Cloud Cache Configuration for Azure Page Blobs

Using Cloud Cache with Azure Page Blobs

Cloud Cache provides native support for Azure Page Blobs and Azure Premium Page Blobs, allowing the use of these storage mechanisms for both FSLogix Profile Containers and FSLogix Office 365 Containers.

Support for Azure Page Blobs utilizes the Azure Storage REST API over port 443 eliminating the need to open special ports to support this functionality.

In order to utilize Azure Page Blobs the system must be configured to use Cloud Cache (Cloud Cache must be utilized even if only one storage location is specified), and CCDLocations must be correctly configured to use Azure Page Blobs.

Configuring CCDLocations for Azure

In order to utilize Azure the following parameters should be set for a connection type in CCD Locations

type=azure
connectionString=

DefaultEndpointsProtocol=[http or https]
AccountName=myAccountName
AccountKey=myAccountKey
EndpointSuffix=mySuffix

The parameters described above are passed to Azure Storage as the connection string. For more information for Azure Connection Strings, please see: https://docs.microsoft.com/en-us/azure/storage/common/storage-configure-connection-string

In actual use the entire connection string is enclosed in "", with each parameter in the connection string separated by a semicolon. Please see example below:

type=azure,connectionString="DefaultEndpointsProtocol=https;AccountName=myAccountName;AccountKey=myAccountKey;EndpointSuffix=mySuffix"

If an Azure Storage Type is going to be utilized with another Cloud Cache Type, then the types should be separated by semicolons, please see example where the first type is SMB, and the second type is Azure Page Blob. NOTE: because SMB is the FIRST type, all reads in this example will be from the SMB type, unless it becomes unavailable, please see Cloud Cache Technology for more information: https://docs.fslogix.com/display/20170529/FSLogix+Cloud+Cache+Technology

type=smb,connectionString=\\FILESERVER\SharedFolder;type=azure,connectionString="DefaultEndpointsProtocol=https;AccountName=myAccountName;AccountKey=myAccountKey;EndpointSuffix=mySuffix"

If you need help getting your Azure Connection String, please see documentation here: https://docs.microsoft.com/en-us/azure/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows#attach-or-detach-an-external-storage-account

Using Windows Credential Manager to protect account information

Sensitive information in Azure connection strings may be protected by using Windows Credential Manager. FSLogix will read system credentials from Windows Credential Manager ONLY if they are saved with *fslogix/* as a prefix, then the name for your key. If you wanted to use credential manager to protect your Azure Account Key, with a credential named myAccountKey then a SYSTEM key should be added as fslogix/myAccountKey. This would then be accessed within the connection string using |key|. Below is an example of the connection string above, modified to use the system key saved in credential manager:

*type=smb,connectionString=\\FILESERVER\SharedFolder;type=azure,connectionString="DefaultEndpointsProtocol=https;AccountName=myAccountName;AccountKey=**|fslogix/myAccountKey|**;EndpointSuffix=mySuffix"*

Any information that you would like to protect may be saved in Credential Manger and accessed in this way. For Instance, if you wanted to protect both the Account Name and the Account Key, then system keys could be created for both and used in the connection string as described above.

There are a number of ways to use Credential Manger, and any will work with the Azure Connection String provided that the credential is stored under the SYSTEM user, the credential type is "generic", and the credential name is prefixed with fslogix/.

In order to simplify managing system keys for Cloud Cache connection strings frx.exe has been enhanced with the ability to create, list and delete system keys.

- frx.exe add-secure-key -key *keyName* -value *keyValue*
    - Creates a key
    - -key = the name of the key that it will referenced by in the connection string. This command will automatically create the fslogix/ prefix, DO NOT manually add fslogix/ when using add-secure-key.
    - -value = the secret value to be associated with the key name
- frx.exe del-secure-key -key *keyName*
    - This will delete the specified key. There is no need to specify fslogix/ when using this command.
- frx.exe list-secure-key
    - This will list all secure keys with a fslogix/ prefix. This will not list the value associated with those keys.

There are several examples available on the internet for using Power Shell scripts and cmdkey.exe to manage keys if an alternative to frx.exe is desired.

Specifying Interval for API Write calls

There may be reasons to specify the time between Write transactions when using Azure Page Blobs. By Default FSLogix performs Writes every 0.5 seconds. This may be changed by specifying the cacheFlushInterval when configuring the Azure Page Blob type in CCDLocations. The cacheFlushInterval is set in milliseconds, so a cacheFlushInterval=1000 would change the time between writes to Azure Page Blobs from the default of0.5 seconds to 1 second. below is an example of specifying the cacheFlushInterval:

type=smb,connectionString=\\FILESERVER\SharedFolder;type=azure,connectionString="DefaultEndpointsProtocol=https; AccountName=myAccountName;AccountKey=myAccountKey;EndpointSuffix=mySuffix", **cacheFlushInterval=1000;**

> (i) **CAUTION**
>
> There are implications to setting cacheFlushInterval up to and including potential data loss. cacheFlushInterval should only be set if there is a compelling use case, and a strong understanding of potential implications.