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

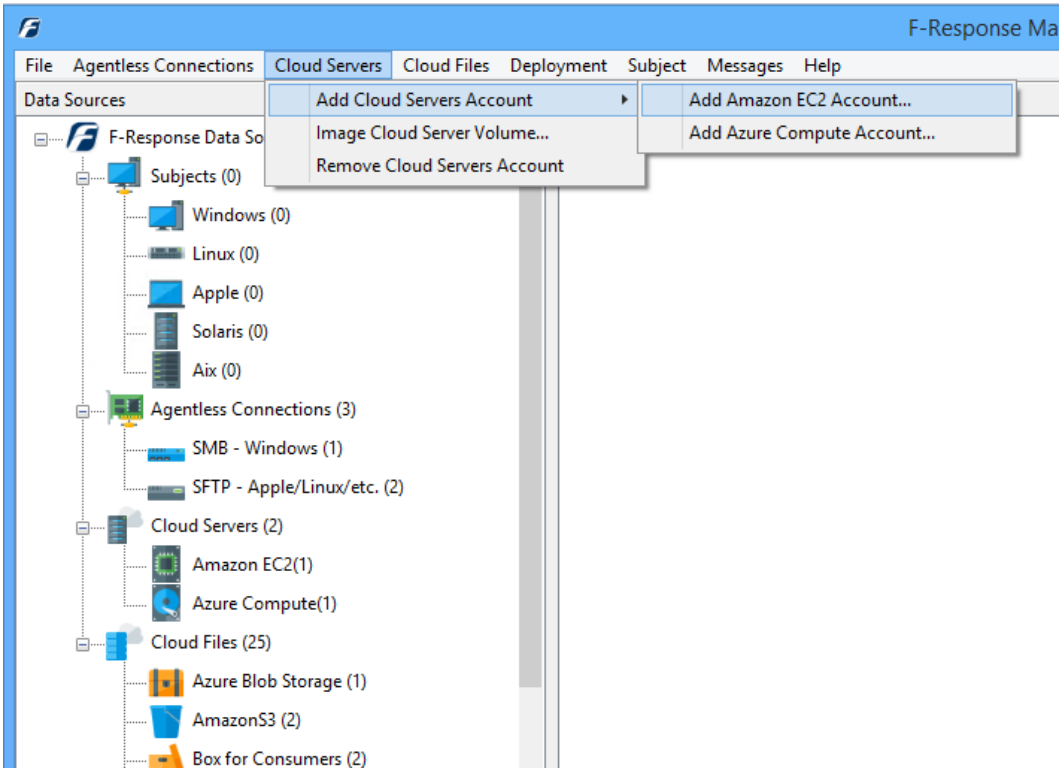
Using F-Response to collect Azure Compute Volume Snapshot(s)

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.



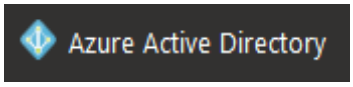
F-Response Management Console

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

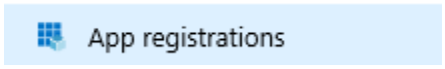
Before you can access Azure Compute and collect volume snapshots, you will need to create a “Client Credentials Flow” account on Azure AD. This is a one-time process and does not need to be done again for a year.

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

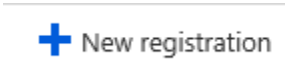
You’ll then need to locate the Azure Active Directory on the left side menu.



