St. JOSEPH'S GROUP OF INSTITUTIONS
OMR, CHENNAI - 119

aws

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: SAIRAM S Department: IT

Introduction and Overview

IAM (Identity and Access Management) is a core service in AWS that allows you to manage access to AWS resources securely. With IAM, you can create and manage AWS users, groups, and roles, and assign them specific permissions.

In this document, we will walk through the process of creating an IAM role, attaching it to an EC2 instance, and testing restricted/allowed actions to verify the permissions.

Objectives

- Understand how to create IAM roles in AWS.
- Attach IAM roles to EC2 instances.
- Test permissions by performing allowed and denied actions on the EC2 instance.

Importance

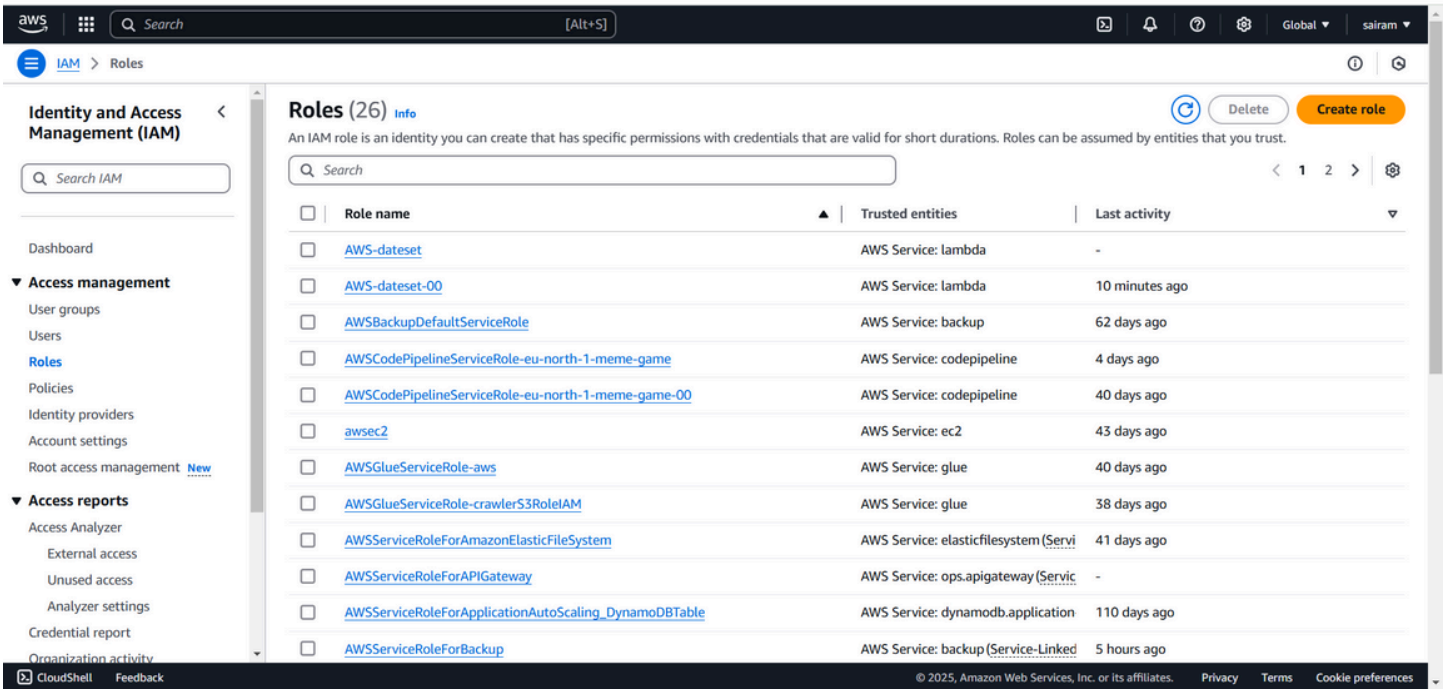
- **Access Control:** Helps manage and restrict access to AWS resources for enhanced security.
- **Scalability:** Allows you to manage permissions at scale for numerous instances, users, and services.
- **Auditing:** IAM roles allow you to track and monitor access, ensuring that only authorized users and instances perform specific actions.
- **Least Privilege:** By granting only the necessary permissions, you ensure your EC2 instance has only the required level of access, reducing the risk of unauthorized actions.

