

Your Mission: Use F-Response to collect Azure Compute Volume Snapshot(s)



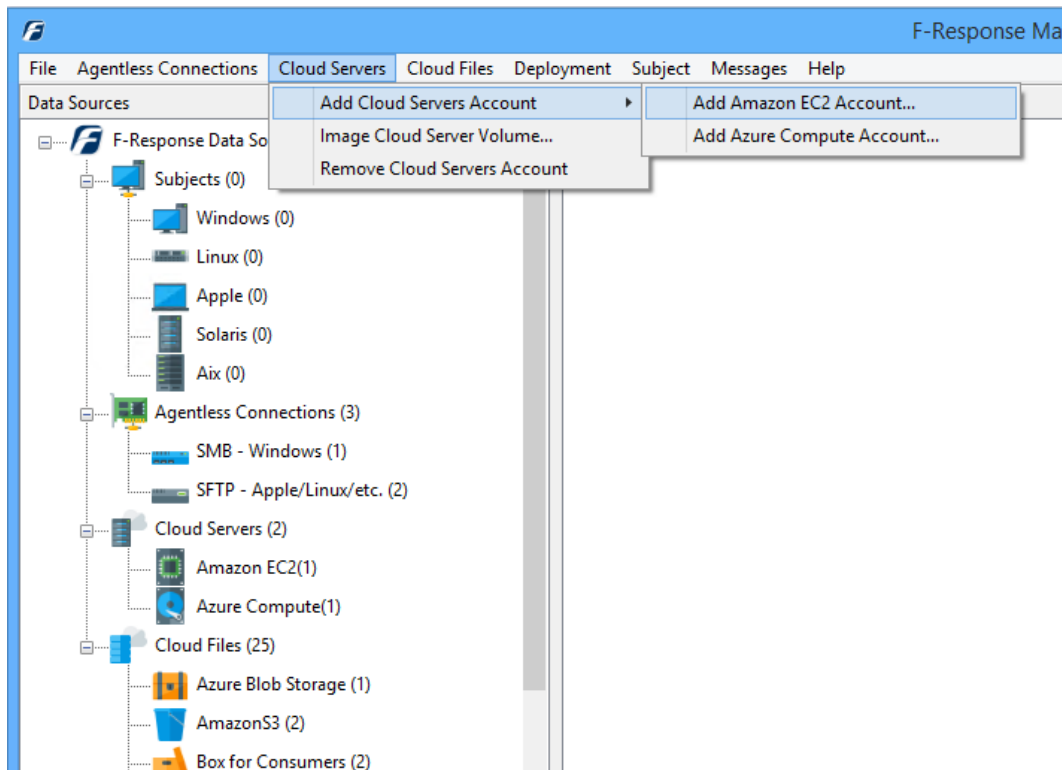
Using F-Response to collect Azure Compute Volume Snapshot(s)

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 Azure Compute Credential Configuration Window

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



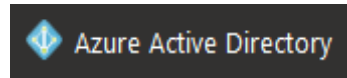
F-Response Management Console

Step 2: Create a Client Credentials Flow Account on Azure AD

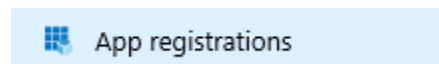
Before you can access Azure Compute and collect volume snapshots, you will need to create a “Client Credentials Flow” account on Azure AD. This is a one-time process and does not need to be done again for a year.

Start by logging into <https://portal.azure.com> with administrator username and password.

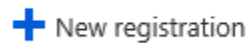
You’ll then need to locate the Azure Active Directory on the left side menu.



From there you will need to select App registrations.



Then press New registration.



The details under new registration aren't important, however feel free to use the following:

Register an application

* Name

The user-facing display name for this application (this can be changed later).

F-Response Application ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (F-Response)
- Accounts in any organizational directory
- Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

Register the new application by pressing the Register.

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

Now that your F-Response App has been created you will need to record multiple values:

Copy the Application (client) ID as well as the Directory (tenant) ID. You will need both of these to move forward. After you have those values safely saved, click on "Client Credentials: Add a certificate or secret" to create a client secret.

