



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.

The screenshot shows the 'Containers' blade for a storage account named 'userdatastorage12'. On the left, there's a sidebar with links like Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), and Data migration. The main area has a search bar and buttons for Container, Change access level, Restore containers, Refresh, Delete, and Give feedback. A table lists containers with columns for Name, Last modified, Anonymous access level, and Lease state. Two containers are listed: '\$logs' and 'data', both created on 4/5/2024 at different times, both set to Private, and both marked as Available.

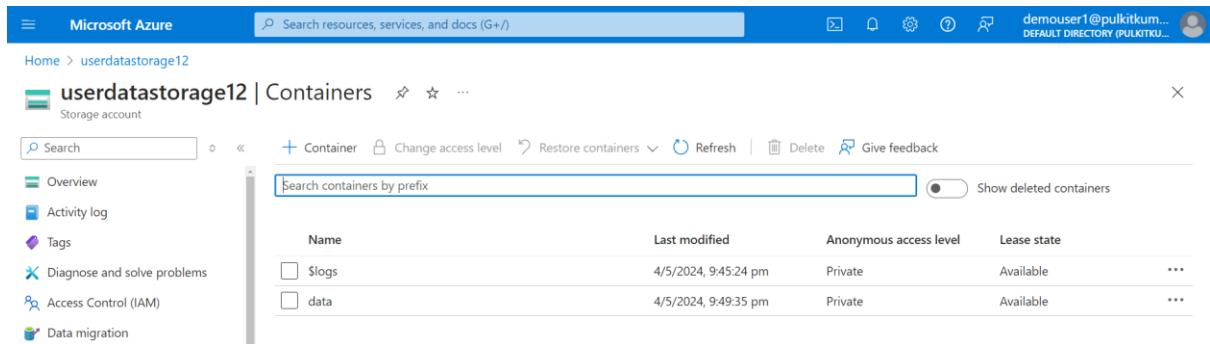
Name	Last modified	Anonymous access level	Lease state
\$logs	4/5/2024, 9:45:24 pm	Private	Available
data	4/5/2024, 9:49:35 pm	Private	Available

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

The screenshot shows the 'File shares' blade for a storage account named 'userdatastorage12_1714839279983'. The sidebar includes links for Overview, Diagnose and solve problems, Access Control (IAM), and a highlighted 'Browse' link. The main area shows the authentication method as 'Access key (Switch to Microsoft Entra user account)'. It features a search bar and buttons for Connect, Upload, Add directory, Refresh, Delete share, Change tier, and Edit quota. A table lists files in the share with columns for Name, Type, and Size. Two files are listed: 'appdeployment.yml' (File, 630 B) and 'Log2.parquet' (File, 464.67 KiB).

Name	Type	Size
appdeployment.yml	File	630 B
Log2.parquet	File	464.67 KiB

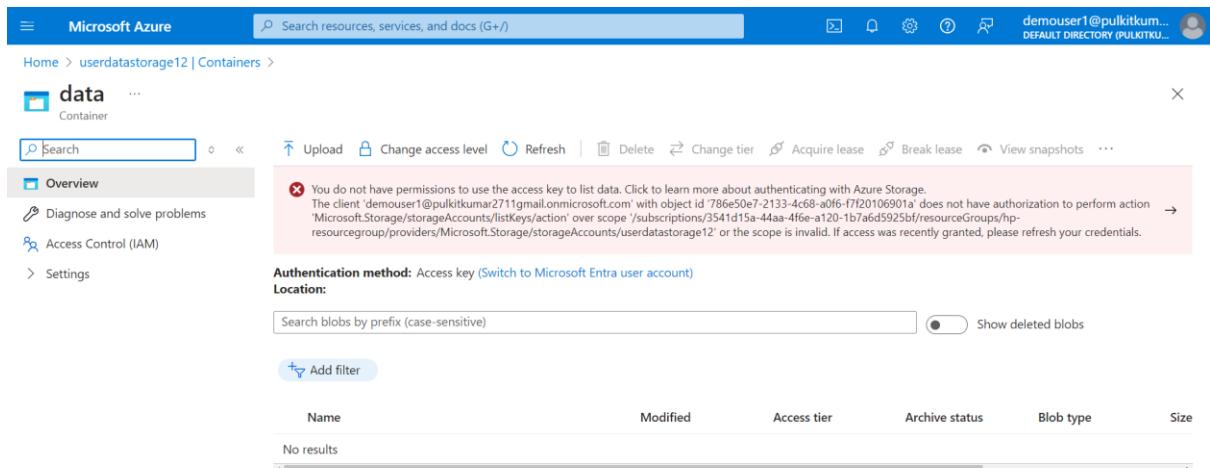
5. Now we need to open the tab in which our demo user1 account is open and we need to navigate to storage account.
6. Here if you go to your container then you will be able to see your container.



