**ANONYMOUS ACCESS LEVEL and ACCESS KEYS**

**ANONYMOUS ACCESS LEVEL**

**What is Anonymous Access Level in Azure?**

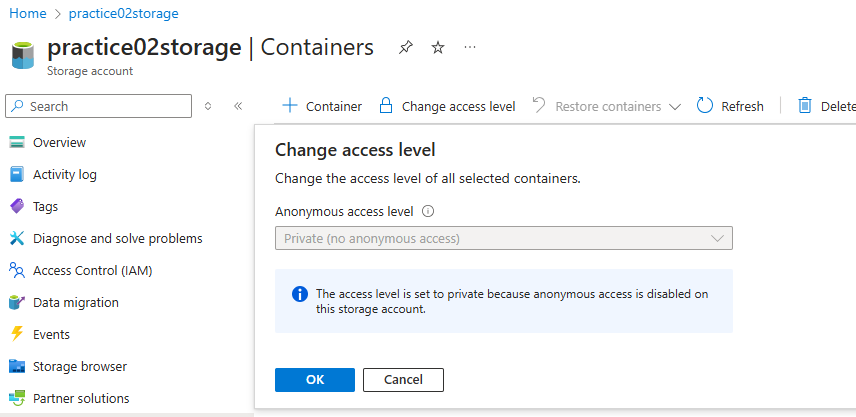
Anonymous access in Azure refers to granting **public access** to resources **without requiring authentication**. This is commonly used in **Azure Storage** (like Blob Storage) when you want to allow users to access files without signing in.

**Types of Anonymous Access in Azure Storage (Blob Storage)**

When you enable anonymous access for an **Azure Blob container**, there are three access levels:

| **Access Level** | **Description** | **Who Can Access?** |
| --- | --- | --- |
| **Private (No Anonymous Access)** | Default setting. The container and its blobs are **not accessible** without authentication. | Only authorized users with **Azure AD roles or shared keys**. |
| **Blob (Public Read Access for Blobs Only)** | Allows anonymous users to **read blobs** inside the container, but the container itself is hidden. | Anyone can access **individual files (blobs)**, but **cannot list all files**. |
| **Container (Public Read Access for Container & Blobs)** | Allows anonymous users to **read blobs and list all blobs** inside the container. | Anyone can view all blobs in the container and see their names. |

So when I first tried to set anonymous level access it is not allowing me to enable the anonymous access level like I need as shown :



So here we should do the following to enable the public anaonymous access:

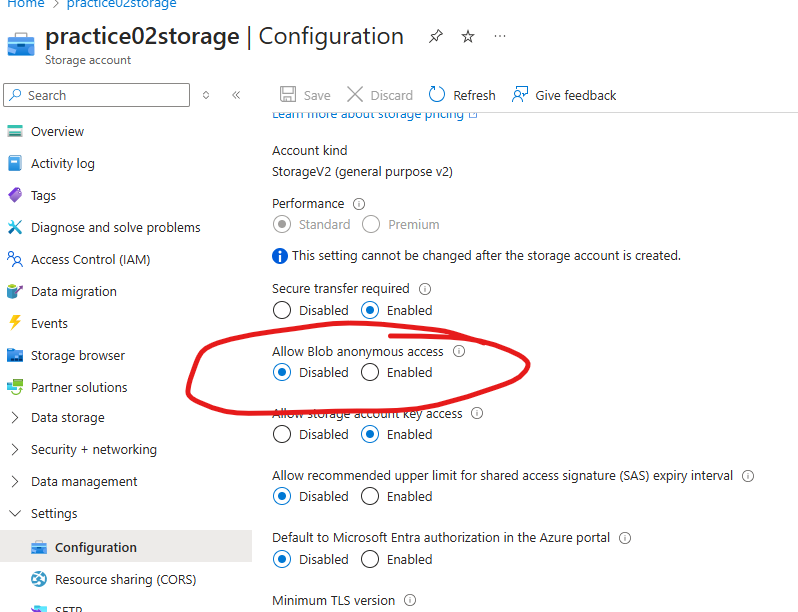
**tep 1: Enable Public Access at Storage Account Level**

1. **Go to Azure Portal** → Open your **Storage Account**.
2. In the left menu, select settings🡪**Configuration**.
3. Look for the setting **"Allow Blob Public Access"**.
4. If it is **disabled**, click **Enabled**.
5. Click **Save** at the top.

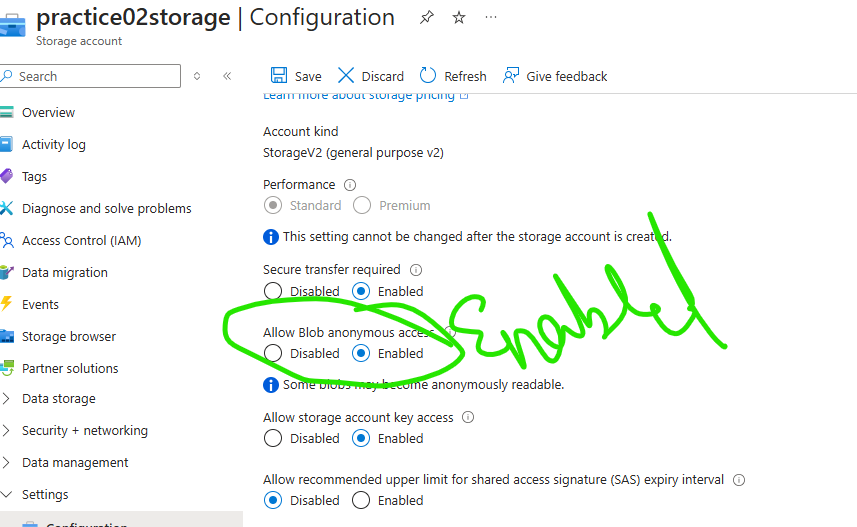
**Step 2: Change Access Level for the Container**

1. Navigate to **Containers** → Select your container.
2. Click on **Change access level**.
3. Now, you should be able to select:
   * **Blob (Public Read Access for Blobs Only)**
   * **Container (Public Read Access for Container & Blobs)**
4. Click **OK** to save changes.

