

2018

UPD and FSLogix Containers

Deployment Details

A detailed overview of UPD support on all major platforms and how it compares to FSLogix containers



Contents

Introduction	3
Implementing User Profile Disks.....	4
Command line implementation	7
GPO Implementation	9
UPD Limitations.....	13
Overcoming UPD limitations.....	15
FSLogix Office 365 Containers with UPDs.....	16
FSLogix Containers – Full implementation.....	24
Conclusion.....	29

Introduction

For quite a long time, several companies have been deploying centrally hosted solutions like Citrix Virtual Apps, VMware Horizon, Microsoft Remote Desktop Services (RDS) and Parallels RAS to deliver the Microsoft Office suite to its users. For as long as we all have been in IT, one of the main challenges with such suite is related to Microsoft Outlook and the way it deals with its locally cached data and index. Further complicating the issue, several companies adopted Microsoft OneDrive for Business (OD4B) as their main solution for sharing files.

Traditionally, these were paired with some profile management solution and folder redirection policies, to minimize the impact seen on performance and logon times. This solved part of the problem but created several other ones, leaving some crucial issues unresolved.

When Microsoft introduced Windows Server 2012, it brought User Profile Disks (UPDs) along. By shifting the whole user profile to a Virtual Hard Disk (VHD) based container, logon performance is dramatically improved as the profile is simply 'attached' at logon to the machine where the user is logging in. Space wise, nothing is used locally as it is all part of the VHD. Even what is stored on the container can be customized to minimize its size, if required.

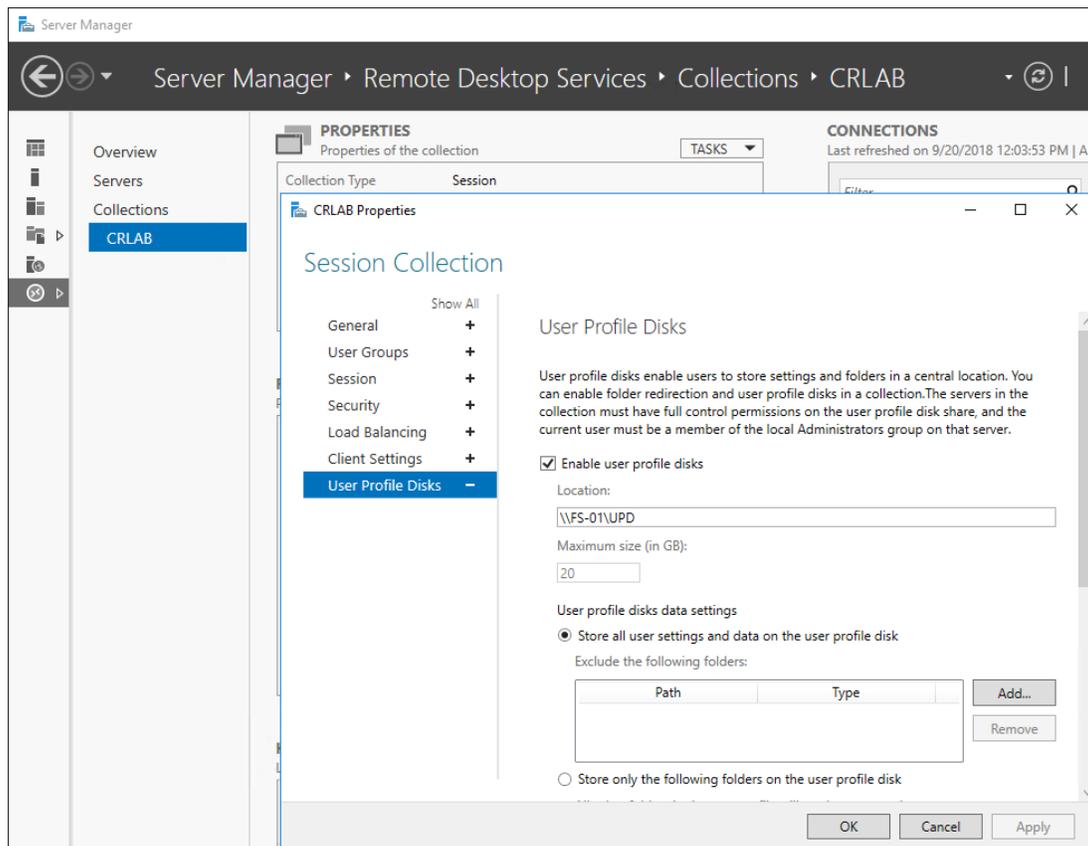
That said, most solutions, for unknown reasons, do not support UPDs out-of-the-box (RDS and Parallels RAS as the exceptions).

The purpose of this whitepaper is to show you how to enable UPDs on any platform and how it compares to FSLogix. It is important to highlight that FSLogix can indeed replace UPDs completely but for many companies, using UPDs with FSLogix as a complement, is not only supported but highly effective in terms of performance and costs.

Implementing User Profile Disks

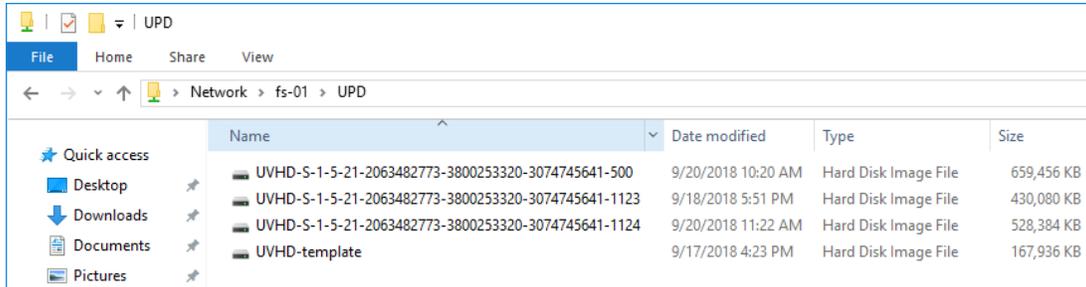
The process used to enable UPDs is exactly the same, no matter the platform in place. The main requirement is to make sure the servers involved (where users will launch their sessions from) do have full rights on the share and on the actual folder (NTFS permissions) where the UPDs will be stored. This is critical.

Being a Microsoft solution, RDS does allow you to enable UPDs through its management GUI, RDMS. This is done by launching server manager on a connection broker and enabling it for a particular collection:

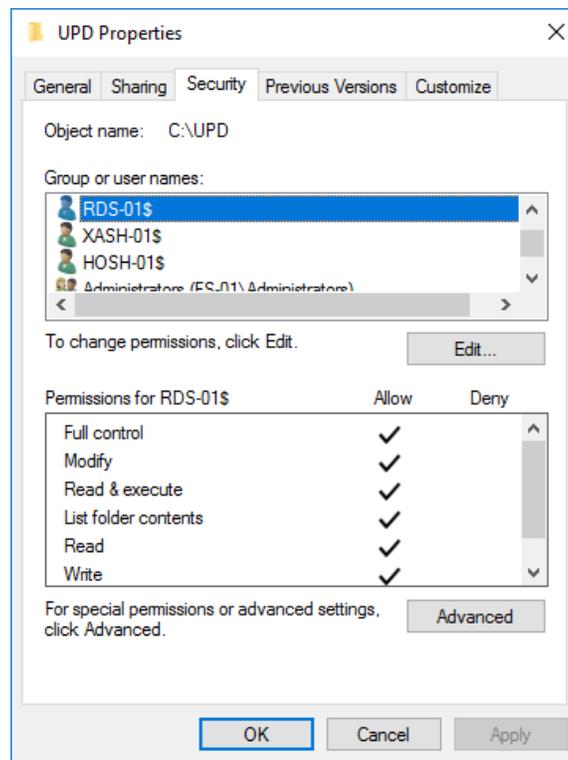


Right there in the GUI you can set the size of the UPD (a VHDX file) and which folders to include as part of it. By default, all folders are included what eliminates the need for folder redirection, greatly simplifying and speeding up backup operations.

Once this is enabled, a template VHDX file is created on the share and named 'UVHD-template'. This is the file that will be used as a starting point for all users that have access to that particular RDS collection. During the first logon on a server that is part of it, a file for the user is created based on the template and named with the user's SID as seen below:

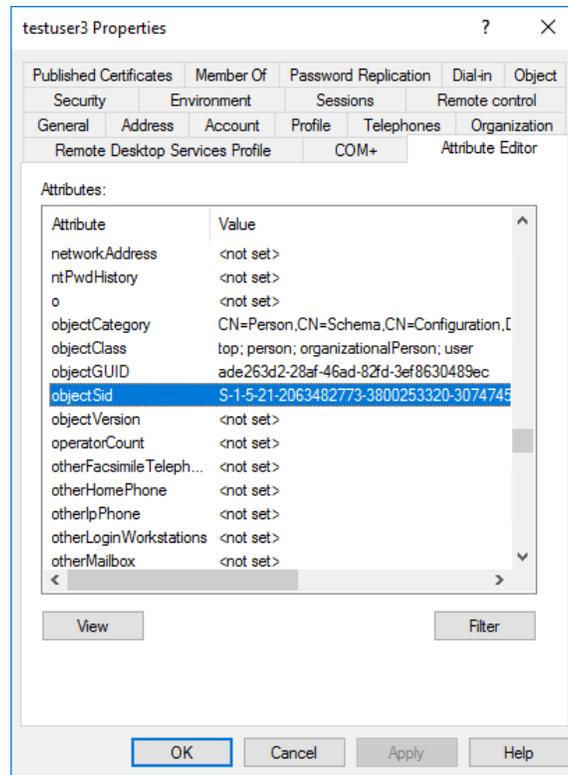


Note: when UPDs are enabled in an RDS deployment for a particular session collection, under the hood, the computer objects part of the collection are assigned full rights on the UPD share and NTFS folder as seen below:



These permissions must be manually set when enabling UPD under all other platforms (i.e. Citrix Virtual Apps, VMware Horizon, etc) in order for it to work properly.

