Use Cloud Storage Create a storage bucket on your cloud platform and upload/download files. Configure access permissions for the bucket.

ABOUT:

Cloud storage allows users to store and manage data in a secure and scalable environment, providing access to files from anywhere with an internet connection. By creating a storage bucket on a cloud platform, users can efficiently store files such as documents, images, and backups. In this task, we will walk through the process of creating a storage bucket, uploading and downloading files, and configuring access permissions to ensure that only authorized users can interact with the stored data. Cloud storage solutions, such as those provided by platforms like AWS, Google Cloud, and Azure, offer flexibility and robustness in managing large amounts of data.

SIGNIFICANCE:

Scalability: Cloud storage provides virtually unlimited space, allowing users to store large volumes of data without worrying about running out of storage or managing physical hardware.

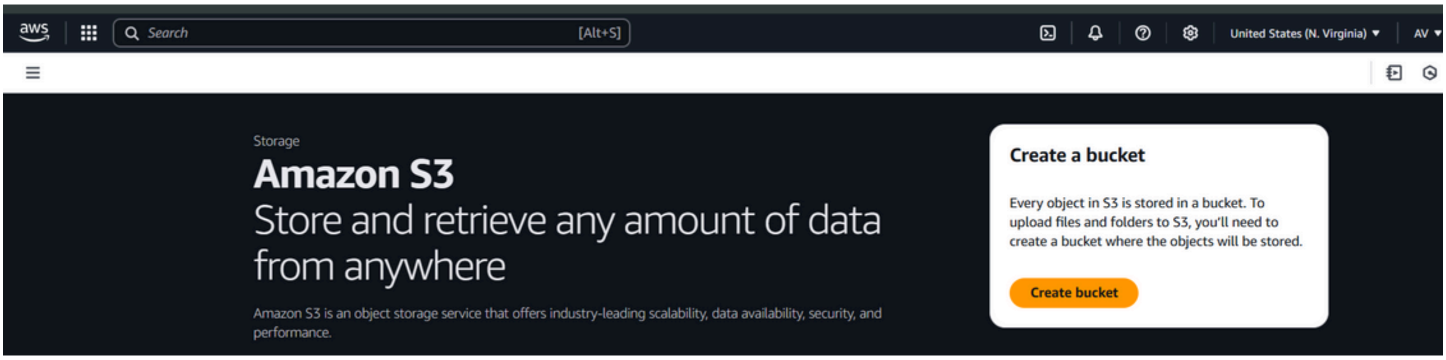
Accessibility: Files stored in the cloud can be accessed from anywhere, at any time, using an internet connection, ensuring flexibility for users who need to retrieve or share data remotely.

Security: Cloud platforms offer advanced security features, such as encryption, access control, and backup options, ensuring data is protected against unauthorized access, loss, or corruption.

Cost Efficiency: With cloud storage, users only pay for the storage they use, eliminating the need for upfront capital investment in physical hardware, maintenance, and upgrades.

STEP 1:

Sign in to your AWS console and search for S3 bucket



Storage

Amazon S3

Store and retrieve any amount of data from anywhere

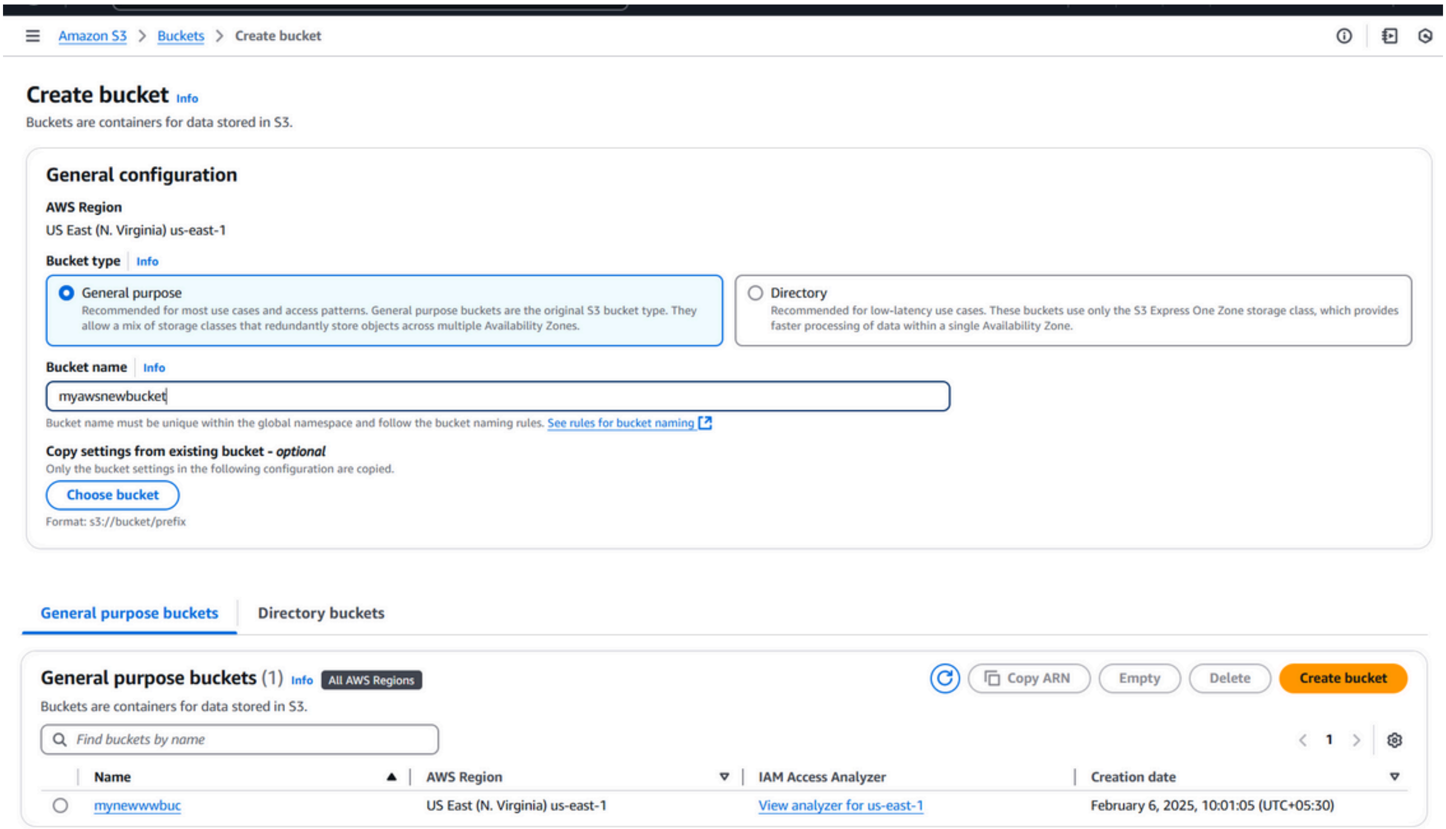
Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

STEP 2:

Create a new bucket with unique bucket



Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

US East (N. Virginia) us-east-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

