# Placement Empowerment Program

***Cloud Computing and DevOps Centre***

Set Up IAM Roles and Permissions : Create an IAM role on your cloud platform. Assign the role to your VM to restrict/allow specific actions.

Name: Harivasan S

Department: ADS



# Introduction:

This Proof of Concept (PoC) showcases the implementation of IAM roles and permissions in AWS. It aims to highlight secure resource management by using roles instead of embedding credentials. The PoC involves creating an IAM role, attaching it to an EC2 instance, and validating the instance's access to AWS services like Amazon S3.

# Overview:

The process is divided into several key steps:

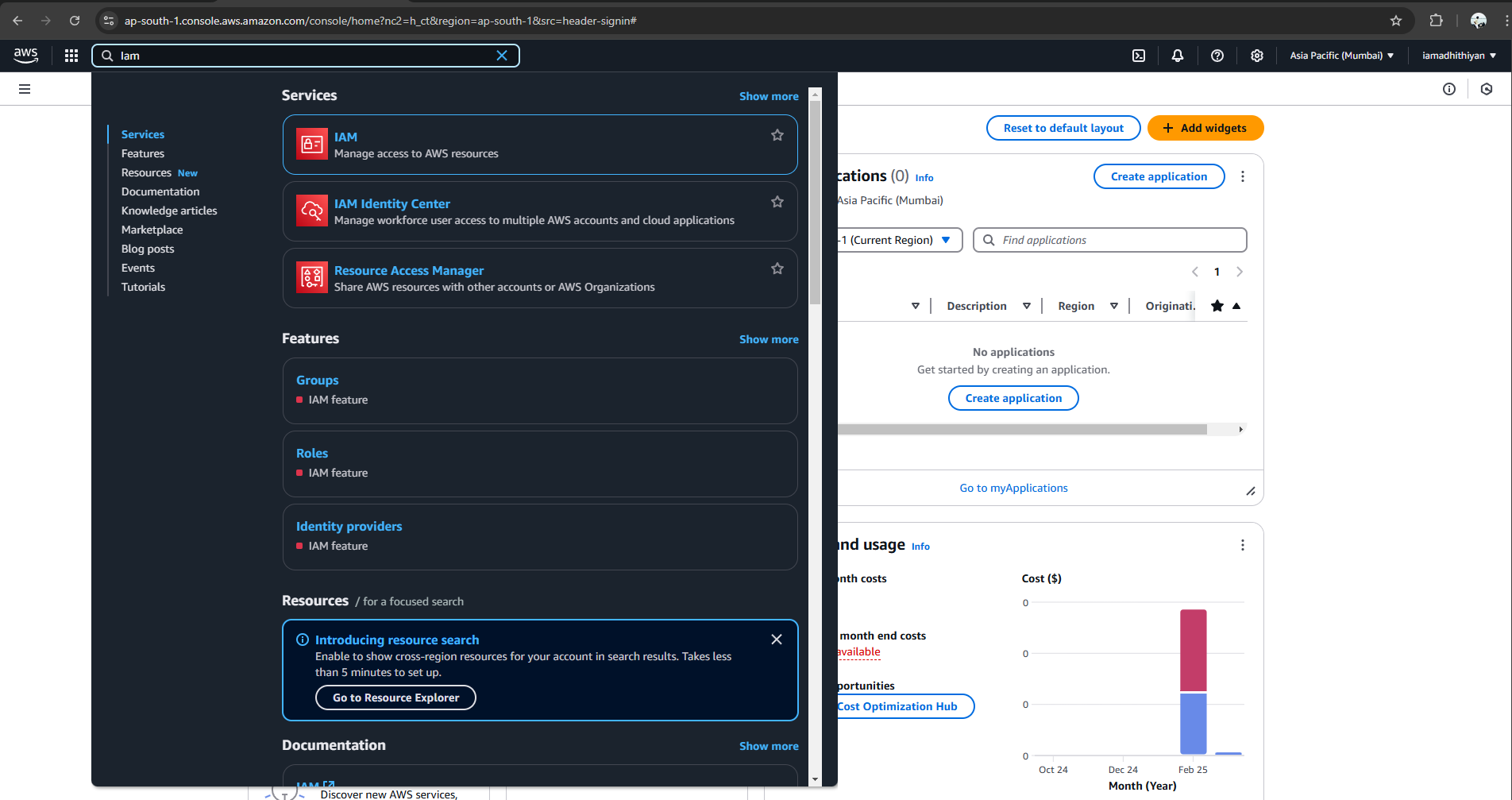
1. **Create an IAM Role**: Set up an IAM role in AWS and apply policies that grant access to specific AWS services.
2. **Launch an EC2 Instance**: Deploy a virtual machine (VM) in AWS and configure it to test the assigned IAM role.
3. **Attach the IAM Role to the EC2 Instance**: Link the IAM role to the EC2 instance, allowing it to access AWS services without requiring access keys.
4. **Validate Access**: Verify the EC2 instance’s permissions by interacting with AWS services such as Amazon S3.