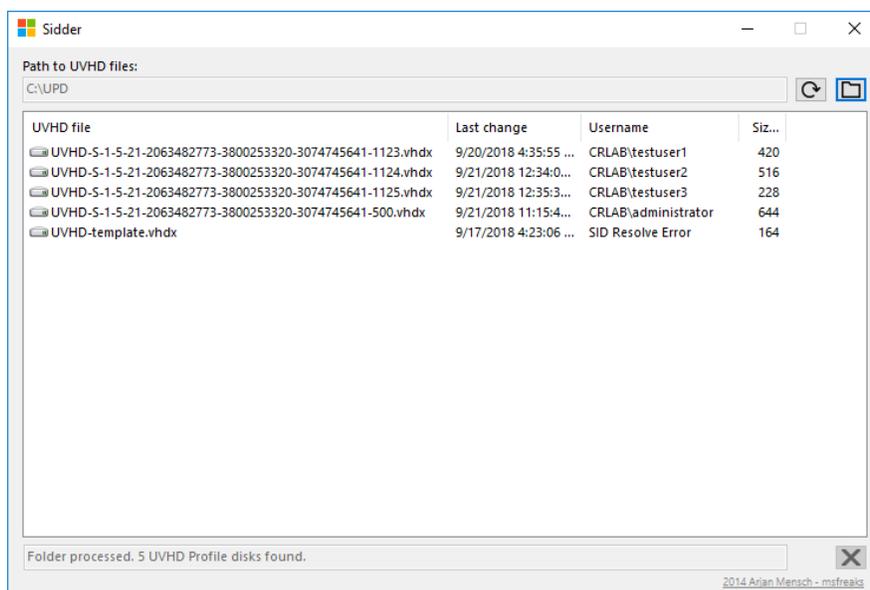
It is possible, if required, to pre-stage the creation of the UPD files to speed up the logon process even further. It is just a matter of copying the template file to a file named 'UVHD-**USER_SID**.vhdx'. The **USER_SID** can be retrieved directly from the objectSid LDAP property under Active Directory as seen below.



As you noticed, identifying the UPDs based on the SID is not the easiest. To fix that, Arjan Mensch released a very nice tool, SIDDER, that you can download at:

<https://gallery.technet.microsoft.com/Sidder-Quickly-see-which-fa6360b3>

Once you run the executable and point it to the file share where your UPDs are stored, you should see something similar to the screenshot below, showing which UPD belongs to which user.

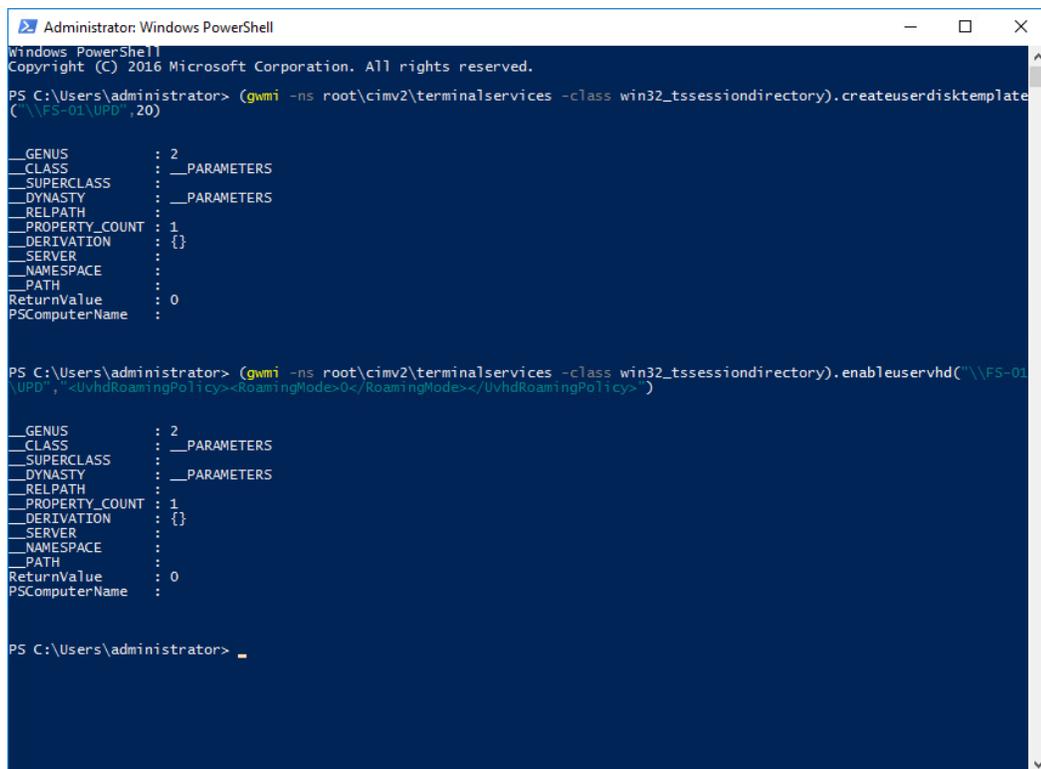


Command line implementation

As Citrix and VMware do not offer support for UPDs out-of-the-box, there is no way to do this through their management GUI. That said, this can still be enabled using PowerShell in one server and once done, a group policy can be put in place to enable it on all the remaining servers.

To enable UPDs on a server (RDS Session Host), follow this procedure:

1. Open PowerShell with administrator rights. Make sure the server where you are logged in has full rights to the share and folder as explained previously.
2. Run the following commands in sequence (these are one liners – make sure you replace **FILE_SERVER**, **SHARE** and **SIZE** - in GB, i.e. 20 for 20 gigabytes for the UPD size per user - with the correct values for your environment):
 - (gwmi -ns root\cimv2\terminalservices -class win32_tssessiondirectory).createuserdisktemplate("**FILE_SERVER****SHARE**",**SIZE**)
 - (gwmi -ns root\cimv2\terminalservices -class win32_tssessiondirectory).enableuservhd("**FILE_SERVER****SHARE**", "<UvhdRoamingPolicy><RoamingMode>0</RoamingMode></UvhdRoamingPolicy>")
3. If everything worked as expected you should see the following (or similar) screen:



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator> (gwmi -ns root\cimv2\terminalservices -class win32_tssessiondirectory).createuserdisktemplate("\\FS-01\UPD",20)

__GENUS           : 2
__CLASS           : __PARAMETERS
__SUPERCLASS     : 
__DYNASTY        : __PARAMETERS
__RELPATH        : 
__PROPERTY_COUNT : 1
__DERIVATION     : {}
__SERVER        : 
__NAMESPACE     : 
__PATH          : 
ReturnValue      : 0
PSComputerName   :

PS C:\Users\administrator> (gwmi -ns root\cimv2\terminalservices -class win32_tssessiondirectory).enableuservhd("\\FS-01\UPD", "<UvhdRoamingPolicy><RoamingMode>0</RoamingMode></UvhdRoamingPolicy>")

__GENUS           : 2
__CLASS           : __PARAMETERS
__SUPERCLASS     : 
__DYNASTY        : __PARAMETERS
__RELPATH        : 
__PROPERTY_COUNT : 1
__DERIVATION     : {}
__SERVER        : 
__NAMESPACE     : 
__PATH          : 
ReturnValue      : 0
PSComputerName   :

PS C:\Users\administrator> _
```

Note: The first command is only needed the first time, to get the template VHDX created. The second command enables UPD on the machine you are running the command and sets it to roam every single folder that would be part of the user profile. That includes folders that usually would not roam (i.e. AppData\Local). What gets into the UPD is controlled by a file named UvhdRoamingPolicy.xml, saved under C:\Windows\RemotePackages\RDFarm.

GPO Implementation

Another alternative is to use a GPO, with a computer start-up script, that will run the second command in order to enable UPD on a particular machine. This may be required if you do want different UPDs for certain machines due to the following:

- Different operating systems (i.e. Windows Server vs Windows desktop)
- Different collections/silos (i.e. servers that only run financial apps, servers that only run sales apps, etc)

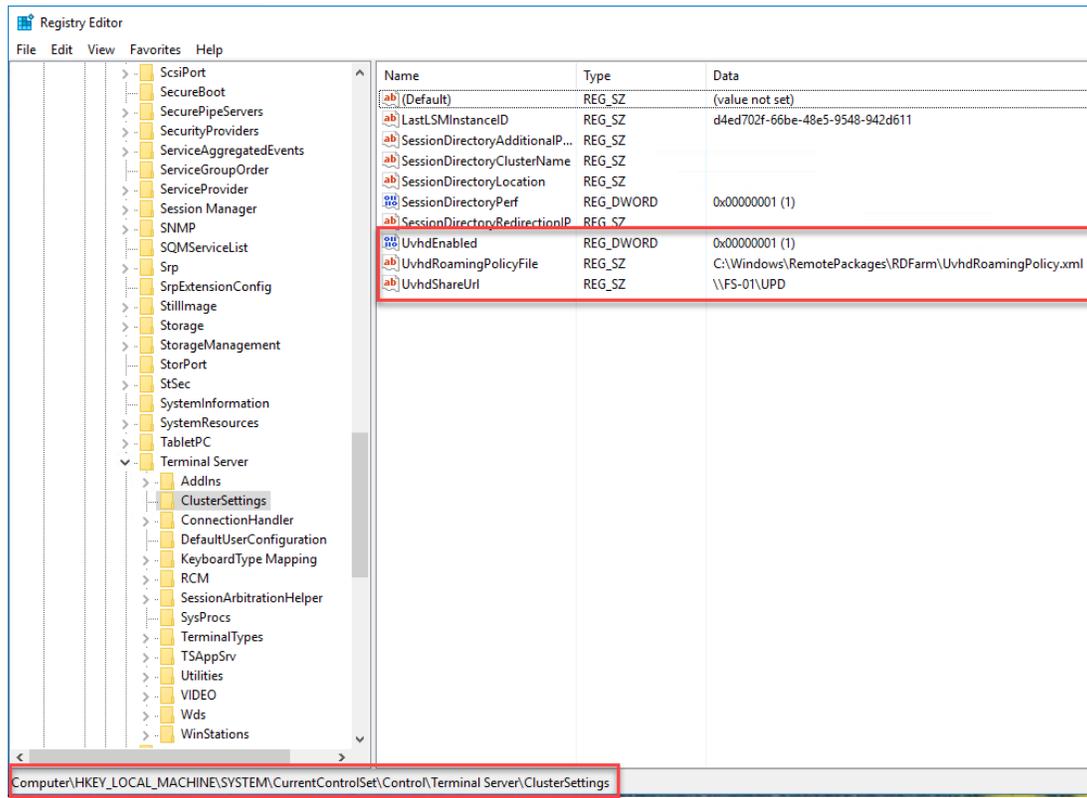
You may even want different UPD settings (i.e. size or folders that should be part of the UPD). The XML file below shows an example that could be used to store only the Outlook cache within the UPD, leaving everything else to be handled by another solution (i.e. Citrix UPM):

UvhdRoamingPolicy.XML file

