Microsoft

Microsoft Learn
Spark possibility

Thomas Jäkel

brainymotion

Lead Trainer Cloud Infrastructure

Microsoft Certified Trainer since 1999

github.com/www42/az-900

Let’s have a great time together

We all contribute to a great class

$9^{00} - 17^{00}$

$12^{30} - 13^{30}$

What you should know about our facilities

Microsoft

Microsoft Applied Skills

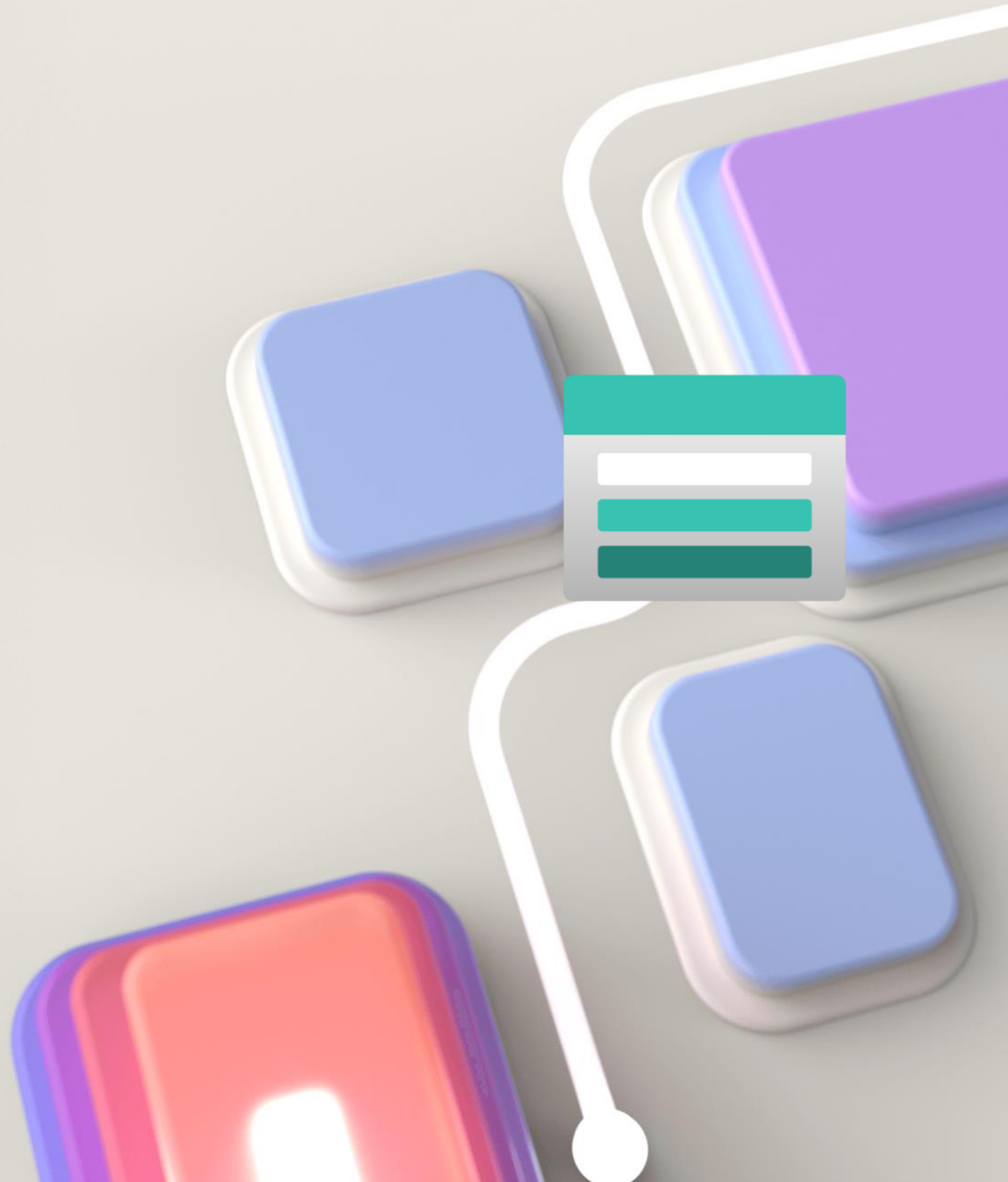
AZ-1003

Secure storage for Azure Files and Azure Blob Storage

Secure storage for Azure Files and Azure Blob Storage credential

Create and configure a storage account	Create and configure Blob Storage	Create and configure Azure Files	Configure networking for storage	Configure encryption for storage
• Configure the appropriate storage account tier (standard versus premium) • Configure redundancy settings • Configure secure transfer and TLS version • Configure replication	• Create a Blob Storage container • Configure access level for Blob Storage • Configure the Blob Storage tiers • Configure lifecycle management • Configure data protection for Blob Storage	• Create an Azure Files share • Configure performance tiers • Configure data protection for Azure Files	• Create and configure private endpoints • Create and configure service endpoints • Configure Azure Storage firewalls and virtual networks	• Configure encryption for data at rest, including Microsoft managed keys and customer managed keys • Configure encryption for data in transit

