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: Harshana Perianayaki B Department : IT

INTRODUCTION

Identity and Access Management (IAM) in **Microsoft Azure** ensures that users and services have **appropriate permissions** to access resources securely. Azure uses **Role-Based Access Control (RBAC)** to manage these permissions effectively. By assigning IAM roles to a **Virtual Machine (VM)**, you can restrict or allow specific actions, ensuring a **least privilege access model** for enhanced security.

OVERVIEW

When deploying a VM in Azure, it often requires access to other services, such as **Azure Storage, Databases, or APIs**. Instead of using static credentials, Azure provides **Managed Identities** and **RBAC roles**, which allow you to securely control what actions the VM can perform. This process includes:

1. **Creating an IAM role** (Managed Identity or Custom Role).
2. **Assigning the role to the VM**.
3. **Defining permissions** to restrict/allow specific actions.
4. **Verifying the role assignment and access permissions**.

OBJECTIVES

- Understand how IAM roles function in **Azure Role-Based Access Control (RBAC)**.
- Learn how to **create and assign IAM roles** to a Virtual Machine.
- Implement **least privilege access** to improve security.
- Ensure the VM can access necessary resources without exposing **sensitive credentials**.

IMPORTANCE

✅ **Security** – Prevents unauthorized access to resources.

✅ **Access Control** – Grants only the necessary permissions for VM operations.

✅ **Scalability** – Enables easy role management for multiple VMs.

✅ **Compliance** – Helps meet industry security standards (e.g., ISO, NIST, GDPR).

✅ **Automation** – Reduces manual effort in managing credentials.

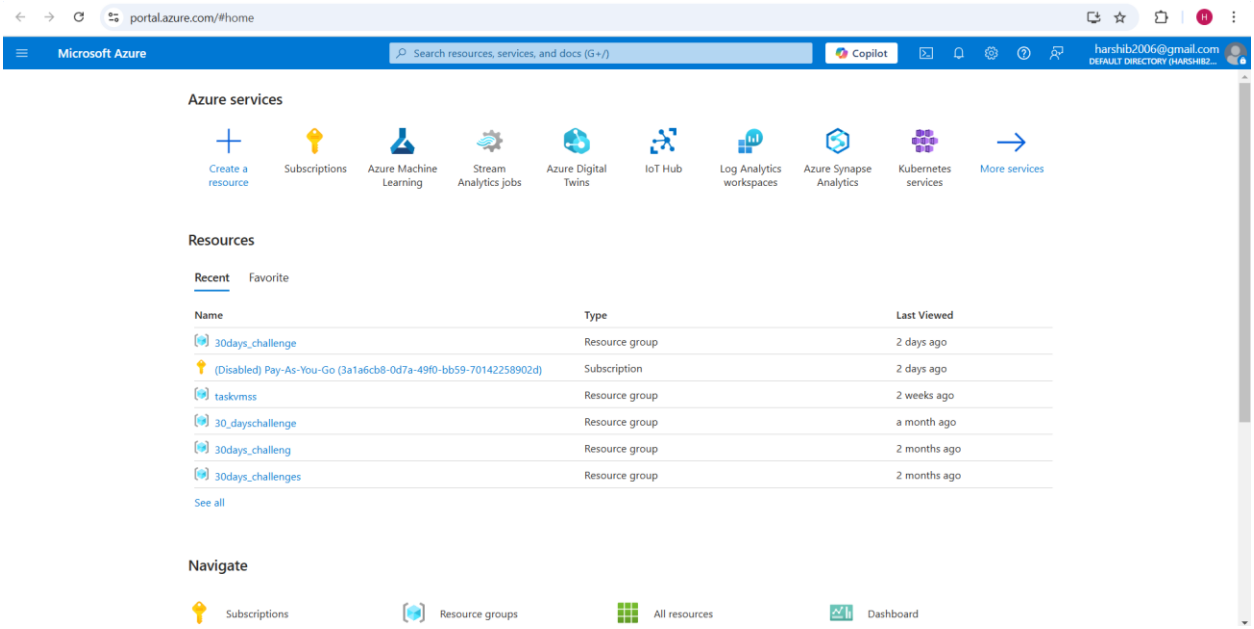
STEP-BY-STEP OVERVIEW

In **Microsoft Azure**, **Identity and Access Management (IAM)** is managed through **Azure Role-Based Access Control (RBAC)**. To set up IAM roles and permissions for a **Virtual Machine (VM)**, follow these steps:

