Placement Empowerment Program
Cloud Computing and DevOps Centre

Use Cloud Storage Create a storage bucket on your cloud platform and upload/download files. Configure access permissions for the bucket.

Name: Keshika D

Department:ADS

INTRODUCTION:

Cloud storage in Microsoft Azure enables scalable, secure, and highly available data storage. Azure Blob Storage is commonly used for storing unstructured data like documents, images, and backups. Users can create a Storage Account and Blob Container to upload, download, and manage files. Access control can be configured using RBAC, Shared Access Signatures (SAS), or private/public permissions. Azure provides multiple ways to interact with storage, including the Azure Portal, CLI, SDKs, and Storage Explorer.

OBJECTIVE:

The objective is to set up Azure Cloud Storage for secure file management. Users will create a Storage Account and Blob Container to upload/download files. Access control will be configured using RBAC or SAS tokens for security. This ensures efficient, scalable, and secure cloud storage management.

Step 1:

Create a Storage Account

In the Azure Portal, search for "Storage accounts" in the search bar.
Click "Create".

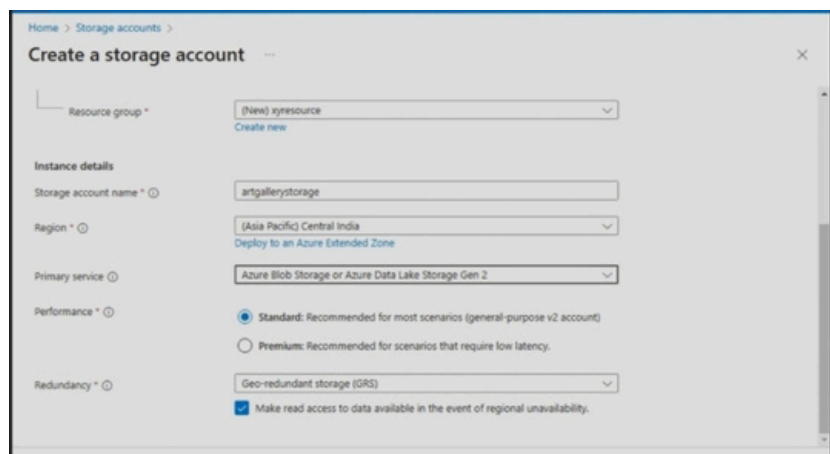Select the Subscription and Resource Group (create a new one if needed).

Provide a Storage account name (must be unique globally).

Choose the Region closest to your users.

Select Performance (Standard or Premium, Standard is sufficient for most use cases).

Choose Redundancy (LRS, GRS, etc., LRS is sufficient for most users).
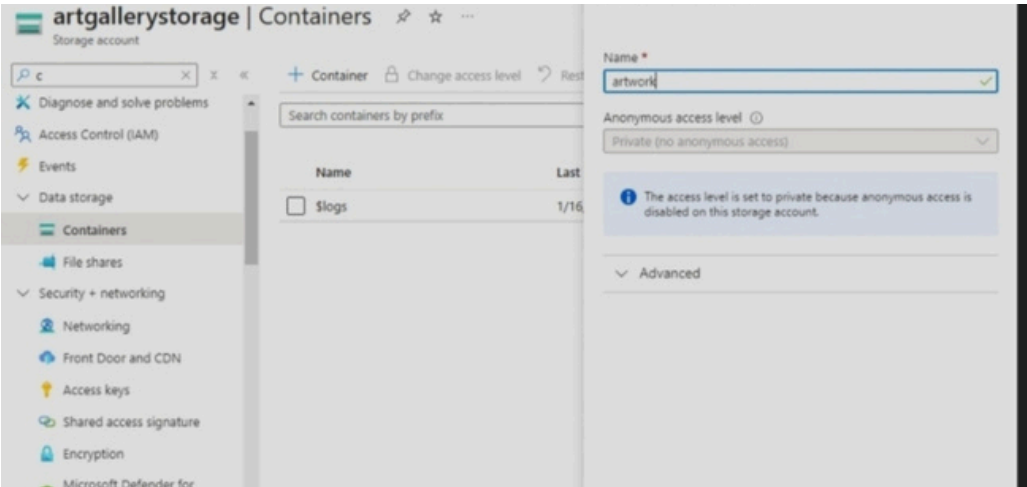
Click Review + Create, then Create.

