😊 Assigning an Azure AD built-in Role

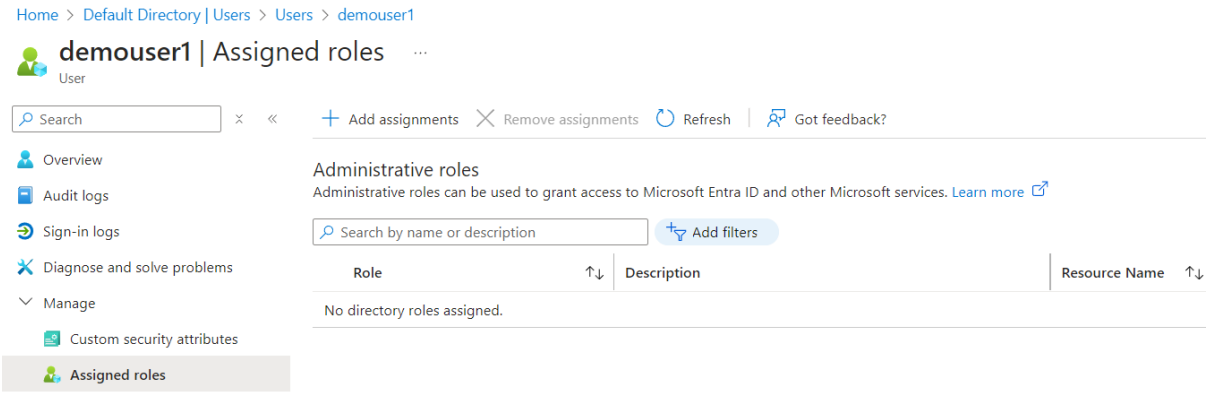
Azure AD built-in roles are a set of predefined roles that provide granular access to various Azure AD resources and functionalities. These roles are designed to facilitate access management and delegation of administrative tasks within Azure AD. Here are some key points about Azure AD built-in roles:

1. **Predefined Permissions:** Each built-in role comes with a set of permissions that define what actions a user assigned to that role can perform within Azure AD.
2. **Granular Access Control:** Azure AD built-in roles offer granular access control, allowing administrators to assign specific roles to users based on their responsibilities and the tasks they need to perform.
3. **Common Scenarios:** Built-in roles cater to common administrative scenarios, such as user management, application management, password management, and role management.
4. **Scope of Permissions:** Some built-in roles have permissions that are limited to specific scopes, such as management of users within a single directory or across multiple directories.
5. **Hierarchy of Roles:** Azure AD built-in roles follow a hierarchical structure, with roles at different levels of privilege. For example, the "Global Administrator" role has the highest level of privilege and encompasses permissions across the entire Azure AD tenant, while other roles may have more limited scopes.
6. **Role-Based Access Control (RBAC):** Azure AD built-in roles are part of the Role-Based Access Control (RBAC) model, which allows organizations to manage access to Azure resources based on assigned roles.

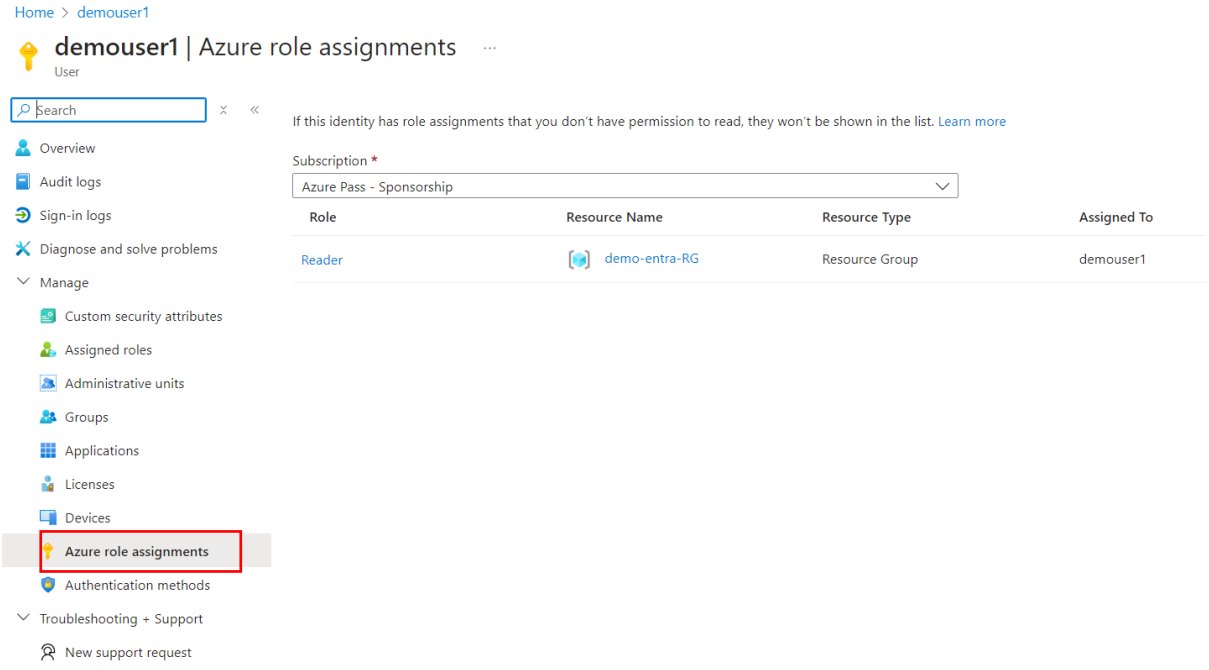
In this lab, we're showcasing how to assign Azure AD built-in roles to user accounts within the Azure AD environment. The end goal is to delegate specific administrative tasks to users by granting them appropriate permissions defined by these built-in roles. By assigning roles such as User Administrator, we empower users to perform tasks like creating new user accounts, thus streamlining administrative processes and enhancing efficiency in managing Azure AD resources. Ultimately, this exercise aims to demonstrate effective access management and delegation of administrative responsibilities within Azure AD.