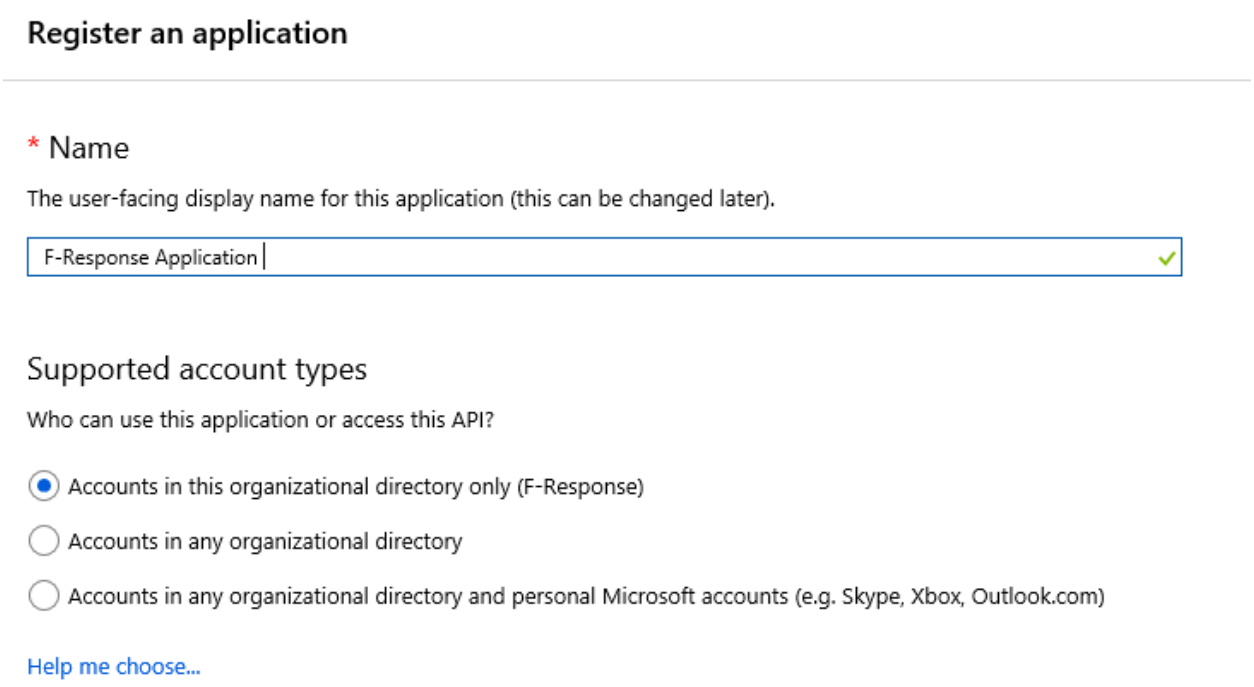
From there you will need to select App registrations.



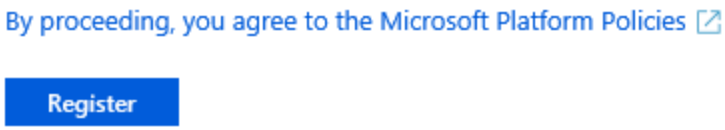
Then press New registration.



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

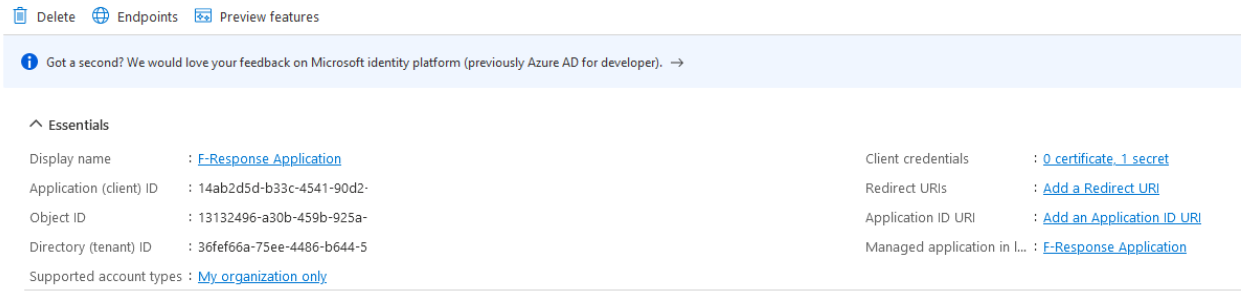


Register the new application by pressing the Register.