**Step-by-Step Overview :**

Step 1:

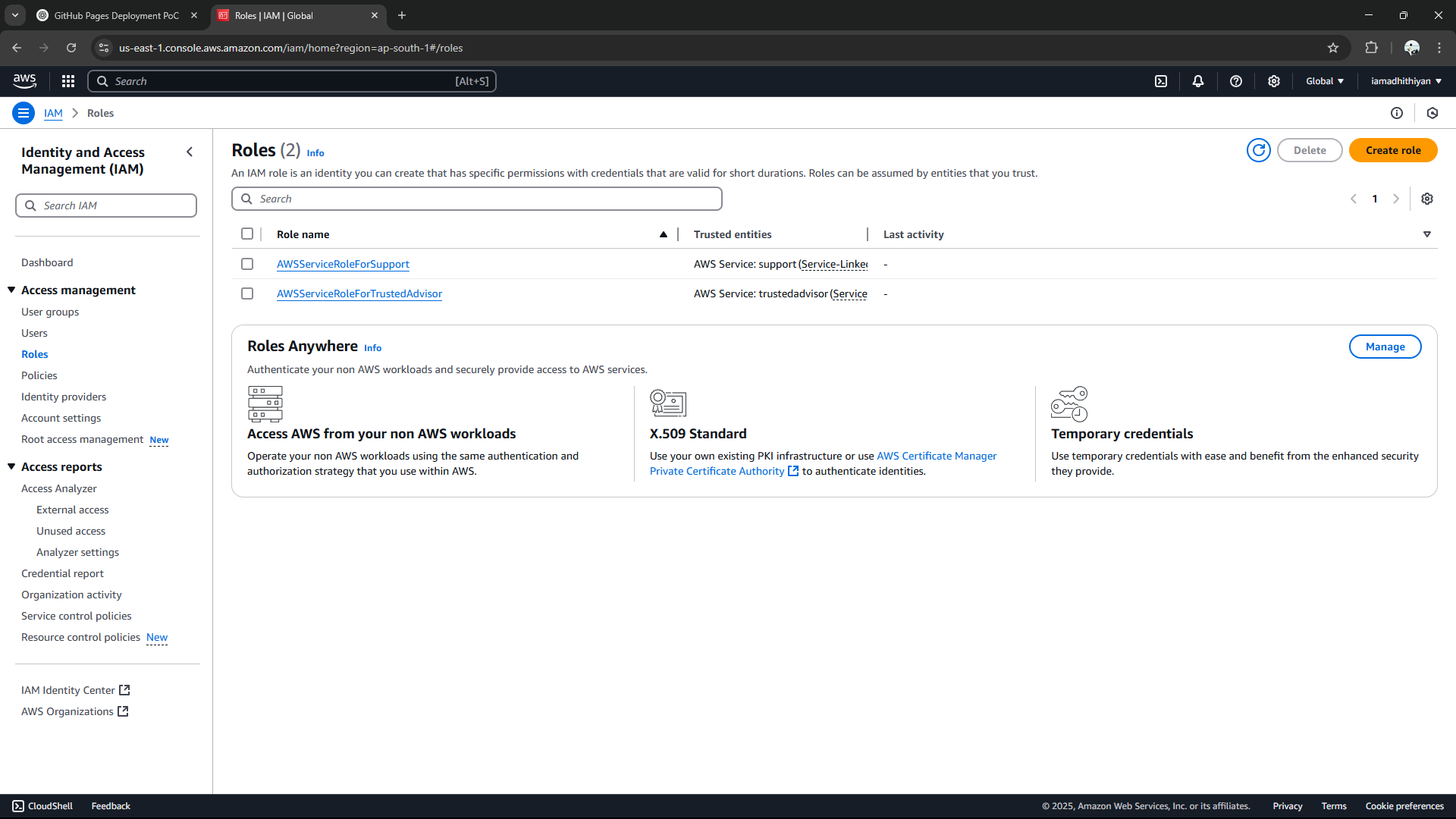
Open [AWS Management Console](https://aws.amazon.com/console/) by using the username and password.

