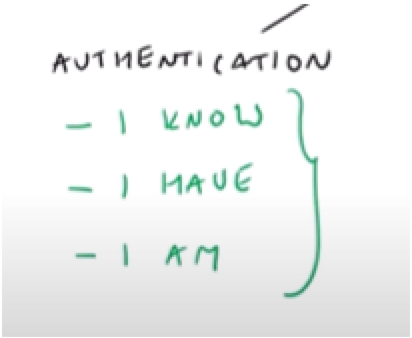
DP-203: 17 - Azure Data Lake Security

Authentication and authorization

1. Here accessing can be given in 2 ways…first is authentication it says “ it is really me who is trying to access this resource”...we can prove authentication in 3 ways
2. Using

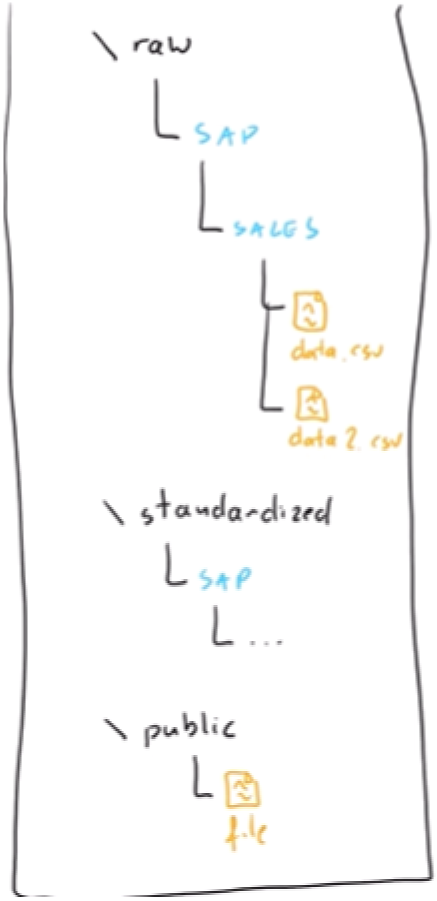
here if we have any password to access..then it comes under I know a password to authenticate
3. 2nd is I have..” If we have a device..then we can take help of this device to authenticate(like get otp and authenticate)”
4. 3rd is I AM ..”like finger print or face id” ..it says that it is really me who is authenticating



5. Here the good practice is to use ..any of two ways to authenticate(Multi factor authentication)
6. Authorization
7. It is nothing but what kind of permissions does the user/service who authenticated has