```
<UvhdRoamingPolicy>
  <RoamingMode>2</RoamingMode>
  <Include>
    <Folder>AppData\Local\Microsoft\Outlook</Folder>
  </Include>
</UvhdRoamingPolicy>
```

Another option is to use a similar start-up script that will set the registry keys seen below and copy from a central location the required UvhdRoamingPolicy.xml file to the proper folder (again, C:\Windows\RemotePackages\RDFarm) on each machine that will have UPDs enabled.

Once UPDs are enabled, the following registry keys are set on the machine:



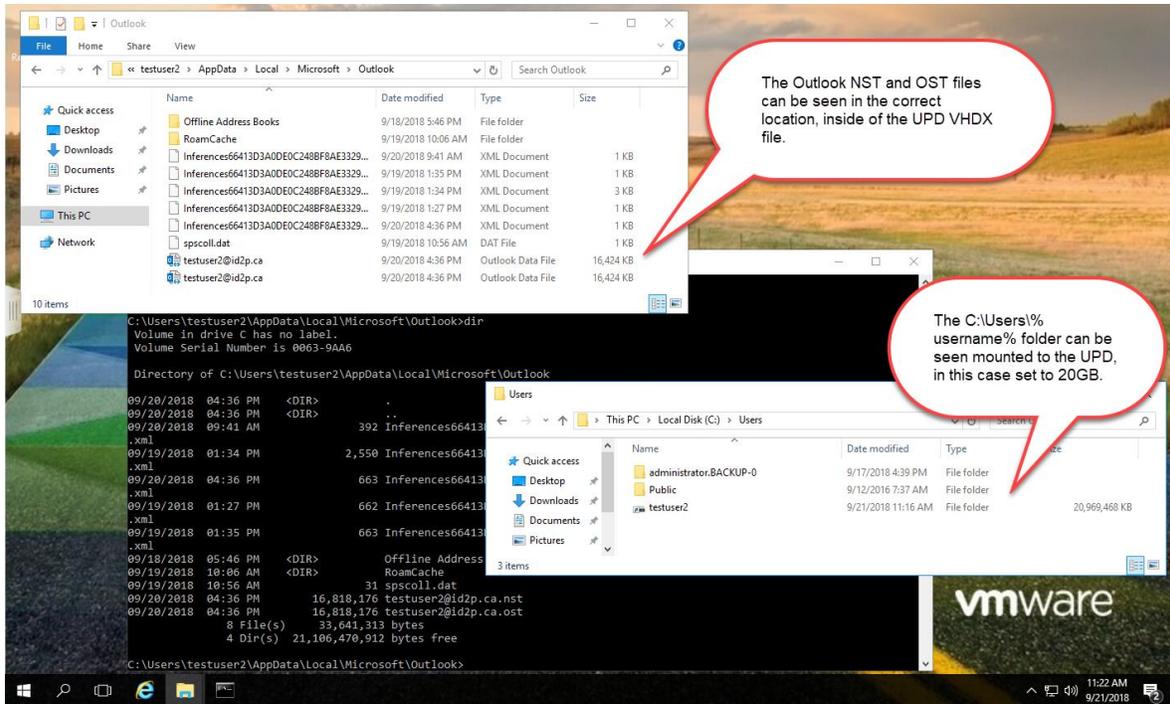
Of course these keys can be exported to a REG file and added to the machines required as part of a startup script (you can copy and paste the contents below to a .REG file and make sure it is set on all your machines that will have UPD enabled):

Windows Registry Editor Version 5.00

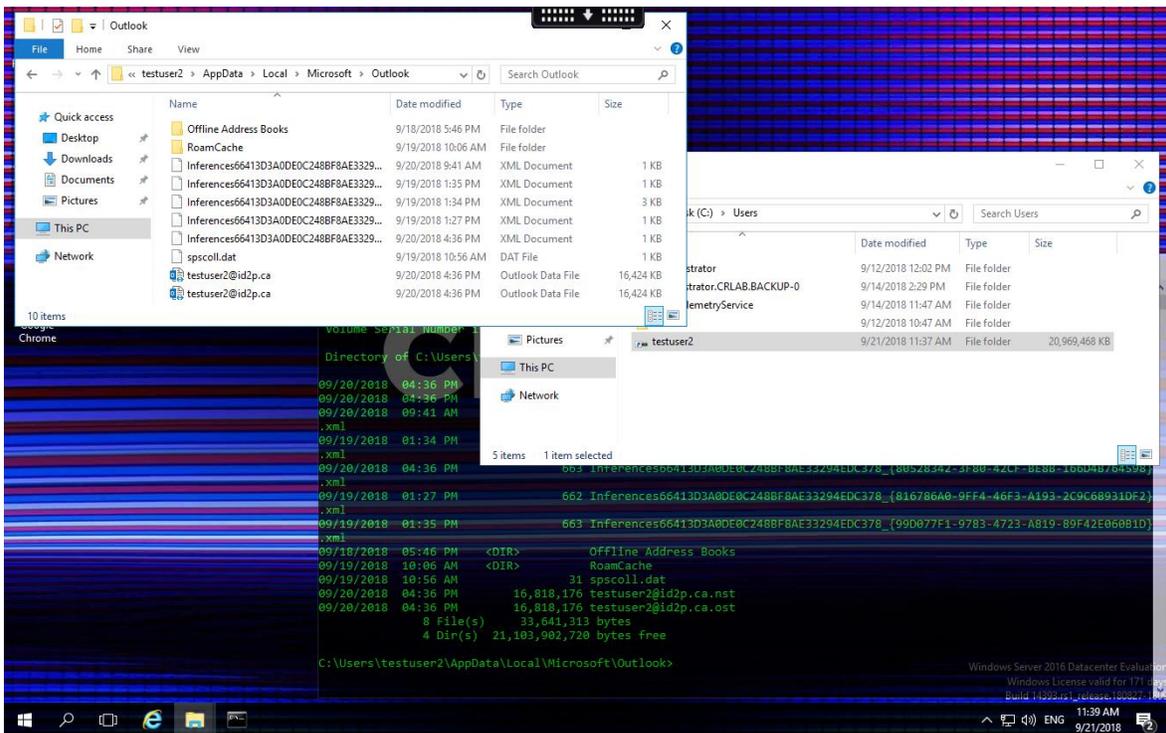
```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\ClusterSettings]
"UvhdEnabled"=dword:00000001
"UvhdShareUrl"=\\\\FILE SERVER\\SHARE
"UvhdRoamingPolicyFile"="C:\\Windows\\RemotePackages\\RFarm\\UvhdRoamingPolicy.xml"
```

Jeroen Tielen created a nice ADMX template you can import to set all these using group policies settings instead of importing the .REG file if you prefer that method. It can be downloaded at <https://www.jeroentielen.nl/microsoft-user-profile-disks-gpo/upd/>.

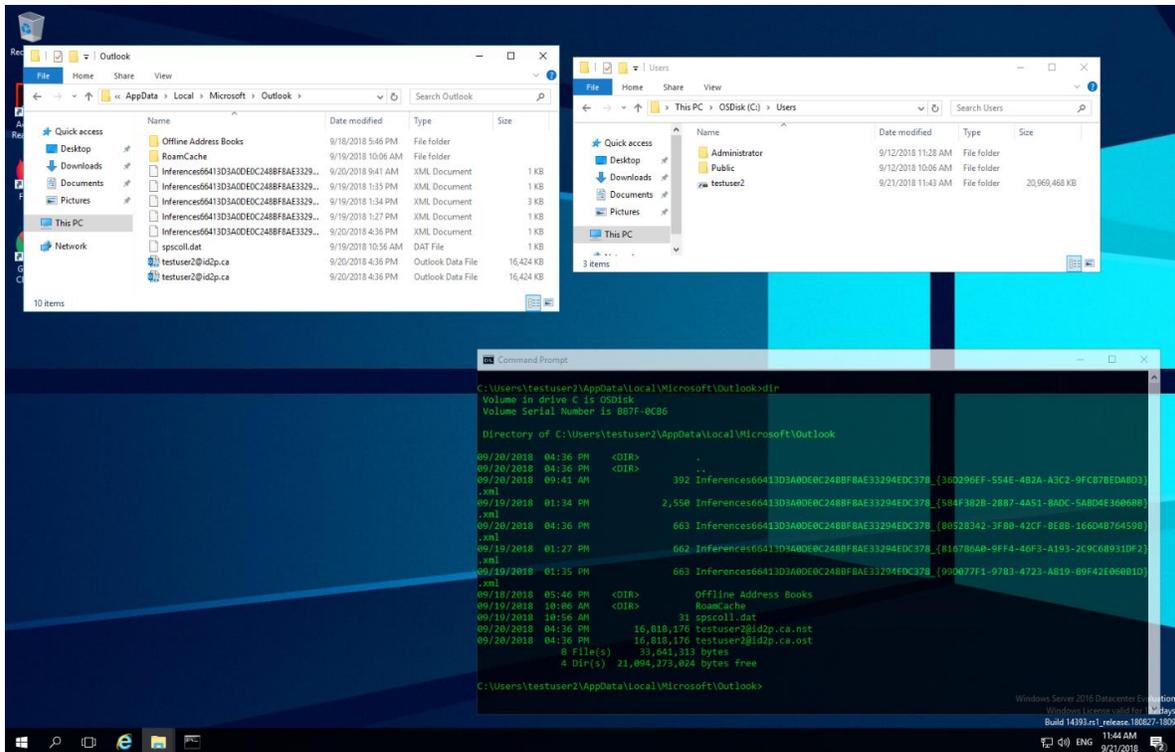
As you realize, you can indeed have different XML files and set different UPD sizes through the command line. This allows you to have completely different settings per OU. For example, for some particular application servers you do want a smaller UPD that only stores certain folders but for your main common servers you do want to use a larger UPD storing all the user data.



The screenshot above shows a VMware Horizon 7.5 session running on Windows Server 2016 with Office 365 installed. As expected, the Outlook files, stored under AppData\Local\Microsoft\Outlook are all there and working. The following screenshots show the same user logged in to the Citrix and RDS environments and mounting the exact same UPD.



Citrix Virtual Apps 7 1808 with Office 365



Microsoft RDS 2016 with Office 365

For this whitepaper, we created three separate environments running RDS, Citrix Virtual Apps and VMware Horizon 7.5. All these environments had UPD enabled and pointing to the exact same file server and share. This allowed the users to move from solution to solution and regardless of the environment they were logged in their UPD would follow them, bringing all their data (i.e. Outlook files), settings and preferences (including full roaming of the Windows start screen), what makes UPD completely agnostic. More than that, it allows for an easy migration from platform to platform, without losing any of the user data and eliminating the need to migrate these settings from one solution to another (i.e. from Citrix UPM to VMware UEM).

UPD Limitations

Even though UPD does provide an easy and fast way to address some Office 365 and profile management needs, it does have several limitations that may apply to your particular environment depending on your needs. The following table shows the main limitations seen with UPD as of September, 2018 (and on the Windows Server 2016/Windows 10 1803 releases).

Description	Limitations
Concurrent Access	As the VHDX file is mounted for the user upon logon, it cannot be mounted a second time while the user still has a session running on a particular server. If the user tries to connect to another machine while the UPD is in use, a temporary profile will be created on the second machine
Windows Search	When dealing with RDSH or pooled VMs (i.e. pooled Citrix Virtual Desktops), the index cache for Windows Search has to be recreated every single time a user logs in. As this is machine based, it does not work with UPDs. This is a critical piece of the puzzle as it directly affects search within Outlook. Depending on the mailbox size, the recreation of the cache alone may take a long time, severely impairing the end-user experience
OneDrive	Being able to handle the Outlook OST/NST files just solves part of the problem. Office 365 includes components like OneDrive. By default, the OneDrive cache is saved within the user profile and due to the technical implementation seen with UPDs (a junction point), OneDrive cannot use UPDs to store its cache
Platform Support	Officially UPDs are supported by Microsoft only. You may use it at your own risk with Citrix and VMware products
Migration Support	Out-of-the-box there is no way to migrate an existing user profile to an UPD based solution. That said, this could be potentially achieved using scripts but the effort required is certainly high
Mounting Mechanism	UPDs are mounted as a computer object what may not be ideal. Adding to that, it is just an NTFS file system junction, what many applications do not support (see OneDrive above)

Resiliency

