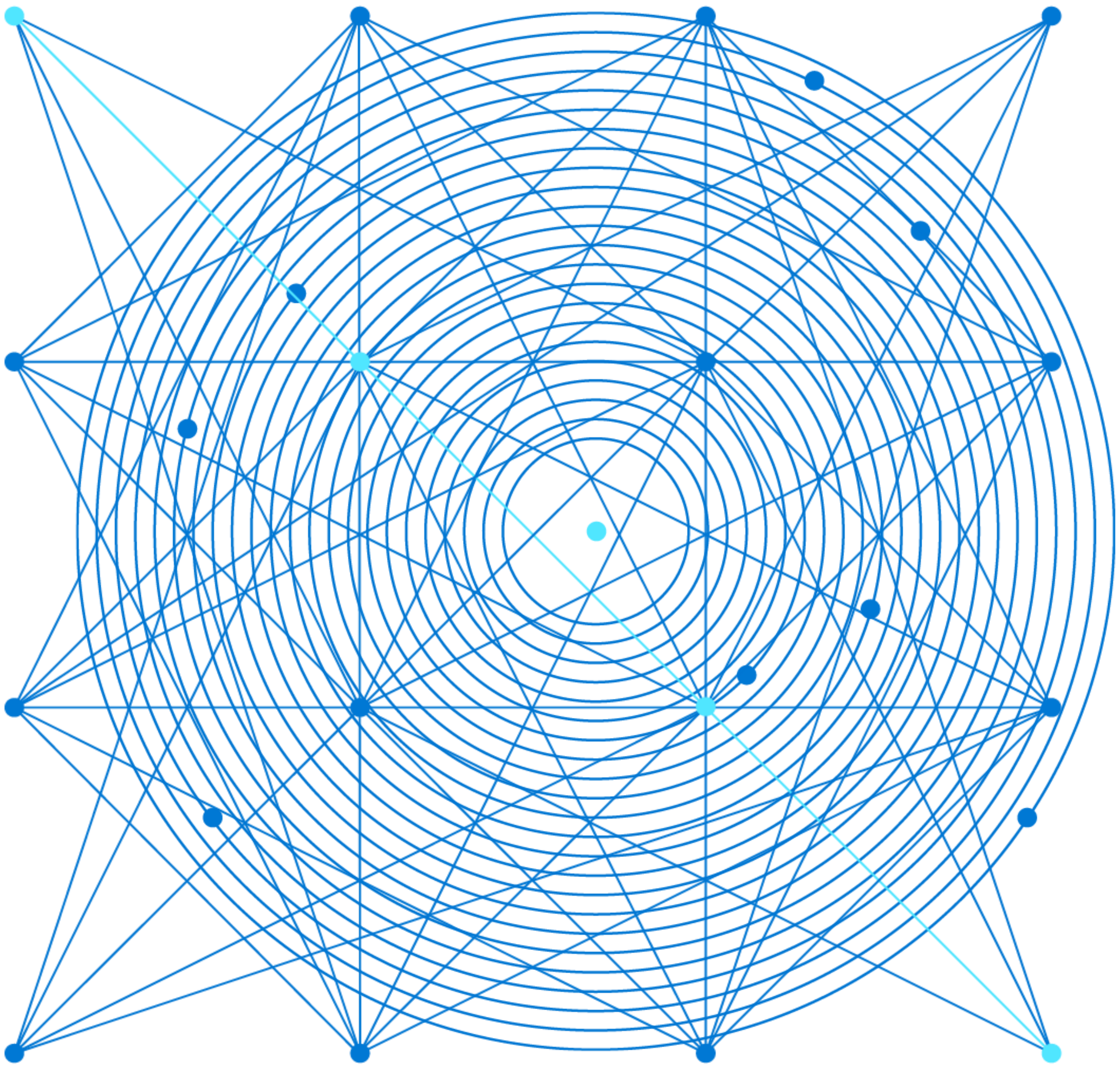
AZ-303: Microsoft Azure Architect Technologies



Module 6: Implement Storage Accounts

Azure Blog Storage, Storage Security, and Azure Storage Firewalls

Learning Objectives

You will learn the following concepts:

- Storage Accounts
- Blob Storage
- Storage Security
- Accessing Blobs and Queues using AAD
- Managing Storage
- Configure Azure Storage Firewalls and Virtual Networks
- Managing Storage

Storage Accounts

Azure Storage

Azure storage is:

- Durable and highly available
- Secure
- Scalable
- Managed
- Accessible

Three categories of Azure storage

- Storage for virtual machines
- Unstructured data
- Structured data

General purpose storage accounts have two tiers

- Standard
- Premium

Azure Storage Services

Azure Containers (blobs)

- Accessible from anywhere via HTTP or HTTPS
- Stores massive amounts of unstructured data, such as text or binary

Azure Files

- Accessible from anywhere via SMB 3.0
- Hosts highly available network file shares

Azure Queues

- Accessible from anywhere via HTTP or HTTPS Provides a queue-based mechanism for asynchronous communication
- Stores messages of up to 64 KB in size in queues

Azure Tables

- Accessible from anywhere via HTTP or HTTPS
- Stores NoSQL tables

Azure Storage Account Types (1 of 2)

A *storage account* is a container that groups a set of Azure Storage services together. Only data services from Azure Storage can be included in a storage account.

Azure storage accounts:

General-purpose v1/v2

Blob, File, Queue, Table, and Disk

File-storage accounts

Files only

Blob-storage accounts (and BlockBlob)

Block blobs and append blobs only

Azure storage services:

Azure Containers (Blobs): A massively scalable object store for text and binary data.

Azure Files: Managed file shares for cloud or on-premises deployments.

Azure Queues: A messaging store for reliable messaging between application components.

Azure Tables: A NoSQL store for schemaless storage of structured data.

Azure Storage Account Types (2 of 2)

Storage account type	Supported services	Supported performance tiers	Replication options
BlobStorage	Blob (block blobs and append blobs only)	Standard	LRS, GRS, RA-GRS
General-purpose V1	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS
General-purpose V2	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS, ZRS, ZGRS (preview), RA-ZGRS (preview)
Block blob storage	Blob (block blobs and append blobs only)	Premium	LRS, ZRS (limited regions)
FileStorage	Files only	Premium	LRS, ZRS (limited regions)

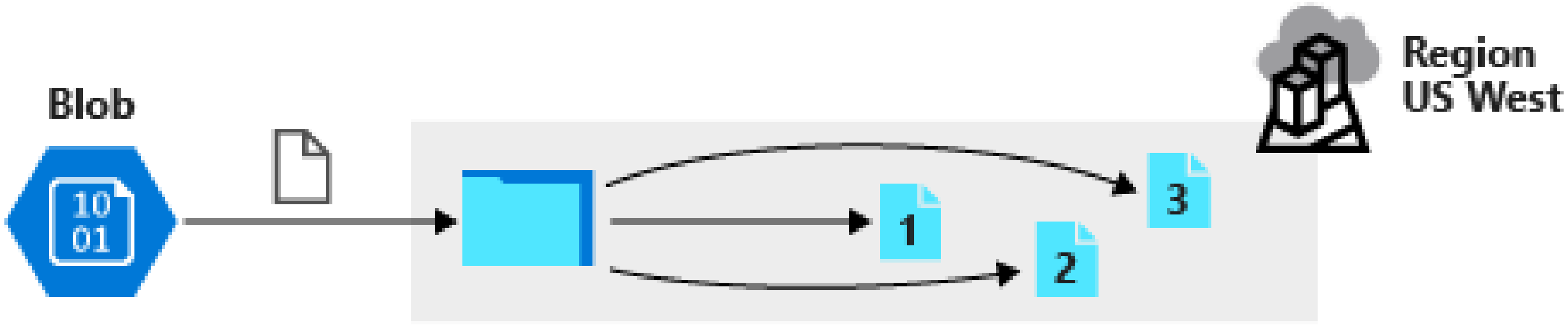
Azure Storage Account Replication Features (1 of 5)

Data redundancy:

- Locally redundant storage (LRS)
- Zone-redundant storage (ZRS)
- Geographically redundant storage (GRS)
- Read-access geo-redundant storage (RA-GRS)
- Geo-zone-redundant storage (GZRS)
- Read-access geo-zone-redundant storage (RA-GZRS)

Azure Storage Account Replication Features (2 of 5)

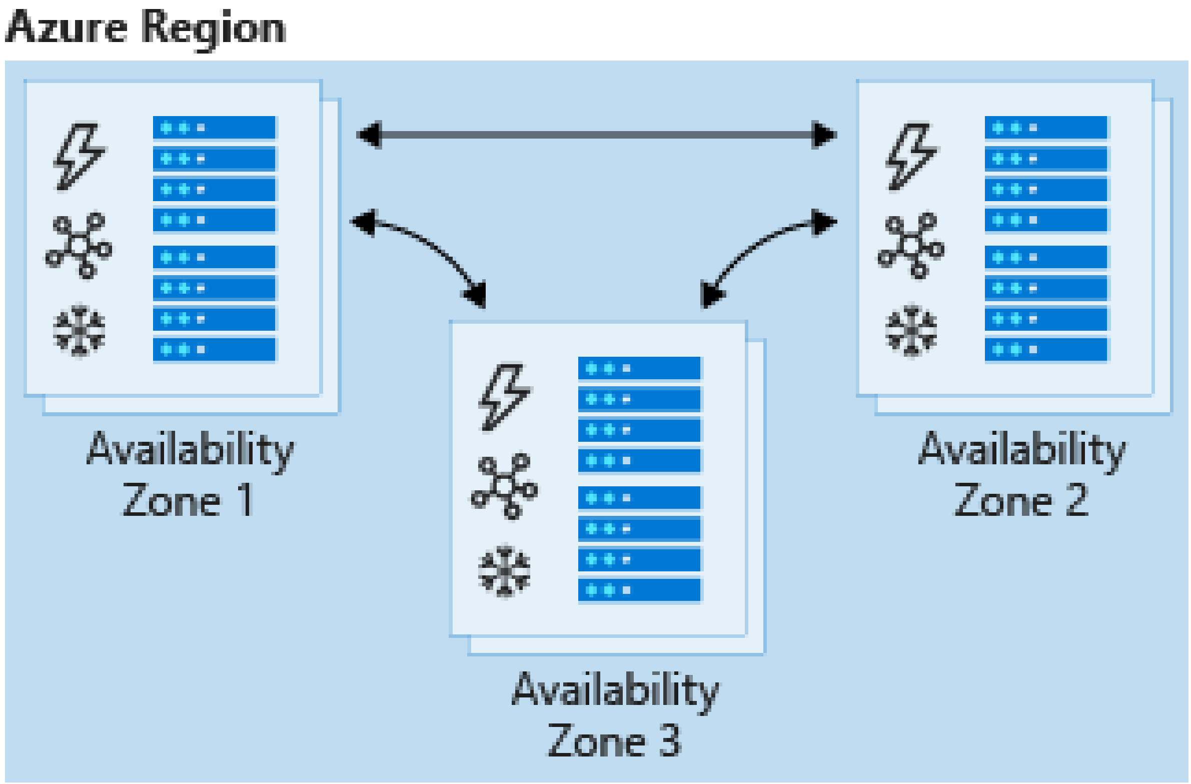
What is locally redundant storage (LRS)?



