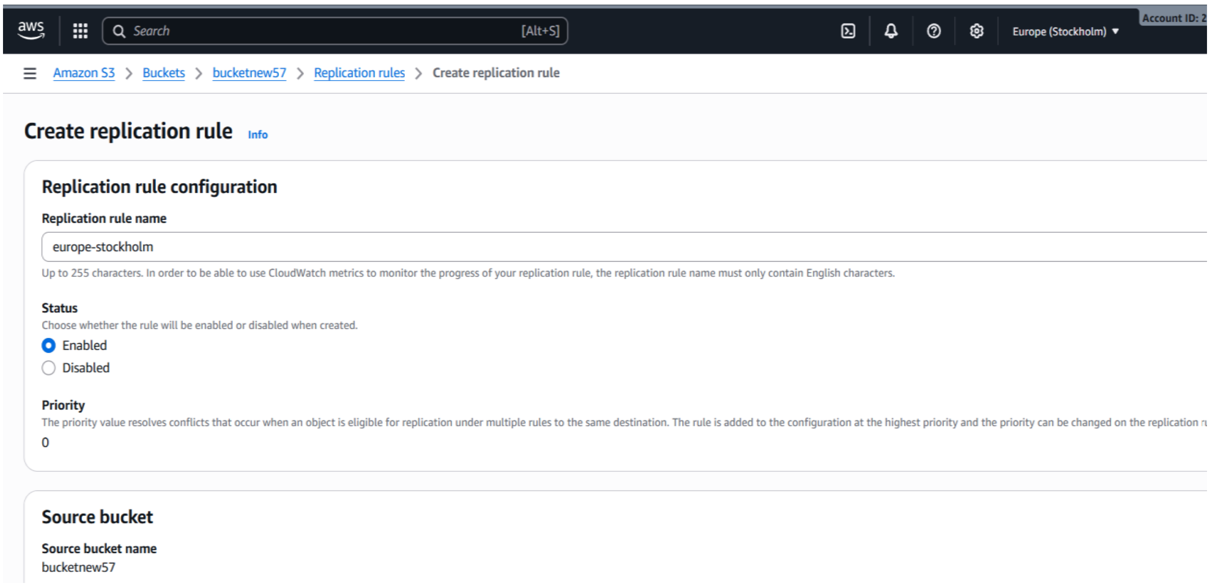
Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more

Disabled

Select your source bucket and go to management go to replication rule and create replication rule.

Give the source region replication.


aws
Search [Alt+S]
Europe (Stockholm) ▾
Account ID: 2
Amazon S3 > Buckets > bucketnew57 > Replication rules > Create replication rule

Create replication rule Info

Replication rule configuration

Replication rule name

europe-stockholm

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

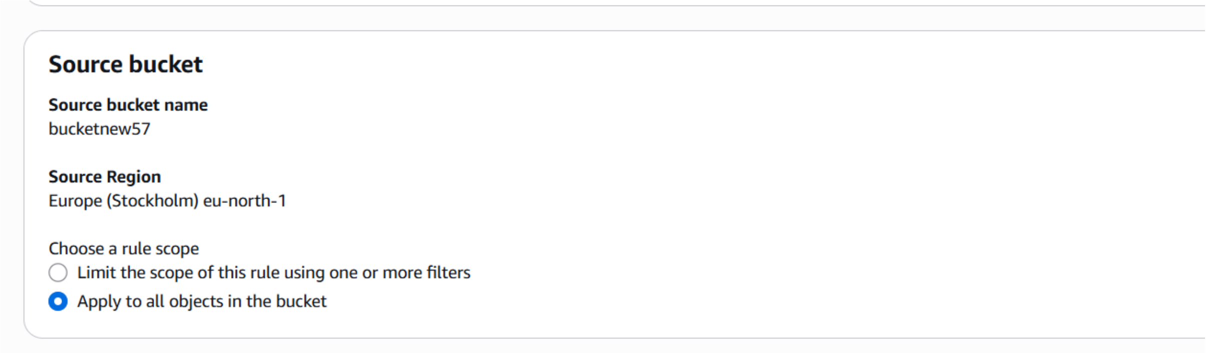
The priority value resolves conflicts that occur when an object is eligible for replication under multiple rules to the same destination. The rule is added to the configuration at the highest priority and the priority can be changed on the replication r

0

Source bucket

Source bucket name

bucketnew57



Source bucket

Source bucket name

bucketnew57

Source Region

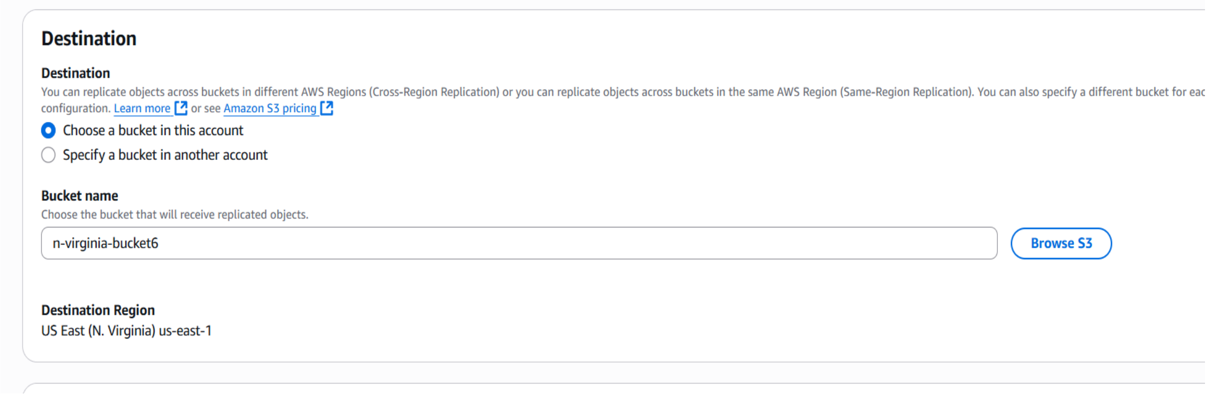
Europe (Stockholm) eu-north-1

Choose a rule scope

○ Limit the scope of this rule using one or more filters

● Apply to all objects in the bucket

Give the destination of bucket that you created in another region.



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 eac configuration. Learn more or see Amazon S3 pricing

● Choose a bucket in this account

○ Specify a bucket in another account

Bucket name

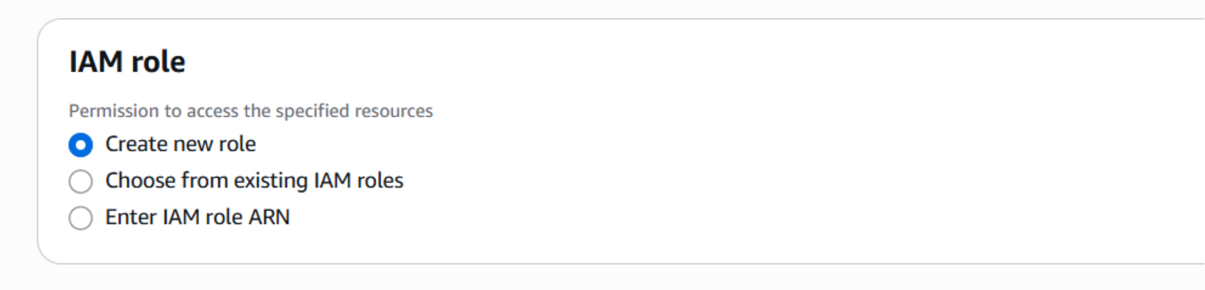
Choose the bucket that will receive replicated objects.

n-virginia-bucket6

Destination Region

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

Create an IAM role. AWS automatically creates the necessary IAM policy and trust relationship for the role.