UPDs must be available at all times, making it almost impossible to guarantee its availability. If the connection to the share is affected for any period of time, the user will immediately lose access to anything stored within the UPD

Overcoming UPD limitations

When compared to the technologies used in the past to deal with user profiles and everything that goes along these, UPD is certainly a huge improvement. Even though it does work well for many use cases, the lack of full Office 365 support poses a real challenge for enterprises that rely on the full Office 365 stack.

This is where FSLogix and its technologies come to the picture. To understand how it solves the UPD problem, let's take a quick look at what FSLogix has to offer and how these compare to UPDs.

- **FSLogix Profile Containers.** The full profile handling solution. It takes care of everything happening under the C:\Users\%username% folder. System folders (i.e. Desktop, Downloads, etc) are all there along all the user settings and preferences (i.e. registry, AppData, etc). As Office 365 components fall under these, everything related to it is therefore handled as part of the Profile Container.
- **FSLogix O365 Containers.** A subset of the Profile Containers solution, dealing exclusively with Office 365 components. This means everything outside Office 365 has to be managed using a complementary technology (i.e. Citrix UPM, Microsoft UPD, etc).

From a licensing perspective, if you do have an FSLogix Full Suite license, if Profile Containers is in use, all the Office 365 functionality will be there, working as expected. In case you only have the FSLogix Office 365 Containers license, then everything related to Office 365 specific settings/needs (i.e. Outlook caching, OneDrive support, etc) will be handled. That means, as explained above, you will have to use other solutions to handle the remaining parts of the user profile.

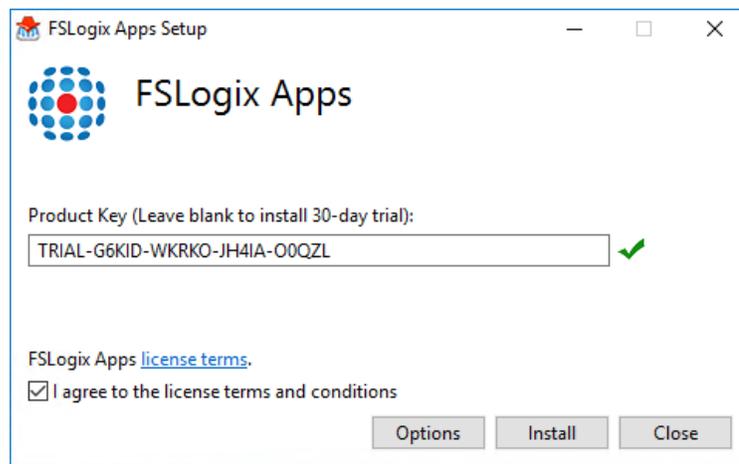
FSLogix Office 365 Containers with UPDs

The first use case is simple to understand. Imagine you already have UPD in place, working as expected for your particular case and you accept most of its shortcomings. But your users need to go that extra mile and now require full Office 365 support so they can access files on OneDrive, cache everything they have for OneNote and so on.

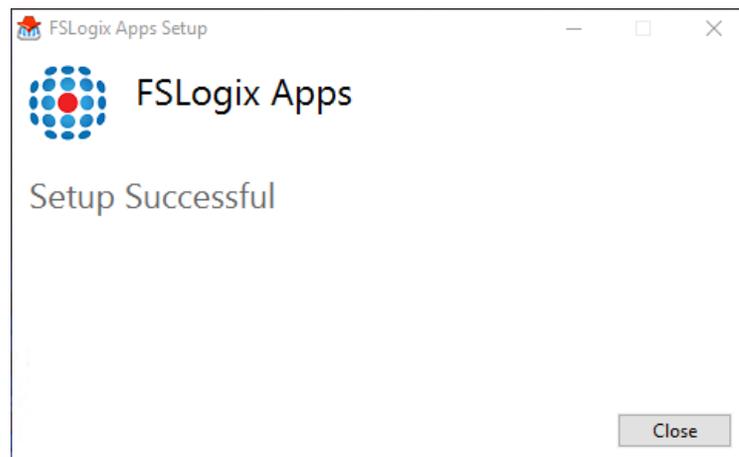
In this case, you can simply license the FSLogix Office 365 Containers and use UPD for everything else.

Let's take a look at how this is implemented and what the end result looks like.

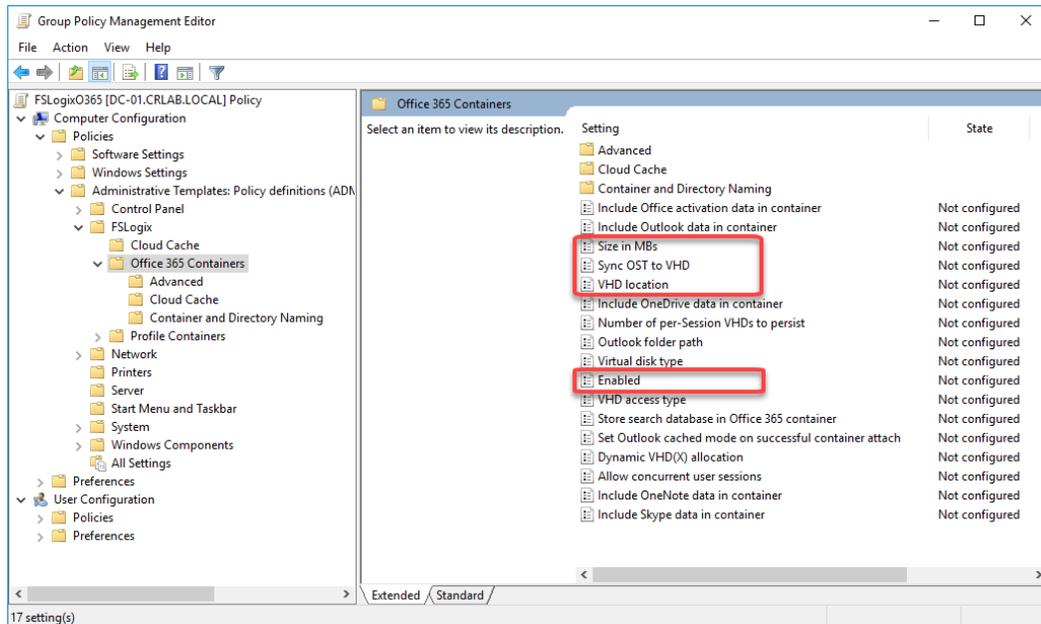
1. Go to <http://info.fslogix.com/request-an-evaluation> to get an evaluation license and download the FSLogix bits.
2. Once you download the software, on each machine hosting a desktop (RDSH or Windows desktop VM), launch FSLogixAppsSetup.exe. Accept the licensing terms and click 'Install'.



3. Within a few seconds the installation is done and no reboots are required. Click 'Close'.



4. Next step, if you do want to use GPOs to manage FSLogix, is to copy the required ADMX/ADML files to the machine where you use the Group Policy Management console:
 - a. FSLogix.ADMX to C:\Windows\PolicyDefinitions.
 - b. FSLogix.ADML to C:\Windows\PolicyDefinitions\en-US
5. Create a new GPO and link it to the right OU where your machines reside. At a minimum these must be set:



6. For this particular paper, we used the following:
 - a. Under 'Office 365 Containers'
 - Include Office activation data in container: enabled, checked.
 - Include Outlook data in container: enabled, checked.
 - Size in MBs: enabled, set to 4096 (4 GB)
 - Sync OST to VHD: enabled, 'Move OST to VHD'.
 - VHD location: enabled, set to '\\FILE_SERVER\FsLogix'
 - Include OneDrive data in container: enabled and checked.
 - Enabled: enabled, checked.
 - Store search database in Office 365 container: enabled, 'Multi-user search' (as this was tested on RDSH).
 - Set Outlook cached mode on successful container attach: enabled, checked.
 - Include OneNote data in container: enabled
 - Include Skype data in container: enabled

Note: the following permissions must be applied to the folder holding the share for FSLogix containers:

User Account	Folder	Permissions
CREATOR OWNER	Subfolders and Files Only	Full Control
SYSTEM	This Folder, Subfolders and Files	Full Control
Administrator	This Folder, Subfolders and Files	Full Control
Users	This Folder Only	Create Folder/Write Data
Users	This Folder Only	List Folder/Read Data
Users	This Folder Only	Read Attributes
Users	This Folder Only	Traverse Folder/Execute File

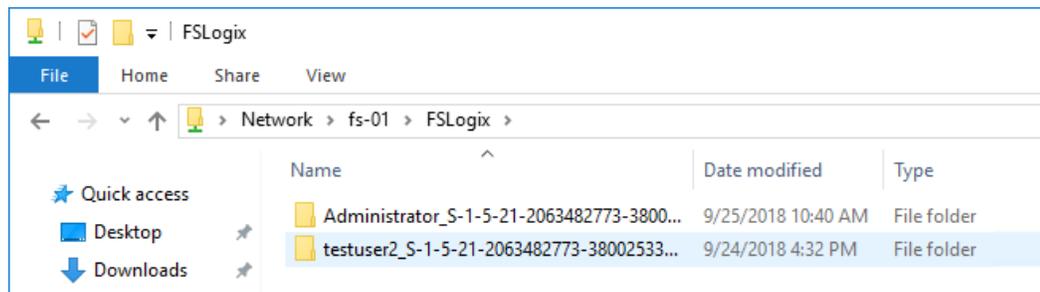
- b. Under 'Container and Directory Naming'.
 - Swap directory name components: enabled, checked.
7. As FSLogix is now handling all the Office 365 data, the UPD has to be adjusted not to interfere with FSLogix. More than that, it has to be configured to handle the 'Start' menu/screen as seen on Windows 10/Windows Server 2016. This is done by using a customized UvhdRoamingPolicy.xml file as shown below:

```

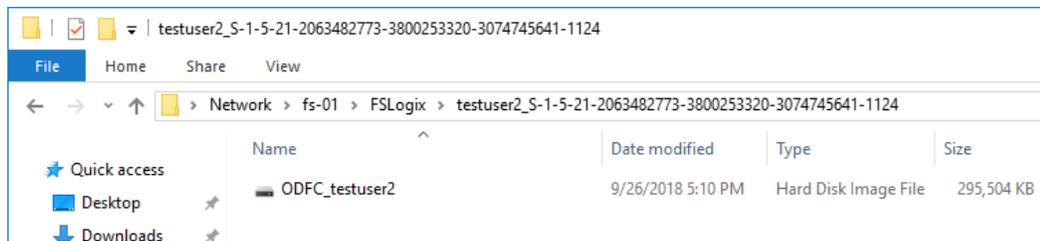
<UvhdRoamingPolicy>
  <RoamingMode>2</RoamingMode>
  <Include>
    <Folder>Contacts</Folder>
    <Folder>Desktop</Folder>
    <Folder>Documents</Folder>
    <Folder>Downloads</Folder>
    <Folder>Links</Folder>
    <Folder>Music</Folder>
    <Folder>Pictures</Folder>
    <Folder>AppData\Roaming</Folder>
    <Folder>AppData\Local\TileDataLayer</Folder>
    <Folder>AppData\Local\Microsoft\Windows\CloudStore</Folder>
    <Folder>AppData\Local\Microsoft\Windows\Caches</Folder>
    <Folder>AppData\Local\Microsoft\Windows\Explorer</Folder>
    <File>ntuser.dat</File>
    <File>ntuser.dat.LOG1</File>
    <File>ntuser.dat.LOG2</File>
  </Include>
</UvhdRoamingPolicy>

```

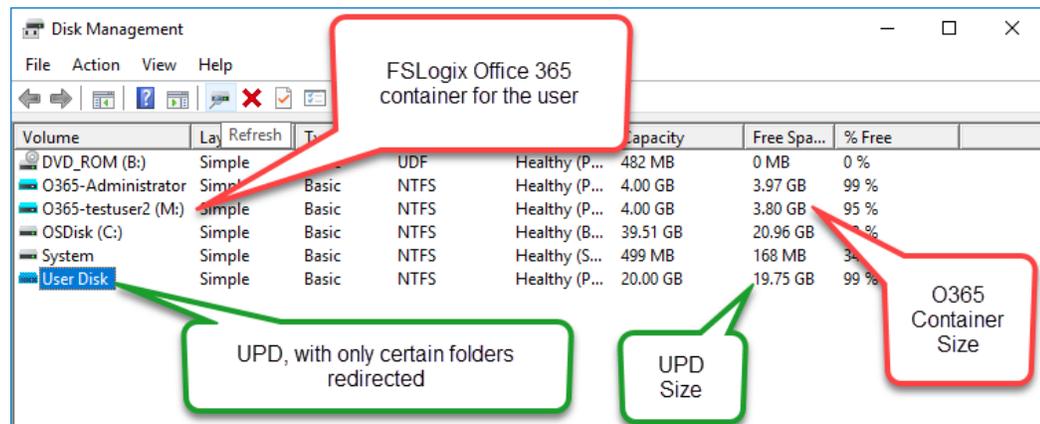
8. That is all you need done. Once a user logs in, under the 'VHD Location' set by policy, you will see the following:



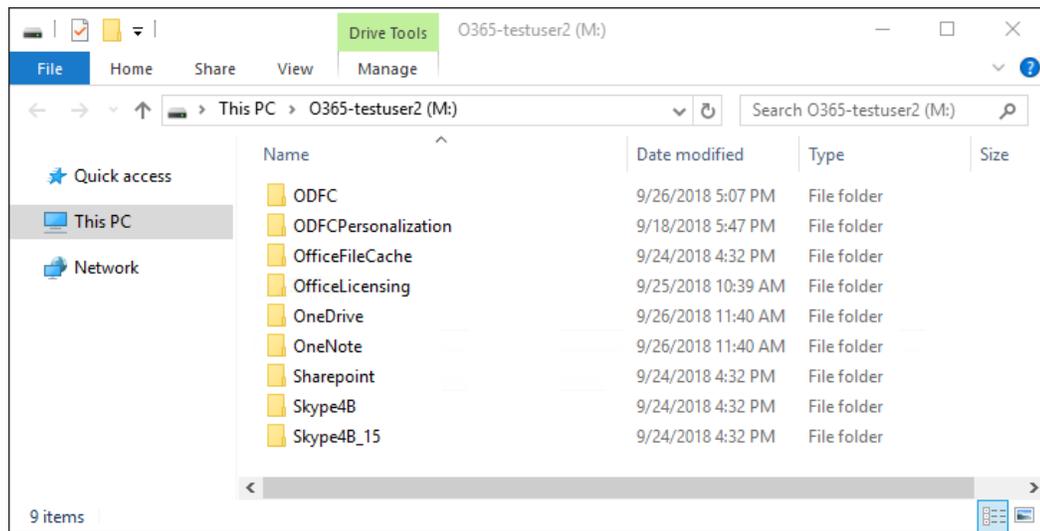
9. And inside each user's folder, the Office 365 container will be there:



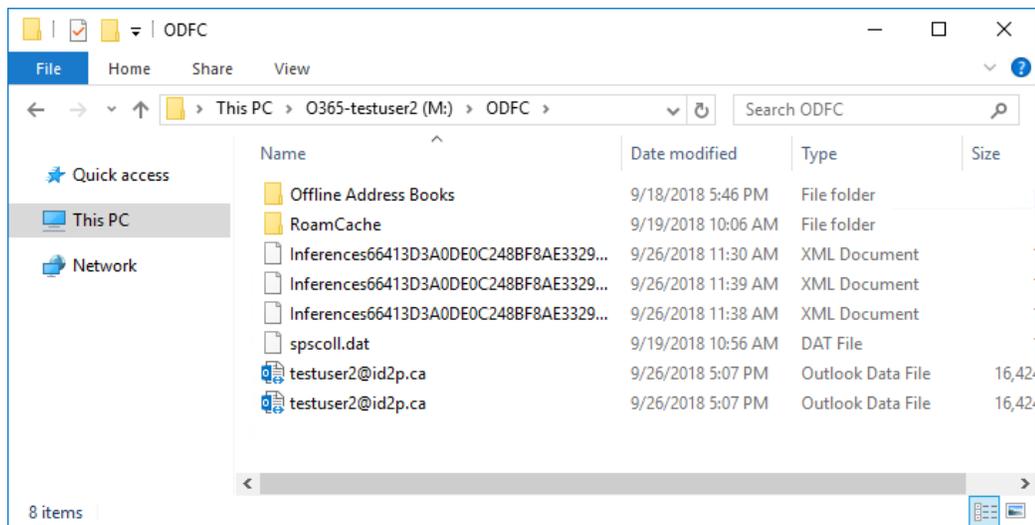
10. When logging in as an administrator to the same server where users have a running session, under 'Disk Management', after assigning a drive letter to the O365 container for a particular user, we can see the following:



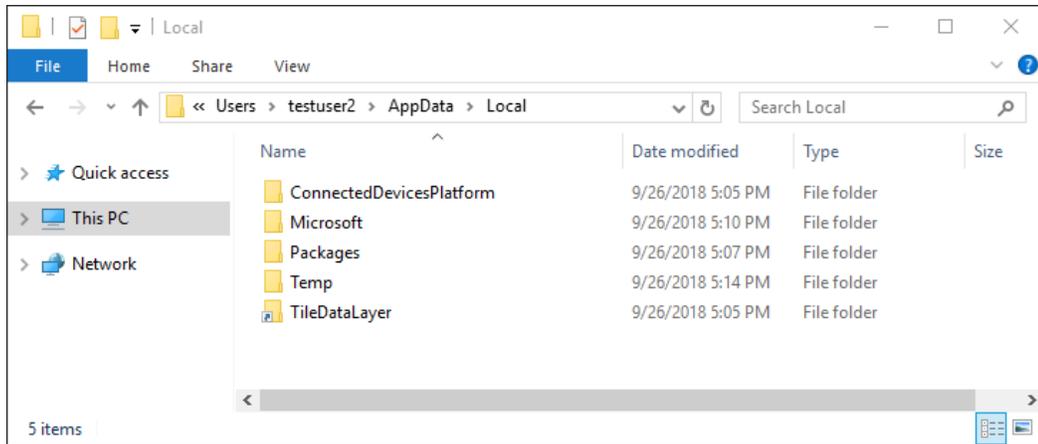
11. Looking inside the VHD files for FSLogix and the UPD we can clearly see what is saved for the user:



FSLogix O365 Container – note all the Office folders holding everything related to Office 365

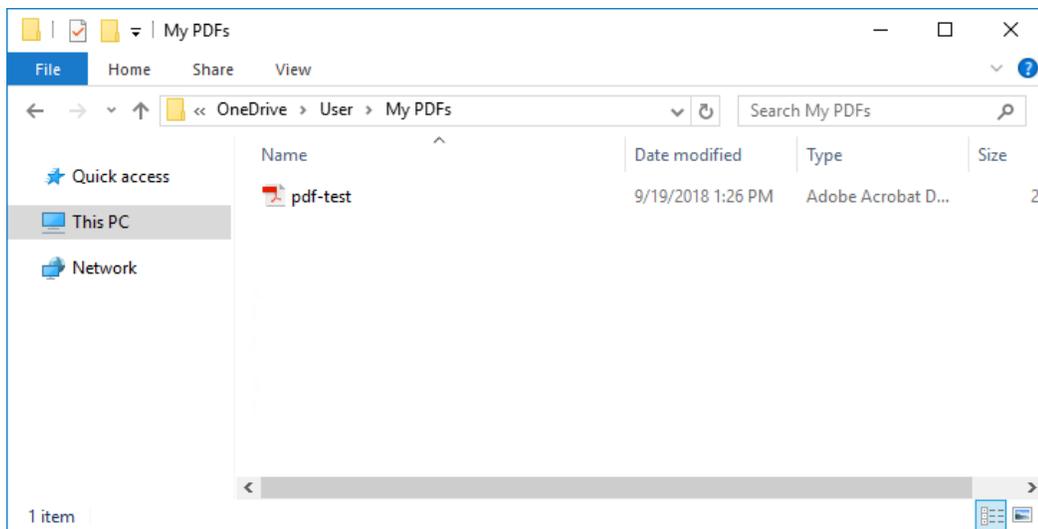


Outlook 2016 files, under the ODFC folder inside the FSLogix O365 Container

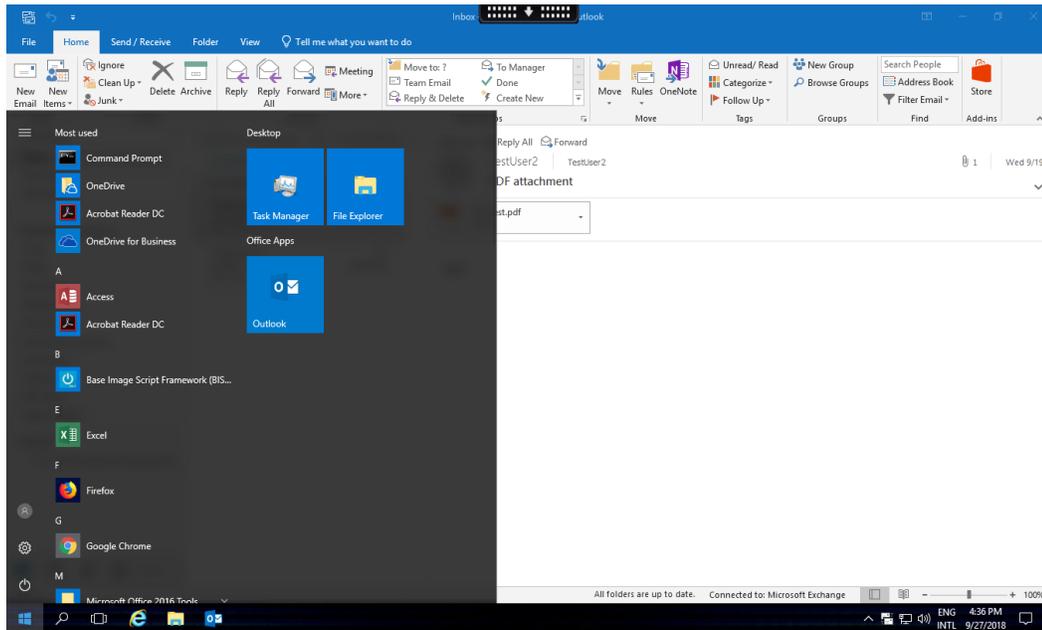


UPD, note the 'TileDataLayer' folder, storing the 'Star Menu' for the user under Windows Server 2016

12. As expected, OneDrive works properly, what fails during the configuration when only UPDs are in place.



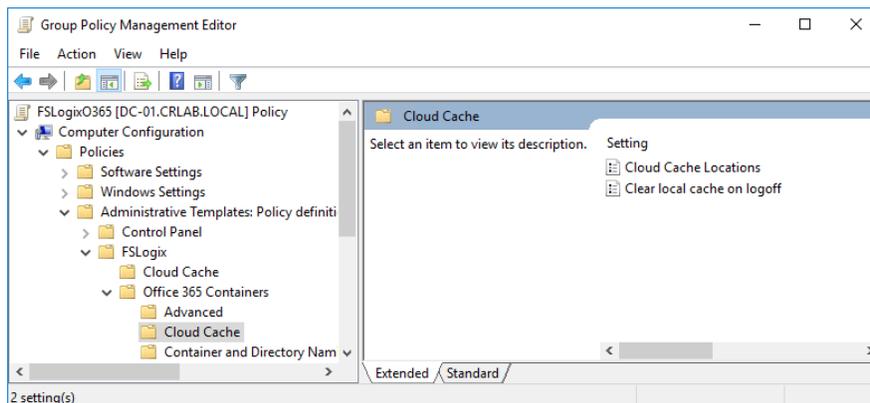
13. And our 'Start' menu is indeed available and roaming with the user, handled by the UPD.



A couple things to notice:

- Once a container (or even the UPD) size is set, the only way to resize it is using DISKPART. From an FSLogix perspective, changing the policy will only apply to new containers. Existing ones will have to be resized using the same mechanism.
- Additional folders can be added to the UPD by changing the UvhdRoamingPolicy.xml file accordingly.

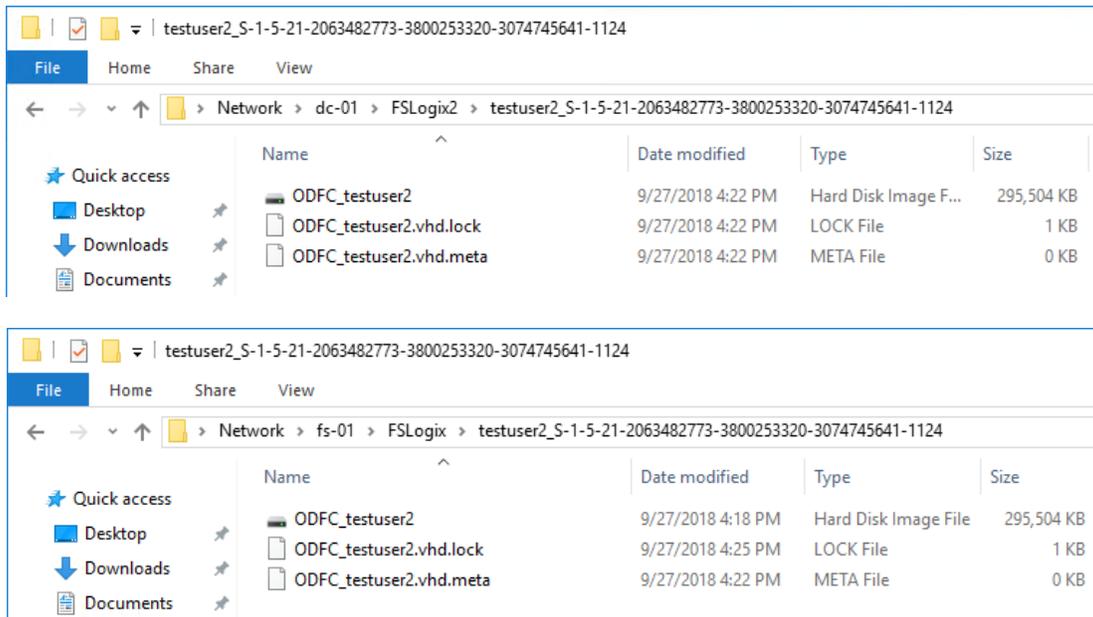
