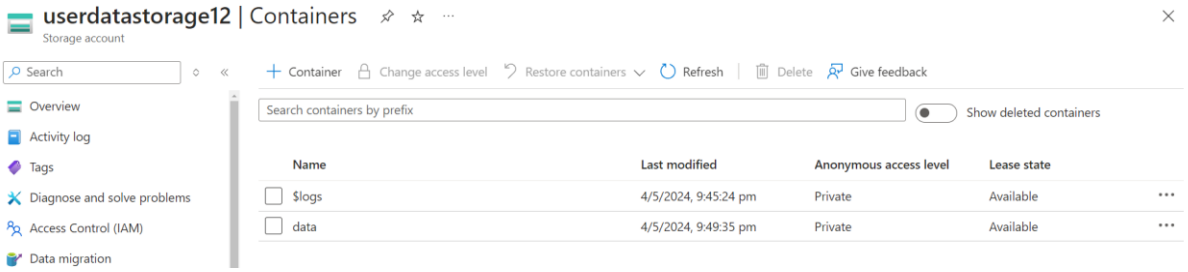
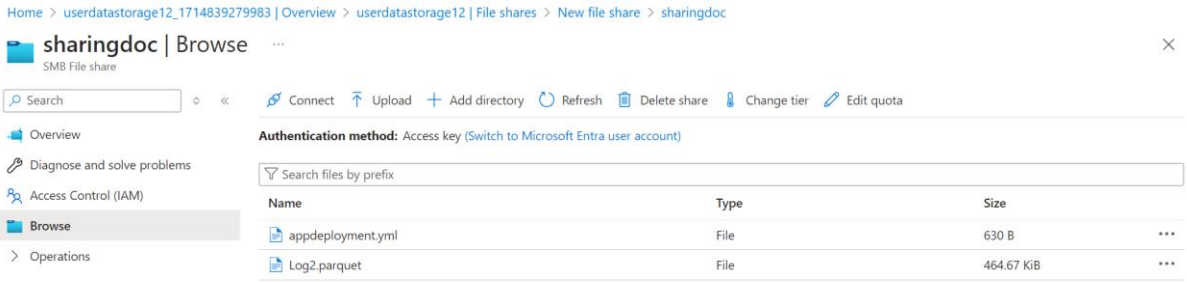
😊 More on Storage Account Roles

In this scenario, you're demonstrating how to manage access to Azure Storage resources using role-based access control (RBAC). The end goal is to ensure that users have the appropriate permissions to access and manage storage containers and file shares within Azure, while also maintaining security by restricting access to sensitive resources like access keys. By assigning roles such as reader or contributor, you control who can view, modify, and manage storage resources, thereby optimizing security and resource management within your Azure environment.

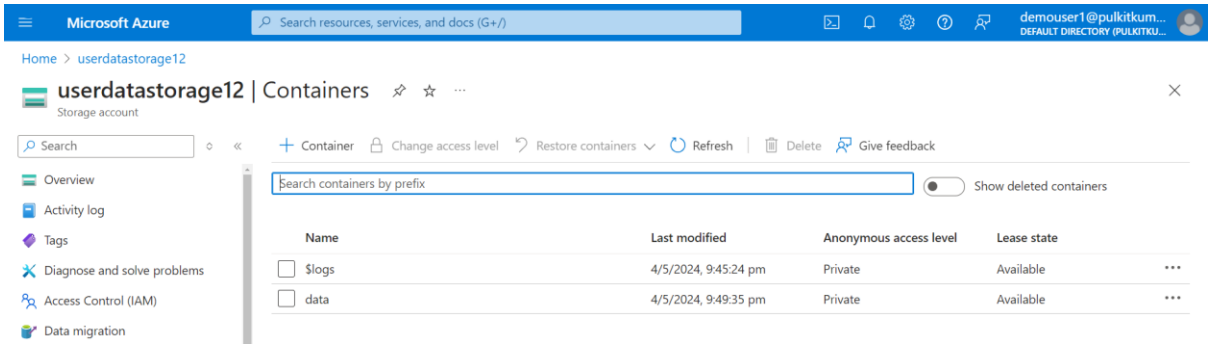
1. Until now we have a storage account, and we have reader role assignment added to demo user1.
2. Now in the Azure Admin account we will create a container and put some data in it. Then we will create a file share and again put some data in it.
3. Below you can see that we have created a container and put some data in it. You can put any data in it.



