

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:

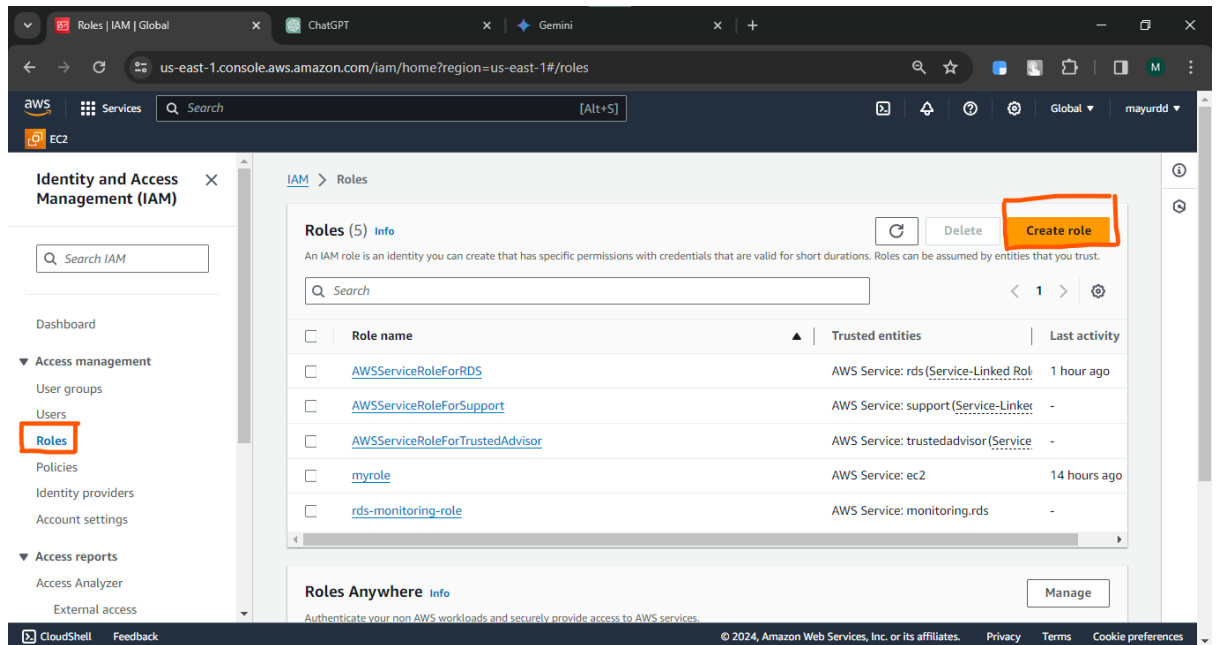
1. Roles are temporary identities, unlike permanent user accounts.
2. They provide secure access with defined permissions.
3. They're ideal for automation and shared access scenarios.

How Roles Work:

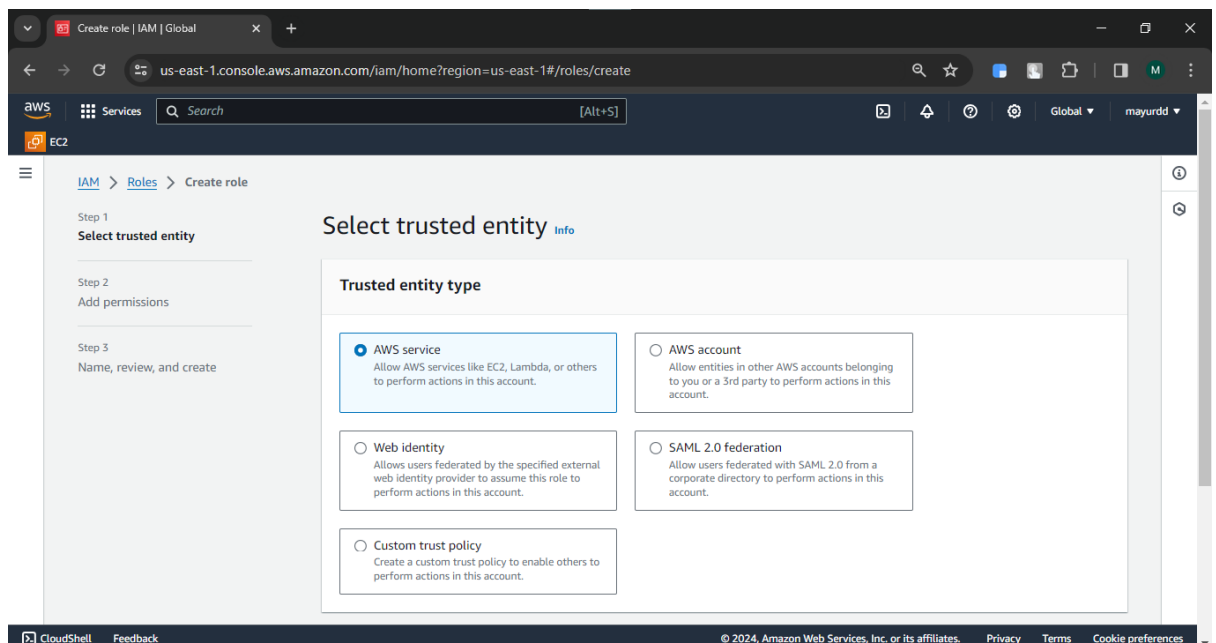
1. Create a Role: You define what actions the role can perform (e.g., starting an EC2 instance, uploading files to S3).
2. Grant Access: You provide temporary credentials (like a passcode) for someone or an application to "assume" the role, granting them the defined permissions.
