😊 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.

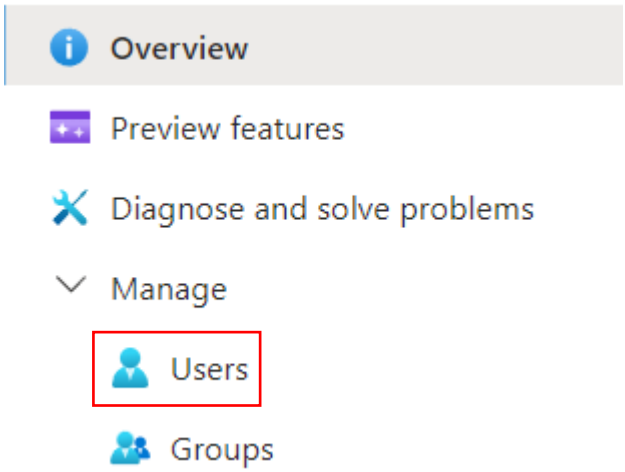
End Goal

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:

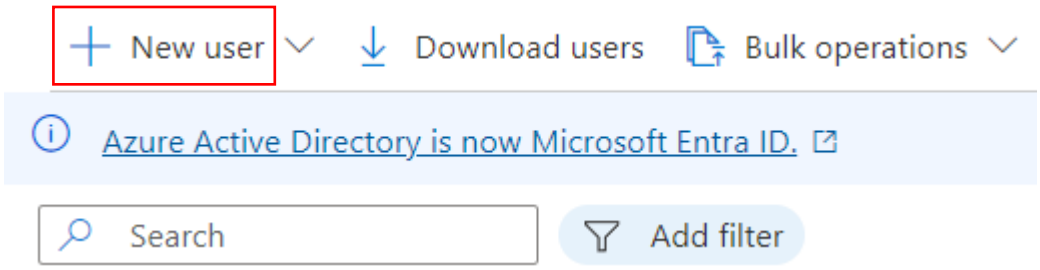
1. Create and manage users in Microsoft Entra ID.
2. Assign and evaluate built-in roles like Owner, Contributor, and Reader.
3. Create custom roles with specific permissions.
4. Understand the impact of these roles at various scopes within Azure (management group, subscription, resource group, and resource).

😄 To begin with the Lab

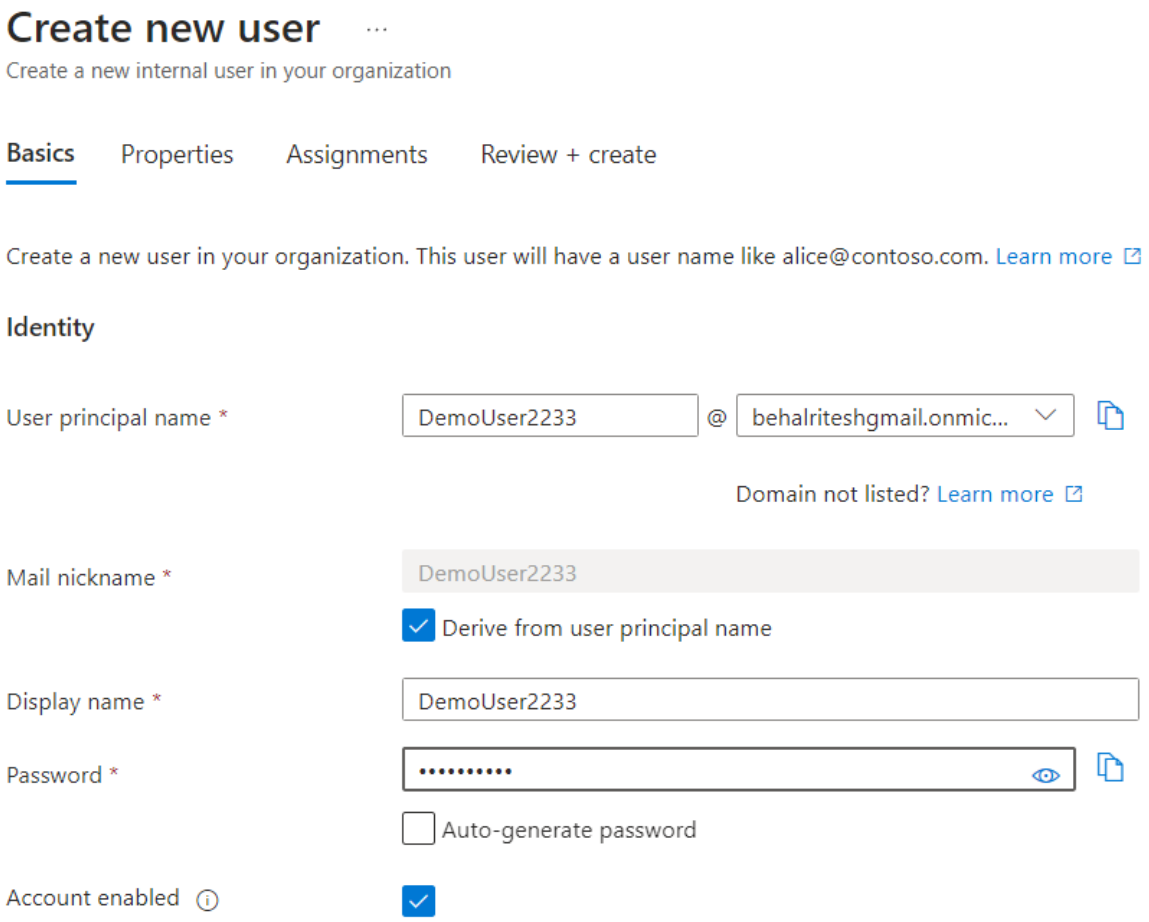
1. Login to Azure Portal and then go to Microsoft Entra ID. Here we are going to create a new user. But first, you need to search for Microsoft Entra ID and go to it. Then from the left pane you need to expand the Manage tab and you will see the user’s section. Open it.



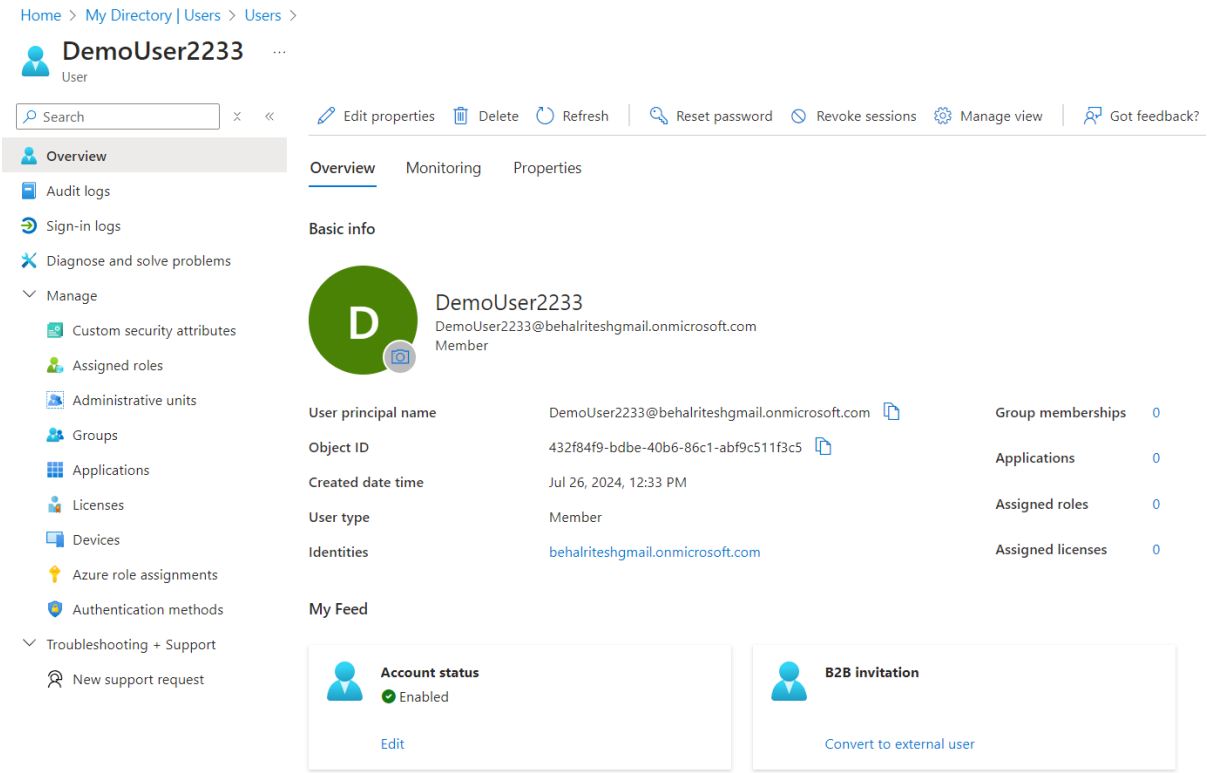
2. Then you need to click on new user to create one.



