Microsoft

Desktop-as-a-Service (DaaS) using Windows Virtual Desktop (WVD)

Productivity Suite with O365 and FSLogix

Prepared for

Service Providers

Oct, 2019

Prepared by

Microsoft – **O**ne **C**ommercial **P**artner (OCP)

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Contents

1. Overview

This guide illustrates the required steps for implementing the Office 365 productivity suite, along with FSLogix to manage user profiles, upon persistent virtual desktops within the new Windows Virtual Desktop (WVD) Service in Microsoft Azure. In this walk-through, we'll create a new WVD tenant, configure a persistent desktop optimized for O365, and setup an FSLogix file-share.

Please be advised this information is provided to help understand/summarize this process and your enterprises` implementation may contain additional customizations and/or settings that ***might not*** be covered in this document.

2. Prerequisites

Azure & Windows Active Directory Prerequisites

Before getting started, **all** items listed below **must** be checked/validated to ensure the most basic requirements are in place to proceed with executing the remaining steps in this guide.

- An Azure Active Directory
- A Windows Server Active Directory in sync with Azure Active Directory. This can be enabled through:
  - Azure AD Connect
  - Azure AD Domain Services
- An Azure subscription, containing a virtual network that either contains or is connected to the Windows Server Active Directory

General Best Practices

Since everyone's business and technical requirements vary across the board, it is always a good idea to familiarize yourselves with the standard best practices across the different Azure technologies & services.

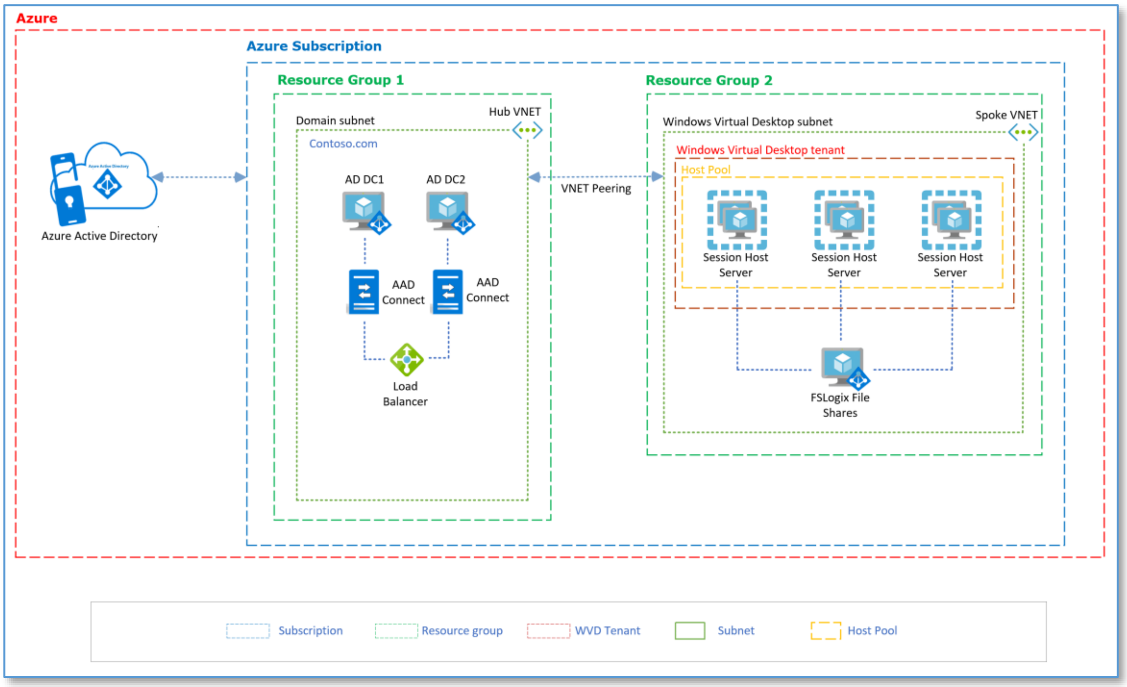
- Please follow the guidance here to maintain a consistent naming convention across your resources, unless you are already using a method.
- Azure security best practices and patterns
- Azure Active Directory Hybrid Identity best practices
- Azure identity management and access control security best practices
- Azure Networking & security Best Practices
- Azure Storage security overview
- Best practices for Azure VM security

Azure Networking

The recommendation is to design your Azure Networking using a Hub-Spoke topology. Consider the HUB like a DMZ deployed with your Virtual network Gateways and other security/edge appliances like Firewalls Etc. while the Spoke will act as the backend zone where your session hosts servers are deployed to and is peered with the HUB. This is our design for this walk-through, so you'll need this already setup before proceeding.

Azure Architectural Diagram

Below is a diagram of the Azure environment that we'll use. It shows the objects created in Azure and their relationships within the environment. In this example, the company name will be Contoso.



3. Creating a WVD Tenant

Creating a tenant in Windows Virtual Desktop Preview is the first step toward building your desktop virtualization solution. A tenant is a group of one or more host pools. Each host pool consists of multiple session hosts, running as virtual machines in Azure and registered to the Windows Virtual Desktop service.

Grant Azure Active Directory permissions to WVD

Granting permissions to the Windows Virtual Desktop service lets it query Azure Active Directory for administrative and end-user tasks. If you have already granted permissions to Windows Virtual Desktop for this Azure Active Directory instance, skip this section.

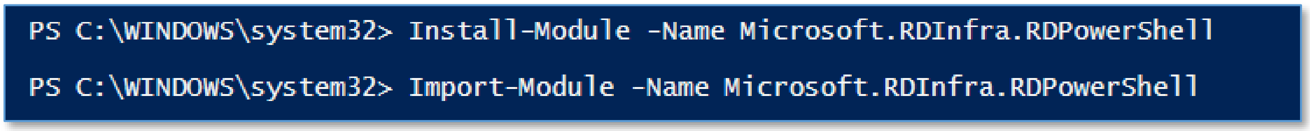
1. Open a browser and connect to the Windows Virtual Desktop consent page.
2. For **Consent Option** > **Server App**, enter the Azure Active Directory tenant name or Directory ID, and then select **Submit**.

   For Cloud Solution Provider customers, the ID is the customer's Microsoft ID from the Partner Portal. For Enterprise customers, the ID is located under **Azure Active Directory** > **Properties** > **Directory ID**.
3. Sign in to the Windows Virtual Desktop consent page with a global administrator account. For example, if you were with the Contoso organization, your account might be admin@contoso.com or admin@contoso.onmicrosoft.com.
4. Select **Accept**.
5. Wait for one minute.
6. Go back to the Windows Virtual Desktop consent page.
7. Go to **Consent Option** > **Client App**, enter the same Azure Active Directory tenant name or Directory ID, and then select **Submit**.
8. Sign in to the Windows Virtual Desktop consent page as global administrator, as you did in step 3.
9. Select **Accept**.

Create a WVD tenant

- Launch PowerShell as an Administrator and run the following commands. If prompted, select “Yes to all“:

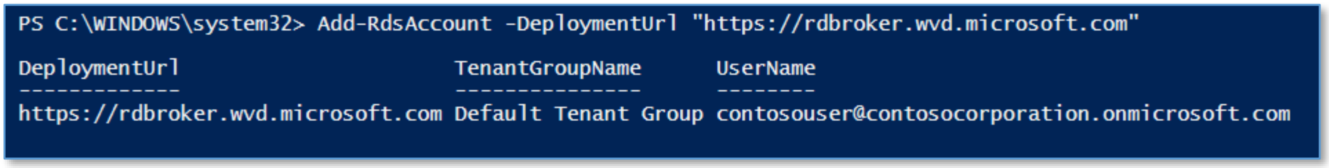
  ```
  Install-Module -Name Microsoft.RDInfra.RDPowerShell
  Import-Module -Name Microsoft.RDInfra.RDPowerShell
  ```



```
PS C:\WINDOWS\system32> Install-Module -Name Microsoft.RDInfra.RDPowerShell

PS C:\WINDOWS\system32> Import-Module -Name Microsoft.RDInfra.RDPowerShell
```

- Run the following command to sign into Windows Virtual Desktop using the TenantCreator user account

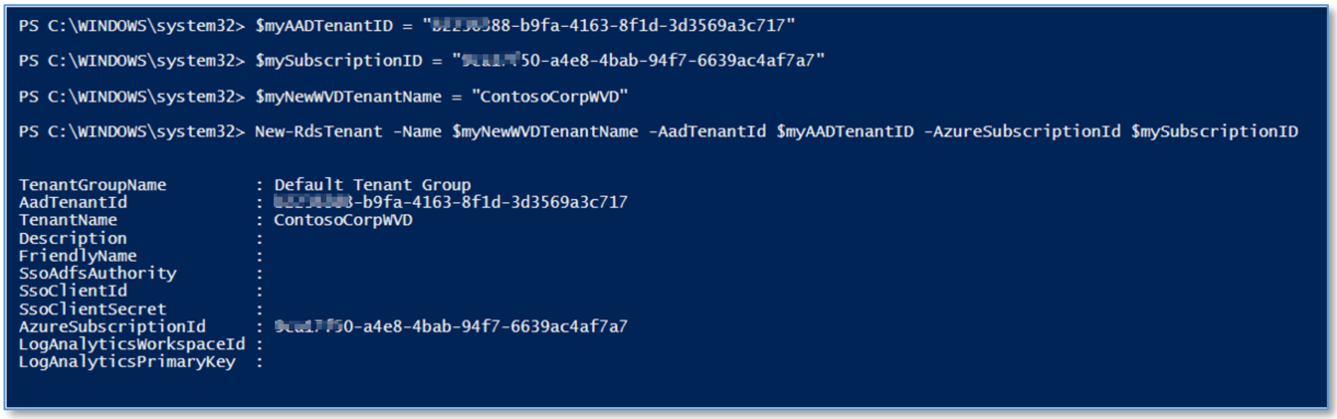
```
Add-RdsAccount -DeploymentUrl https://rdbroker.wvd.microsoft.com
```



```
PS C:\WINDOWS\system32> Add-RdsAccount -DeploymentUrl "https://rdbroker.wvd.microsoft.com"

DeploymentUrl                     TenantGroupName      UserName
-------------                     ---------------      --------
https://rdbroker.wvd.microsoft.com Default Tenant Group contosouser@contosocorporation.onmicrosoft.com
```

- Create a Windows Virtual Desktop tenant associated with the Azure Active Directory tenant:

```
$myAADTenantID = "12345678-b9fa-4163-8f1d-3d3569a3c717"

$mySubscriptionID = "abcd1234-a4e8-4bab-94f7-6639ac4af7a7"

$myNewWVDTenantName = "ContosoCorpWVD"

New-RdsTenant -Name $myNewWVDTenantName -AadTenantId $myAADTenantID -
AzureSubscriptionId $mySubscriptionID
```



```
PS C:\WINDOWS\system32> $myAADTenantID = "[redacted]88-b9fa-4163-8f1d-3d3569a3c717"

PS C:\WINDOWS\system32> $mySubscriptionID = "[redacted]50-a4e8-4bab-94f7-6639ac4af7a7"

PS C:\WINDOWS\system32> $myNewWVDTenantName = "ContosoCorpWVD"

PS C:\WINDOWS\system32> New-RdsTenant -Name $myNewWVDTenantName -AadTenantId $myAADTenantID -AzureSubscriptionId $mySubscriptionID


TenantGroupName          : Default Tenant Group
AadTenantId              : [redacted]-b9fa-4163-8f1d-3d3569a3c717
TenantName               : ContosoCorpWVD
Description              :
FriendlyName             :
SsoAdfsAuthority         :
SsoClientId              :
SsoClientSecret          :
AzureSubscriptionId      : [redacted]50-a4e8-4bab-94f7-6639ac4af7a7
LogAnalyticsWorkspaceId :
LogAnalyticsPrimaryKey   :
```

Assign a WVD tenant security principal

A user account must be assigned a role within Windows Virtual Desktop to facilitate automation of management and deployment task. If the User has MFA enabled, then it is required to create a Service Principal in Azure Active directory.

