Stories 4 : Azure Active Directory (Entra ID)

Microsoft Entra ID is a cloud-based identity and access management solution. It is a directory and identity management service that operates in the cloud and offers authentication and authorization services to various Microsoft services such as Microsoft 365, Dynamics 365, and Microsoft Azure.

Microsoft Entra ID is the next evolution of identity and access management solutions for the cloud.

Azure Active Directory (Azure AD)

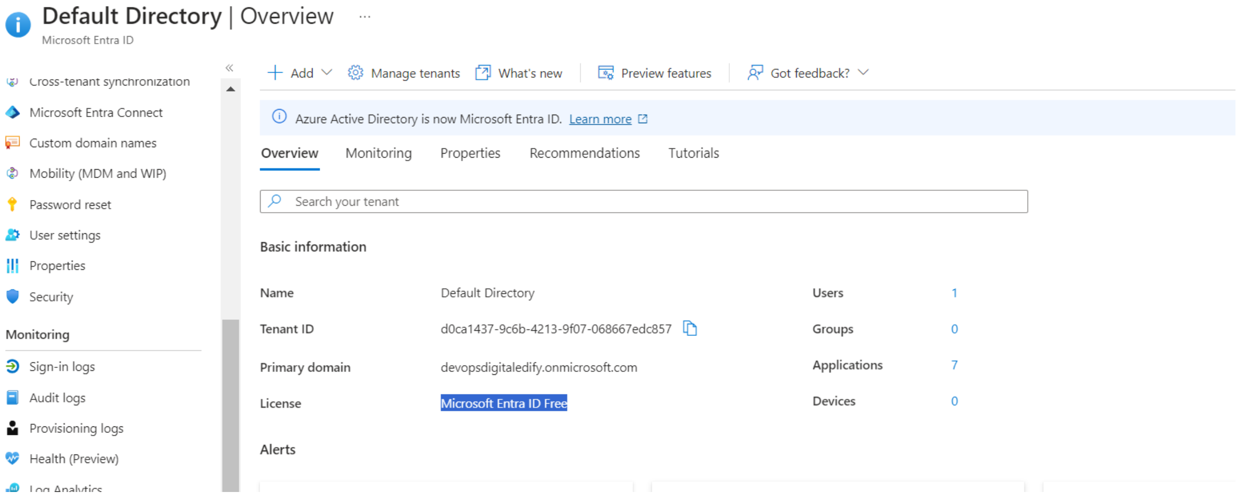
Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service. It serves as a comprehensive identity and authentication platform for securing and managing access to various applications and services.

Here's an overview:

1. **Identity Management:** Azure AD enables organizations to manage and secure user identities and credentials. It supports single sign-on (SSO) for a seamless user experience across applications and devices.
2. **Single Sign-On (SSO):** With SSO, users can sign in once and access multiple applications without the need to re-enter their credentials. This enhances user productivity and reduces the number of passwords users need to remember.
3. **Multi-Factor Authentication (MFA):** Azure AD supports MFA, adding an extra layer of security by requiring users to provide additional verification, such as a phone prompt or a biometric check, in addition to their password.
4. **Application Access Management:** Azure AD allows administrators to control and manage access to applications. This includes both Microsoft 365 applications and a

wide range of third-party applications.

5. **Device Management:** Organizations can use Azure AD to manage and secure devices that access corporate resources. This includes features like device registration, conditional access policies, and the ability to enforce security measures on devices.
6. **Role-Based Access Control (RBAC):** Azure AD integrates with Azure's RBAC system, enabling organizations to define fine-grained access controls based on roles. This ensures that users have the necessary permissions to perform their tasks while maintaining security.
7. **Identity Protection:** Azure AD includes features for detecting and responding to identity-based threats. It can analyze user behavior and sign-in patterns to identify suspicious activities, triggering alerts and remediation actions.
8. **Integration with Microsoft 365 and Azure Services:** Azure AD seamlessly integrates with Microsoft 365 services, as well as a wide range of Azure services, providing a unified identity platform for both cloud and on-premises resources.



Default Directory | Overview

Microsoft Entra ID

Azure Active Directory is now Microsoft Entra ID. Learn more

Search your tenant

Basic information

Name	Default Directory	Users	1
Tenant ID	d0ca1437-9c6b-4213-9f07-068667edc857	Groups	0
Primary domain	devopsdigitaledify.onmicrosoft.com	Applications	7
License	Microsoft Entra ID Free	Devices	0

Alerts

AD plans

https://www.microsoft.com/en-us/security/business/microsoft-entra-pricing

Sign logs : Sign in infromation about ip address location etc

You can use the sign-in logs to answer questions such as:

- How many users signed into a particular application this week?
- How many failed sign-in attempts occurred in the last 24 hours?
- Are users signing in from specific browsers or operating systems?
- Which of my Azure resources were accessed by managed identities and service principals?