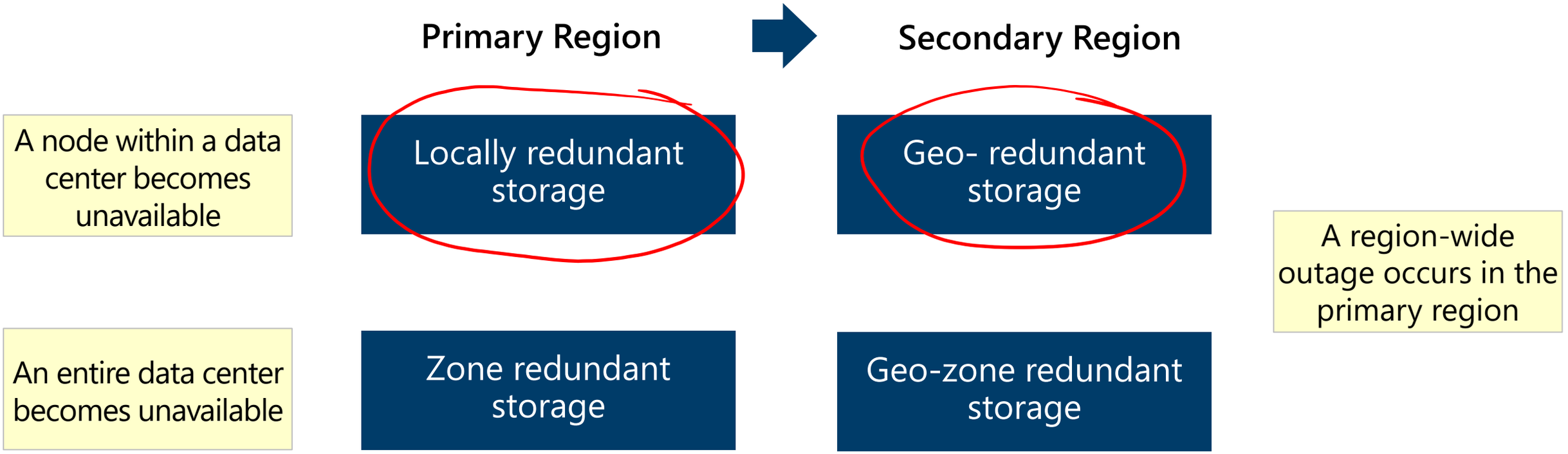
Create and configure storage accounts



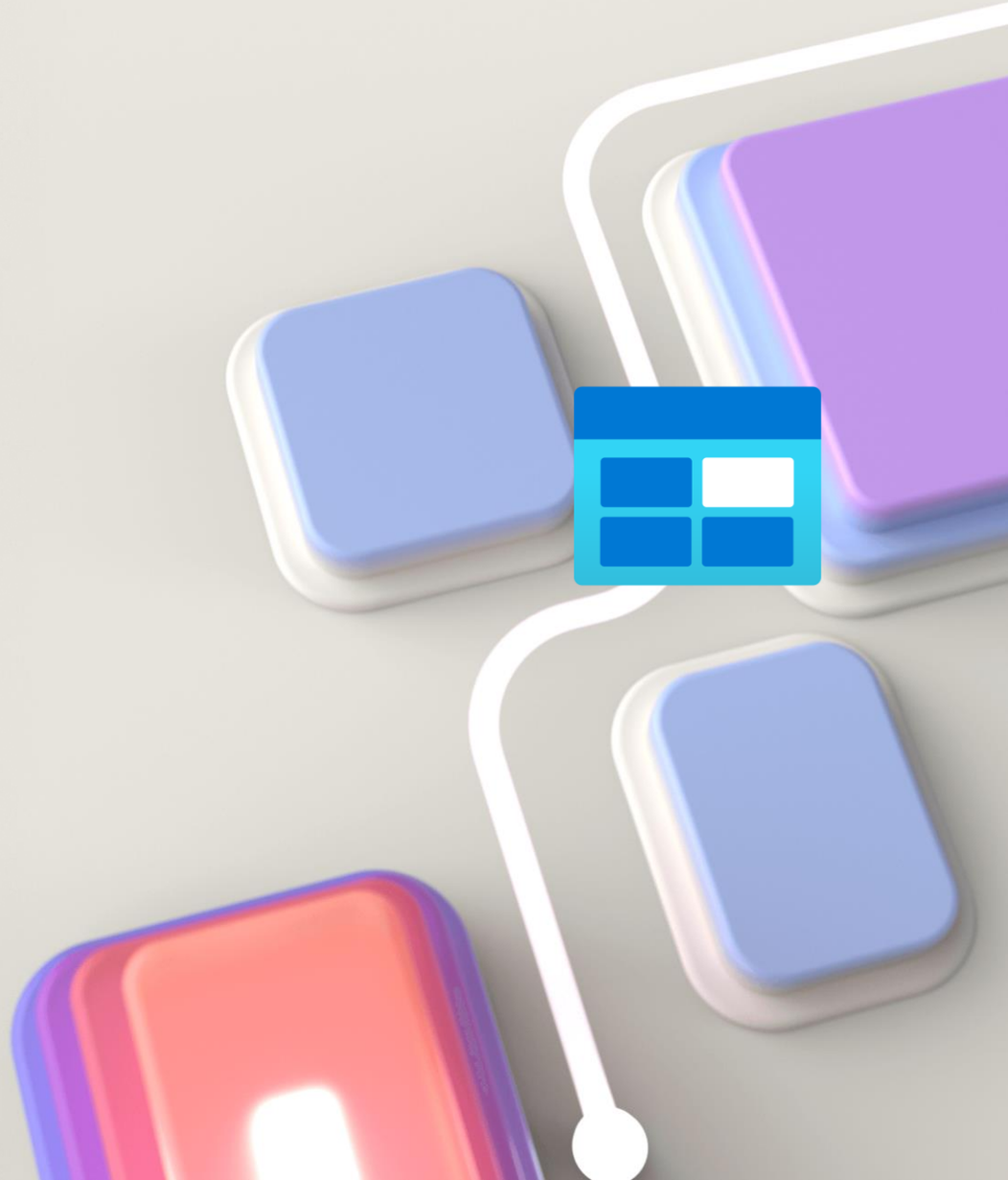
Should you use a standard or premium storage account?

Storage Account	Recommended usage
Standard general-purpose v2	Most scenarios including Blob, File, Queue, Table, and Data Lake Storage.
Premium block blobs	Block blob scenarios with high transactions rates, or scenarios that use smaller objects or require consistently low storage latency.
Premium file shares	Enterprise or high-performance file share applications.
Premium page blobs	Premium high-performance page blob scenarios.

What level of redundancy do you require?



Create and configure blob storage



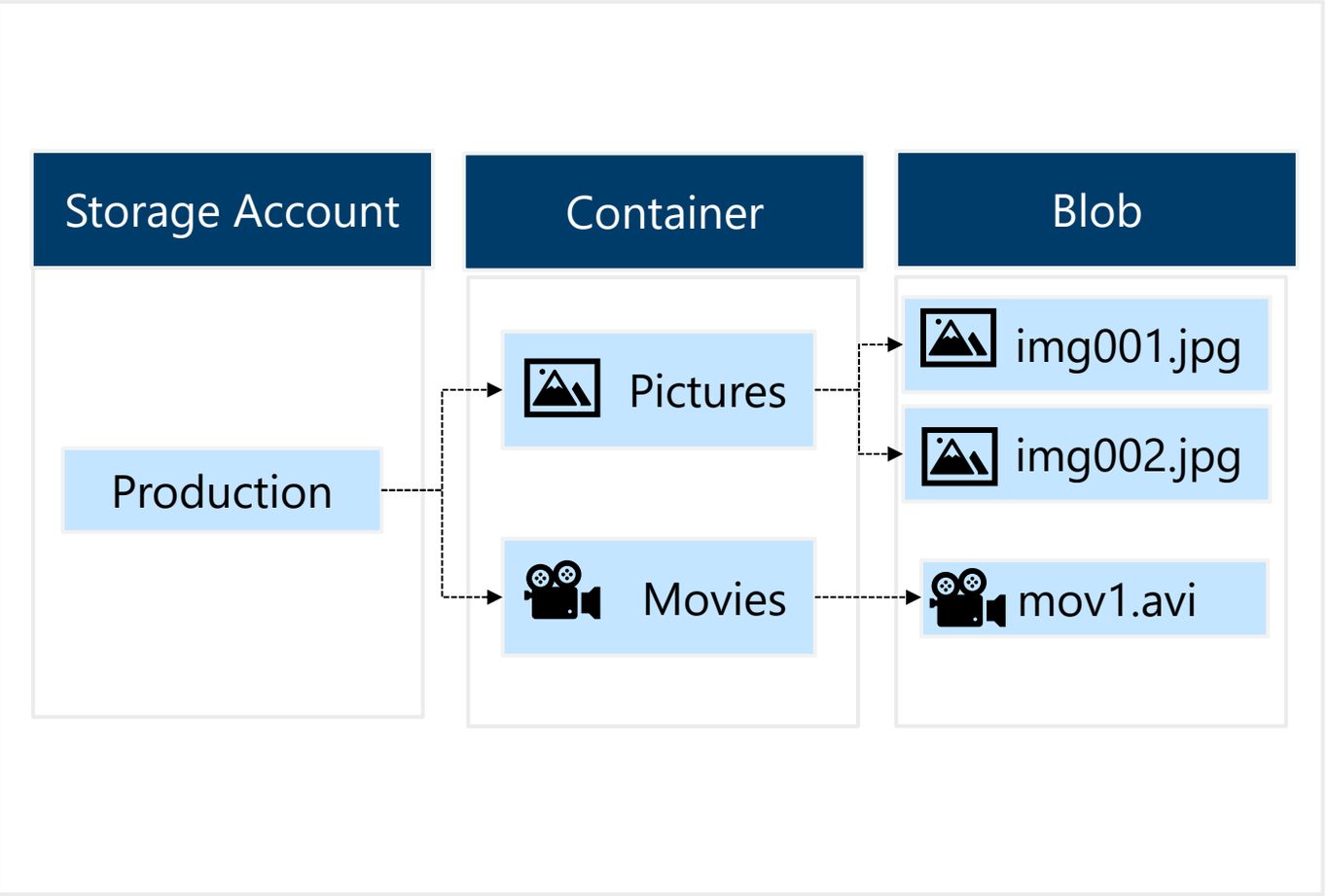
What is blob storage?

