

IAM Roles and Permissions

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:

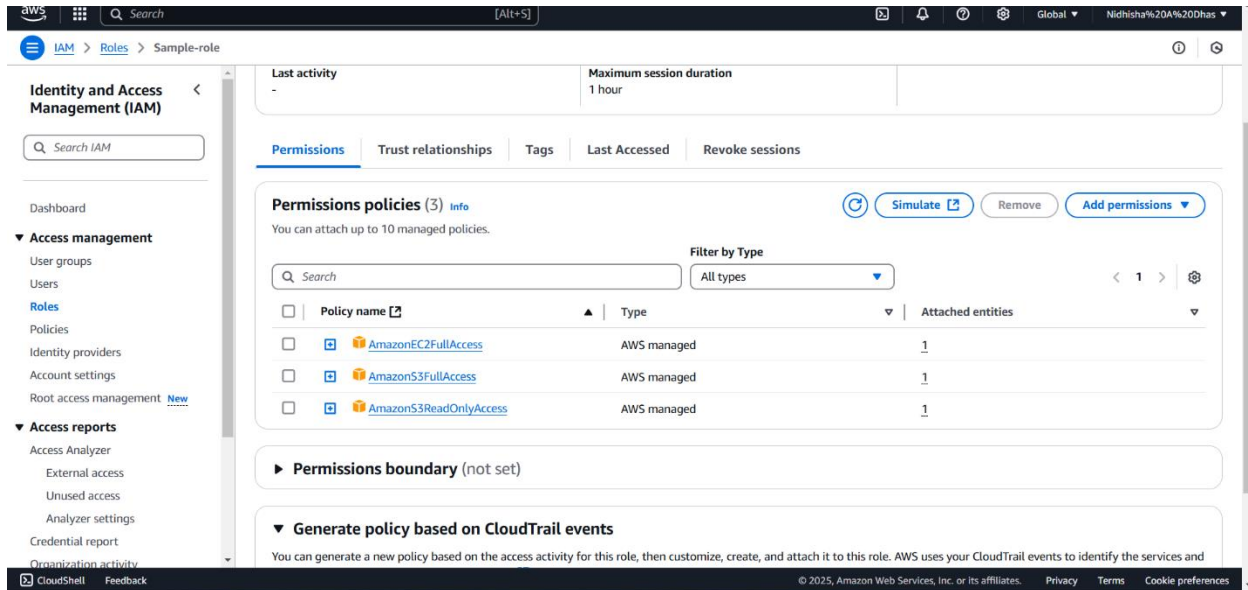
Step 1: CREATING AN IAM ROLE

- ✓ 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.

The screenshot shows the AWS IAM console interface for creating a new role. The top navigation bar includes the AWS logo, a search bar, and user information. The left-hand navigation pane shows the 'IAM' menu with 'Roles' selected, leading to the 'Create role' page. A progress indicator on the left shows three steps: 'Step 1: Select trusted entity' (active), 'Step 2: Add permissions', and 'Step 3: Name, review, and create'. The main content area is titled 'Select trusted entity' and contains a section for 'Trusted entity type' with five radio button options: 'AWS service' (selected), 'AWS account', 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. Below this is a 'Use case' section with a description and a dropdown menu for 'Service or use case', which currently shows 'EC2'. At the bottom, there is a list of use cases for 'EC2', with the first one, 'Allows EC2 instances to call AWS services on your behalf', being selected.

