

Cloud
Computing

Caltech

Center for Technology &
Management Education

Post Graduate Program in Cloud Computing

Cloud Computing

Caltech

**Center for Technology &
Management Education**

**PG CC - Microsoft Azure Architect
Technologies: AZ:303**



Implement Storage Accounts

Learning Objectives

By the end of this lesson, you will be able to:

- Describe the Azure Storage Account
- Illustrate Storage Account Replication
- Implement Storage Account Failover
- Implement Azure Blob Storage
- Create Azure Files



Learning Objectives

By the end of this lesson, you will be able to:

- 🕒 Configure Storage Security
- 🕒 Configure Azure AD Authentication
- 🕒 Implement Azure Storage Firewalls
- 🕒 Implement Azure Virtual Networks



A Day in the Life of an Azure Architect

You are working for an organization as an Azure Architect that wants to "lift and shift" an application to the cloud. The application basically deals with massive amounts of unstructured data.

- This application supports streaming video and audio and should be accessible from anywhere. Also, the application is required to store data for backup and restore, disaster recovery, and archiving.
- It will be a plus point if the solution can store multiple copies of the data to avoid failure or power outage.



A Day in the Life of an Azure Architect

- Additionally, the company is looking for a solution that allows users to access files via the Server Message Block (SMB) protocol and mount file shares on Windows.
- The company would also need an option that can provide delegated access to resources and also grants access to clients without sharing storage access key that provides full access to the account.

Being an Architect, you are now supposed to advise the organization with azure solutions that will help achieve the given scenario.

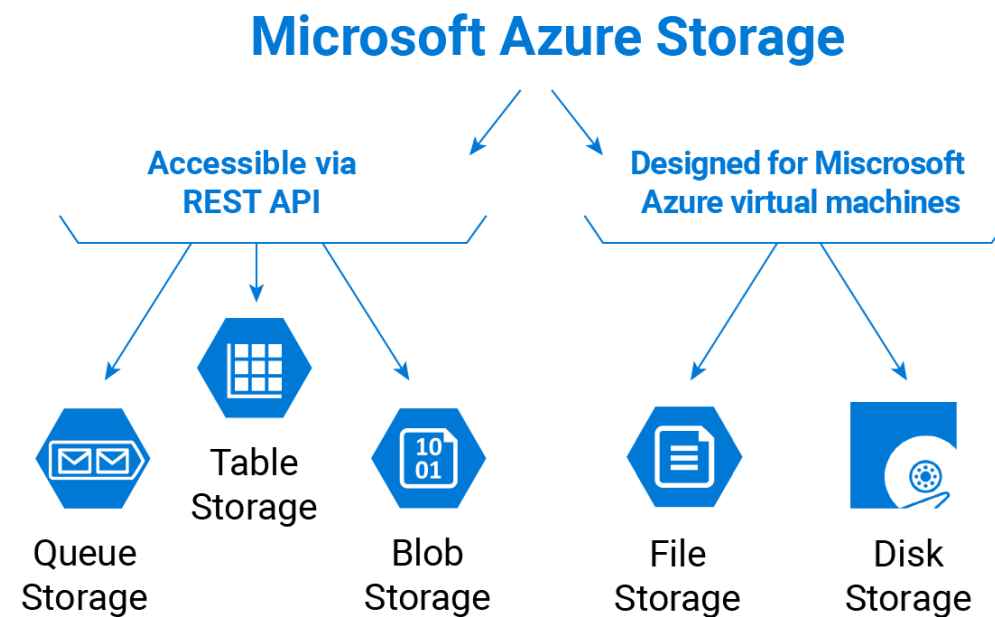


Storage Account

Azure Storage

It is a cloud storage platform designed for modern data storage scenarios.

A massively scalable object store for data objects, as well as disk storage for Azure virtual machines, is available via core storage services (VMs).



The service encrypts all data written to an Azure storage account.

image source: <https://docs.microsoft.com/en-in/>

Azure Storage Services

These are the Azure Storage services:

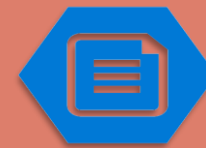
Azure Blobs

A text and binary data object store with huge scalability.



Azure Tables

A schemaless NoSQL store for structured data storage.



Azure Files

For cloud or on-premise deployments, managed file shares are available.



Azure Queues

A messaging store that allows application components to communicate reliably.

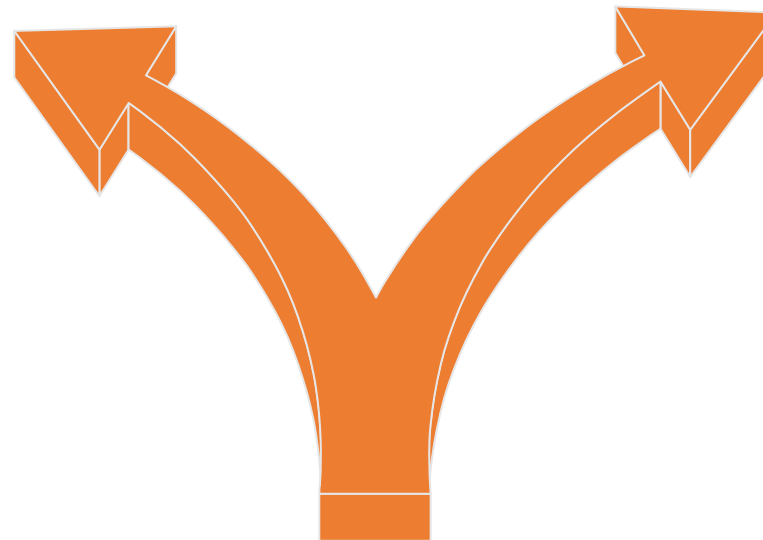
Azure Storage Services

Storage Services	Description
Azure Blobs	Allow unstructured data to be stored and accessed as block blobs on a huge scale
Azure Files	Use the industry standard Server Message Block (SMB) protocol; the user can access fully managed cloud file shares from anywhere
Azure Tables	Allow the user to store structured NoSQL data in the cloud and provides a schemaless key/attribute store
Azure Queues	Asynchronous message queueing between application components is possible

Standard and Premium Storage Accounts

Storage Accounts are of two types:

Standard Storage Account



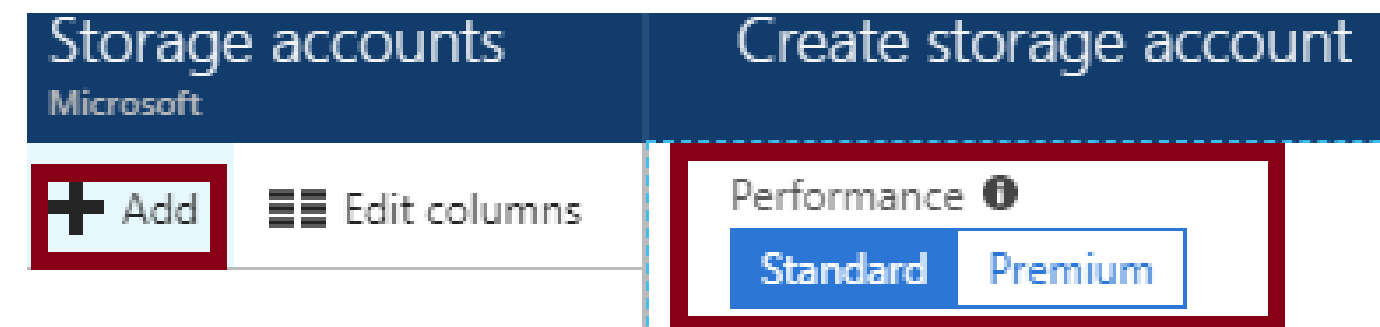
Premium Storage Account

Storage Accounts

Standard Storage Account

Most apps use standard storage, which is less expensive and slower.

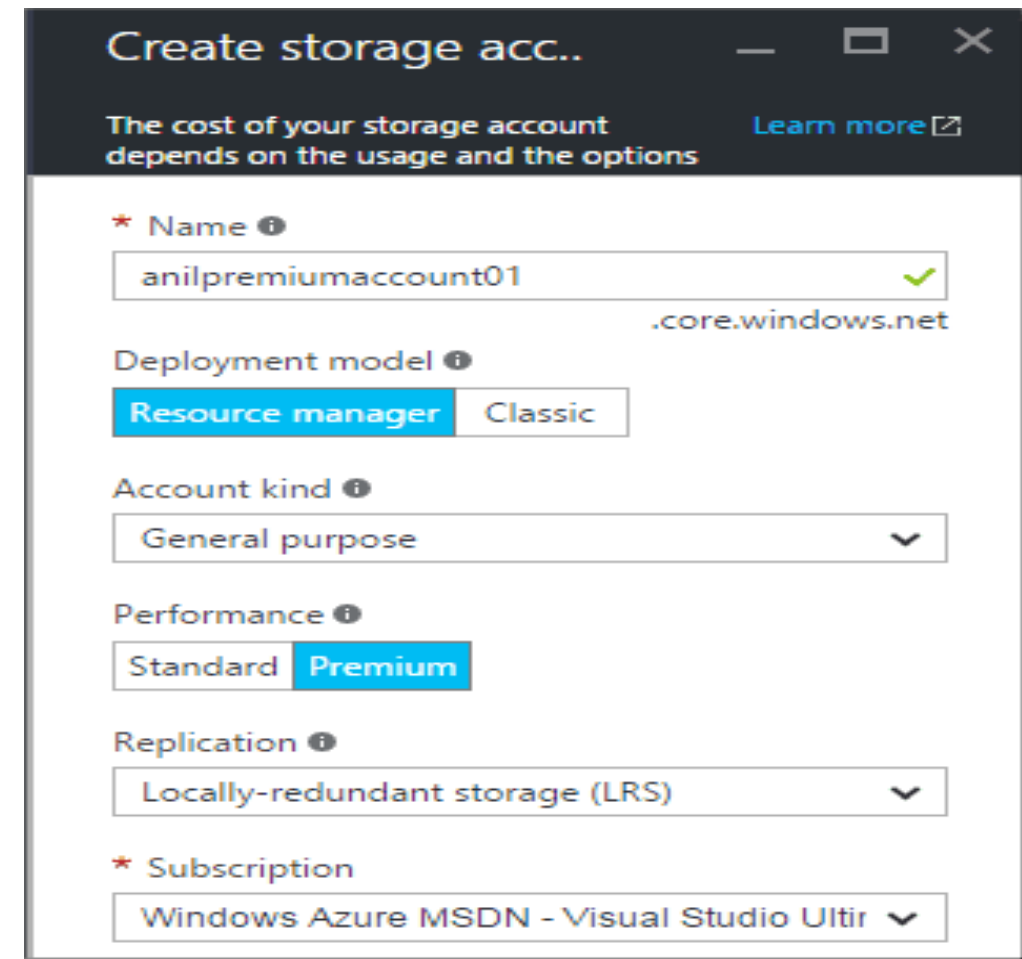
- The user is in charge of the data consumed.
- It is the data on the disk that is important, not its size.
- The standard storage performance tier can store Tables, Queues, Files, Blobs, and Azure virtual machine disks.



