



Azure Active Directory (AD) Authentication

"Azure Active Directory (Azure AD) is a cloud-based identity and access management service that allows the users to access the resources. Azure AD provides different benefits, based on their roles, to the users"

Login to Azure Portal, for this lab you must have a Storage Account and container including temporary files in it.

Step 1: See for the all Menus on the Left-hand side Pane.

- Click on Azure Active Directory.

The screenshot shows the Azure Portal interface. On the left, the sidebar includes options like 'Create a resource', 'Home', 'Dashboard', 'All services' (which is selected), 'FAVORITES' (empty), 'All resources', 'Resource groups', 'App Services', 'Function App', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', 'Azure Active Directory' (highlighted with a red box), 'Monitor', 'Advisor', and 'Microsoft Defender for Cloud'. The main content area displays a grid of service icons: Function App, Azure compute galleries, Images, App Services, Virtual networks, Virtual machines, Storage accounts, and Cost Management Below this is a 'Recent' section listing various resources with their type and last viewed time. At the bottom, the URL 'https://portal.azure.com/#allservices/category/All' is shown.

Type	Last Viewed
Azure compute gallery	an hour ago
Azure compute gallery	an hour ago
Virtual network	an hour ago
Virtual network	an hour ago
Virtual network	an hour ago
Subscription	2 hours ago
Network security group	2 days ago
Network security group	2 days ago
Network security group	2 days ago
Network security group	2 days ago

Step 2: On the Azure Directory Page, you can see the Users on your Account. Click on Create New user and Create a New Demo User.

Home > Default Directory | Users >

Users ...

Download users Bulk operations Refresh Manage view Delete Per-user MFA Got feedback?

All users

Audit logs Sign-in logs Diagnose and solve problems

Manage Deleted users Password reset User settings Bulk operation results

Troubleshooting + Support New support request

Azure Active Directory is becoming Microsoft Entra ID.

1 user found

Display name	User principal name	User type	On-premises sync	Identities	Company name
AP	anilreddy@contoso.on...	Member	No	MicrosoftAccount	

- Enter the Name for your New User, Uncheck Auto-Generated password and enter the custom password. Click on Review + Create.

Home > Default Directory | Users > Users >

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 @ Domain not listed

Mail nickname * readonly Derive from user principal name

Display name*

Password* Auto-generate password

Account enabled

Review + create Previous Next: Properties Give feedback

- After Successful Creation of the new user, you can see the newly created user on the Users Page.

Home >

Users

All users

Audit logs Sign-in logs Diagnose and solve problems

Deleted users Password reset User settings Bulk operation results

New support request

Search New user Download users Bulk operations Refresh Manage view Delete Per-user MFA Got feedback?

Azure Active Directory is becoming Microsoft Entra ID.

Display name	User principal name	User type	On-premises sync	Identities	Company name
AP	behalrithesh@gmail.onmicrosoft.com	Member	No	MicrosoftAccount	
	readcr...@outlook.com	Member	No	MicrosoftAccount	

👉 Step 3: Click on the recent Created User and copy User principal Name.