3. Use the Tools: Whoever 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 :-

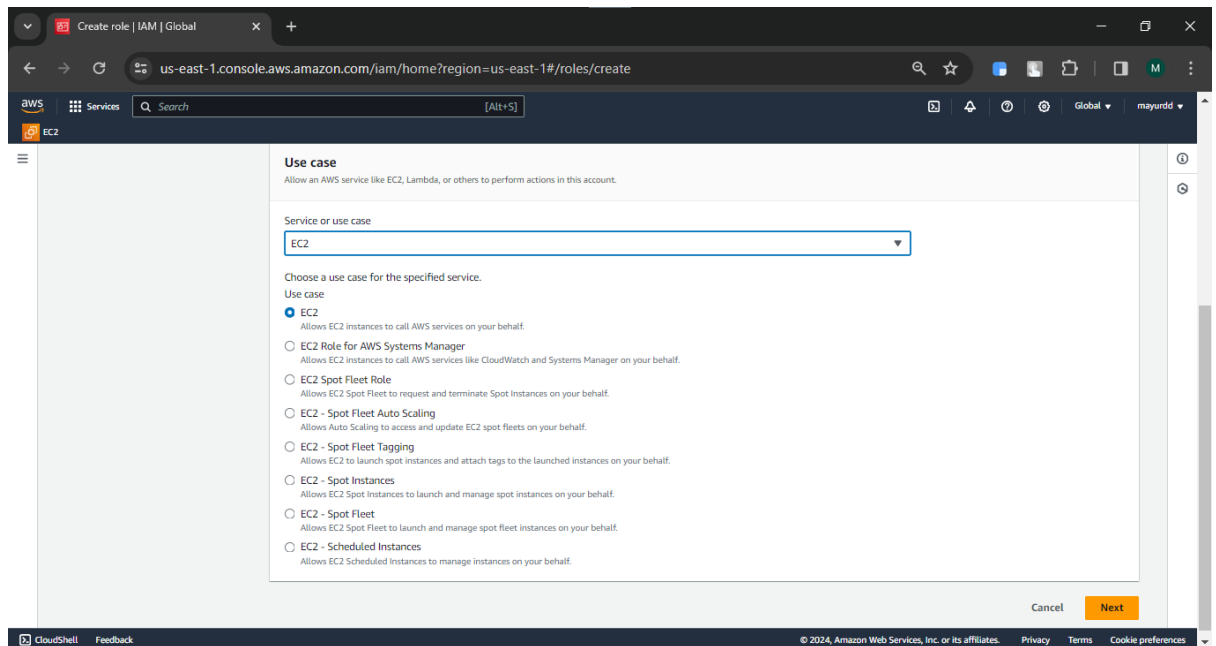
1. Click on **Roles** and **Create role** option



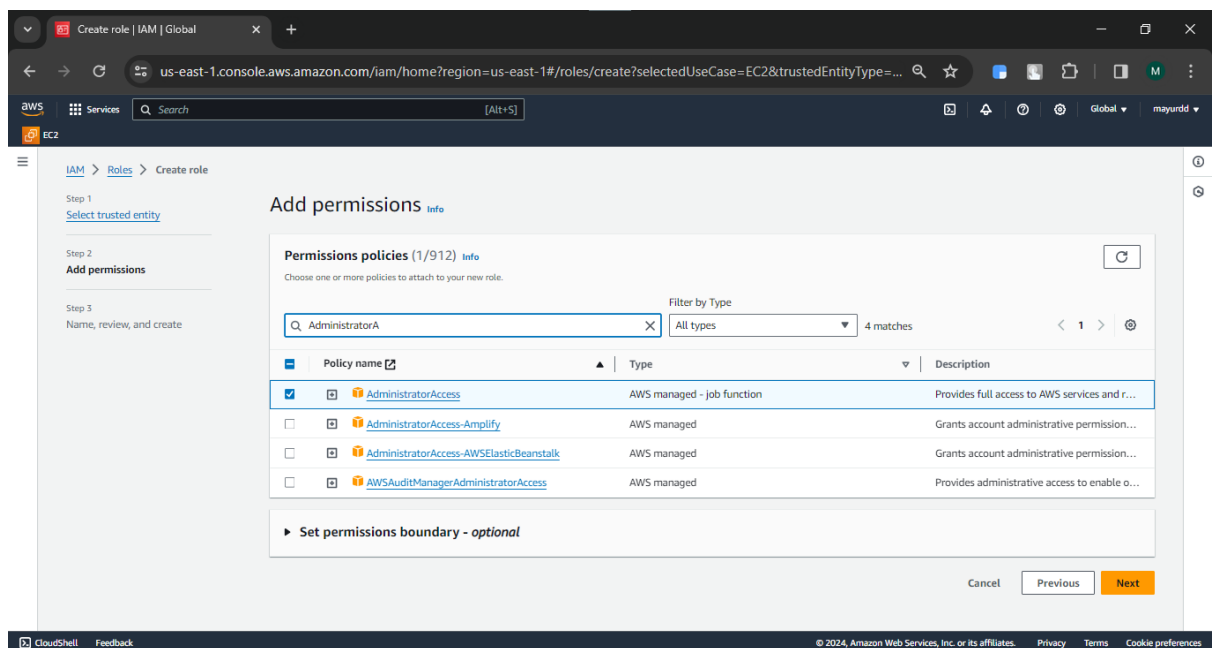
2. Select **AWS service** option



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

The screenshot shows the AWS IAM console 'Create role' page. The browser address bar indicates the URL: `us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create?selectedUseCase=EC2&trustedEntityType=...`. The page title is 'Create role | IAM | Global'. The left sidebar shows the navigation menu with 'IAM > Roles > Create role' selected. The main content area is titled 'Name, review, and create'. It contains a 'Role details' section with a 'Role name' field containing 'role_for_ec2' and a 'Description' field containing 'Allows EC2 instances to call AWS services on your behalf.' Below this is a 'Step 1: Select trusted entities' section with a 'Trust policy' field containing a JSON policy. The bottom of the page shows the 'CloudShell' and 'Feedback' buttons, and the copyright notice '© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

Step 1: Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
role_for_ec2
Maximum 64 characters. Use alphanumeric and '+', '@', '-' characters.

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.

Step 1: Select trusted entities

Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "Service": "ec2.amazonaws.com"  
