Microsoft

Tag 2

Applied Skills!

Azure Implement & Manage

Guten Morgen!

Azure - Implement & Manage (Applied Skills)

AZ-1002
Configure secure access to your workloads using Azure virtual networking

AZ-1003
Secure storage for Azure Files and Azure Blob Storage

AZ-1004
Deploy and configure Azure Monitor

AZ-1007
Deploy and administer Linux virtual machines on Azure

44 andere

No Assessment

Microsoft

AZ-1003
Secure storage for Azure Files and Azure Blob Storage

Introduction to the course scenario – business group requirements

IT department (test and training)

- The IT department needs storage so they can test different scenarios.
- They also need to train new Help Desk personnel on how to configure storage.

Marketing (public website)

- The Marketing team needs storage for the public website.
- The website provides images, videos, and product literature.

Company offices (private)

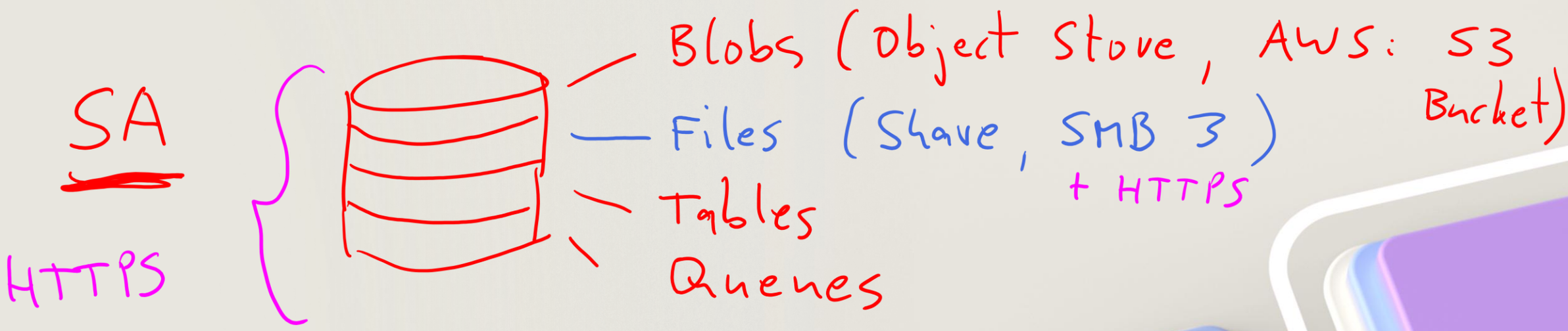
- The corporate office needs private storage for day-to-day business documents.
- Business partners may need access to this content.

Finance (file sharing)

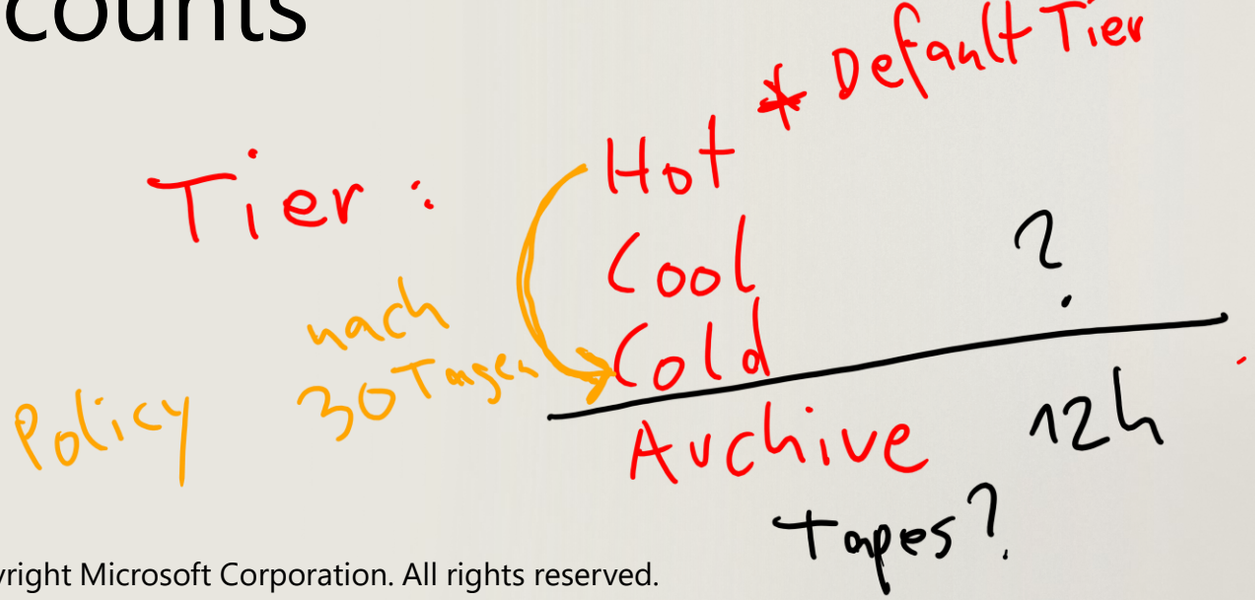
- The company offices are located worldwide.
- Need file storage to efficiently share information.

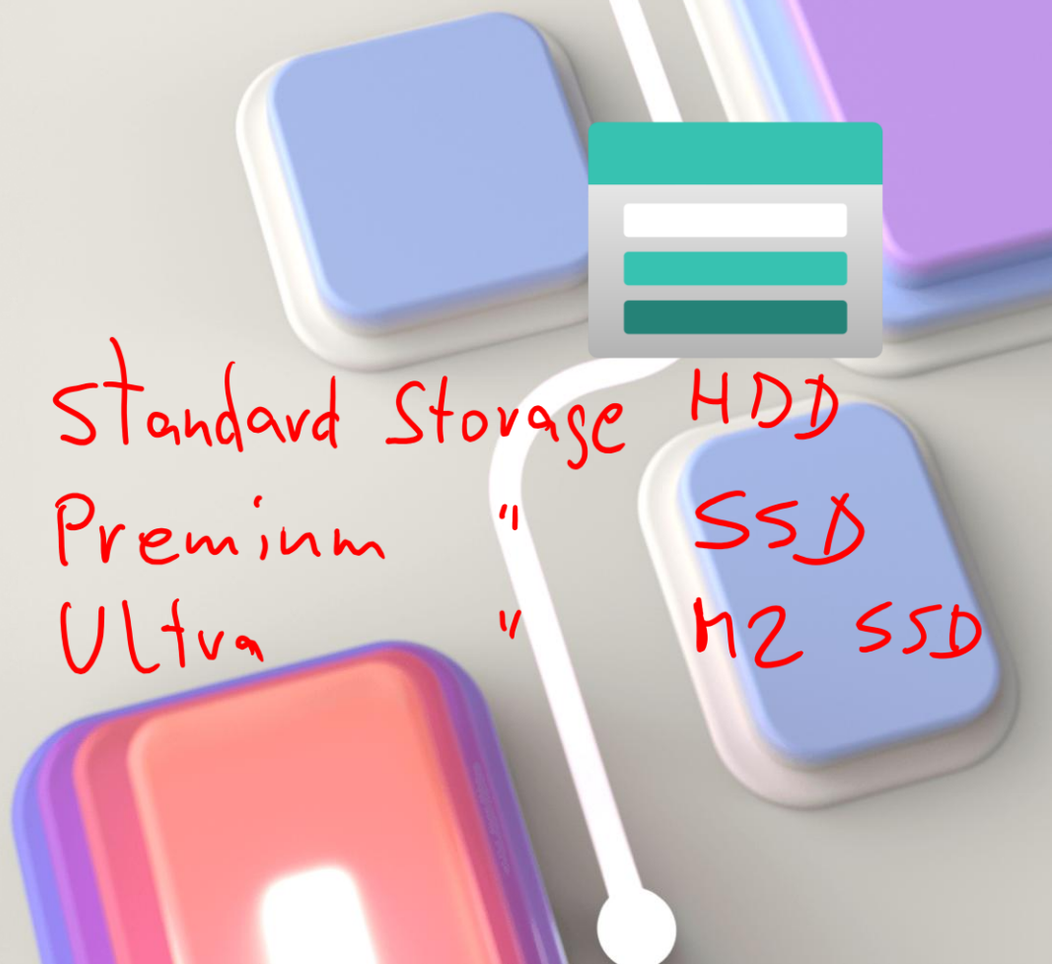
Developers (apps)

- Developers need storage for new apps.
- There needs to be a secure way of accessing that storage.



Create and configure storage accounts



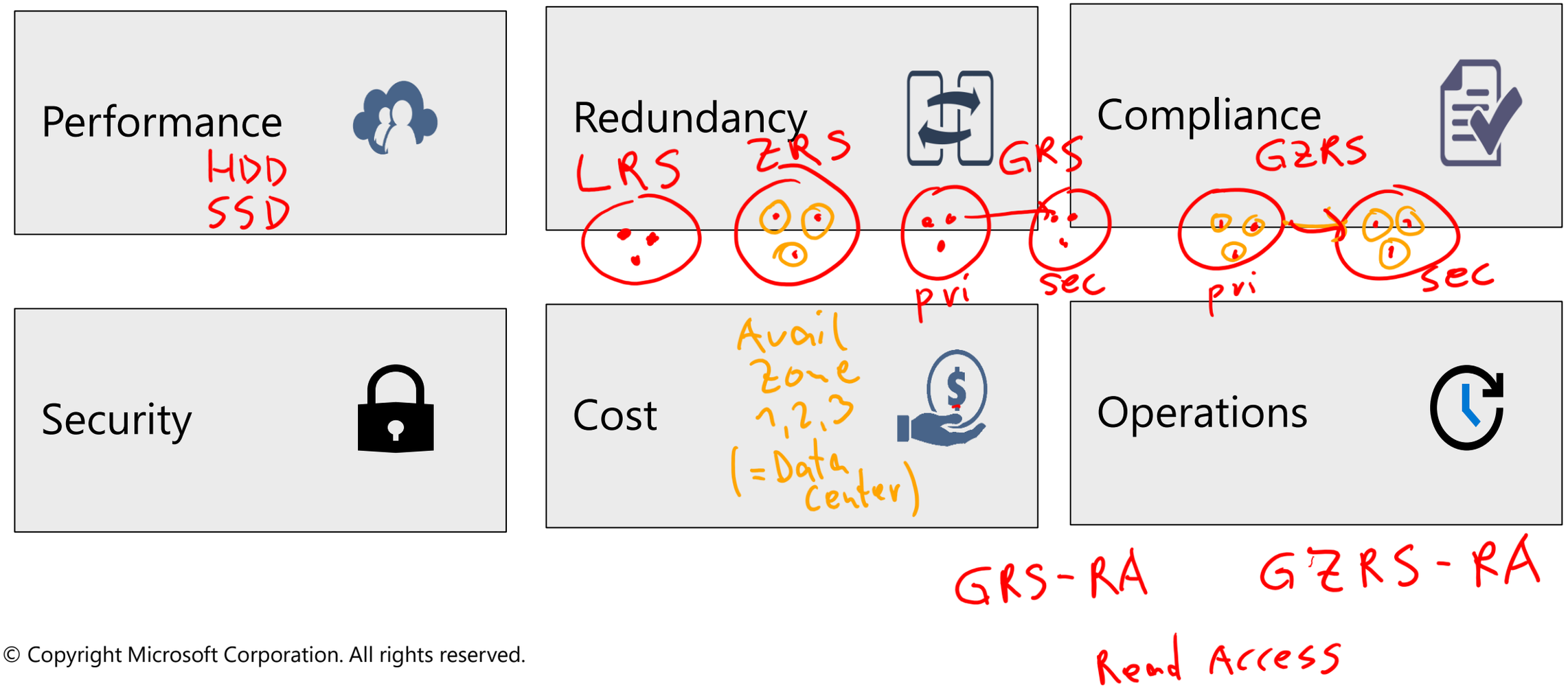


Agenda – Create and configure a storage account

- What are storage accounts?
- Instructor demonstration
  - Should you use a standard or premium storage account?
  - What level of redundancy do you need?
- Student exercise: Provide storage for test and development
- Review questions and reference module

What are storage accounts?