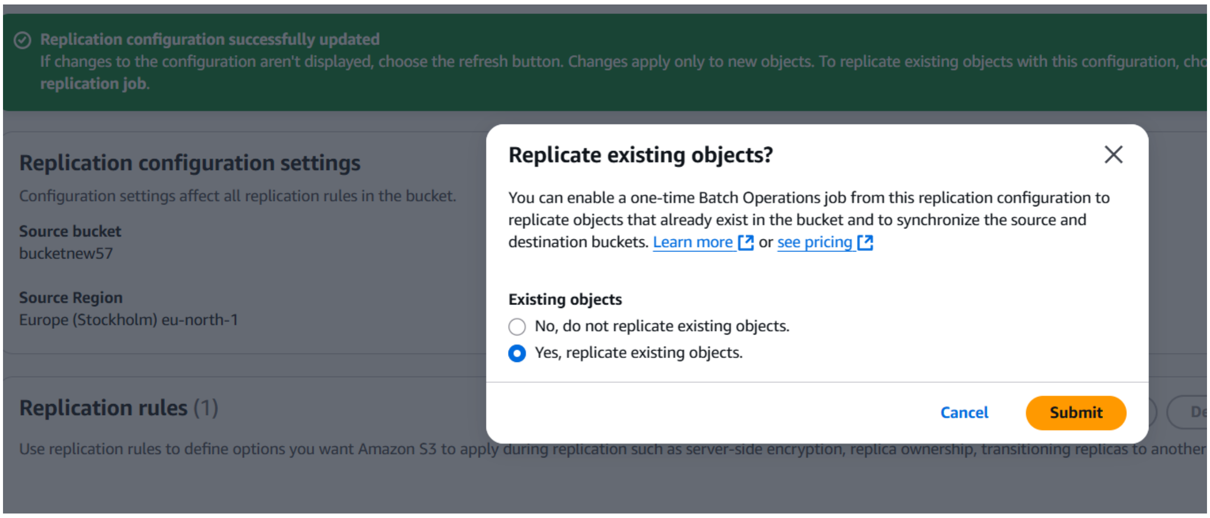


IAM role

Permission to access the specified resources

● Create new role
○ Choose from existing IAM roles
○ Enter IAM role ARN

Save it, then it will shows a pop message select 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, cho
replication job.

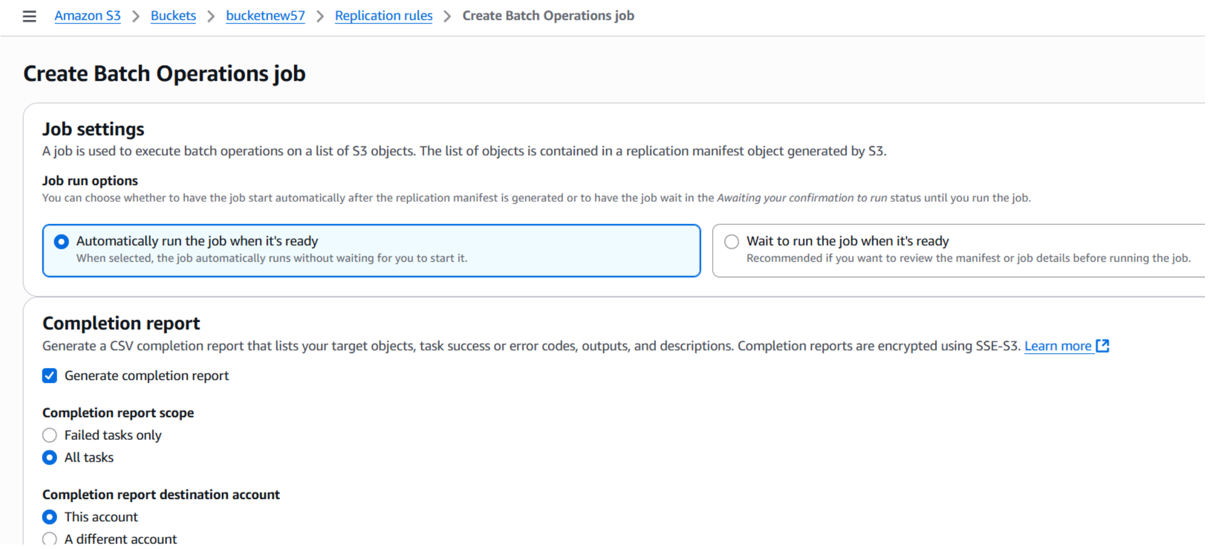
Replication configuration settings
Configuration settings affect all replication rules in the bucket.
Source bucket
bucketnew57
Source Region
Europe (Stockholm) eu-north-1

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

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.



Amazon S3 > Buckets > bucketnew57 > 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.

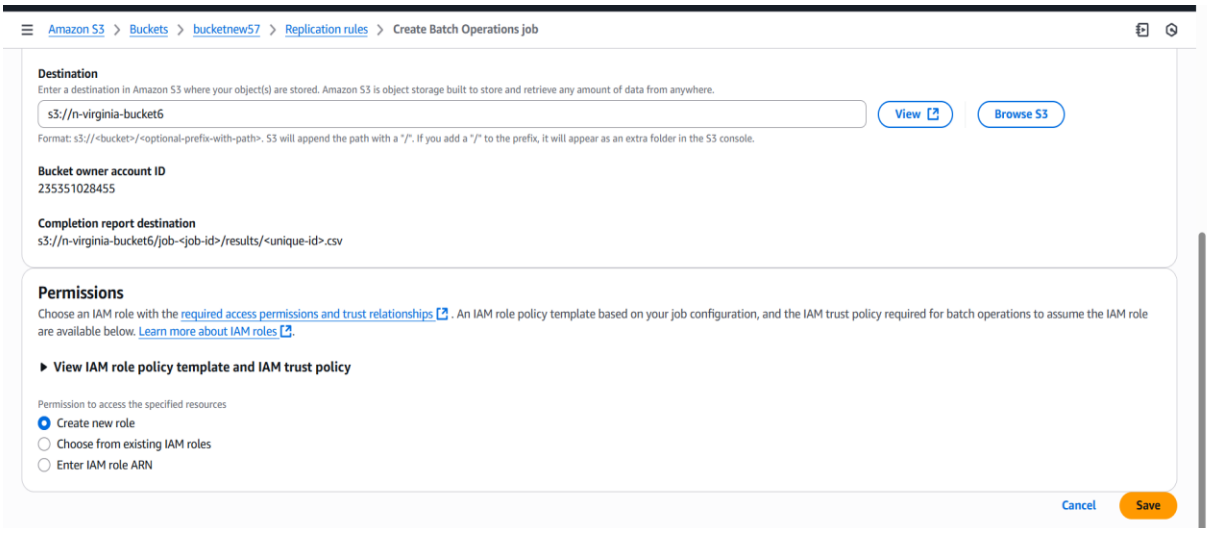
○ Wait to run the job when it's ready
Recommended if you want to review the manifest or job details before running the job.

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 account
● This account
○ A different account



Amazon S3 > Buckets > bucketnew57 > Replication rules > Create Batch Operations job
View
Browse S3
Cancel
Save

Destination

Enter a destination in Amazon S3 where your object(s) are stored. Amazon S3 is object storage built to store and retrieve any amount of data from anywhere.

s3://n-virginia-bucket6

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.

