WHITEPAPER

Retrospect
A StorCentric Company
Data Protection for Businesses

Retrospect Backup

Cloud Data Protection: Protect Data on Microsoft Azure Blob Storage

Backup Less. Manage Less. Worry Less.

Microsoft Azure Blob Storage provides a low-cost, scalable cloud storage location for a multitude of corporate assets.

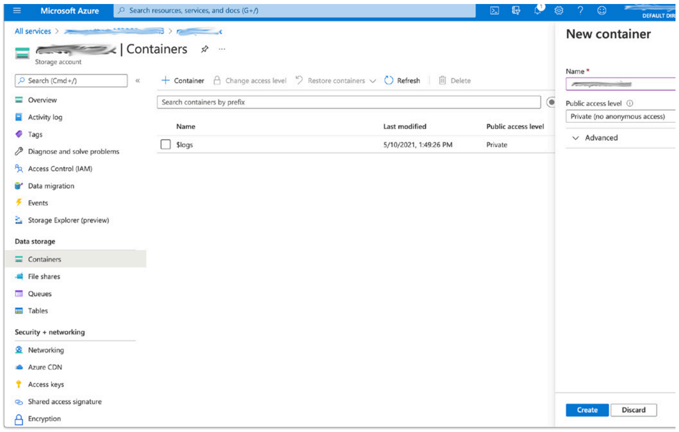
Why You Should Protect Cloud Data

Data loss can happen for a multitude of reasons. Someone might accidentally delete a file or a folder. A malicious person might destroy what they have access to. The administrator might simply lose the credentials. All of these scenarios apply to the cloud as well. You need to protect your data, wherever it resides.

Companies use cloud storage for all sorts of data, from website assets to affordable sharing to ingestable data, and Retrospect Backup includes cloud data protection support for cloud storage as a first-class backup volume. Cloud volumes enable businesses to protect their cloud content on-site with an incremental backup or on a different cloud with an automated policy-driven workflows.

Step-by-Step Guide

Cloud data protection is easy with Retrospect. Let's walk through adding an Azure Blob volume to Retrospect and then setting up a policy to protect it on-premise.



All services > [redacted] > [redacted]

[redacted] | Containers

	Name	Last modified	Public access level
□	$logs	5/10/2021, 1:49:26 PM	Private

New container

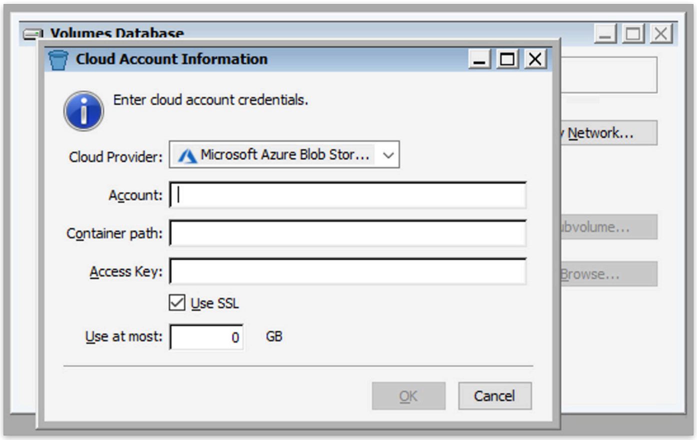
Name * [redacted]

Public access level: Private (no anonymous access)

1) In Azure Console, you will need the container name from Azure as well as the Account ID and Access Key. These are available in the Azure Console. 9 azure new container

2) Click on "Access keys" and click "Show keys" to get your secret key from under key1 > Key.

3) In Retrospect, click on "Volumes" (Windows) or "Sources" (Mac).



Cloud Account Information

Enter cloud account credentials.

Cloud Provider: Microsoft Azure Blob Stor...

Account:

Container path:

Access Key:

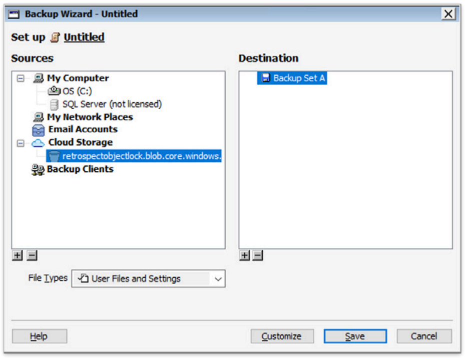
☑ Use SSL

Use at most: 0 GB

4) Select "Microsoft Azure Blob Storage".

5) Type in your container information from above and click "OK".

6) Create a backup script policy for protecting that volume by clicking "Backup Now" (Windows) or "Backup" (Mac).



