

## 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:Madhumitha.H

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).

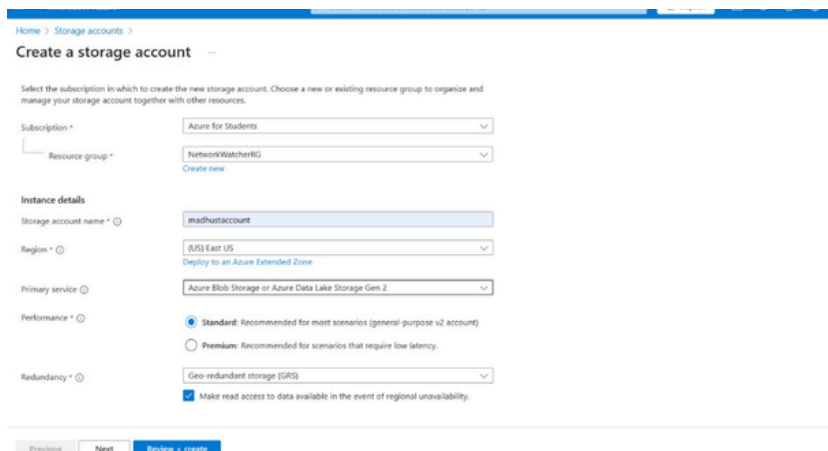
Provide a Storage account name (must be unique globally).

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.



The screenshot shows the 'Create a storage account' page in the Azure Portal. The breadcrumb navigation at the top reads 'Home > Storage accounts >'. The page title is 'Create a storage account'. Below the title, there is a instruction: 'Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.'

The form contains the following fields and options:

- Subscription \***: A dropdown menu with 'Azure for Students' selected.
- Resource group \***: A dropdown menu with 'Netecor/WatcherRG' selected. Below it is a link 'Create new'.
- Instance details**: A section header.
- Storage account name \***: A text input field with 'madhustaccount' entered.
- Region \***: A dropdown menu with '(US) East US' selected. Below it is a link 'Deploy to an Azure Extended Zone'.
- Primary service**: A dropdown menu with 'Azure Blob Storage or Azure Data Lake Storage Gen 2' selected.
- Performance \***: Two radio button options: 'Standard: Recommended for most scenarios (general-purpose v2 account)' (selected) and 'Premium: Recommended for scenarios that require low latency'.
- Redundancy \***: A dropdown menu with 'Geo-redundant storage (GRS)' selected. Below it is a checked checkbox 'Make read access to data available in the event of regional unavailability'.

At the bottom of the form, there are three buttons: 'Previous', 'Next', and 'Review + create' (highlighted in blue).

## Step2:

### Step 2: Create a Container (Bucket Equivalent)

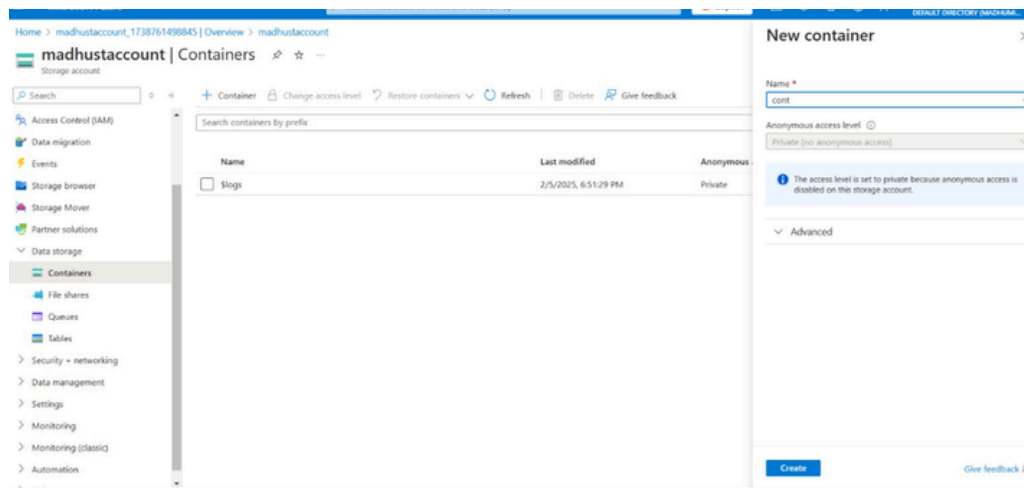
After the storage account is deployed, open it.

