Microsoft

Windows Virtual Desktop (How-To) Deployment Guide *(WVD-Native only)*

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

Contents

1. Introduction

The ***primary intent of this guide is to illustrate the deployment steps for a Windows Virtual Desktop (WVD) solution in Azure***. It is intended to be used by Customer & Partners to help familiarize themselves with the processes, methodologies and tools required to implement& manage a WVD solution in Azure.

2. Target Audience

This document is ***Level 400+ technical guide*** primarily intended for Azure Specialists, Cloud Solution Architects, Migration experts, System Administrators & anyone else who are going to be hands-on in executing the technical steps to implementing the solution. It is assumed that the audience has deep insights into their on-premise workload architectures, storage & networking capabilities along with the interdependencies across multiple services/components involved like Active Directory, RDS deployments, Microsoft Azure and its core services (compute, storage & Network).

Please note that this document will primarily focus on the detailed process & methodologies and is NOT a primer for the technologies afore mentioned.

3. WVD Deployment Scenarios

Based on any existing infrastructure and/or providing WVD a new service for your customers, the WVD deployment will be classified into 2 scenarios as listed below. The idea is to provide a checklist in either scenario to be followed in a sequential format to ensure all the required components are available and working for successful deployments.

3.1. Greenfield (new) Deployments

Follow this section if you do not have any existing VDI like services and are deploying WVD to be your primary remote desktop offering.

1. Pre-Requisites/Requirements - Complete the basic items like access to Azure tenant/Subscription, permissions ~~Etc~~. (call out top items)
2. Licensing and Entitlements - Access Windows 10 Enterprise and Windows 7 Enterprise desktops and apps at no additional cost if you have an eligible Windows or Microsoft 365 license.
3. Application Assessment – Application assessments provide the current performance and usage details like OS, CPU, etc., VM sizing recommendations by classifying users into Personas (task workers, power users, knowledge worker

etc.) the applications accessed by the users and related, Azure costs. ~~This is an optional step for greenfield deployments but can be performed to get detailed insights into their current applications.~~

4. Azure Networking – As networking plays a crucial role in any cloud service, designing it to satisfy all the requirements is important.
5. Security and Compliance - Customers need to strengthen the security and access of their WVD deployments as they are governed by corporate policies (compliance, regulations etc.).
6. Identity and Access Management - WVD service in Azure requires authentication and Session host domain join using Windows Active Directory (AD), either from the on-premise environment or Azure AD Domain Services (AAD-DS).
7. Deploy and Configure Storage for User Profile(s) - A user profile contains data elements about an individual user, 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.
8. Image Management - Organizations use Custom Images to implement their security controls and configurations, pre-install their IT applications for users.
9. WVD Deployment – This section describes the steps required to deploy the WVD service.
10. FSLogix Setup and Configuration for WVD User Profiles - FSLogix is a set of solutions that enhance, enable, and simplify non-persistent Windows computing environments. FSLogix solutions are appropriate for Virtual environments in both public and private clouds. As part of WVD, we will utilize the FSLogix Profile Containers to manage User profile data.
11. Application and Desktop Management – Manage publishing applications and desktops in WVD.
12. Patch Management - Patch Management is the process of updating and patching the Session host VMs to avoid any security vulnerabilities and applying any configuration controls as required.
13. WVD Management and Monitoring - Management of WVD plays a crucial role in how the users interact with the service. You can grant/revoke access to published applications or desktops through Management, debug any issues that users come across when they access the service.

14. Business Continuity and Disaster Recovery - Customers can implement BCDR for their Session hosts using ASR. This would protect the VMs and provide faster recovery from disasters.

3.2. Migrate Apps/Desktops from on-premises to WVD

Follow this section if you already have a VDI/RDS solution on-prem (Ex: Microsoft Remote Desktop Services) and would like to upgrade/migrate to WVD.

1. Pre-Requisites/Requirements - Complete the basic items like access to Azure tenant/Subscription, permissions Etc.
2. Licensing and Entitlements - Access Windows 10 Enterprise and Windows 7 Enterprise desktops and apps at no additional cost if you have an eligible Windows or Microsoft 365 license.
3. Application Assessment – Application assessments provide the current performance and usage details like OS, CPU, etc., VM sizing recommendations by classifying users into Personas (task workers, power users, knowledge worker etc.) the applications accessed by the users and related, Azure costs. This is an optional step for greenfield deployments but can be performed to get detailed insights into their current applications.
4. Azure Networking – As networking plays a crucial role in any cloud service, designing it to satisfy all the requirements is important.
5. Identity and Access Management - WVD service in Azure requires authentication and Session host domain join using Windows Active Directory (AD), either from the on-premise environment or Azure AD Domain Services (AAD-DS).
6. Security and Compliance - Customers need to strengthen the security and access of their WVD deployments as they are governed by corporate policies (compliance, regulations etc.).
7. Deploy and Configure Storage for User Profile(s) - A user profile contains data elements about an individual user, 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.
8. Image Management - Organizations use Custom Images to implement their security controls and configurations, pre-install their IT applications for users.
9. WVD Deployment – This section describes the steps required to deploy the WVD service. **Please follow the below links only**

a. Grant Azure Active Directory permissions to the Windows Virtual Desktop service
b. Assign the Tenant Creator Application role to a user in your Azure Active Directory.
c. Download the WVD PowerShell Module
d. Create the WVD Tenant

10. Migrate Existing RDS/VDI infrastructure to WVD - Customers running an existing RDS/VDI infrastructure running on-premises, WVD makes it easier to migrate the Session Hosts/VDIs and run them in Azure.
11. Convert and Migrate User Profiles – Customers running an existing RDS/VDI Infrastructure and migrating to WVD may also want to move their User's profile data to WVD.
12. FSLogix Setup and Configuration for WVD User Profiles - FSLogix is a set of solutions that enhance, enable, and simplify non-persistent Windows computing environments. FSLogix solutions are appropriate for Virtual environments in both public and private clouds. As part of WVD, we will utilize the FSLogix Profile Containers to manage User profile data.
13. Application and Desktop Management – Manage publishing applications and desktops in WVD.
14. Patch Management - Patch Management is the process of updating and patching the Session host VMs to avoid any security vulnerabilities and applying any configuration controls as required.
15. WVD Management and Monitoring - Management of WVD plays a crucial role in how the users interact with the service. You can grant/revoke access to published applications or desktops through Management, debug any issues that users come across when they access the service.
16. Business Continuity and Disaster Recovery - Customers can implement BCDR for their Session hosts using ASR. This would protect the VMs and provide faster recovery from disasters.

4. Detailed Implementation Steps

Please note that any screenshots you see in the subsequent sections are purely for visual reference/guidelines purposes and details in the screenshot might be

different from the actual implementation details. Ensure that you read ALL instructions very carefully

4.1. Pre-Requisites/Requirements

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. ***For any reason, if you do NOT meet all requirements, then either get the required access or get in touch with a team/person who can help you achieve the same.***

- ✓ An Azure tenant (Ex: yourdomain.onmicrosoft.com) environment along with at least 1 active subscription.
    - If you are a customer, then reach out to your CSP partner who can provide you with the required tenant information and access
    - If you are the CSP partner, then you can get the customer details by logging onto the Microsoft Partner Portal > dashboard > customers . Here you can see the domain under the column Primary Domain Name
- ✓ Ensure that the user who will provision & configure WVD must have "Global Admin" rights to the Azure tenant they are a part of.
    - Based on the operating model, some customers might not have this enabled so contact your CSP-Partner who can help with the same.
- ✓ Ensure that the user who will provision & configure WVD must have at least "Contributor" rights to the Azure subscription
    - Based on the operating model, some customers might not have this enabled so contact your CSP-Partner who can help with the same.
- ✓ Knowledge and comfortability in managing Azure services like:
    - Azure Networking (VNET/Subnets/NIC/NSGs)
    - Azure Active Directory (AAD), Azure Active Directory Domain Services (AAD-DS) & Azure AD Connect
    - Azure Compute (VMs/Availability Sets)
    - Azure Storage (disks/storage accounts)
    - Azure Networking (VNET/Subnets/NIC/NSGs)
    - Ability to work with command line implementation using PowerShell, Azure Modules.
    - The ability to manage ARM templates and deploy azure resources with it.
- ✓ Knowledge of FSlogix Profile Containers

4.2. Licensing and Entitlements

The links below should include the details of auditing licenses for users to remain compliant with Microsoft licensing terms.

