

**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: Aksha S Department : CSE

**Introduction and Overview**

Identity and Access Management (IAM) roles and permissions are critical components of cloud security. IAM allows administrators to define who can access specific cloud resources and what actions they can perform. By creating and assigning IAM roles, you can control the level of access that users, applications, or services have over your cloud infrastructure, ensuring the principle of least privilege is followed.

In this exercise, you will learn how to set up IAM roles on a cloud platform, such as **Microsoft Azure**, to restrict or allow specific actions for users or virtual machines (VMs). By assigning these roles to your VM, you can control the permissions granted to the machine or its users, ensuring that only authorized actions are performed.

This is an essential skill for securing cloud environments, particularly as cloud infrastructure becomes increasingly complex and integrated with various services.

**Objective**

The primary objectives of this task are:

1. To understand how IAM roles and permissions work within a cloud environment.
2. To create a custom IAM role on Azure (or any other cloud platform) for controlling access.
3. To assign the IAM role to a Virtual Machine (VM) to restrict or allow specific actions.
4. To ensure that users or VMs have only the permissions they need to perform their tasks, following the least privilege principle.
5. To gain practical experience with managing roles and access permissions within a cloud platform.

**Importance**

The importance of this task lies in:

* Cloud Security: Setting up IAM roles and permissions is crucial for securing cloud resources and ensuring that only authorized individuals and systems can perform certain actions.
* Access Control: Proper access management reduces the risk of unauthorized access, accidental data exposure, and security vulnerabilities in your cloud environment.
* Regulatory Compliance: Many industries have compliance requirements (e.g., GDPR, HIPAA) that demand precise access controls. IAM roles help meet these requirements.
* Scalability and Flexibility: By assigning granular permissions to roles, organizations can scale their security policies efficiently and manage complex cloud environments without giving unnecessary access to users or systems.
* Cost Management: Limiting access to only what’s necessary helps prevent misuse of cloud resources, potentially reducing costs associated with over-provisioning *or mismanagement.*

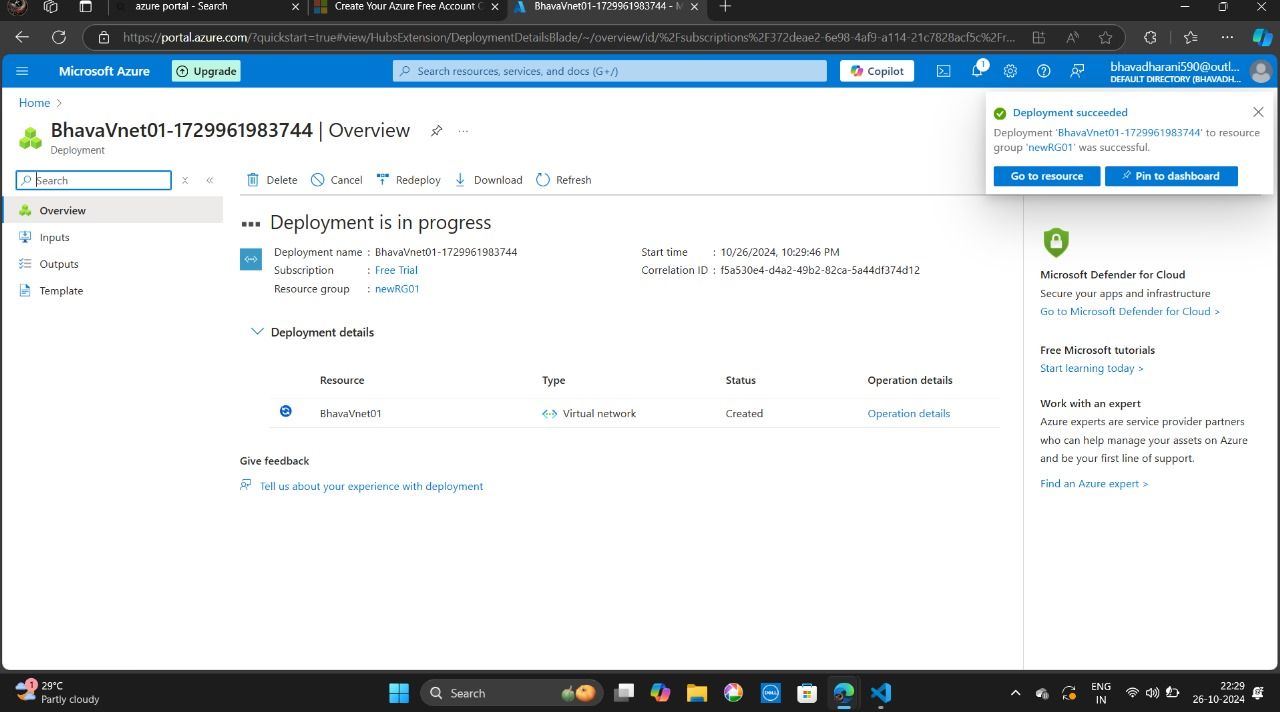
**Step-by-Step Overview**

STEP 1:

LOGIN TO THE AZURE PORTAL.

STEP 2:

Navigate to your virtual machine that your created



In your virtual machine search for security >>identity.

A white background with black text

Description automatically generated

STEP 3:

Enable system assigned option “on”.

A screenshot of a computer

Description automatically generated

STEP 4:

Now search for Access control IAM.

A white background with black text

Description automatically generated

STEP 5:

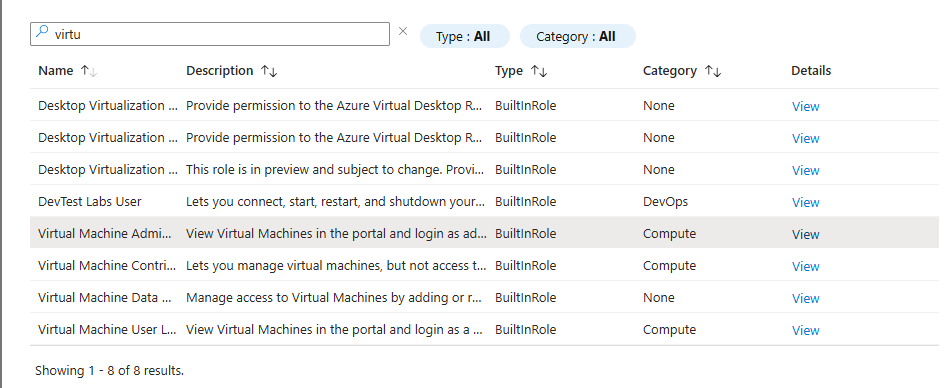
Click on add to add role assignment.

A screenshot of a computer

Description automatically generated

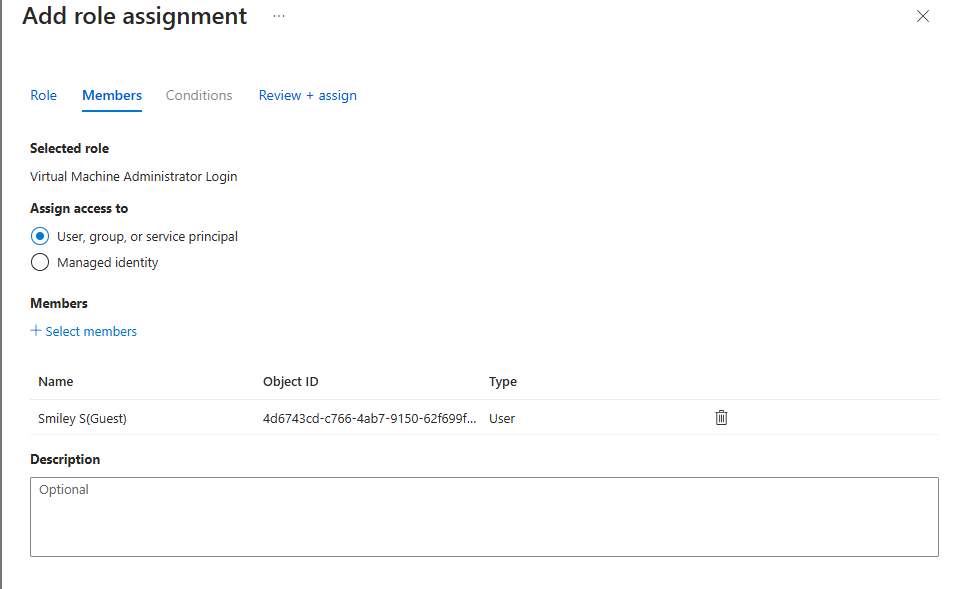
STEP 6:

Choose the roles according to your need .



STEP 7:

Go to members option there your configure your role assignments and their works in description part.



STEP 8:

Once you done go to “role assignments” and can check that the role is assigned or not.