

# AZ-104 Azure - Configuring blob object replication

- [Object replication configuration](#)
- [Object replication overview](#)

Object replication asynchronously copies blocks of blobs between storage accounts

- Requires source and destination storage accounts
- Requires versioning and change feed
- Support cross-tenant replication

Diagram showing how object replication works

- Minimize latency - reduce latency for read requests.
- Increased efficiency - Processing block blob in different regions.
- Data distribution - Processing and analyzing data in one location that replicate to other regions.
- Cost Optimization -moving replicate data to the archive tier can reduce cost.

- Versioning: Versioning must be enabled on both the source and destination accounts to perform replication
- Change feed: Change feed must be enabled on the source account. Azure storage monitors the \$blobchangeFeed to advise replication.
- Cross subscription and azure AD: Object replication is supported across subscriptions and azure AD tenants
- Replication Policy: A Storage account can be a source for up to two destination accounts. Each policy supports only a single pairing using a policy ID.

Create a destination storage account and make sure versioning for blobs its enabled

Microsoft Azure

Home > Storage accounts > deststorageaccountcloud1

### Storage accounts

Pluralsight Cloud (realhandsonlabs.com)

+ Create Restore ...

Filter for any field...

Name ↑

- deststorageaccountcloud1
- teststoragecloud1

Containers

- File shares
- Queues
- Tables

Security + networking

- Networking
- Front Door and CDN
- Access keys
- Shared access signature
- Encryption
- Microsoft Defender for Cloud

Data management

- Storage tasks (preview)
- Redundancy
- Data protection
- Object replication
- Blob inventory
- Static website
- Lifecycle management
- Azure AI Search

Settings

- Configuration
- Data Lake Gen2 upgrade

## deststorageaccountcloud1 | Data protection

Storage account

Data protection provides options for recovering your data when it is erroneously modified or deleted.

Recovery

- Enable Azure Backup for blobs
- Enable point-in-time restore for containers
- Enable soft delete for blobs
  - Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)
  - Keep deleted blobs for (in days) \*
- Enable soft delete for containers
  - Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)
  - Keep deleted containers for (in days) \*
- Enable permanent delete for soft deleted items

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 m](#)
  - Keep all versions
  - Delete versions after (in days)
- Enable blob change feed

Access control

Save Discard

For source storage account we will enable versioning and change feed.

Microsoft Azure

Home > Storage accounts > srcstorageaccountcloud1

### Storage accounts

Pluralsight Cloud (realhandsonlabs.com)

+ Create Restore ...

Filter for any field...

Name ↑

- deststorageaccountcloud1
- srcstorageaccountcloud1
- teststoragecloud1

Containers

- File shares
- Queues
- Tables

Security + networking

- Networking
- Front Door and CDN
- Access keys
- Shared access signature
- Encryption
- Microsoft Defender for Cloud

Data management

- Storage tasks (preview)
- Redundancy
- Data protection
- Object replication
- Blob inventory
- Static website
- Lifecycle management
- Azure AI Search

Settings

- Configuration
- Data Lake Gen2 upgrade
- Resource sharing (CORS)
- Advisor recommendations

## srcstorageaccountcloud1 | Data protection

Storage account

Data protection provides options for recovering your data when it is erroneously modified or deleted.

Recovery

- Enable Azure Backup for blobs
- Enable point-in-time restore for containers
- Enable soft delete for blobs
  - Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)
  - Keep deleted blobs for (in days) \*
- Enable soft delete for containers
  - Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)
  - Keep deleted containers for (in days) \*
- Enable permanent delete for soft deleted items