Stores unstructured data in the cloud

Can store any type of text or binary data

Common uses:

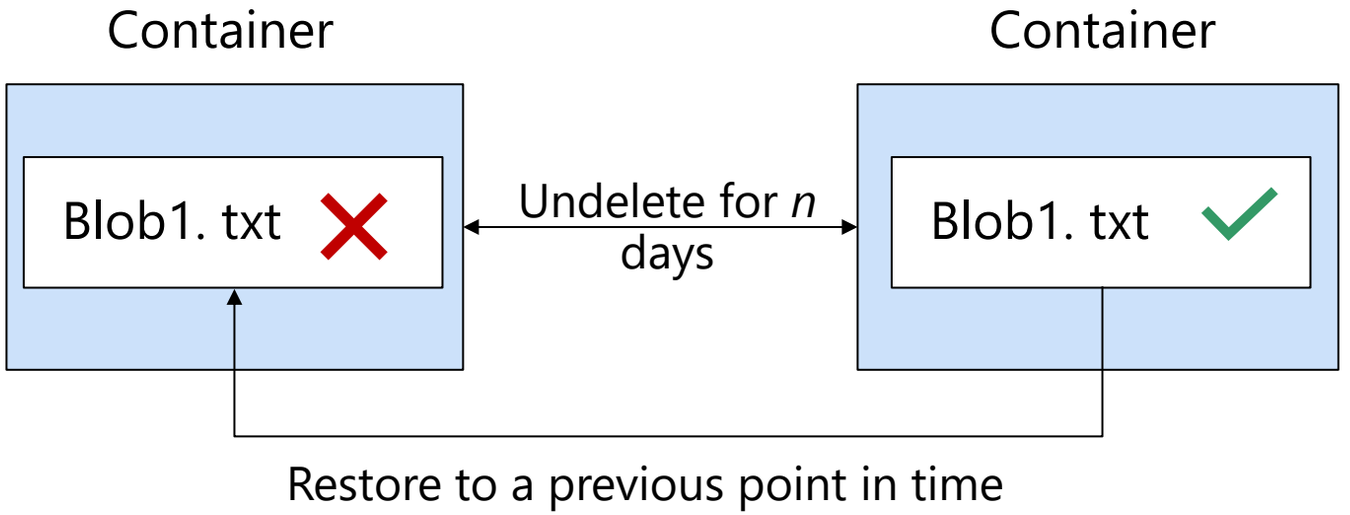
- Serving images or documents directly to a browser
- Storing files for distributed access
- Streaming video and audio
- Storing data for backup and restore, disaster recovery, or archiving
- Storing data for analysis



Which blob storage tier do you require?

Tier	Recommended retention	Optimized for
Standard Hot	N/A	• Data that is accessed or modified frequently.
Standard Cool	Minimum of 30 days	• Data that is infrequently accessed or modified.
Standard Cold	Minimum of 90 days	• Data that is infrequently accessed or modified.
Standard Archive	Minimum of 180 days	• Data that is rarely accessed, and that has flexible latency requirements, on the order of hours.

What is soft delete?



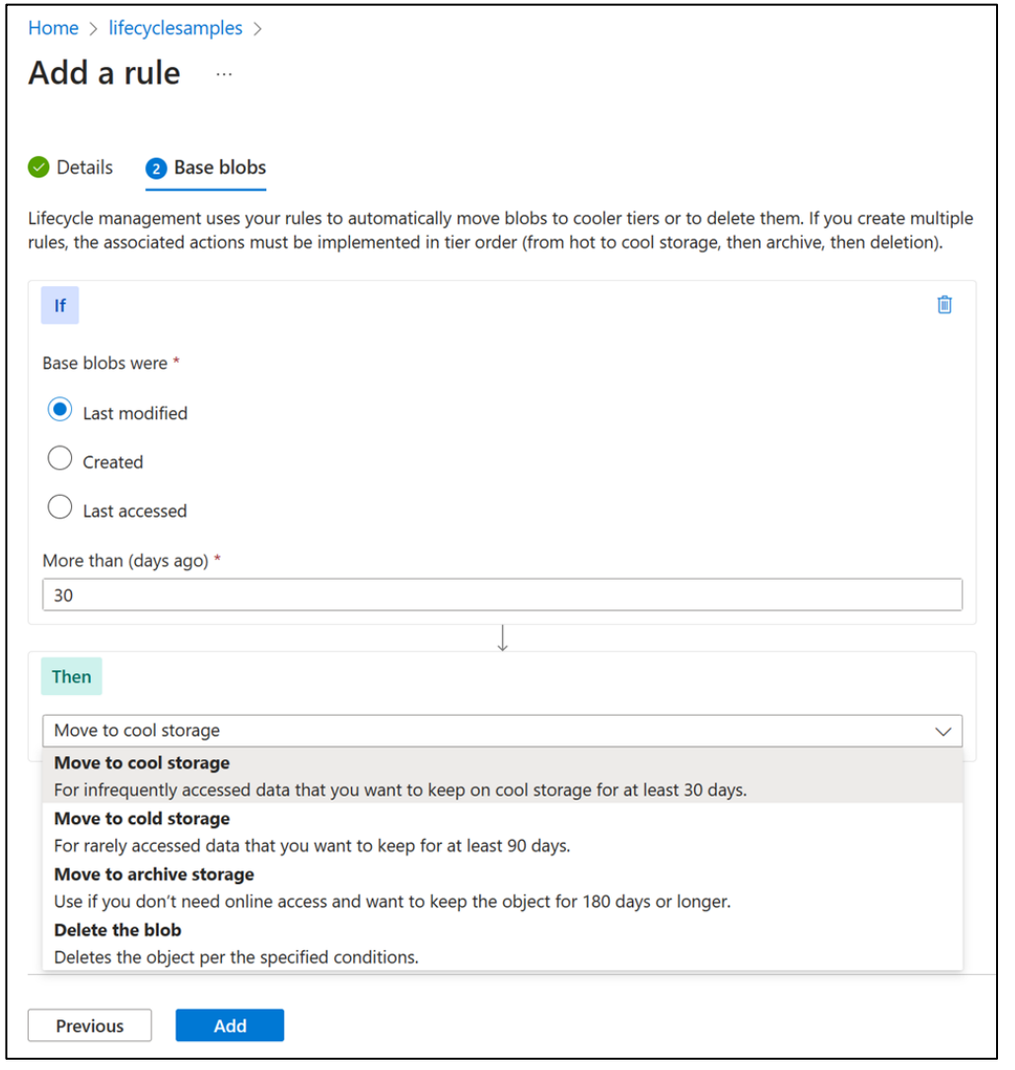
Scoped to either the container or blob level

