# IAM Roles and Permissions

## NAME: Swathika K
## DEPARTMENT: AML

## OBJECTIVE:

To set up IAM Roles and Permissions - Create an IAM role on cloud platform. Assign the role to your VM to restrict/allow specific actions.

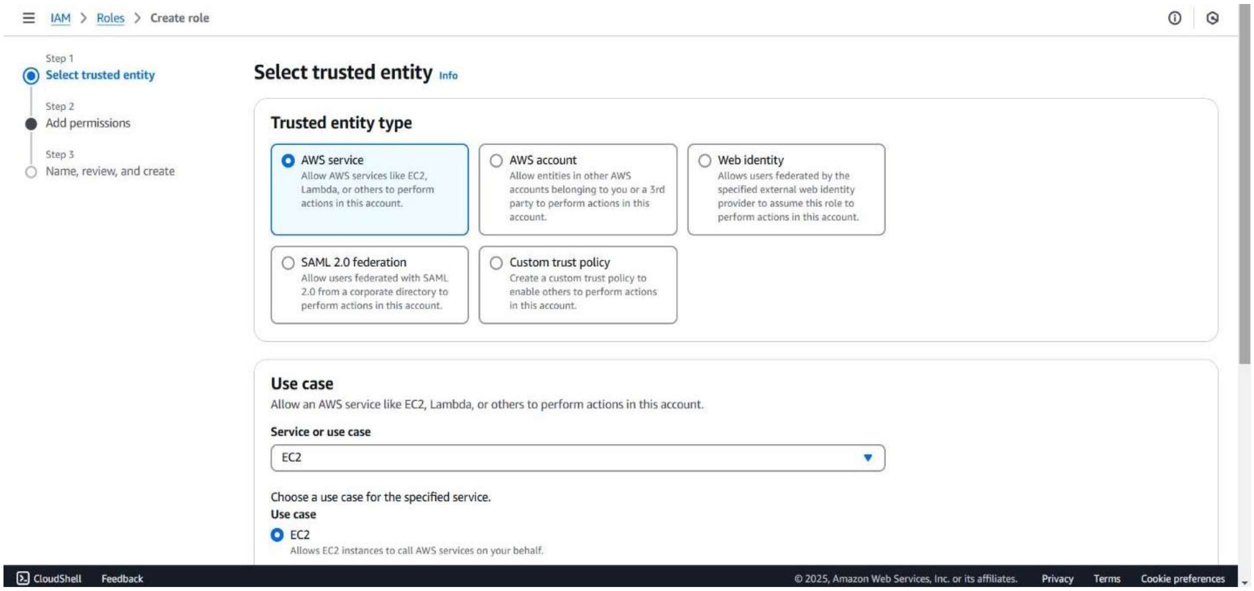
## IAM:

IAM -Identity and Access Management. This in AWS is a security feature that helps control access to resources within AWS environments. It allows you to define users, groups, and roles, granting permissions that determine what actions can be performed on which resources.

## HANDS-ON:

### Step 1: CREATING AN **IAM** ROLE

- ✓ Go to the **AWS IAM Console**.
- ✓ Click **Roles** on the left panel and click **Create role**.
- ✓ Under **Trusted entity type**, choose **AWS Service**. Also, select **EC2** as the trusted service.
- ✓ Click **Next** to add permissions.



IAM > Roles > Create role
Info
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 1
● Select trusted entity

