Mission Guide: Amazon S3

Your Mission: Use F-Response to collect Amazon S3 Bucket data

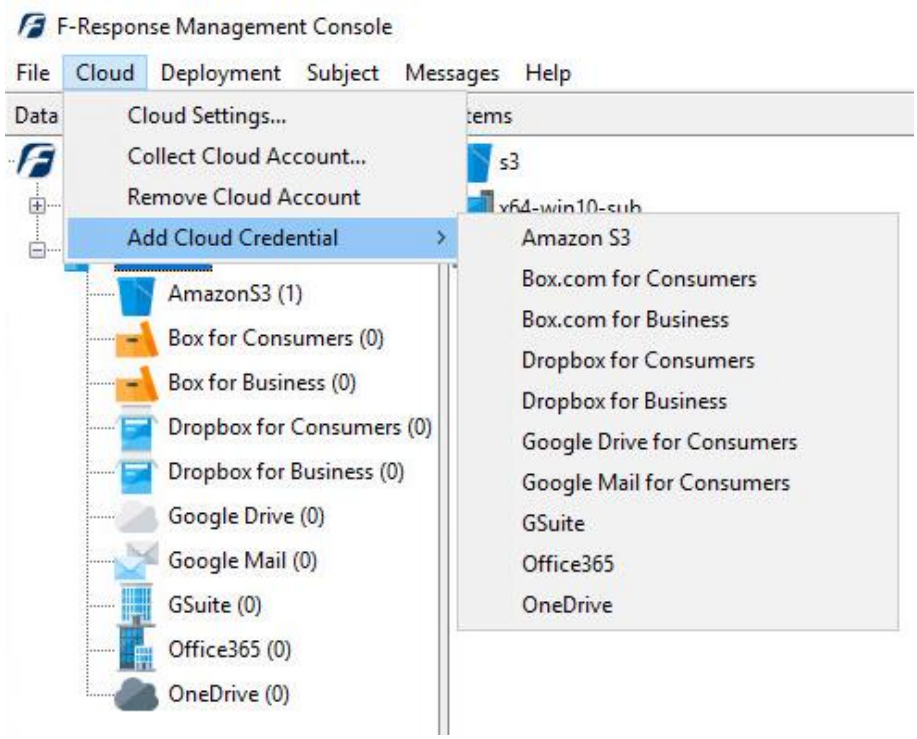
Using F-Response to collect Amazon S3 Storage Bucket contents

Important Note	*Disclaimer: F-Response provide access to 3rd party data sources via Application Programming Interfaces (APIs) and internal structures presented by the provider. 3rd party provided data sources by their very nature are volatile. The afore mentioned F-Response products provide "best effort" for accessing and interacting with those 3rd party data sources however service disruptions, API changes, provider errors, network errors, as well as other communications issues may result in errors or incomplete data access. F-Response always recommends secondary validation of any 3rd party data collection.*

F-Response Cloud Collector Options Supported		
Revision History	Not available.	Amazon S3 does not support revision history. Enabling Revision History in F-Response will have no effect on the collection.
Hash Verification	Available and supported.	Amazon S3 provides md5 hashes of items which will be automatically checked in F-Response if Verify Hashes is enabled. **NOTE Hashes for Multi-part uploads will not be verified.**
Rerun Collection	Not Available.	Rerunning a collection to target specific items that may have errored is not an option.

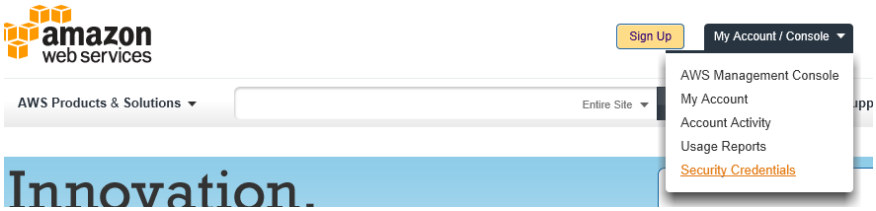
Step 1: Open the Amazon S3 Credential Configuration Window

Open the F-Response Management Console and navigate to Cloud->Add Cloud Credential->Amazon S3, or double click on the appropriate icon in the Data Sources pane.



