Azure Storage redundancy

06/17/2020 • 13 minutes to read • +12

In this article

Azure Storage always stores 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. Redundancy ensures that your storage account meets the Service-Level Agreement (SLA) for Azure Storage even in the face of failures.

When deciding which redundancy option is best for your scenario, consider the tradeoffs between lower costs and higher availability and durability. The factors that help determine which redundancy option you should choose include:

- How your data is replicated in the primary region
- Whether your data is replicated to a second location that is geographically distant to the primary region, to protect against regional disasters
- Whether your application requires read access to the replicated data in the secondary region if the primary region becomes unavailable for any reason

Redundancy in the primary region

Data in an Azure Storage account is always replicated three times in the primary region. Azure Storage offers two options for how your data is replicated in the primary region:

- **Locally redundant storage (LRS)** copies your data synchronously three times within a single physical location in the primary region. LRS is the least expensive replication option, but is not recommended for applications requiring high availability.
- **Zone-redundant storage (ZRS)** copies your data synchronously across three Azure availability zones in the primary region. For applications requiring high availability,

Microsoft recommends using ZRS in the primary region, and also replicating to a secondary region.

Locally-redundant storage

Locally redundant storage (LRS) replicates your data three times within a single physical location in the primary region. LRS provides at least 99.999999999% (11 nines) durability of objects over a given year.

LRS is the lowest-cost redundancy option and offers the least durability compared to other options. LRS protects your data against server rack and drive failures. However, if a disaster such as fire or flooding occurs within the data center, all replicas of a storage account using LRS may be lost or unrecoverable. To mitigate this risk, Microsoft recommends using zone-redundant storage (ZRS), geo-redundant storage (GRS), or geo-zone-redundant storage (GZRS).

A write request to a storage account that is using LRS happens synchronously. The write operation returns successfully only after the data is written to all three replicas.

LRS is a good choice for the following scenarios:

- If your application stores data that can be easily reconstructed if data loss occurs, you may opt for LRS.
- If your application is restricted to replicating data only within a country or region due to data governance requirements, you may opt for LRS. In some cases, the paired regions across which the data is geo-replicated may be in another country or region. For more information on paired regions, see Azure regions.

Zone-redundant storage

Zone-redundant storage (ZRS) replicates your Azure Storage data synchronously across three Azure availability zones in the primary region. Each availability zone is a separate physical location with independent power, cooling, and networking. ZRS offers durability for Azure Storage data objects of at least 99.9999999999% (12 9's) over a given year.

With ZRS, your data is still accessible for both read and write operations even if a zone becomes unavailable. If a zone becomes unavailable, Azure undertakes networking updates, such as DNS re-pointing. These updates may affect your application if you access data before the updates have completed. When designing applications for ZRS, follow practices for transient fault handling, including implementing retry policies with exponential back-off.

A write request to a storage account that is using ZRS happens synchronously. The write operation returns successfully only after the data is written to all replicas across the three availability zones.

Microsoft recommends using ZRS in the primary region for scenarios that require consistency, durability, and high availability. ZRS provides excellent performance, low latency, and resiliency for your data if it becomes temporarily unavailable. However, ZRS by itself may not protect your data against a regional disaster where multiple zones are permanently affected. For protection against regional disasters, Microsoft recommends using geo-zone-redundant storage (GZRS), which uses ZRS in the primary region and also geo-replicates your data to a secondary region.

The following table shows which types of storage accounts support ZRS in which regions:

Storage account type	Supported regions	Supported services
General-purpose v2[1]	Asia Southeast Australia East Europe North Europe West France Central Japan East South Africa North UK South US Central US East US East 2 US West 2	Block blobs Page blobs[2] File shares (standard) Tables Queues
BlockBlobStorage[1]	Asia Southeast Europe West US East	Block blobs only
FileStorage	Asia Southeast Europe West US East	Azure Files only

[1] The archive tier is not currently supported for ZRS accounts.
[2] Storage accounts that contain Azure managed disks for virtual machines always use LRS. Azure unmanaged disks should also use LRS. It is possible to create a storage account for Azure unmanaged disks that uses GRS, but it is not recommended due to potential issues with consistency over asynchronous geo-replication. Neither managed nor unmanaged

disks support ZRS or GZRS. For more information on managed disks, see Pricing for Azure managed disks.

For information about which regions support ZRS, see **Services support by region** in What are Azure Availability Zones?.