Premium Storage Account

Transaction fees are not applied on premium disks.

- It is more of a flat-fee arrangement.
- The user is only paying for the size of the disk, not for the written data.
- Azure virtual machine disks are supported by the Premium storage performance tier only.

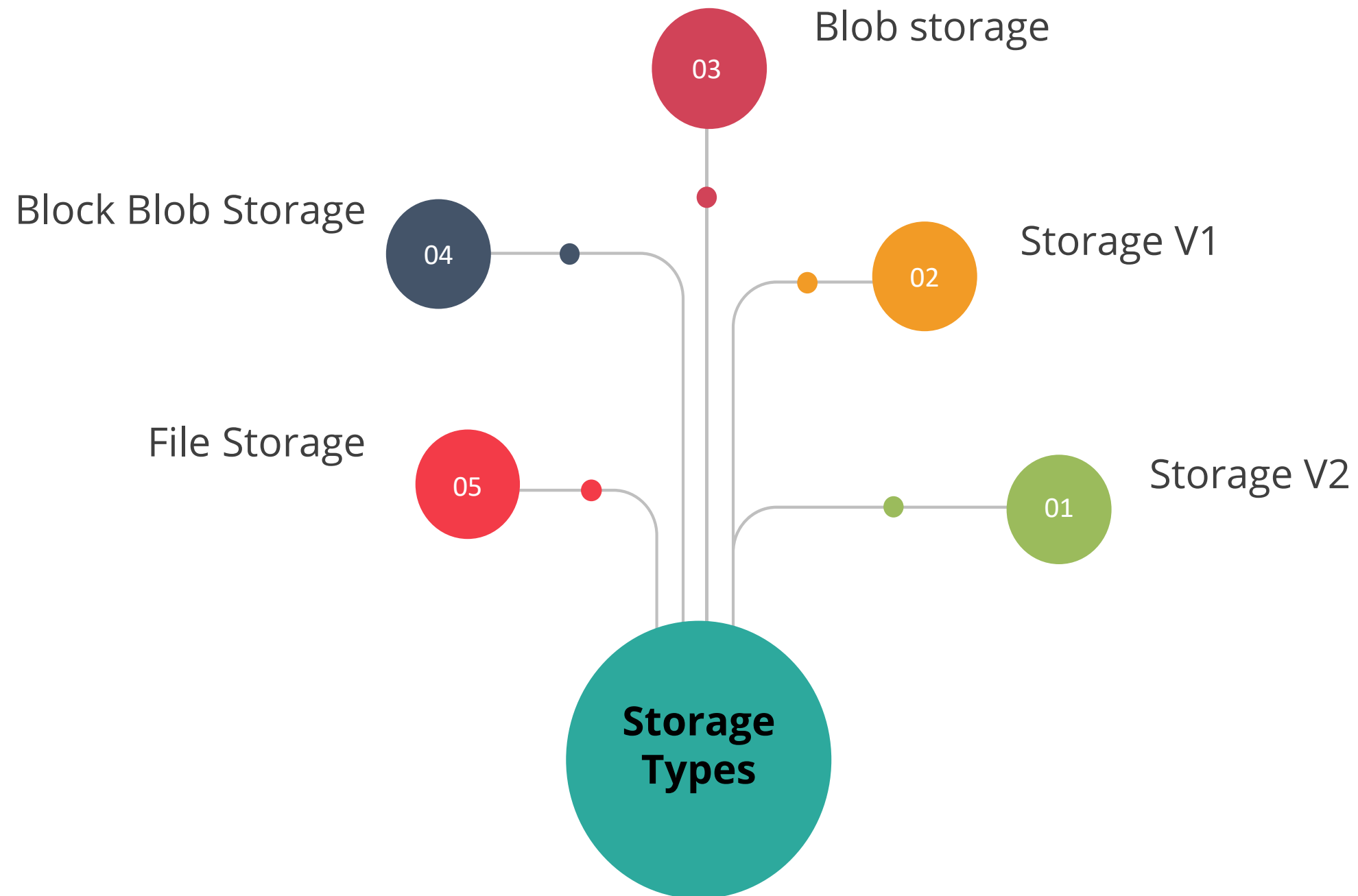


The screenshot shows the 'Create storage account' wizard in the Azure portal. The title bar reads 'Create storage acc..' with standard window controls. Below the title, a message states: 'The cost of your storage account depends on the usage and the options' with a 'Learn more' link. The form contains the following fields:

- Name:** A text input field containing 'anilpremiumaccount01' with a green checkmark icon on the right. Below the input, the text '.core.windows.net' is displayed.
- Deployment model:** Two radio buttons, 'Resource manager' (selected) and 'Classic'.
- Account kind:** A dropdown menu showing 'General purpose'.
- Performance:** Two radio buttons, 'Standard' and 'Premium' (selected).
- Replication:** A dropdown menu showing 'Locally-redundant storage (LRS)'.
- Subscription:** A dropdown menu showing 'Windows Azure MSDN - Visual Studio Ultr'.

Storage Types

There are five types of Storage:



Storage Types

Storage types	Supported services	Supported performance tiers	Replication options
Blob storage	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)
File storage	Files only	Premium	LRS, ZRS (limited regions)

Accessing Storage



- A storage account gives user's data its own namespace.
- Every item the user saves on Azure Storage has a unique account name as part of its address.
- The endpoints for a user's storage account are made up of the account name and the Azure Storage service endpoint.

Accessing Storage

The endpoint format for each Azure Storage service is listed in the table below:

Storage Services	Endpoint
Azure Blobs	https://<storage-account>.blob.core.windows.net
Azure Files	https://<storage-account>.file.core.windows.net
Azure Tables	https://<storage-account>.table.core.windows.net
Azure Queues	https://<storage-account>.queue.core.windows.net

Storage Account Replication

Storage Account Replication

Storage Account Replication stores multiple copies of user data to protect from planned and unplanned events such as:



Hardware failures

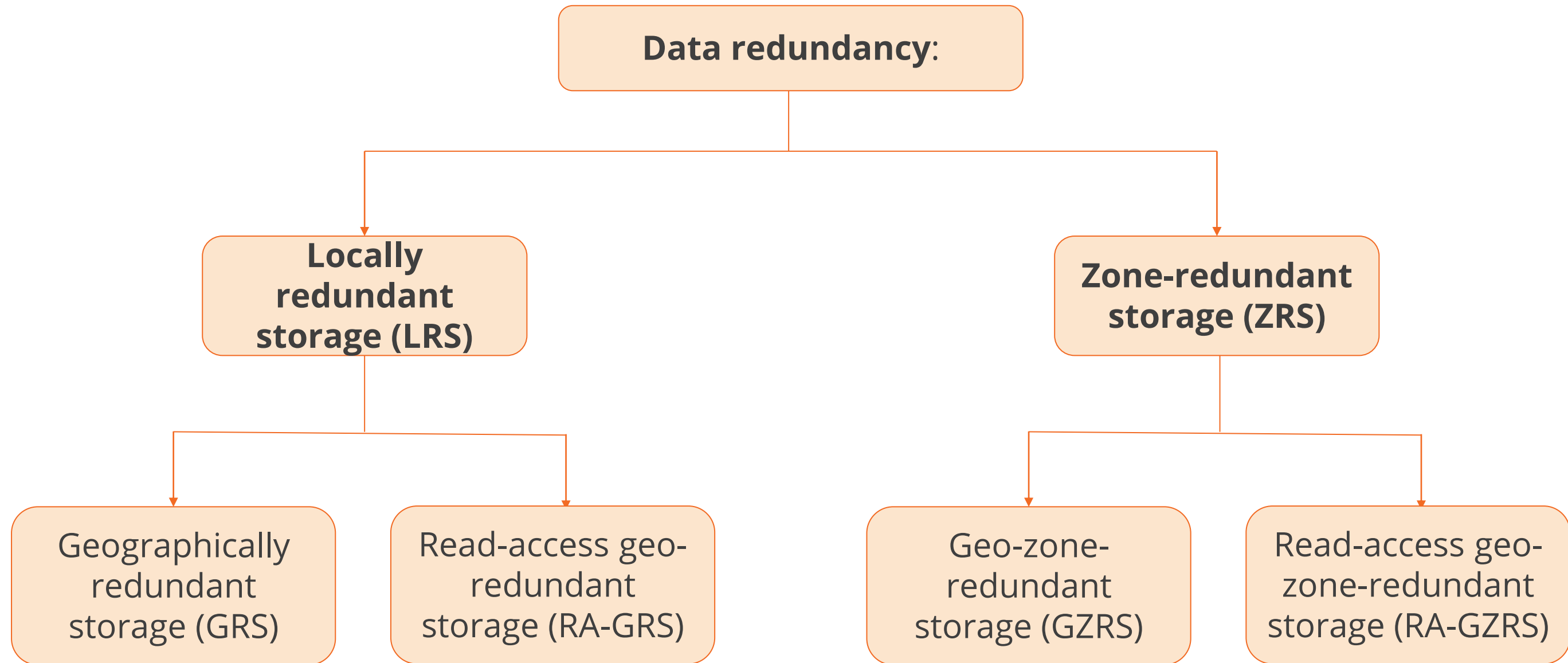
Network or power outages

Massive natural disasters

It ensures user storage account have their backup even in the case of failure.

Storage Account Replication

Below are the types of replication models:



Data in an Azure Storage account is always replicated three times in the primary region.

Locally Redundant Storage

This type of Replication model copies data synchronously three times within a single physical location in the primary region.



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

image source: <https://docs.microsoft.com/en-in/>

Zone Redundant Storage

This type of Replication model copies data synchronously across three Azure availability zones in the primary region.