Your Azure unstructured storage is organized into storage accounts



Instructor demonstration: Storage accounts

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

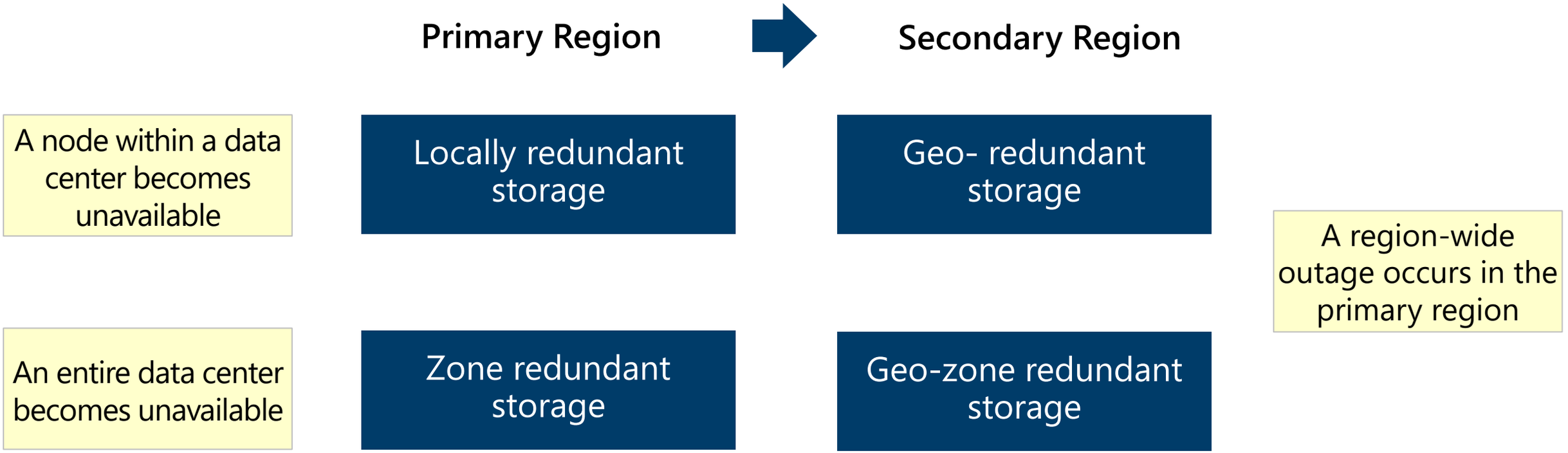
IT department (test and training)

- The IT department needs storage so they can test different scenarios.
- They also need to train new Help Desk personnel on how to configure storage.

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.

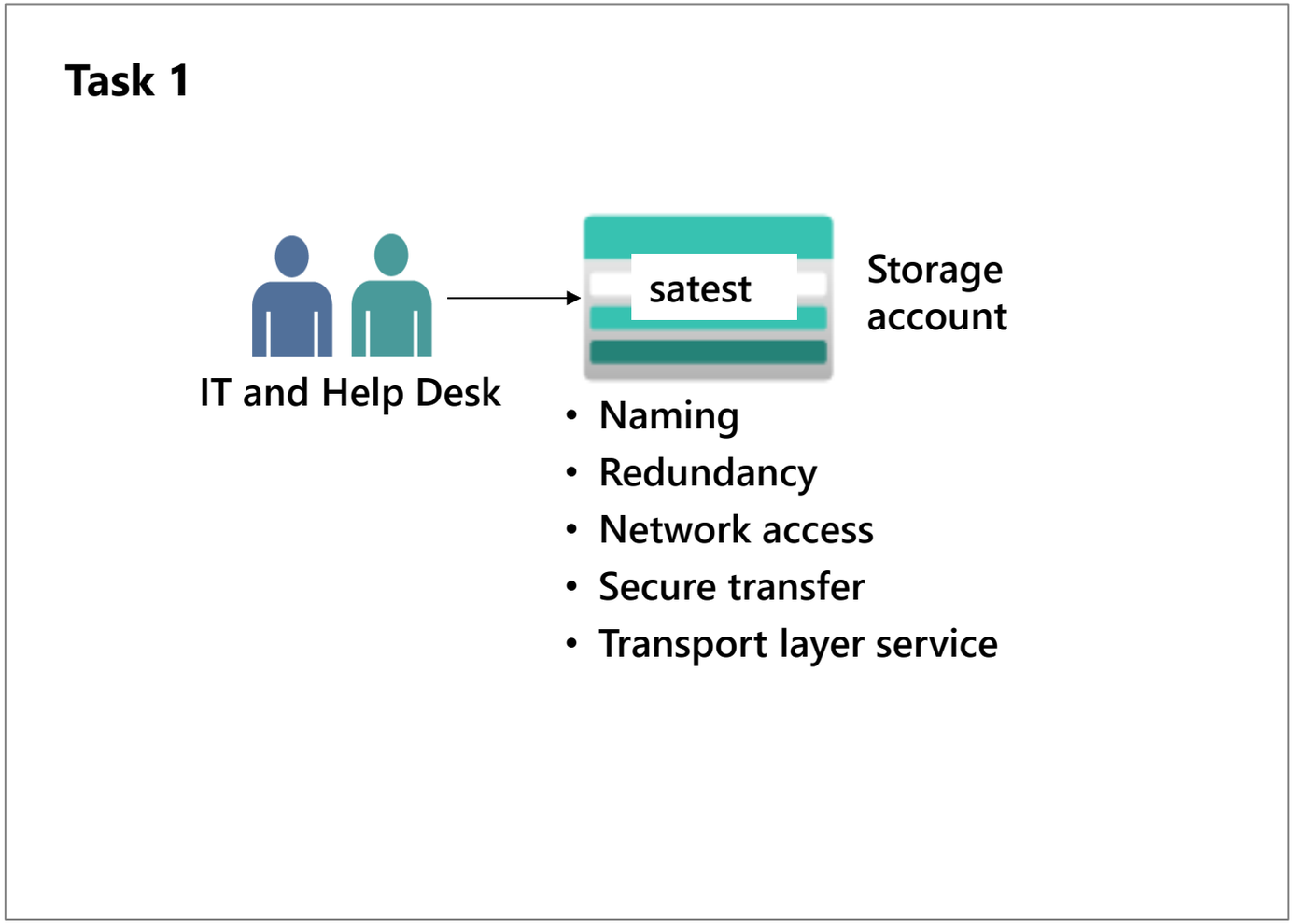
What level of redundancy do you require?



Student exercise: Provide storage for test and development

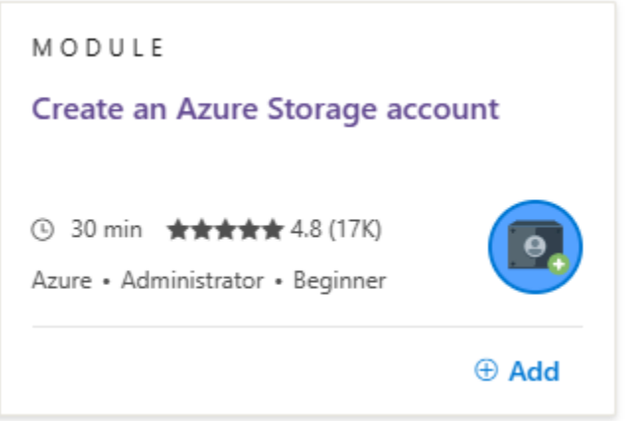
Skilling tasks:

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



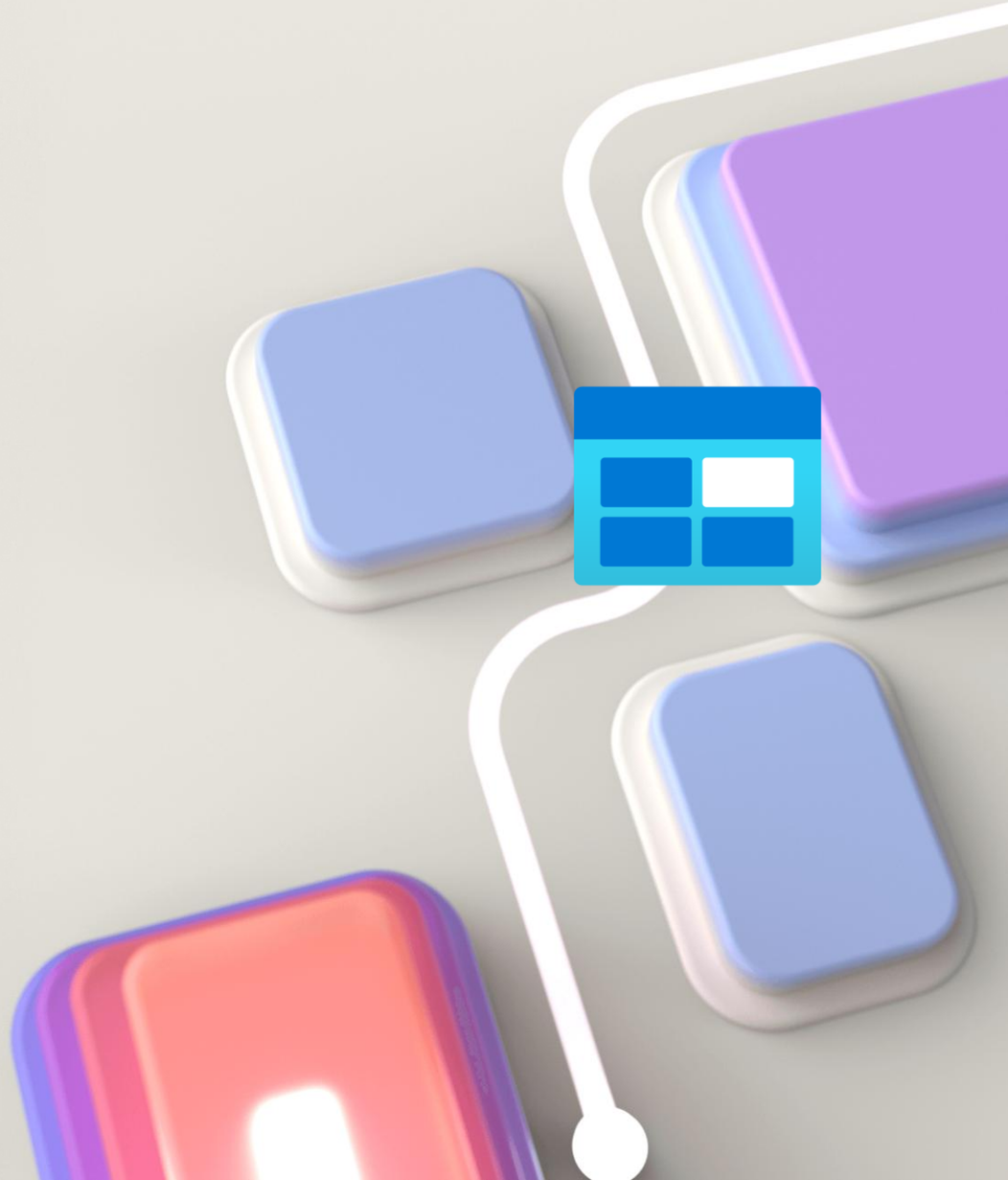
Review questions and reference module – Storage Accounts

1. How will you decide how many storage accounts you need?
2. List the two basic types of storage accounts
3. Which redundancy option provides failover in the event of a primary region outage?
4. Your organization requires HTTPS connections to Azure storage. What should you do?
5. What level of access do storage account keys provide?