You can also describe the activity associated with a sign-in request by identifying the following details:

- **Who** – The identity (User) performing the sign-in.
- **How** – The client (Application) used for the sign-in.
- **What** – The target (Resource) accessed by the identity.

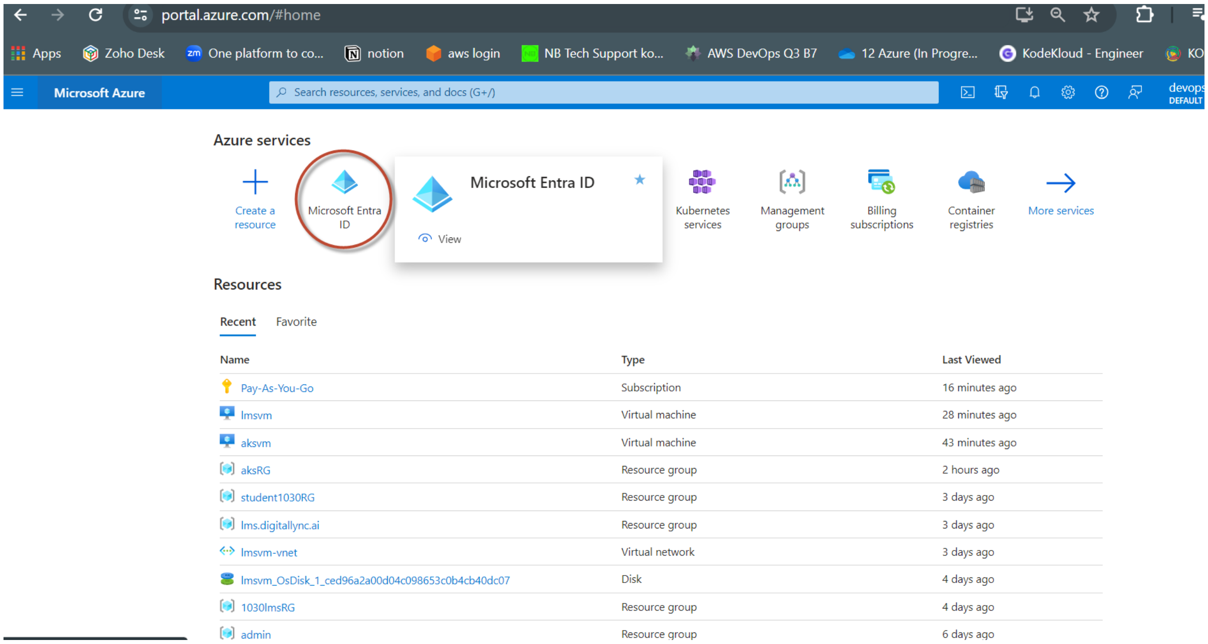
Audit Logs : Audit log is a record of system activities for an Azure subscription. It provides information about operations that were performed on resources in your subscription. Azure Audit Logs help you track changes and troubleshoot any issues by providing a detailed history of operations.