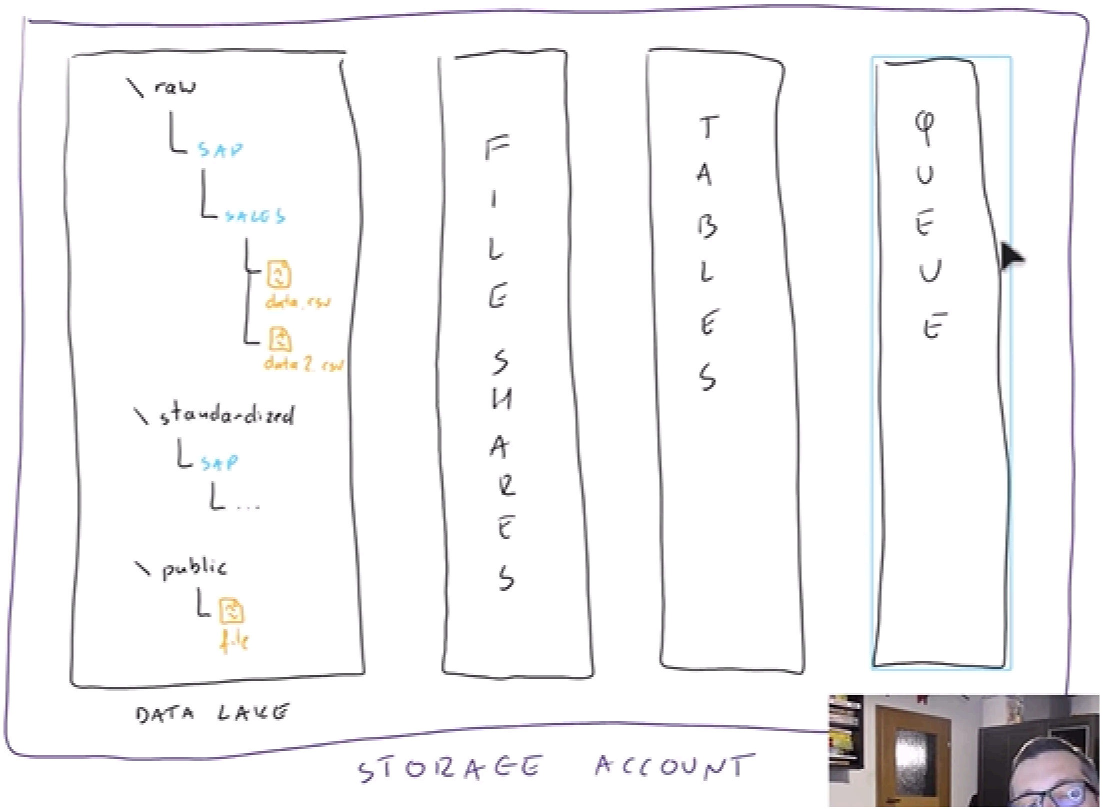
Sample Storage Structure

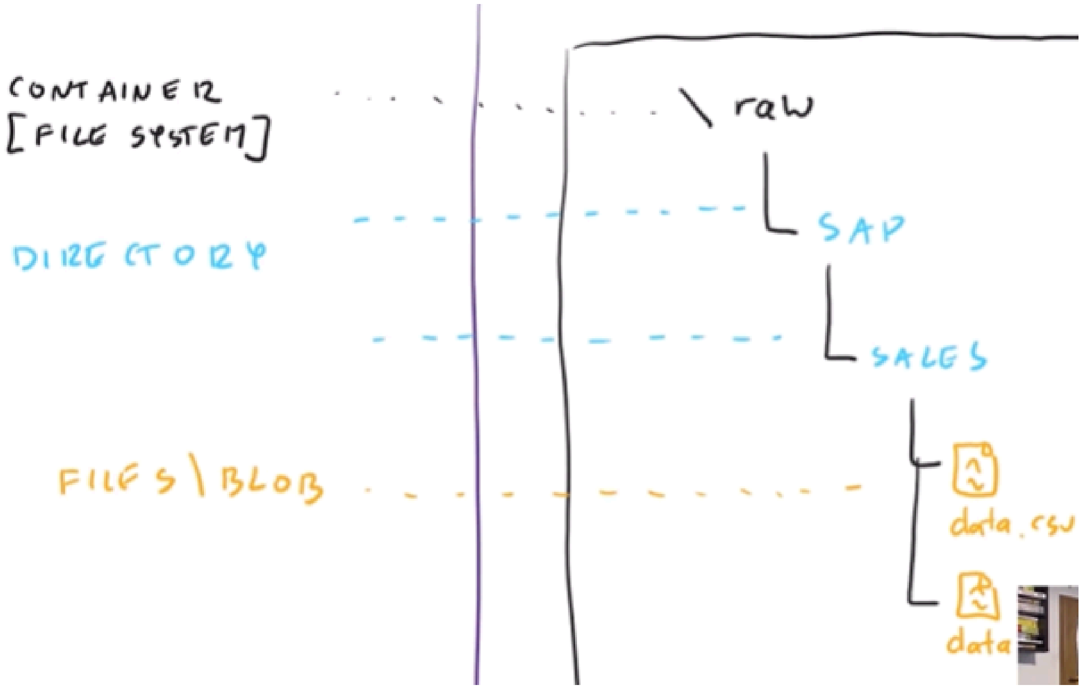
1. Lets suppose we have this folder hierarchy inside the datalake



