St. JOSEPH'S GROUP OF INSTITUTIONS
OMR, CHENNAI - 119

PLACEMENT EMPOWERMENT PROGRAM

CLOUD COMPUTING AND DEVOPS CENTRE

TASK 10 - 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 - MAHASHREE U

DEPT - ADS

Introduction

Identity and Access Management (IAM) is a critical component of modern cloud security. IAM enables organizations to manage access to cloud resources by defining who can do what under specific conditions. In this task, you'll create an IAM role, assign permissions to the role, and associate it with a Virtual Machine (VM). This ensures the VM only performs specific actions, reducing security risks and maintaining compliance.

Objectives

1. Understand IAM roles and their application in managing access to cloud resources.
2. Create an IAM role with specific permissions on your cloud platform (e.g., AWS, Azure, or GCP).
3. Attach the role to a Virtual Machine to control its access to other resources.
4. Test and verify the role's permissions by performing actions from the VM.

Importance of IAM Roles and Permissions

1. **Security**: Restricts access to sensitive resources, reducing the risk of unauthorized access or accidental changes.
2. **Granular Control**: Provides fine-grained access control by allowing or denying specific actions at a resource level.
3. **Compliance**: Helps organizations meet regulatory requirements by limiting access to resources based on job roles.
4. **Scalability**: Easily manage permissions for multiple VMs and resources by attaching or modifying roles without reconfiguring individual VMs.
5. **Operational Efficiency**: Automates access management, reducing manual intervention and the risk of errors.
6.

Outcomes

1. **Role Created**: Successfully define an IAM role with specific permissions.
2. **Permissions Applied**: Restrict/allow VM actions based on the role.
3. **Enhanced Security**: Ensure only authorized actions are performed by the VM.
4. **Improved Compliance**: Demonstrate fine-grained access control for audit purposes.
5. **Operational Insight**: Gain visibility into the VM’s activities through monitoring and logs.

This setup ensures robust access control for your VMs, aligning security and functionality with your organization's needs. Let me know if you'd like a specific example for AWS, Azure, or GCP!

Step by step Process

Steps to Set Up IAM Roles for Virtual Machines in Azure

Step 1: Enable a Managed Identity for the VM

A **Managed Identity** allows Azure VMs to authenticate to Azure services without storing credentials.

Go to the Azure Portal:

- Open the Azure Portal.

Navigate to Your VM:

- Go to **Virtual Machines** and select the VM you want to configure.

Enable Managed Identity:

- In the left menu, select **Identity**.
- Under the **System assigned** tab, toggle the status to **On**.
- Click **Save**. A managed identity is now assigned to your VM.

Step 2: Assign a Role to the Managed Identity

You can assign a role to the VM's managed identity to grant specific permissions.

1. **Go to Access Control (IAM):**
   - Still on the VM page, select **Access Control (IAM)** from the left menu.
2. **Add a Role Assignment:**
   - Click **+ Add** > **Add role assignment**.
   - Select a role that matches the permissions needed.

3.**Assign the Role to the Managed Identity:**

- Under the **Members** tab, select **Managed Identity**.
- Search for your VM's managed identity and select it.
- Click **Review + Assign** to complete the process.

Step 3: Test the Role Assignment

Log in to the VM:

- Use SSH or RDP to connect to your VM.

Log in with the Managed Identity:

- Run the following command to authenticate the VM using its managed identity

Step 4

Test Unauthorized Actions:

- Attempt an action not covered by the assigned role to confirm access is restricted.

Test Unauthorized Actions:

- Attempt an action not covered by the assigned role to confirm access is restricted.

Outcomes

1. **Managed Identity Configured:** The VM can securely access Azure resources without credentials.
2. **Role Assignment Applied:** Permissions are granted to the VM based on the selected role.
3. **Enhanced Security:** No hardcoded credentials are used, reducing the attack surface.
4. **Principle of Least Privilege:** The VM has only the access it needs to perform its tasks.
5. **Auditable Activity:** All actions are logged, ensuring transparency and compliance.