



Retrospect Backup

Anti-Ransomware: Immutable Backups with Amazon S3

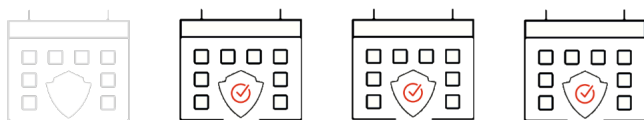
Backup Less. Manage Less. Worry Less.

Amazon S3 provides a low-cost, scalable cloud storage location for secure off-site data protection. With its Object Lock capabilities, S3 enables customers to lock specific files for a retention period, such that no one, not even the root user on the account, can delete the files until the time has passed. See [Amazon S3 documentation](#) for more details.



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.



Immutable Backups

Retrospect Backup 18 integrates seamlessly with this new object lock feature. Users can set a retention period for backups stored on supporting cloud platforms. Within this immutable retention period, backups cannot be deleted by any user, even if ransomware or a malicious actor acquires the root credentials. Retrospect Backup 18's powerful policy-based scheduling allows it to predict when those backups will leave the retention policy and protect any files that will no longer be retained,

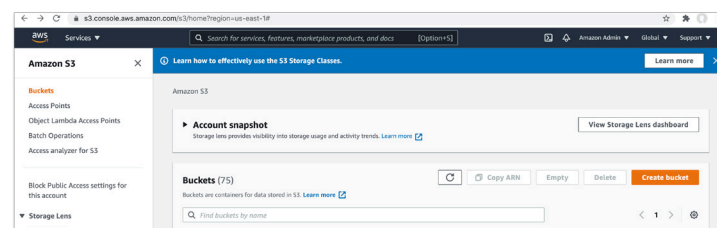
ensuring businesses always have point-in-time backups to restore within the immutable retention policy window.

Step-by-Step Guide

Retrospect Backup makes it easy to add an immutable retention policy with Amazon S3. When creating a backup set, simply check "Immutable Retention Policy" and specify the number of days. Retrospect Backup will mark any backups to Amazon S3 as immutable until that date in the future and delete any backups that are no longer protected by the retention policy, saving costs on storage space.

Let's walk through the steps to create an immutable backup.

- 1) Amazon S3: [Create an account on Amazon S3](#) if you have not already.
- 2) Amazon S3: Click "Create Bucket".



- 3) Amazon S3: Enter a bucket name.

- 4) Amazon S3: Enable "Bucket Versioning". This option is required for Object Lock. It means S3 will store versions of each file, and to delete one, you need to delete every version of it.

Bucket Versioning

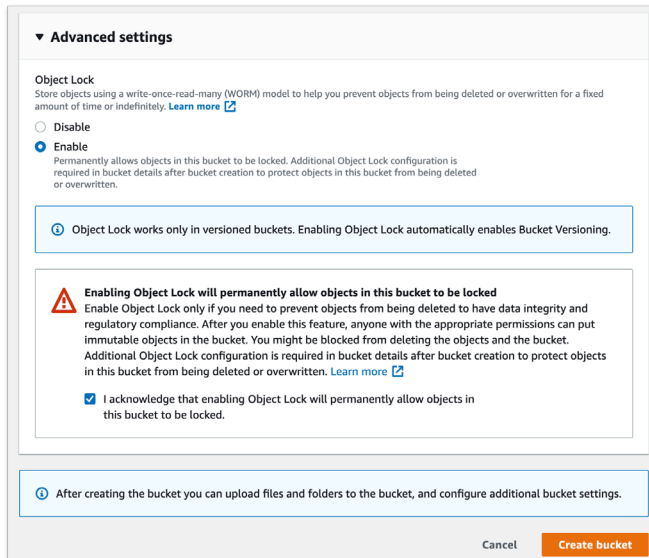
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

- ☐ Disable
☒ Enable

5) Amazon S3: Enable "Object Lock" then click "Create Bucket". Enabling "Object Lock" does not enforce a retention period. It simply allows Retrospect to add one to each file.

6) Retrospect: Add a destination. On Windows, select "Backup Sets" then "Create". On Mac, select "Media Sets" and click "Add". Select type "Cloud". Then click "Immutable Retention Policy" and specify the number of days to protect your backups.



The screenshot shows the 'Advanced settings' dialog in Retrospect. The 'Object Lock' section is expanded, showing options to 'Disable' or 'Enable' it. The 'Enable' option is selected. Below this, there is a warning message: 'Enabling Object Lock will permanently allow objects in this bucket to be locked'. It explains that once enabled, objects cannot be deleted or overwritten, and that additional configuration is required in bucket details. A checkbox 'I acknowledge that enabling Object Lock will permanently allow objects in this bucket to be locked.' is checked. At the bottom, there is a note: 'After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.' The 'Create bucket' button is highlighted in orange.

