



Retrospect Backup Anti-Ransomware: Immutable Backups with Microsoft Azure Blob

Backup Less. Manage Less. Worry Less.

Microsoft Azure Blob Storage provides a low-cost, scalable cloud storage location for secure off-site data protection. Immutable Storage for Azure Blob enables customers to lock files that are under a certain age in that bucket.

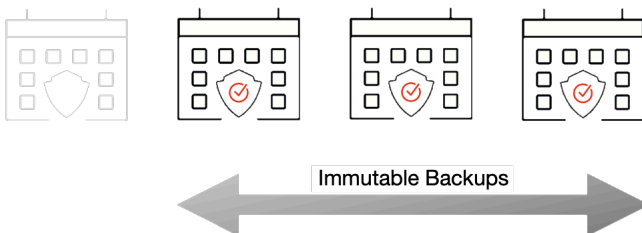


This per-bucket policy approach differs from Microsoft Azure's per-object policy approach, such that Retrospect Backup cannot set the retention policies for individual files that make up a backup. However, setting a bucket policy enables customers to lock the files for a certain period of time, so this is a great anti-ransomware solution for Microsoft Azure customers.

Microsoft Azure Blob Storage provides a low-cost, scalable cloud storage location for secure off-site data protection. Immutable Storage for Azure Blob enables customers to lock files that are under a certain age in that bucket.

Overview

Ransomware attacks are increasingly sophisticated, having the capability of watching for cloud account credentials, deleting backups and cloud storage, then encrypting everything and demanding a ransom. It's imperative to build defenses against this escalating attack. SMBs and large businesses need a backup target that allows them to lock backups for a designated time period. Many of the major cloud providers now support object locking, also referred to as Write-Once-Read-Many (WORM) storage or immutable storage. Users can mark objects as locked for a designated period of time, preventing them from being deleted or altered by any user.



Backups made to a Microsoft Azure Blob container with a re-

ention period are immutable backups, with a retention period that prevents deletion by anyone accessing the container.

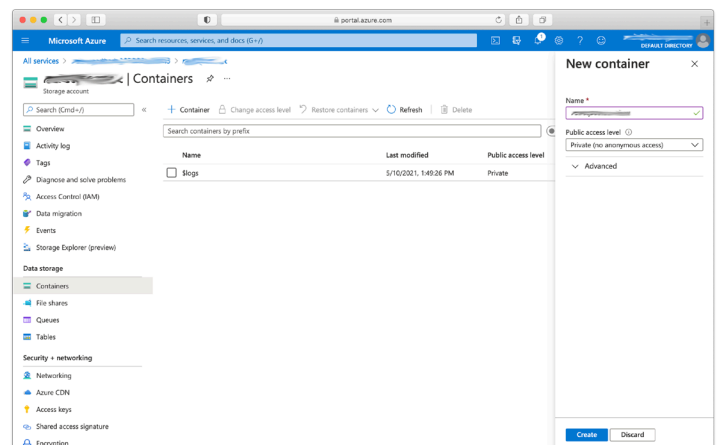
Note that customers are responsible for keeping track of the retention period and modifying it accordingly to ensure all of the backups inside the container continue to be marked as immutable backups.

For more information about backing up to Microsoft Azure Blob Storage container with Retrospect Backup, see [How to Set Up a Microsoft Azure Blob Storage Account](#).

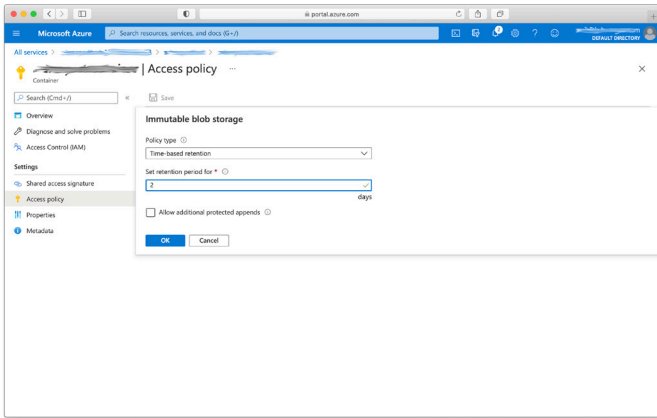
Step-by-Step Guide

Retrospect Backup makes it easy to back up to Microsoft Azure Blob Storage container. Let's walk through the steps for creating a bucket with a Bucket Lock retention policy.