The screenshot shows the Microsoft Azure Storage Container list page for the userdatastorage12 account. The left sidebar includes links for Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), and Data migration. The main area displays a table with two rows: \$logs and data. The \$logs row was modified on 4/5/2024 at 9:45:24 pm, has Private anonymous access, and is Available. The data row was modified on 4/5/2024 at 9:49:35 pm, has Private anonymous access, and is Available.

Name	Last modified	Anonymous access level	Lease state
\$logs	4/5/2024, 9:45:24 pm	Private	Available
data	4/5/2024, 9:49:35 pm	Private	Available

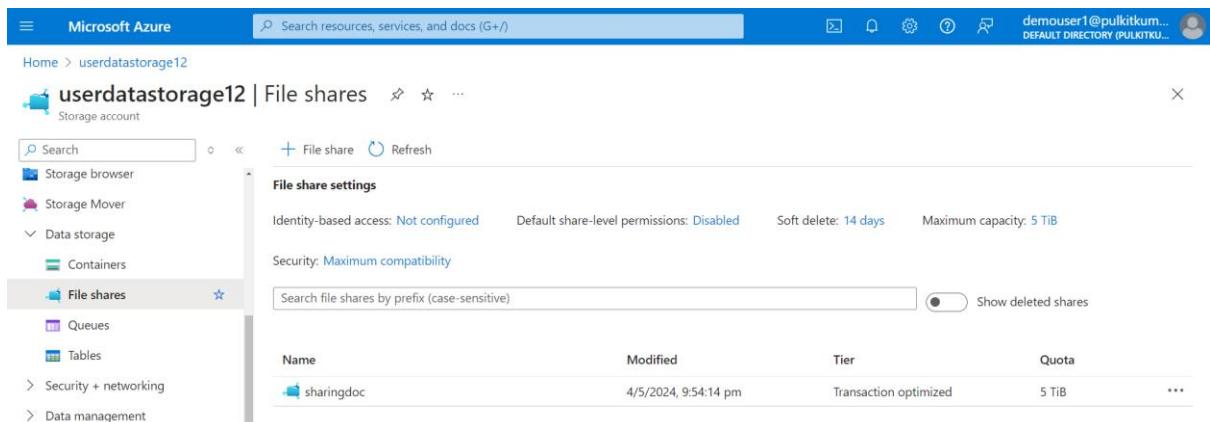
7. But if you try to access the container then you'll get an error message which says that you don't have permission to list the data.



The screenshot shows the Microsoft Azure Storage Container details page for the 'data' container. The left sidebar includes links for Overview, Diagnose and solve problems, Access Control (IAM), and Settings. A prominent error message states: "You do not have permissions to use the access key to list data. Click to learn more about authenticating with Azure Storage. The client 'demouser1@pulkitkumar2711@gmail.onmicrosoft.com' with object id '786e50e7-2133-4c68-a0f6-77f20106901a' does not have authorization to perform action 'Microsoft.Storage/storageAccounts/listKeys/action' over scope '/subscriptions/3541d15a-44aa-4f6e-a120-157af6d5925bf/resourceGroups/hp-resourcegroup/providers/Microsoft.Storage/storageAccounts/userdatastorage12' or the scope is invalid. If access was recently granted, please refresh your credentials." Below the error message, there is a note about the authentication method: "Authentication method: Access key (Switch to Microsoft Entra user account)" and a location field. The main table shows no results.