Home >

storageacc

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

Overview Monitoring Properties

Basic info

storageacc Member

User principal name behalrithesh@gmail.onmicrosoft.com 

Object ID d4353a3b-1980-4df1-af55-d9e7610b004d

Created date time Aug 25, 2023, 11:57 AM

User type Member

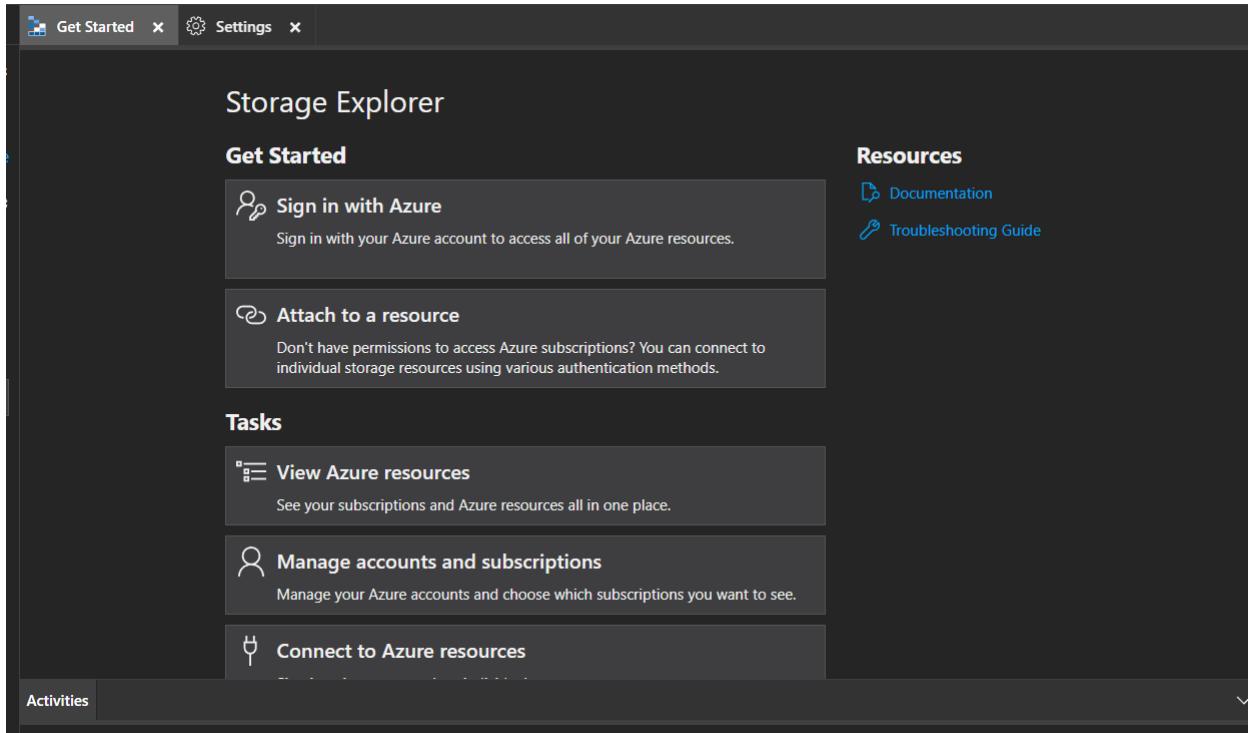
Identities behalrithesh@gmail.onmicrosoft.com

Group members 0 Applications 0 Assigned roles 0 Assigned licenses 0

My Feed

Account status Enabled B2B collaboration

👉 Step 4: Open the Azure Storage Explorer and Click on Sign in with Azure.



- You will be redirected to the Azure Sign in Page on your Browser.
- Paste the copied UserID and Click on Next.
- Enter the Password given by you while creating the user & Sign in.

Microsoft Azure



Sign in

storageaccountname@outlook.onmicrosoft.com

No account? [Create one!](#)

