 

**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 action

Name :S.KRITHIKA Department: ADS



**Introduction and Overview**

In cloud computing, Identity and Access Management (IAM) plays a crucial role in securing resources by controlling who can perform specific actions. IAM roles define permissions and grant controlled access to resources, ensuring security and compliance. This document provides a step-by-step guide to creating an IAM role, assigning it to a virtual machine (VM), and restricting or allowing specific actions.

**Objective**

The primary objective of this guide is to:

* Understand IAM roles and permissions.
* Create an IAM role on a cloud platform.
* Assign the role to a VM.
* Define permissions to restrict or allow specific actions.
* Enhance security and operational efficiency.

**Importance of Local Hosting**

Local hosting of services and applications in a controlled environment ensures:

* **Better security**: Fine-grained access control prevents unauthorized access.
* **Performance efficiency**: Direct control over resources optimizes performance.
* **Compliance**: Ensures adherence to industry regulations and policies.
* **Cost management**: Controlled resource allocation helps in cost efficiency.

**Step-by-Step Overview**

**Step 1: Create an IAM Role**

1. **Navigate to IAM Console**: Log into your cloud platform (e.g., AWS, GCP, or Azure) and go to the IAM service.
2. **Create a new role**:
   * AWS: Choose "Create Role" > Select "EC2 Service" > Attach policies.
   * GCP: Go to "IAM & Admin" > "Roles" > "Create Role".
   * Azure: Navigate to "Roles" > "Add a custom role".
3. **Define Permissions**: Add specific policies that restrict or allow actions like Start/Stop VM, Read-Only Access, or Full Admin.

**Step 2: Assign the Role to a Virtual Machine**

1. **Select the Virtual Machine**:
   * AWS: Navigate to EC2, choose your VM, and modify IAM role settings.
   * GCP: Go to Compute Engine, select the VM, and modify permissions.
   * Azure: Assign the role in the "Access Control (IAM)" section of the VM.
2. **Attach the IAM Role**: Ensure that the selected role is applied to enforce access policies.

**Step 3: Verify Permissions**

1. **Test Restricted Actions**: Try performing actions that should be blocked and ensure they are denied.
2. **Test Allowed Actions**: Perform permitted operations to verify correct access.
3. **Monitor IAM Logs**: Check activity logs for any unauthorized access attempts.

**Expected Outcome**

* A properly configured IAM role with specific permissions.
* The assigned VM follows defined access controls.
* Improved security and controlled access management.
* Compliance with best security practices.