

5.- AZ-104 Azure - Storage

- [AZ-104 Azure - Storage Accounts](#)
- [AZ-104 Azure - Conceptualizing Azure Blob Storage](#)
- [AZ-104 Azure - Configuring blob object replication](#)
- [AZ-104 Azure - Configuring Blob Lifecycle Management](#)

AZ-104 Azure - Storage Accounts

- [Storage Account Overview](#)
- [Create Storage Account](#)
- [Data Redundancy Options](#)

1. Azure Queue: Message Based storage for microservices.
2. Azure Table: Non-relational semi-structured data storage service.
3. Azure Files: Cloud-based file-sharing service.
4. Azure blob: object-oriented storage solutions (store jpgs, mp4s, etc).

Type of storage account	Supported storage services	Redundancy options	Usage
Standard general-purpose v2	Blob Storage (including Data Lake Storage ¹), Queue Storage, Table Storage, and Azure Files	Locally redundant storage (LRS) / geo-redundant storage (GRS) / read-access geo-redundant storage (RA-GRS) Zone-redundant storage (ZRS) / geo-zone-redundant storage (GZRS) / read-access geo-zone-redundant storage (RA-GZRS) ²	Standard storage account type for blobs, file shares, queues, and tables. Recommended for most scenarios using Azure Storage. If you want support for network file system (NFS) in Azure Files, use the premium file shares account type.
Premium block blobs ³	Blob Storage (including Data Lake Storage ¹)	LRS ZRS ²	Premium storage account type for block blobs and append blobs. Recommended for scenarios with high transaction rates or that use smaller objects or require consistently low storage latency. Learn more about example workloads.

Type of storage account	Supported storage services	Redundancy options	Usage
Premium file shares ³	Azure Files	LRS ZRS ²	Premium storage account type for file shares only. Recommended for enterprise or high-performance scale applications. Use this account type if you want a storage account that supports both Server Message Block (SMB) and NFS file shares.
Premium page blobs ³	Page blobs only	LRS ZRS ²	Premium storage account type for page blobs only. Learn more about page blobs and sample use cases.

Storage accounts

- Account type: determines feature and costs.
- Performance tier: determines performance levels.
- Replication: determines infrastructure redundancy.
- Access tier: determines access level and data costs.

Azure Storage Redundancy

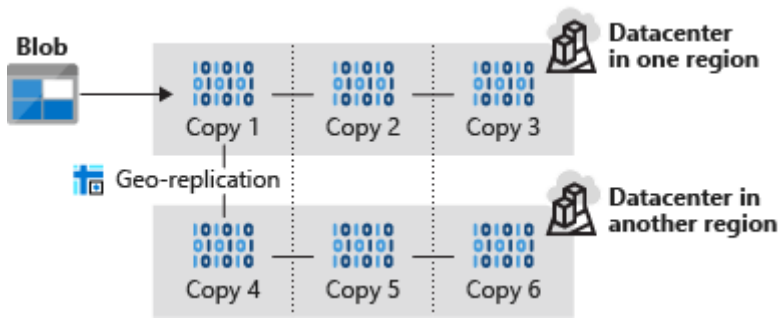
Locally redundant storage

Illustration that shows three copies of blob data stored in the same datacenter with LRS.

Locally redundant storage (LRS) copies your data three times across separate racks of hardware in a datacenter inside one region. Even if there's a hardware failure or if there's maintenance work in the datacenter, this replication type ensures data is available for use.

LRS doesn't protect you from a datacenter-wide outage. If the datacenter goes down, you could lose your data.

Geographically redundant storage



Read-access geo-redundant storage

With GRS, your secondary region isn't available for read access until the primary region fails. If you want to read from the secondary region, even if the primary region hasn't failed, use Read-access geo-redundant storage (RA-GRS) for your replication type.

Zone-redundant storage

Illustration of data copied to three storage clusters in separate availability zones with ZRS.

Zone-redundant storage (ZRS) copies your data in three storage clusters in a single region. Each cluster is in a different physical location and is considered as a single availability zone. Each cluster uses its own separate utilities for things like networking and power. If one datacenter is experiencing an outage, your data remains accessible from another availability zone in the same Azure region.

Because all availability zones are in a single region, ZRS can't protect your data from a regional-level outage.

Geo-zone-redundant storage

Geo-zone-redundant storage (GZRS) combines the high availability benefits of ZRS with GRS. With this replication type, your data is copied across three availability zones in one region. Data is also replicated three times to another secondary region that's paired with it. This way, your zone-redundant data is also secure from regional-level outages.