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

Back

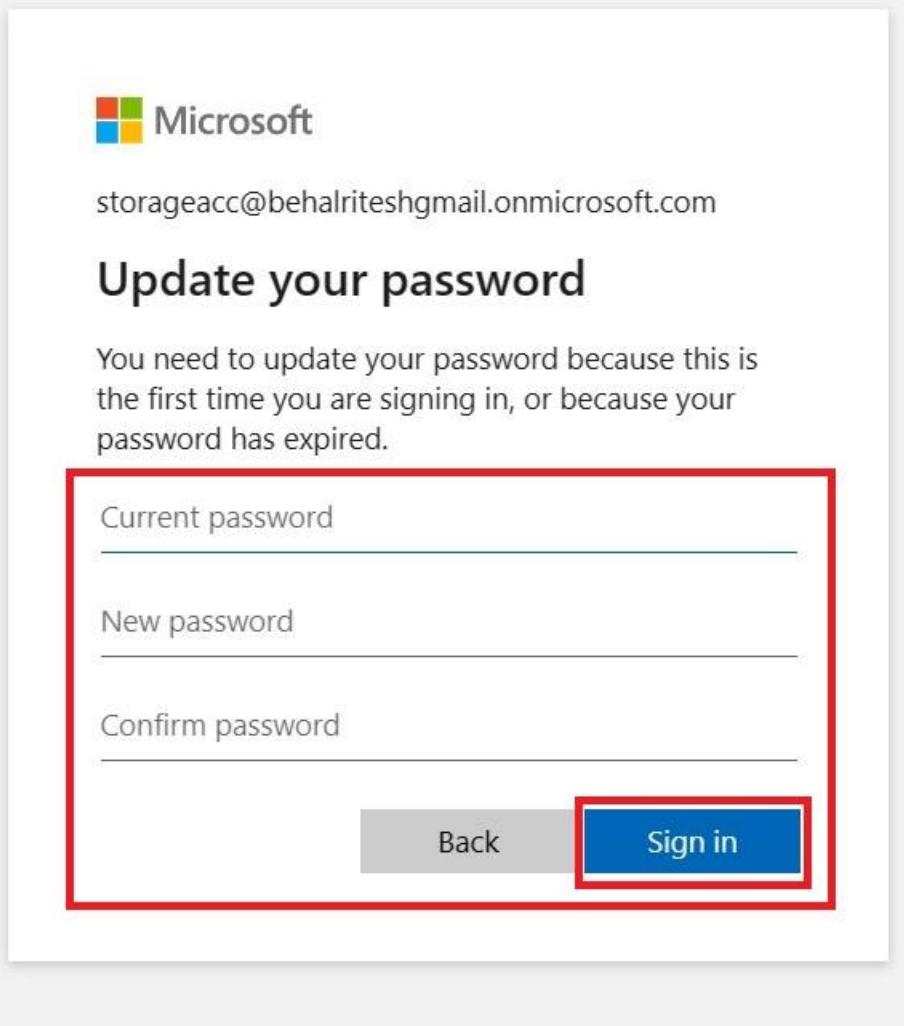
Next



Sign-in options

- After Signing in a New User Account, Azure asks you to Change the Password.
- Enter the Current & New Password and click on Sign in.

Microsoft Azure



The screenshot shows a Microsoft Azure password update interface. At the top left is the Microsoft logo. Below it is the email address: storageacc@behalritesgmail.onmicrosoft.com. The main title is "Update your password". A message below the title states: "You need to update your password because this is the first time you are signing in, or because your password has expired." There are three input fields: "Current password", "New password", and "Confirm password", each with a horizontal line for input. Below these fields is a button bar with "Back" and "Sign in" buttons. The "Sign in" button is highlighted with a red border.

storageacc@behalritesgmail.onmicrosoft.com

Update your password

You need to update your password because this is the first time you are signing in, or because your password has expired.

Current password

New password

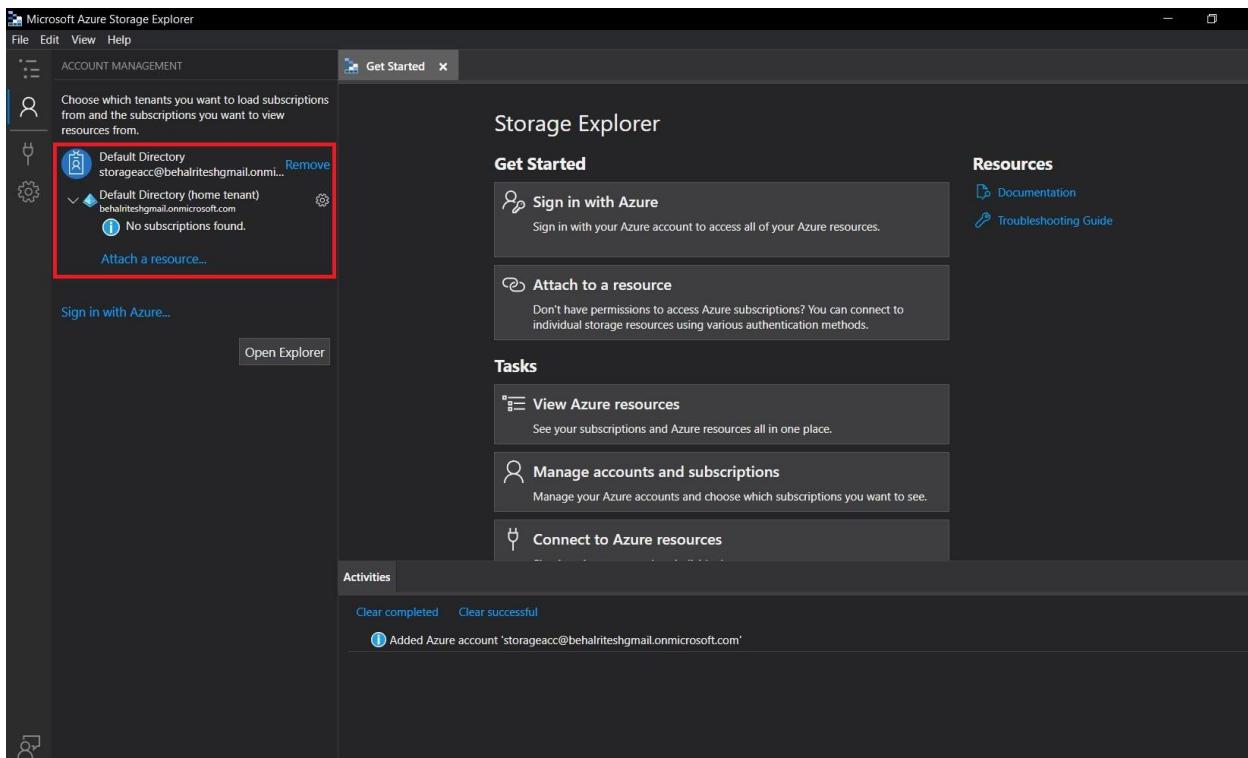
Confirm password

Back Sign in

- It will take a few minutes to Authenticate.

