

Your Mission: Use F-Response to collect Azure Container data



Using F-Response to collect Microsoft Azure Blob Storage Container contents

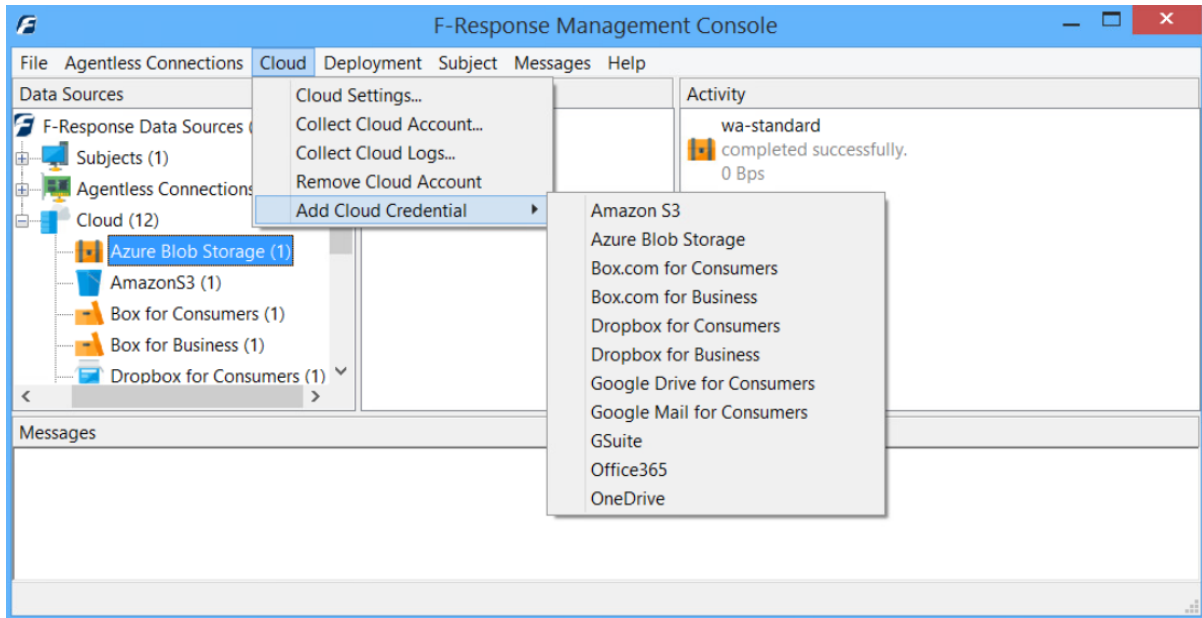
Important Note

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.	Azure does not support revision history. Enabling Revision History in F-Response will have no effect on the collection.
Hash Verification	Available and supported.	Azure 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 Azure Credential Configuration Window