Bucket owner account ID

235351028455

Completion report destination

s3://n-virginia-bucket6/job-<job-id>/results/<unique-id>.csv

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

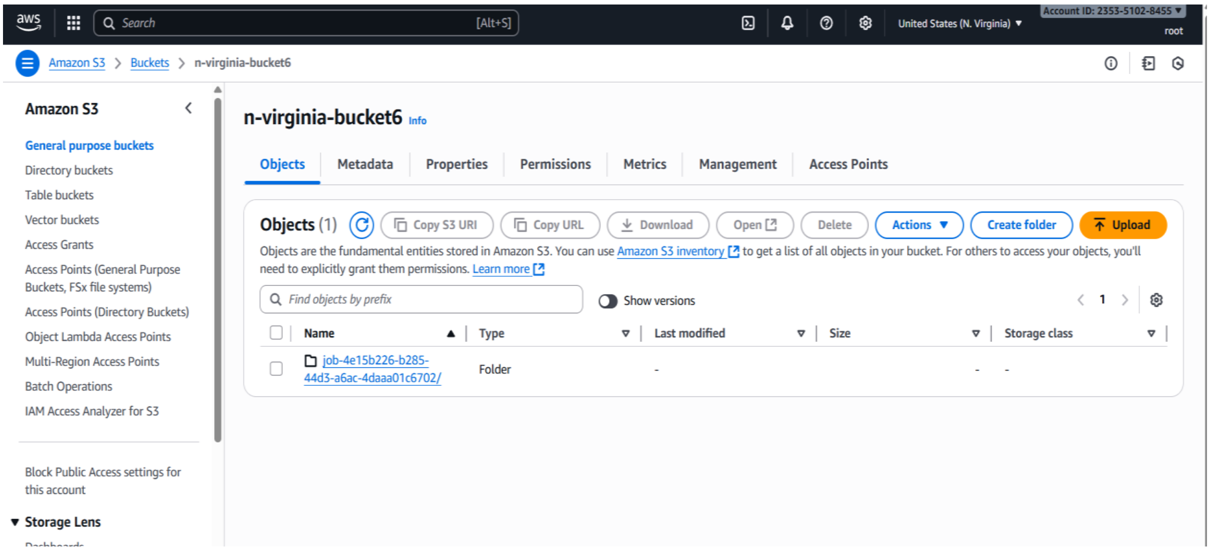
Permission to access the specified resources

● Create new role

○ Choose from existing IAM roles

○ Enter IAM role ARN

You can see a job was created in the destination region.



aws
Search
[Alt+S]
United States (N. Virginia) ▾
Account ID: 2353-5102-8455 ▾
root
Amazon S3 > Buckets > n-virginia-bucket6
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
Info
Objects
Metadata
Properties
Permissions
Metrics
Management
Access Points
Copy S3 URI
Copy URL
Download
Open
Delete
Actions ▾
Create folder
Upload
Find objects by prefix
Show versions
1

n-virginia-bucket6

Objects (1)

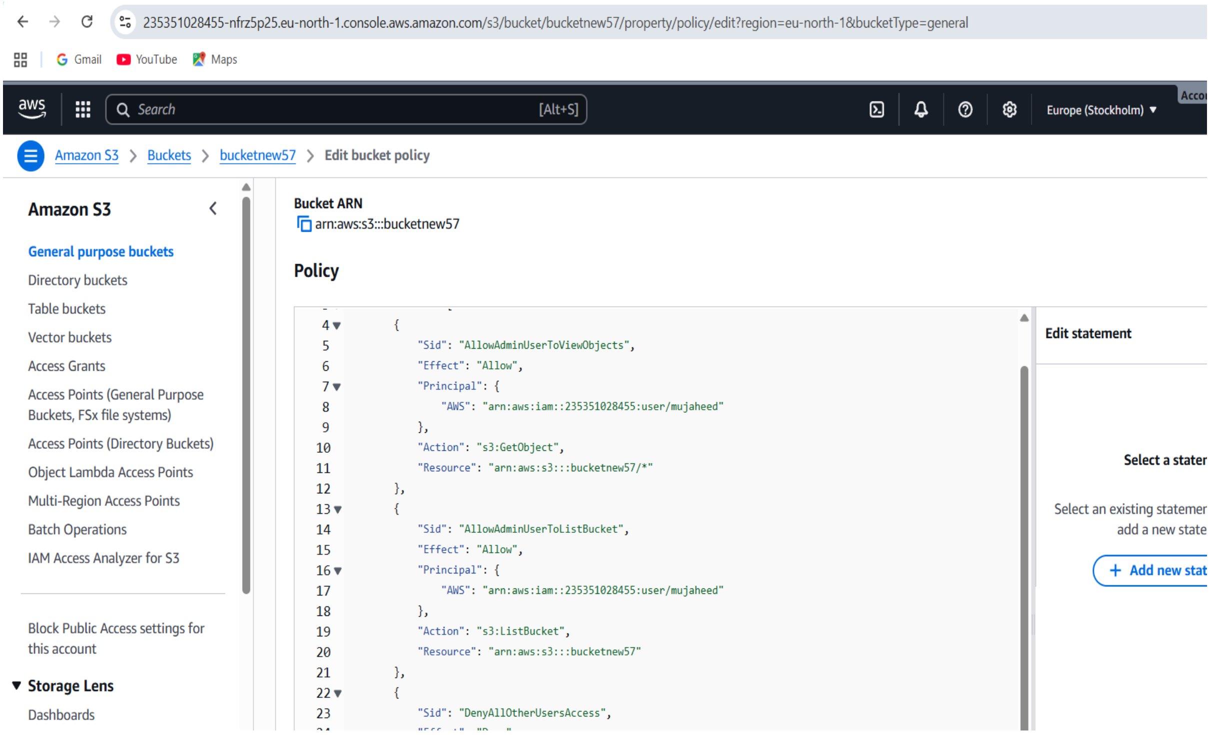
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

	Name	Type	Last modified	Size	Storage class
□	job-4e15b226-b285-44d3-a6ac-4daaa01c6702/	Folder	-	-	-

4. Configure a bucket policy so only the Admin user can see the objects of the S3 bucket.

Go to buckets select the wanted bucket and go to permissions edit policies and write the script.

Give your’s account I’d, Admin name, Bucket name to the script.

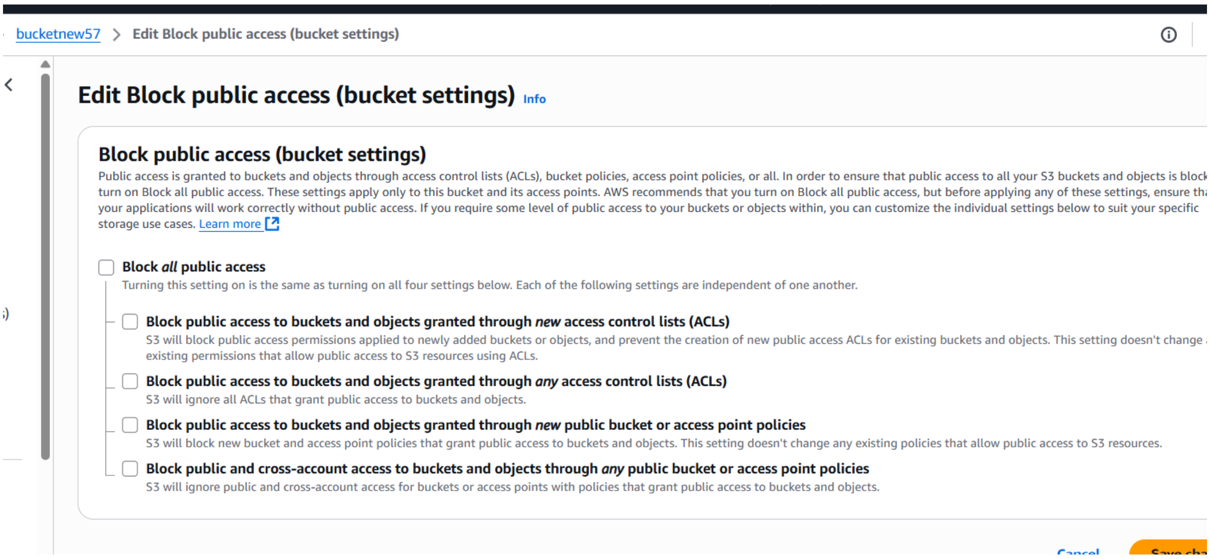

235351028455-nfrz5p25.eu-north-1.console.aws.amazon.com/s3/bucket/bucketnew57/property/policy/edit?region=eu-north-1&bucketType=general
Gmail
YouTube
Maps
aws
Search
[Alt+S]
Europe (Stockholm) ▼
Acco
Amazon S3 > Buckets > bucketnew57 > Edit bucket policy
Amazon S3
General purpose buckets
Directory buckets
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
Edit statement
Select a stater
Select an existing statemer add a new state
+ Add new stat