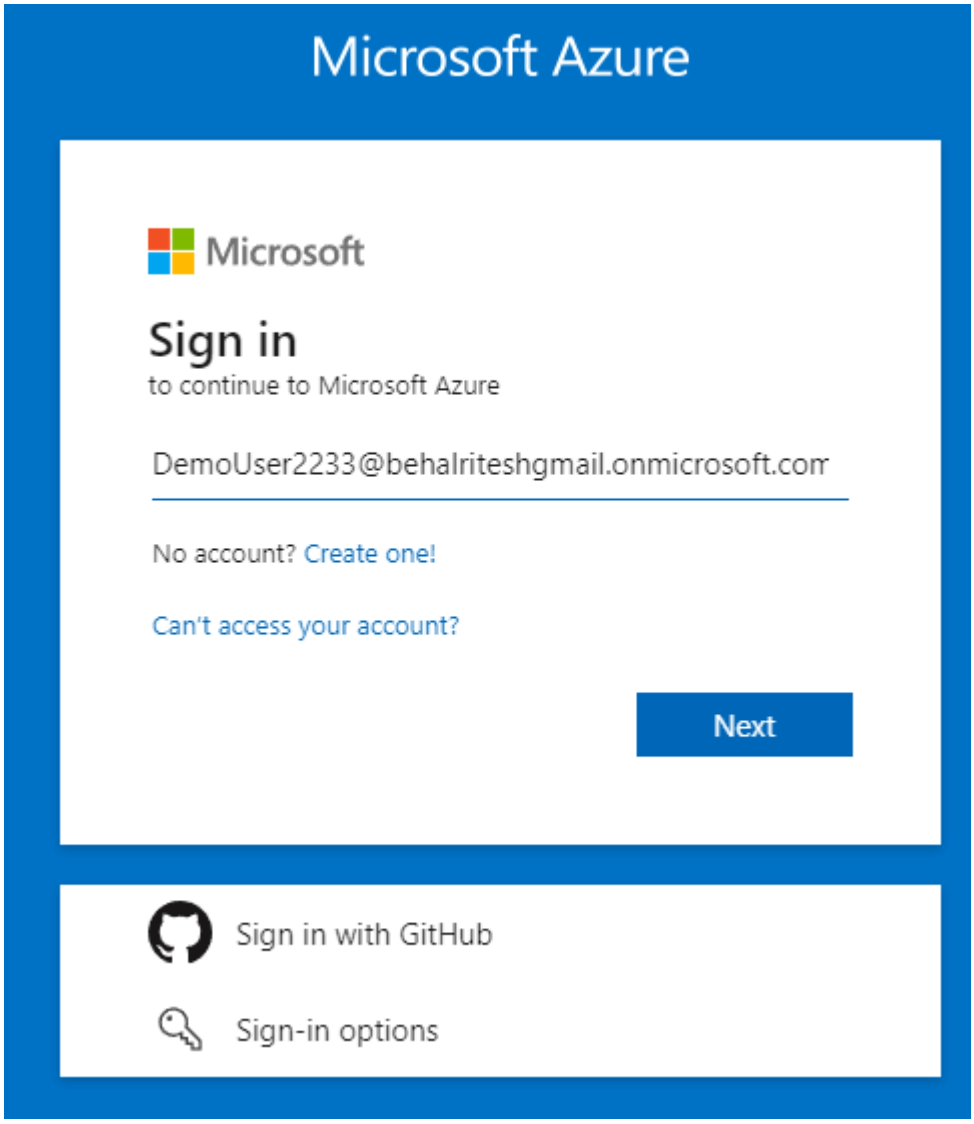
3. Now you need to give it a user principal name and choose the same for the display name, if you wish to do the same, then give it a password or you can choose the auto-generated password. But in any case, you need to remember that password.
4. After that move to the review page and create your user.



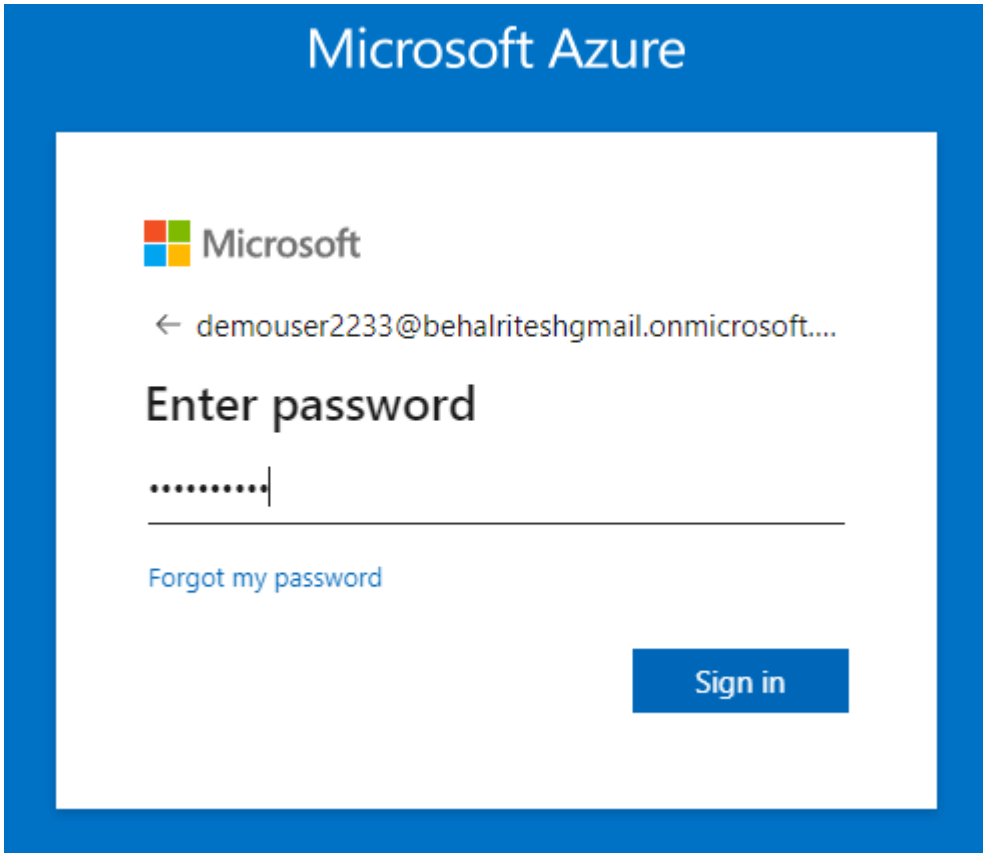
5. Once you have created your user refresh the page and you can view your newly created user. Now you need to get inside of your user and copy the user's principal name because this is your login ID for your user.



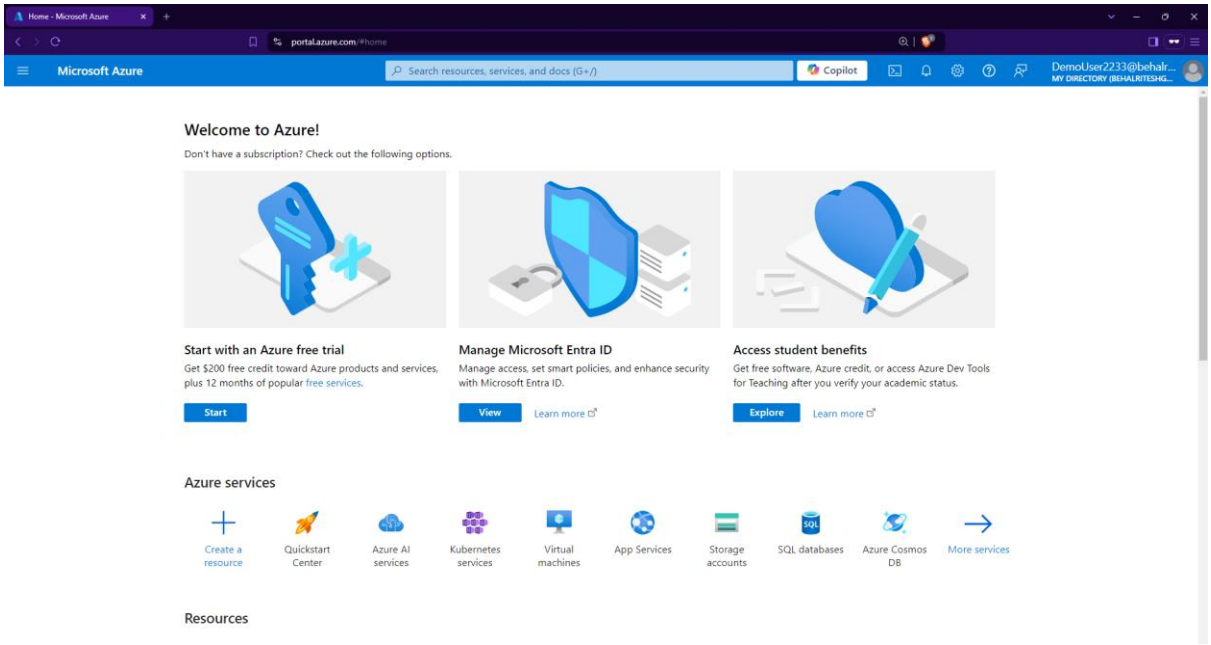
6. Then in the new browser of the private tab you need to log in with the new user.