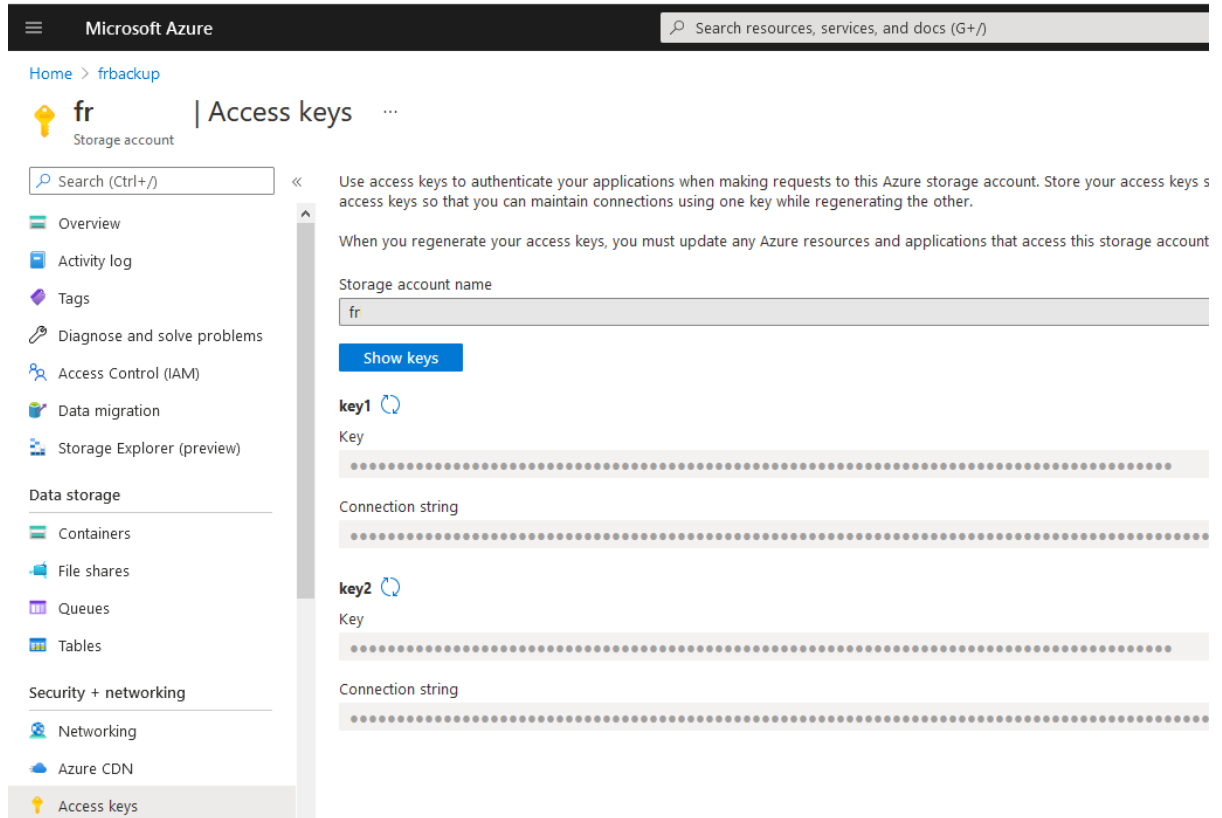
Open the F-Response Management Console and navigate to Cloud->Add Cloud Credential->Azure Blob Storage, or double click on the appropriate icon in the Data Sources pane.



F-Response Management Console

Step 2: Obtain Azure Credentials

Windows Azure Storage Credentials are found on the Windows Azure Storage Portal (see <https://portal.azure.com>). The specific credentials required are available under the “**Settings - Access Keys**” link under **Storage Account** you wish to access, see below:



The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar and the text "Microsoft Azure". Below this, the breadcrumb "Home > frbackup" is visible. The main content area is titled "Access keys" and includes a search bar and a list of navigation options. The "Access keys" option is selected. The main content area contains instructions on using access keys and a "Show keys" button. Below this, two keys are displayed: "key1" and "key2". Each key has a "Key" field and a "Connection string" field. The "key1" key is highlighted.

Azure Access Keys Page

Locate the keys, record (copy/paste) **Key1**, this will be your **Account Secret**.