- requirements and licenses

4.3. Discovery & Assessment

This can be done using multiple tools described in the section below. Please choose anyone (1) from the below recommendations

4.3.1. Lakeside

Please refer to https://partners.lakesidesoftware.com for details on Lakeside's SysTrack Assessment tool.

4.3.2. Azure Migrate

The Azure Migrate service assesses on-premises workloads for migration to Azure. The service assesses the migration suitability of on-premises machines, performs performance-based sizing, and provides cost estimations for running on-premises machines in Azure. If you're contemplating lift-and-shift migrations, or are in the early assessment stages of migration, this service is for you.

In case you already have the Azure Total Cost Ownership (TCO) and/or the azure VM SKU requirements for your WVD infrastructure finalized, then skip this section all together.

The steps below will provide guidance on how to get started with a quick assessment of your existing RDS/VDI infrastructure, download the assessment report and convert those details into a meaningful plan for your WVD planning.

- Start with the Azure migrate-overview to generally understand the product and it's requirements.
- Based on the Hypervisor infrastructure being used on-prem, choose the respective option to deploy the Azure migrate project and start the assessment.

  NOTE: If your end goal is to migrate to WVD, the recommendation is to assess the session hosts and exclude the core services (Connection Broker/Gateway/Web/SQL) which will not be migrated to Azure. Alternatively,

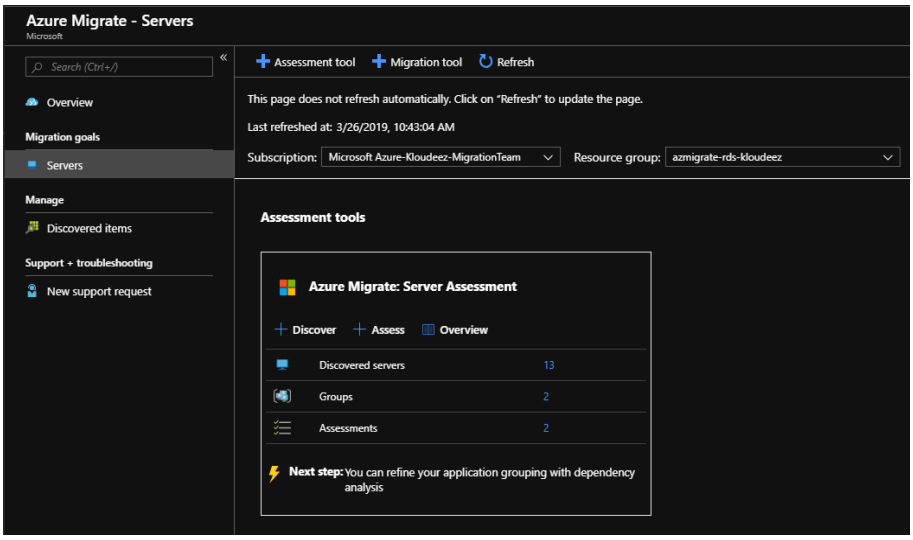
if the business driver today is to just migrate everything to Azure (But not migrate to WVD) then include your entire RDS infrastructure in the assessment.

- Assess VMware VMs - If your infrastructure operates on VMware
- Assess Hyper-V VMs - If your infrastructure operates on Hyper-V. *Please note that this feature is in preview.*

Azure Migrate Assessment Results

Once your assessment results are ready, follow the instructions below on how to use that assessment data and plan for your WVD infrastructure.

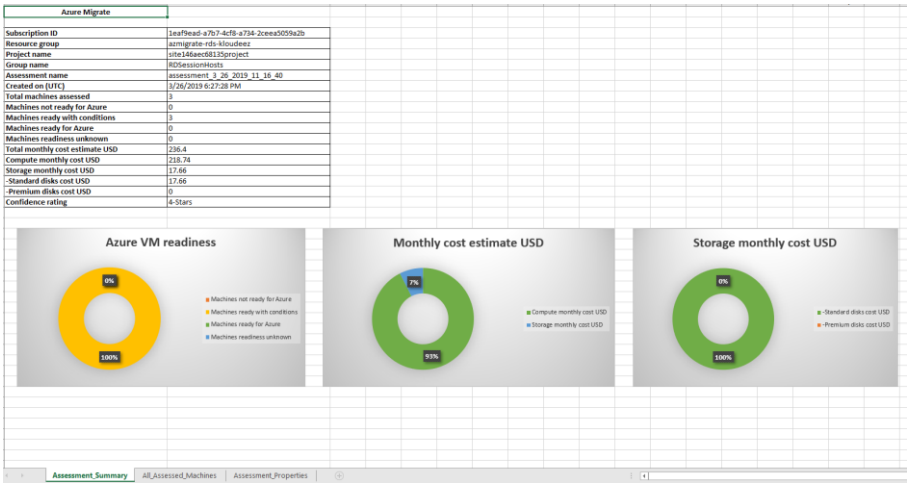
1. Export the Assessment Data. Open the Azure Migrate Overview through the Private Preview link and select the appropriate resource group to get the Assessment tools.



2. Click on the Assessments to open them.

3. Click on the Session Host Assessment to view and click on Export assessment to download as an Excel.

4. The first sheet in the assessment lists out the Azure TCO calculations for running these VMs in Azure. *This is an FYI and if you need to modify and adjust the TCO to a desired $ then please follow the Azure Migrate documentation links shared earlier in this section.*