Read-access geo-zone-redundant storage

Read-access geo-zone-redundant storage (RA-GZRS) uses the same replication method as GZRS, but lets you read from the secondary region. If you want to read the data that's replicated to the secondary region, even if your primary isn't experiencing downtime, use RA-GZRS for your replication type.

GZRS and RA-GZRS are currently available in the following regions:

- South Africa North
- Australia East
- East Asia
- Japan East
- Korea Central
- Southeast Asia
- Central India
- France Central
- Germany West Central
- North Europe
- Norway East
- Sweden Central
- Switzerland North
- UK South
- West Europe
- Canada Central
- Central US
- East US
- East US 2
- South Central US
- West US 2
- West US 3
- US Gov Virginia
- Brazil South

Paired regions

A paired region is where an Azure region is paired with another in the same geographical location to protect against regional outage. Paired regions are used with GRS and GZRS replication types.

Illustration that shows a hierarchy of geography, regional pair, region, and datacenters.

Here's a list showing some of the regions that are paired together. You can get the full list at [Azure paired regions](#).

	Region	Region
Asia	East Asia	Southeast Asia
Australia	Australia East	Australia Southeast
Canada	Canada Central	Canada East
China	China North	China East

	Region	Region
Europe	North Europe (Ireland)	West Europe (Netherlands)
Japan	Japan East	Japan West
North America	East US	West US
South Africa	South Africa North	South Africa West
UK	UK West	UK South

Use cases for each replication type

The following table summarizes how many copies you get with each replication type and when you should use it.

Replication type	Copies	Use case
LRS	3	Data remains highly available, but for compliance reasons, isn't allowed to leave the local datacenter.
GRS	6	App has access to the data, even if an entire region has an outage.
RA-GRS	6	App reads from multiple geographical locations, so you can serve users from a location that's closer to them.
ZRS	3	Need redundancy in multiple physical locations, but because of compliance, data isn't allowed to leave a region.
GZRS	6	App can access data, even if the primary region has failed, and your secondary region has a datacenter that's experiencing an outage, but you don't want to read from the secondary region unless the primary region is down.

Replication type	Copies	Use case
RA-GZRS	6	Regularly read data from your secondary region, perhaps to serve users from a location closer to them, even if a datacenter is up in your primary region.

Creating a storage account

Navigate to Storage accounts and then create

The screenshot shows the 'Create a storage account' page in the Microsoft Azure portal. The page is divided into several sections: 'Project details', 'Instance details', and 'Performance'. Five red numbered callouts (1-5) are overlaid on the page, pointing to specific elements:

- 1**: Points to the 'Subscription' dropdown menu.
- 2**: Points to the 'Resource group' dropdown menu.
- 3**: Points to the 'Storage account name' text input field.
- 4**: Points to the 'Performance' radio button options.
- 5**: Points to the 'Make read access to data available in the event of regional unavailability' checkbox.

The page includes a navigation bar at the top with 'Microsoft Azure' and a search bar. Below the navigation bar, there are breadcrumb links: 'Home > Storage accounts >'. The main heading is 'Create a storage account'. Below the heading, there are tabs for 'Basics', 'Advanced', 'Networking', 'Data protection', 'Encryption', 'Tags', and 'Review'. The 'Basics' tab is selected. Below the tabs, there is a link for 'storage accounts'. The 'Project details' section contains a description and two dropdown menus for 'Subscription' and 'Resource group'. The 'Instance details' section contains a text input for 'Storage account name', a dropdown for 'Region', and radio buttons for 'Performance'. The 'Performance' section contains radio buttons for 'Standard' and 'Premium'. The 'Redundancy' section contains a dropdown for 'Geo-redundant storage (GRS)' and a checked checkbox for 'Make read access to data available in the event of regional unavailability'. At the bottom of the page, there is a 'Review' button and a 'Next: Advanced >' button.

Select type of redundancy

Instance details

Storage account name ⓘ *

Region ⓘ *

Performance ⓘ *

Redundancy ⓘ *

Locally-redundant storage (LRS):

Lowest-cost option with basic protection against server rack and drive failures. Recommended for non-critical scenarios.

Geo-redundant storage (GRS):

Intermediate option with failover capabilities in a secondary region. Recommended for backup scenarios.

Zone-redundant storage (ZRS):

Intermediate option with protection against datacenter-level failures. Recommended for high availability scenarios.