This module has a **sandbox**

Create and configure blob storage



Agenda – Blob Storage

- What is blob storage?
- Instructor demonstration: Blob Storage
  - Which blob storage tier do you need?
  - When to use blob lifecycle management policies?
  - What is blob object replication?
- Student exercise: Provide storage for the public website
- Student exercise: Provide storage for the company documents
- Review questions and reference module

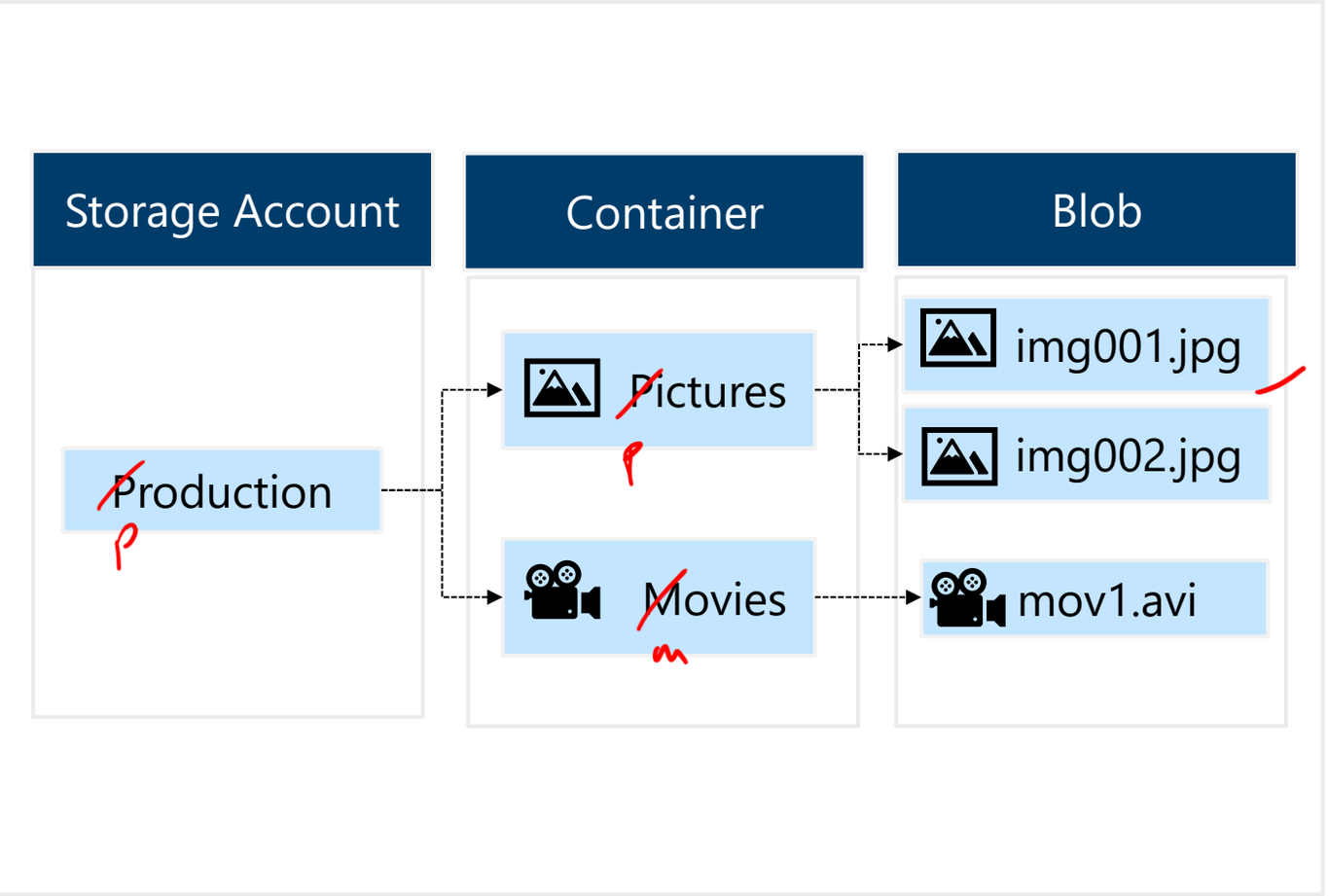
What is blob storage?

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



Instructor demonstration: Blob Storage

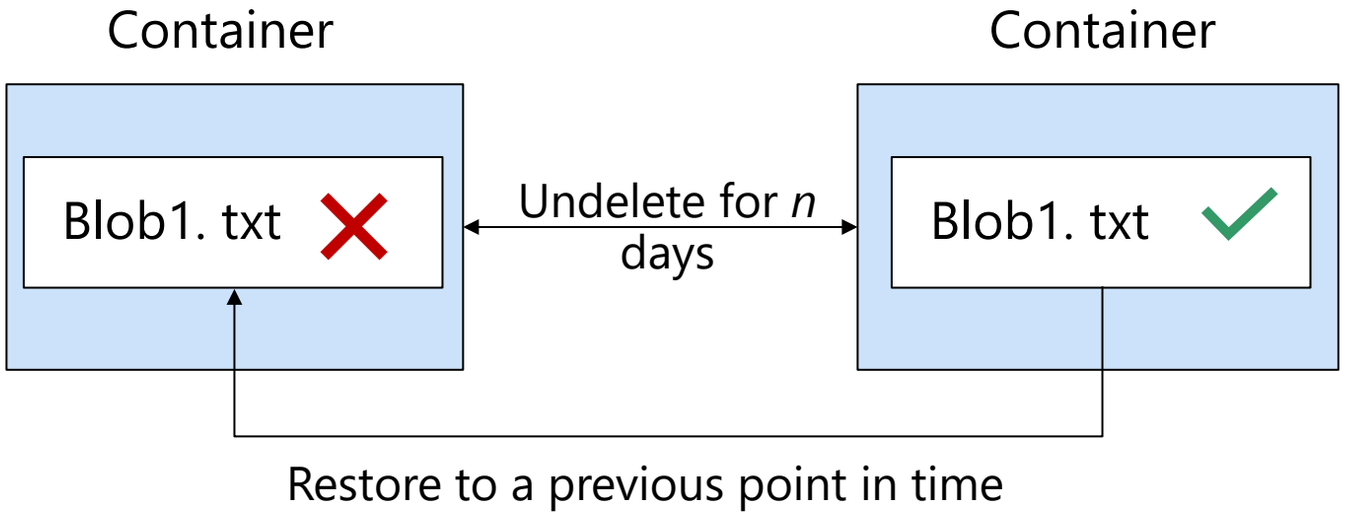
- Creating blob containers
- Enabling soft delete
- Enabling blob versioning
- Providing public and private access to documents
- Automatically move documents between access tiers
- Backing up storage documents
- Providing partners limited access to specific documents
- Replicating data across storage accounts

Marketing (public website)	Company offices (private)
• The Marketing team needs storage for the public website. • The website provides images, videos, and product literature.	• The corporate office needs private storage for day-to-day business documents. • Business partners may need access to this content.

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?



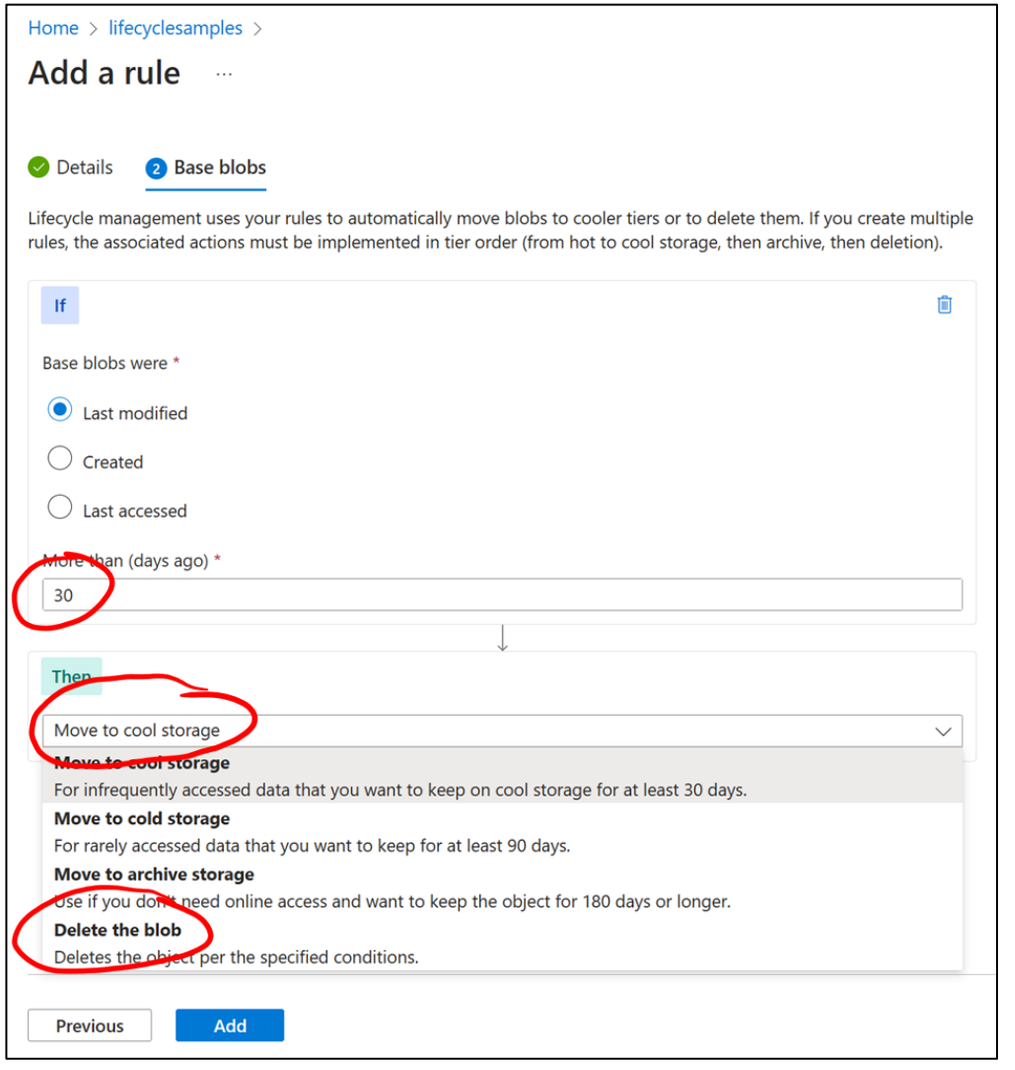
Scoped to either the container or blob level

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?

