[AZ-104] AZURE ADMINISTRATOR

STORAGE

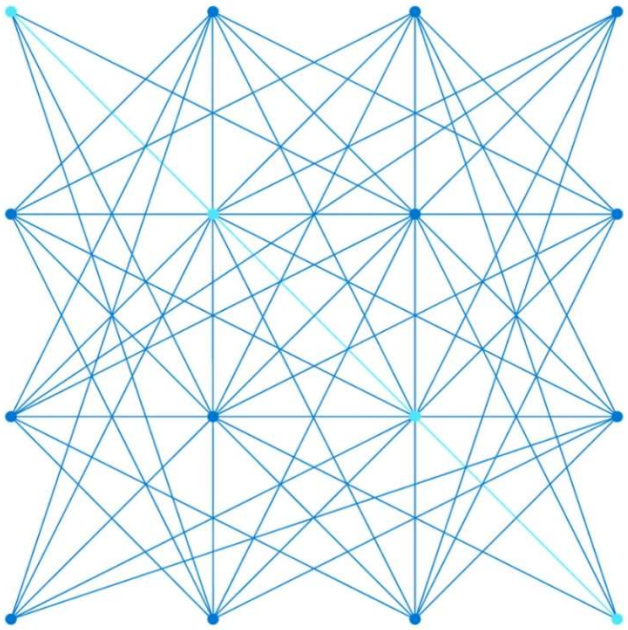
AZ-104T00A Content:

07- Azure Storage

7-1- Configure Storage Accounts
7-2- Blob Storage
7-3- Storage Security
7-4- Azure Files and

Microsoft Azure

AZ-104
Azure Storage



Administer Azure Storage Introduction

- Storage Accounts
- Blob Storage
- Storage Security
- File Sync
- *Lab 07 – Manage Azure Storage*

7.1 Configure Storage Accounts

Configure Storage Accounts Introduction

- Implement Azure Storage
- Explore Azure Storage Services
- Determine Storage Account Kinds
- Determine Replication Strategies
- Access Storage
- Secure Storage Endpoints
- *Demonstration – Secure a Storage Endpoint*
- *Summary and Resources*

Implement Azure Storage

A service that you can use to store files, messages, tables, and other types of information

- Durable ✓
- Secure ✓
- Scalable ✓
- Managed ✓
- Accessible ✓

Storage for ...
- virtual machines ✓
- unstructured data ✓
- structured data ✓

SA

Two performance options:

- (●) **Standard:** Recommended for most scenarios (general-purpose v2 account)
- ( ) **Premium:** Recommended for scenarios that require low latency.

Storage Performance Options – Standard and Premium

	Storage Account Performance	Recommended usage
✓	Standard: general-purpose v2	Recommended for most scenarios including Blob, File, Queue, Table, and Data Lake Storage. LRS GRS ZRS GZRS
o	Premium: Block blobs	Block blob scenarios with high transactions rates, or scenarios that use smaller objects or require consistently low storage latency. LRS ZRS
o	Premium: File shares	Enterprise or high-performance file share applications. LRS ZRS
o	Premium: Page blobs	Premium high-performance page blob scenarios. LRS ZRS

✓ **All storage accounts are encrypted using Storage Service Encryption (SSE) for data at rest**

Compare Files to Blobs

Feature	Description	When to use
Azure Files	SMB interface, client libraries, and a REST interface that allows access from anywhere to stored files	• Lift and shift an application to the cloud • Store shared data to be accessed across multiple virtual machines • Store development and debugging tools that need to be accessed from many virtual machines
Azure Blobs	Client libraries and a REST interface that allows unstructured data (flat namespace) to be stored and accessed at a massive scale in block blobs	• Support streaming and random-access scenarios • Access application data from anywhere

Compare Files to Blobs

Feature	Description	When to use
Azure Files	SMB interface, client libraries, and a REST interface that allows access from anywhere to stored files	• Lift and shift an application to the cloud • Store shared data to be accessed across multiple virtual machines • Store development and debugging tools that need to be accessed from many virtual machines
Azure Blobs	Client libraries and a REST interface that allows unstructured data (flat namespace) to be stored and accessed at a massive scale in block blobs	• Support streaming and random-access scenarios • Access application data from anywhere