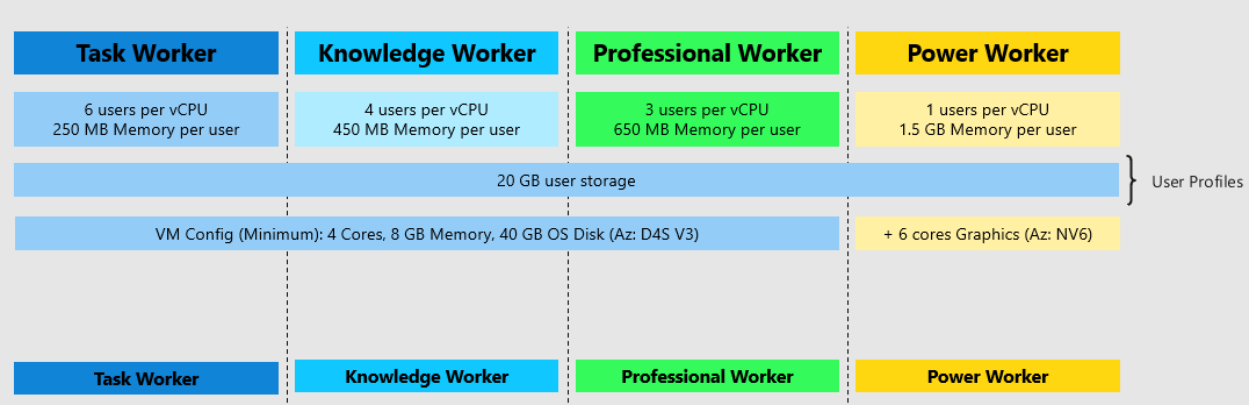


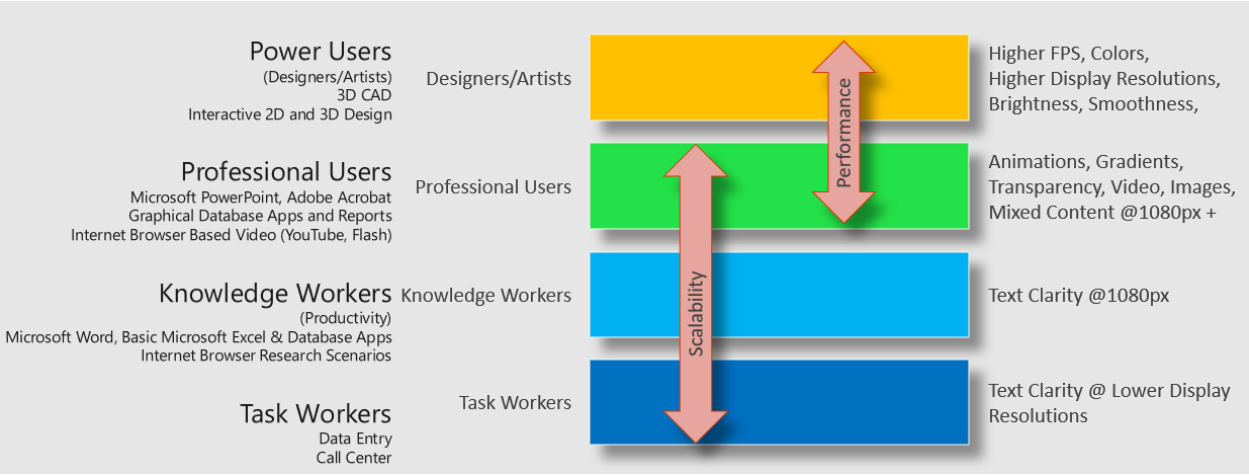
5. Navigate to the All_assessed_Machines sheet to view the recommended VM SKUs and Disk sizing based on the Assessment.
    i. Recommended Azure VM SKUs
    ii. Memory & CPU details
    iii. Disk sizing & SKU classification (Standard Vs Premium)

4.3.3. Manual VM & Storage Sizing Guidance

Based on your end goals & requirements, the planning & selection of the WVD session host VM SKUs can be done in a couple of different ways.

1. Using the recommendations in the chart(s) below, split your current users into different WVD personas based on their workload requirements.





- For example, if there are 100 users of each WVD persona. At a minimum, you would need the below VM requirements for a Host Pool with at least 2 session hosts

WVD User Persona	Min vCPU per server	Min Memory (GB) per server	Min SMB Storage endpoint (TB) per server	Notes
Task Worker	8 (~6 users per vCPU)	16 (~250 MB per user)	2 (~ 20GB per user)	Ideally, let's assume each server will have a max of 50 user at any given time. Although, if one of the session hosts goes down (maintenance Etc.),
Knowledge Worker	24 (~4 users per vCPU)	64 (~450 MB per user)	2 (~ 20GB per user)	

Professional Users	32(~3 users per vCPU)	64 (~650 MB per user)	2 (~ 20GB per user)	there should be enough capacity on the other server to accommodate additional users. *Apply a relative model when planning for more than 2 session hosts in your hostpool (scale-out)* Min RAM is rounded off to the next highest available config. [EX: Knowledge users need min of 45GB of RAM, so it is rounded off to higher config of 64GB and not then lower config of 32GB]
Power Users *[GPU enabled VMs]*	100 (~1 user per vCPU)	1600 (~1.6 GB per user)	2 (~ 20GB per user)	

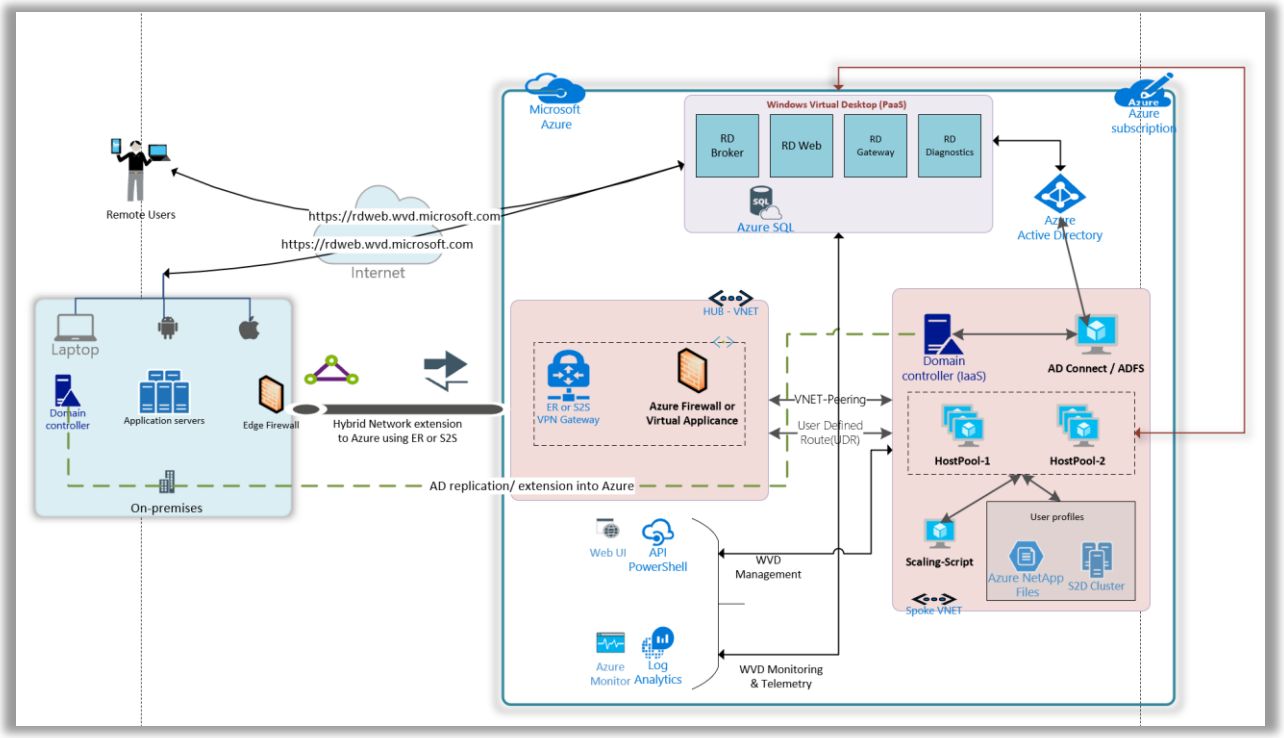
3 WVD Session Host guidance

2. Depending on the customer's flexibility, they can also choose a SKU that better suits their needs. Such as a Compute Optimized vs Memory Optimized vs High Performance Compute etc.

4.4. 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.

Below is the architecture diagram that outlines the Azure Networking plan that was deployed for the sake of this migration guide.