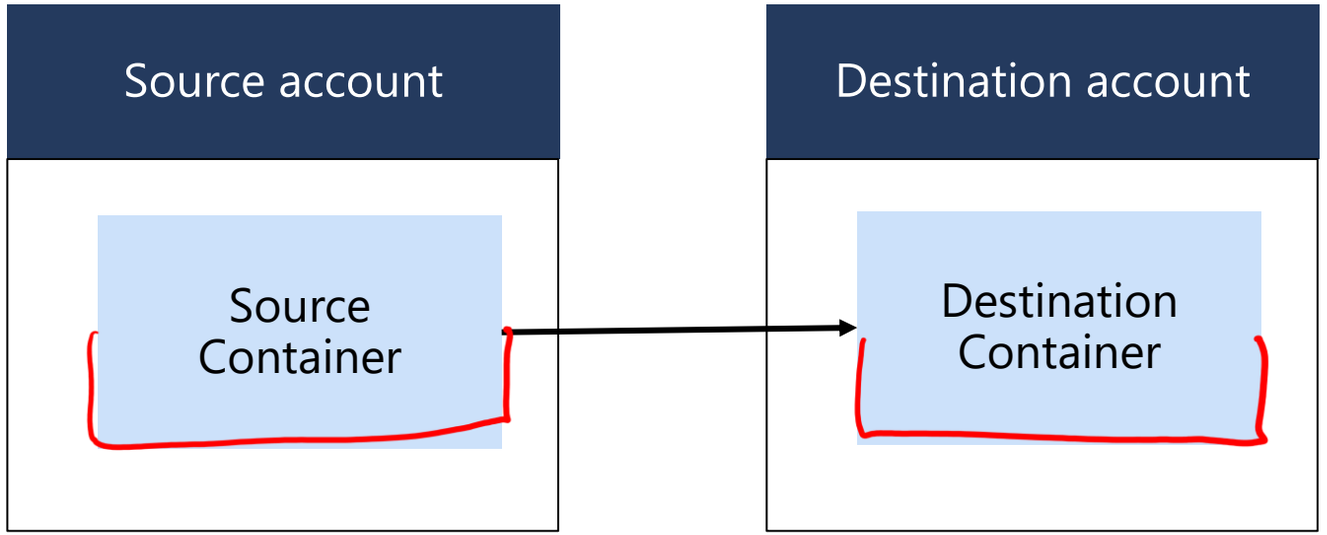
Asynchronous to any other Region

Minimizes latency for read requests

Increases efficiency for compute workloads

Optimizes data distribution

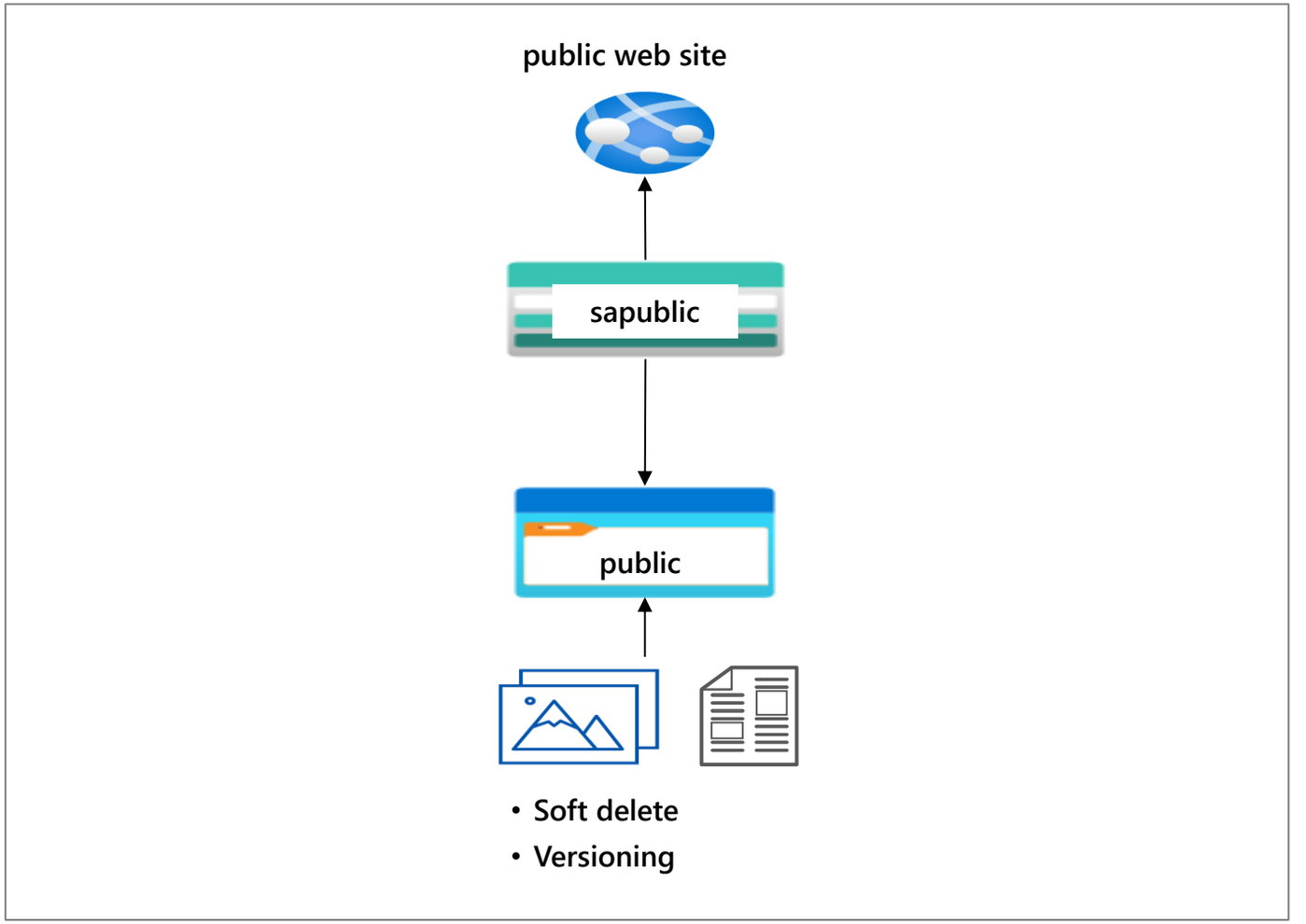
Optimizes costs



Student exercise: Provide storage for the public website

Skilling tasks:

- ❑ Configure anonymous access to a storage account
- ❑ Create blob containers
- ❑ Upload and manage blob files
- ❑ Enable and test soft delete
- ❑ Enable blob versioning

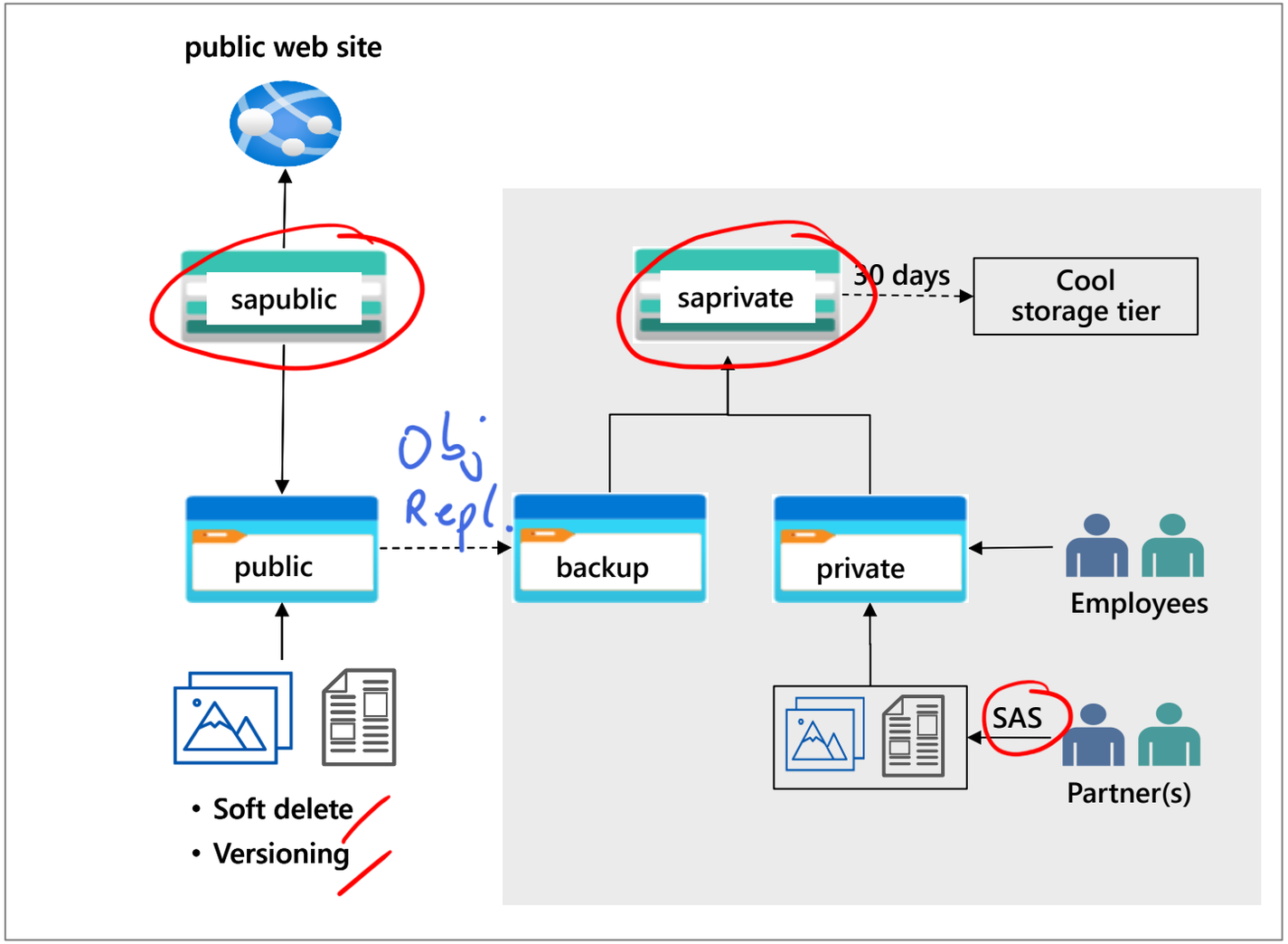


Continued next slide

Student exercise: Provide storage for the company documents

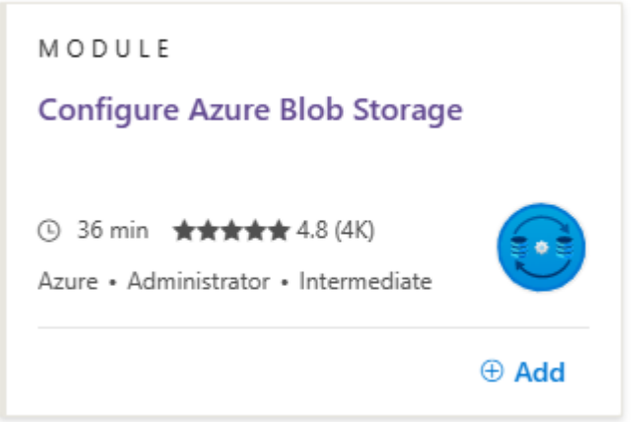
Skilling tasks:

- ❑ 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

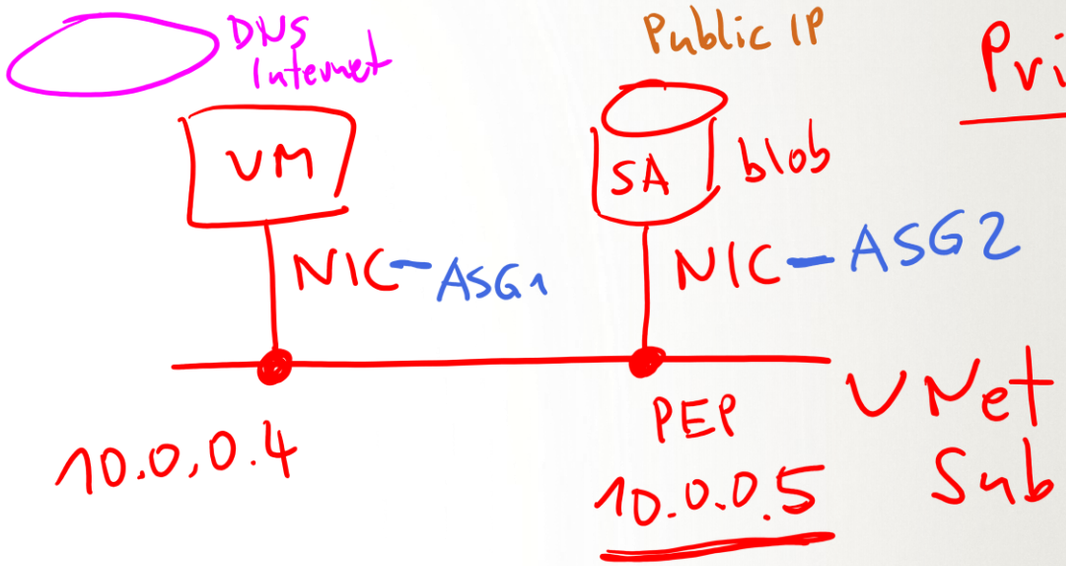


Review questions and reference module – Azure Blob Storage

1. What standard access tiers are available for blob storage?
2. What is blob soft delete and how does the retention period work?
3. What is the purpose of a Shared Access Signature? What parameters are included?
4. How would you automatically move content between access tiers?