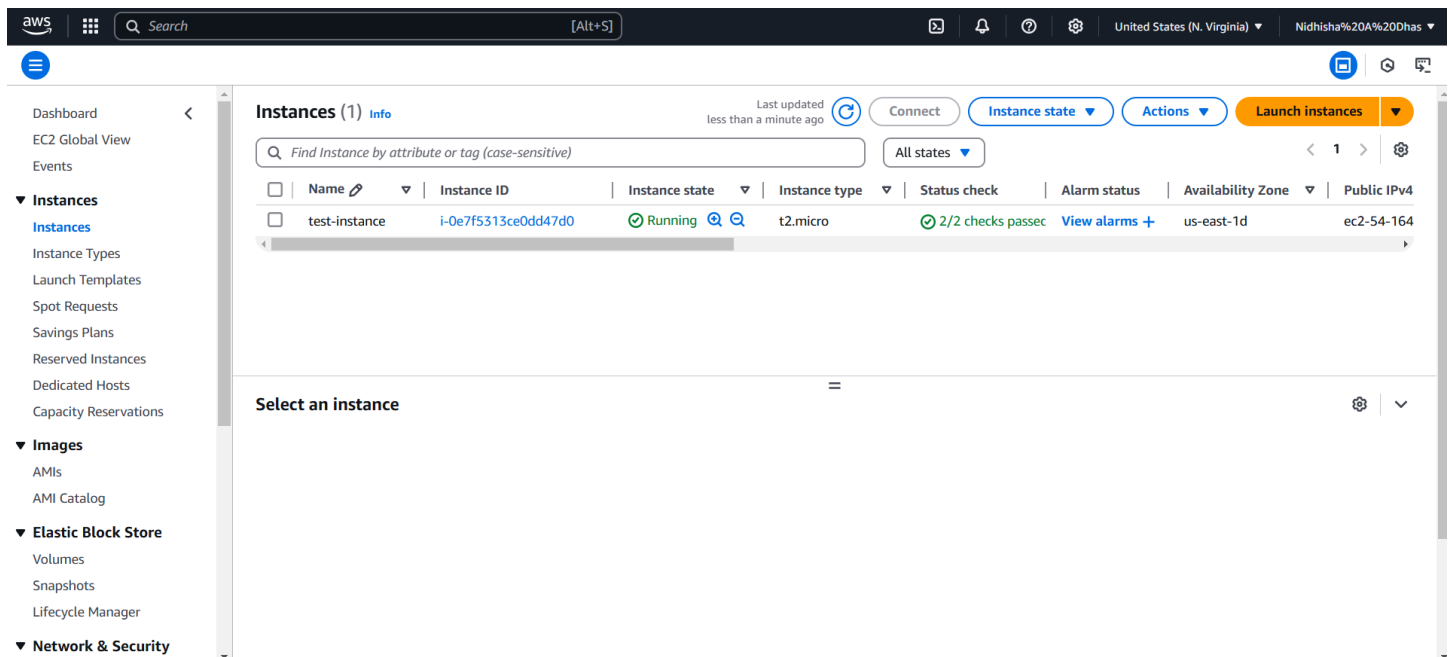
Step 2: ATTACH POLICIES

- 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**.



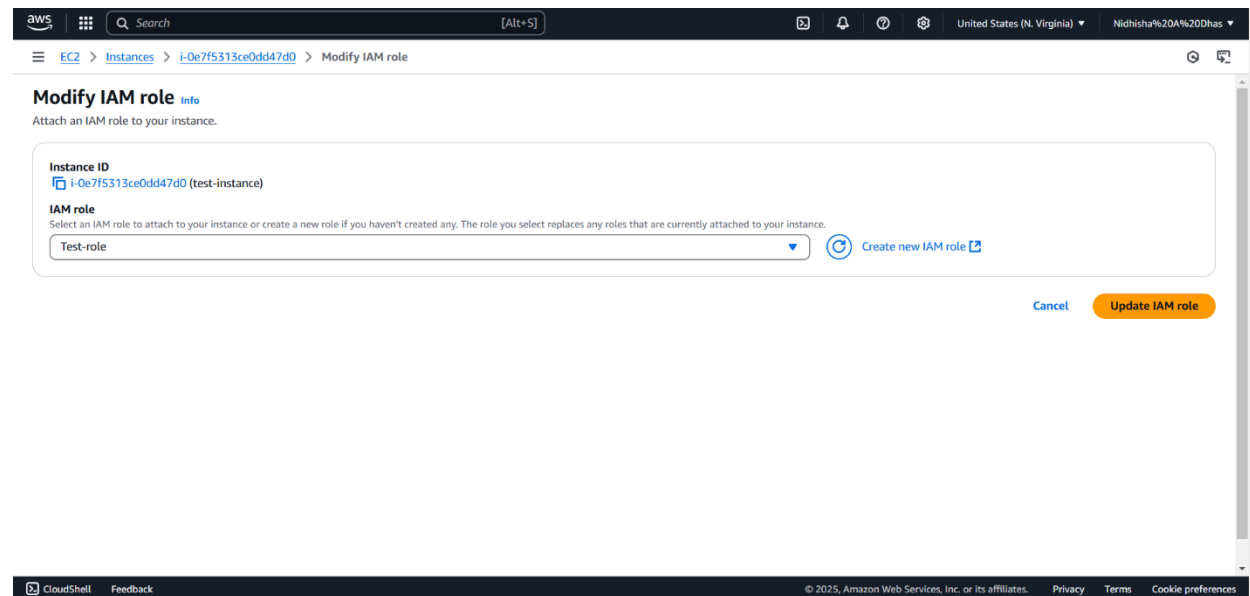
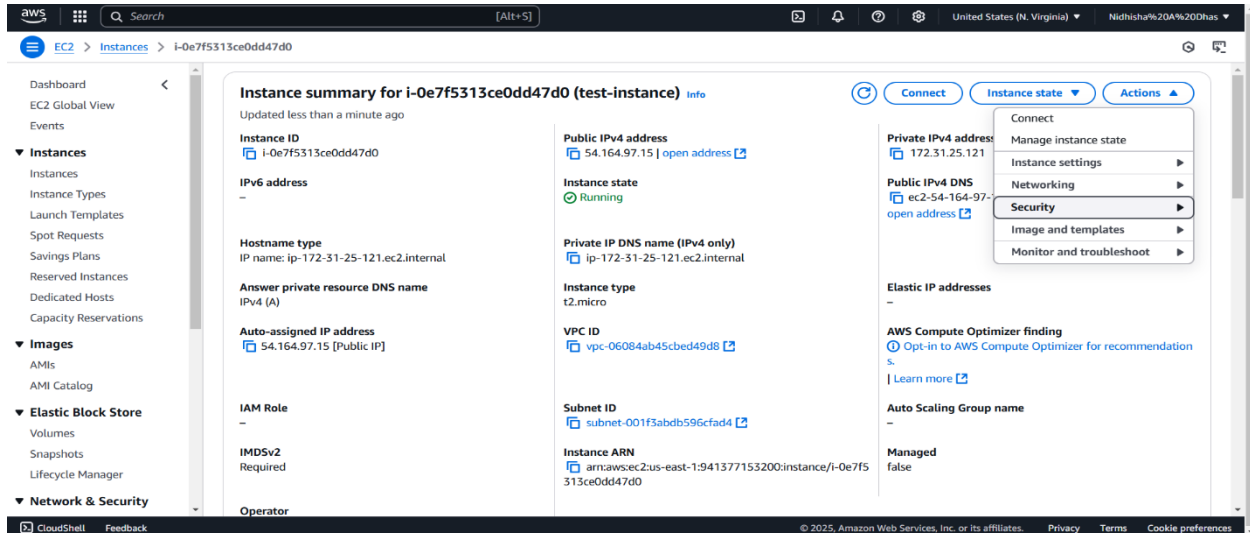
Step 3: CREATING AN EC2 INSTANCE

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



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.



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.