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



Using F-Response to collect Amazon EC2 Volume Snapshots



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 **Important** 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.



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**.

Created	Access Key ID	Secret Access Key	Status
August 19, 2010	agh423jka941dlt0438	Show	Active (Make Inactive)

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").

Ado	d Amazon EC2 Credential	
Amazon Elastic Compute C	Cloud (EC2) Credentials	
Name		
Access Key		<u></u>
Secret Key		
	Add	Cancel

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.

Select one or more AWS Regions

Region	^
us-east-2	
us-east-1	
us-west-1	
us-west-2	
af-south-1	
ap-east-1	
ap-south-2	
ap-southeast-3	
ap-southeast-4	
ap-south-1	
ap-northeast-3	~
	OK Cancel

		Create Amazon	EC2 Volume Imag	e	
<u> </u>	VolumeId	InstanceId	Device	Size	Region
	vol-0d5798			100	us-east-1
volume	vol-0e1851			8	us-east-1
	vol-02d0c4			750	us-east-1
	vol-097a16			500	us-east-1
	vol-0d4f7cł			8	us-east-1
	vol-07a055	i-0f23a2f	/dev/sdh	1000	us-east-1
	vol-094078			1000	us-east-1
	vol-0c4e56			8	us-east-1
	vol-03044fi	i-0f23a2f	/dev/sdg	256	us-east-1
	vol-04a2bb	i-0f23a2f	/dev/sdf	100	us-east-1
	vol-06174f	i-0f23a2f	/dev/sda1	8	us-east-1
	vol-0efbc6ł			8	us-east-1
	vol-1411f1			10	us-east-1
	<				>
Collection Path					
					Collect Cancel

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.

·····	ec2test - vol-0d4f7cbcc9d9559a2
<u>.</u>	Downloading snapshot

Active Collections

	Cloud Servers Collection Activity Details	
Name	ec2test-amazon-vol-0d4f7cbcc9d9559a2-10-4-2022-13-46-	O
Volume	vol-0d4f7cbcc9d9559a2	• •
State	Downloading snapshot	
Destination	\\?\G:\	
Performance	OGB at 1701kbps	
Last Message	Downloading snapshot, total bytes 59244544	
	· · · · · · · · · · · · · · · · · · ·	
Duration	2222.22.24	
Duration	0000:00:34	
Total Bytes	59244544	
	ОК	

Collection Details ...

Step 5: Review the Completed Collection

Name

ec2test-amazon-vol-0d4f7cbcc9d9559a2-10-4-2022-13-46-42

ec2test-amazon-vol-0d4f7cbcc9d9559a2-10-4-2022-13-46-42.txt

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

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.