Three copies of the same data, stored in the same data center

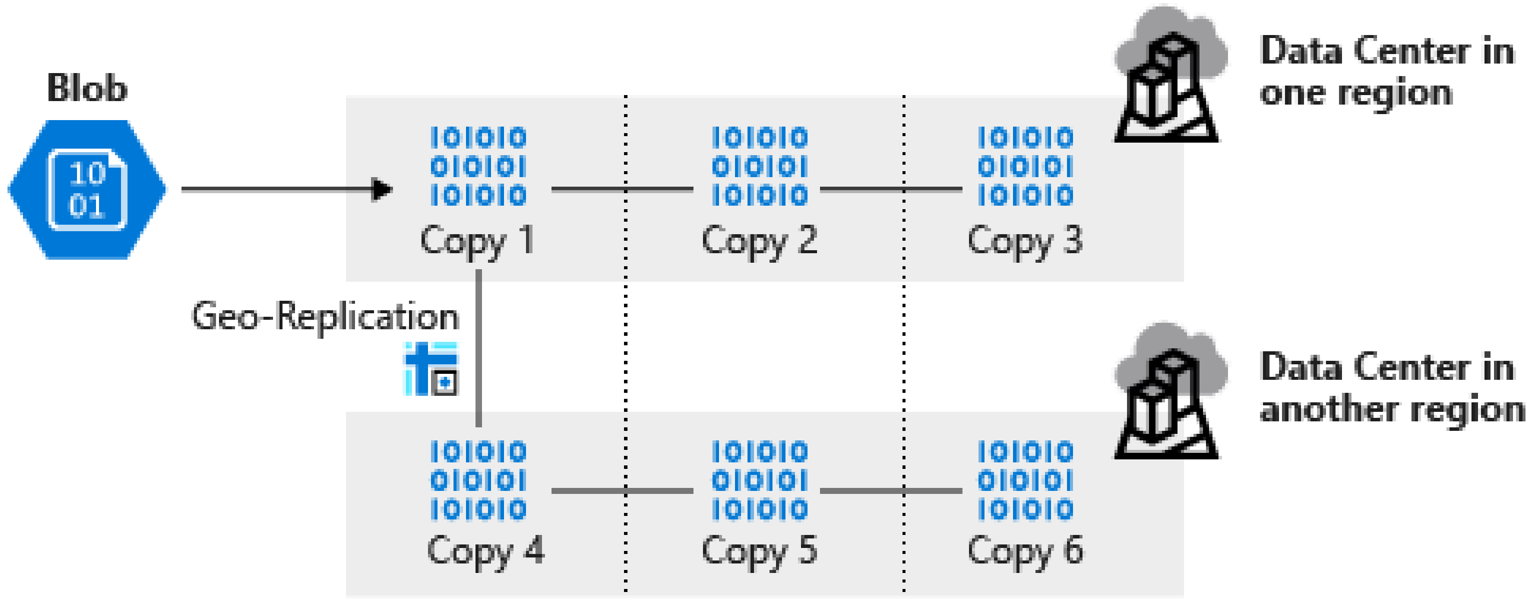
Azure Storage Account Replication Features (3 of 5)

What is zone-redundant storage (ZRS)?



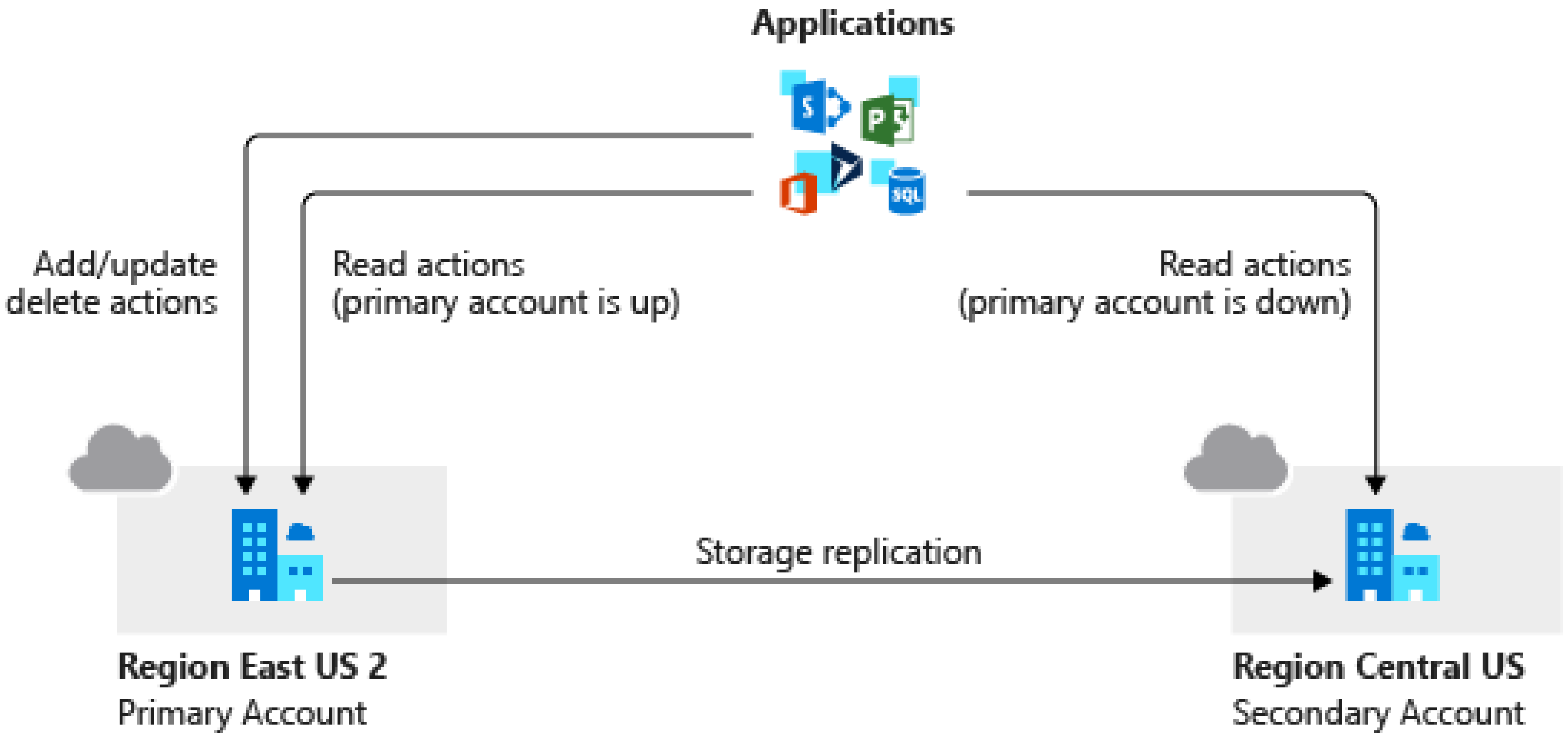
Azure Storage Account Replication Features (4 of 5)

What is geographically redundant storage (GRS)?



Azure Storage Account Replication Features (5 of 5)

What is read-access geo-redundant redundant storage (RA-GRS)?



Accessing Storage

Every object that you store in Azure Storage has a unique URL address:

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

There are two ways to configure a custom domain for accessing blob storage:

- Direct **CNAME** mapping
- Intermediary mapping with `asverify`

Blob Storage

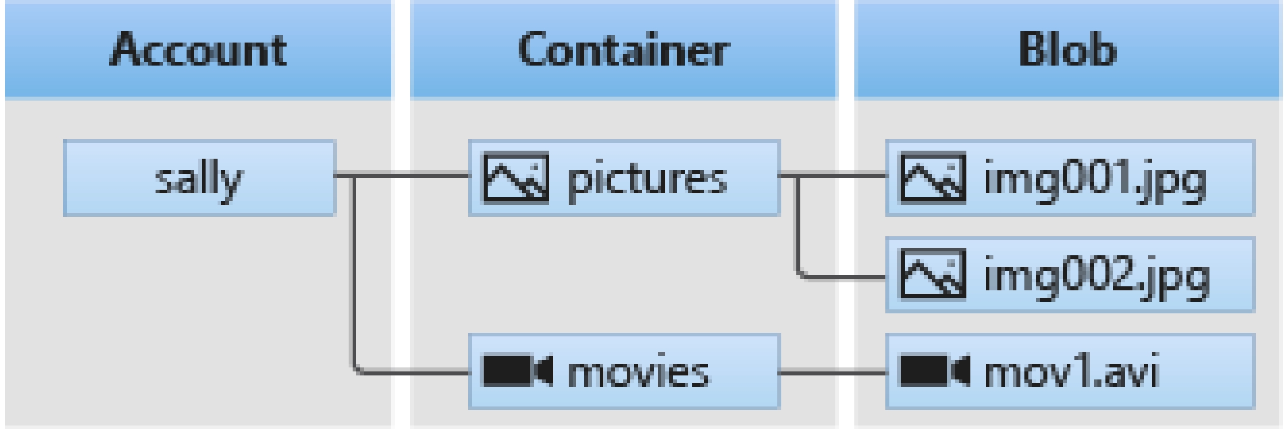
Blob Storage

Common uses of blob storage:

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

Blob service includes three types of resources:

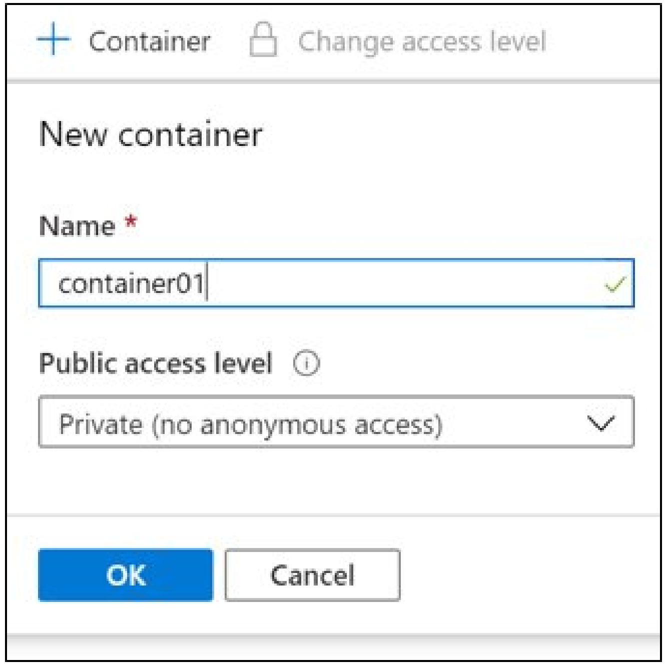
- The storage account
- Containers in the storage account
- Blobs in a container



Blob Containers

To create a container, you specify:

- Name
- Public access level (private, blob, or container)



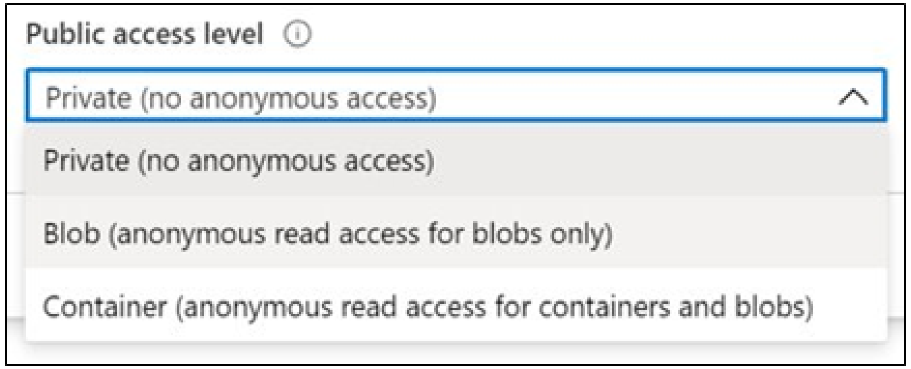
New container

Name *

container01

Public access level ⓘ

Private (no anonymous access)



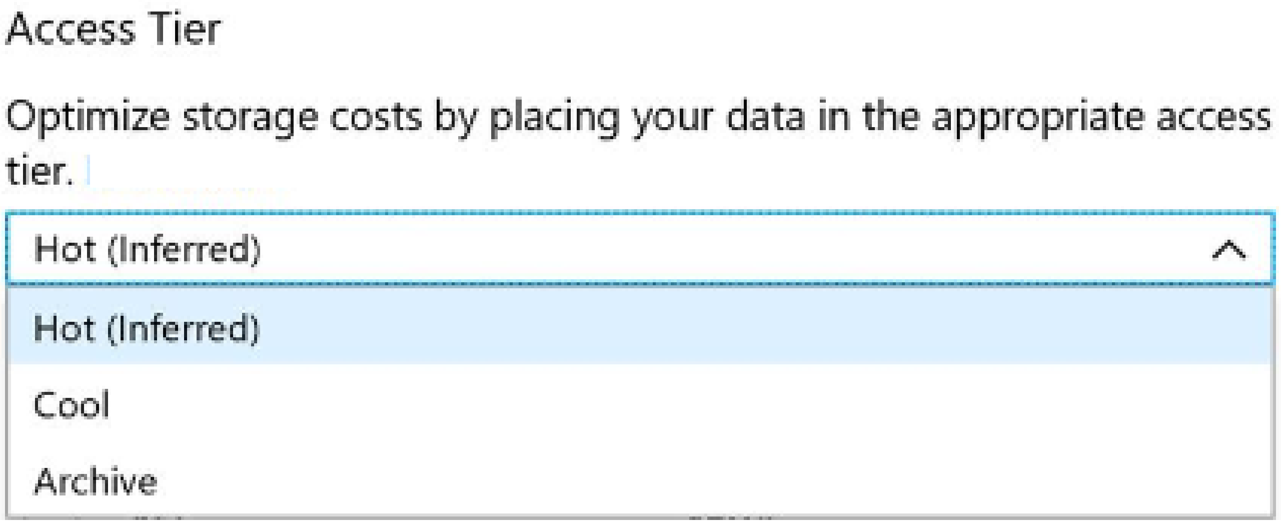
Public access level ⓘ

Private (no anonymous access)

Private (no anonymous access)
Blob (anonymous read access for blobs only)
Container (anonymous read access for containers and 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



Access Tier

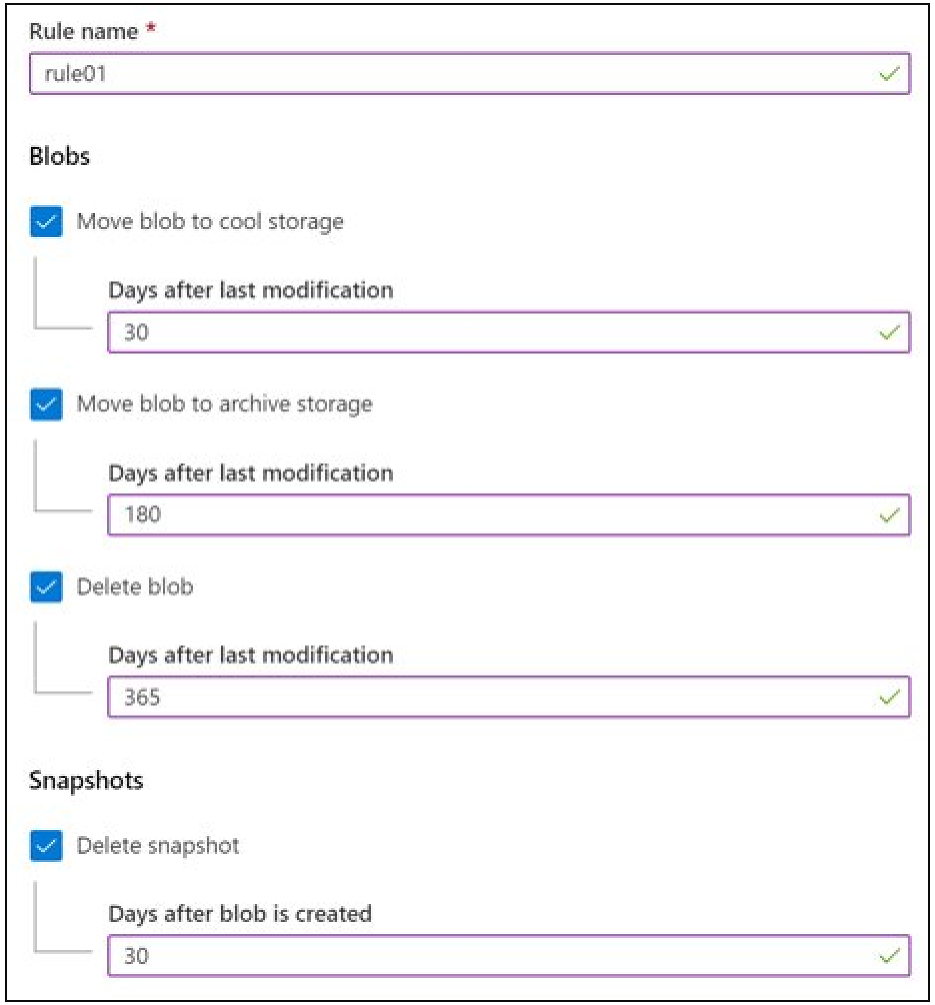
Optimize storage costs by placing your data in the appropriate access tier.

Hot (Inferred)

Blob Lifecycle Management

Blob lifecycle management policy lets you:

- Transition blobs to a cooler storage tier (hot to cool, hot to archive, or cool to archive) to optimize for performance and cost
- Delete blobs at the end of their lifecycles
- Define rules to be run once per day at the storage account level
- Apply rules to containers or a subset of blobs (using prefixes as filters).



