STEP 1 — Create the IAM User (NEW AWS UI)

1. Go to IAM → Users → Create user
2. Enter username: user1
3. Click Next
4. Do NOT expect access key option here (AWS removed it)
5. Click Create user

✔ Your user is created.

✅ STEP 2 — Add Permissions

1. Click on the newly created user: user1
2. Go to Permissions tab
3. Click Add permissions
4. Choose Attach policies directly
5. Search → AmazonEC2ReadOnlyAccess
6. Select it → Add permissions

✔ user1 now has EC2 Read-Only access.

✅ STEP 3 — Create Access Key (Programmatic Access)

This is the new way AWS wants you to do it.

1. In IAM → Users → user1
2. Go to Security credentials tab
3. Scroll down to Access keys
4. Click Create access key
5. AWS will ask: "What type of access do you need?"
   Choose:
   ✔ Command Line Interface (CLI)
6. Check the confirmation box → Click Next
7. Click Create Access Key

You will now see:

- Access Key ID

- Secret Access Key (only once)

⚠️ Save the keys safely.
You cannot view the secret again later.

✅ **STEP 4 — Create IAM Group "admin-group"**

1. In AWS IAM → Left menu → Click **User groups**
2. Click **Create group**
3. Group name: **admin-group**
4. Do NOT attach any policies yet
5. Click **Create group**

✓ admin-group created successfully.

✅ **STEP 5 — Create Users "admin1" and "admin2"**

Repeat this process twice:

For admin1

1. IAM → **Users → Create user**
2. Username: **admin1**
3. Click **Next** → **Create user**

For admin2

1. IAM → **Users → Create user**
2. Username: **admin2**
3. Click **Next** → **Create user**

✓ Two admin users created.

✅ **STEP 6 — Add admin1 and admin2 to admin-group**

1. Go to **User groups**
2. Click **admin-group**
3. Open **Users** tab
4. Click **Add users**
5. Select **admin1** and **admin2**
6. Click **Add users**

✓ Both users are now members of admin-group.

✅ **STEP 7 — Attach "AdministratorAccess" Policy to admin-group**

1. Still in admin-group → Go to **Permissions**
2. Click **Add permissions**
3. Select **Attach policies**
4. Search: **AdministratorAccess**
5. Select it
6. Click **Add permissions**

✓ admin-group now has FULL ACCESS to AWS
✓ Therefore: admin1 + admin2 also have full access.

⭐ **Now Group and User part is completed.**

Next, we will create the custom policy.

✅ **STEP 8 — Create Custom Policy "custom-policy"**

This will allow full access to S3 + DynamoDB.

1. IAM → Left menu → **Policies**
2. Click **Create policy**
3. Click the **JSON** tab
4. Delete everything inside
5. Paste this:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "s3:*",
    "dynamodb:*"
   ],
   "Resource": "*"
```

```
    }
  ]
}
```

6. Click **Next**
7. Name the policy: **custom-policy**
8. Click **Create policy**

✓ Your custom policy is now created.

✅ **STEP 9 — Create IAM User "user2"**

1. IAM → **Users → Create user**
2. Type username: **user2**
3. Click **Next** → **Create user**

✓ user2 created.

✅ **STEP 10 — Attach custom-policy to user2**

1. IAM → **Users** → click **user2**
2. Go to **Permissions** tab
3. Click **Add permissions**
4. Choose **Attach policies directly**
5. Search: **custom-policy**
6. Select it → **Add permissions**

✓ user2 now has S3 + DynamoDB permissions.