



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”.

IAM > Roles > Create role

Step 1: Select trusted entity

Select trusted entity

Trusted entity type

- ☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
EC2

2. Attach permissions to the role

IAM > Roles > Create role

Step 1: Select trusted entity

Step 2: Add permissions

Add permissions

Permissions policies (1/1036)

Choose one or more policies to attach to your new role.

Filter by Type: All types (33 matches)

Search: ec2

Policy name	Type	Description
<input type="checkbox"/> AmazonEC2ContainerRegistryFullAccess	AWS managed	Provides administrative access to Ama...
<input type="checkbox"/> AmazonEC2ContainerRegistryPowerUser	AWS managed	Provides full access to Amazon EC2 Co...
<input type="checkbox"/> AmazonEC2ContainerRegistryPullOnly	AWS managed	Provides access to pull images from A...
<input type="checkbox"/> AmazonEC2ContainerRegistryReadOnly	AWS managed	Provides read-only access to Amazon E...
<input type="checkbox"/> AmazonEC2ContainerServiceAutoscaleRole	AWS managed	Policy to enable Task Autoscaling for A...
<input type="checkbox"/> AmazonEC2ContainerServiceEventsRole	AWS managed	Policy to enable CloudWatch Events fo...
<input type="checkbox"/> AmazonEC2ContainerServiceforEC2Role	AWS managed	Default policy for the Amazon EC2 Rol...
<input type="checkbox"/> AmazonEC2ContainerServiceRole	AWS managed	Default policy for Amazon ECS service ...

CloudShell Feedback © 2015, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

3. Name the Role

IAM > Roles > Create role

Step 1: Select trusted entity

Step 2: Add permissions

Step 3: Name, review, and create

Name, review, and create

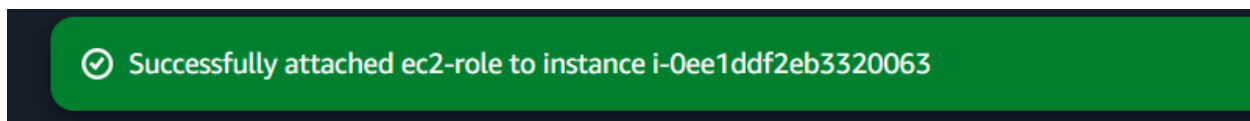
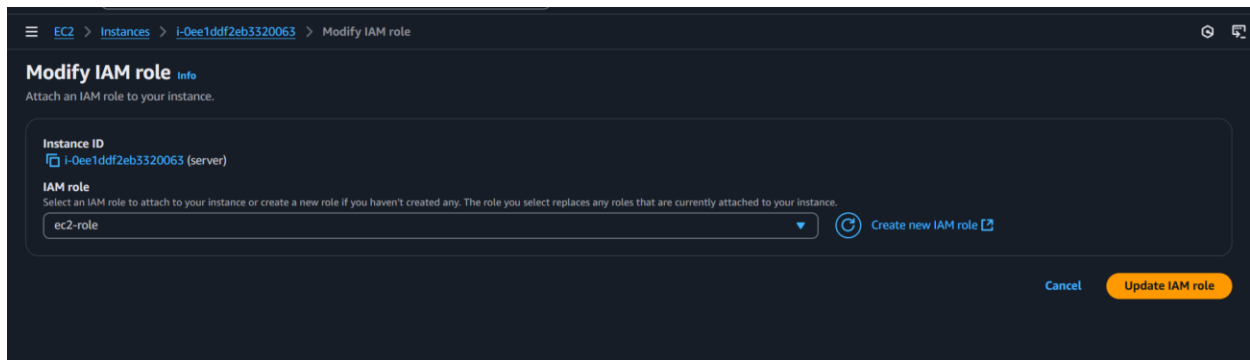
Role details

Role name
Enter a meaningful name to identify this role.
ec2-role
Maximum 64 characters. Use alphanumeric and "+,=,@,-" characters.

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use letters [A-Z and a-z], numbers [0-9], tabs, new lines, or any of the following characters: "+,=,@,-,/,/[]!#\$%^&*~'"

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.