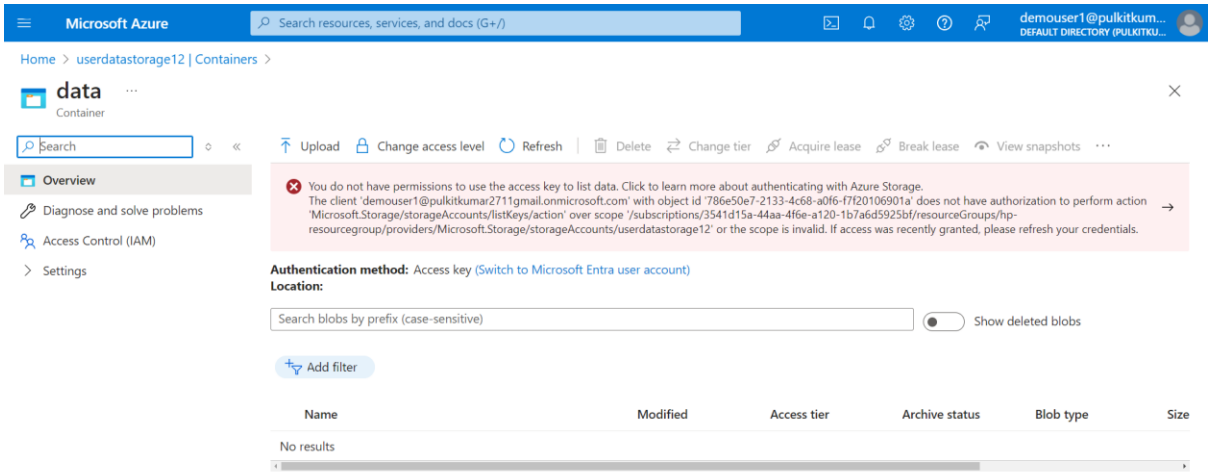
4. Below you can see that we created a file share and uploaded some files in it.



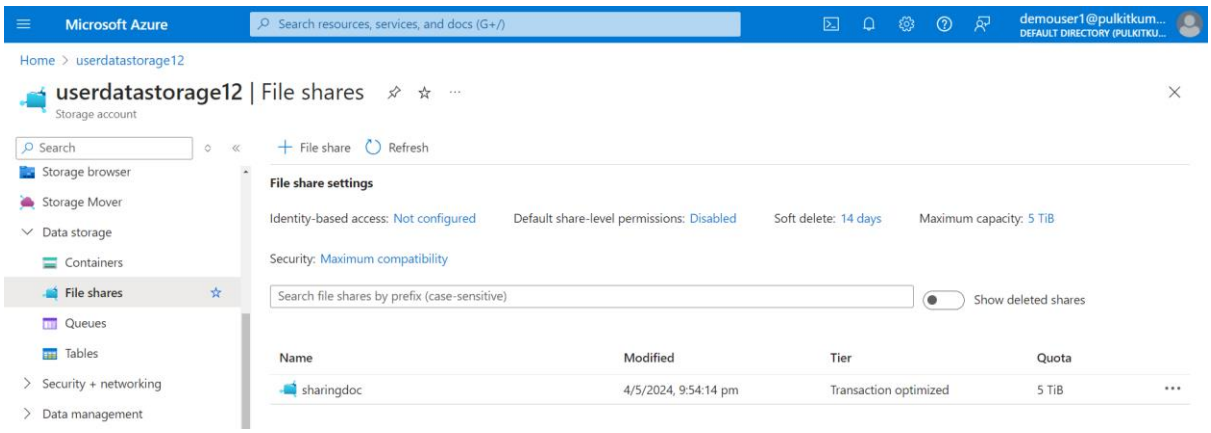
5. Now we need to open the tab in which our demo user1 account is open and we need to navigate to storage account.
6. Here if you go to your container then you will be able to see your container.