Search for IAM ona open IAM



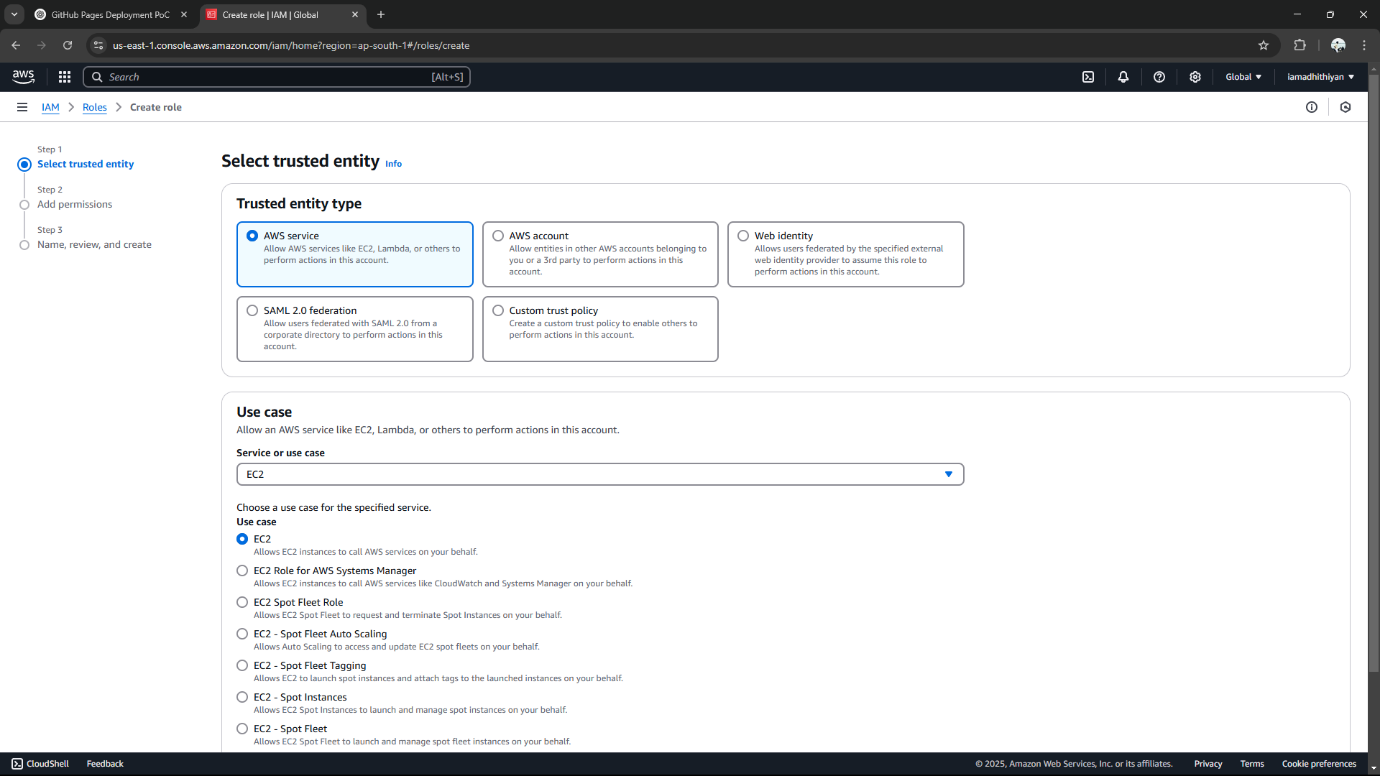
Step 2:

Create Role in IAM



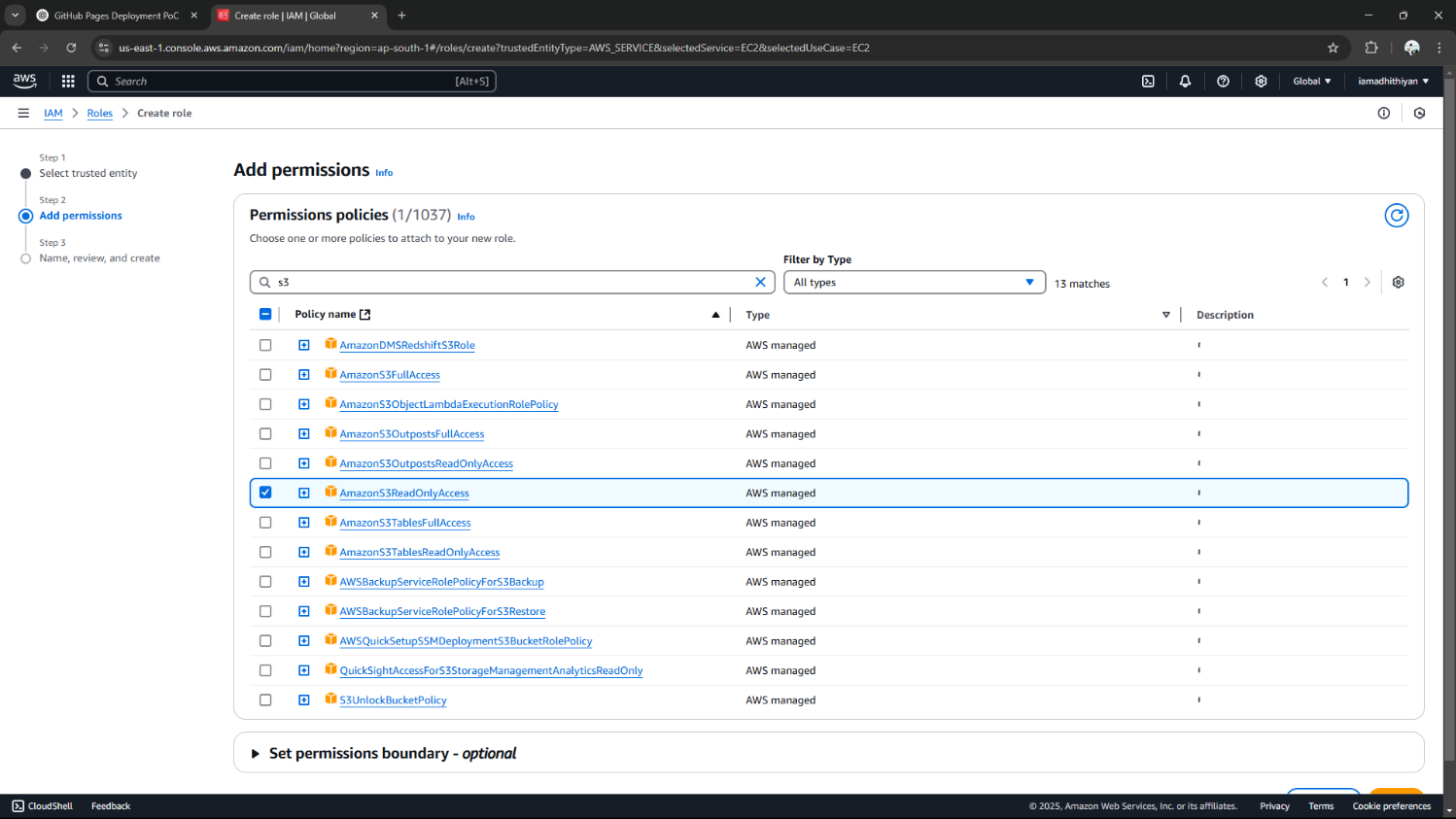
Step 3:

Give access to EC2 and select aws service.



Step 4:

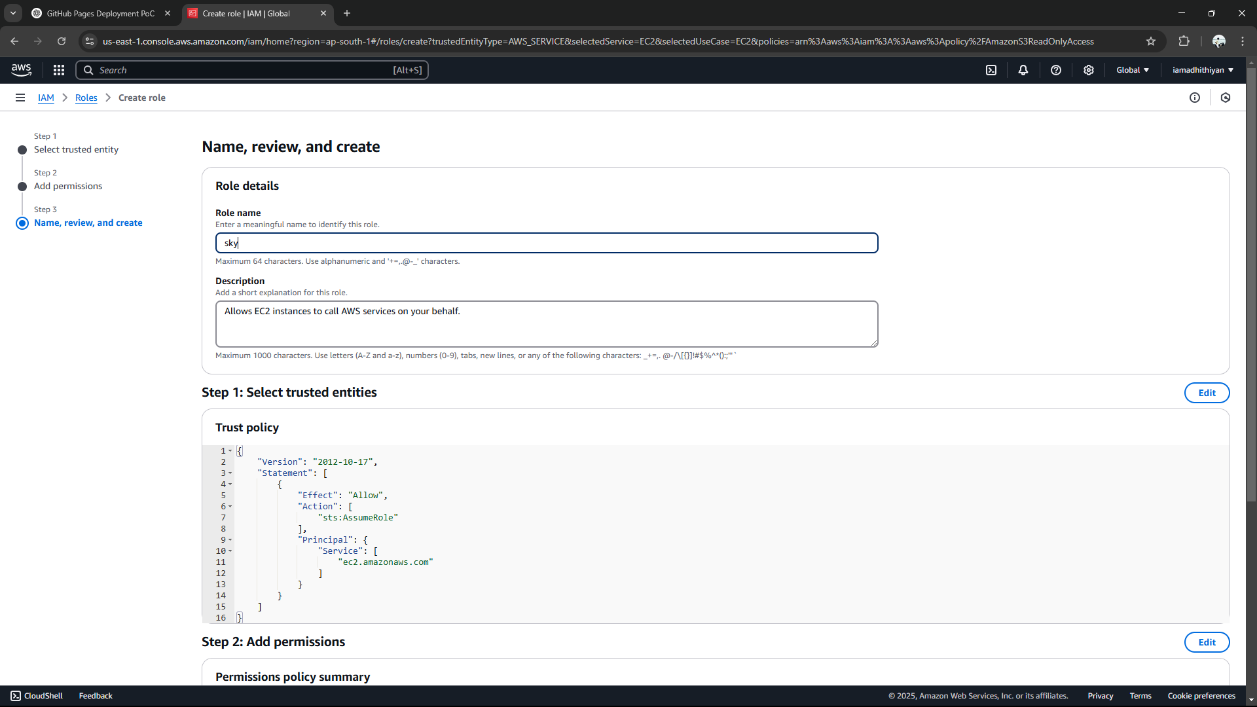
Select **AmazonS3ReadOnlyAccess**

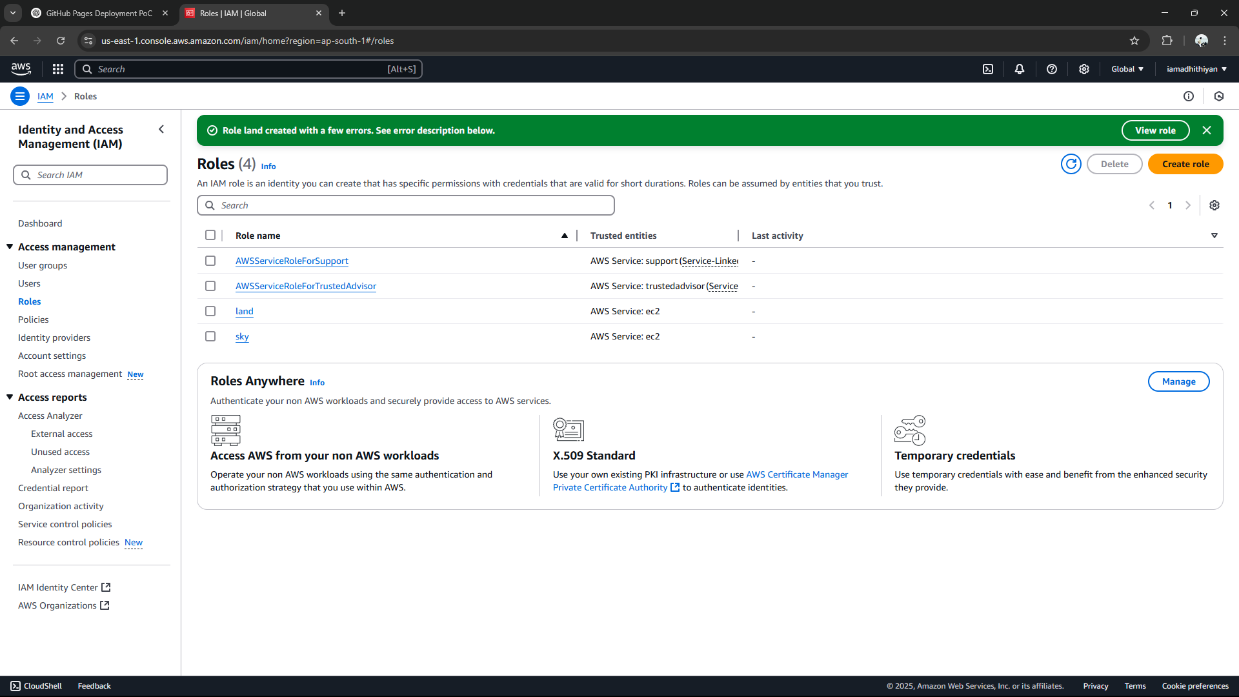


Step 5:

Enter a name for your role

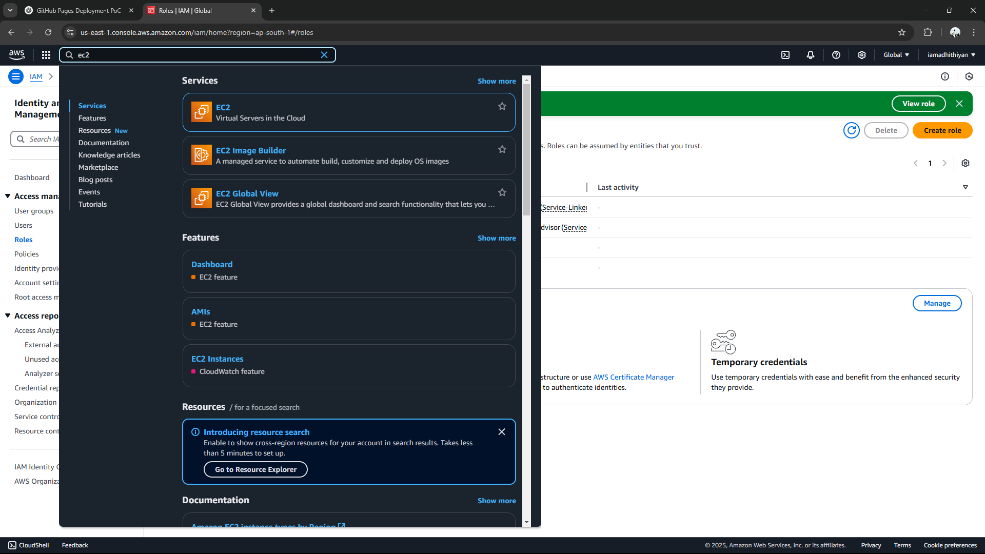
Click **Create Role** to finish.