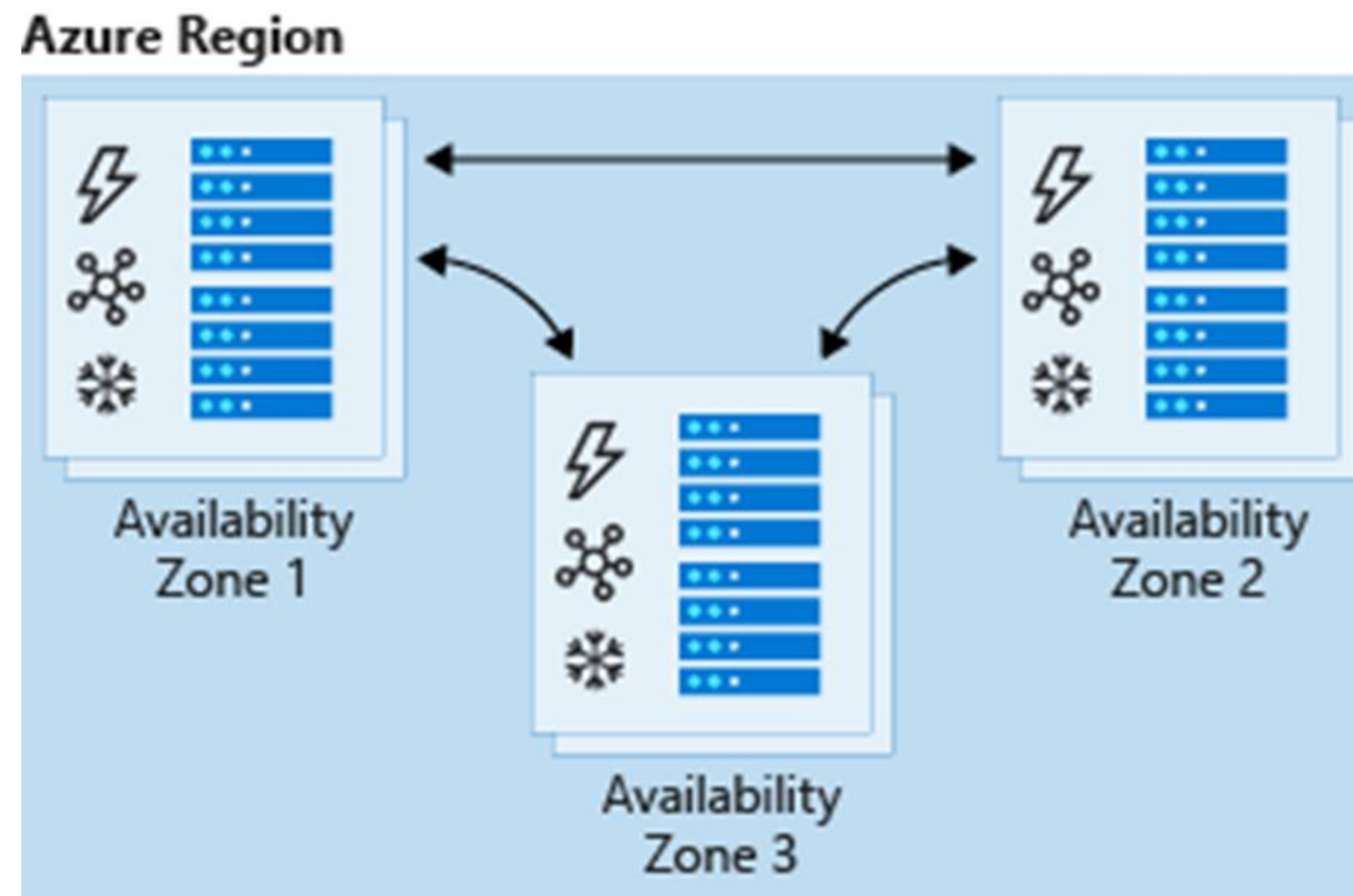


image source: <https://docs.microsoft.com/en-in/>

Geographically Redundant Storage

This type of Replication model copies data synchronously three times within a single physical location in the primary region using LRS.

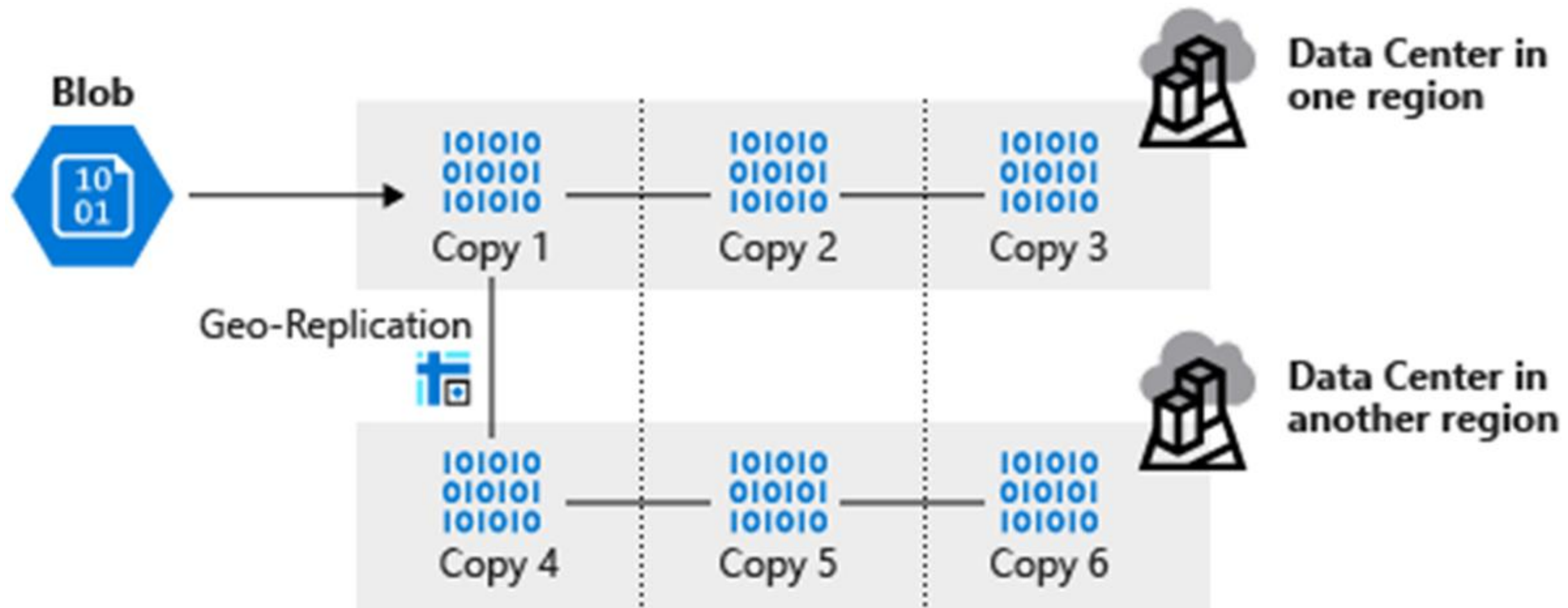


image source: <https://docs.microsoft.com/en-in/>

Geographically Redundant Storage

it copies your data asynchronously in a secondary region hundred of miles from the primary region to a single physical location.

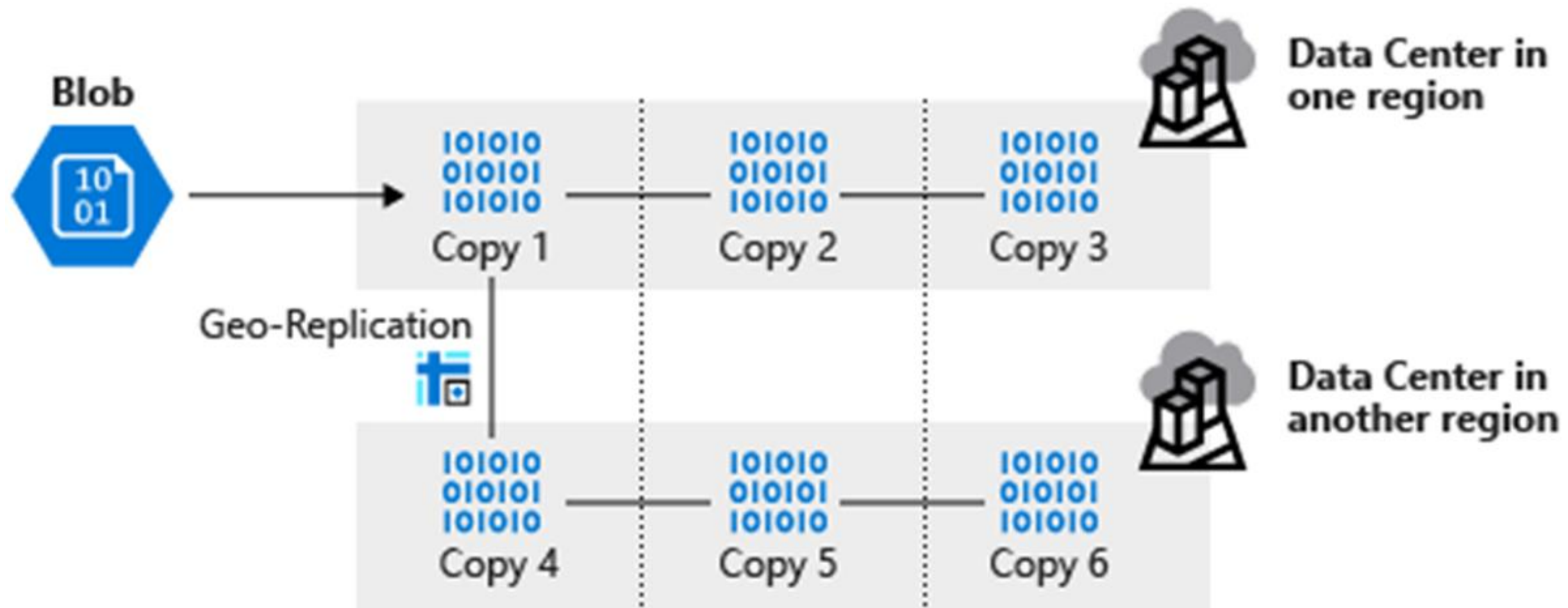


image source: <https://docs.microsoft.com/en-in/>

Read-access Geo-redundant Storage

When the read access is enabled to the secondary region, data is available to be read, where the primary region becomes unavailable.