In our example, we're creating a service principal for that purpose. All these commands must be run within the same PowerShell session, in "run as administrator" mode:

- First, in PowerShell, install the AzureAD module, if you haven't already, by running:

```
Install-Module AzureAD
Import-Module AzureAD
```

- Modify the parameters below to add the Azure Active Directory Tenant ID and run:

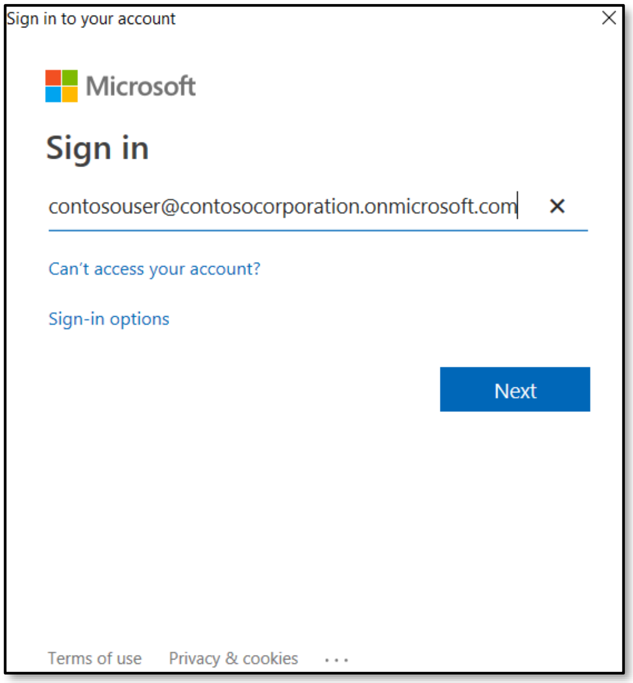
```
$myAADTenantID = "12345678-b9fa-4163-8f1d-3d3569a3c717"
```

- Run this WVD tenant name parameter:

```
$myNewWVDTenantName = "ContosoCorpWVD"
```

- Logon to Azure:

```
$aadContext = Connect-AzureAD -TenantID $myAADTenantID
```



Sign in to your account

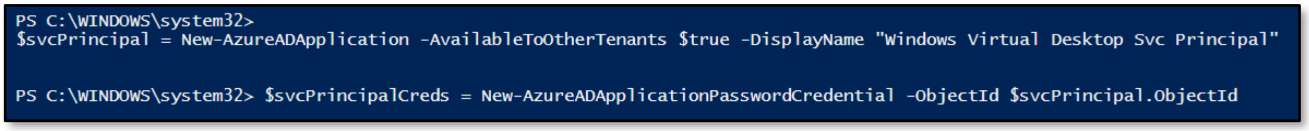
Microsoft

Sign in

contosouser@contosocorporation.onmicrosoft.com

- Create the service principal:

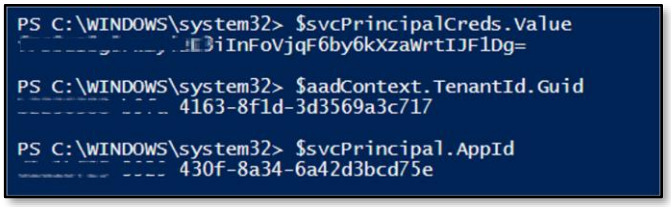
```
$svcPrincipal = New-AzureADApplication -AvailableToOtherTenants $true -
DisplayName "Windows Virtual Desktop Svc Principal"

$svcPrincipalCreds = New-AzureADApplicationPasswordCredential -ObjectId
$svcPrincipal.ObjectId
```



```
PS C:\WINDOWS\system32>
$svcPrincipal = New-AzureADApplication -AvailableToOtherTenants $true -DisplayName "Windows Virtual Desktop Svc Principal"

PS C:\WINDOWS\system32> $svcPrincipalCreds = New-AzureADApplicationPasswordCredential -ObjectId $svcPrincipal.ObjectId
```

- Run below PS commands to obtain the service principals ID and password. Store them somewhere safe. Once the PowerShell session has ended, they cannot be obtained:

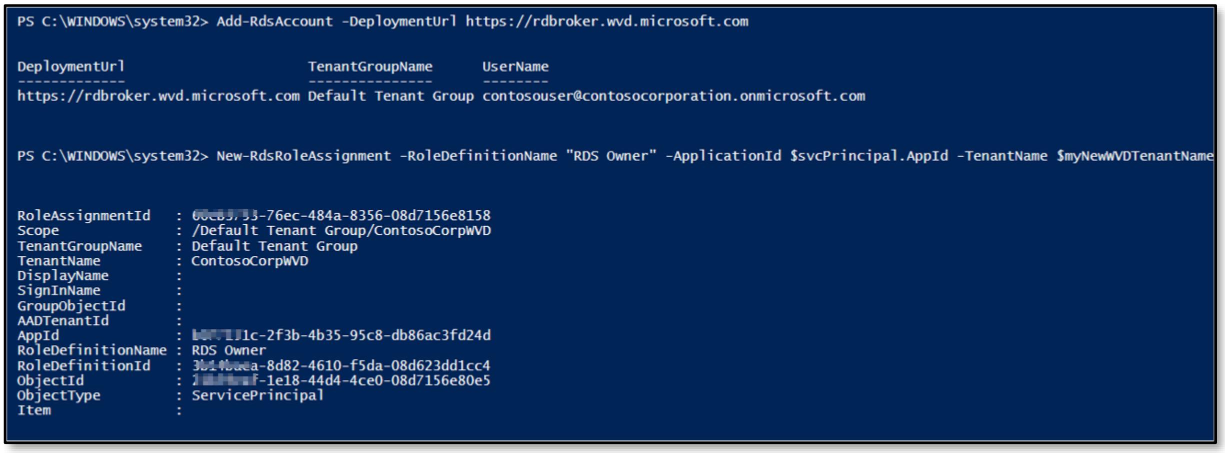
```
#Password
$svcPrincipalCreds.Value

#Tennant id
$aadContext.TenantId.Guid

#Application id
$svcPrincipal.AppId
```



```
PS C:\WINDOWS\system32> $svcPrincipalCreds.Value
[redacted]iInFoVjqF6by6kXzaWrtIJF1Dg=

PS C:\WINDOWS\system32> $aadContext.TenantId.Guid
[redacted] 4163-8f1d-3d3569a3c717

PS C:\WINDOWS\system32> $svcPrincipal.AppId
[redacted] 430f-8a34-6a42d3bcd75e
```

- Assign the Tenant Creator role to the service principal:

```
Add-RdsAccount -DeploymentUrl https://rdbroker.wvd.microsoft.com

New-RdsRoleAssignment -RoleDefinitionName "RDS Owner" -ApplicationId
$svcPrincipal.AppId -TenantName $myNewWVDTenantName
```



```
PS C:\WINDOWS\system32> Add-RdsAccount -DeploymentUrl https://rdbroker.wvd.microsoft.com


DeploymentUrl                    TenantGroupName      UserName
-------------                    ---------------      --------
https://rdbroker.wvd.microsoft.com Default Tenant Group contosouser@contosocorporation.onmicrosoft.com


PS C:\WINDOWS\system32> New-RdsRoleAssignment -RoleDefinitionName "RDS Owner" -ApplicationId $svcPrincipal.AppId -TenantName $myNewWVDTenantName


RoleAssignmentId   : [redacted]-76ec-484a-8356-08d7156e8158
Scope              : /Default Tenant Group/ContosoCorpWVD
TenantGroupName    : Default Tenant Group
TenantName         : ContosoCorpWVD
DisplayName        :
SignInName         :
GroupObjectId      :
AADTenantId        :
AppId              : [redacted]1c-2f3b-4b35-95c8-db86ac3fd24d
RoleDefinitionName : RDS Owner
RoleDefinitionId   : [redacted]a-8d82-4610-f5da-08d623dd1cc4
ObjectId           : [redacted]-1e18-44d4-4ce0-08d7156e80e5
ObjectType         : ServicePrincipal
Item               :
```

4. Deploying Windows Virtual Desktops

Follow the steps in this section to create a host pool within the Windows Virtual Desktop tenant using an O365-optimized, multi-session VM. This includes creating a host pool in Windows Virtual Desktop, creating a resource group with VMs in an Azure subscription, joining those VMs to the Active Directory domain, and registering the VMs with Windows Virtual Desktop.

Create a Windows 10 Enterprise multi-session host pool using an ARM template

Host pools are a collection of one or more identical virtual machines within a Windows Virtual Desktop tenant environment. Each host pool can contain an app group that users can interact with as they would on a physical desktop.

You may also create a host pool via the portal using these instructions

Run the WVD Host Pool Provisioning PowerShell ARM template:

4.1 Browse to the GitHub repository here and select **Deploy to Azure**
4.2 Update the following parameters ONLY, leaving all others at default settings:

- **Resource group** = "RG-ContosoWVD"
- **Rdsh Number Of Instances** = 2
- **Domain To Join** = "Contoso.com"
- **Existing Domain UPN** = "adAdmin@contoso.com" (This UPN must have appropriate permissions to join the virtual machines to the domain and organizational unit)
- **Existing Domain Password** = "CoNtOsOpW" (password to the account above)
- **Existing Vnet Name** = "HUB-VNET"
- **Existing Subnet Name** = "Spoke-VNET"
- **Virtual Network Resource Group Name** = "RG-ContosoWVD" (the appropriate ResourceGroup Name where the VNET exists)
- **Existing Tenant Name** = "ContosoWVD" (Provide the WVD Tenant name created earlier)
- **Host Pool Name** = "HP-PD-W10ENT" (name based on what purpose the hostpool will serve. In this example the hostpool is a collection of Win 10 Enterprise multi-session.)
- **Enable Persistent Desktop** = true
- **Tenant Admin Upn Or Application Id**= "12345678-1234-1234-1234-123456789012" (If you are creating a new host pool, this principal must be assigned either the RDS Owner or RDS Contributor role at the tenant scope (or higher). If you are registering these virtual machines to an existing host pool, this principal must be assigned either the RDS Owner or RDS Contributor role at the host pool scope (or higher))

WARNING! You cannot enter a UPN that requires MFA to successfully authenticate. If you do, this template will create the virtual machines but fail to register them to a host pool.

- **Tenant Admin Password** = “…sPubjyKQ80C7Qq…” (password for above account)
- **Is Service Principal** = true (Default is false. Set to true if you are providing an ApplicationId for TenantAdminUpnorApplicationId AND providing the respective ServicePrincipal Key for TenantAdminPassword.) *We are in this example*.

4.3 Execute the ARM template by pressing the **Purchase** button.

4.4 Once deployment completes, we will validate the newly created host pool. Open PS and connect to the WVD tenant using below commands:

```
$module = "C:\temp\RDPowershell"
$TenantGroupName = “Default Tenant Group”

$brokerURL= “https://rdbroker.wvd.microsoft.com”
Import-Module $module\Microsoft.RDInfra.RDPowershell.dll
Add-RdsAccount -DeploymentUrl $brokerURL
Set-RdsContext -TenantGroupName $TenantGroupName
```

4.5 Check for the new Host Pool using below command:

```
$TenantName = “ContosoWVD”
Get-RdsHostPool -TenantName $TenantName
```

4.6 Check for the Session hosts in the Host Pool and ensure the status is **Available**

```
$HostPoolName = “HP1”
Get-RdsSessionHost -TenantName $TenantName `
-HostPoolName $HostPoolName
```

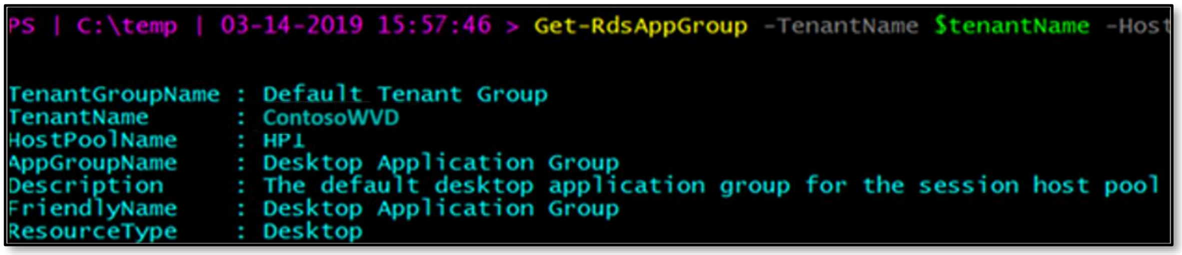
5. Managing App Groups

A default app group is automatically created for a new host pool that publishes the full desktop. In addition, you can create one or more application groups for the host pool. Host pools should be named so that it is easy to know what desktop types they contain. For example, if the host pool will host Windows 10 Multi-session VMs, then a name such as RDP-W10-MS would be a good choice.

In this section, we will create a RemoteApp AppGroup and publish individual Start menu apps.