Geo-zone-redundant storage (GZRS):

Optimal data protection solution that includes the offerings of both GRS and ZRS. Recommended for critical data scenarios.

Geo-redundant storage (GRS) ▾

Make read access to data available in the event of regional unavailability.

[Home](#) >

 **htflearning1_1709165080802** | Overview  

Search < Delete Cancel Redeploy Download Refresh


Overview


Inputs

Outputs

Template

Deployment is in progress

 Deployment name: htflearning1_1709165080802
Subscription: [PS-Real Hands-On Labs](#)
Resource group: [1-df4064bd-playground-sandbox](#)

Start time: 2/28/2024, 6:04:44 PM
Correlation ID: [bcd9a695-ba96-4d05-a581-3fd2cb892d72](#) 

Deployment details

Resource	Type	Status	Operation details
No results.			

Give feedback

[Tell us about your experience with deployment](#)

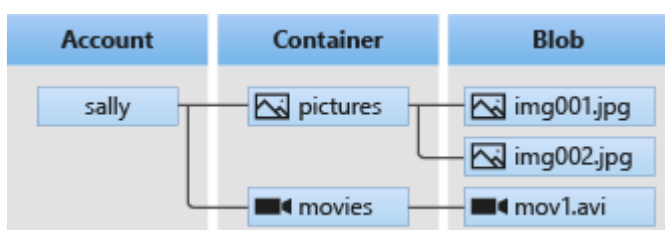
Account Type	General purpose v1	Legacy for blobs, files, queues, and tables
	General purpose v2	Recommended for blobs, files, queues, and tables
Performance Tier	Blob storage	Legacy blob-specific accounts
	Standard	Default storage performance tier
	Premium	High-performance storage tier
Replication	Locally redundant storage (LRS)	Three copies in a physical location within a region
	Zone-redundant storage (ZRS)	Three copies across zones within a region
	Geo-redundant storage (GRS)	LRS in a primary and secondary region
	Geo-zone-redundant storage (GZRS)	ZRS in a primary region and LRS in a secondary region
Access Tier	Hot	Frequently accessed data
	Cold	Infrequently accessed data
	Archive	Backup data rarely accessed

AZ-104 Azure - Conceptualizing Azure Blob Storage

- [What is blob storage](#)
- [Introduction to Azure Blob Storage](#)

1. Describing Azure Blob Storage
2. Components of Blob Architecture
3. Type of Blobs
4. Container Access Levels

Azure Blob Storage is Microsoft's object storage solution for the cloud. Blob Storage is optimized for storing massive amounts of unstructured data. Unstructured data is data that doesn't adhere to a particular data model or definition, such as text or binary data. Its object based and easily accessible from HTTP/REST



Blob Storage is designed for:

- Serving images or documents directly to a browser.
- Storing files for distributed access.
- Streaming video and audio.
- Writing to log files.
- Storing data for backup and restore, disaster recovery, and archiving.
- Storing data for analysis by an on-premises or Azure-hosted service.

Blob Architecture

- Blob Service: A sub service for storage accounts.
- Blob Container: The container where we store our blobs.
- Blobs: The data we store in our containers.

Types of Blobs

- Block blobs: Storing images or videos best suited for streaming.
- Append blobs: Log files
- Page Blobs: Virtual machine disks

Container Access Level

- Access control: By default, public access to blobs is granted at the storage account level

Container Access Levels:

- Private: No anonymous access.
- Blob: Anonymous access to blob
- Container: Anonymous access to container and blobs it contains.

Now let's access our Storage account ,below we can see the system storage account, here we will crate a container

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below that, the breadcrumb path is 'Home > htflearning1_1709165080802 | Overview > htflearning1'. The main header shows 'htflearning1 | Containers' with a storage account icon and name. Below the header, there's a search bar and several action buttons: '+ Container', 'Change access level', 'Restore containers', 'Refresh', 'Delete', and 'Give feedback'. A table lists the containers, with one entry: '\$logs'.