Step 2
● Add permissions

Step 3
○ Name, review, and create

## Select trusted entity

### Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

### Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

**Service or use case**

EC2 ▼

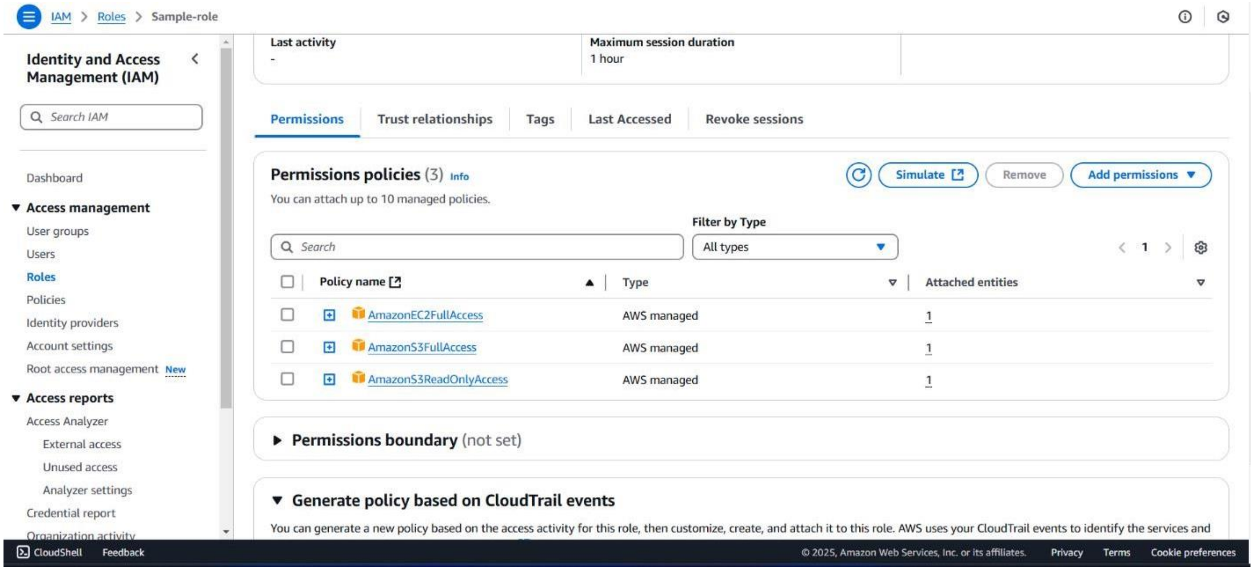
Choose a use case for the specified service.

**Use case**

● EC2
Allows EC2 instances to call AWS services on your behalf.

## Step 2: ATTACH **POLICIES**

- Choose from AWS-managed policies (e.g., AmazonS3ReadOnlyAccess, AmazonEC2FullAccess) or create a **custom policy**.
- Click **Next** and give the role a name (e.g., EC2InstanceRole).
- Click **Create role**.



Last activity: -

Maximum session duration: 1 hour

**Permissions policies** (3) Info

You can attach up to 10 managed policies.

Filter by Type: All types

| □ | Policy name | Type | Attached entities |
|---|---|---|---|
| □ | AmazonEC2FullAccess | AWS managed | 1 |
| □ | AmazonS3FullAccess | AWS managed | 1 |
| □ | AmazonS3ReadOnlyAccess | AWS managed | 1 |

▶ **Permissions boundary** (not set)

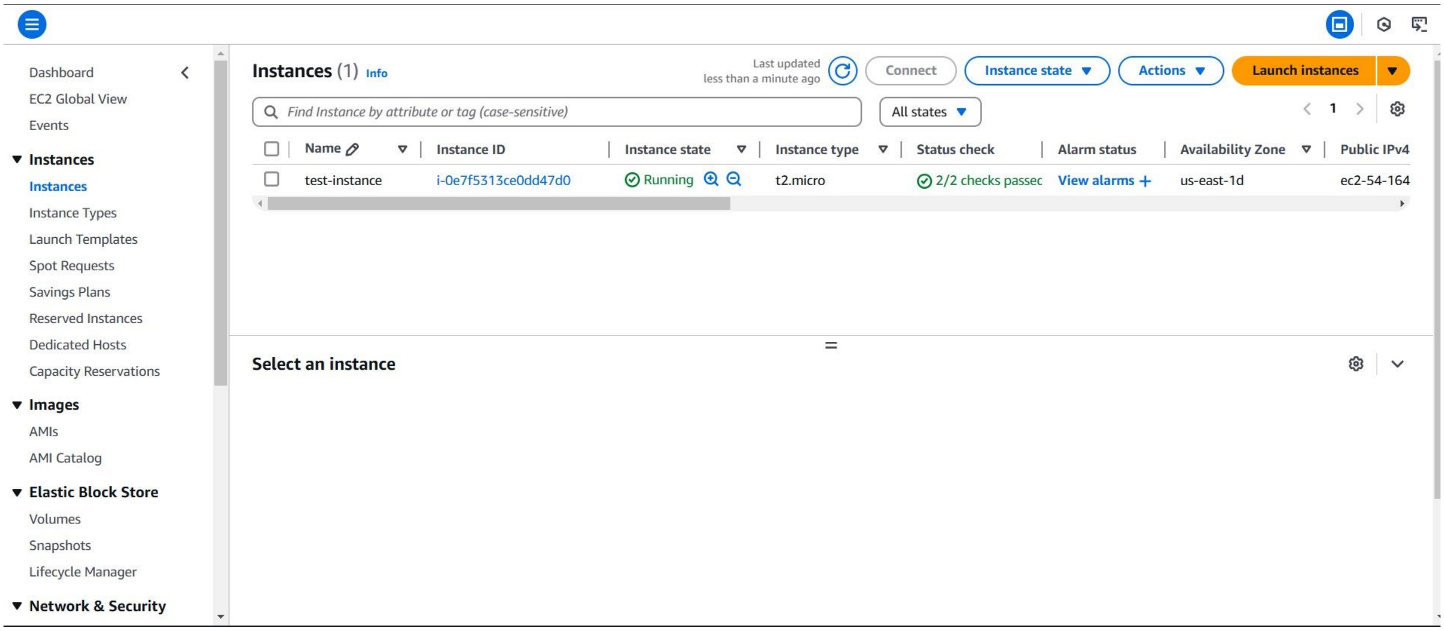
▼ **Generate policy based on CloudTrail events**