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.



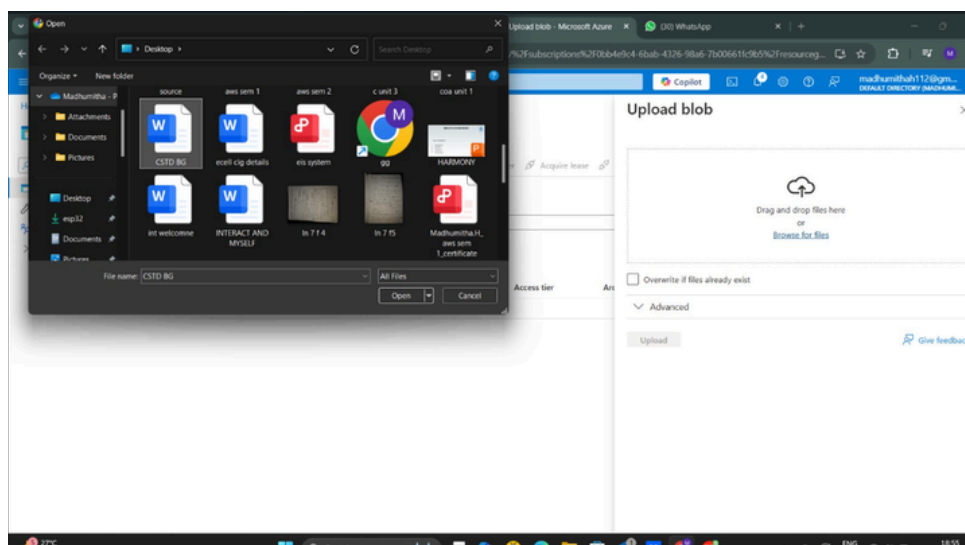
### Step 3: Upload Files to the Container

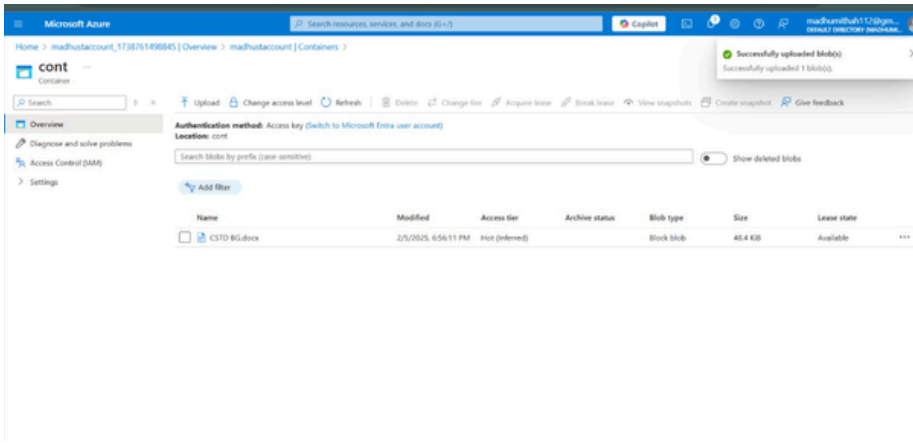
Open the created container.

Click Upload at the top.

Browse and select a file from your system.