Name	Last modified	Anonymous access level	Lease state
<input type="checkbox"/> \$logs	2/28/2024, 6:05:06 PM	Private	Available

First check if blob anonymous access its enabled if not click on the link to enable

- Upload
- Open in Explorer
- Delete
- Move
- Refresh
- Open in mobile
- CLI / PS
- Feedback

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
- Front Door and CDN
- Access keys
- Shared access signature
- Encryption

Essentials

Resource group (move) : [1-df4064bd-playground-sandbox](#)
Location : eastus
Subscription (move) : [P5-Real Hands-On Labs](#)
Subscription ID : 80ea84e8-afce-4851-928a-9e2219724c69
Disk state : Available
Tags (edit) : [Add tags](#)

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

Blob service

Hierarchical namespace	Disabled
Default access tier	Cool
Blob anonymous access	Enabled
Blob soft delete	Enabled (7 days)
Container soft delete	Enabled (7 days)
Versioning	Disabled
Change feed	Disabled
NFS v3	Disabled
Allow cross-tenant replication	Disabled
Storage tasks assignments	None

File service

now create a new container, anonymous access level will only be available if blob anonymous access its enabled.

 + Container Change access level Restore containers Refresh Delete Give feedback Show deleted container

Name	Last modified	Anonymous access level
Slugs	2/28/2024, 6:05:06 PM	Private

New container

Name * privatecontainer

Anonymous 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)

3 different levels of containers with different access.

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

Home > htflerning1_1709165080802 | Overview > htflerning1

htflerning1 | Containers

Storage account

Search containers by prefix Show deleted containers

Name	Last modified	Anonymous access level	Lease state
<input type="checkbox"/> \$logs	2/28/2024, 6:05:06 PM	Private	Available
<input type="checkbox"/> blobcontainer	2/28/2024, 6:16:54 PM	Blob	Available
<input type="checkbox"/> containeraccesscontainer	2/28/2024, 6:17:09 PM	Container	Available
<input type="checkbox"/> privatecontainer	2/28/2024, 6:16:36 PM	Private	Available

Left sidebar: Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover

We can see each container has its own url to access the container

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

Home > htflerning1_1709165080802 | Overview > htflerning1 | Containers > containeraccesscontainer

containeraccesscontainer | Properties

Refresh Give feedback

NAME
containeraccesscontainer

URL
<https://htflerning1.blob.core.windows.net/containeraccesscontainer>

LAST MODIFIED
2/28/2024, 6:17:09 PM

ETAG
0x8DC388BC52E5805

LEASE STATUS
Unlocked

LEASE STATE
Available

LEASE DURATION
-

ENCRYPTION SCOPE
\$account-encryption-key

VERSION-LEVEL IMMUTABILITY SUPPORT
Disabled

now let's upload a random file to our private container, we can see it has its own url to access the file directly

privatecontainer

Container

Search [] Upload Change access level ...

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

Search blobs by prefix (case-...)
 Show deleted blobs

Add filter

Name
<input checked="" type="checkbox"/> azure.png

azure.png

Blob

Save Discard Download Refresh Delete Change tier Acquire lease Break lease Give feedback

Overview Versions Snapshots Edit Generate SAS

Properties

URL: <https://htflarning1.blob...>

LAST MODIFIED	2/28/2024, 6:21:08 PM
CREATION TIME	2/28/2024, 6:21:08 PM
VERSION ID	-
TYPE	Block blob
SIZE	288.39 KiB
ACCESS TIER	Cool (Inferred)
ACCESS TIER LAST MODIFIED	N/A
ARCHIVE STATUS	-
REHYDRATE PRIORITY	-
SERVER ENCRYPTED	true
ETAG	0x8DC38BC53BC6C26
VERSION-LEVEL IMMUTABILITY POLICY	Disabled
CACHE-CONTROL	
CONTENT-TYPE	image/png
CONTENT-MD5	RBEEeh9FaW1dsFVobvP28w==
CONTENT-ENCODING	
CONTENT-LANGUAGE	
CONTENT-DISPOSITION	
LEASE STATUS	Unlocked
LEASE STATE	Available
LEASE DURATION	-