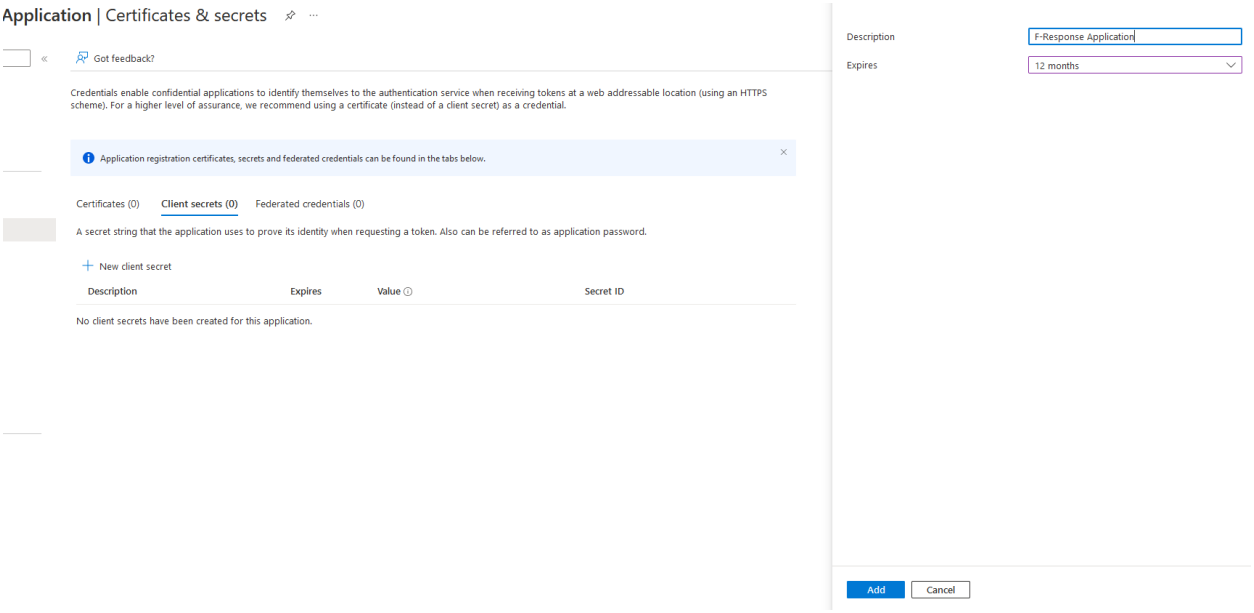


Now that your F-Response App has been created you will need to record multiple values:

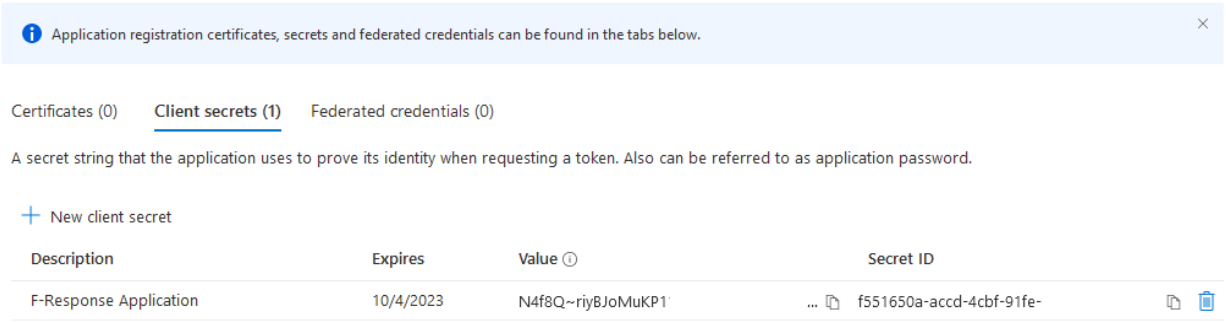
Copy the Application (client) ID as well as the Directory (tenant) ID. You will need both of these to move forward. After you have those values safely saved, click on "Client Credentials: Add a certificate or secret" to create a client secret.



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.