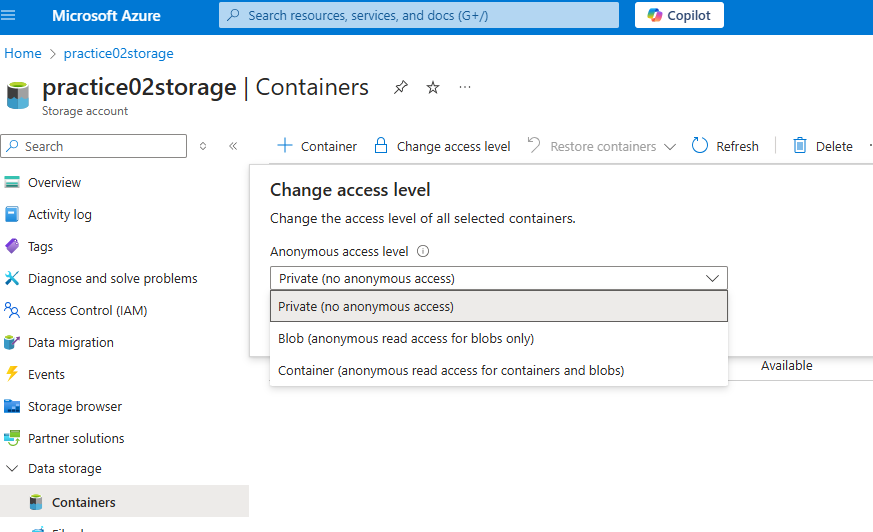
After following above steps I am now able to change the access levels:



Enabled it:



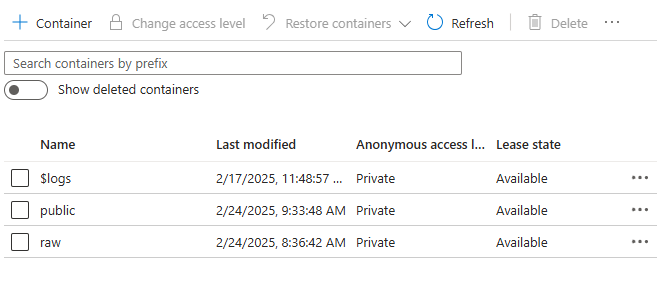
Now the access level is enabled and I saved it and now I am able to set the anonymous public access:



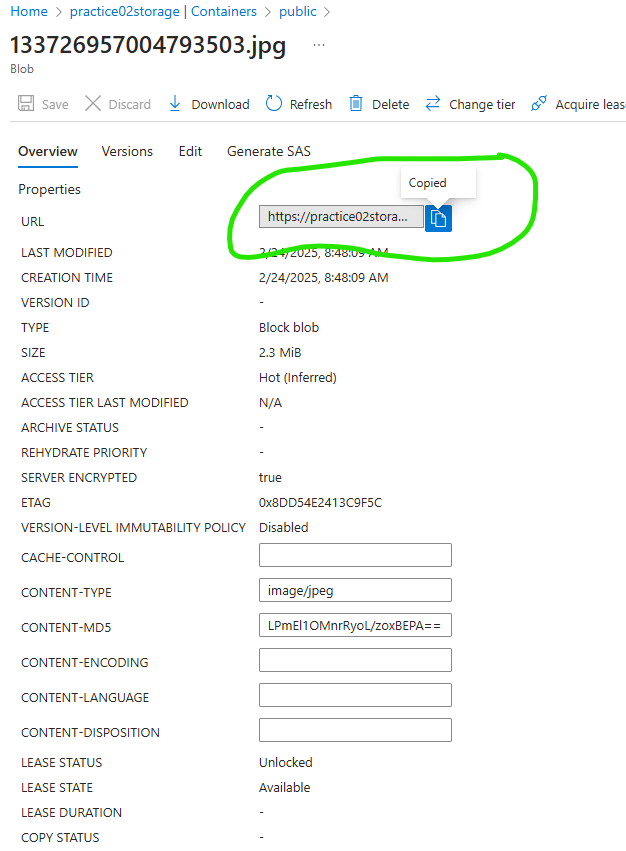
Now I will try to access files and containers, directories by enabling various levels and will see how the changes work :

So currently I have three containers :

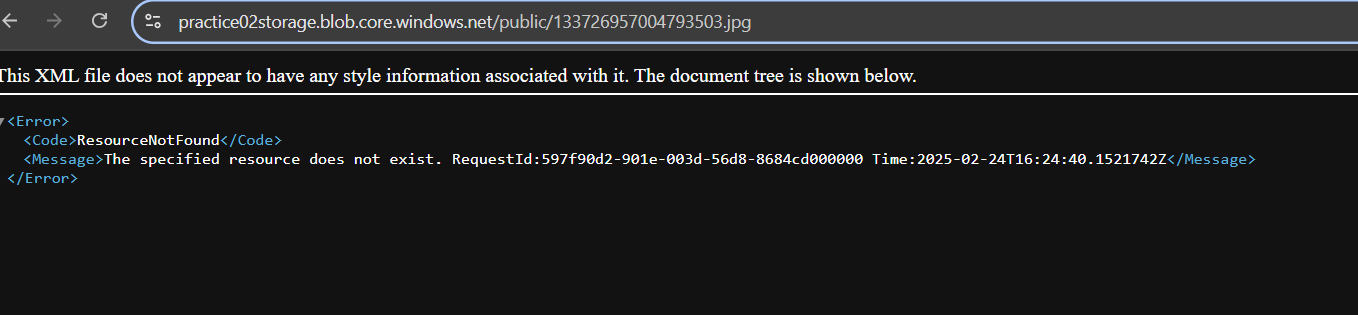
Logs, public,raw



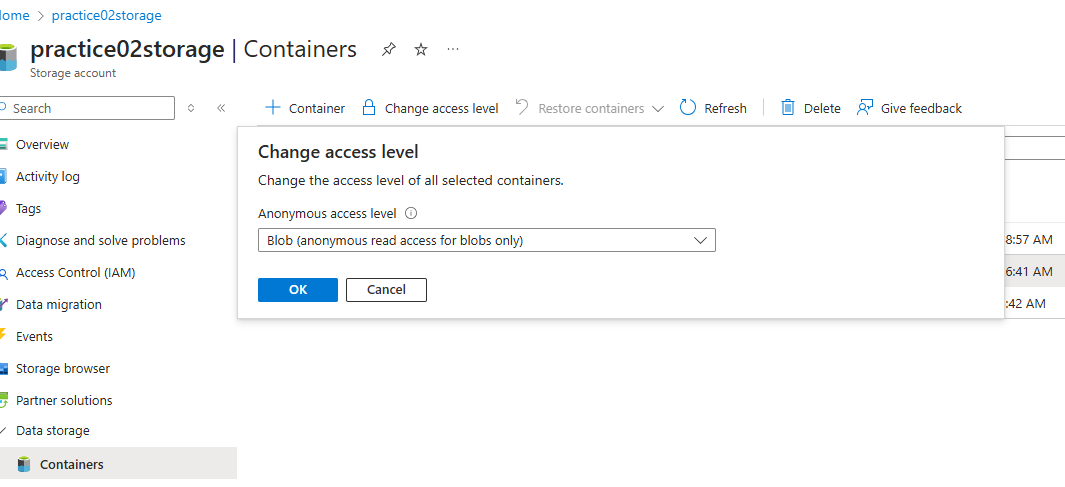
I already uploaded a file and will see if I can access the file in the public container if I can access it:



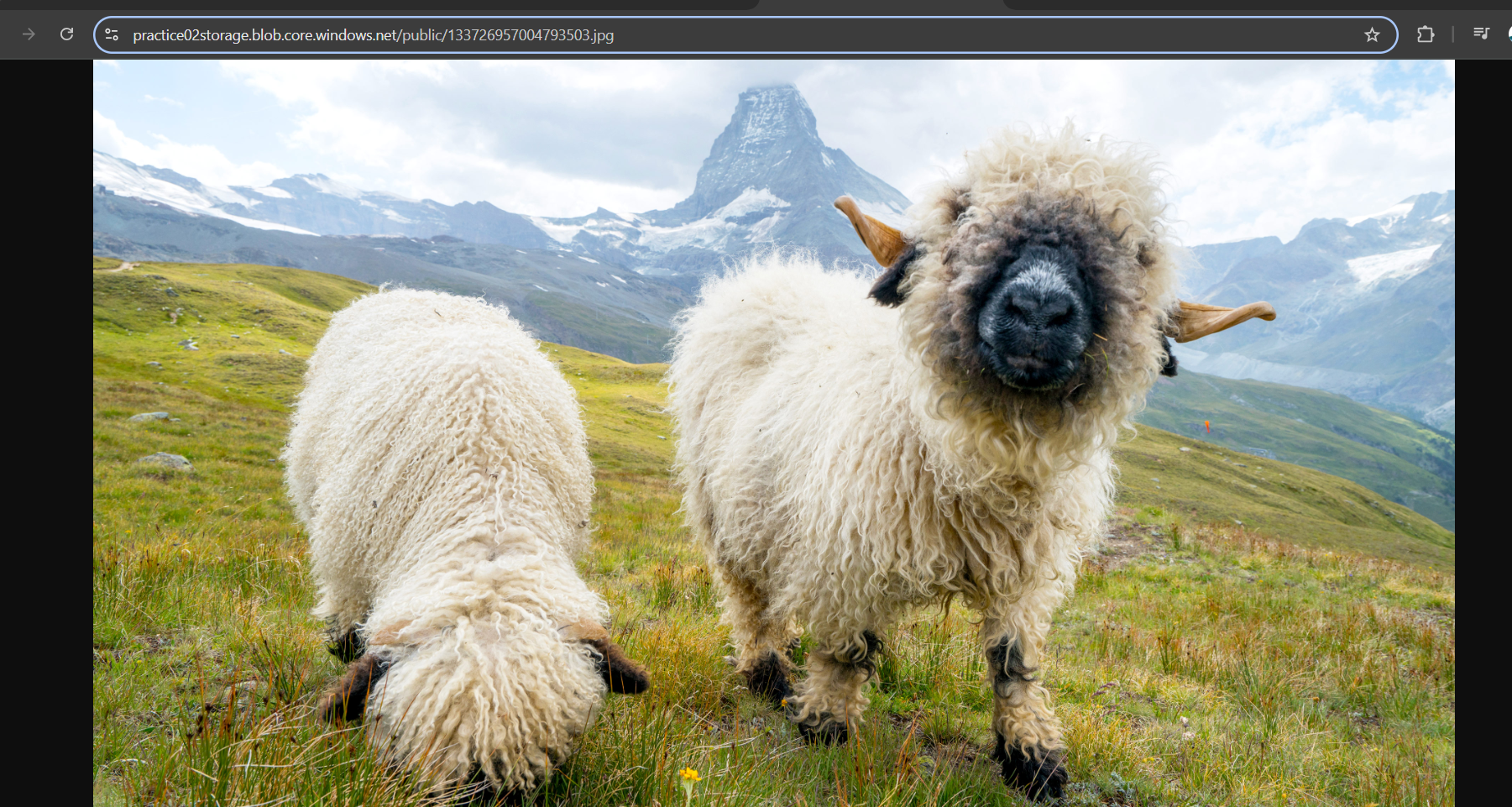
I copied the above URL and I am using another browser (accessing it anontmously) to see if I can access the file :



It gave me the following error saying that it is unable to access that Now I want to change the anonymous access level to BLOB and see if I can access that :



So I will reload my other browser where I pasted the link and will see If I can access it:

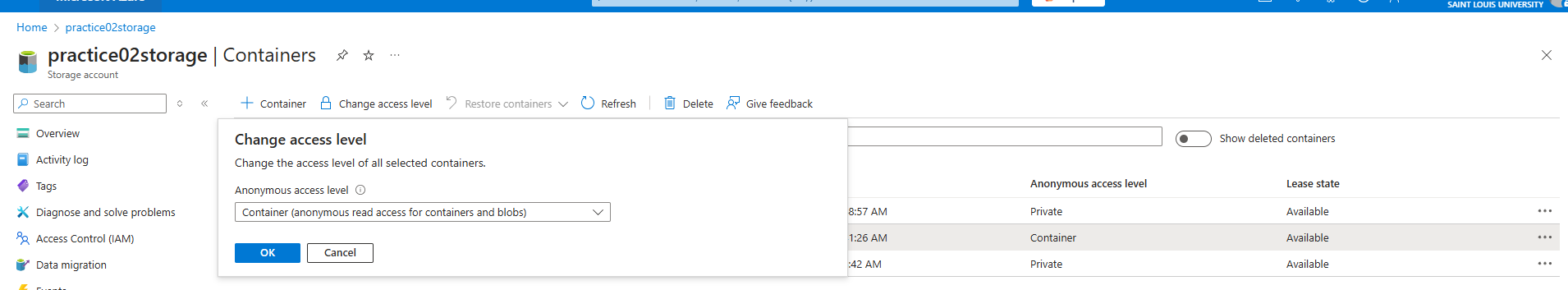


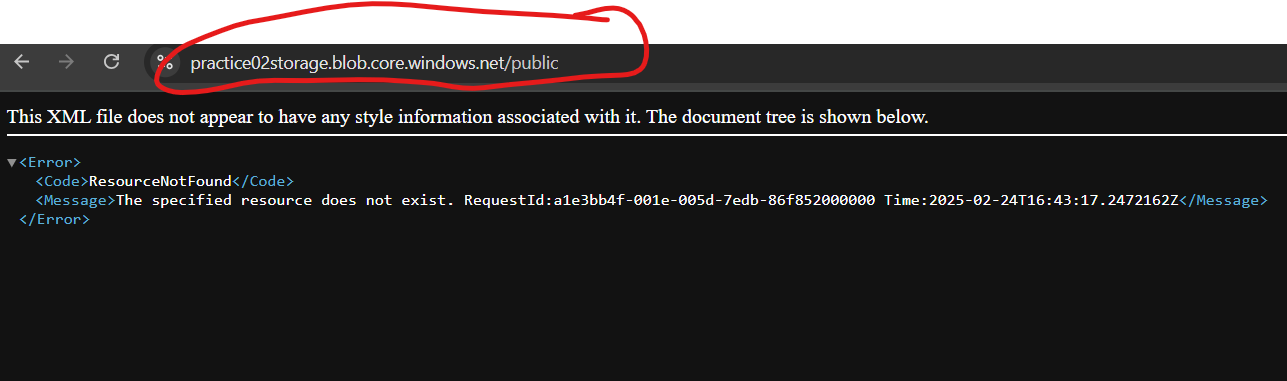
Now I am able to access the link

So here after we assign the blob anonymous access , we can see that we can only access the file we specified but anonymous people can access all the files in the container ,

Also it is READ ONLY ACCESS**( BECAUSE THE PEOPLE WHO DON’T HAVE KEY OR SOMETHING CAN ONLY READ IT BUT CANNOT MODIFY IT)**

Now I changed the access level to : Container access level and I tried accessing the container it self with the following link: **https://practice02storage.blob.core.windows.net/public**



I am unable to see anything as follows: 

So I asked chatgpt:

You're right that setting the **container access level to "Container"** should allow public access to both the **blobs (files) and the listing of files** inside the container. However, the issue here is that you're trying to access the **container URL directly** instead of an actual **blob (file)** inside it.

**Why Are You Getting "ResourceNotFound" Error?**

* The **URL https://practice02storage.blob.core.windows.net/public only points to the container itself**, but **browsers cannot list blobs automatically**.
* The **correct way to access public files is by specifying the full blob (file) URL**.

**✅ How to Fix This and Access the Files**

1. **Manually get a blob (file) URL**:
   * Go to **Azure Portal** → Open your **Storage Account**.
   * Click **Containers** → Open the **"public"** container.
   * Click on any file (blob) inside the container.
   * Copy its **Blob URL** (e.g., https://practice02storage.blob.core.windows.net/public/sample.txt).
   * Paste it in the browser → You should be able to access it.
2. **Use Azure Storage REST API to List Files**:
   * Since you set access to **"Container"**, you can get a list of blobs using this API in a browser:

bash

CopyEdit

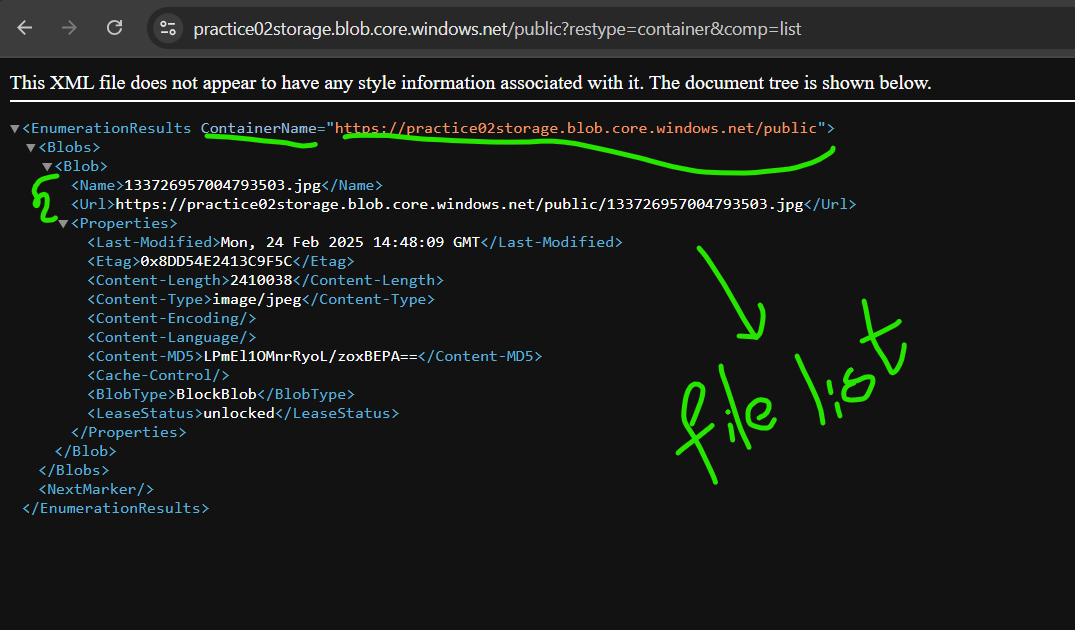
https://practice02storage.blob.core.windows.net/public?restype=container&comp=list

* + This will return an XML response listing all files in the container.