here this is the datalake with the raw,standardized and public containers

2. Here all of this is Storage account

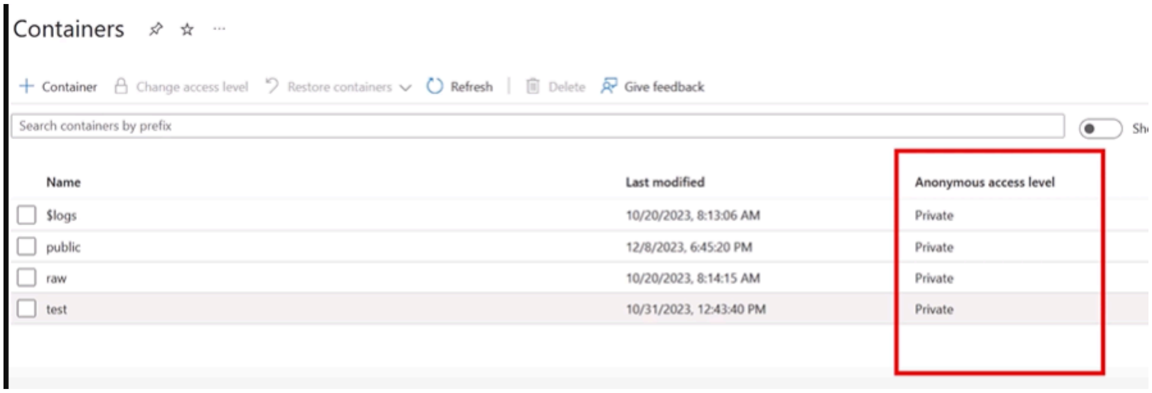




3. Next we will create this structure in the ADLSg2

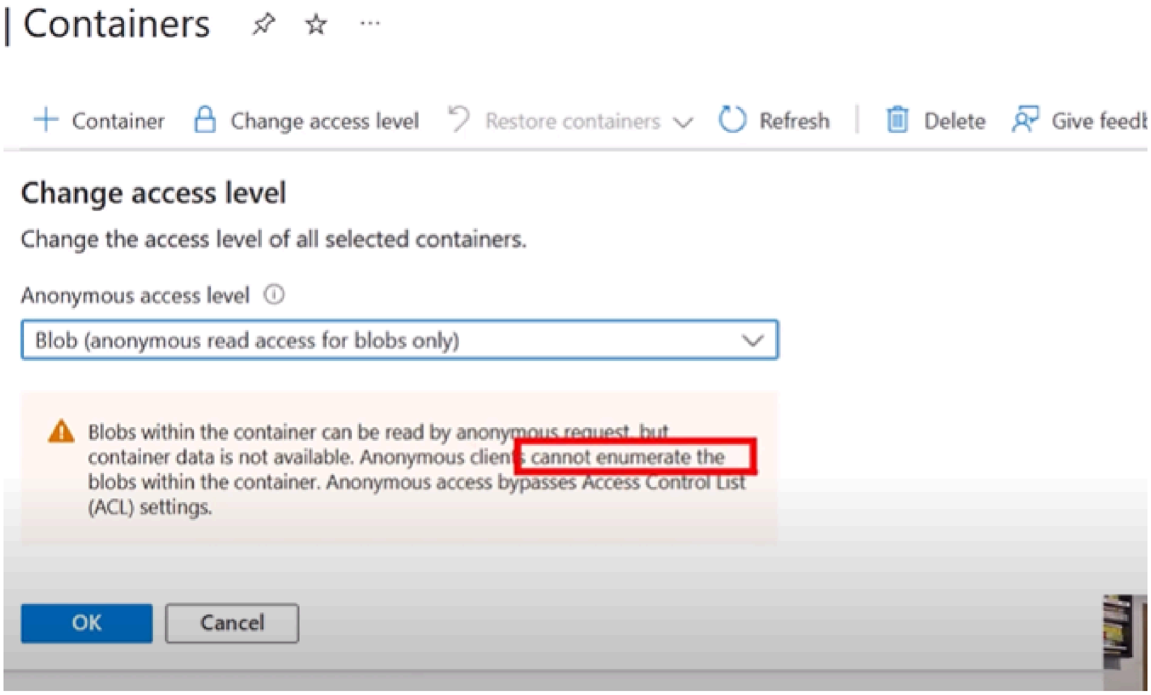
No Identity - Anonymous Access

1. We can access the datalake in two ways..Without identity and With Identity
2. Lets focus on No Identity
3. Inside No ..first we have is anonymous access
4. Here default …every container will be in private



Name	Last modified	Anonymous access level
□ $logs	10/20/2023, 8:13:06 AM	Private
□ public	12/8/2023, 6:45:20 PM	Private
□ raw	10/20/2023, 8:14:15 AM	Private
□ test	10/31/2023, 12:43:40 PM	Private

5. We can go to change access level to provide anonymous access
6. We'll change the access of public container to

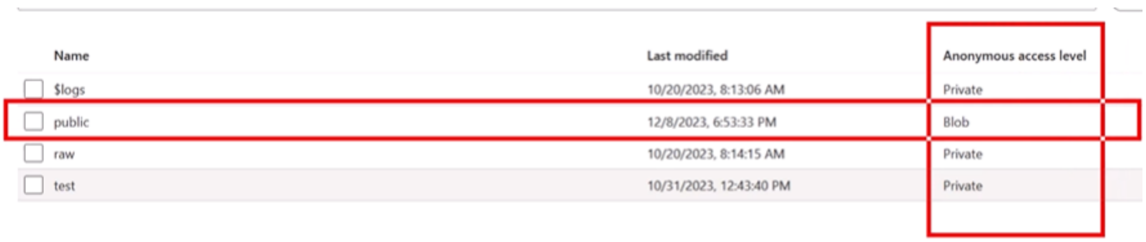


Change access level

Change the access level of all selected containers.

