 

**Placement Empowerment Program**

***Cloud Computing and DevOps Centre***

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

Name: MIRDULA C Department: ADS



**Introduction**

### Cloud-based monitoring services allow users to track, analyze, and optimize their cloud resources in real time. AWS CloudWatch is a powerful monitoring tool that collects and visualizes key performance metrics such as CPU usage, memory utilization, network activity, and disk I/O. By enabling CloudWatch, users can proactively monitor system health, troubleshoot performance issues, and optimize resource allocation.

### ****Overview****

In this guide, you will:

1. **Create a cloud storage bucket** on a cloud platform (e.g., AWS S3).
2. **Upload and download files** to/from the bucket.
3. **Set access permissions** to control who can access stored files.
4. **Test access to ensure secure file sharing and retrieval**.

Cloud storage simplifies data management by providing accessibility, redundancy, and security features.

### ****Objectives****

 Learn how to **create a storage bucket** in the cloud.

 Upload and download files using **cloud CLI or web console**.

 Configure **access control policies** for secure data management.

 Understand **public vs. private storage settings**.

**Importance**

✅ Real-time Performance Monitoring – Helps track application health and performance.  
✅ Automated Alerts – Notifies users of unusual activity or resource spikes.  
✅ Cost Optimization – Helps identify underutilized or over-provisioned resources.  
✅ Security & Troubleshooting – Detects potential threats and resolves issues faster.

**Step-by-Step Overview**

**Step 1: Create a Cloud Storage Bucket**

On AWS (Amazon S3)

1. Log in to AWS Console → Navigate to Amazon S3.
2. Click Create Bucket.
3. Enter a unique bucket name (e.g., my-cloud-bucket).
4. Select the AWS Region where the bucket will be stored.
5. Choose Public or Private Access:
   * Private (default): Files can only be accessed by the owner.
   * Public: Anyone can access files (not recommended for sensitive data).
6. Click Create Bucket.

**Step 2: Upload Files to the Storage Bucket**

Using AWS Console

1. Open your S3 bucket.
2. Click Upload and select a file from your local system.
3. Set permissions and storage class (Standard, Infrequent Access, Glacier).
4. Click Upload to store the file.

Using AWS CLI

1. Install AWS CLI (if not already installed)
2. Configure AWS CLI with your credentials
3. Upload a file

**Step 3: Download Files from the Storage Bucket**

Using AWS Console

1. Open the S3 bucket.
2. Click on the file you want to download.
3. Click Download to save it to your local machine.

**Step 4: Configure Access Permissions for the Bucket**

Make the File Public (AWS S3)

Open the S3 bucket → Click on the file.

Click Permissions → Edit Object Public Access.

Enable Public Read Access and save changes.

The file will have a public URL like:

Restrict Access with IAM Policies

Open IAM Console → Navigate to Policies.

Create a policy to allow access to specific users.

Assign the policy to a specific IAM user or group.

**Outcome**

After completing this setup, you will have:  
✅ A **storage bucket** ready for use.  
✅ Successfully **uploaded and downloaded files**.  
✅ Configured **secure access permissions**.  
✅ Learned how to manage **cloud storage efficiently**.