Mission Guide: Amazon EC2

Your Mission: Use F-Response to collect Amazon EC2 Volume Snapshots

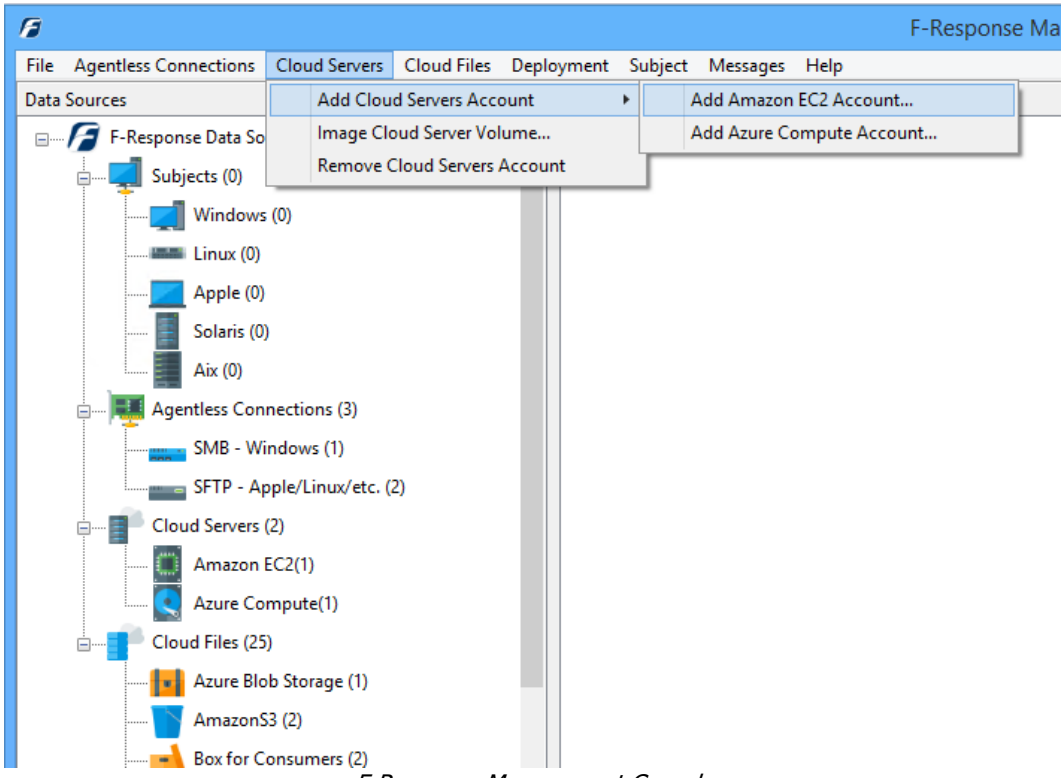
Using F-Response to collect Amazon EC2 Volume Snapshots

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.

Step 1: Open the Amazon EC2 Credential Configuration Window

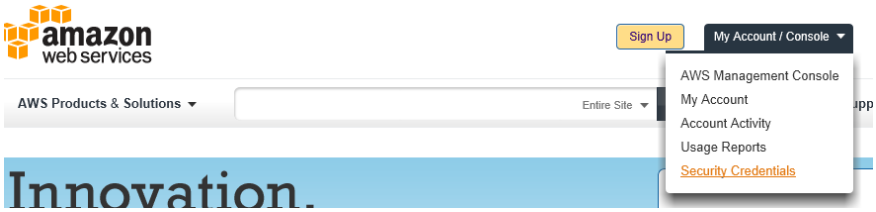
Open the F-Response Management Console and navigate to Cloud Servers->Add Cloud Servers Account->Add Amazon EC2 Account…, or double click on the appropriate icon in the Data Sources pane.



F-Response Management Console

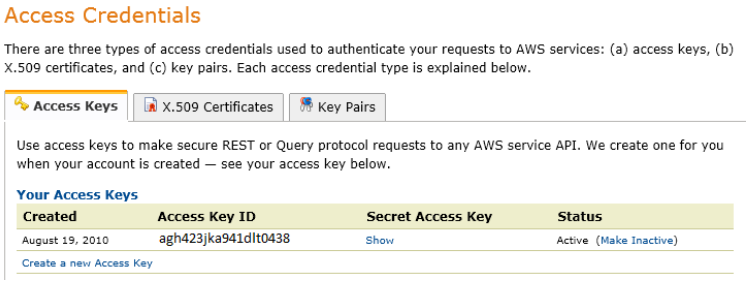
Step 2: Obtain Amazon EC2 Credentials

Amazon EC2 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:



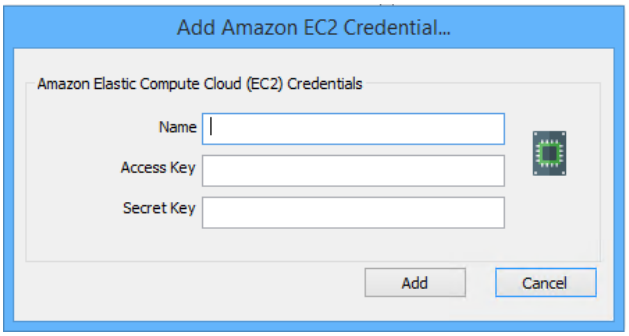
Amazon Web Services Main Page

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

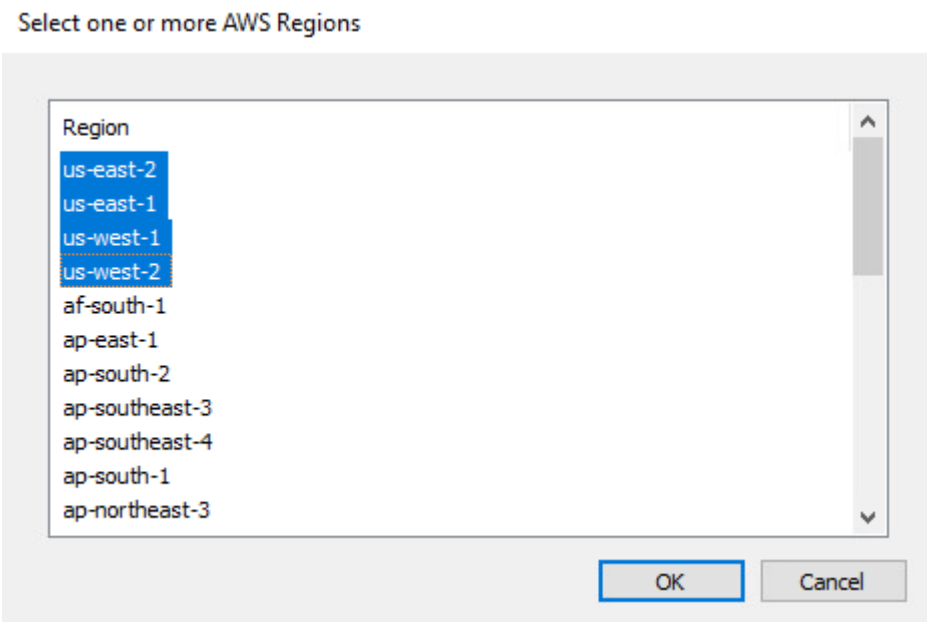
The preceding credentials (Access Key and Secret Key) must be entered in the corresponding fields in the **Configure Amazon EC2 Credentials** dialog. The Name field is **not** optional and is used to provide a secondary human readable identifier for the credential set (Ex "Client X Account").



