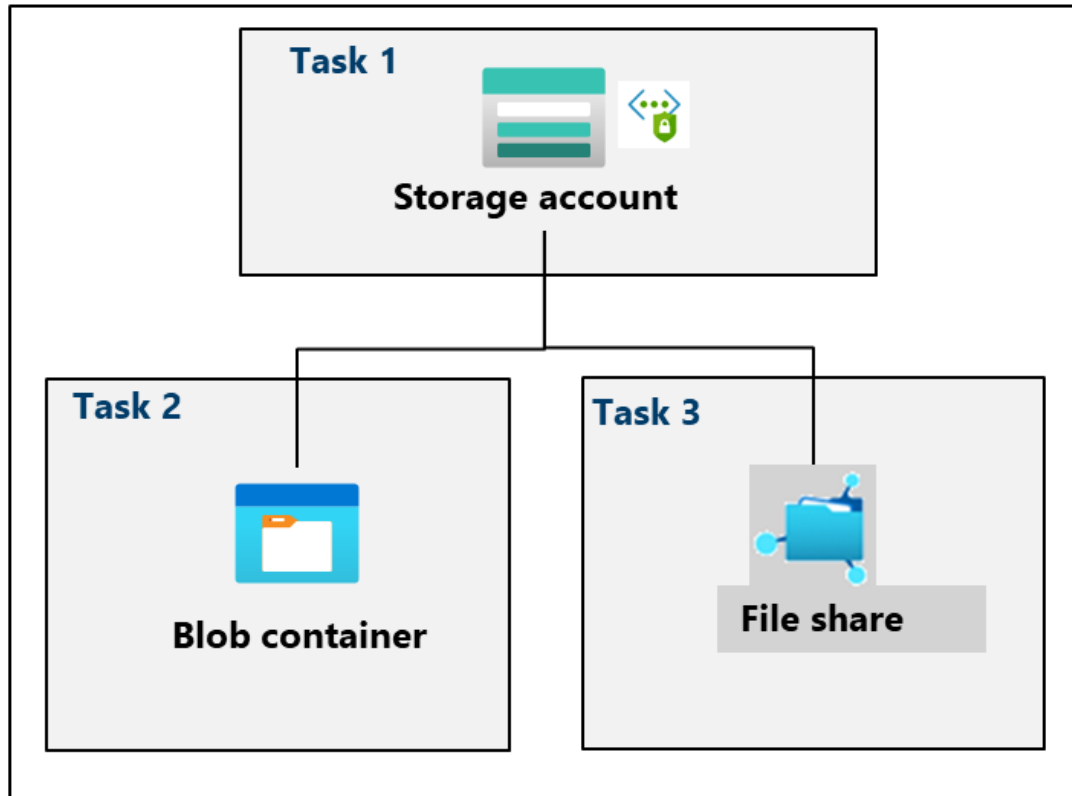




az104-07-rg7



#### Task 1: Create and Configure a Storage Account

##### Steps Taken

- Created a storage account with:
- **Geo-redundant storage**
- **Public network access disabled**
- **Lifecycle rule: Move blobs older than 30 days to cool tier**

##### Screenshot Suggestions

- Storage account creation settings

## Create a storage account ...

[Create new](#)

**Instance details**

Storage account name \* ⓘ

Region \* ⓘ  [Deploy to an Azure Extended Zone](#)

Preferred storage type

**Performance** \* ⓘ ☒ **Standard:** Recommended for most scenarios (general-purpose v2 account)  
☐ **Premium:** Recommended for scenarios that require low latency.

**Redundancy** \* ⓘ  ☒ Make read access to data available in the event of regional unavailability.

[Previous](#) [Next](#) [Review + create](#)

- Networking tab showing public access disabled

Basics Advanced **Networking** Data protection Encryption Tags [Review + create](#)

**Public access**

Access your resource from anywhere through a public network.

Note: Allowing access to your resource through a public network increases security risk. [Learn more](#)


Public network access \* ⓘ ☐ **Enable**  
Allow inbound and outbound access with the option to restrict select inbound access using resource access configurations for this resource.

☒ **Disable**  
Restrict inbound access while allowing outbound access.

☐ **Secure by perimeter (Most restricted)**  
Restrict inbound and outbound access using a network security perimeter. Secure by perimeter offers the greatest level of inbound and outbound restriction to secure your resource.

Public network access scope ☐ Enable from all networks

[Previous](#) [Next](#) [Review + create](#)



- Lifecycle rule configuration (Movetocool)

## Add a rule ...

Lifecycle management uses your rules to automatically move blobs to cooler tiers or to delete them. If you create multiple rules, the associated actions must be implemented in tier order (from hot to cool storage, then archive, then deletion).