Rule name *

rule01

Blobs

☑ Move blob to cool storage

Days after last modification

30

☑ Move blob to archive storage

Days after last modification

180

☑ Delete blob

Days after last modification

365

Snapshots

☑ Delete snapshot

Days after blob is created

30

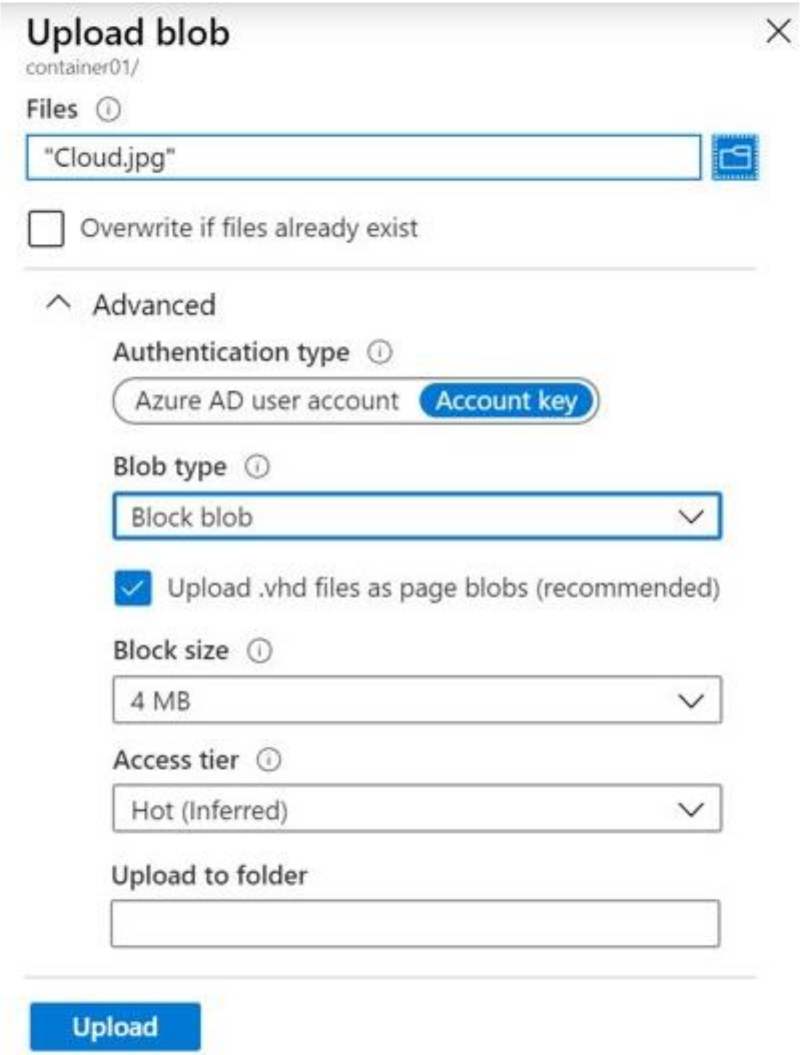
Uploading Blobs

Azure Storage supports three types of blobs:

- Block blobs (default)
- Append blobs
- Page blobs

Blob upload tools include:

- AzCopy
- Azure Storage Data Movement Library
- Azure Data Factory
- Blobfuse
- Azure Data Box Disk
- Azure Import/Export



Upload blob

container01/

Files

"Cloud.jpg"

□ Overwrite if files already exist

Advanced

Authentication type

Azure AD user account [✓ Account key]

Blob type

Block blob

☑ Upload .vhd files as page blobs (recommended)

Block size

4 MB

Access tier

Hot (Inferred)

Upload to folder

Upload

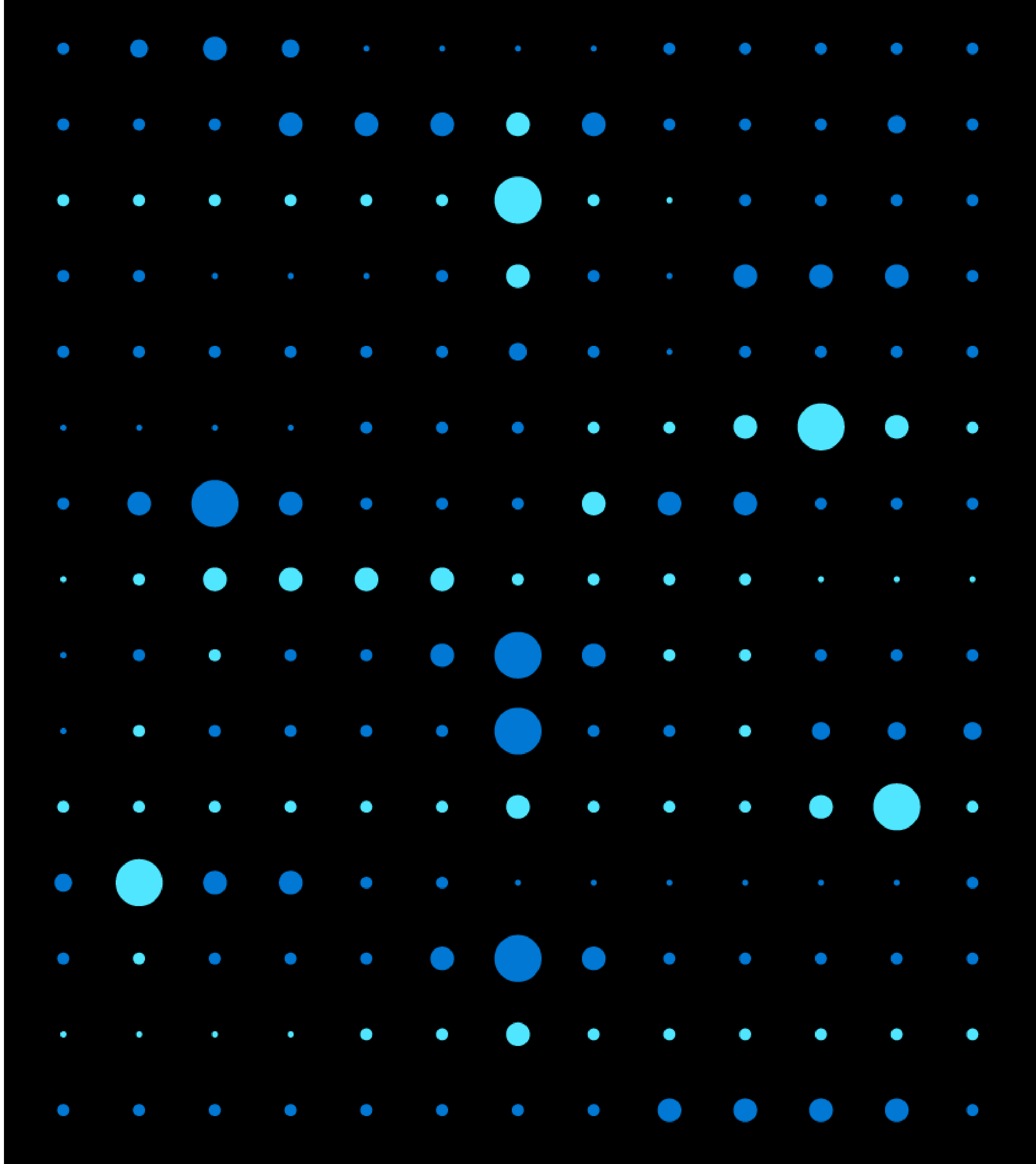
Storage Pricing

When using a storage account, the following billing considerations apply:

- Performance tiers
- Data access costs
- Transaction costs
- Geo-replication data transfer costs
- Outbound data transfer costs
- Changing the storage tier

Demonstration: Blob Storage

- Create a container
- Upload a block blob
- Download a block blob



Storage Security

Storage Security

High-level security capabilities for Azure storage:

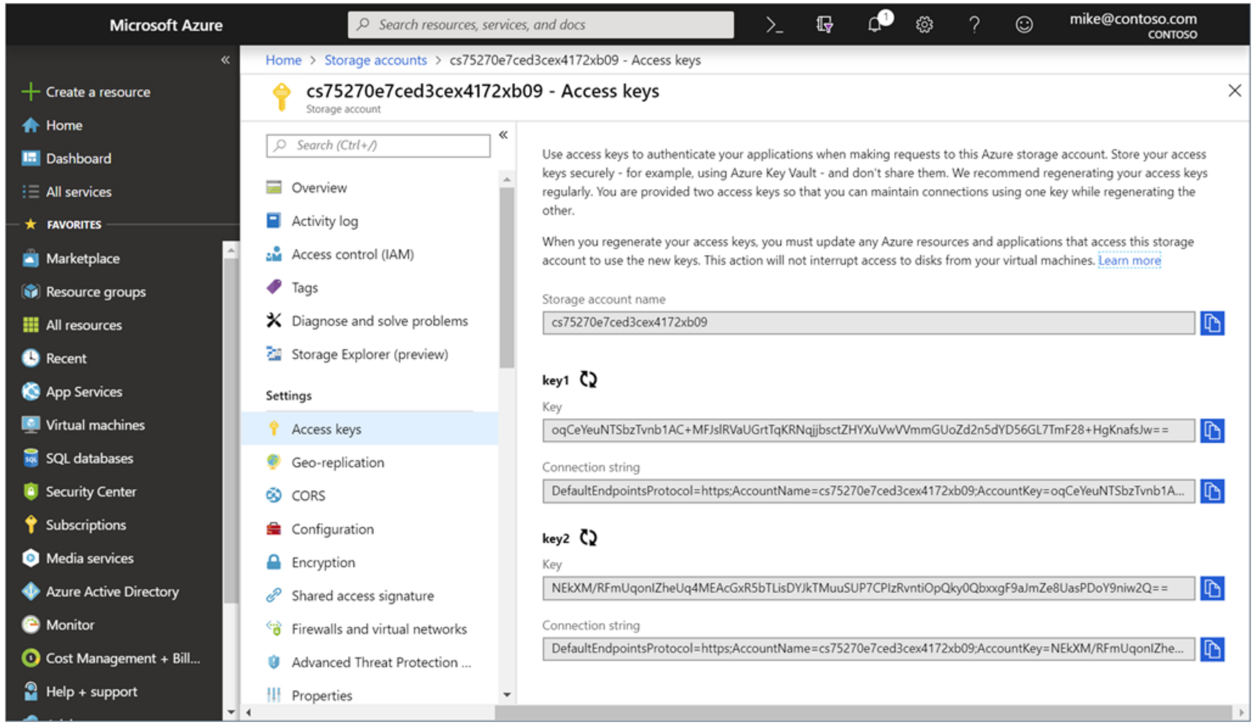
- Encryption
- Authentication
- Data in transit
- Disk encryption
- Shared access signatures

Authorization options:

- Azure Active Directory (Azure AD)
- Shared key
- Shared access signatures
- Anonymous access to containers and blobs

Storage Account Keys

- Azure creates two keys (primary and secondary) for each storage account
- Either of the keys provides full access to the account
- You should regenerate keys on a regular basis or if they are compromised



Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action will not interrupt access to disks from your virtual machines. Learn more

Storage account name
cs75270e7ced3cex4172xb09

key1

Key
oqCeYeuNTSbzTvnb1AC+MFJslRVaUGrtTqKRNqjjbsctZHYXuVwVVmmGUoZd2n5dYD56GL7TmF28+HgKnafsJw==

Connection string
DefaultEndpointsProtocol=https;AccountName=cs75270e7ced3cex4172xb09;AccountKey=oqCeYeuNTSbzTvnb1A...

