Placement Empowerment Program

Cloud Computing and DevOps Centre

Creating an IAM role on your cloud platform. Assign the role to your VM to restrict/allow specific actions.

Name: Esly Abro **Department: IT**

Setting Up IAM Roles and Permissions

Introduction

In this POC, we will demonstrate how to create an IAM role on a cloud platform, assign the role to a virtual machine (VM), and restrict/allow specific actions (e.g., accessing an S3 bucket). This is a

fundamental aspect of cloud security, ensuring that resources are accessed only by authorized entities with appropriate permissions.

Overview

This POC covers the basics of setting up and managing IAM roles, including role creation, permission assignment, and testing access. By the end of this POC, you'll understand how to control access to cloud resources using IAM roles and test access to ensure security policies are enforced.

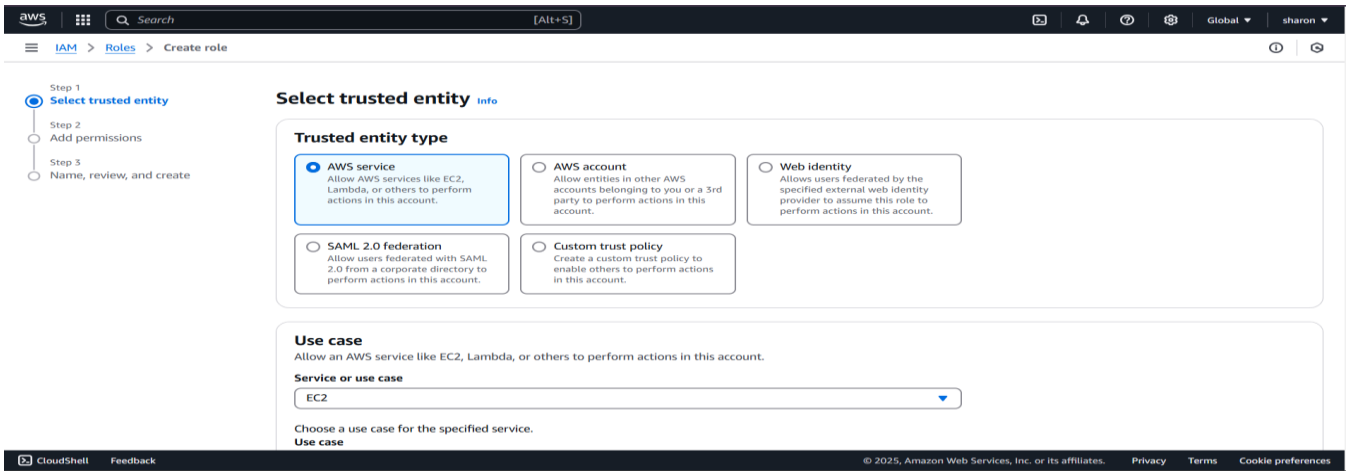
Objectives

- Create an IAM role with custom permissions (e.g., access to S3)
- Assign the IAM role to a VM (EC2 in AWS)
- Verify the role's permissions by testing both allowed and denied actions

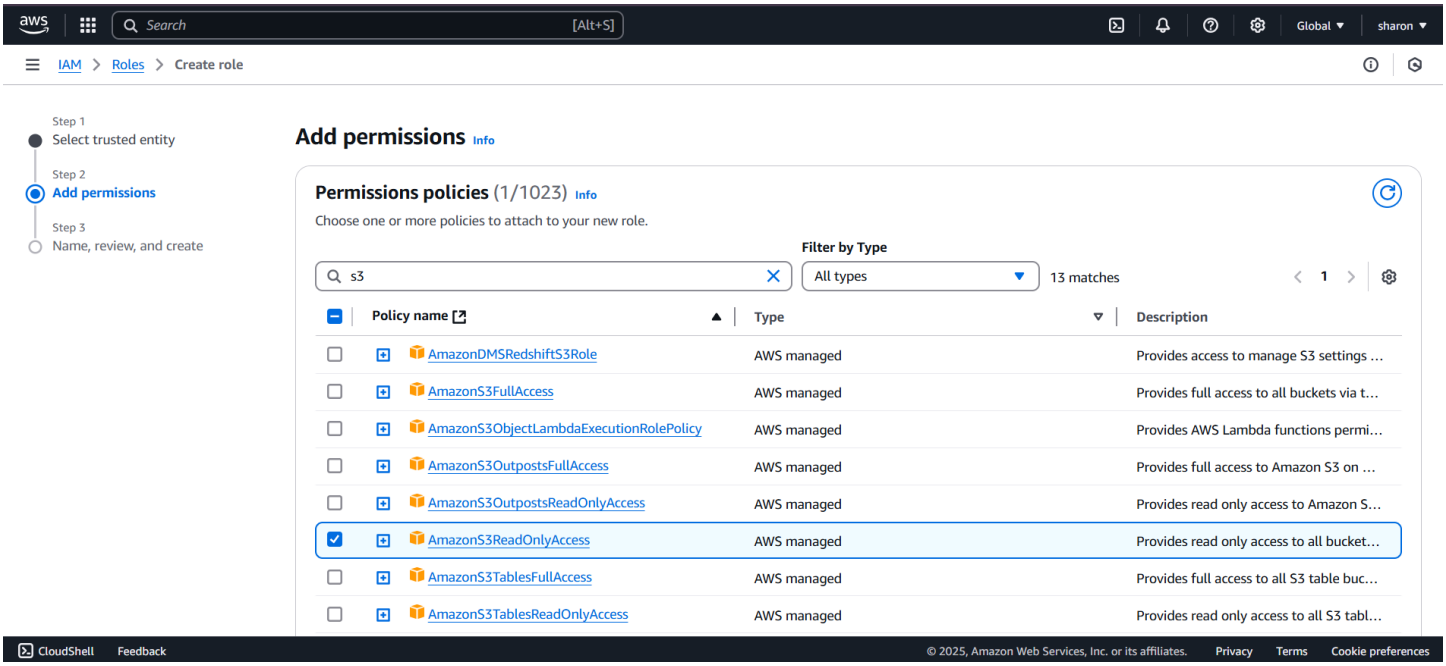
Step-by-Step Process

Step 1: Create an IAM Role

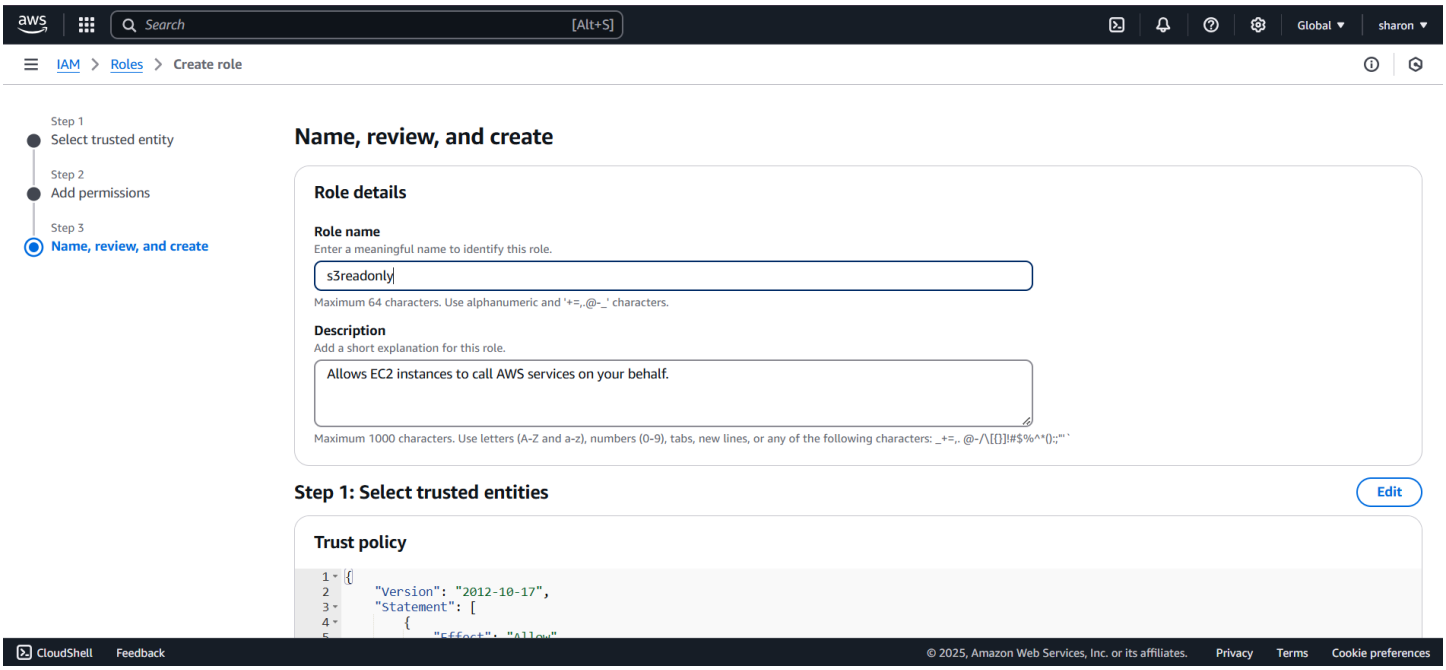
1. **Login to AWS Console**:
    a. Go to AWS Management Console.
2. **Navigate to IAM**:
    a. From the Services menu, select **IAM**.



3. **Create New Role**:
    a. Click on **Roles** in the left sidebar, then click **Create Role**.
    b. Choose **AWS Service** as the trusted entity, and select **EC2** (for VM).
    c. Click **Next**.
4. **Attach Policies**:
    a. In the **Permissions** section, attach a managed policy (e.g., `AmazonS3ReadOnlyAccess`) to give read access to S3.
    b. Click **Next: Tags**, and then **Next: Review**.

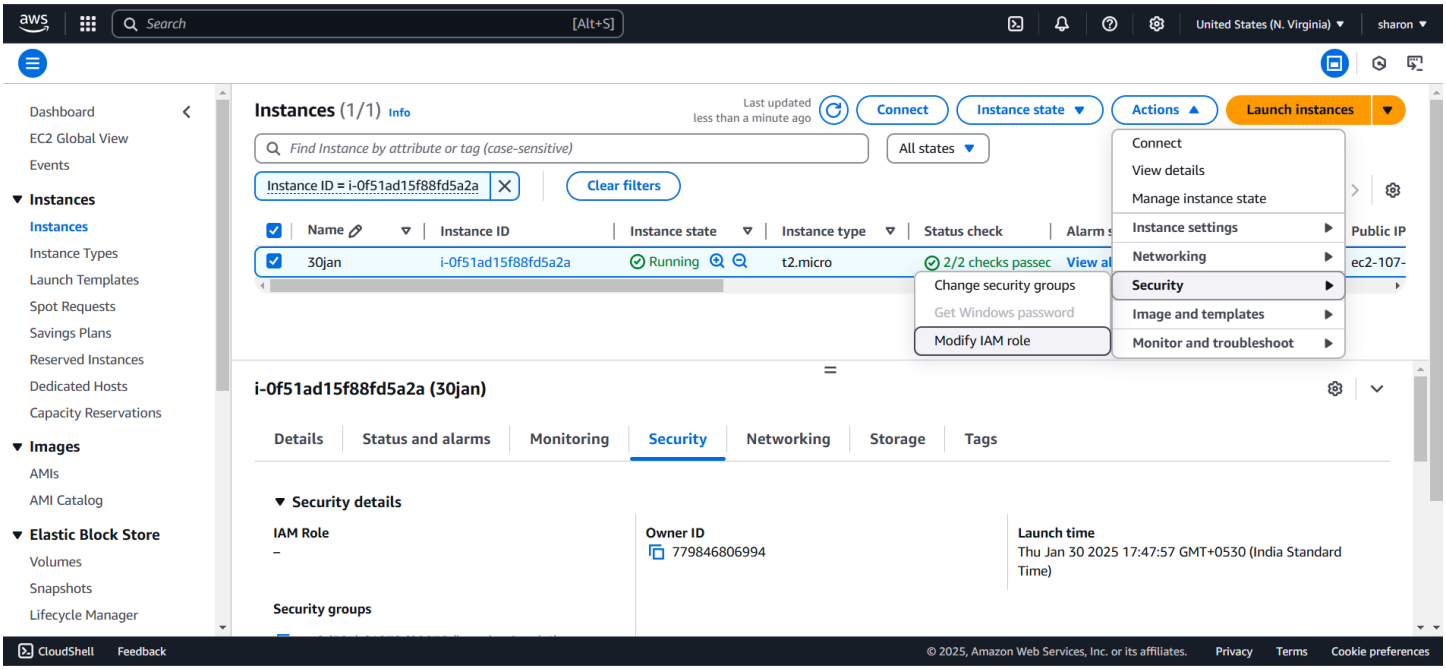


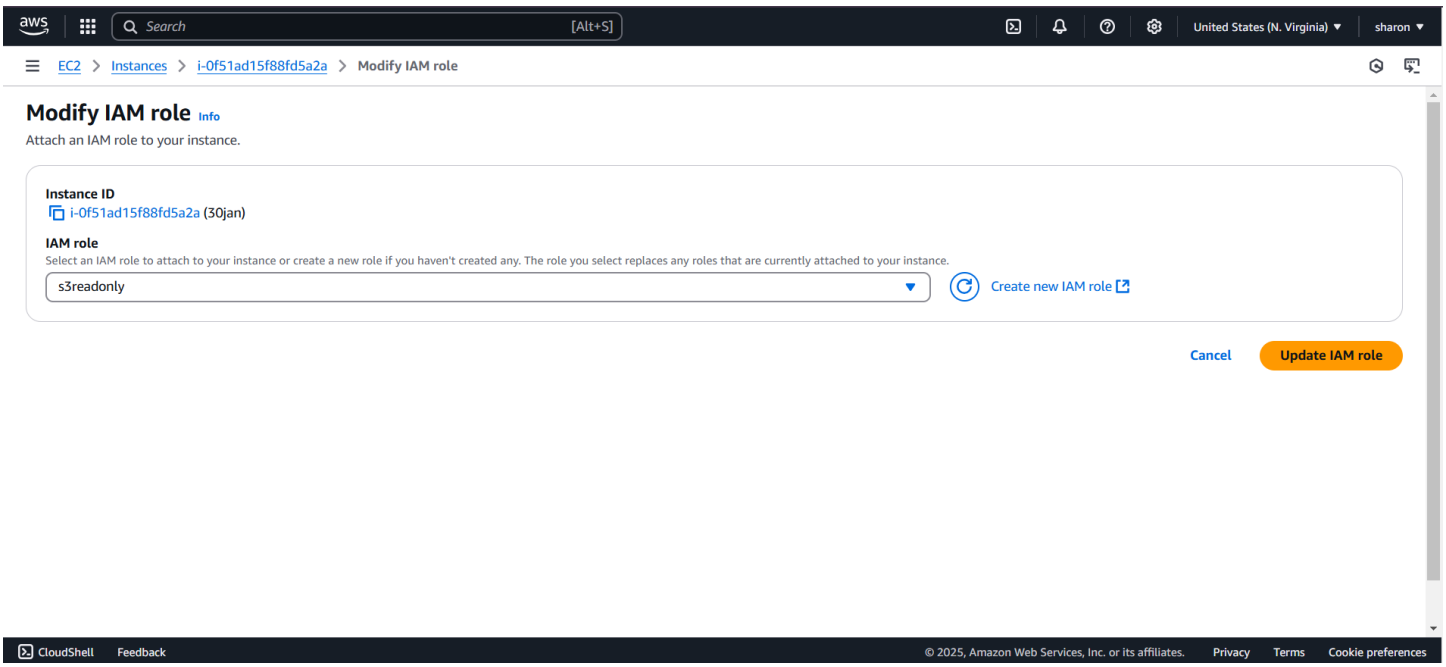
5. **Review and Create**:
    a. Name the role (e.g., `S3ReadOnlyRole`) and click **Create Role**.



Step 2: Assign Role to an EC2 Instance

1. **Launch or Select an EC2 Instance**:
    a. Navigate to **EC2** under Services and either create or select an existing EC2 instance.
2. **Modify IAM Role**:
    a. Select the instance, click on **Actions**, choose **Security**, then **Modify IAM Role**.
    b. Assign the newly created IAM role (e.g., `S3ReadOnlyRole`) to the instance.
    c. Save the changes.





Step 3: Verify Permissions

1. **SSH into the EC2 Instance**:
    a. Connect to the instance via SSH (or EC2 Instance Connect).
2. **Install AWS CLI (if not installed)**: `sudo apt-get update`
   `sudo apt-get install awscli`

3. **Test Allowed Actions**:
    a. Run the following command to list S3 buckets (allowed by the assigned role):

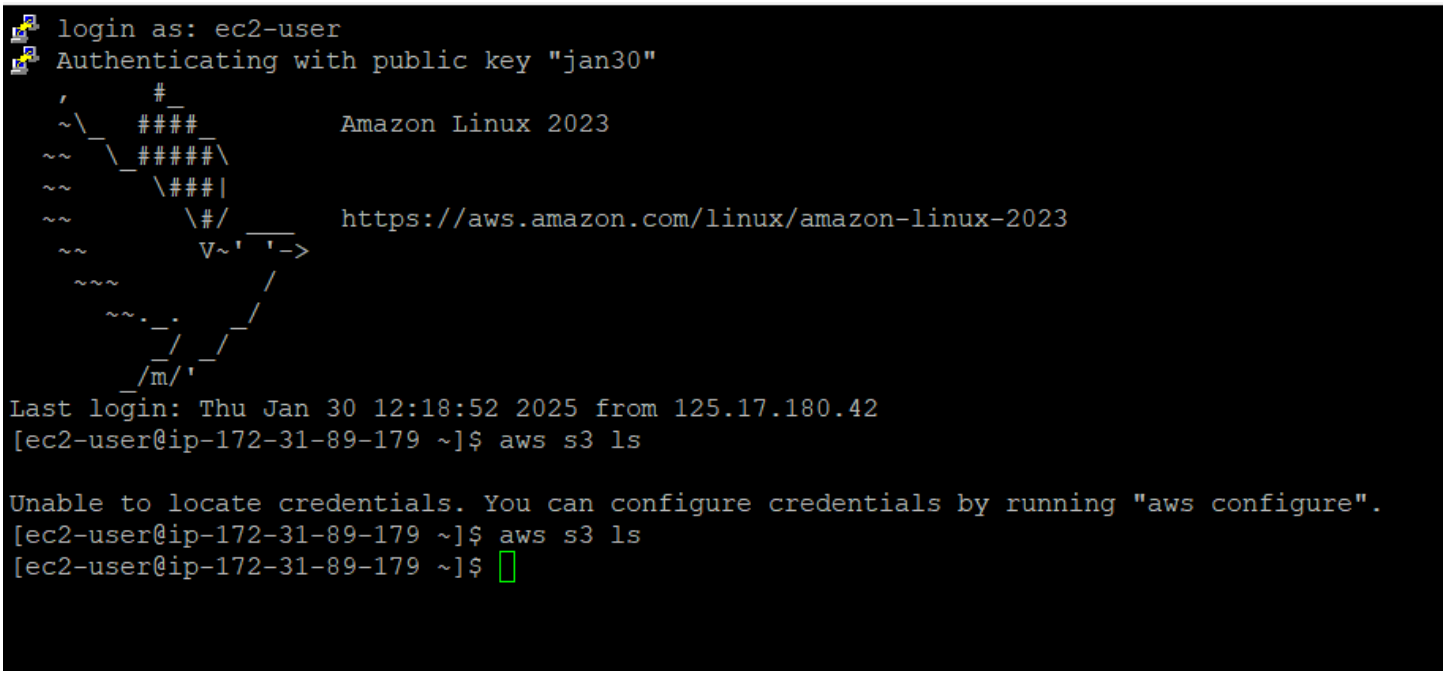
`aws s3 ls`

You should see a list of S3 buckets because the role has read-only access.

4. **Test Denied Actions**:
    a. Try to upload a file to an S3 bucket:

```
aws s3 cp testfile.txt s3://bucket-name/
```

This should result in an "Access Denied" error, as the role does not have permission to upload files.



Step 4: Clean Up

1. **Terminate the EC2 Instance** (if no longer needed):
    a. Navigate to EC2, select the instance, and terminate it.
2. **Delete the IAM Role** (if no longer needed):
    a. Go to **IAM Roles**, select the created role, and click **Delete Role**.

Outcomes

- Successfully created an IAM role (`S3ReadOnlyRole`) with restricted permissions.
- Assigned the role to an EC2 instance and verified that it can access permitted resources (S3 read-only) and was denied other actions (uploading to S3).