

## 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: Keshika D

Department:ADS

# INTRODUCTION:

## Introduction to Setting Up IAM Roles and Permissions in Azure

In cloud environments, managing access control is crucial for security and efficient resource management. In this task, we set up IAM (Identity and Access Management) roles and permissions in Microsoft Azure to control access to a Virtual Machine (VM). By assigning a built-in role to a user, group, or service principal, we define the specific actions they can perform on the VM. This ensures that only authorized users have the necessary permissions while maintaining security and compliance.

### OBJECTIVE:

Understand the concept of IAM roles and permissions in Azure.

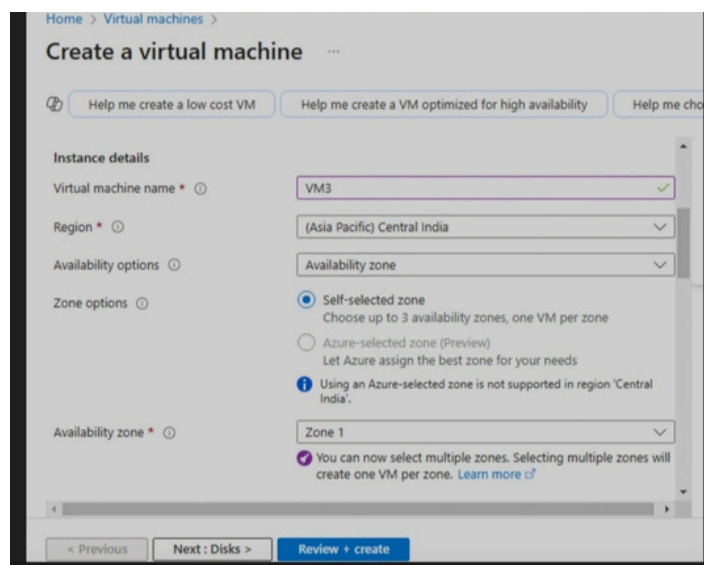
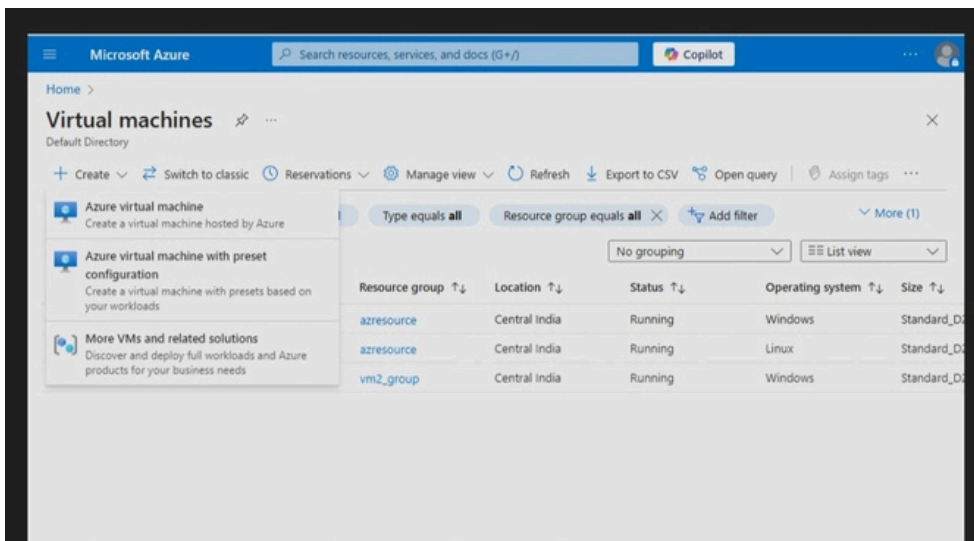
Assign a built-in IAM role to control access to a Virtual Machine (VM).

Configure role-based access at the subscription, resource group, or VM level.

Verify and test the assigned role to ensure proper access control.

Review and secure access by checking role assignments and monitoring logs.

