



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



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.

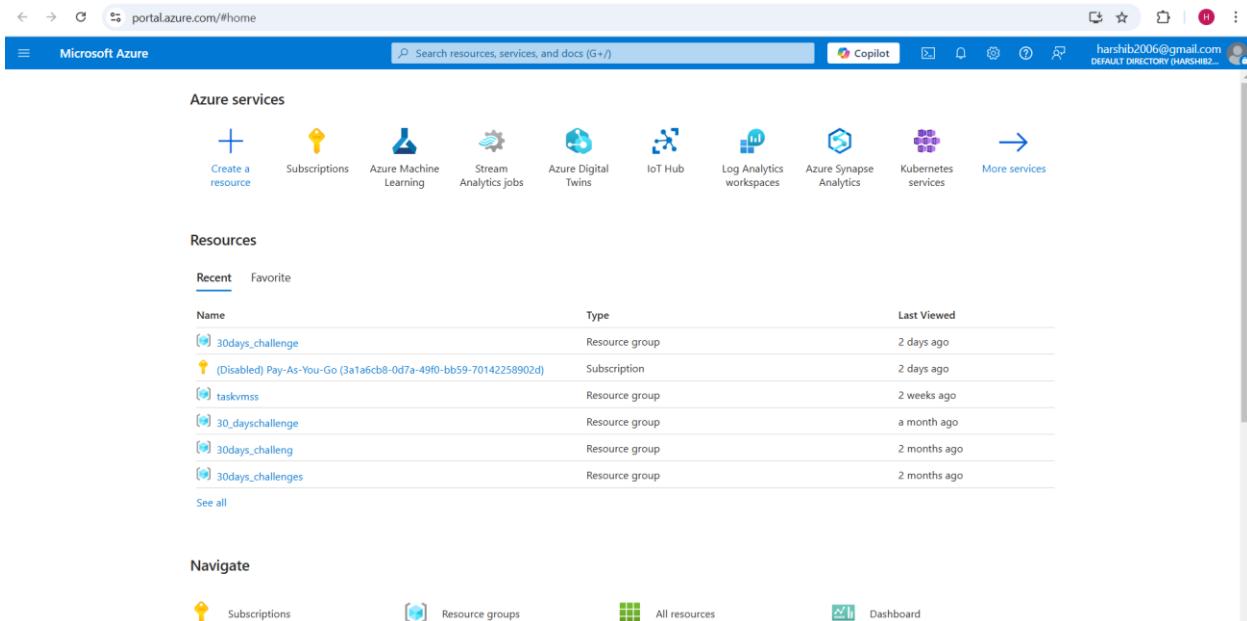
STEP-BY-STEP OVERVIEW

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.

Microsoft Azure

Virtual machines

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

Microsoft Azure

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_daychallenge
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
Site	Standard B1s (1 vCPU, 1 GiB memory)
Enable Hibernation	No
Authentication type	SSH public key

Estimated monthly costs

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

The screenshot shows the Microsoft Azure portal's Deployment Details blade for a completed deployment named "CreateVm-canonical.ubuntu-24_04-lts-server-20250131064506". The status is "Deployment succeeded". Key details include:

- Deployment name:** CreateVm-canonical.ubuntu-24_04-lts-server-20250131064506
- Subscription:** Pay-As-You-Go (21b1c014-8356-4dca-ad53-ab5d71f790d7)
- Resource group:** 30_dayschallenge
- Start time:** 1/31/2025, 6:47:16 AM
- Correlation ID:** 462dc784-bdfa-47df-a3b1-d8bac84ecb4f

The blade includes sections for "Deployment details" (with a "Next steps" section), "Cost Management", "Microsoft Defender for Cloud", "Free Microsoft tutorials", and "Work with an expert". Buttons at the bottom include "Go to resource" and "Create another VM".

The screenshot shows the Microsoft Azure portal's Virtual Machine Overview blade for a VM named "vm1". The main details are:

- Resource group:** 30_dayschallenge
- Status:** Running
- Location:** East US (Zone 1)
- Subscription:** Pay-As-You-Go
- Subscription ID:** 21b1c014-8356-4dca-ad53-ab5d71f790d7
- Availability zone:** 1
- Operating system:** Linux (ubuntu 24.04)
- Size:** Standard B1s (1 vcpu, 1 GiB memory)
- Public IP address:** 172.208.64.159
- Virtual network/subnet:** vm1-vnet/default
- DNS name:** Not configured
- Health state:** -
- Time created:** 1/31/2025, 1:17 AM UTC

The blade includes tabs for "Properties", "Monitoring", "Capabilities (7)", "Recommendations", and "Tutorials". It also shows "Networking" details like Public IP address (172.208.64.159) and Private IP address (10.0.0.4). A left sidebar lists various management options for the VM.

