Roles in IAM Service

IAM Roles: Temporary IDs for Secure Access.

Imagine you have a toolbox with different tools for various tasks. IAM roles are like sets of specific tools (permissions) that you can temporarily give to people or applications who need them. **These roles don't have permanent access** like keys, so they're more secure.

Key Points:

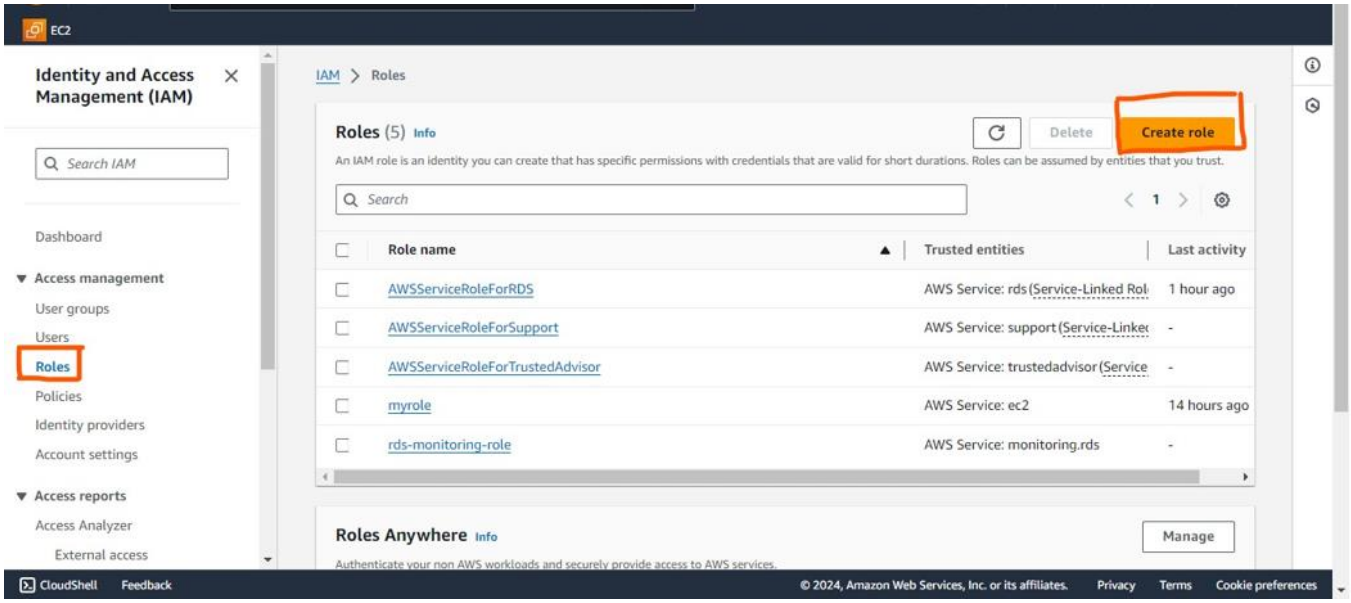
1. Roles are temporary identities, unlike permanent user accounts.
2. They provide secure access with defined permissions.
3. They're ideal for automation and shared access scenarios.

How Roles Work:

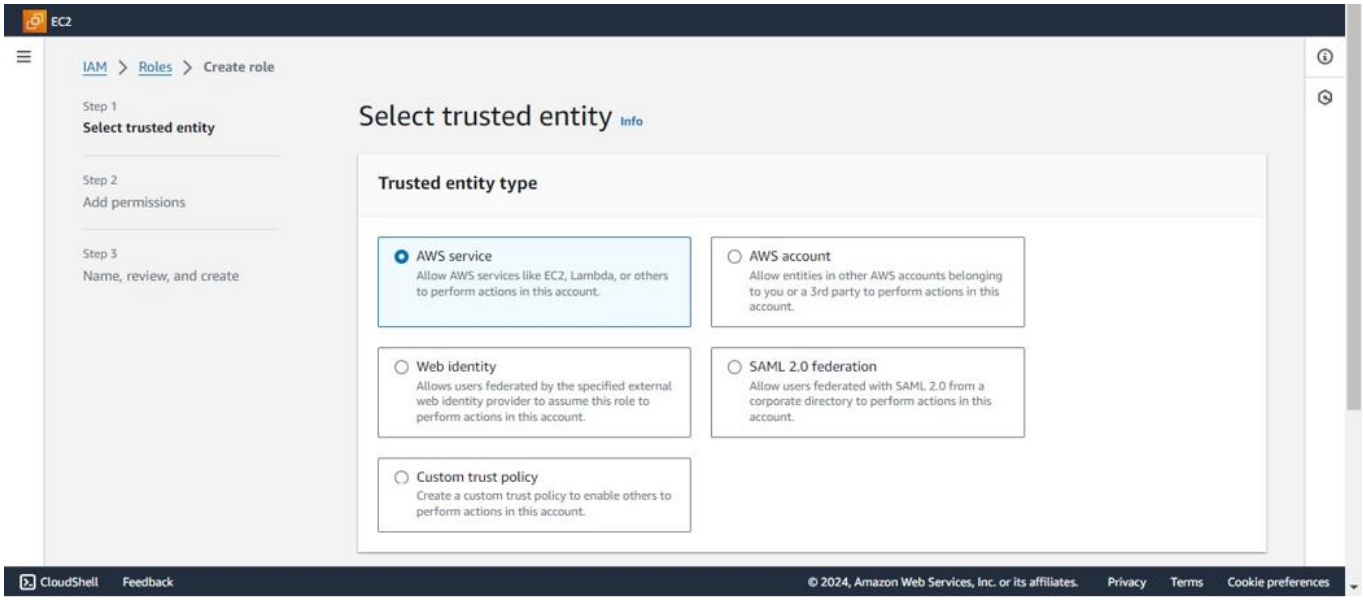
1. Create a Role: You define what actions the role can perform (e.g., starting an EC2 instance, uploading files to S3).
2. Grant Access: You provide temporary credentials (like a passcode) for someone or an application to "assume" the role, granting them the defined permissions.
3. Use the Tools: Whoever assumes the role can use the allowed tools for a limited time, like in a construction project where workers use specific tools for specific tasks.
4. Return the Tools: When they're done, the temporary credentials expire, and the access goes away.

