Assigning Roles In Azure

A Whitepaper Written For KAMIND IT, Inc.

By Ravi Das

Contents

Introduction

One of our previous blogs examined at a very high level what “Role Based Access Controls” (also known as “RBACs) are. Essentially with this methodology, you are assigning the rights, privileges, and permissions based upon not only the job title but also the specific job tasks that they do on a daily basis. This is based upon the premise of “Least Privilege”, where you and your employees are also given no more and no less than what they absolutely need.

In this whitepaper, we examine other roles in more depth, and how to assign them.

From The Few To The Many

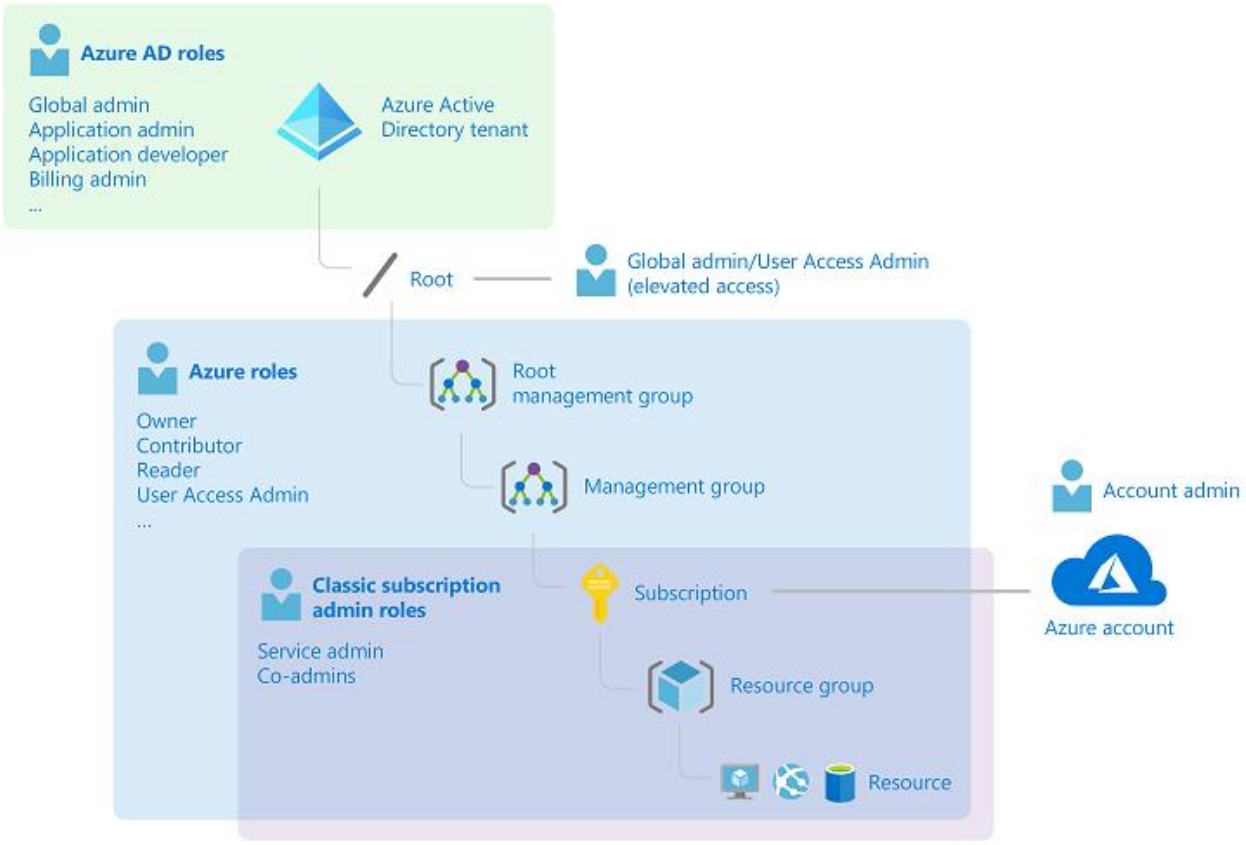
When Microsoft Azure first came out, there were only three basic roles, which are:

- The Account Administrator
- The Service Administrator
- The Co-Administrator (this was essentially a sub role, designed for employees with administrative tasks in the IT Department, such as the Network Administrator, Database Administrator, etc.).

But given the explosion of other technological factors, such as the Internet of Things (IoT), the Hybrid Workforce, Artificial Intelligence (AI) and Machine Learning (ML, advances in the Cyber Threat Landscape, etc., there has been a much greater need now to create a whole new slate of permissions, and the ways to assign them.

The Roles Now

The illustration below gives a high-level overview of the Roles that are now available in Microsoft Azure:



(SOURCE: 1).

The following matrix examines these roles in more detail:

Role	*Rights, Permissions, and Privileges*
The Owner	*Grants full access to manage all resources. *Assign roles in Azure RBAC.
The Contributor	*Grants full access to manage all resources. *Can't assign roles in Azure RBAC. *Can't manage assignments in Azure Blueprints or share image galleries.
The Reader	*Can view all of the Azure based resources.
	*Can manage user access to Azure resources.

The RBAC Administrator	*Can assign roles in Azure RBAC. *Can assign themselves or others the Owner role. *Can't manage access using other ways
The User Access Administrator	*Can manage user access to Azure resources * Can assign roles in Azure RBAC. *Can assign themselves or others the Owner role

(SOURCE: 1).

It should be noted that the above Roles are considered to be "global" in nature. The "Built In Roles" are those that manage the specific Microsoft Azure Resources. For a full and detailed listing of these, click on the link below:

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

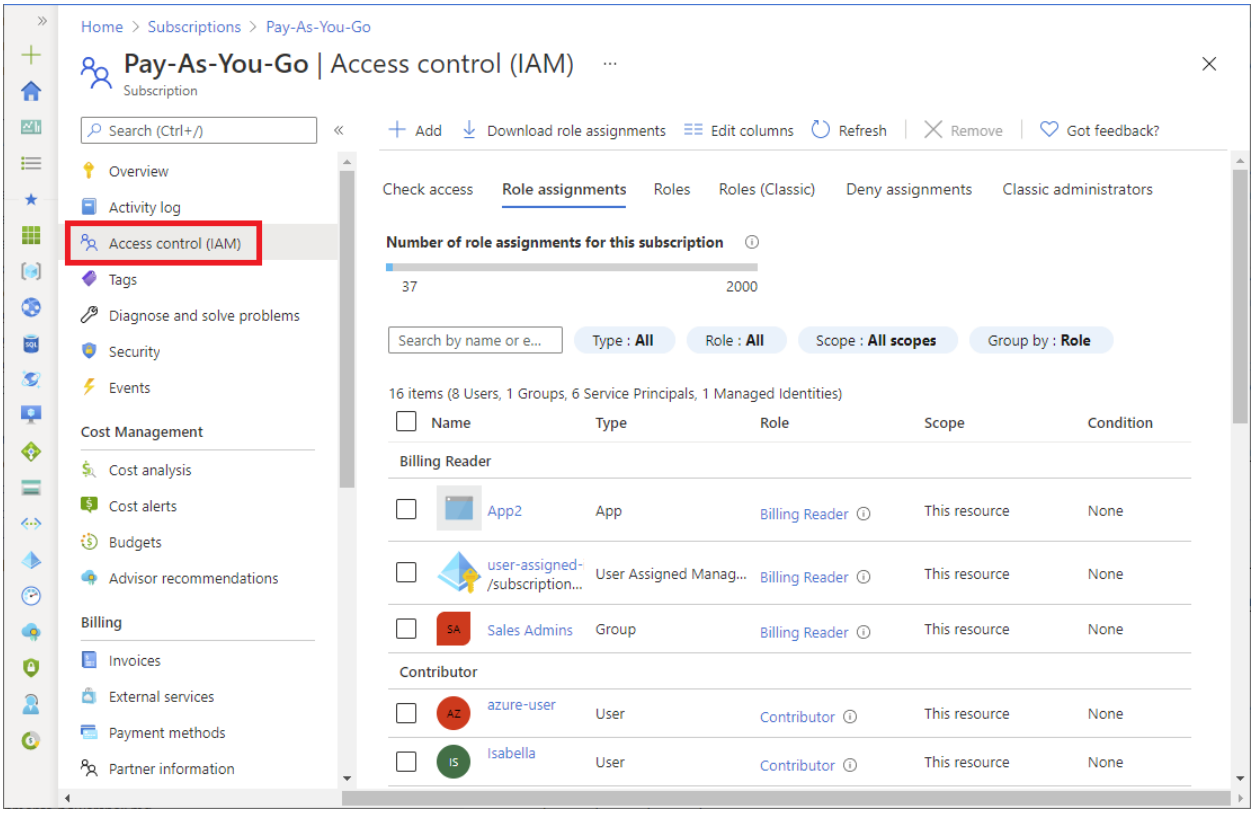
Accessing The Various Roles Tabs

To so this, follow these steps:

1) Log into Azure Portal:

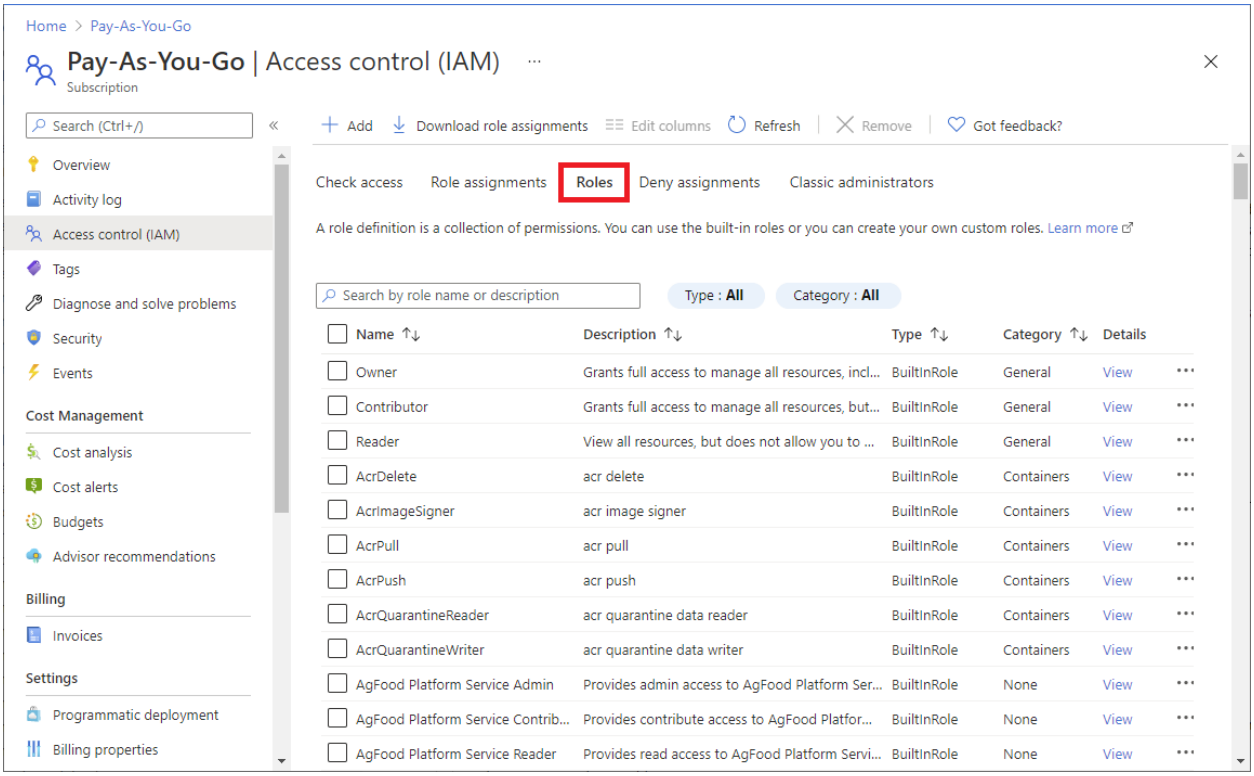
   Azure.portal.com

2) Navigate to the "Access Control (IAM)" page. This is illustrated in the diagram below:



(SOURCE: 1).

3) From the last step, click on the "Roles" tab to view the Built In Roles and any other customized Roles that you may create. This is illustrated in the diagram below:



(SOURCE: 1).

The Roles In Microsoft Entra

For the last twenty years, it has been the Azure Directory which as the heart of any Windows based Server Operating Systems. When it was first deployed into Microsoft Azure, it became known as the "Azure Active Directory", or the "AAD" for short. But just recently, the name of it has changed once again. Now it is called the "Microsoft Entra".

The Roles that are available in Microsoft Entra are exhibited in the matrix below:

Role	*Rights, Permissions, and Privileges*
The Global Administrator	*Manages access to all administrative features in Microsoft Entra ID, as well as services that federate to Microsoft Entra ID. *Assigns administrator roles to others. *Resets the password for any user and all other administrators.
The User Administrator	*Creates and manage all aspects of users and groups. *Manages support tickets. *Monitors service health of the deployed resources.

	*Changes passwords for users, Helpdesk administrators, and other User Administrators.
The Billing Administrator	*Can make purchases. *Manages subscriptions. *Manages support tickets. *Monitors service health

(SOURCE: 1).

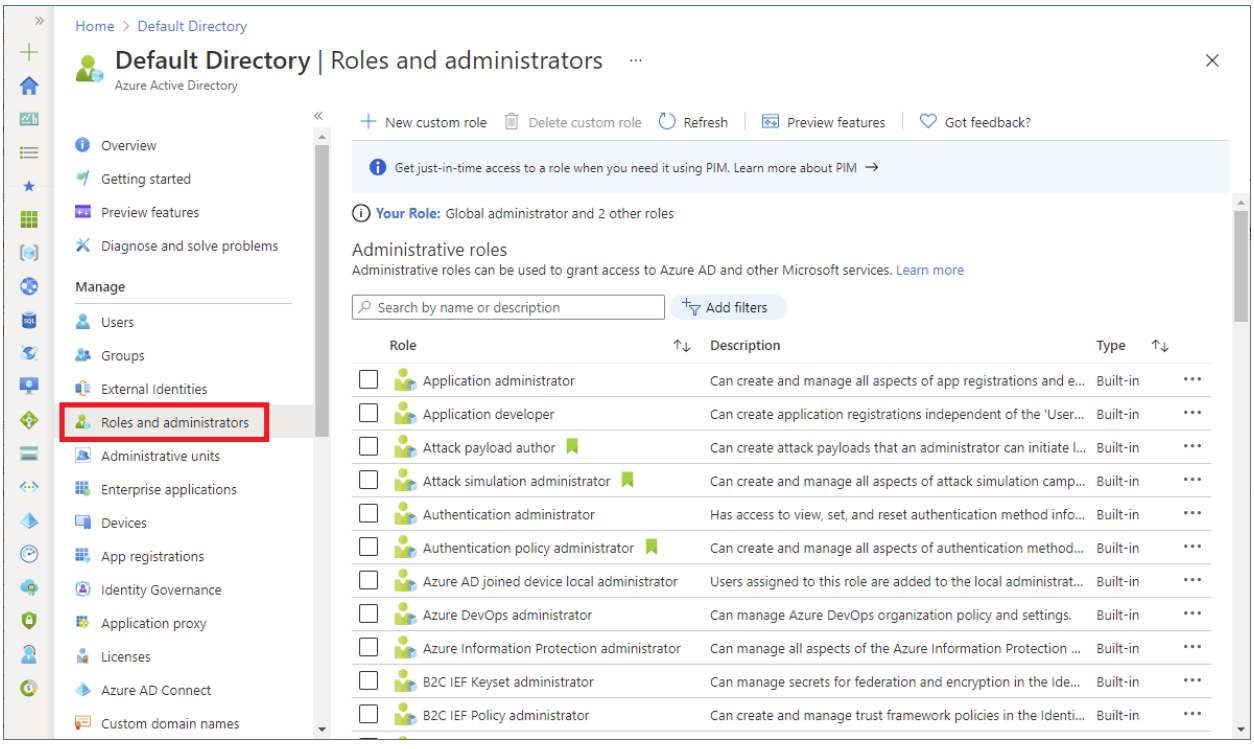
Accessing The Various Roles Tabs In Microsoft Entra

To so this, follow these steps:

1) Log into Azure Portal:

   Azure.portal.com

2) Navigate to the "Roles and Administrators" page. This is illustrated in the diagram below:



(SOURCE: 1).