If

Base blobs were \*

☒ Last modified

☐ Created

More than (days ago) \*

30

↓

Then

Move to cool storage

↓

[+ Add conditions](#)

### Notes

- Used Standard performance tier
- Enabled read access in case of regional outage
- Lifecycle rule created successfully

### Task 2: Secure Blob Storage

#### Steps Taken

- Created blob container data with **private access**
- Added **time-based retention policy** (180 days)
- Uploaded file to folder securitytest
- Verified access denial via direct URL
- Generated **SAS token** for limited access

### Screenshot Suggestions

- Container creation with private access


# New container



Name \*

datadata 

Anonymous access level ⓘ

Private (no anonymous access) 



The access level is set to private because anonymous access is disabled on this storage account.



Advanced


- Retention policy setup

# Immutable Storage policy





Policy type


Time-based retention 

Set retention period for \* 

180   
days

☐ Enable version-level immutability 

 In order to enable version-level immutability support, your storage account must have versioning turned on.

Allow protected append writes to 

- ☒ None  
☐ Append blobs  
☐ Block and append blobs

- Upload blade with advanced settings

## Upload blob



Block size ⓘ

4 MiB



Access tier ⓘ

Hot (Inferred)



Upload to folder

securitytest

Blob index tags ⓘ

Key

Value

Encryption scope

☒ Use existing default container scope

☐ Choose an existing scope

Retention policy ⓘ

☐ Use container-level retention period: 180 day(s)

☐ Choose custom retention period

- SAS token generation and access test

## Generate SAS

range without sharing your storage account key. [Learn more about creating an account SAS](#)

Signing method

☒ Account key ☐ User delegation key

Signing key ⓘ

Key 1

Stored access policy

None

Permissions \* ⓘ

Read

Start and expiry date/time ⓘ

Start

09/05/2025

6:42:07 AM

(UTC-08:00) Pacific Time (US & Canada)

Expiry

09/07/2025

2:57:07 PM

(UTC-08:00) Pacific Time (US & Canada)

Allowed IP addresses ⓘ

### Notes

- Blob type: Block blob
- Access tier: Hot
- SAS token worked as expected for limited access

### Task 3: Configure Azure File Storage

#### Steps Taken

- Created file share share1 with **transaction optimized tier**
- Disabled backup
- Uploaded file via Storage Browser
- Created folder structure using "+ Add directory"

### Screenshot Suggestions

- File share creation

[Home](#) > [storageaccount22\\_1757166327254 | Overview](#) > [storageaccount22 | File shares](#) >

## New file share ...



✓ Validation passed

[Basics](#) [Backup](#) [Review + create](#)

### Basics

|                 |                      |
|-----------------|----------------------|
| File share name | share1               |
| Access Tier     | TransactionOptimized |
| Protocol        | SMB                  |

- Storage Browser view of share1

 **storageaccount22 | Storage browser** ☆ ... 

Storage account

»

storageaccount22

<

★ Favorites

⚙ Recently viewed

📁 Blob containers

📁 File shares

📁 Queues


📁 Tables

⚙ Privacy settings

🗨 Feedback

### Storage account metrics

The data provided is regularly updated about 2-4 times a day and published hourly. If you have extremely large objects, it may be over a day between updates.


 **Blob containers**

Number of containers

Number of blobs

Total data stored

-  
-  
-

 **File shares**

Number of file shares

Number of files

Total data stored

-  
-  
-

- Upload confirmation



## Upload files




Drag and drop files here  
or  
[Browse for files](#)

☐ Overwrite if files already exist

Upload

Current uploads

Dismiss: [Completed](#) [All](#)

az104-lab07-architecture...  33.08 KiB / 33.08 KiB

### Notes

- Storage Browser is intuitive for file management
- No restrictions initially

### Restrict Network Access

### Steps Taken

- Created virtual network vnet1
- Added service endpoint for Microsoft.Storage
- Linked vnet1 to storage account
- Removed public IP access

### Screenshot Suggestions

- Virtual network creation

## Create virtual network ...

✓ Validation passed

Basics Security IP addresses Tags Review + create

[View automation template](#)

### Basics

|                |                       |
|----------------|-----------------------|
| Subscription   | AZ-104T00A CSR 2      |
| Resource Group | az104-rg7-lod54409035 |
| Name           | vnet1                 |
| Region         | East US               |

### Security

|                               |          |
|-------------------------------|----------|
| Azure Bastion                 | Disabled |
| Azure Firewall                | Disabled |
| Azure DDoS Network Protection | Disabled |

Previous

Next

Create

[Download a template for automation](#)

- Service endpoint configuration

## Add service endpoints



Service \*

Microsoft.Storage



Service endpoint policies

0 selected



Subnets \*

default



With service endpoints, the source IP address for service traffic from this subnet will switch from using public IPv4 addresses to using private IPv4 address. Existing IP firewall rules using Azure public IP addresses will stop working with this switch. Please ensure IP firewall rules allow for this switch before setting up service endpoints. You may also experience temporary interruption to service traffic from this subnet while configuring service endpoints.

- Networking blade showing vnet restriction

## Add networks



Subscription \*

AZ-104T00A CSR 2



Virtual networks \*

vnet1



Subnets \*

default



Successfully configured secure Azure Storage using Blob and File services.

Tested access control via SAS tokens and virtual network restrictions.

Validated lifecycle management and retention policies.