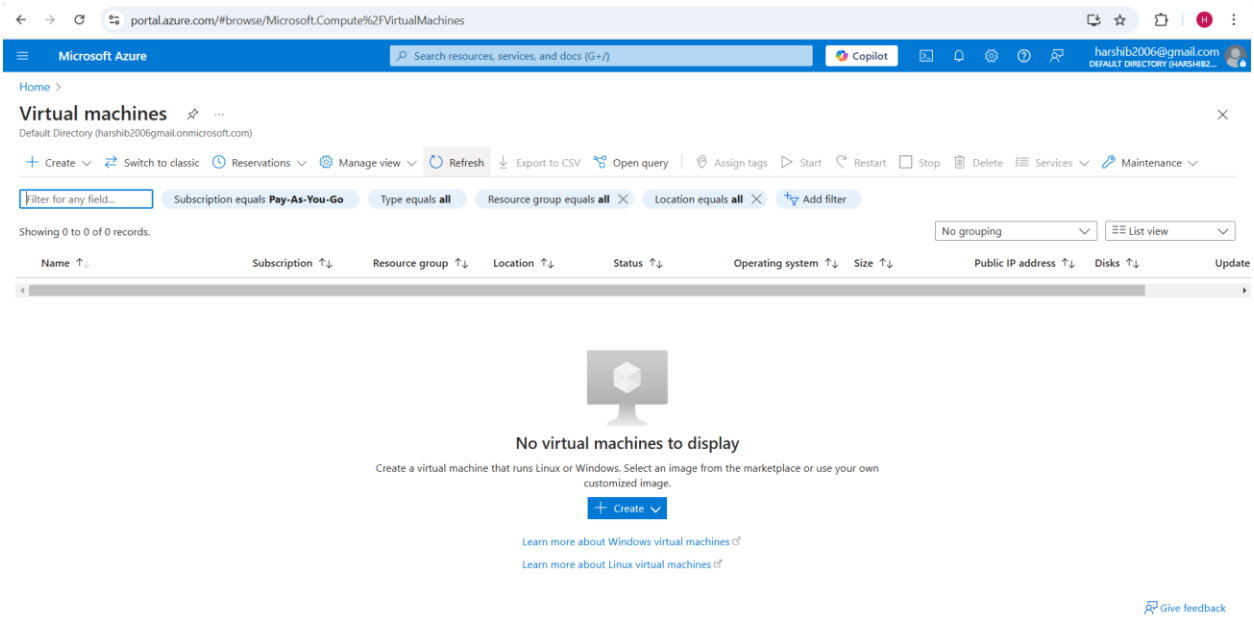
Step 1 : Create an IAM role (Managed Identity)

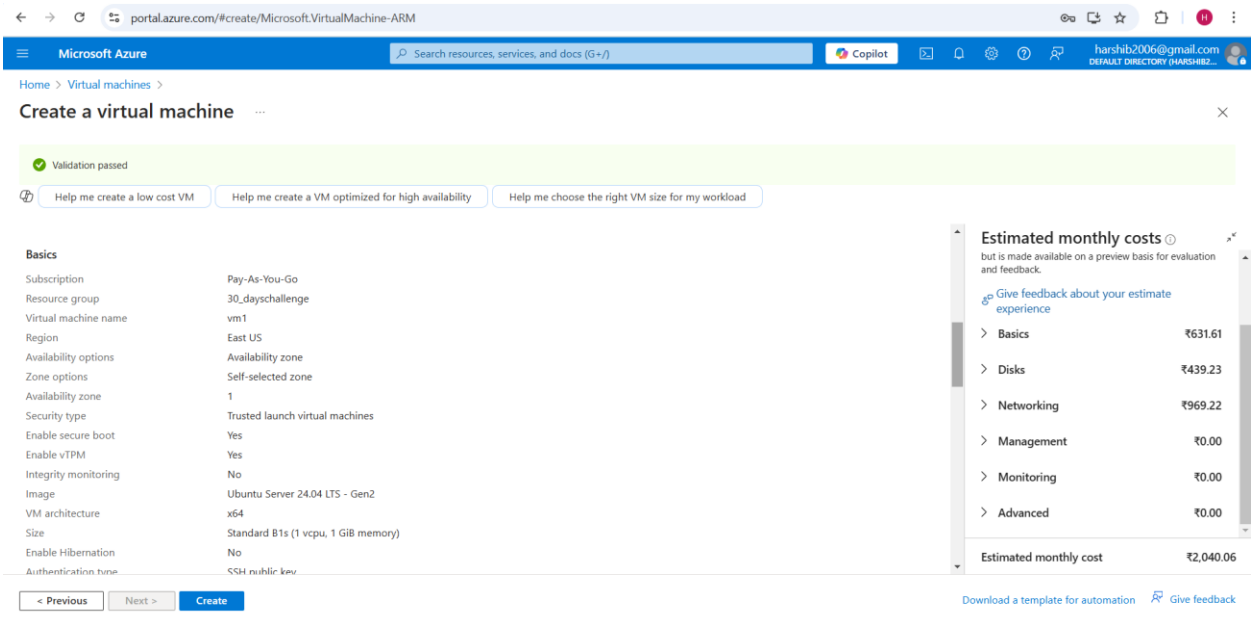
In Azure, an IAM role is typically created using a **Managed Identity** (either system-assigned or user-assigned). This allows the VM to authenticate and access resources securely.