Bucket ARN

arn:aws:s3:::bucketnew57

Policy

```
        {
            "Sid": "AllowAdminUserToViewObjects",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::235351028455:user/mujaheed"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::bucketnew57/*"
        },
        {
            "Sid": "AllowAdminUserToListBucket",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::235351028455:user/mujaheed"
            },
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::bucketnew57"
        },
        {
            "Sid": "DenyAllOtherUsersAccess",
```



Edit Block public access (bucket settings)

Block public access (bucket settings)

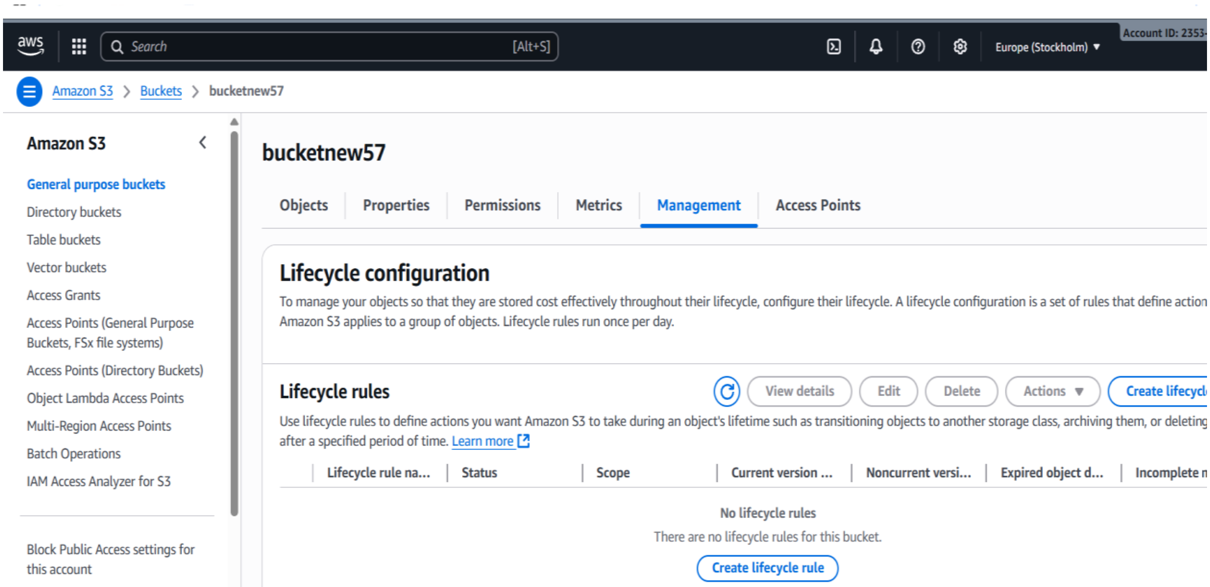
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is block turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure tha your applications will work correctly without public access. If you require some level of public access to your buckets 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 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.

5. Set up lifecycle policies to automatically transition or delete objects based on specific criteria.

Select the bucket where you need to do the life cycle policies go to management.



bucketnew57

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 action 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 after a specified period of time. Learn more

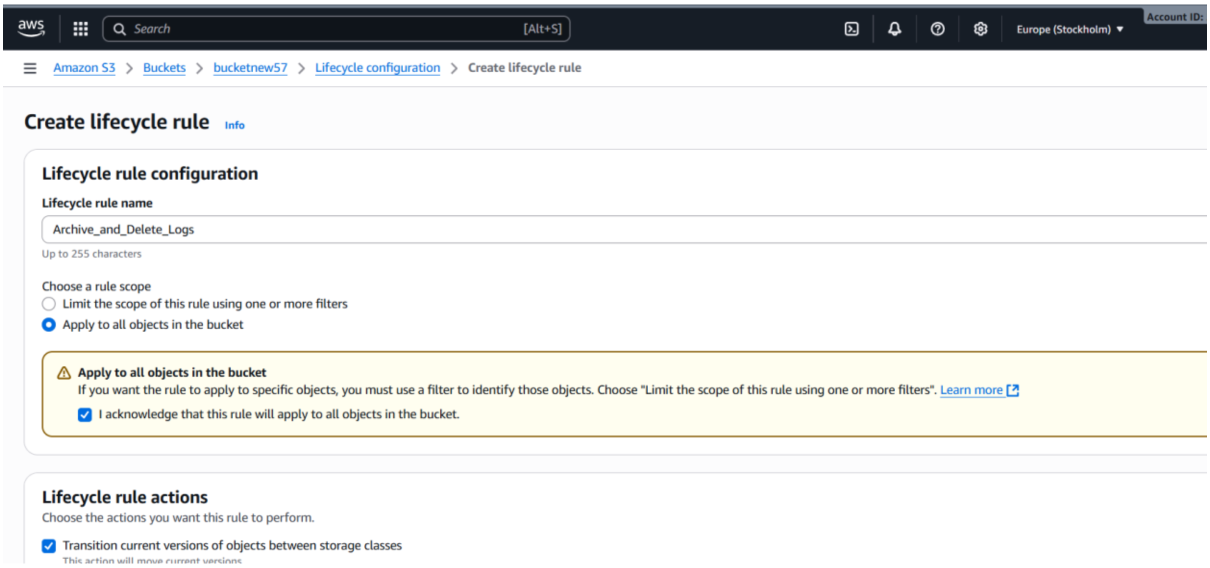
Lifecycle rule na...	Status	Scope	Current version ...	Noncurrent versi...	Expired object d...	Incomplete m

No lifecycle rules

There are no lifecycle rules for this bucket.

Select create life cycle rule and give the details.

Rule name and apply to all objects in the bucket.


aws
Search [Alt+S]
Europe (Stockholm) ▾
Account ID:
Amazon S3 > Buckets > bucketnew57 > Lifecycle configuration > Create lifecycle rule
Info

Create lifecycle rule

Lifecycle rule configuration

Lifecycle rule name

Archive_and_Delete_Logs

Up to 255 characters

Choose a rule scope

○ Limit the scope of this rule using one or more filters

● Apply to all objects in the bucket

Apply to all objects in the bucket

If you want the rule to apply to specific objects, you must use a filter to identify those objects. Choose "Limit the scope of this rule using one or more filters". Learn more

☑ I acknowledge that this rule will apply to all objects in the bucket.