3. Enable Managed Identity:

a. In the left menu, go to Identity.

Home > vm1

vm1 | Identity

System assigned User assigned

A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Microsoft Entra ID, so you don't have to store any credentials in code.

Status: Off

https://portal.azure.com/#@harshib2006@gmail.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.

Home > vm1

vm1 | Identity

System assigned User assigned

A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Microsoft Entra ID, so you don't have to store any credentials in code.

Status: On

ii. Click Save.

Enable system assigned managed identity

'vm1' will be registered with Microsoft Entra ID. Once it is registered, 'vm1' can be granted permissions to access resources protected by Microsoft Entra ID. Do you want to enable the system assigned managed identity for 'vm1'?

Status: On

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.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and various icons. The URL in the address bar is https://portal.azure.com/#@harshib2006@gmail.onmicrosoft.com/resource/subscriptions/21b1c014-8356-4dca-ad53-ab5d71f790d7/resourceGroups/30_dayschallenge/providers/Microsoft.Compute/virtualMachines/vm1/users. The left sidebar shows a tree view with 'vm1' selected, and under it, 'Access control (IAM)' is highlighted. The main content area has a heading 'vm1 | Access control (IAM)'. It contains several sections: 'My access' (with a 'View my access' button), 'Check access' (with a 'Check access' button), 'Grant access to this resource' (with a 'Learn more' link and an 'Add role assignment' button), 'View access to this resource' (with a 'View' button), and 'View deny assignments' (with a 'View' button). A banner at the bottom says 'New! Permissions Management'.

- c. Click **Add role assignment**.

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Reader	View all resources, but does not allow you to make any changes.	BuiltinRole	General	View
App Compliance Automation Administrator	Create, read, download, modify and delete reports objects and related other resource objects.	BuiltinRole	None	View
App Compliance Automation Reader	Read, download the reports objects and related other resource objects.	BuiltinRole	None	View
Avere Contributor	Can create and manage an Avere vFXT cluster.	BuiltinRole	Storage	View
Avere Operator	Used by the Avere vFXT cluster to manage the cluster	BuiltinRole	Storage	View
Azure Backup Snapshot Contributor	Provide permissions to backup identity to manage RPC snapshots	BuiltinRole	None	View
Azure Center for SAP solutions administrator	This role provides read and write access to all capabilities of Azure Center for SAP solutions.	BuiltinRole	None	View
Azure Center for SAP solutions reader	This role provides read access to all capabilities of Azure Center for SAP solutions.	BuiltinRole	None	View

[Review + assign](#) [Previous](#) [Next](#) [Feedback](#)

2. Choose a Role:

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

3. Assign Role to the Managed Identity:

- Under **Assign access to**, select **Managed Identity**.

Select managed identities

⚠ Some results might be hidden due to your ABAC condition.

Subscription * Pay-As-You-Go (21b1c014-8356-4dca-ad53-ab5d71f790d7)

Managed identity Virtual machine (1)

Select ⓘ

Search by name

Selected members: vm1 /subscriptions/21b1c014-8356-4dca-ad53-ab5d71f790d7/resourceGroups... Remove

- b. Click **Select members** → Choose your VM's **System Assigned Identity**.
- c. Click **Review + Assign**.

Members	Name	Object ID	Type
	vm1	9e3d6aee-d554-4ae6-b0f1-cb51877b1790	Virtual machine ⓘ