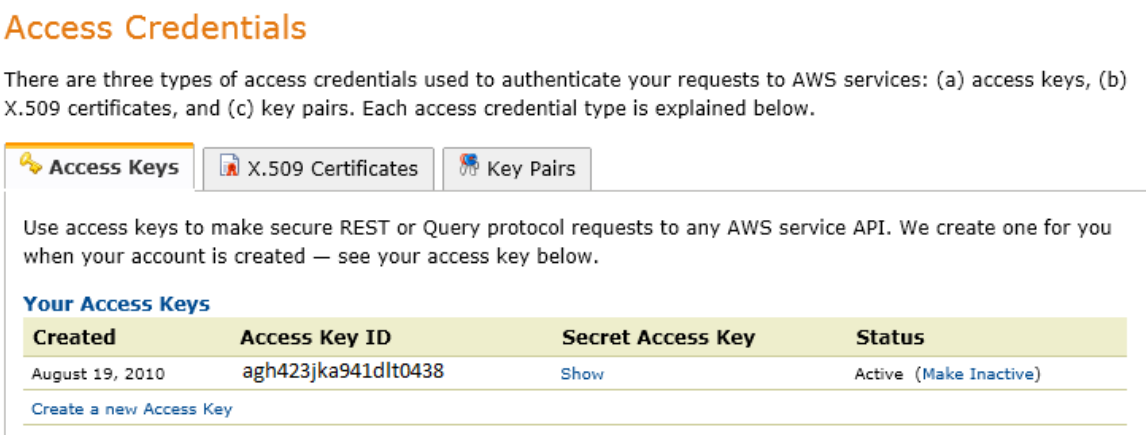
Step 2: Obtain Amazon S3 Credentials

Amazon S3 Storage Credentials are found on the Amazon AWS Console (see **aws.amazon.com**). The specific credentials required are available under the "**Security Credentials**" link under **My Account**, see below:



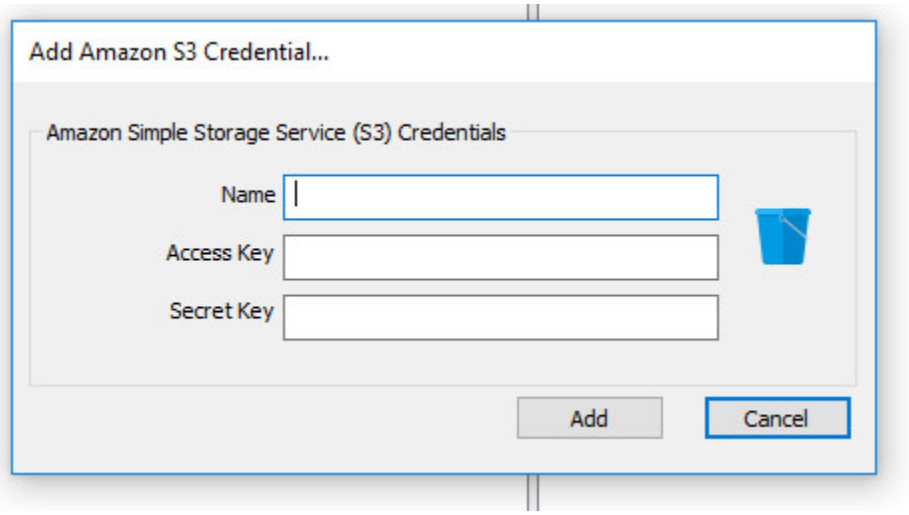
Amazon Web Services Main Page

Locate the **Access Credentials** section and record (copy/paste) **the Access Key ID**, then click "**Show**" to open a secondary window containing the **Secret Access Key**.