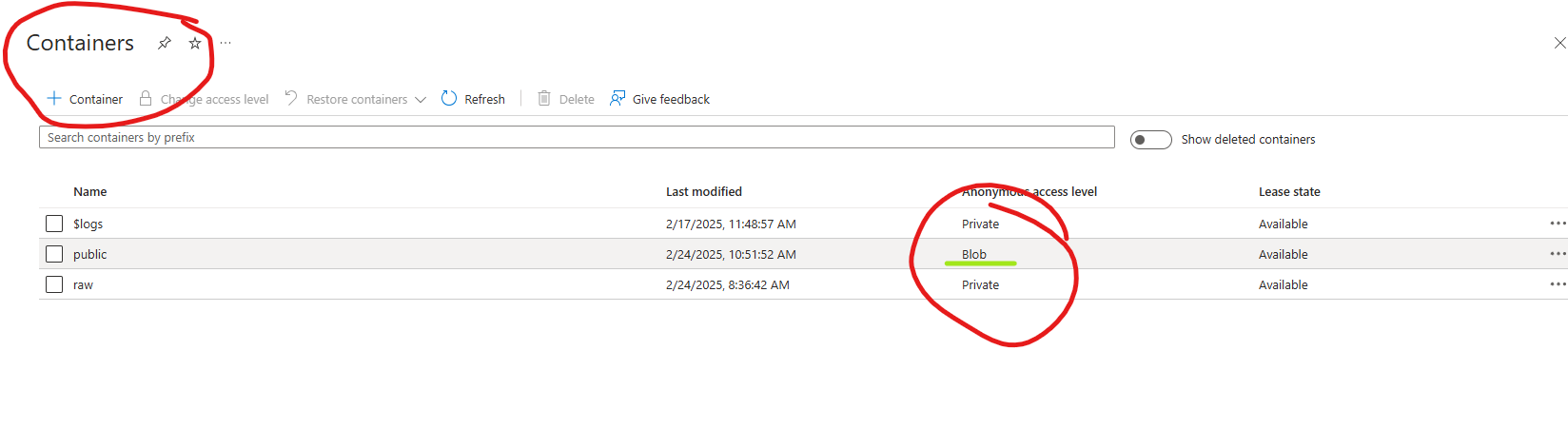
**🔎 Understanding the Access Levels Again**

| **Access Level** | **Can Access Files Directly?** | **Can List Files in Browser?** | **Container URL Works?** |
| --- | --- | --- | --- |
| **Private** (Default) | ❌ No | ❌ No | ❌ No |
| **Blob** | ✅ Yes (with direct file URL) | ❌ No | ❌ No |
| **Container** | ✅ Yes | ✅ Yes (via API) | ❌ No (browser cannot list files) |

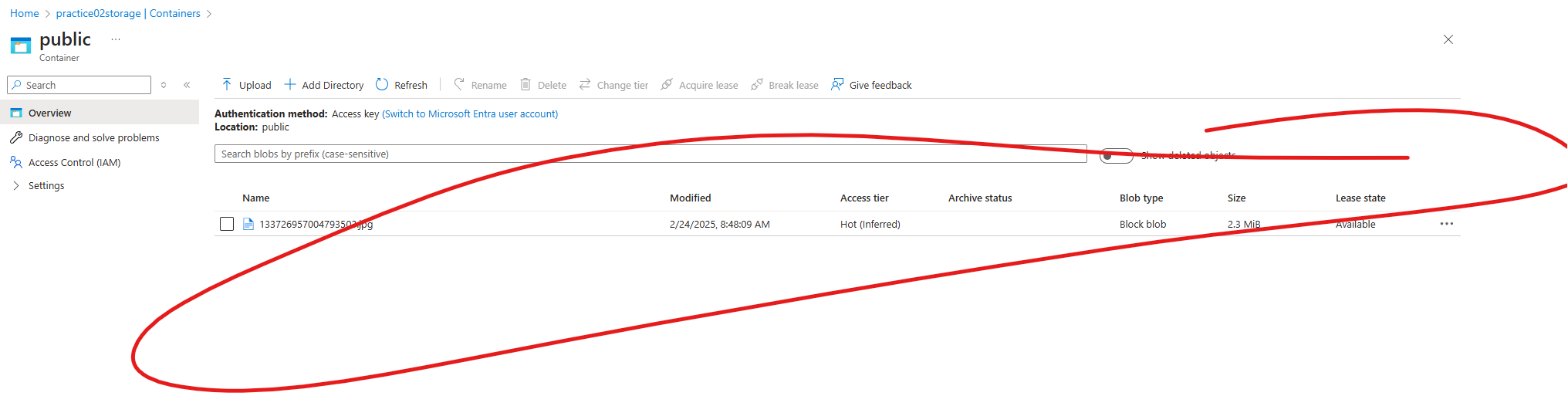
So I tried pasting the URL in my private browser and it gave me the following:



Here we can only set the access level settings at container level and not at file level as we can see the following example:



But here inside the public container I am unable to set the access at directory and file level:



I am unable to see any access level setting here

So we can only set the access at container level and not at directory and file levels.

**ACCESS KEYS**

🔑 Access Keys in Azure Storage

Azure Access Keys are authentication credentials that allow you to access your Azure Storage Account programmatically without using Azure AD authentication.

**🔑 What Can Someone Do If They Have the Access Key?**

If someone gets an **access key** for your storage account, they can **completely control everything** inside your storage account.

**🚨 They Can:**

✅ **Access Any Data** → They can read, download, and list files (even from private containers).  
✅ **Upload or Modify Data** → They can overwrite existing files and add new ones.  
✅ **Delete Data** → They can permanently delete files, blobs, tables, and queues.  
✅ **Create, Delete, or Modify Containers** → They can change container properties, delete them, or create new ones.  
✅ **Access All Storage Services** → They can control **Blob Storage, Table Storage, Queue Storage, and File Shares**.  
✅ **Generate SAS Tokens** → They can create **temporary access tokens** and share them with others, making tracking harder.

So I wanna demonstrate that as follows:

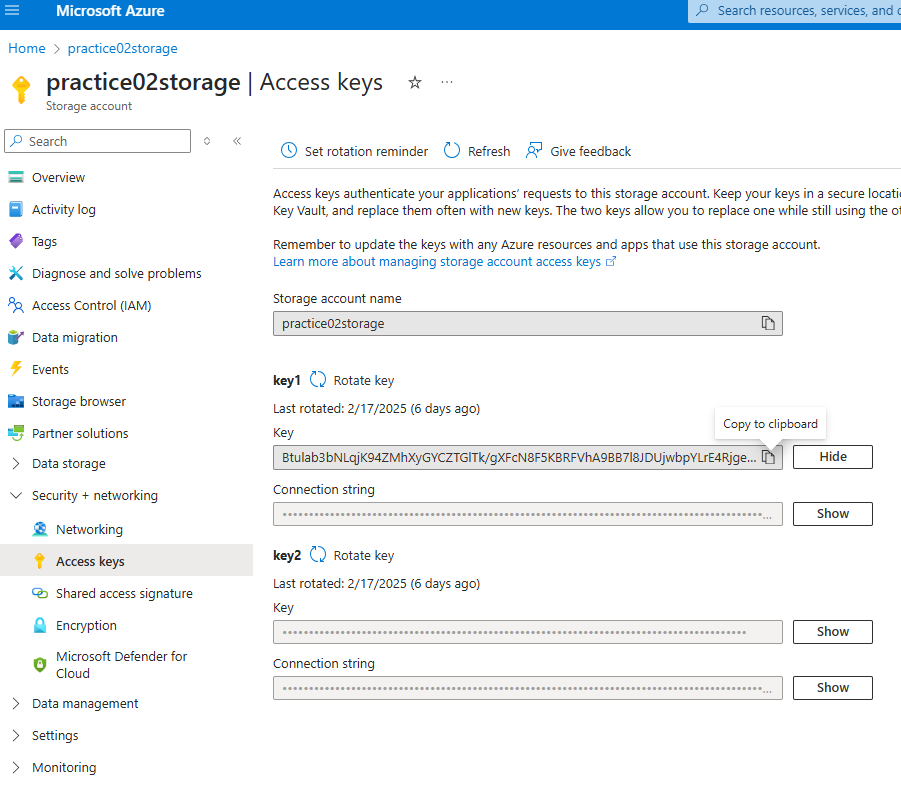
SO I am copying an access key to see If I can access the files inside the PRIVATE CONTAINER , let us use the above container : Public( the name of container is public and It is set to level--- private anaonymous level actually).

So here I will copy the key first:

 **Go to Azure Portal** → Open your **Storage Account**.

 In the left menu, go to **Security + Networking** → Click **Access keys**.

 Click **Show keys** → Copy **Key1** or **Key2**.



I copied the key:

And now I am trying to list the files of container using the follwong :

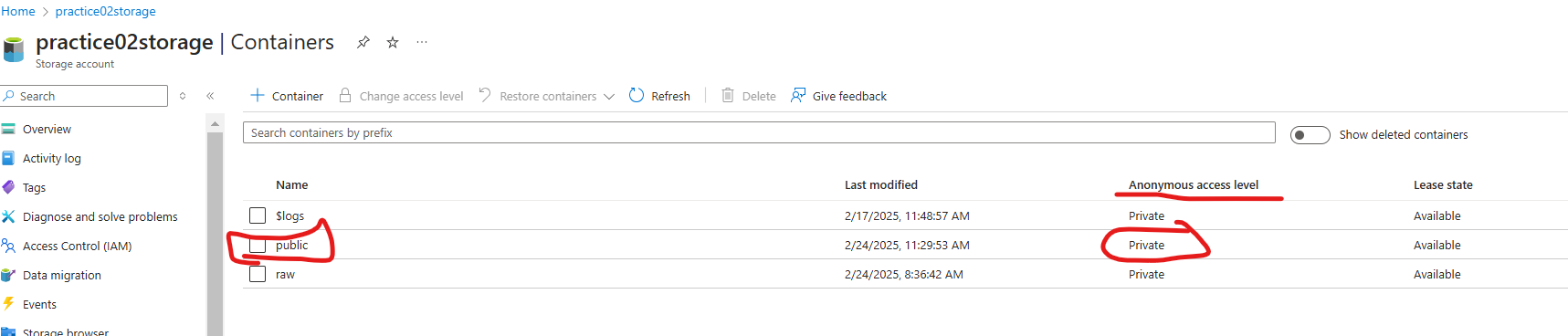
**Step 2: List Files from a Private Container**

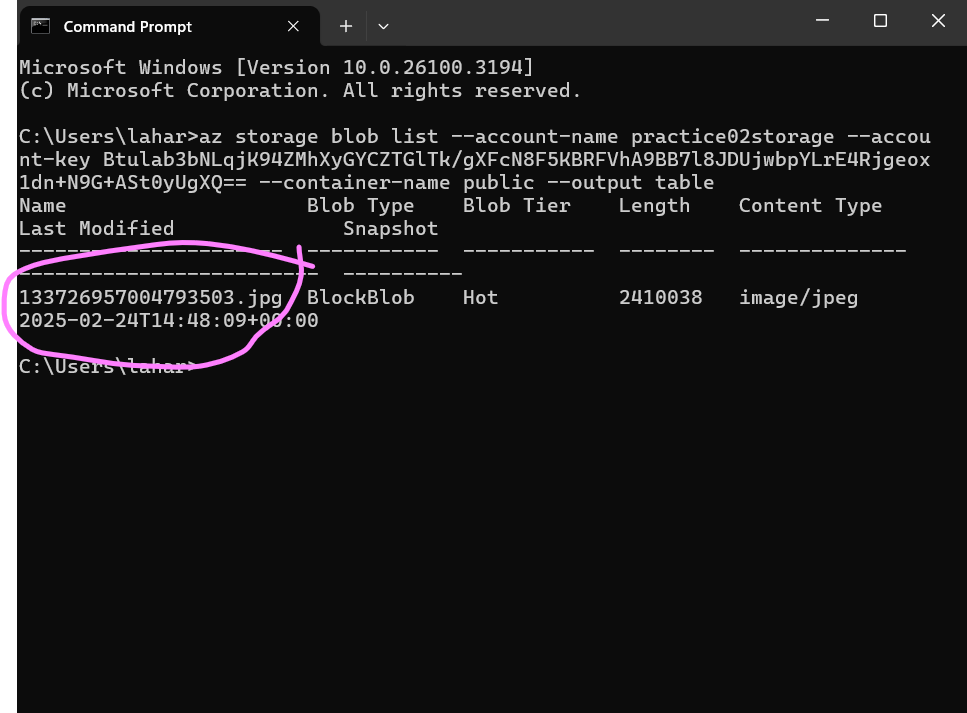
Now, open **Command Prompt (CMD) or PowerShell** and run the following Azure CLI command:

az storage blob list --account-name yourstorageaccount --account-key your\_access\_key --container-name your\_private\_container --output table

**🔹 Replace:**

* yourstorageaccount → Your actual **Storage Account name**
* your\_access\_key → The **access key** you copied
* your\_private\_container → Name of the **private container**



