CST8912 – Cloud Solution Architecture

Graded Lab Activity #3 - Lab Report

Student Name: ZheZhang
Student ID: 041109657
Date: 2025.1.30
Submitted to: Prof. Tanishq Bansal

Azure Cloud Storage Management & Access Control

Introduction or Purpose

The purpose of this lab is to:

- Set up and configure an Azure Storage Account.
- Upload and manage Blob storage within a secure environment.
- Test restricted access to Blob storage and use SAS tokens to grant controlled access.
- Implement lifecycle management policies to optimize cloud storage efficiency.

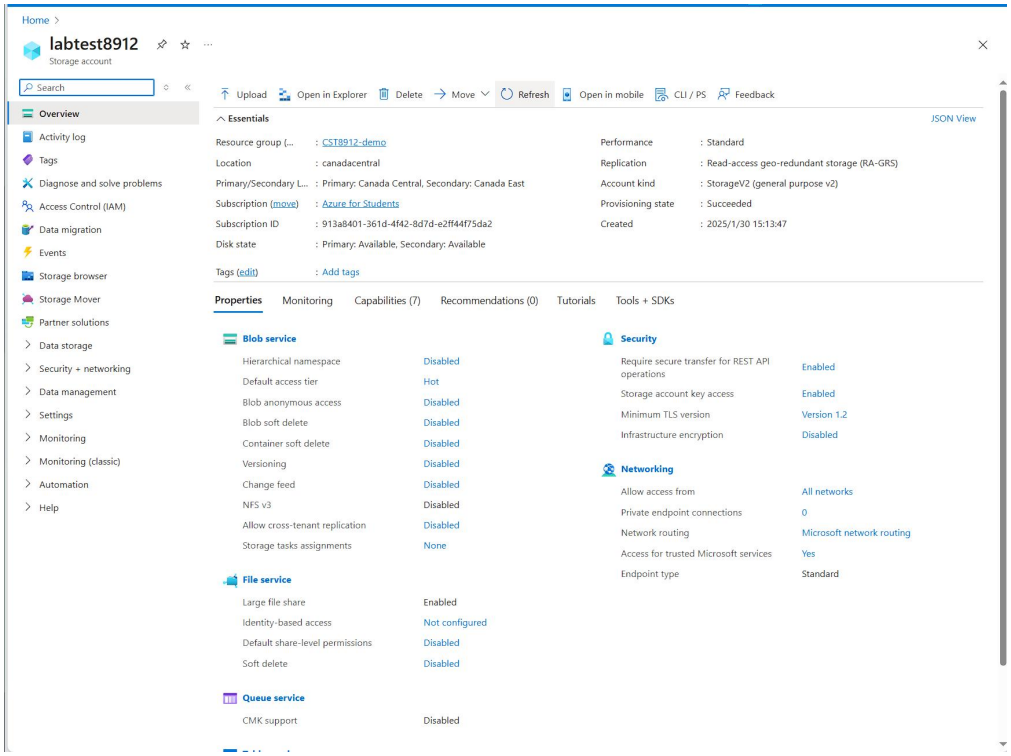
Through this experiment, we will understand the essential components of Azure cloud storage and how they contribute to secure and cost-effective cloud solutions.

Steps Covered in the Lab

Step 1: Create a Storage Account

1. Log in to Azure Portal.
2. Navigate to **Storage Accounts** and click **"+ Create"**.
3. Select **Azure for Students** subscription and create a resource group named **CST8912-demo**.
4. Set the storage account name as **labtest8912**, choose **Canada Central** region.
5. Select **Geo-Redundant Storage (GRS)** for redundancy.
6. Click **"Review + Create"** and wait for deployment to complete.