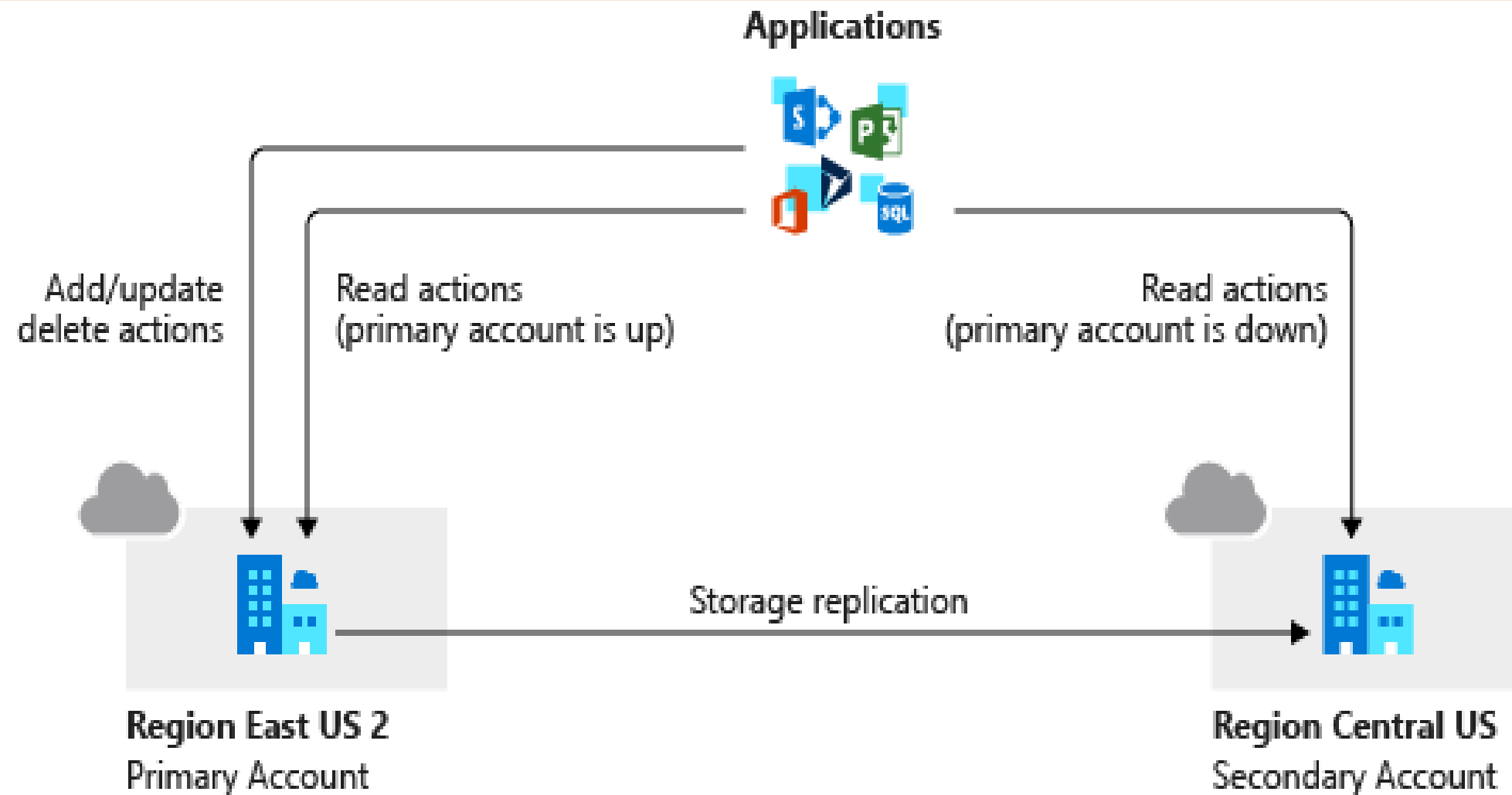


image source: <https://docs.microsoft.com/en-in/>

Azure Storage Account Failover

Storage Account Failover

Storage Account Failover prevents user against unplanned service outages.



- It is an integral part of disaster recovery plan
- It helps you in the event of primary endpoint becoming unavailable

Storage Account Failover

If the primary endpoint becomes impossible to access, the user can start the storage account failover process.

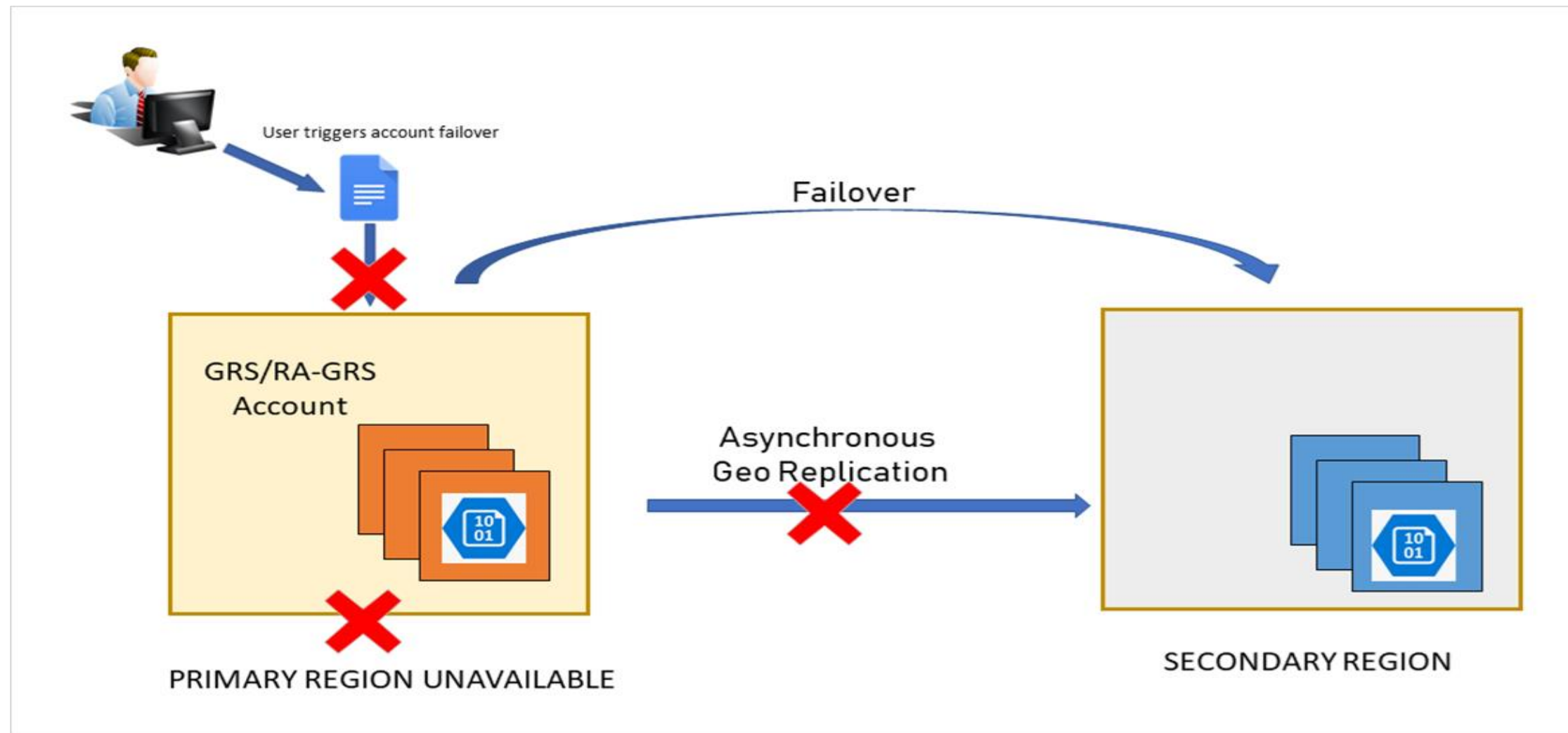
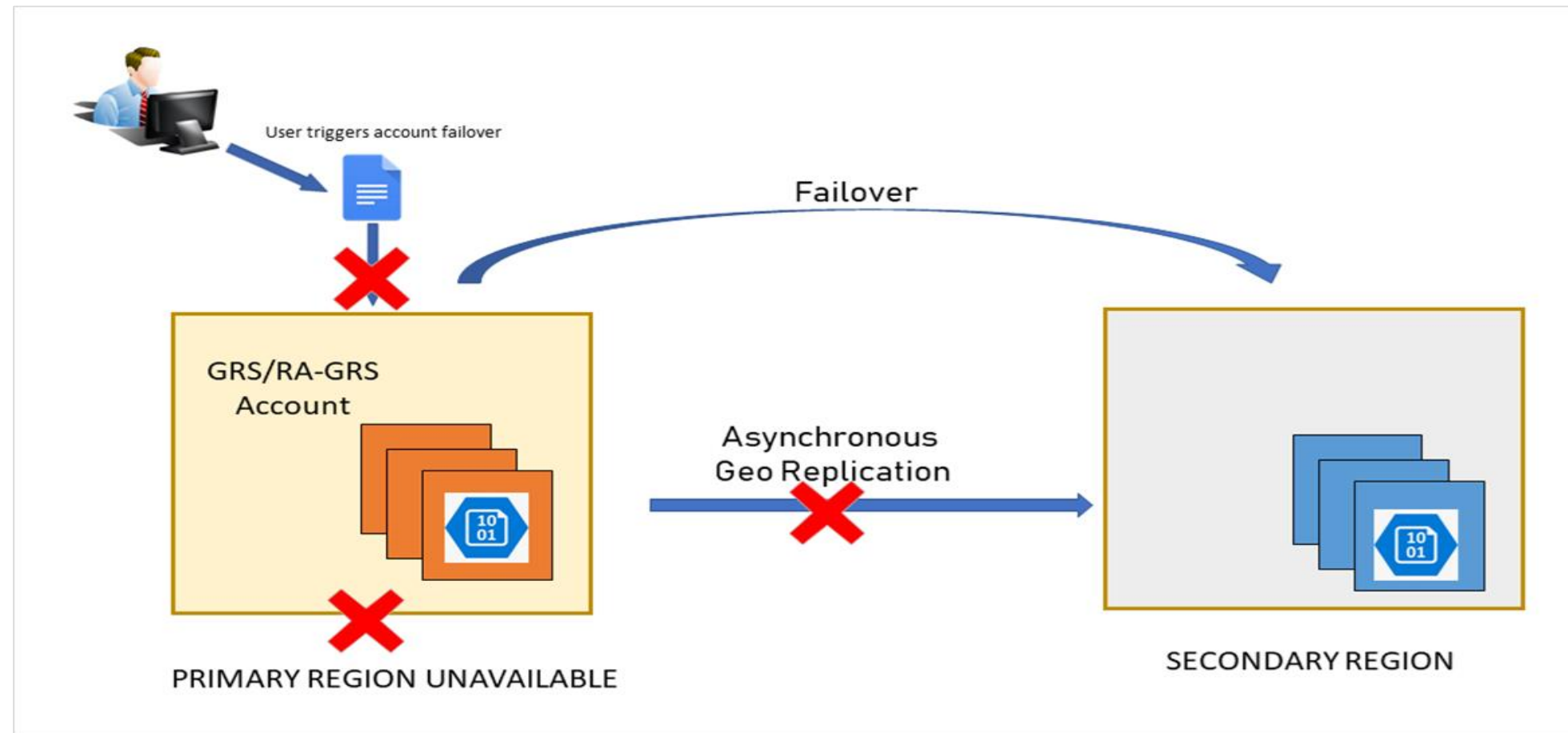


image source: <https://docs.microsoft.com/en-in/>

Storage Account Failover

The failover updates the secondary endpoint to become the primary endpoint for your storage account.