Retention period: 1 to 365 days

Permanently deleted after the retention period

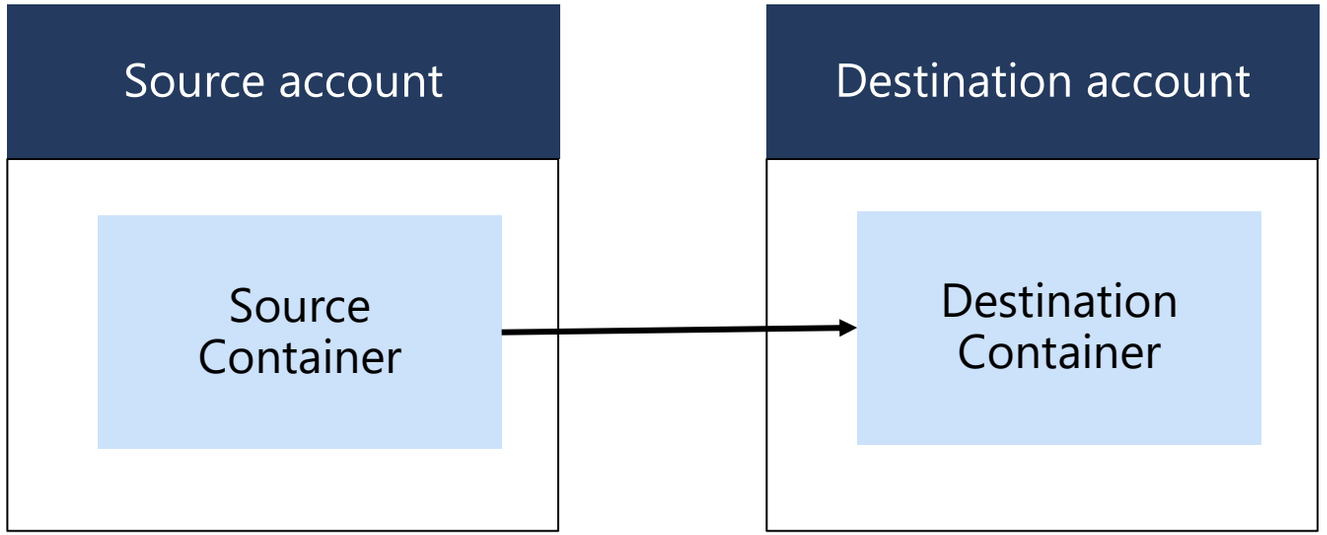
When to use blob lifecycle management policies?

- Optimize costs by automatically managing the data lifecycle
- Transitions blob data to the appropriate access tiers or expires data at the end of the data lifecycle
- Composed of one or more rules that define a set of actions to take based on a condition
- Optionally applies to blob versions and snapshots



What is blob object replication?

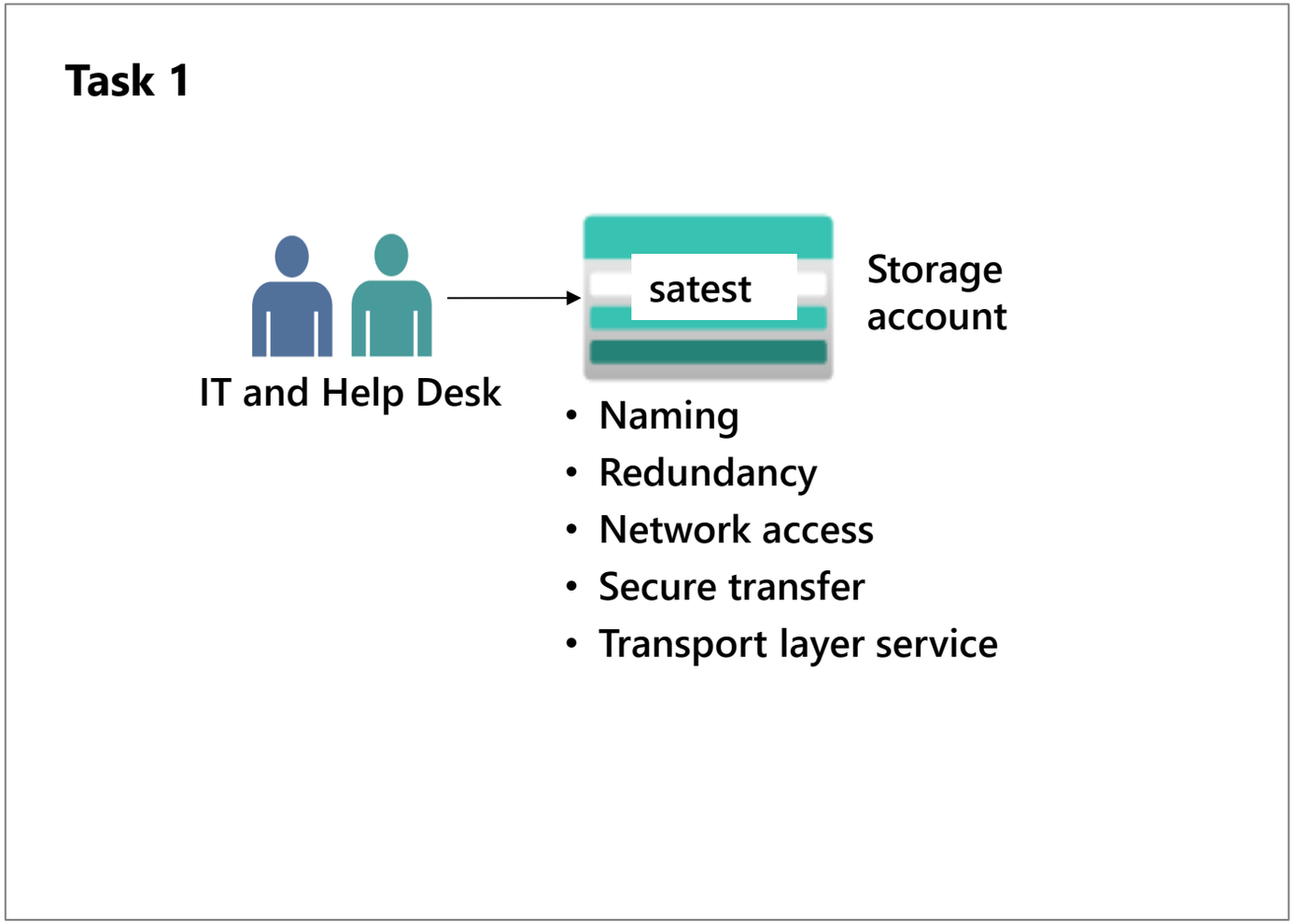
- Asynchronous to any other Region
- Minimizes latency for read requests
- Increases efficiency for compute workloads
- Optimizes data distribution
- Optimizes costs



