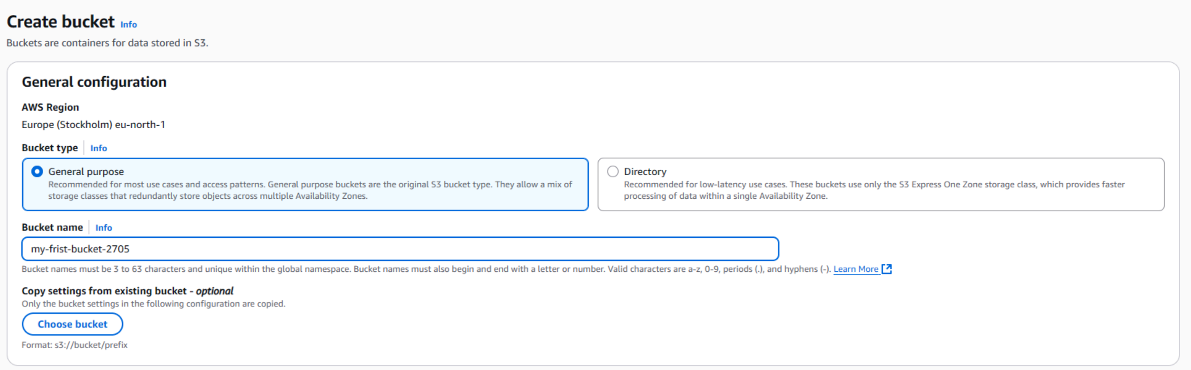
Cloud Intern (CodTech)

Task-1 : Cloud Storage Setup

CREATE AND CONFIGURE CLOUD STORAGE ON AWS S3 OR GOOGLE CLOUD STORAGE.

Go search S3 bucket → click on it → click create bucket



Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

Europe (Stockholm) eu-north-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

my-frist-bucket-2705

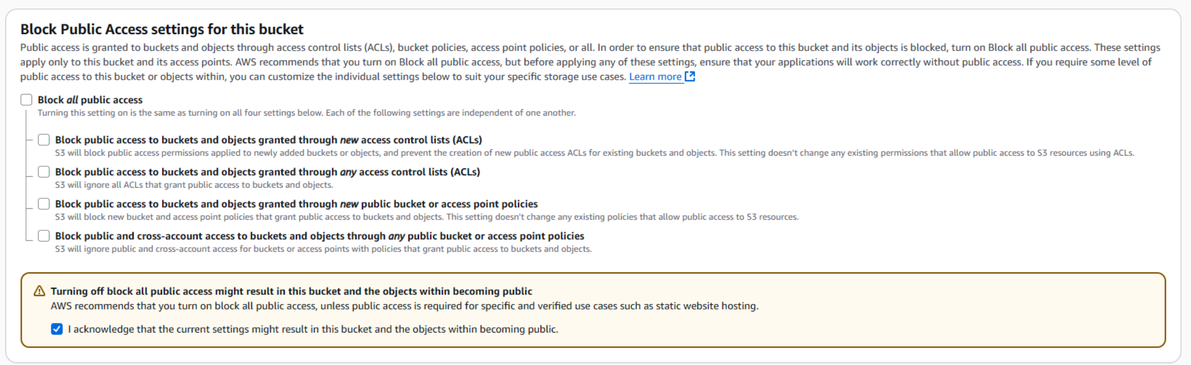
Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). Learn More

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

Give a unique name for the bucket, make sure that your name is having some numbers(ID)



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

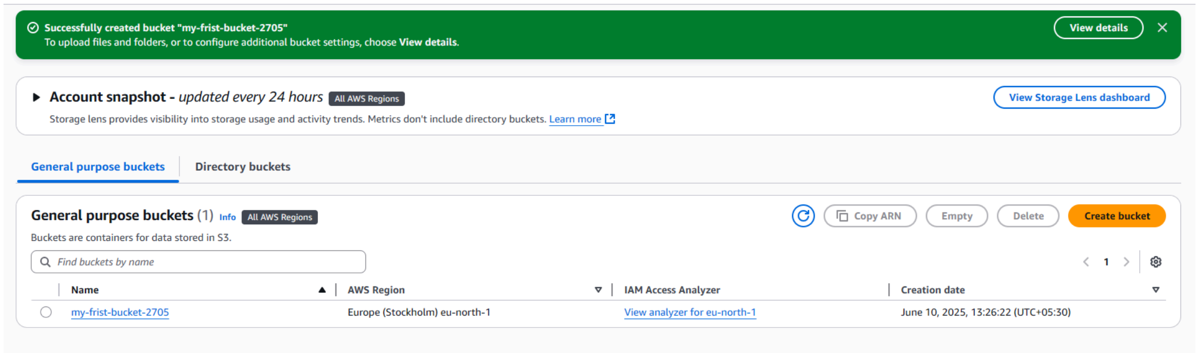
□ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- □ **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.

