



Role Based Access Control (RBAC)

Role-Based Access Control (RBAC) in Azure is a system that helps manage who has access to Azure resources, what they can do with those resources, and what areas they have access to. RBAC provides fine-grained access management for Azure resources, enabling you to grant only the necessary permissions that users need to perform their tasks. Here's an overview:

Key Concepts

1. **Security Principal:** An object that represents a user, group, service principal, or managed identity that requests access to Azure resources.
2. **Role Definition:** A collection of permissions. It's sometimes referred to as a role. A role definition lists the operations that can be performed, such as read, write, and delete. Azure includes several built-in roles, like Owner, Contributor, and Reader.
3. **Role Assignment:** The process of attaching a role definition to a security principal at a particular scope. This determines the level of access to resources.

Scopes

Scopes are the set of resources that the access applies to. In Azure, the following levels of scope are available:

1. **Management Group:** A container for managing access, policies, and compliance across multiple Azure subscriptions.
2. **Subscription:** A logical container for Azure resources.
3. **Resource Group:** A container that holds related resources for an Azure solution.
4. **Resource:** A specific instance of a service, like a virtual machine, SQL database, or storage account.

How RBAC Works

1. **Role Assignment:** You assign roles to users, groups, service principals, or managed identities at a specific scope (management group, subscription, resource group, or resource).
2. **Evaluate Role Assignments:** When a security principal attempts to perform an action, Azure evaluates all the role assignments for that principal and determines if the action is allowed.

Built-in Roles

Azure provides several built-in roles that you can use:

- **Owner:** Full access to all resources, including the ability to delegate access to others.
- **Contributor:** Can create and manage all types of Azure resources but can't grant access to others.
- **Reader:** Can view existing Azure resources.

Custom Roles

If built-in roles don't meet your needs, you can create custom roles with specific permissions.

Benefits of RBAC

- **Least Privilege:** Granting only the necessary permissions reduces the risk of unauthorized actions.
- **Granular Control:** Fine-tuned permissions help ensure compliance and security.
- **Separation of Duties:** Different roles for different tasks can help prevent conflicts of interest and reduce the risk of accidental or malicious changes.

Example Scenario

Imagine you have a development team and a production team. You can assign the "Contributor" role to the development team at the resource group level, allowing them to create and manage resources within that group. For the production team, you might assign the "Reader" role at the subscription level, enabling them to view resources without making changes.

In summary, Azure RBAC is a powerful tool for managing access to resources, helping ensure security, compliance, and efficient management of Azure environments.



What are we doing in this Lab?

In this lab exercise, you are exploring the practical implementation of Role-Based Access Control (RBAC) in Azure. The process involves creating a new user in Microsoft Entra ID, assigning various built-in roles (Owner, Contributor, Reader) to this user, and observing the resulting permissions at different scopes (subscription, resource group). Additionally, you will create a custom role to understand how to define specific permissions tailored to your needs.

End Goal

The end goal of this lab is to understand how to manage access to Azure resources using RBAC effectively. By completing this exercise, you will learn how to:

1. Create and manage users in Microsoft Entra ID.
2. Assign and evaluate built-in roles like Owner, Contributor, and Reader.
3. Create custom roles with specific permissions.
4. Understand the impact of these roles at various scopes within Azure (management group, subscription, resource group, and resource).



To begin with the Lab

1. Login to Azure Portal and then go to Microsoft Entra ID. Here we are going to create a new user. But first, you need to search for Microsoft Entra ID and go to it. Then from the left pane you need to expand the Manage tab and you will see the user's section. Open it.

Overview

Preview features

Diagnose and solve problems

Manage

Users

Groups

New user

Download users

Bulk operations

Azure Active Directory is now Microsoft Entra ID.

Search

Add filter

2. Then you need to click on new user to create one.

3. Now you need to give it a user principal name and choose the same for the display name, if you wish to do the same, then give it a password or you can choose the auto-generated password. But in any case, you need to remember that password.
4. After that move to the review page and create your user.

Create new user ...