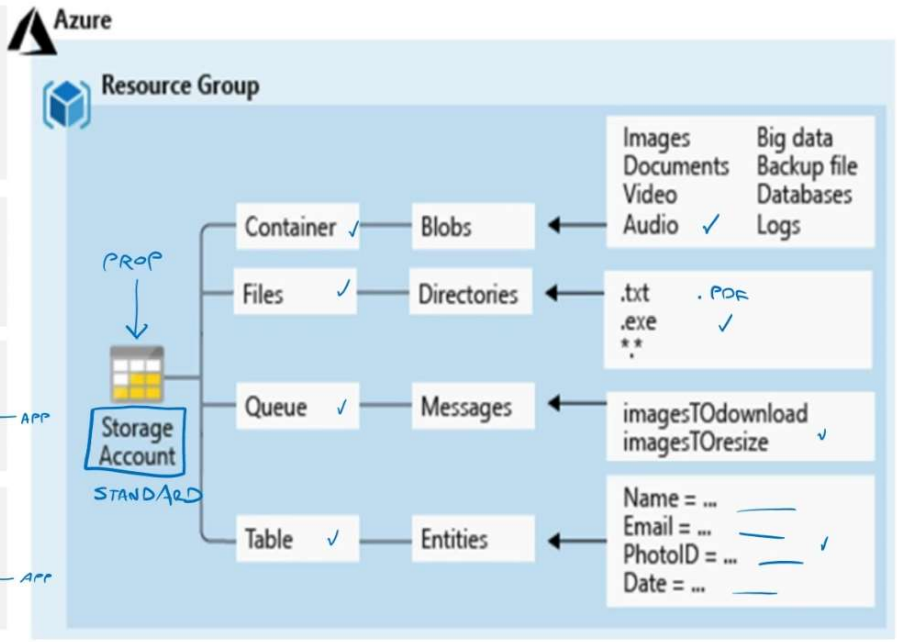
Azure Storage Services

Containers: A massively scalable object store for text and binary data

File shares: Managed file shares for cloud or on-premises deployments

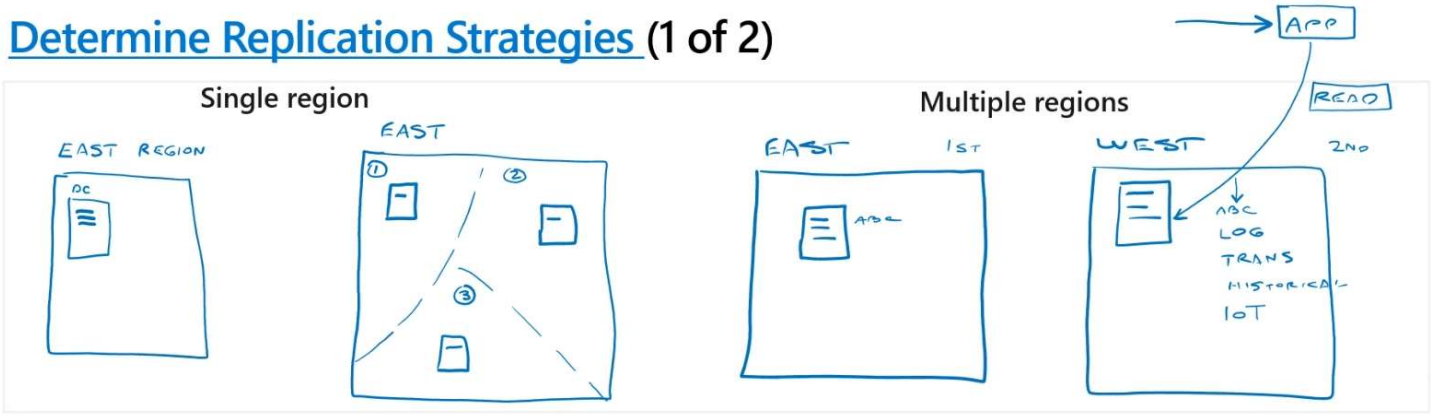
Queues: A messaging store for reliable messaging between application components

Tables: Ideal for storing structured, non-relational data



[Azure services that support availability zones | Microsoft Learn]

Determine Replication Strategies (1 of 2)



LRS

- Three replicas, one region
- Protects against disk, node, rack failures
- Write is acknowledged when all replicas are committed
- Superior to dual-parity RAID

ZRS

- Three replicas, three zones, one region
- Protects against disk, node, rack, and zone failures
- Synchronous writes to all three zones

GRS

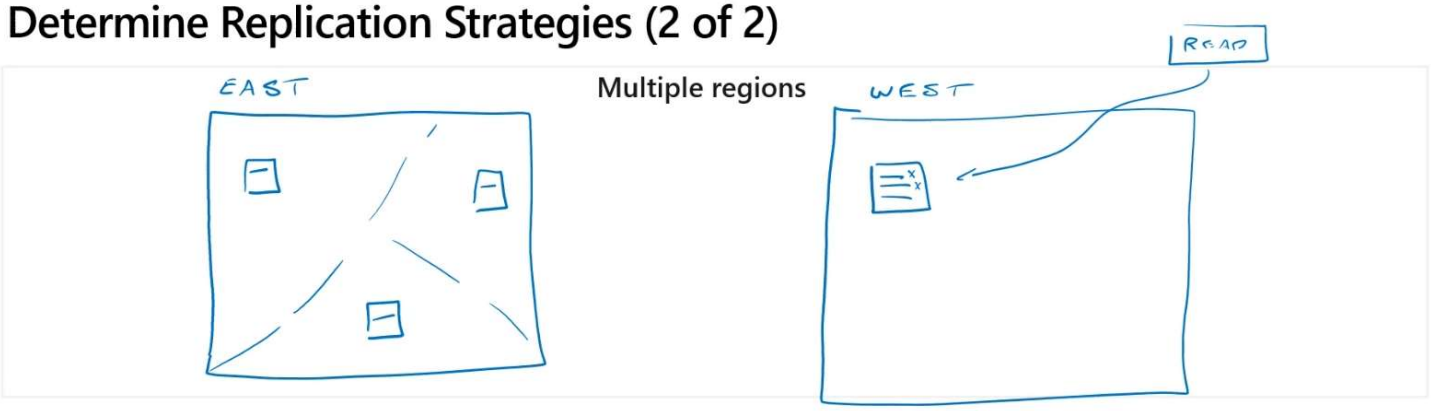
- Six replicas, two regions (three per region)
- Protects against major regional disasters
- Asynchronous copy to secondary