Creating a role :-

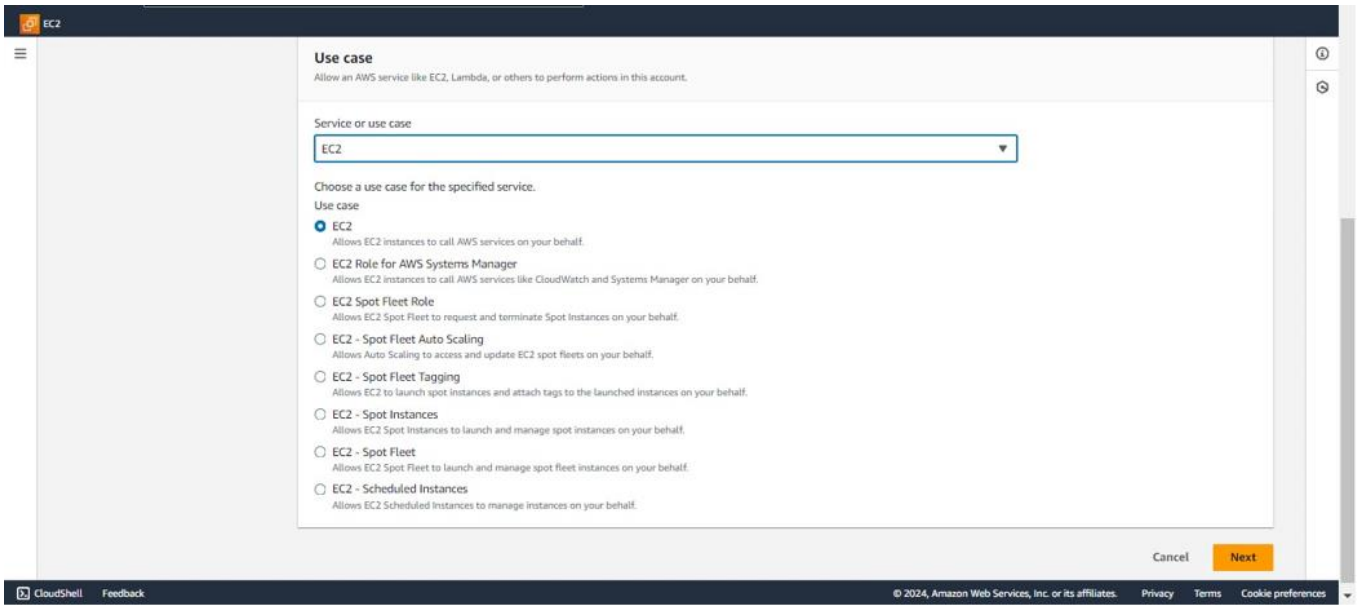
1. Click on **Roles** and **Create role** option



