

Object Replication

Object replication in Azure refers to the process of automatically copying data (objects) from one Azure Storage account to another, typically in a different region, to achieve data redundancy, disaster recovery, and compliance requirements. Azure offers several options for object replication, each designed to meet specific business needs and data management scenarios:

1. **Geo-Redundant Storage (GRS):** Geo-Redundant Storage is a built-in replication option for Azure Storage accounts. With GRS, Azure automatically replicates your data to a secondary Azure region, providing an extra layer of redundancy in case of data center failures or regional disasters. GRS maintains six copies of your data across two paired regions, ensuring high durability and availability. In the event of a regional outage, Azure fails over to the secondary region seamlessly, minimizing downtime and data loss.
2. **Read-Access Geo-Redundant Storage (RA-GRS):** Read-Access Geo-Redundant Storage extends the capabilities of GRS by allowing read access to the replicated data in the secondary region. This enables scenarios such as read-only access for analytics, reporting, or failover testing without impacting production workloads.
3. **Zone-Redundant Storage (ZRS):** Zone-Redundant Storage replicates data across multiple availability zones within the same Azure region. Availability zones are physically separate data centers within a region with independent power, cooling, and networking. ZRS provides higher durability and availability than standard storage replication options by distributing data across multiple fault domains within a region.
4. **Locally-Redundant Storage (LRS):** Locally-Redundant Storage replicates data within the same data center to protect against hardware failures. With LRS, Azure maintains three copies of your data within a single storage scale unit (a cluster of storage servers), providing basic redundancy and durability at a lower cost compared to geo-replication options.
5. **Cross-Region Replication (CRR):** Cross-Region Replication is a feature available for Azure Blob Storage that allows you to asynchronously replicate blobs from a source storage account to a destination storage account in a different region. CRR enables you to satisfy data residency requirements, implement disaster recovery strategies, or distribute data closer to your users for better performance.

By leveraging object replication options in Azure, organizations can ensure data resilience, compliance, and high availability for their applications and workloads, regardless of their scale or geographic distribution. Each replication option offers different levels of redundancy, durability, and cost-effectiveness, allowing organizations to choose the most suitable option based on their specific requirements and budget constraints.



Use cases of Object Replication:

Object replication in Azure Storage offers various use cases across different industries and scenarios, providing redundancy, disaster recovery, compliance, and performance optimization. Here are some common use cases for object replication in Azure:

1. **Disaster Recovery:** Replicating data across multiple Azure regions or availability zones ensures business continuity in the event of regional outages, natural disasters, or data center failures. By maintaining copies of critical data in geographically dispersed locations, organizations can quickly recover from disasters and minimize downtime.
2. **High Availability:** Object replication enhances application availability by ensuring that data remains accessible even in the face of hardware failures or transient issues within a single data center. Replicating data across multiple fault domains or regions enables applications to maintain uninterrupted service levels and meet stringent uptime requirements.
3. **Data Residency Compliance:** Organizations subject to data residency regulations or compliance requirements can use object replication to maintain copies of data within specific geographic regions or jurisdictions. By replicating data to designated regions, organizations can ensure compliance with data sovereignty laws and regulations, safeguarding sensitive data and mitigating regulatory risks.
4. **Global Content Distribution:** Replicating data closer to end-users or customers across different regions improves content delivery performance and reduces latency for accessing data-intensive applications, media files, or web content. By distributing content across geographically dispersed locations, organizations can deliver a superior user experience and optimize network bandwidth usage.
5. **Data Migration and Hybrid Cloud Scenarios:** Object replication facilitates seamless data migration between on-premises environments and Azure cloud storage or between different Azure regions. Organizations can replicate data incrementally or in real-time, ensuring a smooth transition to the cloud and minimizing downtime during migration processes. Additionally, object replication supports hybrid cloud architectures by synchronizing data between on-premises and cloud storage environments for hybrid cloud scenarios.
6. **Backup and Archiving:** Replicating backup data to secondary storage locations provides an extra layer of protection against data loss and corruption. Organizations can replicate backups to geographically dispersed regions or storage tiers, ensuring data durability and long-term retention for compliance and archival purposes. Object replication also enables efficient data recovery and restoration in the event of data loss or corruption.

