Step 1: S3 Bucket Creation

create an S3 bucket called **my-company-bucket-2025**. Now, grant **read-only access** to a specific IAM user.(ex-developer-user is the user that I've granted the access to)

Step 2: Create a Custom IAM Policy

1. **Go to the AWS IAM Console**: IAM Management Console
2. **Click on "Policies"** in the left sidebar.
3. **Click on "Create Policy".**
4. **Select the JSON tab** and paste the following policy:

```
    {
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"s3:GetObject",
"s3:ListBucket"
],
"Resource": [
"arn:aws:s3:::my-company-bucket-2025",
"arn:aws:s3:::my-company-bucket-2025/*"
]
}
]
}
```

5. **Click "Next"**
6. **Name the policy**: S3ReadOnlyAccess.
7. **Click "Create Policy".**

Step 3: Attach the Policy to an IAM User

1. **Go to the IAM Console** > Click **Users**.
2. **Select the user** (developer-user).
3. **Go to the "Permissions" tab** > Click **"Attach Policies"**.
4. **Search for S3ReadOnlyAccess**, select it, and click **Attach policy**.

Step 4: Configure AWS CLI

If you haven't configured AWS CLI yet,

RUN**: aws configure**

It will prompt you to enter:

- AWS Access Key ID
- AWS Secret Access Key
- Default region name (us-west-2)
- Default output format (json)

```
C:\Users\Harshitha Basavaraju>aws configure
AWS Access Key ID [****************M4MD]: AKIA52J2NMSVJBXIOIDE
AWS Secret Access Key [****************M2c5]: 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
Default region name [us-west-2]: us-west-2
Default output format [json]: json
```

Step 5: Verify the Read-Only Access

Now, test whether your IAM user has **read-only permissions** by running these commands:

RUN: aws s3 ls (to list the buckets you've created)

RUN: aws s3 ls s3://my-company-bucket-2025/ (list content of S3 bucket)

```
C:\Users\Harshitha Basavaraju>aws s3 ls
2025-04-02 19:32:54 my-company-bucket-2025

C:\Users\Harshitha Basavaraju>aws s3 ls s3://my-company-bucket-2025
2025-04-02 19:34:40     189207 basic aws class.pdf
```

Step 6: Test Upload (Should Fail)

Since your IAM policy does **not** allow s3:PutObject, trying to upload a file should result in an **Access Denied** error.

RUN : **aws s3 rm s3://my-company-bucket-2025/sample-file.txt**

RUN : **aws s3 cp test-file.txt s3://my-company-bucket-2025/**

```
C:\Users\Harshitha Basavaraju>aws s3 rm s3://my-company-bucket-2025/sample-file.txt
delete failed: s3://my-company-bucket-2025/sample-file.txt An error occurred (AccessDenied) when calling the DeleteObject operation: User: arn:aws:iam::9498
47155882:user/developer-user is not authorized to perform: s3:DeleteObject on resource: "arn:aws:s3:::my-company-bucket-2025/sample-file.txt" because no ide
ntity-based policy allows the s3:DeleteObject action

C:\Users\Harshitha Basavaraju>echo "This is a test file" > test-file.txt

C:\Users\Harshitha Basavaraju>aws s3 cp test-file.txt s3://my-company-bucket-2025/
upload failed: .\test-file.txt to s3://my-company-bucket-2025/test-file.txt An error occurred (AccessDenied) when calling the PutObject operation: User: arn
:aws:iam::949847155882:user/developer-user is not authorized to perform: s3:PutObject on resource: "arn:aws:s3:::my-company-bucket-2025/test-file.txt" becau
se no identity-based policy allows the s3:PutObject action

C:\Users\Harshitha Basavaraju>
```