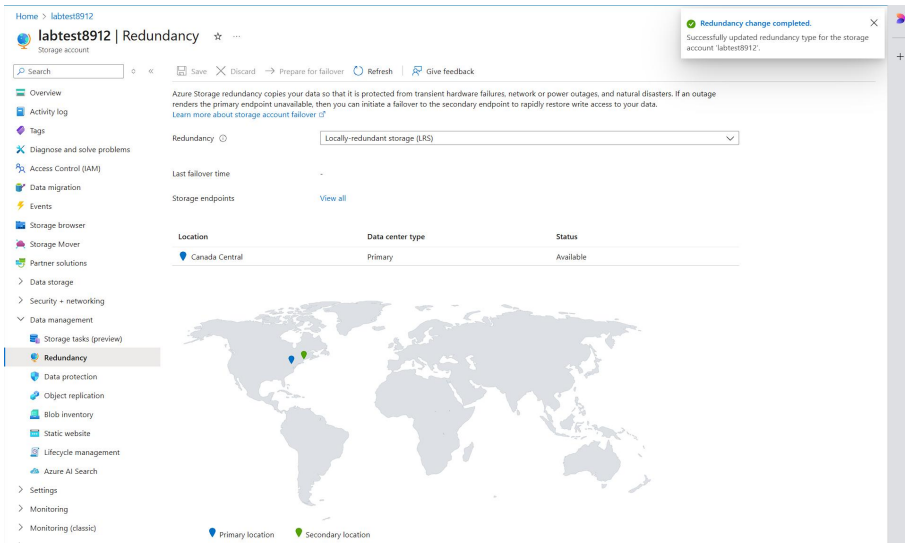
Screenshot 1: Successful creation of labtest8912 storage account.



Step 2: Change Storage Redundancy

1. Navigate to **labtest8912** Storage Account.
2. Under **Data Management**, go to **Redundancy**.
3. Change redundancy from **Geo-Redundant Storage (GRS)** to **Local-Redundant Storage (LRS)**.
4. Click **Save**.

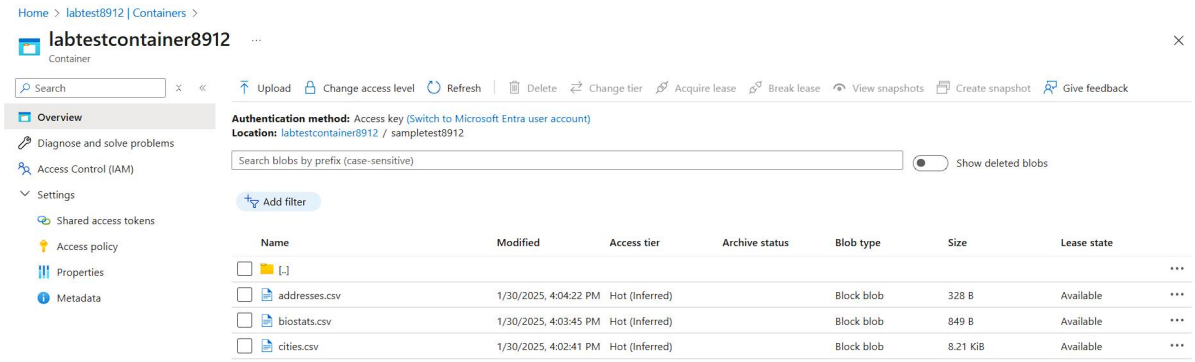
Screenshot 2: Successfully changed storage redundancy.



Step 3: Create Storage Container and Upload Blob

1. Inside **labtest8912**, click **Containers** under **Data Storage**.
2. Create a new container named **labtestcontainer8912** with **Private** access level.
3. Download sample CSV files from: Sample Files.
4. Click **"Upload"**, select CSV files, and set **Upload to folder** as sampletest8912.
5. In **Advanced Settings**, set **Access Tier** to **Hot**.
6. Ensure successful file upload.

Screenshot 3: Successfully uploaded files to sampletest8912 in labtestcontainer8912.