[Delete](#) [Endpoints](#) [Preview features](#)

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

^ Essentials

Display name	: F-Response Application	Client credentials	: 0 certificate, 1 secret
Application (client) ID	: 14ab2d5d-b33c-4541-90d2-	Redirect URIs	: Add a Redirect URI
Object ID	: 13132496-a30b-459b-925a-	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 36fef66a-75ee-4486-b644-5	Managed application in l...	: F-Response Application
Supported account types	: My organization only		

Use the “New Client Secret” to create a secret valid for up to 24 months. In our example we use the name “F-Response Application” but that is not required.

Application | Certificates & secrets

Got feedback?

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

Description: F-Response Application
Expires: 12 months

Add Cancel

You will need to save only the “Value” which is the Client Secret.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
F-Response Application	10/4/2023	N4f8Q~riyBJoMukP1	... f551650a-accd-4cbf-91fe-

Lastly, we need to find your subscription and give this application rights to it.

Return to the Azure home page and click on Subscription(s).

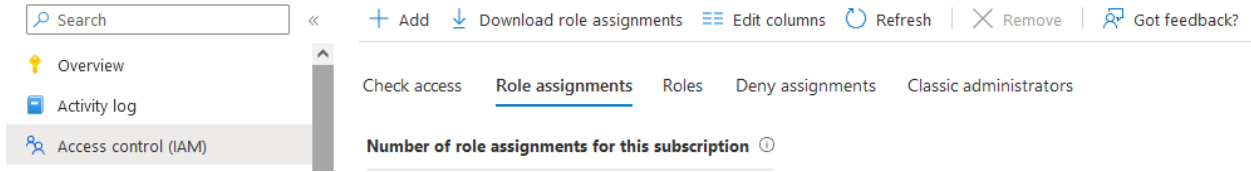
Search resources, services, and docs (G+)

Azure services

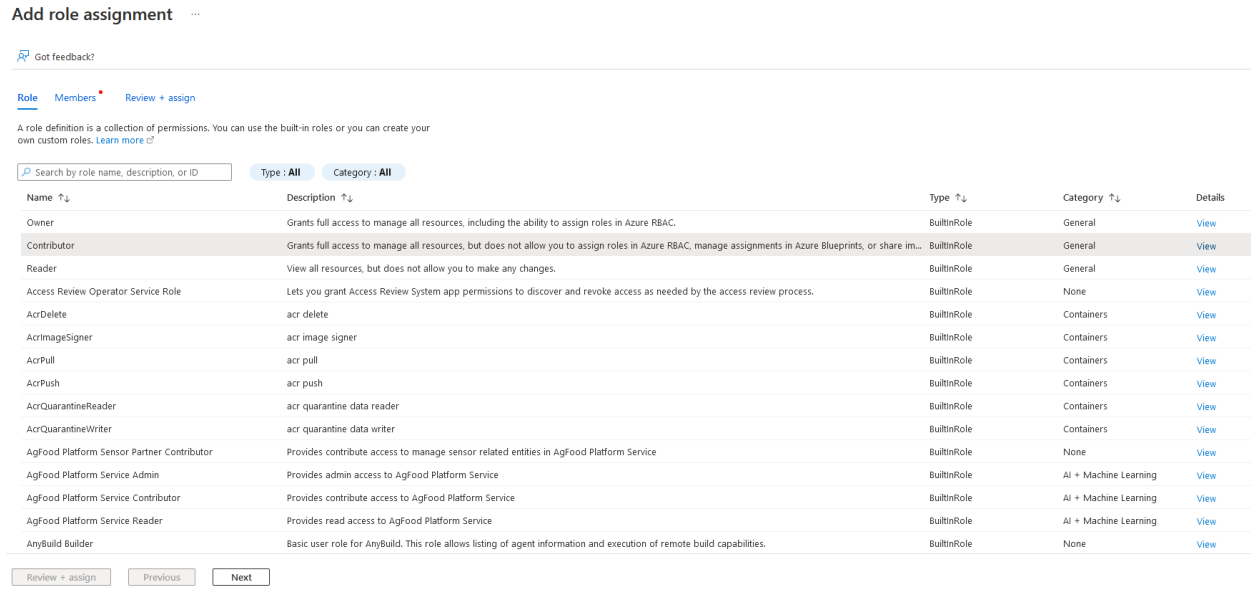
- Create a resource
- Azure Active Directory
- Snapshots
- Disk Accesses
- Subscriptions
- Subscriptions (starred)
 - View
 - Free training from Microsoft
- App Services
- More services