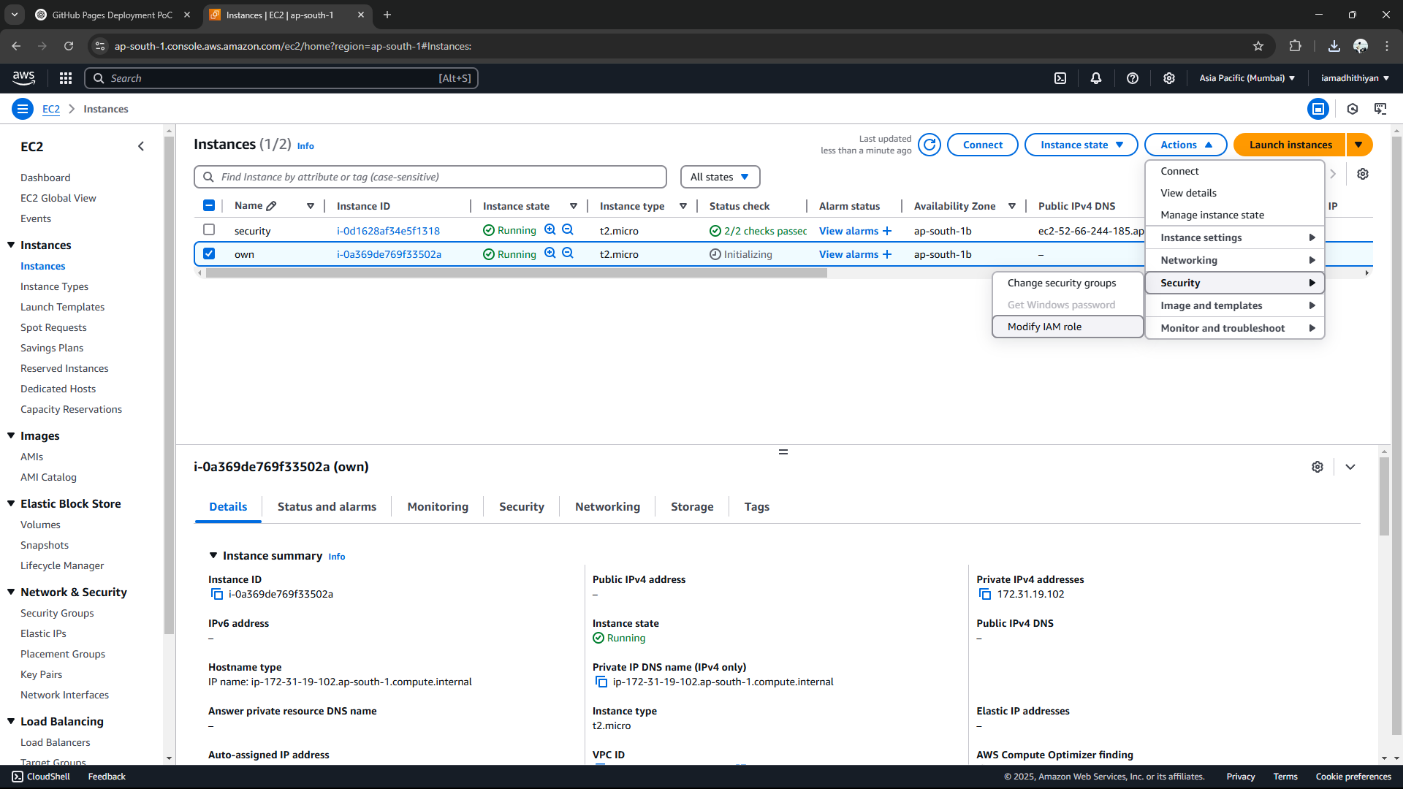
Step 6:

In AWS management console search for **EC2** and click to open the **EC2 Dashboard**.