Lab 1: Provide storage for the IT department testing and training

Skilling tasks:

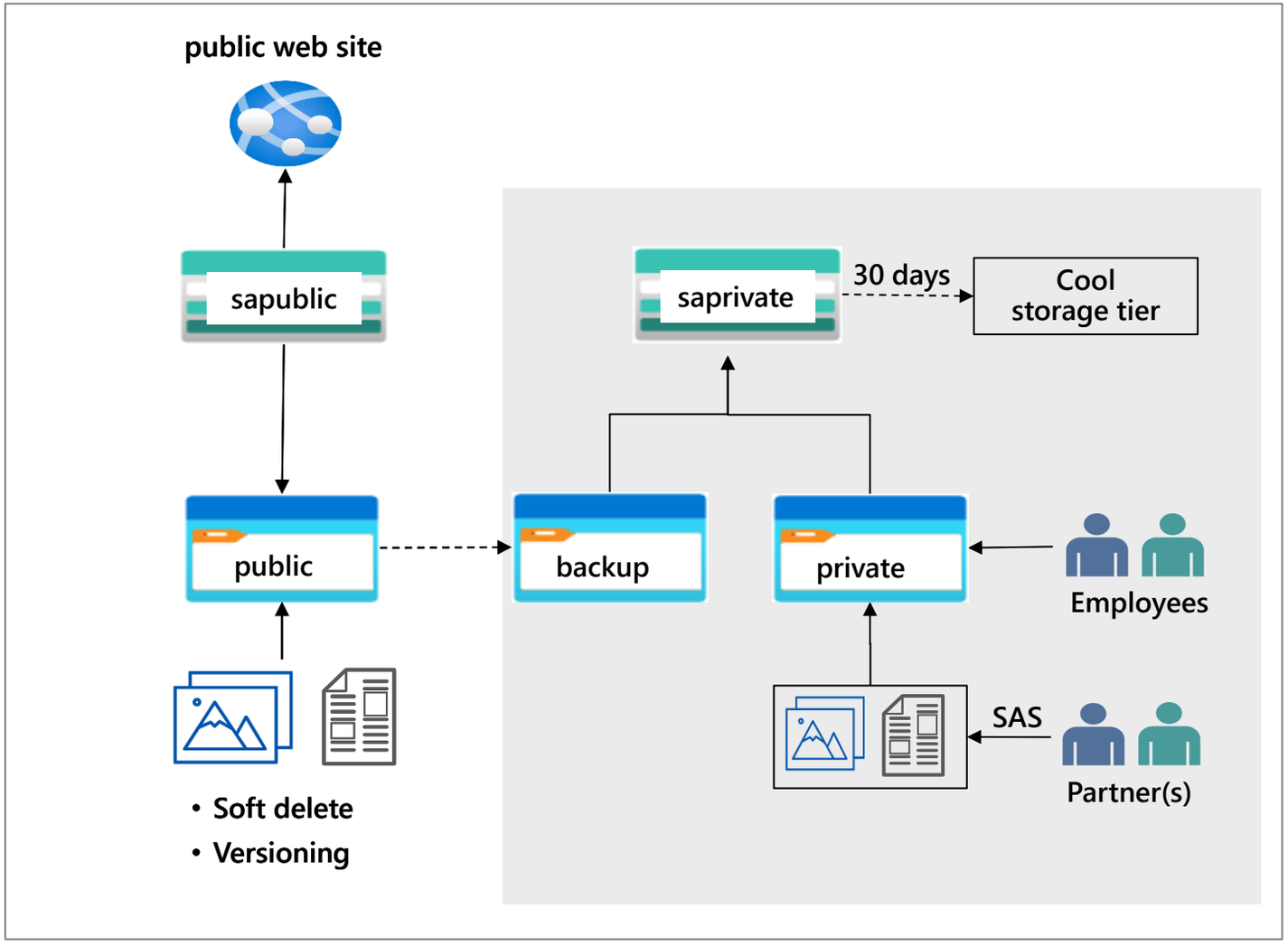
- ❑ Navigating the portal
- ❑ Storage account naming
- ❑ Performance options
- ❑ Redundancy options
- ❑ Network access options
- ❑ Secure transfer
- ❑ Transport layer security