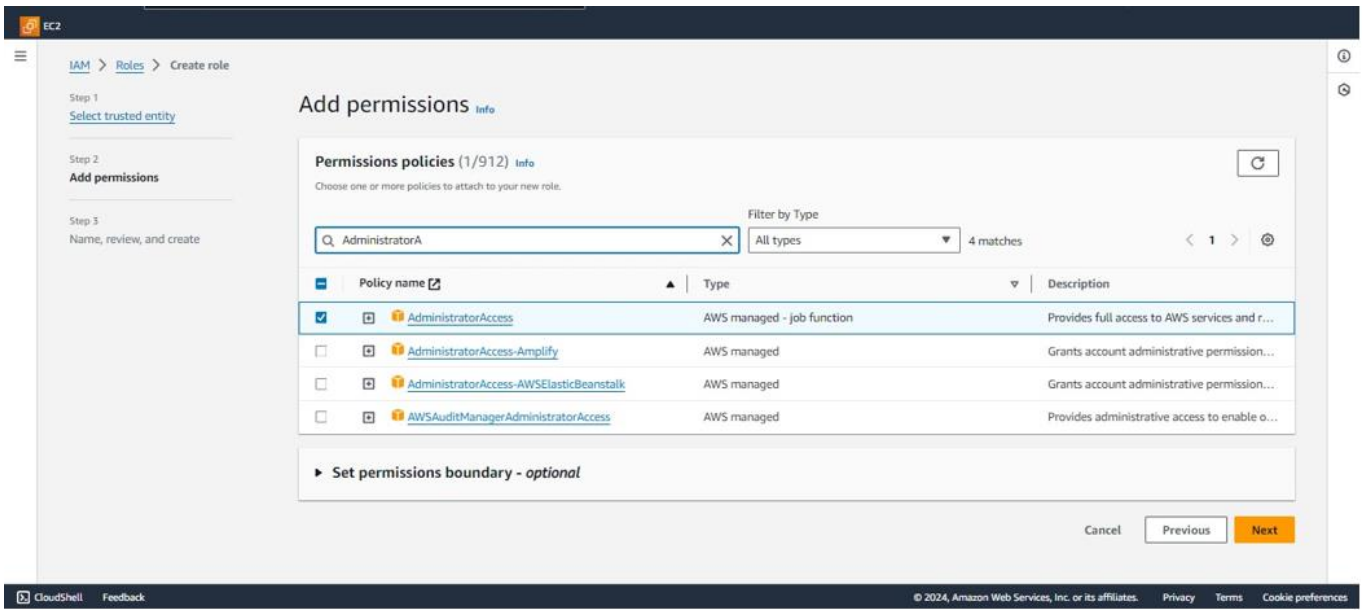
2. Select **AWS service** option



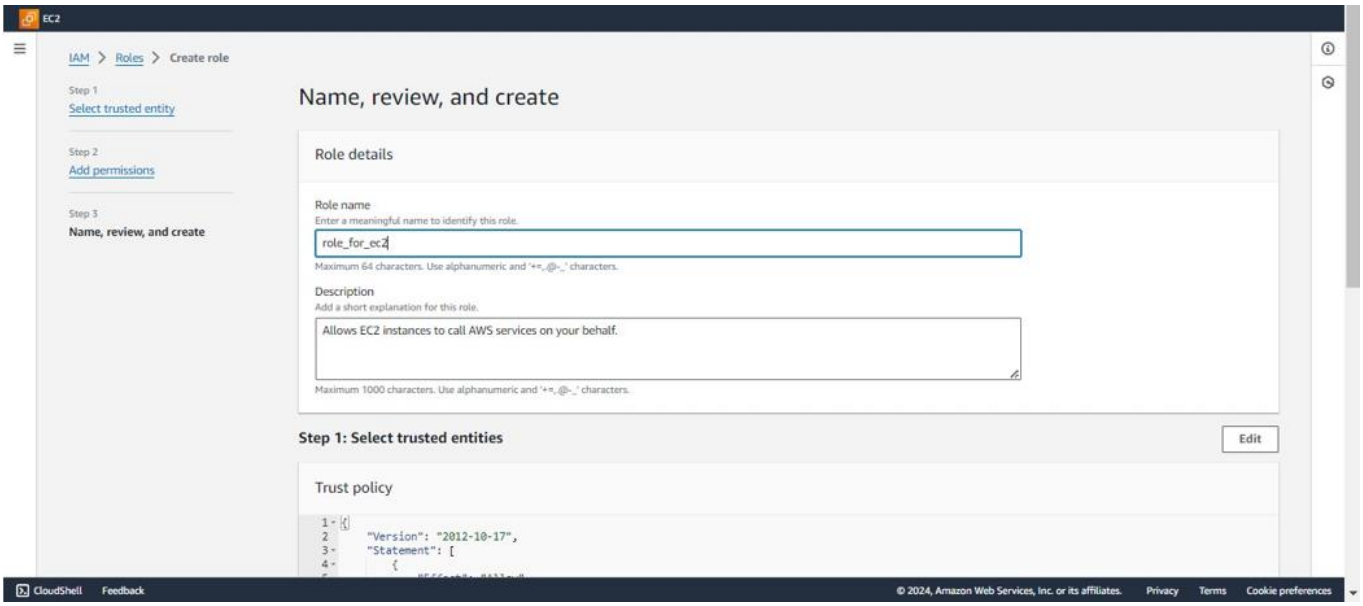
3. Select the service type (in this case EC2 is selected)