RA-GRS

- GRS + read access to secondary
- Separate secondary endpoint
- Recovery point objective (RPO) delay to secondary can be queried

Continued next slide

Determine Replication Strategies (2 of 2)



GZRS

- Six replicas, 3+1 zones, two regions
- Protects against disk, node, rack, zone, and region failures
- Synchronous writes to all three zones and asynchronous copy to secondary

RA-GZRS

- GZRS + read access to secondary
- Separate secondary endpoint
- RPO delay to secondary can be queried

Access Storage

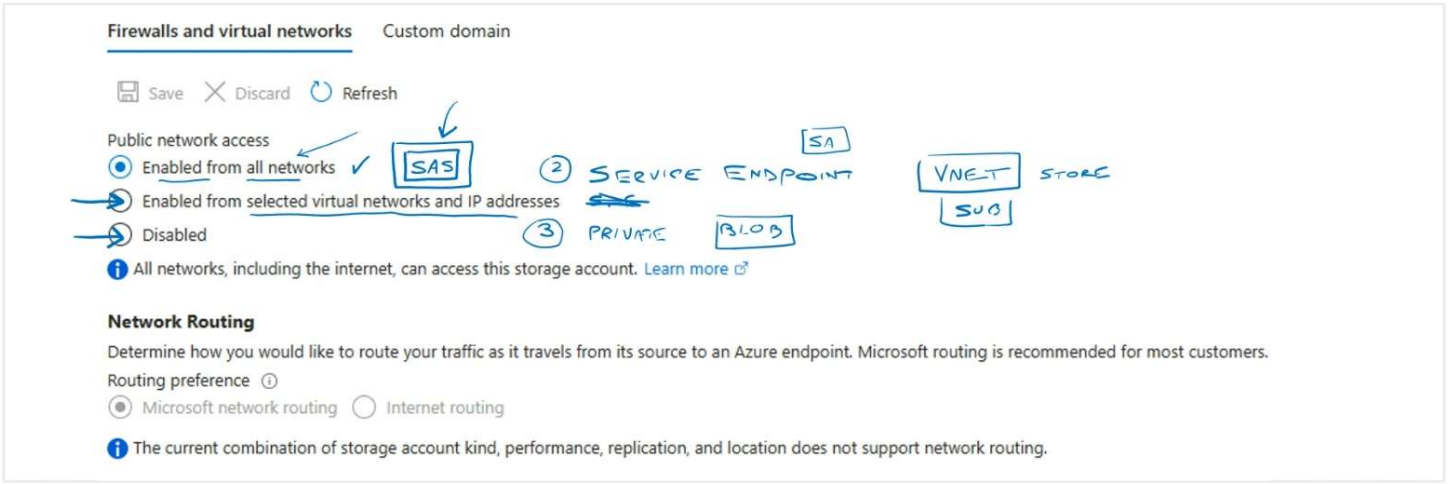
Every object has a unique URL address – based on account name and storage type

Container service: https://*mystorageaccount*.blob.core.windows.net
File service: https://*mystorageaccount*.file.core.windows.net
Table service: https://*mystorageaccount*.table.core.windows.net
Queue service: https://*mystorageaccount*.queue.core.windows.net

If you prefer you can configure a custom domain name

CNAME record	Target
blobs.contoso.com	contosoblobs.blob.core.windows.net

Secure Storage Endpoints



Firewalls and Virtual Networks restrict access to the Storage Account from specific Subnets on Virtual Networks or public IP's

DEMO 1 – Create a Storage Account, SAS, and Endpoint

- Create a storage account
- Create a File Shares data storage – upload files
- Connect to file shares from Storage Explorer – Shared Access Signature
- Secure with Storage Endpoint

Which of the following replicates your data to a secondary region and maintains six copies of your data?
Select one.

A) Locally-redundant storage LRS
B) Geo-redundant storage GRS
C) Zone-redundant storage ZRS

b

You have two video files stored as blobs. One of the videos is business-critical and requires a replication policy that creates multiple copies across geographically diverse datacenters. The other video is non-critical, and a local replication policy is sufficient. Which of the following options would satisfy both data diversity and cost sensitivity consideration?

A) Create a single storage account that makes use of Local-redundant storage (LRS) and host both videos from here.

B) Create a single storage account that makes use of Geo-redundant storage (GRS) and host both videos from here.