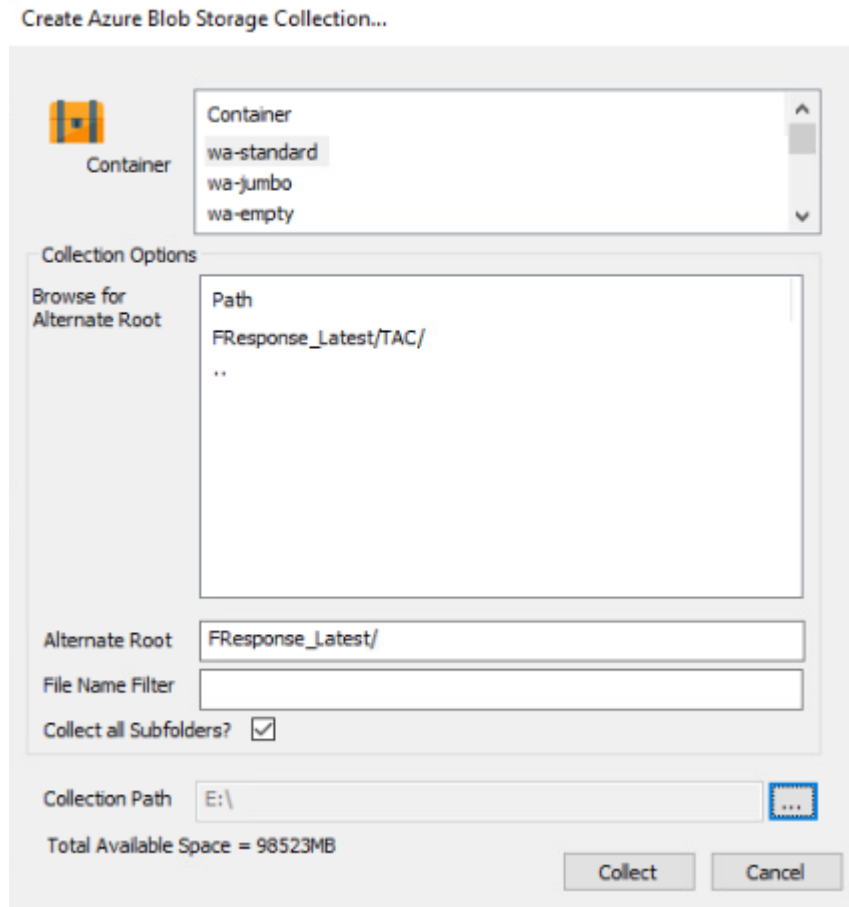
The Storage Account name must be entered into the **Account ID**, and Key1 into the **Account Secret** field in the **Add Azure Blob Storage Credential...** dialog. The **Name** field is not optional and must be used to provide a secondary human readable identifier for the credential set (Ex "Client X Account").

The image shows a dialog box titled "Add Azure Blob Storage Credential...". Inside the dialog, there is a section titled "Azure Blob Storage Credential" which contains three text input fields: "Name", "Account Id", and "Account Secret". To the right of the "Account Id" field is a small orange and black icon. At the bottom right of the dialog are two buttons: "Add" and "Cancel".

Configure Azure Credentials

Step 3: Start a collection

Select the Azure icon under **Data Sources** and then double click on the newly added Azure account under **Items**. This will prepare a new dialog for collecting a container's contents.



Starting a new collection

Select the specific container you would like to collect. A collection of the container 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 container, simply highlight the container, 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:

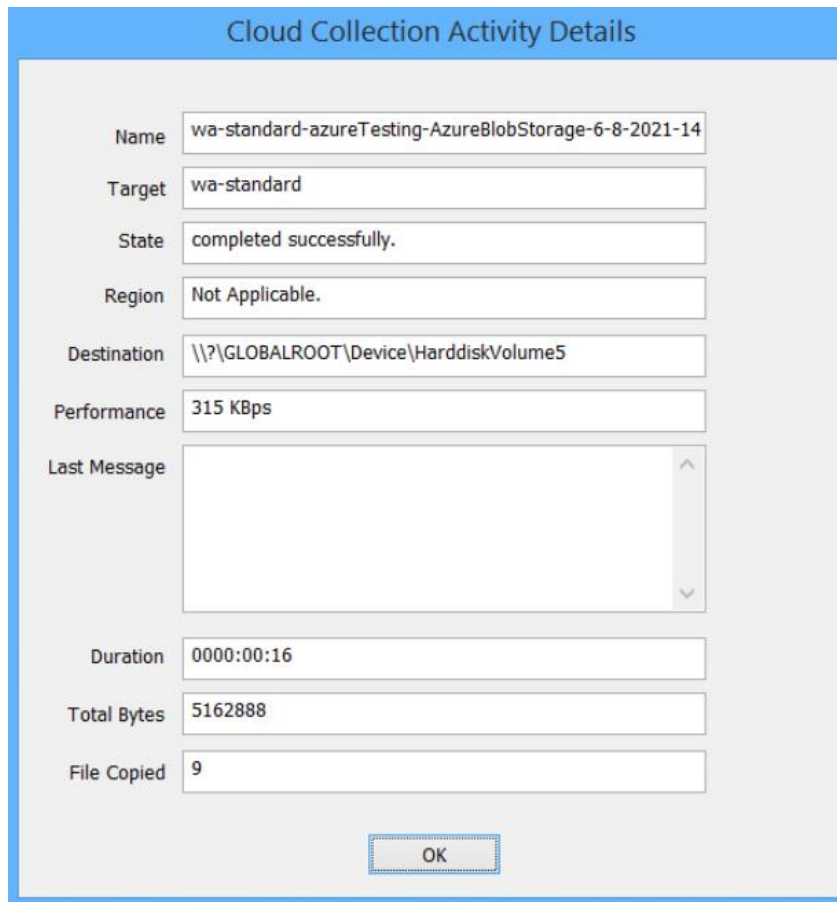
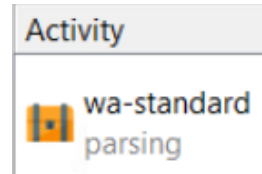
Browse for Alternate Root: This option will allow you to select a different starting location to pull data from. Click on an item and wait a moment for the subdirectories to parse. Continue to click and drill as far down the path as you need to narrow the scope of the collection accordingly (the 'double 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