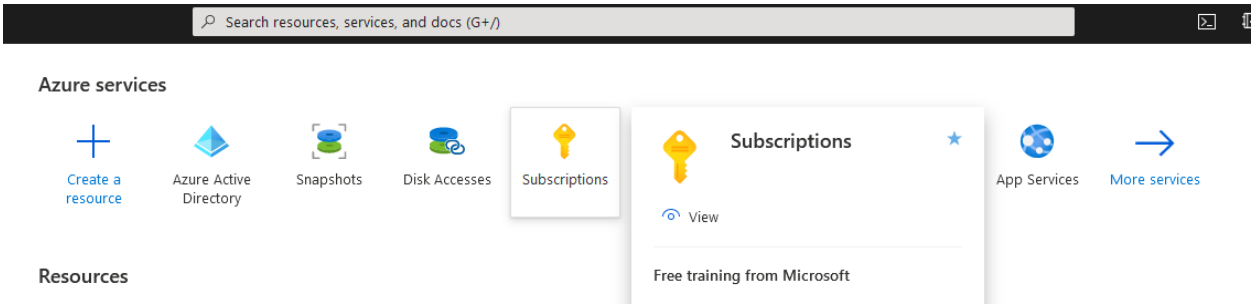


You will need to save only the “Value” which is the Client Secret.

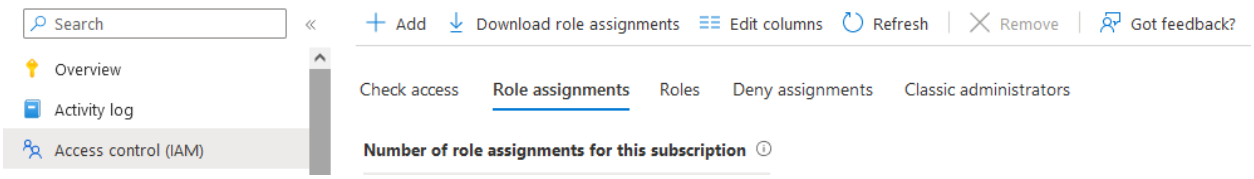


Lastly, we need to find your subscription and give this application rights to it.

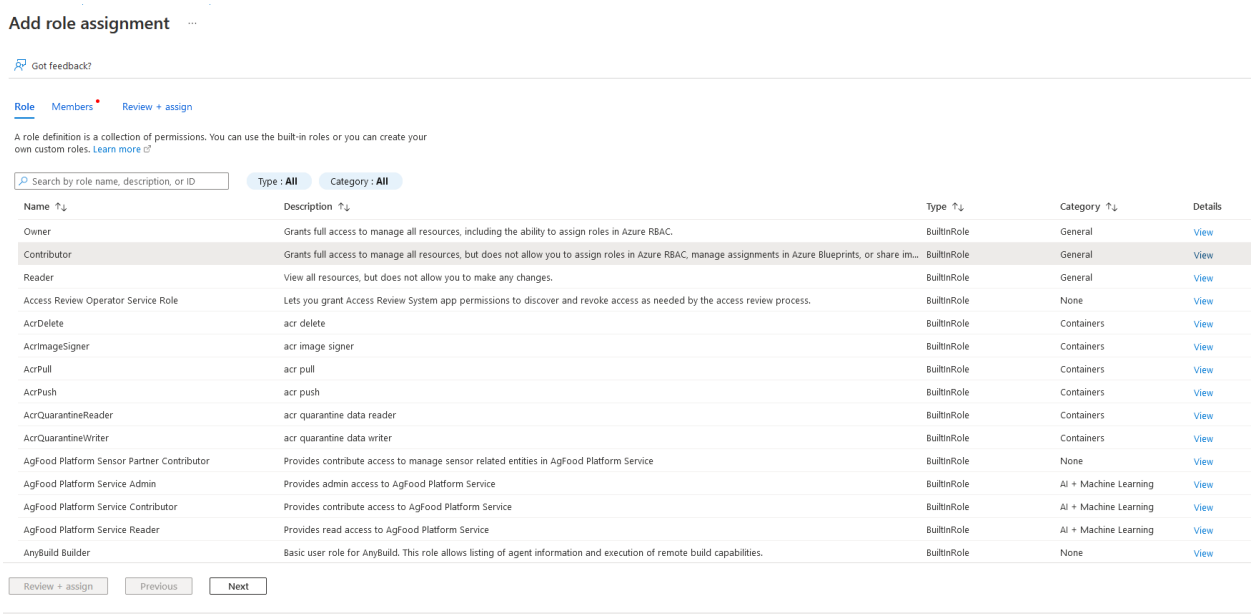
Return to the Azure home page and click on Subscription(s).