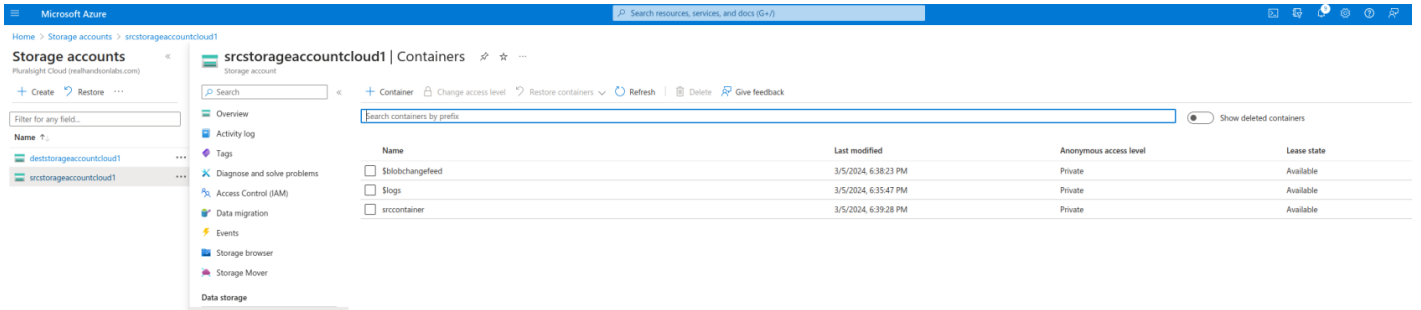
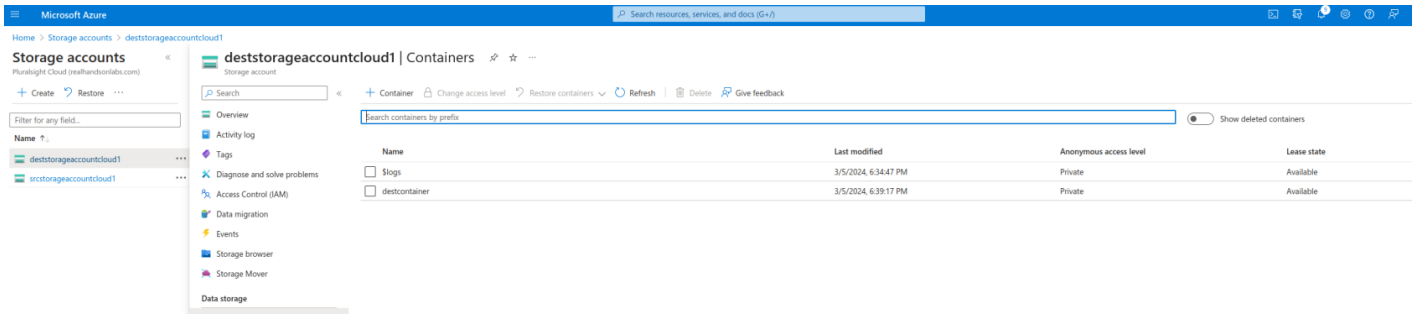
Tracking

- 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 m](#)
  - 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)

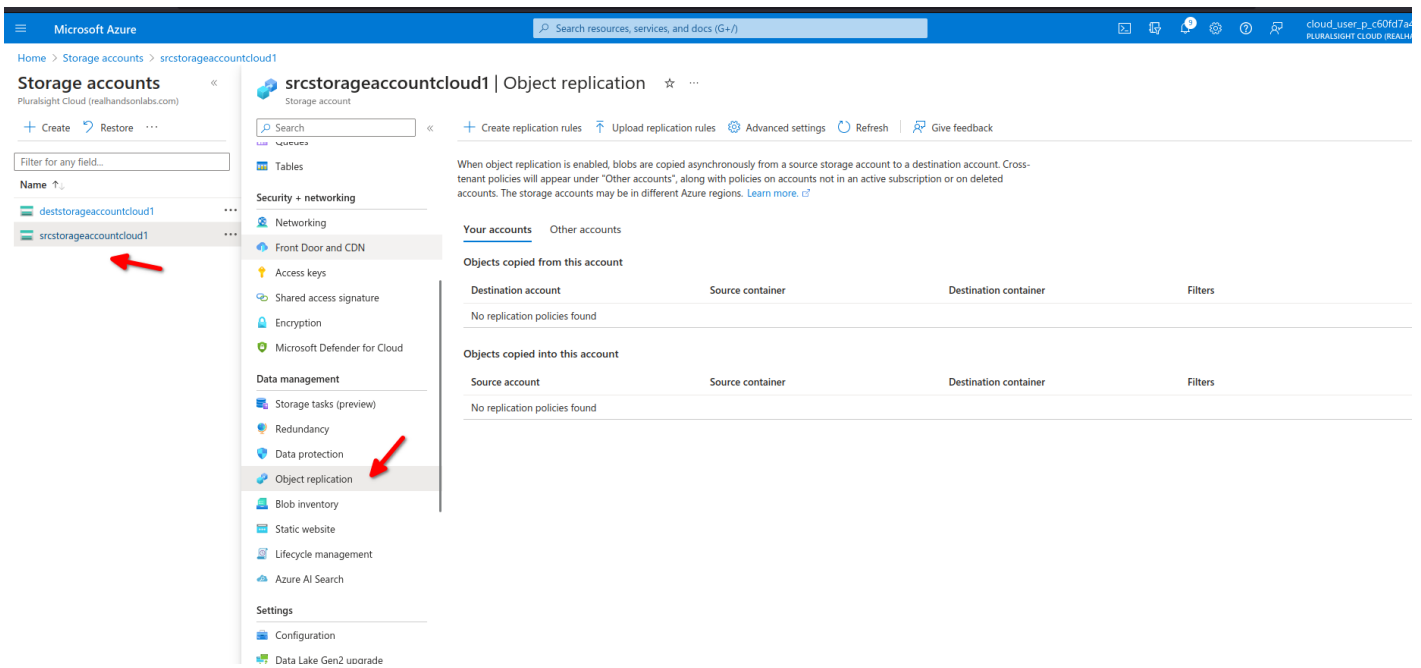
Access control

Save Discard

now we need to add our containers one on source and one on destination storage account.



