Assigning Roles In Azure A Whitepaper Written For KAMIND IT, Inc.



By Ravi Das

Contents

| Introduction | 3 |
|---|----|
| From The Few To The Many | 3 |
| The Roles Now | 4 |
| Accessing The Various Roles Tabs | 5 |
| The Roles In Microsoft Entra | 7 |
| Accessing The Various Roles Tabs In Microsoft Entra | 8 |
| A Deeper Dive Into The Traditional Roles In Microsoft Azure | 9 |
| Accessing The Traditional Roles Tabs In Microsoft Entra1 | .0 |
| For Viewing1 | 0 |
| For Modifying The Properties1 | 0 |
| The Key Differences Between The Roles And The Microsoft Entra Roles | .1 |
| How To Assign The Roles In Microsoft Azure1 | .2 |
| Conclusions2 | 2 |
| Sources2 | 2 |

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

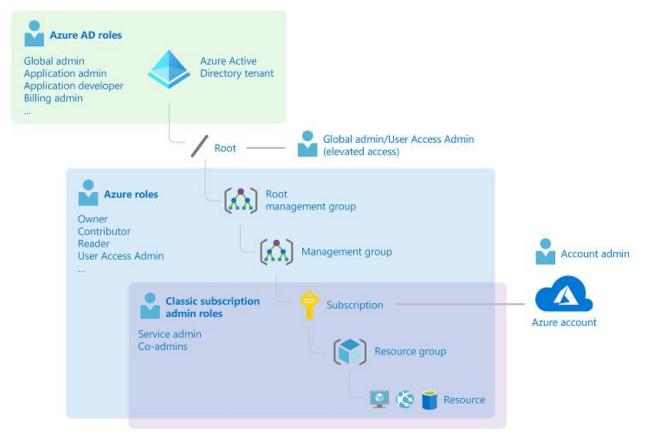
When Microsoft Azure first came out, there were only three basic roles, which are:

- 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:

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 |

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:

| >> | Home > Subscriptions > Pay-As-You-G | D | | | | | |
|----------|--|--------------------------------|----------------------------|----------------------|-------------------|----------------|----------|
| + | Reversion Pay-As-You-Go Act | cess control (IAM) | | | | | \times |
| | Subscription P Search (Ctrl+/) « | + Add ↓ Download role | e assignments 🛛 🗮 Edit c | olumns () Refresh | X Pamaya | Got foodback? | |
| = | | | | olumns 🔾 Reliesh | X Remove | GOT REGDACK: | |
| * | Overview | Check access Role assign | ments Roles Role | es (Classic) Deny as | signments Classic | administrators | - 1 |
| | Activity log | | | _ | | | |
| | Access control (IAM) | Number of role assignment: | for this subscription | 0 | | | - 8 |
| () | 🔷 Tags | 37 | 200 | 00 | | | - 1 |
| ۲ | Diagnose and solve problems | | | | | | - 1 |
| SQL | 🌻 Security | Search by name or e | Type : All Role : | All Scope : All s | Group by : | Role | - 1 |
| 8 | 🗲 Events | 16 items (8 Users, 1 Groups, 6 | Service Principals, 1 Mana | aged Identities) | | | |
| • | Cost Management | Name | Туре | Role | Scope | Condition | |
| • | Section Cost analysis | Billing Reader | | | | | |
| | Cost alerts | App2 | Арр | Billing Reader 🛈 | This resource | None | |
| | Budgets | | | | | | |
| ◆ ⊘ | Advisor recommendations | user-assigned /subscription. | | Billing Reader 🛈 | This resource | None | |
| | Billing | SA Sales Admins | Group | Billing Reader 🛈 | This resource | None | |
| 0 | Invoices | Contributor | | | | | |
| 2 | External services | Az azure-user | User | Contributor (1) | This resource | None | |
| 6 | Payment methods | | | contributor () | | | |
| | ⁸ ∞ Partner information | Isabella | User | Contributor 🛈 | This resource | None | - |
| | ٩ | | | | | | Þ |