Lab 1 : Give Access to Resource Level

Create a User and assign role and subscrition to it give VM access

1. VM resource Acess

Create user in microsoft Entra ID

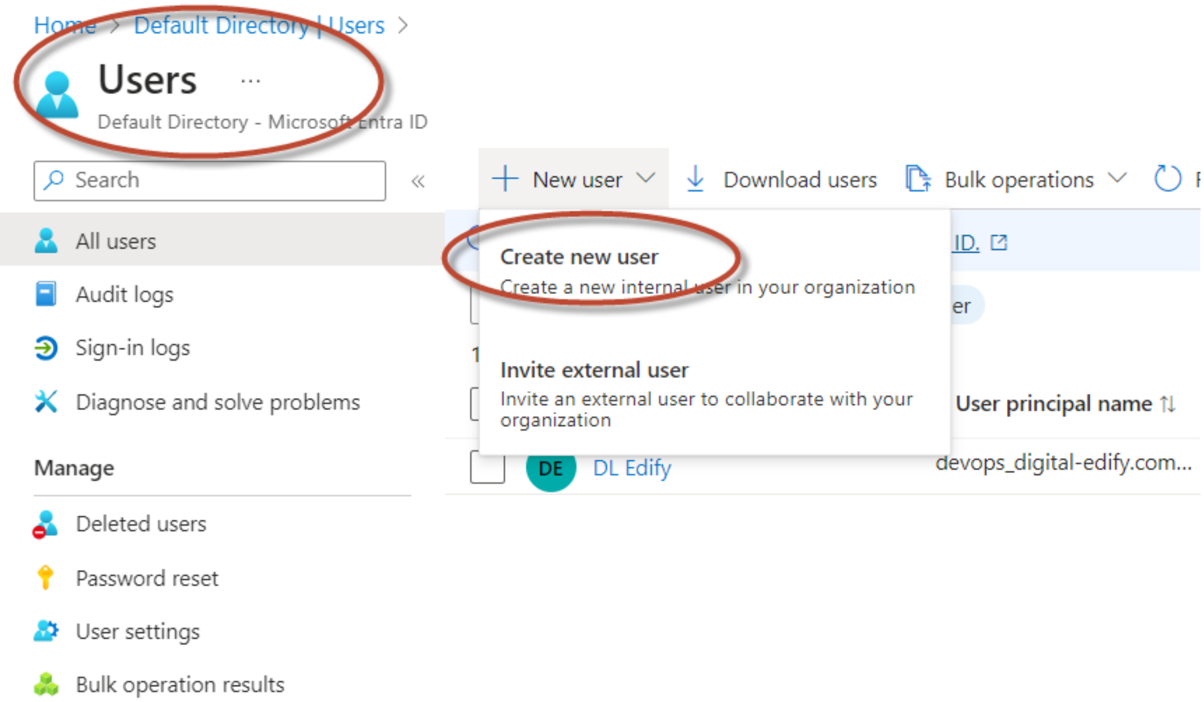


Resources

Recent Favorite

Name	Type	Last Viewed
Pay-As-You-Go	Subscription	16 minutes ago
lmsvm	Virtual machine	28 minutes ago
aksvm	Virtual machine	43 minutes ago
aksRG	Resource group	2 hours ago
student1030RG	Resource group	3 days ago
lms.digitallync.ai	Resource group	3 days ago
lmsvm-vnet	Virtual network	3 days ago
lmsvm_OsDisk_1_ced96a2a00d04c098653c0b4cb40dc07	Disk	4 days ago
1030lmsRG	Resource group	4 days ago
admin	Resource group	6 days ago

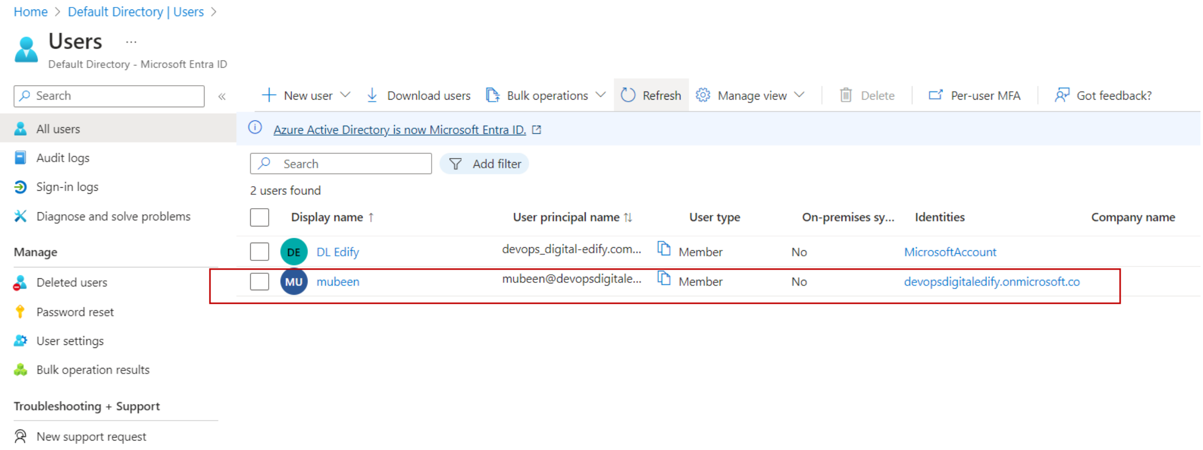
Create a user



Create a new internal user in your organization

Invite an external user to collaborate with your organization

devops_digital-edify.com...

