FSlogix On Azure Virtual Desktop

Agenda:

Section 4:

1. What is Fslogix
2. Storage for FSLogix components
3. Storage account for FSlogix Profile Container (Overview)
4. Configure storage for FSLogix components
5. AVD User Data Storage

1. What is Fslogix:

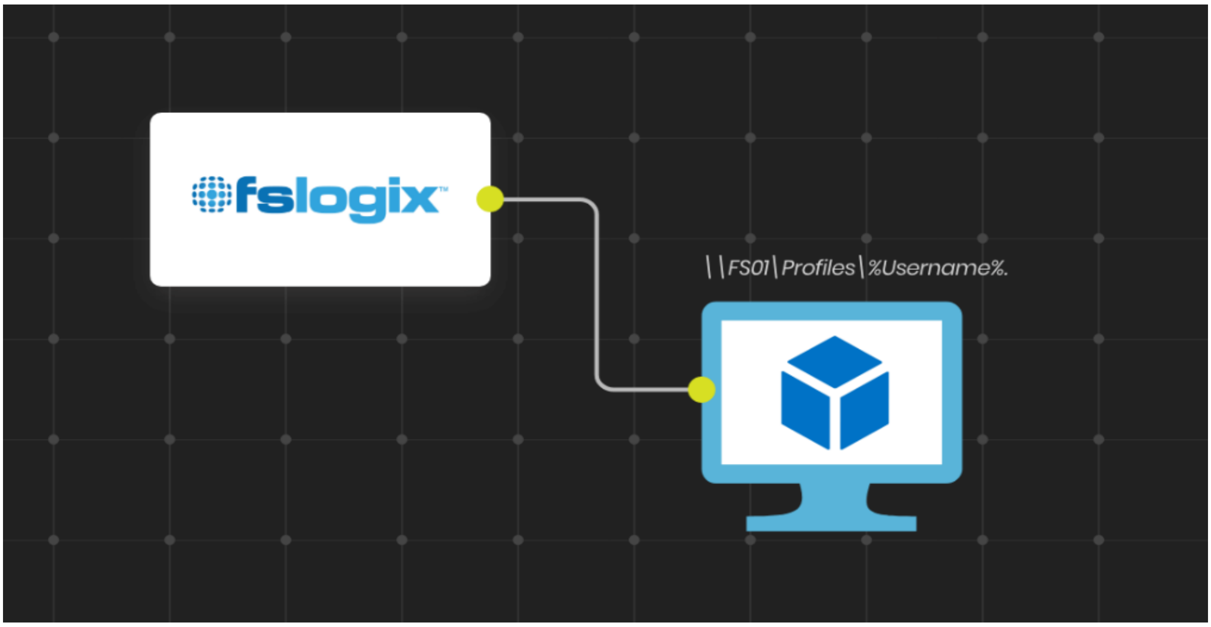
FSLogix : Profile management solution that can be configured to entirely or partially redirect user profiles to a remote location when working over non-persistent Windows computing environments.

FSLogix includes:

Profile Container :Profile containers are used to redirect entire user profiles. Similar to Microsoft roaming/Citrix UPM/VMware Persona

Office Container: Office Container redirects only the specific part of a user profile that contains Microsoft Office cached data such as .OST files, MS teams data.

Application Masking :Application Masking significantly decreases the complexity of managing large numbers of gold images.Cloud Cache :It's a high availability/Disaster recovery solution Allows users to access their data even in the case of networking or storage issues.



FSLogix allows you to:

Roam user data between remote computing session hosts

Minimize sign in times for virtual desktop environments

Optimize file IO between host/client and remote profile store

Provide a local profile experience, eliminating the need for roaming profiles.

