How to implement FSLogix Profile container using Azure Files and Active Directory authentication for Windows Virtual Desktop (WVD)

With FSLogix Profile container you can maintain user context (for example application settings) in non-persistent environments like within a Pooled Windows Virtual Desktop Host pool. It will optimize the sign-in time for the end user because the user profiles are stored in VHD(X) file that is mounted to the concerning Session host VM every time the user signs in and therefor nothing has to be downloaded first.

There are several options for the storage location like an existing (or new) Windows File server, but since Azure Files with Active Directory authentication is GA, I personally prefer this option. Azure Files is an Azure service that is scalable on-demand and which is not dependent on a VM that needs to be running 24/7.

In this blog I will show you step-by-step how to deploy FSLogix Profile container user Azure Files and Active Directory authentication for Windows Virtual Desktop. This blog is divided into the following steps:

1. Create a Storage account with a Private endpoint
2. Create a File Share
3. Enable Active Directory authentication on the Storage account
4. Configure Storage account Access control (IAM)
5. Configure NTFS rights on the Azure File Share
6. Install FSLogix Profile Container in your WVD Host pool
7. Configure FSLogix Profile Container via GPO
8. Test the results

**Prerequisites**

The following prerequisites must be in place:

* Up and running Azure tenant, including configured with Azure AD Connect
* Up and running Windows Virtual Desktop environment ([click here for guide](https://www.robinhobo.com/how-to-deploy-and-manage-windows-virtual-desktop-spring-release/))
* Azure Global Administrator account
* Owner permissions on the Azure subscription
* For the local domain you need to have the rights to create groups, users, add ADMX files to the Policy repository and create and edit GPO objects

**Performance and Account type**

During the creation of the storage account you get the option to select **Standard** (HHD) with account type **GPv2**or **Premium** (SSD) with account type **FileStorage**. Premium storage account have more IOPS, but file share size is provisioned (Standard HHD is Pay-as-you-Go), so in general you pay more for your storage, at least in the beginning. Standard storage account general-purpose file shares are good for dev/test environments with up to 200 concurrent active users.

**Step 1 : Create a Storage account with a Private endpoint**

Login to the [Microsoft Azure Portal](https://portal.azure.com/) to perform the steps below.

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-01.jpg)

Open the **Storage accounts** blade and click the **+ Add** button to add a new storage account.

[Graphical user interface, text, application

Description automatically generated with medium confidence](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-02.jpg)

Select your **Subscription** and **Resource group**(or create a new one). Give this storage account a name (must be globally unique) and select the Azure **Location**.

Select the **Performance** type, **Account kind** (see intro of this blog for more info) and **Replication** type and click **Next : Networking**

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-03.jpg)

Select the preferred **Connectivity method**. In this case I will use **Private endpoint** (for security reasons). Click the **+ Add** button to add a Private endpoint.

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-04.jpg)

Select your **Subscription, Resource group** and **Location.** Give this Private endpoint a name. Select **file** as **Storage sub-resource**.

Under **Networking**, select your **Virtual network** and **Subnet**. Under **Private DNS integration** set **Integrate with private DNS zone** to **Yes** and click **OK**and **Next : Data protection**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-05.jpg)

**File share soft delete** is optionally, but I think it is always good to have a quick restore option in case the Azure File Share is accidently been deleted. Therefore I will set this option to **Enabled** and set the **File share retainment period in days**to **7 days**.

Click **Next : Advanced**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-06.jpg)

Set **Secure transfer required**to **Enabled** and **Blob public access**to **Disabled**. Click **Next : Tags**

[Graphical user interface, text

Description automatically generated with medium confidence](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-07.jpg)

Optionally you can add tags to this Storage account. Click **Next : Review + create**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-08.jpg)

Click **Create**

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-09.jpg)

After the deployment is complete, click **Go to resources**

**Step 2 : Create a File Share**

In this step we are going to create the file share itself.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-10.jpg)

On the **Overview** page of the Storage account, click **File shares**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-11.jpg)

Click the **+ File share** button

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-12.jpg)

Give this File share a **Name** and fill in the number of GiB by **Provisioned capacity**. The default size of a FSLogix Profile container is 30 GiB, so in general you can use the following calculation: # of users X 30.

Click **Create**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-13.jpg)

The new File share is now created

Step 3 : Enable Active Directory authentication on the Storage account

For the next steps you need to logon to a domain controller and download the AzFilesHybrid PowerShell module from [here](https://github.com/Azure-Samples/azure-files-samples/releases). After downloading, unzip the file to a folder like c:\AzFilesHybrid.

Start an elevated PowerShell prompt and run the following commands:

Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope CurrentUser

Install NuGet by running the following command:

Install-PackageProvider -Name NuGet -Force

Within the PowerShell prompt, navigate to c:\AzFilesHybrid, and run the following command:

Import-Module -Name .\AzFilesHybrid.psd1

[Text

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-14.jpg)

The Az PowerShell module is required, if not already installed on the machine you will be asked to install it at this moment, type **A**for **Yes to All**

Connect to Azure via PowerShell by running the following command:

Connect-AzAccount

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-15.jpg)

A login prompt will appear, login with an Azure Global Administrator account

Select an Azure Subscription by running the following command:

Select-AzSubscription -SubscriptionName "<your subscription name>"

[Graphical user interface, website

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-16.jpg)  
To connect the Storage account with Active Directory, run the following command:

join-AzStorageaccountForAuth -ResourceGroupName "<Resource Group Name>" -Name "<Storage Account Name>" -DomainAccountType "ComputerAccount" -OrganizationalUnitDistinguishedName "<OU Distinguished Name>"

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-17.jpg)

Close the PowerShell prompt.