7. Now you need to enter the password.

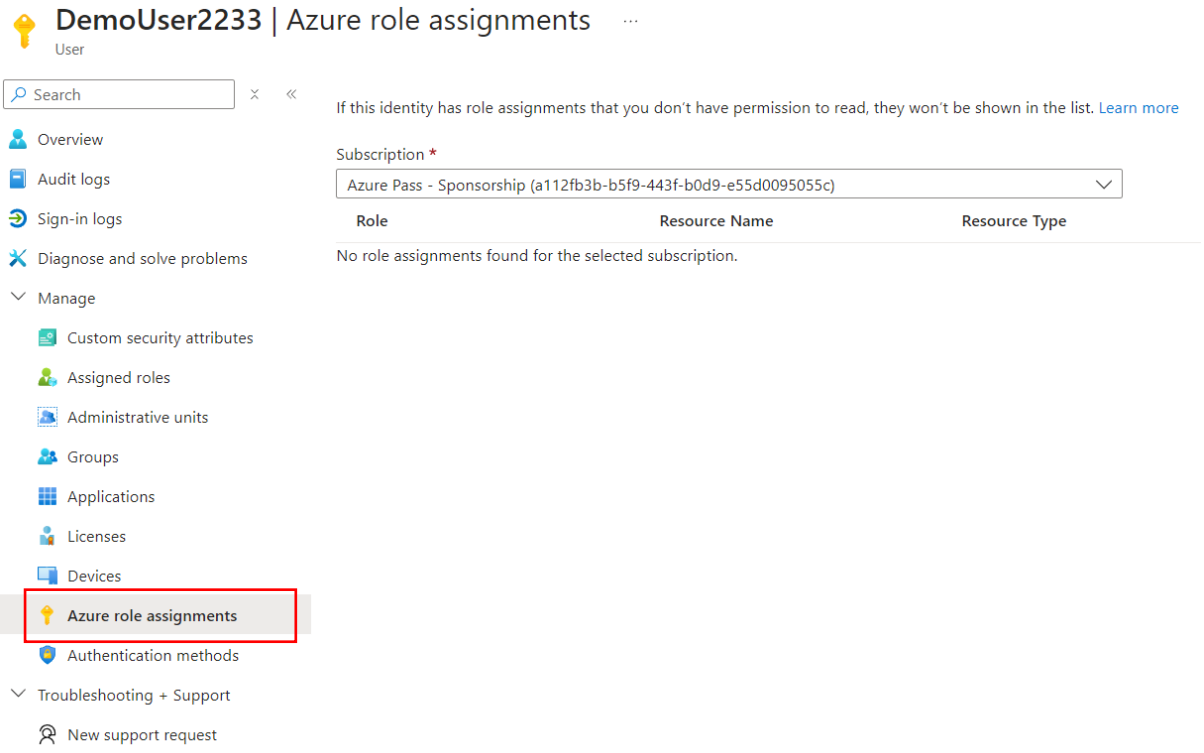


8. After that it will ask you to create a new password. You need to do that it is compulsory for you to create a new password every time you log in with the new user.
9. Now just log in with your user. Below you can see that we have logged in with the new user.
10. But you will also notice that you don't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

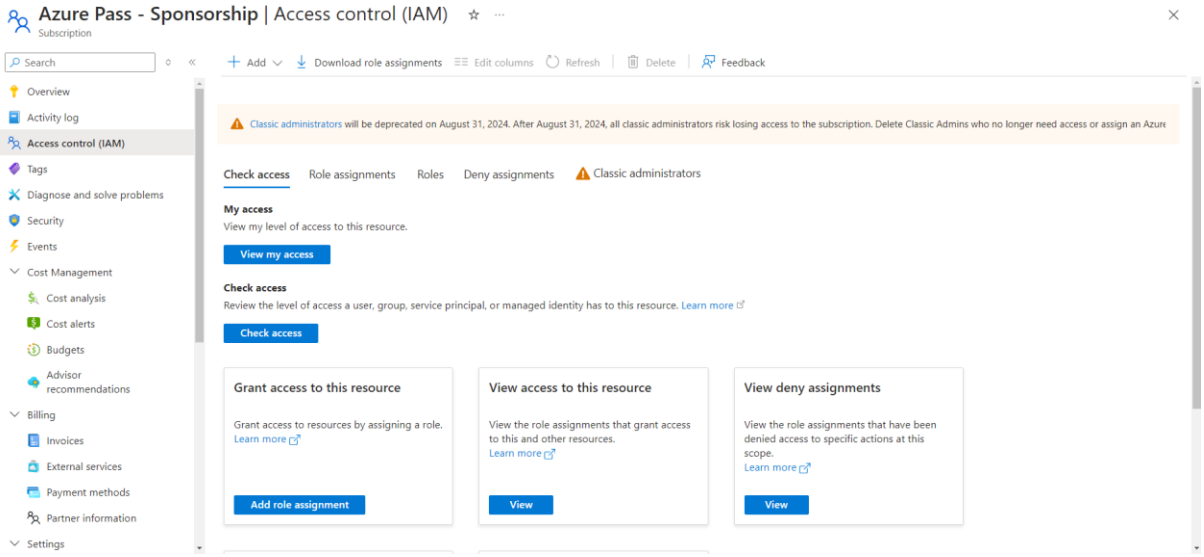


😁 RBAC: Giving Owner role

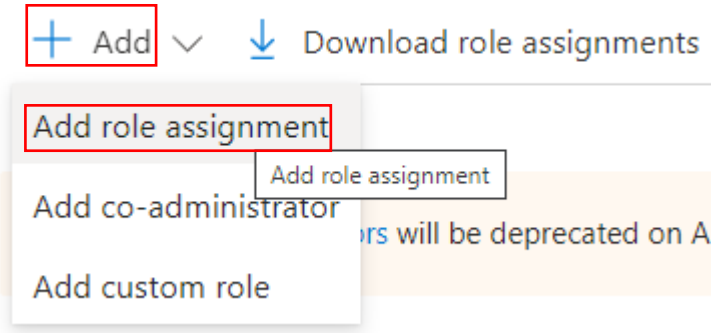
1. This is because we didn't give this user any sort of permission. Now if you go to Microsoft Entra ID in your main account.
2. Now go to users open your user and go to Azure role assignments here you will see that this user doesn't have any permission.
3. Now we are going to add roles to this user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



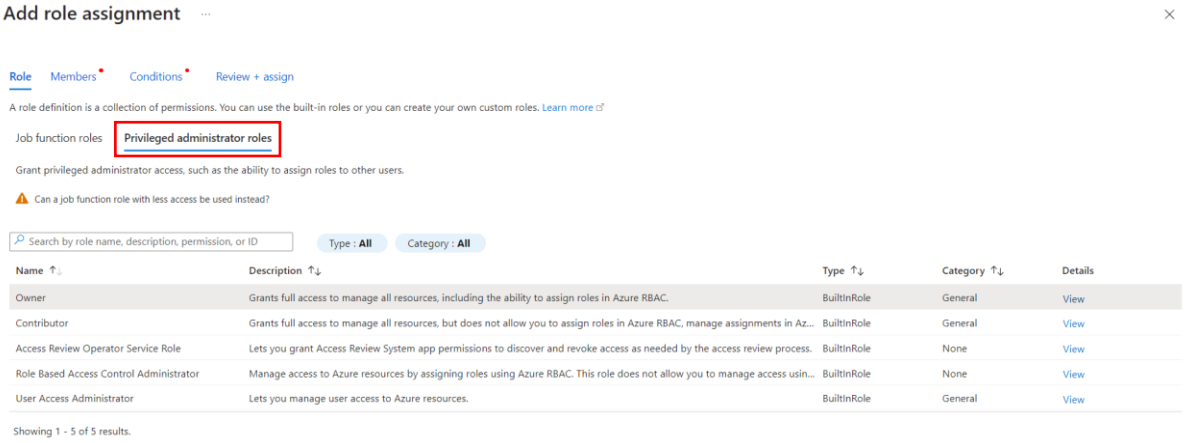
4. So, go to your subscriptions, and here go to Access Control (IAM). Now you are going to assign roles to your user.



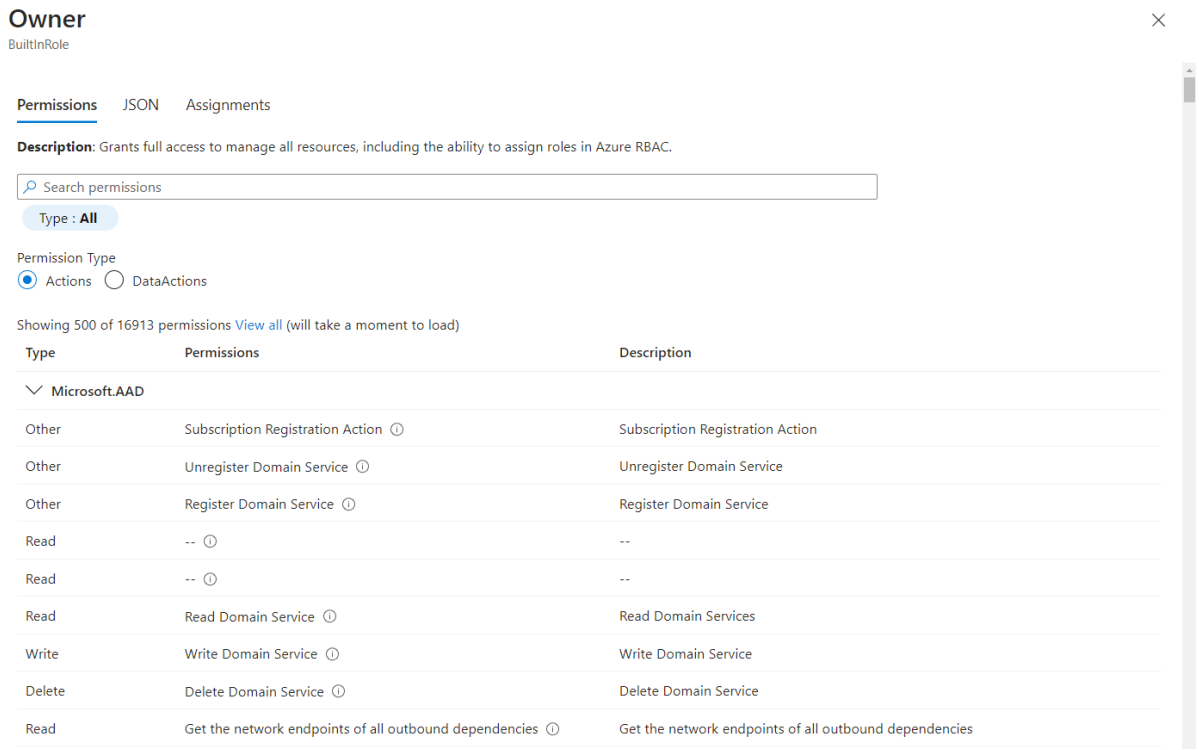
5. For that click on Add and choose Add role assignment. So, there are so many types of role assignments in RBAC but for now, we will learn about 3 role assignments. First is the owner, the second one is the contributor, and the third one is the Reader.