8       },  
9       "Action": "iam:passrole"  
10    }  
11  ]  
12 }  
13  
14  
15  
16 }
```

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

6. Scroll down and click on create role

The screenshot shows the AWS IAM console 'Create role' page, Step 2: Add permissions. The browser address bar indicates the URL: `us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create?selectedUseCase=EC2&trustedEntityType=...`. The page title is 'Create role | IAM | Global'. The left sidebar shows the navigation menu with 'IAM > Roles > Create role' selected. The main content area is titled 'Step 2: Add permissions'. It contains a 'Permissions policy summary' table with one row: 'AdministratorAccess' (AWS managed - job function) attached as 'Permissions policy'. Below this is a 'Step 3: Add tags' section with an 'Add tags - optional' link and a message 'No tags associated with the resource.' and an 'Add new tag' button. The bottom of the page shows the 'Cancel', 'Previous', and 'Create role' buttons. The footer shows the 'CloudShell' and 'Feedback' buttons, and the copyright notice '© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AdministratorAccess	AWS managed - job function	Permissions policy

Step 3: Add tags

Add tags - optional [Info](#)
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

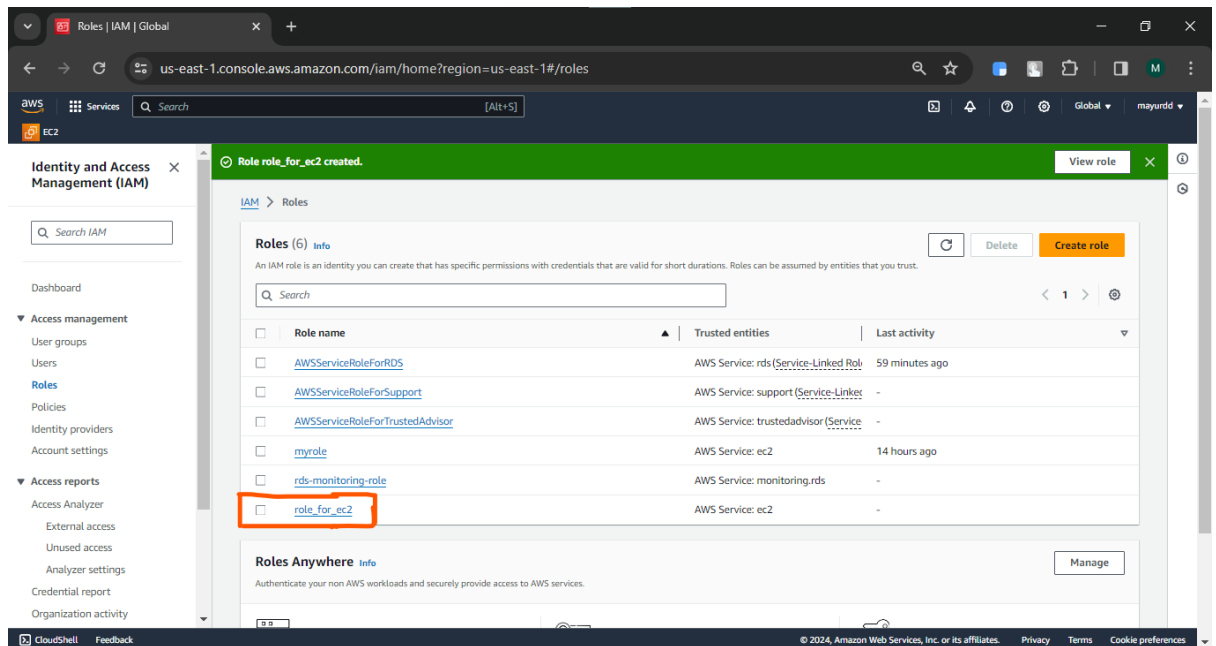
No tags associated with the resource.

