Placement Empowerment Program

Cloud Computing and DevOps Centre

Set Up IAM Roles and Permissions

Name: Shalini D Department : IT

Introduction and Overview

To effectively manage AWS resources, one powerful approach is to create IAM (Identity and Access Management) roles with specific permissions and assign these roles to your EC2 instances. This not only enhances security but also ensures that your instances can only perform actions they are explicitly allowed to. For example, you might create an IAM role with S3 access permissions, assign it to an EC2 instance, and then verify its effect by attempting actions that should be permitted or denied based on the role's permissions. This method provides a practical way to manage access controls and automate tasks in a secure manner, making cloud management more efficient and reliable. Let's dive into the detailed steps to achieve this!

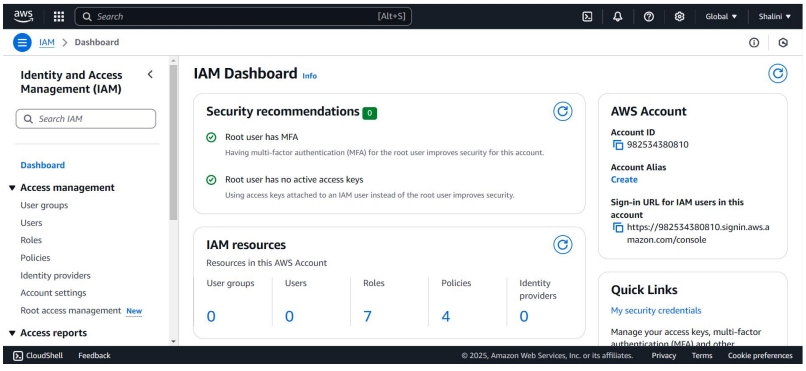
Objective

The objective of creating an IAM role with specific permissions (e.g., S3 access), assigning the role to your EC2 instance, and verifying its effect is to ensure that your EC2 instance can securely access and perform only the actions it is explicitly allowed to. This approach enhances security by implementing the principle of least privilege, which means granting only the permissions necessary for the instance to perform its tasks. Additionally, verifying the role's effect by attempting permitted and denied actions ensures that the IAM role is correctly configured and functioning as intended, providing a practical way to manage access controls and automate tasks in a secure manner.

Step-by-Step Overview

Step1:

Sign in to the AWS Management Console and open the IAM console.



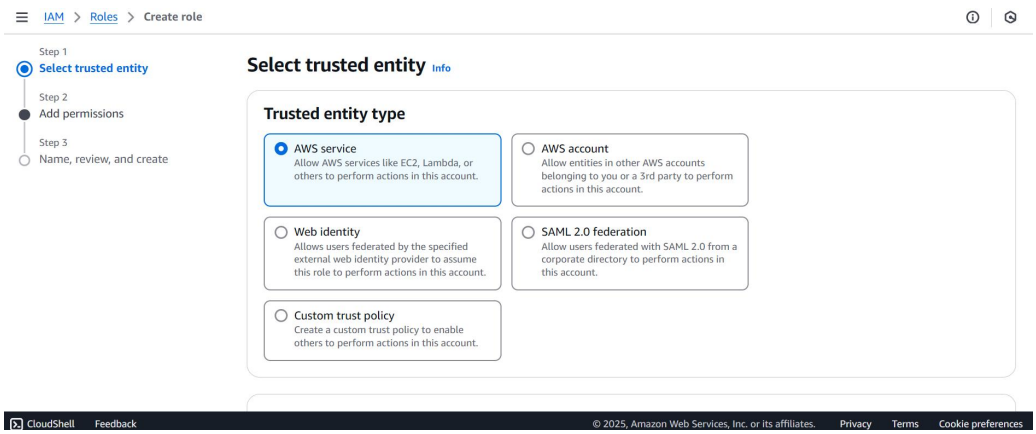
Step 2 :

Create a new role:

Go to **Roles** in the left navigation pane and click **Create role**.

