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: Joan Festina J

Department :ECE

Introduction

In AWS, Identity and Access Management (IAM) allows you to define roles and permissions that control access to your resources. With IAM roles, you can manage who can do what within your AWS account. This document will walk you through creating an IAM role, assigning it to an EC2 instance, and verifying the permissions.

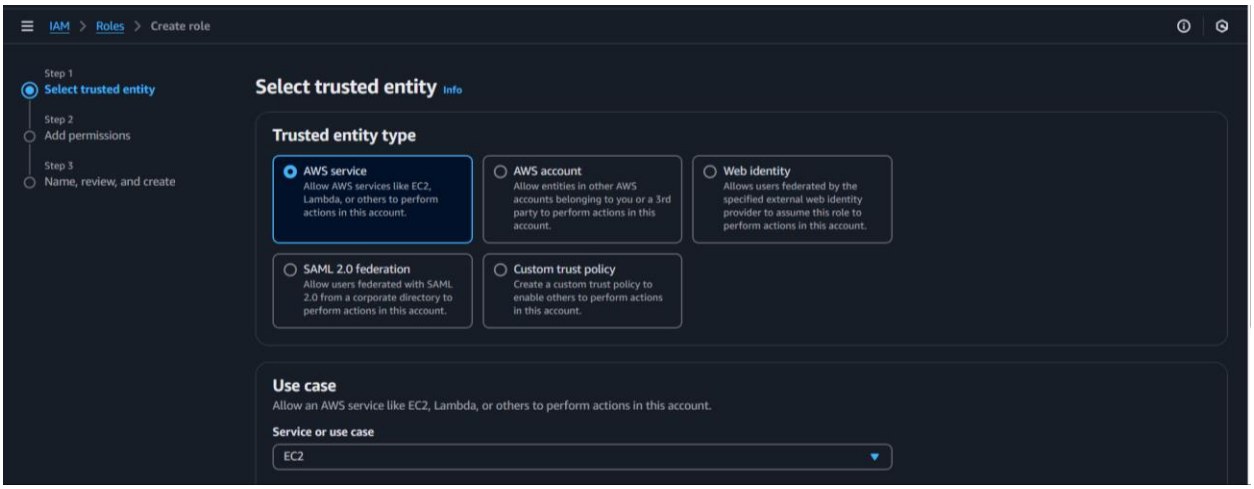
Understanding Key Concepts

- **IAM Policies** – Understanding JSON/YAML-based policy structures is essential for defining precise permissions.
- **Service Accounts** – Assigning IAM roles to a VM often involves linking it with a service account, which acts on behalf of the VM.
- **IAM Audit and Monitoring** – Regularly reviewing role assignments using audit logs and monitoring tools helps prevent misconfigurations and unauthorized access.