WVD Architecture

The sections below will briefly summarize the components deployed as a part of the Azure networking plan. ***It is *highly recommended* that your networking team is consulted during this phase for an optimal implementation.***

4.4.1. Azure Virtual Networks (VNET)

Like discussed earlier we are going to create 2 VNETs in a HUB and Spoke model using the below details.

HUB

- First create-a-virtual-network in Azure
  - For the subnet, create one called "Edge Security" (or something relative) where you will be deploying your firewall and/or other perimeter security devices.
- Now, in the Azure portal, goto All Services > Virtual Networks > choose HUB VNET > Subnets > Click on + Gateway Subnet and provide the appropriate CIDR in consultation with your networking team.

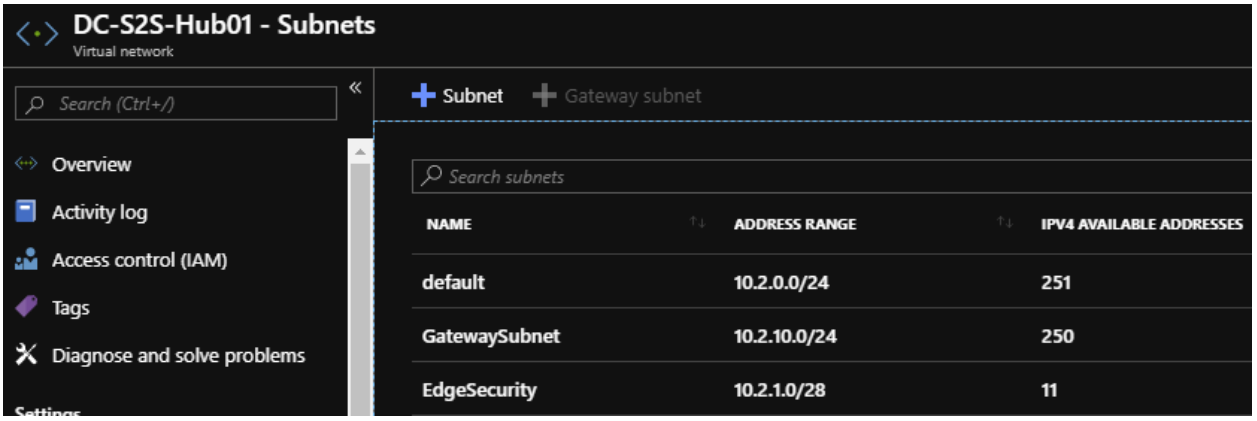


Figure 1 *HUB VNET with Gateway & Security subnets*

Spoke

- create-a-virtual-network called DC-S2S-Hub01 (or relative)
  - Create a subnet called "Default" (or make it specific based on how you want to isolate & manage servers). This will be the subnet where your WVD session hosts will live.

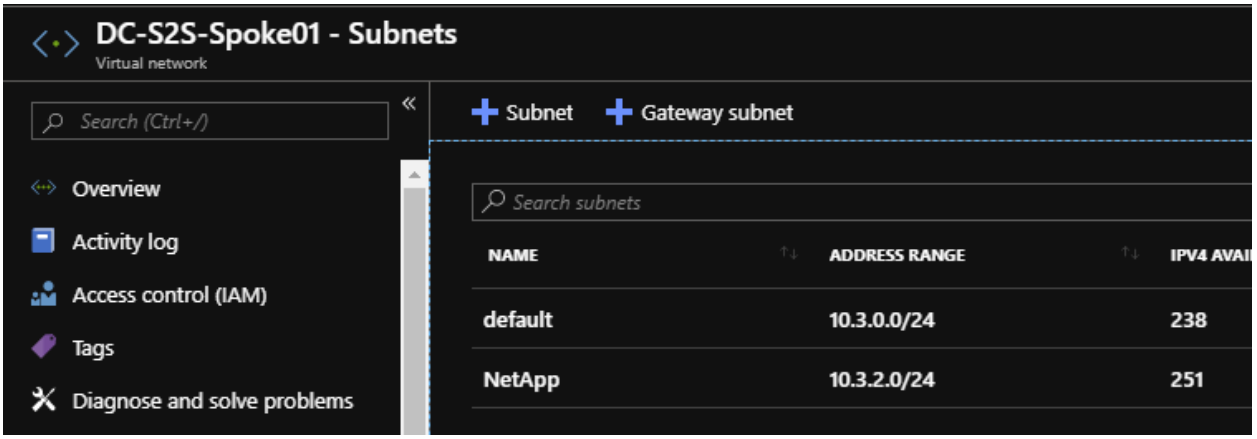


Figure 2 SPOKE VNET with subnets

VNET Peering

- Create a peering across the HUB & Spoke VNETs so that resources in networks Hub & Spoke can communicate with each other. Pay special attention to Configure virtual network access settings, configure forwarded traffic settings and Gateway transit settings to ensure traffic flows across both networks.

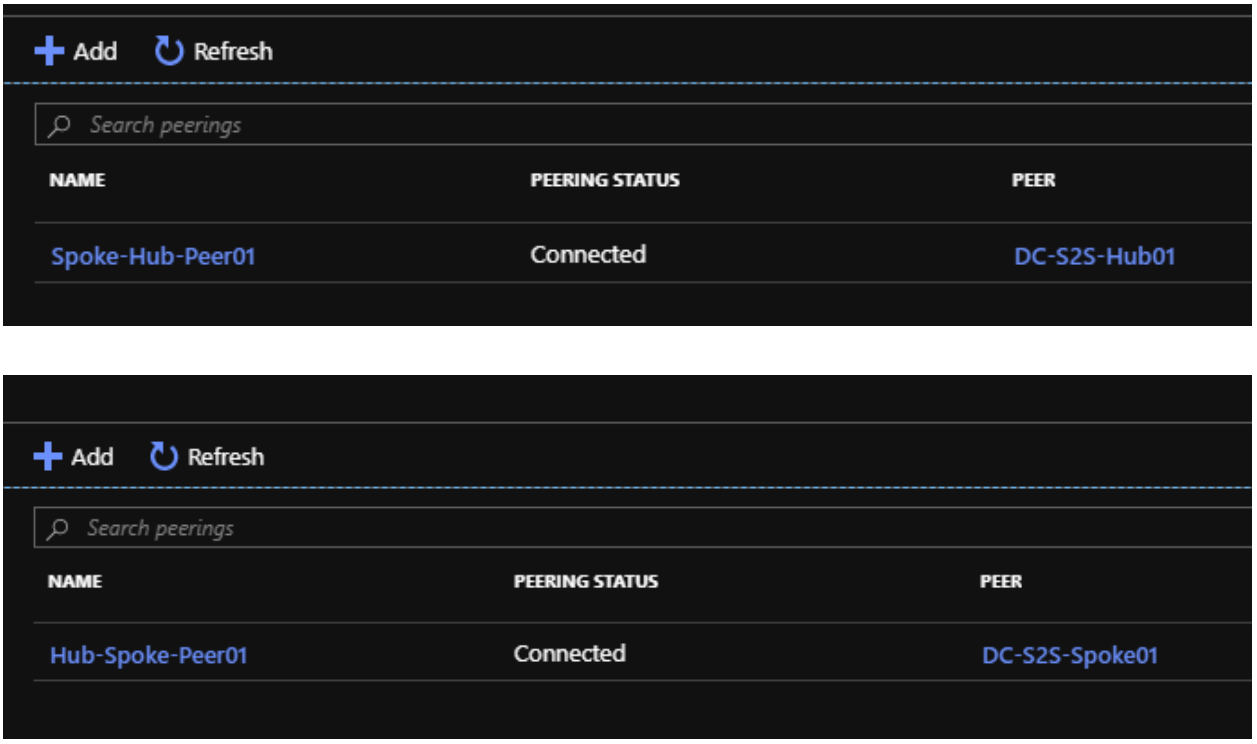


Figure 3 Peering configured between HUB & SPOKE VNETS

4.4.2. S2S Connectivity between on-premises & Azure.

This is ONLY required if you have an on-premises environment that you want to sync/extend into azure or have any service dependencies. we recommend that you consult your networking team to understand and implement steps in this section. If you are a cloud-only organization, you can skip this section