Create a new internal user in your organization

Basics Properties Assignments Review + create

Create a new user in your organization. This user will have a user name like alice@contoso.com. [Learn more](#)

Identity

User principal name *

DemoUser2233 @ behalritesgmail.onmic...  

Domain not listed? [Learn more](#)

Mail nickname *

DemoUser2233

Derive from user principal name

Display name *

DemoUser2233

Password *

*****  

Auto-generate password

Account enabled 

- Once you have created your user refresh the page and you can view your newly created user. Now you need to get inside of your user and copy the user's principal name because this is your login ID for your user.

DemoUser2233 ...

User

Search X < Edit properties Delete Refresh Reset password Revoke sessions Manage view Got feedback?

Overview Overview Monitoring Properties

Basic info

DemoUser2233
DemoUser2233@behalritesgmail.onmicrosoft.com
Member

User principal name: DemoUser2233@behalritesgmail.onmicrosoft.com [Edit](#)
Object ID: 432f84f9-bdbe-40b6-86c1-abf9c511f3c5 [Edit](#)
Created date time: Jul 26, 2024, 12:33 PM
User type: Member
Identities: behalritesgmail.onmicrosoft.com

Manage

- Custom security attributes
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

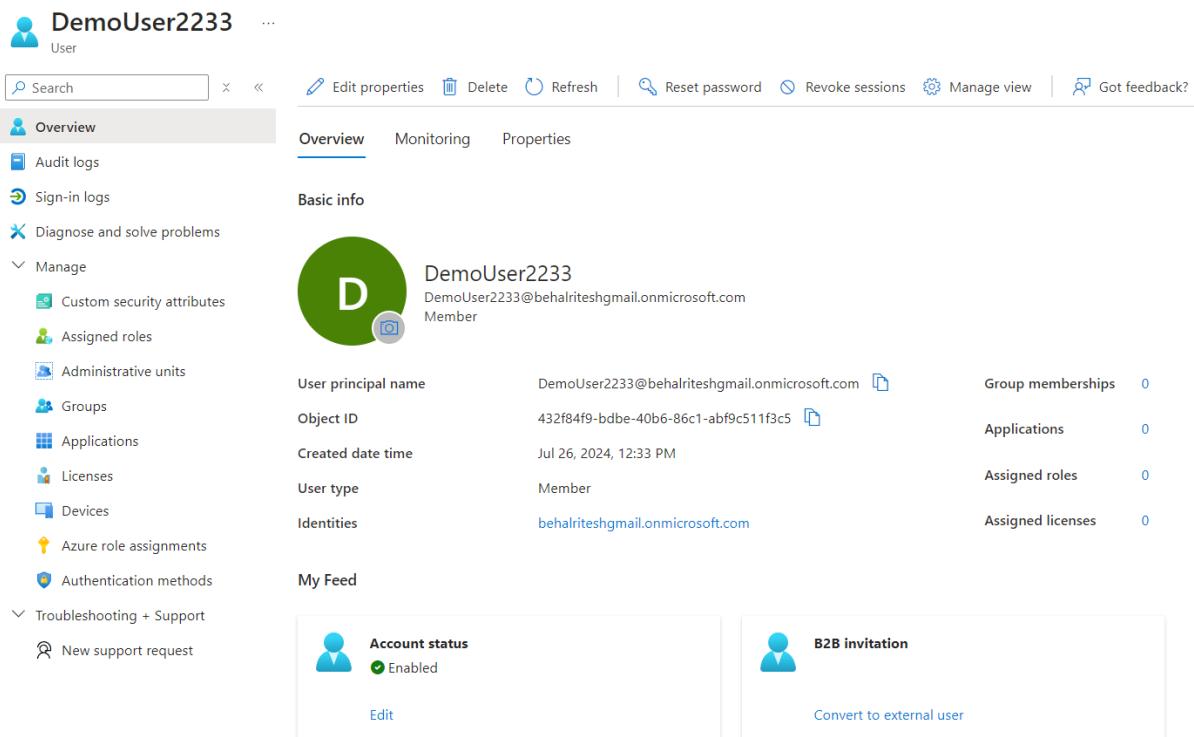
Troubleshooting + Support

- New support request

My Feed

Account status Enabled [Edit](#)