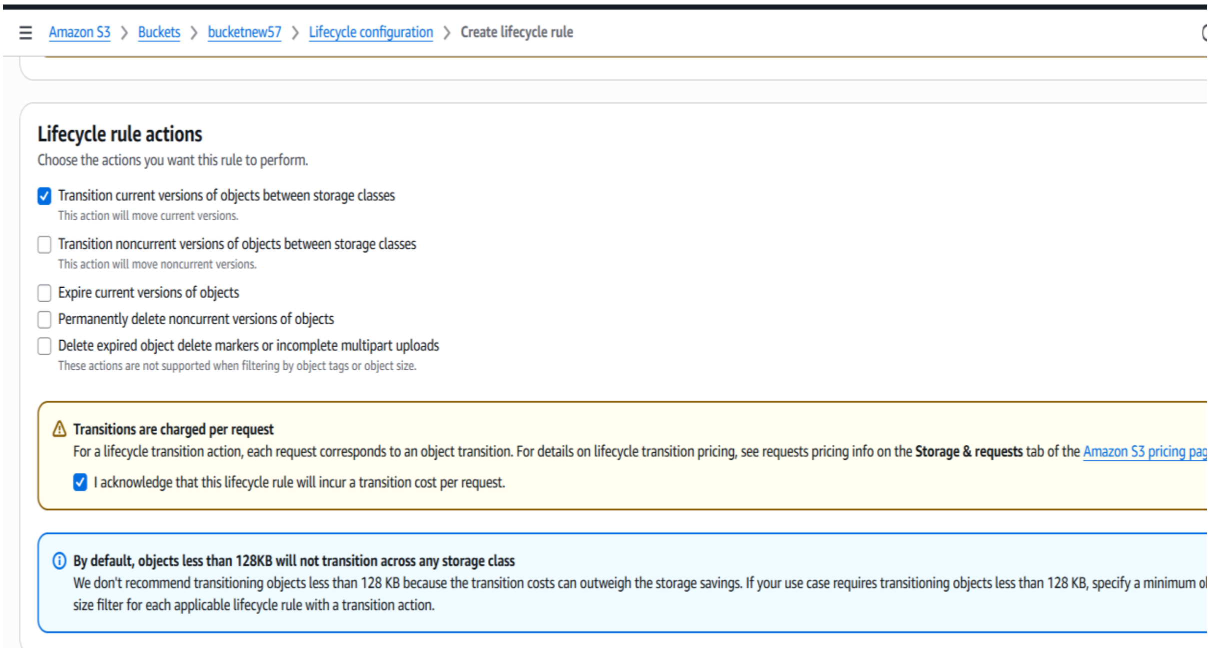
Lifecycle rule actions

Choose the actions you want this rule to perform.

☑ Transition current versions of objects between storage classes

This action will move current versions

Select Transition current versions of objects between storage classes.



☰ Amazon S3 > Buckets > bucketnew57 > Lifecycle configuration > Create lifecycle rule

Lifecycle rule actions

Choose the actions you want this rule to perform.

☑ Transition current versions of objects between storage classes
This action will move current versions.

□ Transition noncurrent versions of objects between storage classes
This action will move noncurrent versions.

□ Expire current versions of objects

□ Permanently delete noncurrent versions of objects

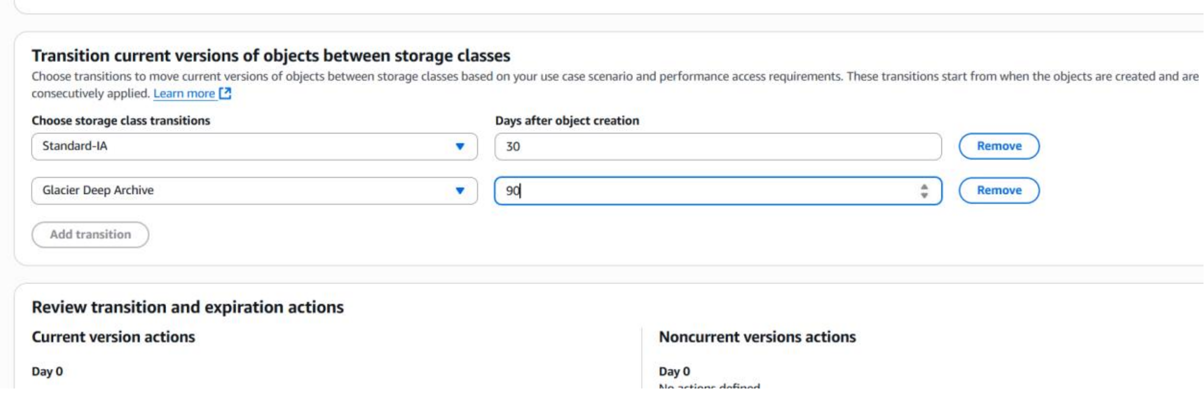
□ Delete expired object delete markers or incomplete multipart uploads
These actions are not supported when filtering by object tags or object size.

⚠ **Transitions are charged per request**
For a lifecycle transition action, each request corresponds to an object transition. For details on lifecycle transition pricing, see requests pricing info on the **Storage & requests** tab of the Amazon S3 pricing pag

☑ I acknowledge that this lifecycle rule will incur a transition cost per request.

ⓘ **By default, objects less than 128KB will not transition across any storage class**
We don't recommend transitioning objects less than 128 KB because the transition costs can outweigh the storage savings. If your use case requires transitioning objects less than 128 KB, specify a minimum o size filter for each applicable lifecycle rule with a transition action.

Select standard IA for 30 days after that and glacier deep archive for 90 days.



Transition current versions of objects between storage classes

Choose transitions to move current versions of objects between storage classes based on your use case scenario and performance access requirements. These transitions start from when the objects are created and are consecutively applied. Learn more

Choose storage class transitions	Days after object creation	
Standard-IA	30	Remove
Glacier Deep Archive	90	Remove

Review transition and expiration actions

Current version actions

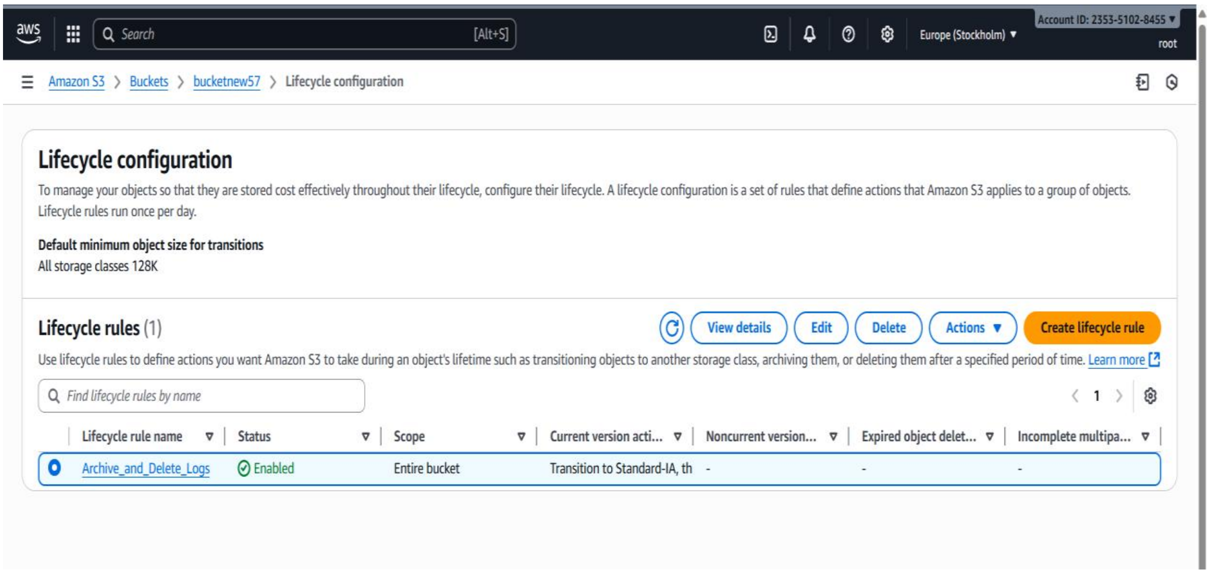
Day 0

Noncurrent versions actions

Day 0

No actions defined

I have created lifecycle policy for specific time to delete objects.