Simplify the management of applications and 'Gold Images'

License Requirements:

Microsoft 365 A3/A5,F1/F3,E3/E5

Remote Desktop Services (RDS) Client Access License (CAL), Subscriber Access License (SAL)

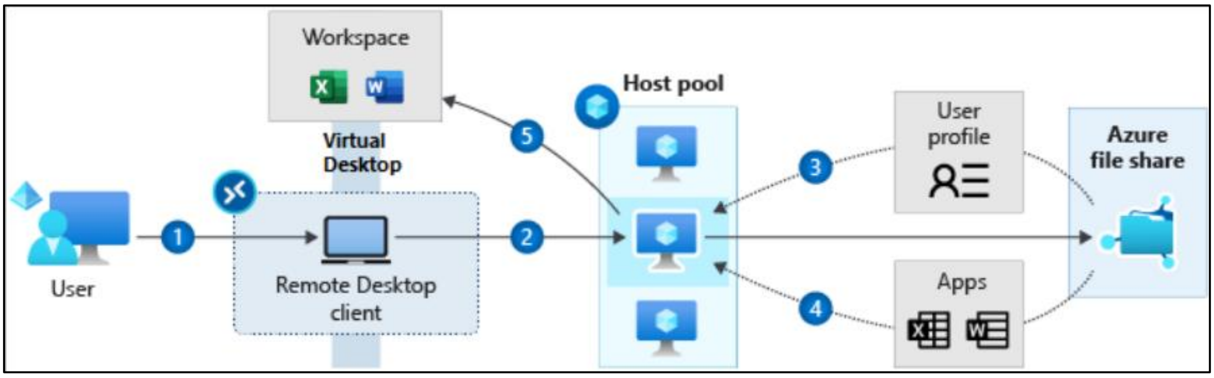
Azure Virtual Desktop per-user access license.

2. Storage for FSLogix components:

Azure Virtual Desktop service recommends FSLogix profile containers as a user profile solution. FSLogix is designed to roam profiles in remote computing environments, such as Azure Virtual Desktop. It stores a complete user profile in a single container. At sign-in, this container is dynamically attached to the computing environment using natively supported Virtual Hard Disk (VHD) and Hyper-V Virtual Hard disk (VHDX).

The VHD or VHDX files are stored to this location and attached to users the next time they sign in.

The following diagram shows the process of getting the user profile after sign-in to the Remote Desktop client.