Verify that the Default Desktop Application Group is created using below command:

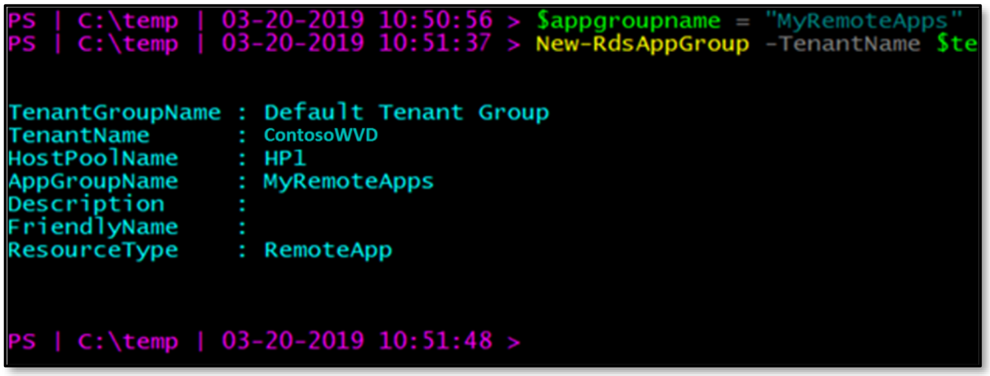
```
Get-RdsAppGroup -TenantName $TenantName -HostPoolName $HostPoolName
```



```
PS | C:\temp | 03-14-2019 15:57:46 > Get-RdsAppGroup -TenantName $tenantName -Host

TenantGroupName : Default Tenant Group
TenantName      : ContosoWVD
HostPoolName    : HP1
AppGroupName    : Desktop Application Group
Description     : The default desktop application group for the session host pool
FriendlyName    : Desktop Application Group
ResourceType    : Desktop
```

5.1 Now run the following PowerShell cmdlet to create a new empty RemoteApp group

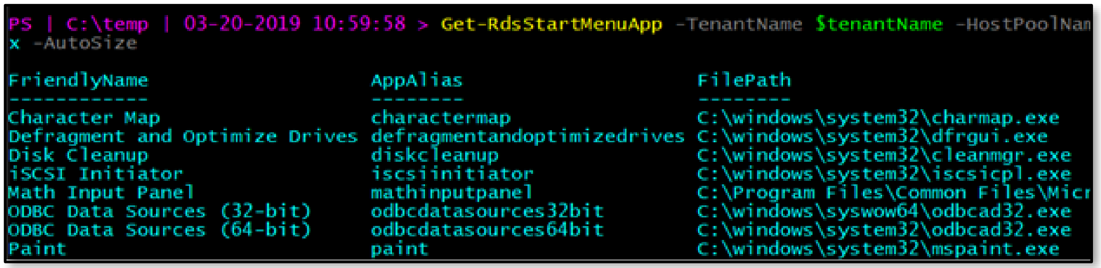
```
$appgroupname = “MyRemoteApps”
New-RdsAppGroup -TenantName $TenantName `
-HostPoolName $HostPoolName -Name $AppGroupName `
-ResourceType “RemoteApp”
```



```
PS | C:\temp | 03-20-2019 10:50:56 > $appgroupname = "MyRemoteApps"
PS | C:\temp | 03-20-2019 10:51:37 > New-RdsAppGroup -TenantName $te

TenantGroupName : Default Tenant Group
TenantName      : ContosoWVD
HostPoolName    : HP1
AppGroupName    : MyRemoteApps
Description     :
FriendlyName    :
ResourceType    : RemoteApp


PS | C:\temp | 03-20-2019 10:51:48 >
```

5.2 Run the following cmdlet to see a list of start menu apps available on the host pool's virtual machine image.

```
Get-RdsStartMenuApp -TenantName $TenantName `
-HostPoolName $HostPoolName `
-appgroupname $AppGroupName | FT `
FriendlyName,AppAlias,FilePath,IconPath,IconIndex -AutoSize
```

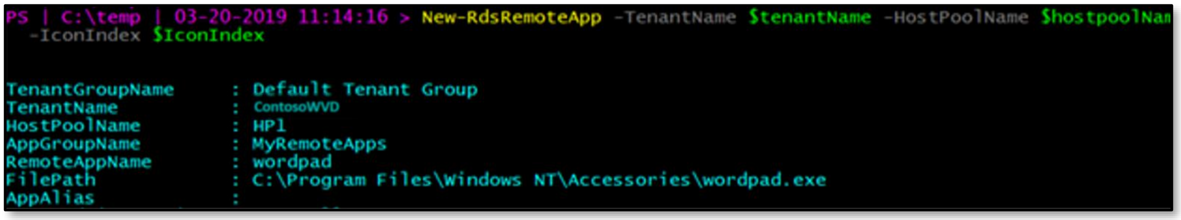


```
PS | C:\temp | 03-20-2019 10:59:58 > Get-RdsStartMenuApp -TenantName $tenantName -HostPoolNam
x -AutoSize

FriendlyName                    AppAlias                          FilePath
------------                    --------                          --------
Character Map                   charactermap                      C:\windows\system32\charmap.exe
Defragment and Optimize Drives  defragmentandoptimizedrives       C:\windows\system32\dfrgui.exe
Disk Cleanup                    diskcleanup                       C:\windows\system32\cleanmgr.exe
iSCSI Initiator                 iscsiinitiator                    C:\windows\system32\iscsicpl.exe
Math Input Panel                mathinputpanel                    C:\Program Files\Common Files\Micr
ODBC Data Sources (32-bit)      odbcdatasources32bit              C:\windows\syswow64\odbcad32.exe
ODBC Data Sources (64-bit)      odbcdatasources64bit              C:\windows\system32\odbcad32.exe
Paint                           paint                             C:\windows\system32\mspaint.exe
```

5.3 Run the following cmdlet to publish a new WordPad RemoteApp to the application group. Using the values listed from the step before, run again for each app you want to publish.

```
$AppAlias = “wordpad”
$FilePath = “C:\Program Files\Windows NT\Accessories\wordpad.exe”
$IconPath = “C:\Program Files\Windows NT\Accessories\wordpad.exe”
$IconIndex = 0
```

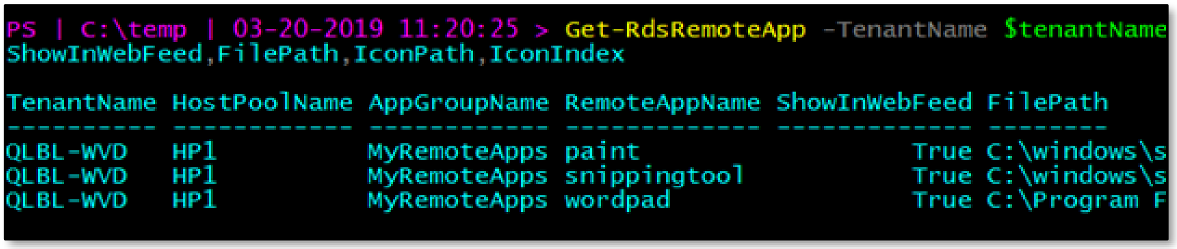
```
New-RdsRemoteApp -TenantName $TenantName -HostPoolName $HostPoolName `
-appgroupname $AppGroupName -Name $AppAlias -Filepath $FilePath `
-IconPath $IconPath -IconIndex $IconIndex
```



```
PS | C:\temp | 03-20-2019 11:14:16 > New-RdsRemoteApp -TenantName $tenantName -HostPoolName $hostpoolNam
  -IconIndex $IconIndex


TenantGroupName       : Default Tenant Group
TenantName            : ContosoWVD
HostPoolName          : HP1
AppGroupName          : MyRemoteApps
RemoteAppName         : wordpad
FilePath              : C:\Program Files\Windows NT\Accessories\wordpad.exe
AppAlias              :
```

5.4 To verify that the app was published, run the following cmdlet.

```
Get-RdsRemoteApp -TenantName $tenantName -HostPoolName $hostpoolName `
-AppGroupName $appgroupname | FT `
IconIndex,RemoteAppName,TenantName,HostPoolName,AppGroupName,ShowInWebFeed
```



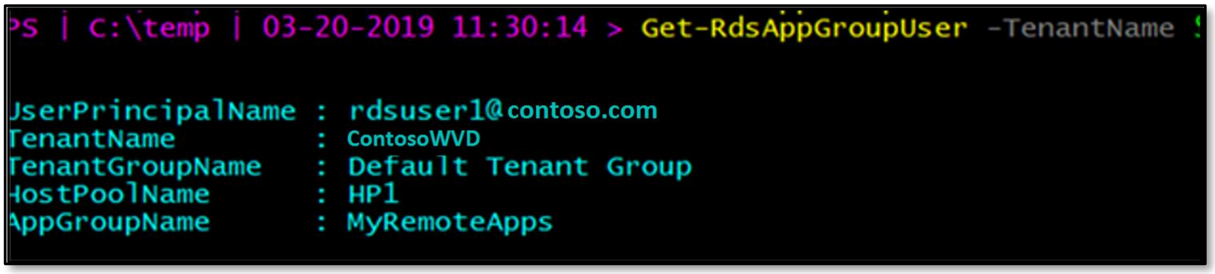
```
PS | C:\temp | 03-20-2019 11:20:25 > Get-RdsRemoteApp -TenantName $tenantName
ShowInWebFeed,FilePath,IconPath,IconIndex

TenantName HostPoolName AppGroupName RemoteAppName ShowInWebFeed FilePath
---------- ------------ ------------ ------------- ------------- --------
QLBL-WVD   HP1          MyRemoteApps paint                  True C:\windows\s
QLBL-WVD   HP1          MyRemoteApps snippingtool           True C:\windows\s
QLBL-WVD   HP1          MyRemoteApps wordpad                True C:\Program F
```

5.5 Run the following cmdlet to grant users access to the remote apps in the app group:

```
$AppGroupName = “MyRemoteApps”
$upn = “rdsuser1@contoso.com”
Add-RdsAppGroupUser -TenantName $TenantName -HostPoolName $HostPoolName `
-AppGroupName $AppGroupName -UserPrincipalName $upn
```

Verify that the ACL has been applied using:

```
Get-RdsAppGroupUser -TenantName $TenantName `
-HostPoolName $HostPoolName -AppGroupName $AppGroupName
```



```
PS | C:\temp | 03-20-2019 11:30:14 > Get-RdsAppGroupUser -TenantName $


UserPrincipalName  : rdsuser1@contoso.com
TenantName         : ContosoWVD
TenantGroupName    : Default Tenant Group
HostPoolName       : HP1
AppGroupName       : MyRemoteApps
```

6. FSLogix configuration for WVD

For persistent desktops, the Windows Virtual Desktop service offers FSLogix containers as the recommended user profile solution. The traditional windows user profile disk (UPD) solution is not recommended and will be deprecated in future versions of Windows Virtual Desktop.

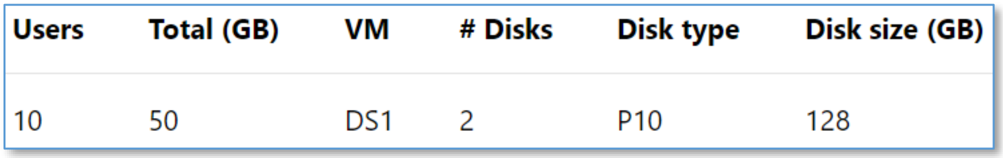
Scale Out File Server (SOFS) with Storage Spaces Direct (S2D)

Scale out File server (SOFS) with Storage Spaces Direct (S2D) is the recommended storage solution in Azure to host user profiles.

NOTE: The Windows Virtual Desktop (WVD) service offers FSLogix containers as the recommended user profile solution. The user profile disk (UPD) solution is not recommended and will be deprecated in future versions of Windows Virtual Desktop.

Based on the total # of users and their profile size requirements, first plan for the SOFS cluster size and SKU requirements in Azure using these guidelines

For the purposes of this PoC, we'll choose the first configuration offered:



Users	Total (GB)	VM	# Disks	Disk type	Disk size (GB)
10	50	DS1	2	P10	128

Run the SOFS Provisioning PowerShell ARM template:

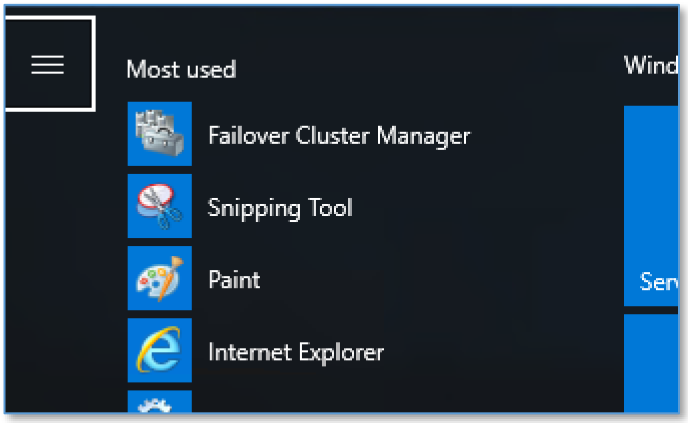
6.1 Browse to the GitHub repository here and select **Deploy to Azure**
6.2 Update the following parameters ONLY, leaving all others at default settings:

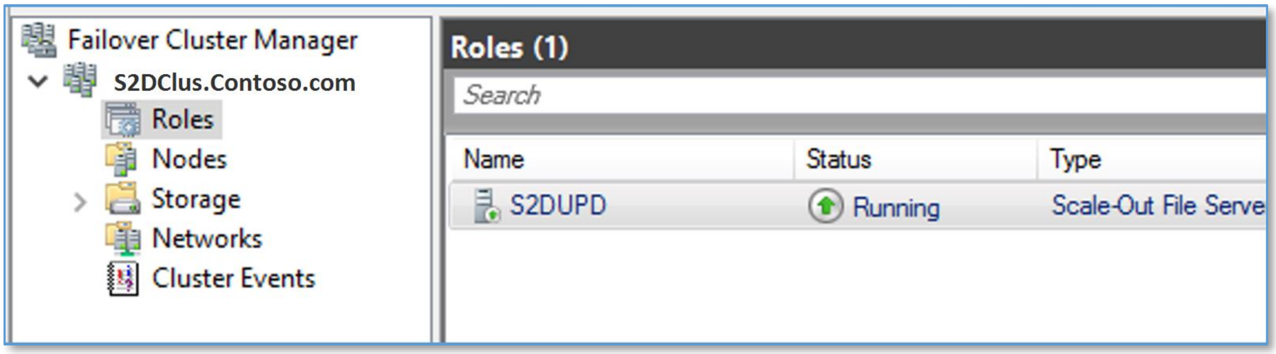
- **Resource group** = "RG-ContosoWVD"
- **Name Prefix** = "S2D-" (Naming prefix for each new resource created)
- **Existing Domain Name**= "contoso.com" (Active Directory DNS name)
- **Admin Username**= "adAdmin@Contoso.com" (AD admin)
- **Admin Password**= "CoNtOsOpW"
- **Existing Virtual Network RG Name**= "RG-ContosoWVD"
- **Existing Virtual Network Name**= "VNET1"
- **Existing Subnet Name**= "SN-WVD"

6.3 Execute the ARM template by pressing the **Purchase** button.

After the CSV file shares are created to host user profile data, the correct NTFS and Share permissions must be applied **on each share** for data security & integrity using the steps below.

