**Steps to Create and Configure an S3 Bucket**

**1. Create an S3 Bucket**

1. Log in to your **AWS Management Console**.
2. Navigate to **S3**.
3. Click **"Create bucket"**.
4. Provide a **unique bucket name** (e.g., sahil-bucket-123).
5. Choose an **AWS region** closest to your users.
6. Select **Block Public Access settings** (Keep private unless public access is required).
7. Click **Create bucket**.

**2. Upload Example Files**

1. Open your bucket.
2. Click **"Upload"**.
3. Add example files (e.g., MyDoc.txt).
4. Click **Upload**.

**3. Configure Bucket Permissions**

**Option A: Public Read-Only Bucket (If Needed)**

* Uncheck **"Block all public access"**.
* Add a **Bucket Policy** for public access:

{

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

"Statement": [

{

"Effect": "Allow",

"Principal": "\*",

"Action": "s3:GetObject",

"Resource": "arn:aws:s3:::sahil-bucket-123/\*"

}

]

}

**4. Configure IAM Policy for Specific Users**

1. Go to **IAM** in AWS Console.
2. Create an IAM **User/Role**.
3. Attach an **S3 access policy**, e.g., for read-only(read\_s3):

{

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

"Statement": [

{

"Effect": "Allow",

"Action": ["s3:ListBucket", "s3:GetObject"],

"Resource": [

"arn:aws:s3:::sahil-bucket-123",

"arn:aws:s3:::sahil-bucket-123/\*"

]

}

]

}

1. Assign the policy to the user.

**Verification**

* Use aws s3 ls s3://sahil-bucket-123/ to confirm file uploads.
* Test access with different IAM users.
* If public, verify by accessing https://sahil-bucket-123.s3.amazonaws.com/MyDoc.txt.