Anonymous access level: Blob (anonymous read access for blobs only)

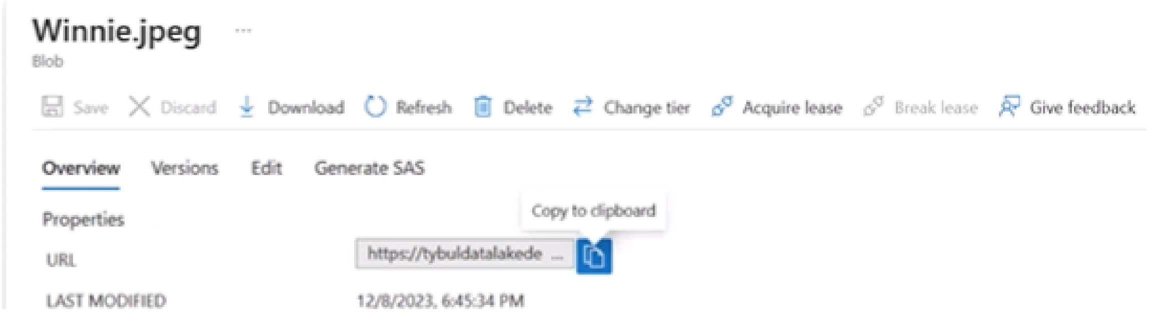
Blobs within the container can be read by anonymous request, but container data is not available. Anonymous clients cannot enumerate the blobs within the container. Anonymous access bypasses Access Control List (ACL) settings.



Name	Last modified	Anonymous access level
□ $logs	10/20/2023, 8:13:06 AM	Private
□ public	12/8/2023, 6:53:33 PM	Blob
□ raw	10/20/2023, 8:14:15 AM	Private
□ test	10/31/2023, 12:43:40 PM	Private

7.

