az104-07-rg7

Task 1
Storage account

Task 2
Blob container

Task 3
File share
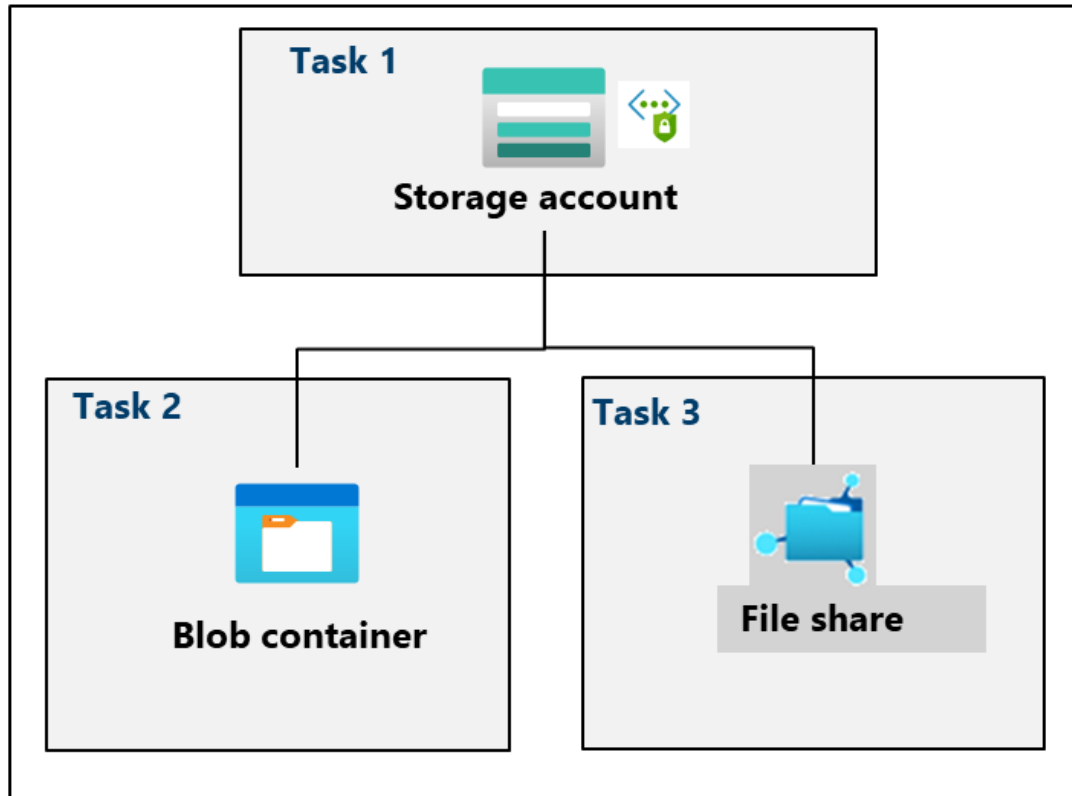
🛠 Task 1: Create and Configure a Storage Account

◈ 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

- Networking tab showing public access disabled

- 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

- Storage Browser view of share1

- 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

- Service endpoint configuration

- 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.