 **Step 5:** After the authentication, Come back to your Storage Explorer. You have Successfully Signed in with your user account.

- Till now you can see there is no subscription found.
- We have to assign the roles to get the information fetched to our Storage Explorer.



Step 6: In azure Portal, Go to your Storage Account. On the left Side pane Click on access control.

- Click on Add or Add role assignment.

The screenshot shows the 'Access Control (IAM)' blade for a storage account named 'objreplica_1692945788810'. The left sidebar has a red box around the 'Access Control (IAM)' item. The main area has a red box around the '+ Add' button in the top navigation bar. Below it, there are sections for 'Check access', 'My access', and three buttons: 'Grant access to this resource', 'View access to this resource', and 'View deny assignments'. Each button has a red box around it.

You have a different role Available for your Storage Account.

- Select for the Reader role and Click on Next.

Home > objreplica_169294578810 | Overview > objreplica | Access Control (IAM) > Add role assignment ...

Add role assignment

Role Members 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](#)

Assignment type

Job function roles Privileged administrator roles

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

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View
App Compliance Automation Administ...	Create, read, download, modify and delete reports objects and related other resource objects.	BuiltInRole	None	View
App Compliance Automation Reader	Read, download the reports objects and related other resource objects.	BuiltInRole	None	View
Azure Center for SAP solutions administ...	This role provides read and write access to all capabilities of Azure Center for SAP solutions.	BuiltInRole	None	View
Azure Center for SAP solutions reader	This role provides read access to all capabilities of Azure Center for SAP solutions.	BuiltInRole	None	View
Defender for Storage Data Scanner	Grants access to read blobs and update index tags. This role is used by the data scanner of Defend...	BuiltInRole	None	View
Loq Analytics Contributor	Loq Analytics Contributor can read all monitoring data and edit monitoring settings. Editing monit...	BuiltInRole	Analytics	View

Review + assign Previous Next

Feedback

- Select Member in which account you have to assign the selected roles.

Home > objreplica_1692945788810 | Overview > objreplica | Access Control (IAM) >
Add role assignment ...

Role **Members*** Review + assign

Selected role Reader

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

Members [+ Select members](#) 1

Name	Object ID	Type
No members selected		

Description Optional

Review + assign Previous Next 4

Select members

Select

Search by name or email address

DE	-	2
DE	-	
RB	abhishek_gmail.com#EXT#@abhishek.onmicrosoft.com	
US	user1@onmicrosoft.com	

Selected members:

ST	st	3
----	----	---

[Remove](#)

3 [Select](#) Close

- After Selecting the member has been added. Click on Review + Assign.

In a few minutes the role will be assigned to the user.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > objreplica_1692945788810 | Overview > objreplica | Access Control (IAM) > Add role assignment

Role **Members** Review + assign

Selected role Reader

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

Members + Select members

Name	Object ID	Type
storageacc	d4353a3b-1980-4df1-af55-d9e7610b00...	User

Description Optional

Review + assign Previous Next Feedback

- Refresh the storage explorer and you can see now the subscriptions are shown below User.

Microsoft Azure Storage Explorer

File Edit View Help

ACCOUNT MANAGEMENT

Get Started

Choose which tenants you want to load subscriptions from and the subscriptions you want to view resources from.

Default Directory
storageacc@behalrites@gmail.onmicrosoft.com Remove

Default Directory (home tenant)
behalrites@gmail.onmicrosoft.com

Select All Subscriptions

Azure Pass - Subscription
cb22fa00-bc06-41b6-9733-00fc299841a5

Sign in with Azure...