8. This is the URL to access the blob in public container

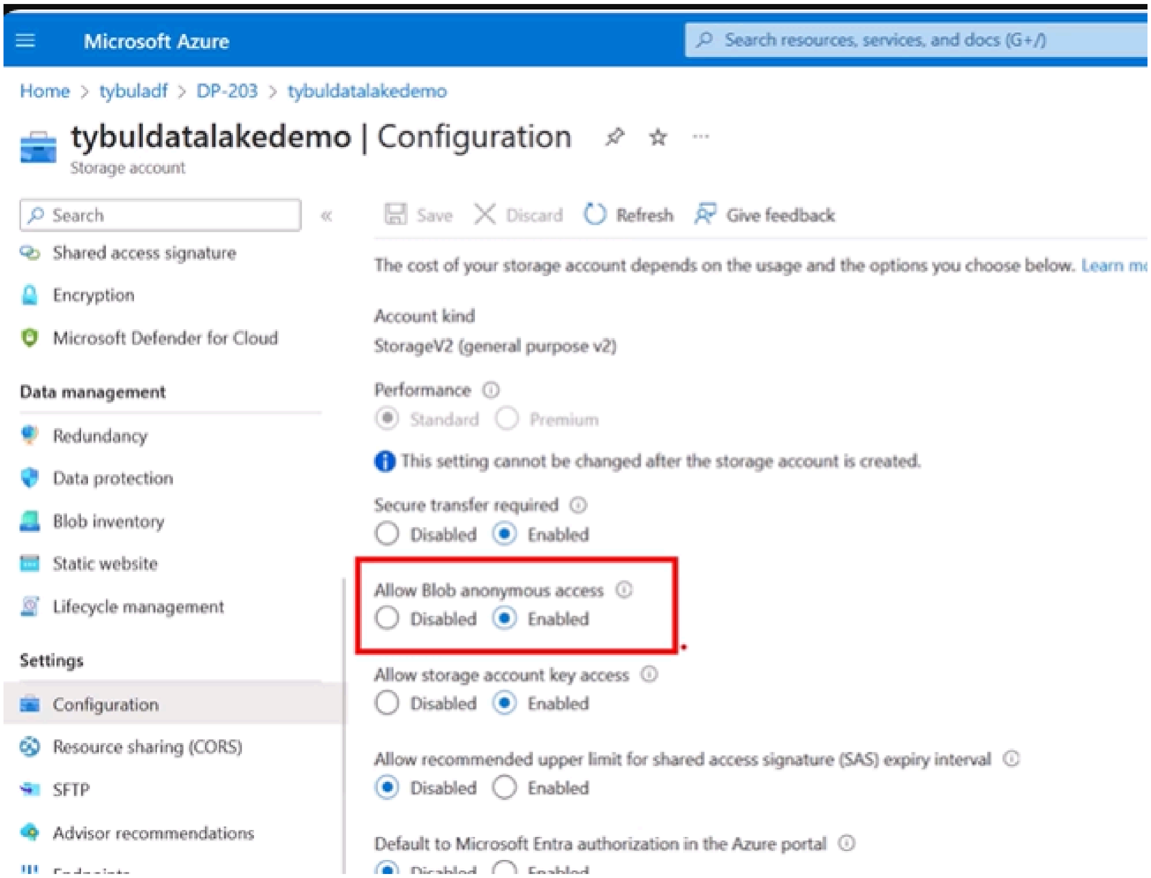


Properties

URL https://tybuldatalakede ...

LAST MODIFIED 12/8/2023, 6:45:34 PM

9. If we paste this url in browser we can see blob
10. We can also disable change access policies



The cost of your storage account depends on the usage and the options you choose below. Learn m

Account kind
StorageV2 (general purpose v2)

Performance
● Standard ○ Premium

This setting cannot be changed after the storage account is created.

Secure transfer required
○ Disabled ● Enabled

Allow Blob anonymous access
○ Disabled ● Enabled

Allow storage account key access
○ Disabled ● Enabled

Allow recommended upper limit for shared access signature (SAS) expiry interval
● Disabled ○ Enabled

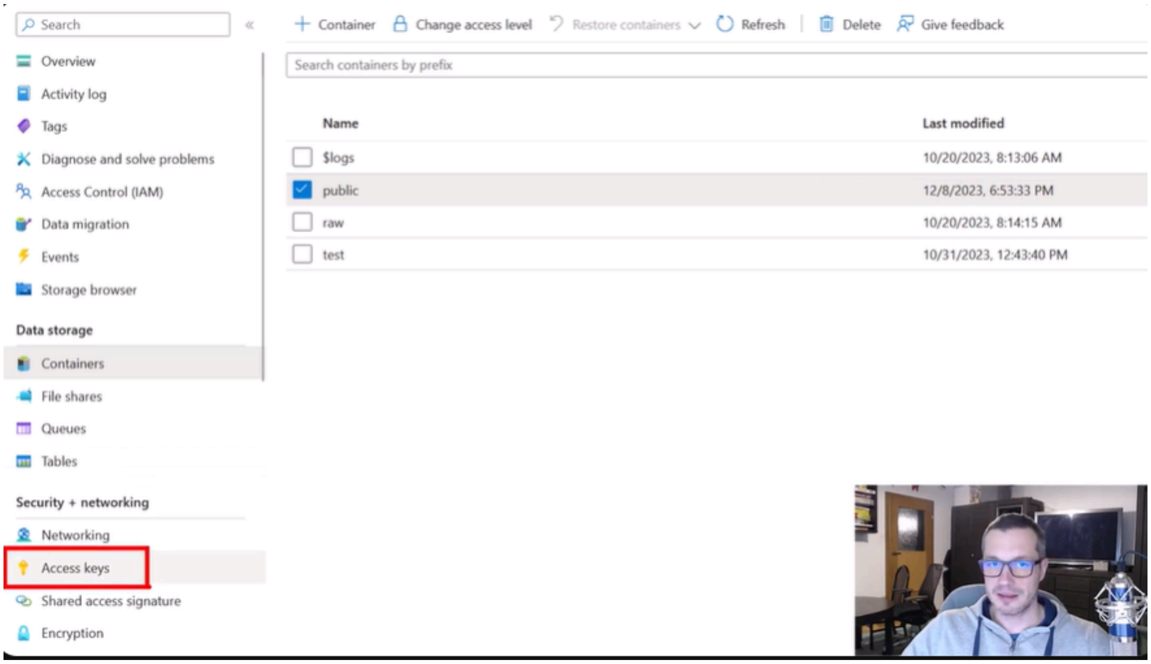
Default to Microsoft Entra authorization in the Azure portal
● Disabled ○ Enabled