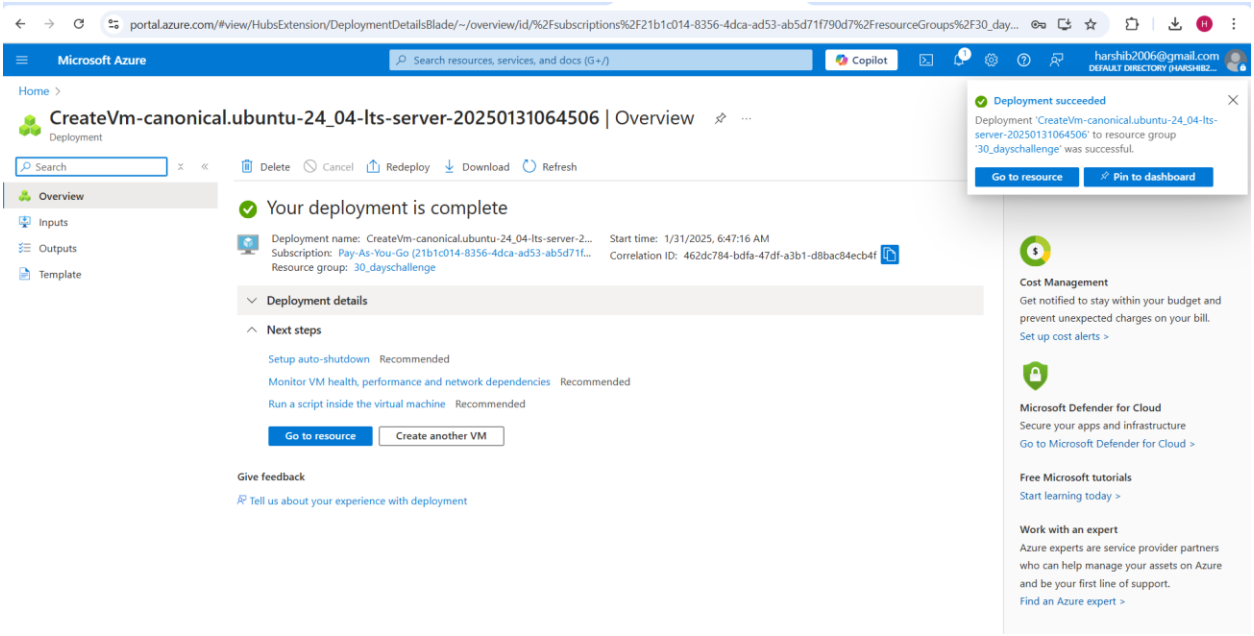
1. **Go to Azure Portal**

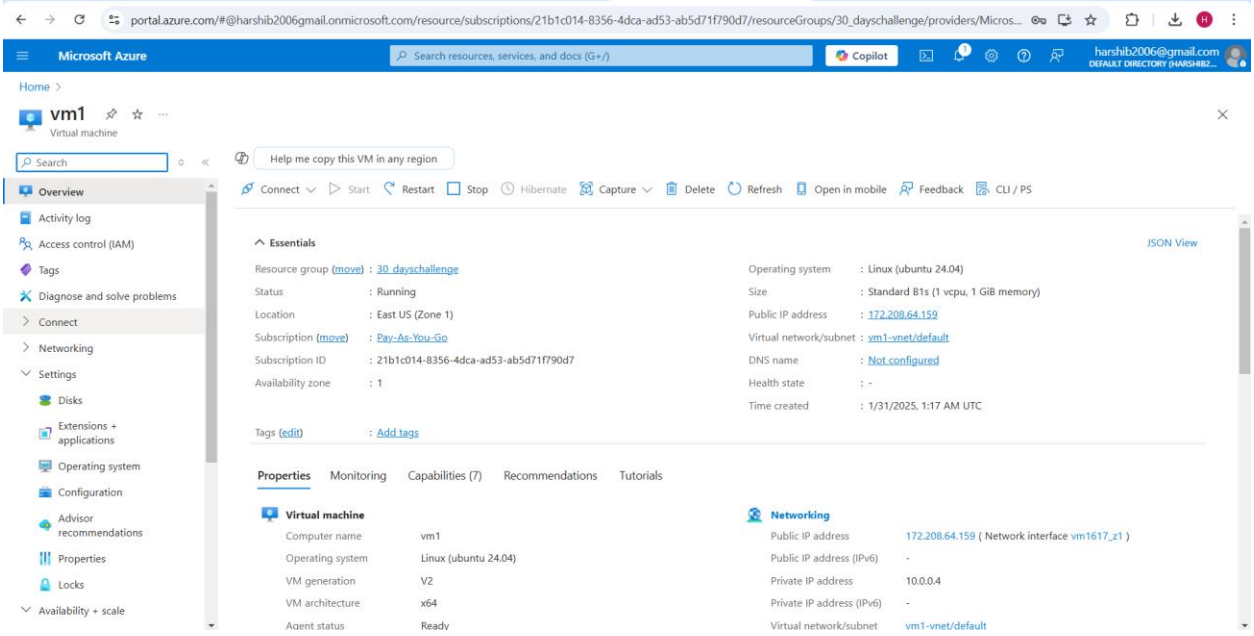


2. **Navigate to your Virtual Machine**:
    a. Click on **Virtual Machines** → Select your VM.