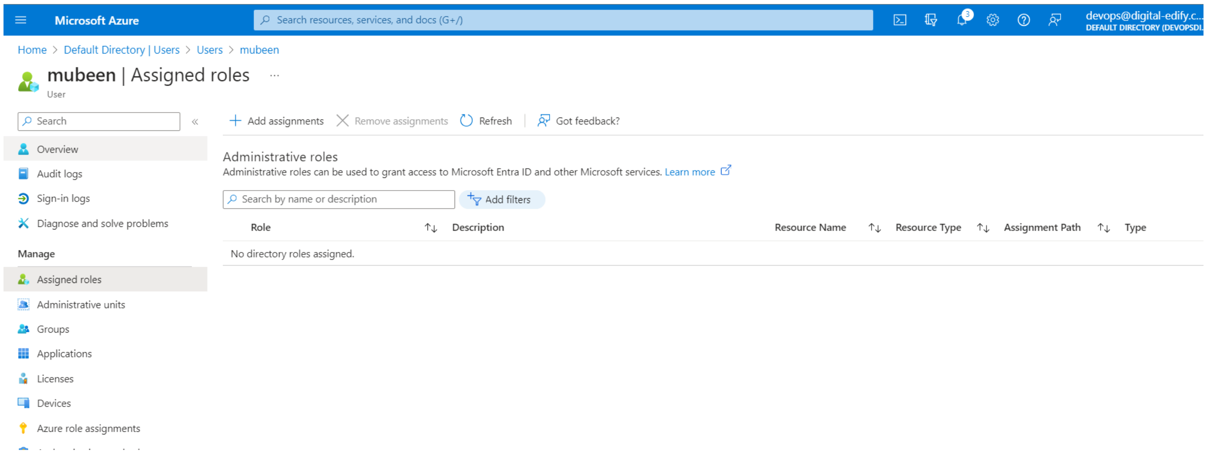


Azure Active Directory is now Microsoft Entra ID.

2 users found

□	Display name ↑	User principal name ⇅		User type	On-premises sy...	Identities	Company name
□	DE DL Edify	devops_digital-edify.com...		Member	No	MicrosoftAccount	
□	MU mubeen	mubeen@devopsdigitale...		Member	No	devopsdigitaledify.onmicrosoft.co	

WE will roles for this user now



mubeen | Assigned roles

User

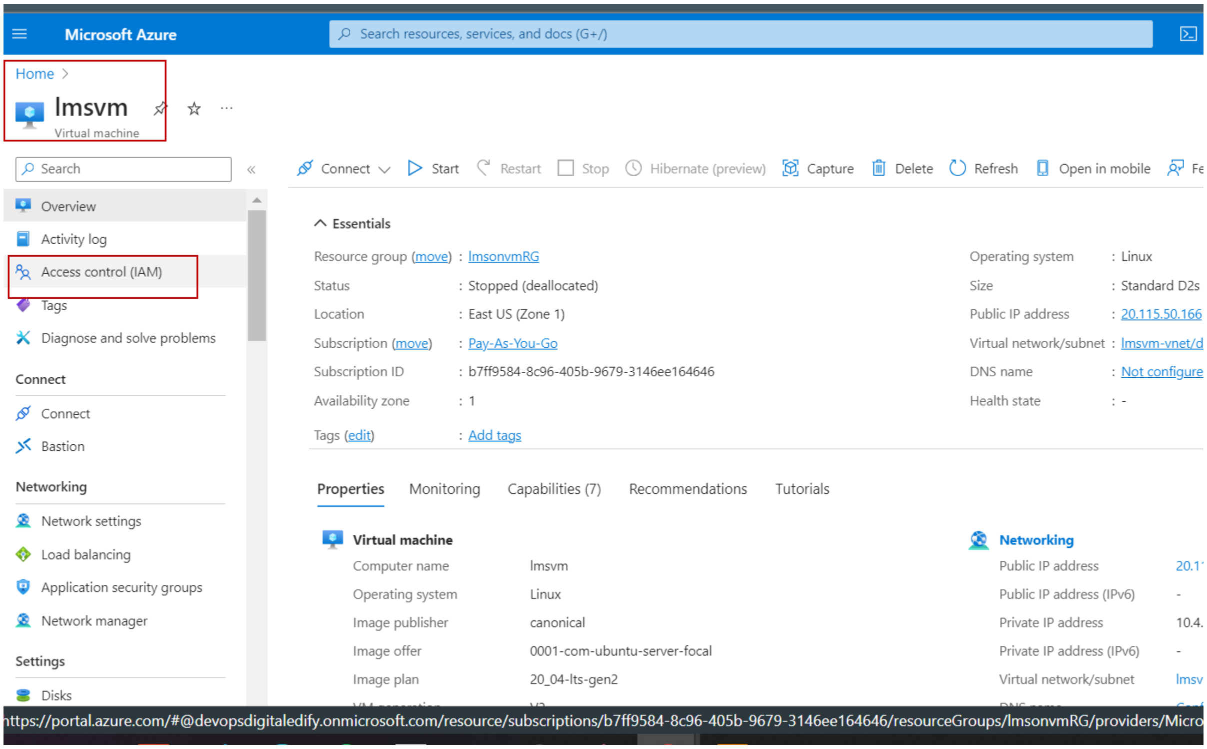
Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. Learn more

Role	Description	Resource Name	Resource Type	Assignment Path	Type
No directory roles assigned.					