C) Create two storage accounts. The first account makes use of Geo-redundant storage (GRS) and hosts the business-critical video content. The second account makes use of Local-redundant storage (LRS) and hosts the non-critical video content.

c

The name of a storage account must be:

A) Unique within the containing resource group.
B) Unique within your Azure subscription.
C) Globally unique.

c

In a typical project, when would you create your storage account(s)?

A) At the beginning, during project setup.

B) After deployment, when the project is running.

C) At the end, during resource cleanup.

A

Multiple choice

A manufacturing company has several sensors that record time-relative data. Only the most recent data is useful. The company wants the lowest cost storage for this data. What is the best kind of storage account for them?

A) LRS
B) GRS
C) ZRS

A

7.2 Configure Blob Storage

Configure Blob Storage Introduction

- Implement Blob Storage
- Create Blob Containers
- Create Blob Access Tiers
- Add Blob Lifecycle Management Rules
- Determine Blob Object Replication
- *Demonstration – Blob Storage*
- *Summary and Resources*

* Upload Blobs and Determine Storage Pricing are not covered.

Implement Blob Storage

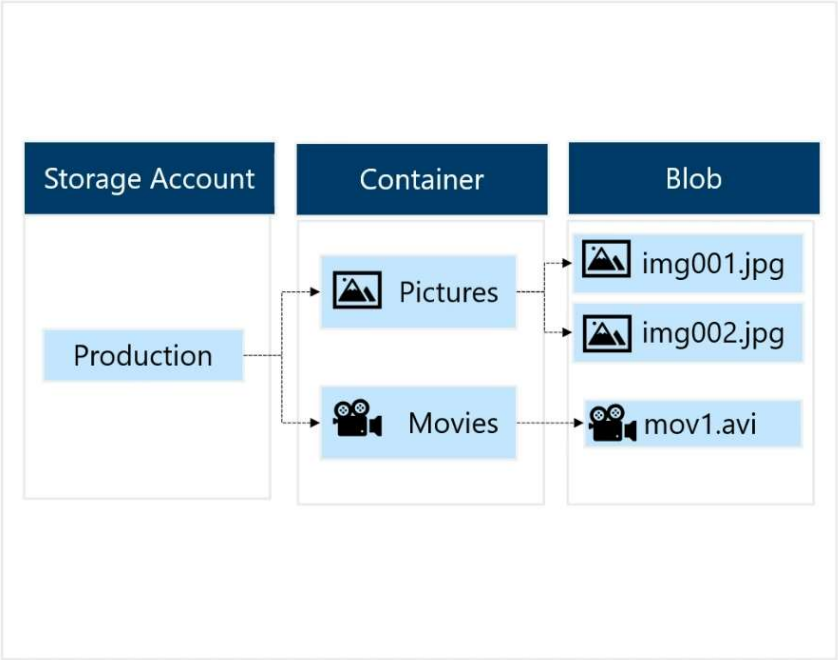
Stores unstructured data in the cloud

Can store any type of text or binary data

Also referred to as *object storage*

Common uses:

- Serving images or documents directly to a browser
- Storing files for distributed access
- Streaming video and audio
- Storing data for backup and restore, disaster recovery, archiving
- Storing data for analysis by an on-premises or Azure-hosted service



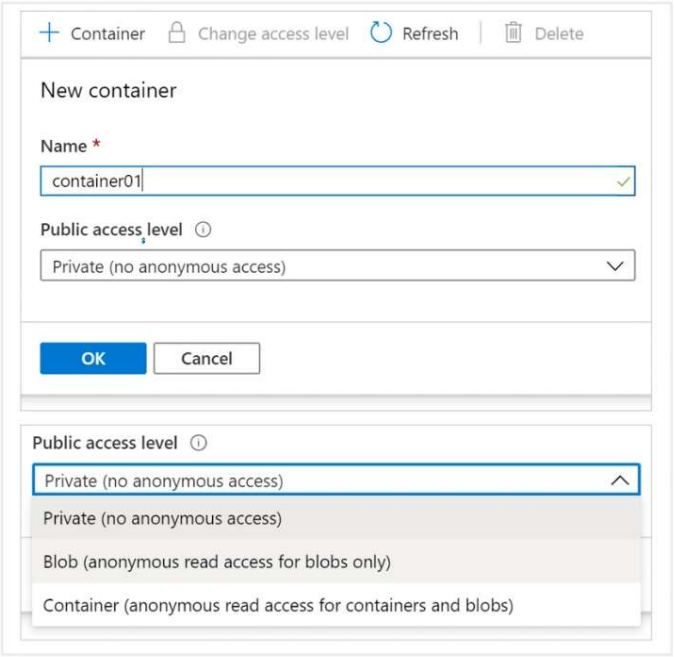
Blob Containers

All blobs must be in a container

Accounts have unlimited containers

Containers can have unlimited blobs ✓

- **Private blobs** – no anonymous access
- **Blob access** – anonymous public read access for blobs only
- **Container access** – anonymous public read and list access to the entire container, including the blobs