Click Upload to store it in the blob container



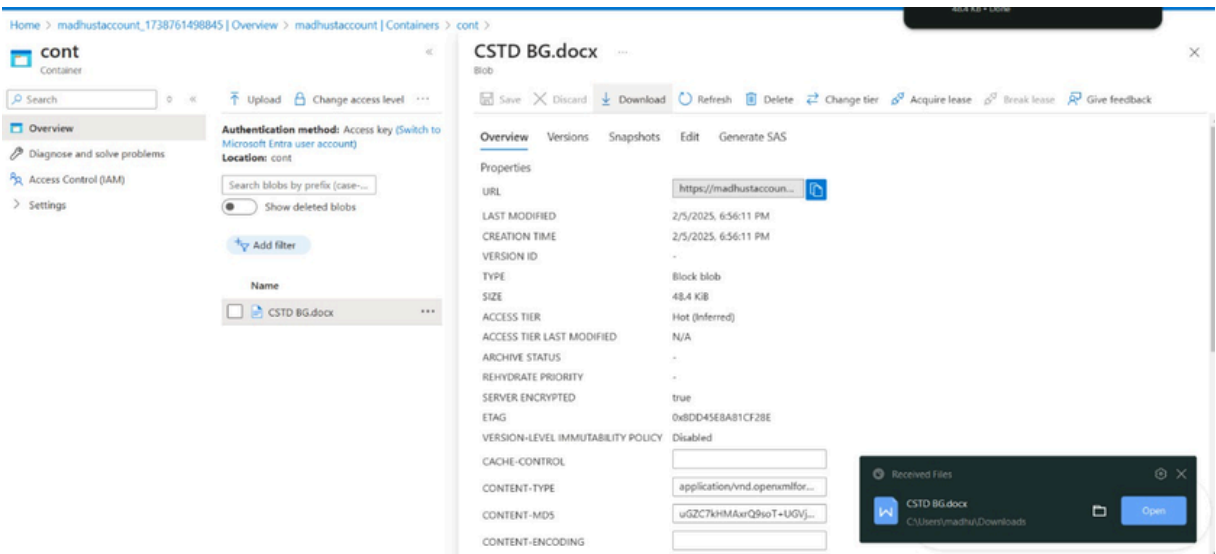
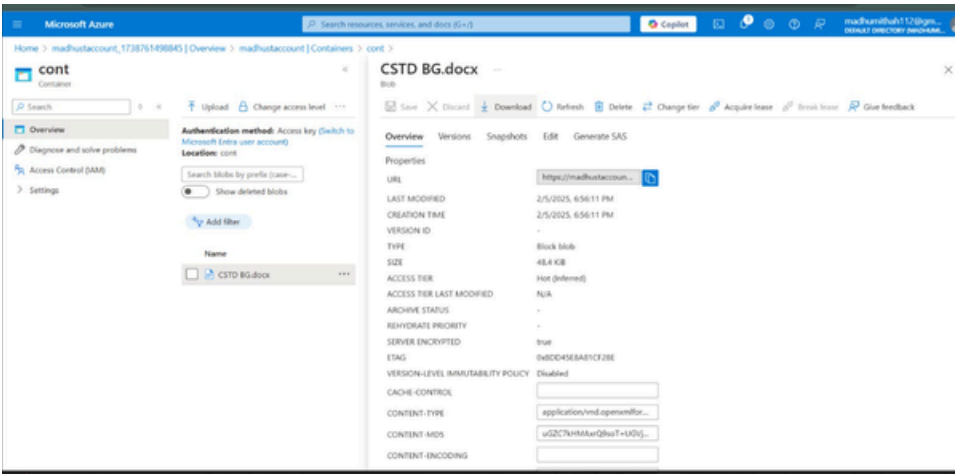


Step 4: Download Files from the Container

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):