Step2:

Step 2: Create a Container (Bucket Equivalent)
After the storage account is deployed, open it.

In the left menu, go to Containers under Data storage.

Click + Container, provide a Container name (e.g., mybucket).

Set Public access level (Private by default for security).
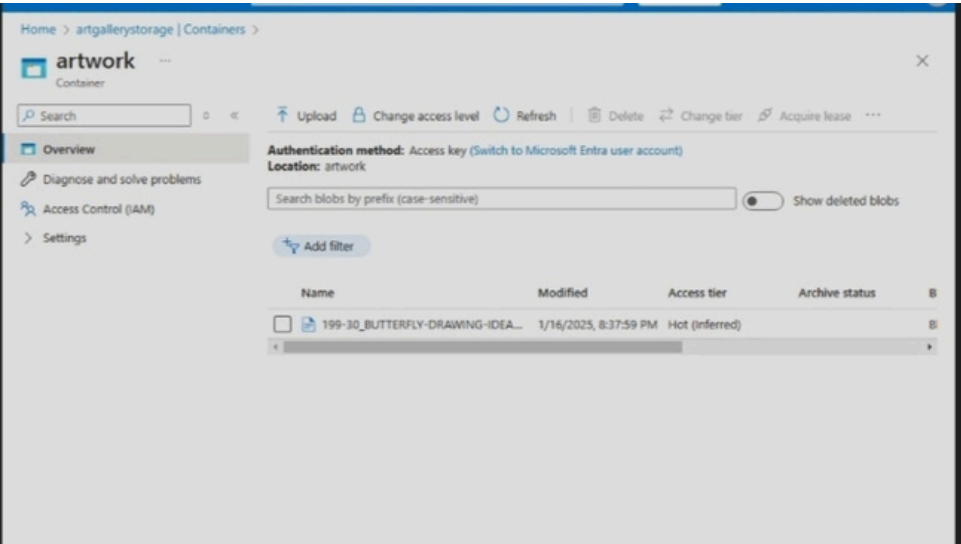Click Create.