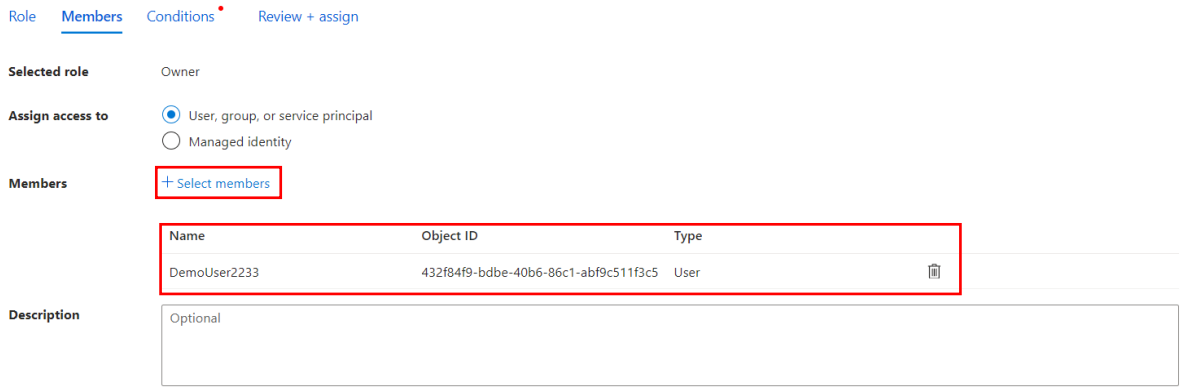
6. Here you need to go to privileged administrator roles and choose the owner. You can also click on view to see the details about the roles.



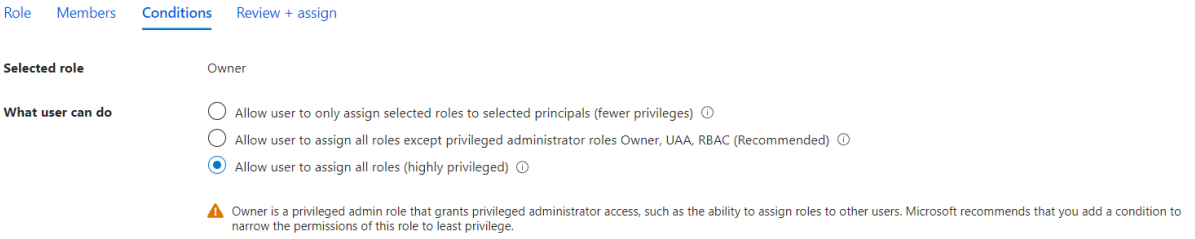
7. Below you can see that there are a lot of permissions in this owner role. Basically, this role grants you the supreme power to do anything in Azure Portal even as a user.



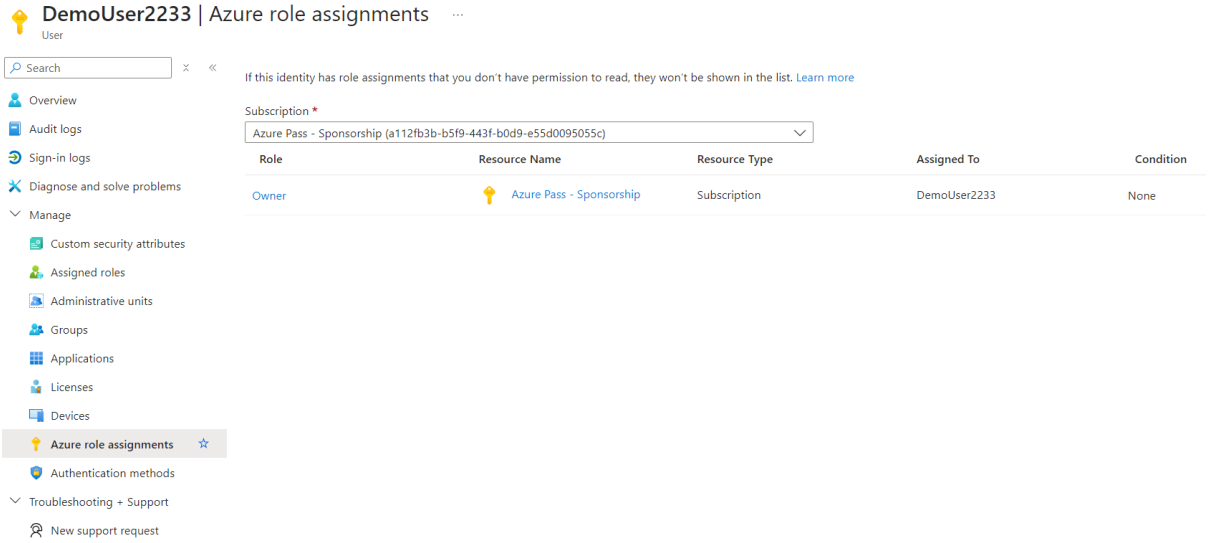
8. Then you need to add the member which you want to add. It can be a user, a group or a service principal as you can see in the snapshot. But for now, we just need a user so, we will click on Select members search for it then add it and move to the next option.



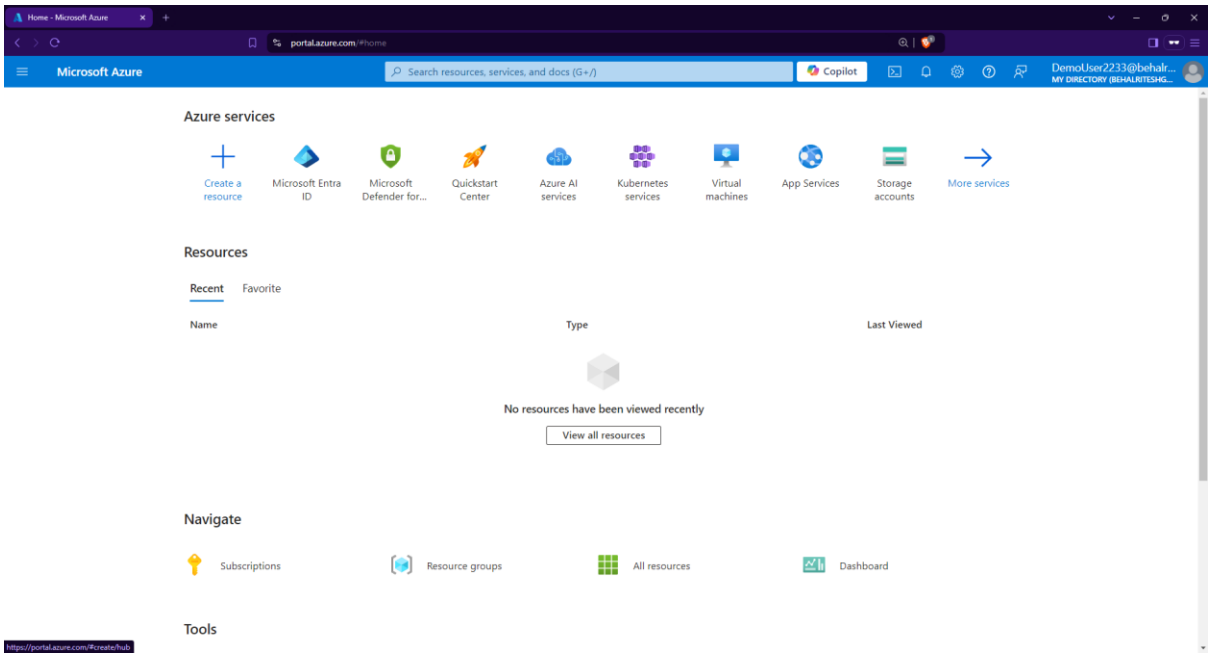
9. Now in the conditions you need to choose any one condition for the user. Read them and based on your choice apply a condition and move to the review page then assign this role to your user.



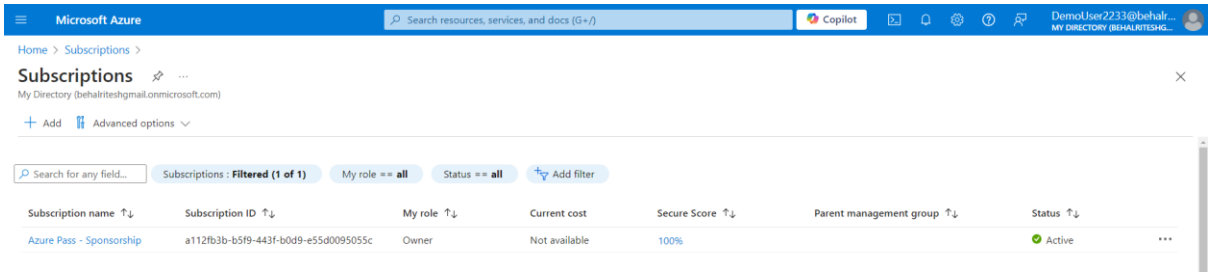
10. Once the role has been assigned, now go to Microsoft Entra ID and open your User. Then again go to Azure role assignments, and you will see that the owner role has been assigned to this user without any condition, which means that this user has full access to Azure Portal.



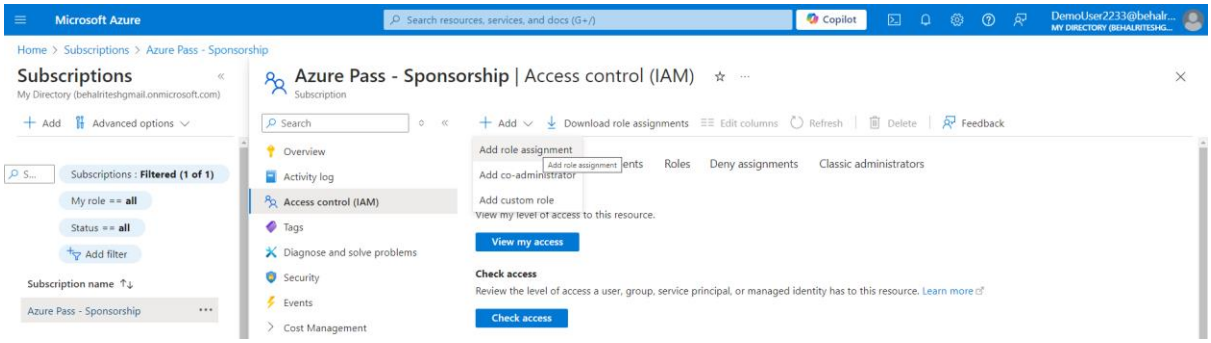
11. Now go to this user where you have logged in with it. Clear the cache and refresh the page. You will see that it has access to the portal now.