B2B invitation [Convert to external user](#)



6. Then in the new browser of the private tab you need to log in with the new user.

Microsoft Azure



Sign in

to continue to Microsoft Azure

DemoUser2233@behalritesgmail.onmicrosoft.com

No account? [Create one!](#)

[Can't access your account?](#)

[Next](#)

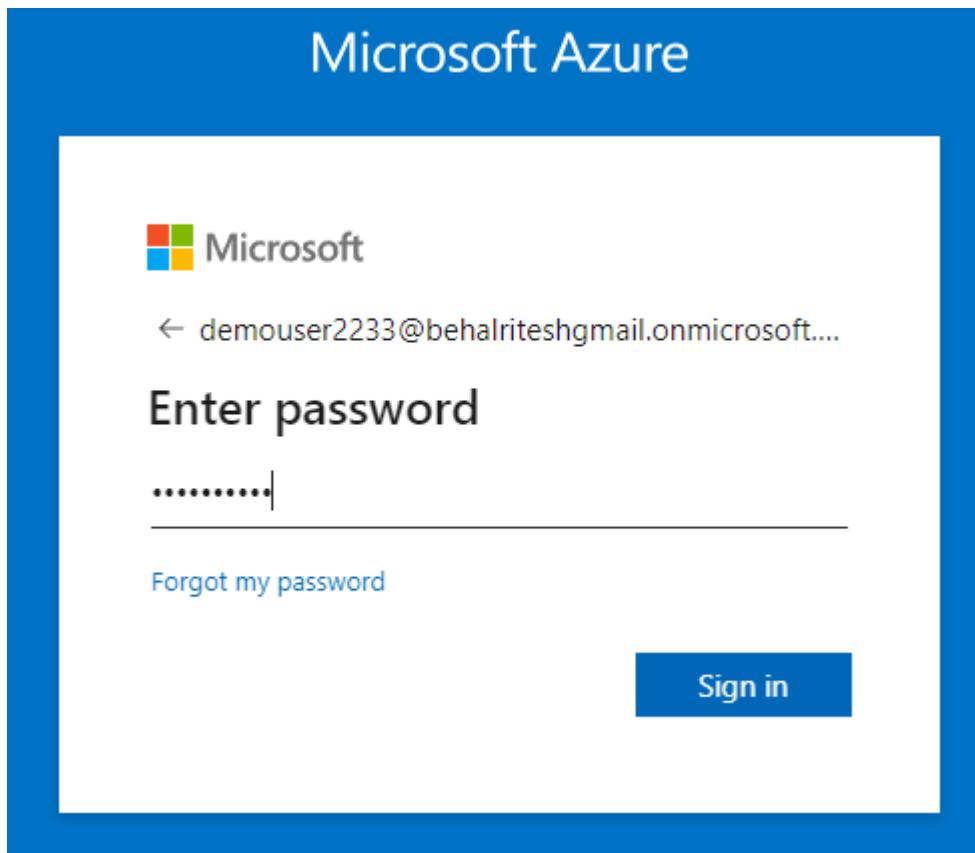


[Sign in with GitHub](#)



[Sign-in options](#)

7. Now you need to enter the password.



8. After that it will ask you to create a new password. You need to do that it is compulsory for you to create a new password every time you log in with the new user.
9. Now just log in with your user. Below you can see that we have logged in with the new user.
10. But you will also notice that you don't have access to perform any action here.

A screenshot of the Microsoft Azure portal home page. The browser address bar shows "portal.azure.com/#home". The top navigation bar includes "Microsoft Azure", a search bar, and a user profile with the name "Demouser2233@behalr...".

Welcome to Azure!

Don't have a subscription? Check out the following options.

