 

**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: Tamizhvanan V Department: ECE



**Introduction:**

Cloud storage services like **Amazon Simple Storage Service (S3)** offer a scalable, reliable, and low-latency solution for storing and retrieving any amount of data from anywhere on the web. S3 is widely used for hosting websites, storing backups, sharing large files, and more. It provides various features like data encryption, access control policies, and versioning to ensure data security and flexibility.

In this tutorial, we will guide you through the process of creating an **S3 bucket**, uploading and downloading files, and configuring access permissions to control who can access the data. You'll learn how to use both the AWS Management Console and AWS Command Line Interface (CLI) to interact with S3. Additionally, we'll explore how to manage public and private access to your S3 bucket.

**Objective:**

The objective of this exercise is to:

1. Understand the basics of cloud storage and Amazon S3.
2. Create an S3 bucket to store files.
3. Upload files to the S3 bucket using the AWS Management Console and AWS CLI.
4. Download files from the S3 bucket.
5. Configure the bucket’s permissions to allow or restrict public access to the files.
6. Test accessibility based on the configured permissions.

By the end of this tutorial, you will have hands-on experience with AWS S3 for storing and managing data in the cloud.

**Prerequisites:**

* An AWS account.
* Basic knowledge of using the AWS Management Console and AWS CLI.
* Familiarity with file management concepts (uploading/downloading).

**Steps to Use AWS S3 for Cloud Storage:**

**1. Creating an S3 Bucket:**

1. **Sign in to your AWS Management Console** and navigate to the **S3 Dashboard**.
2. Click on **Create bucket**.
3. Provide a unique **bucket name** (e.g., my-s3-bucket-unique123) and select an AWS region for the bucket (ensure it's a region close to your location for better performance).
4. **Bucket settings**:
   * You can choose to enable or disable options like versioning, logging, and encryption. For this tutorial, you can leave these options as default.
5. **Configure permissions**:
   * In this step, ensure that the bucket's public access settings are set appropriately. For now, we will leave the default settings that **block all public access** for security.
6. Click **Create bucket** to create your S3 bucket.

**2. Uploading Files to the S3 Bucket:**

**Option 1: Using the AWS Management Console:**

1. After creating the bucket, click on your newly created bucket name to open the bucket details page.
2. Click **Upload**.
3. In the **Upload files** section, click **Add files** to select files from your local computer.
4. Click **Next** to proceed through the options.
5. Review and click **Upload** to upload the files to your S3 bucket.

**3. Downloading Files from the S3 Bucket:**

**Option 1: Using the AWS Management Console:**

1. Navigate to the **S3 bucket** in the AWS Console.
2. Find the file you want to download.
3. Click the file name and select **Download**.

**4. Configuring Bucket Permissions:**

**Restricting Public Access:**

By default, AWS S3 buckets block all public access. You can either allow or restrict access based on your use case.

1. Navigate to your **S3 bucket** in the AWS Console.
2. In the bucket details, go to the **Permissions** tab.
3. Under **Block public access (bucket settings)**, you will see options to block all public access. By default, these options are enabled.
4. You can disable these settings if you want to allow public access to your bucket (for example, if you're hosting a website), but be cautious about exposing sensitive data.

**Setting Bucket Policy for Public Access:**

1. You can also define a bucket policy to control access. For instance, to allow public read access to all files, you can create a policy like this:

{

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

"Statement": [

{

"Effect": "Allow",

"Principal": "\*",

"Action": "s3:GetObject",

"Resource": "arn:aws:s3:::your-bucket-name/\*"

}

]

}

This policy grants **read access** to all files in your bucket. Replace your-bucket-name with your actual bucket name.

1. To apply the policy, go to the **Permissions** tab in your bucket, and under **Bucket Policy**, paste the policy and click **Save**.

**Testing Bucket Permissions:**

1. To test the public access (if you’ve allowed it), navigate to one of the uploaded files in your S3 bucket.
2. Click on the file name and click **Copy URL**.
3. Open the copied URL in a browser. If public access is allowed, you should be able to view or download the file directly from the browser.

**5. Best Practices for Managing S3 Buckets:**

* **Encryption:** Enable server-side encryption to protect data at rest.
* **Versioning:** Enable versioning to keep track of changes to files and allow rollback to previous versions.
* **Access Control:** Use IAM policies, bucket policies, and ACLs to control access to your S3 bucket and files. Avoid using public access unless absolutely necessary.
* **Lifecycle Policies:** Set lifecycle policies to automatically archive or delete files after a certain period to save on storage costs.

**Conclusion:**

In this tutorial, you learned how to create an AWS S3 bucket, upload and download files using both the AWS Console and AWS CLI, and configure bucket permissions for managing access to your data. By utilizing S3's flexible permissions system, you can securely manage access to your stored data, making it a powerful tool for cloud storage and data management.