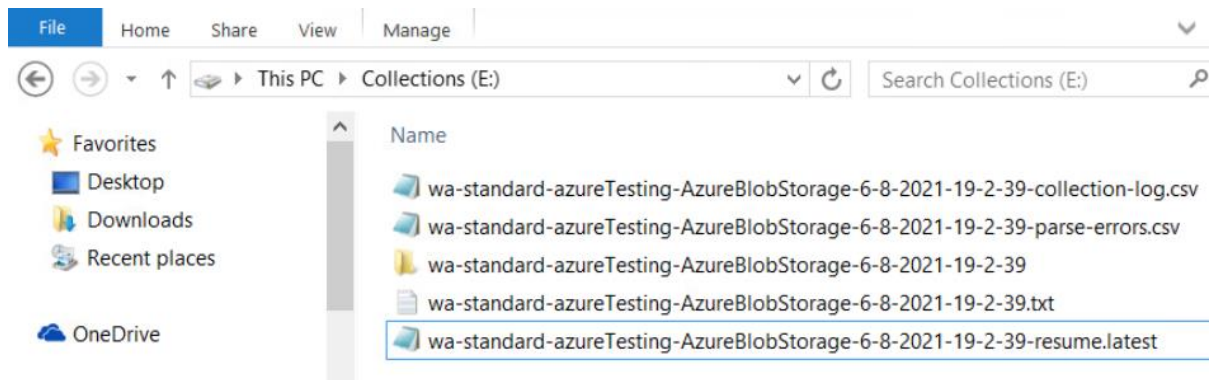
The Activity Pane shows the active collection. Double clicking on the collection will provide additional details.

The image shows a dialog box titled "Cloud Collection Activity Details" with a blue header bar. The dialog contains several fields for displaying activity information. The fields are: Name (wa-standard-azureTesting-AzureBlobStorage-6-8-2021-14), Target (wa-standard), State (completed successfully.), Region (Not Applicable.), Destination (\\?\GLOBALROOT\Device\HarddiskVolume5), Performance (315 KBps), Last Message (empty text area with scroll arrows), Duration (0000:00:16), Total Bytes (5162888), and File Copied (9). An "OK" button is located at the bottom center of the dialog.

Name	wa-standard-azureTesting-AzureBlobStorage-6-8-2021-14
Target	wa-standard
State	completed successfully.
Region	Not Applicable.
Destination	\\?\GLOBALROOT\Device\HarddiskVolume5
Performance	315 KBps
Last Message	
Duration	0000:00:16
Total Bytes	5162888
File Copied	9

Step 5: Review the Completed Collection

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



Reviewing the completed collection.

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	