Placement Empowerment Program

Cloud Computing and DevOps Centre

Task:

Set Up IAM Roles and PermissionsCreate an IAM role on your cloud platform. Assign the role to your VM to restrict/allow specific actions.

Name: Venkata Sai M Department:CSE

Introduction

Introduction: Setting Up IAM Roles and Permissions for Cloud VMs

In modern cloud computing environments, security and access control play a crucial role in managing resources effectively. Identity and Access Management (IAM) enables administrators to define granular permissions, ensuring that users and services have only the necessary access required to perform specific tasks.

This Proof of Concept (PoC) focuses on creating and assigning IAM roles to a Virtual Machine (VM) on a cloud platform (such as AWS, Google Cloud, or Azure). By doing so, we can restrict or allow certain actions for the VM, enhancing security while maintaining operational efficiency.

In this guide, we will:

1. Create an IAM Role with specific permissions.
2. Assign the IAM Role to a cloud VM instance.
3. Verify the Role's Effectiveness by testing access to cloud services.

By implementing IAM roles, organizations can enforce the principle of least privilege, ensuring that VMs only have the necessary permissions required for their tasks, reducing the risk of unauthorized access or data exposure.

Let me know if you need further refinements! 🚀

Overview

This Proof of Concept (PoC) demonstrates how to create and assign IAM roles to a cloud VM to control access and permissions securely. By implementing IAM roles, we ensure the VM has the least privilege required to interact with cloud services. The process includes creating a role, attaching policies, assigning it to the VM, and verifying access. This enhances security by restricting unauthorized actions while enabling necessary operations. 🚀

Key Steps Involved:

Step 1: Create an IAM Role

Step 2: Attach Policies to the IAM Role

Step 3: Assign the IAM Role to the VM

Step 4: Verify Role Permissions

Objectives

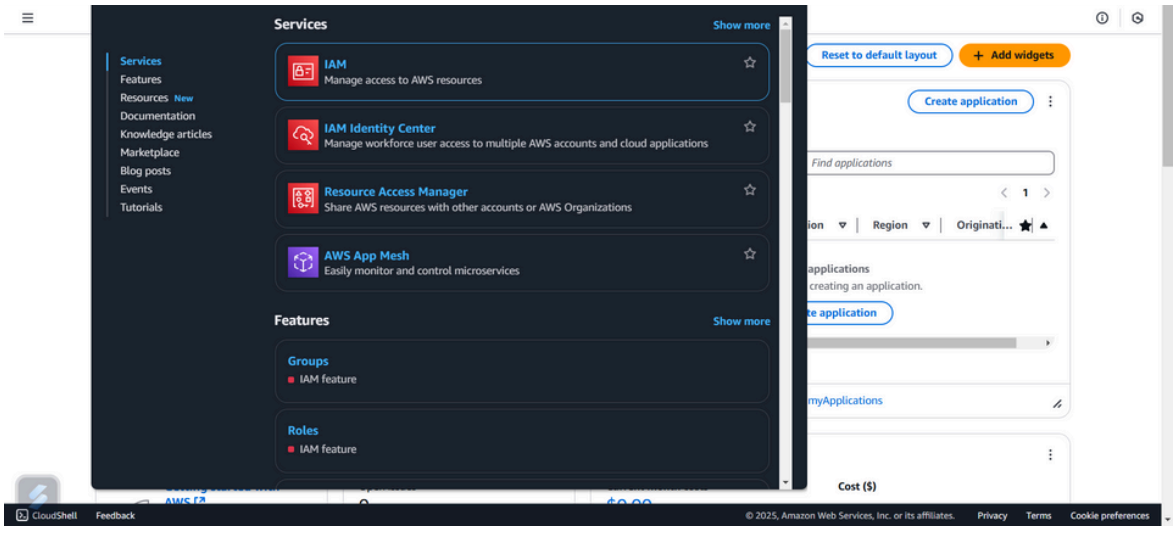
- Implement Secure Access Control – Establish IAM roles to manage and restrict access to cloud resources, ensuring only authorized actions are allowed.
- Enforce Least Privilege Principle – Grant the VM only the necessary permissions required for its tasks, reducing security risks.
- Streamline Role-Based Access Management – Simplify permission management by using IAM roles instead of hardcoded credentials within the VM.
- Enhance Cloud Security and Compliance – Prevent unauthorized access and maintain compliance with security best practices by using IAM policies.
- Validate Role Functionality – Test and verify that the assigned IAM role allows or restricts access as intended by executing relevant commands from the VM.

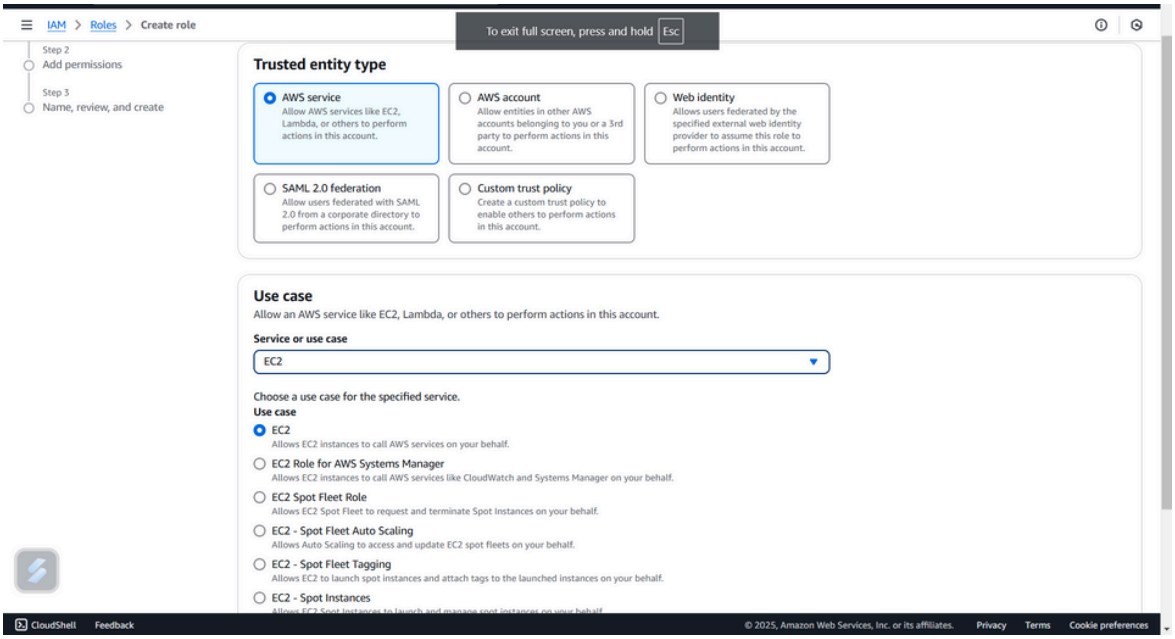
Step-by-Step Overview

Step 1:

Navigate to the AWS Managment Console

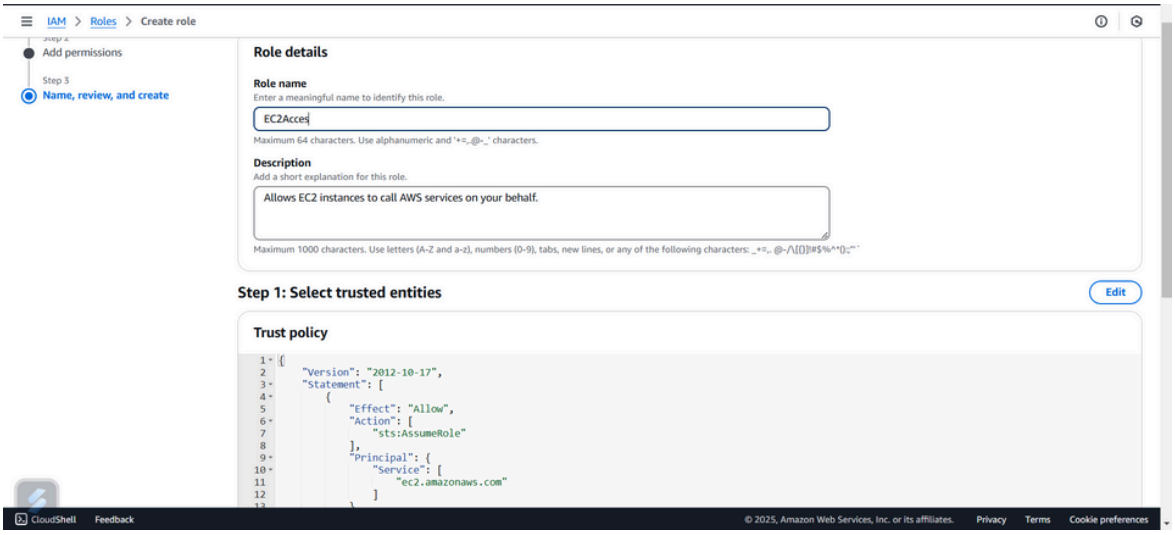
In a Managment Console open IAM in the left side
navigate to the roles

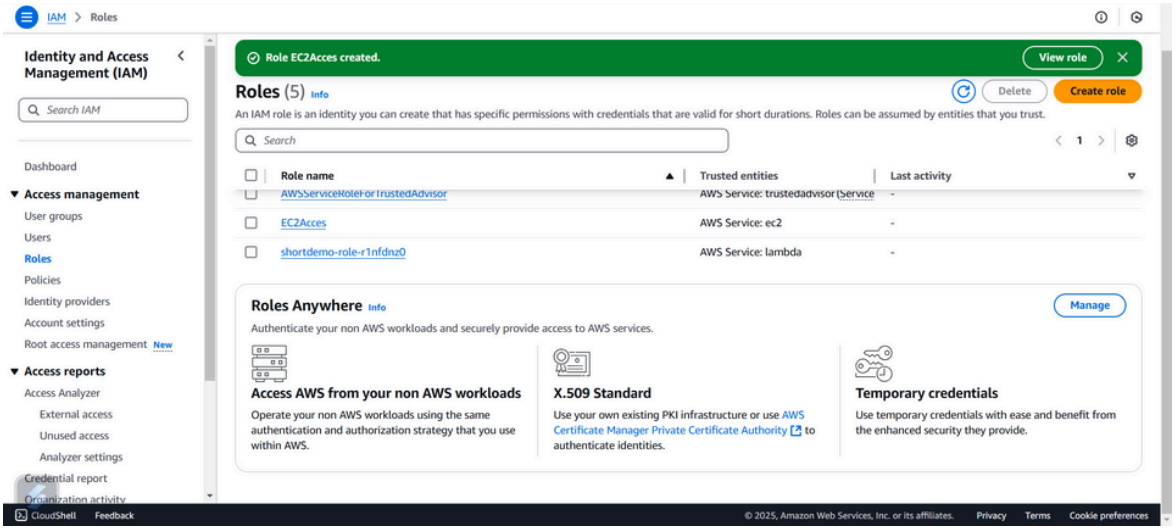




Step 2:

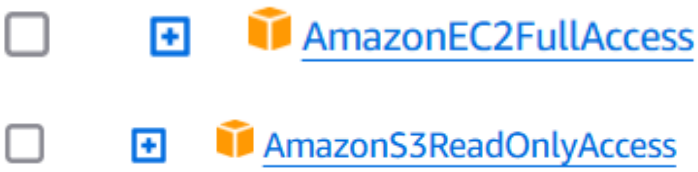
Navigate to the roles enter the role name and give access to the EC2 and create the role

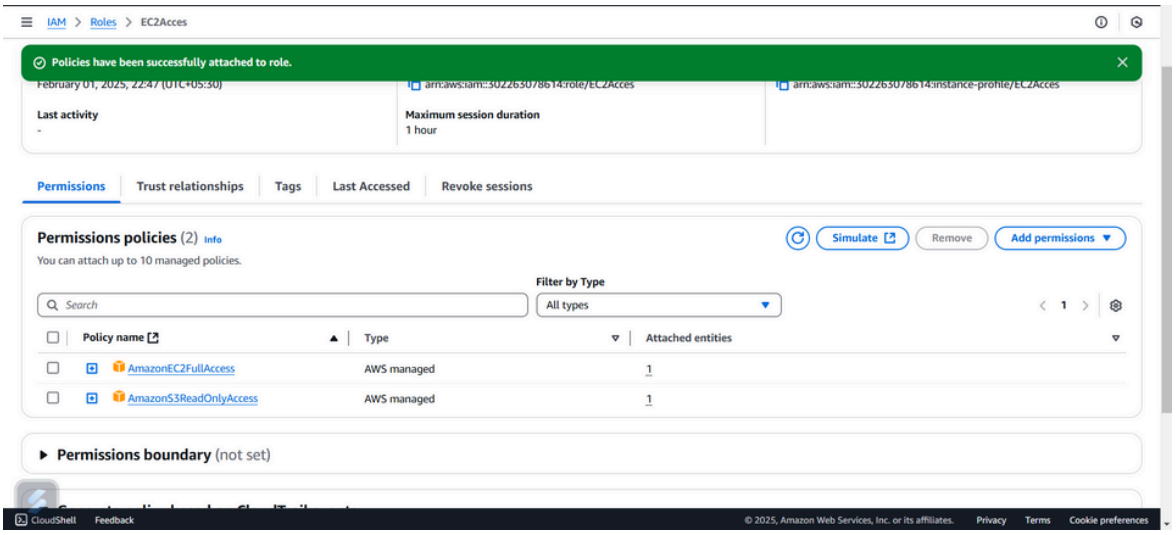




Step 3:

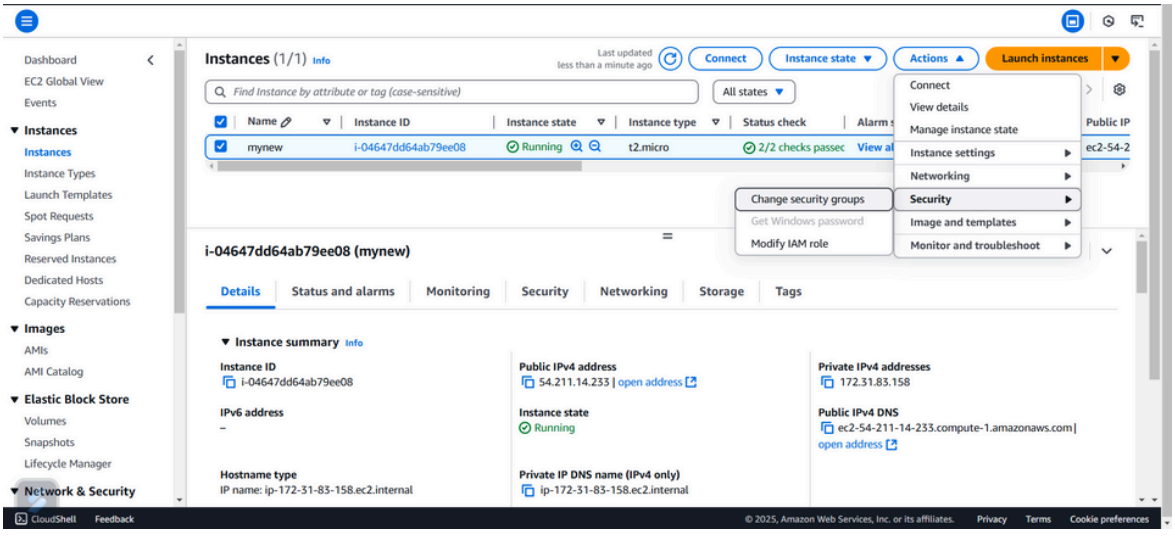
Open the created role and give access the given policy





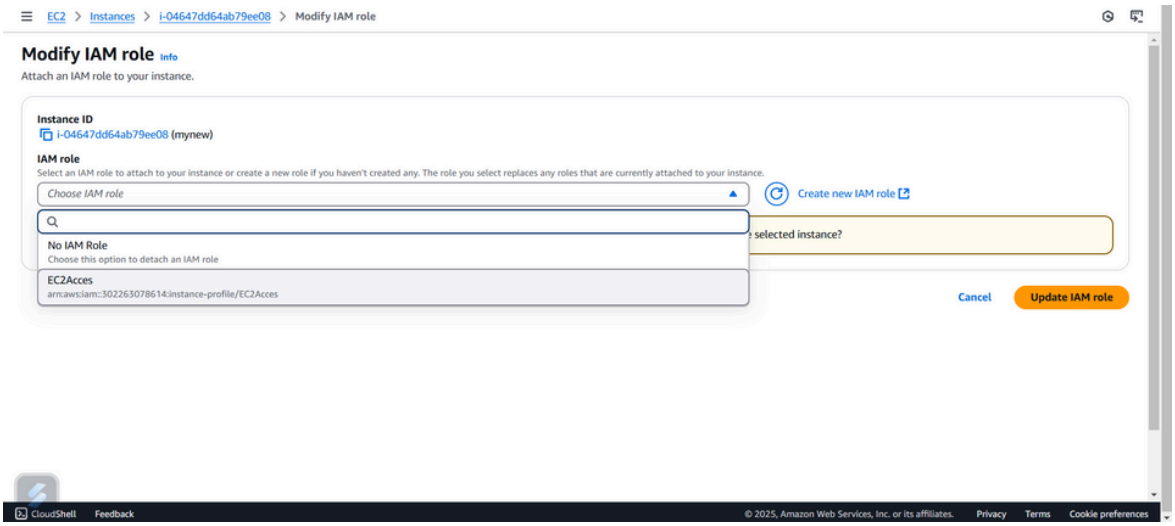
Step 4:

In this step first simply lauch an ec2 instance and click the tick mark on the created instances.Then click on the action open security the click modify IAM role

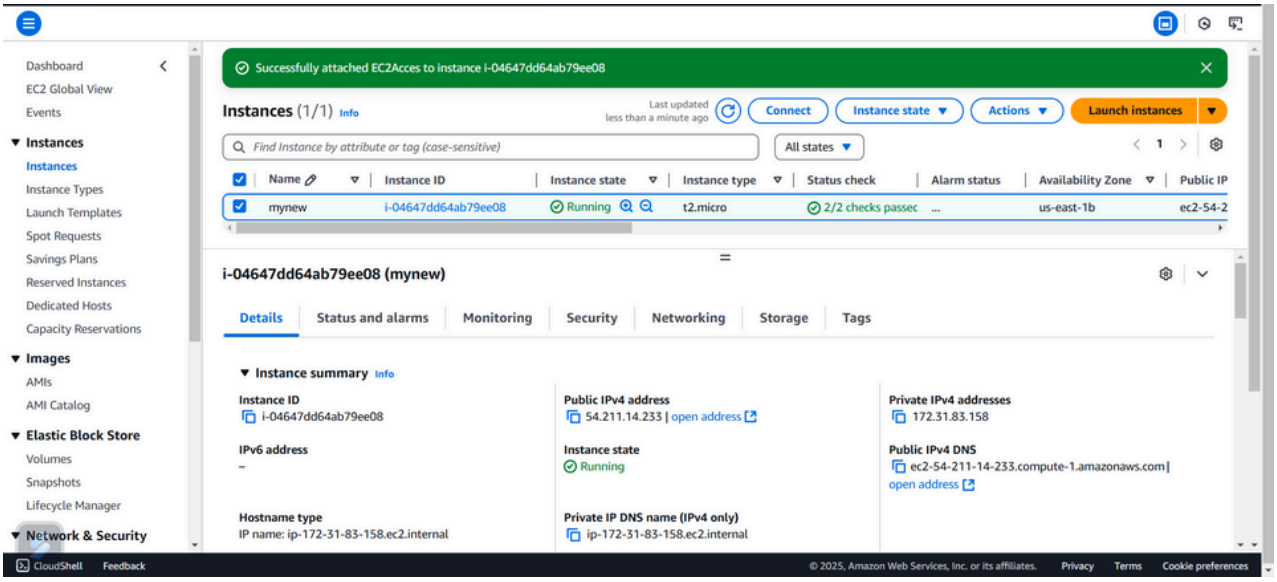


Step 5:

Then finally choose the IAM role which have been created so far.



Then click on the update IAM role



Expected Outcomes:

Expected Outcomes for This Proof of Concept (PoC)

1. Successful IAM Role Creation – An IAM role with the necessary permissions is created and available for assignment.
2. Role Assigned to the VM – The IAM role is successfully attached to the cloud VM instance without using static credentials.
3. Controlled Access to Cloud Services – The VM is able to perform only the permitted actions (e.g., accessing specific cloud storage, databases, or APIs) based on assigned policies.
4. Prevention of Unauthorized Actions – Attempts to perform actions outside the defined role permissions result in access denied errors, confirming security enforcement.
5. Improved Security & Compliance – The setup adheres to the principle of least privilege, reducing risks of unauthorized access and security breaches.
6. Verification and Testing Success – Running test commands from the VM confirms that access permissions function as expected.

By achieving these outcomes, the PoC ensures secure, role-based access control for cloud VMs, enhancing security and operational efficiency. 🚀