6.4 Logon to any of the file server nodes and click Start > Failover cluster manager > expand cluster > Click roles > Click S2DUPD Role

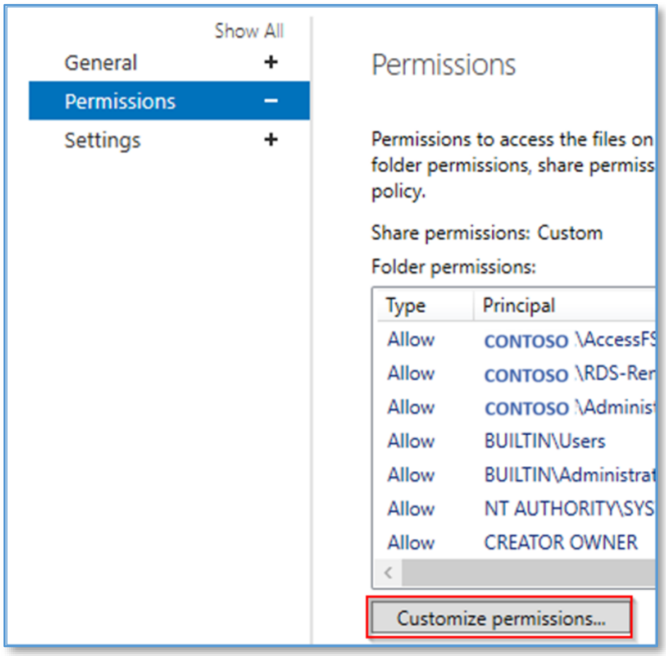




Name	Status	Type
S2DUPD	Running	Scale-Out File Serve

6.5 Now click Shares at the bottom > Right click the Share (Ex: RemoteApps) > click properties

6.6 In the new window > click permissions > customize permissions:



Show All

General +

Permissions −

Settings +

Permissions

Permissions to access the files on
folder permissions, share permiss
policy.

Share permissions: Custom

Folder permissions:

Type	Principal
Allow	CONTOSO \AccessFS
Allow	CONTOSO \RDS-Rer
Allow	CONTOSO \Adminis
Allow	BUILTIN\Users
Allow	BUILTIN\Administrat
Allow	NT AUTHORITY\SYS
Allow	CREATOR OWNER

6.7 Now let’s set the NTFS Permissions. In the new window, ensure you are under the Permissions tab > click **Add**

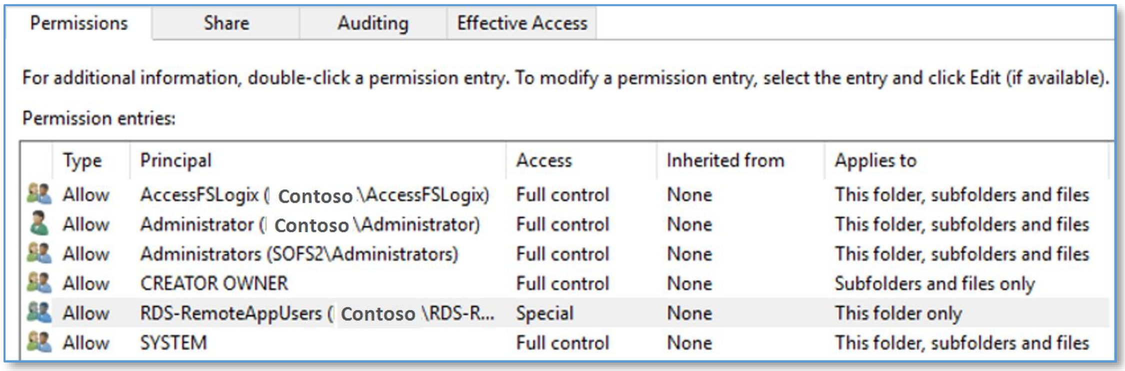
6.8 Click Select a principal > Select the respective AD object we want to set permissions > click **ok** > Set Type = Allow > Applies To = value under Folder in the table below > Click Show advanced permissions and select respective values from Permissions column below:

User Account	Description	Folder	Permissions
CREATOR OWNER	CREATOR OWNER	Subfolders and Files Only	Full Control
SYSTEM	SYSTEM	This Folder, Subfolders and Files	Full Control
Domain Administrators	Your Domain Administrator AD Security Group	This Folder, Subfolders and Files	Full Control
File cluster Administrators	The local File cluster Administrator	This Folder, Subfolders and Files	Full Control
Domain\AccessFSLogix	AD Security group containing Session Host computer objects that can access/control these shares to store ser profile data	This Folder, Subfolders and Files	Full Control
Domain\RDS-RemoteAppUsers	The AD security group containing	This Folder Only	Create Folder/Write Data List Folder/Read Data

	users that use RemoteApps		Read Attributes Traverse Folder/Execute File

6.9 Repeat step 5 for all other objects (in the above table) you need to set permissions for

6.10 Once done, your NTFS permissions window should look relative to below. Now click Apply



For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	AccessFSLogix (Contoso \AccessFSLogix)	Full control	None	This folder, subfolders and files
Allow	Administrator (Contoso \Administrator)	Full control	None	This folder, subfolders and files
Allow	Administrators (SOFS2\Administrators)	Full control	None	This folder, subfolders and files
Allow	CREATOR OWNER	Full control	None	Subfolders and files only
Allow	RDS-RemoteAppUsers (Contoso \RDS-R...	Special	None	This folder only
Allow	SYSTEM	Full control	None	This folder, subfolders and files

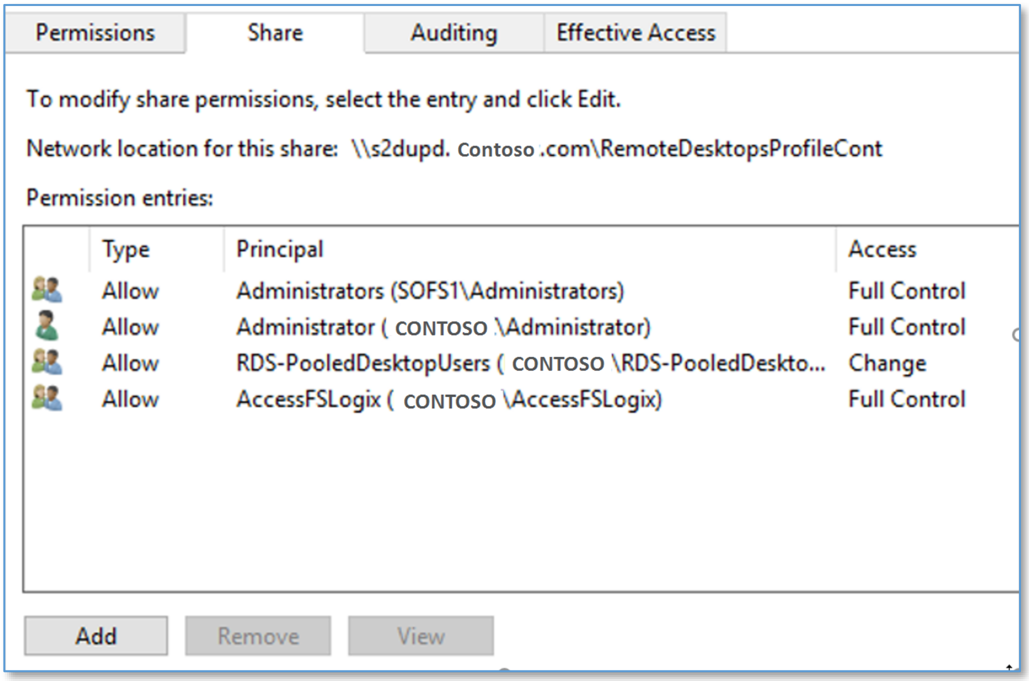
6.11 Now we will set Share permissions. Click on Share at the top > click Add

6.12 Click **Select a principal** & select the AD object we want to set permissions.

6.13 Click **ok** & Set Type = **Allow**, Permissions = value from Permissions column below:

User Account	Description	Permissions
Domain Administrators	Your Domain Administrator AD Security Group	Full Control
File cluster Administrators	The local File cluster Administrator	Full Control
Domain\AccessFSLogix	AD Security group containing Session Host computer objects that can access/control these shares to store ser profile data	Full Control
Domain\RDS-RemoteAppUsers	The AD security group containing users that use RemoteApps	Change

6.14 Once done, your Share permissions window should look relative to below. Now click Apply



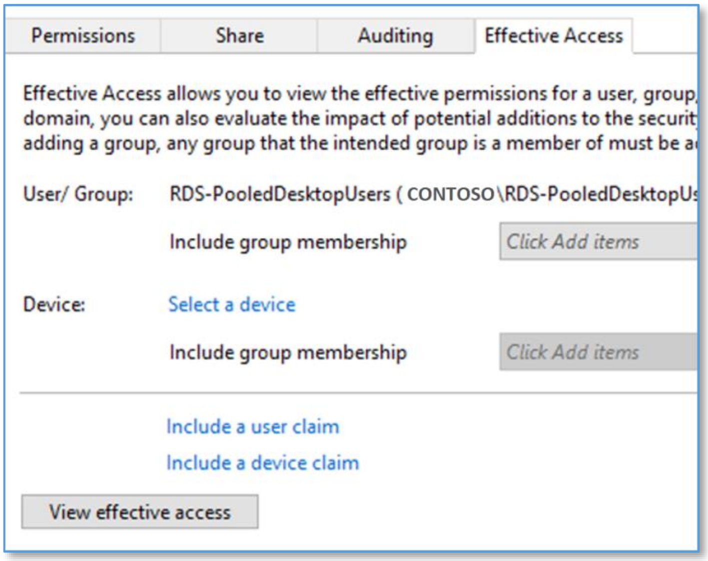
To modify share permissions, select the entry and click Edit.

Network location for this share: \\s2dupd. Contoso .com\RemoteDesktopsProfileCont

Permission entries:

Type	Principal	Access
Allow	Administrators (SOFS1\Administrators)	Full Control
Allow	Administrator (CONTOSO \Administrator)	Full Control
Allow	RDS-PooledDesktopUsers (CONTOSO \RDS-PooledDeskto...	Change
Allow	AccessFSLogix (CONTOSO \AccessFSLogix)	Full Control

6.15 Validate the required users have access by doing the following. Click Effective access at the top > click Select User, choose respective Security Group OR user, click ok > click effective access > scroll down and ensure the minimum access to list/read/write files & folders is present.