Redundancy in a secondary region

For applications requiring high availability, you can choose to additionally copy the data in your storage account to a secondary region that is hundreds of miles away from the primary region. If your storage account is copied to a secondary region, then your data is durable even in the case of a complete regional outage or a disaster in which the primary region isn't recoverable.

When you create a storage account, you select the primary region for the account. The paired secondary region is determined based on the primary region, and can't be changed. For more information about regions supported by Azure, see Azure regions.

Azure Storage offers two options for copying your data to a secondary region:

- **Geo-redundant storage (GRS)** copies your data synchronously three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in the secondary region.
- **Geo-zone-redundant storage (GZRS)** copies your data synchronously across three Azure availability zones in the primary region using ZRS. It then copies your data asynchronously to a single physical location in the secondary region.

The primary difference between GRS and GZRS is how data is replicated in the primary region. Within the secondary location, data is always replicated synchronously three times using LRS. LRS in the secondary region protects your data against hardware failures.

With GRS or GZRS, the data in the secondary location isn't available for read or write access unless there is a failover to the secondary region. For read access to the secondary location, configure your storage account to use read-access geo-redundant storage (RA-GRS) or read-access geo-zone-redundant storage (RA-GZRS). For more information, see Read access to data in the secondary region.

If the primary region becomes unavailable, you can choose to fail over to the secondary region. After the failover has completed, the secondary region becomes the primary region, and you can again read and write data. For more information on disaster recovery and to

learn how to fail over to the secondary region, see Disaster recovery and storage account failover.

> **Important**
>
> Because data is replicated to the secondary region asynchronously, a failure that affects the primary region may result in data loss if the primary region cannot be recovered. The interval between the most recent writes to the primary region and the last write to the secondary region is known as the recovery point objective (RPO). The RPO indicates the point in time to which data can be recovered. Azure Storage typically has an RPO of less than 15 minutes, although there's currently no SLA on how long it takes to replicate data to the secondary region.

Geo-redundant storage

Geo-redundant storage (GRS) copies your data synchronously three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in a secondary region that is hundreds of miles away from the primary region. GRS offers durability for Azure Storage data objects of at least 99.99999999999999% (16 9's) over a given year.

A write operation is first committed to the primary location and replicated using LRS. The update is then replicated asynchronously to the secondary region. When data is written to the secondary location, it's also replicated within that location using LRS.

Geo-zone-redundant storage

Geo-zone-redundant storage (GZRS) combines the high availability provided by redundancy across availability zones with protection from regional outages provided by geo-replication. Data in a GZRS storage account is copied across three Azure availability zones in the primary region and is also replicated to a secondary geographic region for protection from regional disasters. Microsoft recommends using GZRS for applications requiring maximum consistency, durability, and availability, excellent performance, and resilience for disaster recovery.

With a GZRS storage account, you can continue to read and write data if an availability zone becomes unavailable or is unrecoverable. Additionally, your data is also durable in the case of a complete regional outage or a disaster in which the primary region isn't

recoverable. GZRS is designed to provide at least 99.99999999999999% (16 9's) durability of objects over a given year.

Only general-purpose v2 storage accounts support GZRS and RA-GZRS. For more information about storage account types, see Azure storage account overview. GZRS and RA-GZRS support block blobs, page blobs (except for VHD disks), files, tables, and queues.

GZRS and RA-GZRS are supported in the following regions:

- Asia Southeast
- Europe North
- Europe West
- Japan East
- UK South
- US Central
- US East
- US East 2
- US West 2

For information on pricing, see pricing details for Blobs, Files, Queues, and Tables.

Read access to data in the secondary region

Geo-redundant storage (with GRS or GZRS) replicates your data to another physical location in the secondary region to protect against regional outages. However, that data is available to be read only if the customer or Microsoft initiates a failover from the primary to secondary region. When you enable read access to the secondary region, your data is available to be read if the primary region becomes unavailable. For read access to the secondary region, enable read-access geo-redundant storage (RA-GRS) or read-access geo-zone-redundant storage (RA-GZRS).

Design your applications for read access to the secondary

If your storage account is configured for read access to the secondary region, then you can design your applications to seamlessly shift to reading data from the secondary region if the primary region becomes unavailable for any reason. The secondary region is always available for read access after you enable RA-GRS or RA-GZRS, so that you can test your application in advance to make sure that it will properly read from the secondary in the event of an outage. For more information about how to design your applications for high availability, see Use geo-redundancy to design highly available applications.

When read access to the secondary is enabled, your data can be read from the secondary endpoint as well as from the primary endpoint for your storage account. The secondary endpoint appends the suffix *–secondary* to the account name. For example, if your primary endpoint for Blob storage is `myaccount.blob.core.windows.net`, then the secondary endpoint is `myaccount-secondary.blob.core.windows.net`. The account access keys for your storage account are the same for both the primary and secondary endpoints.