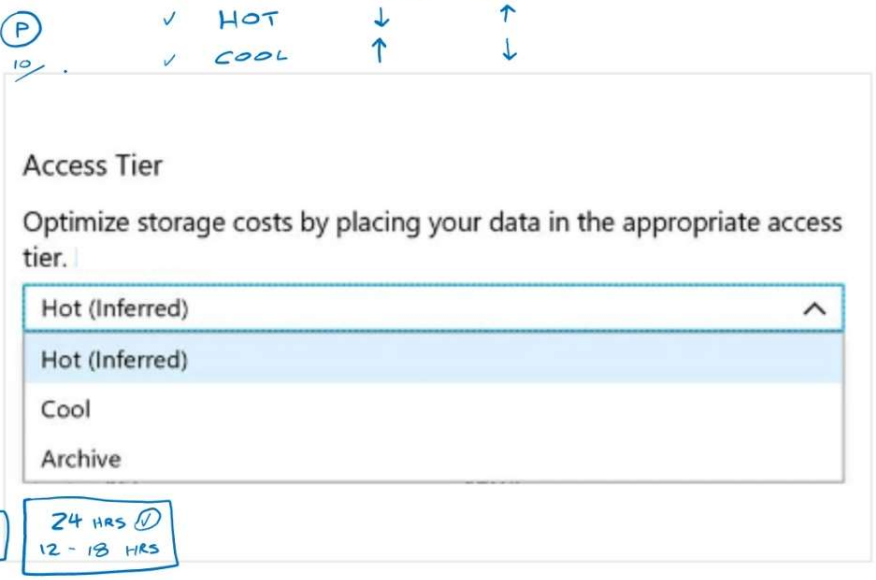


Blob Access Tiers

Hot – Optimized for frequent access of objects in the storage account

Cool – Optimized for storing large amounts of data that is infrequently accessed and stored for at least 30 days

Archive – Optimized for data that can tolerate several hours of retrieval latency and will remain in the Archive tier for at least 180 days



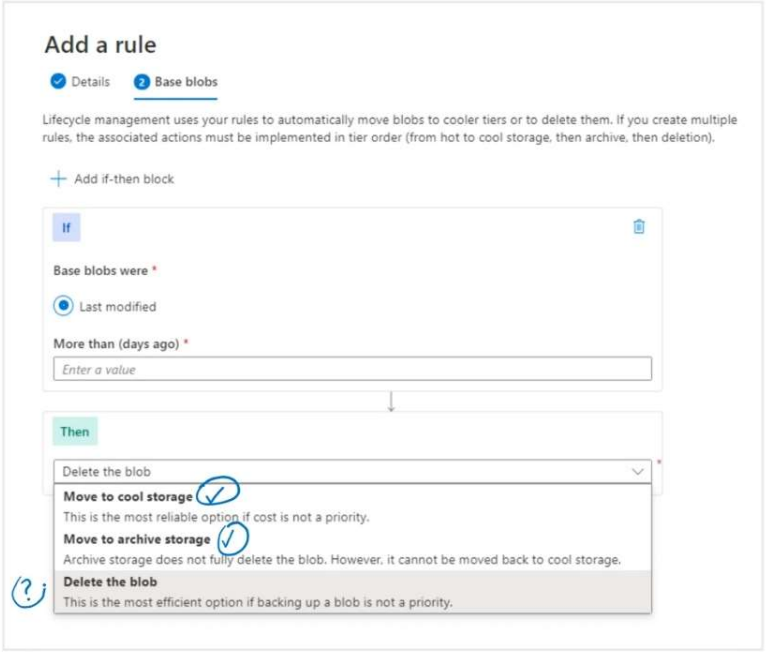
✓ **You can switch between these access tiers at any time**

Blob Lifecycle Management Rules

Transitioning of blobs to a cooler storage tier to optimize for performance and cost

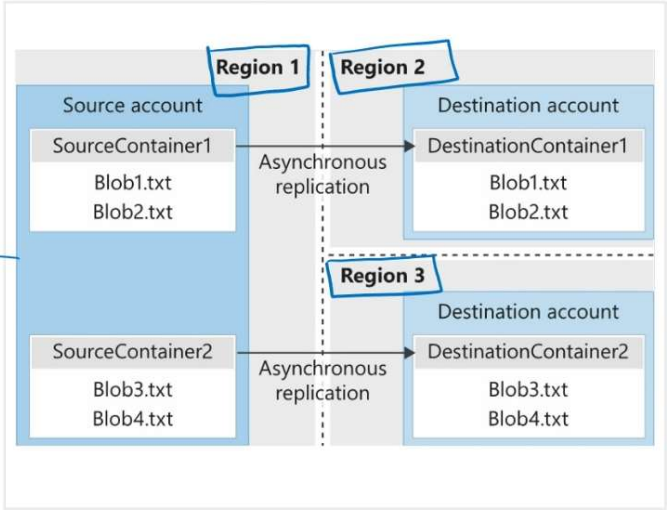
Delete blobs at the end of their lifecycle

Apply rules to filtered paths in the Storage Account



Blob Object Replication

- Asynchronous to any other Region
- Minimizes latency for read requests
- Increases efficiency for compute workloads
- Optimizes data distribution



Multiple choice

Which of these changes between access tiers will happen immediately?