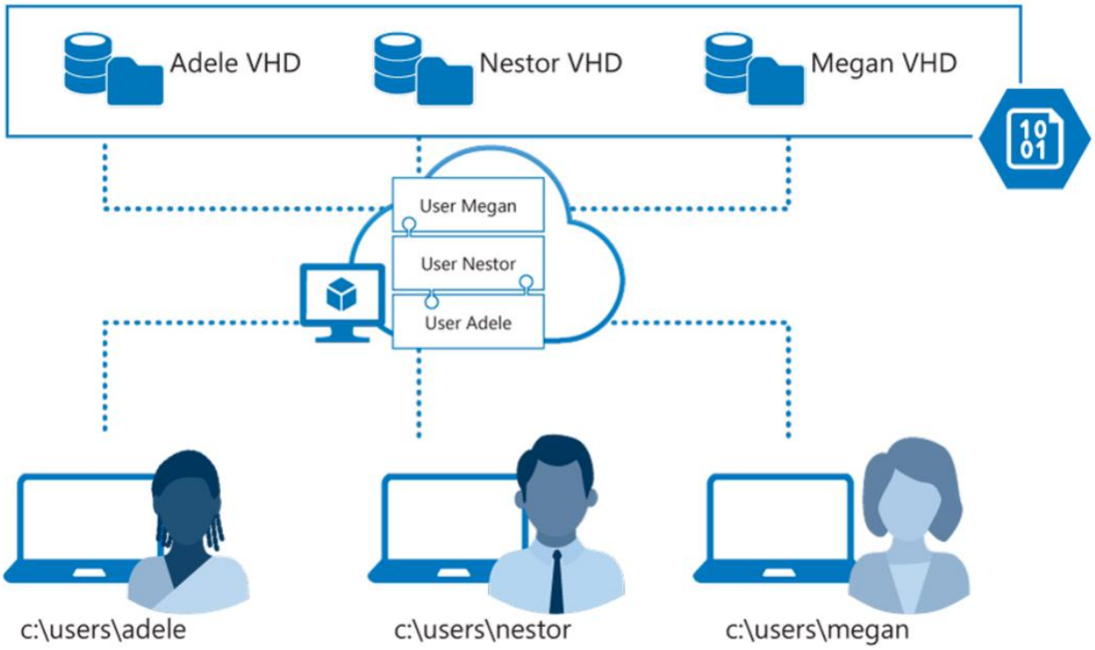


1) User signs into the Remote Desktop client
2) User gets assigned to a session host virtual machine (VM)
3) VM gets the user profile from the Azure file share.
4) (Preview) If you have MSIX app attach configured, apps are dynamically delivered to the session host VM. MSIX app attach uses FSLogix storage concepts, but for applications.
5) User gets their Azure Virtual Desktop workspace populated with their assigned app(s) or session desktop.

The user profile is immediately available and appears in the system exactly like a native user profile.

User profiles

A user profile contains data elements including desktop settings, persistent network connections, and application settings. By default, Windows creates a local user profile that is tightly integrated with the operating system.



A remote user profile provides a partition between user data and the operating system. It allows the operating system to be replaced or changed without affecting the user data. In Remote Desktop Session Host (RDSH) and Virtual Desktop Infrastructures (VDI), the operating system may be replaced for the following reasons:

- An upgrade of the operating system
- A replacement of an existing Virtual Machine (VM)
- A user being part of a pooled (non-persistent) RDSH or VDI environment

Microsoft products operate with several technologies for remote user profiles, including these technologies:

- Roaming user profiles (RUP)
- User profile disks (UPD)
- Enterprise state roaming (ESR)

UPD and RUP are the most widely used technologies for user profiles in Remote Desktop Session Host (RDSH) and Virtual Hard Disk (VHD) environments.

3. Storage account for FSlogix Profile Container (Overview):

- An Azure storage account contains all of your Azure Storage data objects: blobs, file shares, queues, tables, and disks.

Azure Files→ Premium file shares³

- LRS
- ZRS2

Premium storage account type for file shares only. Recommended for enterprise or high-performance scale applications. Use this account type if you want a storage account that supports both SMB and NFS file shares.

- Azure Premium Files

provides fully managed file services optimized to deliver consistent performance. It's designed for IO intensive enterprise workloads that require high throughput and a single digit millisecond latency.

Premium Files stores data on the latest solid-state drives (SSDs), which makes it suitable for a wide variety of workloads like file services, databases

- Burst IOPS

Azure Netapp Files

The Azure NetApp Files service is an enterprise-class, high-performance, metered file storage service

FSLogix addresses many profile container challenges. Key among them are:

- Performance: The FSLogix profile containers are high performance and resolve performance issues that have historically blocked cached exchange mode.
- OneDrive: Without FSLogix profile containers, OneDrive for Business is not supported in non-persistent RDSH or VDI environments.
- Additional folders: FSLogix provides the ability to extend user profiles to include additional folders.

Microsoft has started replacing existing user profile solutions, like UPD, with FSLogix profile containers.

4. Configure storage for FSLogix components:

The Azure Virtual Desktop service offers FSLogix profile containers as the recommended user profile solution. We don't recommend using the User Profile Disk (UPD) solution, which will be deprecated in future versions of Azure Virtual Desktop.

This unit explains how to set up a FSLogix profile container share for a host pool using a virtual machine-based file share.

Create a new virtual machine that will act as a file share:

When creating the virtual machine, be sure to place it on either the same virtual network as the host pool virtual machines or on a virtual network that has connectivity to the host pool virtual machines.

After creating the virtual machine, join it to the domain by doing the following things:

- Connect to the virtual machine with the credentials you provided when creating the virtual machine.
- On the virtual machine, launch **Control Panel** and select **System**.
- Select **Computer name**, select **Change settings**, and then select **Change…**
- Select **Domain** and then enter the Active Directory domain on the virtual network.
- Authenticate with a domain account that has privileges to domain-join machines.