No roles has been assigned

To assign role Goto IAM of VM



Essentials

Resource group (move)	: ImsonvmRG	Operating system	: Linux
Status	: Stopped (deallocated)	Size	: Standard D2s
Location	: East US (Zone 1)	Public IP address	: 20.115.50.166
Subscription (move)	: Pay-As-You-Go	Virtual network/subnet	: lmsvm-vnet/d
Subscription ID	: b7ff9584-8c96-405b-9679-3146ee164646	DNS name	: Not configure
Availability zone	: 1	Health state	: -
Tags (edit)	: Add tags		

Virtual machine

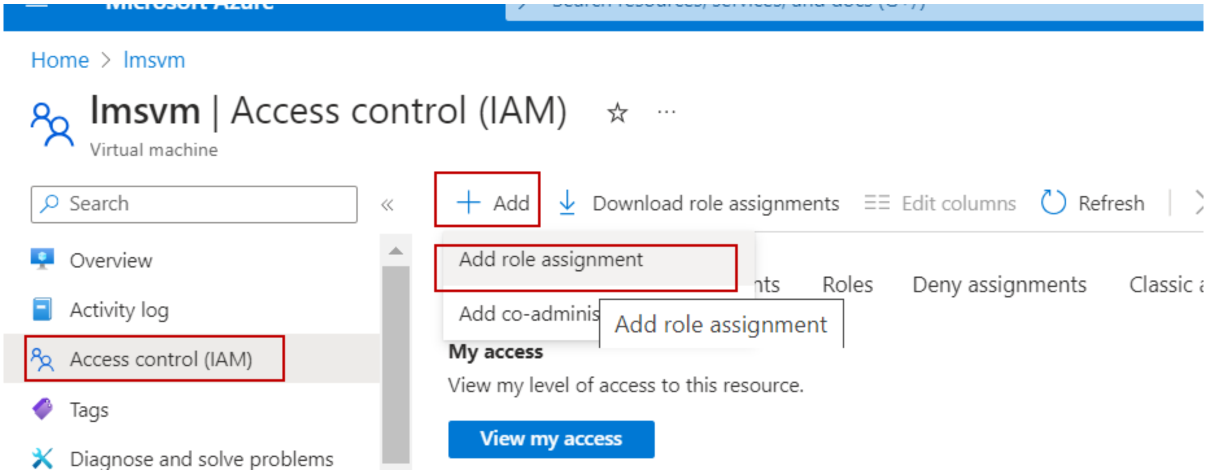
Computer name	lmsvm
Operating system	Linux
Image publisher	canonical
Image offer	0001-com-ubuntu-server-focal
Image plan	20_04-lts-gen2

Networking

Public IP address	20.1
Public IP address (IPv6)	-
Private IP address	10.4.
Private IP address (IPv6)	-
Virtual network/subnet	lmsv

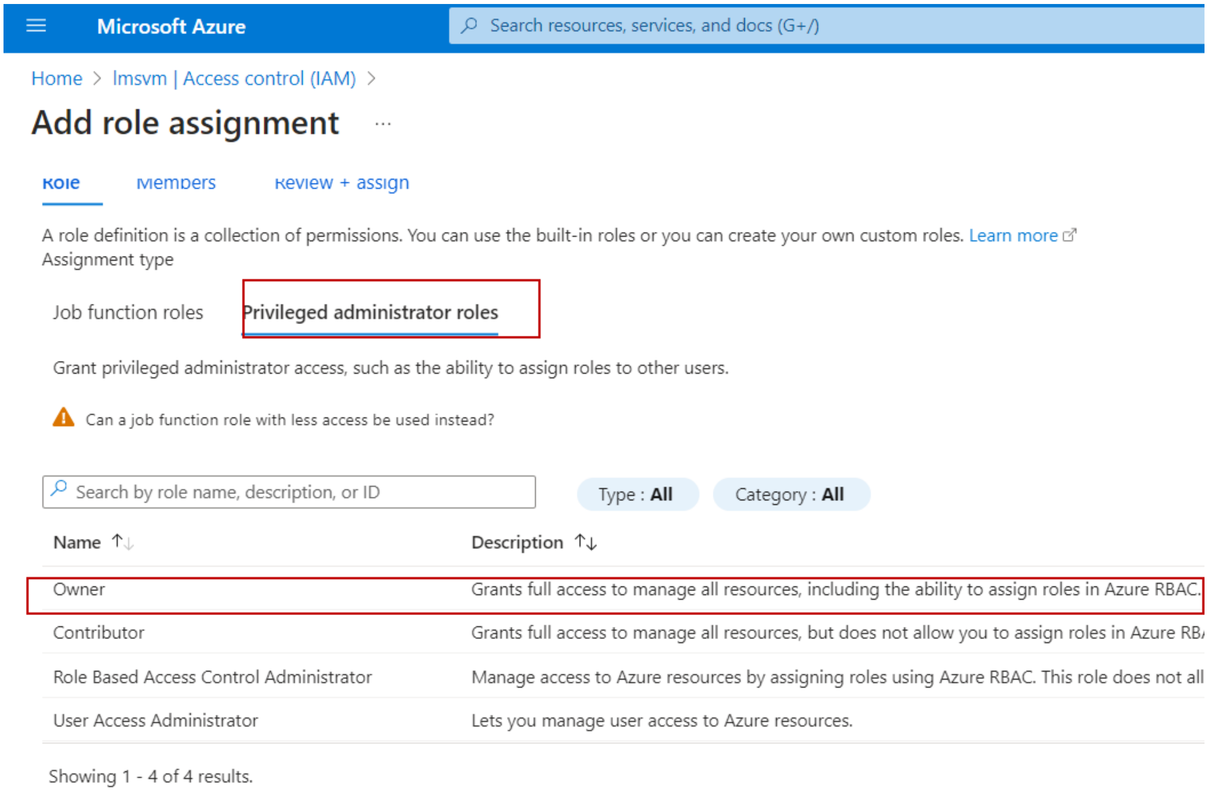
ttps://portal.azure.com/#@devopsdigitaledify.onmicrosoft.com/resource/subscriptions/b7ff9584-8c96-405b-9679-3146ee164646/resourceGroups/lmsonvmRG/providers/Micro