A) Hot to Cool
B) Archive to Cool
C) Archive to Hot

a

Your company is building an app in Azure. The storage must be reachable programmatically through a REST API. The storage must be globally redundant. The storage must be accessible privately within the company's Azure environment. The storage must be optimal for unstructured data. Which type of Azure storage should you use for the app? Select one.

A) Azure Table Storage
B) Azure Blob Storage
C) Azure File Storage

b

You are using blob storage. Which of the following is true? Select one.

A) The cool access tier is for frequent access of objects in the storage account.

B) The hot access tier is for storing large amounts of data that is infrequently accessed.

C) You can switch between hot and cool performance tiers at any time.

c

Configure Storage Security Introduction

- Review Storage Security Strategies
- Create Shared Access Signatures
- Identify URI and SAS Parameters
- Demonstration – Configure storage security
- Determine Storage Service Encryption
- Create Customer Managed Keys
- Apply Storage Security Best Practices
- Summary and Resources

Review Storage Security Strategies

- **Encryption**. All data written to Azure Storage is automatically encrypted using Storage Service Encryption (SSE).
- **Authentication**. ~~Azure Active Directory (Azure AD)~~ and Role-Based Access Control (RBAC) are supported for Azure Storage for both resource management operations and data operations.
- **Azure AD integration** is supported for data operations on the Blob and Queue services.
- **Data in transit**. Data can be secured in transit between an application and Azure by using Client-Side Encryption, HTTPS, or SMB 3.0.
- **Disk encryption**. OS and data disks used by Azure virtual machines can be encrypted using Azure Disk Encryption.
- **Shared Access Signatures**. Delegated access to the data objects in Azure Storage can be granted using Shared Access Signatures.

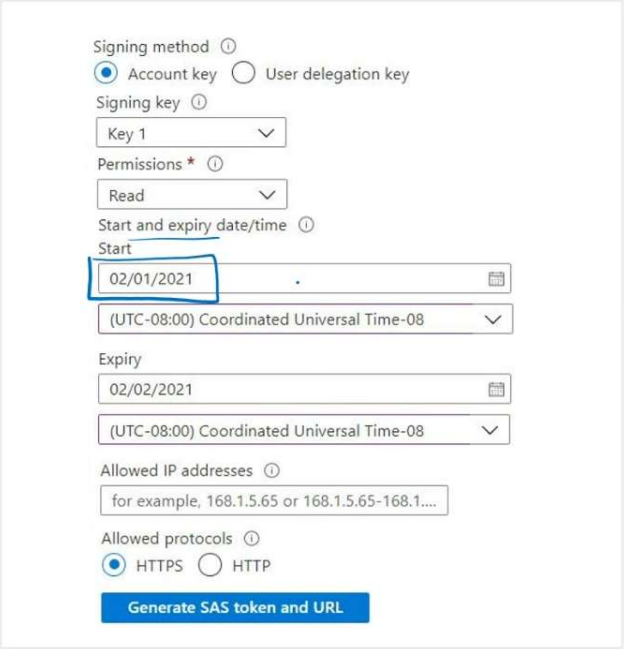
Shared Access Signatures

Provides delegated access to resources

Grants access to clients without sharing your storage account keys

The account SAS delegates access to resources in one or more of the storage services

The service SAS delegates access to a resource in just one of the storage services



Identify Uniform Resource Indicator (URI) and SAS Parameters

- A SAS is a signed URI that points to one or more storage resources
- Consists of a storage resource URI and the SAS token


```
https://myaccount.blob.core.windows.net/?sp=r&st=2020-05-
11T18:31:43Z&se=2020-05-12T02:31:43Z&spr=https&sv=2019-10-
10&sr=b&sig=jOqABJZHfUVeBQ3yVn7kWiCKlO0sxCiK1rzEchfAz8U%3D
```

Includes parameters for resource URI, storage services version, services, resource types, start time, expiry time, resource, permissions, IP range, protocol, signature

Storage Service Encryption

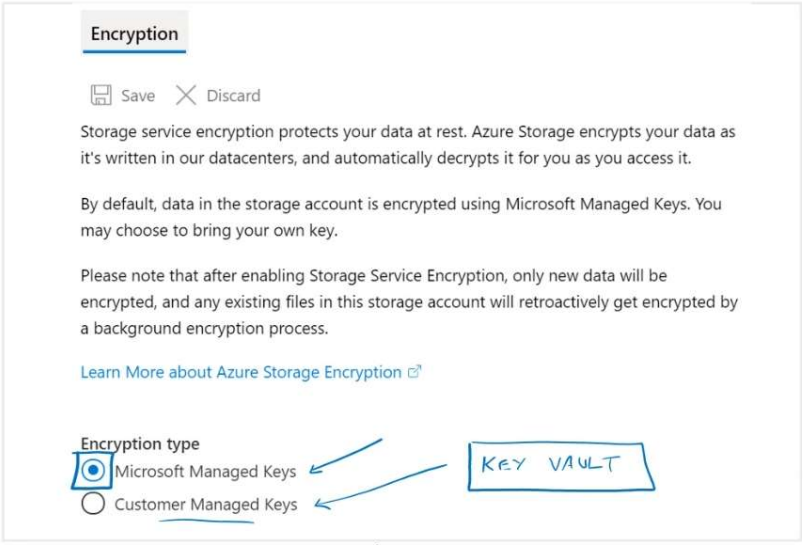
Protects your data for security and compliance