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.

Default minimum object size for transitions
All storage classes 128K

Lifecycle rules (1)

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.

Find lifecycle rules by name

	Lifecycle rule name	Status	Scope	Current version acti...	Noncurrent version...	Expired object delet...	Incomplete multipa...
●	Archive_and_Delete_Logs	✓ Enabled	Entire bucket	Transition to Standard-IA, th	-	-	-

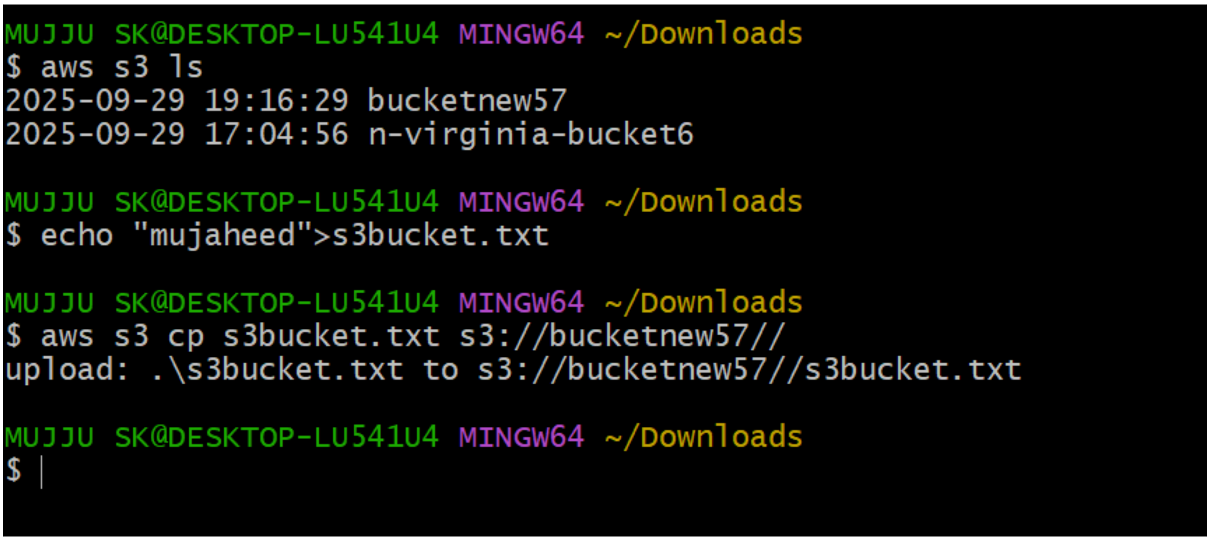
6. Push some objects to S3 using the AWS CLI.

Go to aws console and go to s3 .select bucket it should have s3 full access.

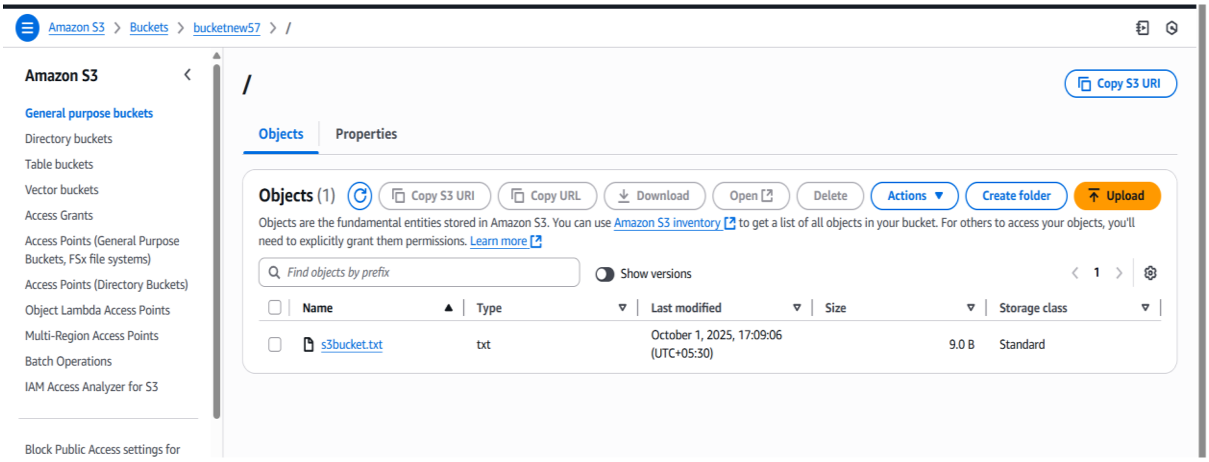
Check the cli is installed or not.

- Aws --version this will show uh the version of cli.
- Then aws configure.

- We already created bucket and we have txt file in our bucket.
- Use the command aws s3 cp file.txt s3://bucket_name



```
MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ aws s3 ls
2025-09-29 19:16:29 bucketnew57
2025-09-29 17:04:56 n-virginia-bucket6

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ echo "mujaheed">s3bucket.txt

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ aws s3 cp s3bucket.txt s3://bucketnew57//
upload: .\s3bucket.txt to s3://bucketnew57//s3bucket.txt

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ |
```



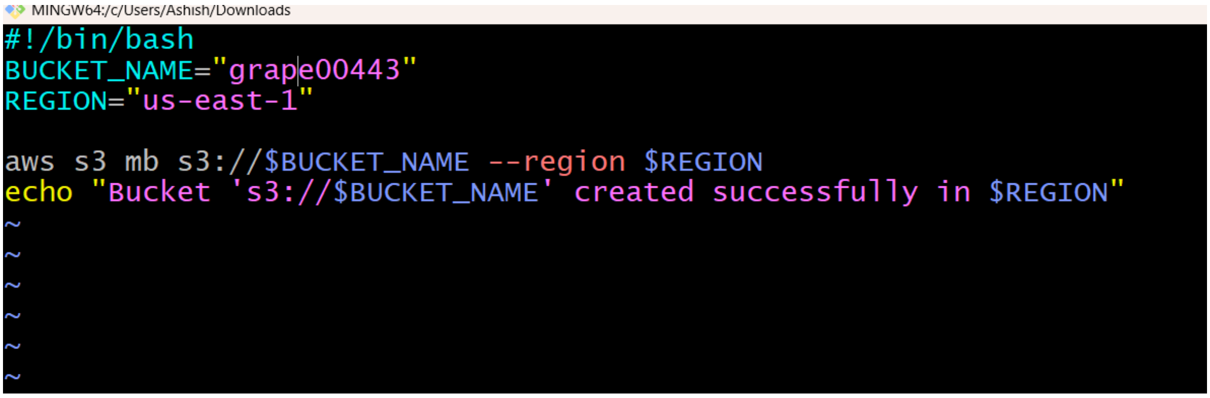
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	Storage class
□	s3bucket.txt	txt	October 1, 2025, 17:09:06 (UTC+05:30)	9.0 B	Standard