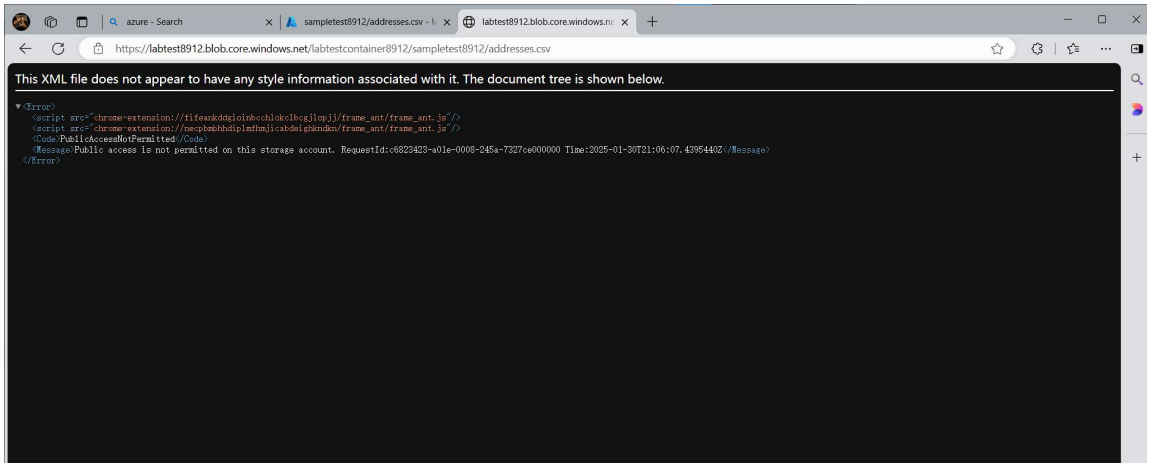


Step 4: Test Blob Access Permissions

1. Open **labtestcontainer8912**, select an uploaded CSV file.

2. Copy **Blob URL** and paste it in an incognito browser window.
3. The expected result is an error message: **"PublicAccessNotPermitted"**.

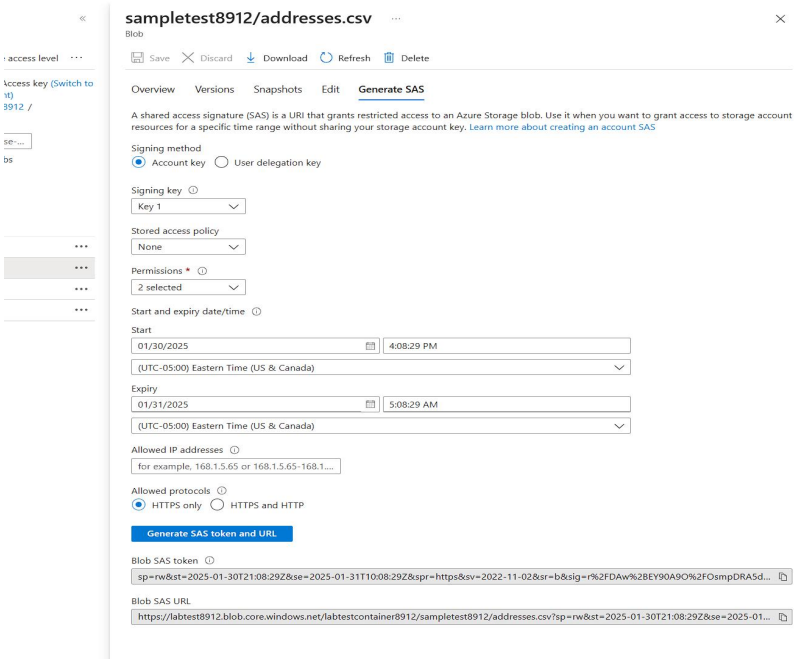
Screenshot 4: Access denied error (PublicAccessNotPermitted).



Step 5: Generate SAS Token and Access Blob

1. In Azure Portal, go to the uploaded Blob file.
2. Click **"Generate SAS"**.
3. Select **Read** permission and set an expiration time.
4. Click **"Generate SAS and URL"**, copy the **SAS URL**.
5. Paste the **SAS URL** in an incognito browser window; the file should be accessible.