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:

| Pay-As-You-Go A | ccess control (IAM) | | | | | × |
|-----------------------------|--------------------------------------|--|----------------------------|---------------------|---------|-------|
| P Search (Ctrl+/) | + Add 🔸 Download role | assignments | X Remove | Got feedback? | | |
| Overview Activity log | Check access Role assignm | | ssic administrators | | | |
| Access control (IAM) | A role definition is a collection of | f permissions. You can use the built-in roles or | you can create your own cu | stom roles. Learn n | nore 🗗 | |
| Tags | | | | | | |
| Diagnose and solve problems | Search by role name or des | cription Type : All Ca | tegory : All | | | |
| Security | Name ↑↓ | Description ↑↓ | Туре ↑↓ | Category ↑↓ | Details | |
| Events | Owner | Grants full access to manage all reso | urces, incl BuiltInRole | General | View | ••• |
| ost Management | Contributor | Grants full access to manage all reso | urces, but BuiltInRole | General | View | ••• |
| Cost analysis | Reader | View all resources, but does not allo | w you to BuiltInRole | General | View | ••• |
| Cost alerts | AcrDelete | acr delete | BuiltInRole | Containers | View | ••• |
| Budgets | AcrImageSigner | acr image signer | BuiltInRole | Containers | View | • • • |
| Advisor recommendations | AcrPull | acr pull | BuiltInRole | Containers | View | ••• |
| | AcrPush | acr push | BuiltInRole | Containers | View | ••• |
| illing | AcrQuarantineReader | acr quarantine data reader | BuiltInRole | Containers | View | ••• |
| Invoices | AcrQuarantineWriter | acr quarantine data writer | BuiltInRole | Containers | View | ••• |
| ettings | AgFood Platform Service | Admin Provides admin access to AgFood Pl | atform Ser BuiltInRole | None | View | ••• |
| | | | d Platfor BuiltInRole | | | |

(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 |

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:

| >> | Home > Default Directory | | |
|-------------|---|--|-----|
| + | Azure Active Directory | Roles and administrators | × |
| | < | K + New custom role 📋 Delete custom role 💍 Refresh 💀 Preview features 🛇 Got feedback? | |
| ≔ * | Overview Getting started | lacksquare Get just-in-time access to a role when you need it using PIM. Learn more about PIM $ ightarrow$ | |
| | +- Preview features | () Your Role: Global administrator and 2 other roles | |
| [13] | 🔀 Diagnose and solve problems | Administrative roles | |
| ۲ | Manage | Administrative roles can be used to grant access to Azure AD and other Microsoft services. Learn more | |
| SQL | 🚨 Users | P Search by name or description + → Add filters | |
| 32 | A Groups | Role 1 Description Type 1 | ł. |
| | External Identities | Can create and manage all aspects of app registrations and e Built-in | |
| | Roles and administrators | Can create application registrations independent of the 'User Built-in | ••• |
| = | Administrative units | 🗌 🍰 Attack payload author 📕 Can create attack payloads that an administrator can initiate I Built-in | ••• |
| ~ -> | Enterprise applications | 🗌 🍰 Attack simulation administrator 📕 🛛 Can create and manage all aspects of attack simulation camp Built-in | |
| ٠ | Devices | 🗌 🍰 Authentication administrator 🛛 Has access to view, set, and reset authentication method info 🛛 Built-in | |
| ۲ | App registrations | 🗌 🍰 Authentication policy administrator 📕 🛛 Can create and manage all aspects of authentication method Built-in | |
| | Identity Governance | 🗌 🍰 Azure AD joined device local administrator 🛛 Users assigned to this role are added to the local administrat Built-in | |
| 0 | Application proxy | 🗌 🍰 Azure DevOps administrator Can manage Azure DevOps organization policy and settings. Built-in | |
| 2 | 🔓 Licenses | 🗌 🍰 Azure Information Protection administrator 🛛 Can manage all aspects of the Azure Information Protection 🛛 Built-in | |
| 0 | Azure AD Connect | 🗌 🍰 B2C IEF Keyset administrator Can manage secrets for federation and encryption in the Ide Built-in | |
| | 🔁 Custom domain names | B2C IEF Policy administrator Can create and manage trust framework policies in the Identi Built-in | ••• |