Uncheck the “Block all public access” and check the acknowledgement.



Successfully created bucket "my-frist-bucket-2705"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

Account snapshot - *updated every 24 hours* All AWS Regions

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more

General purpose buckets (1) Info All AWS Regions

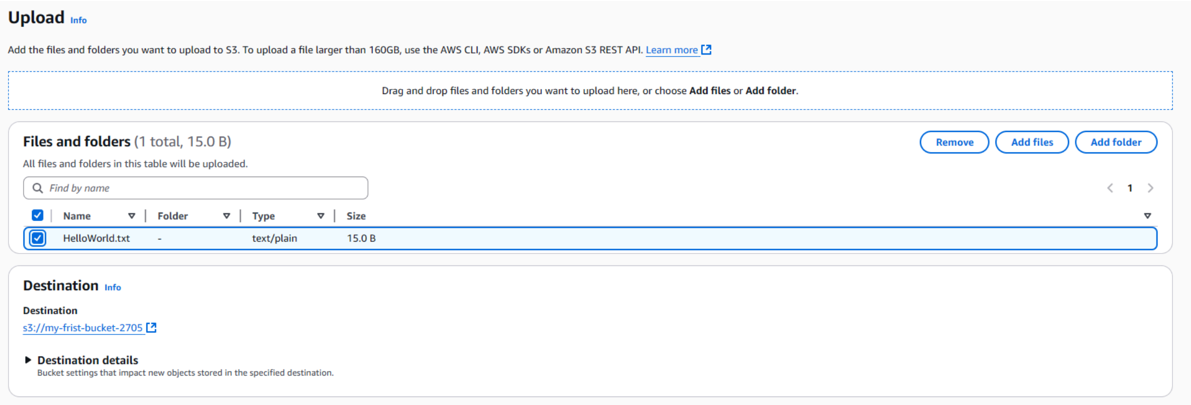
Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
my-frist-bucket-2705	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	June 10, 2025, 13:26:22 (UTC+05:30)

Bucket created

DELIVERABLE: A BUCKET SETUP WITH EXAMPLE FILES UPLOADED AND ACCESS PERMISSIONS CONFIGURED

Uploading file



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, 15.0 B)

All files and folders in this table will be uploaded.

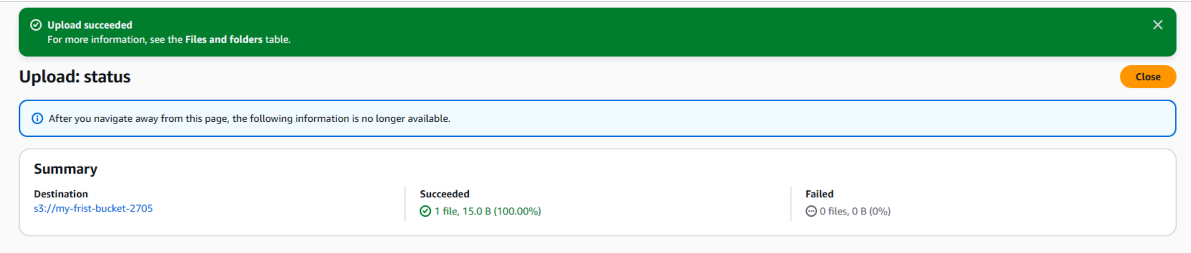
☑	Name	Folder	Type	Size
☑	HelloWorld.txt	-	text/plain	15.0 B

Destination Info

Destination
s3://my-frist-bucket-2705

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

click add files → add the file → select the file you want to upload → click upload



Upload succeeded
For more information, see the **Files and folders** table.