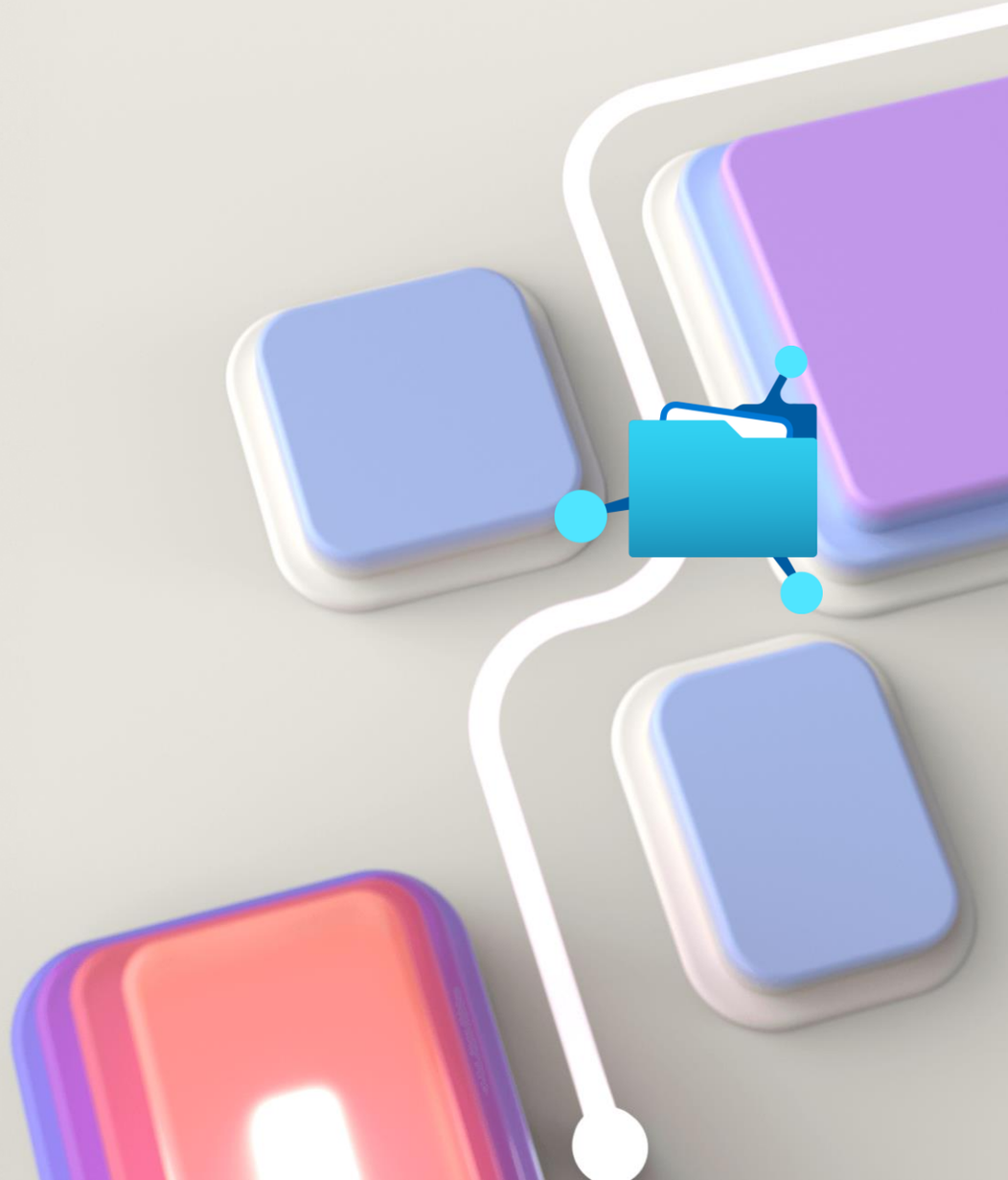
Lab 2: Provide storage for the public website and provide private storage for internal company documents

Skilling tasks:

- ❑ Configure private access to a storage account
- ❑ Provide partners limited access to specific documents
- ❑ Automatically move documents between storage tiers
- ❑ Backup the public website documents – asynchronous replication



Create and Configure Azure Files and Networking



How are Azure Files different from Azure blobs?

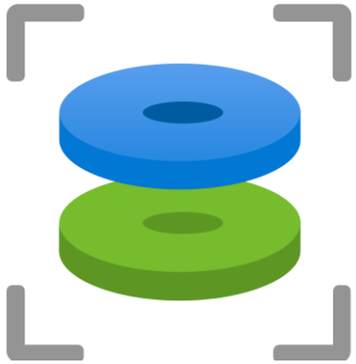
Feature	Description	When to use
Azure Files	Distributed cloud-based file system. SMB/NFS interface, client libraries, and a REST interface that allows access from anywhere to stored files.	• Lift and shift an application to the cloud • Store shared data across multiple virtual machines • Store development 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. Accessed at a massive scale in block blobs.	• Support streaming and random-access scenarios • Access application data from anywhere

Which Azure Files tier do you need?

Share type	Tier	Description
Premium (SSD)	Premium	• High I/O-intensive workloads, with high throughput and low latency. • Best for the most demanding file share workloads.
Standard (HDD)	Transaction optimized	• Transaction-heavy workloads that don't need the consistently low latency offered by premium file shares. • Best for applications that require file storage or backend storage.
Standard (HDD)	Hot	• Optimized for general purpose file sharing • Best for team shares.
Standard (HDD)	Cool	• Cost-efficient storage optimized for online archive storage scenarios. • Best for data at rest.

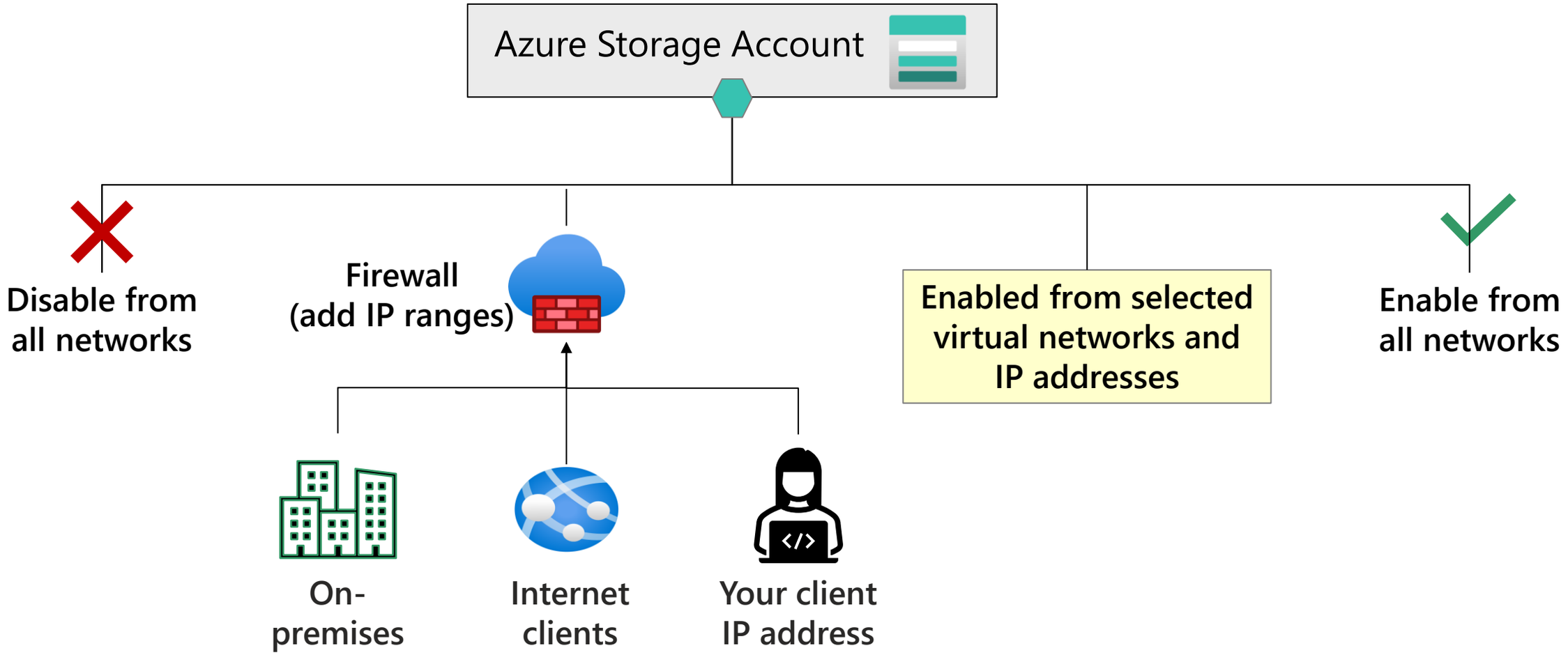
Why create a file share snapshot? (optional)