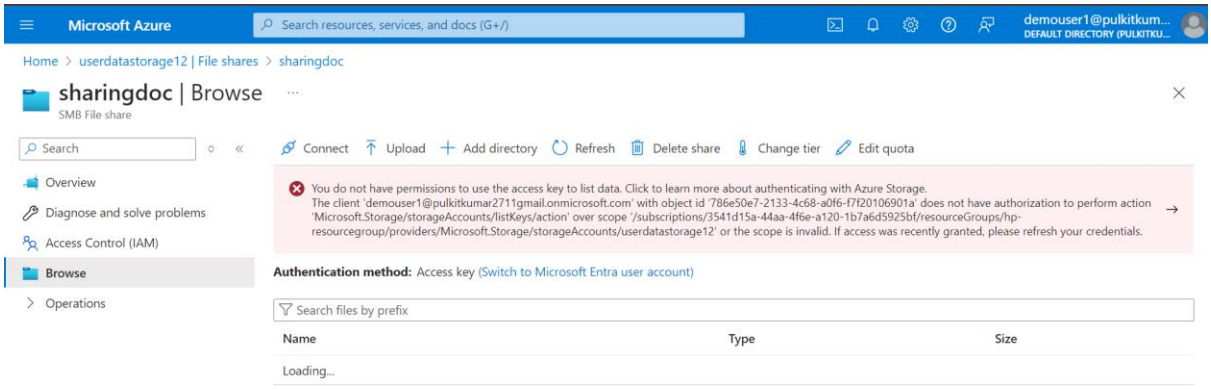


7. But if you try to access the container then you'll get an error message which says that you don't have permission to list the data.

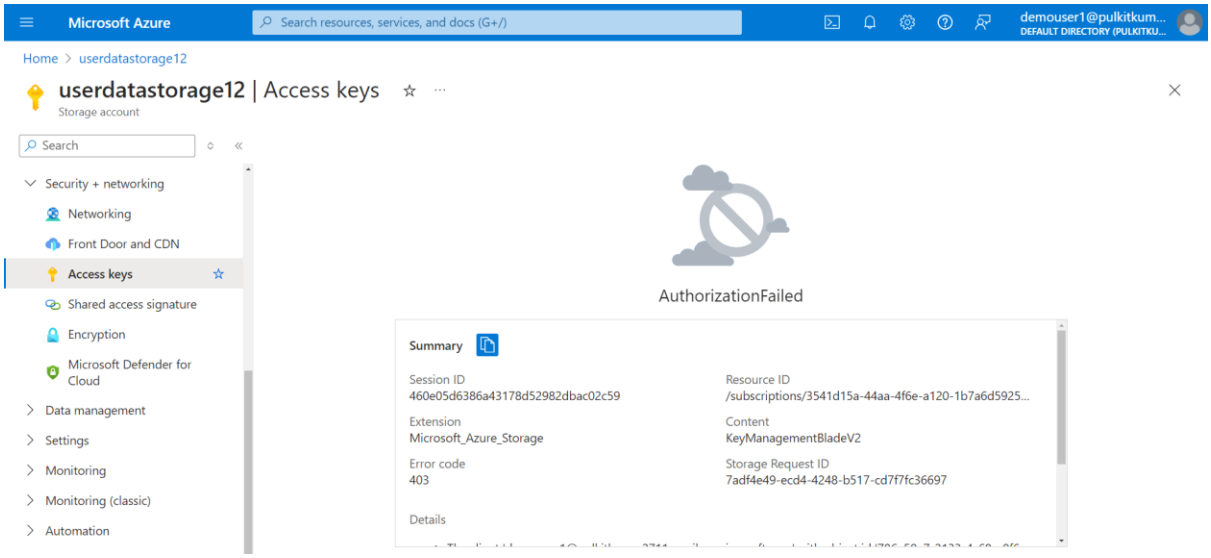


8. Same thing for file shares you can see the file share in place but if you try to access the data then you don't the required permissions for that.