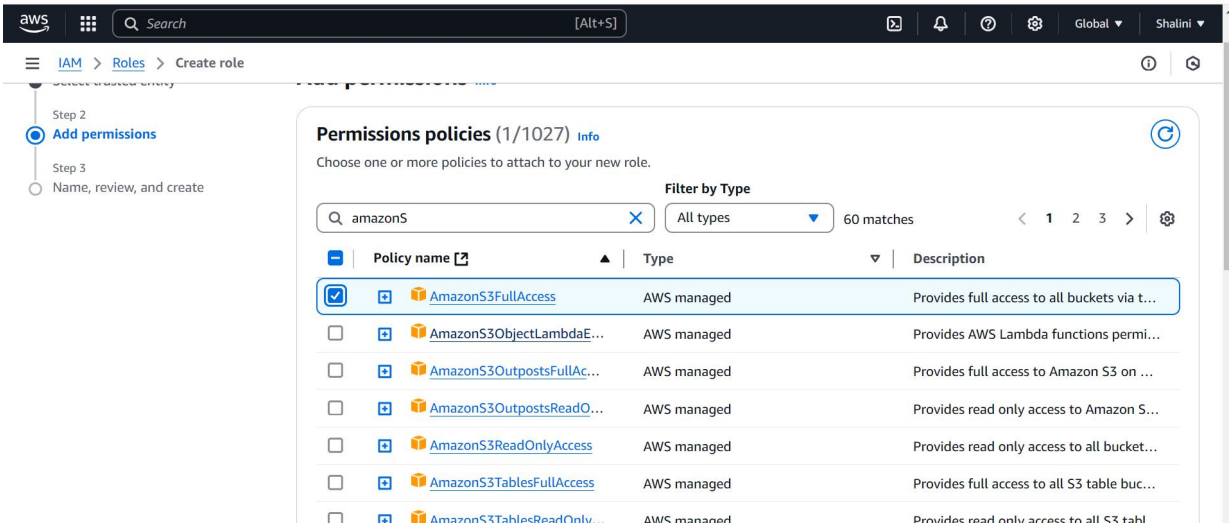
Select **AWS service** as the trusted entity.

Choose **EC2** as the use case and click **Next: Permissions**



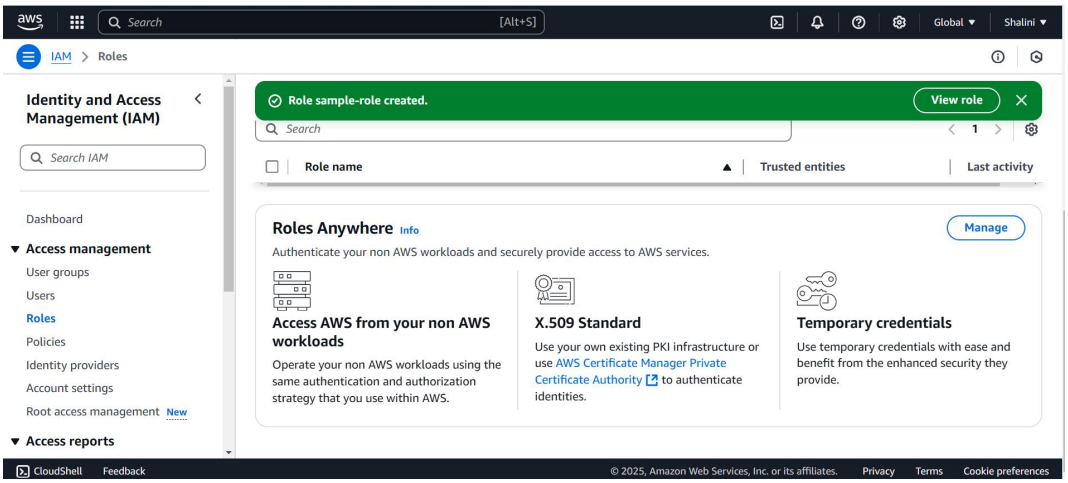
Step 3 :

Attach permissions policies:



Step 4 :

Creation of IAM Role



Expected OutcomeSS

By creating an IAM role with specific permissions (e.g., S3 access), assigning the role to your EC2 instance, and verifying its effect, you can expect the following outcomes:

1. **Secure and Controlled Access**: Your EC2 instance will have the ability to perform actions that are explicitly allowed by the IAM role, ensuring secure and controlled access to AWS resources.

2. **Successful Role Assignment**: The IAM role will be correctly attached to your EC2 instance, allowing it to inherit the permissions defined in the role.

3. **Permission Verification**: By attempting permitted actions (e.g., accessing S3) and denied actions (e.g., accessing EC2 if not permitted), you will verify that the role's permissions are correctly enforced.

4. **Enhanced Security Posture**: Implementing the principle of least privilege, your instance will have only the necessary permissions, reducing the risk of unintended access or actions.

5. **Operational Efficiency**: Automated access management via IAM roles will streamline your cloud operations, making it easier to manage and secure your resources.

In summary, you will achieve a secure, efficient, and manageable way to control access to AWS resources from your EC2 instances.