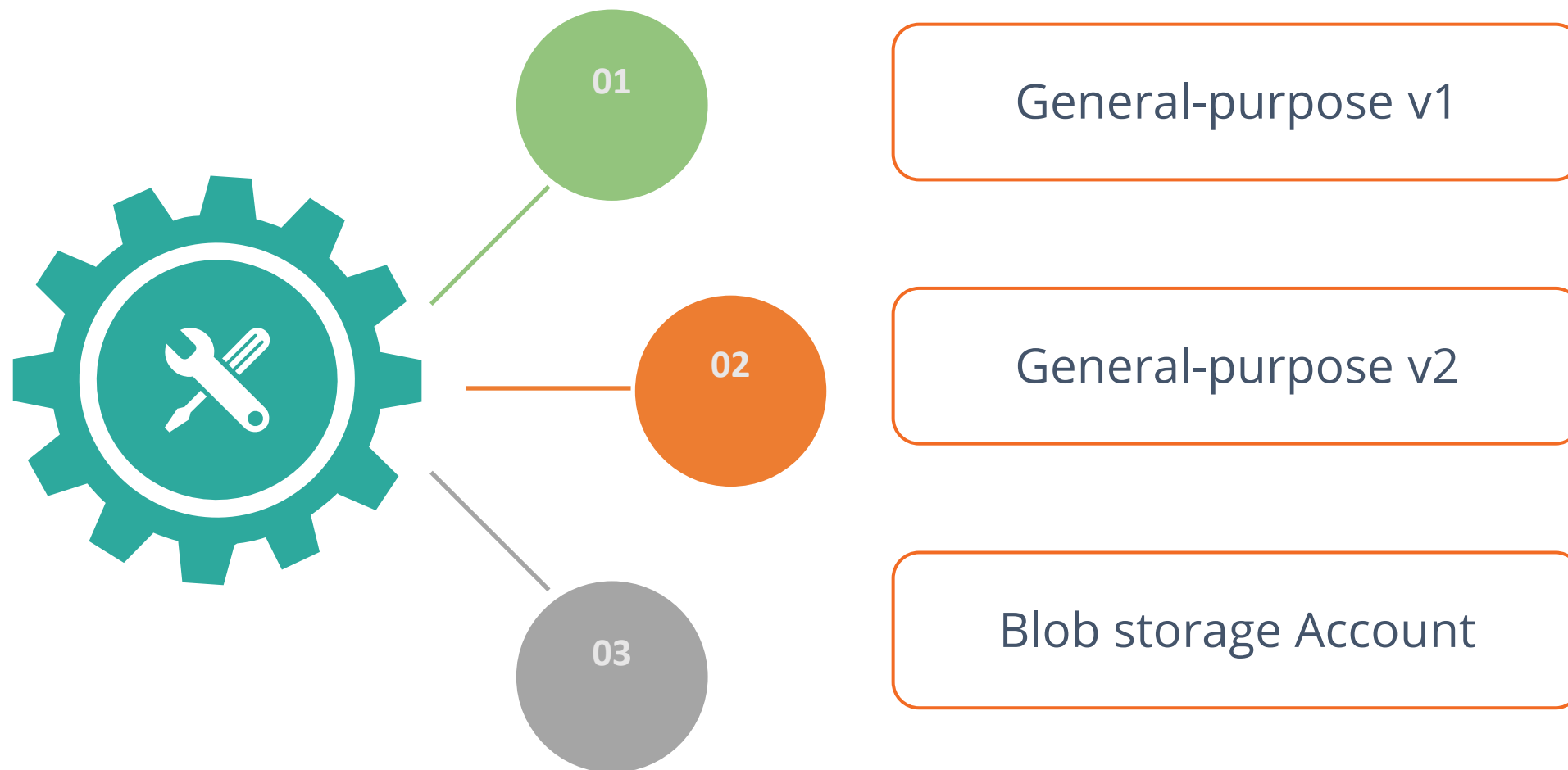


Once the failover is complete, clients can begin writing to the new primary endpoint.

Storage Account Failover

Azure Storage supports account failover for geo-redundant storage accounts.

Storage Account Failover is available for the following account types:



Blob Storage

Blob Storage

It is an object storage solution for cloud, which is optimized for storing unstructured data.

It can store any type of text or binary data.



Blobs

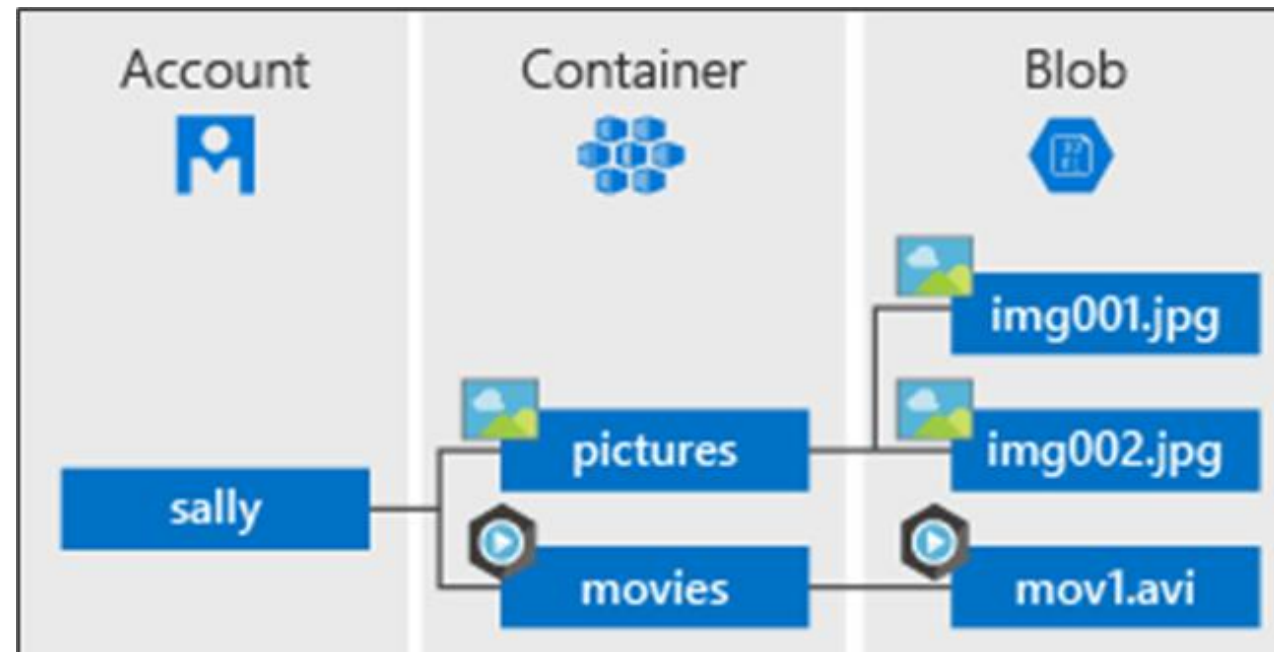
REST-based object storage for unstructured data

[Learn more](#)

[Explore data using Azure AD preview](#)

image source: <https://docs.microsoft.com/en-in/>

Blob 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, and archiving
- Storing data for analysis by an on-premise or Azure-hosted service

image source: <https://docs.microsoft.com/en-in/>

Blob Containers

Blob service
ashstorage12345

+ Container

Refresh

Delete

New container

* Name

blobstorage

Public access level ⓘ

Private (no anonymous access) ^

Private (no anonymous access)

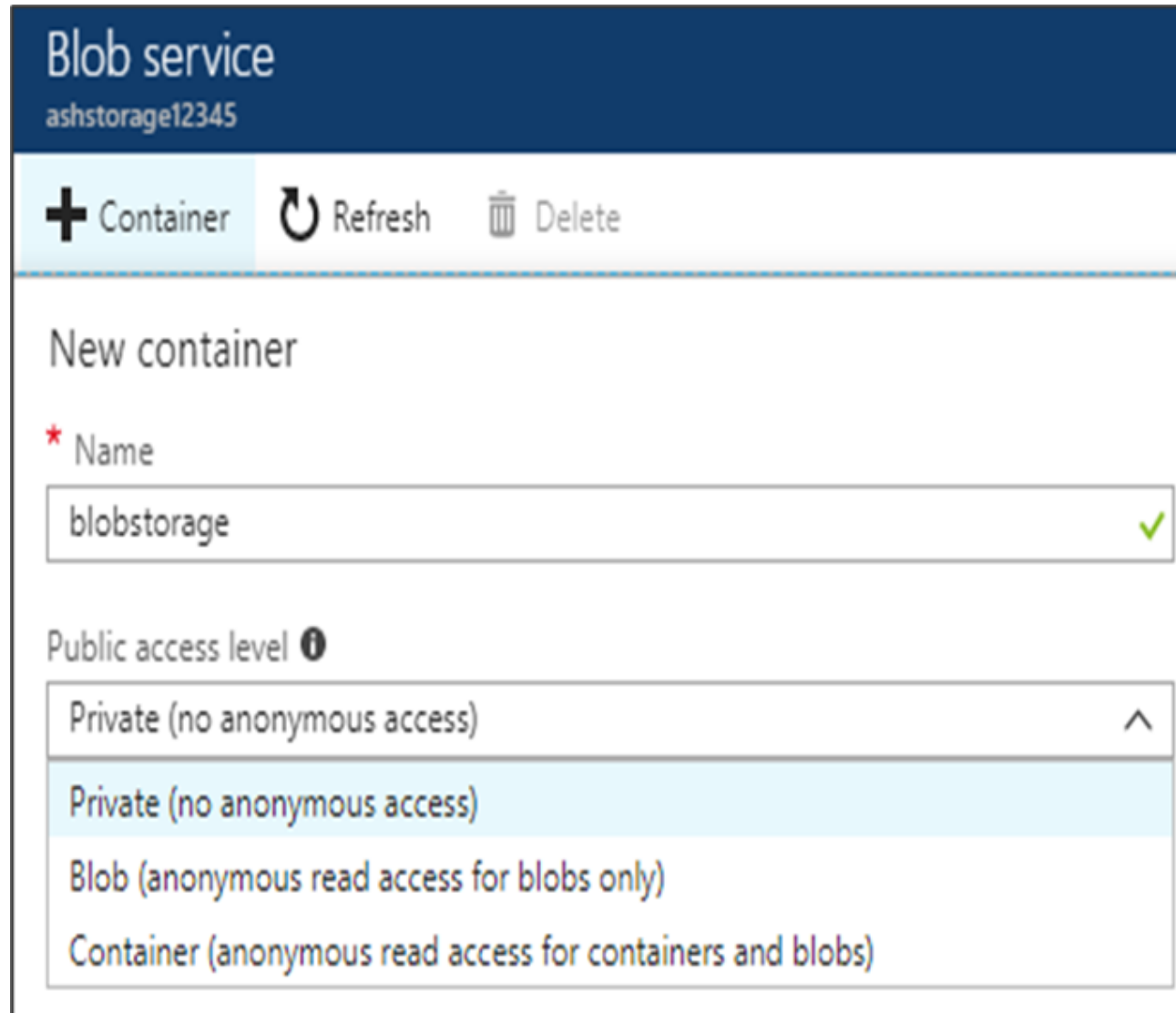
Blob (anonymous read access for blobs only)

Container (anonymous read access for containers and blobs)

- A container organizes a set of blobs.
- A storage account can include an unlimited number of containers.
- A container can store an unlimited number of blobs.