- Based on your bandwidth, latency & security requirements first choose between the connectivity model.
  - S2S or Express Route. *[For the sake of this document, we will be using S2S IPSEC tunnel]*
- Follow the instructions below to build an S2S-IPSEC tunnel using the on-premises edge networking device.
  - Read through the vpn-gateway, Bandwidth requirements to finalize your requirements first
  - Create the VPN Gateway in the HUB VNET/GatewaySubnet created earlier

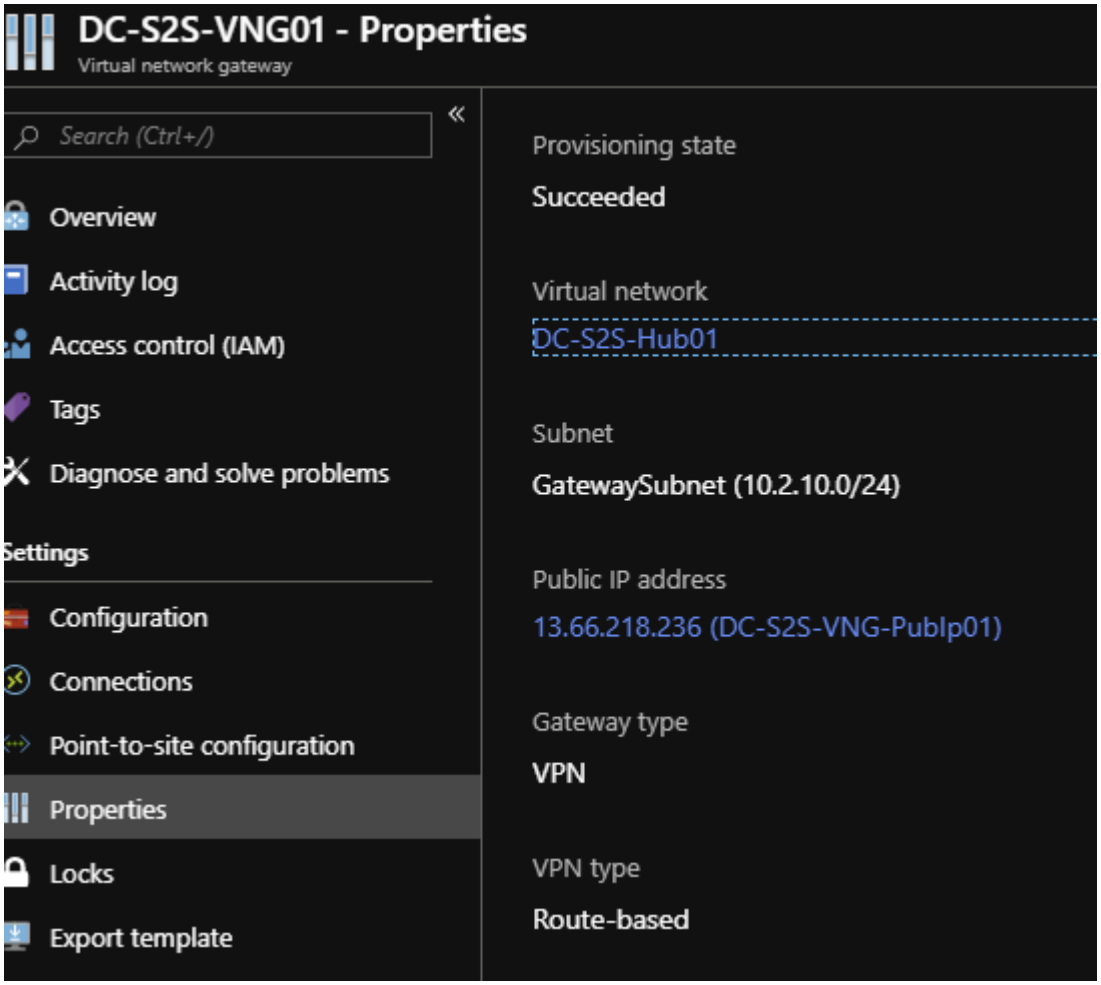
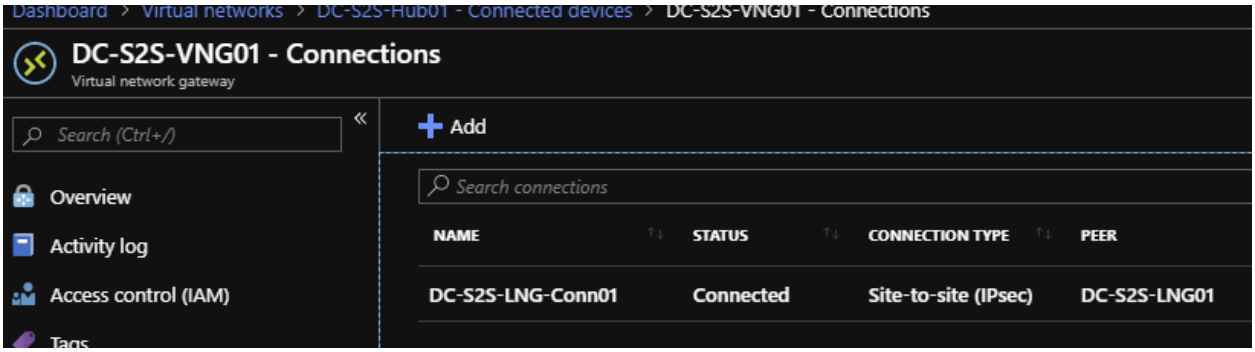


Figure 4 Azure virtual network gateway called "DC-S2S-VNG01" has been deployed to the HUB VNET and a static publicIP address 13.66.218.236 assigned to it.

- Use the instructions at [Build an S2S IPSEC tunnel with Azure] complete the connectivity to azure.



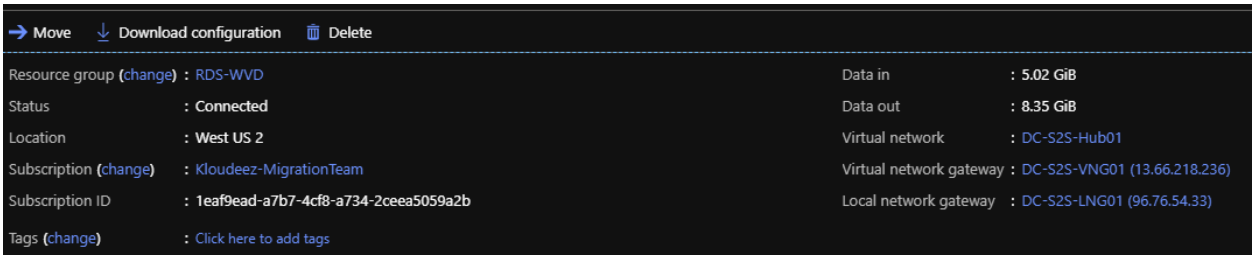


Figure 5 A connection "DC-S2S-LNG-CONN01" back to the on-premises device (96.76.54.33) has been created in Azure.