Open Explorer

Storage Explorer

Get Started

Sign in with Azure

Attach to a resource

Resources

Documentation Troubleshooting Guide

Tasks

View Azure resources

Manage accounts and subscriptions

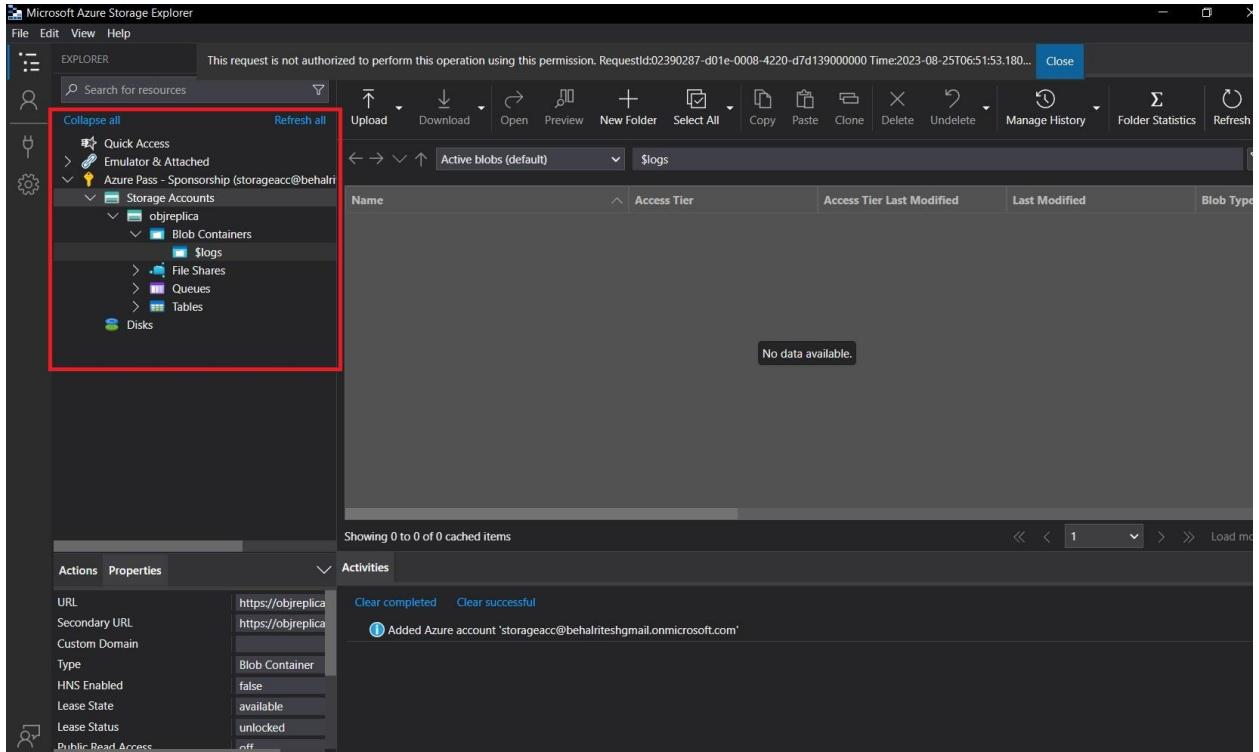
Connect to Azure resources

Activities

Clear completed Clear successful

Added Azure account 'storageacc@behalrites@gmail.onmicrosoft.com'

- As we assigned the “Reader” role to our storage account.the only storage account services and subscription will be visible to us.



Step 7: To view our data stored in containers we have to assign the “Storage Blob Data Reader” role to our User.

- Go back to Storage Account Control, Select & assign the role as shown below.