Amazon AWS Access Key and Secret Access Key

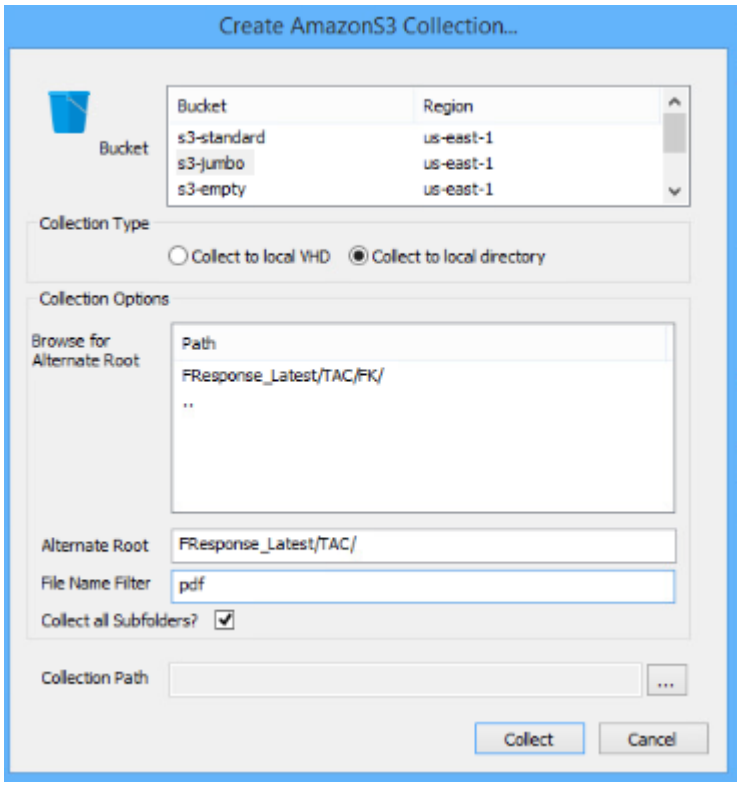
The preceding credentials (Access Key and Secret Key) must be entered in the corresponding fields in the **Configure Amazon S3 Credentials** dialog. The Name field is **not** optional and is used to provide a secondary human readable identifier for the credential set (Ex "Client X Account").



Configure S3 Credentials

Step 3: Start a collection

Select the Amazon S3 Bucket icon under Data Sources and then double click on the newly added Amazon S3 account under Items. This will prepare a new dialog for collecting a bucket's contents.



Starting a new collection

Select the specific bucket you would like to collect, as well as whether you would like to collect the bucket to a virtual hard disk or a local directory. In either case a collection of the bucket contents will be made, along with a log file and error file to indicate any errors that might have occurred during the collection.

To collect the full bucket, simply highlight the bucket, choose the location to store the data in the **Collection Path,** and click the **Collect** button. (Note: collection path must be local as you cannot collect to a network share).

To refine the scope of the collection some, or all, of the **Collection Options** can be invoked to reduce the size of the data set to be collected. The options are as follows:

Browse for Alternate Root: This option will allow you to select a different starting location to pull data from. Click on an item and wait a moment for the subdirectories to parse. Continue to click and drill as far down the path as you need to narrow the scope of the collection accordingly (the 'double dot' option will take you back). The **Alternate Root** field below will populate with the correct information.

File Name Filter: Will check the string entered here against files as presented by the provider. There is no need to enter wildcards (*.*) and it does not use regular expressions. For example, to collect only Excel files in the account, just type **.xls** in the box.

Collect all Subfolders? If checked, it will collect the content of all subfolders, if unchecked, it will only collect that folder's file contents.