myawsnewbucket

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

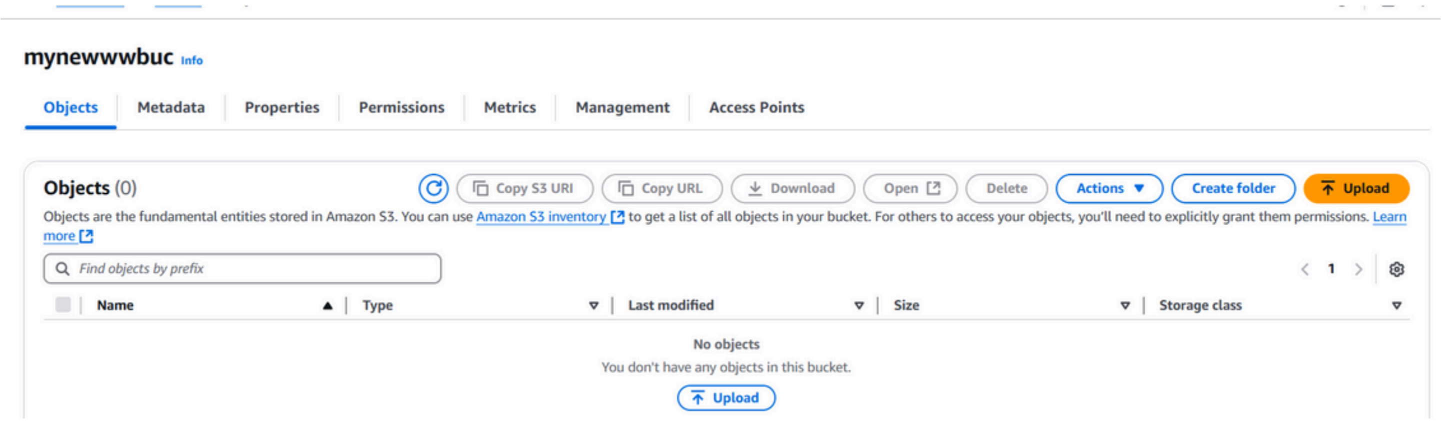
General purpose buckets (1) Info All AWS Regions

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	mynewwwbuc	US East (N. Virginia) us-east-1	View analyzer for us-east-1	February 6, 2025, 10:01:05 (UTC+05:30)

STEP 3:

Go to created bucket and click on upload and add the files from your PC to the bucket



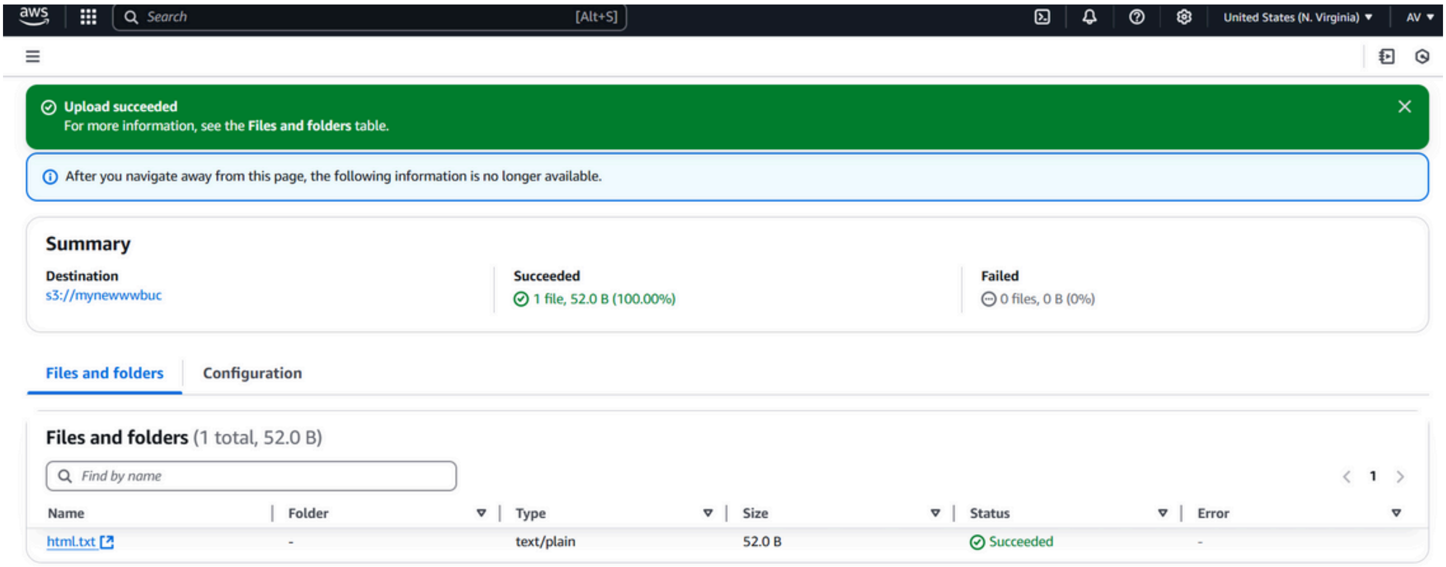
Objects (0)

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.