It should also be noted that the above Roles reviewed in the above matrix are considered to be “global” in nature as well. For a comprehensive listing of all of the Built In Roles for Microsoft Entra, click on the link below:

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

A Deeper Dive Into The Traditional Roles In Microsoft Azure

At the beginning of this whitepaper, we took a look at the three traditional Roles that first evolved. At this point, it is important to review them in further detail, as can be seen in the matrix below:

Role	*Rights, Permissions, and Privileges*
The Account Administrator	*Can access the Azure portal and manage billing. *Manages the billing for all subscriptions in the account. *Creates new subscriptions. *Can cancel subscriptions. *Can change the billing for a subscription. *Can change the Service Administrator. *They can't cancel subscriptions unless they have the Service Administrator or subscription Owner role.
The Service Administrator	*Manages services in the Azure portal. *Can cancel the subscription. *Can assign users to the Co-Administrator role.
The Co Administrator	Same access privileges as above, but they can’t change the association of the differing subscriptions to the various Microsoft Entra directories. *Can assign users to the Co-Administrator role, but can't change the Service Administrator.

It should be noted that for all of the roles, only one Microsoft Azure subscription can be managed at a time.

Accessing The Traditional Roles Tabs In Microsoft Entra

To view and modify the settings for the Service Administrator and the Co Administrator, follow these steps:

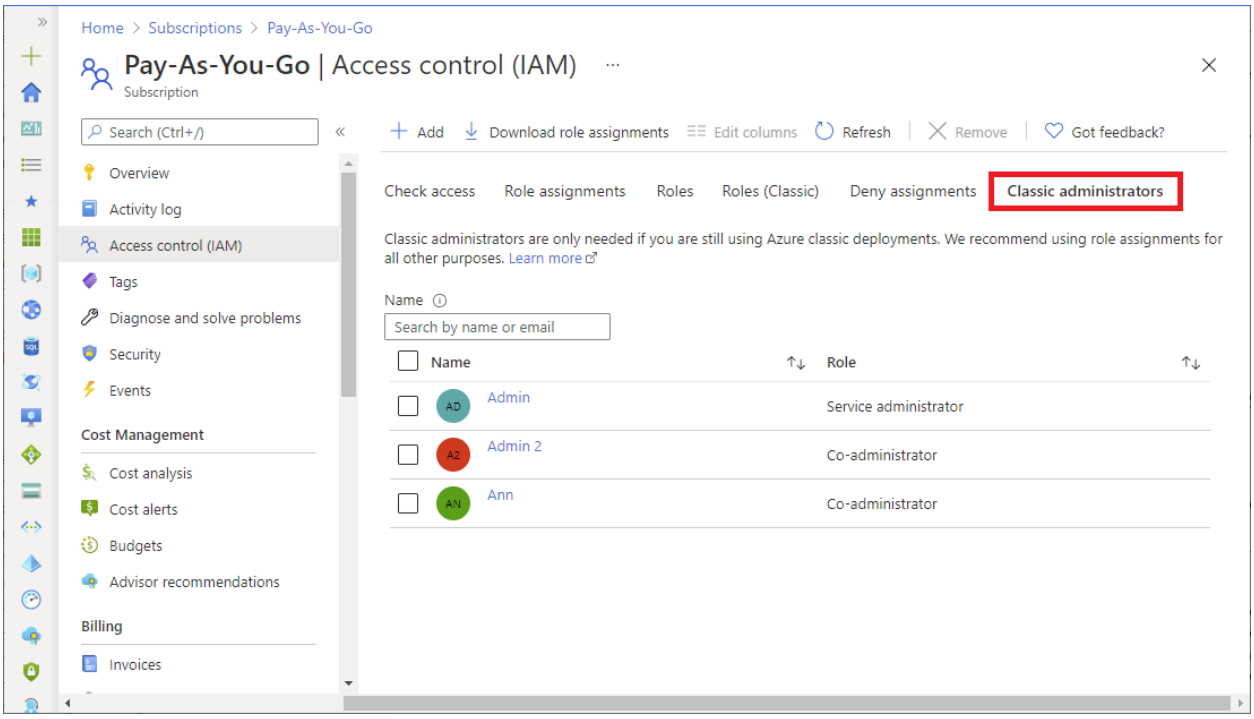
For Viewing

1) Log into Azure Portal:

   Azure.portal.com

2) Navigate to the “Access Control (IAM)” page.

3) Click on the “Classic Administrators” tab. This is illustrated in the diagram below:



(SOURCE: 1).

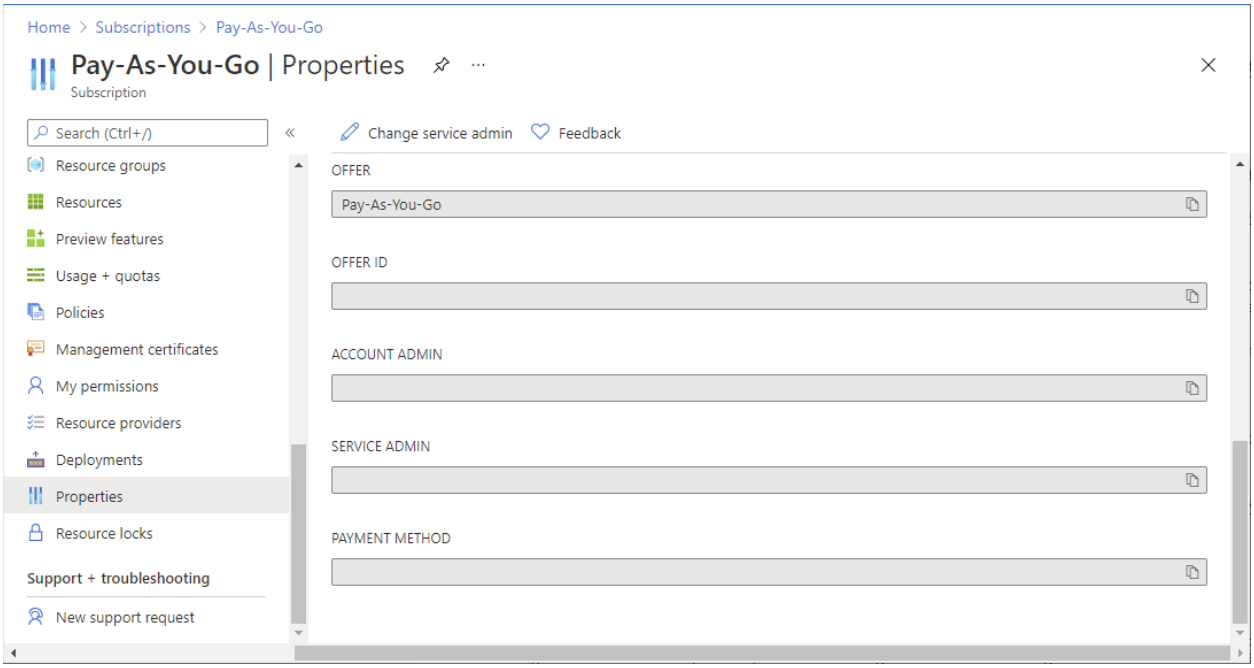
For Modifying The Properties

4) Log into Azure Portal:

   Azure.portal.com

5) Navigate to the “Access Control (IAM)” page.