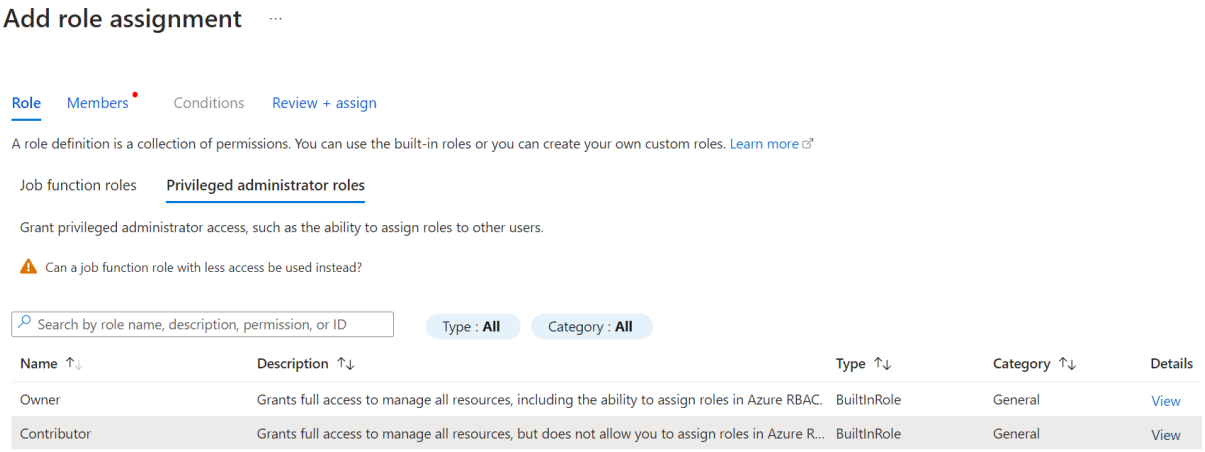




9. Moreover, if you try to see the access keys then you'll get error here too.

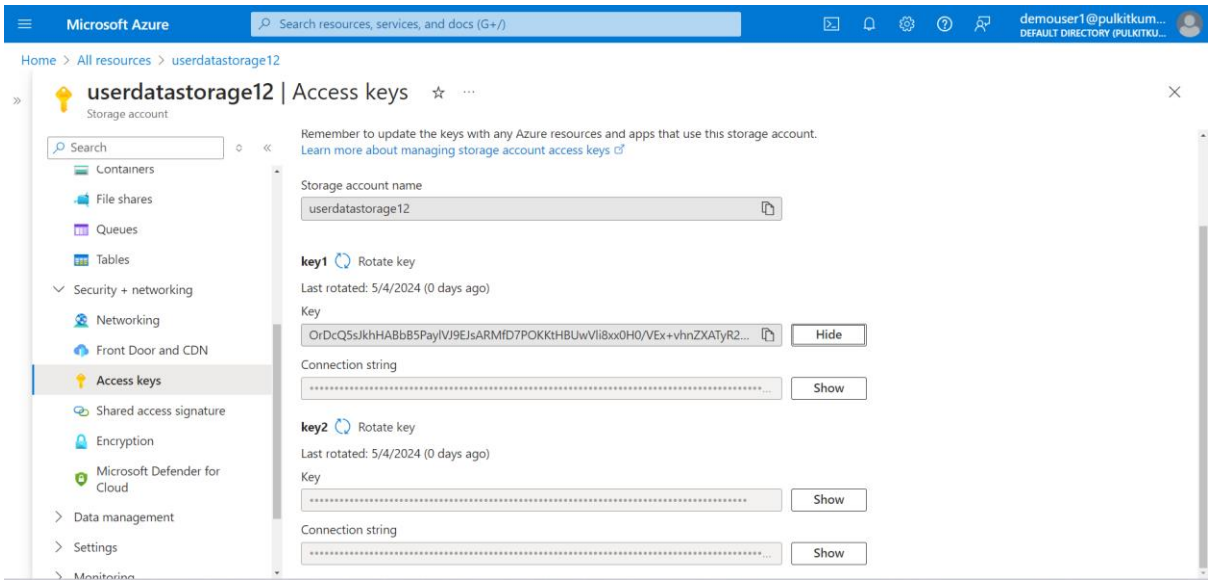


10. As you know currently, we just have attached reader role to it nothing more. This reader role does not give the permission to view the access keys.
11. Now we are going to attach the contributor role to it. Go to IAM of your storage account and click on add role assignment, then choose privileged administrator roles and choose contributor from here.