Captures the file share state at a point in time



- Read-only copy of your data
- Snapshot at the file share level
- Restore at the file level
- Protect against application error and data corruption
- Protect against accidental deletions or unintended changes
- Use for general backup purposes

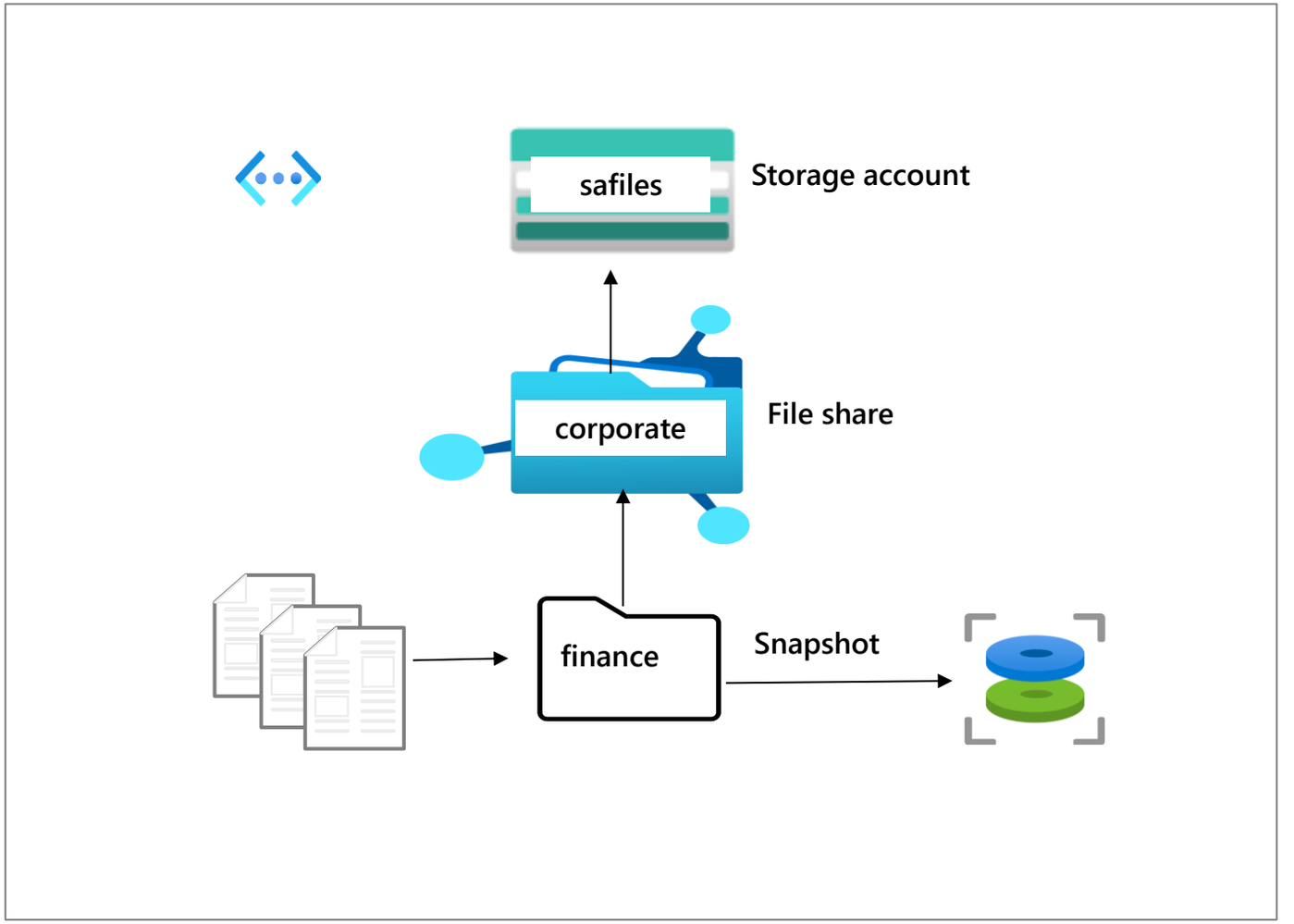
How to control public network traffic to the storage?



Lab 3: Provide shared file storage for company offices

Skilling tasks:

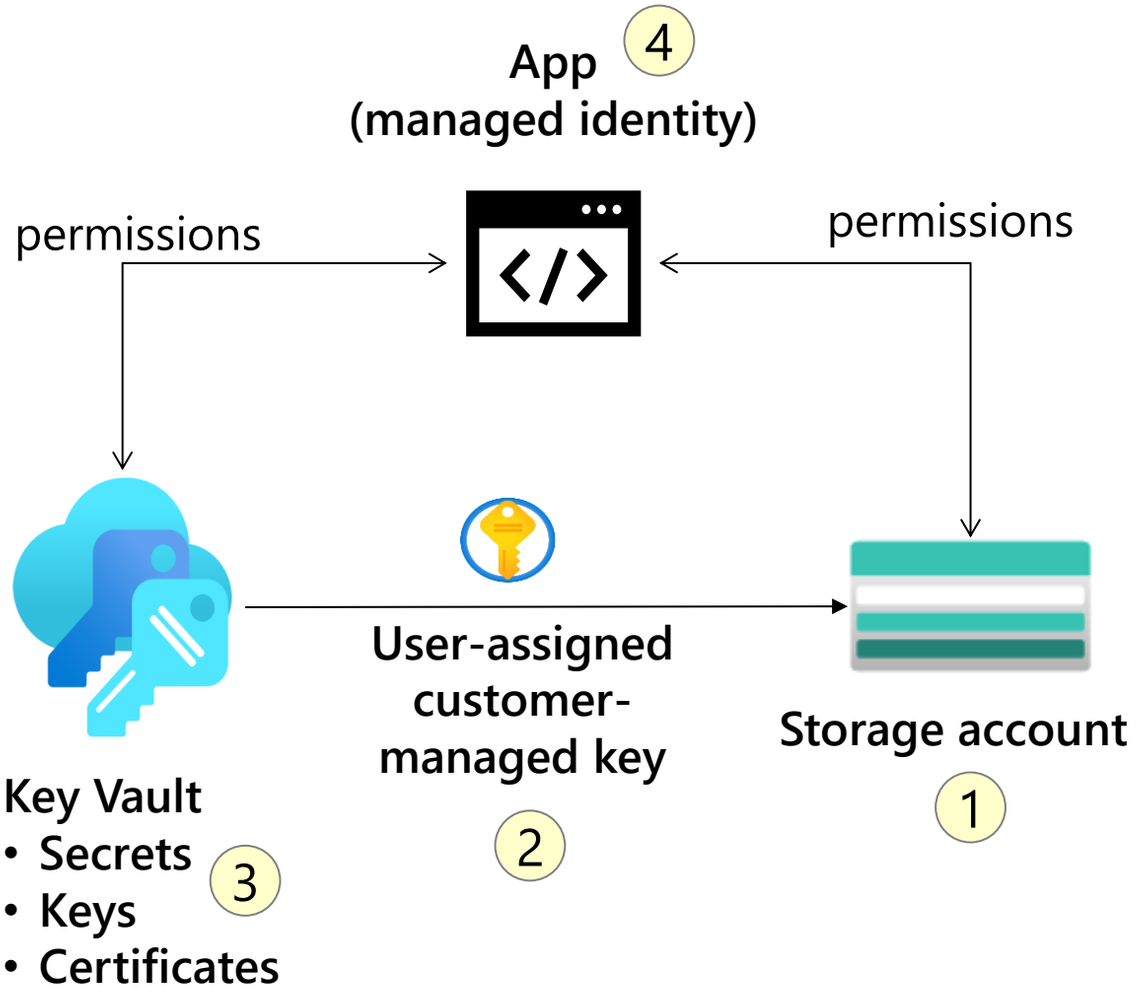
- ❑ Create an Azure file share
- ❑ Create a file share directory
- ❑ Create snapshots to backup and restore the data
- ❑ Secure access to the data to a specific virtual network
- ❑ Use Storage Browser (optional)