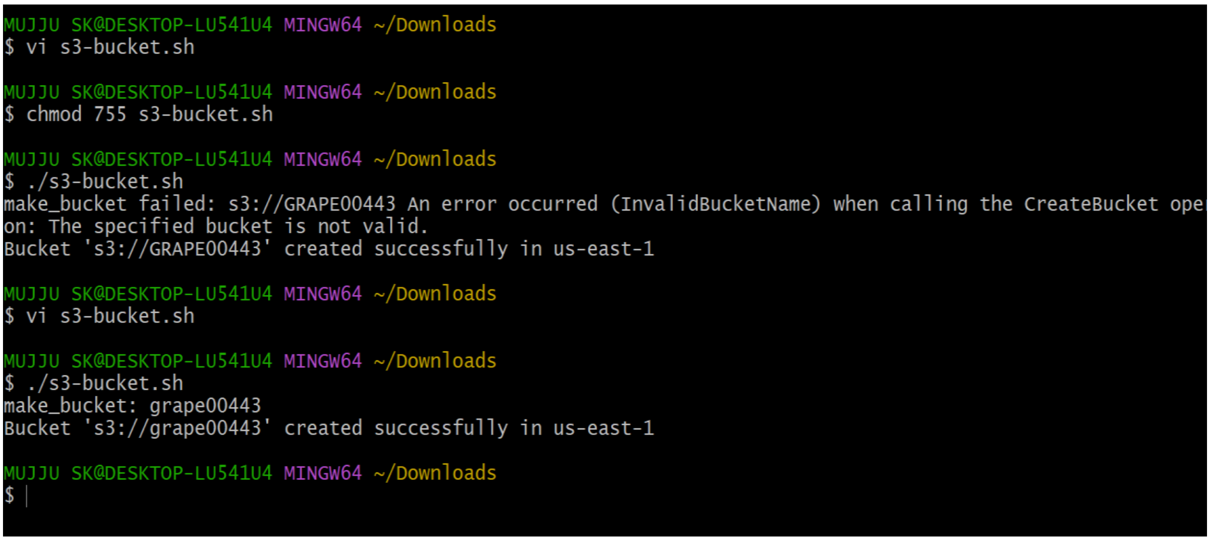
7. Write a Bash script to create an S3 bucket.

Open git bash

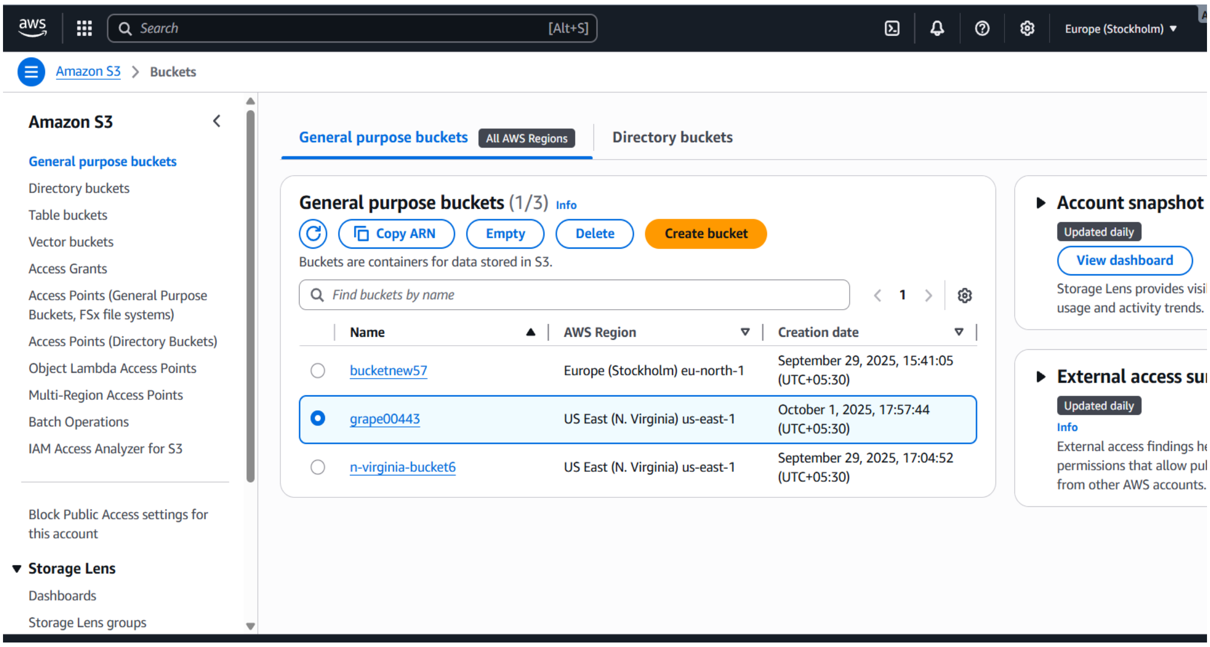
- Check cli upadate.
- Aws configure.
- Then create one file with name of s3bucket.sh
- Write a if bash script for create a bucket.
- Then gave permisson of chmod755 and file name.



```
#!/bin/bash
BUCKET_NAME="grape00443"
REGION="us-east-1"

aws s3 mb s3://$BUCKET_NAME --region $REGION
echo "Bucket 's3://$BUCKET_NAME' created successfully in $REGION"
~
~
~
~
~
~
```



```
MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ vi s3-bucket.sh

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ chmod 755 s3-bucket.sh

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ ./s3-bucket.sh
make_bucket failed: s3://GRAPE00443 An error occurred (InvalidBucketName) when calling the CreateBucket ope
on: The specified bucket is not valid.
Bucket 's3://GRAPE00443' created successfully in us-east-1

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ vi s3-bucket.sh

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ ./s3-bucket.sh
make_bucket: grape00443
Bucket 's3://grape00443' created successfully in us-east-1

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ |
```



General purpose buckets (1/3) Info

Buckets are containers for data stored in S3.

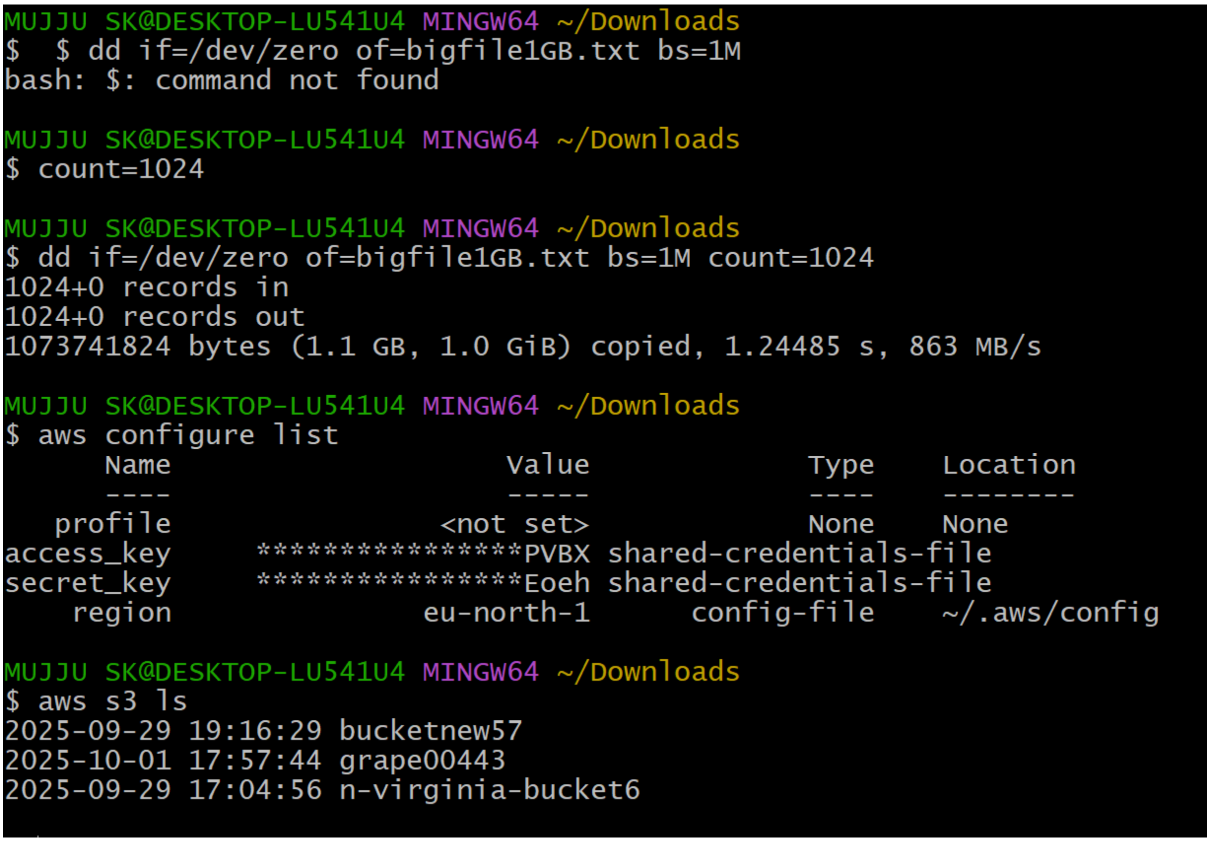
	Name ▲	AWS Region ▽	Creation date ▽
○	bucketnew57	Europe (Stockholm) eu-north-1	September 29, 2025, 15:41:05 (UTC+05:30)
●	grape00443	US East (N. Virginia) us-east-1	October 1, 2025, 17:57:44 (UTC+05:30)
○	n-virginia-bucket6	US East (N. Virginia) us-east-1	September 29, 2025, 17:04:52 (UTC+05:30)

