

Azure Storage and Resource Governance

Project Overview

This document summarizes hands-on experience configuring Azure storage services and applying governance controls using the Azure Portal.

- Configured Azure Blob Storage for cloud-based data management
- Applied resource locks to protect critical Azure resources

Azure Blob Storage Configuration

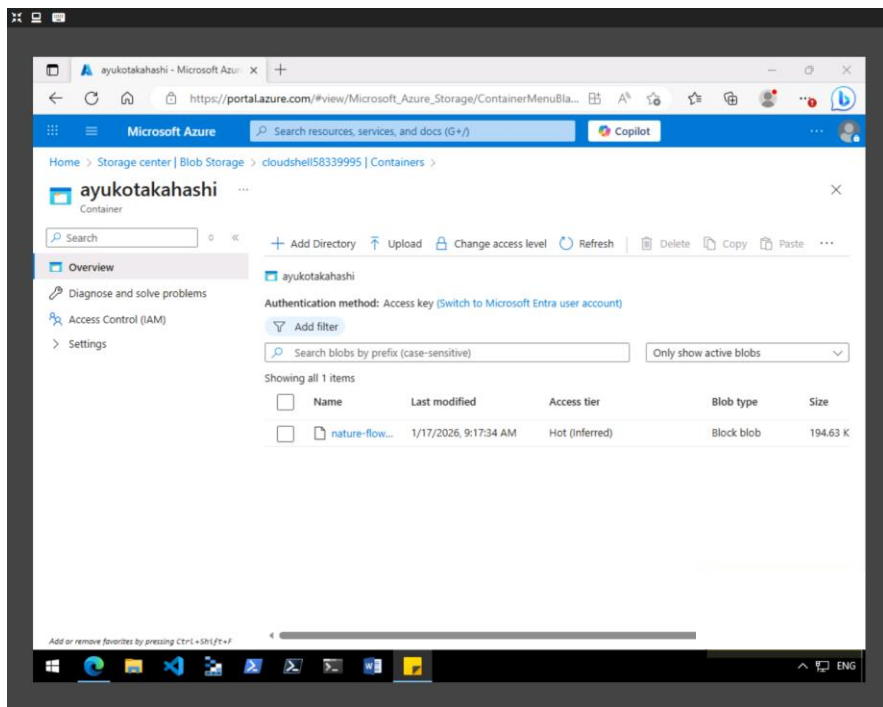
This section documents the creation and configuration of Azure Blob Storage using the Azure Portal, including storage account setup, container creation, and basic configuration decisions for managing cloud-based data.

The screenshot displays the Azure Portal interface for configuring a storage account. The main window shows the 'cloudshell58339995' storage account overview, including details like Resource group (myRGKV-lod58339995), Location (eastus), Subscription (AZ-900T00-A-CSR-1), and Subscription ID (f3fead34-0c35-4a23-b037-6ac13ce0d38b). The 'Properties' tab is active, showing the account's performance, replication, and provisioning state. A sidebar on the right, titled 'Create a storage blob', provides a step-by-step guide for creating a resource, selecting storage categories, and configuring the account settings. The sidebar includes a table of settings and values, and a progress bar indicating 19 minutes remaining.

Setting	Value
Subscription	AZ-900T00-A-CSR2
Resource Group	myRGKV-lod58339995
Storage account name	cloudshell58339995
Region	Default
Performance	Standard
Redundancy	Locally redundant storage (LRS)

Work with blob storage

19 Minutes Remaining



Create a storage blob

Instructions Resources

Save the image to your computer.

4. Back in the Azure portal select the container you created, then select Upload.
5. Browse for the image file you want to upload. Select it and then select upload.

You can upload as many blobs as you like in this way. New blobs will be listed within the container.