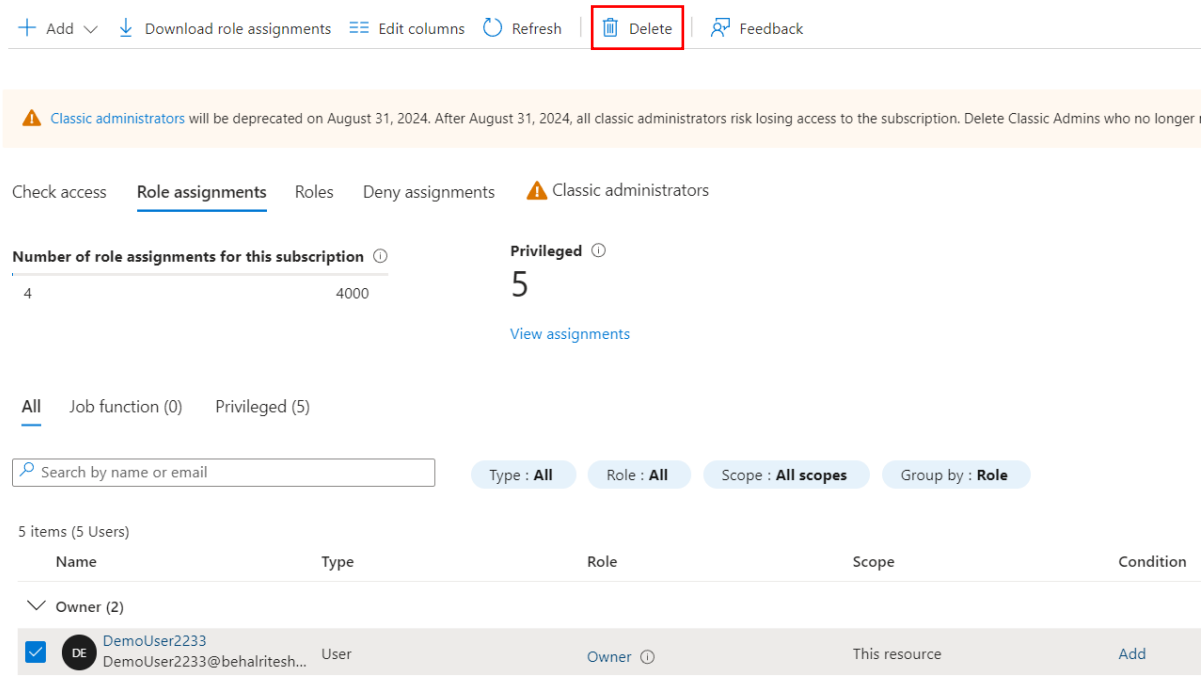
12. Now if go to subscriptions you will see that it has access to the subscription which was not granted before.



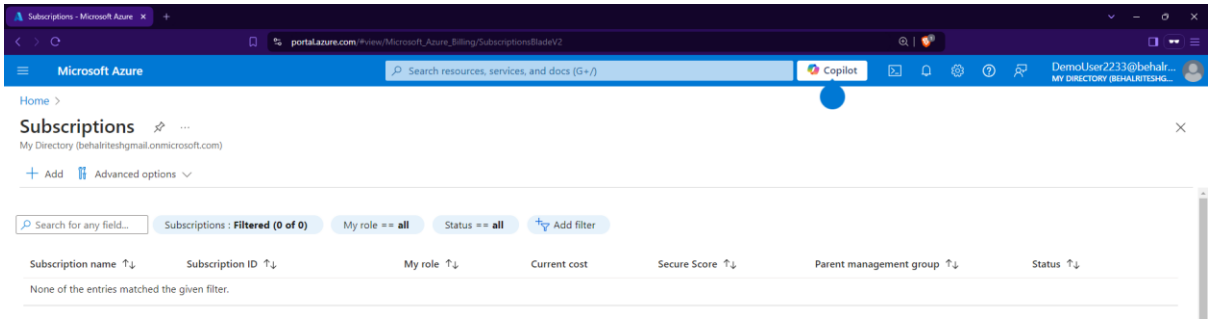
13. Also, you can go to the subscription and add the role assignment by yourself.



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.

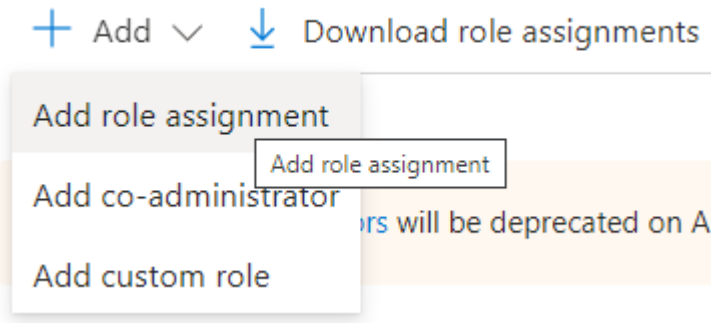


15. Here you will see that the access has gone, and this user cannot do anything on the Azure Portal.

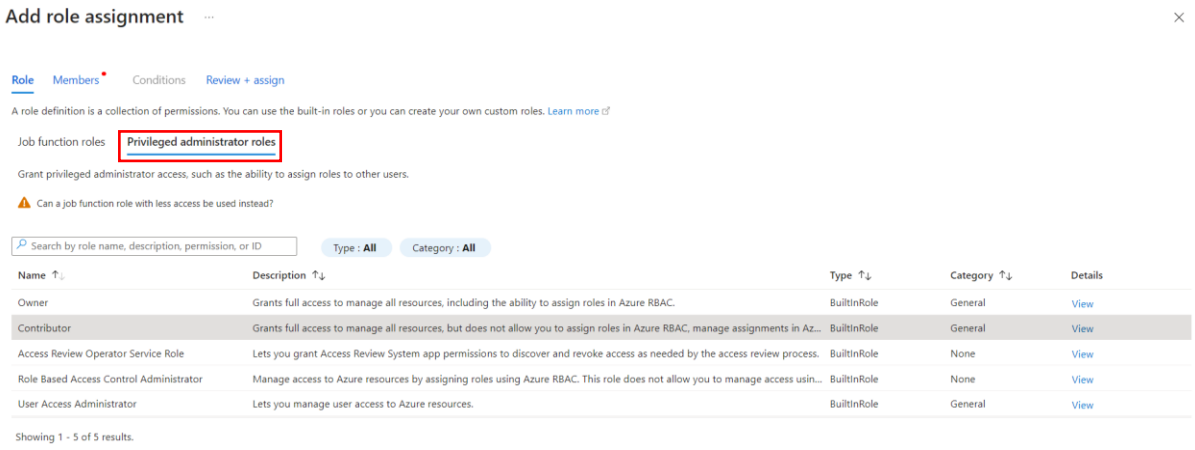


😁 RBAC: Giving Contributor Role

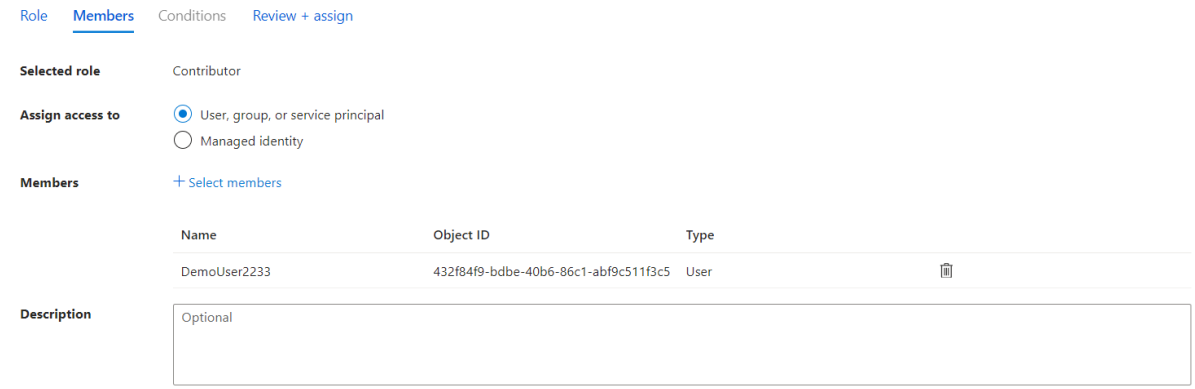
1. Now we will give this user the role of contributor. For that again you need to do the same things. First, you need to go to your main account and go to subscriptions then go to Access Control (IAM) click on Add roles, and choose Add role assignment.



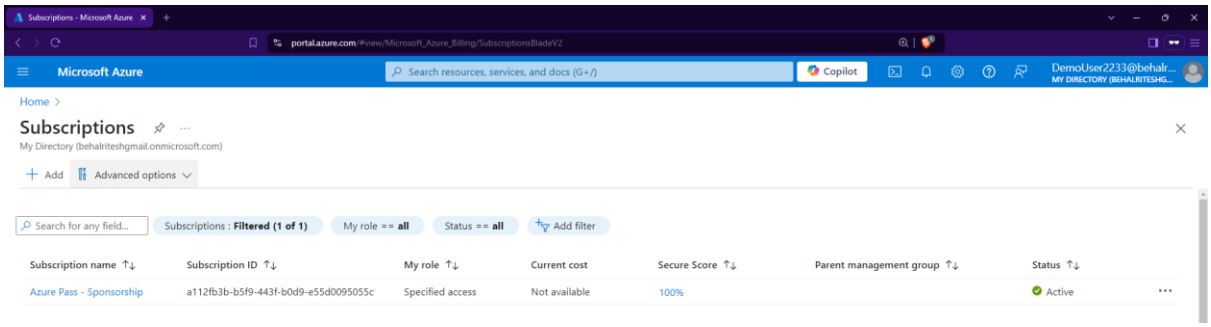
2. After that again go to privileged administrator roles and choose contributor roles this time. Then move to members.