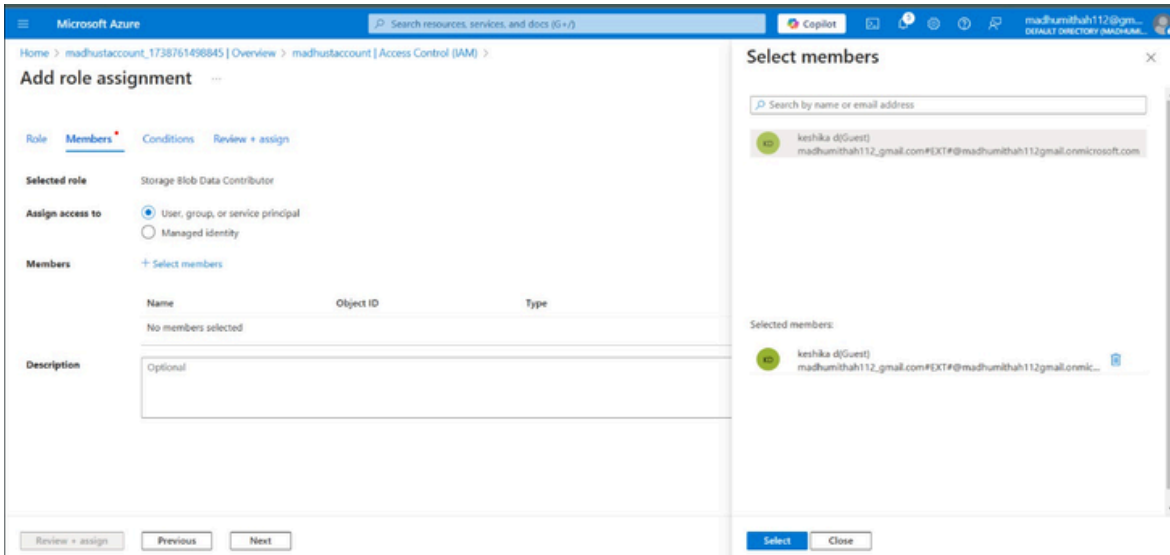
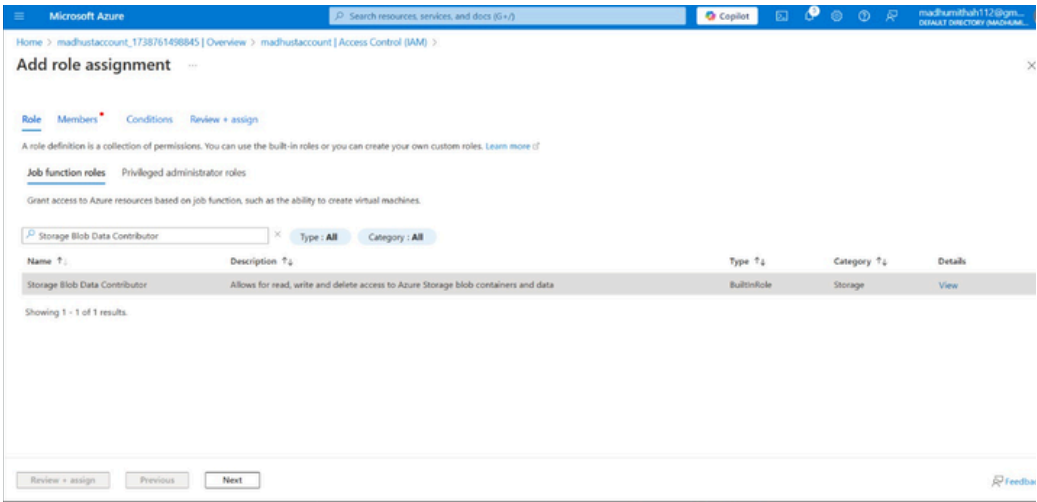
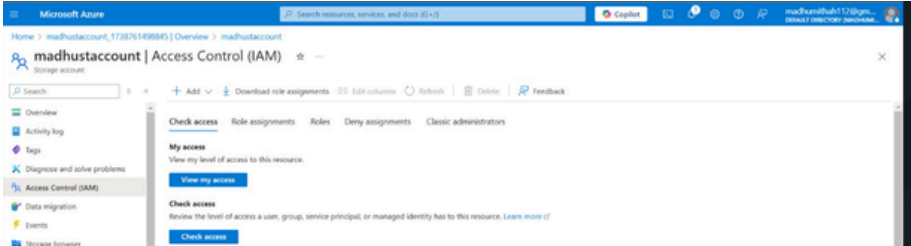
Go to Storage account → Access Control (IAM).

Click Add role assignment.

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

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

save



+ Add Download role assignments Edit columns Refresh Delete Feedback

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)**
- Data migration
- Events
- Storage browser
- Storage Mover
- Partner solutions
- Data storage
  - Containers
  - File shares
  - Queues
  - Tables
- Security + networking
  - Networking

All Job function (1) Privileged (4)






Type: All

Role: All

Scope: All scopes

Group by: Role

5 items (2 Users, 1 Service Principals, 2 Unknown)

	Name	Type	Role	Scope	Condition
Owner (1)					
<input type="checkbox"/>	 keshika.d.madhumithah112@gmail.com#... User	User	Owner	Subscription (Inherited)	None
Contributor (3)					
<input type="checkbox"/>	 Identity not found. Unable to find identity.	Unknown	Contributor	Subscription (Inherited)	None
<input type="checkbox"/>	 Identity not found. Unable to find identity.	Unknown	Contributor	Subscription (Inherited)	None
<input type="checkbox"/>	 orgnewmad-projdemo-759ce12	App	Contributor	Subscription (Inherited)	None
Storage Blob Data Contributor (1)					
<input type="checkbox"/>	 keshika.d.madhumithah112@gmail.com#... User	User	Storage Blob Data Contributor	This resource	Add