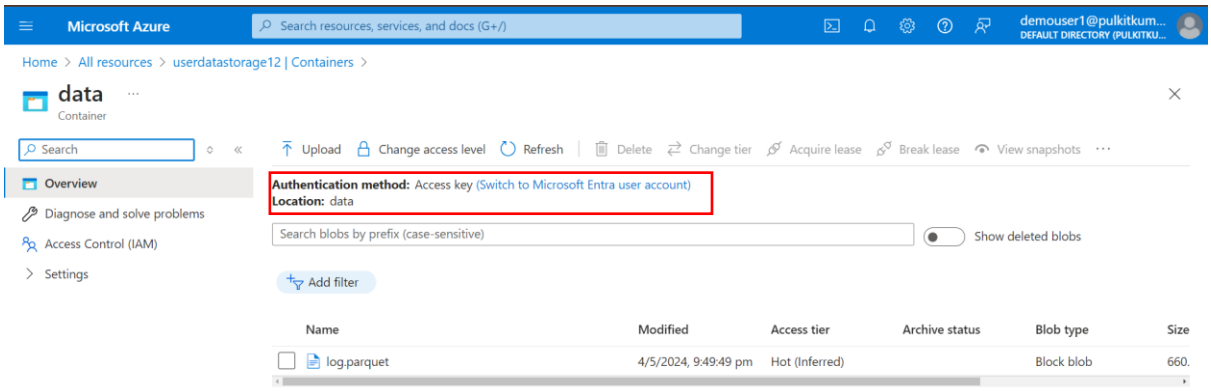


12. Then choose your user and create your role assignment.

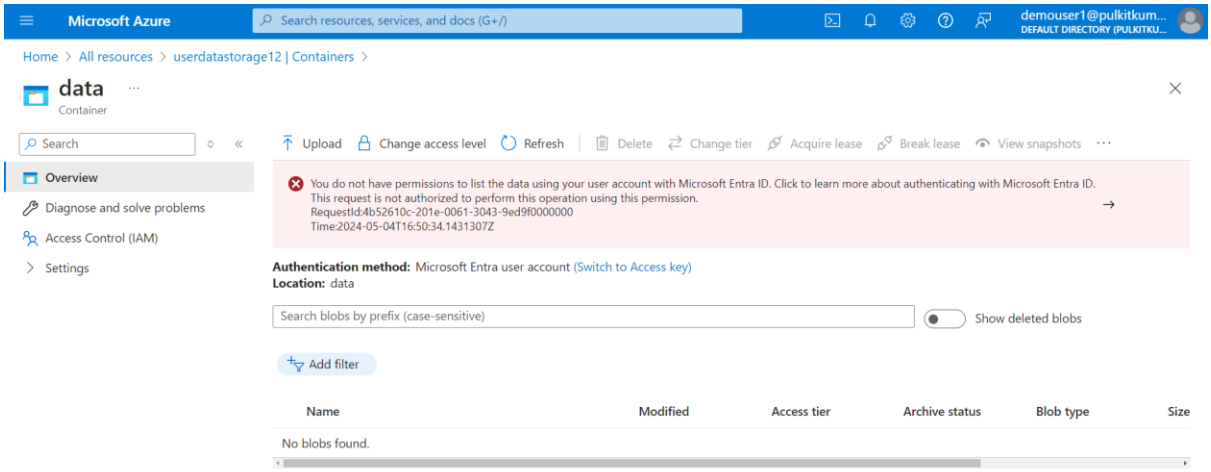
13. Once your role is created, then come back to the demo user1 tab and go to access keys in your storage account.
14. This time you'll be able to list the access keys.



15. Then go to containers and open your container and you can see your file there. But if you pay close attention then you can see that the authentication method is via Access keys.



16. Now if you click on switch to Microsoft entra user account or say azure active directory. Then you will get the error message again.



17. The same thing will be applicable for file shares too.