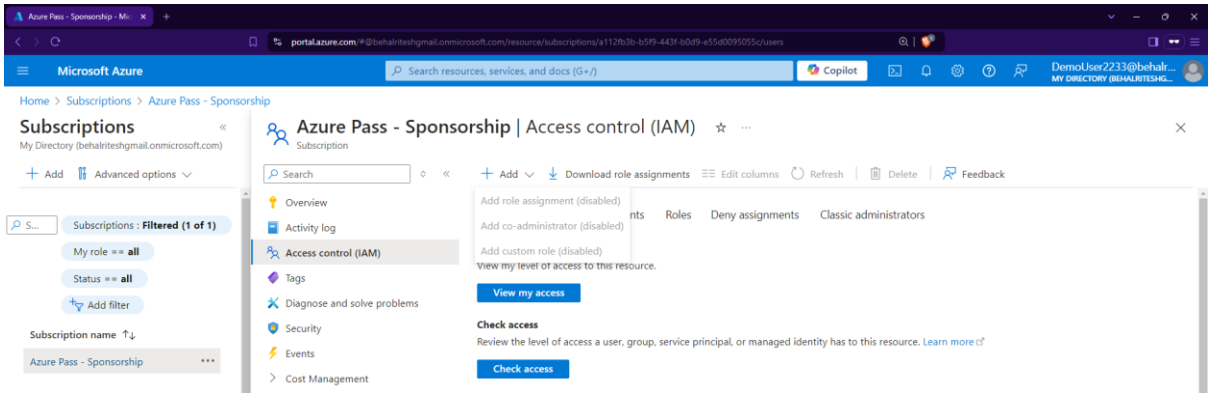
3. Again, select your user and move to the review page, in the contributor role we don't need any condition to specify. So, just move to the review page and assign this role.



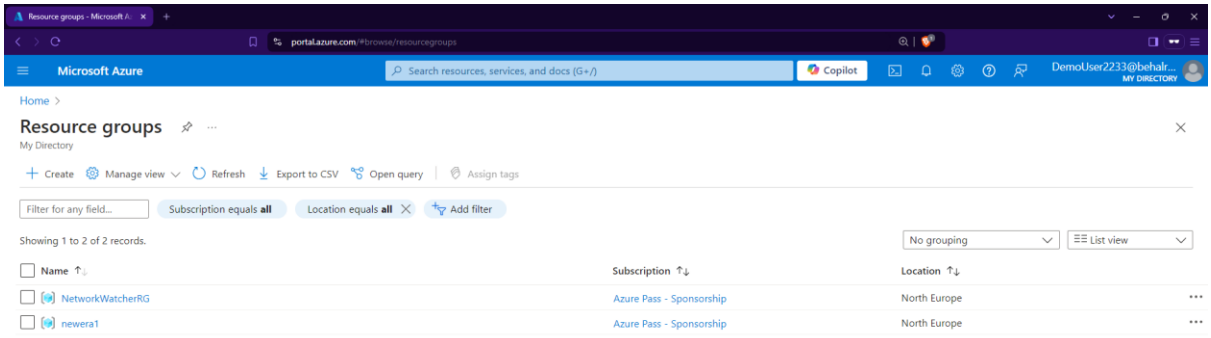
4. Now come back to your user in the subscriptions if you do a refresh, also clear your cache. So, you will be able to see your subscription again.



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

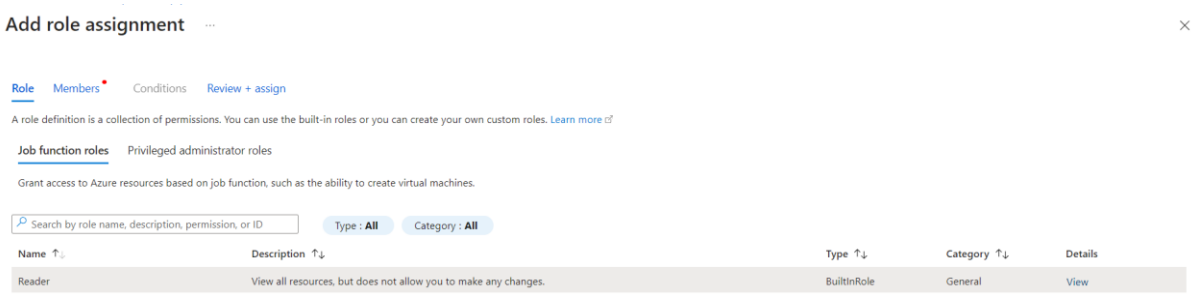


6. Also, if you want to know about what the contributor role can do then while assigning it you can view the details for this role like we did with the owner role.
7. But you can go to a resource group create a resource group and you can also create resources.

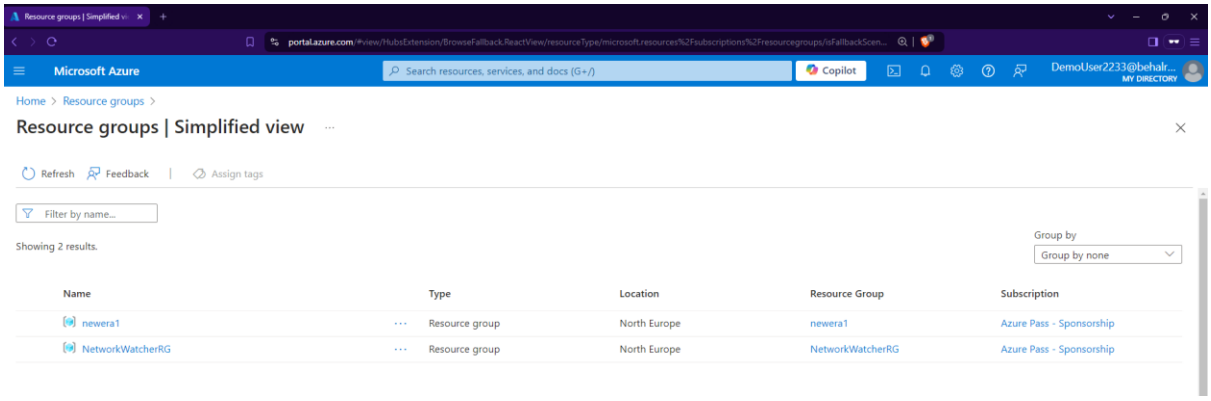


😁 RBAC: Giving Reader Role

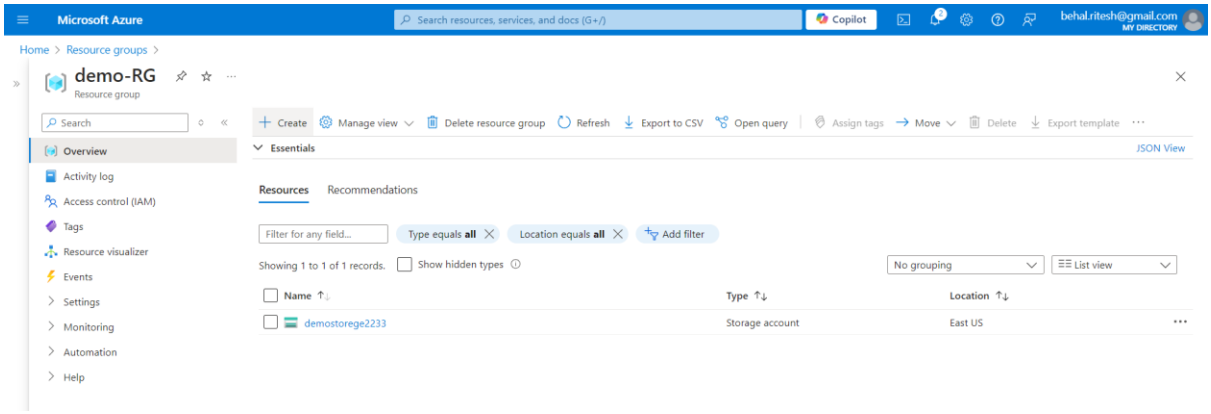
1. By its name you can understand that the reader's role is just to permit a user so that it can view the resources only. It cannot make any changes on its own, it can only view what the resources are.
2. Also, if you want to see the how reader role works then you can create some resources and at your 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.



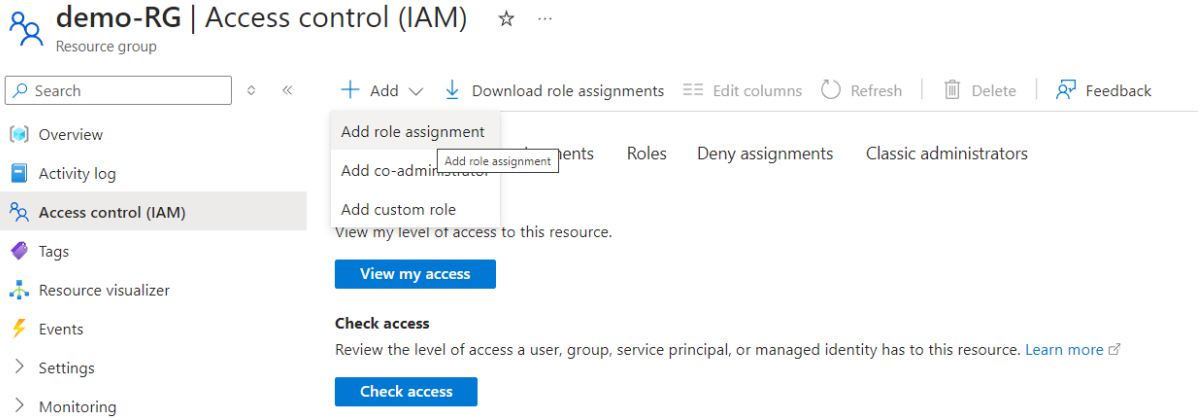
3. Below you can see that by using the reader role you can only view the resource group or the resources.