[Graphical user interface, text, application, Word

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-18.jpg)

When you take a look in **Active Directory Users and Computers** you will now find a Computer account in the OU you specified in the previous step.

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-19.jpg)

Within the Azure Portal, go to the **Storage account** and open the **Configuration** blade. Now you can see here that **Active Directory Domain Services (AD DS)** is enabled.

Step 4 : Configure Storage account Access control (IAM)

We need to set some permissions to the Storage account, there must be a Administrator (or a group of administrators) with the **Storage File Data SMB Elevated Contributor**rights to set NTFS permissions on the file share. Next to the administrator, all users that will use FSLogix profile container needs to have the **Storage File SMB Share Contributor**rights.

[](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-20.jpg)

That’s why I created two security groups in Active Directory (as displayed in the screenshot above) and added the right users to it.

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-21.jpg)

Once the AD security groups are synced to Azure AD, navigate to your Storage account within the Azure portal and open the **Access control (IAM)** blade. In the **Add a role assignment** part, click **Add**

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-22.jpg)

Add the **Storage File Data SMV Share Contributor** role to your “user security group”, in my case “FSLogix Share Contributor”

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-23.jpg)

Click the **Add**button again and give the **Storage File Data SMB Share Elevated Contributor**role to the “administrators security group”, in my case “FSLogix Share Elevated Contributor”.

Step 5 : Configure NTFS rights on the Azure File Share

Next step is to set the rights on NTFS level, but first we need to obtain the full UNC path of the File Share.

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-24.jpg)

Navigate to the Storage account and open the **Properties** blade. Copy the **File service** URL to a Notepad.

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-25.jpg)

Next, open the **File shares** blade and copy the File share name to the same Notepad

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-26a.jpg)

Remove “https://” and replace the forward slash with the back slash is shown in the screenshot above. Copy this UNC path, open Windows Explorer and past the UNC path in the address bar.

[Graphical user interface, application, Word

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-27a.jpg)

Open the **Home** tab and click the **Properties** button. Open the **Security**tab and click **Advanced**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-28.jpg)

Change the permissions to how it is displayed in the screenshot above (remove everything else).

Step 6 : Install FSLogix Profile Container in your WVD Host pool

If using [WVD Image management](https://www.robinhobo.com/windows-virtual-desktop-wvd-image-management-how-to-manage-and-deploy-custom-images-including-versioning-with-the-azure-shared-image-gallery-sig/), login to your “Master VM” (otherwise login to a Session host VM as Administrator) and download the latest FSLogix software from [here](https://aka.ms/fslogix_download).

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-29.jpg)

Unzip de source file and navigate to the **x64 > Release** folder and run **FSLogixAppsSetup**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-30.jpg)

Select **I agree to the license terms and conditions** (if you do) and click **Install**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-31.jpg)

Click **Close**

If FSLogix is installed on the Master VM, deploy the new image in your Windows Virtual Desktop Host pool.

Step 7 : Configure FSLogix Profile Container via GPO

The final implementation step is to configure and enable FSLogix within the Windows Virtual Desktop environment. You can do this easily via GPO.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-32.jpg)

The installation source of FSLogix includes a custom ADMX and ADML file.

[Graphical user interface, table

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-33.jpg)

Copy the **fslogix.admx** file  to the **\\<AD Domain Name > SYSVOL > <AD Domain Name> > Policies > PolicyDefinitions** folder.

[Graphical user interface, table

Description automatically generated with medium confidence](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-34.jpg)

Copy the **fslogix.adml** file  to the **\\<AD Domain Name > SYSVOL > <AD Domain Name> > Policies > PolicyDefinitions > en-US** folder.

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-35.jpg)

Open or create a GPO that will apply on your Windows Virtual Desktop Host pool Session Host VMs. And navigate to:

**Computer Configuration > Policies > Administrative Templates > FSLogix > Profile Containers**

**Enable** the following settings:

* **Set Outlook cached mode on successful container attach**
* **Enabled**
* **VHD location**
* **Delete local profile when FSLogix Profile should apply**

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-36.jpg)

When enabling the **VHD location**setting, set the location to the Azure File share UNC path.

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-37.jpg)

Navigate to: **Computer Configuration > Policies > Administrative Templates > FSLogix > Profile Containers > Container and Directory Naming**

**Enable** the following settings:

* **Virtual disk type**
* **Swap directory name components**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-38.jpg)

When enabling the **Virtual disk type**, select the **VHDX** format.

Step 8 : Test the results

When the GPO is applied to the Windows Virtual Desktop Session Host VMs, you can logon with a user that is member of the **Storage File Data SMV Share Contributor**related AD security group.

[A picture containing text, nature, cloud, night sky

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-39.jpg)

When login you will notice the **Please wait for the FSLogix Apps Services** notification.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2020/07/FSLogix-40.jpg)

After login, you can open **Disk Management**, if FSLogix is configured correctly, a **Profile-<name>** disk is mounted to the VM.