Name	Modified	Access tier	Archive status	Blob type	Size
No results					

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 have the required permissions for that.



The screenshot shows the Microsoft Azure Storage File shares list page for the userdatastorage12 account. The left sidebar includes links for Storage browser, Storage Mover, Data storage, Containers, File shares, Queues, Tables, Security + networking, and Data management. The main area displays a table with one row: sharingdoc. The sharingdoc file share was modified on 4/5/2024 at 9:54:14 pm, is in the Transaction optimized tier, has a Quota of 5 TiB, and is listed under the Maximum compatibility security setting.

Name	Modified	Tier	Quota
sharingdoc	4/5/2024, 9:54:14 pm	Transaction optimized	5 TiB

You do not have permissions to use the access key to list data. Click to learn more about authenticating with Azure Storage.
The client 'demouser1@pulkitkumar271@gmail.onmicrosoft.com' with object id '786e50e7-2133-4c68-a0f6-f7f2016901a' does not have authorization to perform action 'Microsoft.Storage/storageAccounts/listKeys/action' over scope '/subscriptions/3541d15a-44aa-4f6e-a120-1b7a6d5925b1/resourceGroups/hip-resourcegroup/providers/Microsoft.Storage/storageAccounts/userdatastorage12' or the scope is invalid. If access was recently granted, please refresh your credentials.

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

AuthorizationFailed

Summary	
Session ID	460e05d6386a43178d52982dbac02c59
Extension	Microsoft_Azure_Storage
Error code	403
Details	Resource ID /subscriptions/3541d15a-44aa-4f6e-a120-1b7a6d5925b1... Content KeyManagementBladeV2 Storage Request ID 7adf4e49-ecd4-4248-b517-cd7f7fc36697

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.

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 **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 R...	BuiltInRole	General	View

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.

The screenshot shows the 'Access keys' section of the Azure Storage blade for the 'userdatastorage12' account. The left sidebar has 'Access keys' selected. The main area displays two sets of keys: 'key1' and 'key2'. Each key includes a 'Rotate key' button, a 'Last rotated' timestamp (5/4/2024), a 'Key' field containing a long hex string, and a 'Show' button. Below each key is a 'Connection string' field with a 'Show' button. A note at the top says 'Remember to update the keys with any Azure resources and apps that use this storage account.' and a link to 'Learn more about managing storage account 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.

The screenshot shows the 'Containers' blade for the 'userdatastorage12' account, specifically the 'data' container. The left sidebar has 'Overview' selected. The top navigation bar includes 'Upload', 'Change access level', 'Refresh', 'Delete', 'Change tier', 'Acquire lease', 'Break lease', 'View snapshots', and a '... More' button. A red box highlights the 'Authentication method: Access key (Switch to Microsoft Entra user account)' and 'Location: data' text. Below this is a search bar and a 'Show deleted blobs' toggle. The main table lists one blob named 'log.parquet' with details: Name (log.parquet), Modified (4/5/2024, 9:49:49 pm), Access tier (Hot (Inferred)), Archive status (Not yet archived), Blob type (Block blob), and Size (660).

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.

The screenshot shows the Microsoft Azure Storage Explorer interface. At the top, there's a search bar and a user profile for 'demouser1@pulkitum...'. Below the header, the navigation path is 'Home > All resources > userdatasastorage12 | Containers > data'. The main area is titled 'Overview' and contains a message: 'You do not have permissions to list the data using your user account with Microsoft Entra ID. Click to learn more about authenticating with Microsoft Entra ID.' It also shows a request ID and timestamp. Below this, there's a section for 'Authentication method: Microsoft Entra user account' with a link to 'Switch to Access key'. A 'Search blobs by prefix (case-sensitive)' input field and a 'Show deleted blobs' toggle are present. A 'Add filter' button is available. A table header with columns 'Name', 'Modified', 'Access tier', 'Archive status', 'Blob type', and 'Size' is shown, followed by a message 'No blobs found.'

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