6) Click on the “Properties” tab. This is illustrated in the diagram below:



(SOURCE: 1).

The Key Differences Between The Roles And The Microsoft Entra Roles

At this point, we have reviewed all of the Roles that are available in an overall Microsoft Azure subscription and those that are available specifically in Microsoft Entra. At this point, you might be wondering what some of the key differences between then. This is detailed in the matrix below:

The Microsoft Azure Roles	*The Microsoft Entra Roles*
*Can manage access to specific Azure resources.	*Can ***only manage*** Entra based resources.
*Can support the Customized Roles.	*Can support the Customized Roles.
*The Scope can be specified at these levels: ➢ The Management Group ➢ The Azure Subscription ➢ The Resource Group ➢ The specific Resource	*The Scope can be specified at these levels: ➢ The Tenant ➢ The Administrative Unit ➢ An individual Object
*Information and data about the Roles can be accessed from the following portals: ➢ The Azure Portal ➢ The Azure PowerShell ➢ The Azure Resource Manager Templates ➢ The REST APIs	*Information and data about the Roles can be accessed from the following portals: ➢ The Azure Administrative Portal ➢ The M365 Administrative Center ➢ The Microsoft Graph ➢ The AzureAD PowerShell

(SOURCE: 1).

How To Assign The Roles In Microsoft Azure

To start assigning roles and their corresponding roles, rights, and responsibilities in Microsoft Azure, follow these steps:

1) Ascertain the needed scope:

   For purposes of this whitepaper, a Scope can be defined as follows:

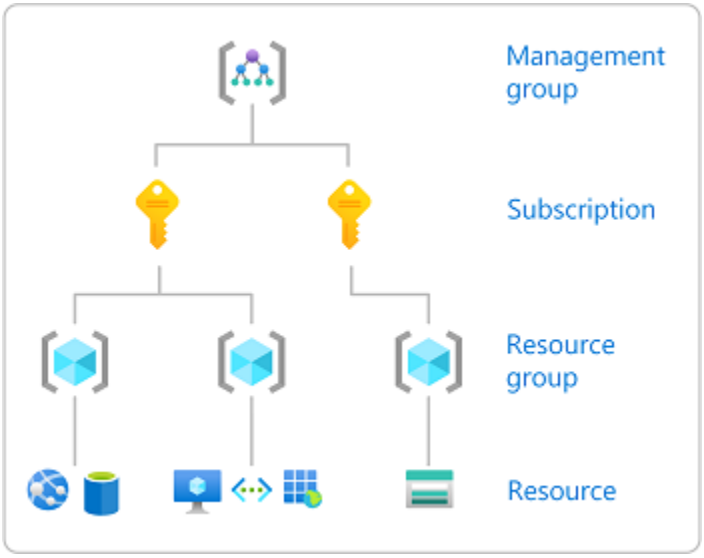
   "Scope is the set of resources the access applies to. In Azure."

   (SOURCE: 1)

   It is important to note that you can specify a Scope at four distinct levels:

   - The Management Group
   - The Resource
   - The Resource Group
   - The Subscription

   This is illustrated in the diagram below:



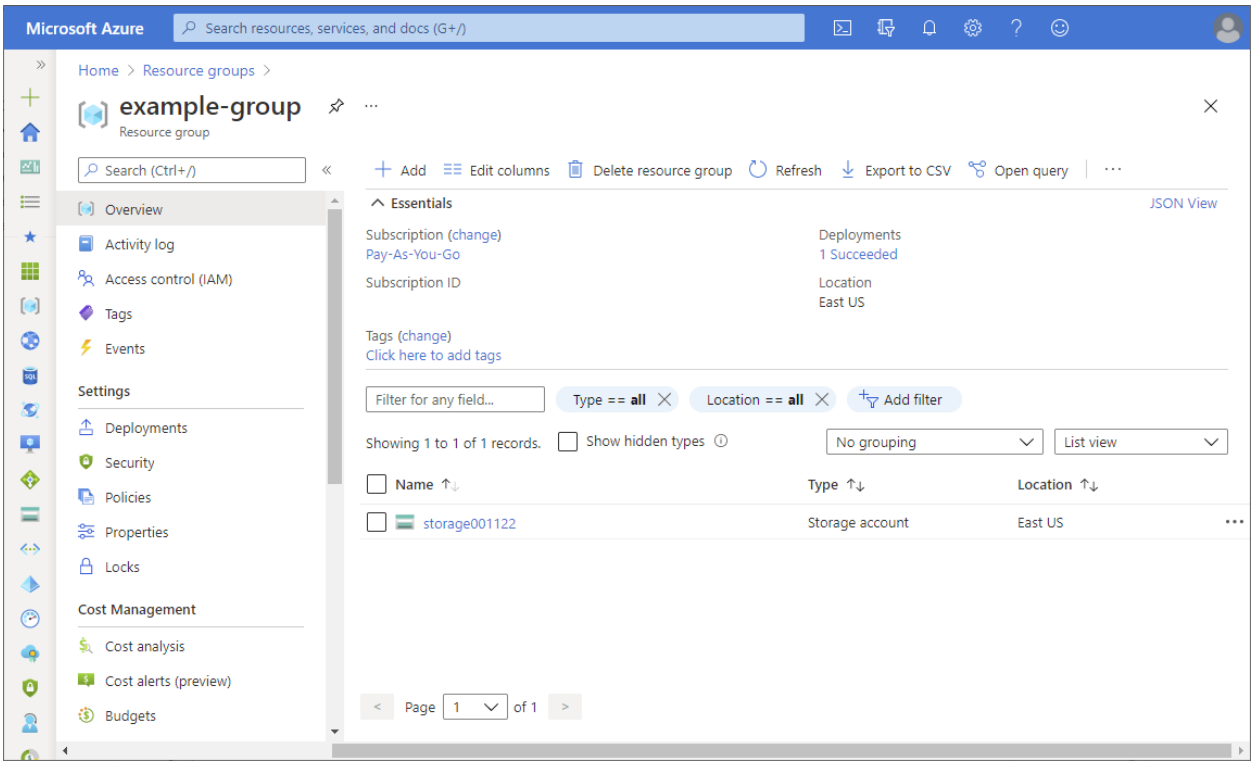
   (SOURCE: 2).

   *Log into your Microsoft Azure portal:

   (portal.azure.com)

   *A Search Box will appear, and from here, select the appropriate Scope you need to assign the permissions to, as just previously described.