Start with an Azure free trial
Get \$200 free credit toward Azure products and services, plus 12 months of popular free services.
[Start](#)

Manage Microsoft Entra ID
Manage access, set smart policies, and enhance security with Microsoft Entra ID.
[View](#) [Learn more](#)

Access student benefits
Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.
[Explore](#) [Learn more](#)

Azure services

[More services](#)

Resources

_RBAC: Giving Owner role

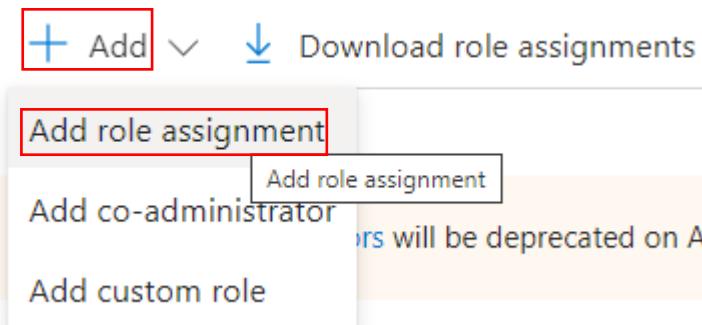
1. This is because we didn't give this user any sort of permission. Now if you go to Microsoft Entra ID in your main account.
2. Now go to users open your user and go to Azure role assignments here you will see that this user doesn't have any permission.
3. Now we are going to add roles to this user basically we will add RBAC roles and give this user permission based on our preference.

The screenshot shows the Azure portal interface for a user named 'DemoUser2233'. The left sidebar has a 'Manage' section with several options: Custom security attributes, Assigned roles, Administrative units, Groups, Applications, Licenses, Devices, and Azure role assignments. The 'Azure role assignments' option is highlighted with a red box. The main content area shows a table with columns: Role, Resource Name, and Resource Type. A message at the top states: 'If this identity has role assignments that you don't have permission to read, they won't be shown in the list. [Learn more](#)'.

4. So, go to your subscriptions, and here go to Access Control (IAM). Now you are going to assign roles to your user.

The screenshot shows the Azure portal interface for the 'Azure Pass - Sponsorship' subscription. The left sidebar has a 'Access control (IAM)' section with various options like Tags, Diagnose and solve problems, Security, Events, Cost management, Advisor recommendations, Billing, Invoices, External services, Payment methods, Partner information, and Settings. The 'Check access' tab is selected in the main content area. It displays sections for 'My access', 'Check access', 'Grant access to this resource', 'View access to this resource', and 'View deny assignments'. A warning message at the top states: 'Classic administrators will be deprecated on August 31, 2024. After August 31, 2024, all classic administrators risk losing access to the subscription. Delete Classic Admins who no longer need access or assign an Azure AD admin role.' A 'Feedback' button is also present.

5. For that click on Add and choose Add role assignment. So, there are so many types of role assignments in RBAC but for now, we will learn about 3 role assignments. First is the owner, the second one is the contributor, and the third one is the Reader.



6. Here you need to go to privileged administrator roles and choose the owner. You can also click on view to see the details about the roles.

Add role assignment ... X

[Role](#) [Members](#) [Conditions](#) [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](#)

Job function roles [Privileged administrator 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?

Name ↑..	Description ↑..	Type ↑..	Category ↑..	Details
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.	BuiltInRole	General	View
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Az...	BuiltInRole	General	View
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	None	View
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 usin...	BuiltInRole	None	View
User Access Administrator	Lets you manage user access to Azure resources.	BuiltInRole	General	View

Showing 1 - 5 of 5 results.

7. Below you can see that there are a lot of permissions in this owner role. Basically, this role grants you the supreme power to do anything in Azure Portal even as a user.

Owner

BuiltinRole

Permissions JSON Assignments

Description: Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.