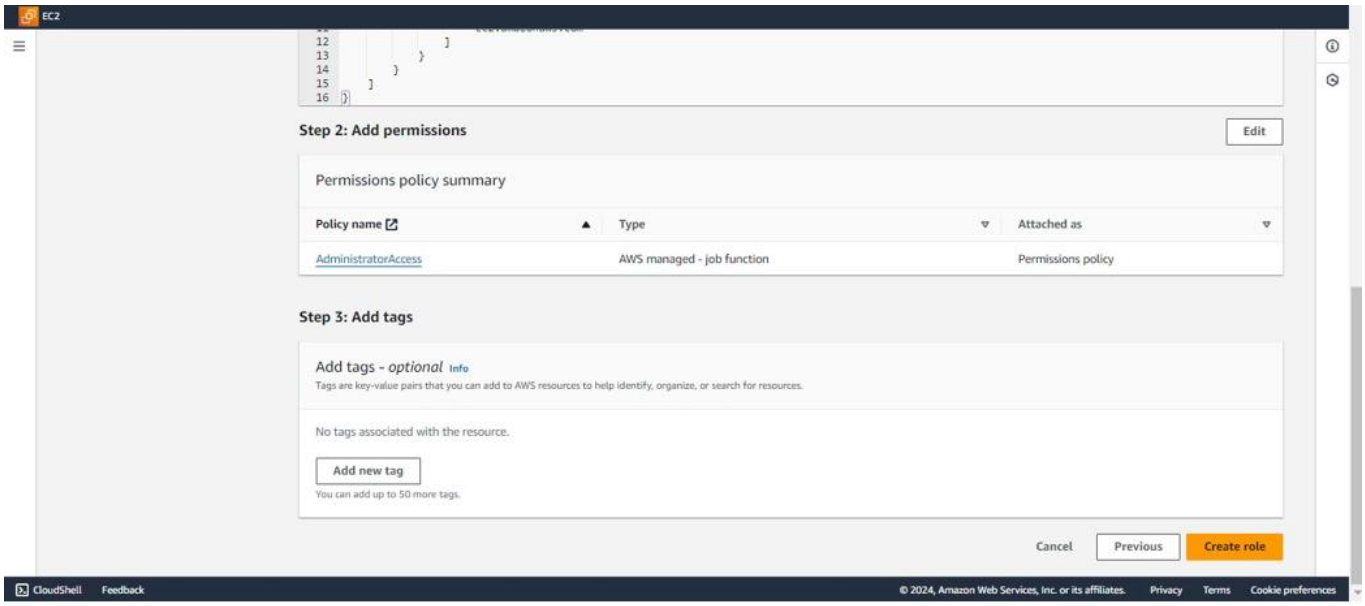
4. Select policy as per you choice (in this case Admin all access is selected)