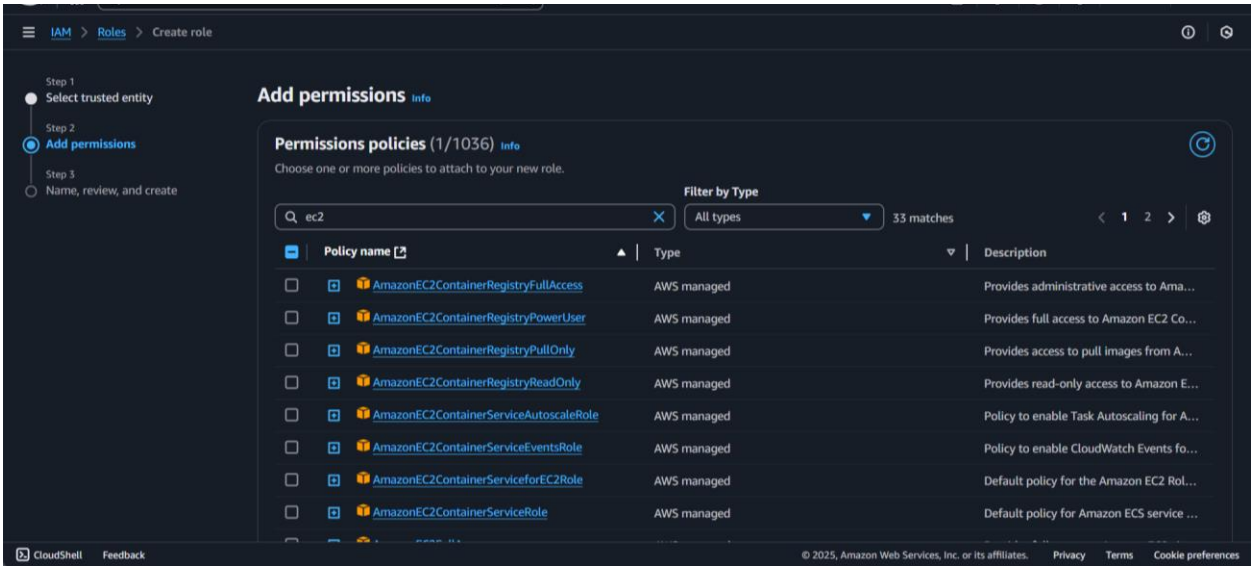
Step by Step Overview

1. Create an IAM Role

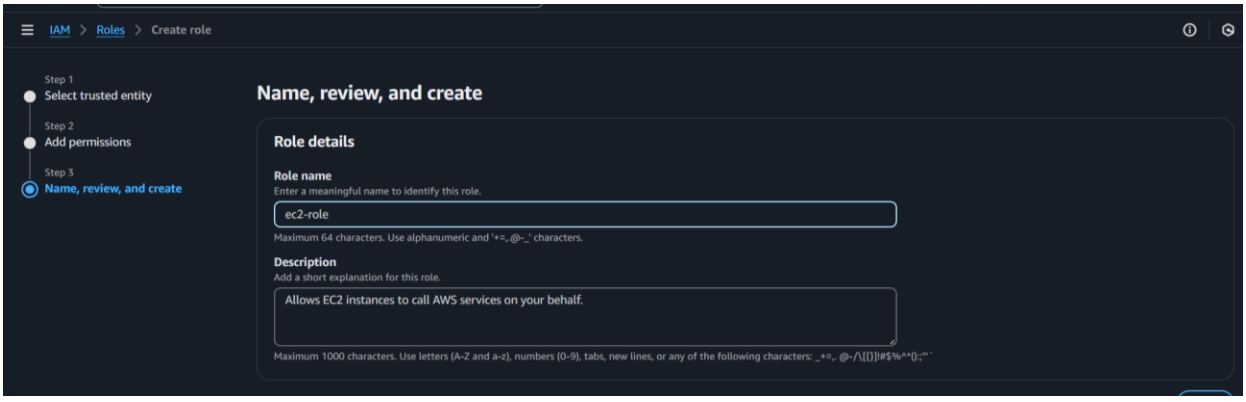
- Log in to your AWS management console.
- Search IAM service and Click on Create Role
- Choose the AWS service option. Under the use case choose "EC2".



2. Attach permissions to the role

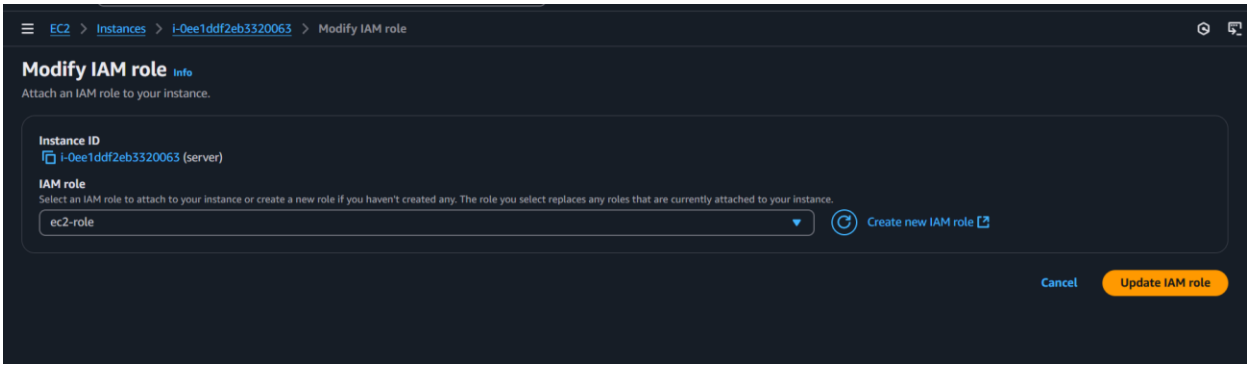


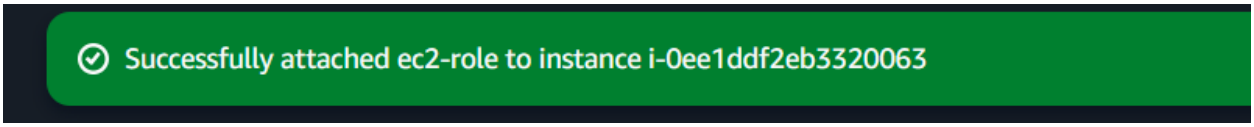
3. Name the Role



4. Attach to an EC2 instance

- Select Your EC2 Instance
- With your instance selected, click on the Actions dropdown at the top right.
- Choose Security and then select Modify IAM role.
- Select the role we previously created.





Outcome:

By following this process, you've successfully created an IAM role, assigned it to an EC2 instance, and tested the permissions to ensure it works as intended. IAM roles provide fine-grained control over access to AWS resources, ensuring your EC2 instance can only perform the actions you've authorized.