Automatically encrypts and decrypts your data

Encrypted through 256-bit AES encryption

Is enabled for all new and existing storage accounts and cannot be disabled

Is transparent to users



✓ **You can use your own key (next topic)**

Compare Files to Blobs

Feature	Description	When to use
Azure Files	SMB interface, client libraries, and a REST interface that allows access from anywhere to stored files	• Lift and shift an application to the cloud • Store shared data to be accessed across multiple virtual machines • Store development and debugging tools that need to be accessed from many virtual machines
Azure Blobs	Client libraries and a REST interface that allows unstructured data (flat namespace) to be stored and accessed at a massive scale in block blobs	• Support streaming and random-access scenarios • Access application data from anywhere

You need to provide an employee temporary read-only access to the contents of an Azure storage account container named media. It is important that you grant access while adhering to the security principle of least-privilege.
What should you do? Select one.

A) Set the public access level to Container.
B) Generate a shared access signature (SAS) token for the container.
C) Configure a Cross-Origin Resource Sharing (CORS) rule for the storage account.

b

You are planning a delegation model for your Azure storage. The company has issued the following requirement for Azure storage access:
-Apps in the non-production environment must have automated time-limited access.

You need to configure storage access to meet the requirements. What should you do?

A) Use shared access signatures for the non-production apps.
B) Use access keys for the non-production apps.
C) Use Stored Access Policies for the production apps..

a

When configuring network access to your Azure Storage Account, what is the default network rule?

A) To allow all connections from all networks
B) To allow all connection from a private IP address range
C) To deny all connections from all networks

a

Configure Azure Files Introduction

Connect to File Shares

Create File Share Snapshots

→ Azure File Sync (*see below*)

Configure Storage with Tools (*optional*)

Summary and Resources

* File Sync is part of the Learn module but not included here ?