Step 7:

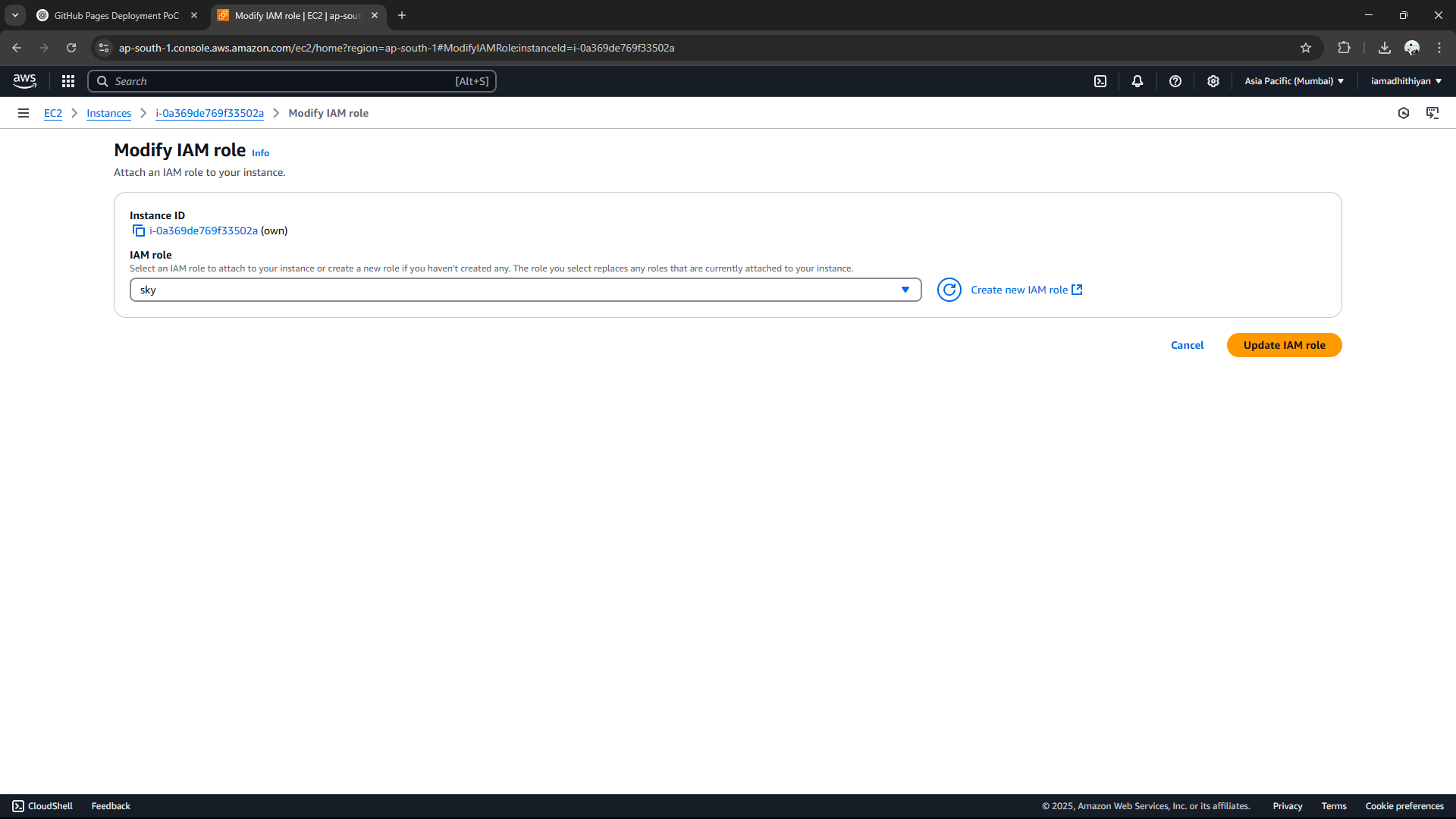
1. In the **Instance details** section, click **Actions** in the top right corner.
2. Choose **Security** > **Modify IAM Role**.



Step 8:

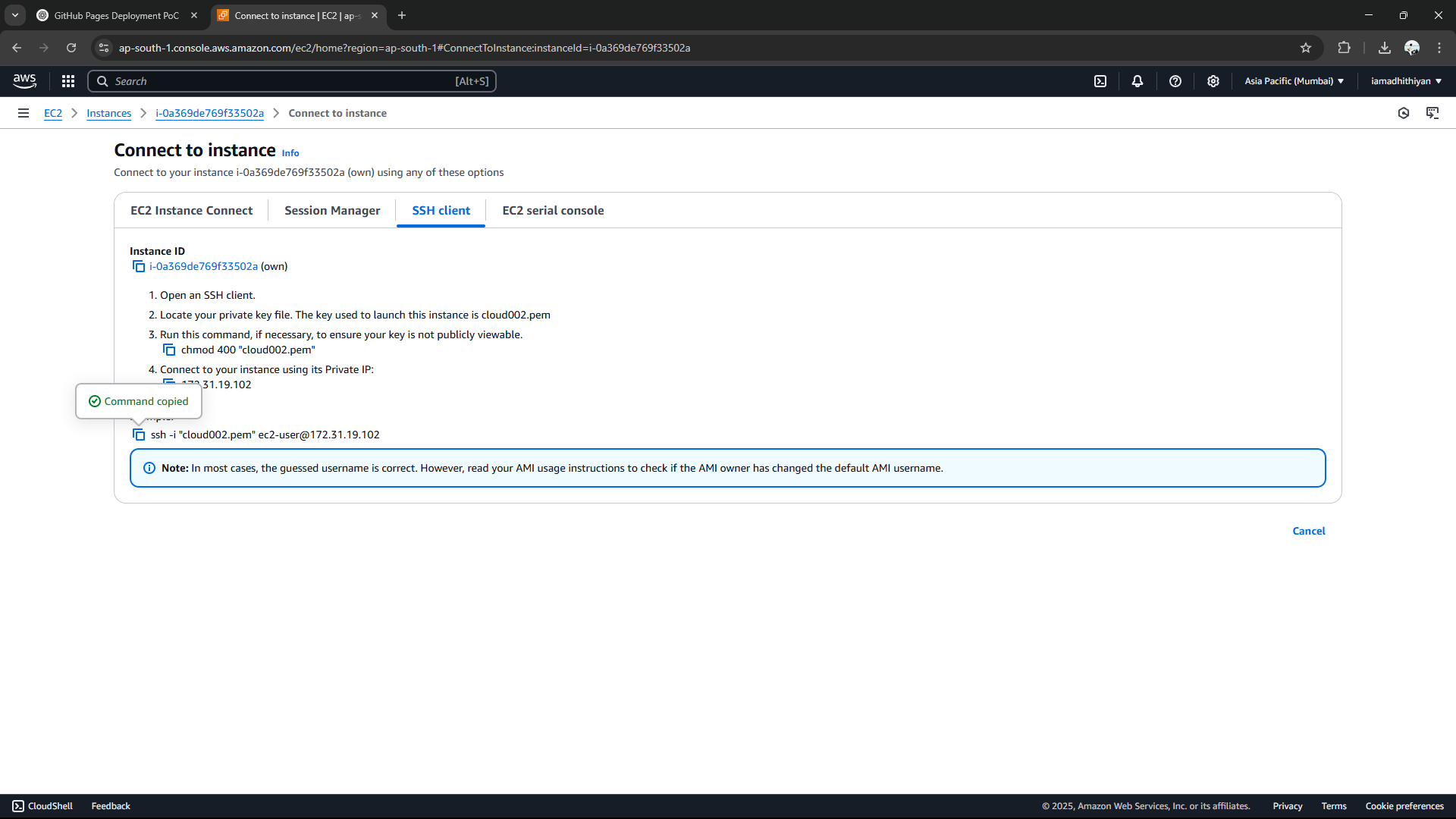
Select the role you created earlier

Click **Update IAM role** to apply the changes



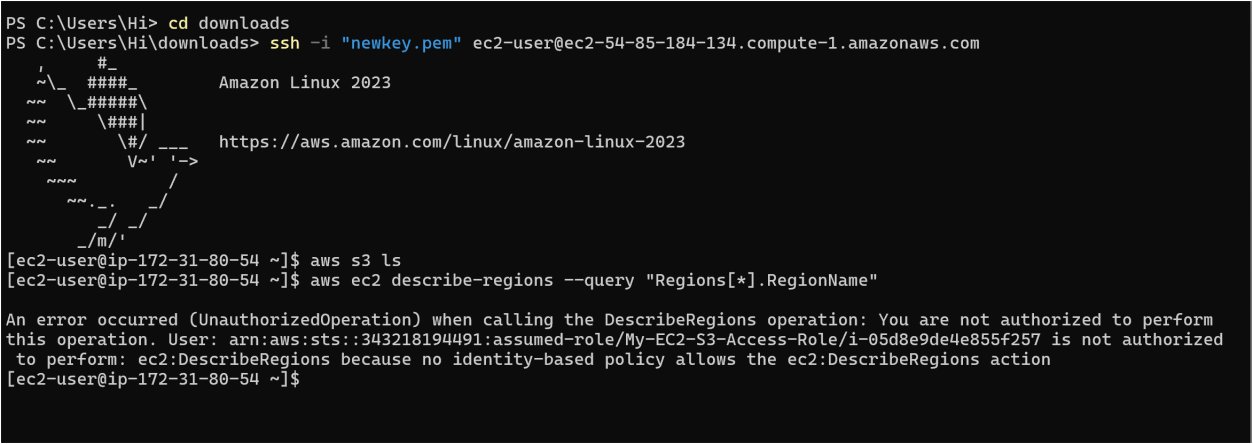
Step 9:

Copy the SSH client command



Step 10:

Open powershell and paste this link in it and ind it will display.



**Expected Outcome :**

1. Set up an IAM role and apply policies to restrict access to specific AWS services.
2. Deploy and configure an EC2 instance for testing.
3. Securely associate the IAM role with the EC2 instance without using access keys.
4. Test permissions by accessing AWS services from the EC2 instance, such as listing S3 buckets.
5. Enforce the principle of least privilege by granting only essential permissions.