😄 To begin with the Lab:

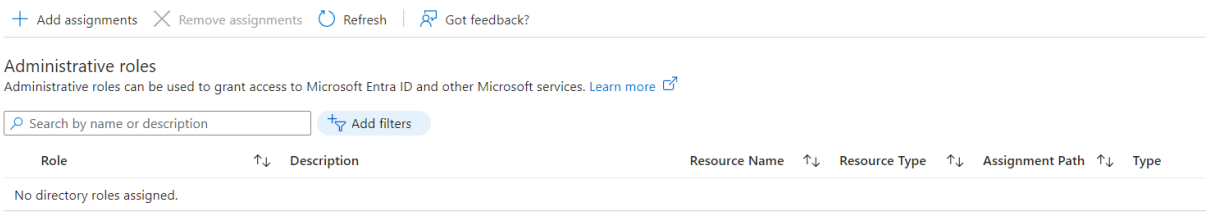
1. In this lab we are going to assign our demo user an Azure AD built-in role.
2. For that you should navigate to Microsoft Entra ID from your Azure Admin Account.
3. Then open users, from all users you need to open the demo user and then expand the Manage section. There you have to choose assigned roles.
4. Here you will see that currently you have zero roles assigned to it.



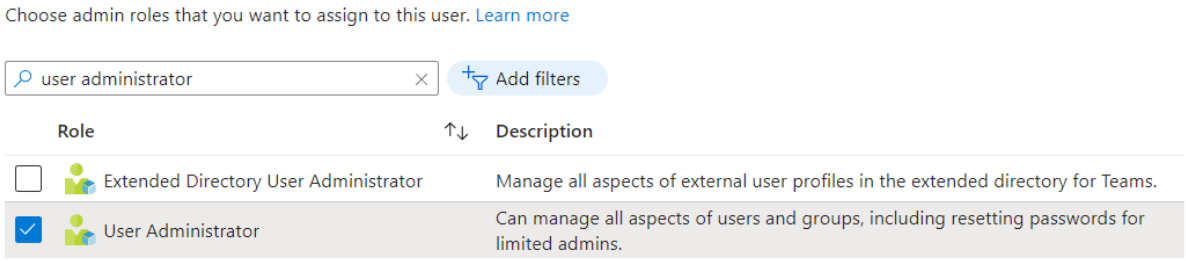
5. But if you check in Azure role assignments, you will see that you have a reader role assigned here.
6. This role is associated with RBAC (role-based access control).



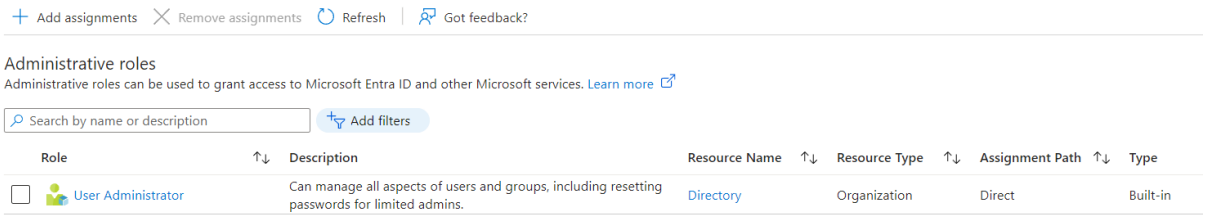
7. But when you are in assigned roles then it is know as Azure AD roles.
8. Now come back to assigned roles and click on add assignments.