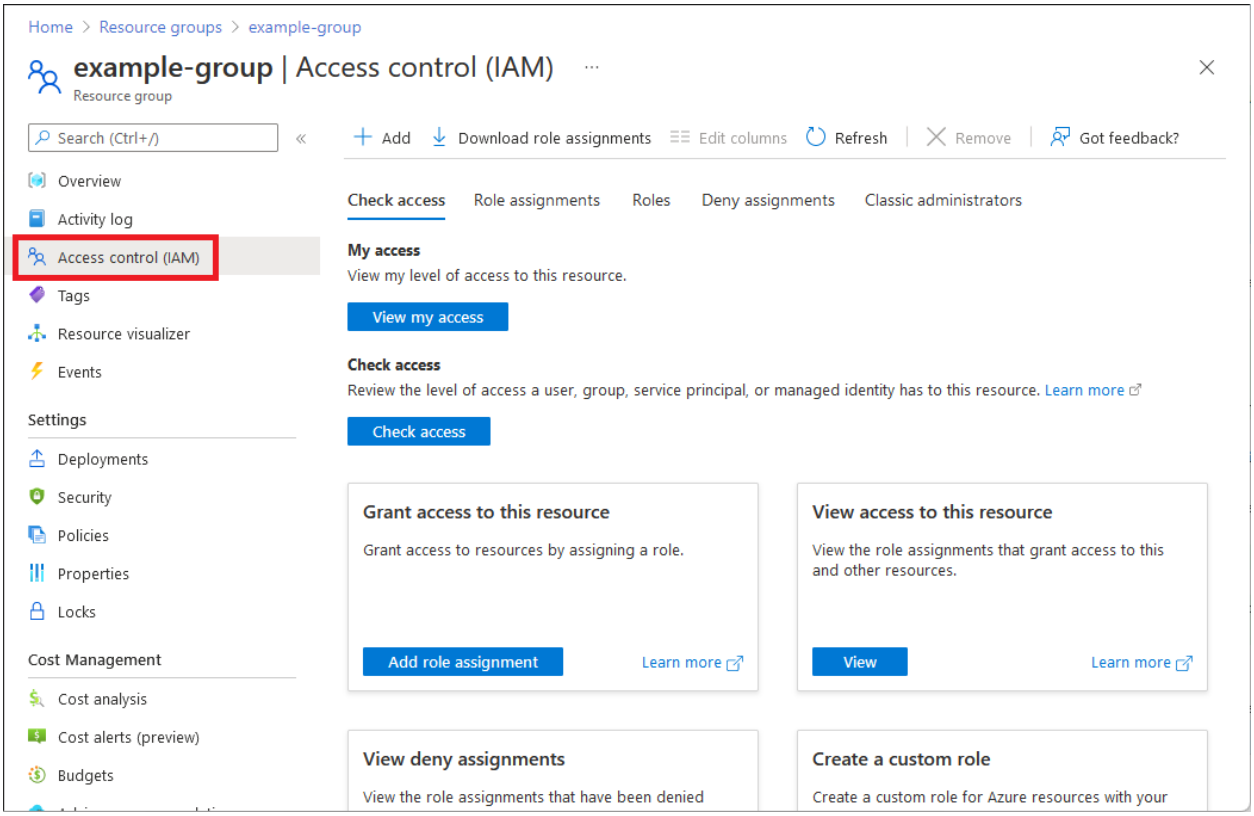
   *Click on that specific Resources. This is illustrated in the diagram below:



(SOURCE: 2).

2) Click on the “Access Control (IAM)” tab:

This is illustrated below:



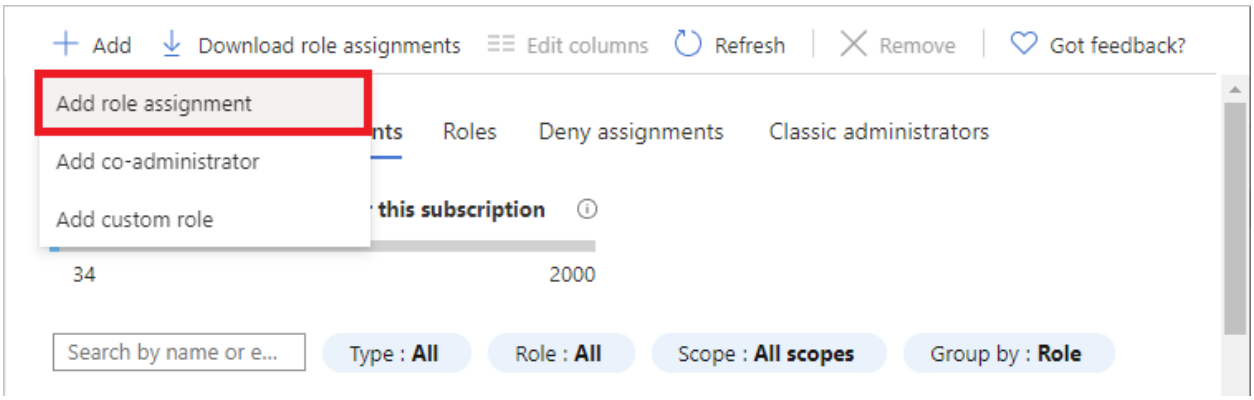
(SOURCE: 2).

It is important to note that this is the place where all of the permissions, rights, and privileges are granted to the employees for them to access the resources in Microsoft Azure.

3) Click on the "Role Assignments" tab to view any Role Assignments that may have been populated ahead of time.
4) Click on:

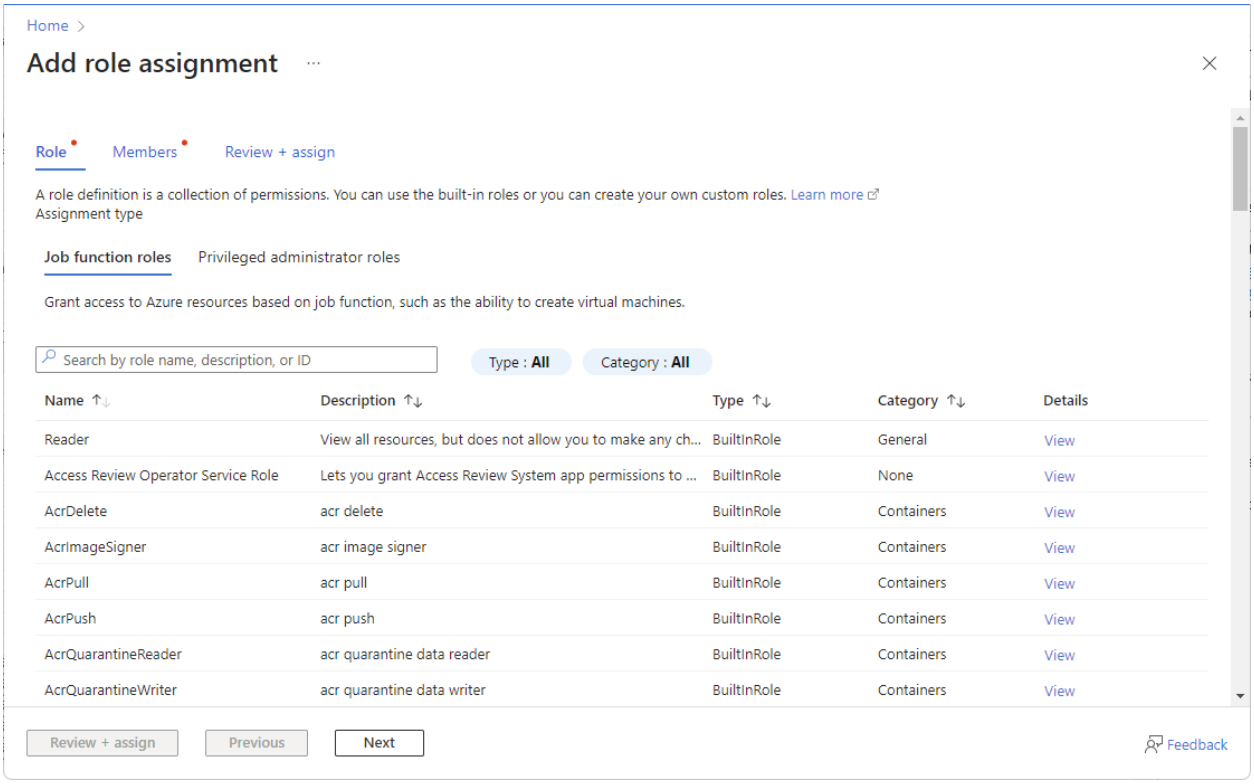
   - Add
   - Add Role Assignments

This can be seen in the diagram below:



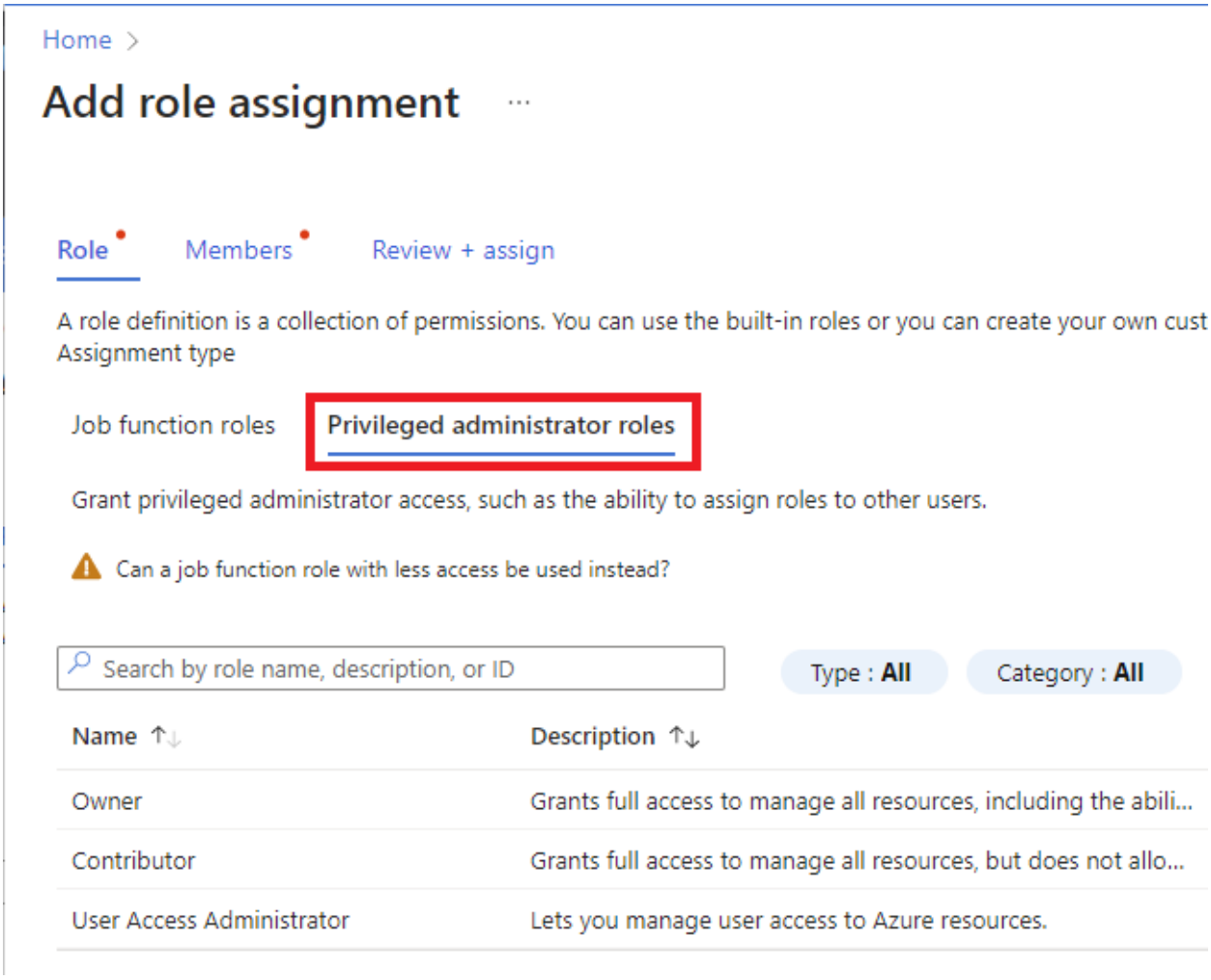
(SOURCE: 2).

5) The "Role Assignments" tab will now appear. From here, select the appropriate Role. An example of this page can be seen in the diagram below:



(SOURCE: 2).

NOTE: If you want to assign Privileged Access rights, permissions, and privileges, simply click on the "Privileged Administrator Roles" tab. This can be seen below:

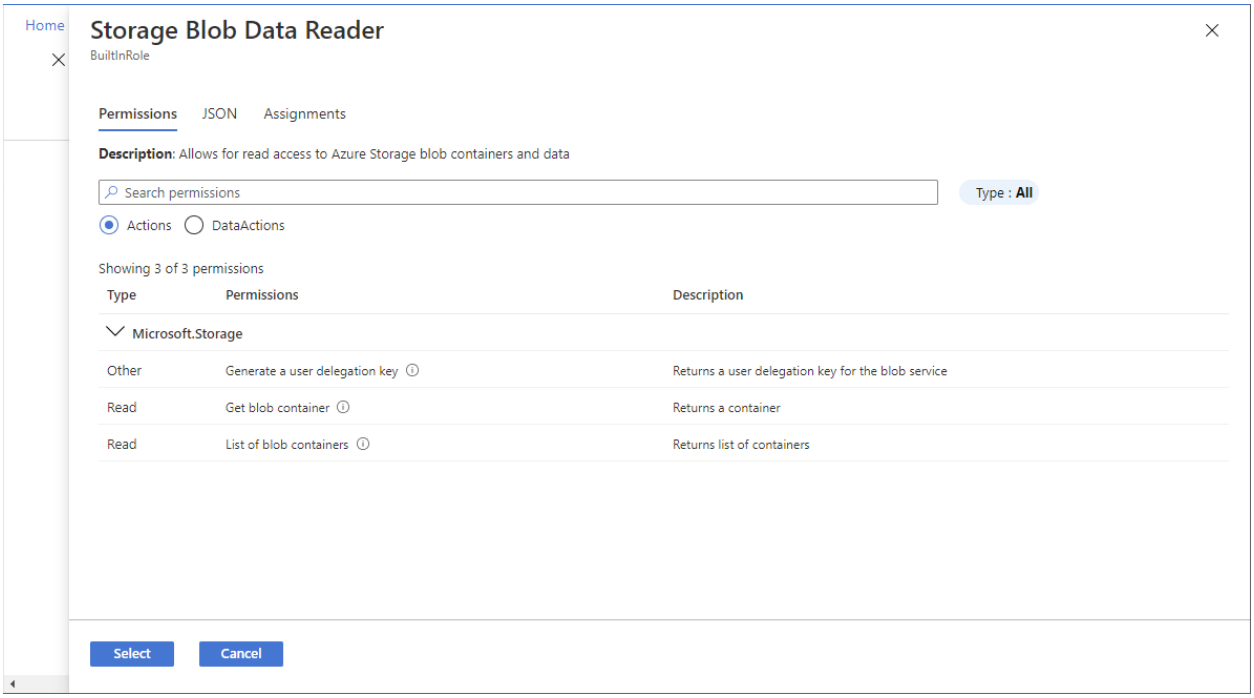


(SOURCE: 2).

If you need more help in how to set up the Privileged Access Accounts, refer to the link below:

https://learn.microsoft.com/en-us/azure/role-based-access-control/best-practices#limit-privileged-administrator-role-assignments

6) There will also be a “Details” column that will now appear. Click on “View” if you want to see more information about the Privileged Access Account(s) that you have just created. This can also be seen in the illustration below:

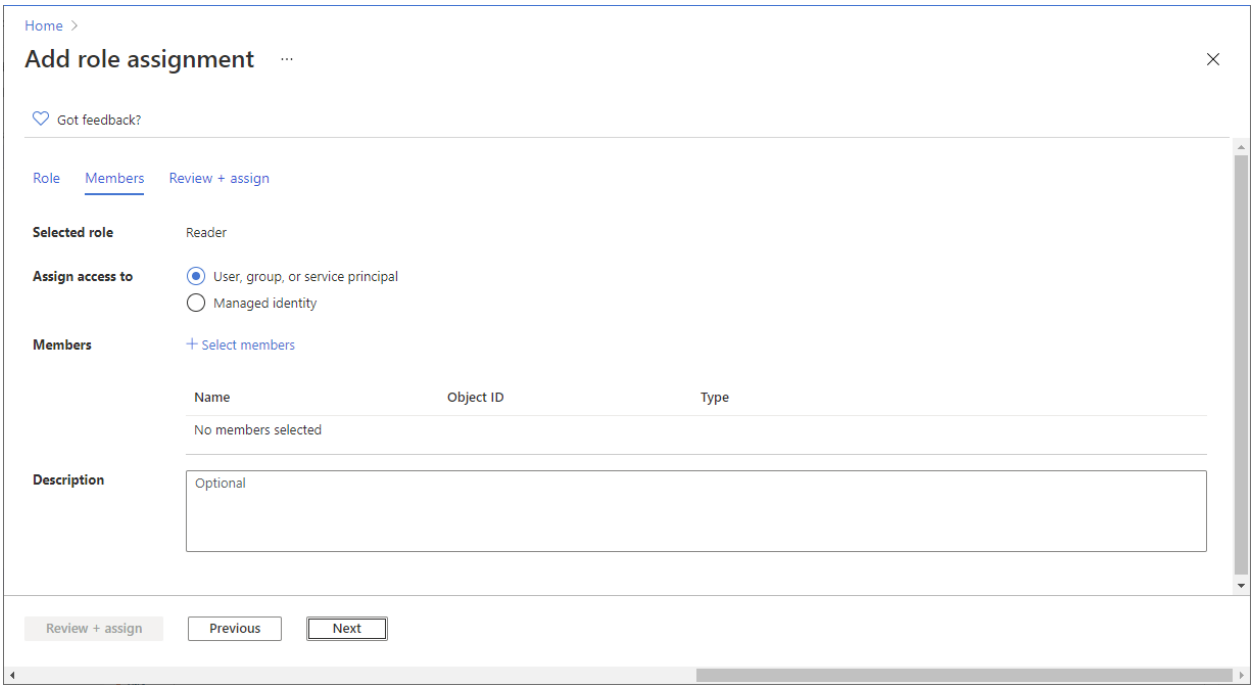


(SOURCE: 2).

7) Click on “Next”.

8) At this point, you need to decide now who will get the rights, permissions, and privileges to which resource(s). Once you have decided this, follow these steps:

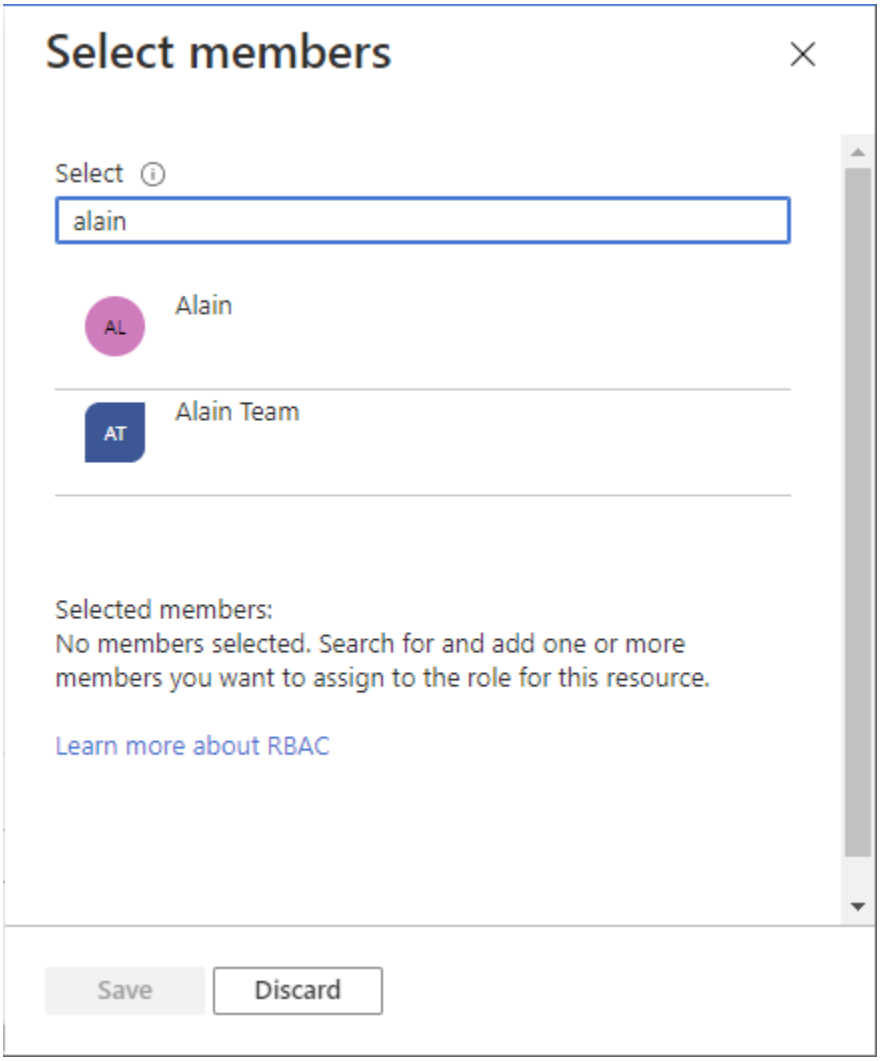
   *Select the “User, Group, or Service Principal” to assign the newly created role. This can be seen in the illustration below:



(SOURCE: 2).

9) Click on “Select Members”.

10) You can use the “Select Members” box to find the name of the employee and their associated contact information. This is illustrated below:



(SOURCE: 2).

11) Click on “Select Users, Groups, or Service Principals” to the Members list.

12) Select the “Managed Identity” option if you need to assign the roles to two or more Managed Identities.

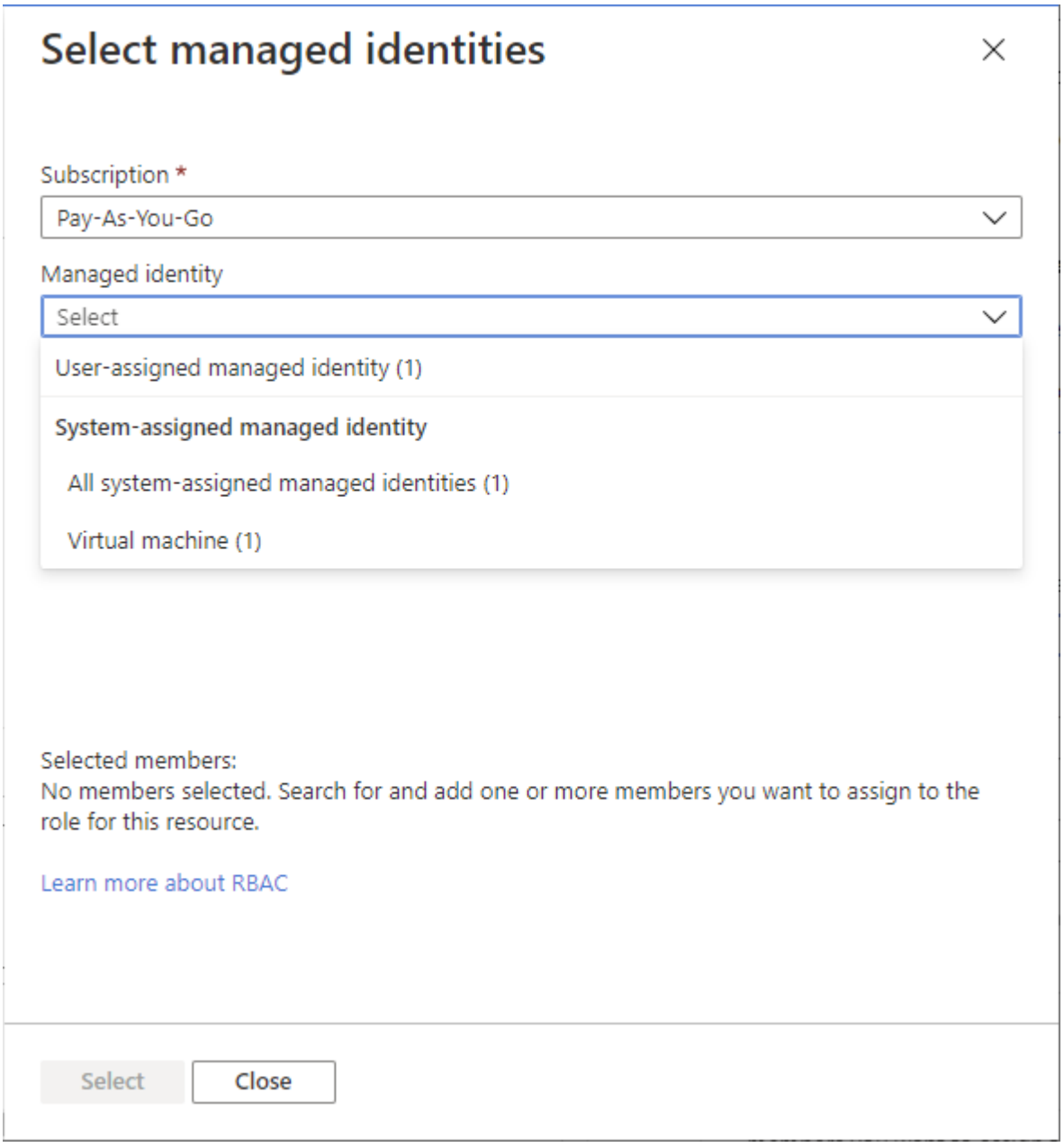
13) Click on “Select Members”.