Add new tag
You can add up to 50 more tags.

Cancel Previous Create role

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

7. Role created successfully



The screenshot shows the AWS IAM console interface. A green banner at the top states "Role role_for_ec2 created." The left sidebar contains the "Identity and Access Management (IAM)" menu with options like Dashboard, Access management, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access Analyzer, External access, Unused access, Analyzer settings, Credential report, and Organization activity. The main content area displays a list of roles under the heading "Roles (6)". The roles listed are:

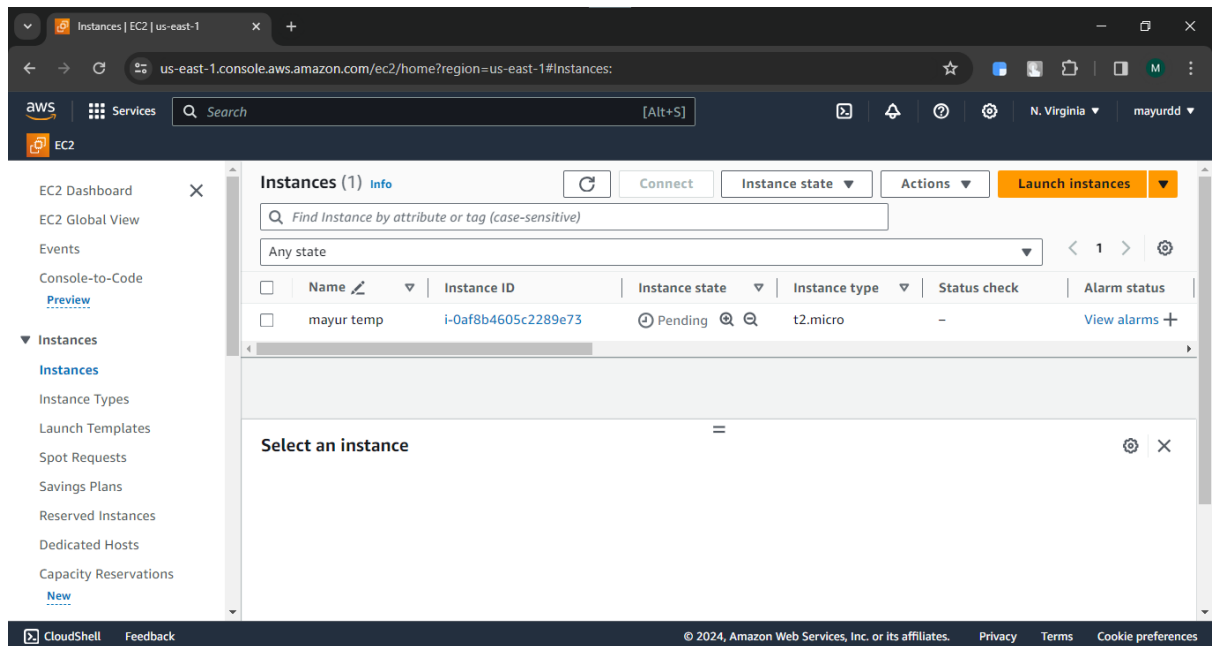
Role name	Trusted entities	Last activity
