



St. JOSEPH'S
GROUP OF INSTITUTIONS
OMR, CHENNAI - 119



Placement Empowerment Program

Cloud Computing and DevOps Centre

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

Name: CHELSIAH M

Department: CSE



Introduction:

Cloud Storage is a scalable and secure solution for storing data in the cloud. It allows users to store and retrieve files such as images, videos, backups, and other types of data from anywhere. Cloud storage is commonly used for hosting static files, backups, and large datasets in cloud environments like **AWS S3 (Simple Storage Service)**. A **storage bucket** is a logical container for storing objects (files) in the cloud. Configuring **access permissions** for the bucket ensures that only authorized users, applications, or services can upload, download, or modify files.

Objective:

Understand cloud storage concepts and how storage buckets work.

Create a storage bucket in a cloud platform (AWS, GCP, or Azure).

Upload and download files using both the cloud console and CLI.

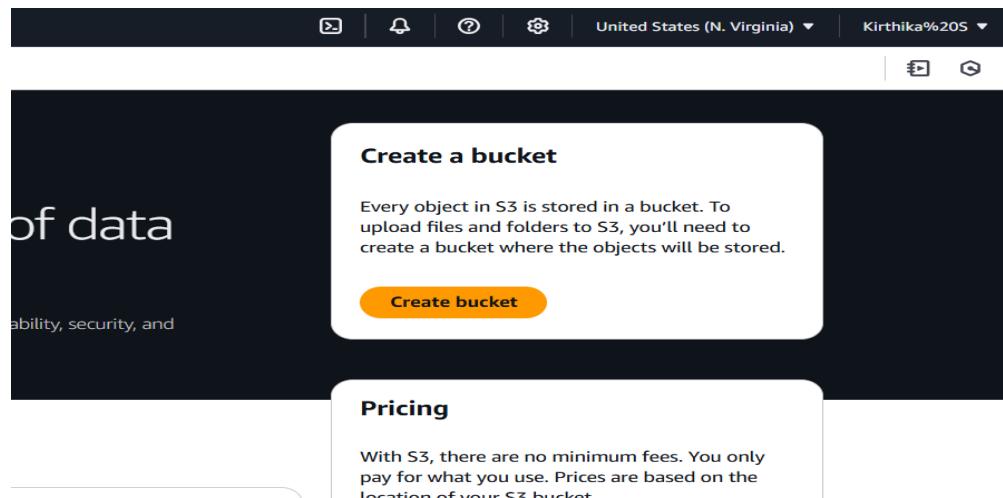
Configure permissions to manage access control and security.

Ensure data protection by restricting or granting access based on policies.

Step 1:

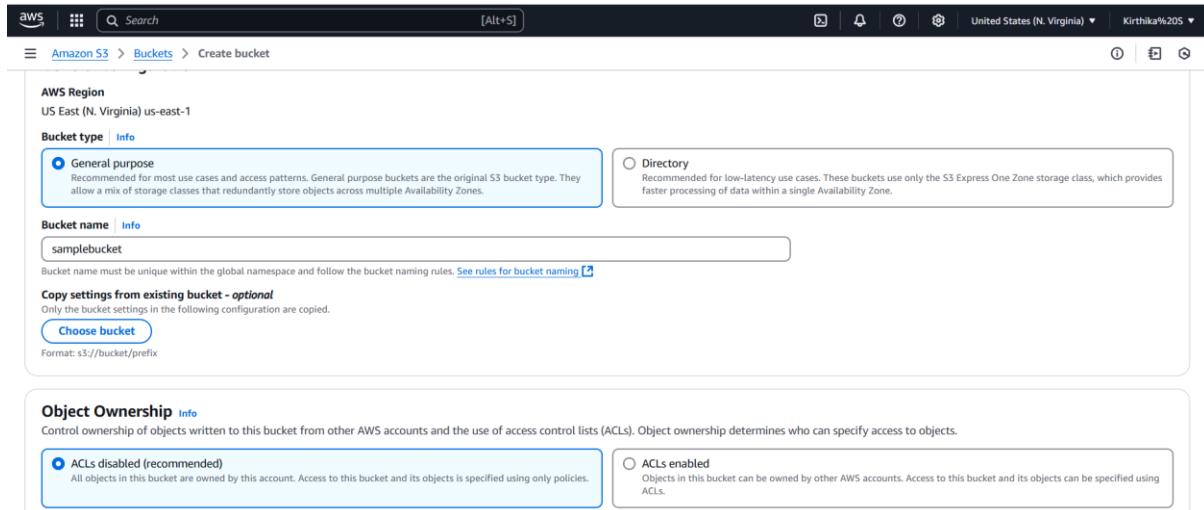
Sign in to your cloud provider's console:

AWS: Navigate to the S3 service



Step 2:

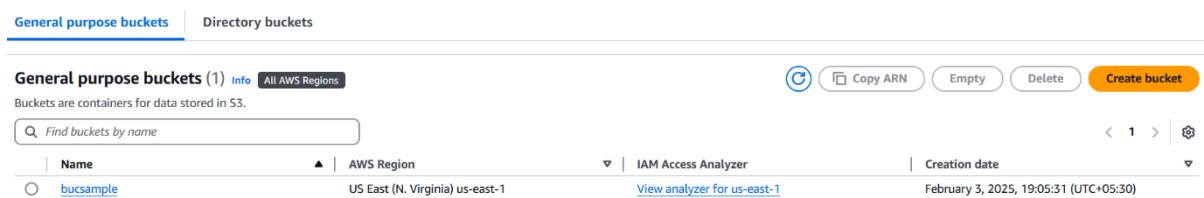
Create bucket with **unique name** and Leave other settings as default,
Configure **versioning** (optional) to keep previous versions of files.



The screenshot shows the 'Create bucket' wizard in the AWS S3 console. Under 'Bucket type', 'General purpose' is selected. The 'Bucket name' field contains 'samplebucket'. Under 'Object Ownership', 'ACLs disabled (recommended)' is selected. Other tabs like 'Info', 'Copy settings from existing bucket - optional', and 'Choose bucket' are also visible.

Step 3:

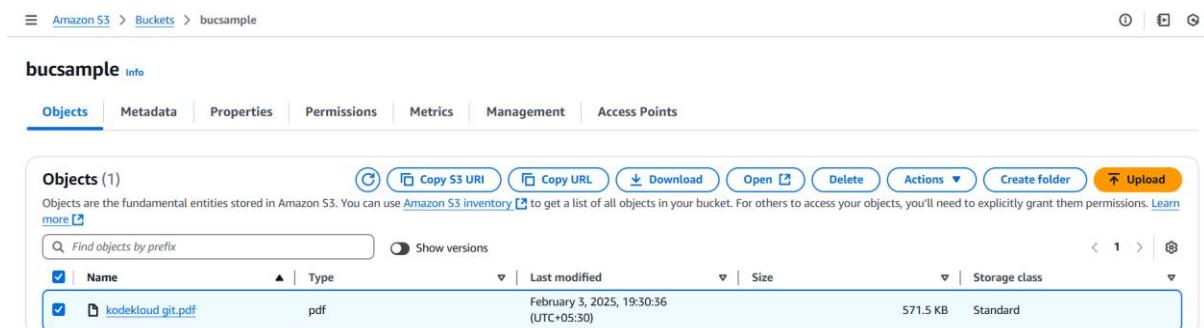
Bucket created,



The screenshot shows the 'General purpose buckets' list. It displays one bucket named 'bucsample' located in 'US East (N. Virginia) us-east-1'. The bucket was created on 'February 3, 2025, 19:05:31 (UTC+05:30)'. Action buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket' are visible.

Step 4:

Upload the files by click the Add new files, you can download the file



The screenshot shows the 'Objects' list for the 'bucsample' bucket. It lists one object named 'kodekloud git.pdf' which is a 'pdf' file. The file was uploaded on 'February 3, 2025, 19:30:36 (UTC+05:30)' and has a size of '571.5 KB' and 'Standard' storage class. Action buttons for 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload' are available.

Step 5:

Go to the **Permissions** tab of your bucket

Enable the public access by clicking **edit option**, then click save changes

The screenshot shows the 'Edit Block public access (bucket settings)' page. It includes a detailed description of what each setting does and a list of five options under 'Block public access (bucket settings)'. At the bottom right are 'Cancel' and 'Save changes' buttons.