portal.azure.com/#browse/Microsoft.Compute%2FVirtualMachines
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
harshib2006@gmail.com
DEFAULT DIRECTORY (HARSHIB2...
Home
Virtual machines
Default Directory (harshib2006gmail.onmicrosoft.com)
Create
Switch to classic
Reservations
Manage view
Refresh
Export to CSV
Open query
Assign tags
Start
Restart
Stop
Delete
Services
Maintenance
Filter for any field...
Subscription equals Pay-As-You-Go
Type equals all
Resource group equals all
Location equals all
Add filter
Showing 0 to 0 of 0 records.
No grouping
List view
Name
Subscription
Resource group
Location
Status
Operating system
Size
Public IP address
Disks
Update
No virtual machines to display
Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.
Create
Learn more about Windows virtual machines
Learn more about Linux virtual machines
Give feedback

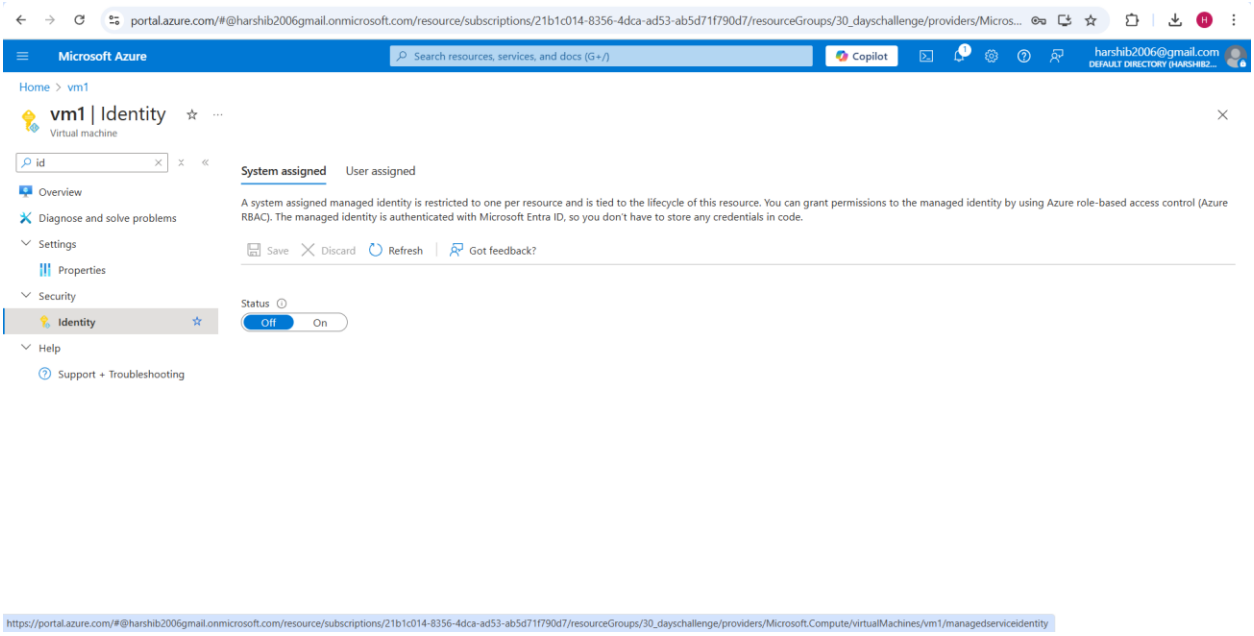

portal.azure.com/#create/Microsoft.VirtualMachine-ARM
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
harshib2006@gmail.com
DEFAULT DIRECTORY (HARSHIB2...
Home
Virtual machines
Create a virtual machine
Validation passed
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Subscription
Pay-As-You-Go
Resource group
30_dayschallenge
Virtual machine name
vm1
Region
East US
Availability options
Availability zone
Zone options
Self-selected zone
Availability zone
1
Security type
Trusted launch virtual machines
Enable secure boot
Yes
Enable vTPM
Yes
Integrity monitoring
No
Image
Ubuntu Server 24.04 LTS - Gen2
VM architecture
x64
Size
Standard B1s (1 vcpu, 1 GiB memory)
Enable Hibernation
No
Authentication type
SSH public key
Estimated monthly costs
but is made available on a preview basis for evaluation and feedback.
Give feedback about your estimate experience
Basics ₹631.61
Disks ₹439.23
Networking ₹969.22
Management ₹0.00
Monitoring ₹0.00
Advanced ₹0.00
Estimated monthly cost ₹2,040.06
< Previous
Next >
Create
Download a template for automation
Give feedback





3. **Enable Managed Identity**:

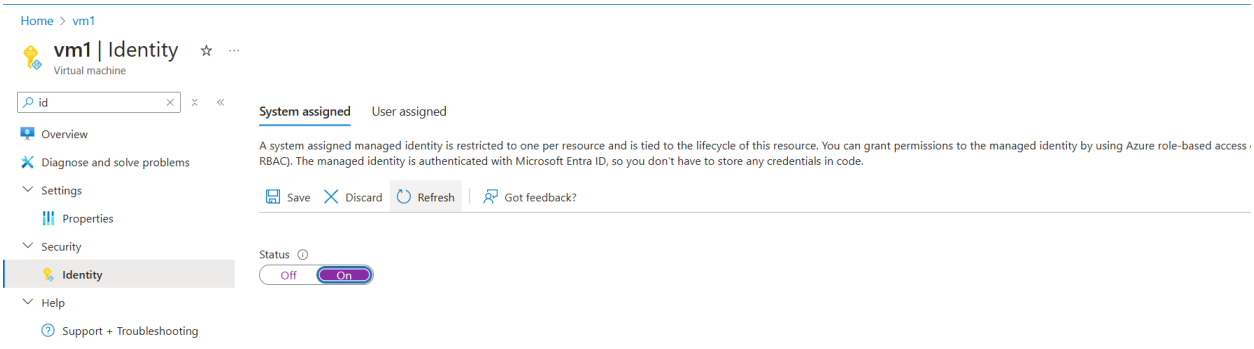
   a. In the left menu, go to **Identity**.



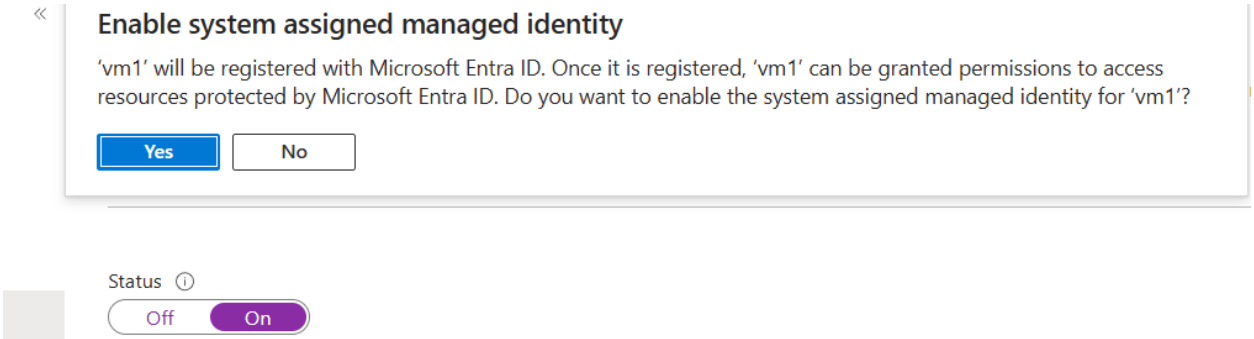
https://portal.azure.com/#@harshib2006gmail.onmicrosoft.com/resource/subscriptions/21b1c014-8356-4dca-ad53-ab5d71f790d7/resourceGroups/30_dayschallenge/providers/Microsoft.Compute/virtualMachines/vm1/managedserviceidentity

b. Under the **System assigned** tab:

i. Toggle **Status** to **On**.



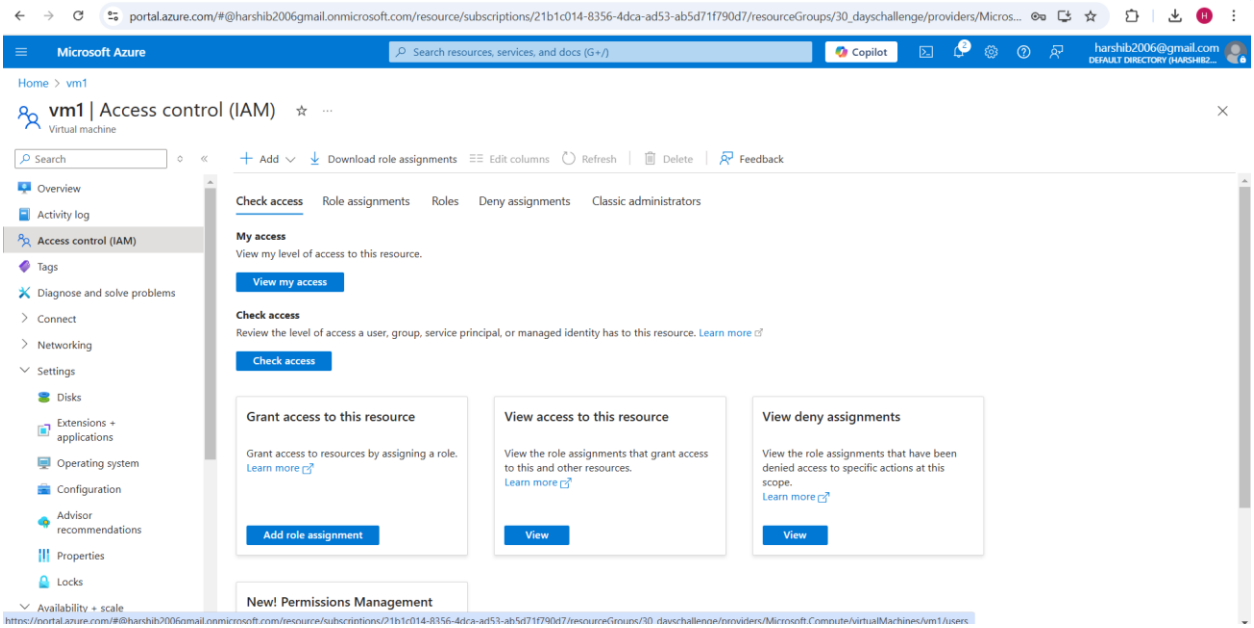
ii. Click **Save**.