Home > objreplica_1692945788810 | Overview > objreplica | Access Control (IAM) >

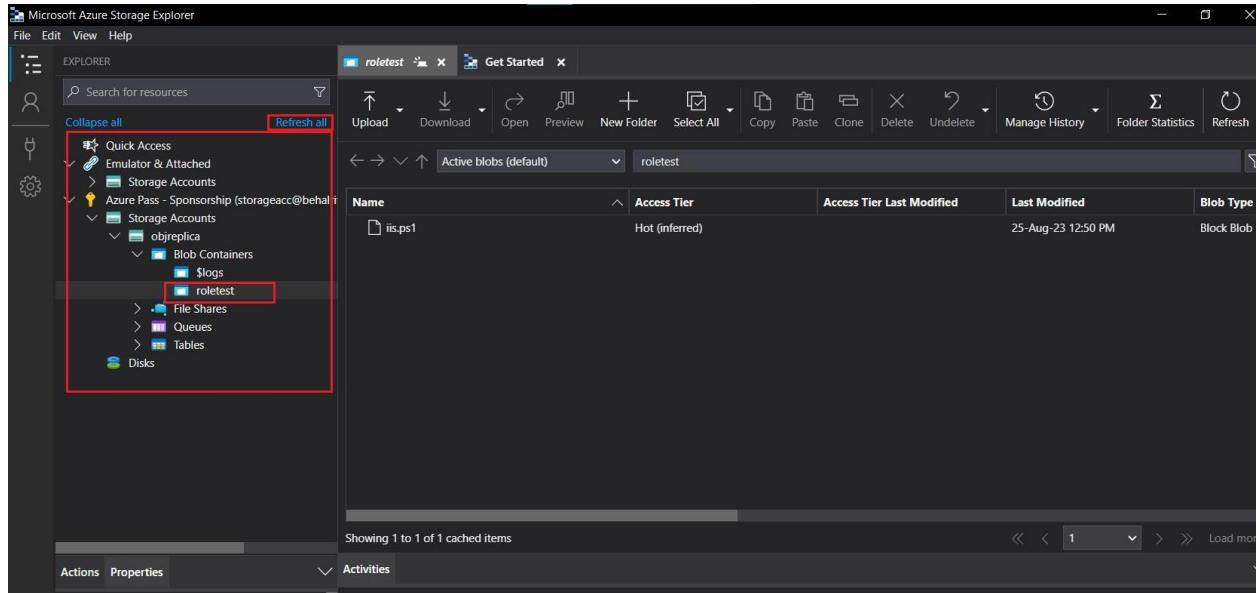
Add role assignment X

Role	Description	Type	Actions	View
Monitoring Contributor	Can read all monitoring data and update monitoring settings.	BuiltInRole	Monitor	View
Monitoring Reader	Can read all monitoring data.	BuiltInRole	Monitor	View
Reader and Data Access	Lets you view everything but will not let you delete or create a storage account or contained resour...	BuiltInRole	Storage	View
Resource Policy Contributor	Users with rights to create/modify resource policy, create support ticket and read resources/hierarc...	BuiltInRole	Management + Gover...	View
Storage Account Backup Contributor	Lets you perform backup and restore operations using Azure Backup on the storage account.	BuiltInRole	Storage	View
Storage Account Contributor	Lets you manage storage accounts, including accessing storage account keys which provide full acc...	BuiltInRole	Storage	View
Storage Account Key Operator Service ...	Storage Account Key Operators are allowed to list and regenerate keys on Storage Accounts	BuiltInRole	Storage	View
Storage Blob Data Contributor	Allows for read, write and delete access to Azure Storage blob containers and data	BuiltInRole	Storage	View
Storage Blob Data Owner	Allows for full access to Azure Storage blob containers and data, including assigning POSIX access ...	BuiltInRole	Storage	View
Storage Blob Data Reader	Allows for read access to Azure Storage blob containers and data	BuiltInRole	Storage	View
Storage Blob Delegator	Allows for generation of a user delegation key which can be used to sign SAS tokens	BuiltInRole	Storage	View
Storage File Data Privileged Contributor	Customer has read, write, delete and modify NTFS permission access on Azure Storage file shares.	BuiltInRole	None	View
Storage File Data Privileged Reader	Customer has read access on Azure Storage file shares.	BuiltInRole	None	View
Storage File Data SMB Share Contribut...	Allows for read, write, and delete access in Azure Storage file shares over SMB	BuiltInRole	Storage	View
Storage File Data SMB Share Elevated ...	Allows for read, write, delete and modify NTFS permission access in Azure Storage file shares over S...	BuiltInRole	Storage	View

Review + assign Previous Next Feedback

Step 8: On your storage explorer, Refresh the Page and dropdown the Storage account and Blob Container.

- The data stored on your Container is visible now.



- You can also add several permissions to your user as per need and security purpose.

Step 9: Remove the role assigned by you when not in use.

A screenshot of the Azure portal's Access Control (IAM) page for the 'roletest' container. The left sidebar shows 'Access Control (IAM)', 'Overview', 'Diagnose and solve problems', and 'Shared access tokens'. The main area shows 'Number of role assignments for this subscription' at 2. A table lists two users with 'Reader' roles: 'storageacc' (User, Reader, Parent resource (Inherited), None) and 'Storage Blob Data Reader' (User, Storage Blob Data Reader, Parent resource (Inherited), None). Both rows are highlighted with a red border. The top navigation bar includes 'Search', 'Add', 'Download role assignments', 'Edit columns', 'Refresh', 'Remove' (button), and 'Feedback'.