Prepare the virtual machine to act as a file share for user profiles:

The following are general instructions about how to prepare a virtual machine to act as a file share for user profiles:

- Add the Azure Virtual Desktop Active Directory users to an Active Directory security group. This security group will be used to authenticate the Azure Virtual Desktop users to the file share virtual machine you created.
- Connect to the file share virtual machine.
- On the file share virtual machine, create a folder on the **C drive** that will be used as the profile share.
- Right-click the new folder, select **Properties**, select **Sharing**, then select **Advanced sharing...**.
- Select **Share this folder**, select **Permissions...**, then select **Add...**.
- Search for the security group to which you added the Azure Virtual Desktop users, then make sure that group has **Full Control**.
- After adding the security group, right-click the folder, select **Properties**, select **Sharing**, then copy down the **Network Path** to use for later.

Configure the FSLogix profile container:

To configure the virtual machines with the FSLogix software, do the following on each machine registered to the host pool:

- Connect to the virtual machine with the credentials you provided when creating the virtual machine.
- Launch an internet browser and navigate to this link to download the FSLogix agent.
- Navigate to either *\Win32\Release* or *\X64\Release* in the .zip file and run **FSLogixAppsSetup** to install the FSLogix agent.
- Navigate to **Program Files > FSLogix > Apps** to confirm the agent installed.
- From the start menu, run **RegEdit** as an administrator. Navigate to **Computer\HKEY_LOCAL_MACHINE\software\FSLogix**.
- Create a key named **Profiles**.
- Create the following values for the Profiles key:

5. AVD User Data Storage:

FSLogix for User Data Storage:

- The Azure Virtual Desktop service recommends FSLogix profile containers as a user profile solution.
- FSLogix is designed to roam profiles in remote computing environments, such as Azure Virtual Desktop.
- It stores a complete user profile in a single container.
- At sign in, this container is dynamically attached to the computing environment using natively supported Virtual Hard Disk (VHD) and Hyper-V Virtual Hard disk (VHDX).
- The user profile is immediately available and appears in the system exactly like a native user profile. • This article describes how FSLogix profile containers used with Azure Files function in Azure Virtual Desktop.

User Profiles:

A user profile contains data elements about an individual, including configuration information like desktop settings, persistent network connections, and application settings. By default, Windows creates a local user profile that is tightly integrated with the operating system. A remote user profile provides a partition between user data and the operating system. It allows the operating system to be replaced or changed without affecting the user data. In Remote Desktop Session Host (RDSH) and Virtual Desktop Infrastructures (VDI), the operating system may be replaced for the following reasons:
• An upgrade of the operating system
• A replacement of an existing Virtual Machine (VM)
• A user being part of a pooled (non-persistent) RDSH or VDI environment

FSLogix profile containers:

On November 19, 2018, Microsoft acquired FSLogix. FSLogix addresses many profile container challenges. Key among them are:
• Performance: The FSLogix profile containers are high performance and resolve performance issues that have historically blocked cached exchange mode.
• OneDrive: Without FSLogix profile containers, OneDrive for Business is not supported in nonpersistent RDSH or VDI environments. The OneDrive VDI support page will tell you how they interact. For more information, see Use the sync client on virtual desktops.
• Additional folders: FSLogix provides the ability to extend user profiles to include additional folders.

Azure Files integration with Azure Active Directory Domain Service:

• FSLogix profile containers' performance and features take advantage of the cloud.
• Microsoft Azure Files now supports authentication with Azure Active Directory Domain Service (Azure AD DS).
• By addressing both cost and administrative overhead, Azure Files with Azure AD DS Authentication is a premium solution for user profiles in the Azure Virtual Desktop service.

Best practices for Azure Virtual Desktop:

Azure Virtual Desktop offers full control over size, type, and count of VMs that are being used by customers. To ensure your Azure Virtual Desktop environment follows best practices:

- Azure Files storage account must be in the same region as the session host VMs.
- Azure Files permissions should match permissions described in Requirements - Profile Containers.
- Each host pool VM must be built of the same type and size VM based on the same master image.
- Each host pool VM must be in the same resource group to aid management, scaling and updating.
- For optimal performance, the storage solution and the FSLogix profile container should be in the same data center location.
- The storage account containing the master image must be in the same region and subscription where the VMs are being provisioned.