Search permissions

Type : All

Permission Type
 Actions DataActions

Showing 500 of 16913 permissions [View all](#) (will take a moment to load)

Type	Permissions	Description
▼ Microsoft.AAD		
Other	Subscription Registration Action ⓘ	Subscription Registration Action
Other	Unregister Domain Service ⓘ	Unregister Domain Service
Other	Register Domain Service ⓘ	Register Domain Service
Read	-- ⓘ	--
Read	-- ⓘ	--
Read	Read Domain Service ⓘ	Read Domain Services
Write	Write Domain Service ⓘ	Write Domain Service
Delete	Delete Domain Service ⓘ	Delete Domain Service
Read	Get the network endpoints of all outbound dependencies ⓘ	Get the network endpoints of all outbound dependencies

- Then you need to add the member which you want to add. It can be a user, a group or a service principal as you can see in the snapshot. But for now, we just need a user so, we will click on Select members search for it then add it and move to the next option.

Role **Members** **Conditions** [Review + assign](#)

Selected role Owner

Assign access to
 User, group, or service principal
 Managed identity

Members [+ Select members](#)

Name	Object ID	Type
DemoUser2233	432f84f9-bdbe-40b6-86c1-abf9c511f3c5	User

Description
Optional

- Now in the conditions you need to choose any one condition for the user. Read them and based on your choice apply a condition and move to the review page then assign this role to your user.

Role **Members** **Conditions** [Review + assign](#)

Selected role Owner

What user can do
 Allow user to only assign selected roles to selected principals (fewer privileges) ⓘ
 Allow user to assign all roles except privileged administrator roles Owner, UAA, RBAC (Recommended) ⓘ
 Allow user to assign all roles (highly privileged) ⓘ

⚠️ 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.

10. Once the role has been assigned, now go to Microsoft Entra ID and open your User. Then again go to Azure role assignments, and you will see that the owner role has been assigned to this user without any condition, which means that this user has full access to Azure Portal.

Role	Resource Name	Resource Type	Assigned To	Condition
Owner	Azure Pass - Sponsorship	Subscription	DemoUser2233	None

11. Now go to this user where you have logged in with it. Clear the cache and refresh the page. You will see that it has access to the portal now.

12. Now if go to subscriptions you will see that it has access to the subscription which was not granted before.

The screenshot shows the Microsoft Azure Subscriptions page. At the top, there's a search bar and a Copilot button. The main area displays a table with one row for 'Azure Pass - Sponsorship'. The columns include Subscription name, Subscription ID, My role, Current cost, Secure Score, Parent management group, Status, and a More options menu. Filter buttons at the top of the table allow searching by field, role, status, and adding filters.

13. Also, you can go to the subscription and add the role assignment by yourself.

The screenshot shows the 'Azure Pass - Sponsorship | Access control (IAM)' page. On the left, there's a navigation sidebar with links like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Security, Events, and Cost Management. The main content area is titled 'Add role assignment' and includes tabs for Add role assignments, Roles, Deny assignments, and Classic administrators. A note says 'View my level of access to this resource.' Below this are 'Check access' buttons for 'View my access' and 'Check access'.

14. Now if you go back to your main account go to subscriptions then to IAM, select the user, and choose to delete the role that you just assigned. Once the role is deleted go back to your user in the other browser.

The screenshot shows the 'Role assignments' tab under 'Access control (IAM)'. It displays the number of role assignments (4) and a warning about classic administrators being deprecated. Below this, it shows a summary for 'Privileged' roles (5) and a 'View assignments' link. At the bottom, there are filters for search, type, role, scope, and group by, followed by a table of users with their names, types, roles, scopes, and conditions. One user, 'DemoUser2233', is selected and has a checked checkbox.

15. Here you will see that the access has gone, and this user cannot do anything on the Azure Portal.

The screenshot shows the Microsoft Azure Subscriptions blade. At the top, there's a search bar with placeholder text "Search resources, services, and docs (G+/-)". Below it, a navigation bar includes "Copilot", "Home > Subscriptions", and "My Directory (behaltnites@gmail.onmicrosoft.com)". On the right, a user profile for "DemoUser223@behaltnites..." is shown. The main area displays a table with columns: Subscription name, Subscription ID, My role, Current cost, Secure Score, Parent management group, and Status. A message at the bottom states "None of the entries matched the given filter."