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.

[Cancel](#) [Save changes](#)

Step 6:

Scroll down to **Bucket Policy** and click Edit, you

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy [S3 Bucket Policy](#)

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

Effect Allow Deny

Principal

Use a comma to separate multiple values.

AWS Service Amazon S3 All Services (*)

Use multiple statements to add permissions for more than one service.

Actions 1 Action(s) Selected All Actions (*)

Amazon Resource Name (ARN) arn:aws:s3:::bucsample/*

ARN should follow the following format: arn:aws:s3:::\${BucketName}/\${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

[Add Statement](#)

Step 7:

Save 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](#)

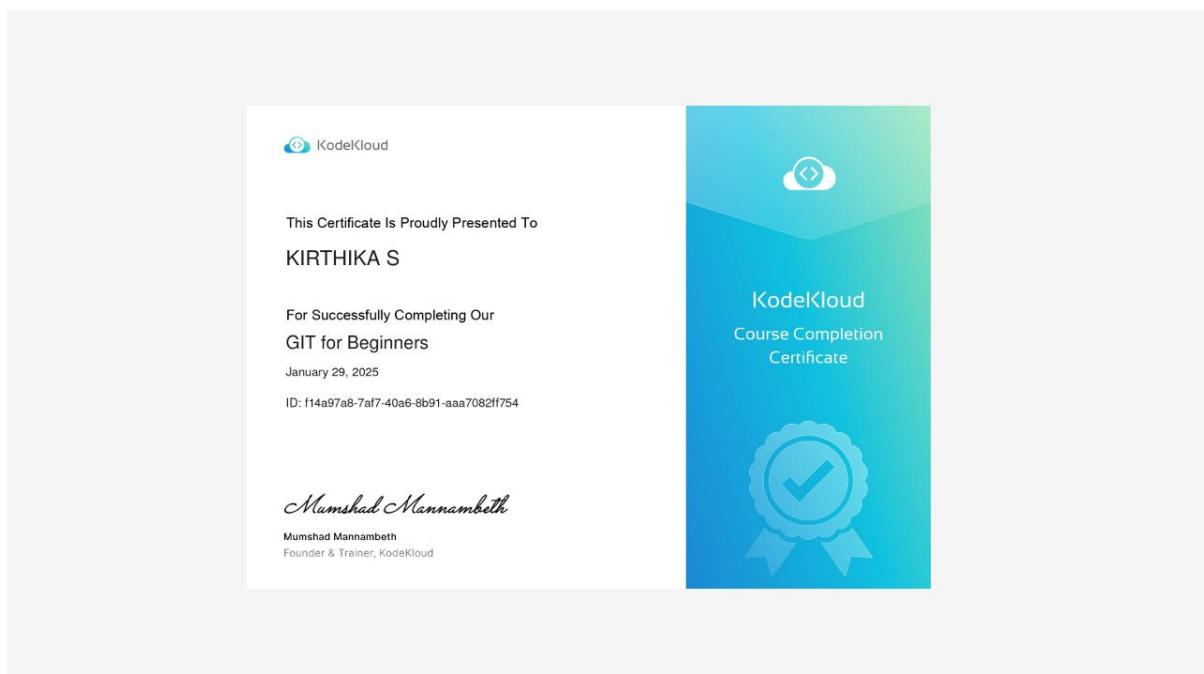
Bucket ARN
 arn:aws:s3:::bucsamp

Policy

```
1 ▼ {  
2   "Id": "Policy1738590993391",  
3   "Version": "2012-10-17",  
4   "Statement": [  
5     {  
6       "Sid": "Stmt1738590982316",  
7       "Action": [  
8         "s3:GetObject"  
9       ],  
10      "Effect": "Allow",  
11      "Resource": "arn:aws:s3:::bucsamp/*",  
12      "Principal": "*"  
13    }  
14  ]  
15 }
```

Step 8:

Copy the **Url** of your uploaded file in Copy URL option and paste it in the new web page



Overview:

- Created a **cloud storage bucket**.
- Uploaded and downloaded files using the cloud console and command-line tools.
- Configured **permissions** to control who can access the storage bucket.