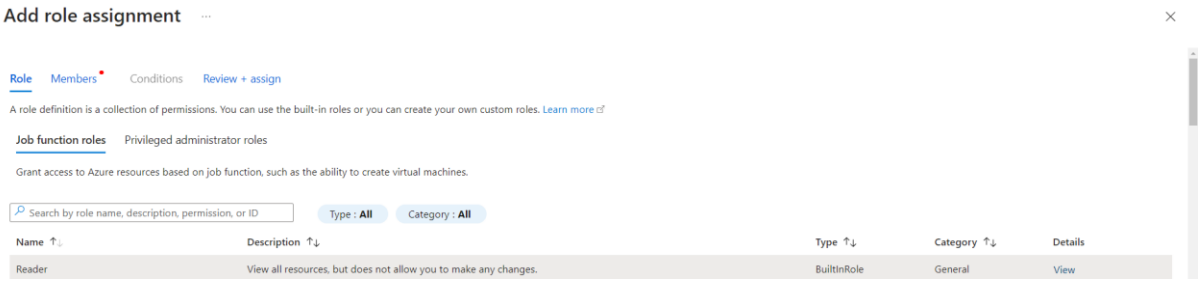
4. So, until now you just have seen the RBAC specification at the subscription level. You can also create RBAC roles at the resource group level too.
5. In the main account we just created a resource group and also a storage account in this resource group. Also, I have removed all the roles from that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



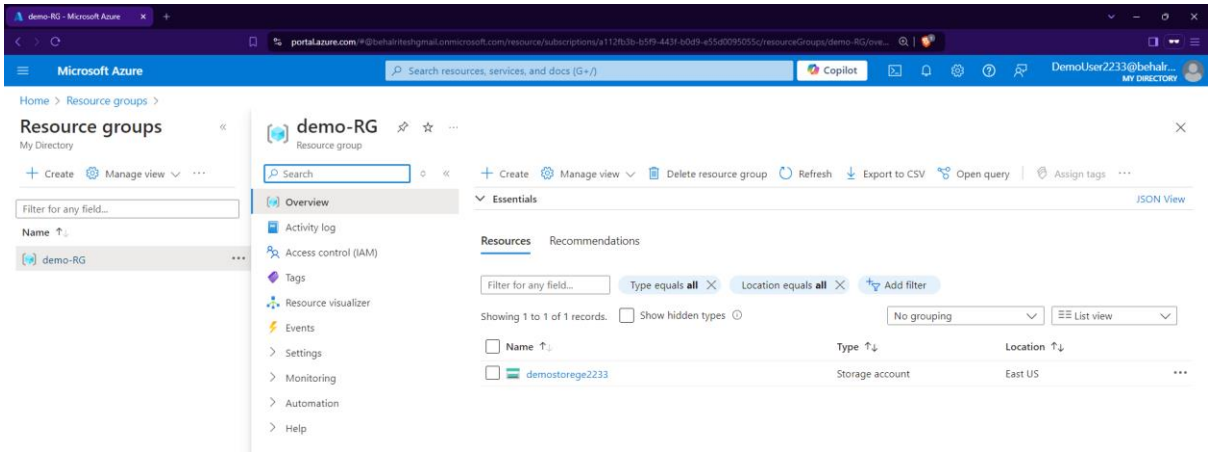
6. Now we are going to add a role assignment for that demo user from our resource group. So, the steps are the same go to Access Control (IAM) and then click on add choose Add role assignment.



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



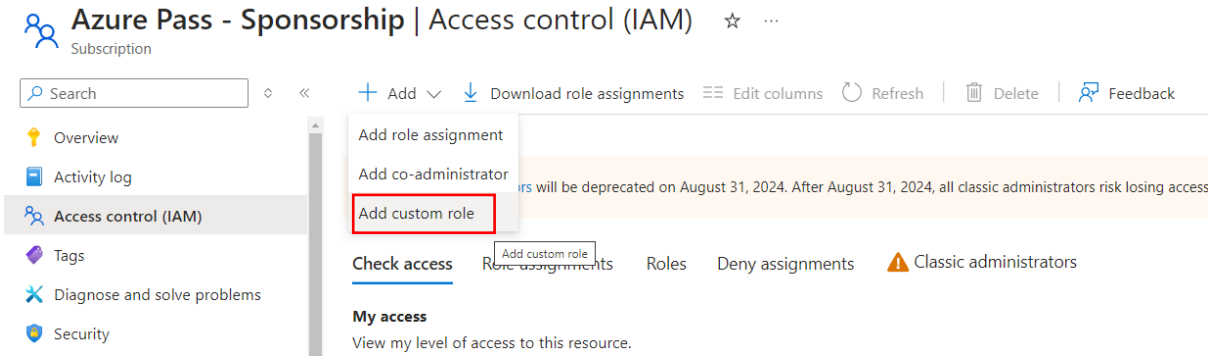
8. Now if you go back to your demo user account and refresh the page after clearing the cache then go to the resource group and here you can see the RG and your storage account.



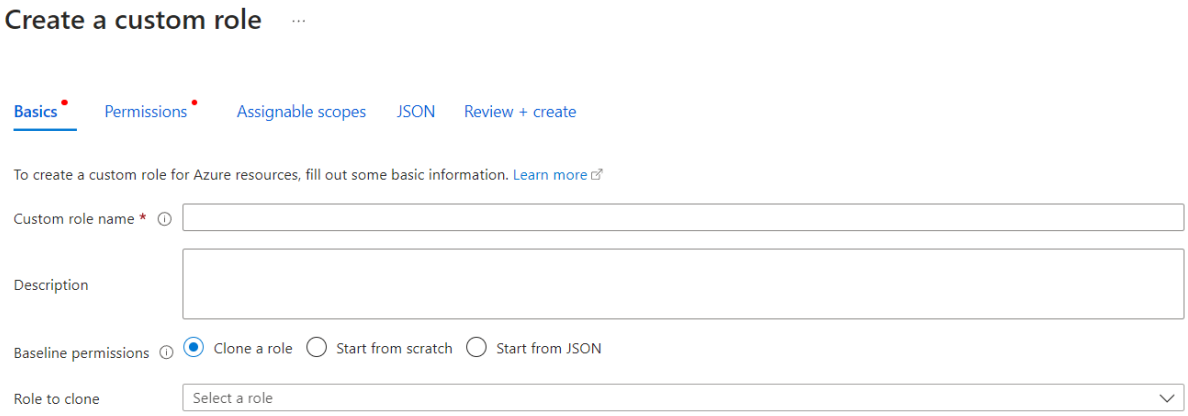
9. You can also read the contents of it, but you cannot make any changes to it.

😁 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.

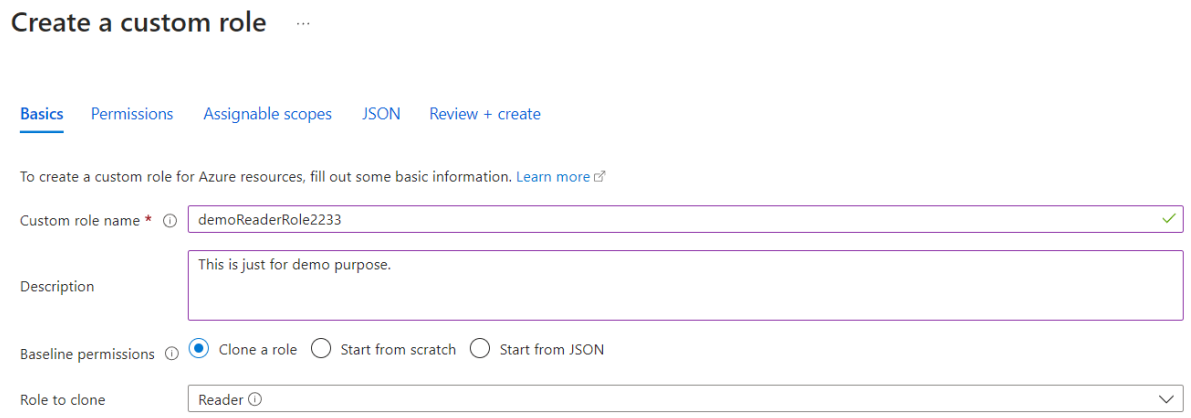


2. So, to create a custom role you have three options, first you can clone using the existing roles that you have in Azure Portal. Second, you can start from Scratch. Third, you can start writing your role in JSON, or if you have any file in which you already a have role written in JOSN then you can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

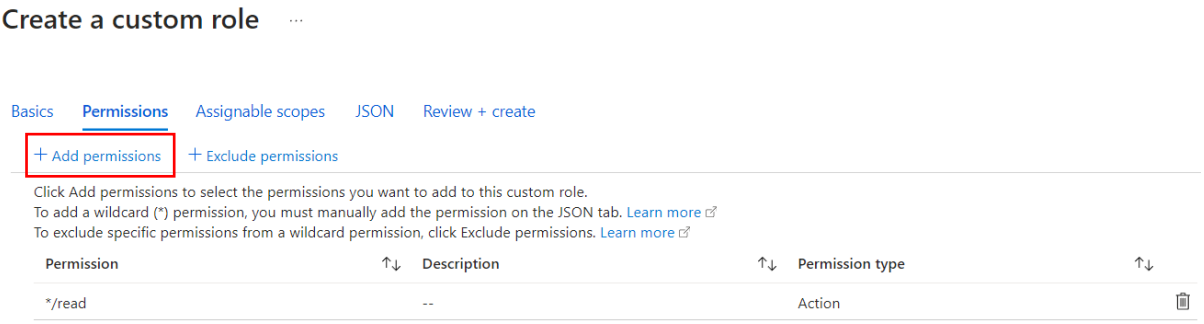


3. But for this demo we are going to choose to clone a role. Now first you need to give a name to your role. Then the description is optional. After that, you need to choose which