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

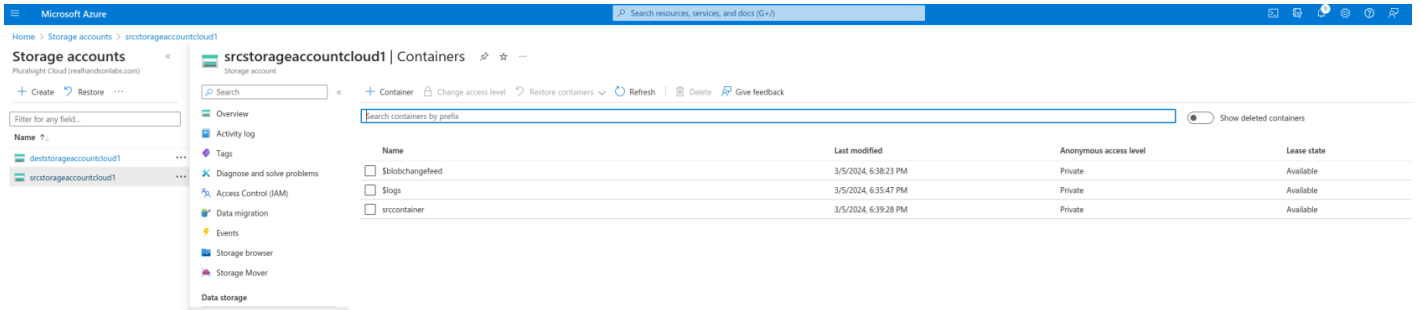
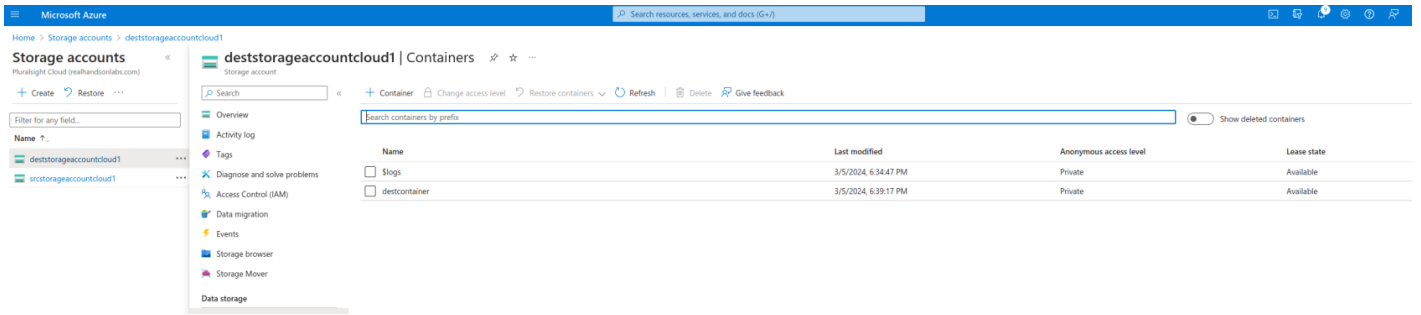
Tracking

- 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)