Blob Access Policies

Below are a few access policies to access blob storage account:



Blob service
ashstorage12345

+ Container Refresh Delete

New container

* Name
blobstorage ✓

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)

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 Performance Tiers

Below are blob performance tiers for storage accounts:

Hot tier (inferred)

Optimized for frequent access of objects in the storage account

Cool tier

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) ^

Hot (Inferred)

Cool

Archive

You can switch between these access tiers at any time.

Blob Lifecycle Management

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

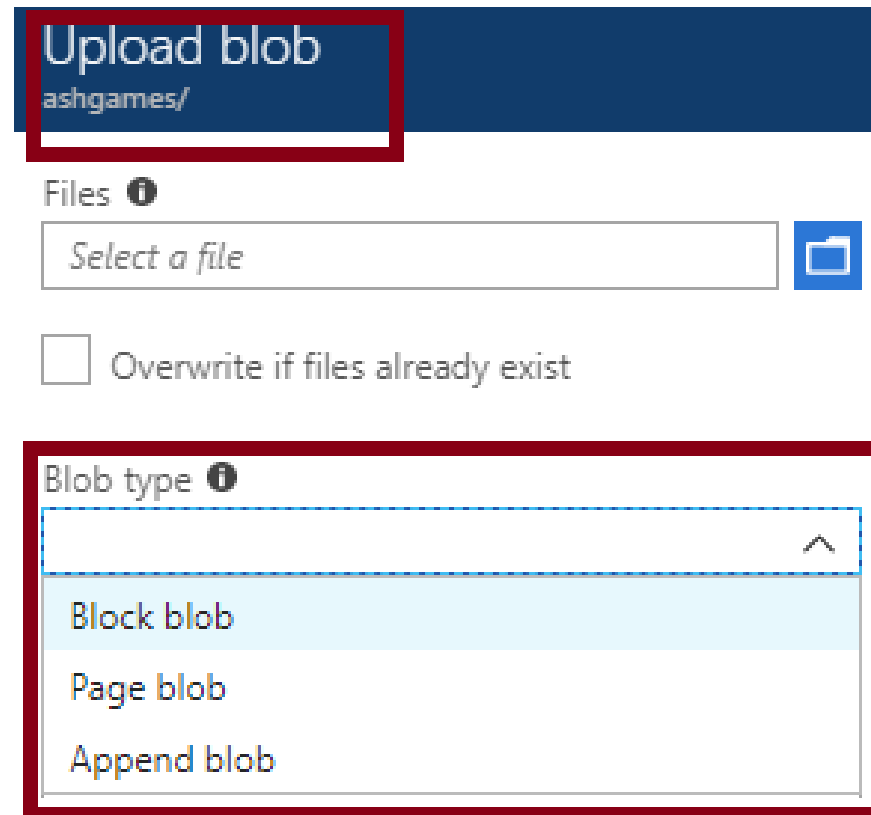
30 ✓

Policy:

- 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 life cycles
- 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)

Uploading Blob

User need to select the blob type to upload a blob.



Upload blob
ashgames/

Files ⓘ

Select a file

☐ Overwrite if files already exist

Blob type ⓘ

- Block blob
- Page blob
- Append blob

- **Block blobs (default)** - useful for storing text or binary files
- **Page blobs** - More efficient for frequent read/write operations
- **Append blobs** - useful for logging scenarios

User cannot change a blob type once it has been created.

Blob Access Policies

The screenshot shows the 'scripts - Access policy' configuration page in the Azure portal. The left-hand navigation pane includes 'Overview', 'Access Control (IAM)', and a 'Settings' section with 'Access policy' highlighted. The main content area features a 'Save' button at the top. Below it is the 'Add policy' section, which contains an 'Identifier' text input field. To the right of the identifier is a 'Permissions' list with checkboxes for 'Read', 'Add', 'Create', 'Write', 'Delete', and 'List'. At the bottom of the 'Add policy' section are 'Start time' and 'Expiry time' fields, each consisting of a date picker (YYYY-MM-DD) and a time zone dropdown menu (h:mm:ss A, UTC-07:00 --- Current Time Zone...).

- Provides an additional level of control over server-side SAS
- Groups SAS to provide additional restrictions for signatures bound to the policy
- Supported for Blob containers, File shares, Tables, and Queues

Storage Pricing

Premium blobs follow the pricing model for the managed discs while standard page blobs are billed for the size and transactions used.

Block Blobs	Files
Scalable object storage for documents, videos, pictures, and unstructured text or binary data. Choose from Hot, Cool, or Archive tiers.	Fully managed file shares in the cloud, accessible via standard Server Message Block (SMB) protocol. Enables sharing files between applications using Windows APIs or REST API.
Prices for locally redundant storage (LRS) Archive Block Blob start from:	Prices for LRS File storage start from:
\$0.002 /GB per month	\$0.06 /GB per month
See Pricing >	See Pricing >

- Storage costs
- Blob storage
- Data access costs
- Transaction costs
- Geo-Replication data transfer costs
- Outbound data transfer costs
- Changing the storage tier

Assisted Practice

Create a Blob Storage

Duration: 10 Min.

Problem Statement:

On Microsoft's data storage platform, you're given a project to construct a blob storage to store massive amounts of unstructured data.

Assisted Practice: Guidelines

Steps to create a blob storage:

1. Log into the Azure portal
2. Create a container
3. Create a Blob storage



Azure Files

Azure Files

Azure Files provides actively managed cloud file shares that can be accessed using the industry standard Server Message Block (SMB) or Network File System (NFS) protocols.

Azure Files are used to:

- Replace and supplement on-premise file servers
- Lift and shift applications
- Azure File sync
- Shared applications
- Diagnostic data
- Tools and utilities



Files

File shares that use the standard SMB 3.0 protocol

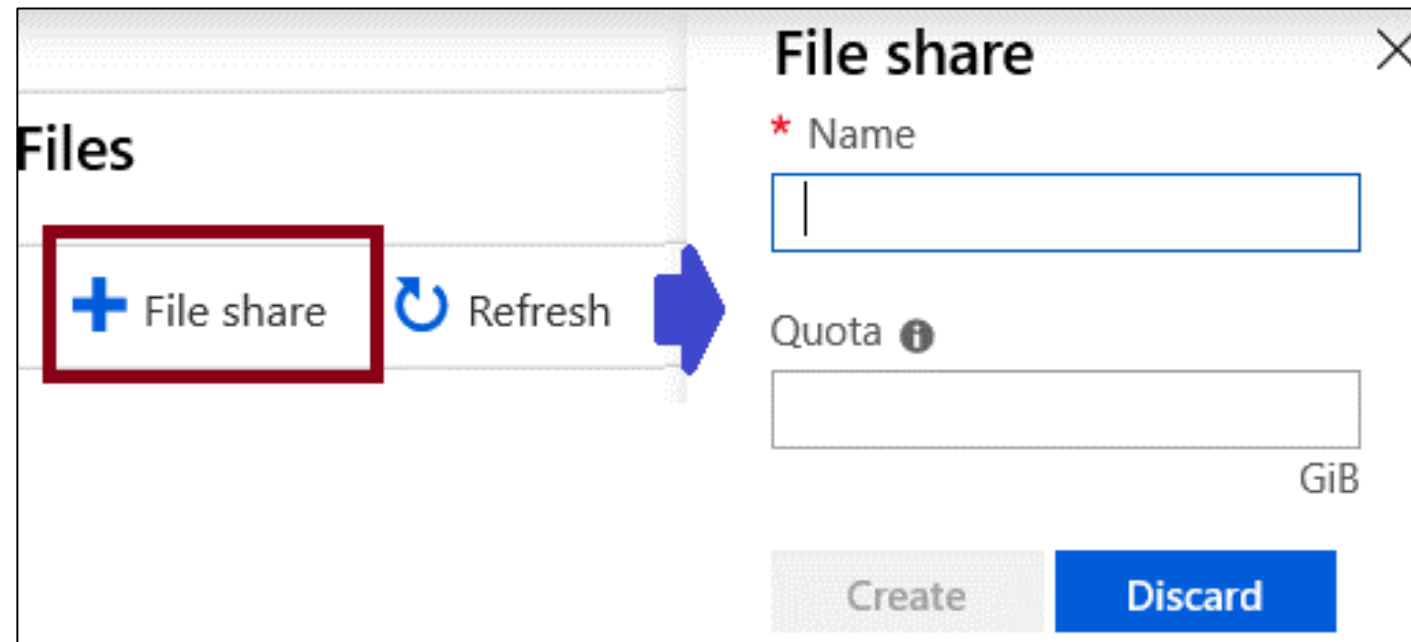
[Learn more](#)

Files vs. Blobs

Feature	Description	When to use
Azure Files	SMB interface, client libraries, and a REST interface that allows access from anywhere to stored files.	<ul style="list-style-type: none">• 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 and accessed at a massive scale in block blobs.	<ul style="list-style-type: none">• Support streaming and random-access scenarios• Access application data from anywhere

Creating File Share

► Portal:



The screenshot shows the Azure Portal interface for creating a file share. On the left, under the 'Files' section, the '+ File share' button is highlighted with a red rectangular box. A blue arrow points from this button to a 'File share' dialog box on the right. The dialog box has a title bar with a close button (X). It contains a 'Name' field with a red asterisk, a 'Quota' field with an information icon, and 'Create' and 'Discard' buttons at the bottom.