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

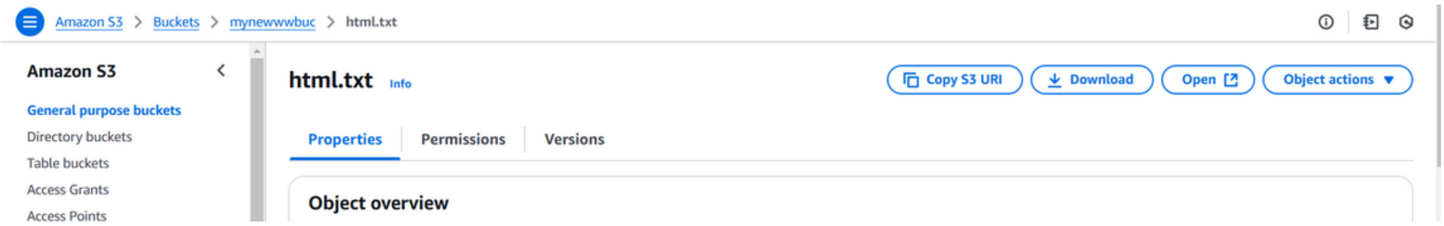
Destination	Succeeded	Failed
s3://mynewwwbuc	✓ 1 file, 52.0 B (100.00%)	0 files, 0 B (0%)

Files and folders (1 total, 52.0 B)

Name	Folder	Type	Size	Status	Error
html.txt	-	text/plain	52.0 B	✓ Succeeded	-

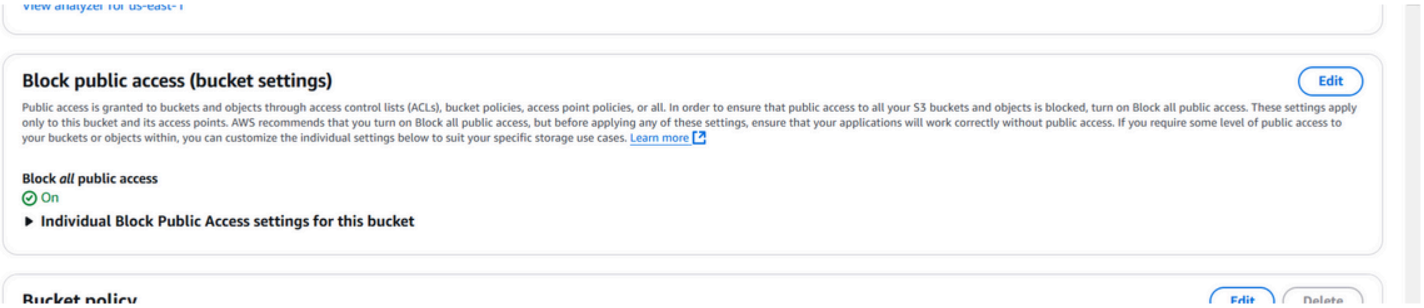
STEP 4:

Click on uploaded file and on the top right corner select download



STEP 5:

Move to the permission table and click on edit public access



Block public access (bucket settings)