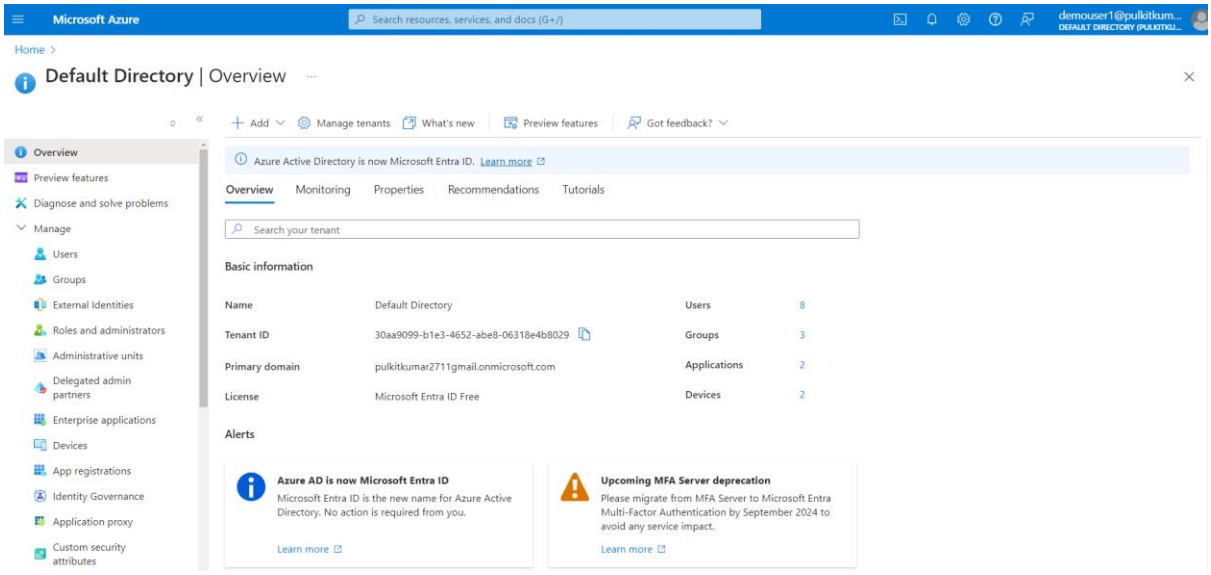
9. Then you need to search user administrator role and choose it accordingly.



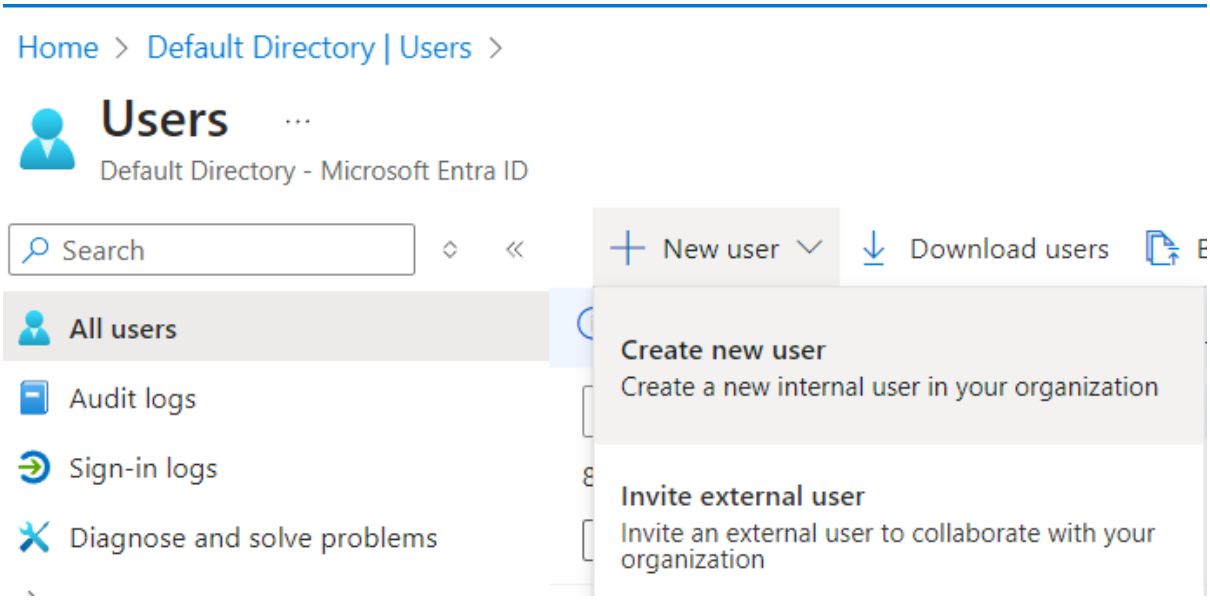
10. After some time you'll be able to see the role in place.