- Update the VNET with your on-premises DNS servers using the instructions at [Change DNS servers]

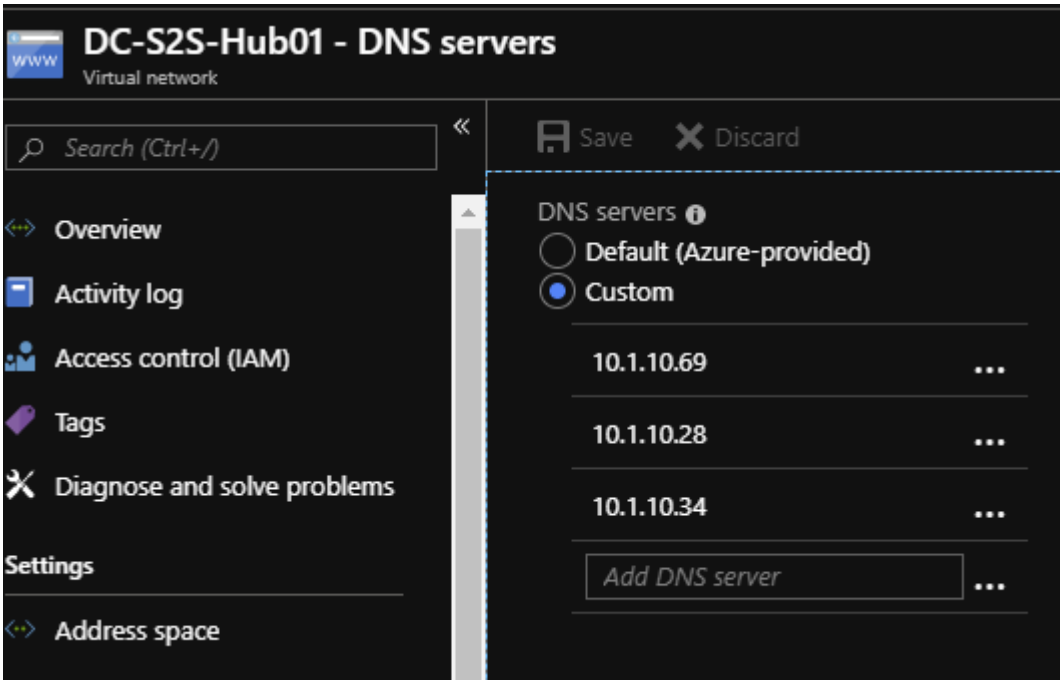


Figure 6 For both the HUB & SPOKE VNETs the DNS servers has been updated to (on-prem). IF you are planning to deploy additional Domain Controllers in Azure, please remember to add those as well once ready.

- Now you should be able to launch a VM in the Spoke VNET > domain join and access it like a local resource.

4.5. WVD Security & Compliance

4.5.1. Azure Firewall or Network Virtual Appliance (NVA)

When you connect your on-premises network to an Azure virtual network to create a hybrid network, the ability to control access to your Azure network resources is an important part of an overall security plan.

You can use Azure Firewall to control network access in a hybrid network using rules that define allowed and denied network traffic.

Please follow the below steps to deploy and configure an Azure Firewall in the Hub VNET created as part of the networking section.

- As part of the Hub VNET creation, create a Subnet for Firewall and name it AzureFirewallSubnet.
- Configure and deploy the firewall
- Configure network rules to allow or deny traffic. Use below table to identify the FQDNs for WVD specific resources and add these rules by following the instructions in the above link

Source	Destination (Target FQDNs)	Protocol	Port	Purpose/Name
Session Host Subnet Subnet should be created for WVD hosts. This can make it easier to identify WVD traffic	*.wvd.microsoft.com	HTTPS	443	Service communication
	login.windows.net	HTTPS	443	
	*.microsoftonline.com	HTTPS	443	
	*.msftauth.net	HTTPS	443	
	*.msauth.net	HTTPS	443	
	*.global.metrics.nsatc.net	HTTPS	443	
	*.metrics.nsatc.net	HTTPS	443	
	mrsglobalsteus2prod.blob.core.windows.net	HTTPS	443	Infra Agent, Stack and Monitoring agent updates
	gsm*.blob.core.windows.net	HTTPS	443	Service telemetry
	production.diagnostics.monitoring.core.windows.net	HTTPS	12000	Service telemetry
	prod.warmpath.msftcloudes.com	HTTPS	443	Service telemetry
	http://169.254.169.254/metadata/instance/network/interface/0/ipv4/ipAddress/0/	HTTP	80	VM telemetry, ACR

	http://169.254.169.254/metadata/instance/compute	HTTP	80	VM telemetry, ACR
	169.254.169.254			VM telemetry, ACR
	https://catalogartifact.azureedge.net/publicartifacts/rds.wvd-provision-host-pool-2636b3e1-9f2b-4349-aeeb-5d84d41b6a3e-preview/Artifacts/DSC/Configuration.zip	HTTPS	443	Marketplace deployments
	https://raw.githubusercontent.com/Azure/RDS-Templates/master/wvd-templates/Create%20ahttps://raw.githubusercontent.com/Azure/RDS-Templates/master/wvd-templates/Create%20and%20provision%20WVD%20host%20pool/nd%20provision%20WVD%20host%20pool/	HTTPS	443	Github Deployments
	https://rdweb.wvd.microsoft.com	HTTPS	443	Windows 10/7 Client. Subscribing makes the resources available on your local PC. https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-windows-7-and-10#subscribe-to-a-feed
	https://rdweb.wvd.microsoft.com/webclient/index.html	HTTPS	443	Web Client

4.5.2. Configure User Defined Routes (UDR)

You can create custom, or user-defined, routes in Azure to override Azure's default system routes, or to add additional routes to a subnet's route table. In Azure, you create a route table, then associate the route table to zero or more virtual network subnets. Each subnet can have zero or one route table associated to it.

Follow the steps below to create user-defined routes.

- Create a route from hub gateway subnet to spoke subnet through firewall IP address
- A default route from spoke subnet through firewall IP address

Refer to Create the routes for additional details.

Ensure these requirements are met after creating the routes.

- A User Defined Route (UDR) on the spoke subnet that points to the Azure Firewall IP address as the default gateway. BGP route propagation must be **Disabled** on this route table.
- A UDR on the hub gateway subnet must point to the firewall IP address as the next hop to the spoke networks.

  No UDR is required on the Azure Firewall subnet, as it learns routes from BGP.

- Make sure to set **AllowGatewayTransit** when peering VNet-Hub to VNet-Spoke and **UseRemoteGateways** when peering VNet-Spoke to VNet-Hub.

4.5.3. Configure MFA/Conditional Access for WVD

To simplify the sign in experience of your users, you might want to allow them to sign into your cloud apps using a username and a password. However, many environments have at least a few apps for which it is advisable to require a stronger form of account verification, such as multi-factor authentication (MFA).

Please follow the steps below to setup MFA using Conditional Access for WVD

- Create your Conditional Access policy
  - Under this step, select Windows Virtual Desktop application when selecting a cloud app.
- Evaluate a simulated Sign in
  - To simulate a sign in, use one of the users who have access to the WVD application.
- Test your Conditional Access policy

4.6. Identity & Access Management

This section will cover a multitude of areas starting for provisioning AD security groups & organizing users, creating GPO objects, extending your Identity into Azure ETC. It is highly recommended to work with your AD team for this section.