You can generate a new policy based on the access activity for this role, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and

© 2025, Amazon Web Services, Inc. or its affiliates.

## Step 3: CREATING AN EC2 INSTANCE

- Create an EC2 instance from the AWS management console by specifying the instance Name, Type and Security group.



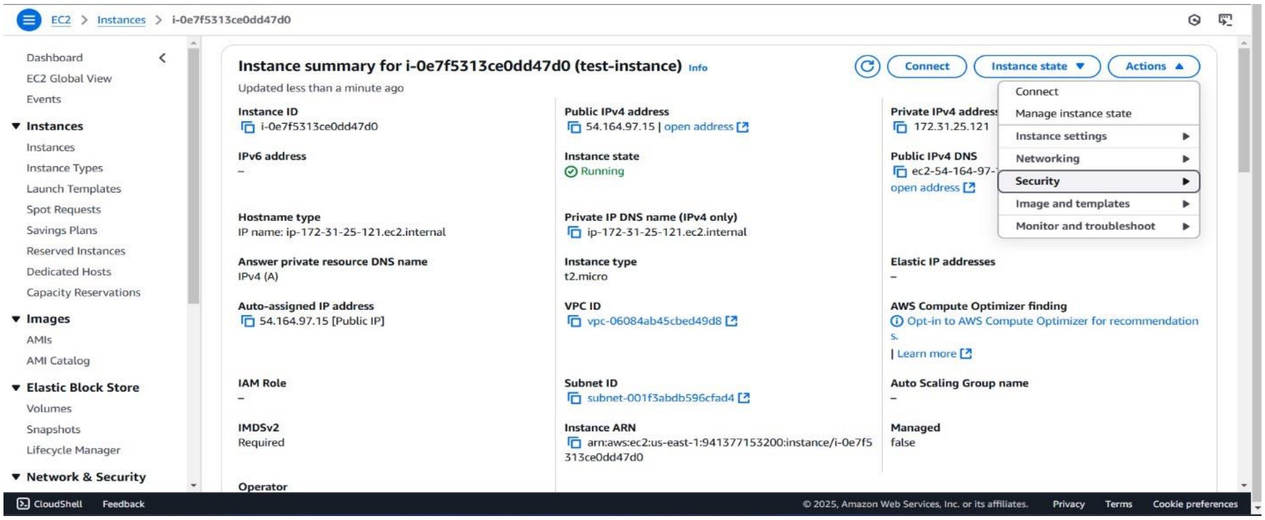
**Instances** (1) Info

Last updated less than a minute ago

| □ | Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 |
|---|---|---|---|---|---|---|---|---|
| □ | test-instance | i-0e7f5313ce0dd47d0 | ✓ Running | t2.micro | ✓ 2/2 checks passec | View alarms + | us-east-1d | ec2-54-164 |

## Step 4: ATTACH IAM ROLE TO THE EC2 INSTANCE

- Select your EC2 instance and click Actions → Security → Modify IAM Role.
- Choose the role you just created and click on update IAM role.