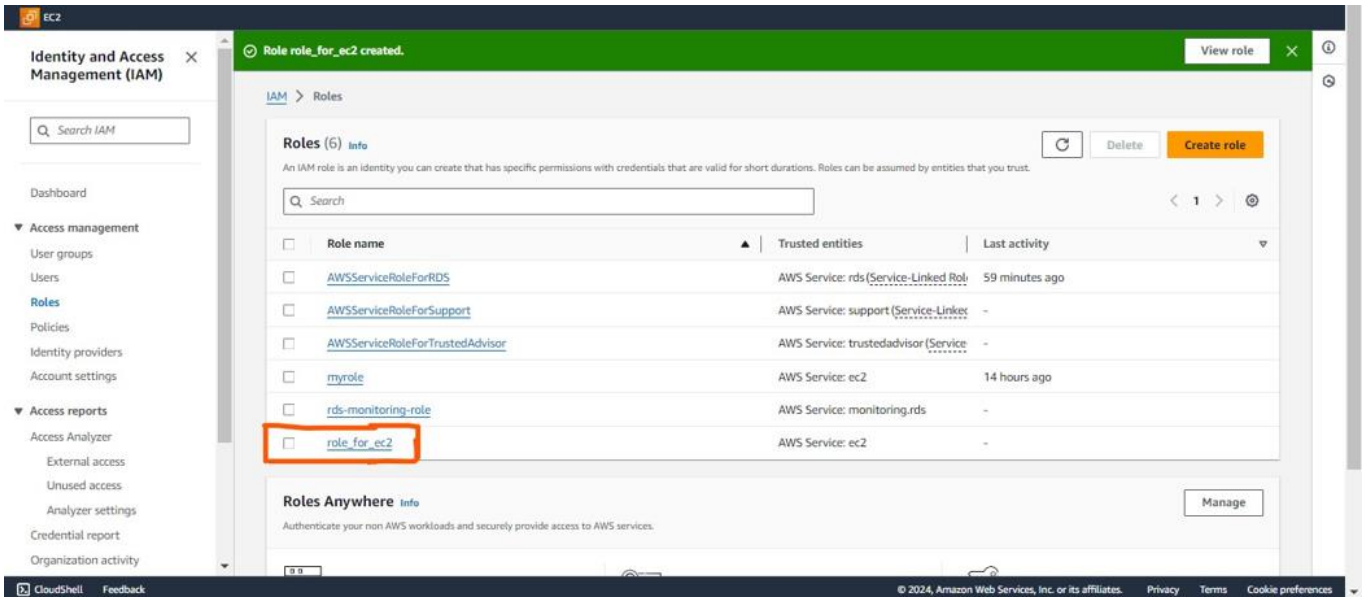
5. Assign any name as per your choice



6. Scroll down and click on create role



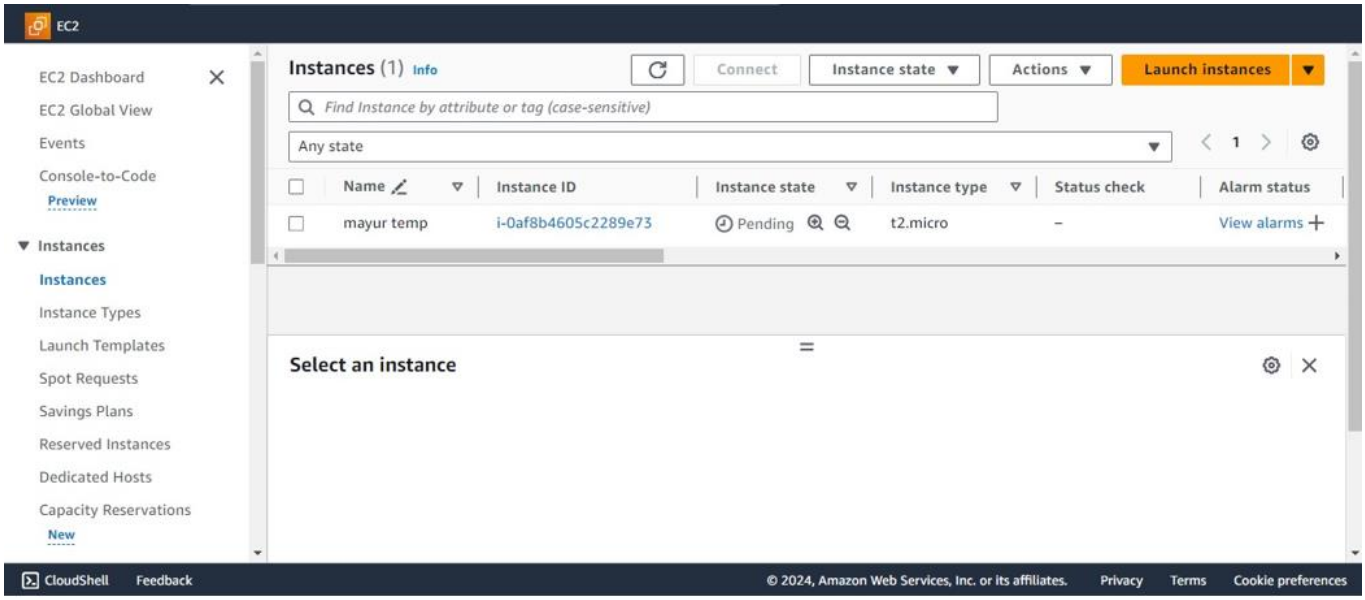
7. Role created successfully



Assigning a role :-

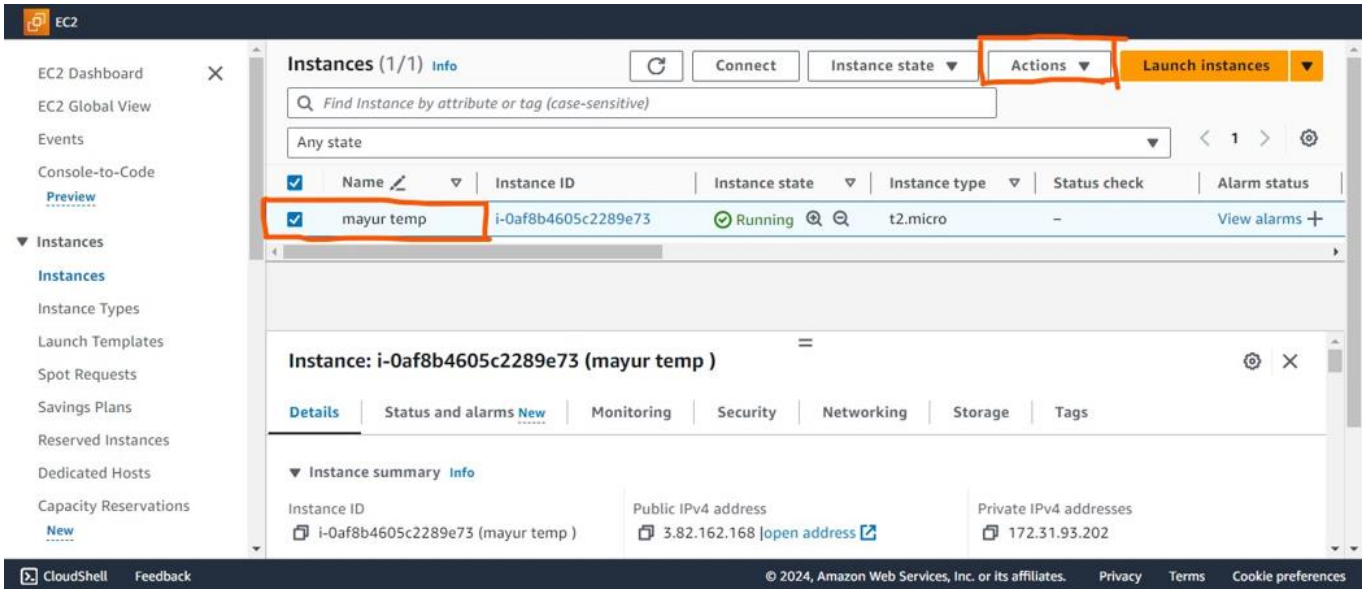
Step1:- Create EC2 Instance

- Search EC2 service in aws search bar
- Click on create instance
- Assign any name as per your choice
- Select any image as per your choice (aws linux is selected)
- Assign a name to key value pair and click on **create new key value pair**
- Download the key value pairs
- Click on launch instance
- Instance Created successfully