Upload: status

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

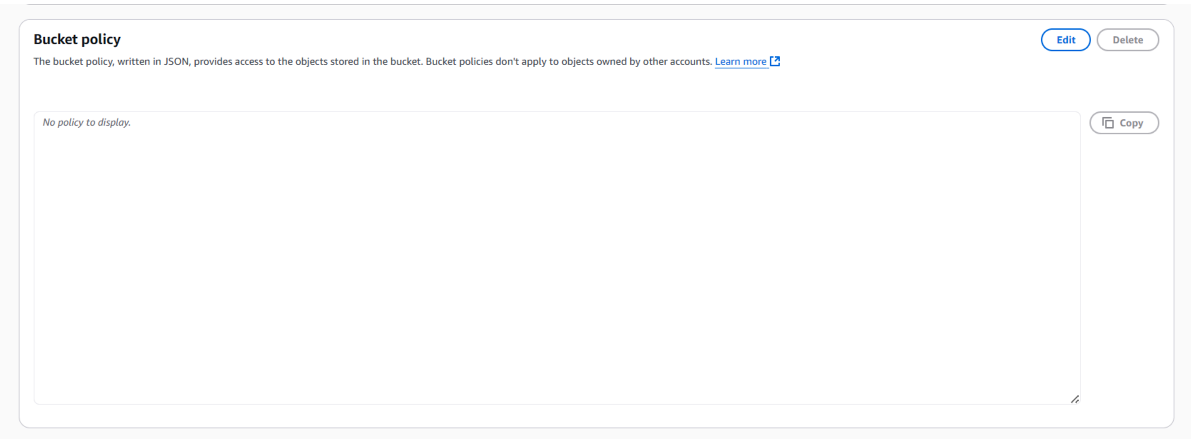
Summary

Destination	Succeeded	Failed
s3://my-frist-bucket-2705	1 file, 15.0 B (100.00%)	0 files, 0 B (0%)

File uploaded

Give Permissions

Click on your bucket name → Go to permissions.



Bucket policy

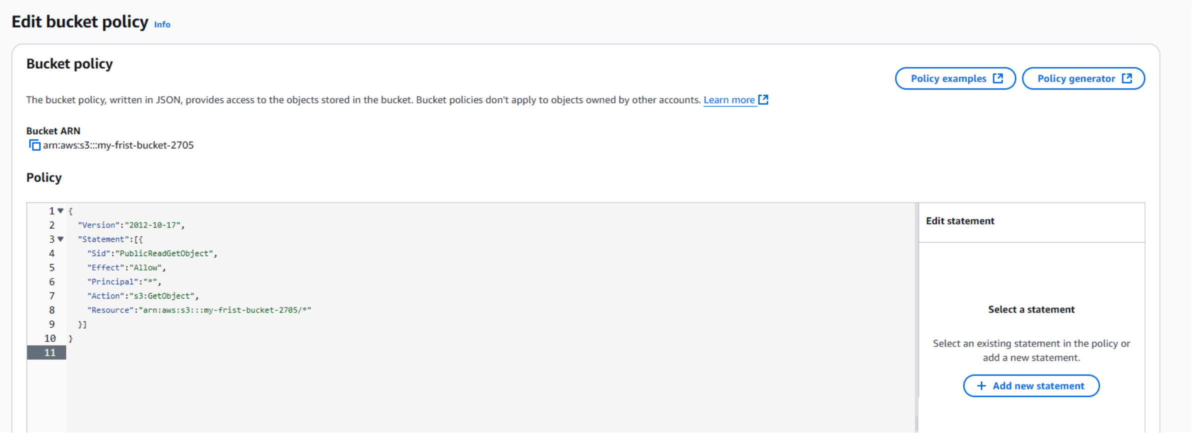
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

No policy to display.

now click edit → copy this json code down below

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

This code will only give a read permissions



Edit bucket policy Info

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

Bucket ARN

arn:aws:s3:::my-frist-bucket-2705

Policy

```
{
  "Version":"2012-10-17",
  "Statement":[{
    "Sid":"PublicReadGetObject",
    "Effect":"Allow",
    "Principal":"*",
    "Action":"s3:GetObject",
    "Resource":"arn:aws:s3:::my-frist-bucket-2705/*"
  }]
}
```

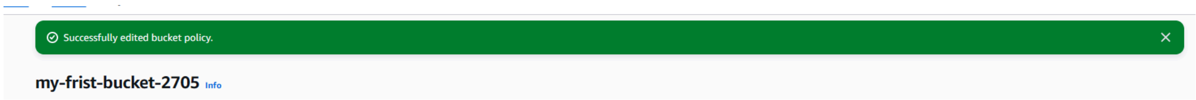
Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

Paste the code in the Policy section

click Save



Successfully edited bucket policy.

my-frist-bucket-2705 Info

Here you gave a permissions