Resources

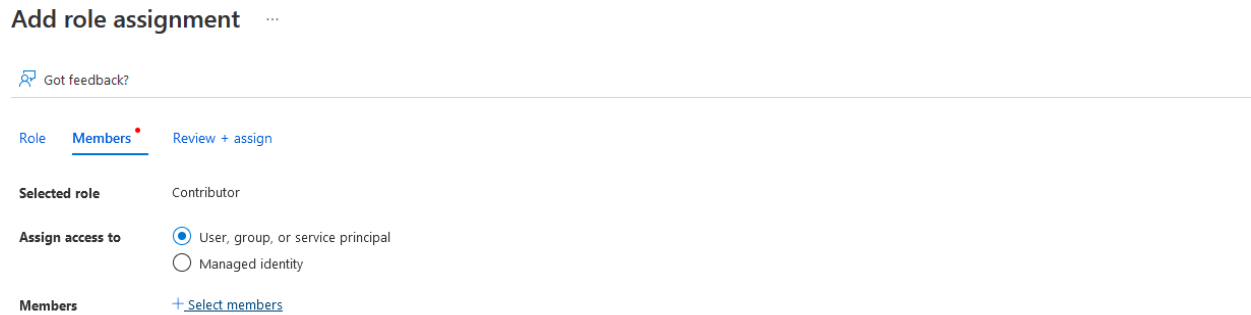
Click on Access Control (IAM) and then Role Assignments:



Then give this newly created application a contributor role. Do this by clicking on “+ Add” and selecting the contributor role, then pressing next.



Use the “+ Select Members” to locate your newly created application.



Use the application name to locate it.

Select members



Select ⓘ

F-Response Application



F-Response Application

Press “Select” and verify the application in the display before pressing “next.”

Add role assignment

Got feedback?

Role **Members** Review + assign

Selected role Contributor

Assign access to
 User, group, or service principal
 Managed identity

Members + Select members

Name	Object ID	Type	
F-Response Application	d281b488-a236-4ca5-a7a1-	App	

Description

Optional

Review + assign

Previous

Next

Press review and assign when complete.

Lastly, return to the Subscriptions page under home and select your subscription, copy down the Subscription Id presented.

Overview

Activity log

^ Essentials

Subscription ID

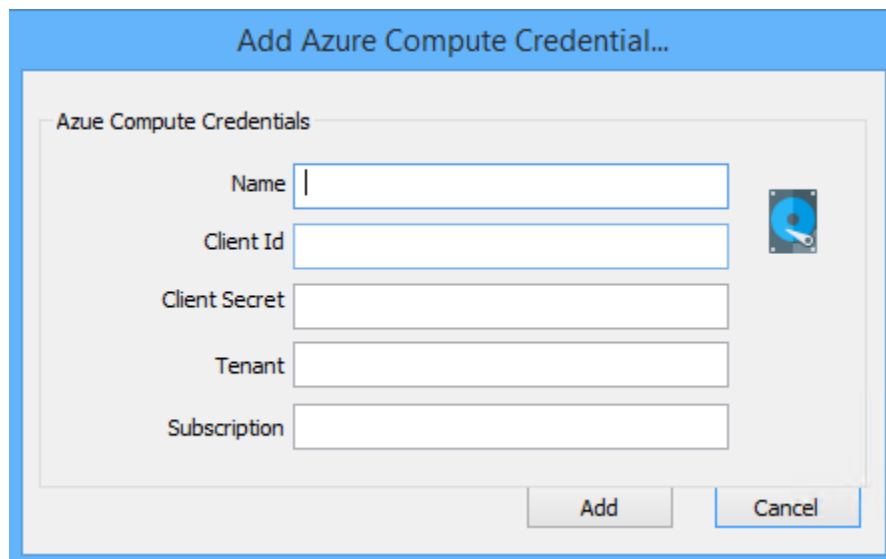
: c0dbe993-0e5c-4b51-bc14-

In summary you should have the following:

- Client Id
- Client Secret
- Tenant Id
- Subscription Id

Step 3: Adding the Azure Compute Account

To configure Azure Compute access, you will need to enter all the values collected prior.