RBAC: Giving Contributor Role

- Now we will give this user the role of contributor. For that again you need to do the same things. First, you need to go to your main account and go to subscriptions then go to Access Control (IAM) click on Add roles, and choose Add role assignment.

The screenshot shows the "Add role assignment" dialog. It has three main buttons: "+ Add" (highlighted), "Download role assignments", and "Add co-administrator". A note below says "This feature will be deprecated on April 1, 2024". There is also a "Add custom role" button.

- After that again go to privileged administrator roles and choose contributor roles this time. Then move to members.

The screenshot shows the "Add role assignment" blade with the "Members" tab selected. It displays a list of roles under "Privileged administrator roles". The "Contributor" role is highlighted. Other roles listed include Owner, Access Review Operator Service Role, Role Based Access Control Administrator, and User Access Administrator. The blade also includes sections for "Conditions" and "Review + assign".

Name	Description	Type	Category	Details
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.	BuiltinRole	General	View
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Az...	BuiltinRole	General	View
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	None	View
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 usin...	BuiltinRole	None	View
User Access Administrator	Lets you manage user access to Azure resources.	BuiltinRole	General	View

- Again, select your user and move to the review page, in the contributor role we don't need any condition to specify. So, just move to the review page and assign this role.

Role Members Conditions Review + assign

Selected role Contributor

Assign access to User, group, or service principal Managed identity

Members [+ Select members](#)

Name	Object ID	Type
DemoUser2233	432f84f9-bdbe-40b6-86c1-abf9c511f3c5	User

Description Optional

- Now come back to your user in the subscriptions if you do a refresh, also clear your cache. So, you will be able to see your subscription again.

The screenshot shows the Microsoft Azure Subscriptions blade. At the top, there's a search bar and a Copilot button. Below it, the 'Subscriptions' section has a 'Filtered (1 of 1)' message. The table lists one subscription:

Subscription name	Subscription ID	My role	Current cost	Secure Score	Parent management group	Status
Azure Pass - Sponsorship	a112fb3b-b5f9-443f-b0d9-e55d0095055c	Specified access	Not available	100%		Active

- In the contributor role you will see that you don't have access to add any role assignments.

The screenshot shows the 'Access control (IAM)' blade for the 'Azure Pass - Sponsorship' subscription. On the left, there's a navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Security, Events, and Cost Management. The 'Access control (IAM)' option is selected. In the main area, there's a table with columns for 'Add role assignment (disabled)', 'Add co-administrator (disabled)', 'Add custom role (disabled)', 'Users', 'Roles', 'Deny assignments', and 'Classic administrators'. Below the table, there's a 'View my access' button and a 'Check access' section with a 'Check access' button.

- Also, if you want to know about what the contributor role can do then while assigning it you can view the details for this role like we did with the owner role.
- But you can go to a resource group create a resource group and you can also create resources.

The screenshot shows the Microsoft Azure portal's Resource groups page. At the top, there are navigation links for Home, Resource groups, and My Directory. Below the header, there are buttons for Create, Manage view, Refresh, Export to CSV, Open query, and Assign tags. A search bar is present at the top right. The main area displays a table of resource groups with columns for Name, Subscription, and Location. Two records are listed: NetworkWatcherRG (Subscription: Azure Pass - Sponsorship, Location: North Europe) and newera1 (Subscription: Azure Pass - Sponsorship, Location: North Europe). There are also filter and grouping options at the top of the table.

RBAC: Giving Reader Role

1. By its name you can understand that the reader's role is just to permit a user so that it can view the resources only. It cannot make any changes on its own, it can only view what the resources are.
2. Also, if you want to see how the reader role works then you can create some resources and at your subscription level, you can assign the reader role like we did earlier with the other roles. But first, you have to delete the contributor role.