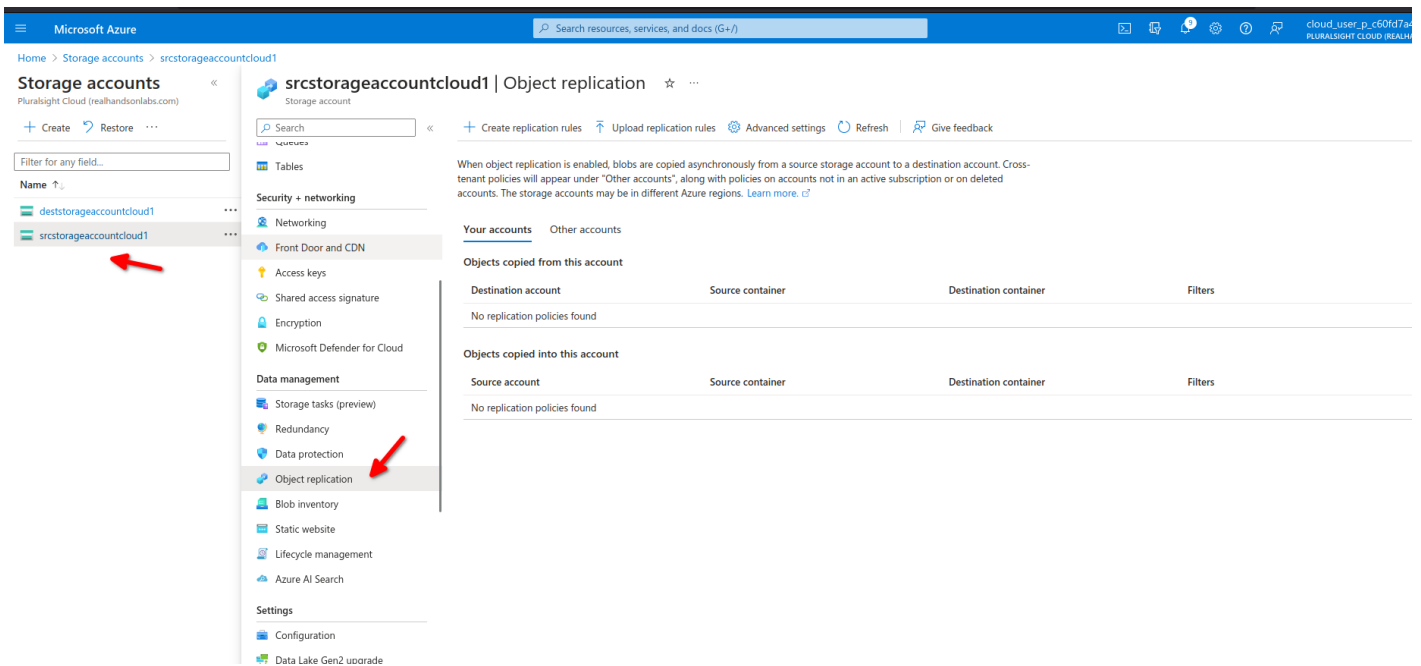
Access control

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

Filter for any field...

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

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

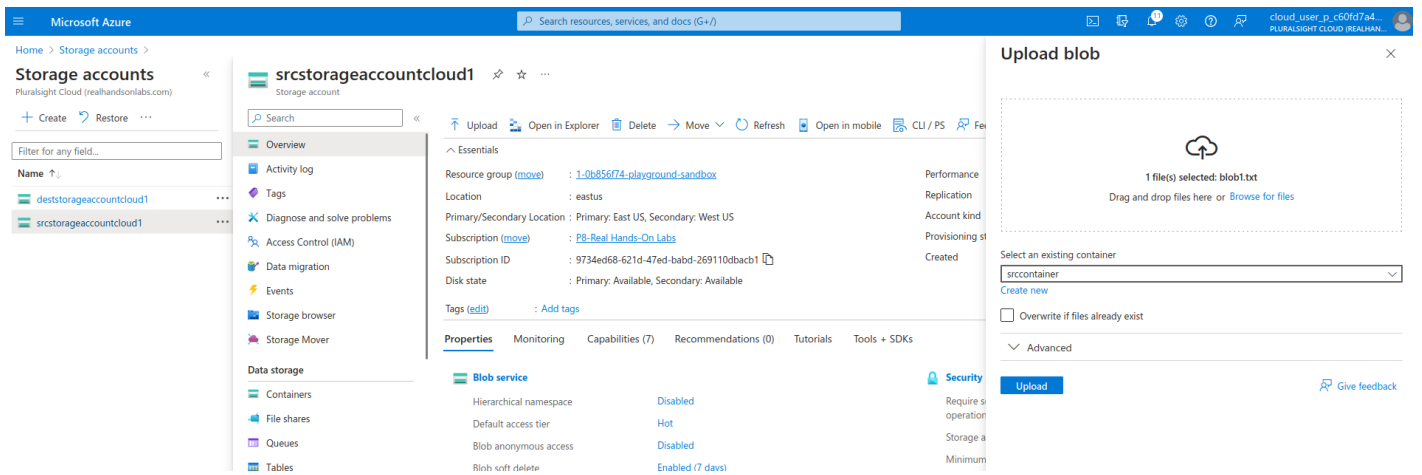
Select an existing container:

Overwrite if files already exist

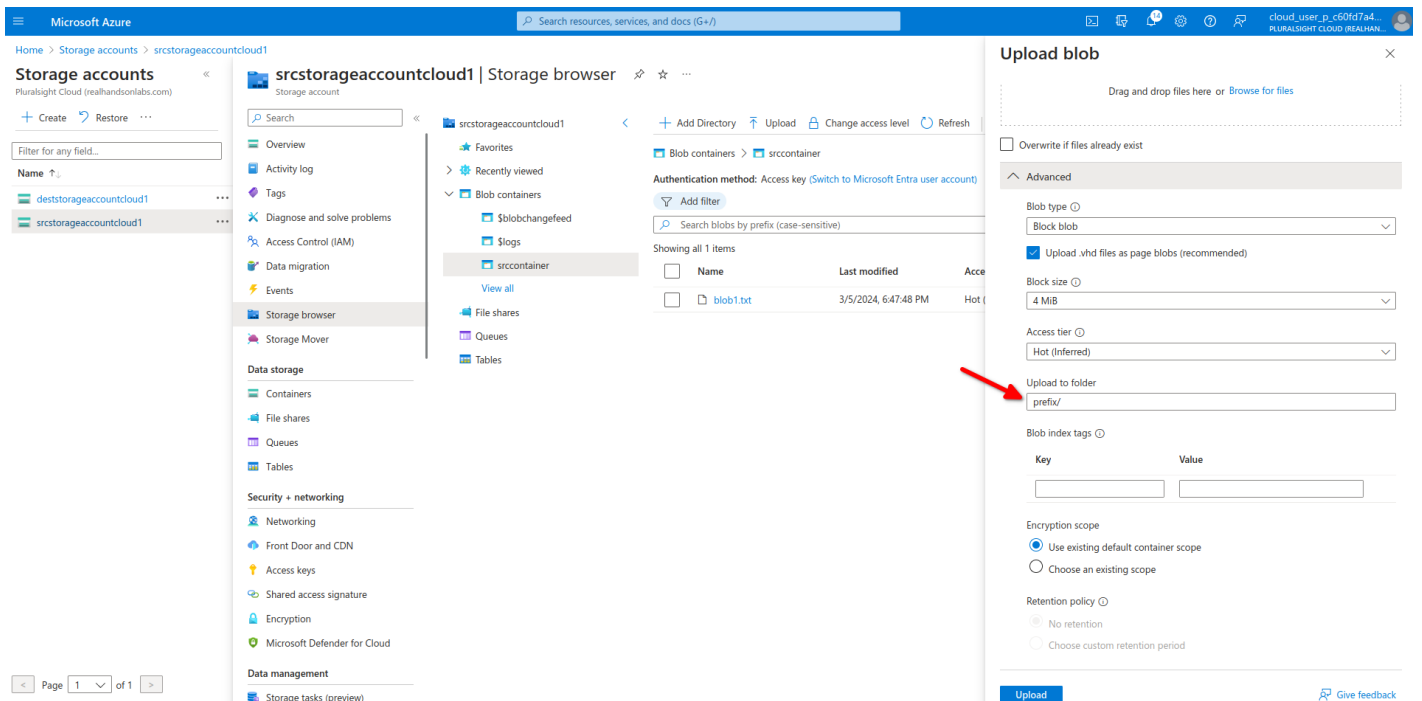
Advanced

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

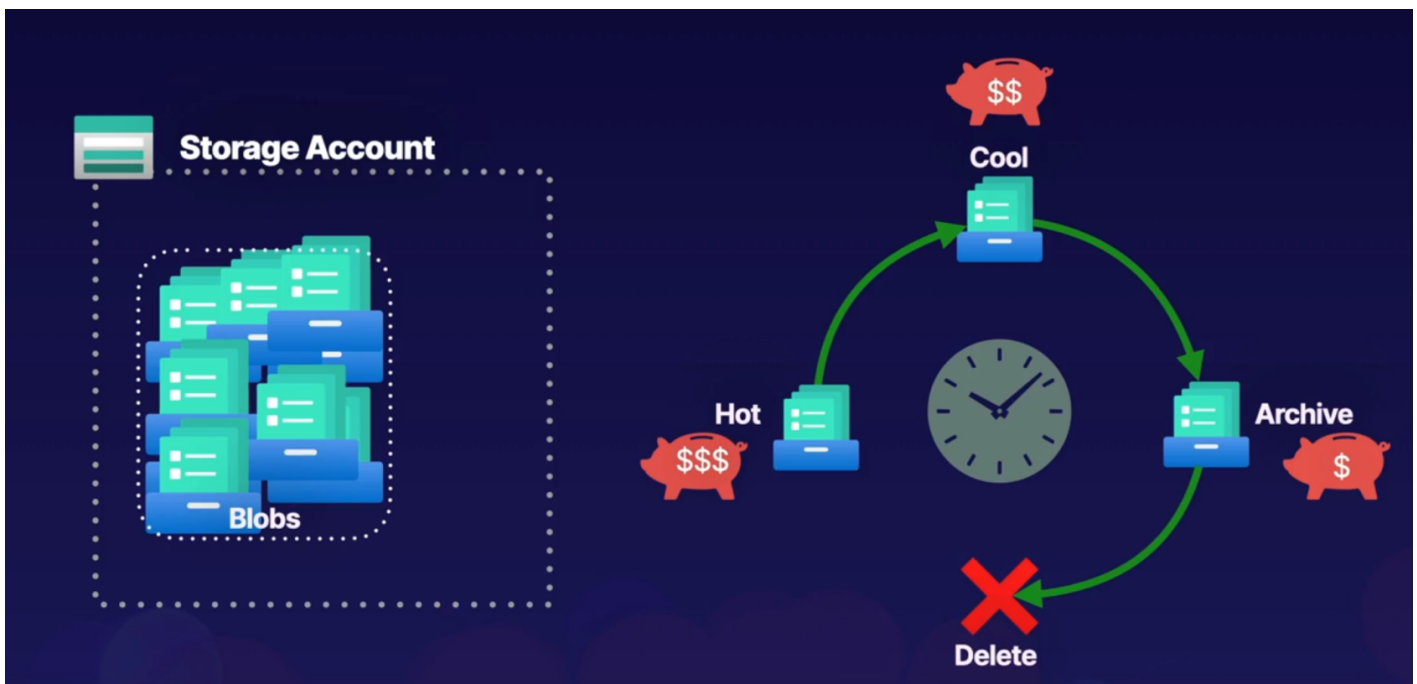
Name	Status	Retention (days)	Modified	Access tier	Archive statu
<input type="checkbox"/> [.]					
<input type="checkbox"/> blob1.txt	Previous version	-	3/5/2024, 6:57:31 PM	Hot (Inferred)	

