



# DENY ACTION ON POLICY

1. In this lab you're going to see what deny action in policy be like.
2. Now open IAM, then navigate to policies.
3. There click on create policy.
4. Now in the service select EC2, select **deny** in **Effect** and check the box under manual actions for All EC2 actions.

▼ EC2  
Deny All actions

Specify what actions can't be performed on specific resources in EC2.

▼ Actions denied

Specify actions from the service to be denied.

Filter Actions

Manual actions | Add actions

☒ All EC2 actions (ec2:\*)

Effect  
☐ Allow ☒ Deny

5. After that in the resources select ALL.
6. Then move forward.

▼ Resources

Specify resource ARNs for these actions.

☒ All

☐ Specific

## ► Request conditions - optional

Actions on resources are allowed or denied only when these conditions are met.

7. Give your policy a name, then attach this policy to IAM user account.
8. After that login with your IAM user account in a different browser.
9. Then navigate to EC2. You will see that you are denied to do anything, because you are not authorized.

Instances Info

Find Instance by attribute or tag (case-sensitive)

You are not authorized to perform this operation. User: arn:aws:iam::463646775279:user/s3-usr01 is not authorized to perform: ec2:DescribeInstances with an explicit deny in an identity-based policy