

CODTECH INTERNSHIP – Cloud Computing

Task-1 : Cloud Storage Setup

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

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

Steps to Complete Task:

Creating an S3 Bucket

Go to AWS and search S3 Bucket → Click to select → Click on Create Bucket

Create bucket [Info](#)
Buckets are containers for data stored in S3.

General configuration

AWS Region
Asia Pacific (Mumbai) ap-south-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](#)

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 name for Bucket name, see that name is unique so that it don't show error note i.e., name already exists.

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.

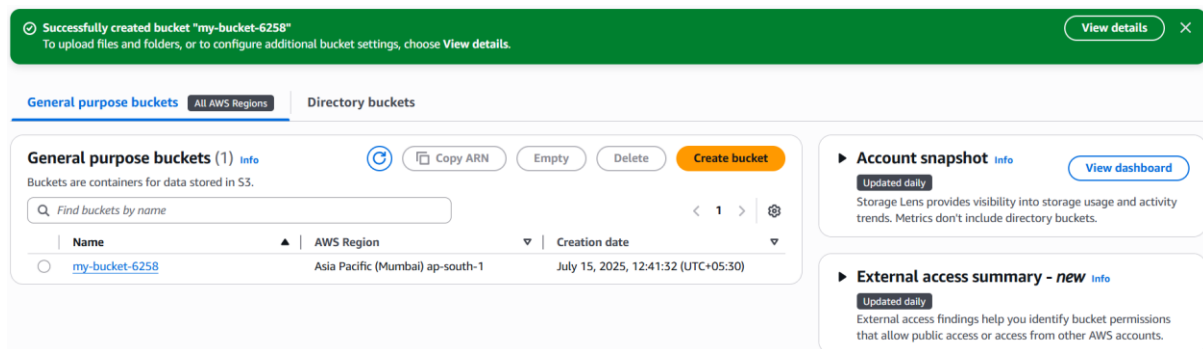
☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

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 acknowledgment.

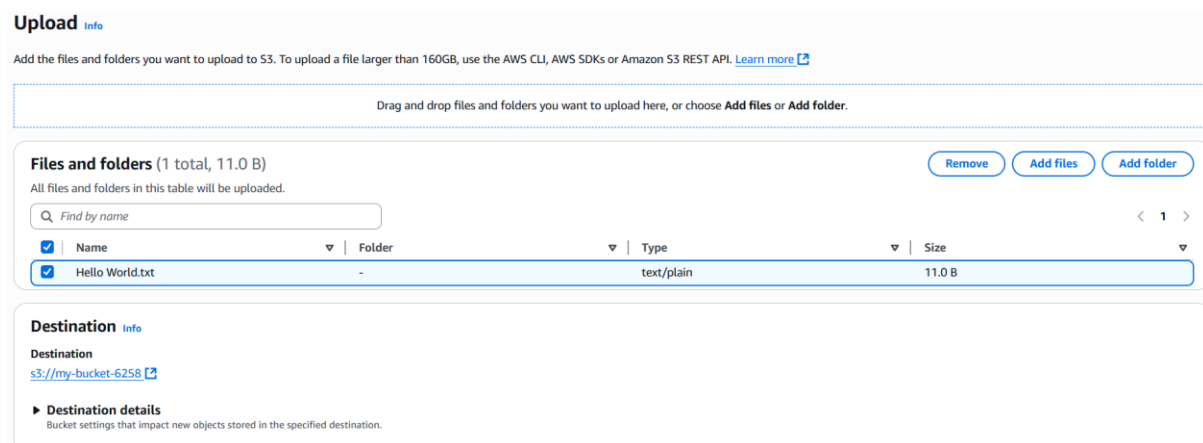
Click on Create Bucket after giving all settings.



Hence, Bucket is Created.

Uploading File and Giving Permissions.

Upload the File.

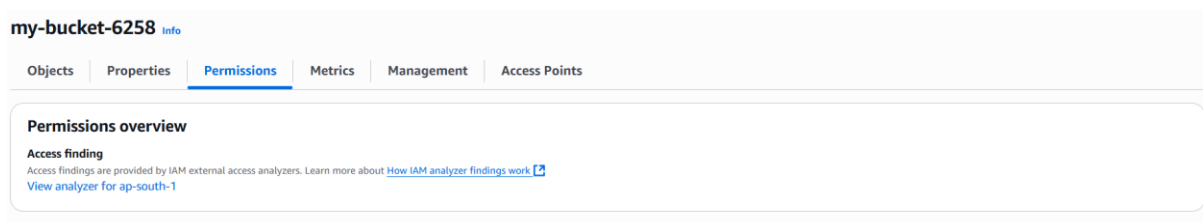


Click on the add files → add the file → select the file you want to upload →

Click on upload.

File will be uploaded.

Click on your bucket name → Go to Permissions



Bucket policy

Edit
Delete

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.

Copy

Click edit → copy the json code below

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

This code will give a read permissions.

Edit bucket policy [info](#)

Bucket policy

[Policy examples](#)
[Policy generator](#)

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-bucket-6258](#)

Policy

1

{

2

"Version": "2012-10-17",

3

"Statement": [{

4

"Sid": "PublicReadGetObject",

5

"Effect": "Allow",

6

"Principal": "*",

7

"Action": "s3:GetObject",

8

"Resource": "arn:aws:s3:::my-bucket-6258/*"

9

]

10

}]

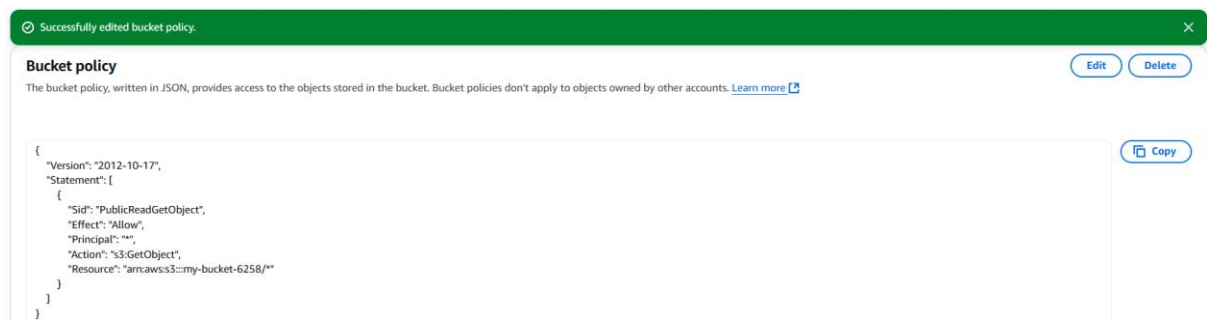
Edit statement

Select a statement

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

[+ Add new statement](#)

Paste the code in the bucket policy section → click save



The Bucket policy will be saved.

The Permissions will be enabled.