The screenshot shows the 'Add role assignment' dialog. It has tabs for Role, Members*, Conditions, and Review + assign. The Role tab is selected, showing 'Job function roles' and 'Privileged administrator roles'. Under 'Job function roles', 'Reader' is selected. A note says: 'Grant access to Azure resources based on job function, such as the ability to create virtual machines.' Below this, there are filters for Type: All and Category: All, and a table listing the Reader role with details like Name, Description, Type, Category, and Details. The 'Description' column for Reader states: 'View all resources, but does not allow you to make any changes.'

3. Below you can see that by using the reader role you can only view the resource group or the resources.

The screenshot shows the 'Resource groups | Simplified view' page. At the top, there are navigation links for Home, Resource groups, and My Directory. Below the header, there are buttons for Refresh, Feedback, and Assign tags. A search bar is present at the top right. The main area displays a table of resource groups with columns for Name, Type, Location, Resource Group, and Subscription. Two records are listed: newera1 (Type: Resource group, Location: North Europe, Resource Group: newera1, Subscription: Azure Pass - Sponsorship) and NetworkWatcherRG (Type: Resource group, Location: North Europe, Resource Group: NetworkWatcherRG, Subscription: Azure Pass - Sponsorship). There are also filter and grouping options at the top of the table.

4. So, until now you just have seen the RBAC specification at the subscription level. You can also create RBAC roles at the resource group level too.
5. In the main account we just created a resource group and also a storage account in this resource group. Also, I have removed all the roles from that demo user.

The screenshot shows the Microsoft Azure Resource Groups interface. The left sidebar lists options like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Monitoring, Automation, and Help. The main area is titled 'Essentials' and shows a table with one record: 'demostorage2233' (Storage account) located in the East US region.

- Now we are going to add a role assignment for that demo user from our resource group. So, the steps are the same go to Access Control (IAM) and then click on add choose Add role assignment.

The screenshot shows the Microsoft Azure Access control (IAM) interface. The left sidebar includes Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, and Monitoring. The main area has a 'Check access' section and a 'View my access' button. A tooltip for the 'Add role assignment' button is visible, showing options like 'Add role assignment', 'Add co-administrator', and 'Add custom role'.

- Then choose the reader role, after that add your user and then move to the review page and assign the role.

The screenshot shows the 'Add role assignment' dialog. The 'Role' tab is selected, showing a list of roles including 'Job function roles' (Privileged administrator roles) and 'Grant access to Azure resources based on job function, such as the ability to create virtual machines'. The 'Members' tab is also visible.

- Now if you go back to your demo user account and refresh the page after clearing the cache then go to the resource group and here you can see the RG and your storage account.

9. You can also read the contents of it, but you cannot make any changes to it.

RBAC: Creating Custom Role

1. Now we will see how to create a custom role. So, for that first go to your subscription then go to Access Control (IAM), and now choose Add custom role.

2. So, to create a custom role you have three options, first you can clone using the existing roles that you have in Azure Portal. Second, you can start from Scratch. Third, you can start writing your role in JSON, or if you have any file in which you already have a role written in JSON then you can upload that file too.

Create a custom role ...

3. But for this demo we are going to choose to clone a role. Now first you need to give a name to your role. Then the description is optional. After that, you need to choose which

role you want to clone. Below you can see that we have chosen the reader role. Then move to the next page.

Create a custom role ...

Basics Permissions Assignable scopes JSON Review + create

To create a custom role for Azure resources, fill out some basic information. [Learn more](#)

Custom role name * ✓

Description

Baseline permissions Clone a role Start from scratch Start from JSON

Role to clone ✓

4. Then you can add some extra permissions by clicking on the highlighted icon.

Create a custom role ...

Basics **Permissions** Assignable scopes JSON Review + create

+ Add permissions + Exclude permissions

Click Add permissions to select the permissions you want to add to this custom role.
To add a wildcard (*) permission, you must manually add the permission on the JSON tab. [Learn more](#)
To exclude specific permissions from a wildcard permission, click Exclude permissions. [Learn more](#)

Permission	Description	Permission type	Actions
*/read	--	Action	

5. Now to add some extra permissions you can search for Microsoft Compute

Add permissions

Search for permissions to add to your custom role. For example, search for "virtual machines" to find permissions related to virtual machines.

microsoft.compute

Microsoft Compute
Access cloud compute capacity and scale on demand (such as virtual machines) and only pay for the resources you use.