Connect to File Shares

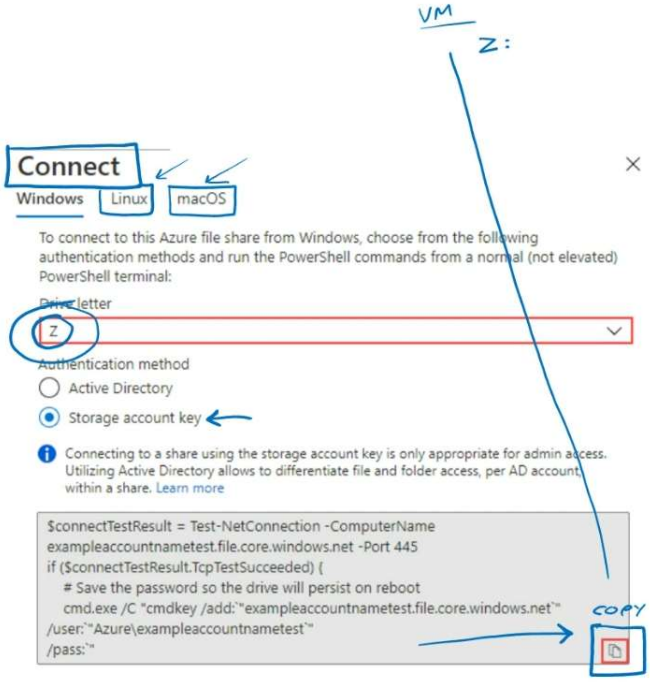
Access across multiple VMs

Windows – ensure port 445 is open

Linux – mount the drive

MacOS – mount the drive

Secure transfer required – SMB 3.0 encryption



Create File Share Snapshots

RSV ← SA

+ Add snapshot ↻ Refresh 🗑 Delete

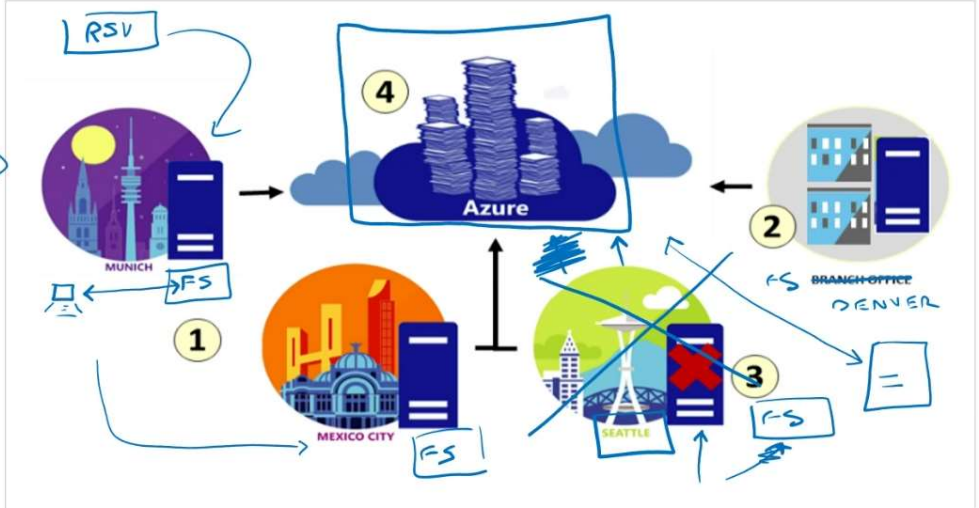
Name	Date created	Initiator
☐ 2020-03-12T00:58:38.0000000Z	3/11/2020, 8:58:38 PM	-

Incremental snapshot that captures the share state at a point in time	Is read-only copy of your data	Snapshot at the file share level, and restore at the file level	• Protection against application error and data corruption • Protection against accidental deletions or unintended changes • General backup purposes

Azure File Sync

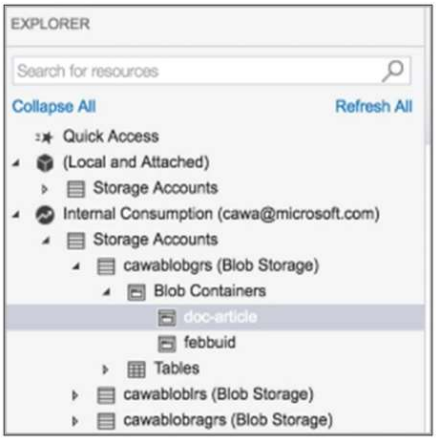
Centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server

1. Lift and shift
2. Branch Office backups
3. Backup and Disaster Recovery
4. File Archiving
5. Cloud Tiering – cache on local server

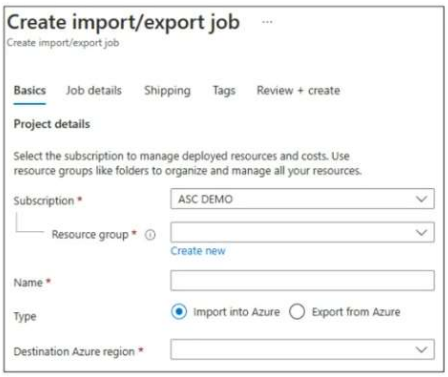


Configure Storage with Tools

Azure Storage Explorer



The Import and Export service



DATA BOX

AZcopy

```
azcopy copy [source] [destination] [flags]
```

Your company is planning to store file data. Company administrators must be able to browse to the data in Storage Explorer. Access over SMB 3.0 must be supported, and the storage must support quotas.
You need to choose the storage type to meet the requirements.
Which storage type should you use? Select one.

A) Azure Files
B) Table storage
C) Blob storage

a

Your company has a file server named FS01. The server has a single shared folder that users' access to shared files. The company wants to make the same files available from other files servers and from Azure. Files deleted should be automatically synchronized. You need to implement a solution to meet the requirements. What should you do? Select one.

A) Install and use AZCopy.
B) Deploy Azure File Sync.
C) Deploy storage tiering.

b

https://docs.microsoft.com/learn/modules/extend-share-capacity-with-azure-file-sync/

https://docs.microsoft.com/learn/modules/implement-hybrid-file-server-infrastructure/

https://docs.microsoft.com/learn/modules/upload-download-and-manage-data-with-azure-storage-explorer/

https://docs.microsoft.com/learn/modules/export-data-with-azure-import-export/

https://docs.microsoft.com/learn/modules/copy-blobs-from-command-line-and-code/

Lab 07- Manage Azure Storage

Lab 07 - Manage Azure Storage - Student lab manual

Lab scenario

You need to evaluate the use of Azure storage for storing files residing currently in on-premises data stores. While majority of these files are not accessed frequently, there are some exceptions. You would like to minimize cost of storage by placing less frequently accessed files in lower-priced storage tiers. You also plan to explore different protection mechanisms that Azure Storage offers, including network access, authentication, authorization, and replication. Finally, you want to determine to what extent Azure Files service might be suitable for hosting your on-premises file shares.

An **interactive lab simulation** is available that allows you to click through this lab at your own pace. You may find slight differences between the interactive simulation and the hosted lab, but the core concepts and ideas being demonstrated are the same.

Objectives

In this lab, you will:

- Task 1: Provision the lab environment
- Task 2: Create and configure Azure Storage accounts
- Task 3: Manage blob storage
- Task 4: Manage authentication and authorization for Azure Storage
- Task 5: Create and configure an Azure Files shares
- Task 6: Manage network access for Azure Storage

Estimated timing: 40 minutes

Architecture diagram