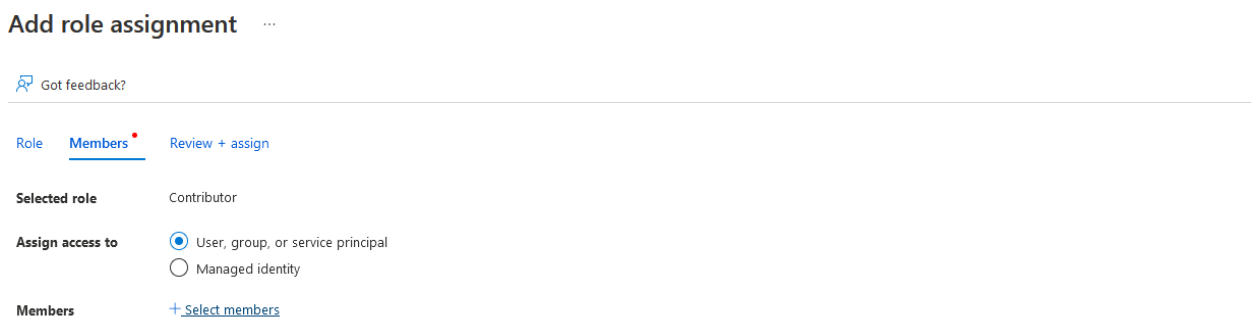
Click on Access Control (IAM) and then Role Assignments:



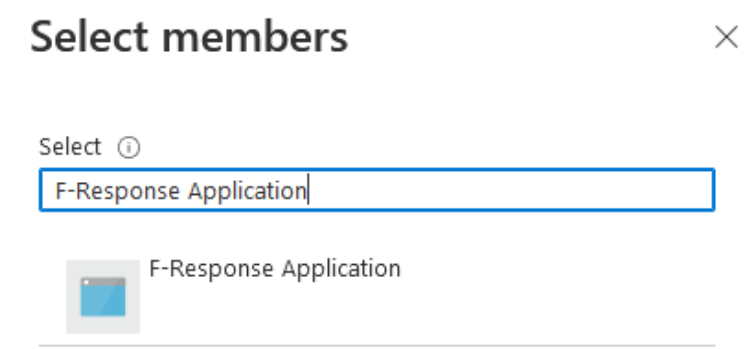
Then give this newly created application a contributor role. Do this by clicking on "+ Add" and selecting the contributor role, then pressing next.