► Powershell:

```
# Retrieve storage account and storage account key
$storageContext = New-AzStorageContext <storage-account-name>
<storage-account-key>
# Create the file share, in this case "logs"
$share = New-AzStorageShare logs -Context $storageContext
```

Mapping File Shares (Windows)

The methods to use an Azure file share with Windows are as follows:

- Mapping drive letter
- UNC path
- Account user
- Storage account key

Connect

test

Windows Linux MacOS

Drive letter

Z

To connect to this file share from a Windows computer, run these PowerShell commands:

Alternatively, run this command if the key doesn't begin with a forward slash:

```
net use Z: \\rgtest11.file.core.windows.net\test /u:AZURE\rgtest11 k3b JEEy0YX41g HtX J==
```

When connecting from a computer from outside Azure, remember to open outbound TCP port 445 in your local network. Some Internet service providers may block port 445. Check with your service provider for details.

✓ Ensure port 445 is open

Assisted Practice

Create an Azure File Share

Duration: 10 Min.

Problem Statement:

You've been assigned a project to construct an Azure file share that allows users to access files via the Server Message Block (SMB) protocol and mount file shares on Windows.

Assisted Practice: Guidelines

Steps to create an Azure File Share:

1. Log into the Azure portal
2. Creating a New storage account in the Azure portal
3. File share listing
4. New file share
5. View the new file share



Storage Security

Storage Security

High-level security capabilities for Azure storage are:

- Storage encryption services
- Authentication with Azure AD and RBAC
- Client-side encryption, HTTPS, and SMB 3.0 for data in transit
- Azure disk encryption
- Shared access signatures – delegated access



Storage Security

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
- Keys should be regenerated on a regular basis or if they are compromised

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with the Microsoft Azure logo, a search bar, and various icons. Below the navigation bar, the page title is 'AccountName | Access keys'. The left sidebar contains a list of navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Data transfer, Events, Storage Explorer (preview), Settings, Access keys (highlighted), Geo-replication, CORS, Configuration, Encryption, and Shared access signature. The main content area shows the 'Access keys' page for a storage account. It includes a search bar, a description of access keys, and instructions on how to regenerate them. Below this, there are two sections for 'key1' and 'key2'. Each section contains a 'Storage account name' field (highlighted with a red box), a 'Key' field (highlighted with a red box), and a 'Connection string' field. The 'key1' section also has a 'key1' label and a refresh icon. The 'key2' section also has a 'key2' label and a refresh icon.

Shared Access Signature (SAS)

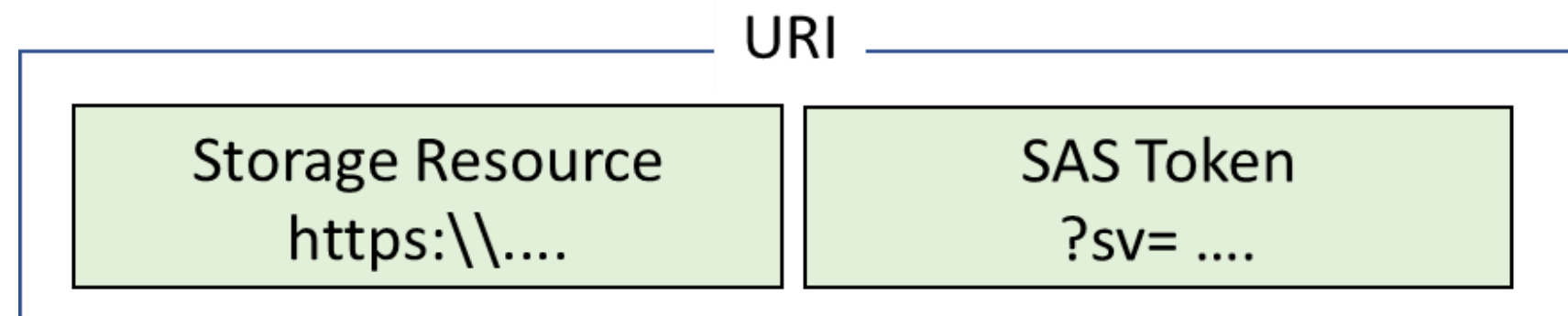
SAS provides delegated access to resources and also grants access to clients without sharing storage account keys.



The account SAS delegates access to resources in one of the storage services that are Blob, Queue, Table, or File service.

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/?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`

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

Storage Service Encryption

- Protects data for security and compliance
- Encrypts and decrypts data
- Encrypts through 256-bit AES encryption
- Is enabled for all new and existing storage accounts and cannot be disabled
- Is transparent to users

Encryption

 Save  Discard

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


✓ You can use your own key

Customer Managed Keys

- Use the Azure Key Vault to manage the encryption keys
- Distinguished personal encryption keys can be created and stored in a key vault
- Azure Key Vault APIs are used to generate encryption keys
- Custom keys gives more flexibility and control

Encryption type

- ☐ Microsoft Managed Keys
- ☒ Customer Managed Keys

i 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](#)

Best Practices



Always use HTTPS to create or distribute an SAS



Reference stored access policies, where possible



Use near-term expiration times on an ad-hoc SAS



Have clients automatically renew the SAS, if necessary



Be careful with SAS start time



Best Practices



Be specific with the resource to be accessed



Understand that your account will be billed for any usage



Validate data written using SAS



Don't assume SAS is always the correct choice



Use storage analytics to monitor your application



Assisted Practice

Create a Storage Account implementing azure storage replication and generate SAS for Storage Account

Duration: 10 Min.

Problem Statement:

You are given a project to create a storage account implementing azure storage replication that helps store multiple copies of your data so that it is protected from planned and unplanned events, including transient hardware failures, network or power outages, and massive natural disasters. and generate SAS that provides delegated access to resources and also grants access to clients without sharing storage account keys.

Assisted Practice: Guidelines

Steps to create a storage account implementing azure storage replication and generate SAS for storage account:

1. Log into the Azure portal at <https://portal.azure.com>
2. Create a Storage accounts
3. Select the allowed resource types
4. Generate SAS and connection string



Assisted Practice

Manage Storage Access Keys

Duration: 10 Min.

Problem Statement:

You are given a project to manage storage access keys to authorize access to data in your storage account via Shared Key authorization.

Assisted Practice: Guidelines

Steps to manage storage access keys:

1. Go to the Azure portal
2. Search for and select Storage Account
3. Manage storage access keys



Azure AD Authentication

Authorized Access

Authorized 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.



Azure AD for Blobs and Queues

Overview

- 1 When a security principal attempts to access a blob or queue resource, the request must be authorized.
- 2 The authentication step requires that an application request an OAuth 2.0 access token during runtime.
- 3 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

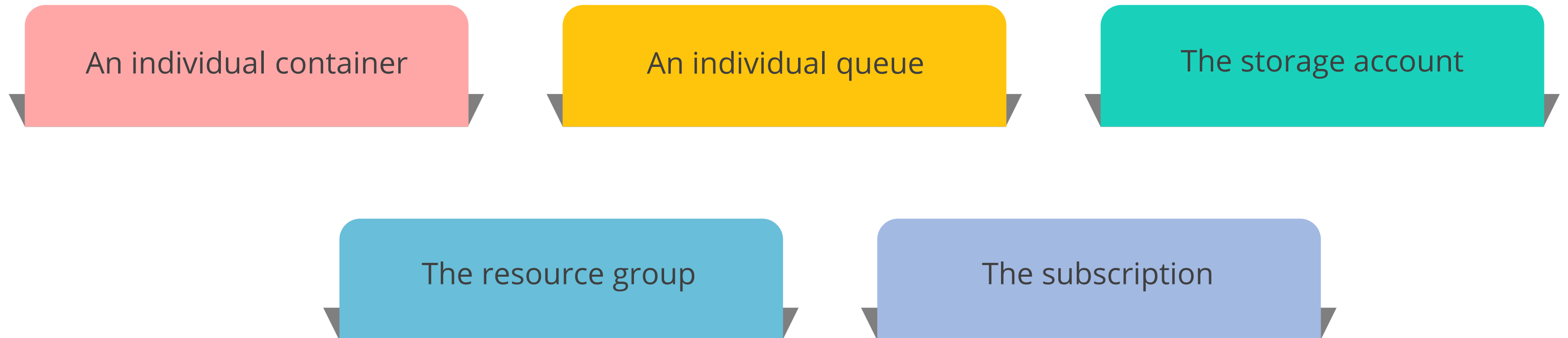
- Storage Blob Data Owner
- Storage Blob Data Contributor
- Storage Blob Data Reader

Queues

- 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:



Access Data with an Azure AD Account

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

1

One of the storage account access keys (requires an RBAC role with Microsoft Storage/storage Accounts/list keys/action permission)



2

An Azure AD account with permissions to access blob or queue data and to navigate through storage account resources

Assisted Practice

Add Azure AD Authentication for Storage

Duration: 10 Min.

Problem Statement:

You are given a project to add Azure AD authentication to your storage account to authorize requests against Azure Storage as Azure AD provides superior security and ease of use over Shared Key authorization.