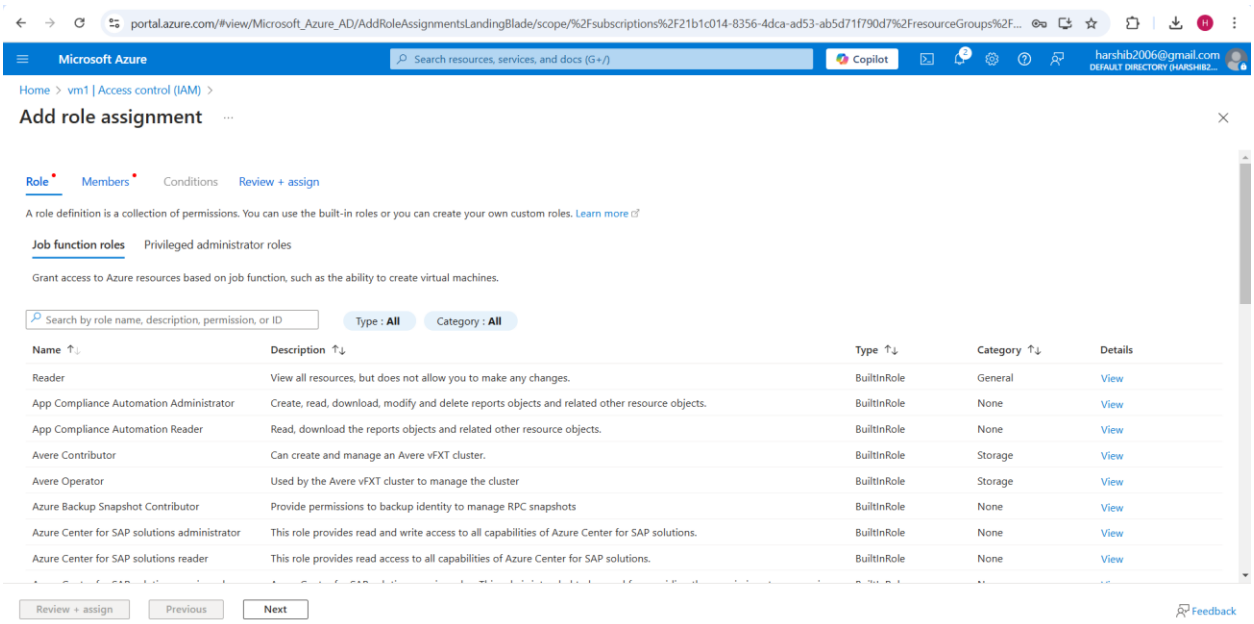
This step automatically registers the VM with an identity in Azure Active Directory (Azure AD).

Step 2 : Assing IAM role to the VM

1. **Go to the IAM (Access control) Section**:
    a. Open your VM in Azure Portal.
    b. Click on **Access control (IAM)** in the left menu.

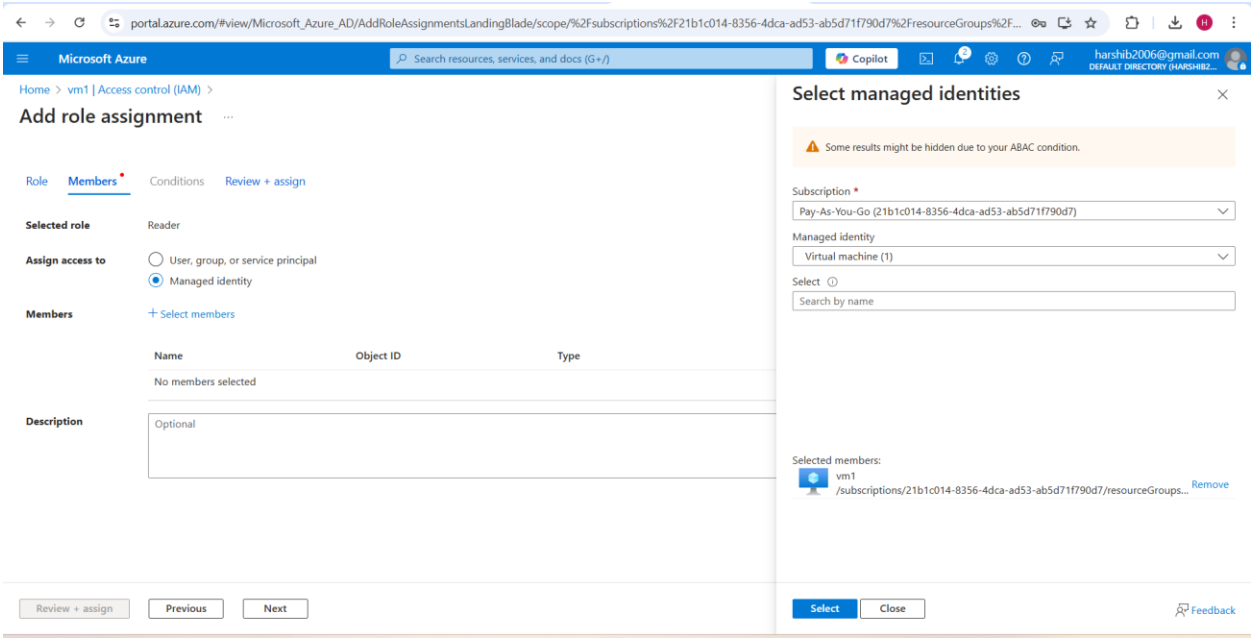


    c. Click **Add role assignment**.