Assign role goto vm and assign IAM role owner or contributor



My access

View my level of access to this resource.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > lmsvm | Access control (IAM) >

Add role assignment ...

Role
Members
Review + assign

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
Assignment type

Job function roles
Privileged administrator roles

Grant privileged administrator access, such as the ability to assign roles to other users.

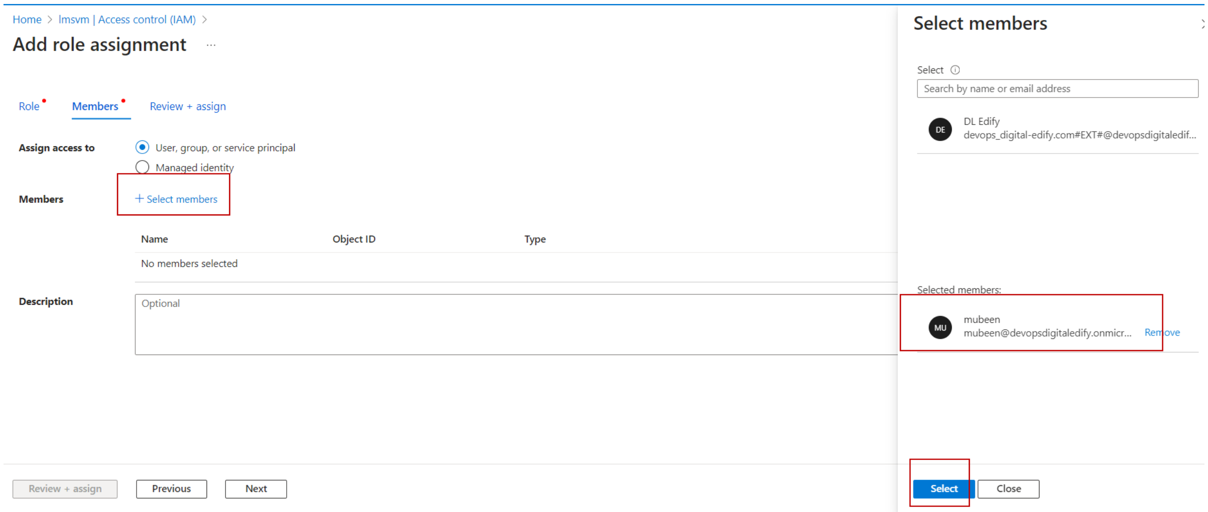
⚠ Can a job function role with less access be used instead?

Search by role name, description, or ID
Type : All
Category : All

Name ↑↓	Description ↑↓
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RB/
Role Based Access Control Administrator	Manage access to Azure resources by assigning roles using Azure RBAC. This role does not all
User Access Administrator	Lets you manage user access to Azure resources.

Showing 1 - 4 of 4 results.

Add member and assign role to selected member



Add role assignment

Assign access to: ● User, group, or service principal ○ Managed identity

Members: + Select members

No members selected

Description: Optional

Select members

Select: Search by name or email address

DL Edify
devops_digital-edify.com#EXT#@devopsdigitaledif...

Selected members:

mubeen
mubeen@devopsdigitaledify.onmicr...