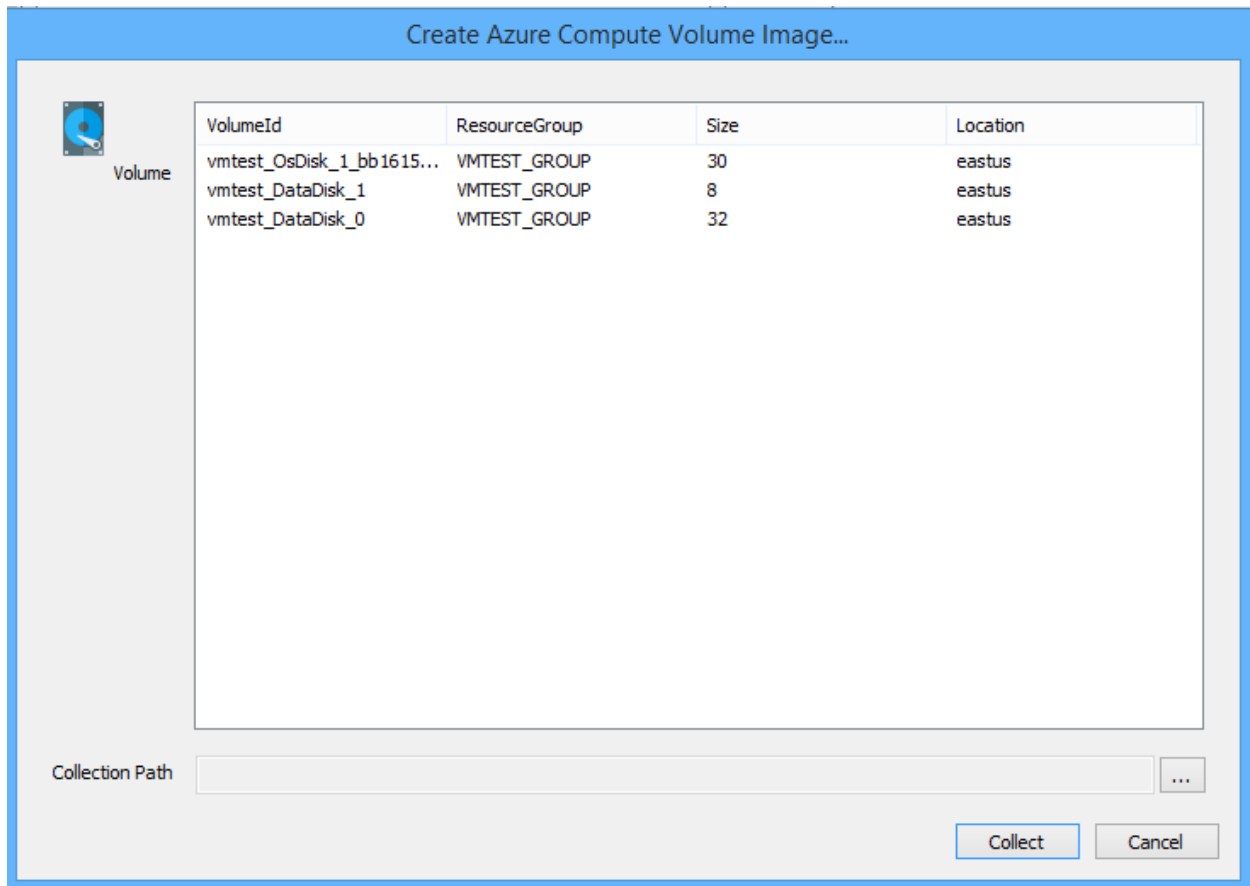


The screenshot shows a dialog box titled "Add Azure Compute Credential...". Inside the dialog, there is a section labeled "Azue Compute Credentials" (with a typo). Below this section are five text input fields: "Name", "Client Id", "Client Secret", "Tenant", and "Subscription". To the right of the "Client Id" field is a small icon of a blue key. At the bottom right of the dialog are two buttons: "Add" and "Cancel".