This module has an **interactive lab simulation**



Private End Point
= NIC

PEP Private EP

Create and Configure Azure Files and Networking

Service End Points
= Routing

Agenda – Azure Files

- How are Azure Files different from Azure blobs?
- Instructor demonstration: Azure Files and storage networking
  - Which Azure Files tier do you need?
  - Why create a file share snapshot?
  - How to control network traffic to the storage?
- Student exercise: Provide storage for the company app
- Review questions and reference module

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

Instructor demonstration: Azure Files and storage networking

- Create storage for shared files
- Create an Azure file share
- Create a file share directory
- Create snapshots to backup and restore data
- Secure access using the storage firewall and virtual networks
- Review storage browser (optional)

Finance (file sharing)

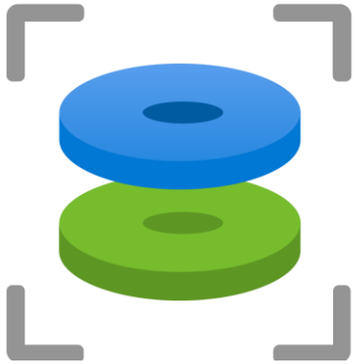
- The company offices are located worldwide.
- Provide file storage to efficiently share information.

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.

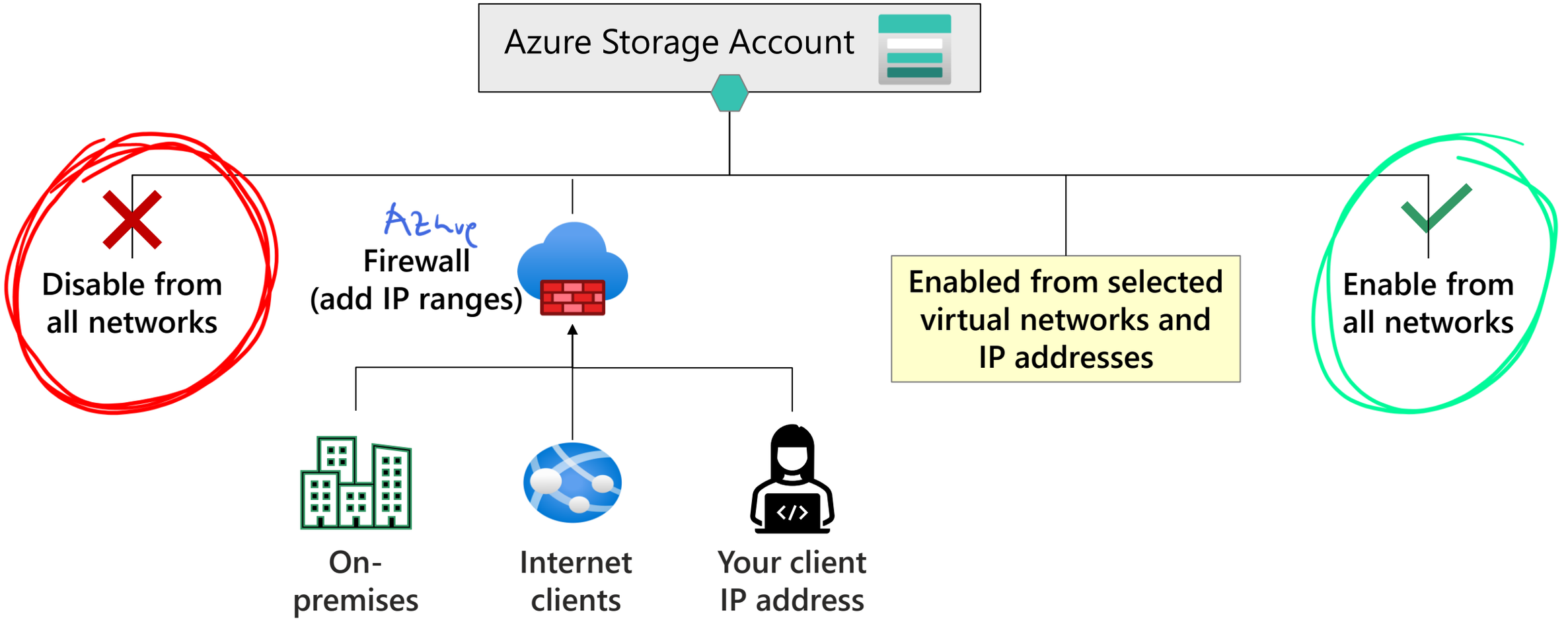
Why create a file share snapshot? (optional)

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

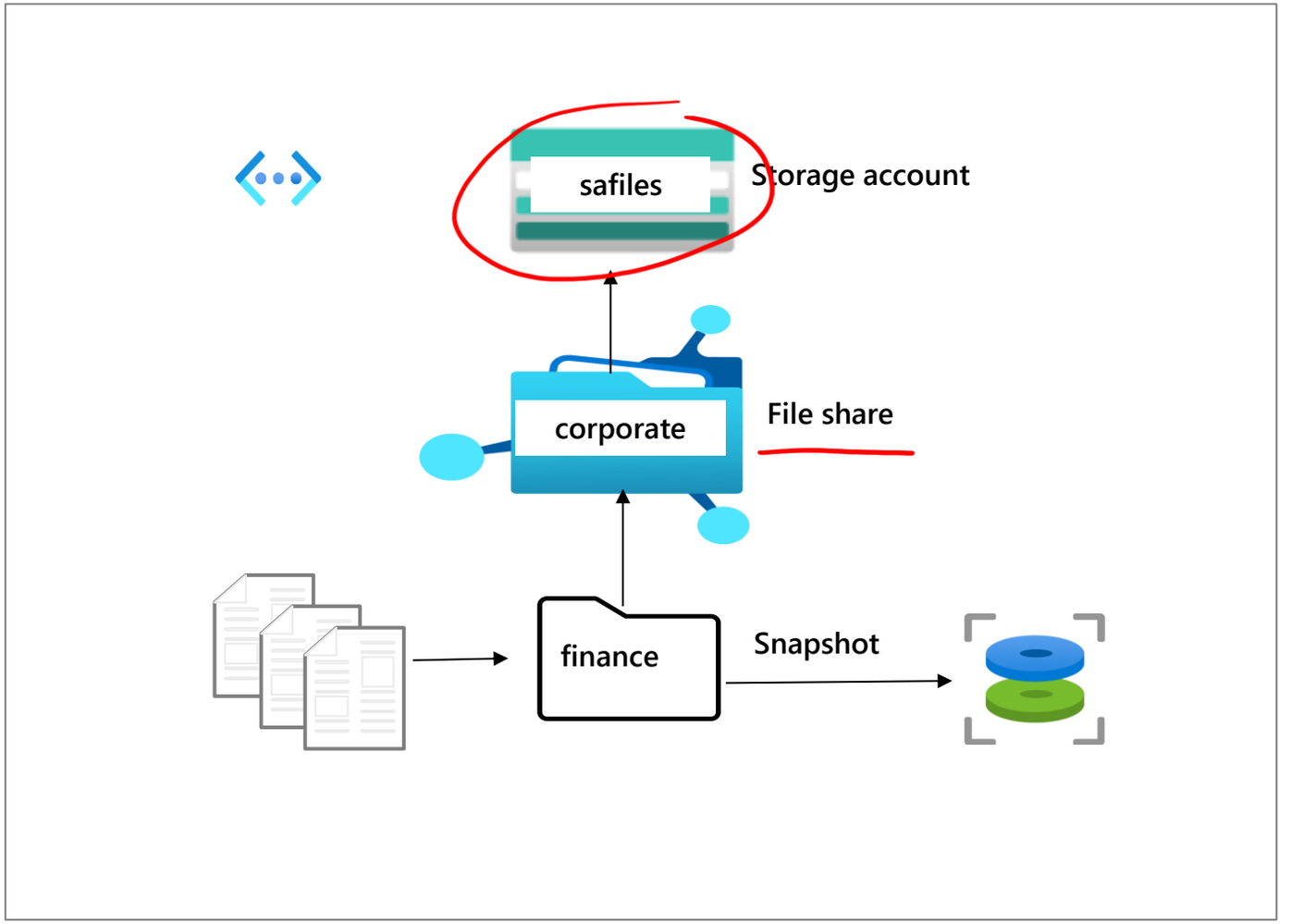
How to control public network traffic to the storage?



Student exercise: Provide shared file storage for corporate

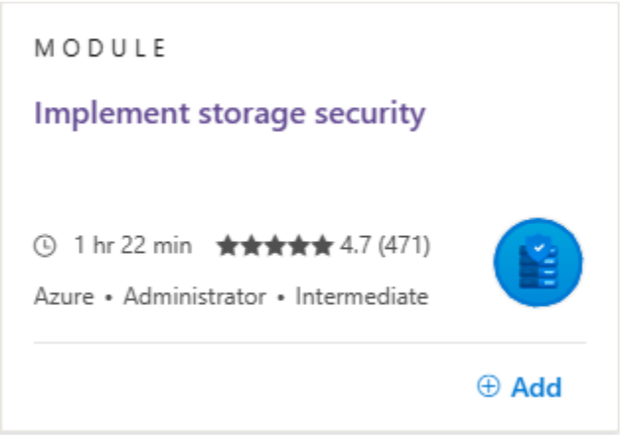
Skilling tasks:

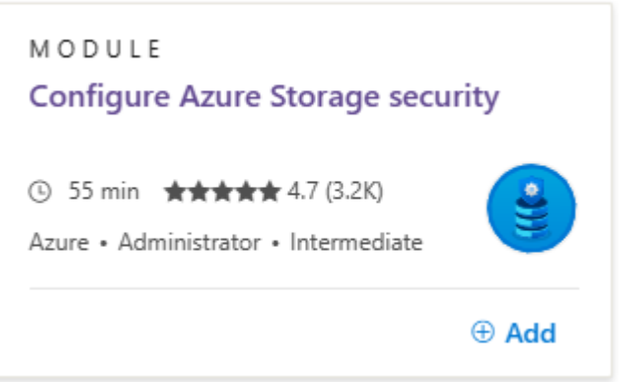
- ❑ Create an Azure file share
- ❑ Create a file share directory
- ❑ Create snapshots to backup and restore the data
- ❑ Secure access to the data to a specific virtual network
- ❑ Use Storage Browser (optional)



Review questions and reference module – Azure Files and Networking

1. What usage cases are best for Azure Files?
2. What is the difference between the Premium and Transaction-optimized tiers?
3. Which technology provides access control to the storage public endpoint?
4. How do file share snapshots work?