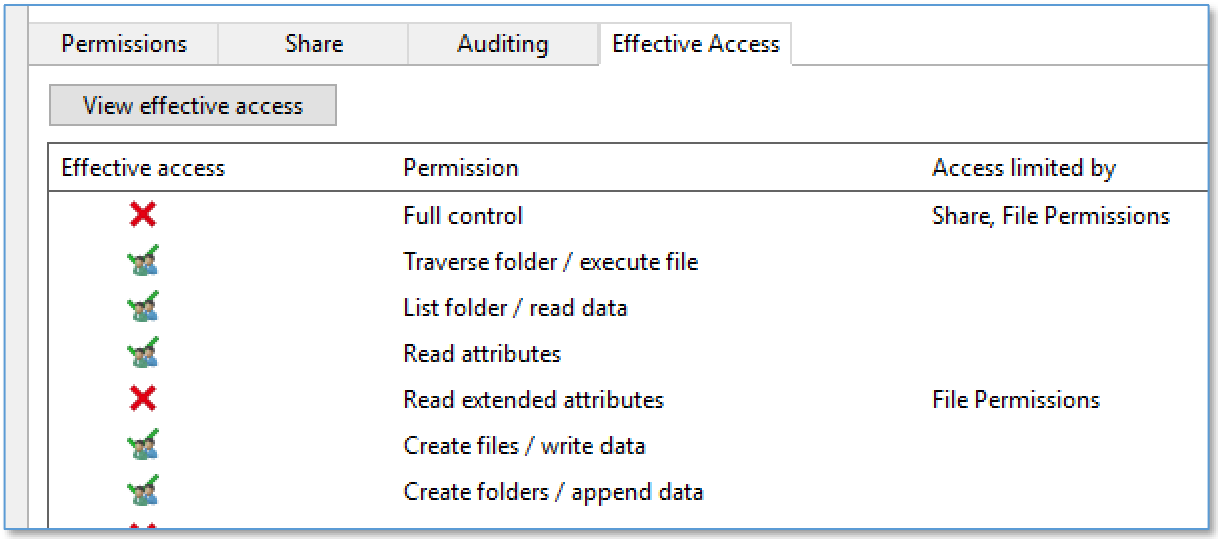
Effective Access allows you to view the effective permissions for a user, group, domain, you can also evaluate the impact of potential additions to the securit adding a group, any group that the intended group is a member of must be a

User/ Group: RDS-PooledDesktopUsers (CONTOSO\RDS-PooledDesktopU

Include group membership Click Add items

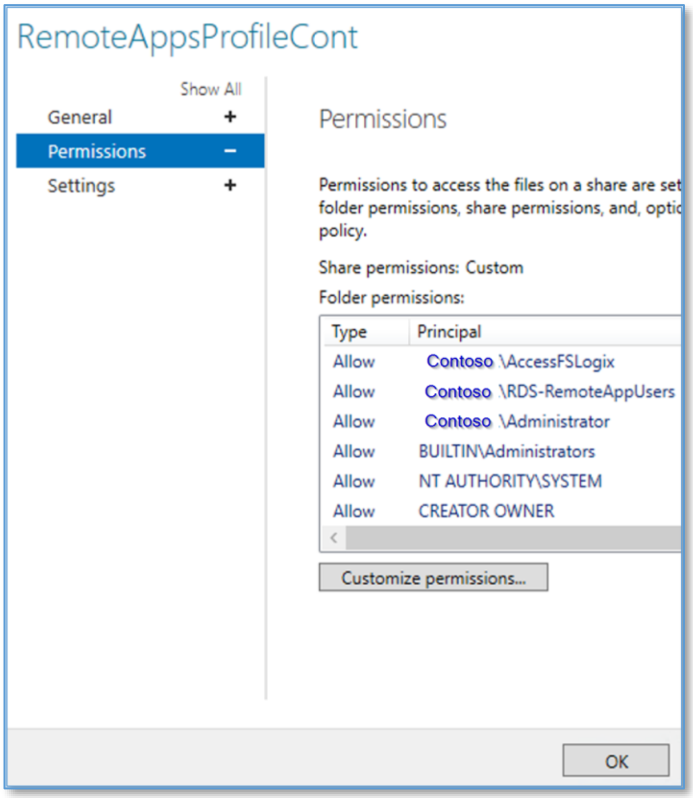
Device: Select a device

Include group membership Click Add items



Effective access	Permission	Access limited by
✗	Full control	Share, File Permissions
✓	Traverse folder / execute file	
✓	List folder / read data	
✓	Read attributes	
✗	Read extended attributes	File Permissions
✓	Create files / write data	
✓	Create folders / append data	

6.16 Click OK > again OK in the Properties window to save your changes:



Permissions

Permissions to access the files on a share are set folder permissions, share permissions, and, optic policy.

Share permissions: Custom

Folder permissions:

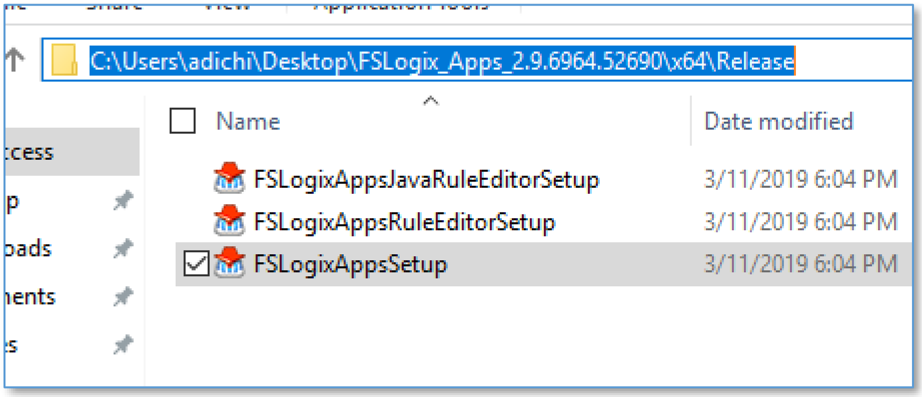
Type	Principal
Allow	Contoso \AccessFSLogix
Allow	Contoso \RDS-RemoteAppUsers
Allow	Contoso \Administrator
Allow	BUILTIN\Administrators
Allow	NT AUTHORITY\SYSTEM
Allow	CREATOR OWNER

6.17 Repeat from step 8.2 for any other shares created for storing user profile data in Azure.

Installing FSLogix on Session Hosts

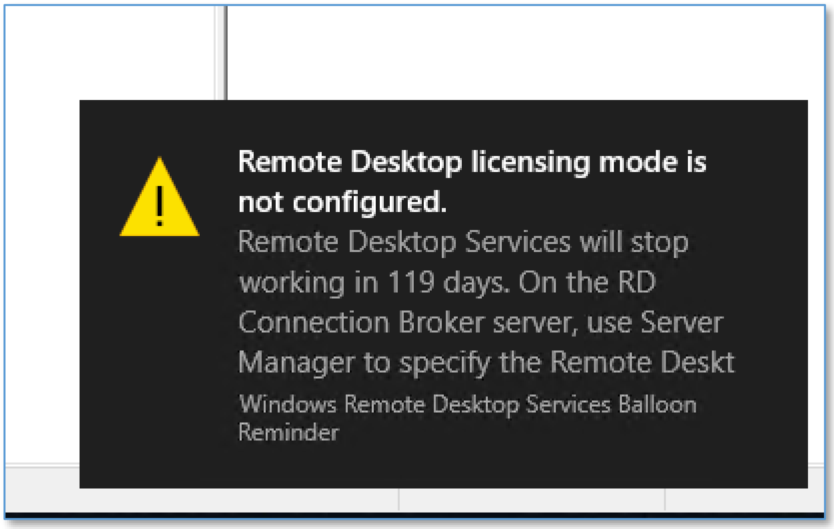
Get a copy of the FSLogix Apps from either your Microsoft or FSlogix representative.

6.18 From your WVD Host pool in Azure, login to one of the session hosts using an administrator account and copy the FSLogix bits locally.
Please ignore the RDLicensing warning at this time



C:\Users\adichi\Desktop\FSLogix_Apps_2.9.6964.52690\x64\Release

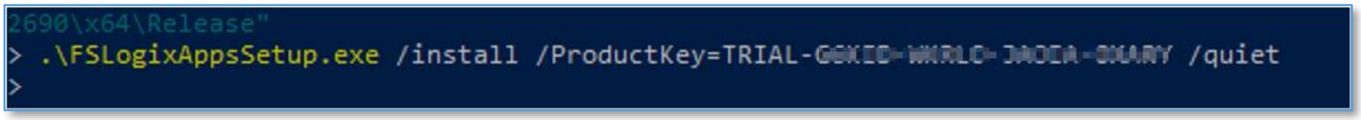
Name	Date modified
FSLogixAppsJavaRuleEditorSetup	3/11/2019 6:04 PM
FSLogixAppsRuleEditorSetup	3/11/2019 6:04 PM
☑ FSLogixAppsSetup	3/11/2019 6:04 PM



Remote Desktop licensing mode is not configured.
Remote Desktop Services will stop working in 119 days. On the RD Connection Broker server, use Server Manager to specify the Remote Deskt
Windows Remote Desktop Services Balloon Reminder

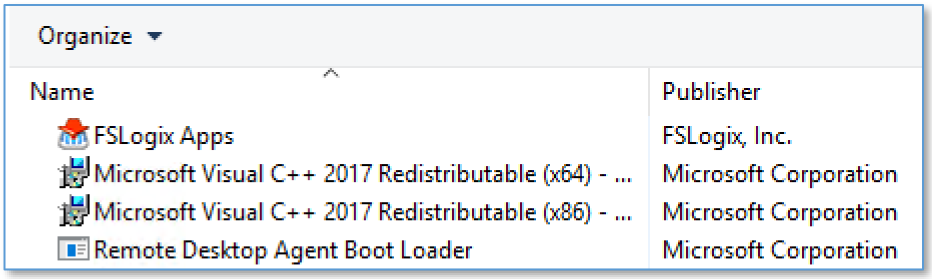
6.19 CD to the path where you copied > open PS > run the below command AND replace the Product key with the licensed one you obtained either directly from FSLogix or Microsoft:

```
.\FSLogixAppsSetup.exe /install /ProductKey=[your key here] /quiet
```



```
2690\x64\Release"
> .\FSLogixAppsSetup.exe /install /ProductKey=TRIAL-[redacted] /quiet
>
```

6.20 After a couple of minutes, go to Control Panel and see that FSLogix is now installed.

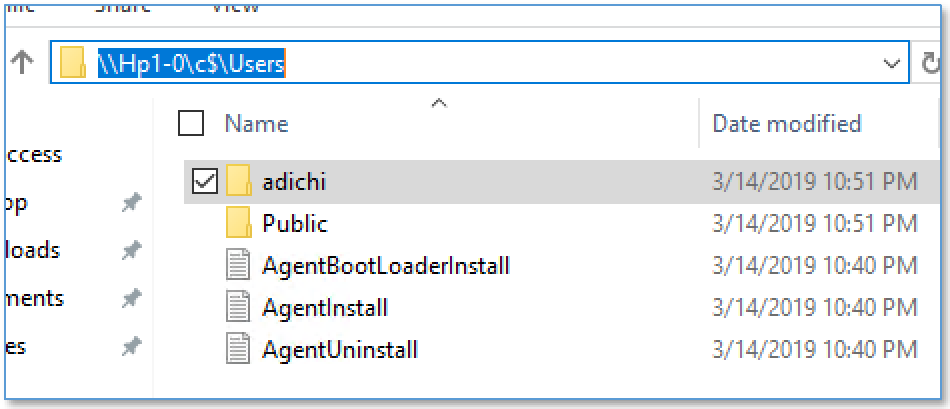


Name	Publisher
FSLogix Apps	FSLogix, Inc.
Microsoft Visual C++ 2017 Redistributable (x64) - ...	Microsoft Corporation
Microsoft Visual C++ 2017 Redistributable (x86) - ...	Microsoft Corporation
Remote Desktop Agent Boot Loader	Microsoft Corporation

6.21 **Logoff (not disconnect/close session)** from this Session host

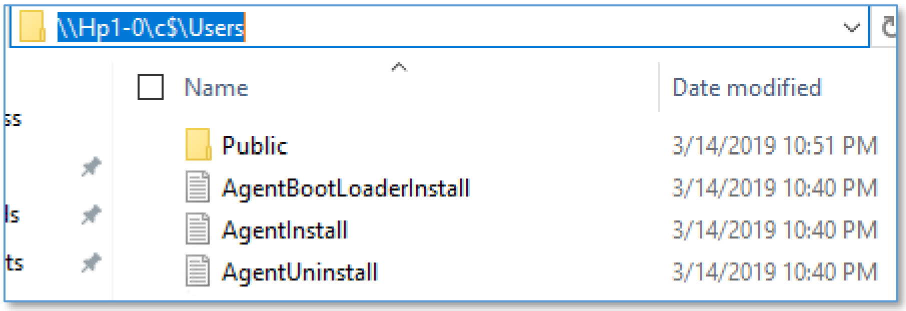
6.22 Now repeat steps 2-5 for the other Session Host(s) in the HostPool.