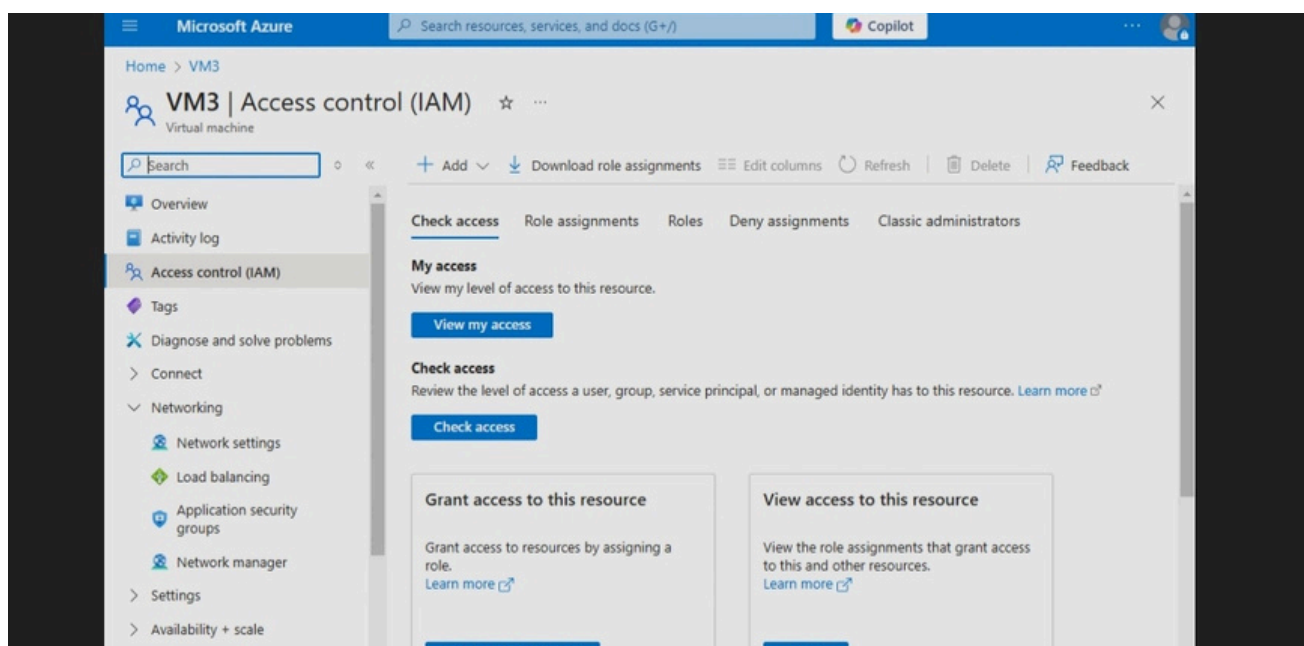
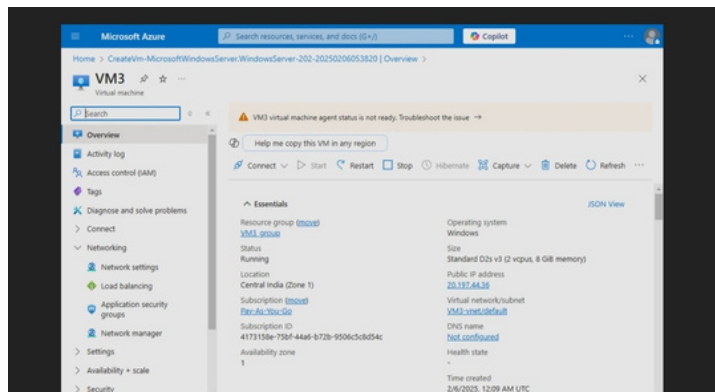
## Step 1: Set Up An Azure Vm



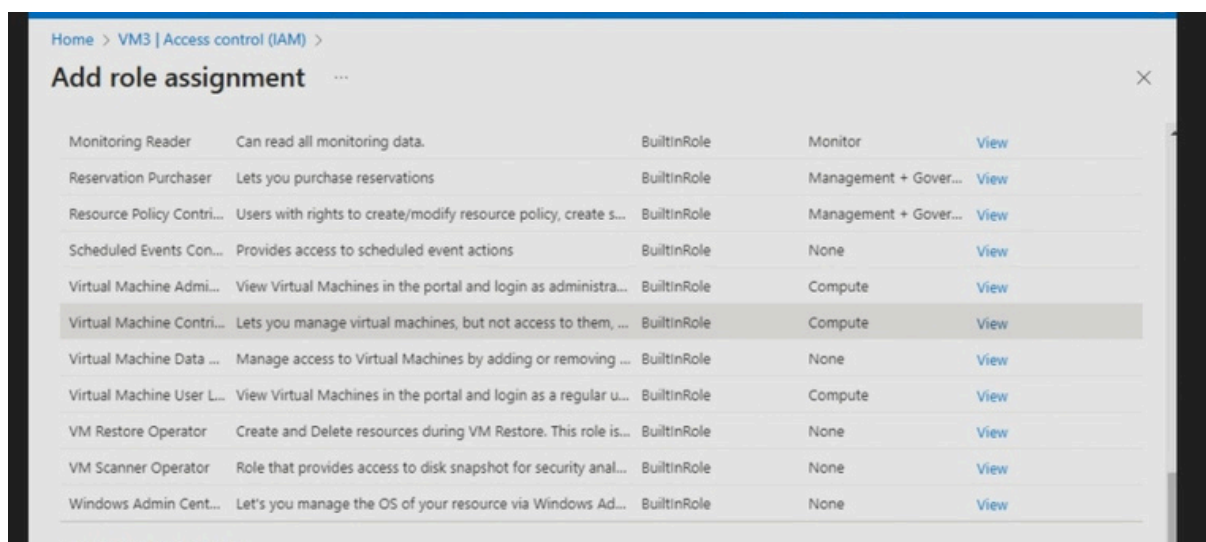
Create a VM with the following configuration and give review +create at the end

