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.

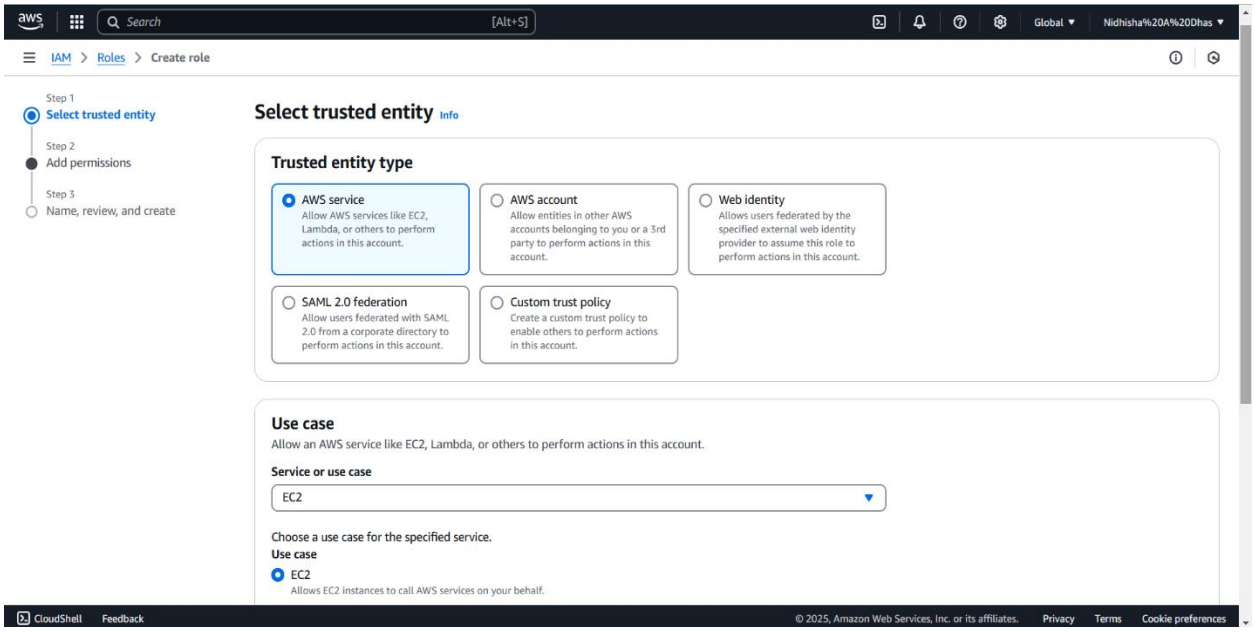
IAM:

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:

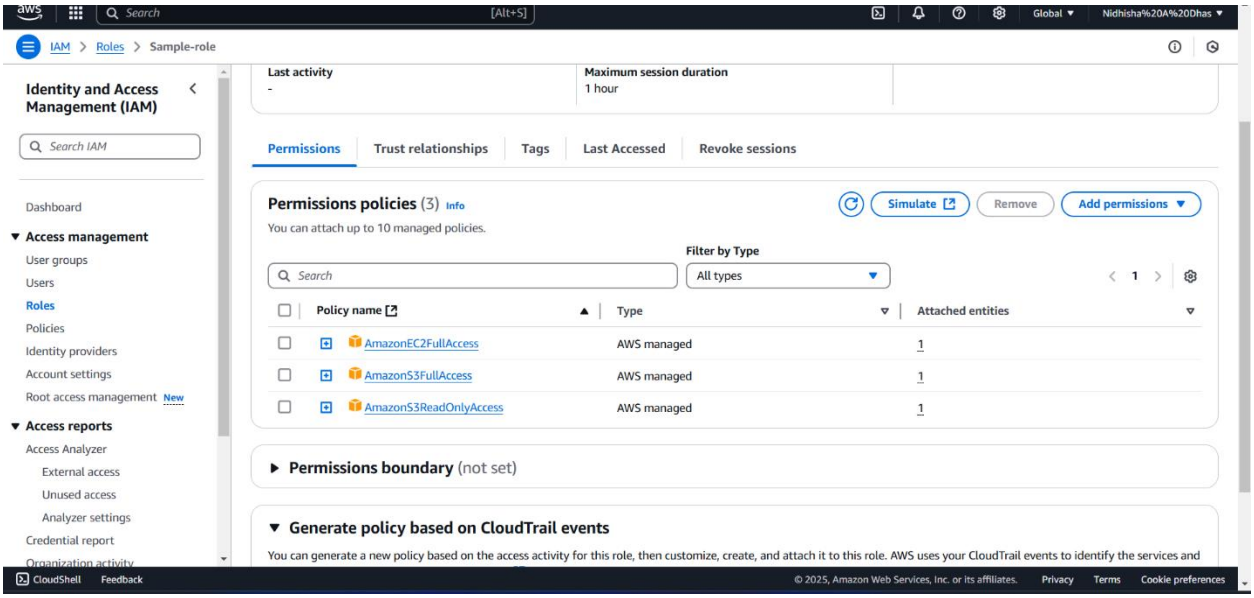
Step 1: CREATING AN **IAM** ROLE

- ✓ 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.



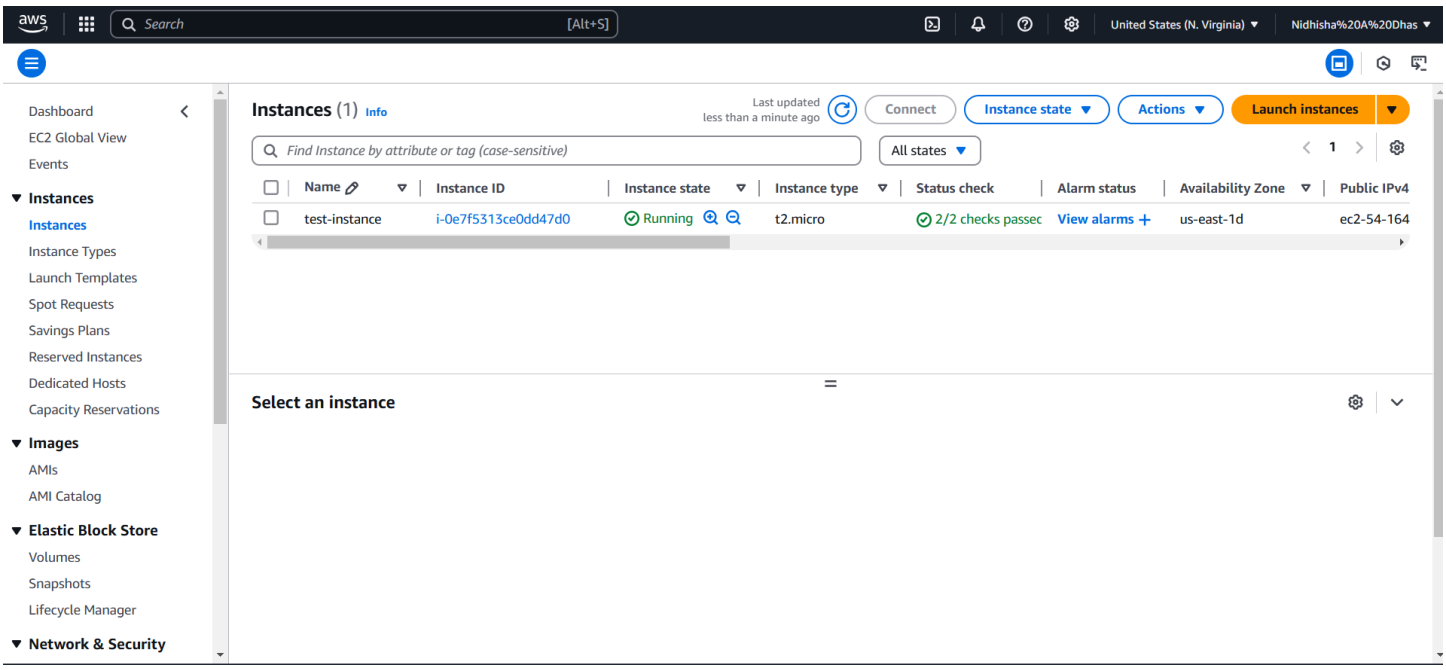
Step 2: ATTACH **POLICIES**

- 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**.