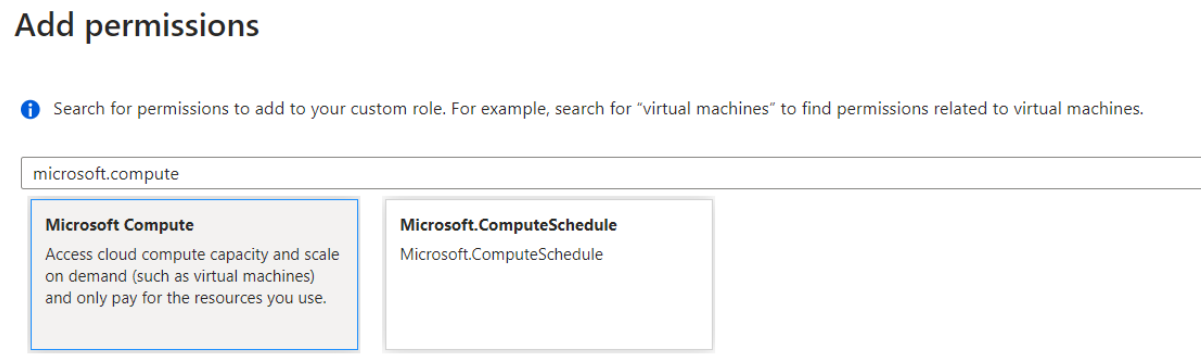
role you want to clone. Below you can see that we have chosen the reader role. Then move to the next page.



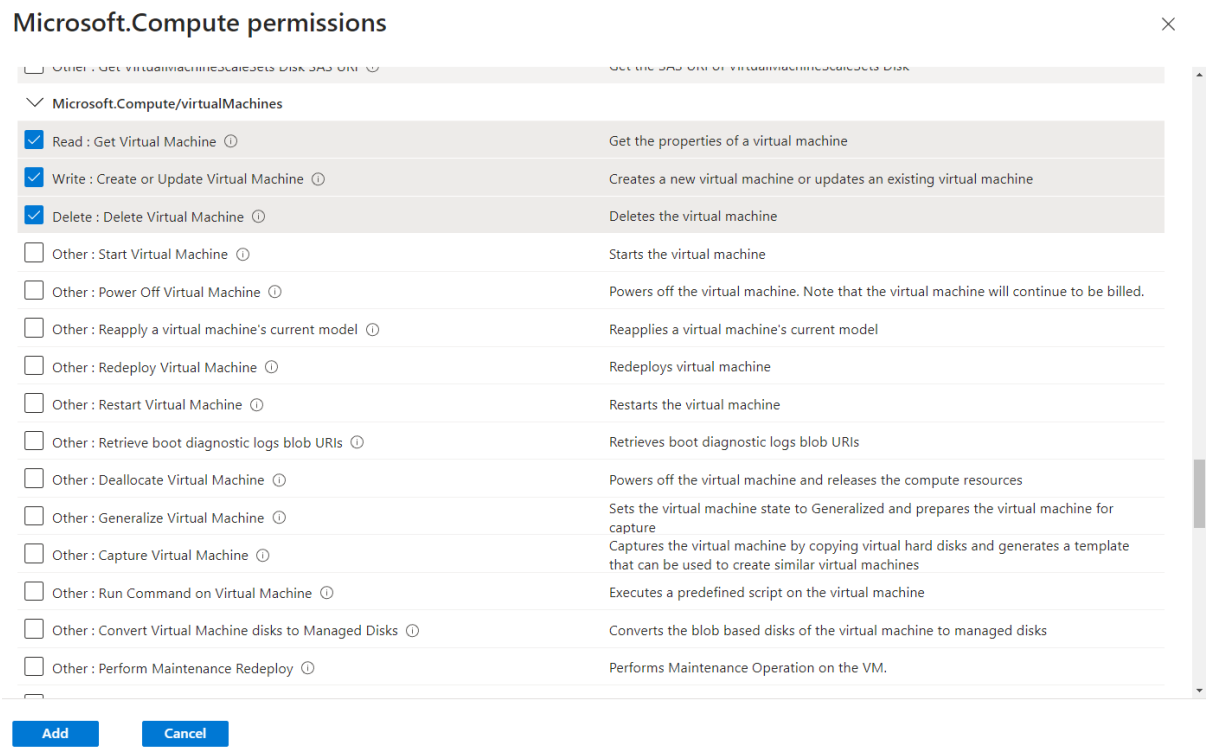
4. Then you can add some extra permissions by clicking on the highlighted icon.



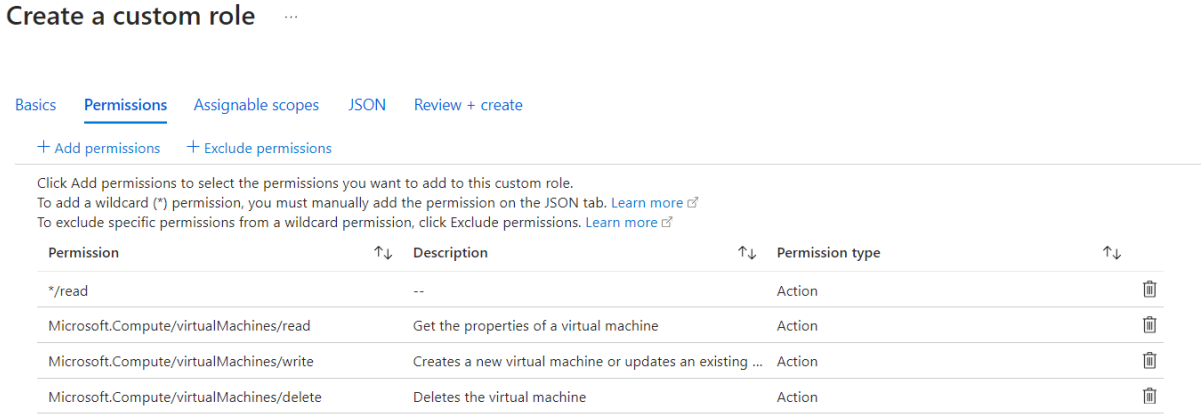
5. Now to add some extra permissions you can search for Microsoft Compute



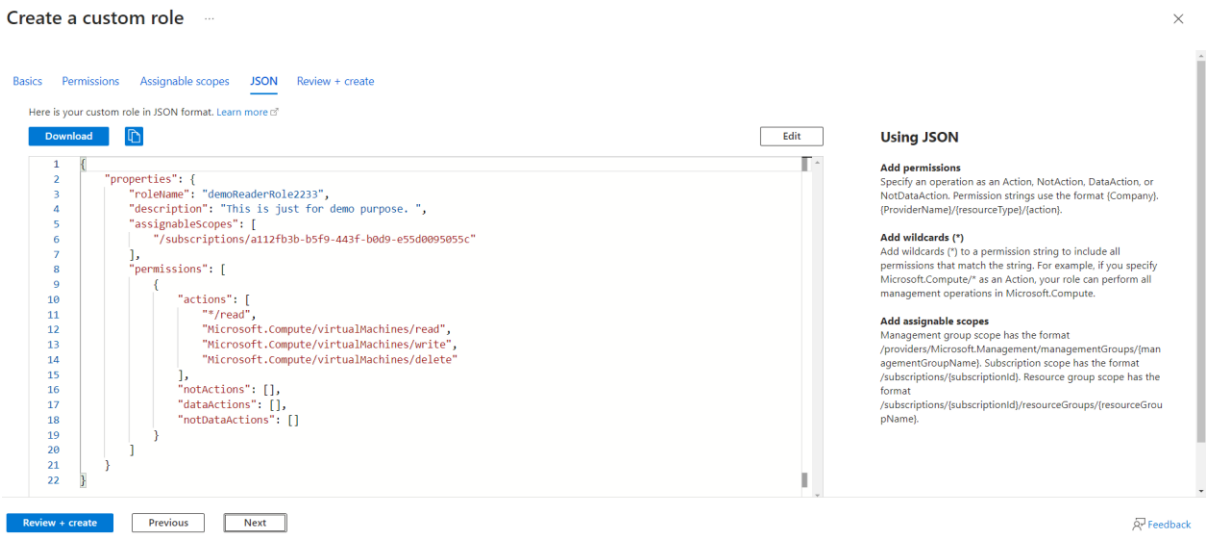
6. Now you need to scroll down to virtual machines, and you can choose the operations you want. Then just click on add.



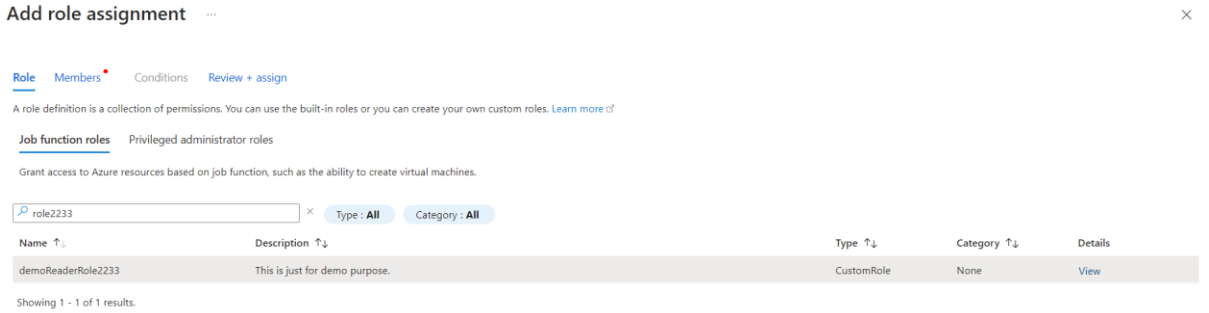
7. Then you can see your extra permission here along with the read permission. Then



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.



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.



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