- 1) Microsoft Azure: [Create a Microsoft Azure Blob Storage Account](#) if you have not already.
- 2) Microsoft Azure: Click "Containers".
- 3) Microsoft Azure: Click "+ Container". Fill out the name and click "Create".



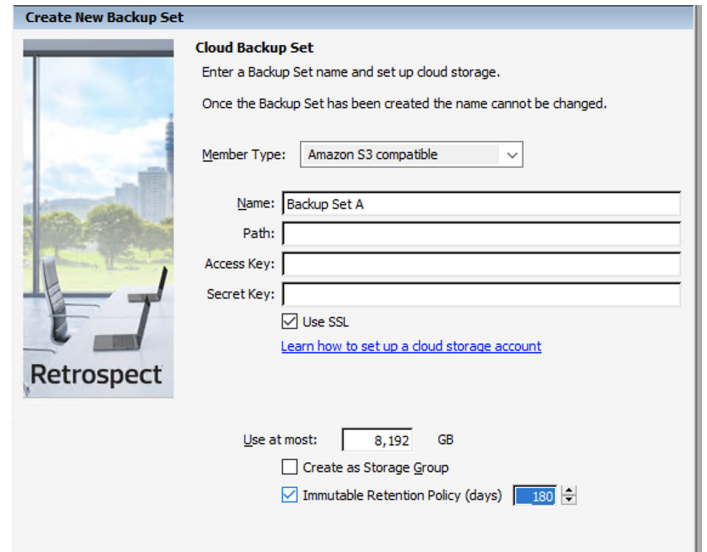
- 4) Microsoft Azure: Click on the new container and then on "Access Policy". Then click "Add policy".
- 5) Microsoft Azure: Enter the period of time for immutable storage and click "OK".



- 6) Microsoft Azure: Your policy has been added.
- 7) Microsoft Azure: To enforce the policy, you must click on the "... " on the right and select "Lock Policy". Note that this will enforce the immutable policy and prevent deletions for the specified period of time.
- 8) Note that you can also add an immutable storage policy to an existing blob container.
- 9) Retrospect: Add a destination. On Windows, select "Backup Sets" then "Create". On Mac, select "Media Sets" and click "Add". Select type "Cloud". Note that the "Immutable Retention Policy" checkbox is not relevant because you'll use the Microsoft Azure Blob storage container with the bucket-level retention policy.
- 10) Retrospect: Add the destination to a script and start protecting your data in Microsoft Azure Blob Storage.

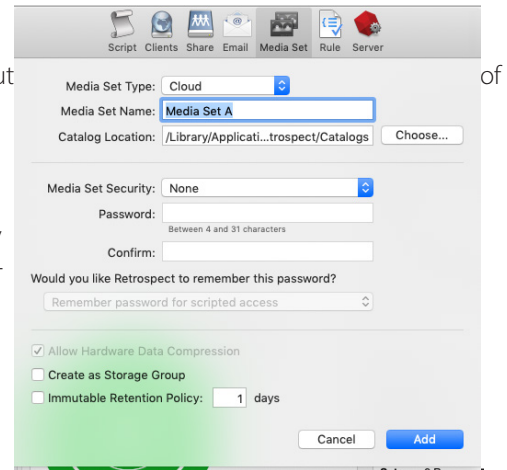
Under The Hood

Every backup within the retention period is an immutable backup with point-in-time restore capabilities. Because each backup is incremental, Retrospect only transfers the files that are new or



have changed since the last backup. However, you can always restore any part of a backup in Retrospect.

Microsoft Azure Blob Storage will mark every new backup file with the specified retention policy, protecting your backups from any accidental or malicious deletion. However, you are responsible for ensuring none of the backup files fall out the retention period, as Microsoft Azure Blob Storage does not provide the ability to change individual file's retention periods.



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.