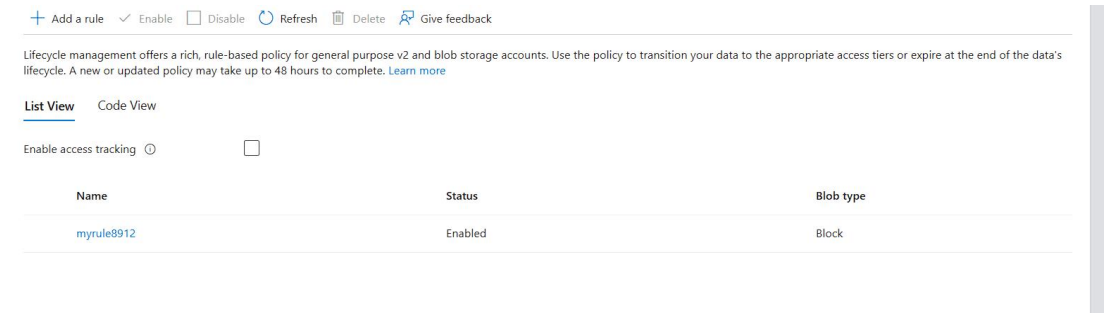
Screenshot 5: Successfully accessed Blob using SAS token.

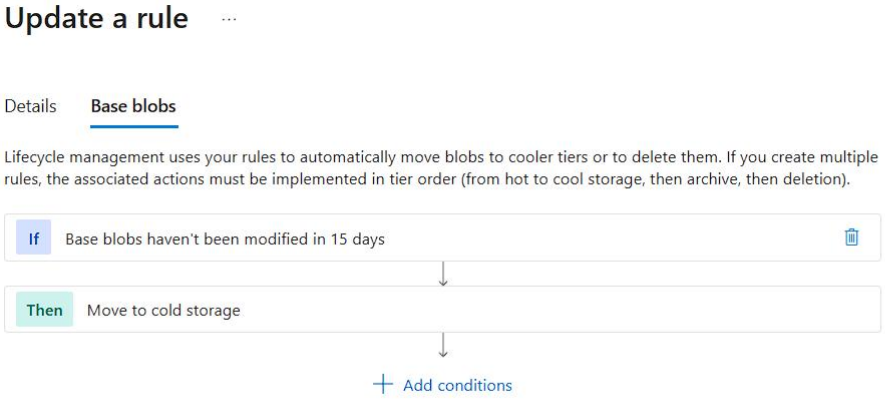


Step 6: Configure Lifecycle Management

1. Navigate to **Lifecycle Management** in the storage account.
2. Create a rule named **myrule8912**, select **Limit blobs with filters**.
3. Set condition: If Blob **was last modified more than 15 days ago**, move it to **Cool storage**.
4. Click **Save**.

Screenshot 6: Successfully created lifecycle management rule.

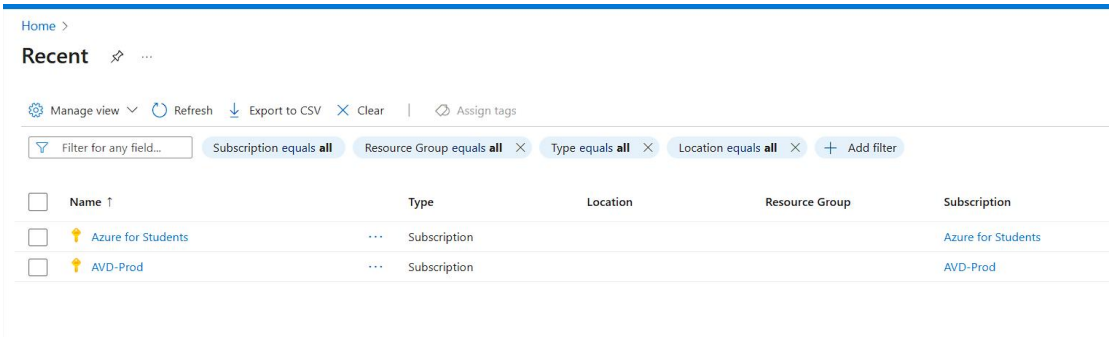




Step 7: Delete Lab Resources

1. Navigate to **Resource Groups**.
2. Select **CST8912-demo**, click **Delete**.

Screenshot 7: Successfully deleted lab resources.



Results

- Successfully created and managed an Azure Storage Account.
- Verified restricted Blob access with default permissions.
- Used SAS tokens to grant controlled access.
- Configured lifecycle management to optimize storage costs.

References

Azure Storage Documentation

YouTube videos provided in the lab.