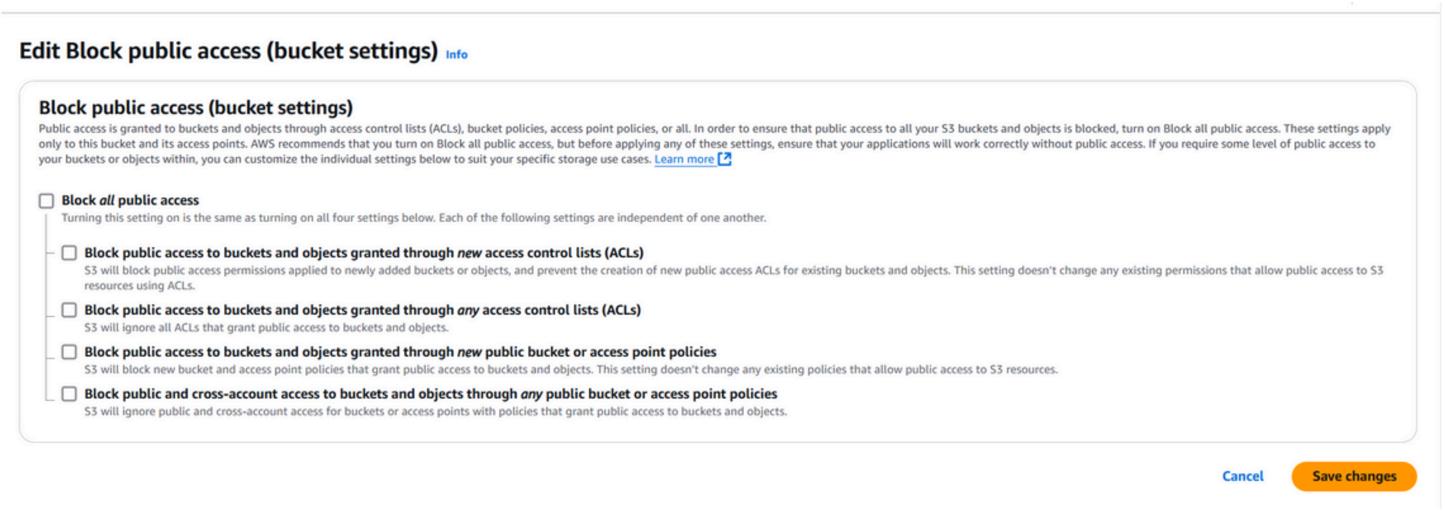
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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
✓ On

▶ Individual Block Public Access settings for this bucket

Bucket policy

Click on save changes after enabling public access



Edit Block public access (bucket settings)

Block public access (bucket settings)

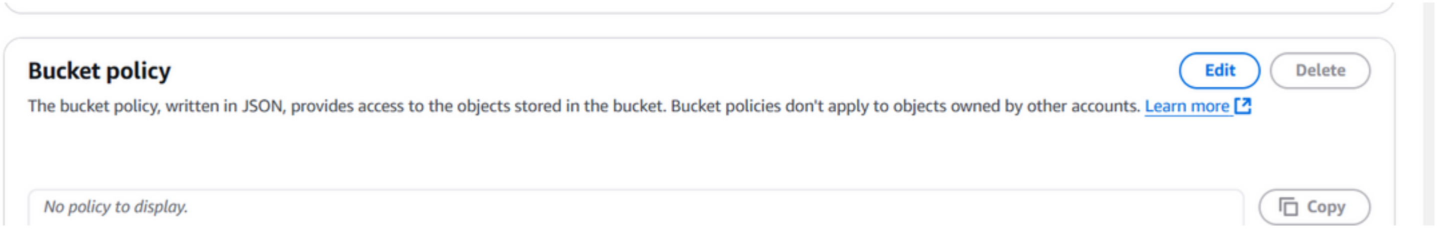
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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.

STEP 6:

Go to permission in your bucket and edit the bucket policy



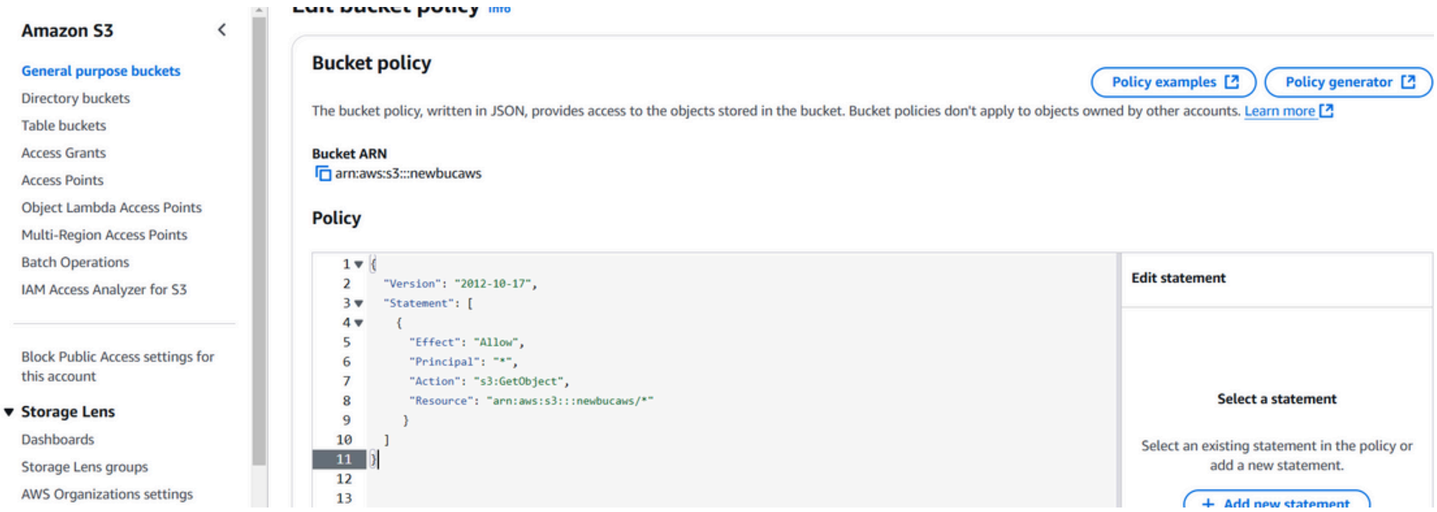
Bucket policy

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

No policy to display.

STEP 7:

Go to permission under bucket and scroll down to bucket policy. Copy the following JSON code