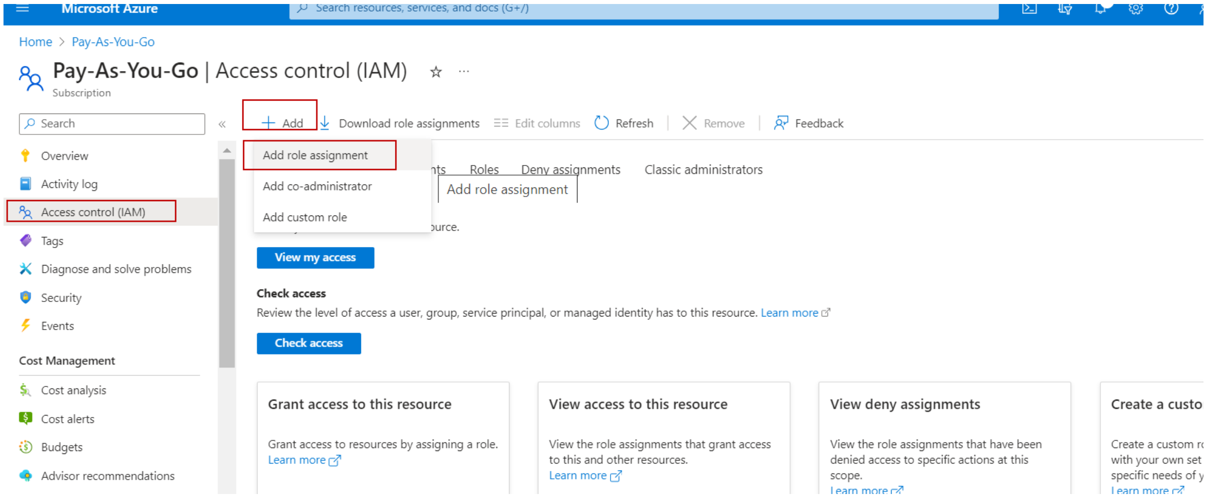
Now open login to other user and refresh

Now you will access to vm

Lab 2. Give the access to Subscription level

Create user

Goto IAM of Subscription



Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Grant access to this resource

Grant access to resources by assigning a role. Learn more

View access to this resource

View the role assignments that grant access to this and other resources. Learn more

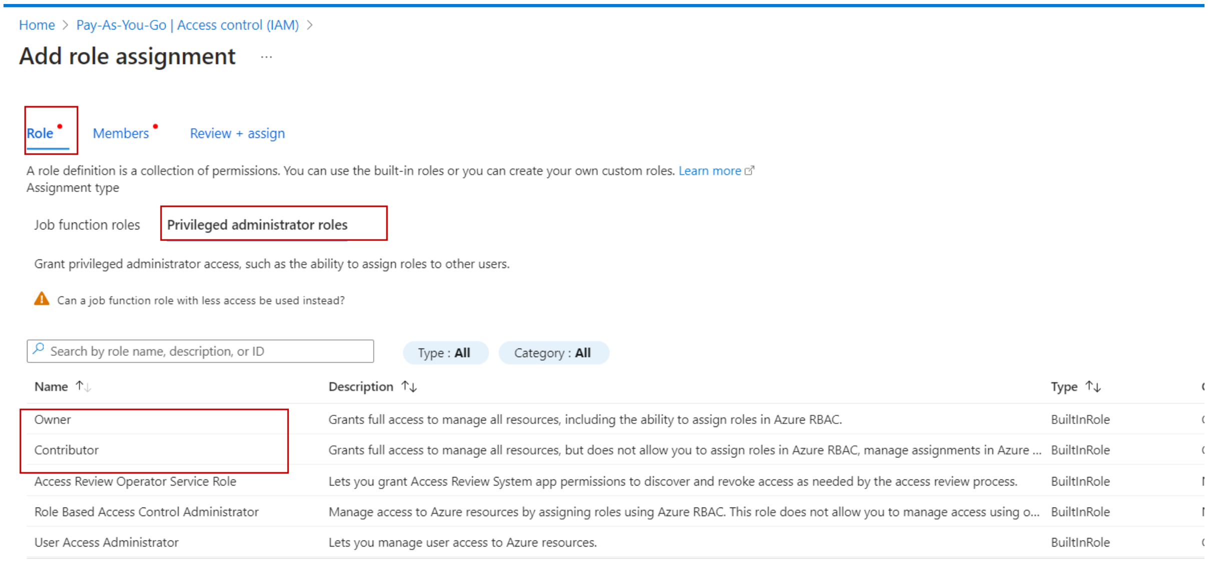
View deny assignments

View the role assignments that have been denied access to specific actions at this scope. Learn more