Step 3: Upload Files to the Container
Open the created container.
Click Upload at the top.
Browse and select a file from your system.
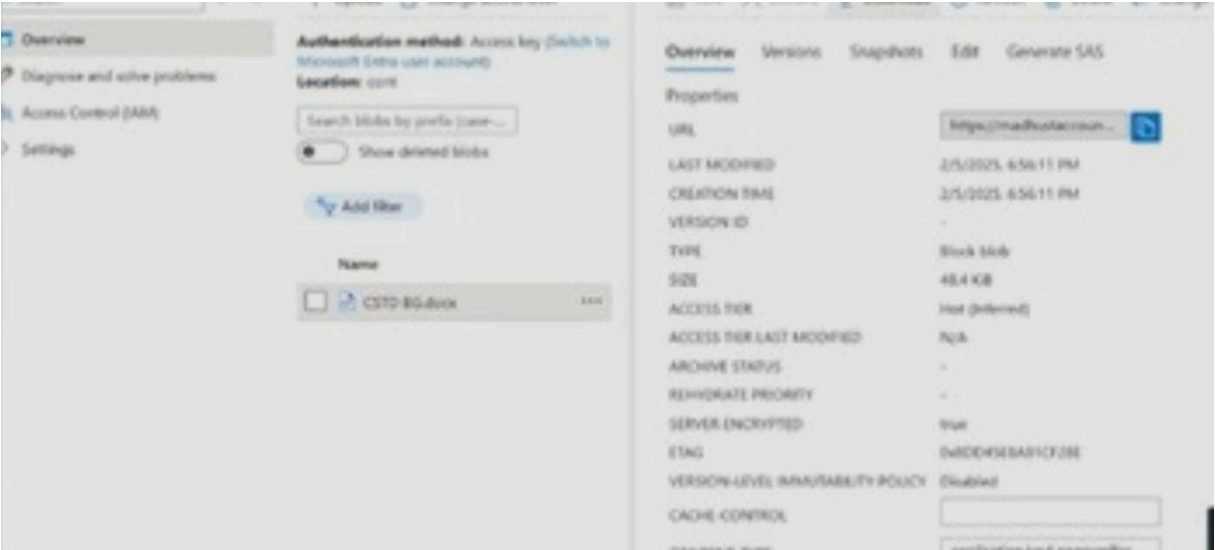Click Upload to store it in the blob container
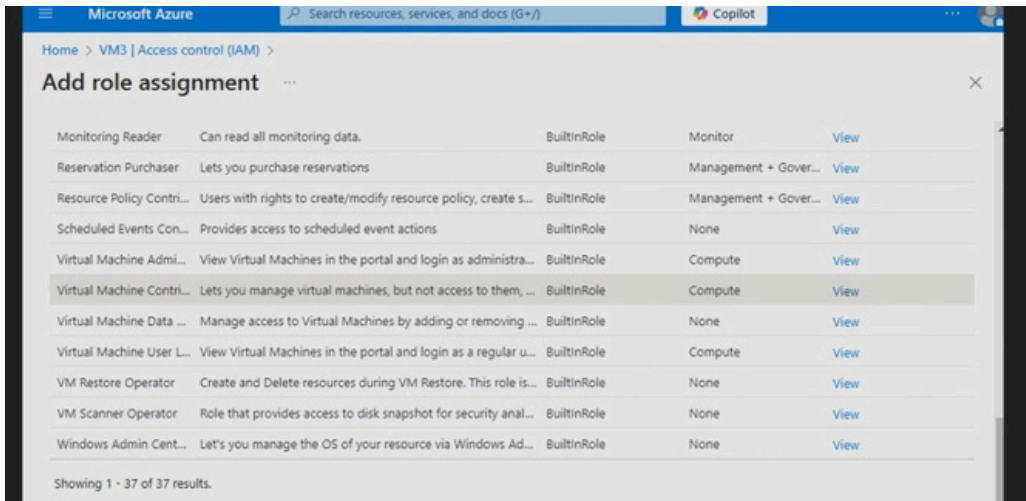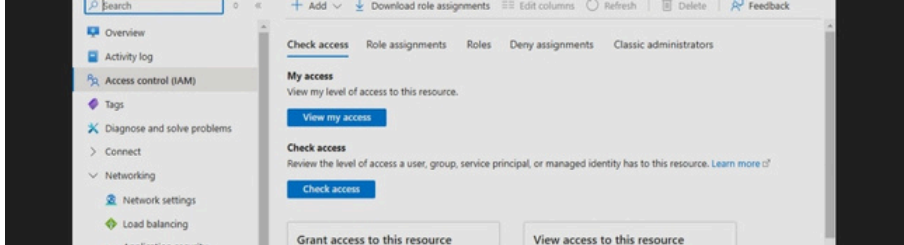
Step 4: Download Files from the Container
Inside the container, locate the uploaded file.
Click on the file name to open details.
Click Download to save it locally.

Role-Based Access Control (RBAC):

Go to Storage account → Access Control (IAM).

Click Add role assignment.

Select a role (e.g., Storage Blob Data Contributor).

Assign it to a user, group, or service principal.

save

VM3 | Access control (IAM)
Virtual machine

+ Add ↓ Download role assignments ☰ Edit columns ↻ Refresh 🗑 Delete 🗨 Feedback

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
> **Connect**
∨ **Networking**
  Network settings
  Load balancing
  Application security groups
  Network manager
> **Settings**

Check access   Role assignments   Roles   Deny assignments   Classic administrators

My access
View my level of access to this resource.

[View my access]

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more ↗

[Check access]

Grant access to this resource

Grant access to resources by assigning a role.
Learn more ↗

View access to this resource

View the role assignments that grant access to this and other resources.
Learn more ↗