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:::newbucaws

Policy

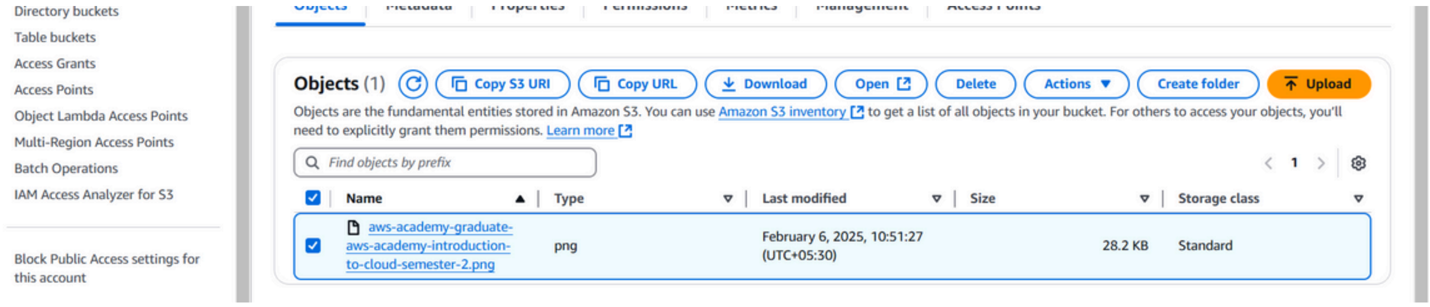
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::newbucaws/*"
    }
  ]
}
```

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

click on save changes

STEP 8:

Go to Objects and copy the URL



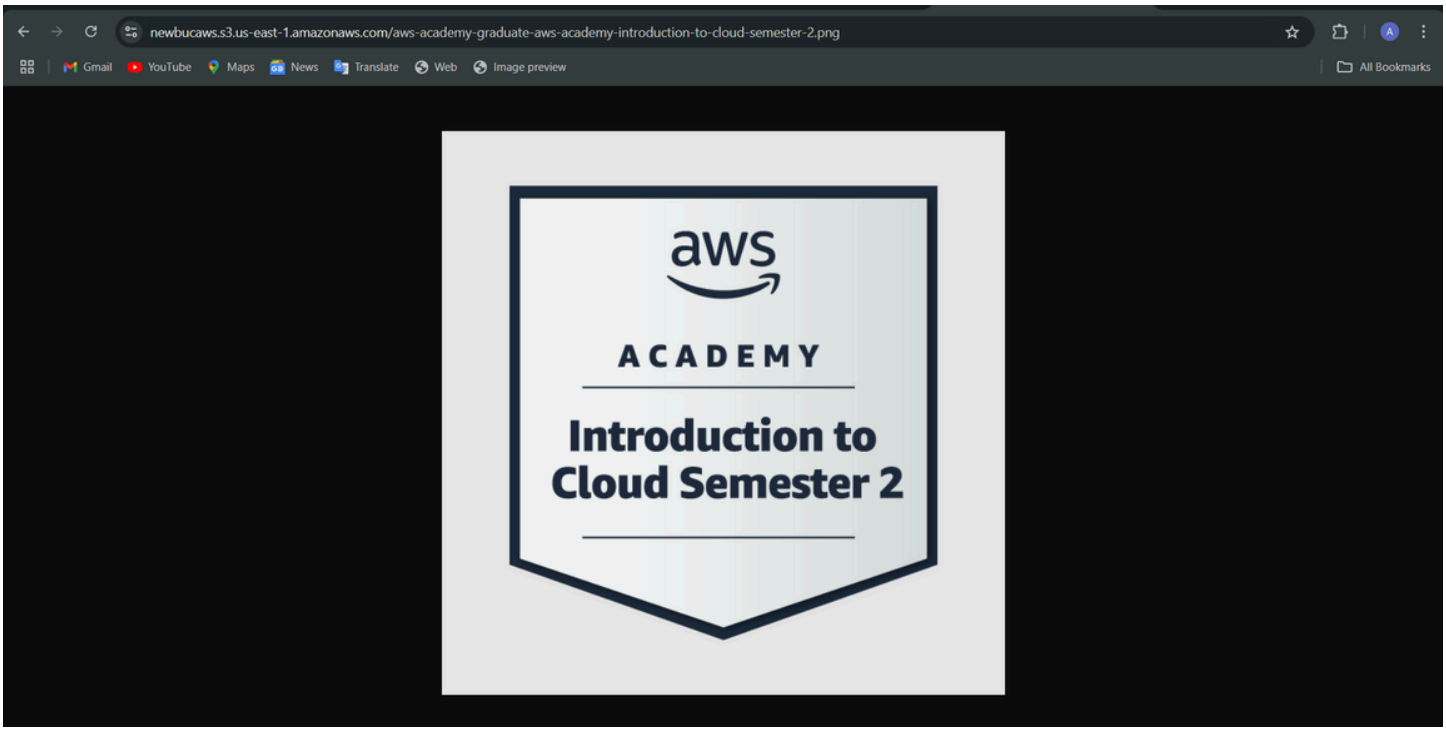
Objects (1)

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
☑	aws-academy-graduate-aws-academy-introduction-to-cloud-semester-2.png	png	February 6, 2025, 10:51:27 (UTC+05:30)	28.2 KB	Standard

STEP 9:

Open a new tab and paste the copied URL link. You will be able to see the file you have uploaded in the S3 Bucket


newbucaws.s3.us-east-1.amazonaws.com/aws-academy-graduate-aws-academy-introduction-to-cloud-semester-2.png
Gmail
YouTube
Maps
News
Translate
Web
Image preview
All Bookmarks
aws
ACADEMY
Introduction to Cloud Semester 2

OUTCOME:

1. **Easy File Management**: Efficient organization and retrieval of files through intuitive interfaces and flexible folder structures.
2. **Streamlined Collaboration**: Multiple users can access, edit, and share files in real-time, improving teamwork and productivity across distributed teams.
3. **Automated Backups**: Cloud storage ensures data is automatically backed up and protected, reducing the risk of data loss due to hardware failure or human error.
4. **Customizable Access Control**: Users can define specific permissions (read, write, delete) for different individuals or groups, ensuring secure and authorized access to sensitive data.
5. **Improved Disaster Recovery**: Cloud storage enables businesses and individuals to quickly recover lost data in the event of hardware failure, accidental deletion, or cyber threats, ensuring minimal downtime.