Storage Lens provides visi usage and activity trends.

External access findings he permissions that allow pul from other AWS accounts.

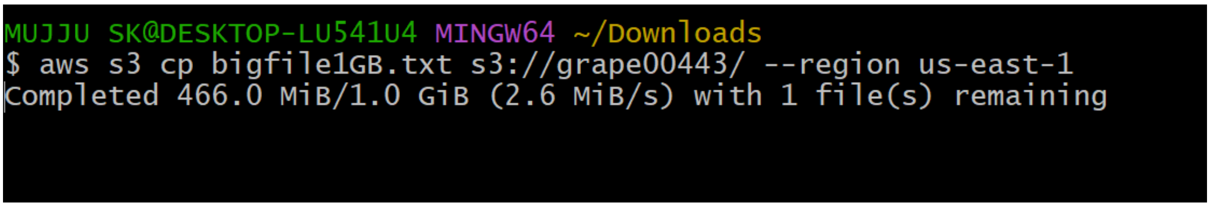
8. Upload a 1 GB file to S3 using the CLI.

Open cli execute a command : dd if=/dev/zero of=file_name.txt bs=1M count=1024.

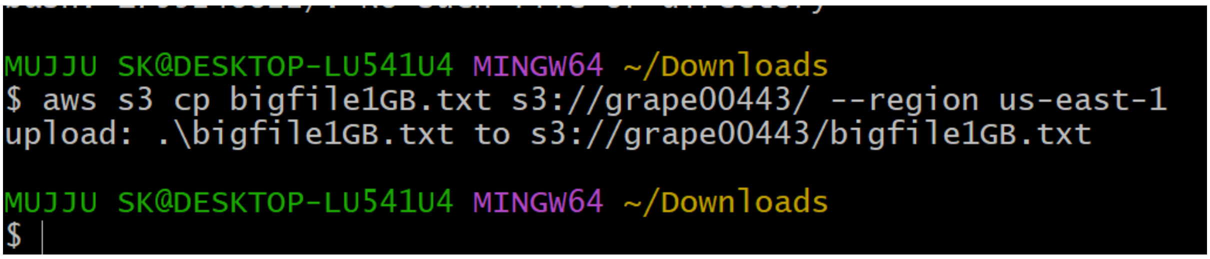


```
MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$  $ dd if=/dev/zero of=bigfile1GB.txt bs=1M
bash: $: command not found

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ count=1024

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ dd if=/dev/zero of=bigfile1GB.txt bs=1M count=1024
1024+0 records in
1024+0 records out
1073741824 bytes (1.1 GB, 1.0 GiB) copied, 1.24485 s, 863 MB/s

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ aws configure list
      Name                    Value             Type    Location
      ----                    -----             ----    --------
   profile                <not set>             None    None
access_key     ****************PVBX shared-credentials-file
secret_key     ****************Eoeh shared-credentials-file
    region               eu-north-1      config-file    ~/.aws/config

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ aws s3 ls
2025-09-29 19:16:29 bucketnew57
2025-10-01 17:57:44 grape00443
2025-09-29 17:04:56 n-virginia-bucket6
```

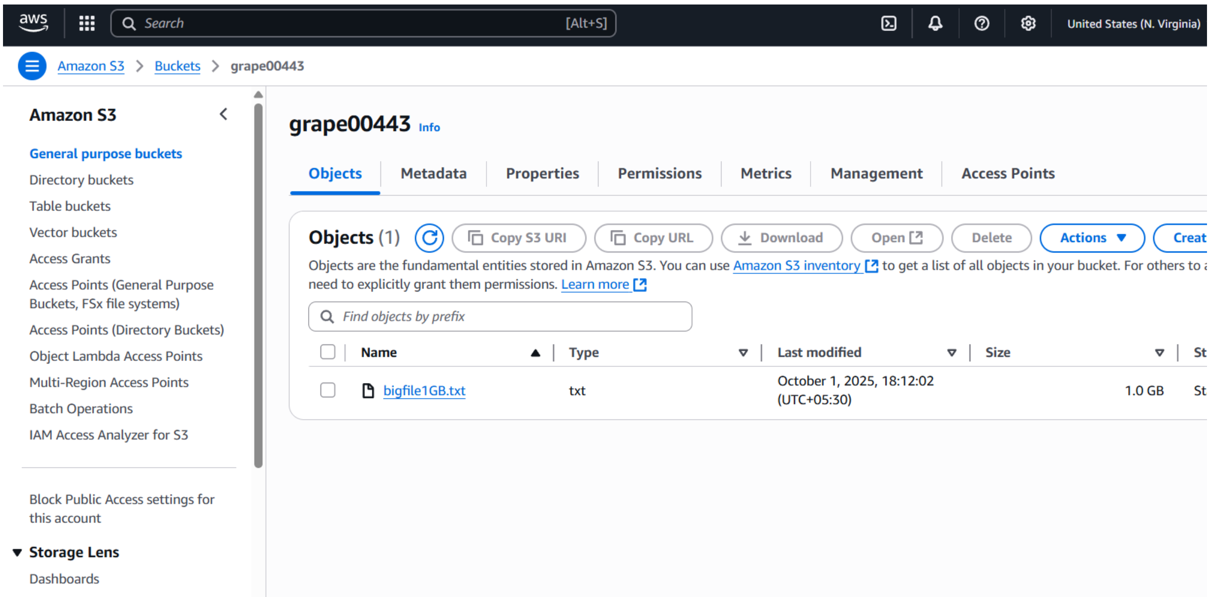
for download purpose use aws s3 cp bigfile1GB.txt s3://bucket_name/--region <bucket_region>.



```
MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ aws s3 cp bigfile1GB.txt s3://grape00443/ --region us-east-1
Completed 466.0 MiB/1.0 GiB (2.6 MiB/s) with 1 file(s) remaining
```



```
bash: [illegible]: No such file or directory

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ aws s3 cp bigfile1GB.txt s3://grape00443/ --region us-east-1
upload: .\bigfile1GB.txt to s3://grape00443/bigfile1GB.txt

MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ 
```



grape00443

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 a need to explicitly grant them permissions. Learn more

□	Name	Type	Last modified	Size	St
□	bigfile1GB.txt	txt	October 1, 2025, 18:12:02 (UTC+05:30)	1.0 GB	St