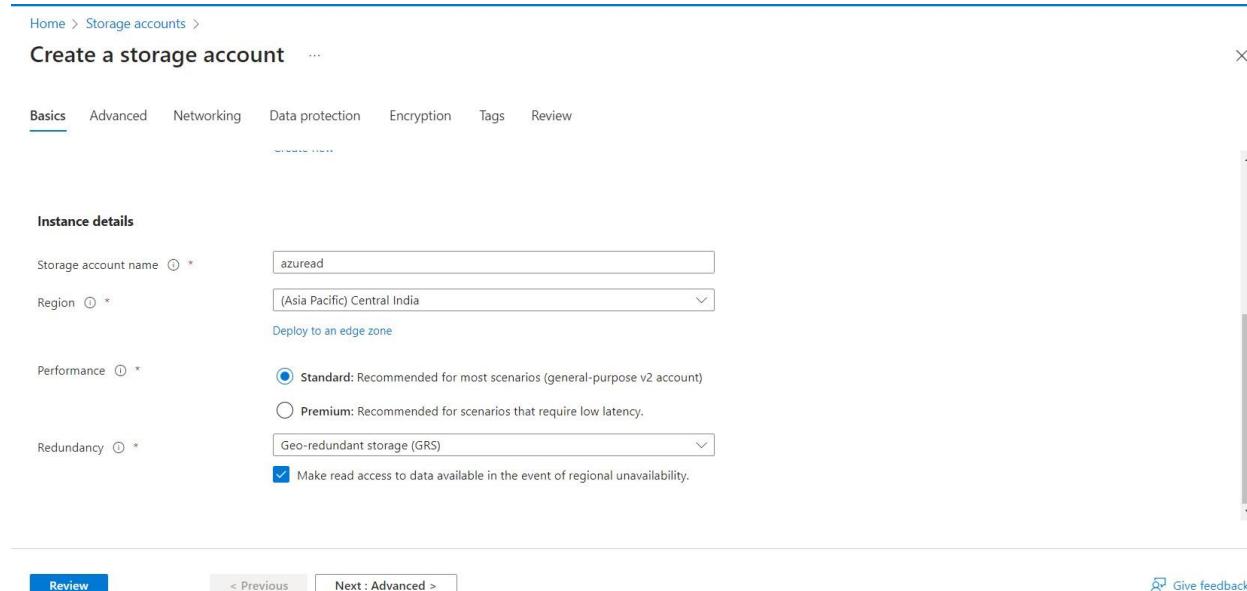
7. **DevOps and Test Environments:** Object replication supports DevOps practices by providing developers and testers with access to consistent and up-to-date copies of production data for development, testing, and debugging purposes. By replicating data to development and test environments, organizations can accelerate application development cycles, improve code quality, and minimize risks associated with production deployments.
8. **Analytics and Reporting:** Replicating data to secondary storage locations allows organizations to perform data analytics, reporting, and business intelligence (BI) operations without impacting production workloads. By replicating data for analytical purposes, organizations can derive valuable insights, uncover trends, and make data-driven decisions to drive business growth and innovation.

In this process, we're setting up object replication between two Azure Storage accounts. The end goal is to ensure data redundancy, disaster recovery, and compliance by automatically copying data from a source storage account to a destination storage account. By enabling versioning, change feed, and configuring replication rules, organizations can maintain synchronized copies of their data across different regions or environments, enhancing data resilience and availability.

To begin with the Lab:

 **Step 1:** In this lab, you create two storage accounts. First will be your source account and second will be your destination account.

- Below we are creating our source storage account.



The screenshot shows the 'Create a storage account' wizard in the Azure portal. The 'Basics' tab is selected. The account name is 'azuread', located in '(Asia Pacific) Central India'. The performance level is set to 'Standard' (selected), and the redundancy is 'Geo-redundant storage (GRS)'. The 'Make read access available in the event of regional unavailability' checkbox is checked. At the bottom, there are 'Review' and 'Next : Advanced >' buttons, along with a 'Give feedback' link.

😊 Step 2: Enable versioning and change feed under the data protection tab.

The screenshot shows the 'Create a storage account' wizard on the 'Data protection' tab. In the 'Tracking' section, there is a checkbox labeled 'Enable versioning for blobs' which is checked and highlighted with a red border. Below it, a note says 'Use versioning to automatically maintain previous versions of your blobs. Learn more'. Another checkbox 'Enable blob change feed' is also present but unchecked. The 'Access control' section contains a checkbox for 'Enable version-level immutability support' which is also unchecked. At the bottom, there are navigation buttons: 'Review' (highlighted with a red border), '< Previous', 'Next : Encryption >', and a 'Give feedback' link.

😊 Step 3: Move to review page and create your source storage account.

The screenshot shows the 'Create a storage account' wizard on the 'Review' tab. It displays basic configuration details: Subscription (Azure Pass - Sponsorship), Resource Group (Ritesh-rg), Location (centralindia), Storage account name (objreplica), Deployment model (Resource manager), Performance (Standard), and Replication (Read-access geo-redundant storage (RA-GRS)). Under 'Advanced' settings, 'Enable hierarchical namespace' and 'Enable network file system v3' are disabled, while 'Allow cross-tenant replication' is enabled. At the bottom, there are buttons for 'Create' (highlighted with a red border), '< Previous', 'Next >', 'Download a template for automation', and a 'Give feedback' link.

😊 Step 4: Go to the Storage account page, scroll down, and click on data protection. **Enable Versioning & Blob change feed and save changes**. You have to do this for both of your storage accounts.