STEPS:

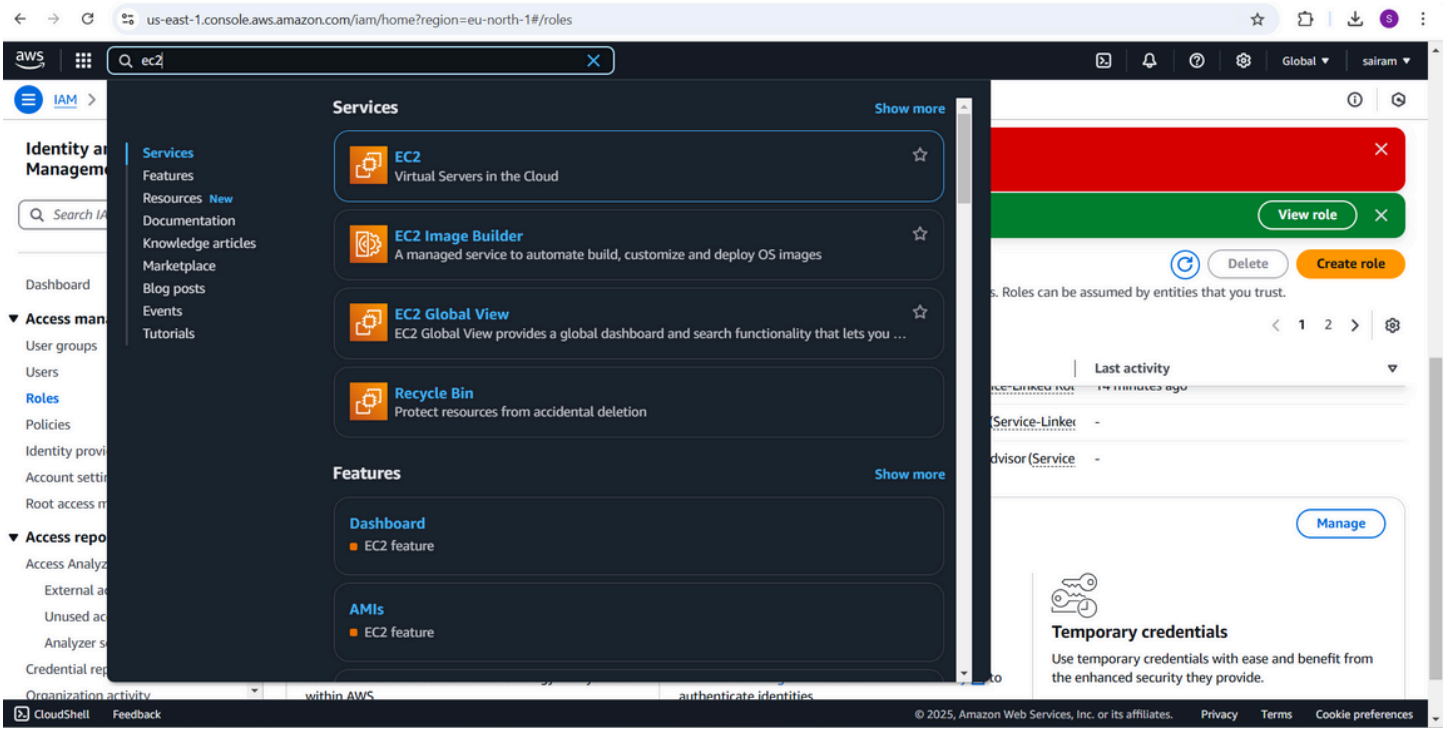
STEP 1: Create an IAM Role

- Sign in to the **AWS Management Console** and go to the **IAM** service.

- In the left sidebar, click **Roles**, then click the **Create role** button.