(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:

| » + | Home > Subscriptions > Pay-As-You- | | |
|-----------|------------------------------------|--|-------------------------|
| | Pay-As-You-Go Ad | ccess control (IAM) … | × |
| ⊠h | ✓ Search (Ctrl+/) « | 🕂 Add 🞍 Download role assignments 📰 Edit columns 💍 Refresh 🛛 🗙 Remove 🗍 💝 Got feedback | ? |
| = | 🕈 Overview 🌰 | Check access Role assignments Roles Roles (Classic) Deny assignments Classic administrators | 7 |
| * | Activity log | Check access Role assignments Roles Roles (Classic) Deny assignments Classic administrators | |
| | Access control (IAM) | Classic administrators are only needed if you are still using Azure classic deployments. We recommend using role assign all other purposes. Learn more 🖻 | ments for |
| [] | 🔷 Tags | Name ① | |
| ٢ | Diagnose and solve problems | Search by name or email | |
| 501 | Security | Name ↑↓ Role | \uparrow_{\downarrow} |
| <u> 3</u> | 🗲 Events | Admin Service administrator | |
| • | Cost Management | Admin 2 Co-administrator | |
| | 🎗 Cost analysis | | |
| | 🏮 Cost alerts | Co-administrator | |
| | 3 Budgets | | |
| P | Advisor recommendations | | |
| | Billing | | |
| O | Invoices | | |
| | 4 | | Þ |

(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:

| Home > Subscriptions > Pay- | As-You-G | io | | |
|-----------------------------|----------|-----------------------------------|--------------|---|
| Pay-As-You-Go | o Pro | operties 🖈 … | × | |
| ₽ Search (Ctrl+/) | ~ | 🖉 Change service admin 🛇 Feedback | | |
| Resource groups | * | OFFER | | * |
| Resources | | Pay-As-You-Go | \mathbb{D} | |
| Preview features | | | | |
| Usage + quotas | | OFFER ID | D. | |
| Policies | | | | |
| 🐖 Management certificates | | ACCOUNT ADMIN | | |
| A My permissions | | | \Box | |
| š≡ Resource providers | | | | |
| 📩 Deployments | - 1 | SERVICE ADMIN | | |
| Properties | | | | I |
| A Resource locks | | PAYMENT METHOD | | I |
| Support + troubleshooting | . 1 | | \mathbb{D} | I |
| 📯 New support request | | | | Ţ |
| 4 | | | | Þ |



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:

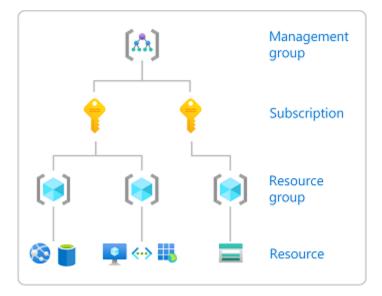
"Scope is the set of resources the access applies to. In Azure."

(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:



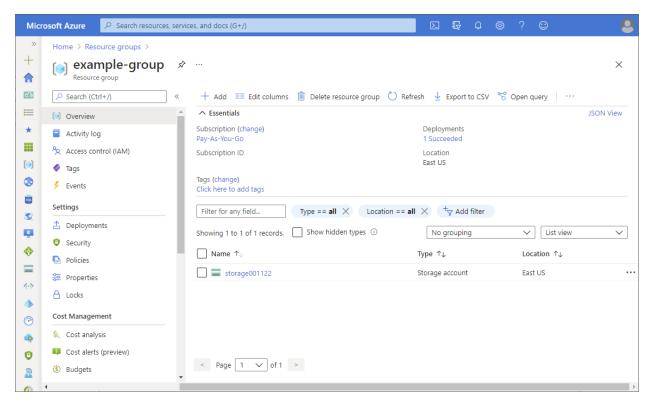
(SOURCE: 2).