Unlike UPDs, FSLogix does allow you to set multiple locations for the VHD storage. This is the CloudCache feature. Its name comes from the fact it can indeed use cloud-based storage for the storage location (i.e. Azure) and in case the primary location fails, FSLogix gracefully falls back to another location as per its policy settings. The policy that controls this for the Office 365 containers is located under 'Computer Configuration' | 'Policies' | 'Administrative Templates' | 'FSLogix' | 'Office 365 Containers' | 'Cloud Cache'.



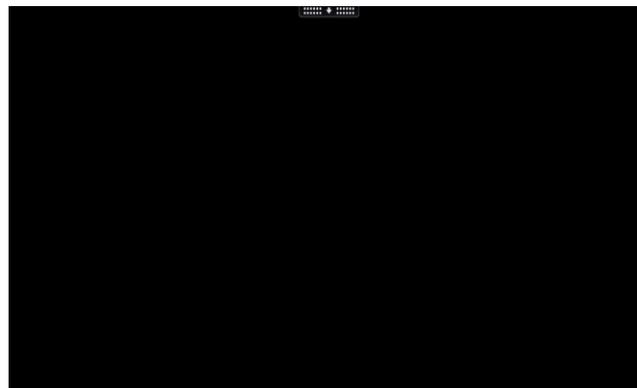
One thing to keep in mind is if you do use the 'Cloud Cache' setting, the 'VHD Location' must not be used. As a test, we removed the setting for the 'VHD Location' and used the following setting for the 'Cloud Cache Locations':

`"type=smb,connectionString=\\FS-01\FSLogix;type=smb,connectionString=\\DC-01\FSLogix"`

This basically means we are using two regular file servers (type=smb) and the location of the shares. After the user logs in, looking at both shares, we can now see the following:



This gives you full resiliency on the FSLogix Office 365 containers. Keep in mind, as we are still using UPDs for everything else, in case the share holding the UPDs is not available users will indeed get an error and will be presented with a nice black desktop as seen below:



If the solution in place must be available at all times, UPD is certainly not the way to go at this stage. Time to move from UPD to a full FSLogix containers solution.

FSLogix Containers – Full implementation

Even though UPD is certainly a vast improvement if compared to regular Windows Roaming Profiles, as we have seen previously, it still lacks features that may be required on your environment. The question here is quite simple. Do you need full resiliency for your profile solution and full Office 365 support? If that is the case, FSLogix is the only way to go.

With that in mind, let's take a look at how to address that final step and move our environment towards a full FSLogix solution.

As per the previous section, we implemented a solution that leverages FSLogix to handle the Office 365 applications while using Microsoft's UPD to deal with everything else (including roaming the 'Start' screen). Now the goal is to move everything to FSLogix, what means using FSLogix Profile Containers and Office 365 ones.

1. The first step is to remove UPDs from the environment. This is done by modifying the registry keys we highlighted previously (make sure you change the first one to 0 and the second one is blank, on all machines leveraging UPDs):