AZ-104 Azure - Configuring Blob Lifecycle Management

Lifecycle Management Concepts

Azure Blob Storage service feature that enables automation to manage lifecycle operations of blobs.

- Automate blob lifecycle: Easily manage blob life-cycles from frequent use to archive or deletion
- Move access tiers: Switch blobs between tiers to meet access or usage needs.
- Optimize cost: Save money by decreasing admin overhead and tiering blobs based on usage requirements.



Let's add random files to our container and add a lifecycle rule

Storage accounts

PluralSight Cloud (realhandsonlabs.com)

+ Create Restore ...

Filter for any field...

Name ↑

- deststorageaccountcloud1
- srcstorageaccountcloud1

srcstorageaccountcloud1 | Lifecycle management

Storage account

Search

+ Add a rule Enable Disable Refresh Delete Give feedback

Lifecycle management offers a rich, rule-based policy for general purpose v2 and blob storage accounts. Use the policy to transition your data to the appropriate access tiers or expire at the end of the data's updated policy may take up to 48 hours to complete. [Learn more](#)

List View Code View

Enable access tracking

Name	Status	Blob type
------	--------	-----------

No rules

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





Add a rule ...

- 1 Details
- 2 Base blobs
- 3 Filter set

A rule is made up of one or more conditions and actions that apply to the entire storage account. Optionally, specify that rules will apply to particular blobs by limiting with filters.

Rule name *

Rule scope *

- Apply rule to all blobs in your storage account
- Limit blobs with filters

Blob type *

- Block blobs
- Append blobs



Blob subtype *

- Base blobs
- Snapshots
- Versions



Home > Storage accounts > srcstorageaccountcloud1 | Lifecycle management >


Add a rule ...

✓ Details **2 Base blobs**

Lifecycle management uses your rules to automatically move blobs to cooler tiers or to delete them. If you create multiple rules, the associated actions must be implemented in tier order (from hot to cool storage, then archive, then deletion).


If

Base blobs were *

Last modified 


Created

More than (days ago) *

30 

↓

Then

Move to cool storage 

Move to cool storage
For infrequently accessed data that you want to keep on cool storage for at least 30 days.

Move to cold storage
For rarely accessed data that you want to keep for at least 90 days.

Move to archive storage
Use if you don't need online access and want to keep the object for 180 days or longer.

Delete the blob
Deletes the object per the specified conditions.

we can also specify a filter to modify only those inside our testcontainer/folder

Home > Storage accounts > srcstorageaccountcloud1 | Lifecycle management >

Add a rule ...

✔ Details ✔ Base blobs **3** Filter set

Blob prefix

Filter blobs by name or first letters. To find items in a specific container, enter the name of the container followed by a forward slash, then the blob name or first letters. For example, to show all blobs starting with "a", type: "mycontainer/a".

Blob prefix

testcontainer/folder



Enter a prefix or file path such as "mycontainer/prefix"

Blob index match

If you have indexed items in containers with keys and values, you can filter for them.

Key

Value

Enter an index key

== ▾

Enter a value

Previous

Add

Now after 30 days all our blobs will move from hot to cold.

- Storage accounts: Support GPv2 storage accounts and blob storage accounts.
- Types and Sub-types: Support block and append blobs and support sub-types such as based blobs snapshots and versions.

- Filtering: filter blobs in the rule using prefix or blob index matches.
- Scoping: Scope at the storage account or limit blobs with filters.
- If/Then Logic: Uses logic in lifecycle rules to move blobs through access tiers based on modification and access times.