14) The “Select Managed Identities” window will now appear, and from here, you will need to select of the following options:

- The User Assigned Managed Identity (More information can be found here: https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/overview)

- The System Assigned Managed Identity (More information can be found here: https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/overview)

15) Locate and select the "Managed Identities". This is illustrated in the diagram below:



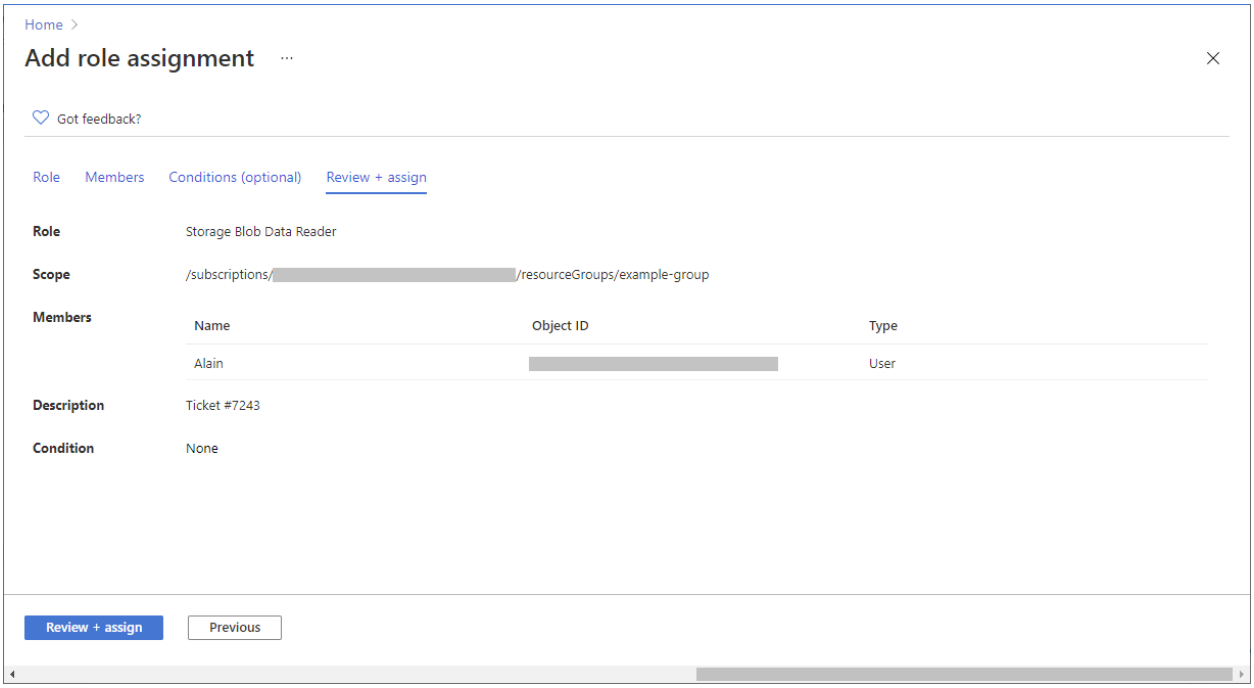
(SOURCE: 2).

16) Click on the "Select" button to add the selected "Managed Identities" for their particular Role Assignments.

17) In the “Description” box, you can add some more details about the particular roles (this is entirely optional to do).

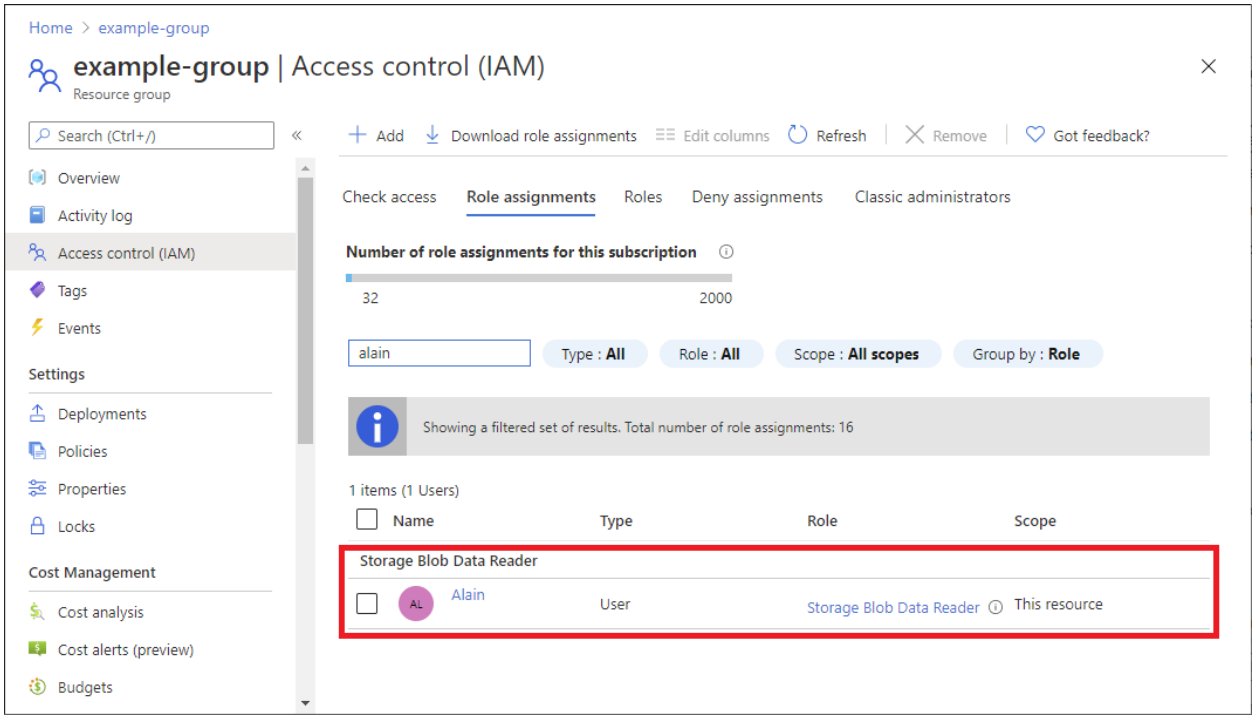
18) Click on “Next”.

19) Now, the “Review + Assign” tab will appear. From here, you can review in detail all of the roles and assignments that you have created. This is illustrated in the diagram below:



(SOURCE: 2).

20) To finally assign the role, click on the “Review + Assign” button. The Scope will now be assigned to it. This is illustrated in the diagram below:



(SOURCE: 2).

NOTE: You can still add information about the particular role by clicking on the "Edit Columns" feature.

Conclusions

Overall, this whitepaper has examined what the Roles are in Microsoft Azure, and how to assign them. If you have further questions or need help in doing this, please contact us.

Sources

1) https://learn.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles
2) https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal?tabs=delegate-condition