Add an Azure Compute Account

Step 4: Start a collection

Select the Azure Compute icon under Data Sources and then double click on the newly added Azure Compute account under Items. This will prepare a new dialog for creating and collecting a volume snapshot.

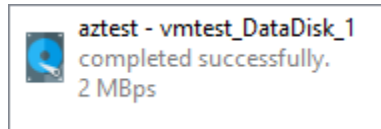


Starting a new collection...

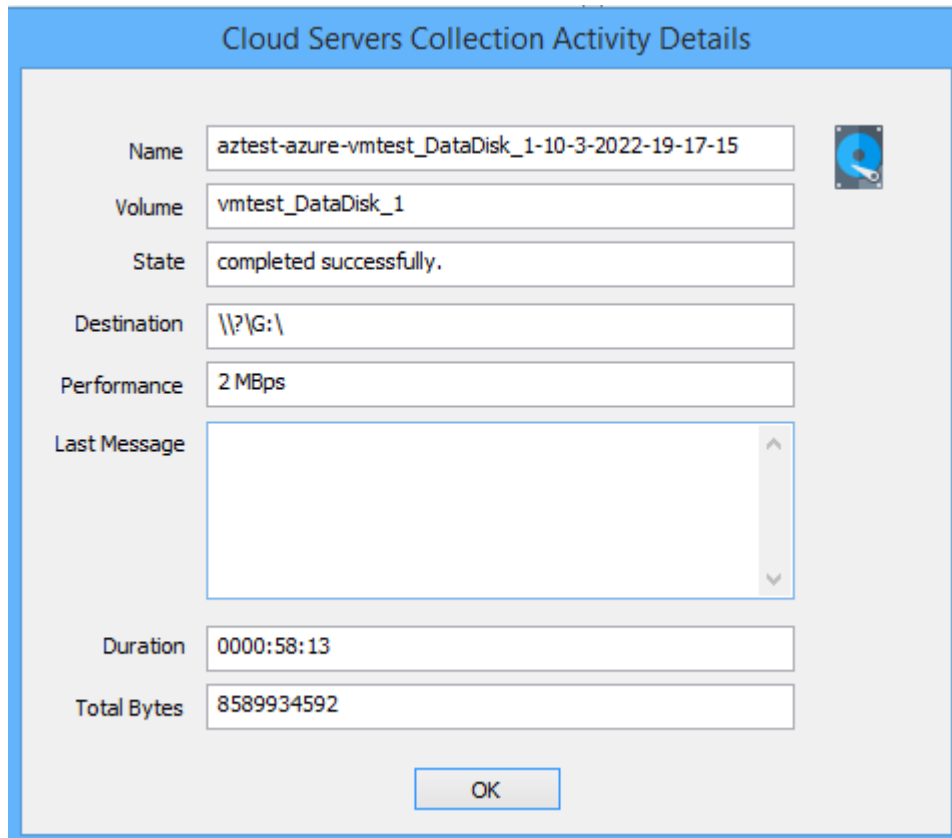
Highlight the specific VolumeId you would like to collect from the list, then, enter the location where the collected data is to be stored in the **Collection Path** and click the **Collect** button to begin the collection. (Note: collection path must be local as you cannot collect to a network share).

Step 5: Check the Activity Pane

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





Activity



Collection Details...

Step 6: Review the collection

Navigate to the destination folder at the completion of the collection to review the snapshot vhd collected and the collection report.

Name
 aztest2-azure-vmtest_DataDisk_1-10-4-2022-17-53-25.txt
 aztest2-azure-vmtest_DataDisk_1-10-4-2022-17-53-25

Collected items

Troubleshooting