4.6.1. Setup & Configure Managed AD (AAD-Domain Services)

This section is required only if you already use (or planning to use) Azure Active Directory Domain Services (AAD-DS) in Azure. If already not setup, please use the instructions at Create and configure an Azure Active Directory Domain Services instances

4.6.2. Setup & Configure Hybrid Connectivity (ADConnect or ADFS)

This section is required if you already use (or planning to use) traditional Active Directory Domain Services (NOT AAD-Domain Services) either on-premises or in Azure IaaS.

If planning to use ADConnect follow instructions from Custom installation of Azure AD Connect **OR** If planning to use ADFS follow instructions from Configuring federation with AD FS

4.6.3. Create Users and AD Security Groups

Please creating some users' objects & AD Security groups that can be used to validate WVD functionality without disrupting everyday operations.

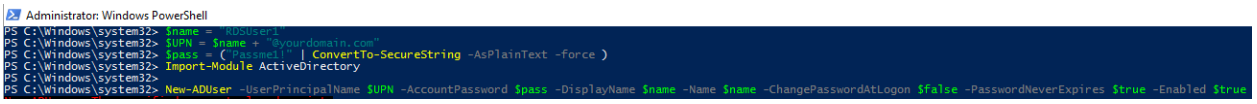
1. Let's start by creating some test users that will later be used to grant access to remote desktops & apps.

2. Log onto the domain controller > open PowerShell and run the below command

```
#update values first
$name = "RDSUser1"
$UPN = $name + "@yourdomain.com"
$pass = ("Passme1!" | ConvertTo-SecureString -AsPlainText -
force )
```

```
Import-Module ActiveDirectory

New-ADUser -UserPrincipalName $UPN -AccountPassword $pass -
DisplayName $name -Name $name -ChangePasswordAtLogon $false -
PasswordNeverExpires $true -Enabled $true
```



Update the values and Repeat the command for as many users you like to test with.

3. Now let's create the Security group(s) that will be required to manage resources and grant access at different stages in the subsequent sections. Below is a list of the security groups we need and why.

SecurityGroupName	Description
AccessFSLogix	Will contains the Session Host computer Objects that need to access the SOFS/S2D cluster to manage user profile containers
RDS-RemoteAppUsers	Contains users that need access to RemoteApps hosted using WVD
RDS-PooledDesktopUsers	Contains users that need access to RemoteDesktop(Pooled) hosted using WVD

Execute below commands on the domain controller in PowerShell

```
#update values using the first
$SecurityGroupName = "value from the SecurityGroupName column"
$Description = ""value from the Description column"

New-ADGroup -Name $SecurityGroupName -SamAccountName
$SecurityGroupName -GroupCategory Security -GroupScope Global
- -Description $Description
```

4. Now let's add the test users to the RemoteApp & PooledDesktop Security Groups. *FYI, I created a total of 4 test users and will be adding 2 users to each group.*

   Execute below commands on the domain controller in PowerShell

```
#update the value and add users to RemoteApp group

$Identity = "RDS-RemoteAppUsers"

Add-ADGroupMember -Identity $Identity -Members
@("rdsuser1","rdsuser2")


#adding users to RemoteDesktop group

$Identity = "RDS-PooledDesktopUsers"

Add-ADGroupMember -Identity $Identity -Members
@("rdsuser3","rdsuser4")
```

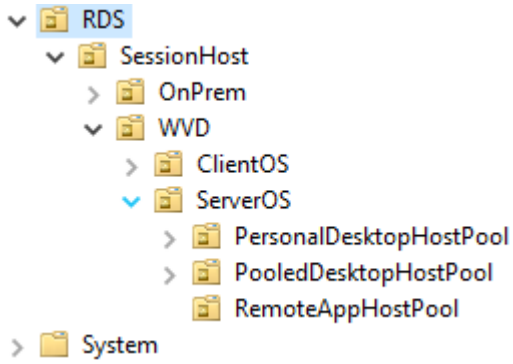
4.6.4. Active Directory Organization Unit (OU) structure for WVD session hosts.

It is strongly recommended to consult your in-house GPO expert for this section. The below guidance is subjective, and every enterprise should already have an established process/guidelines to manage their AD computer objects. Consider the below information as a mere FYI to help understand the steps to setup an OU structure.

Since we are introducing new servers into the existing environment and would most likely manage them using GPOs (Group Policy Objects), it is important to plan for the same. Settings like RDS licensing would already be managed using GPOs and since FSlogix for profile management is being introduced, the below guidance was used to organize WVD session hosts into a specific OU structure where FSLogix settings can be centrally controlled for the WVD sessions hosts across the different HostPools.

1. *On your domain controller, open ADUC (dsa.msc)*

2. *Expand the domain and get to the RDS OU (consider this the main OU where all your on-prem RDS computer objects are stored)*
   - *Under RDS, create a sub OU called Session Host (or Likewise) to manage common settings for all session hosts (on-prem & WVD)*
   - *Under Session Host, create a sub OU called WVD (or Likewise) to manage the WVD session hosts*
   - *Under WVD, create a sub OU called "RemoteAppHostPool" (the idea is to store all session hosts that server remote apps relative to the purpose of your HostPool in WVD)*



   - *Once the WVD session hosts are provisioned in Azure at a later section, steps are provided to move servers into the respective OUs.*

4.7. Deploy & Configure Storage for User Profiles

If you are planning to use non-persistent or pooled desktops/applications and store user profiles in Azure, then please choose any of the below storage solutions to deploy:

4.7.1. Azure NetApp Files

1. Please follow the instructions to plan (network/size Etc.) and deploy a NetApp solution for WVD using instructions at [Create an FSLogix profile container for a host pool using Azure NetApp Files] (from this link only complete the items listed below)
   a. Complete creating a NetApp Account
   b. Complete creating a Capacity Pool
   c. Complete joining to Active Directory
   d. Complete creating a new volume
   e. Complete Configure volume access parameters

2. Once the NetApp volume is ready, mount the volume using the instructions for Windows (SMB) at [Mount or unmount a volume for Windows or Linux virtual machines]