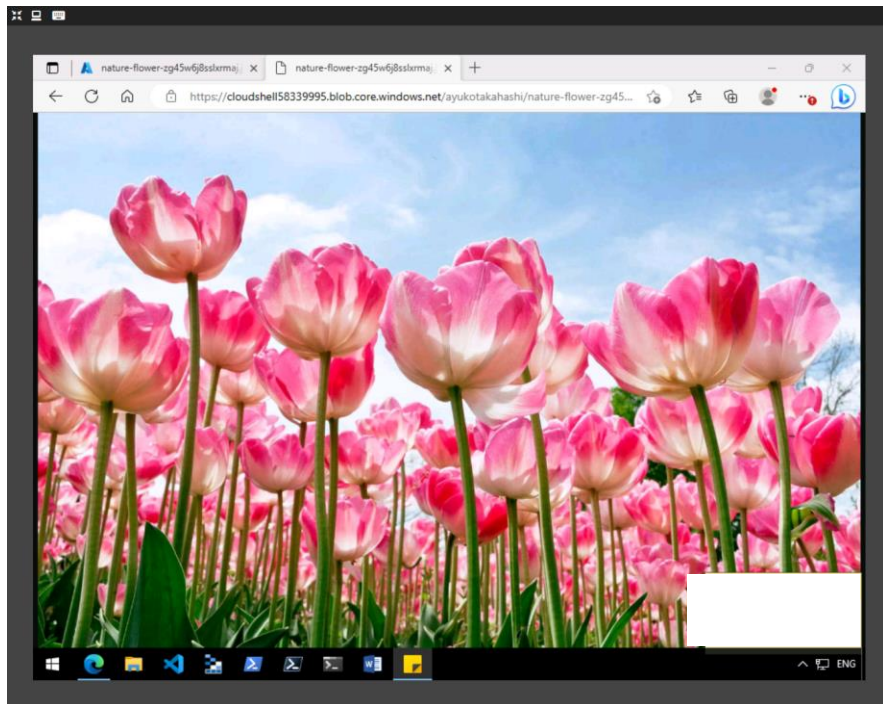
6. Select the Blob (file) you just uploaded. You should be on the properties tab.
7. Copy the URL from the URL field and paste it into a new tab.

You should receive an error message similar to the following.

```
<Error>
  <Code>ResourceNotFound
  <Message>The specified resource does not exist.
</Error>
```

Previous End

17 Minutes Remaining



Create a storage blob

Instructions Resources

Change access level

6. Select OK

7. Refresh the tab where you attempted to access the file earlier.

Congratulations - you've completed this exercise. You created a storage account, added a container to the storage account, and then uploaded blobs (files) to your container. Then you changed the access level so you could access your file from the internet.

Clean up

The sandbox automatically cleans up your resources when you're finished with this module.

When you're working in your own subscription, it's a good idea at the end of a project to identify whether you still need the resources you created. Resources that you leave running can cost you money. You can delete resources individually or delete the resource group to delete the entire set of resources.

Previous End

22 Minutes Remaining

Resource Lock Configuration

This section documents the application of Azure resource locks to protect critical resources from accidental modification or deletion, demonstrating governance and risk management best practices.

The screenshot displays the Azure portal interface for a storage account named 'cloudshell58340346'. The 'Locks' blade is active, showing a table with one lock: 'Read-only Lock01' of type 'Read-only' with scope 'cloudshell5834'. The left sidebar contains navigation options like Overview, Activity log, Tags, and Storage browser. On the right, a task instruction panel titled 'Configure a resource lock' provides steps for applying a read-only lock. The panel includes a list of instructions, a small diagram of the 'Add lock' dialog, and navigation buttons for 'Previous' and 'End'.

Task 2: Apply a read-only resource lock

In this task you apply a read-only resource lock to the storage account. What impact do you think that will have on the storage account?

- ✓ 1. Scroll down until you find the Settings section of the blade on the left of the screen.
- ✓ 2. Select Locks.
- ✓ 3. Select + Add.

Add lock dialog:

- Lock name: [Text input field]
- Lock type: [Read-only selected]
- Scope: [cloudshell5834 selected]

- ✓ 4. Enter a Lock name.
- ✓ 5. Verify the Lock type is set to Read-only.
- ✓ 6. Select OK.

Navigation: Previous End

22 Minutes Remaining