EC2 > Instances > i-0e7f5313ce0dd47d0

**Instance summary for i-0e7f5313ce0dd47d0 (test-instance)** Info

Updated less than a minute ago

**Instance ID**
i-0e7f5313ce0dd47d0

**Public IPv4 address**
54.164.97.15 | open address

**Private IPv4 address**
172.31.25.121

**IPv6 address**
–

**Instance state**
Running

**Public IPv4 DNS**
ec2-54-164-97-
open address

**Hostname type**
IP name: ip-172-31-25-121.ec2.internal

**Private IP DNS name (IPv4 only)**
ip-172-31-25-121.ec2.internal

**Answer private resource DNS name**
IPv4 (A)

**Instance type**
t2.micro

**Elastic IP addresses**
–

**Auto-assigned IP address**
54.164.97.15 [Public IP]

**VPC ID**
vpc-06084ab45cbed49d8

**AWS Compute Optimizer finding**
Opt-in to AWS Compute Optimizer for recommendations.
| Learn more

**IAM Role**
–

**Subnet ID**
subnet-001f3abdb596cfad4

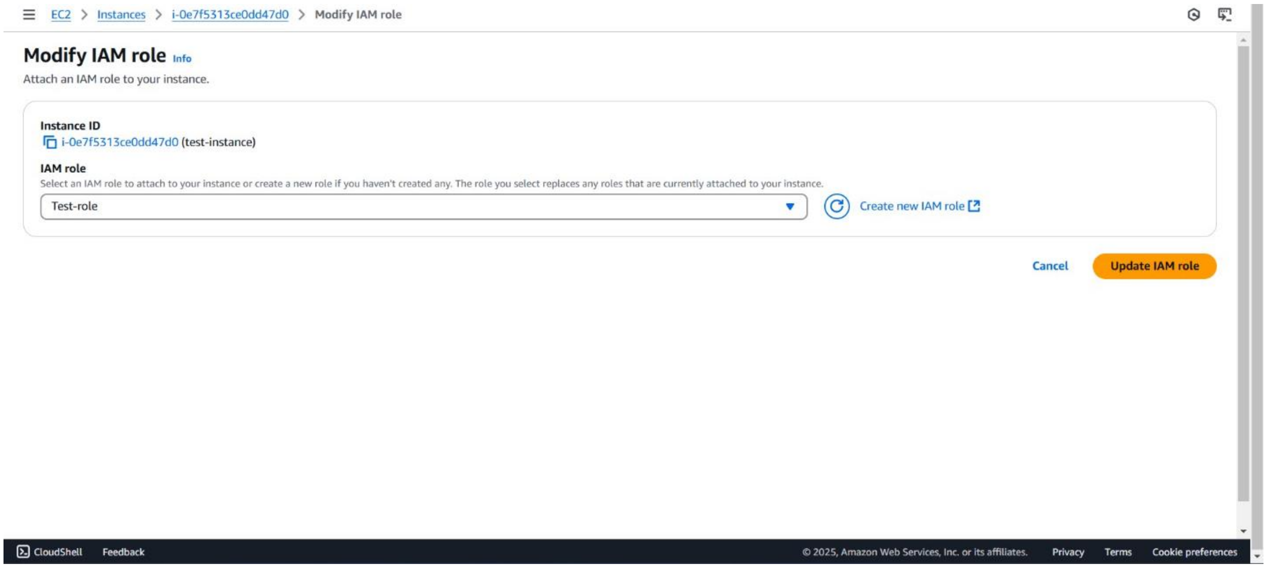
**Auto Scaling Group name**
–

**IMDSv2**
Required

**Instance ARN**
arn:aws:ec2:us-east-1:941377153200:instance/i-0e7f5313ce0dd47d0

**Managed**
false

**Operator**



EC2 > Instances > i-0e7f5313ce0dd47d0 > Modify IAM role

**Modify IAM role** Info

Attach an IAM role to your instance.

**Instance ID**
i-0e7f5313ce0dd47d0 (test-instance)

**IAM role**
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

Test-role

# CONCLUSION:

Thus, in this POC, we have learnt:

1. How to set-up IAM roles and permissions.
2. Assigning role to the virtual machine (EC2) to restrict/allow specific actions.