Windows Registry Editor Version 5.00

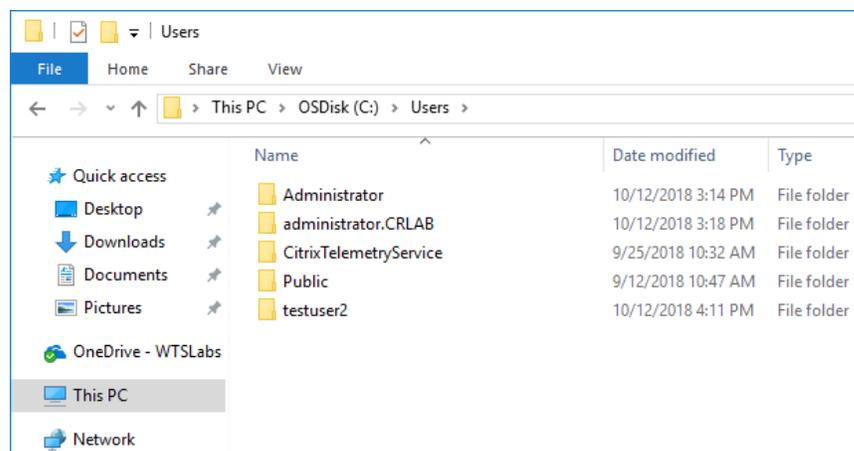
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\ClusterSettings]

"UvhdEnabled"=dword:00000000

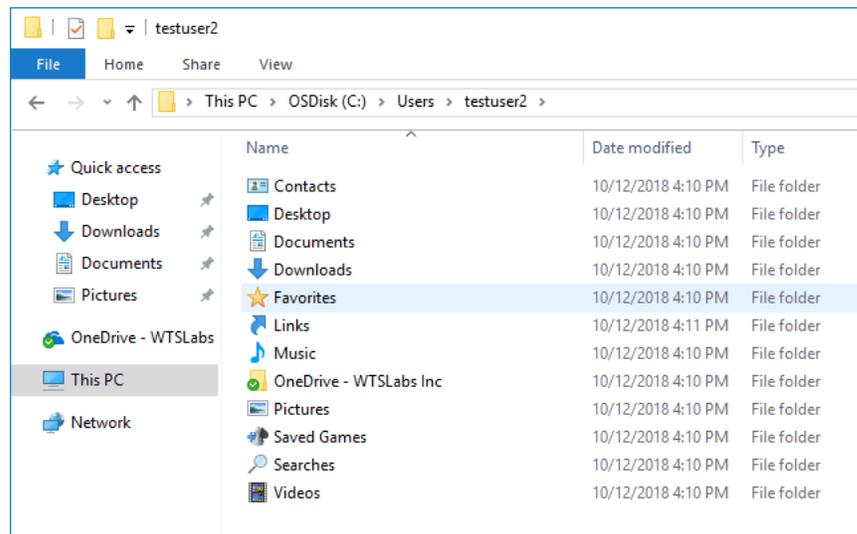
"UvhdShareUrl"=

"UvhdRoamingPolicyFile"="C:\\Windows\\RemotePackages\\RDFarm\\UvhdRoamingPolicy.xml"

2. Once this is done, reboot the server and logon as a regular user. Check the user profile under C:\Users and make sure it shows just a regular icon/folder.

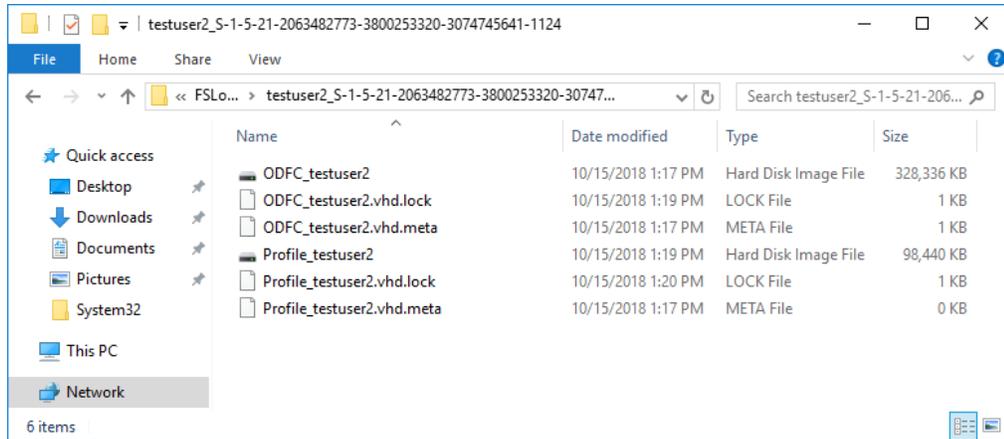


Note the folders that were previously redirected with a customized UvhdRoamingPolicy.xml file are no longer UPD-based.

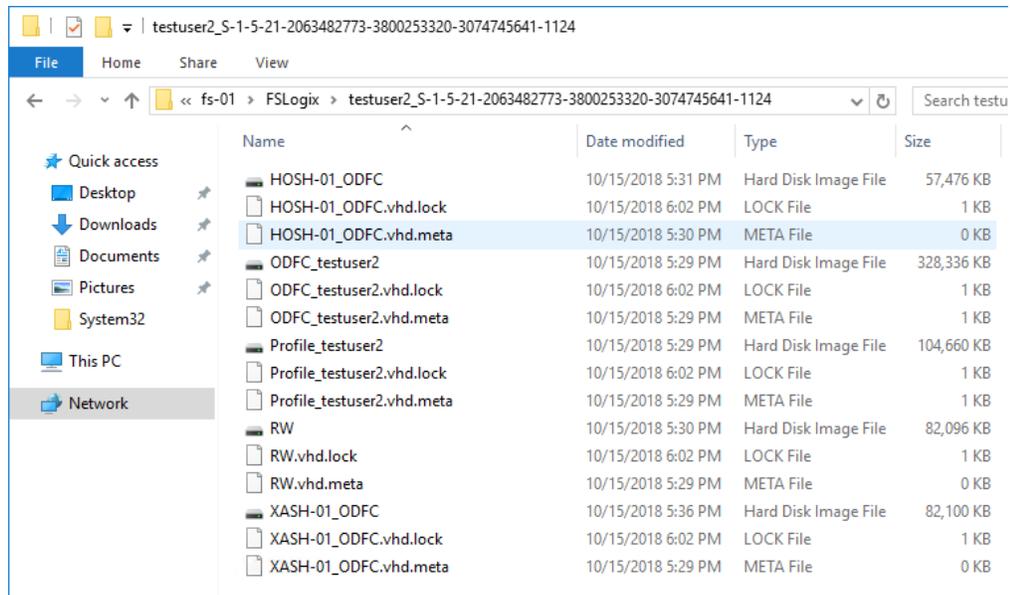


3. Next step is to enable the FSLogix Profile Containers. As with the Office 365 ones, this can be enabled using a simple GPO. In this case we will modify the GPO created previously when configuring the FSLogix Office 365 containers. These are the settings that must be enabled:
 - a. Under 'Profile Containers':
 - Enabled: enabled, checked.
 - Delete local profile when FSLogix Profile should apply: enabled, checked.
 - Size in MBs: enabled, set to 1024 (1 GB)
 - b. Under 'Cloud Cache':
 - Cloud Cache Locations: enabled, set to "type=smb,connectionString=\\FS-01\FsLogix;type=smb,connectionString=\\DC-01\FsLogix2".
 - c. Under 'Container and Directory Naming':
 - Swap directory name components: enabled, checked.

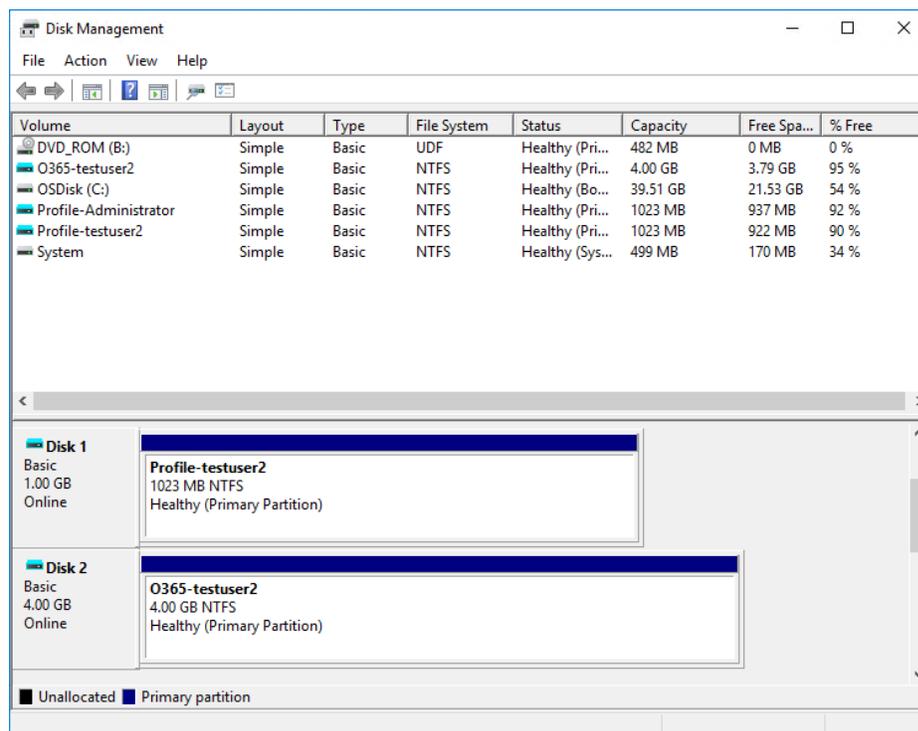
4. This is all that is required. Now, when logging in as any user to the machines that have the policy created applied, under the 'Cloud Cache Locations' defined above, you should see something similar to this:



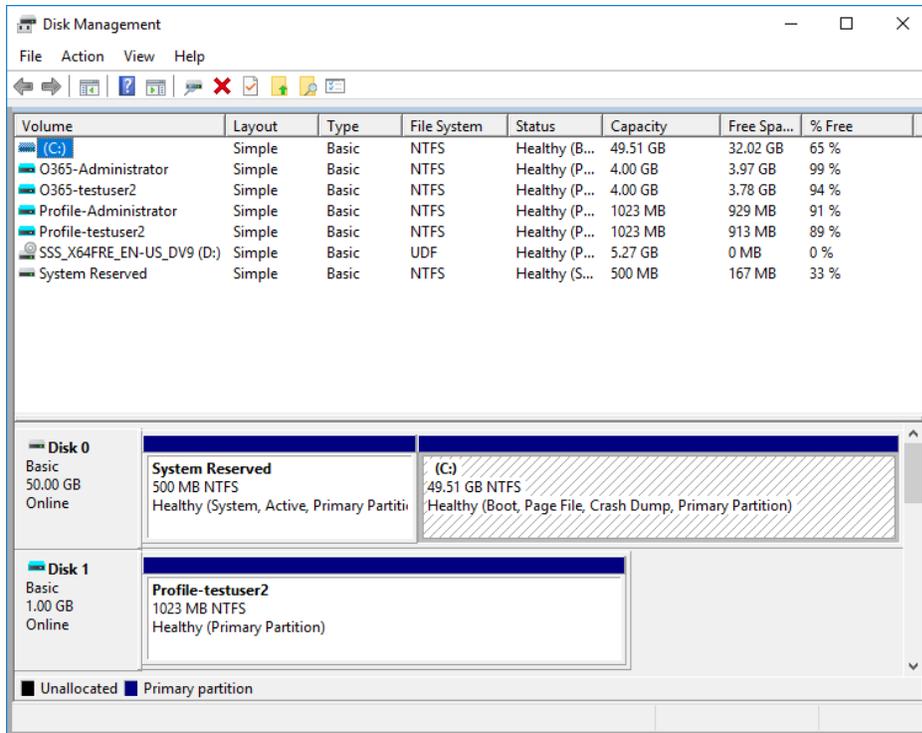
5. As seen above, now the user does have a VHD(x) based profile, handled by FSLogix and as expected, all the user settings, preferences (and the dreaded 'Start' screen) roam with the user now as part of the Profile_%username% container. The main difference is, unlike UPDs, in case the file server holding the containers fails, FSLogix seamlessly switches to the next location available as per the 'Cloud Cache Locations' setting and the user simply keeps working, with zero issues. And as with UPDs, FSLogix Containers are indeed agnostic, being able to work with all major platforms in the EUC space (Citrix Virtual Apps/Desktops, VMware Horizon, Microsoft RDS, Parallels RAS). As already pointed out, this greatly simplifies migrating user data from one solution to another. Also, FSLogix allows concurrent access to the VHDs, not limiting the user to a single connection, what may be a desired feature when running applications from multiple silos. In this case, two additional policies are required:
- Under 'Office 365 Containers'
 - VHD access type: enabled, 'Difference disk stored on network'.
 - Under 'Profile Containers'
 - Profile type: enabled, 'Try for read-write profile and fallback to read-only'.
6. With concurrent access enabled, when looking at the share storing the profiles, we can see VHD files showing the name of the machine where the user is logged in and a read-write file. These take care of the Office 365 and the regular profile container respectively, as seen below:



- When looking at the disks through 'Disk Management', everything is there as expected (these show the same user logged in, at the same time, to a Citrix Virtual Apps environment and to a VMware Horizon 7.5 one).

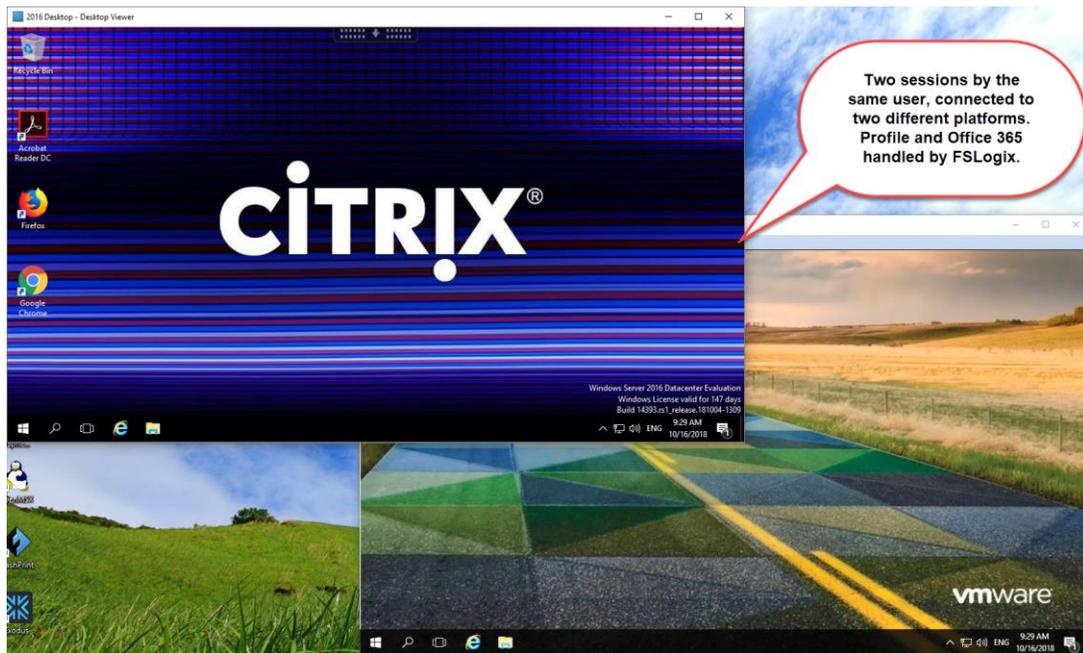


Citrix Virtual Apps - RDSH



VMware Horizon 7.5 - RDSH

The end result is the ability to connect to multiple systems, even running on different platforms, at the same time and with full support for Office 365 and full resiliency.



Conclusion

It is clear that Microsoft's UPD does address a need for better roaming profiles and in certain cases, may be all that you need. The main issue that still remains unsolved to this day is the complete lack of resiliency. Once the connection to the UPD is gone, there is no failsafe. Users lose access to everything they were potentially doing and a new session will have to be established (and the old one killed by technical support, creating a potential support nightmare). That of course assumes the connection to the UPD is now stable.

Another critical point that may cast a huge concern regarding UPDs is the fact that Microsoft, on its own solution, does not offer support for its biggest cloud product, Office 365. Two technologies from the same vendor that to this day, do not work together.

That said, not everyone needs full Office 365 support and full resiliency. If that is your case, UPD will almost certainly fulfill your needs.

Now, if full support for Office 365 is required and you do value peace of mind, knowing you have deployed a solution with built-in resiliency while being completely agnostic, FSLogix is indeed the only way to go as of today.

No other solution on the market, from any vendor, provides you with the same feature set available and more than that, can be transparently migrated to a completely new platform in case you decided to do so.