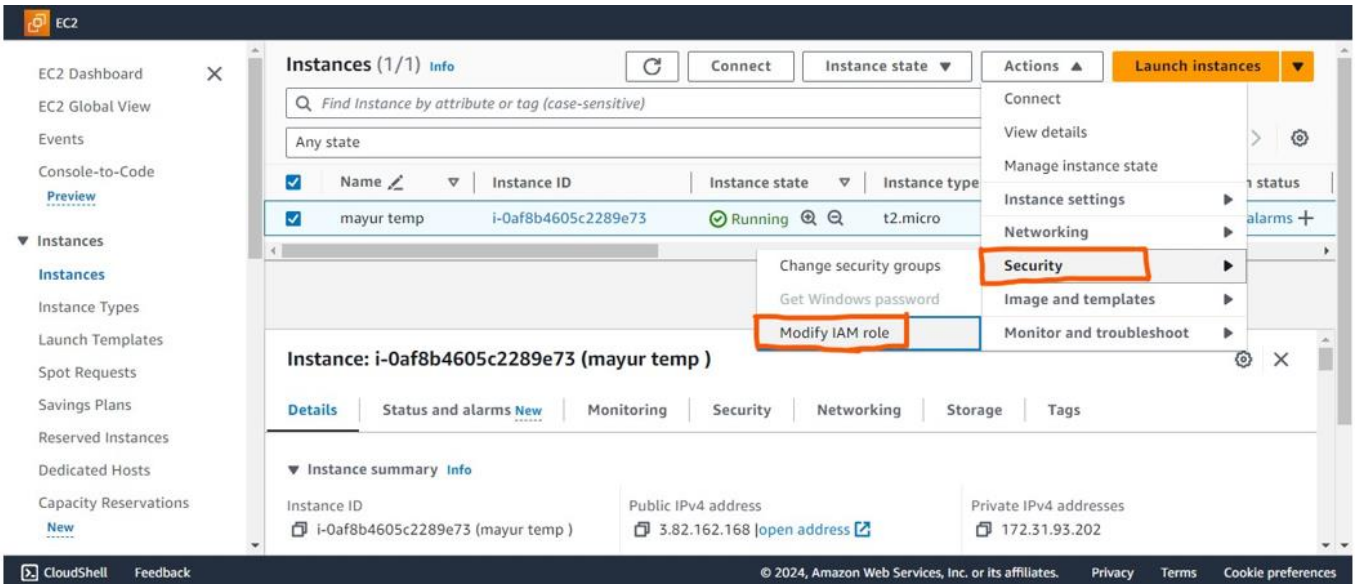


Step 2: Assign role to EC2 instance

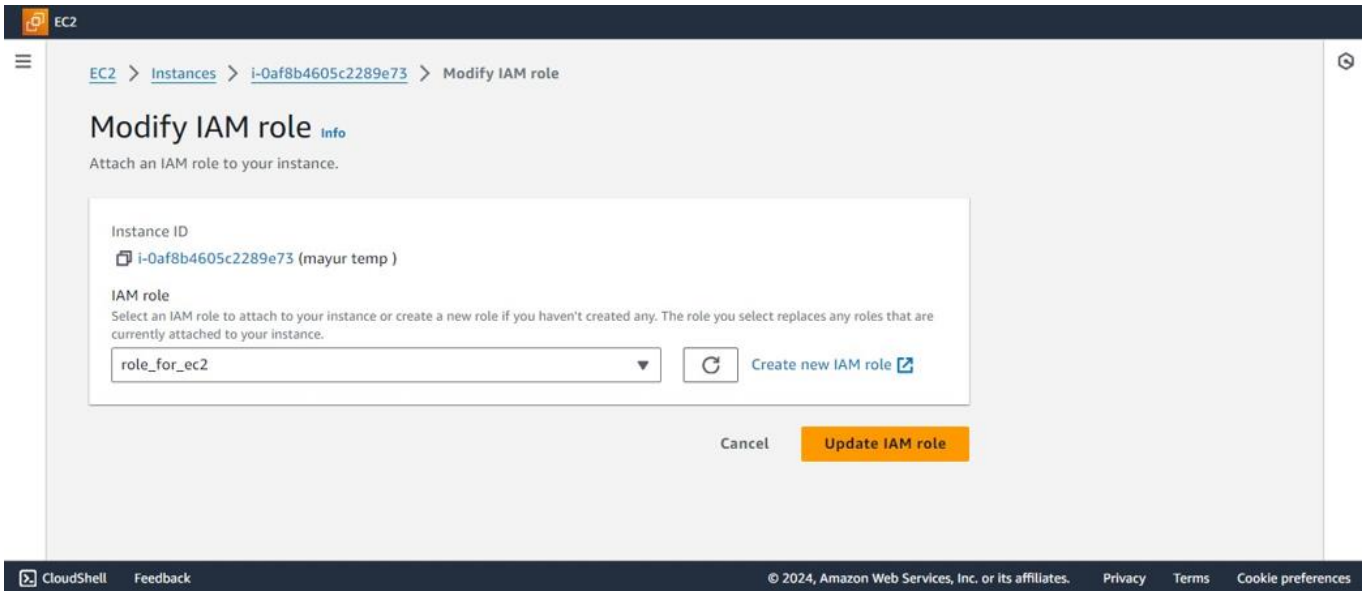
1. Select the created instance and click on **actions**



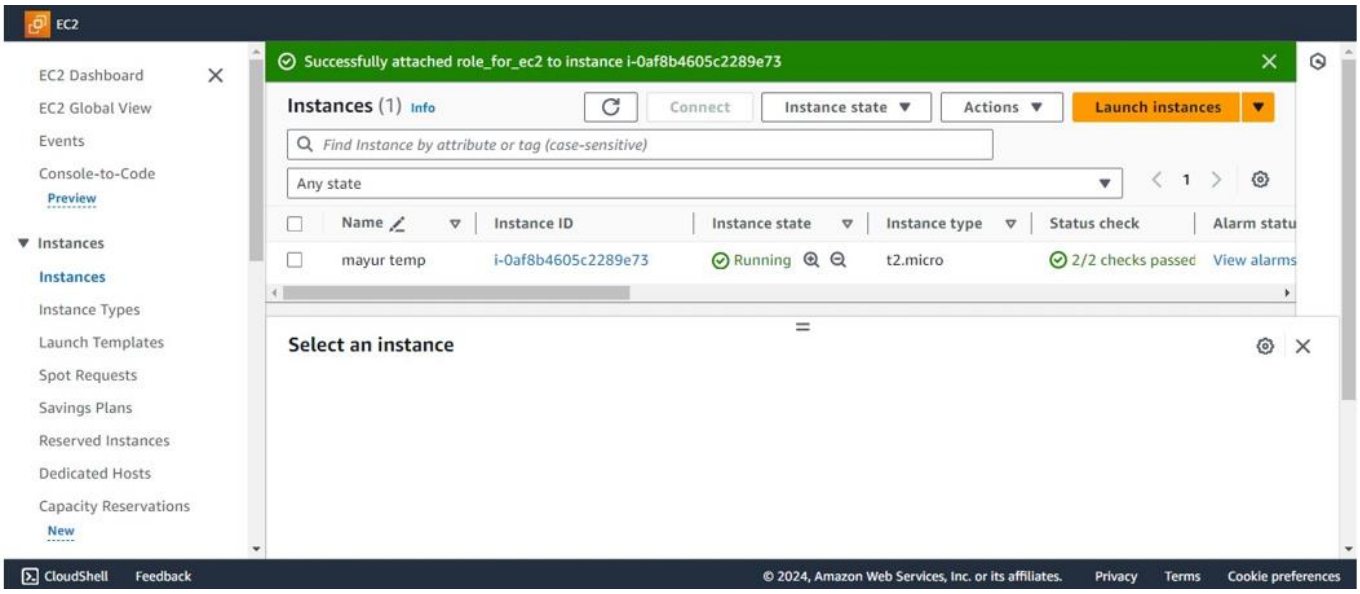
2. Click on **security** and **Modify IAM role**