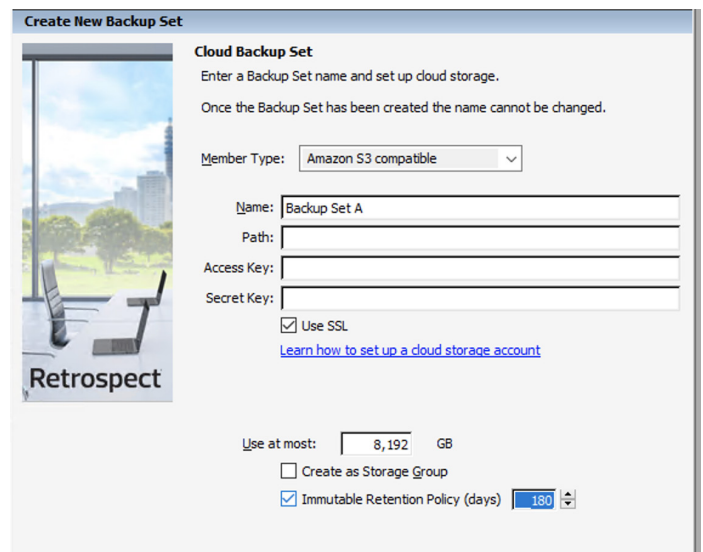
7) Add the destination to a script, and set the script grooming policy to match the retention period. By ensuring the two time periods match, Retrospect Backup will automatically delete backups that fall outside of the retention policy.

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.

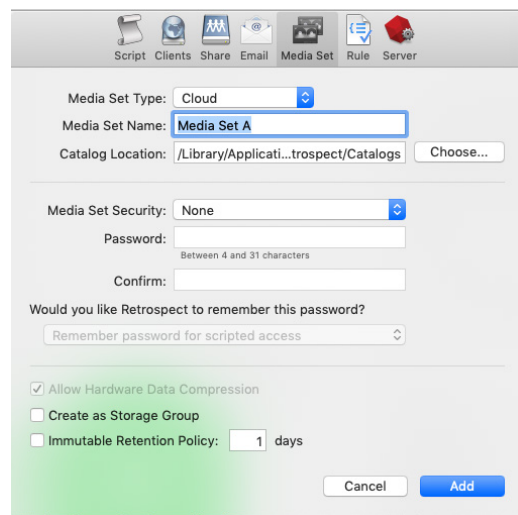
Retrospect Backup uses its advanced scheduling workflow to make sure every immutable backup includes all applicable files. Let's say the chosen retention period is 90 days, and backups occur every week. Retrospect Backup starts backing

up. When it gets to Day 85, it looks ahead to the upcoming back on Day 92, marks which files will no longer be protected on that date based on when they were last backed up, and adds them to the new immutable backup.



The screenshot shows the 'Create New Backup Set' dialog in Retrospect. The 'Cloud Backup Set' section is active, prompting the user to 'Enter a Backup Set name and set up cloud storage.' It notes that the name cannot be changed after creation. The 'Member Type' is set to 'Amazon S3 compatible'. The 'Name' field contains 'Backup Set A'. The 'Path' field is empty. The 'Access Key' and 'Secret Key' fields are empty. The 'Use SSL' checkbox is checked. A link 'Learn how to set up a cloud storage account' is provided. The 'Use at most' field is set to '8,192 GB'. The 'Create as Storage Group' checkbox is unchecked. The 'Immutable Retention Policy (days)' checkbox is checked, and the value is set to '180'.

With the grooming policy set to match the retention policy, Retrospect will automatically delete the backups that are no longer immutable, saving you storage space while ensuring every file is protected by an immutable backup.



The screenshot shows the 'Media Set' dialog in Retrospect. The 'Media Set Type' is set to 'Cloud'. The 'Media Set Name' is 'Media Set A'. The 'Catalog Location' is '/Library/Applicati...trospect/Catalogs'. The 'Media Set Security' is set to 'None'. The 'Password' field is empty, with a note 'Between 4 and 31 characters'. The 'Confirm' field is empty. The 'Would you like Retrospect to remember this password?' dropdown is set to 'Remember password for scripted access'. The 'Allow Hardware Data Compression' checkbox is checked. The 'Create as Storage Group' checkbox is unchecked. The 'Immutable Retention Policy' is set to '1 days'. The 'Add' button is highlighted in blue.

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](https://www.retrospect.com/try)