Home > Storage accounts > objreplica

objreplica | Data protection

Storage account

Search

Front Door and CDN

Access keys

Shared access signature

Encryption

Microsoft Defender for Cloud

Data management

Redundancy

Data protection

Object replication

Blob inventory

Static website

Lifecycle management

Azure search

Settings

Configuration

https://aka.ms/blobchangefeedupgrade

Tracking

Enable versioning for blobs

Use versioning to automatically maintain previous versions of your blobs. Learn more

Consider your workloads, their impact on the number of versions created, and the resulting costs. Optimize costs by automatically managing the data lifecycle.

Learn more

Keep all versions

Delete versions after (in days)

Enable blob change feed

Keep track of create, modification, and delete changes to blobs in your account. Learn more

Keep all logs

Delete change feed logs after (in days)

Access control

Enable version-level immutability support

Save Discard Give feedback

💡 Step 5: Similarly Create the destination Storage account, following Steps 1 to 4.

- Create an empty Blob Container in your destination storage account.

Home > Storage accounts > objreplica2

objreplica2 | Containers

Storage account

Search

+ Container Change access level Restore containers Refresh Delete Give feedback

Search containers by prefix

Show deleted containers

Name	Last modified	Public access level	Lease state	...
Logs	8/25/2023, 1:06:23 PM	Private	Available	...
data	8/25/2023, 1:07:23 PM	Blob	Available	...

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Storage Mover

Data storage

Containers

File shares

Queues

Tables

Security + networking

Networking

💡 Step 6: Now we need to set up an object replication policy in the source storage account. Click on the Create Replication rule.

- Make sure you have some temporary files in your source storage account (Blob) container.

The screenshot shows the Azure Storage Accounts interface for the 'objreplica' account. The left sidebar has a 'Data management' section with 'Object replication' selected, indicated by a red box. At the top, there's a 'Create replication rules' button, also highlighted with a red box. The main content area displays sections for 'Your accounts' and 'Other accounts', both showing 'No replication policies found'. Below these are sections for 'Objects copied from this account' and 'Objects copied into this account', also showing 'No replication policies found'. A status message at the top right says: 'When object replication is enabled, blobs are copied asynchronously from a source storage account to a destination account. Cross-tenant policies will appear under "Other accounts", along with policies on accounts not in an active subscription or on deleted accounts. The storage accounts may be in different Azure regions.' A link 'Learn more' is provided.

💡 **Step 7:** Select resource group, source, destination storage account, and prefix filters (A prefix match will find items like folders and blobs under the specified container.)

The screenshot shows the 'Create replication rules' dialog. It starts with a note: 'When you create object replication rules, blob change feed and blob versioning are automatically enabled for the source and destination storage accounts. Enabling these features may increase costs.' The 'Destination subscription' dropdown is set to 'Azure Pass - Sponsorship'. The 'Destination storage account' dropdown is set to 'objreplica2', highlighted with a red box. The 'Container pair details' section explains that a container pair consists of a container in the source account and a container in the destination account. The 'Source container' dropdown is set to 'roletest', highlighted with a red box. The 'Destination container' dropdown is set to 'data', highlighted with a red box. In the 'Copy over' section, 'Only new objects (change)' is selected. At the bottom, there's a note about configuring more than 10 container pairs using a JSON file, and two buttons: 'Create' (highlighted with a red box) and 'Cancel'.

💡 **Step 8:** Choose the option for copy over options everything (to copy all objects), only new objects (to copy new files or modifications only), custom (from any particular date range)

Create replication rules

When you create object replication rules, blob change feed and blob versioning are automatically enabled for the source and destination storage accounts. Enable

Destination subscription * Azure Pass - Sponsorship

Destination storage account * objreplica2

Container pair details

A container pair consists of a container in the source account and a container in the destination account. Objects in the source container are copied over to the destination container according to the replication rule. You can optionally filter which objects are copied by specifying a prefix match and by copying objects created only after a specified date and time.

Source container	Destination container	Filters	Copy over
roletest	data	0 (add)	Only new objects (
Select a source container	Select a destination container		

To configure more than 10 container pairs (up to 1000), see [Configure object replication using a JSON file](#)

Save **Cancel**

💡 **Step 9:** After a few minutes Head over to your destination storage account, and you should now see the files in the target container.

Home > Storage accounts > objreplica2 | Containers >

data Container

Search

Upload Change access level Refresh Delete Change tier Acquire lease Break lease View snapshots Create snapshot ...

Overview

Authentication method: Access key (Switch to Azure AD User Account)
Location: data

Diagnose and solve problems

Access Control (IAM)

Settings

Shared access tokens

Access policy

Properties

Metadata

Add filter

Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
iis.ps1	8/25/2023, 1:13:44 PM	Hot (Inferred)		Block blob	183 B	Available

If you Make changes like uploading a new file in the source storage account will detect changes and replicate them over to destination storage account.