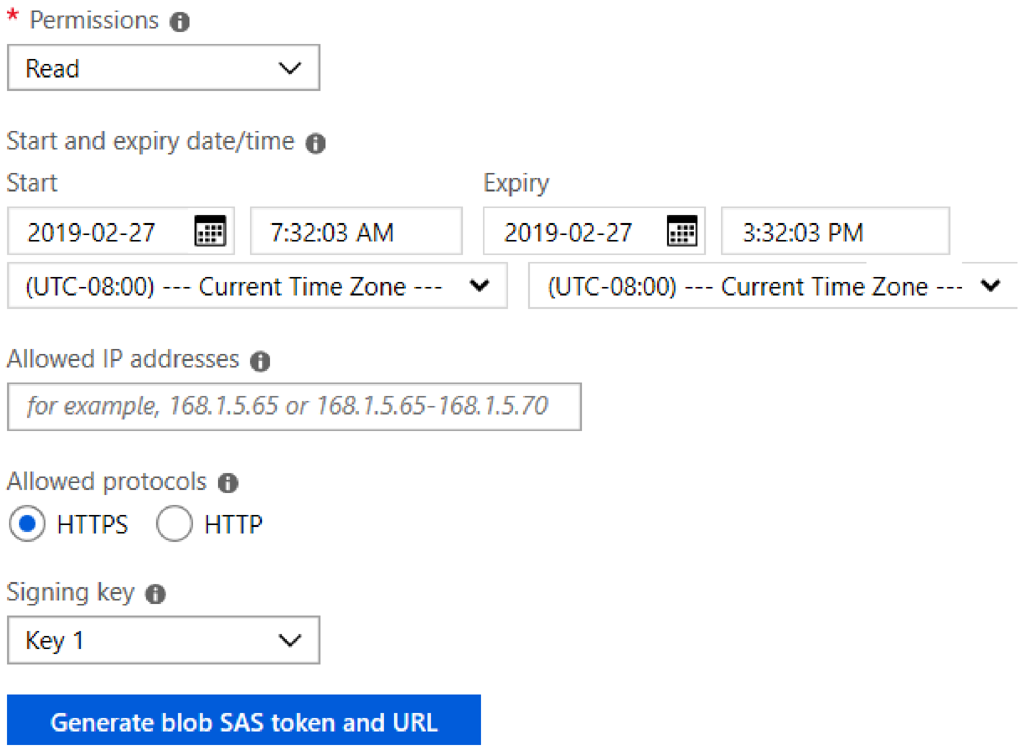
key2

Key
NEkXM/RFmUqonIZheUq4MEAcGxR5bTLisDYJkTMuuSUP7CPIzRvntiOpQky0QbxxgF9aJmZe8UasPDoY9niw2Q==

Connection string
DefaultEndpointsProtocol=https;AccountName=cs75270e7ced3cex4172xb09;AccountKey=NEkXM/RFmUqonIZhe...

Shared Access Signatures

- Shared access signatures (SAS) grant restricted access rights to Azure Storage resources
- Access level can be very granular, including support for:
  - An account-level SAS to delegate access to multiple storage services
  - A time interval during which the SAS is valid
  - Object and container level permissions
  - IP address range from which Azure Storage will accept the SAS token
  - The protocol over which Azure Storage will accept the SAS token



* Permissions

Read

Start and expiry date/time

Start: 2019-02-27 7:32:03 AM (UTC-08:00) --- Current Time Zone ---

Expiry: 2019-02-27 3:32:03 PM (UTC-08:00) --- Current Time Zone ---

Allowed IP addresses

for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols

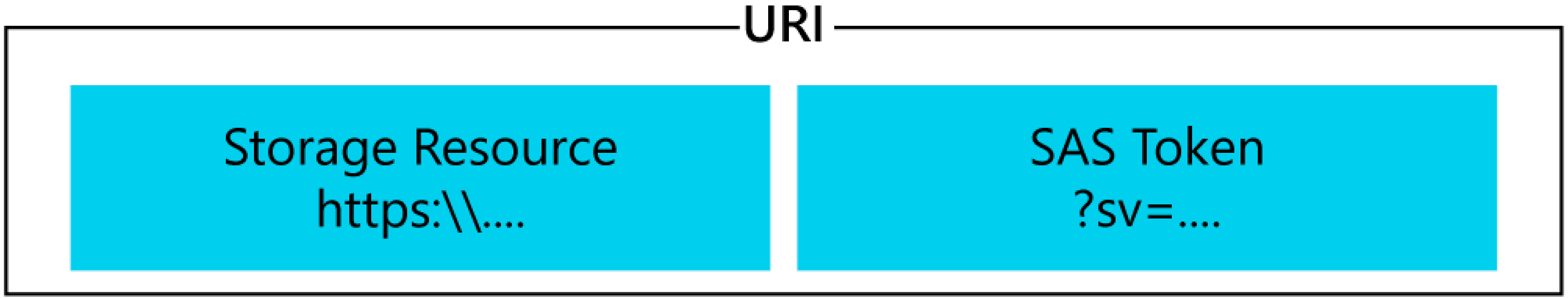
● HTTPS ○ HTTP

Signing key

Key 1

URI and SAS Parameters

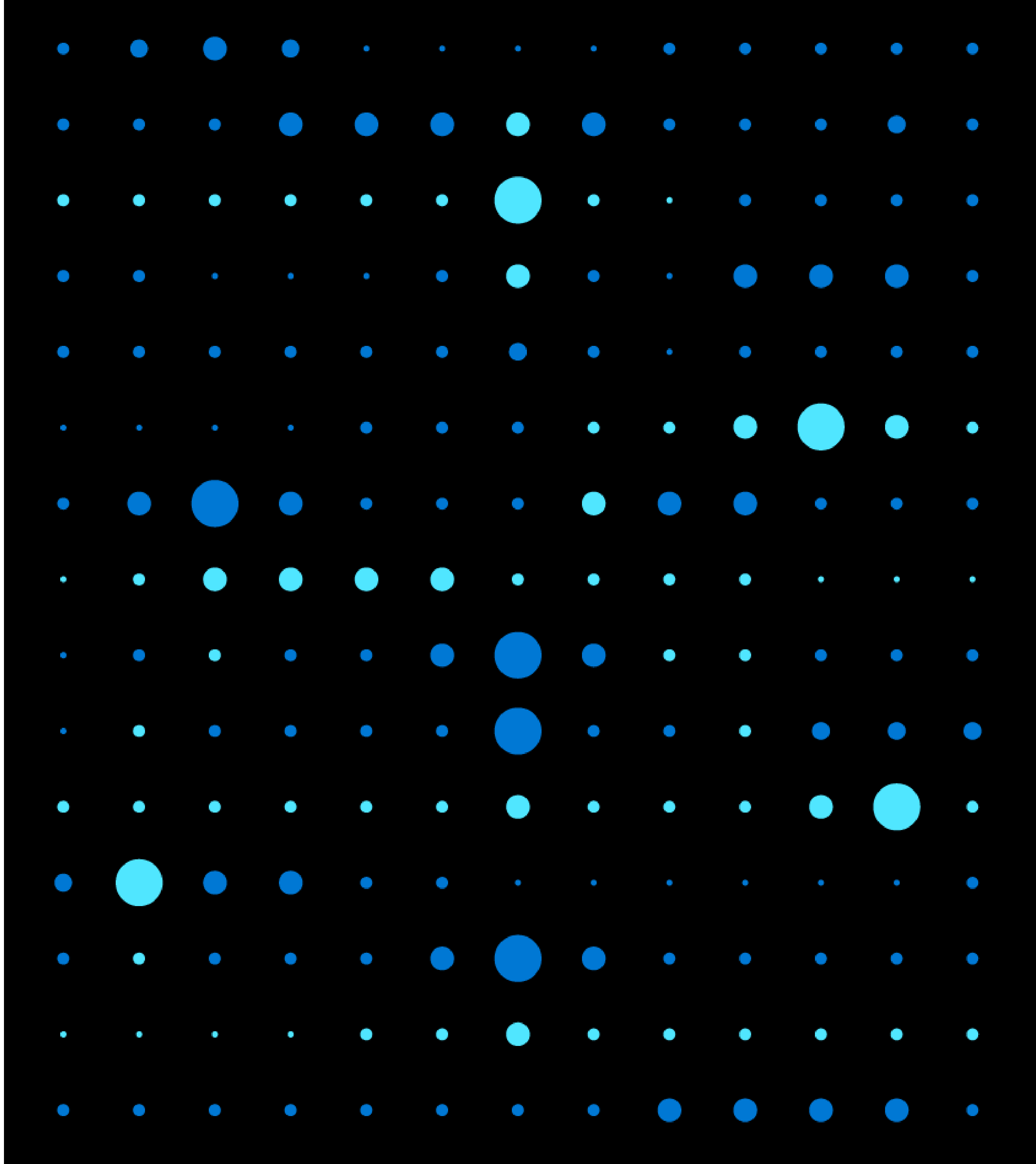
- A URI is created using parameters and tokens as you create your SAS
- The URI consists of your Storage Resource URI and the SAS token