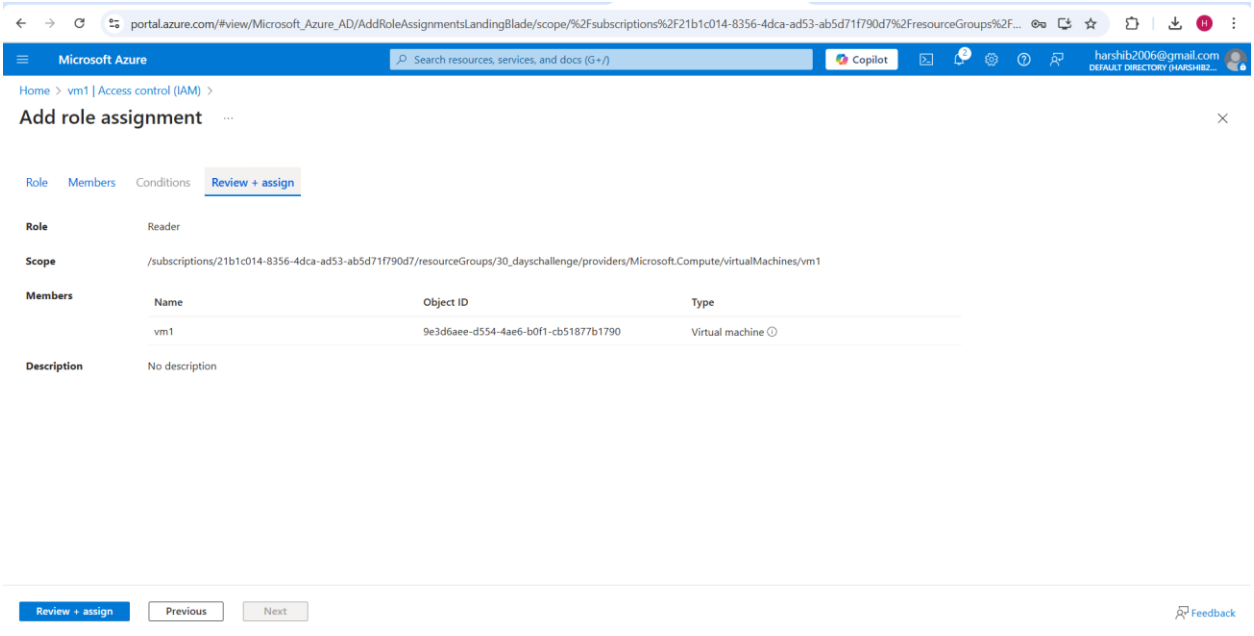
2. **Choose a Role**:
    a. Select the appropriate role based on required permissions, such as:
        i. **Reader** – Read-only access to the VM.
        ii. **Virtual Machine Contributor** – Manage VMs but not assign roles.
        iii. **Storage Blob Data Contributor** – If the VM needs access to storage.
        iv. **Custom Role** – For specific permissions.

3. **Assign Role to the Managed Identity**:
    a. Under **Assign access to**, select **Managed Identity**.