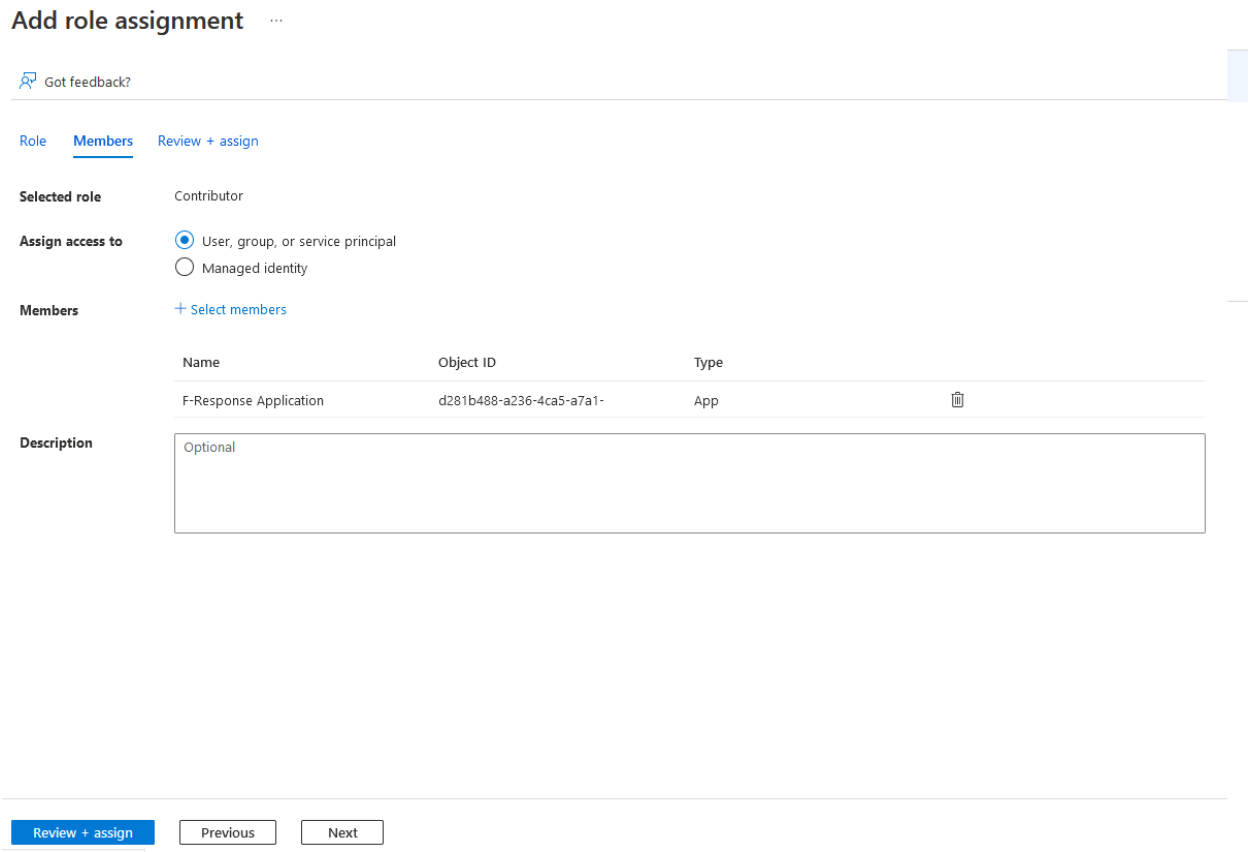
Use the "+ Select Members" to locate your newly created application.



Use the application name to locate it.

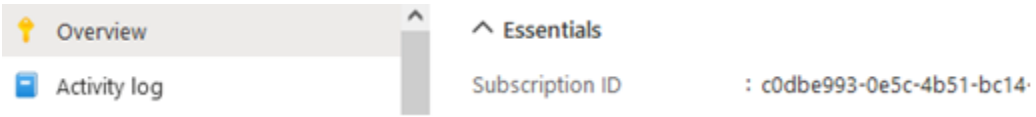


Press “Select” and verify the application in the display before pressing “next.”



Press review and assign when complete.

