WHITEPAPER

Retrospect
A StorCentric Company
Data Protection for Businesses

Retrospect Backup

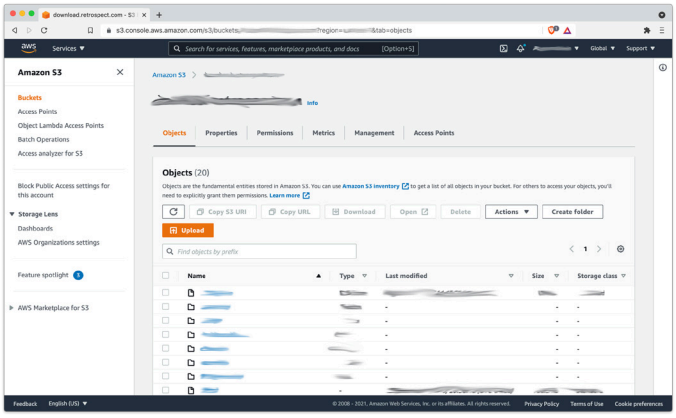
Cloud Data Protection: Protect Data on Amazon AWS S3

Backup Less. Manage Less. Worry Less.

Amazon S3 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.



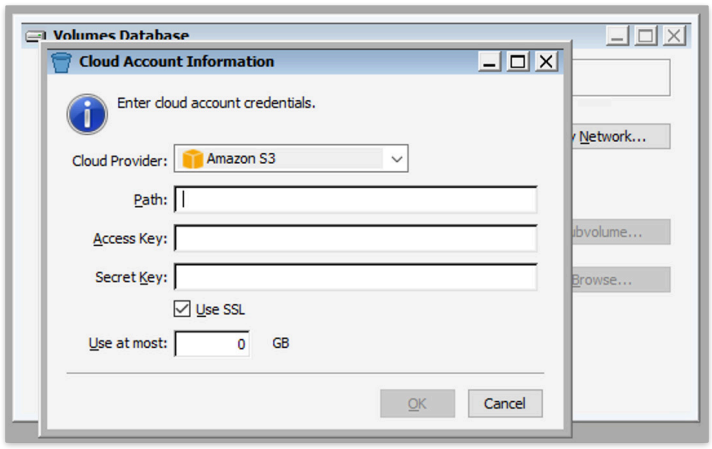
Companies use cloud storage for all sorts of data, from website assets to affordable sharing to ingestable data, and Retrospect Backup includes cloud data protection support for cloud storage as a first-class backup volume. Cloud volumes enable businesses to protect their cloud content on-site with an 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 Amazon S3 volume to Retrospect and then setting up a policy to protect it on-premise.

1) AWS Console: You will need a bucket and path location.

2) AWS Console: When you created your AWS account, you receive a root Access Key and Secret Key. You can also use IAM to create a user with a specific policy.

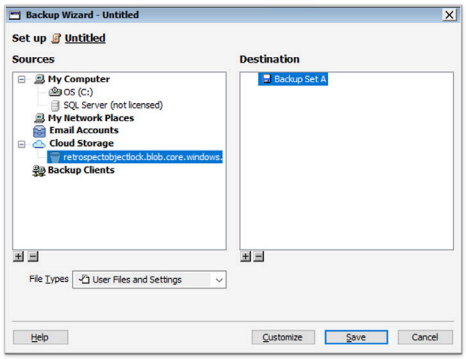


3) In Retrospect, click on "Volumes" (Windows) or "Sources" (Mac).

4) Select "Amazon S3".

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

6) Create a backup script policy for protecting that volume by clicking "Backup Now"



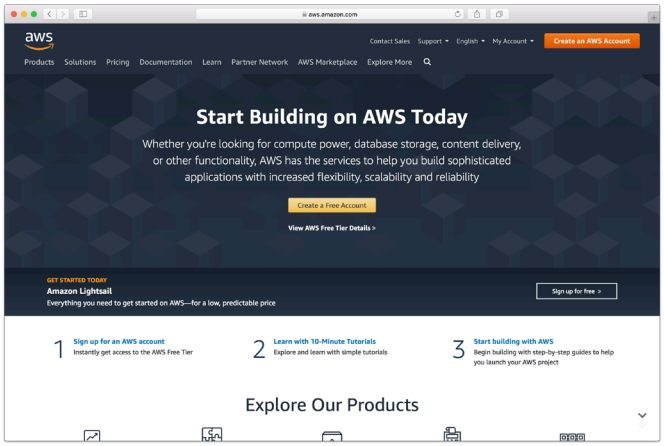
(Windows) or "Backup" (Mac).

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 Amazon S3:

• Virtual-Host Path – your_bucket_name.s3.us-east-1.amazonaws.com
• Access Key – Use the Access Key from above.
• Secret Key – Use the Secret Key from above.

Account Setup Guide
Follow these steps to quickly create a Amazon AWS Account. If you do not already have one, create one for free at Amazon AWS.



1) Visit Amazon AWS to start the account creation process and click "Create an AWS Account".

2) Fill in an email address and password.

3) Complete the contact information form.

4) Complete the payment information form.

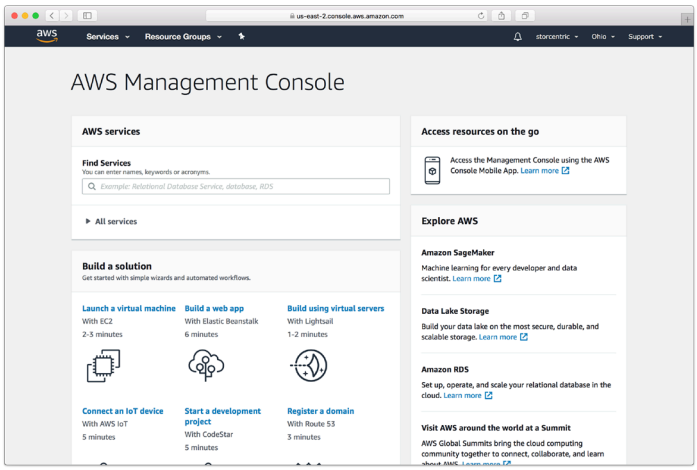
5) Complete the identity verification.

6) Select an appropriate Support Plan.

7) The new account is created.

Storage Setup Guide
Now we will create a bucket that Retrospect can use to store backups.

1) Log into AWS Console.



2) Search for S3 and select.

3) Click "Create Bucket".

4) Type in an appropriate name for the bucket. Note that these are globally-unique names.

5) Continue through the rest of the wizard with default options.

6) Your bucket is now ready. In Retrospect, the "Path" is s3.amazonaws.com/your_bucket_name. Next, you need a set of security credentials for Retrospect to use to access it.

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