- `https://myaccount.blob.core.windows.net/?restype=service&comp=properties&sv=2015-04-05&ss=bf&srt=s&st=2015-04-29T22%3A18%3A26Z&se=2015-04-30T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.5.60-168.1.5.70&spr=https&sig=F%6GRVAZ5Cdj2Pw4txxxxx`

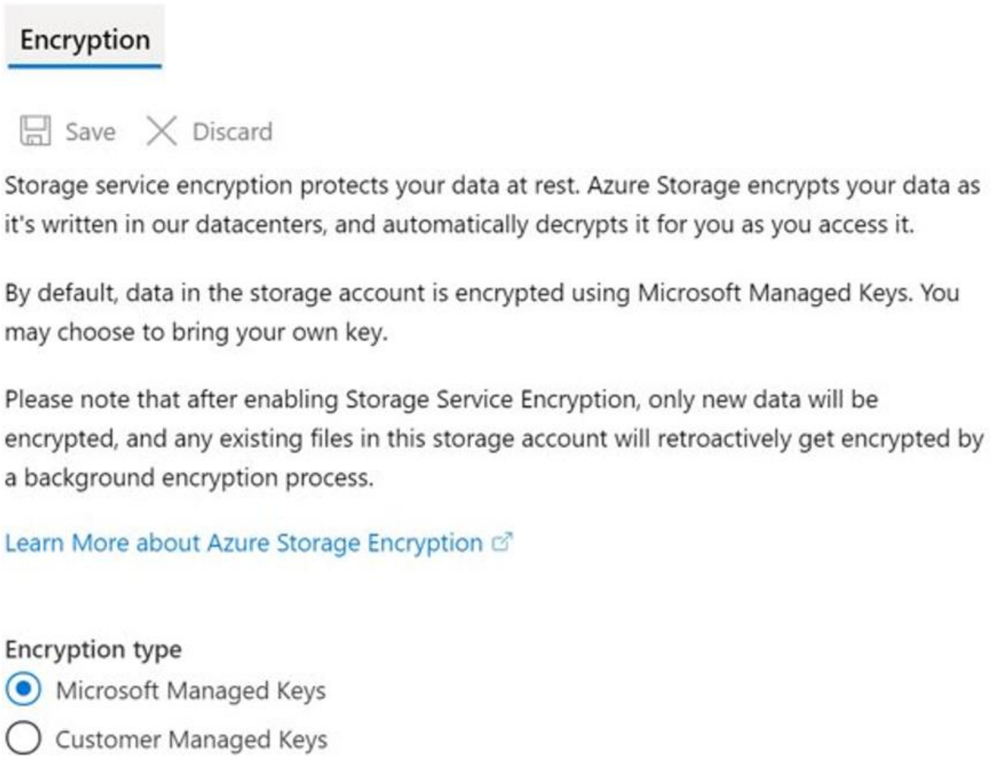
Demonstration: SAS (Portal)

- Create a SAS at the service level
- Create a SAS at the account level



Storage Service Encryption (SSE)

- Azure **Storage Service Encryption** (SSE) for data at rest helps protect data
- SSE is enabled for all new and existing storage accounts and cannot be disabled



Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data in the storage account is encrypted using Microsoft Managed Keys. You may choose to bring your own key.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

Learn More about Azure Storage Encryption

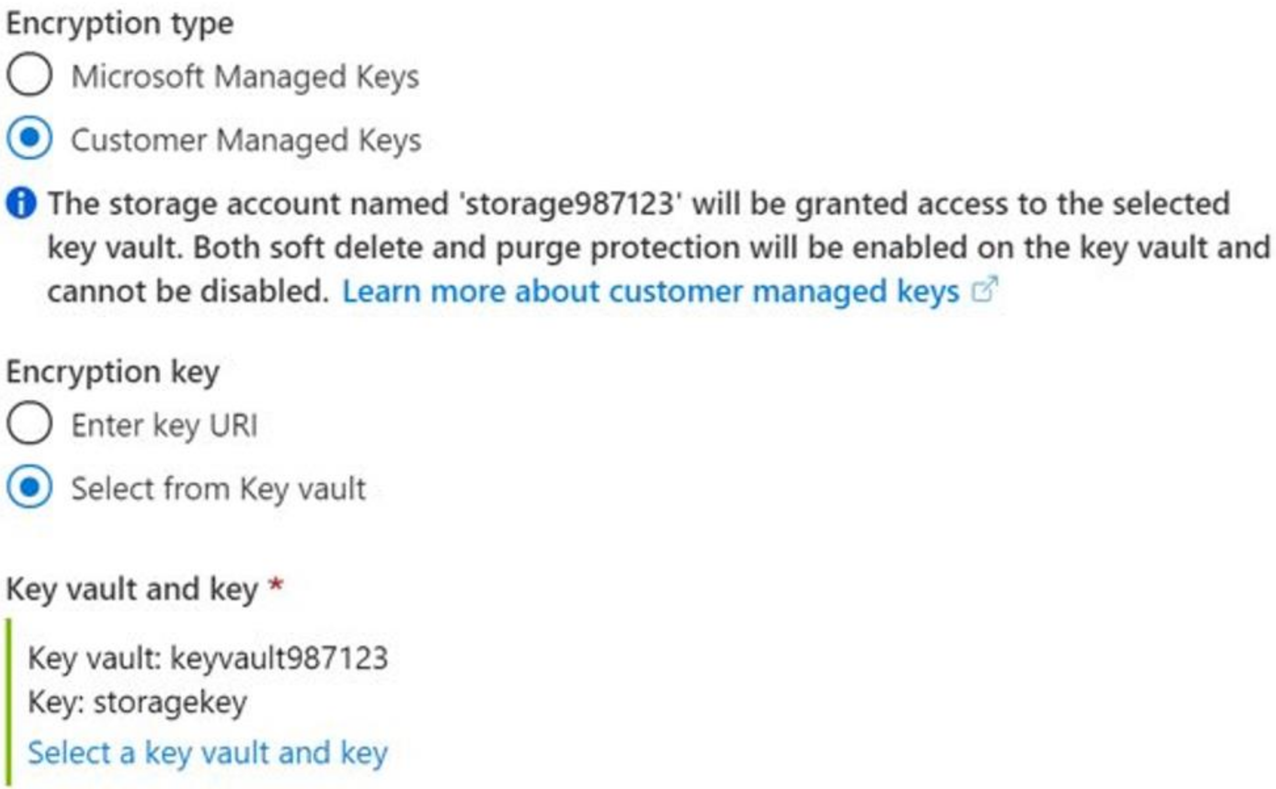
Encryption type

● Microsoft Managed Keys

○ Customer Managed Keys

Customer Managed Keys

Use Azure Key Vault to generate and store encryption keys



Encryption type

○ Microsoft Managed Keys

● Customer Managed Keys

The storage account named 'storage987123' will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and cannot be disabled. Learn more about customer managed keys

Encryption key

○ Enter key URI

● Select from Key vault

Key vault and key *

Key vault: keyvault987123
Key: storagekey

Select a key vault and key

Storage Security Best Practices

Risks:

- If a SAS is compromised, it can be used by anyone who obtains it
- If a SAS provided to a client application expires and the application is unable to retrieve a new SAS from your service, then the application's functionality may be hindered

Recommendations:

- Always use HTTPS to create or distribute a SAS
- Reference stored access policies where possible
- Use near-term expiration dates on an ad hoc SAS
- Have clients automatically renew the SAS
- Be careful with SAS start time
- Be specific with the resource to be accessed
- Your account will be billed for any usage
- Validate data written using SAS
- Don’t assume SAS is the correct choice
- Use Storage Analytics to monitor your application

Accessing Blobs and Queues using AAD

Authorize Access to Blobs and Queues using AAD

- Azure Storage supports using Azure Active Directory (Azure AD) to authorize requests to Blob and Queue storage.
- Authorizing requests against Azure Storage with Azure AD provides superior security.

Overview of Azure AD for Blobs and Queues

- When a security principal attempts to access a blob or queue resource, the request must be authorized
- The authentication step requires that an application request an OAuth 2.0 access token at runtime
- The authorization step requires that one or more RBAC roles be assigned to the security principal

RBAC Roles for Access

Built-in RBAC roles for blobs and queues

- Storage Blob Data Owner
- Storage Blob Data Contributor
- Storage Blob Data Reader
- Storage Queue Data Contributor
- Storage Queue Data Reader
- Storage Queue Data Message Processor
- Storage Queue Data Message Sender

Resource Scope

The levels at which you can scope access to Azure blob and queue resources:

- An individual container
- An individual queue
- The storage account
- The resource group
- The subscription

Access Data with an Azure AD Account

Access to blob or queue data from the Azure portal is available based on either:

- One of the storage account access keys (requires an RBAC role with *Microsoft.Storage/storageAccounts/listkeys/* action permission)
- An Azure AD account with permissions to access blob or queue data and to navigate through storage account resources

Configure Azure Storage Firewalls and Virtual Networks

Azure Storage Firewalls and Virtual Networks

Azure Storage Firewall and Virtual Networks protect storage at the network level.

Considerations:

- Configure a rule to deny access from all networks and then grant access to traffic from specific virtual network subnets only.
- If needed, configure rules to grant access to allow connections from specific internet or on-premises clients.
- Network rules are enforced on all network protocols to Azure storage, including REST and SMB.
- Once network rules are applied, they're enforced for all requests, including those based on SAS.
- Virtual machine disk traffic is not affected by network rules.
- Classic storage accounts do not support firewalls and virtual networks.