AWSServiceRoleForRDS	AWS Service: rds (Service-Linked Rol	59 minutes ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linker	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
myrole	AWS Service: ec2	14 hours ago
rds-monitoring-role	AWS Service: monitoring.rds	-
role_for_ec2	AWS Service: ec2	-

The role "role_for_ec2" is highlighted with a red box. Below the list, there is a section titled "Roles Anywhere" with a description and a "Manage" button. The footer of the console shows "© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

Assigning a role :-

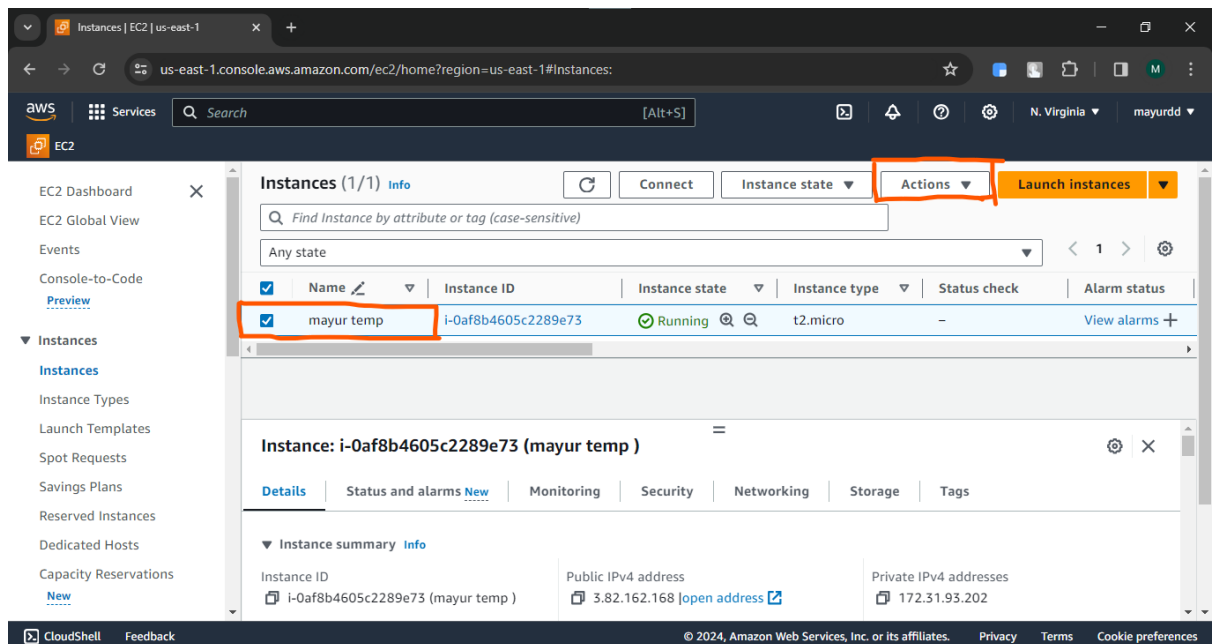
Step1:- Create EC2 Instance

- 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