Configure encryption and secure access

How is encryption and secure access handled?

1. Data at rest is automatically encrypted and decrypted using keys.
2. Customers can create keys – this avoids providing the key in the app code.
3. Keys can be stored in software (key vault) or hardware (HSM).
4. A managed identity, with the correct permissions, can use the key to access storage.



How to assign permissions?

Assignment type
- ✓ Job function
- • Administrator

Role
- ✓ Built-in
- • Custom

Assignment
- • User, group, service identity
- ✓ Managed identity

Built-in Role Examples	Description
Storage Blob Data Owner	Allows for full access to blob containers
Storage Blob Data Contributor	Allows for read, write and delete access to blob containers and data
Storage Blob Data Reader	Allows for read access to blob containers and data

When to use immutable storage policies?

- Apply immutable storage policies at the container level
- Use **time-based retention policies** for business-critical data
- Use **legal-hold policies** for sensitive information to ensure a tamper proof state
- Policies apply only to new content

Time-based retention polices	Legal hold policies
Blob write and delete operations **prohibited for the duration of the retention policy**	Blob write and delete operations **prohibited until the legal hold is cleared**

What is an encryption scope and infrastructure encryption?

Scopes can be managed at the container or individual blob level

Encryption scopes enable you to manage encryption with a key that is scoped to a container or an individual blob

Infrastructure encryption provides a secondary level of encryption - enables double encryption of data

Uses 256-bit AES encryption

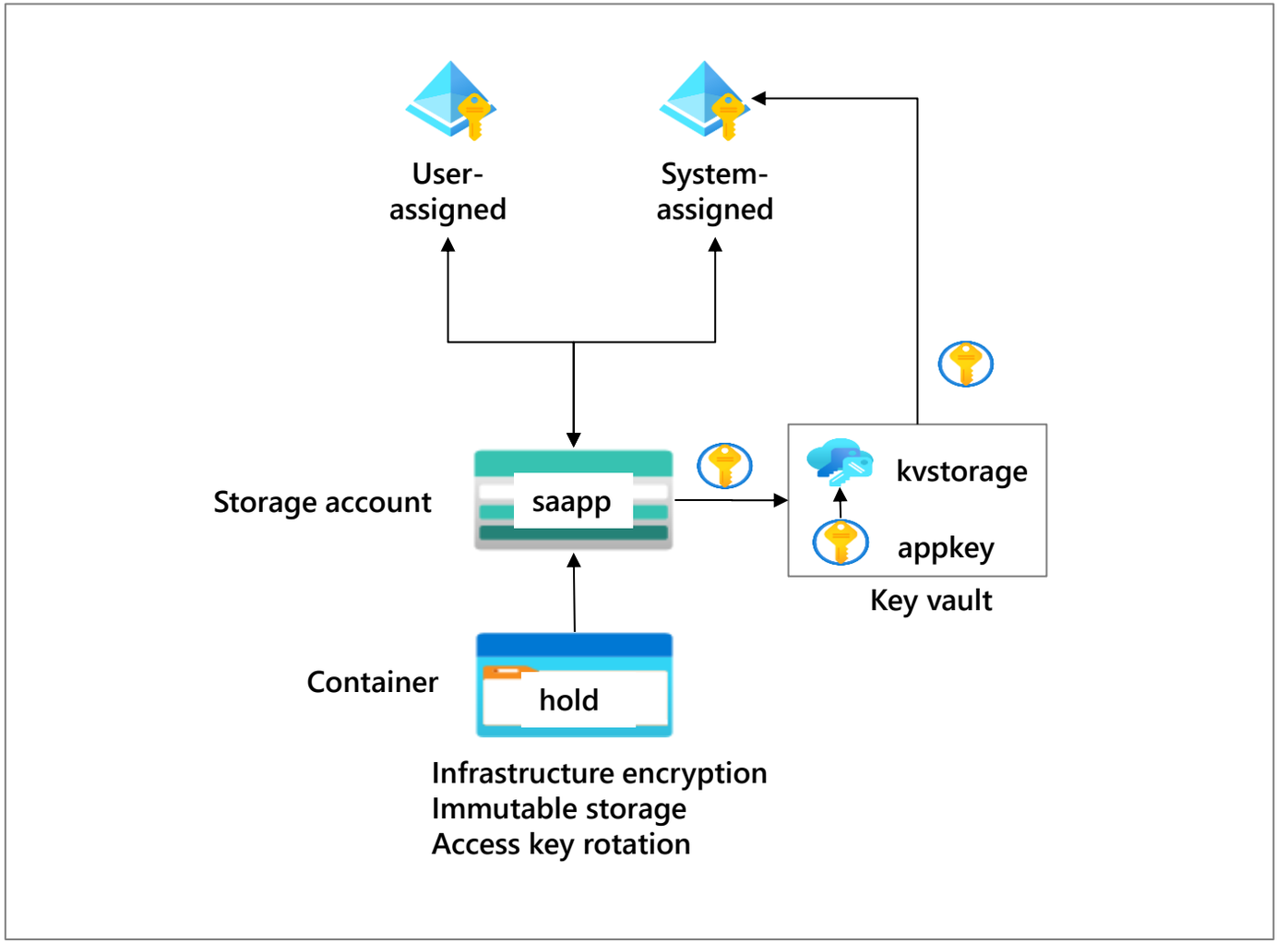
Service level encryption (default)

Infrastructure level encryption (optional)

Lab 4: Provide storage for a new company app

Skilling tasks:

- ❑ Create a user-assigned identity
- ❑ Create a system-assigned identity
- ❑ Create a key vault and key for the storage account
- ❑ Determine and assign role-based permissions
- ❑ Create an encryption scope for infrastructure encryption
- ❑ Create a time-based immutable storage policy



End of presentation