so that no can change the access level

11. Here as we want to protect the data…we wont be using anonymous mode much

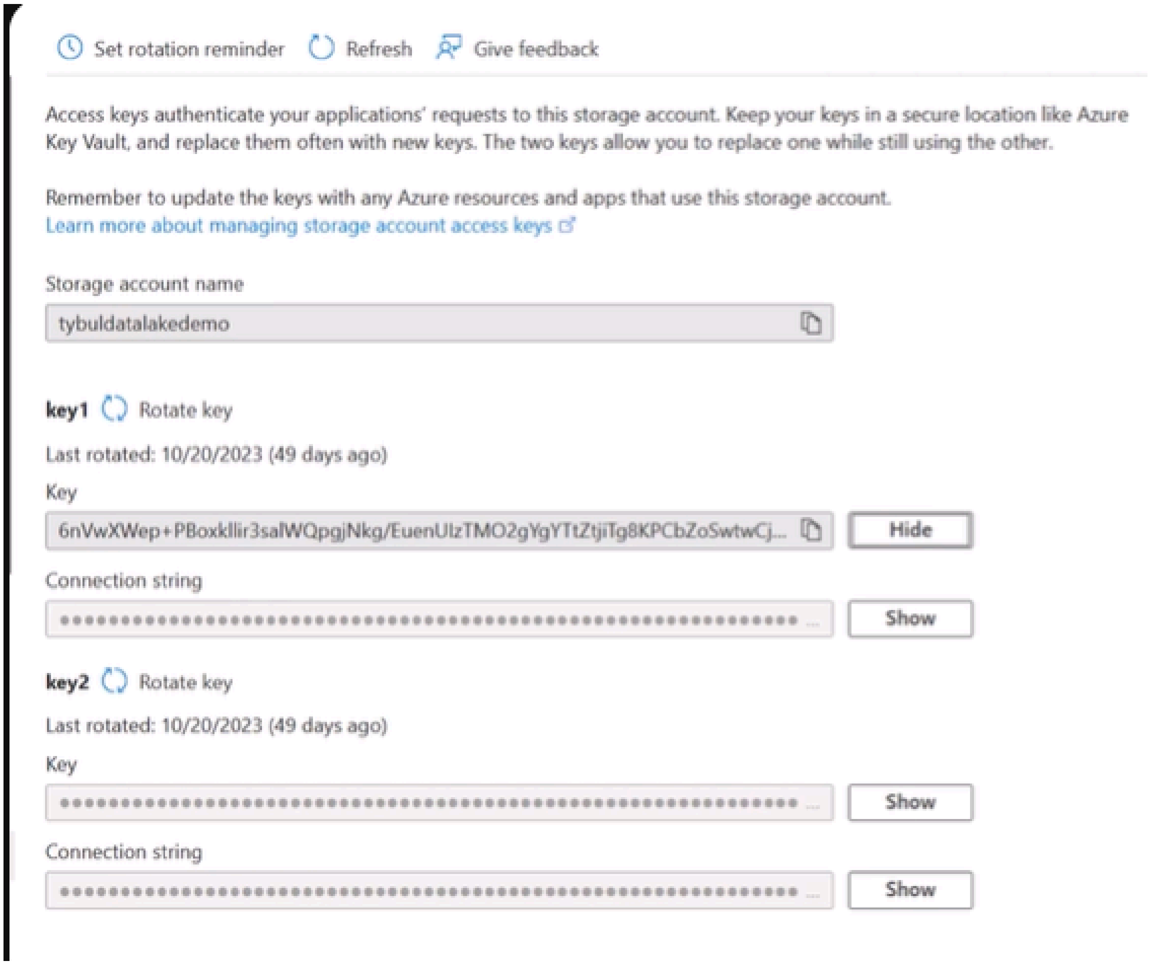
No Identity - Access key

1. Here we have access key option in storage account



	Name	Last modified
□	$logs	10/20/2023, 8:13:06 AM
☑	public	12/8/2023, 6:53:33 PM
□	raw	10/20/2023, 8:14:15 AM
□	test	10/31/2023, 12:43:40 PM

2. And here we have 2 access keys



Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.