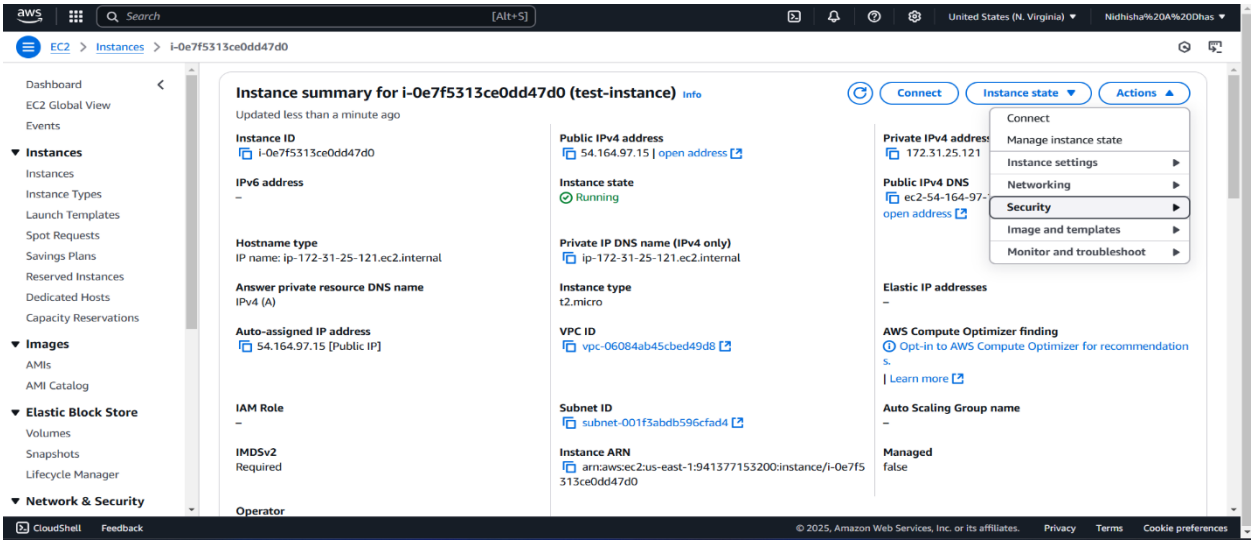
Step 3: CREATING AN EC2 INSTANCE

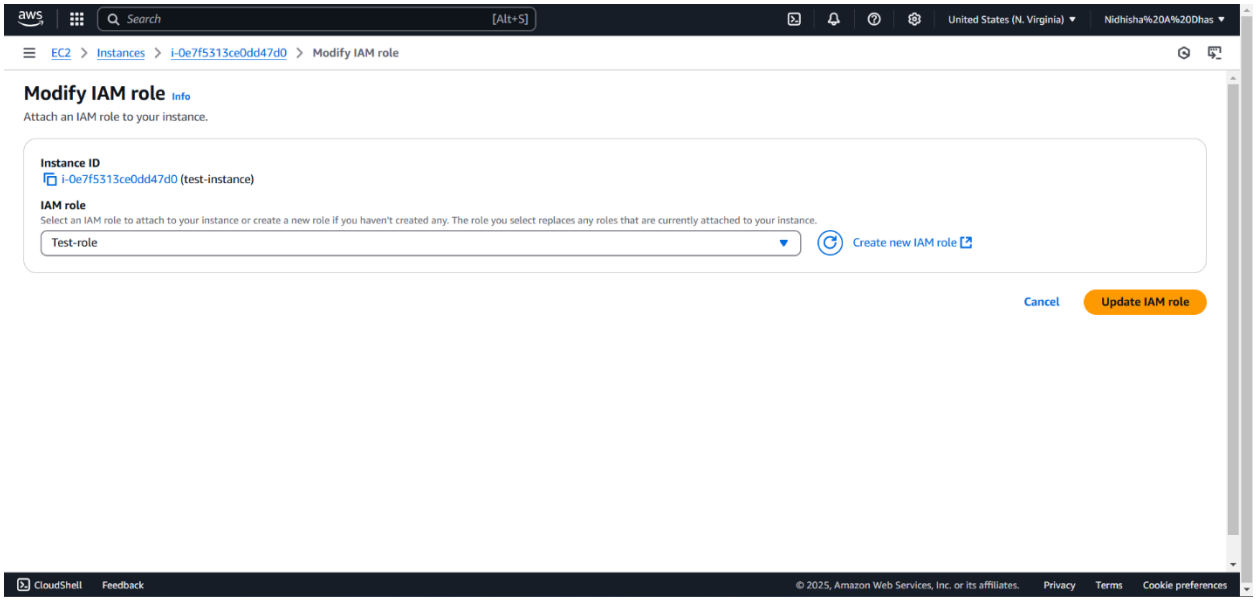
- Create an EC2 instance from the AWS management console by specifying the instance Name, Type and Security group.



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.