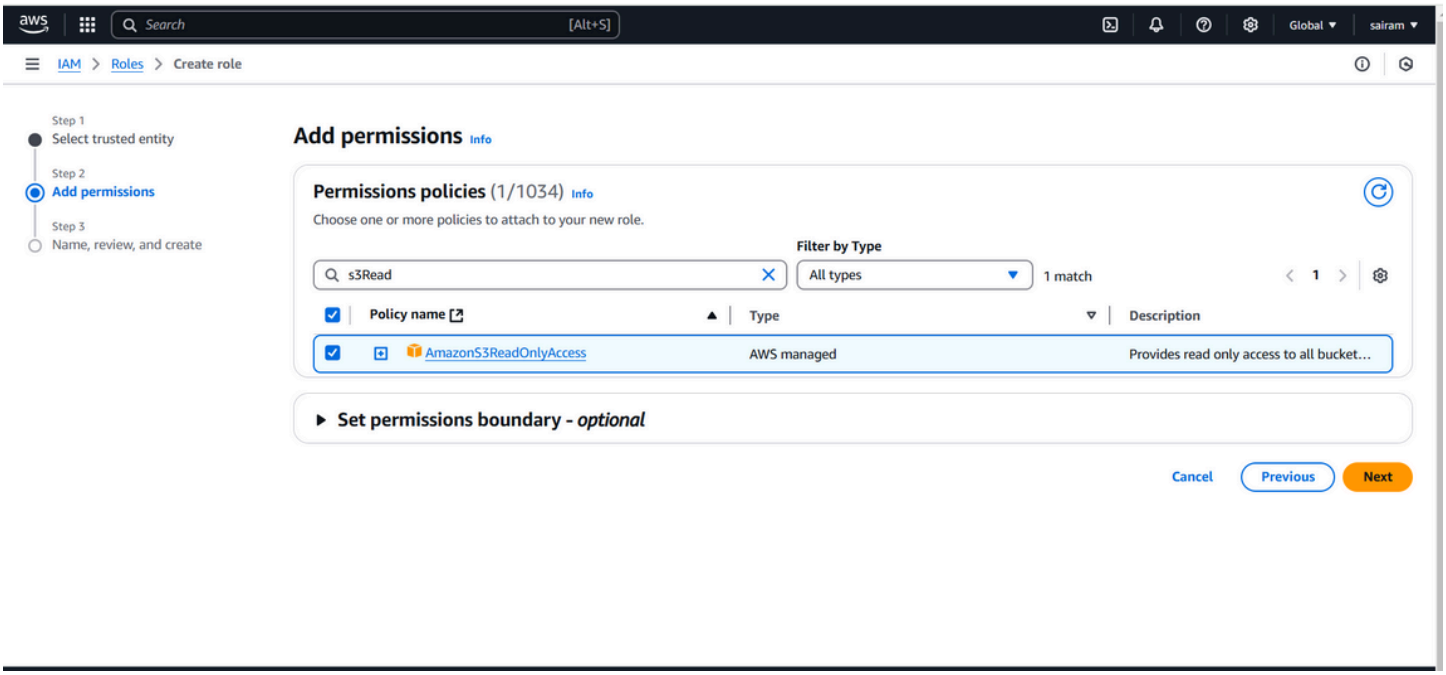


- **Select trusted entity type**:
  - Choose **AWS service** and select **EC2** under "Use case."



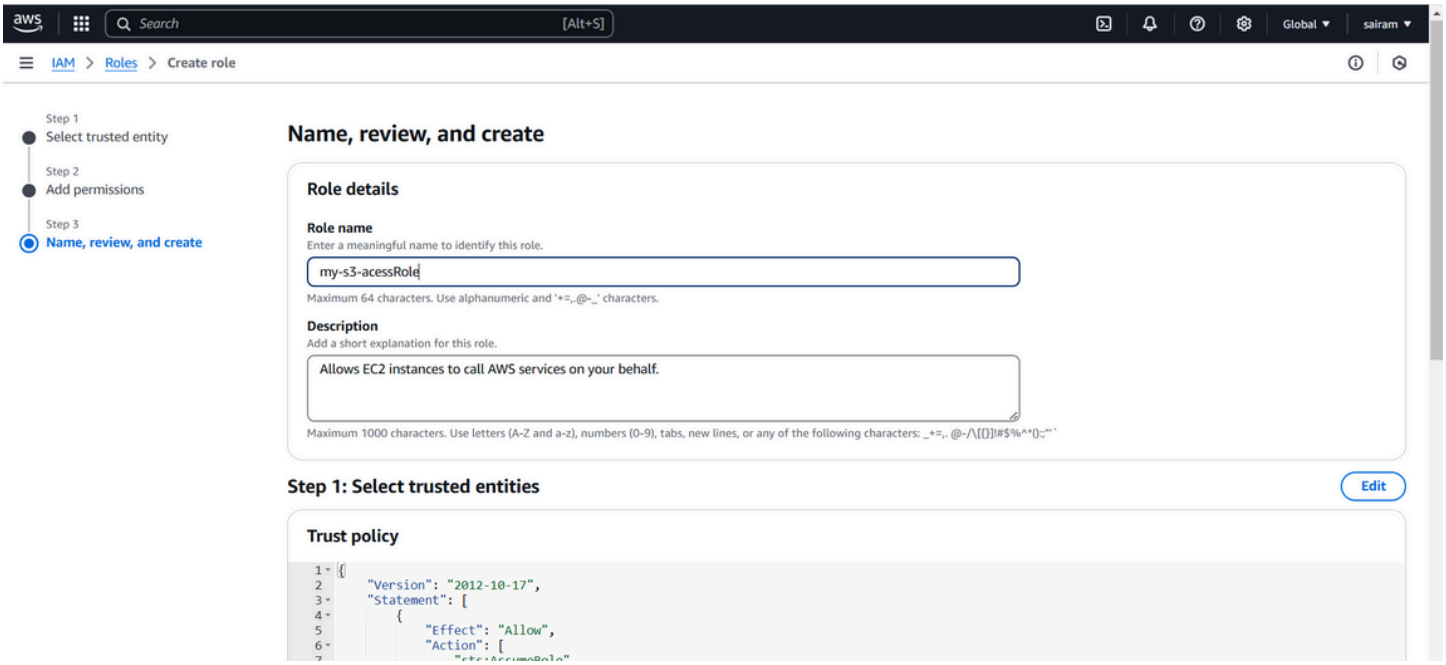
- **Attach permissions policies**:

- For example, to allow access to S3, search for and select the **AmazonS3ReadOnlyAccess** policy.



- You can also create custom policies if needed.

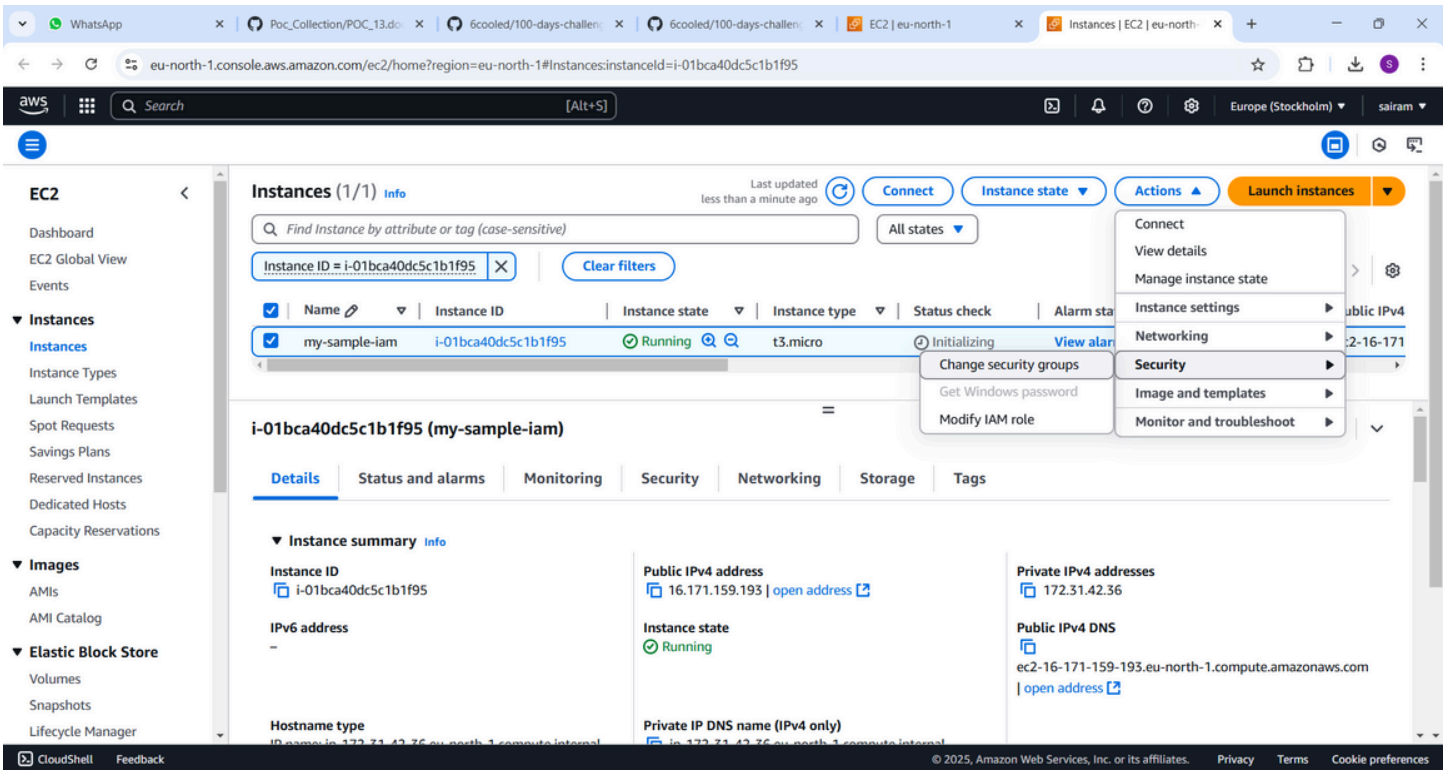
- **Review and create the role**:
  - Name the role (e.g., EC2S3Role) and review the configuration.