Microsoft.ComputeSchedule
Microsoft.ComputeSchedule

6. Now you need to scroll down to virtual machines, and you can choose the operations you want. Then just click on add.

Microsoft.Compute permissions

The screenshot shows a list of permissions under the 'Microsoft.Compute/virtualMachines' scope. The actions listed are:

- Read : Get Virtual Machine ⓘ - Get the properties of a virtual machine
- Write : Create or Update Virtual Machine ⓘ - Creates a new virtual machine or updates an existing virtual machine
- Delete : Delete Virtual Machine ⓘ - Deletes the virtual machine
- Other : Start Virtual Machine ⓘ - Starts the virtual machine
- Other : Power Off Virtual Machine ⓘ - Powers off the virtual machine. Note that the virtual machine will continue to be billed.
- Other : Reapply a virtual machine's current model ⓘ - Reapplies a virtual machine's current model
- Other : Redeploy Virtual Machine ⓘ - Redeploys virtual machine
- Other : Restart Virtual Machine ⓘ - Restarts the virtual machine
- Other : Retrieve boot diagnostic logs blob URIs ⓘ - Retrieves boot diagnostic logs blob URIs
- Other : Deallocate Virtual Machine ⓘ - Powers off the virtual machine and releases the compute resources
- Other : Generalize Virtual Machine ⓘ - Sets the virtual machine state to Generalized and prepares the virtual machine for capture
- Other : Capture Virtual Machine ⓘ - Captures the virtual machine by copying virtual hard disks and generates a template that can be used to create similar virtual machines
- Other : Run Command on Virtual Machine ⓘ - Executes a predefined script on the virtual machine
- Other : Convert Virtual Machine disks to Managed Disks ⓘ - Converts the blob based disks of the virtual machine to managed disks
- Other : Perform Maintenance Redeploy ⓘ - Performs Maintenance Operation on the VM.

At the bottom, there are 'Add' and 'Cancel' buttons.

7. Then you can see your extra permission here along with the read permission. Then

Create a custom role ...

The screenshot shows the 'Permissions' tab of a custom role configuration. The selected permissions are:

- */read
- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/write
- Microsoft.Compute/virtualMachines/delete

Below the table, there is a note: "Click Add permissions to select the permissions you want to add to this custom role. To add a wildcard (*) permission, you must manually add the permission on the JSON tab. Learn more ⓘ To exclude specific permissions from a wildcard permission, click Exclude permissions. Learn more ⓘ".

8. Also, you can see the JSON code of your custom role which you can copy or download for later use. Then just move to the review page and create your role.

Create a custom role ...

Basics Permissions Assignable scopes JSON Review + create

Here is your custom role in JSON format. [Learn more](#)

[Download](#) [Edit](#)

```

1 "properties": {
2     "roleName": "demoReaderRole2233",
3     "description": "This is just for demo purpose. ",
4     "assignableScopes": [
5         "/subscriptions/a112fb3b-b5f9-443f-b0d9-e55d0095055c"
6     ],
7     "permissions": [
8         {
9             "actions": [
10                 "*/read",
11                 "Microsoft.Compute/virtualMachines/read",
12                 "Microsoft.Compute/virtualMachines/write",
13                 "Microsoft.Compute/virtualMachines/delete"
14             ],
15             "notActions": [],
16             "dataActions": [],
17             "notDataActions": []
18         }
19     ]
20 }
21 }
22 }
```

[Review + create](#) [Previous](#) [Next](#)

[Feedback](#)

9. Once your role has been created go to add role assignments and you can search for your custom role and add it to the user then just assign it.

Add role assignment ...

Role Members * Conditions 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](#)

Job function roles Privilaged administrator roles

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

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
role2233	This is just for demo purpose.	CustomRole	None	View

Showing 1 - 1 of 1 results.

10. So, this is how you can create and add the custom roles to your user.