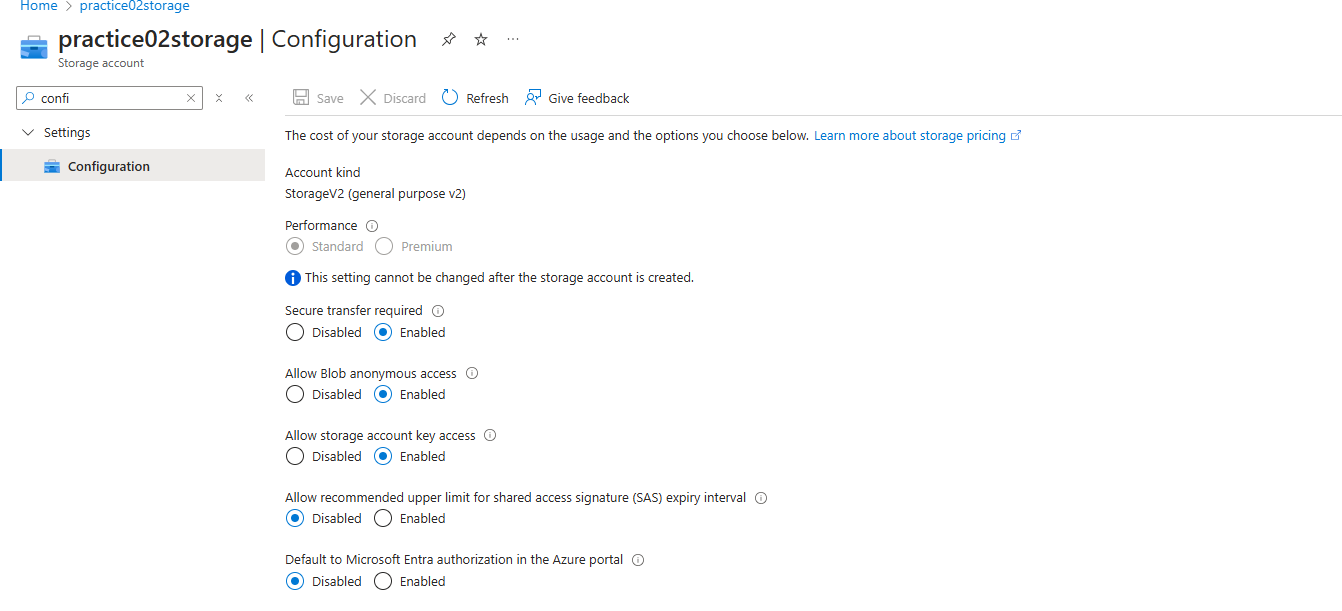


Here you can see even though the container is private I am able to access it from my command prompt without need of any additional permissions such as( Active AD ) or something

So we can make any changes to the storage account using the access keys

And here comes a question if we can actually disable this : YES WE CAN

Here the **storage account access is enabled:**



We can actually disable it and we will try running the above command in Command prompt and see if it actually works:

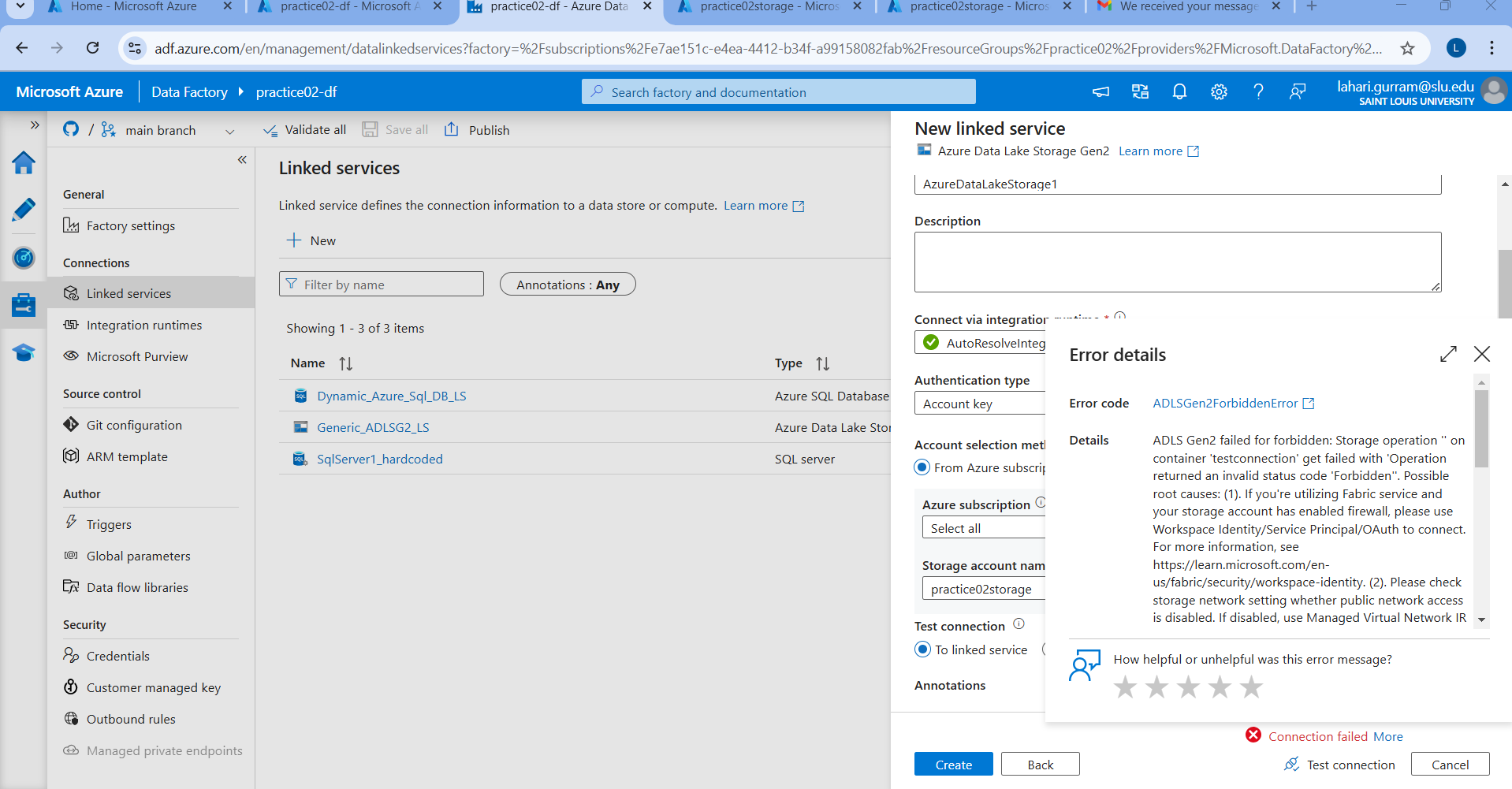


I disable it and now I am gonna see if I can access the command through the command prompt:

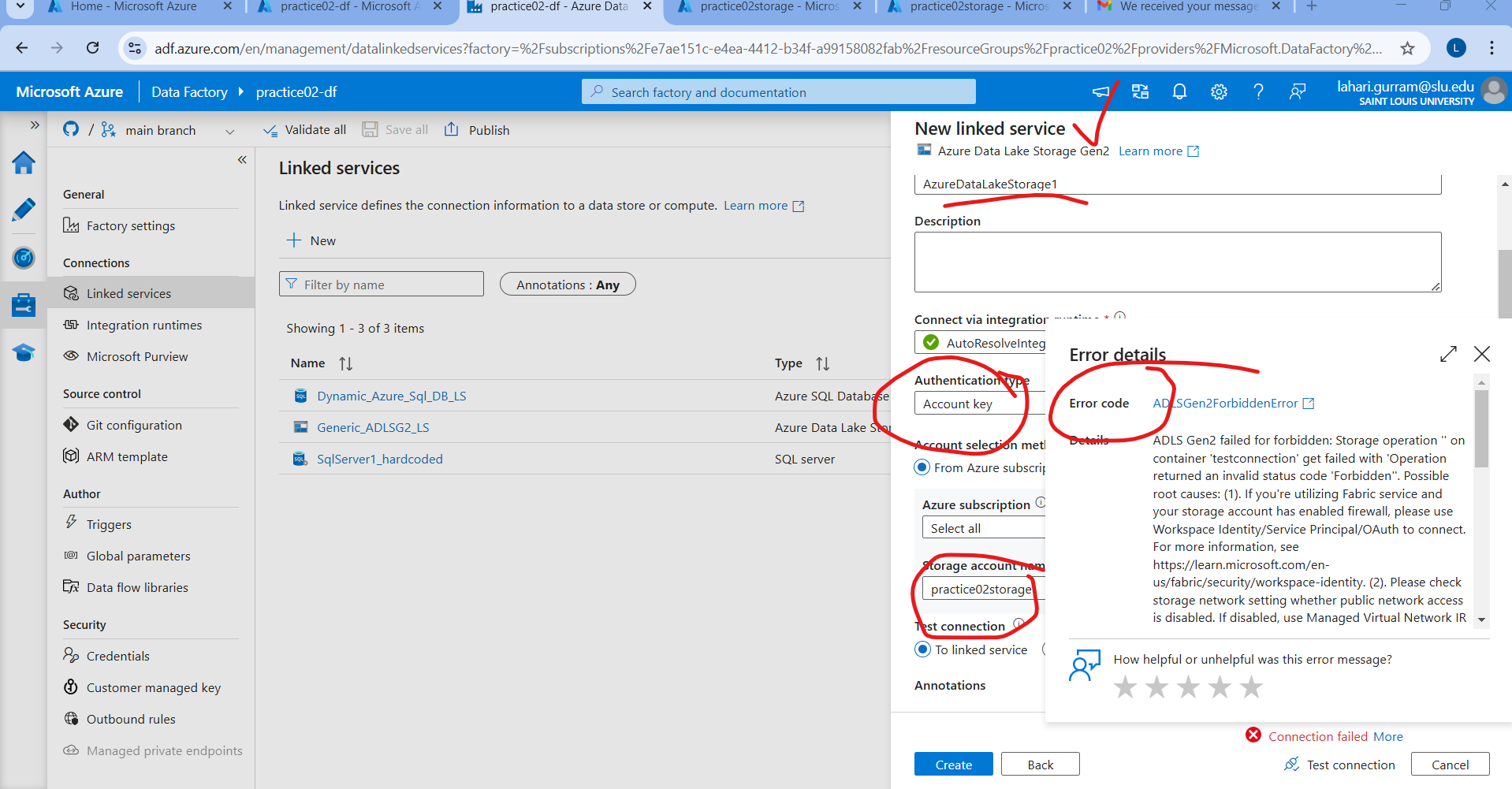


So here it shows that key based authentication is not possible because the key is not enabled

So even if we create a linked service and in authentication type -🡪 if we use “ account key” then it is not gonna accept the connection because I am trying to use the Storage account key(access key ) for the connection let us see:

****

**So when I am trying to connect the linked service using : account key (in linked service) which is access key in storage account : it is giving the error**

****

**So we can disable the accessing of account key and error is:**

ADLS Gen2 failed for forbidden: Storage operation '' on container 'testconnection' get failed with 'Operation returned an invalid status code 'Forbidden''. Possible root causes: (1). If you're utilizing Fabric service and your storage account has enabled firewall, please use Workspace Identity/Service Principal/OAuth to connect. For more information, see https://learn.microsoft.com/en-us/fabric/security/workspace-identity. (2**). Please check storage network setting whether public network access is disabled**. If disabled, use Managed Virtual Network IR and create Private Endpoint to access. https://docs.microsoft.com/en-us/azure/data-factory/managed-virtual-network-private-endpoint. https://docs.microsoft.com/en-us/azure/data-factory/tutorial-copy-data-portal-private (3). It's possible because some IP address ranges of Azure Data Factory are not allowed by your Azure Storage firewall settings. Azure Data Factory IP ranges please refer https://docs.microsoft.com/en-us/azure/data-factory/azure-integration-runtime-ip-addresses. If you allow trusted Microsoft services to access this storage account option in firewall, you must use https://docs.microsoft.com/en-us/azure/data-factory/connector-azure-blob-storage?tabs=data-factory#managed-identity. For more information on Azure Storage firewalls settings, see https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal.. Account: 'practice02storage'. ErrorCode: 'KeyBasedAuthenticationNotPermitted'. Message: **'Key based authentication is not permitted on this storage account**.'. RequestId: '60b534f3-601f-0039-53e6-8609ca000000'. TimeStamp: 'Mon, 24 Feb 2025 18:02:24 GMT'..

Operation returned an invalid status code 'Forbidden'