**Lab Exercise- Creating and Applying an IAM Policy for EC2**

**Objective**

Create a custom IAM policy that allows limited EC2 actions, attach it to a user/role, and test access.

**Step 1: Prerequisites**

* An AWS account with administrator access.
* A test IAM user or role (not your root account).
* Basic knowledge of EC2 (launch/stop/terminate instances).

**Step 2: Create a Custom IAM Policy**

1. Log in to the **AWS Management Console**.
2. Go to **IAM → Policies → Create Policy**.
3. Choose the **JSON tab**.
4. Paste the following sample JSON (allows only *start/stop/describe* on EC2, but not terminate):

{

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

"Statement": [

{

"Effect": "Allow",

"Action": [

"ec2:DescribeInstances",

"ec2:StartInstances",

"ec2:StopInstances"

],

"Resource": "\*"

},

{

"Effect": "Deny",

"Action": [

"ec2:TerminateInstances"

],

"Resource": "\*"

}

]

}

1. Click **Next → Next → Create Policy**.
2. Name it: EC2-StartStop-Policy.

**Step 3: Attach Policy to an IAM User**

1. Go to **IAM → Users**.
2. Select your test user.
3. Under **Permissions → Add Permissions → Attach Policies**, select EC2-StartStop-Policy.
4. Save changes.

**Step 4: Test the Policy**

1. Sign in to the AWS Console as the **test user** (or assume role).
2. Go to **EC2 → Instances**.
3. Try these actions:
   * **Start/Stop** an instance → Allowed.
   * **Terminate** an instance → Should fail (Access Denied).
   * **Describe Instances** → Allowed.

**Step 5: (Optional) Refine Policy for Specific Resources**

* Modify JSON to apply only to certain instances using ARNs:

"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-0123456789abcdef0"

**Step 6: Clean Up**

* Detach the policy from the test user.
* Delete the custom policy if no longer needed.