Change the Default Network Access Rule

Managing default network access rules

- By default, storage accounts accept connections from clients on any network
- To limit access to selected networks, you must first change the default action

Using the Azure portal

- Use the **Firewalls and virtual networks** settings

Using Azure CLI

- az storage account update --resource-group "myresourcegroup" --name "mystorageaccount" --default-action Deny
- az storage account update --resource-group "myresourcegroup" --name "mystorageaccount" --default-action Allow

Grant Access from a Virtual Network

- Consider available virtual network regions
- Consider required permissions

Implement virtual network rules via the Azure portal:

1. Go to the storage account you want to secure
2. Click on the settings menu called **Firewalls and virtual networks**
3. Check that you've selected to allow access from **Selected networks**
4. To grant access to a virtual network with a new network rule, under **Virtual networks**, click **Add existing virtual network,** select **Virtual networks and Subnets** options, and then click **Add**
5. To create a new virtual network and grant it access, click **Add new virtual network**, provide the necessary information, then click **Create**

Grant Access from an Internet IP Range

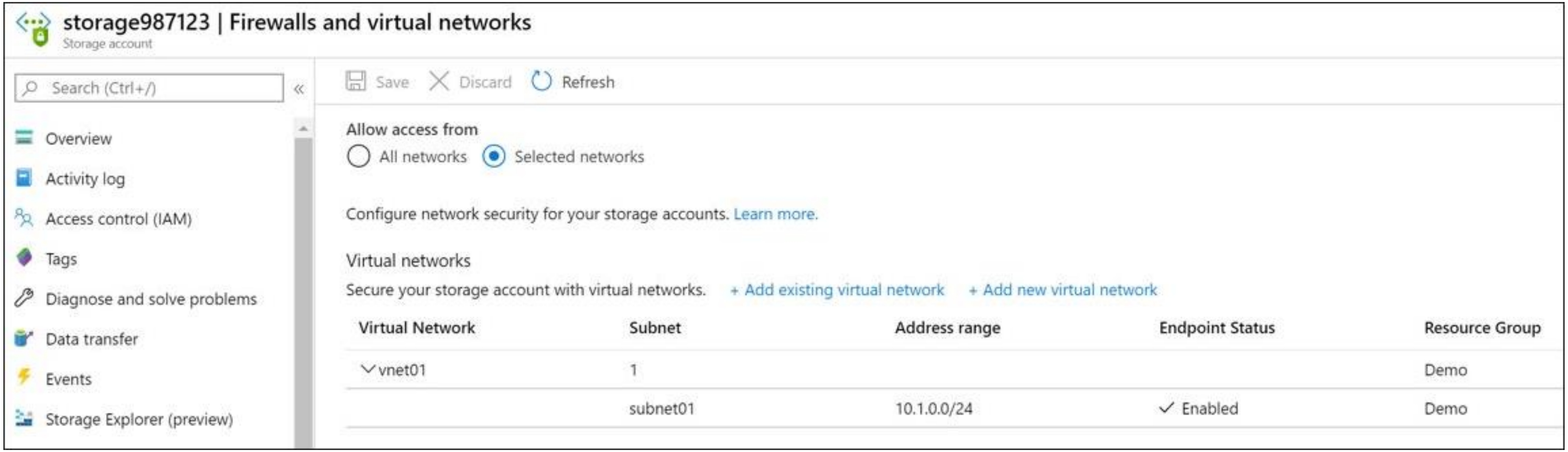
Identify the relevant internet facing IP addresses.

Configure IP network rules:

1. Go to the storage account you want to secure
2. Click on the settings menu called **Firewalls and virtual networks**.
3. Check that you've selected to allow access from Selected networks
4. To grant access to an internet IP range, enter the IP address or address range (in CIDR format) under Firewall > Address Range
5. To remove an IP network rule, click the trash can icon next to the address range
6. Click **Save** to apply your changes

Securing Storage Endpoints

- **Firewalls and virtual networks** settings allow restricting access to a storage account from specific virtual network subnets.
- **Virtual networks and their subnets** must exist in the same Azure region or the region pair as the storage account.



storage987123 | Firewalls and virtual networks

Storage account

Allow access from

○ All networks ● Selected networks

Configure network security for your storage accounts. Learn more.

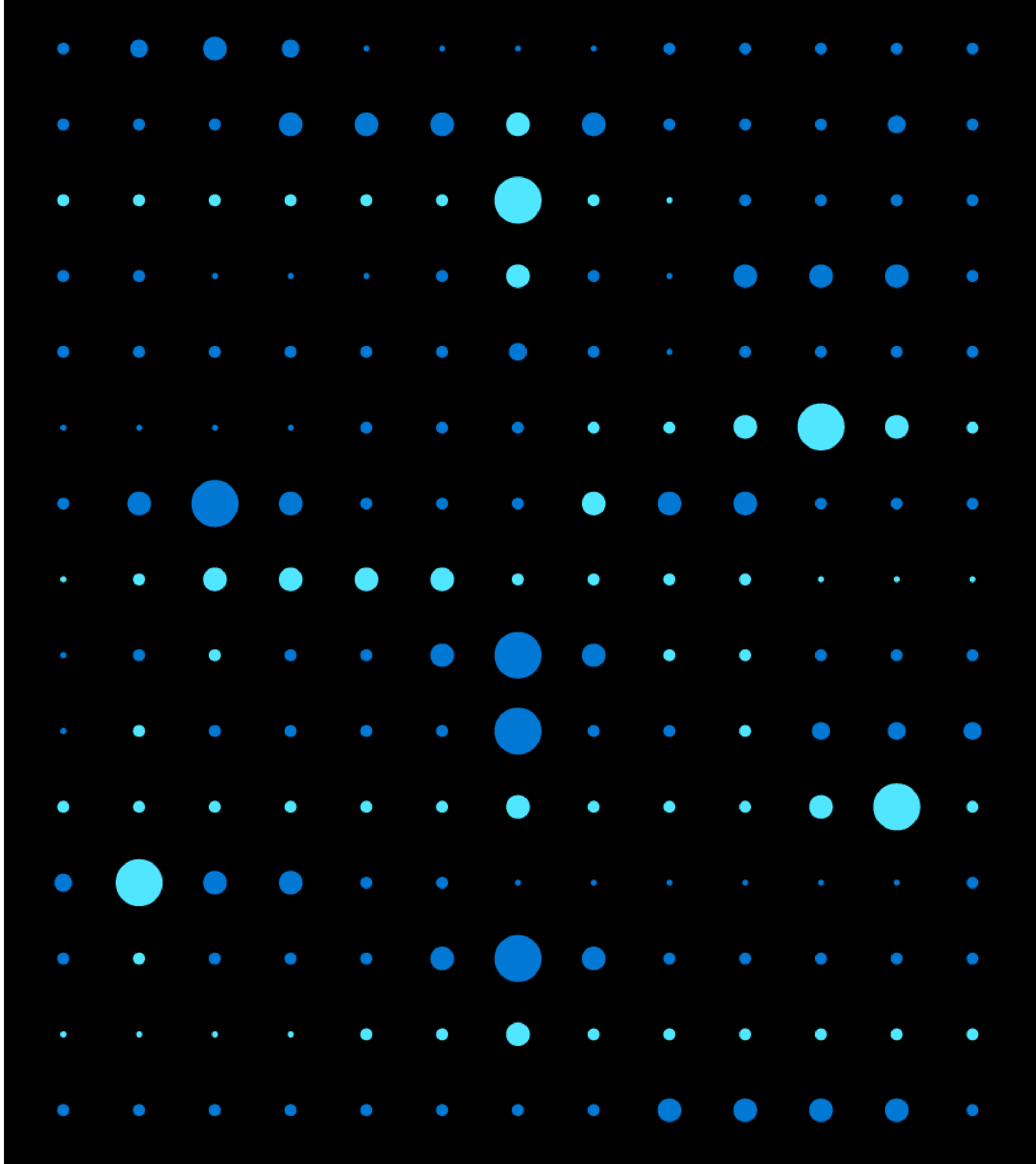
Virtual networks

Secure your storage account with virtual networks. + Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group
⌄vnet01	1			Demo
	subnet01	10.1.0.0/24	✓ Enabled	Demo

Demonstration: Securing storage endpoints

- Create a storage account
- Upload a file
- Secure the file endpoint



Managing Storage

Import and Export Service (1 of 2)

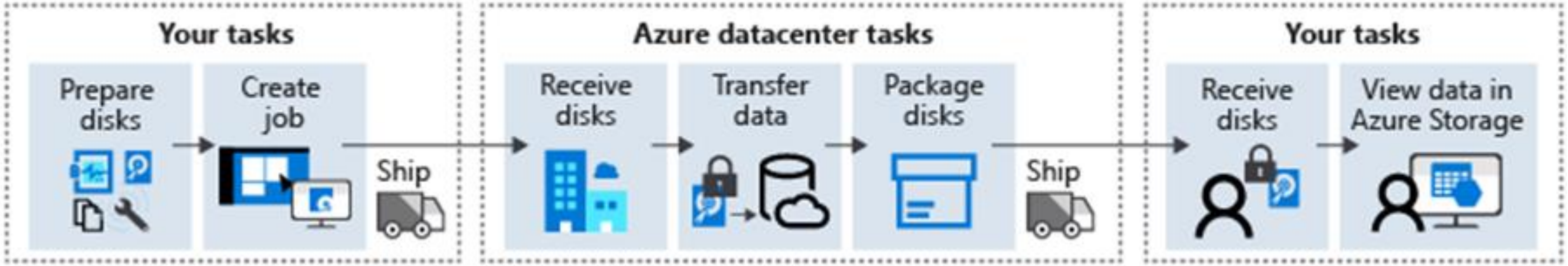
Usage cases:

- Migrating data to the cloud
- Content distribution
- Backup
- Data recovery

Import and Export Service (2 of 2)

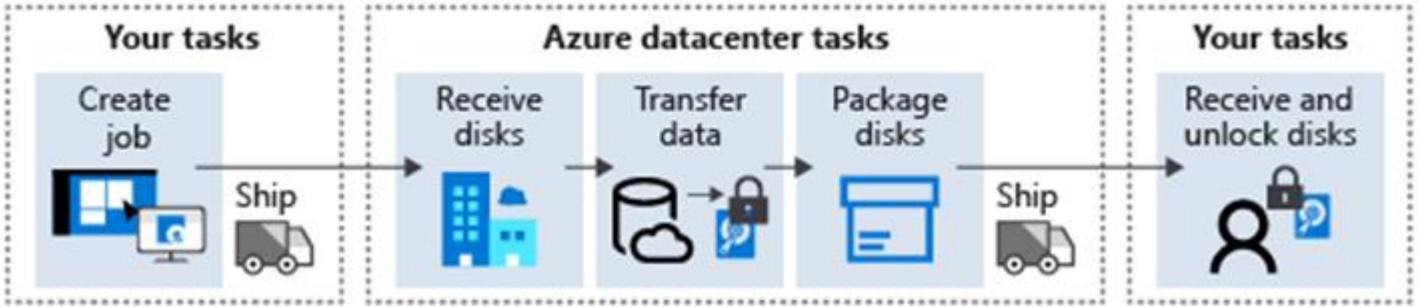
Import jobs:

Import data with Azure Import/Export



Export jobs:

Export data with Azure Import/Export



AzCopy

AzCopy v10 features:

- Supports Azure Data Lake Storage Gen2 APIs
- Supports copying an entire account (Blob service only) to another account
- Account to account copy is now using the new Put from URL APIs
- List/Remove files and blobs in a given path
- Supports wildcard patterns in a path
- Improved resiliency

Authentication options:

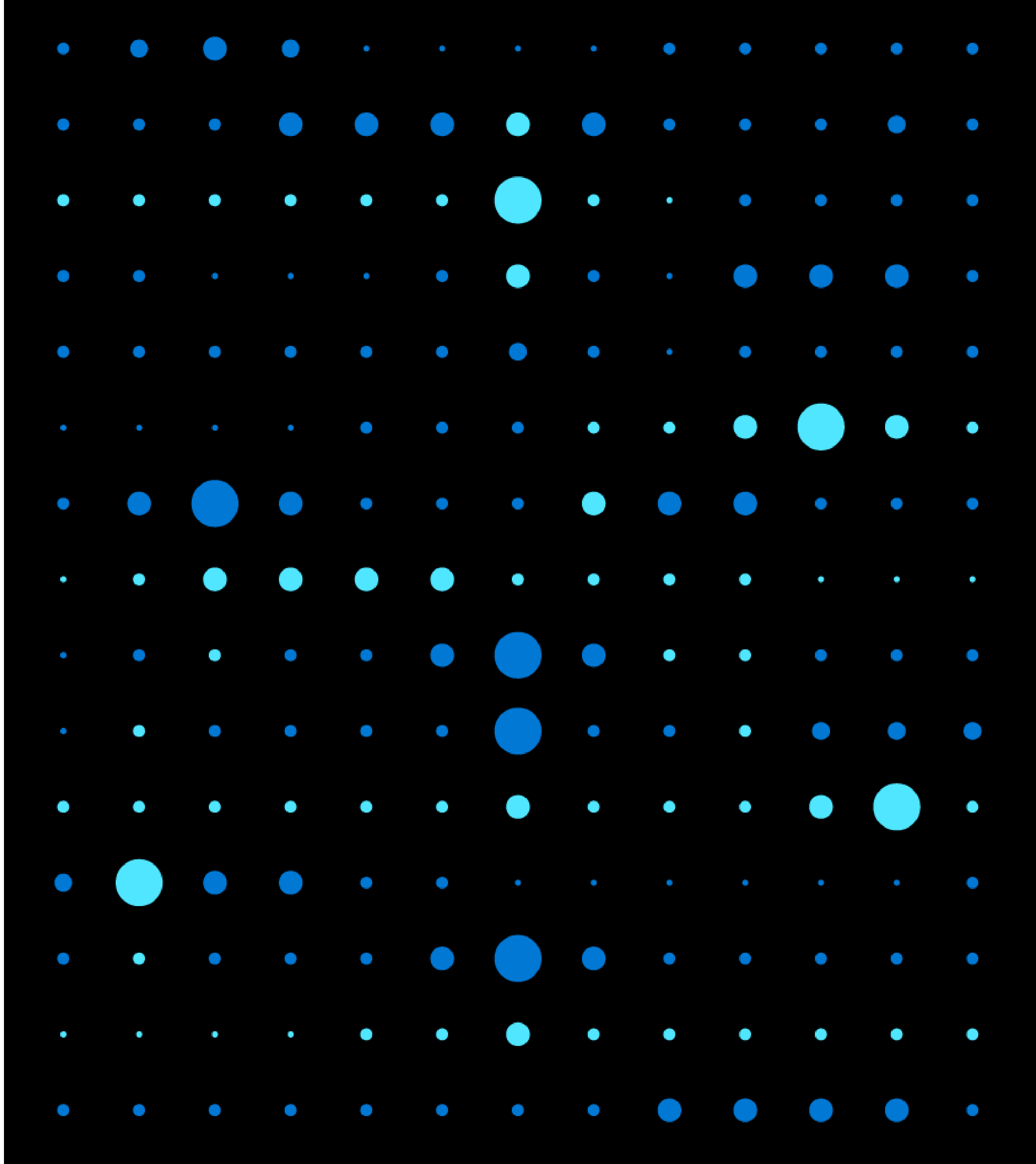
- Azure Active Directory
- SAS tokens

Data Transfer Tool Selection

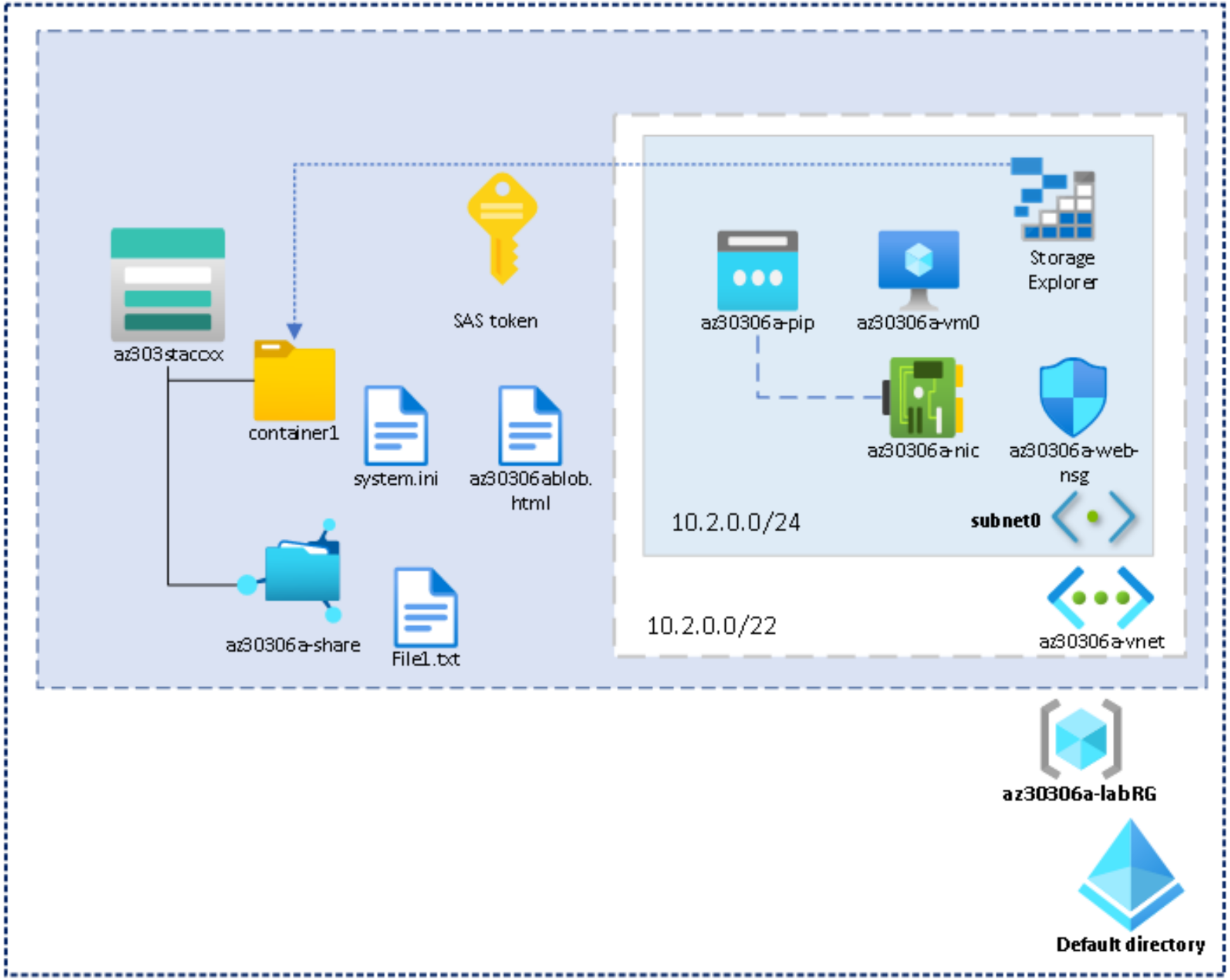
Dataset	Network Bandwidth	Solution to use
Large Dataset	Low-bandwidth network or direct connectivity to on-premises storage is limited by organization policies	Azure Import/Export for export; Data Box Disk or Data Box for import where supported; otherwise use Azure Import/Export
Large Dataset	High-bandwidth network: 1 gigabit per second (Gbps) - 100 Gbps	AZCopy for online transfers; or to import data, Azure Stack Edge, or Azure Data Box Gateway
Large Dataset	Moderate-bandwidth network: 100 megabits per second (Mbps) - 1 Gbps	Azure Import/Export for export or Azure Stack Edge for import where supported
Small Dataset: a few GBs to a few TBs	Low to moderate-bandwidth network: up to 1 Gbps	If transferring only a few files, use Azure Storage Explorer, Azure portal, AZCopy, or AZ CLI

Demonstration: AzCopy

- Install AzCopy
- Explore the help options
- Download a blob from Azure Storage
- Upload files to Azure blob storage



Lab: Implementing and configuring Azure Storage File and Blob Services



Module Review Questions

Microsoft Azure

Online Role-based training resources:

Microsoft Learn

https://docs.microsoft.com/en-us/learn/

Microsoft Azure

Thank you.