6.23 RDP to one of the server nodes of the SOFS cluster (EX: SOFS1) > open Windows explorer > and go to path [\\SessionHost\C$\Users](\\SessionHost\C$\Users) > delete the Admin profile that you just logged with. After that, you should only see the Public folder and the Agent* text files:



\\Hp1-0\c$\Users

□ Name	Date modified
☑ adichi	3/14/2019 10:51 PM
Public	3/14/2019 10:51 PM
AgentBootLoaderInstall	3/14/2019 10:40 PM
AgentInstall	3/14/2019 10:40 PM
AgentUninstall	3/14/2019 10:40 PM



\\Hp1-0\c$\Users

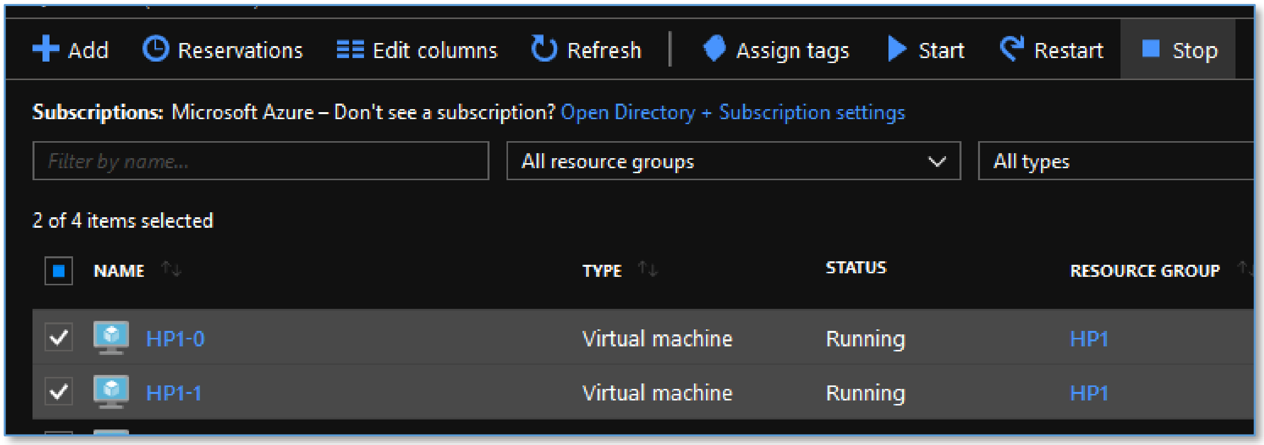
□ Name	Date modified
Public	3/14/2019 10:51 PM
AgentBootLoaderInstall	3/14/2019 10:40 PM
AgentInstall	3/14/2019 10:40 PM
AgentUninstall	3/14/2019 10:40 PM

6.24 Repeat from Step 7.4 for ALL other session hosts in the host pool.

Configure FSLogix GPO Settings

This section will involve making changes to the AD infrastructure along with the Group Policy Objects so please consult/have an AD expert/administrator team present while executing.

6.25 Login to the Azure Portal > go to Virtual Machines and STOP the session hosts



Subscriptions: Microsoft Azure – Don't see a subscription? Open Directory + Subscription settings

Filter by name... | All resource groups | All types

2 of 4 items selected

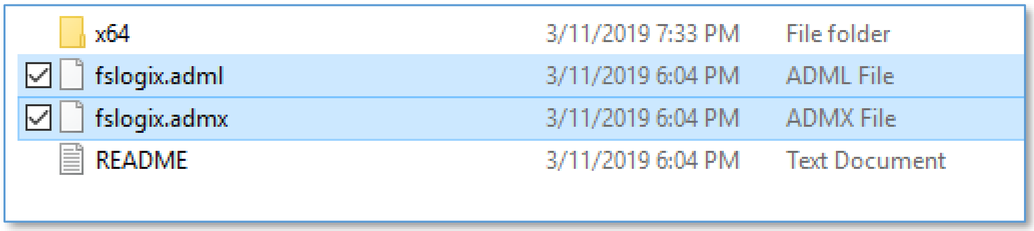
	NAME	TYPE	STATUS	RESOURCE GROUP
☑	HP1-0	Virtual machine	Running	HP1
☑	HP1-1	Virtual machine	Running	HP1

6.26 RDP to the domain controller (ours is **adPDC)** & file-explore to: \Windows\SYSVOL\sysvol\Contoso.com\Policies

6.27 Create a folder called **PolicyDefinitions**

6.28 Within the new **PolicyDefinitions** folder, create another folder called **en-US**

6.29 From the FSlogix installation folder in the section Install FSLogix on Session Hosts copy the **fslogix.ADMX** file to C:\Windows\SYSVOL\sysvol\Contoso.com\Policies\PoliciesDefinition folder on the domain controller

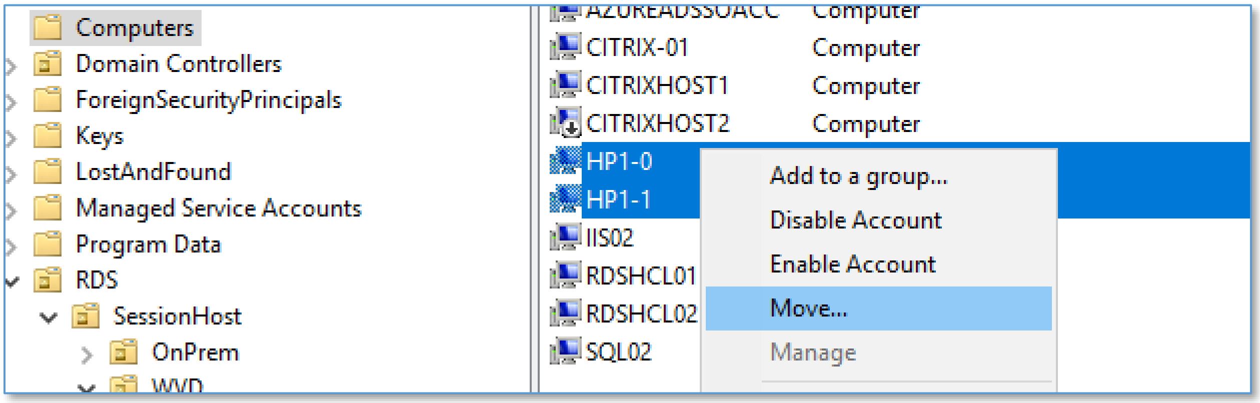


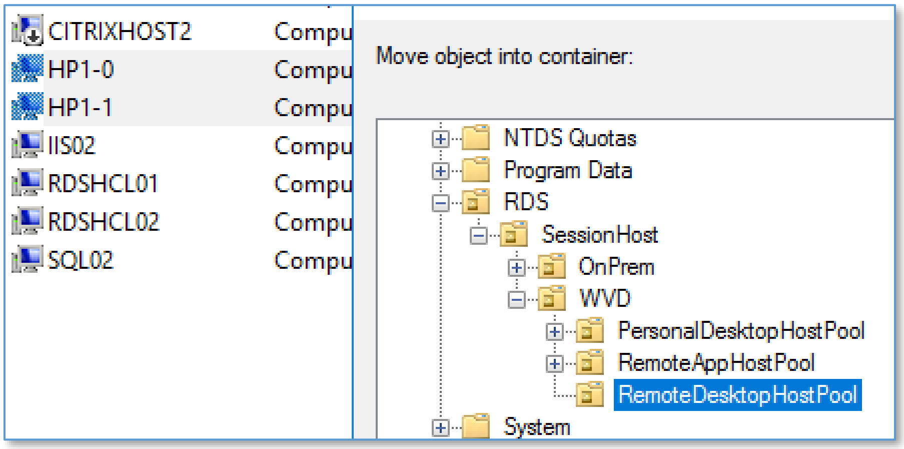
	x64	3/11/2019 7:33 PM	File folder
☑	fslogix.adml	3/11/2019 6:04 PM	ADML File
☑	fslogix.admx	3/11/2019 6:04 PM	ADMX File
	README	3/11/2019 6:04 PM	Text Document

6.30 Similarly, copy the **fslogix.ADML** file to C:\Windows\SYSVOL\sysvol\Contoso.com\Policies\PoliciesDefinition\en-US folder on the domain controller

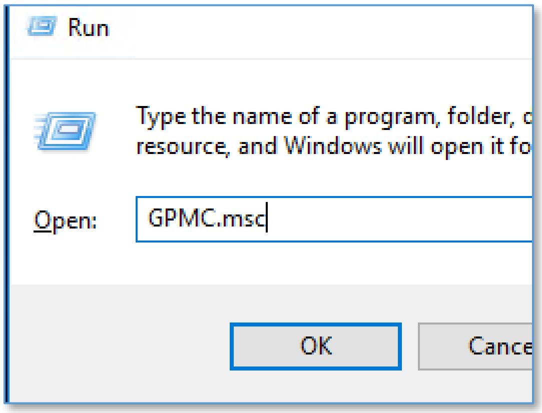
6.31 Open Active directory users & computers (dsa.msc)

6.32 Go to the Container/OU where the session hosts are present > CTRL + select the WVD session hosts > right click > move > and move them to the Respective WVD OU > Click OK





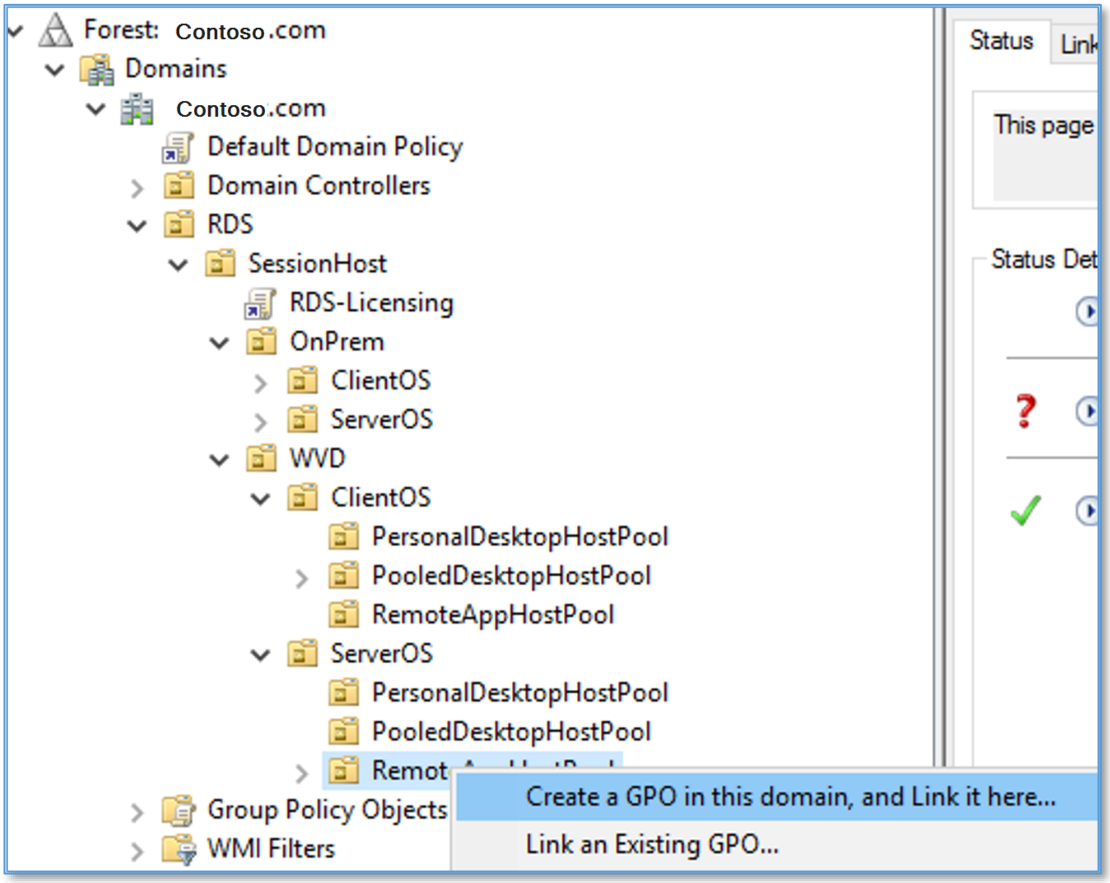
6.33 Hold Windows key + R > type GPMC.msc to open the group policy management console:



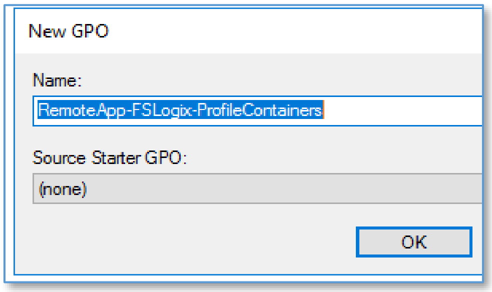
Type the name of a program, folder, d
resource, and Windows will open it fo

Open: GPMC.msc

6.34 Expand the domain and get to the OU where your session hosts exist to create and link a new GPO that will deploy FSlogix container settings:



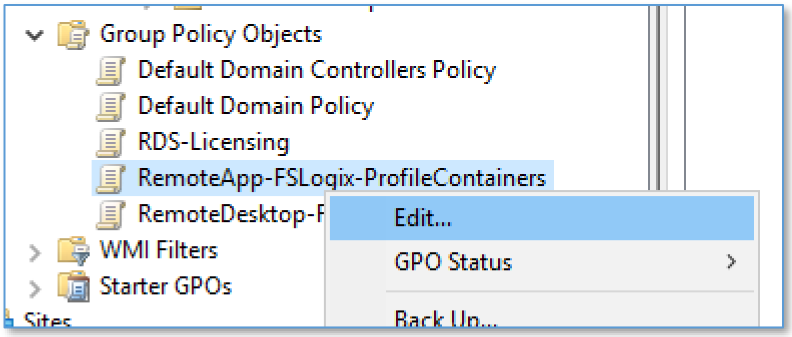
6.35 Provide a meaningful name for the GPO > OK


New GPO

Name: RemoteApp-FSLogix-ProfileContainers

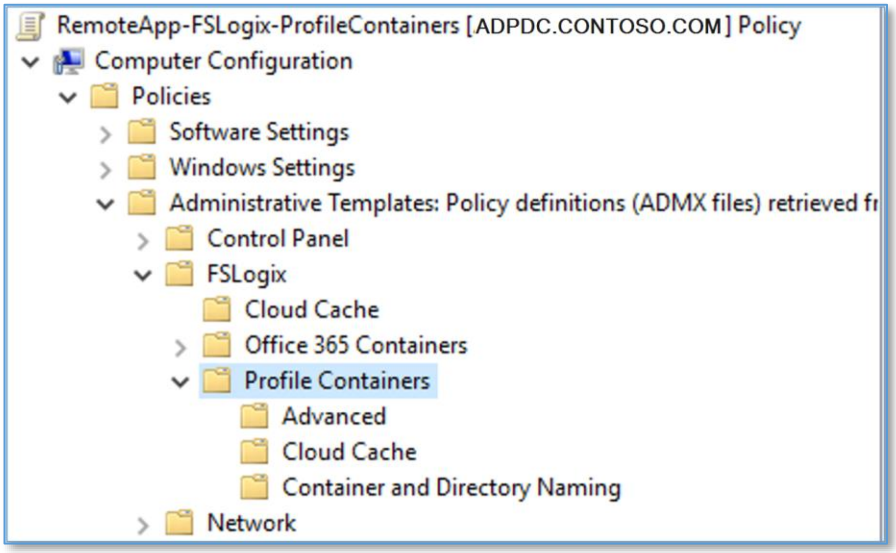
Source Starter GPO: (none)

6.36 Expand the OU to see the new GPO > right click > Edit



6.37 This will open the GPO editor

6.38 Expand Computer Configuration > Policies > Administrative Templates > FSLogix > Profile Containers


RemoteApp-FSLogix-ProfileContainers [ADPDC.CONTOSO.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy definitions (ADMX files) retrieved fr
Control Panel
FSLogix
Cloud Cache
Office 365 Containers
Profile Containers
Advanced
Cloud Cache
Container and Directory Naming
Network

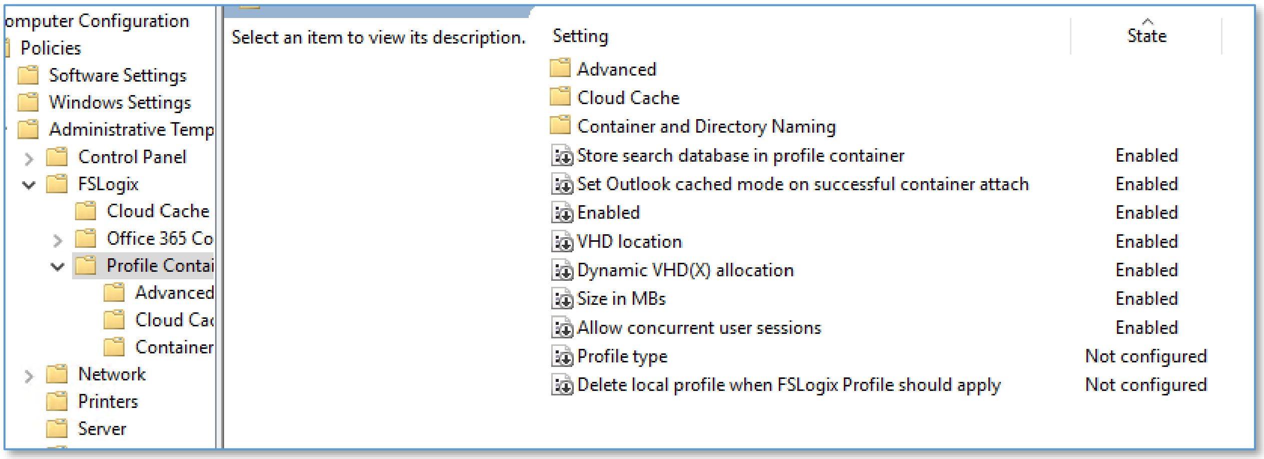
6.39 Now, using the list below, double click on the respective setting and Enable it so that the session hosts with FSLogix installed will have the same settings updated:

Core Settings (These MUST be enabled for FSLogix to function)

- Enabled
- Size in MBs
- Provide Size in MBs for each user profile (Ex: 10000MB / 10GB)
- VHD location
- Use the respective S2D share path you created earlier (EX: \\S2DUPD\RemoteAppsProfileCont)

6.40 *Optional Settings (Consult your user profile expert as these are subject to your requirements. For this document we are enabling them)*

- Allow concurrent user sessions
- Dynamic VHD(X) allocation
- Set Outlook cached mode on successful container attach:



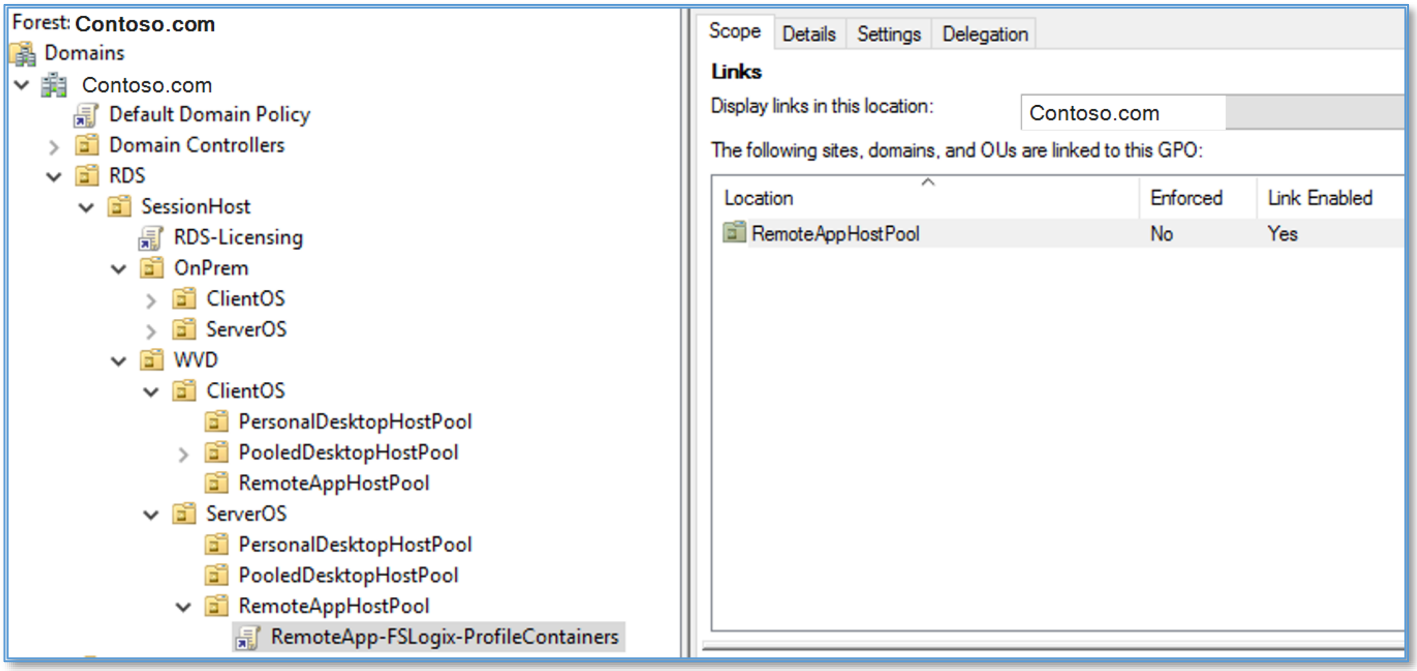
omputer Configuration
Policies
Software Settings
Windows Settings
Administrative Temp
Control Panel
FSLogix
Cloud Cache
Office 365 Co
Profile Contai
Advanced
Cloud Cac
Container
Network
Printers
Server

Select an item to view its description.

Setting	State
Advanced	
Cloud Cache	
Container and Directory Naming	
Store search database in profile container	Enabled
Set Outlook cached mode on successful container attach	Enabled
Enabled	Enabled
VHD location	Enabled
Dynamic VHD(X) allocation	Enabled
Size in MBs	Enabled
Allow concurrent user sessions	Enabled
Profile type	Not configured
Delete local profile when FSLogix Profile should apply	Not configured

6.41 Now close the GPO editor and get back to GPMC

6.42 Select the GPO, & in the right panel under scope, ensure that **Link Enabled**=Yes:



Forest: **Contoso.com**
Domains
Contoso.com
Default Domain Policy
Domain Controllers
RDS
SessionHost
RDS-Licensing
OnPrem
ClientOS
ServerOS
WVD
ClientOS
PersonalDesktopHostPool
PooledDesktopHostPool
RemoteAppHostPool
ServerOS
PersonalDesktopHostPool
PooledDesktopHostPool
RemoteAppHostPool
RemoteApp-FSLogix-ProfileContainers

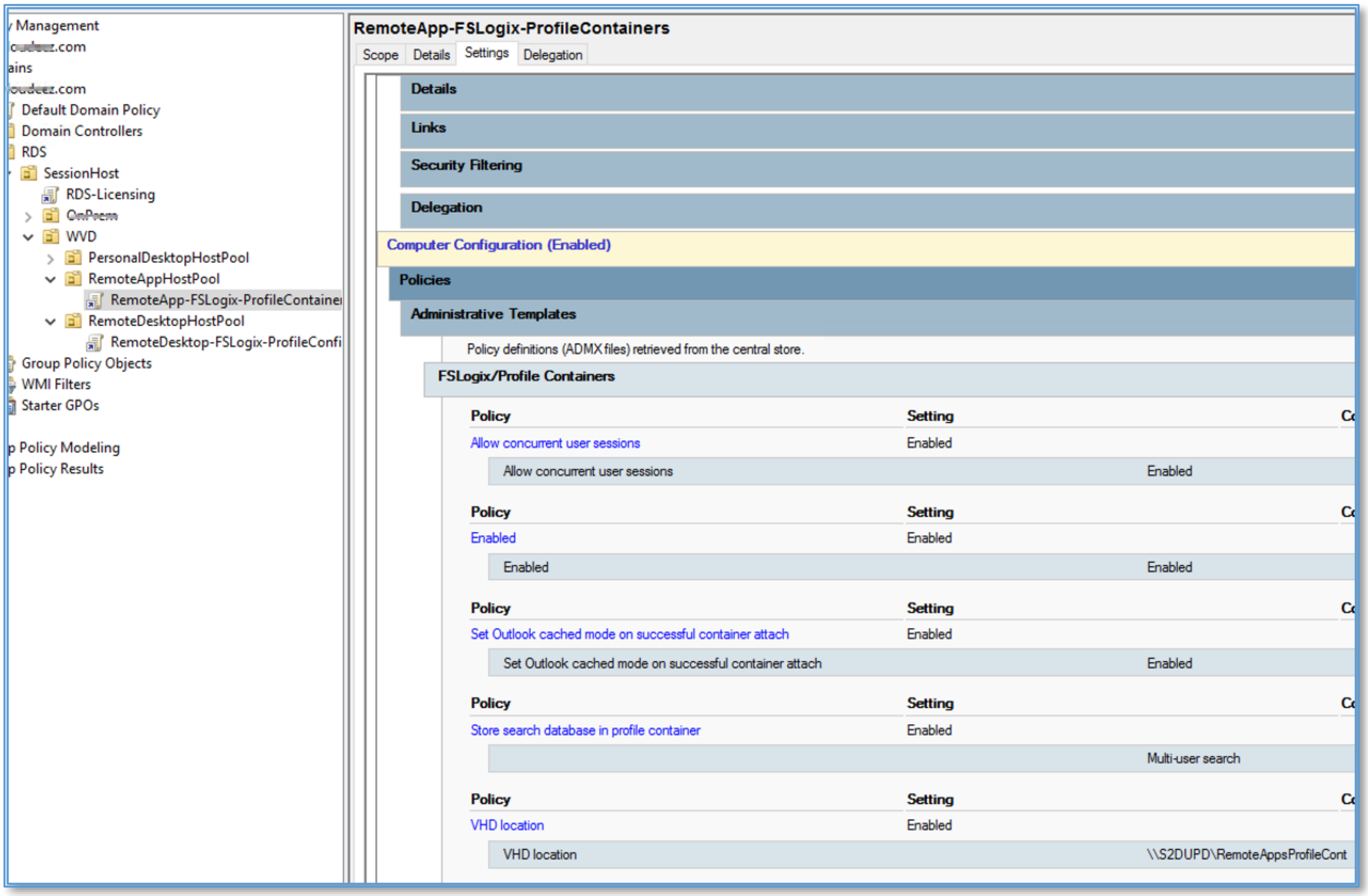
Links

Display links in this location: Contoso.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled
RemoteAppHostPool	No	Yes