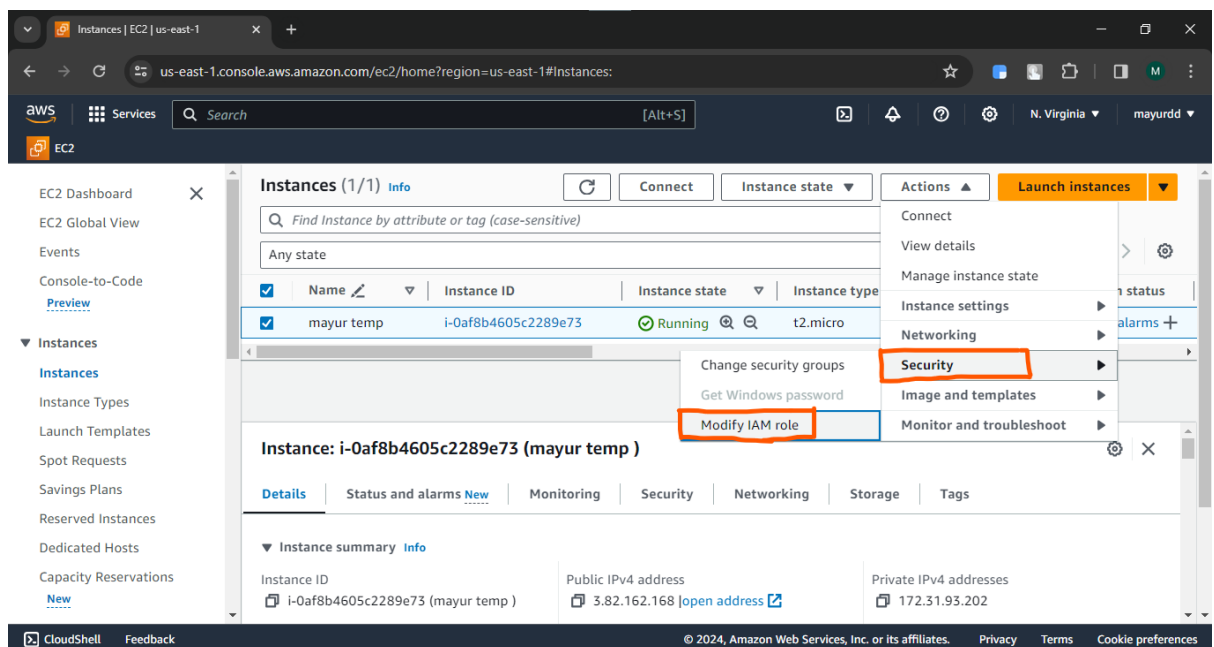


Step 2: Assign role to EC2 instance

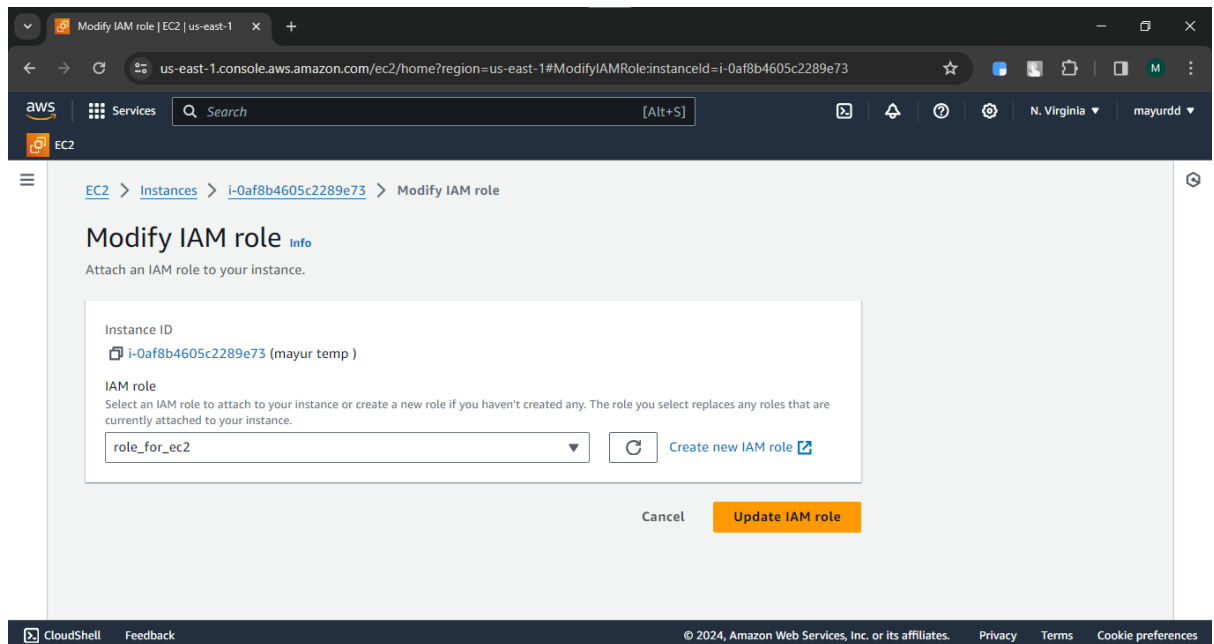
1. Select the created instance and click on **actions**



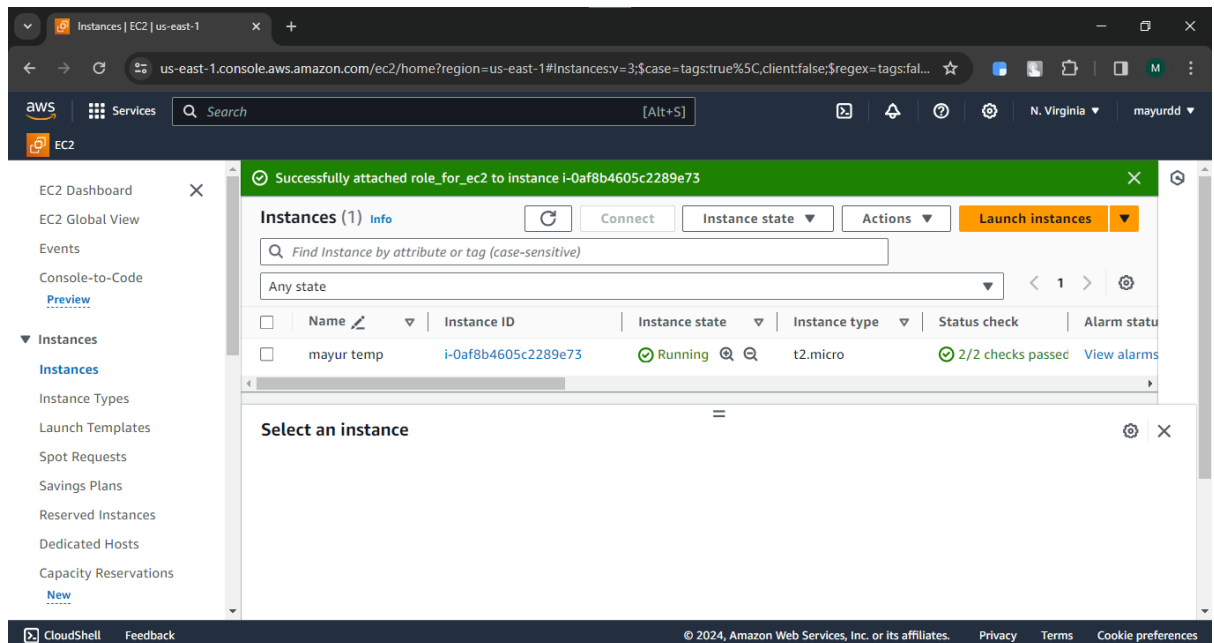
2. Click on **security** and **Modify IAM role**



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

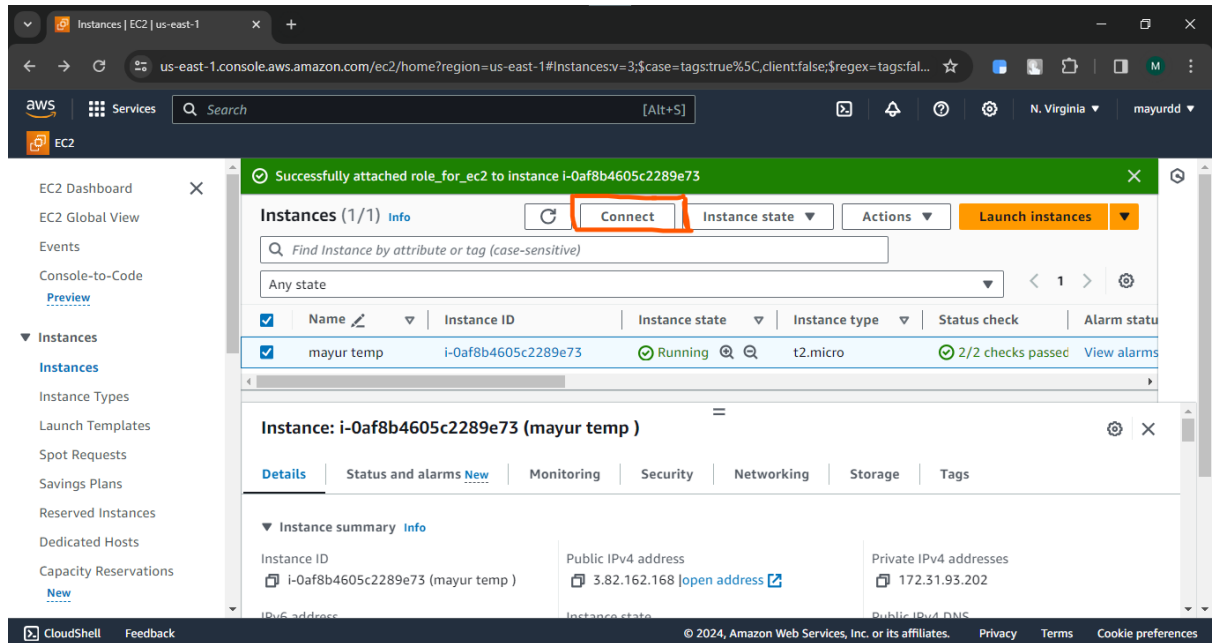


4. Role attached successfully to instance

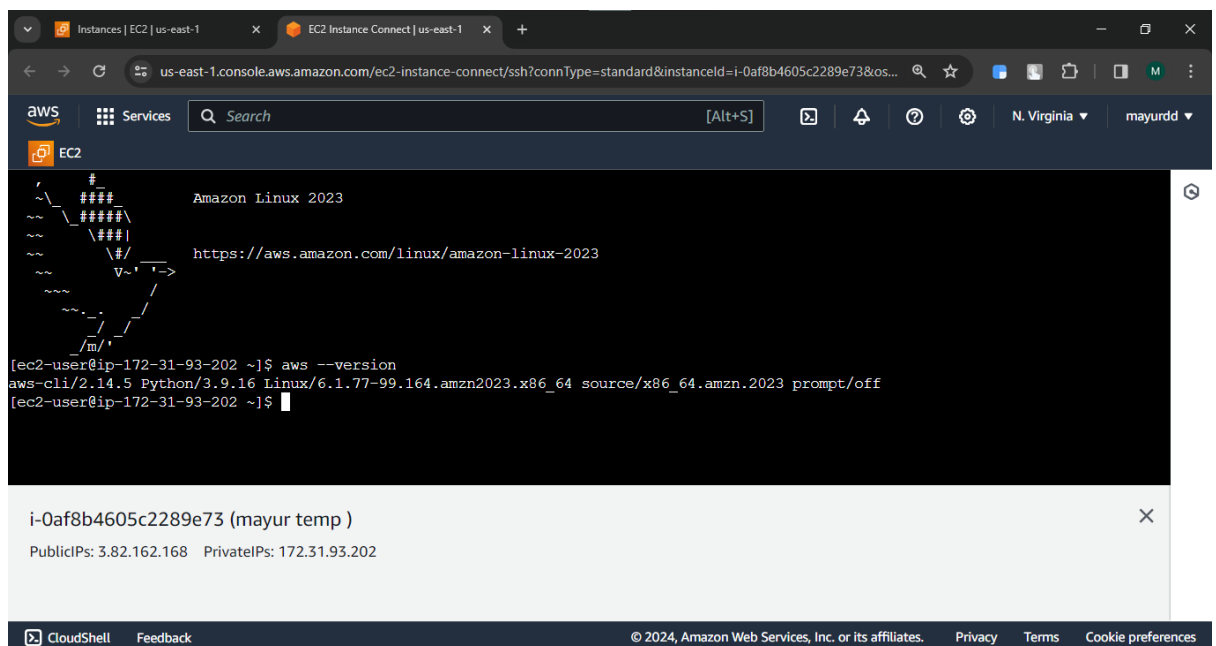


Step 3 :- performing the actions through ec2

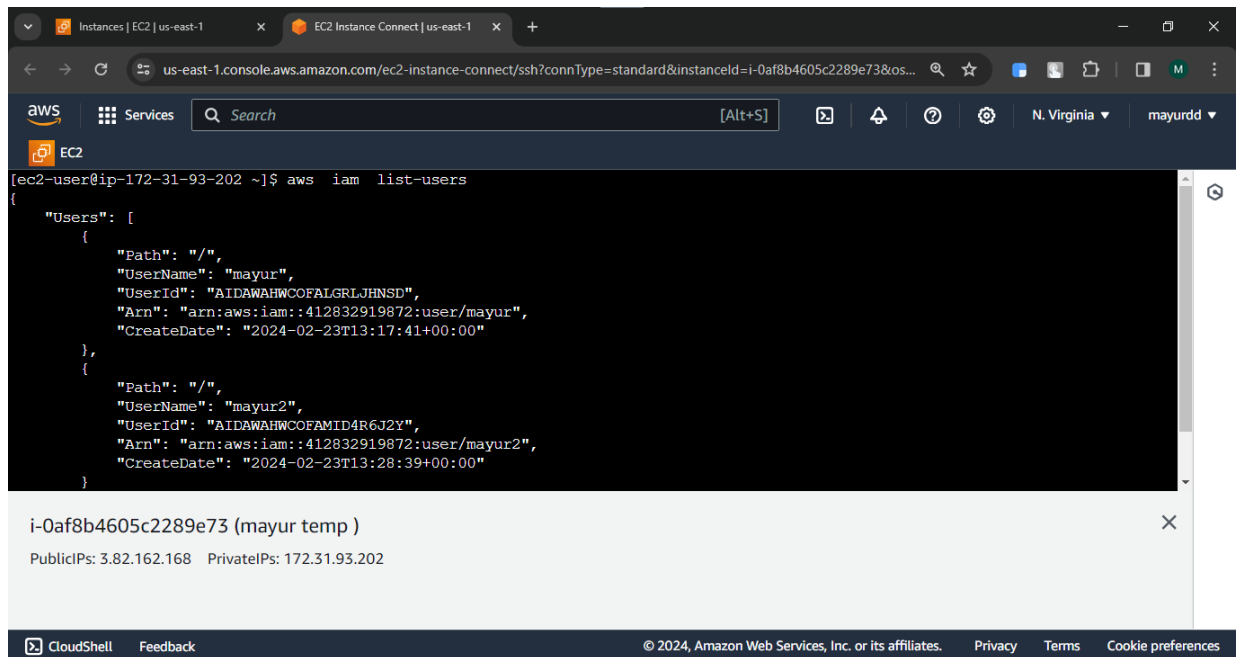
1. Select the instance and click on **connect** option



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



3. Successfully accessing the aws iam users lists