This module has an interactive lab simulation

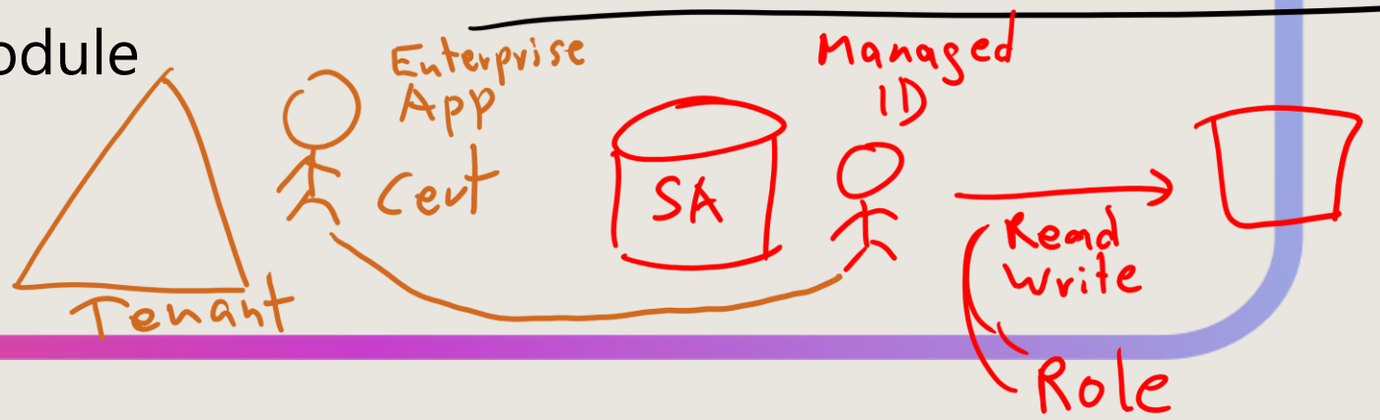
Configure encryption and secure access

Agenda – Encryption and Secure Access

- How is encryption and secure access handled?
- Instructor demonstration: Encryption and secure access
  - How to assign permissions?
  - When to use immutable storage policies?
  - What is an encryption scope and infrastructure encryption?
- Student exercise: Provide storage for the company app
- Review questions and reference module

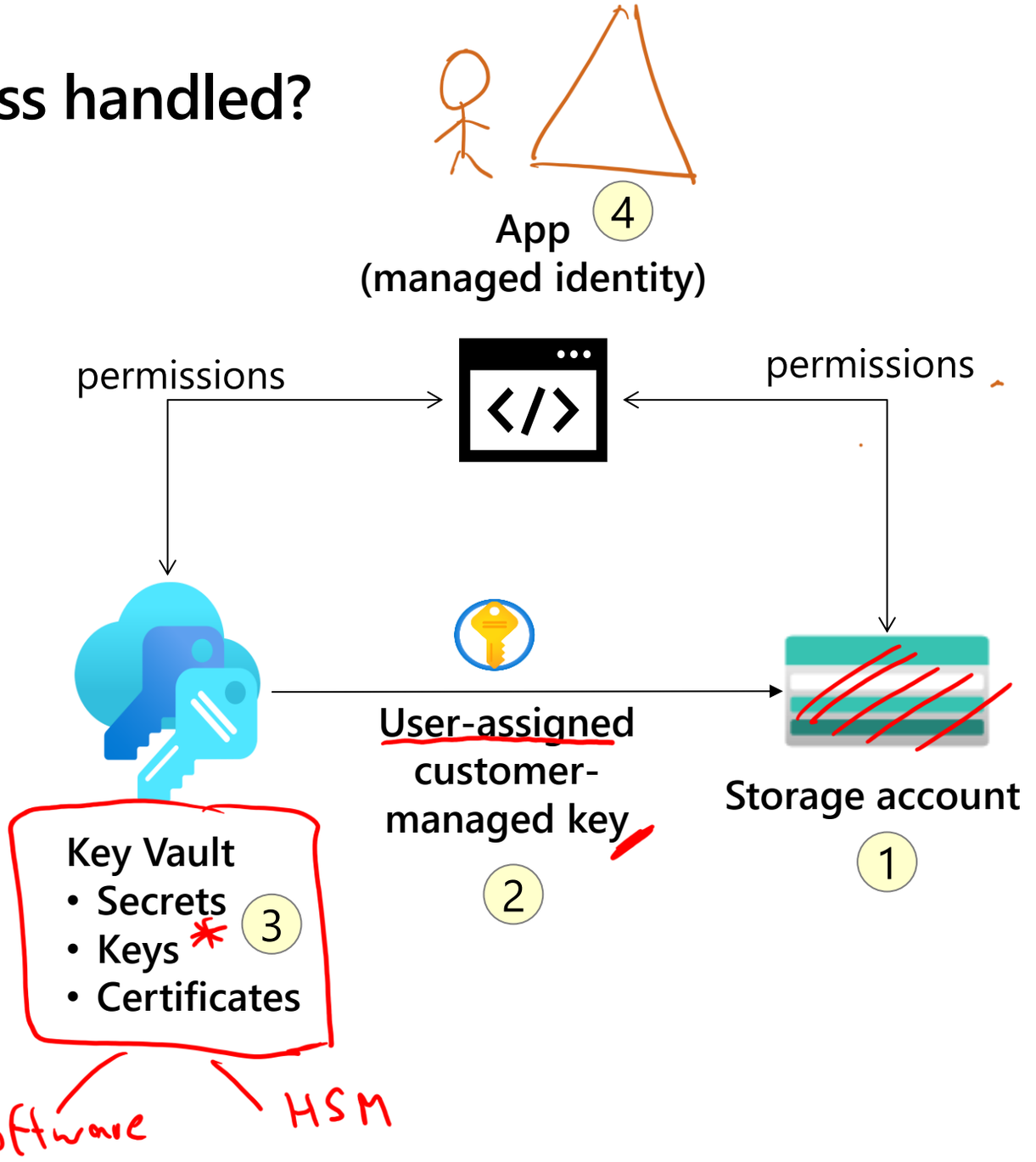
Security

- OAuth 2.0 → App Registr.
- 2 geheime key → Alles
- "Mit Freunden teilen" → SAS Signatur



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.



Instructor demonstration: Storage encryption and secure access

- Configure the storage account to use a managed identity
- Assign permissions to the managed identity
- Secure the storage account with a customer managed key
- Configure a container with immutable storage
- Configure an encryption scope for infrastructure encryption

Developers (app storage)
• Developers need storage for new apps • Provide a secure way of accessing the app storage

How to assign permissions?

Assignment type
- ✓ Job function
- • Administrator

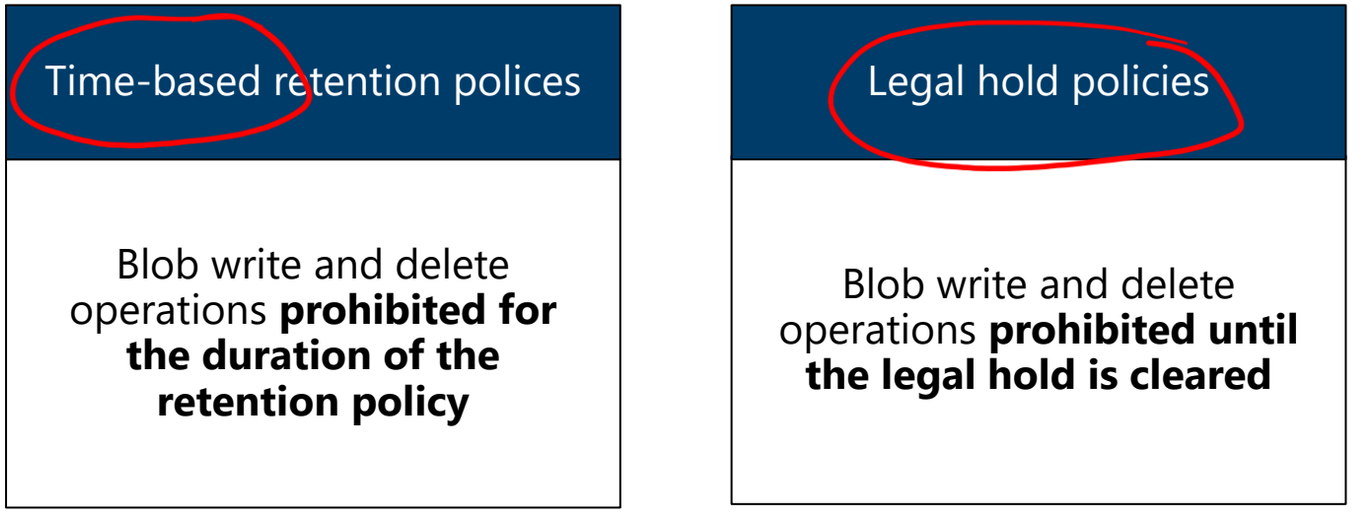
Role
- ✓ Built-in
- • Custom

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



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

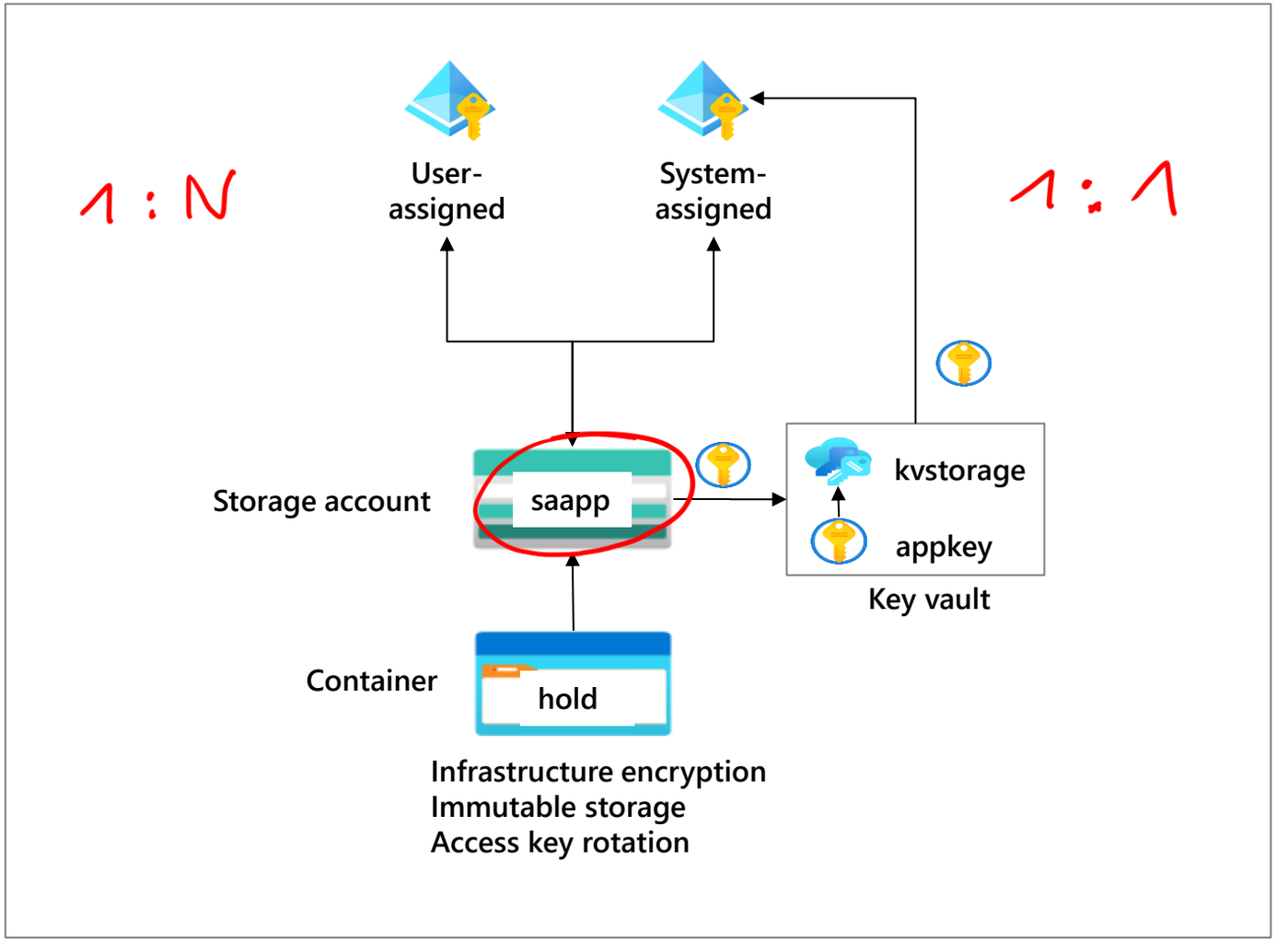
Service level encryption (default)