Remember to update the keys with any Azure resources and apps that use this storage account.
Learn more about managing storage account access keys

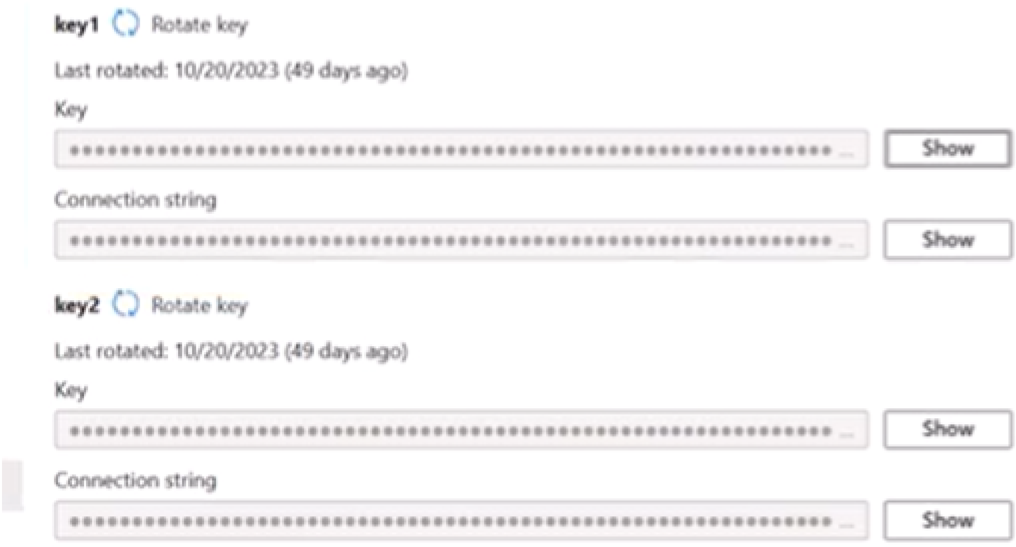
Storage account name
tybuldatalakedemo

key1 Rotate key
Last rotated: 10/20/2023 (49 days ago)
Key
6nVwXWep+PBoxkllir3salWQpgjNkg/EuenUlzTMO2gYgYTtZtjiTg8KPCbZoSwtwCj... Hide
Connection string
•• ... Show

key2 Rotate key
Last rotated: 10/20/2023 (49 days ago)
Key
•• ... Show
Connection string
•• ... Show

3. This access can give complete access to the storage account

4. And it is set at the storage account level…previously in anonymous mode..we can set it up at container level
5. It is very important to secure this access keys
6. But why here we have two keys?



key1 Rotate key

Last rotated: 10/20/2023 (49 days ago)

Key

Show

Connection string

Show

key2 Rotate key

Last rotated: 10/20/2023 (49 days ago)

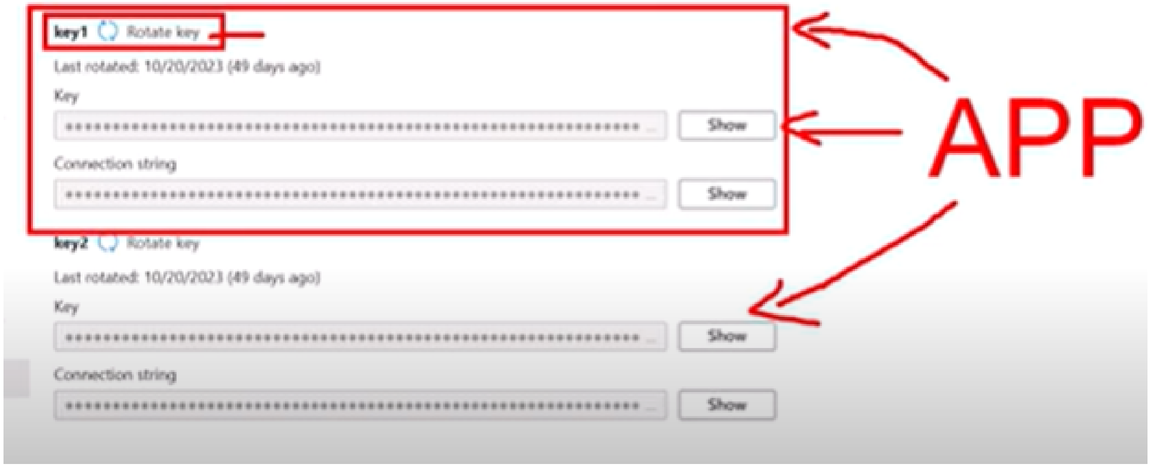
Key

Show

Connection string

Show

7. Let us suppose we have an app which needs access to our datalake and access is given thru access keys
8. If we think that this access keys has been leaked or compromised …with out any downtime in the app…we can redirect our app to use keys2 to access our ADLSg2



key1 Rotate key

Last rotated: 10/20/2023 (49 days ago)