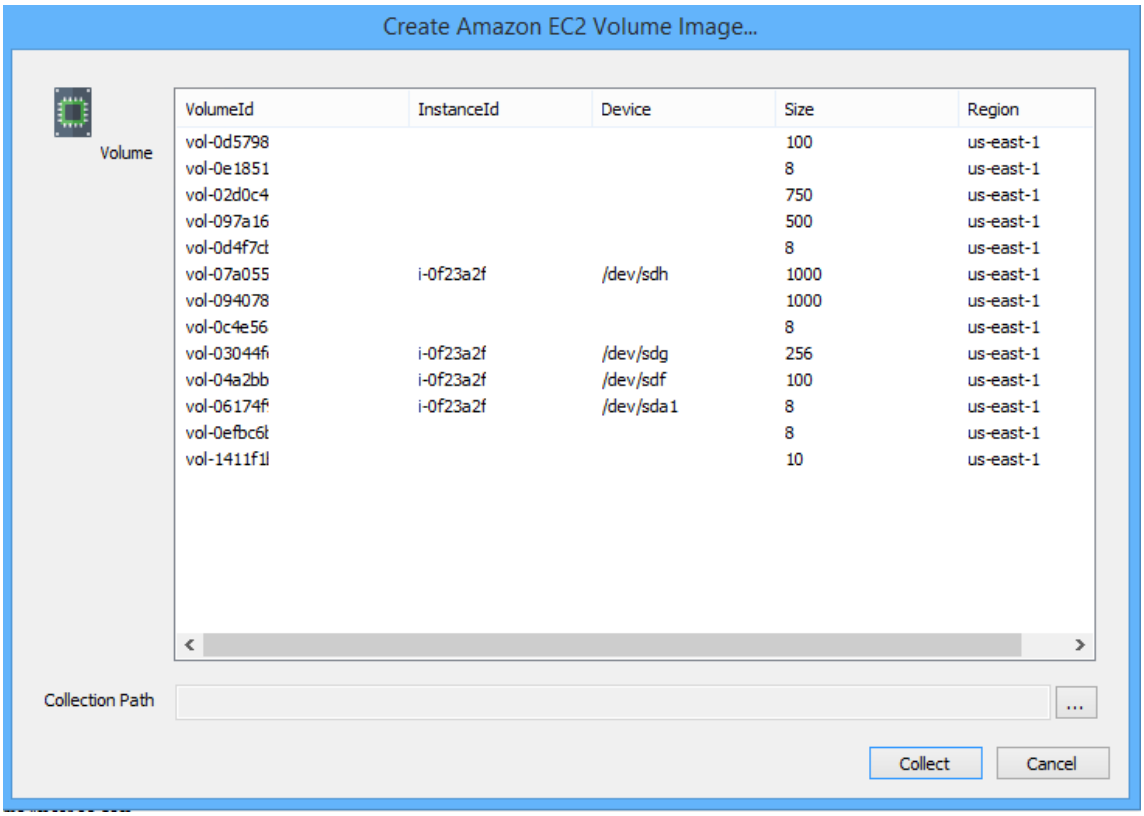
Configure EC2 Credentials

Step 3: Start a collection

Select the Amazon EC2 Snapshot icon under **Data Sources** and then double click on the newly added Amazon EC2 account under **Items**. You will be prompted to select the region the cloud server resides in, choose one or more regions to search.



This will prepare a new dialog for creating and collecting a volume snapshot.



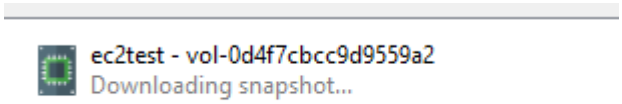
Starting a new collection

Select the Volume you would like to collect, using the instance id and volume id to help you locate the appropriate device.

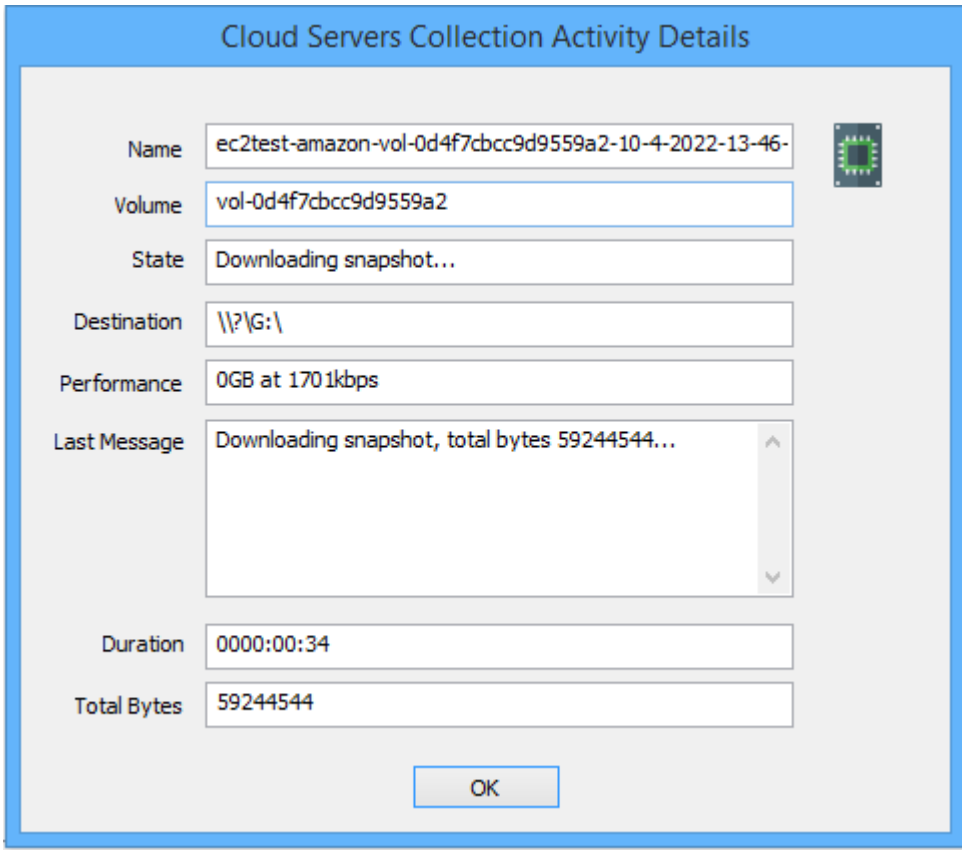
To create a snapshot and collect it, simply highlight the volume, choose the location to store the data in the **Collection Path,** and click the **Collect** button. (Note: collection path must be local as you cannot collect to a network share).

Step 4: Check the Activity Pane

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

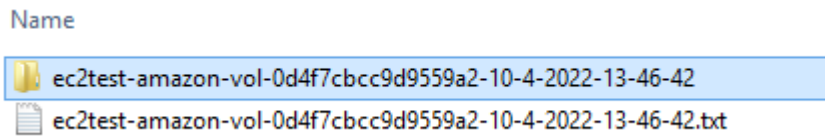


Active Collections



Collection Details…

Step 5: Review the Completed Collection



Navigate to the destination folder at the completion of the collection to review the dd image file and summary report.

Reviewing the completed image.

Troubleshooting

I have valid EC2 Credentials however I get no volumes 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.*