- Click **Create role**.

STEP 2: Attach the IAM Role to Your EC2 Instance

- Go to the **EC2 Dashboard** in the AWS Management Console.
- Select the EC2 instance you want to assign the IAM role to.
- Under **Actions**, select **Security > Modify IAM role**.



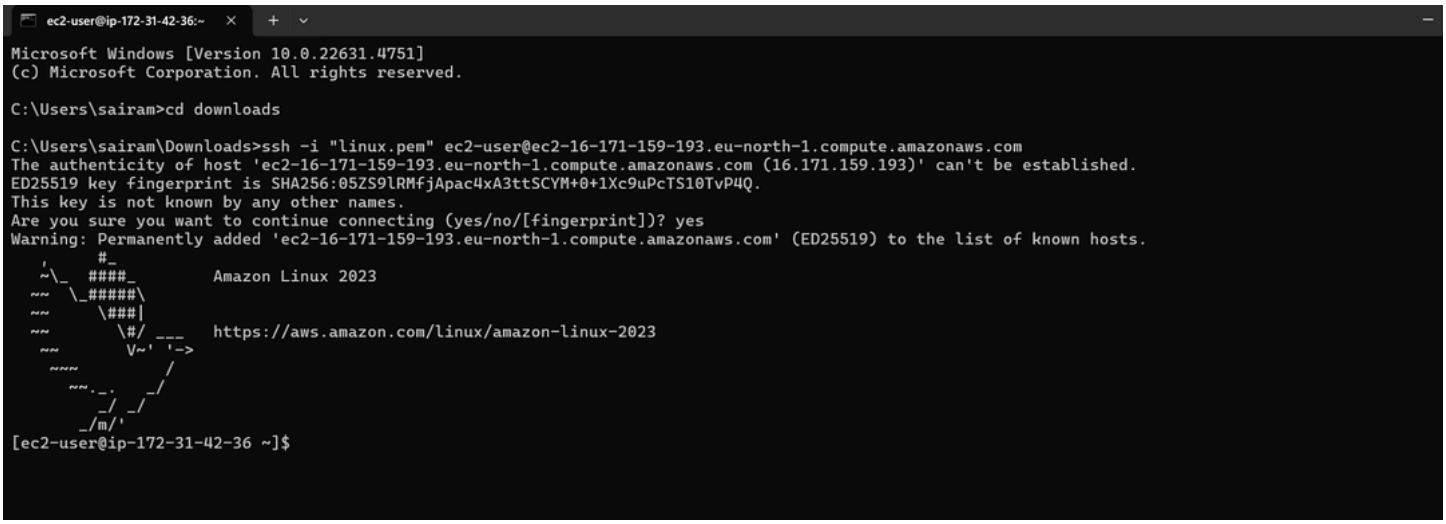
- In the **IAM role** dropdown, select the IAM role you created earlier (e.g., EC2S3Role).

- Click **Update IAM role**.

STEP 3: Verify the IAM Role and Permissions

- **SSH into the EC2 instance** using your terminal or an SSH client.
- Attempt an allowed action (e.g., accessing an S3 bucket):

aws s3 ls



If you have granted S3 permissions, this should list the S3 buckets.

- **Attempt a denied action** (e.g., writing to S3 if the policy doesn't allow it):

aws s3 mb s3://my-new-bucket-name