Next step is to create an object replication rule on our source data storage



for our replication rule we need to select the destination storage account in this case dststorageaccountcloud1 specify the source container and destination container we can also apply filters to replicate only data on specific folder structure ,we can also specify which data to copy over here we select only new objects.

Microsoft Azure | Search resources, services, and docs (G+)

Home > Storage accounts > srcstorageaccountcloud1 | Object replication

### 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. Enabling these features may increase costs.

**Destination details**  
 To begin replicating objects, specify the source storage account and the destination storage account.  
 Learn more about copying objects in object replication

Destination subscription \*

Destination storage account \*

**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: 0 (add) | Copy over: Only new objects (change)

**Add prefix matches**

A prefix match will find items like folders and blobs under the specified container that start with the specified input. For example, inputting "a" would filter any folders or blobs that start with "a". If multiple prefixes are specified, items that have any of these prefixes will be included.

Prefix match:

Create | Cancel | Save | Cancel

srcstorageaccountcloud1 | Object replication

Storage account

Search | Create replication rules | Upload replication rules | Advanced settings | Refresh | Give feedback

**Tables**

**Security + networking**

- Networking
- Front Door and CDN
- Access keys
- Shared access signature
- Encryption
- Microsoft Defender for Cloud

**Data management**

- Storage tasks (preview)
- Redundancy
- Data protection
- Object replication

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. Learn more.

**Your accounts** | Other accounts

**Objects copied from this account**

Destination account	Source container	Destination container	Filters
deststorageaccountcloud1	srccontainer	destcontainer	1

**Objects copied into this account**

Source account	Source container	Destination container	Filters
No replication policies found			

Now we are uploading a new blob on our src storage account and src container

Microsoft Azure | Search resources, services, and docs (G+)

Home > Storage accounts > srcstorageaccountcloud1

Storage accounts | srcstorageaccountcloud1

Overview | Activity log | Tags | Diagnose and solve problems | Access Control (IAM) | Data migration | Events | Storage browser | Storage Mover

**Properties** | Monitoring | Capabilities (7) | Recommendations (0) | Tutorials | Tools + SDKs

**Blob service**

- Hierarchical namespace: Disabled
- Default access tier: Hot
- Blob anonymous access: Disabled
- Blob soft delete: Enabled (7 days)

**Upload blob**

1 file(s) selected: blob1.txt  
 Drag and drop files here or Browse for files

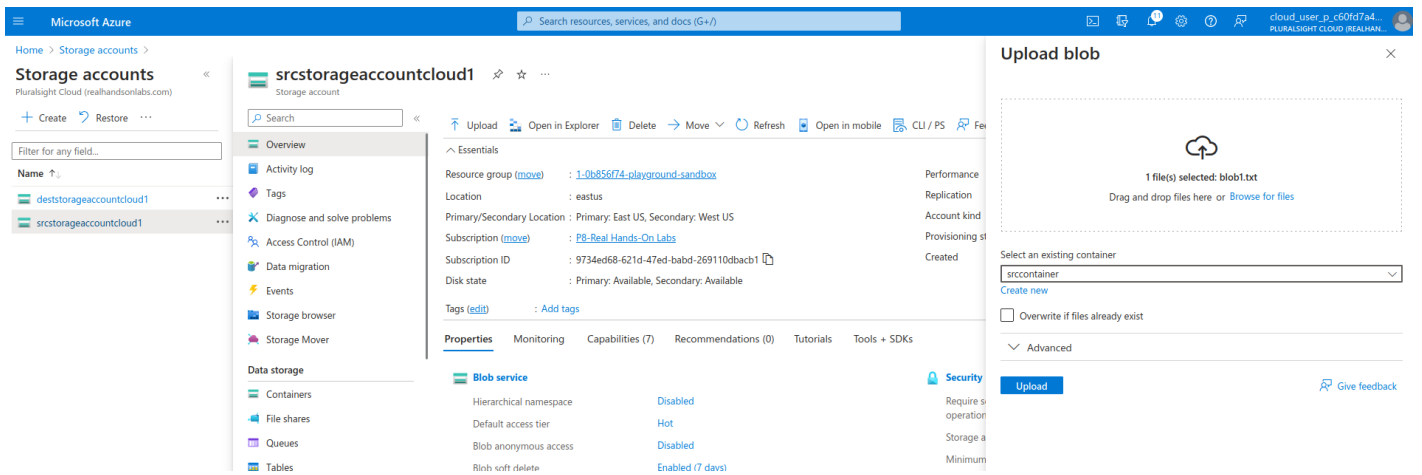
Select an existing container:

Overwrite if files already exist

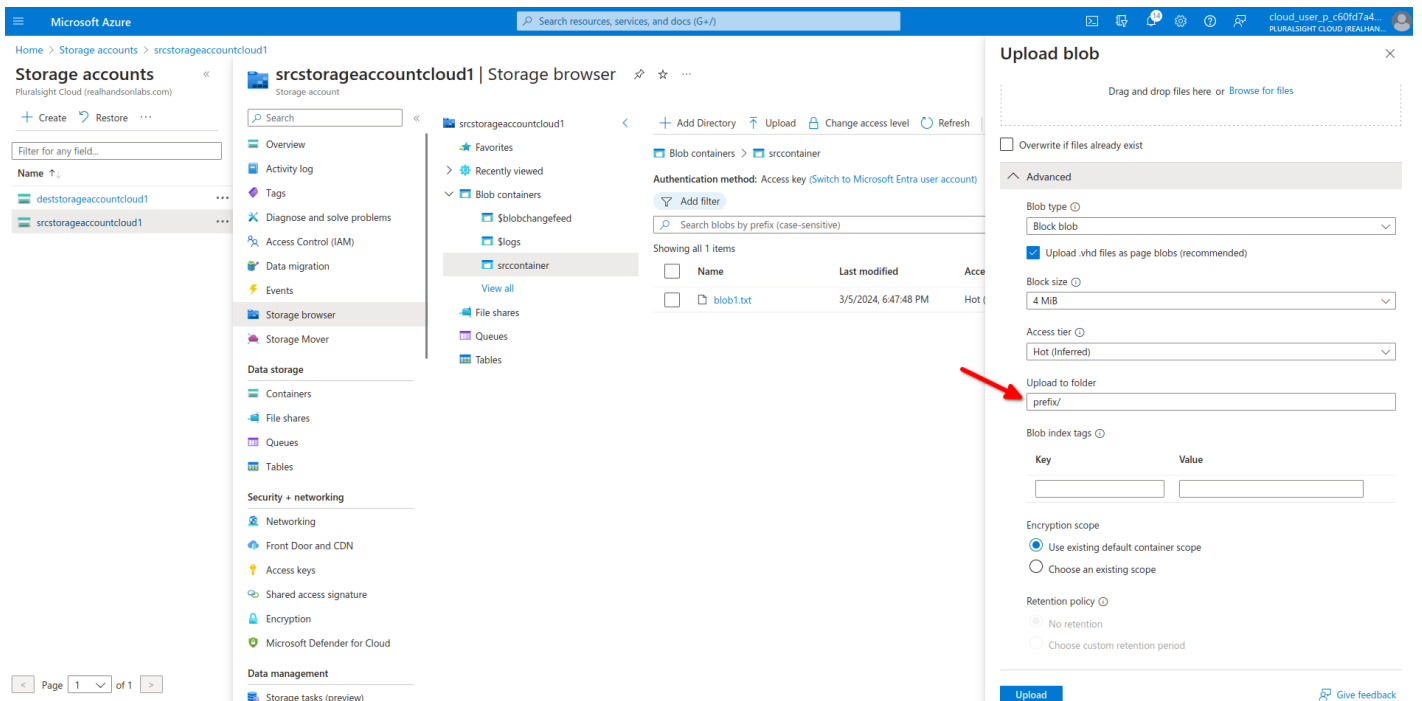
Advanced

Upload | Give feedback

now we can see file blob1.txt on our source account but not on our destination as there is a rule



we are adding our same blob but this time we will specify the folder /prefix to match our object rule.



blob.txt is now also on destination container due to our object replication

# destcontainer

Container

- Upload
- Change access level
- Refresh
- Delete
- Change tier
- Acquire lease
- Break lease
- View snapshots
- Create snapshot
- Give feedback

## Overview

Diagnose and solve problems

Access Control (IAM)

## Settings

Shared access tokens

Access policy

Properties

Metadata

**Authentication method:** Access key (Switch to Microsoft Entra user account)

**Location:** destcontainer / / prefix

Add filter

Name	Status	Retention (days)	Modified	Access tier	Archive statu
<input type="checkbox"/> [.]					
<input type="checkbox"/> blob1.txt	Previous version	-	3/5/2024, 6:57:31 PM	Hot (Inferred)	

Revision #4

Created 5 March 2024 21:53:23 by Cesar Gzz

Updated 6 March 2024 00:59:45 by Cesar Gzz