3. Select a role which you created in previous step and click on **update IAM role**

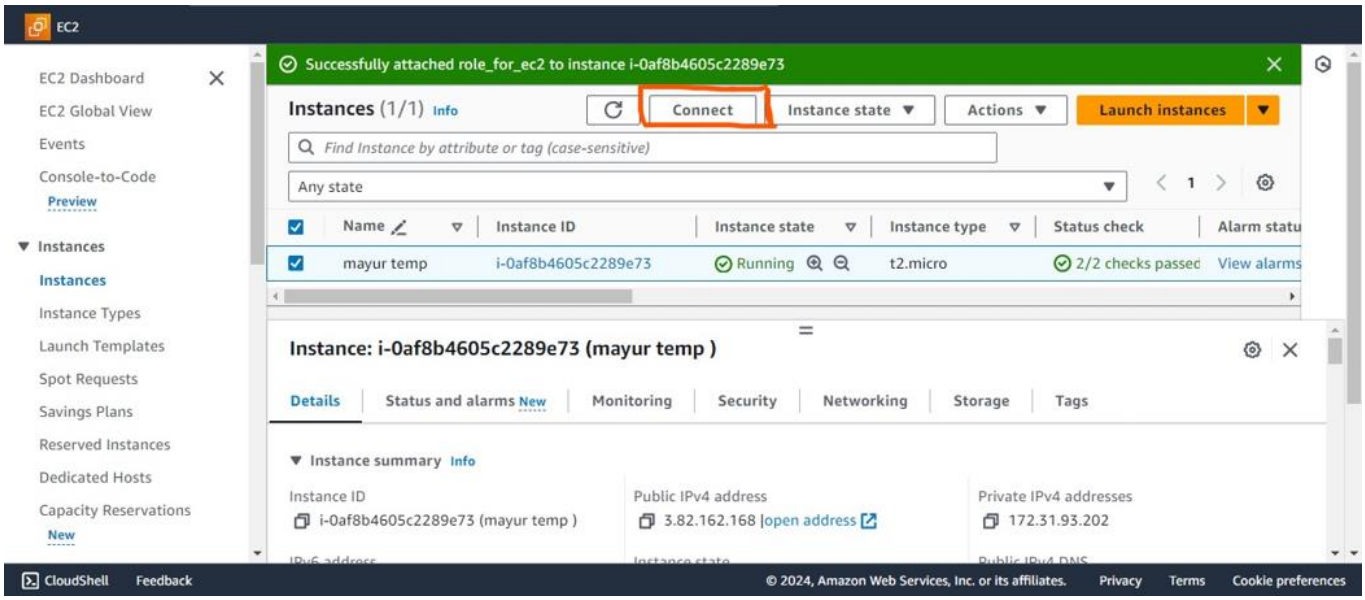


4. Role attached successfully to instance

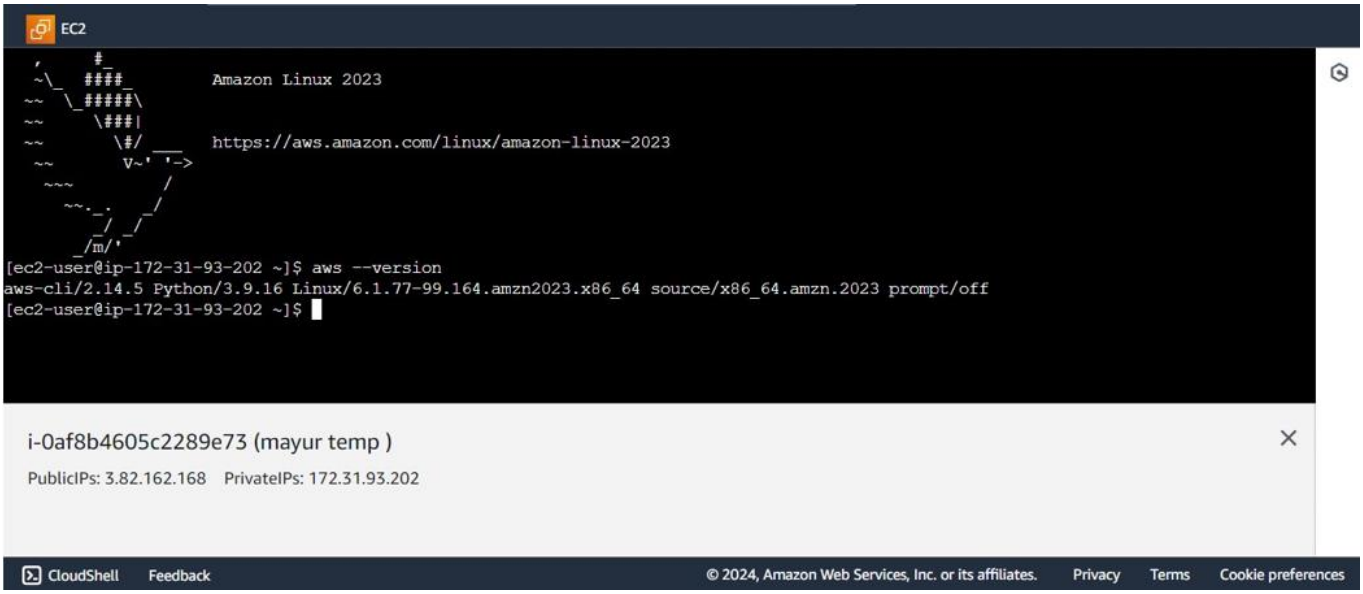


Step 3 :- performing the actions through ec2

1. Select the instance and click on **connect** option



2. Make sure that the aws-cli is installed in ec2 instance using **aws –version** command



3. Successfully accessing the aws iam users lists