Check the Last Sync Time property

Because data is replicated to the secondary region asynchronously, the secondary region is often behind the primary region. If a failure happens in the primary region, it's likely that all writes to the primary will not yet have been replicated to the secondary.

To determine which write operations have been replicated to the secondary region, your application can check the **Last Sync Time** property for your storage account. All write operations written to the primary region prior to the last sync time have been successfully replicated to the secondary region, meaning that they are available to be read from the secondary. Any write operations written to the primary region after the last sync time may or may not have been replicated to the secondary region, meaning that they may not be available for read operations.

You can query the value of the **Last Sync Time** property using Azure PowerShell, Azure CLI, or one of the Azure Storage client libraries. The **Last Sync Time** property is a GMT date/time value. For more information, see Check the Last Sync Time property for a storage account.

Summary of redundancy options

The tables in the following sections summarize the redundancy options available for Azure Storage

Durability and availability parameters

The following table describes key parameters for each redundancy option:

Parameter	LRS	ZRS	GRS/RA-GRS	GZRS/RA-GZR
Percent durability of objects over a	at least 99.999999999% (11 9's)	at least 99.9999999999% (12 9's)	at least 99.99999999999999% (16 9's)	at least 99.9999999999 (16 9's)

Parameter	LRS	ZRS	GRS/RA-GRS	GZRS/RA-GZR
given year[1]				
Availability SLA for read requests[1]	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier) for GRS At least 99.99% (99.9% for cool access tier) for RA-GRS	At least 99.9% for cool access for GZRS At least 99.99% (99.9% for cool tier) for RA-GZI
Availability SLA for write requests[1]	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)	At least 99.9% (99% for cool access tier)	At least 99.9% for cool access

[1] For information about Azure Storage guarantees for durability and availability, see the Azure Storage SLA.

Durability and availability by outage scenario

The following table indicates whether your data is durable and available in a given scenario, depending on which type of redundancy is in effect for your storage account:

Outage scenario	LRS	ZRS	GRS/RA-GRS	GZRS/RA-GZRS
A node within a data center becomes unavailable	Yes	Yes	Yes	Yes
An entire data center (zonal or non-zonal) becomes unavailable	No	Yes	Yes[1]	Yes

Outage scenario	LRS	ZRS	GRS/RA-GRS	GZRS/RA-GZRS
A region-wide outage occurs in the primary region	No	No	Yes[1]	Yes[1]
Read access to the secondary region is available if the primary region becomes unavailable	No	No	Yes (with RA-GRS)	Yes (with RA-GZRS)

[1] Account failover is required to restore write availability if the primary region becomes unavailable. For more information, see Disaster recovery and storage account failover.

Supported storage account types

The following table shows which redundancy options are supported by each type of storage account. For information for storage account types, see Storage account overview.

LRS	ZRS	GRS/RA-GRS	GZRS/RA-GZRS
General-purpose v2 General-purpose v1 Block blob storage Blob storage File storage	General-purpose v2 Block blob storage File storage	General-purpose v2 General-purpose v1 Blob storage	General-purpose v2

All data for all storage accounts is copied according to the redundancy option for the storage account. Objects including block blobs, append blobs, page blobs, queues, tables, and files are copied. Data in all tiers, including the archive tier, is copied. For more information about blob tiers, see Azure Blob storage: hot, cool, and archive access tiers.

For pricing information for each redundancy option, see Azure Storage pricing.

> **Note**
>
> Azure Premium Disk Storage currently supports only locally redundant storage (LRS). Block blob storage accounts support locally redundant storage (LRS) and zone redundant storage (ZRS) in certain regions.

Data integrity

Azure Storage regularly verifies the integrity of data stored using cyclic redundancy checks (CRCs). If data corruption is detected, it is repaired using redundant data. Azure Storage also calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

See also

- Check the Last Sync Time property for a storage account
- Change the redundancy option for a storage account
- Use geo-redundancy to design highly available applications
- Disaster recovery and storage account failover

Related Articles

- Azure storage account overview
- Build highly available Azure Storage applications on zone-redundant storage (ZRS)
- Geo-redundant storage (GRS) for cross-regional durability in Azure Storage
- Locally-redundant storage (LRS) for low-cost redundancy in Azure Storage

Recommendations are based on machine learning analysis and tuned by our content authors.

Is this page helpful?

Yes No