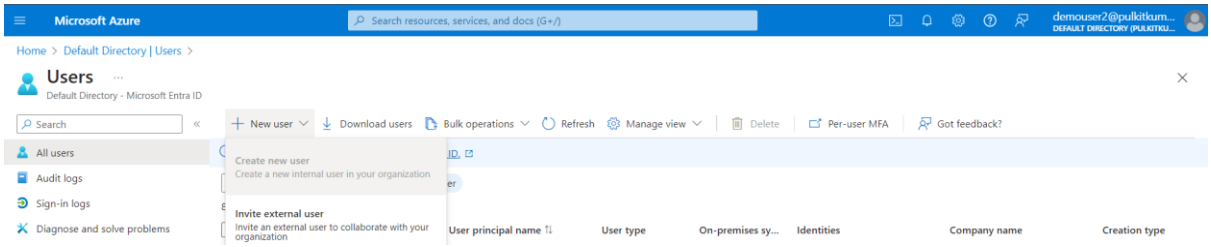
11. Now if you login with your demo user then go to Microsoft Entra then go to users.



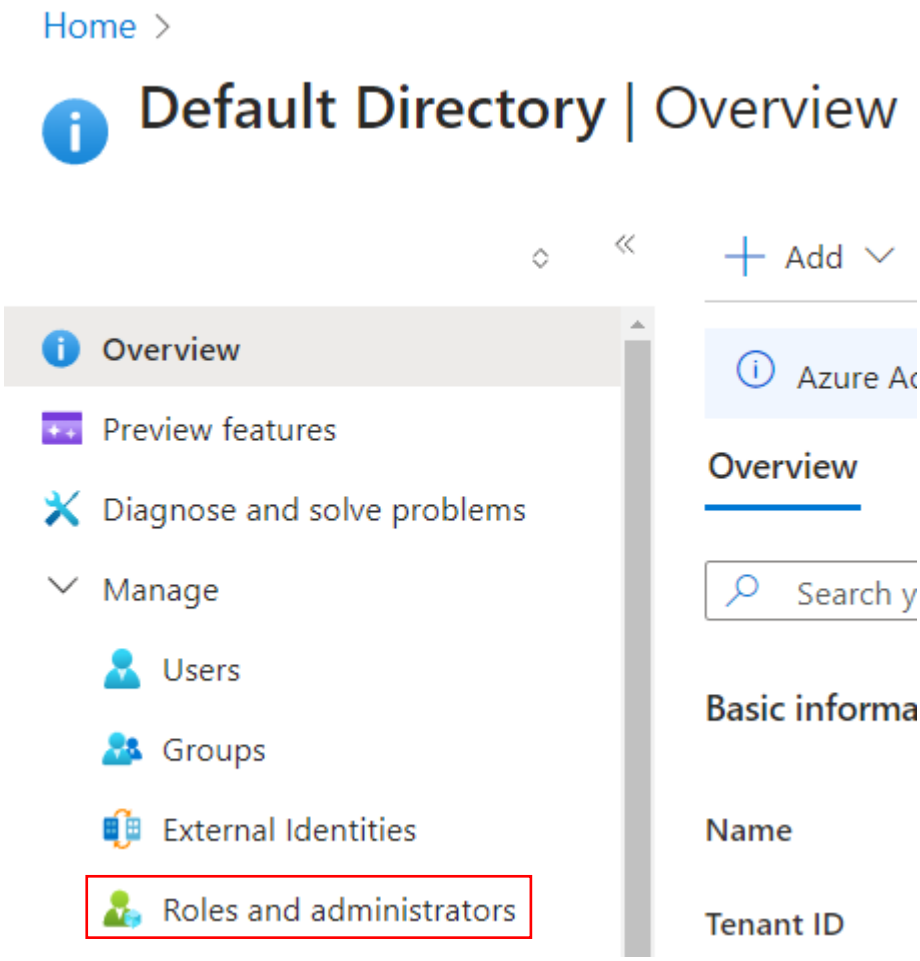
12. Now you can see that you have the ability to create a new user from your demo user.



13. Below you can also see that we have logged in with our demo user 2 account and it does not have the ability to create a new user because we haven't assigned roles to this user yet.



14. Plus, from your default directory of your admin account if you choose roles and administrators.



15. From here also you can directly attach an Azure AD role to user.