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

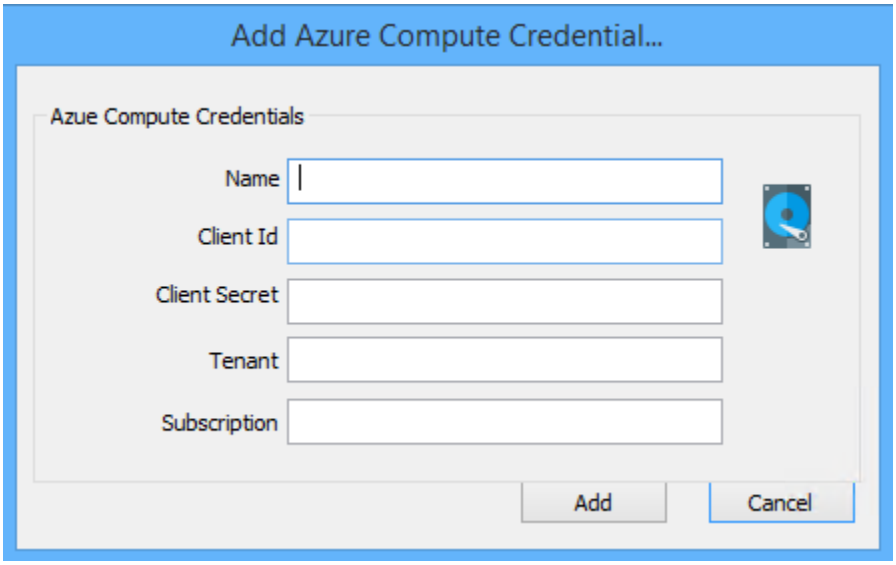


In summary you should have the following:

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

Step 3: Adding the Azure Compute Account

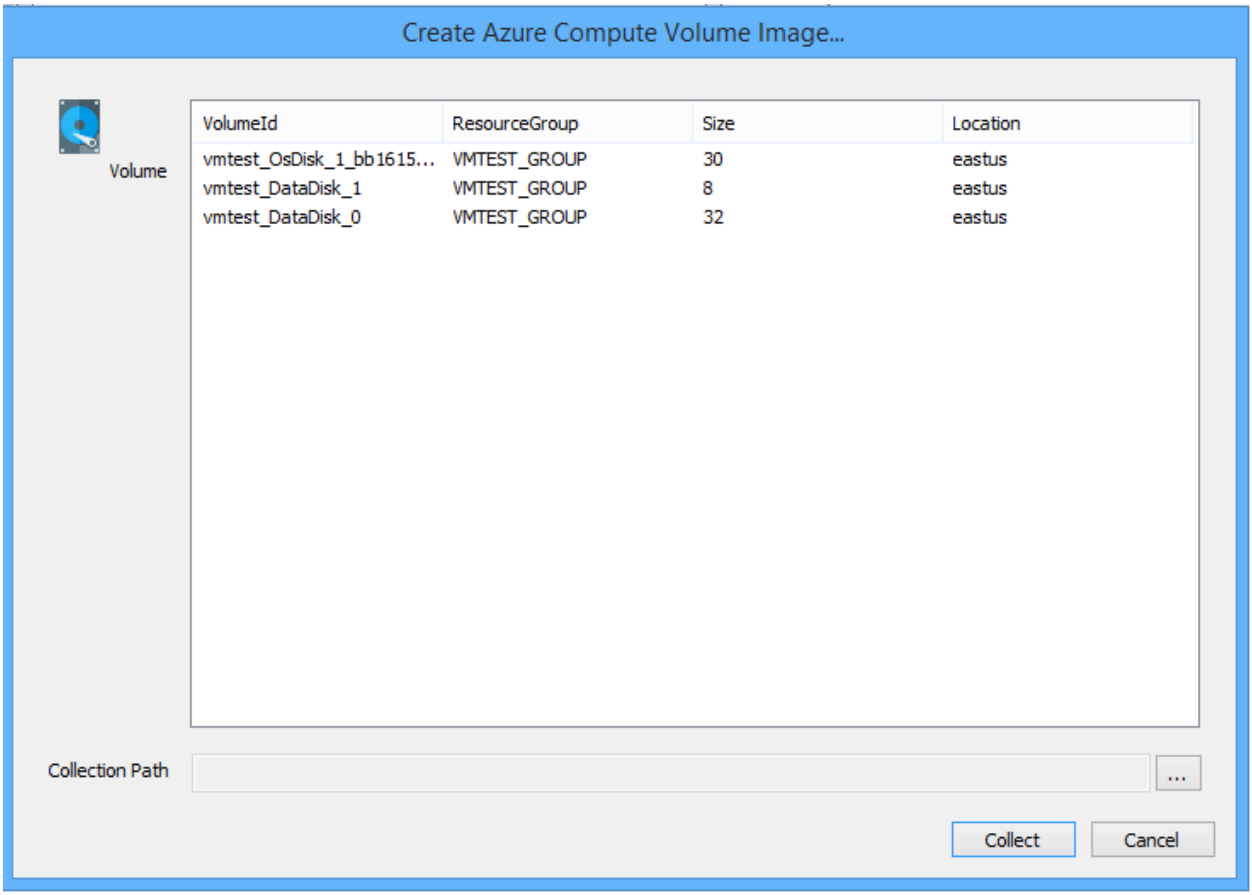
To configure Azure Compute access, you will need to enter all the values collected prior.