The screenshot shows a web browser window with the AWS console open. The browser tabs include 'Instances | EC2 | us-east-1' and 'EC2 Instance Connect | us-east-1'. The address bar shows the URL 'us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0af8b4605c2289e73&os...'. The AWS navigation bar shows the 'aws' logo, 'Services' menu, a search bar, and the region 'N. Virginia' with the user 'mayurdd'. The main content area is titled 'EC2' and shows a terminal session. The terminal prompt is '[ec2-user@ip-172-31-93-202 ~]\$' and the command entered is 'aws iam list-users'. The output is a JSON object with two users: 'mayur' and 'mayur2'. Below the terminal, a box displays the instance ID 'i-0af8b4605c2289e73 (mayur temp)' and its public and private IP addresses. The footer of the console shows 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc. or its affiliates.

```
[ec2-user@ip-172-31-93-202 ~]$ aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "mayur",
      "UserId": "AIDAWAHWC0FALGRLJHNSD",
      "Arn": "arn:aws:iam::412832919872:user/mayur",
      "CreateDate": "2024-02-23T13:17:41+00:00"
    },
    {
      "Path": "/",
      "UserName": "mayur2",
      "UserId": "AIDAWAHWC0FAMID4R6J2Y",
      "Arn": "arn:aws:iam::412832919872:user/mayur2",
      "CreateDate": "2024-02-23T13:28:39+00:00"
    }
  ]
}
```

i-0af8b4605c2289e73 (mayur temp)

PublicIPs: 3.82.162.168 PrivateIPs: 172.31.93.202

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences