 

**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: MIRDULA C Department: ADS



**Introduction**

### Identity and Access Management (IAM) is a critical component of cloud security that allows administrators to control who can access cloud resources and what actions they can perform. By creating IAM roles and assigning them to cloud resources like Virtual Machines (VMs), organizations can enforce security best practices, minimize risks, and ensure that applications and users have the right level of access.

### In this guide, we will create an IAM role on a cloud platform (AWS IAM), assign the role to a VM (AWS EC2), and configure permissions to allow or restrict specific actions.

### ****Overview****

### This tutorial covers the following steps:

### Create an IAM role with specific permissions.

### Assign the IAM role to a Virtual Machine (EC2 instance).

### Test the permissions by running commands with the assigned role.

### Modify and fine-tune permissions as needed for security.

### By setting up IAM roles correctly, we can ensure secure and controlled access to cloud resources without exposing sensitive credentials.

### **Objectives**

* Learn how to create an IAM role with appropriate permissions.
* Assign the IAM role to an AWS EC2 instance.
* Restrict or allow specific actions based on role policies.
* Improve security and access control for cloud resources.

**Importance**

✅ **Enhanced Security** – Reduces the risk of unauthorized access.  
✅ **Least Privilege Access** – Ensures only required permissions are granted.  
✅ **Credential-Free Access** – No need to store access keys on VMs.  
✅ **Scalability** – Easily assign roles to multiple resources without managing individual user permissions.

**Step-by-Step Overview**

**Step 1: Create an IAM Role**

1. Log in to AWS Console → Navigate to IAM.
2. Click Roles → Create Role.
3. Under Trusted Entity, select AWS Service → Choose EC2.
4. Click Next to add permissions:
   * Choose an AWS Managed Policy (e.g., AmazonS3ReadOnlyAccess for read-only S3 access).
   * Or create a Custom Policy for specific access.
5. Name the role (e.g., EC2-S3-Access-Role) and click Create Role.

**Step 2: Assign the IAM Role to a Virtual Machine (EC2 Instance)**

1. Navigate to the EC2 Dashboard.
2. Select the instance to which you want to assign the IAM role.
3. Click Actions → Security → Modify IAM Role.
4. Select the IAM role (EC2-S3-Access-Role) and attach it to the instance.
5. Click Update IAM Role to apply changes.

**Step 3: Test IAM Role Permissions on the VM**

1. Connect to the EC2 instance using SSH
2. Test permissions (if role has S3 access)
   1. If you see a list of S3 buckets, the role has the correct permissions.
   2. If you get an Access Denied error, check the IAM policy.

**Step 4: Modify IAM Role Permissions (Optional)**

1. Go to IAM Console → Roles → Select EC2-S3-Access-Role.
2. Click Permissions → Attach policies or edit inline policy.
3. To allow full access to S3, modify the policy
4. Save changes and re-test access from the VM.

**Outcome**

After completing this setup, you will have:  
✅ An IAM role created with custom permissions.  
✅ The IAM role assigned to a cloud VM (EC2).  
✅ Controlled access to cloud resources without exposing credentials.  
✅ A more secure cloud environment with restricted access.