Assisted Practice: Guidelines

Steps to add Azure AD authentication for storage:

1. Go to the Azure portal
2. Search for and select Storage Account
3. Add Azure AD authentication for Storage



Azure Storage Firewalls and Virtual Networks

Azure Storage Firewalls and Virtual Networks

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

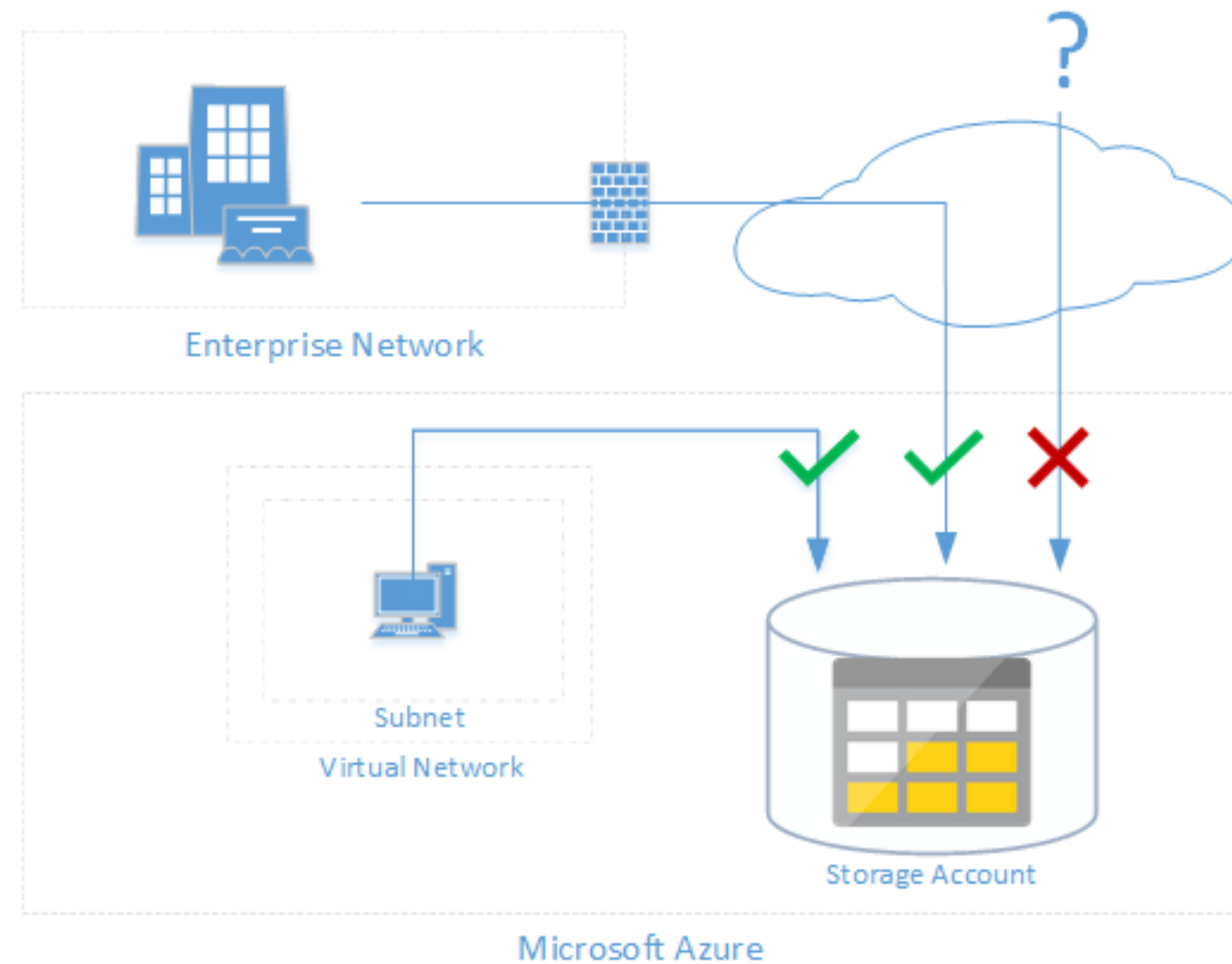


image source: <https://docs.microsoft.com/en-in/>

Azure Storage Firewalls and Virtual Networks

Network access rule considerations

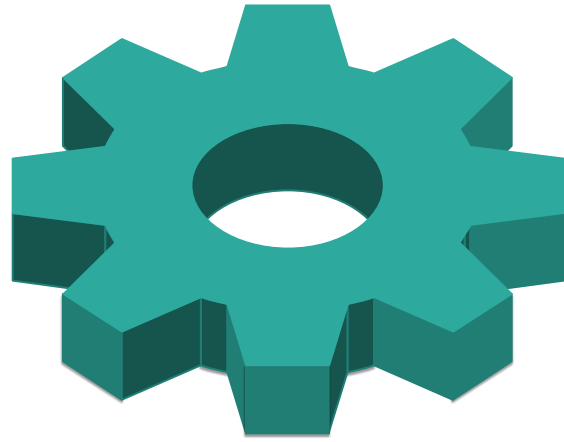
- Configure a rule to deny access from all networks and then grant access to traffic from specific virtual network subnets only.
- Configure rules to grant access to allow connections from specific internet or on-premise clients, if needed,
- Network rules are enforced on all network protocols to Azure storage, including REST and SMB.
- Once network rules are applied, they're enforced for all requests, including those based on SAS.

Note

- Virtual machine disk traffic is not affected by network rules.
- Classic storage accounts do not support firewalls and virtual networks.

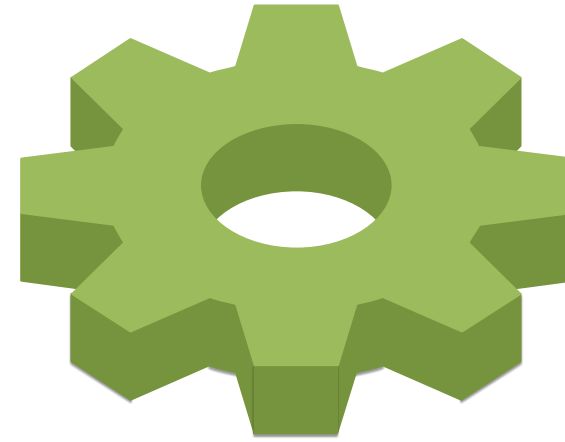
Default Network Access Rule

Following are the different ways to update default network settings:



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/Allow
```

Note

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

Granting Access to Storage Account from a Virtual Network

A user can limit access to a storage account from different subnets by configuring storage account access rules.

Granting access

- A user can add virtual network rules using firewall and virtual network settings
- A user can allow access to any existing virtual network/subnet or can also create new ones to allow access to them



Granting Access to Storage Account from an Internet IP Range

A user can create IP network rules to allow access from unique public internet IP address ranges.

Granting access

- A user can add IP network rules using a firewall and virtual network settings.
- A user can allow access to any an IP address range by adding it under settings.

Note

Each storage account can have upto 200 access rules, which can be a combination of virtual network and IP network rule.



Storage Endpoint Security

- **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

Search (Ctrl+/)

Save Discard Refresh

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

Assisted Practice

Provide Network Access for Storage

Duration: 10 Min.

Problem Statement:

You've been assigned a project to provide network storage access in order to secure and regulate access to your storage accounts.

Assisted Practice: Guidelines

Steps to provide network access for storage:

1. Go to the Azure portal
2. Search for and select Storage Account
3. Provide network access for storage



Key Takeaways

- Azure storage is a cloud storage platform designed for modern data storage scenarios; it provides services like Azure Blobs, Files, Queues, and Tables.
- Data in an Azure Storage account is always replicated three times in the primary region.
- Storage Account Failover prevents users against unplanned service outages.
- Blob Storage is an object storage solution for cloud, which is optimized for storing unstructured data.



Key Takeaways

- SAS provides delegated access to resources and also grants access to clients without sharing storage account keys.
- Azure Storage Firewall and Virtual Networks protect storage at the network level.
- A user can limit access to a storage account from different subnets by configuring storage account access rules.



Implementing Storage Account

Duration: 10 Min.

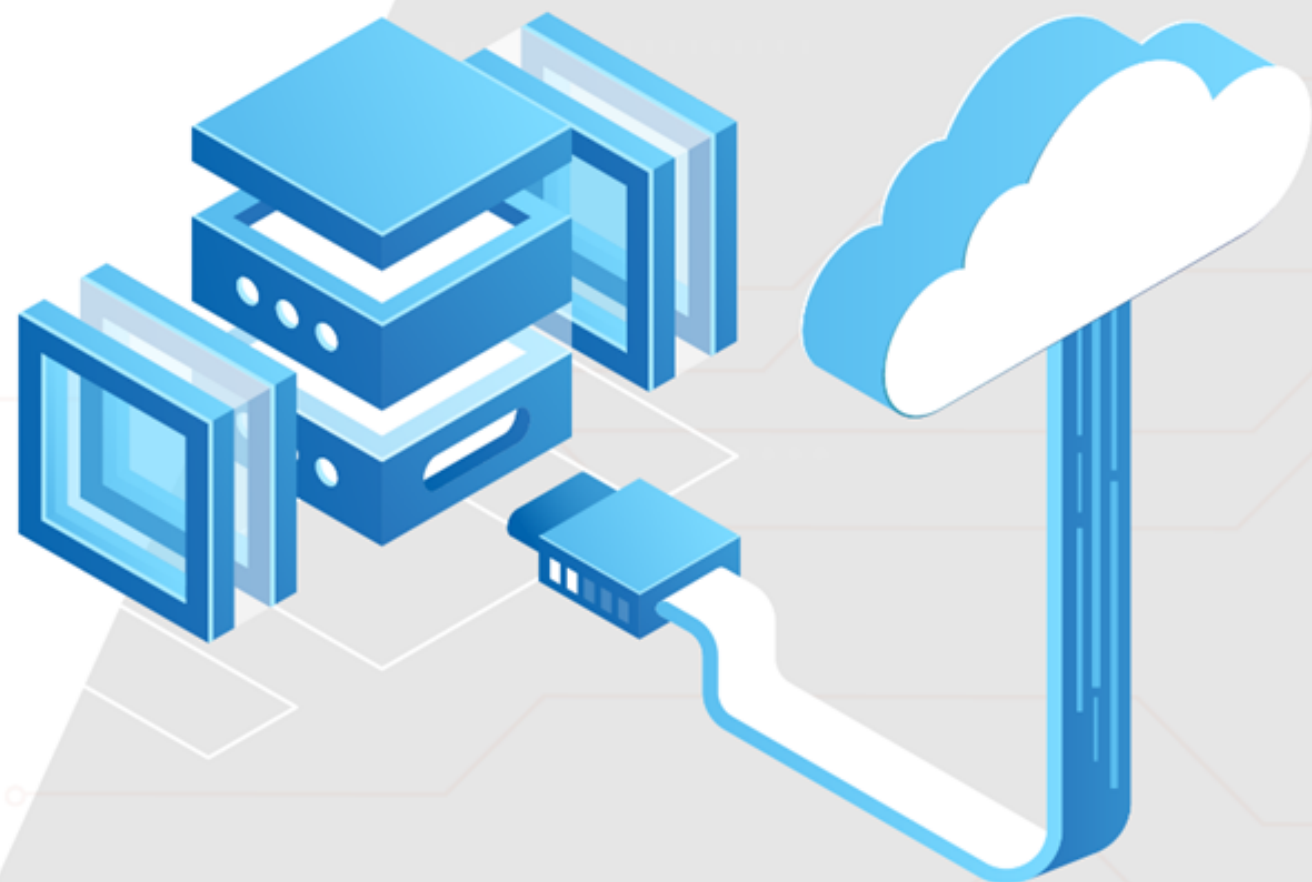
Project agenda: To create a storage account based on the requirements

Description: You have been given a project to create a data store which could store the images being used by an ecommerce application. As a part of this you need to create storage account and create a container with public access enabled which would store the images used by ecommerce application

Perform the following:

Create a storage account first and then a container having public access enabled.





Thank you