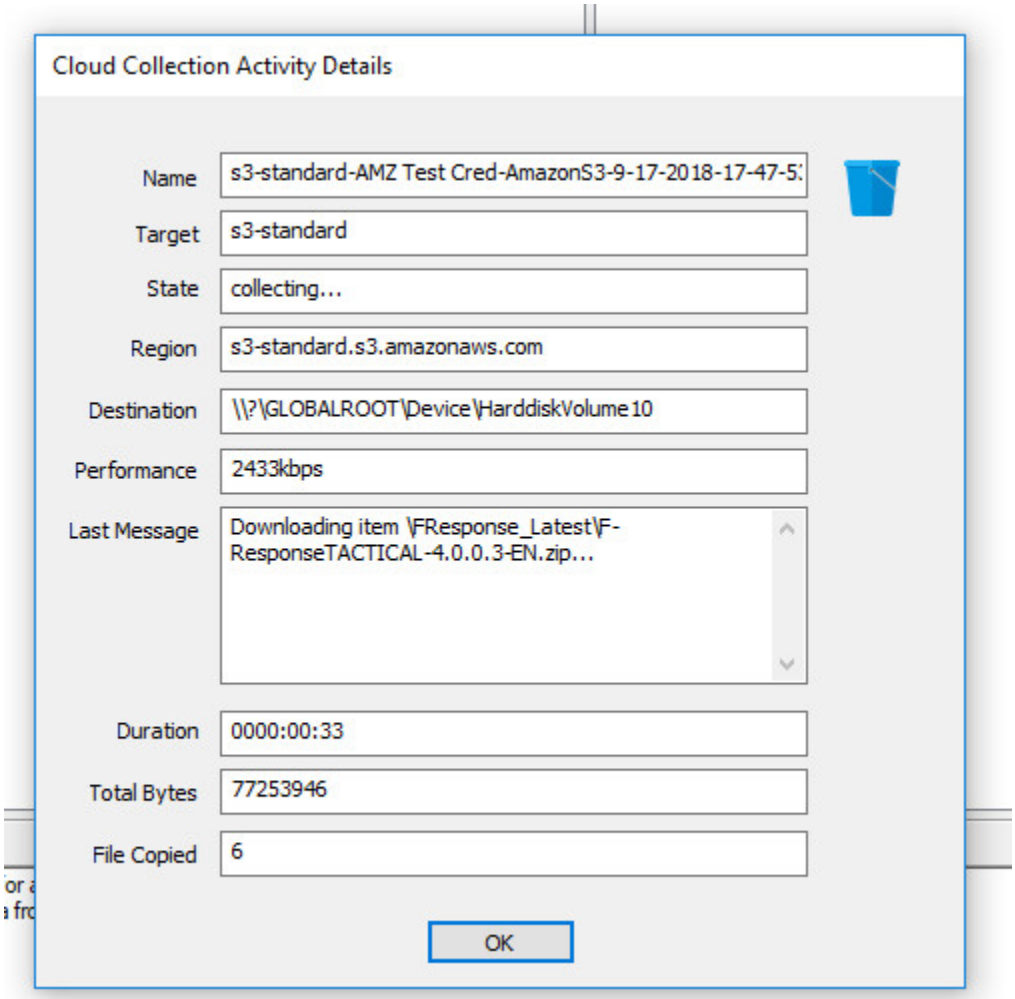
Step 4: Check the Activity Pane

The Activity Pane shows the active collection. Double clicking on the collection will provide additional details.

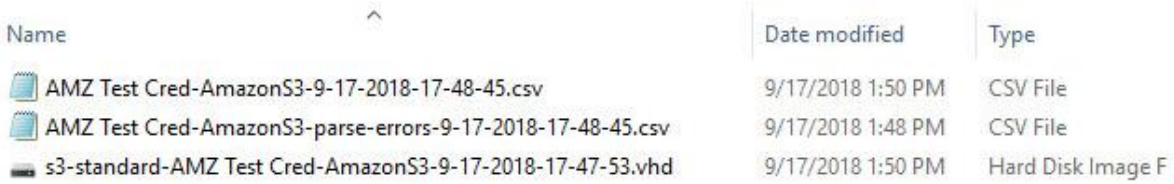
Active Collections

Collection Details…

Step 5: Review the Completed Collection



Navigate to the destination folder at the completion of the collection to review the individual files collected, or the summary VHD, along with any log or error reports.



Reviewing the completed image.

Additional Details

The following file datetime values are used by F-Response during the collection *(Any missing dates are set to 1601-01-01T00:00:01Z)*:

WINDOWS TIME	PROVIDER VALUE
MODIFIED	LastModified
ACCESSED	
CREATED	

Troubleshooting

I have valid S3 Credentials however I get no buckets returned, why?

Most likely your computer's clock is too far skewed from the current time. Your examiner machine's clock must be accurate to within 15 minutes of actual time. The time zone is un-important.