Create a custo

Create a custom r with your own set specific needs of y Learn more

Assign role goto subscription



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

Assignment type

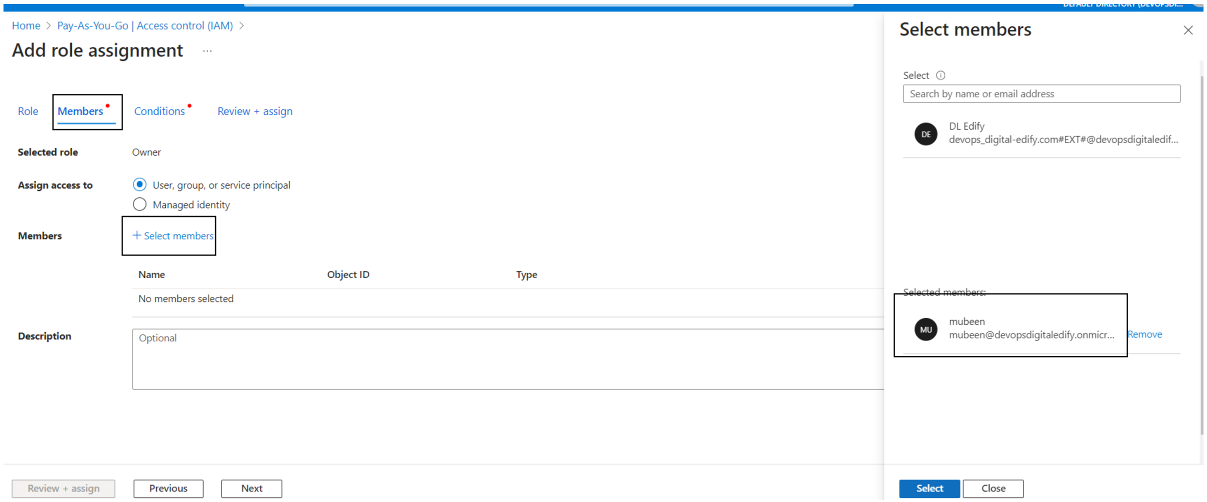
Grant privileged administrator access, such as the ability to assign roles to other users.

⚠ Can a job function role with less access be used instead?

Search by role name, description, or ID

Name ↑↓	Description ↑↓	Type ↑↓
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.	BuiltInRole
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure ...	BuiltInRole
Access Review Operator Service Role	Lets you grant Access Review System app permissions to discover and revoke access as needed by the access review process.	BuiltInRole
Role Based Access Control Administrator	Manage access to Azure resources by assigning roles using Azure RBAC. This role does not allow you to manage access using o...	BuiltInRole
User Access Administrator	Lets you manage user access to Azure resources.	BuiltInRole

Select the members\\



Home > Pay-As-You-Go | Access control (IAM) >

Add role assignment ···

Selected role: Owner

Assign access to: ◉ User, group, or service principal ○ Managed identity

Members: + Select members

Name	Object ID	Type
No members selected		

Description: Optional

Select members

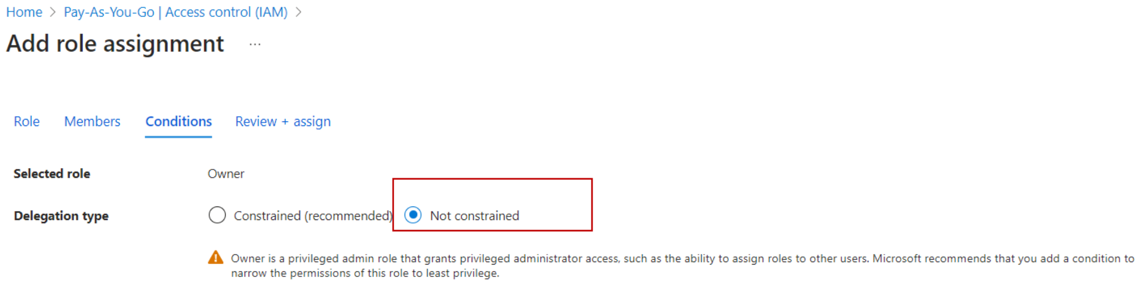
Select ⓘ

Search by name or email address

DE DL Edify devops_digital-edify.com#EXT#@devopsdigitaledif...

Selected members:

MU mubeen mubeen@devopsdigitaledify.onmicr... Remove



Home > Pay-As-You-Go | Access control (IAM) >

Add role assignment ···

Selected role: Owner

Delegation type: ○ Constrained (recommended) ◉ Not constrained

⚠ Owner is a privileged admin role that grants privileged administrator access, such as the ability to assign roles to other users. Microsoft recommends that you add a condition to narrow the permissions of this role to least privilege.

Constrained (recommended):

- When you delegate tasks with constraints, it means you set specific rules or limits on how those tasks should be done. This helps ensure that the tasks are carried out in a particular way or within certain boundaries.

Not Constrained:

- When tasks are delegated without constraints, it means there are fewer rules or restrictions on how the tasks should be completed. This allows more freedom and flexibility for the individuals to whom the tasks are assigned.

Now login to newly created user and check for the subscription

---

Roles : A role definition is **a collection of permissions that can be performed, such as read, write, and delete**. It's typically just called a role. Azure role-based access control (Azure RBAC) has over 120 built-in roles or you can create your own custom roles.

Reader:

1. **Owner:**
   -

The "Owner" role in Azure has full access to all resources and can manage access, including granting or revoking permissions, making them the highest level of authority within a resource group or subscription.

2.

Contributor:

-

The "Contributor" role in Azure allows users to create and manage resources but doesn't grant permissions to manage access. It is suitable for those who need to deploy and manage resources without the ability to modify access control.

3.

Reader:

-

The "Reader" role in Azure provides view-only access, allowing users to see and read resource configurations but not make any changes, making it suitable for individuals who require read-only access for monitoring or auditing purposes.