Infrastructure level encryption (optional)

Student exercise: Provide storage for the company app

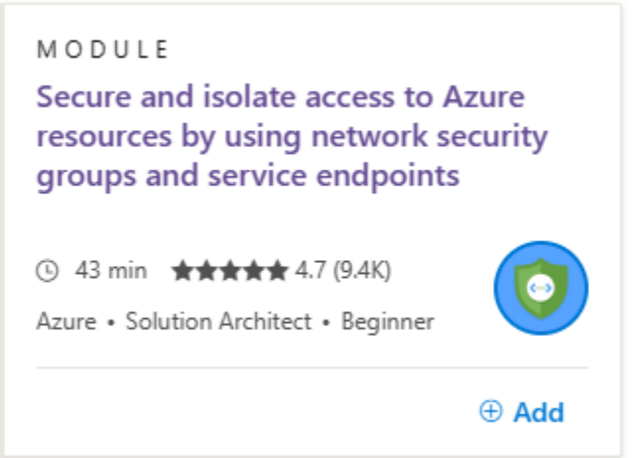
Skilling tasks:

- ❑ 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



Review questions and reference module – Storage Encryption and Access

1. What are some of the ways you can secure your storage?
2. What are the two types of managed identities?
3. How can you protect data from changes during a specific time period?
4. What is infrastructure encryption and how is it enabled?



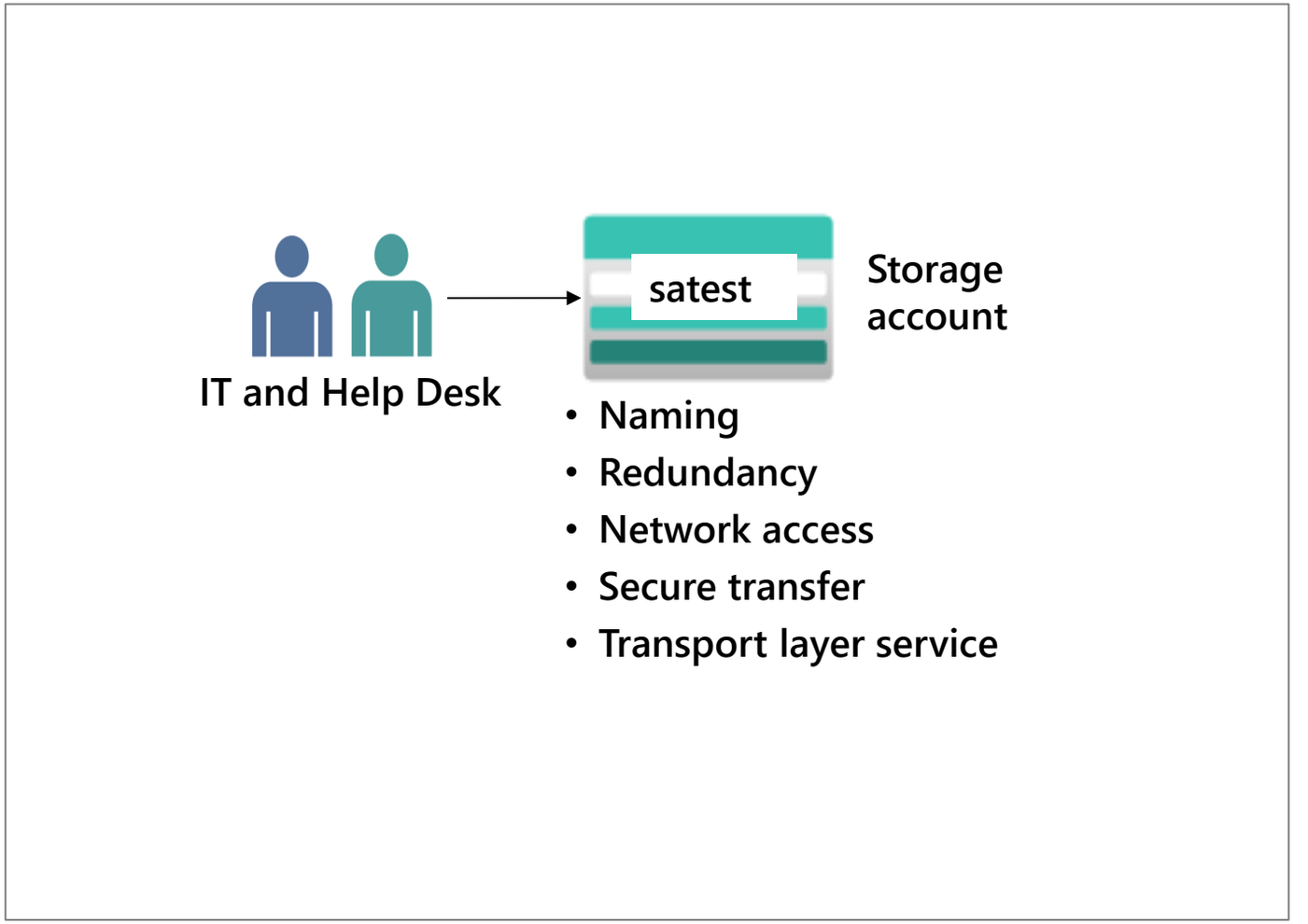
This module has a **sandbox**

Labs

Lab 1: Provide storage for test and development

Skilling tasks:

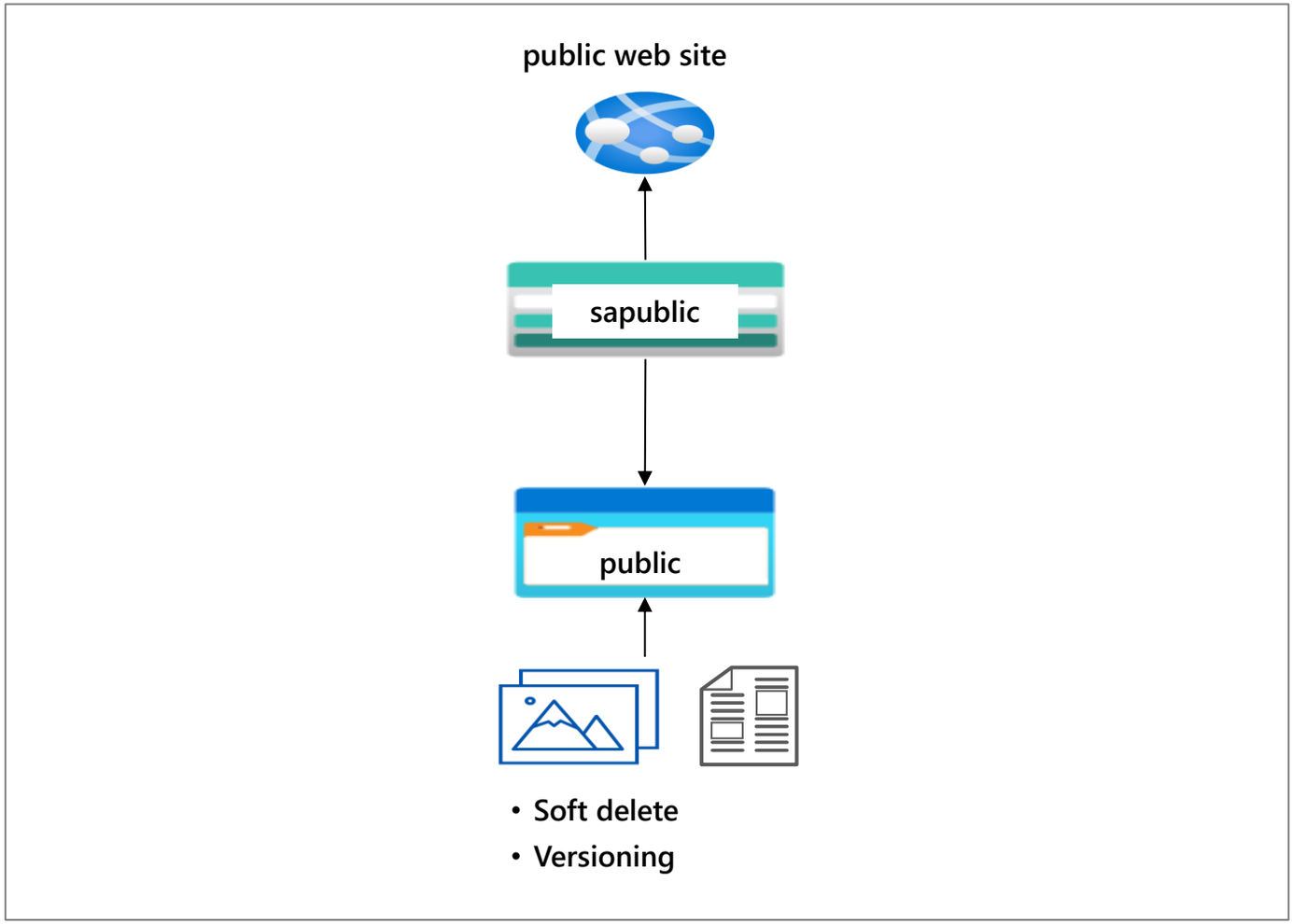
- ❑ Navigating the portal
- ❑ Storage account naming
- ❑ Performance options
- ❑ Redundancy options
- ❑ Network access options
- ❑ Secure transfer
- ❑ Transport layer security



Lab 2a: Provide storage for the public website

Skilling tasks:

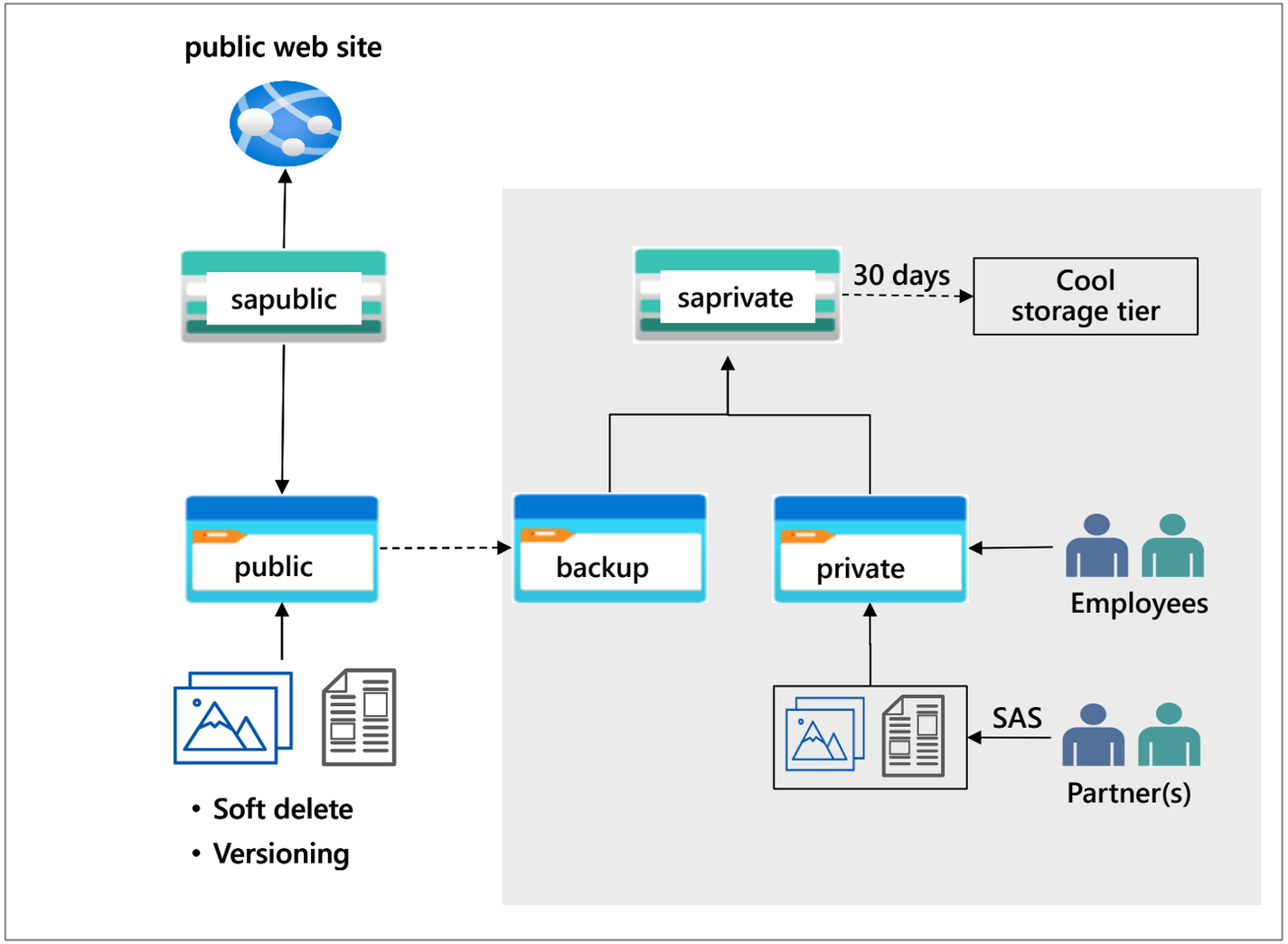
- ❑ Configure anonymous access to a storage account
- ❑ Create blob containers
- ❑ Upload and manage blob files
- ❑ Enable and test soft delete
- ❑ Enable blob versioning



Lab 2b: Provide storage for the company documents

Skilling tasks:

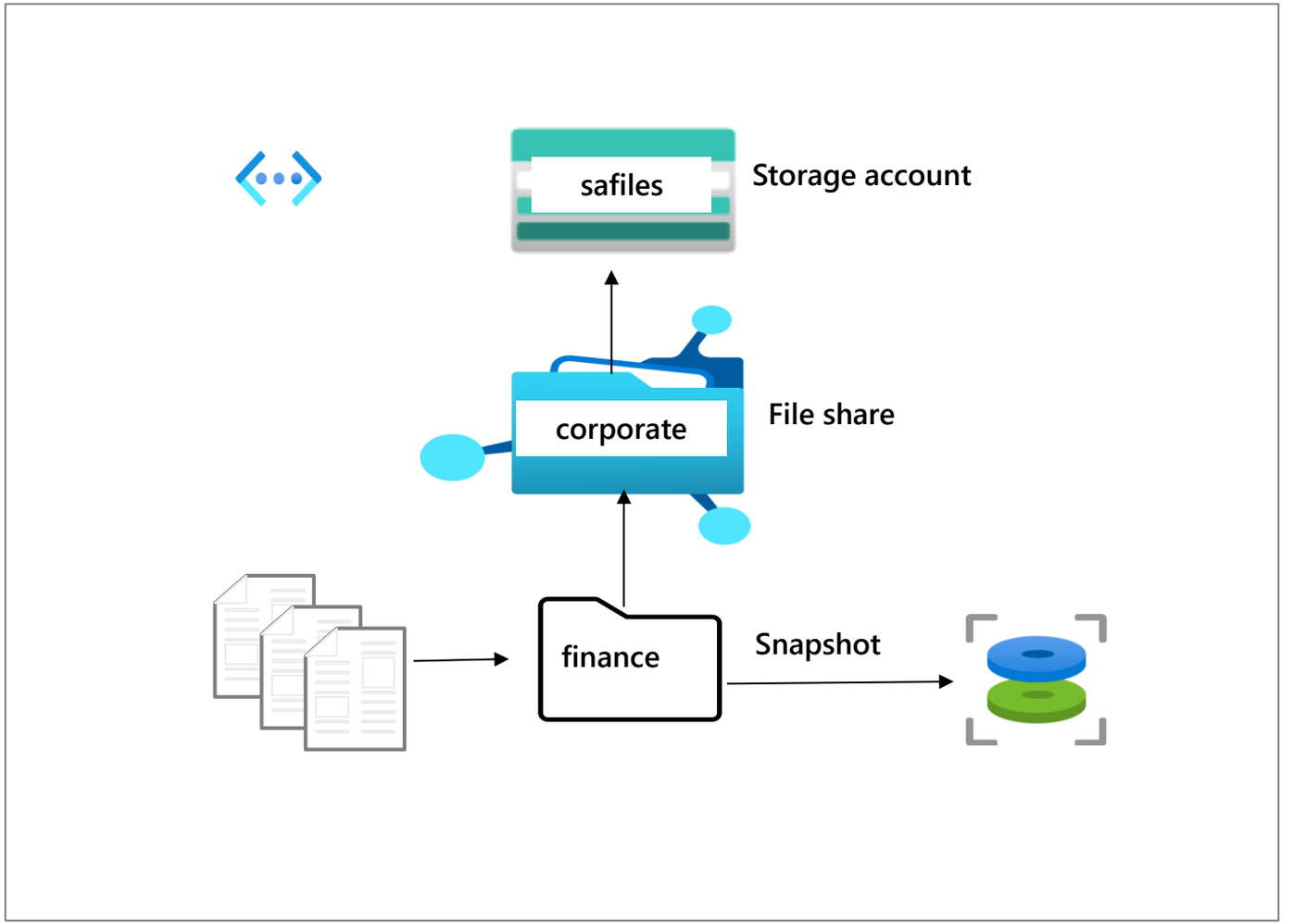
- ❑ Configure private access to a storage account
- ❑ Provide partners limited access to specific documents
- ❑ Automatically move documents between storage tiers
- ❑ Backup the public website documents – asynchronous replication



Lab 3: Provide shared file storage for corporate

Skilling tasks:

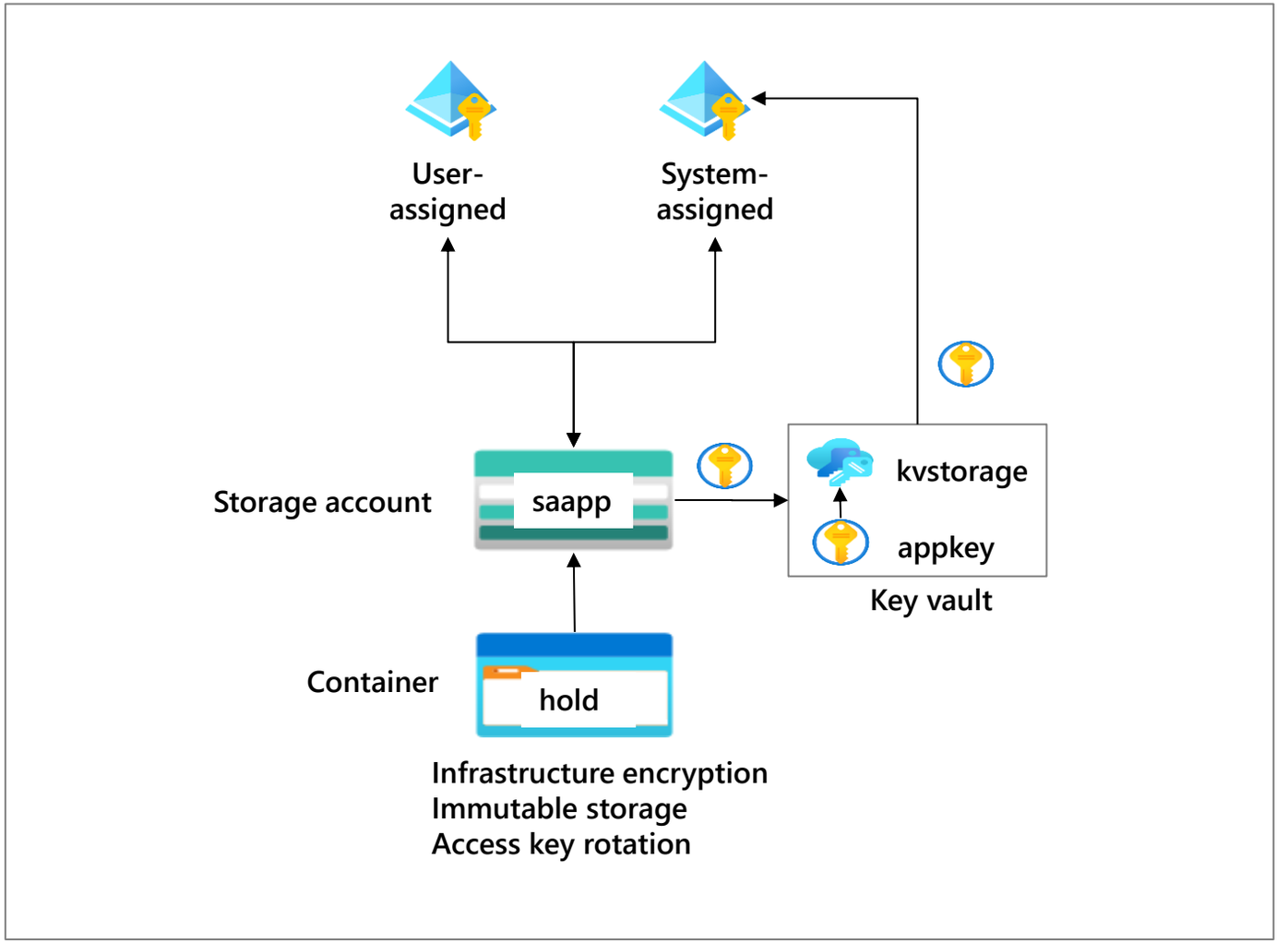
- ❑ Create an Azure file share
- ❑ Create a file share directory
- ❑ Create snapshots to backup and restore the data
- ❑ Secure access to the data to a specific virtual network
- ❑ Use Storage Browser (optional)



Lab 4: Provide storage for the 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