# Step2:

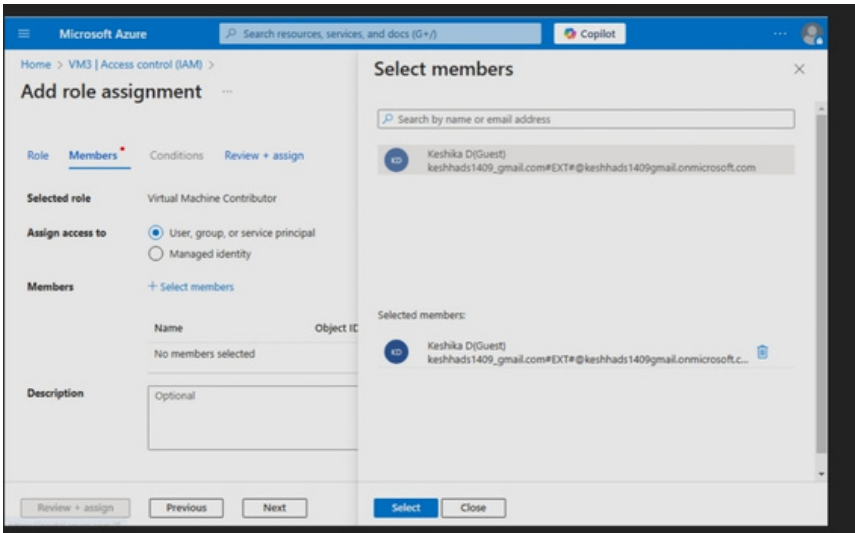
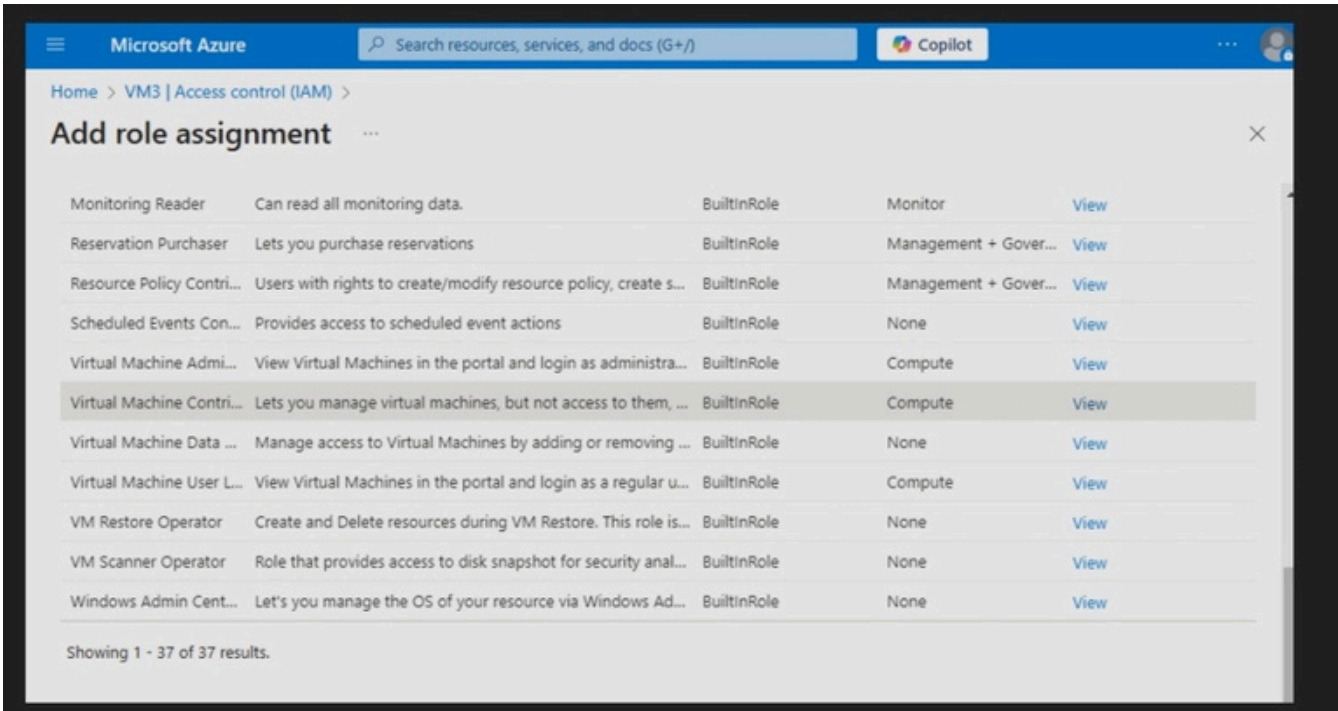
Navigate to Access Control (IAM): Went to the relevant resource (VM, Subscription, or Resource Group) and opened the Access Control (IAM) settings.



Assign Built-In Role: Selected a built-in IAM role (e.g., Virtual Machine Contributor, Reader) and assigned it to the appropriate user or group.



Verify Role Assignment: Ensured the correct role was applied and tested the permissions to check access.



**Review and Secure Access: Checked the VM's network security settings and optionally reviewed logs for monitoring access activities.**