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:

```
Switch to PowerShell ⌘ Restart ⌘ Manage files ⌘ New session Editor Web preview Settings Help

Type "help" to learn about Cloud Shell

Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.

harshana [ ~ ]$ az account get-access-token --resource https://management.azure.com/
{
  "accessToken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIngldCI6I1lUY2VPNU1KeX1xUjZqekRTNWlBYnB1NDKdyIsImtpZCI6I1lUY2VPNU1KeX1xUjZqekRTNWlBYnB1NDKdyJ9.eyJhdQoIojodHRwczovL21hbmlFnZW11bnQuY29yZS53ai5kb3dzLm5ldC81Cjpc3M0i0jodHRwczovL3N0cy53ai5kb3dzLm5dC84ZTlwDQ8y0iZTjKL0TQxMjYjJhnI84Y24Zm20QyN0GuV1iwiawF0joxNzI4Wjg2Wj0LCljUyMj0jE3MzgyODyNTQsIm4cC16MtzcODISyDyzhwiw1YmWjYj0i1NSiIsImPfbpYI6IKfZFUfLzhaQjUFQxFBZlcrakRvAkZqT2t6RV4VEptajNyS8xqemV4cVNsSk1dEkrlwPxehb92RMbDzrcE1Q0Fd5aDFSQxpPU21T22xTm16U1N4RUZlbnFxSTBBZlwiUd4SkwrUEt0K2hEZzUyMHDdkk2VGNZU6ygzDRFcgxjU9WkckzRUF-TZQ4MNKFbkpvTzdCMFw05rV2zbh3CKFJaTm4Q8t0dm1z1DPMK3Ny0iLjCjhlhRzNpZC16IjE6BG12Z55jb286DMzAwMD4NU1Njg5RiSImFtc1I6WjJwd2QjLCjT2mEiXsw1YXbwahQj0i1jNj3Yz1SMC1jZjRilTRh0GUtYTywTS05M0hjhjwYTrhMuLjCjchbPzGfciE6j1aiLjCjhlwPbC16InhrhknNoalWjyMADA20GdtW1sLmNbS1sImZhb1lsev9yM11joiQisImdpdmUv25hbhjw0iJ1jYjzaGFySisIndy3b3Wcyl6WjyM0Gh1MNWjM108yNU08LTrZTAt0DZlNy840GQ1YjyX0TAjN2ExSw1wRljoibG1Z2S5j2b011CjpcHr5CjC16InVzZxi1Cjpc6FKzHi0iXmjuUmcuTgwLjQiyiwibmFzZS1GikhcnNoVWS1hEi1CjvaQj0i15WmZmTgymWS1hNDM1LTrj0QytyjVky1hWDMyMjhkZDM1YmUj1LCjndW1kIjoiMTAwz1wz1DNDFQT200Q50SiIsInjoiMSB5Y11Bu3dTuKpmVwXMeEd5c96NF9bxj8u1pJzJwQxVFB1aBhdZqPmk1CuE6B0hvHQHeU1iwi2c2WnIjoixdX1C19pbXblcnNvbmF0ak9uIwiic2lk1Ijoiy2Q2Ngn1ZDm1YmI4z3aaMDRKLnWjYzitNgtYjdmN2U8mWjUtiwi3ViijoiDvtTz15ujRxExD2JTQTNmEmB0tQNERPOTFRzUsVm5d09saEFTdyisInRpZC16Ijhh0GyWNRDlrlT1VmQtNDfhyyi1mE2LThjzjhmdZy57jQzS1sInVuaXf1Zv9uW11joiibG1Z2S5jzb2jaFyczhpjWmMDA2T21haalwuy29T1iwdxRpj1oimkWwdwzjF1jyQn0Ghve9QVBDBQS1nZlci16j1C16j1C16j1Dz0j1n1580MjM3L1TDeYt1m1z1TQ1z7Te1w1Yz1c5mJNgjtQ2Wm0Se8n5L7gNdtMnz3iTnk0zT1NTA510s1nsInh191z1G921jw0iXkLc4XnfwnaFryZw1i0iXk12i1wiie61z3XjRj0iQj16MzAmjWmNzR.EHMGkr1tLx8dwjwOsUytdyj19Fy1bf4h1z14f4A7HgfaTvnAxNkLkmqDmzR-Rb-GD9-TvY1M2jE-uZwzRld-L1Aj1jC78d1VpQzQdawRHZokUrFrxp9mEBPjTz18pWpxc-811VFrw-88f1TfAYzsK_gnx6z16Wm5RzCh19mW08DP17Rw1Exw0d095E01bu0g4_HoyeqUapbklBDw2MT21DcyTmrnQudSfzxa05i6URXN6giu1Yy_ecsCD3Wysj3m4u5eQulq03yzo-2qb-CRWUUJHxEyFhKdUbUjMjYjw87h0s5j1Y1BD3XqmWzEqf20LDw",
  "expiresOn": "2025-01-31 02:38:32.000000",
  "expiresOn": "1738230632",
  "subscription": "21b1c014-8356-4dca-ad53-ab5d71f798d7",
  "tenant": "8ef944b-5e2d-41ab-b2a6-8cf8df69f44e",
  "tokenType": "Bearer"
}
harshana [ ~ ]$
```

- 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**.

The screenshot shows the Microsoft Azure portal's Access control (IAM) blade for a virtual machine named 'vm1'. The 'Role assignments' tab is active, displaying one privileged role assignment. The assignment is for the user 'Harshana B' (harshib2006@gmail.com#EXT#) with the 'Owner' role at the 'Subscription (Inherited)' scope. The blade also includes sections for 'Check access', 'Roles', 'Deny assignments', and 'Classic administrators'.

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.