*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:



2) Click on the "Access Control (IAM)" tab:

This is illustrated below:

| Home > Resource groups > example-g | roup | | | | | |
|---------------------------------------|--|---|----------|--|--|--|
| Resource group | cess control (IAM) | | \times | | | |
| ₽ Search (Ctrl+/) « | 🕂 Add 🞍 Download role assignments 🛛 🗉 Edit columns | 💍 Refresh \mid $	imes$ Remove \mid $ otin \qquad$ Got feedback? | | | | |
| 间 Overview | Overview Check access Role assignments Roles Deny assignments Classic administrators | | | | | |
| Activity log | | | | | | |
| ^ମ ନ୍ନ Access control (IAM) | My access | | | | | |
| 🗳 Tags | View my level of access to this resource. | | | | | |
| 🛧 Resource visualizer | View my access | | | | | |
| 🗲 Events | Check access | | | | | |
| Settings | Review the level of access a user, group, service principal, or m | anaged identity has to this resource. Learn more 🗠 | | | | |
| Deployments | Check access | | | | | |
| Security | | | | | | |
| Policies | Grant access to this resource | View access to this resource | | | | |
| Properties | Grant access to resources by assigning a role. | View the role assignments that grant access to this and other resources. | | | | |
| A Locks | | | | | | |
| | | | | | | |
| Cost Management | Add role assignment Learn more 🗗 | View Learn more | 8 | | | |
| S. Cost analysis | | | | | | |
| Cost alerts (preview) | View deny assignments | Create a custom role | | | | |
| ③ Budgets | View the role assignments that have been denied | Create a custom role for Azure resources with your | | | | |
| A 10 P | then are role assignments and have been defined | create a custom role for Azare resources with your | | | | |

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:

| Add role assignment | nts Roles Deny assignments Classic administrators |
|----------------------|---|
| Add co-administrator | |
| Add custom role | this subscription ① |
| 34 | 2000 |

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:

| Home > | | | | | |
|---|---|--------------------------|-------------|------------|---|
| Add role assignment | | | | × | |
| | | | | | * |
| Role Members Review + ass | sign | | | | |
| A role definition is a collection of permissio Assignment type | ns. You can use the built-in roles or you can create your own | custom roles. Learn more | ď | | ł |
| Job function roles Privileged admin | histrator roles | | | | |
| Grant access to Azure resources based on | job function, such as the ability to create virtual machines. | | | | |
| | | | | | |
| $^{ ho}$ Search by role name, description, or ID | Type : All Category : All | | | | |
| Name 🛧 | Description \uparrow_{\downarrow} | Type ↑↓ | Category ↑↓ | Details | |
| Reader | View all resources, but does not allow you to make any ch | BuiltInRole | General | View | |
| Access Review Operator Service Role | Lets you grant Access Review System app permissions to | BuiltInRole | None | View | |
| AcrDelete | acr delete | BuiltInRole | Containers | View | |
| AcrImageSigner | acr image signer | BuiltInRole | Containers | View | |
| AcrPull | acr pull | BuiltInRole | Containers | View | |
| AcrPush | acr push | BuiltInRole | Containers | View | |
| AcrQuarantineReader | acr quarantine data reader | BuiltInRole | Containers | View | |
| AcrQuarantineWriter | acr quarantine data writer | BuiltInRole | Containers | View | - |
| Review + assign Previous | Next | | | & Feedback | k |

(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:

| Home > | | | | | |
|--|---|--|--|--|--|
| Add role assignment | Add role assignment | | | | |
| | | | | | |
| Role Members Review | + assign | | | | |
| A role definition is a collection of perm Assignment type | issions. You can use the built-in roles or you can create your own cust | | | | |
| Job function roles | dministrator roles | | | | |
| Grant privileged administrator access | , such as the ability to assign roles to other users. | | | | |
| 🛕 Can a job function role with less acc | tess be used instead? | | | | |
| | | | | | |
| \mathcal{P} Search by role name, description, (| or ID Type : All Category : All | | | | |
| Name $\uparrow \downarrow$ | Description ↑↓ | | | | |
| Owner | Grants full access to manage all resources, including the abili | | | | |
| Contributor | Grants full access to manage all resources, but does not allo | | | | |
| User Access Administrator | Lets you manage user access to Azure resources. | | | | |
| | | | | | |