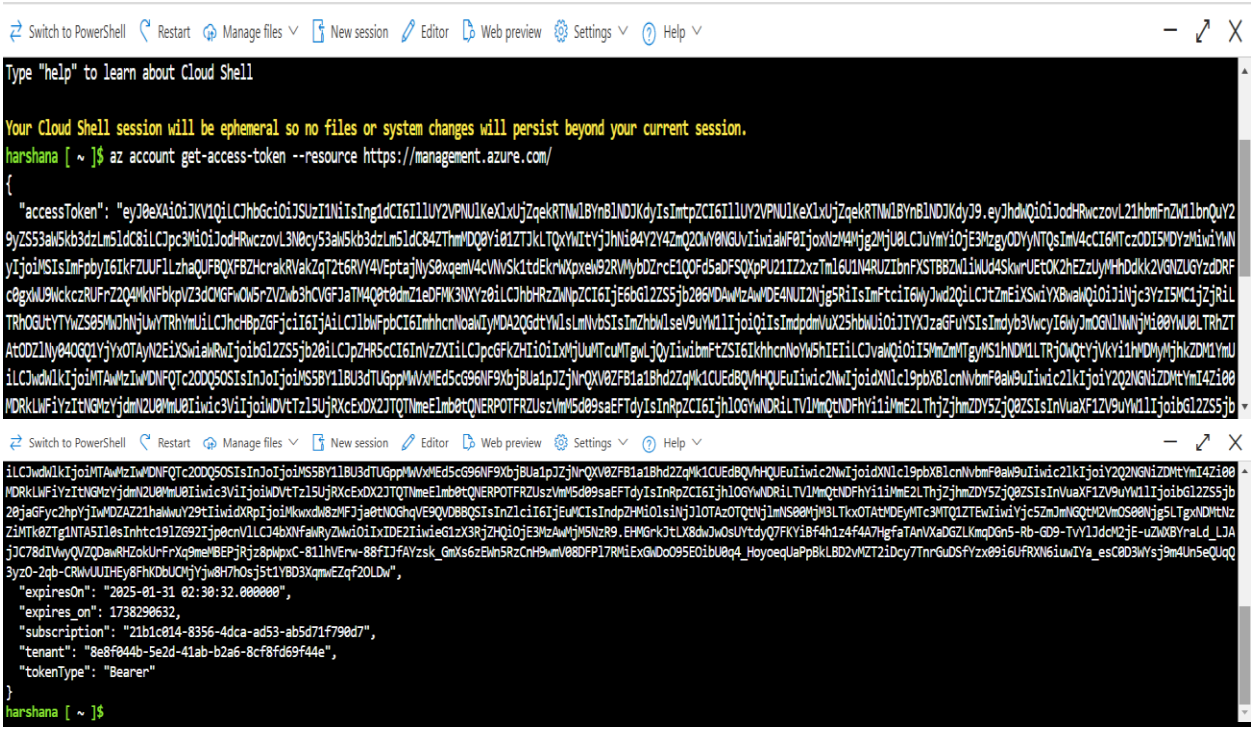
b. Click **Select members** → Choose your VM's **System Assigned Identity**.

c. Click **Review + Assign**.



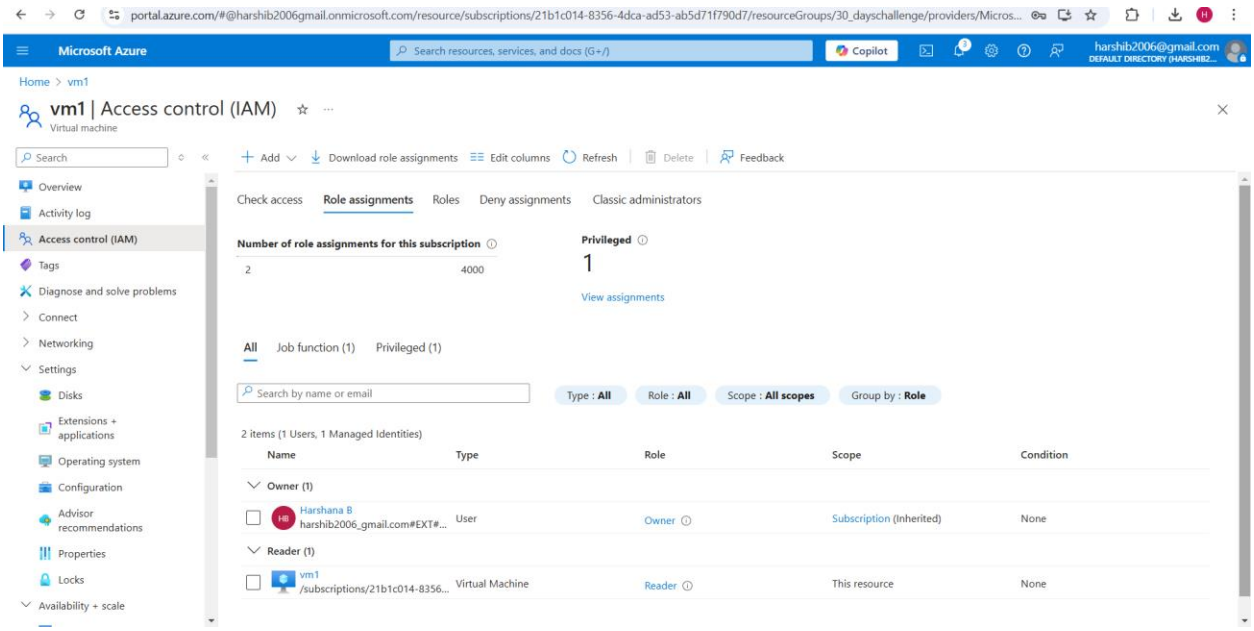
Step 3 : Verify Permissions

1. **Test Access Using Azure CLI**:
    a. Connect to the VM using SSH or RDP.
    b. Run the following command to verify permissions:



    c. If permissions are correct, the token will be generated.

2. **Check Role Assignments**:
    a. In the VM's **Access control (IAM)** tab, verify the assigned roles under **Role assignments**.



OUTCOME

By the end of this process, you will:

✅ Have an **IAM role** created and assigned to your VM.

✅ Ensure the VM has only the **necessary permissions** to perform specific tasks.

✅ Improve **security and manageability** by using **Managed Identities** instead of passwords.

✅ Verify role assignments and confirm **successful access** to required resources.