1- failovers

Table of contents

Globally redundant Storage and failover

- The process of failing over updates the **DNS entries** for your storage account service endpoints.
- Such that the endpoints for the secondary region become the new primary endpoints for your storage account.
- Once the failover is complete, clients can begin writing to the new primary endpoints.
- source

- RA-GRS and RA-GZRS provide read access to the secondary endpoint if there is an outage in the primary region.
- source
- RA-GZRS for maximum availability and durability of your storage accounts.

Storage Account failover

2 types

- #Customer-managed-failover
  - Customers can manage storage account failover if there's an unexpected service outage
  - ! For the ability to selectively failover your individual storage accounts, use customer-managed account failover.
  - Customer-managed account failover is only supported for storage accounts deployed using the Azure Resource Manager (ARM) deployment model.
  - The Azure Service Manager (ASM) deployment model, also known as *classic*, isn't supported.

    - To make classic storage accounts eligible for customer-managed account failover, they must first be migrated to the ARM model.
- #Microsoft-managed-failover
    - Potentially initiated by Microsoft only in the case of a severe disaster in the primary region.
    - ! Only initiated for an entire physical unit, such as region or scale unit. Cant be initialized for individual storage accounts, subs or tenants.
    - Until the Microsoft-managed failover has completed, you won't have write access to your storage account.
    - Your applications can read from the secondary region if your storage account is configured for RA-GRS or RA-GZRS.
    - If there's a disaster that affects the primary region, Microsoft will manage the failover for classic storage accounts.

Anticipate data loss and inconsistencies

source

Last sync Time

- #last-sync-time
- indicates the most recent time that data from the primary region is guaranteed to have been written to the secondary region.
- All the data and metadata before the Last sync time will be present in the secondary region.
- data and metadata written after the last sync time may not have been written to the secondary, and may be lost.
- Use this property if there's an outage to estimate the amount of data loss you may incur by initiating an account failover.
- ! comparing the last write operation with the last sync time to determine which writes haven’t been synced to the secondary.

Time and cost of failing over

- Typically takes less than one hour or vary.
- ! customer-managed failover loses its GRS after a failover.
- storage account is automatically converted to LRS in the 2nd region (new primary region) during the failover.
- storage account is deleted in the primary region.
- source

- can Re-enable GRS or RA-GRS for the account.
- ! Note that converting converting from LRS to GRS or GA-GRS incur additional cost.
- source
- Replication time depends on many factors, which include:
- Storage account failover shouldn't be used as part of your data migration strategy. Failover is a temporary solution to a service outage.

REST API's

#storage-resource-provider

- Microsoft provides two REST APIs for working with Azure Storage resources.
- Azure Storage REST API enables you to work with the data in your storage account, including blob, queue, file, and table data.
- The Azure-Storage-resource-provider REST API enables you to manage the storage account and related resources.

> **Important**
>
> - After the failover is complete, clients can again read and write Azure Storage data in the new primary region.
> - However, the Azure Storage Resource Provider does not fail over.
> - So resource management operations must still take place in the primary region.
> - If the primary region is unavailable, you will not be able to perform management operations on the storage account.

source