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.

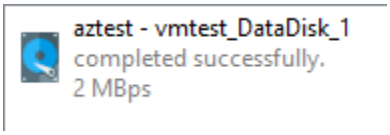


Starting a new collection...

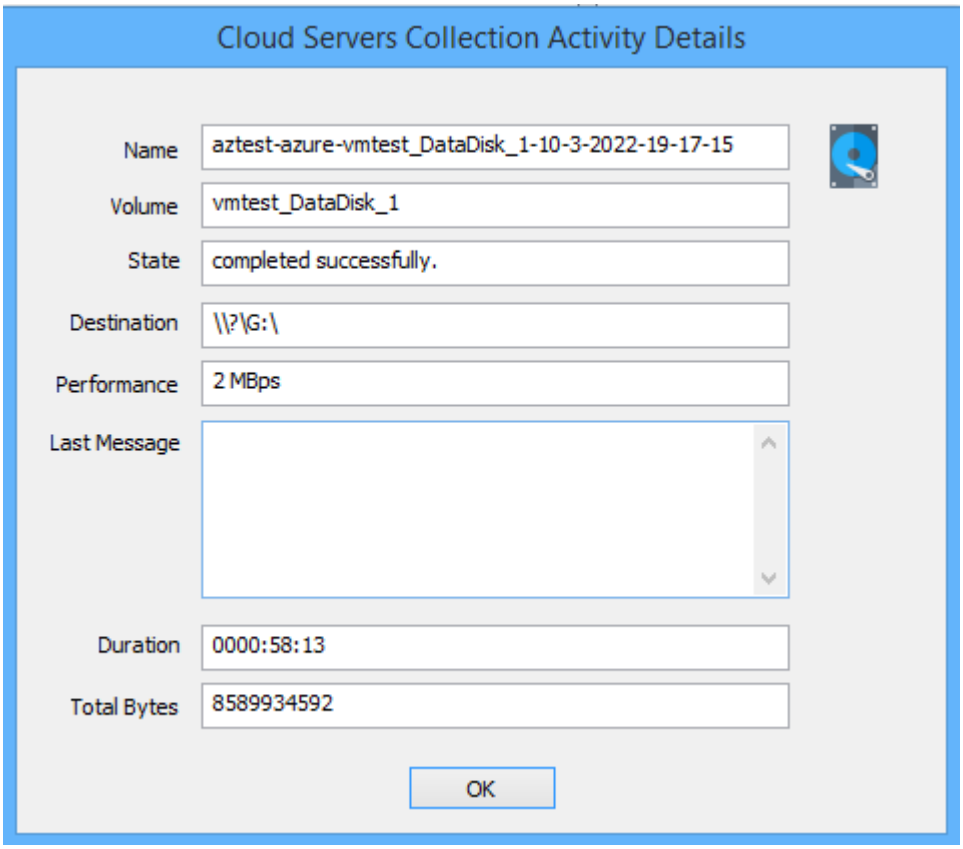
Highlight the specific VolumeId you would like to collect from the list, then, enter the location where the collected data is to be stored in the **Collection Path** and click the **Collect** button to begin the collection. (Note: collection path must be local as you cannot collect to a network share).

Step 5: Check the Activity Pane

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



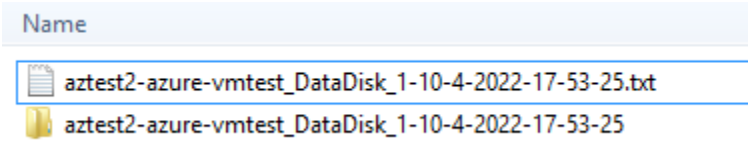
Activity



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.



Collected items

Troubleshooting