Key

Show

Connection string

Show

key2 Rotate key

Last rotated: 10/20/2023 (49 days ago)

Key

Show

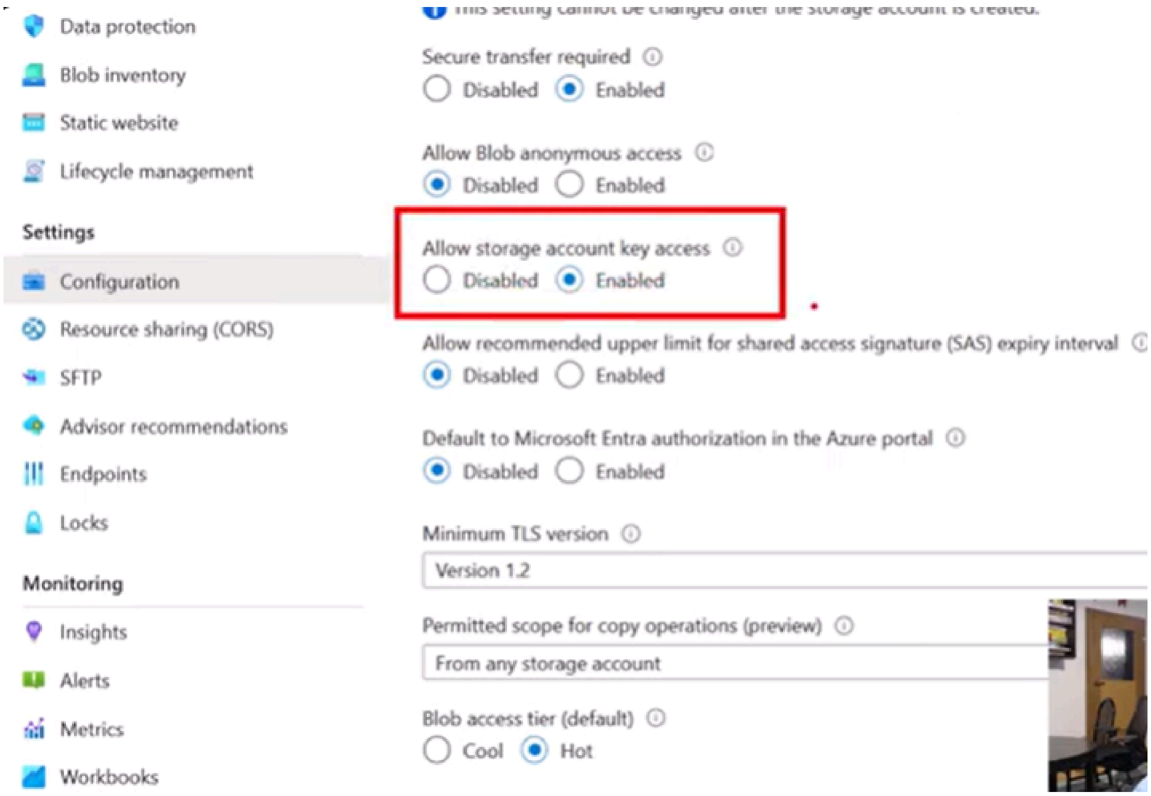
Connection string

Show

After rotating keys1…we can reassign our app to use keys1 if needed

9. In ADF lecture…we have connected our ADF to ADLSg2 using account key(access key) …but it is not recommended
10. Because when we take a look at JSON code of linked service we can see our Access key in JSON code

11. To prevent that…we can disable key access



This setting cannot be changed after the storage account is created.

Secure transfer required

○ Disabled ● Enabled

Allow Blob anonymous access

● Disabled ○ Enabled

Allow storage account key access

○ Disabled ● Enabled

Allow recommended upper limit for shared access signature (SAS) expiry interval

● Disabled ○ Enabled

Default to Microsoft Entra authorization in the Azure portal

● Disabled ○ Enabled

Minimum TLS version

Version 1.2

Permitted scope for copy operations (preview)

From any storage account

Blob access tier (default)

○ Cool ● Hot