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:

| P Search pe | Allows for read access to Azure Storage blob containers and | Type : All |
|----------------|---|--|
| | O DataActions | туре . Ап |
| Showing 3 of : | 3 permissions | |
| Туре | Permissions | Description |
| | ft.Storage | |
| Other | Generate a user delegation key 🛈 | Returns a user delegation key for the blob service |
| Read | Get blob container ① | Returns a container |
| Read | List of blob containers ① | Returns list of containers |
| | | |
| | | |



- 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:

| Home > | | | | |
|------------------|---|-----------|------|---|
| Add role ass | signment … | | | × |
| ♡ Got feedback? | | | | |
| Role Members | Review + assign | | | |
| Selected role | Reader | | | |
| Assign access to | User, group, or service principal Managed identity | | | |
| Members | + Select members | | | |
| | Name | Object ID | Туре | |
| | No members selected | | | |
| Description | Optional | | | |
| | | | | |
| Review + assign | Previous Next | | | |
| | | | | |

- 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:

| Select members | \times |
|--|----------|
| Select 🗊 alain | |
| AL | |
| Alain Team | |
| Selected members: No members selected. Search for and add one or more members you want to assign to the role for this resource. Learn more about RBAC | |
| | - |
| Save Discard | |

- 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: <u>https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/overview</u>)

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

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

| Select managed identities | × |
|--|--------|
| Subscription * | |
| Pay-As-You-Go | \sim |
| Managed identity | |
| Select | \sim |
| User-assigned managed identity (1) | |
| System-assigned managed identity | |
| All system-assigned managed identities (1) | |
| Virtual machine (1) | |
| Selected members: No members selected. Search for and add one or more members you want to assign to t role for this resource. Learn more about RBAC | :he |
| Select Close | |

(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:

| Home > | | | | |
|-----------------|------------------------------------|-------------------------------|------|---|
| Add role as | signment … | | | × |
| ♡ Got feedback? | | | | |
| Role Members | Conditions (optional) Review + ass | ign | | |
| Role | Storage Blob Data Reader | | | |
| Scope | /subscriptions/ | /resourceGroups/example-group | | |
| Members | Name | Object ID | Туре | |
| | Alain | | User | |
| Description | Ticket #7243 | | | |
| Condition | None | | | |
| | | | | |
| | | | | |
| | | | | |
| Review + assign | Previous | | | |
| | | | | |

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:

| Home > example-group | | | | | |
|---------------------------|--------------------------|-------------------------------|----------------------------|--------------------------|---|
| Resource group | cess control (IAM |) | | | × |
| | 🕂 Add 🞍 Download ro | ole assignments 🛛 🗏 Ed | it columns 💍 Refresh 🛛 🗙 | Remove 🛛 💙 Got feedback? | |
| Overview Activity log | Check access Role assig | gnments Roles D | eny assignments Classic ad | ministrators | |
| | Number of role assignmen | te fer this subscription | (i) | | |
| Access control (IAM) | Number of role assignmen | its for this subscription | 0 | | |
| Tags | 32 | : | 2000 | | |
| Events | alain | Type : All Rol | e : All Scope : All scopes | Group by : Role | |
| Settings | alalii | Type : All Kor | scope : All scopes | Group by : Kole | |
| 1 Deployments | Showing a filtered | l set of results. Total numbe | er of role assignments: 16 | | |
| Policies | | | | | |
| 😂 Properties | 1 items (1 Users) | | | | |
| 🔒 Locks | Name | Туре | Role | Scope | |
| Cost Management | Storage Blob Data Reader | r | | | |
| 🔍 Cost analysis | AL Alain | User | Storage Blob Data | Reader ① This resource | |
| Cost alerts (preview) | | | | | |
| ③ Budgets | | | | | |

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 <u>contact</u> us.

Sources

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