6.43 Now click on Details > under Computer Configuration > expand Policies. Administrative templates > FSLogix/Profile Containers to see all the settings you have applied:



y Management
[redacted].com
ains
[redacted].com
Default Domain Policy
Domain Controllers
RDS
SessionHost
RDS-Licensing
[redacted]
WVD
PersonalDesktopHostPool
RemoteAppHostPool
RemoteApp-FSLogix-ProfileContainer
RemoteDesktopHostPool
RemoteDesktop-FSLogix-ProfileConfi
Group Policy Objects
WMI Filters
Starter GPOs

p Policy Modeling
p Policy Results

RemoteApp-FSLogix-ProfileContainers

Details

Links

Security Filtering

Delegation

Computer Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

FSLogix/Profile Containers

Policy	Setting	Co
Allow concurrent user sessions	Enabled	
Allow concurrent user sessions		Enabled

Policy	Setting	Co
Enabled	Enabled	
Enabled		Enabled

Policy	Setting	Co
Set Outlook cached mode on successful container attach	Enabled	
Set Outlook cached mode on successful container attach		Enabled

Policy	Setting	Co
Store search database in profile container	Enabled	
		Multi-user search

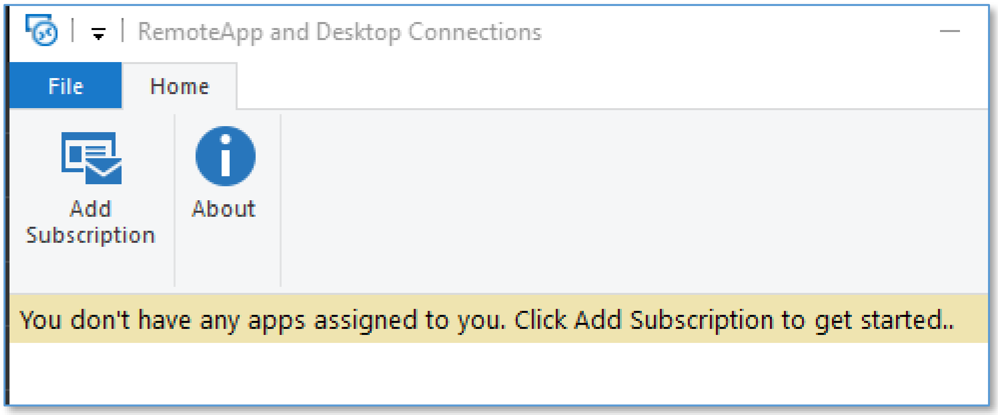
Policy	Setting	Co
VHD location	Enabled	
VHD location		\\S2DUPD\RemoteAppsProfileCont

7. Validate user connections to WVD

At this stage, your RemoteApps are deployed on the WVD session hosts along with the FSLogix configurations in place for the end user profile management (*we are using persistent desktops*.) A downloadable client is available that provides access to Windows Virtual Desktop resources from devices running Windows 7 and Windows 10. There is a web client that can be used as well.

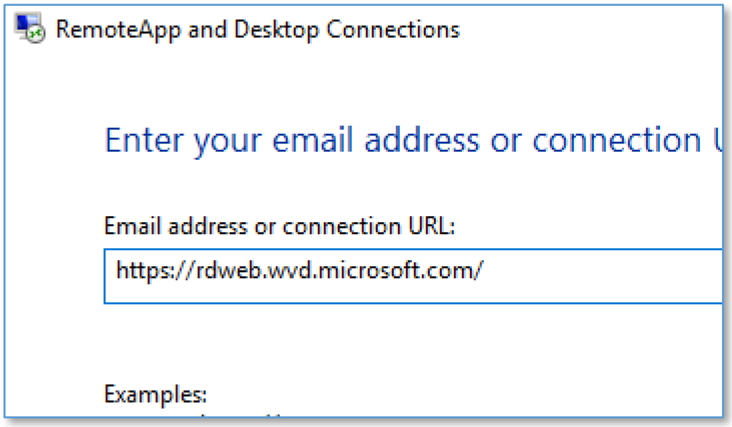
7.1 Download the client and run the MSI to complete the installation.

7.2 Start the client from the All Apps List, look for Remote Desktop.



You don't have any apps assigned to you. Click Add Subscription to get started..

7.3 Click Add Subscription > provide URL = https://rdweb.wvd.microsoft.com/ > Next > Next Again



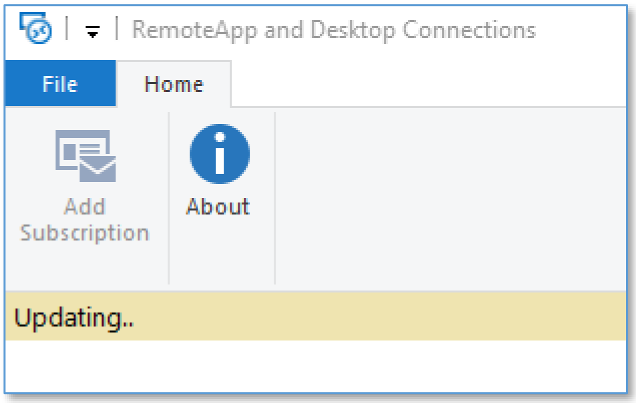
Enter your email address or connection U

Email address or connection URL:

https://rdweb.wvd.microsoft.com/

Examples:

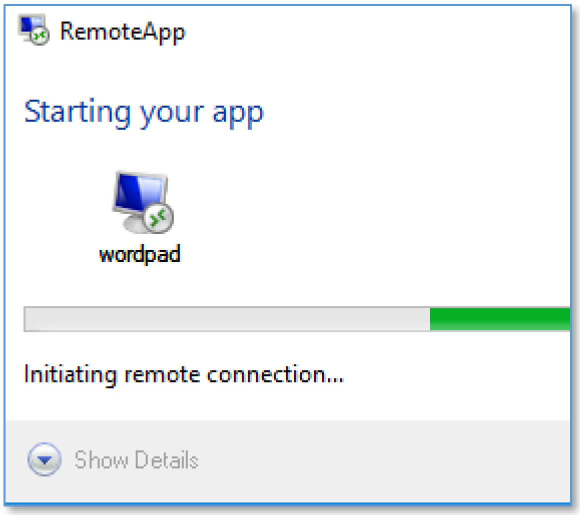
7.4 Sign in with you're the user account that was granted access to the WVD-RemoteApps in the earlier section > Next



Updating..

7.5 After successfully authenticating, you should now see a list of resources available to you.

7.6 Launch any of the resources (EX: WordPad). *please be advised that the first launch may be slow as your user profile is being created.*



RemoteApp

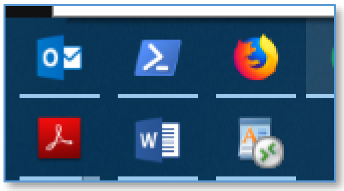
Starting your app

wordpad

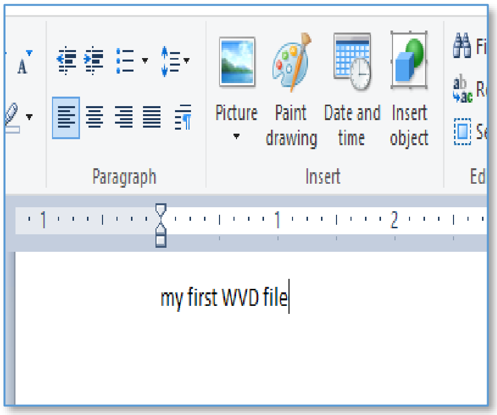
Initiating remote connection...

Show Details

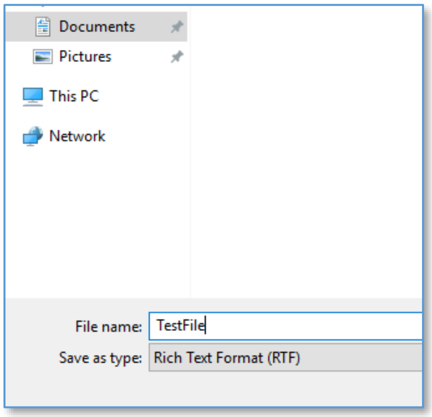
7.7 Once launched, you can see the icon in your taskbar



7.8 Now type something > save your file > close WordPad



my first WVD file



File name: TestFile

Save as type: Rich Text Format (RTF)

7.9 Alternatively, you can have a similar connection experience using a web browser by following the steps below.

NOTE: the browser must be HTML-5 compatible. Supported browsers include latest versions of IE/Edge/Safari/Firefox/Chrome

7.10 Browse to https://rdweb.wvd.microsoft.com

7.11 Login with user domain credentials

7.12 Access Apps & Desktops.

7.13 As an Admin, you can also validate the User Session data from the WVD end using either of the commands:

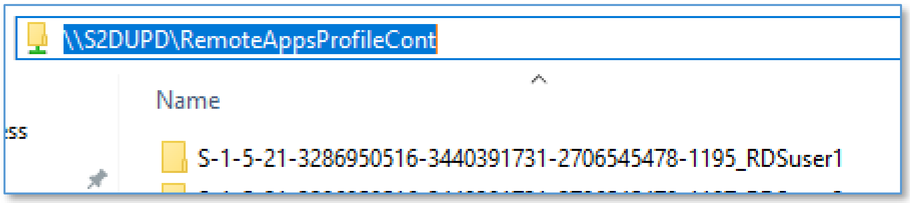
```
#See users of all AppGroups in a HostPool
Get-RdsUserSession -TenantName $TenantName

#Filter sessions by a specific HostPool
Get-RdsUserSession -TenantName $TenantName -HostPoolName $HostPoolName -Verbose
```

8. Validate FSlogix Profile containers

For persistent desktops, we have FSLogix configured on the session hosts for user profile management. All user profiles are saved as FSlogix Profile Containers (VHDx). This section will provide the steps to validate if and where the FSLogix Profile containers are being created.

8.1 From the Domain controller > open windows explorer

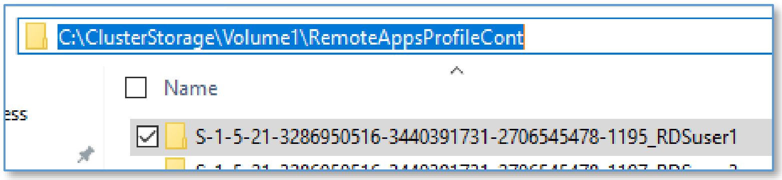
8.2 In the address bar type the S2D cluster share path (EX: \\S2DUPD\RemoteAppsProfileCont) to see the Profile Container for RDSUSER1:



\\S2DUPD\RemoteAppsProfileCont

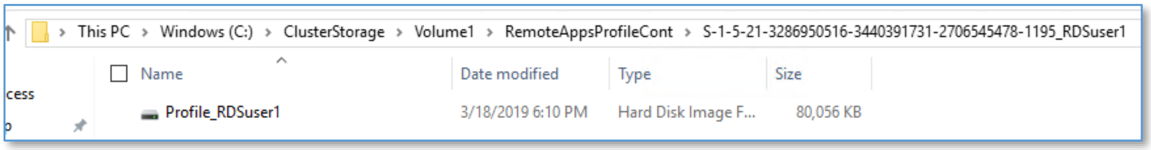
S-1-5-21-3286950516-3440391731-2706545478-1195_RDSuser1

8.3 Alternatively, you can also RDP to one of the SOFS/S2D cluster nodes and go to the CSV volume (in this case C:\ClusterStorage\Volume1\RemoteAppsProfileContainer) to see the profile container (VHDx) for RDSUser1:



C:\ClusterStorage\Volume1\RemoteAppsProfileCont

☑ S-1-5-21-3286950516-3440391731-2706545478-1195_RDSuser1



This PC › Windows (C:) › ClusterStorage › Volume1 › RemoteAppsProfileCont › S-1-5-21-3286950516-3440391731-2706545478-1195_RDSuser1

Name	Date modified	Type	Size
Profile_RDSuser1	3/18/2019 6:10 PM	Hard Disk Image F...	80,056 KB

9. Appendix

10. Additional Resources

11. Support

For support queries, please refer to our support portal where you can submit tickets to get additional assistance.