Backup Wizard - Untitled

Set up Untitled

Sources
- My Computer
  - OS (C:)
  - SQL Server (not licensed)
- My Network Places
- Email Accounts
- Cloud Storage
  - retrospectobjectlock.blob.core.windows.
- Backup Clients

Destination
- Backup Set A

File Types: User Files and Settings

7) You can now protect your cloud volume using Retrospect, either in another cloud destination or on-premise.

Information for Retrospect

Retrospect needs three pieces of information to access Microsoft Azure Blog Storage:

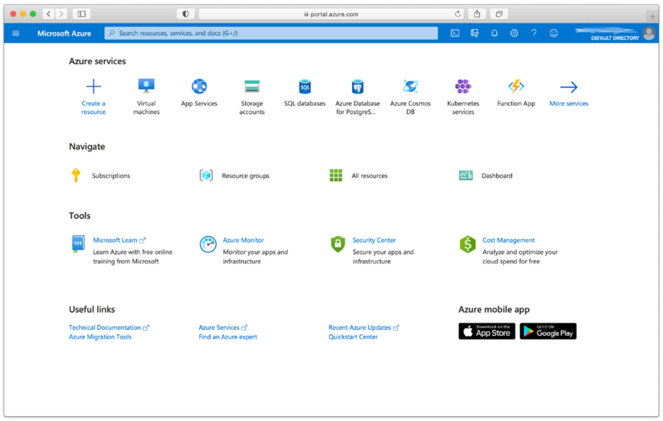
- Account – Use the account name from above.
- Container Path – container_name/path
- Access Key – Use the access key from Storage Account > Access Keys > Secret.

Note that on Mac, "Account" and "Container Path" are combined into "Path", separated with a forward slash.

Account Setup Guide

Follow these steps to quickly create a Microsoft Azure Blob Storage Account. It requires an existing Microsoft Azure Account. If you do not already have one, create one for free at Microsoft Azure.

Visit Microsoft Azure Blob Storage and click "Start free" then click "Start free" for the free Azure account. You'll be able to connect Azure Blob Storage to your existing Azure subscription.



1) Visit Microsoft Azure to see your new account.

2) Create a storage account.

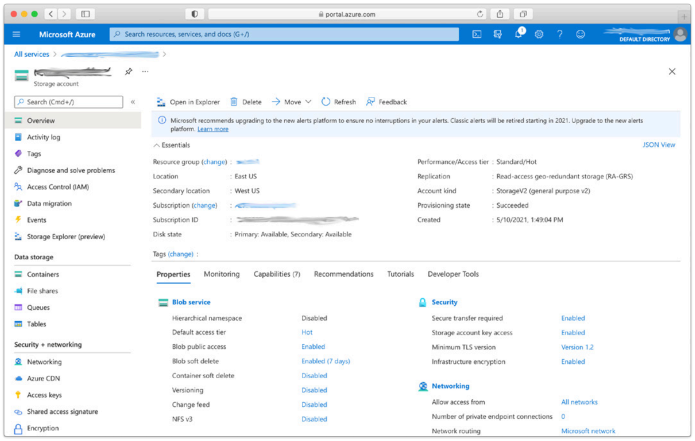
3) Configure your storage account and click "Create".

4) Click "Go to resource" to vist your new storage account.

Storage Setup Guide

Now we will create a container that Retrospect can use to store backups.

1) In your storage account, click on "Containers".



[redacted]

Microsoft recommends upgrading to the new alerts platform to ensure no interruptions in your alerts. Classic alerts will be retired starting in 2021. Upgrade to the new alerts platform. Learn more

Essentials

Resource group (change) : [redacted]
Location : East US
Secondary location : West US
Subscription (change) : [redacted]
Subscription ID : [redacted]
Disk state : Primary: Available, Secondary: Available
Tags (change) :

Performance/Access tier : Standard/Hot
Replication : Read-access geo-redundant storage (RA-GRS)
Account kind : StorageV2 (general purpose v2)
Provisioning state : Succeeded
Created : 5/10/2021, 1:49:04 PM

Blob service

Hierarchical namespace	Disabled
Default access tier	Hot
Blob public access	Enabled
Blob soft delete	Enabled (7 days)
Container soft delete	Disabled
Versioning	Disabled
Change feed	Disabled
NFS v3	Disabled

Security

Secure transfer required	Enabled
Storage account key access	Enabled
Minimum TLS version	Version 1.2
Infrastructure encryption	Enabled

Networking

Allow access from	All networks
Number of private endpoint connections	0
Network routing	Microsoft network

2) Click "+ Container".

3) Fill in your container name and click "Create".

4) Click on "Access keys" and click "Show keys" to get your secret key from under key1 > Key.

About Retrospect, Inc.

Retrospect Backup has been protecting data for small and medium businesses for thirty years. We support businesses where they are, with local sales representation and thousands of partners across the world, on six continents and seven languages. Contact us at https://www.retrospect.com/contact_sales.

retrospect.com/try