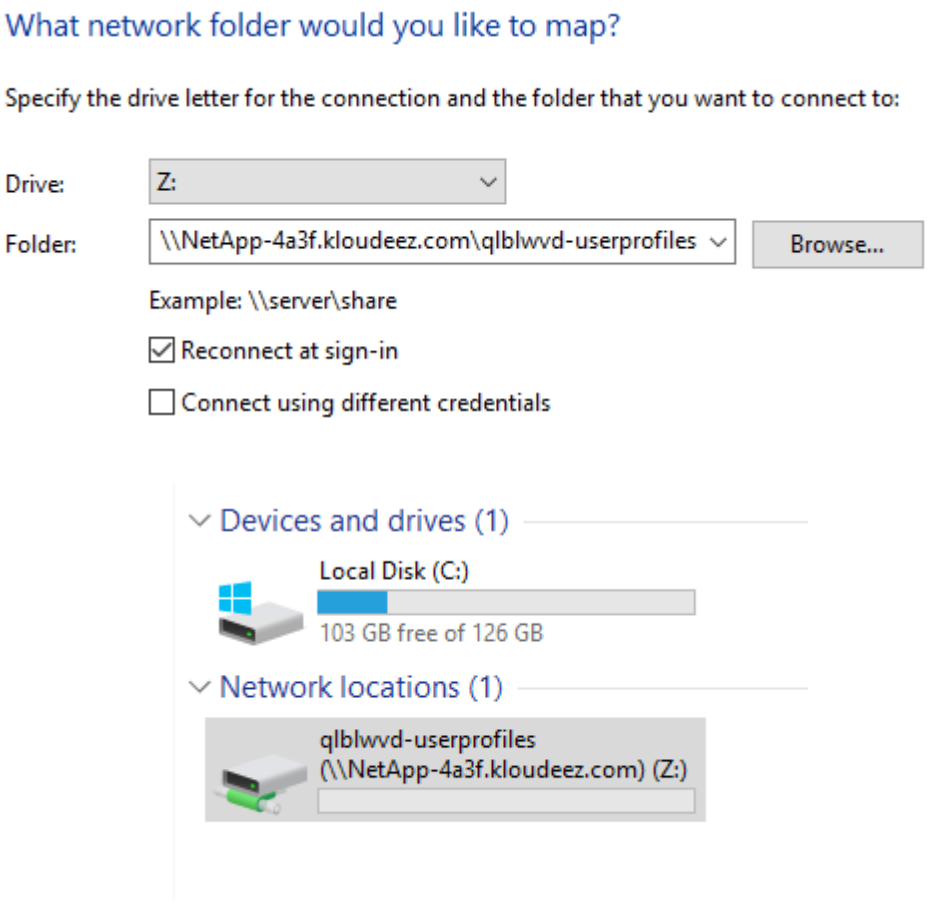


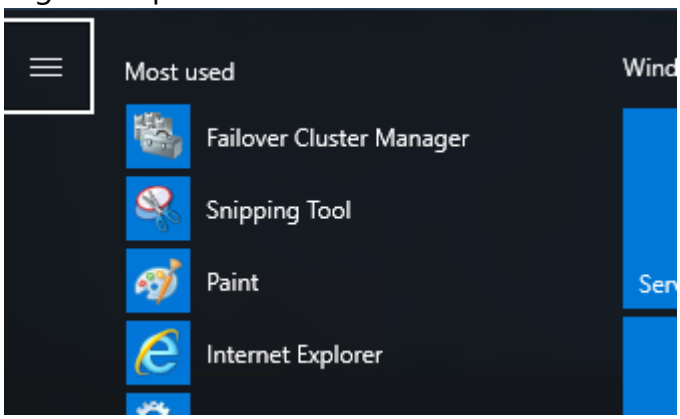
Figure 7 NetApp volume mounted as a windows drive

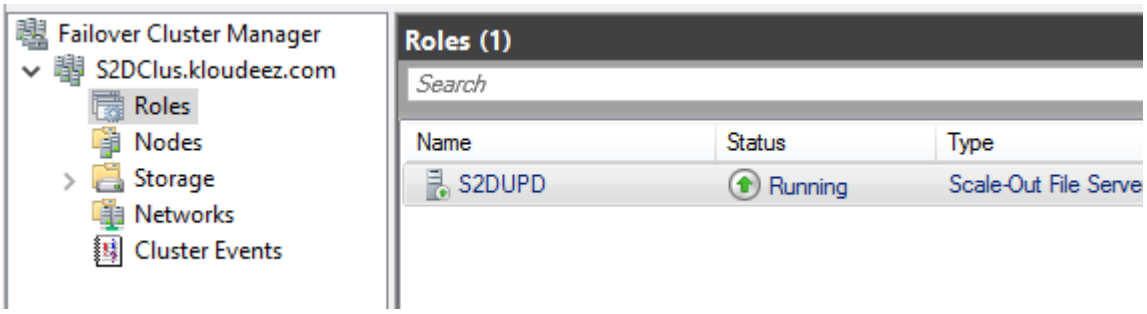
3. To set NTFS & Share permissions on this volume, Follow instructions in section [Set NTFS & Share permissions]

4.7.2. Scale out File server (SOFS) with Storage Spaces Direct (S2D)

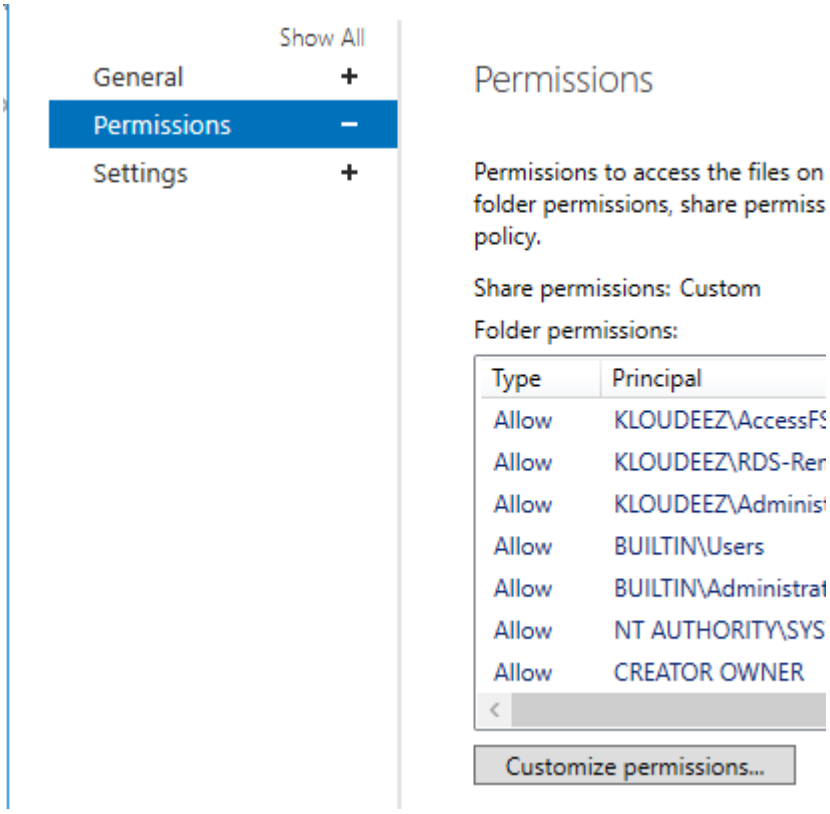
1. Based on the total # of users and their profile size requirements, first plan for the SOFS cluster size and SKU requirements in Azure using these [guidelines]
2. Deploy the SOFS cluster either manually or using ARM templates
    I. [Manual Deployment]
    II. [ARM Template]
3. *For the sake of this guide, the cluster details are as follows:*
    I. Cluster Name: S2DCLUS.Kloudeez.com
    II. *SOFS/S2D Name : S2DUPD.Kloudeez.com*

4. 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.
    I. Logon to any of the file server nodes and click Start > Failover cluster manager > expand cluster > Click roles > Click S2DUPD Role





    II. Now click Shares at the bottom > Right click the Share (Ex: RemoteApps) > click properties
    III. In the new window > click permissions > customize permissions



IV. To se NTFS & Share permissions, follow instructions in section Set NTFS & Share permissions

4.7.3. Azure Files

Please refer to the Azure Files section of WVD Documentation for detailed steps to create SMB share using Azure Files and Azure AD DS.

4.8. WVD Image Management

If you already use an Image management system, continue doing so or you can leverage Azure Image builder as your go-to image management system.

1. Please read the planning & deployment instructions at Preview: Azure Image Builder overview

4.9. WVD Deployment Steps

Creating a WVD (Windows Virtual Desktop) tenant is the first step towards building out 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. Each host pool also consists of one or

more app groups that are used to publish remote desktop and remote application resources to users. With a tenant, you can build out host pools, create app groups, assign users, and make connections through the service.

The subsequent sections will detail the step-step process to implement a working WVD solution in Azure.

4.9.1. Grant Azure Active Directory permissions to the Windows Virtual Desktop service

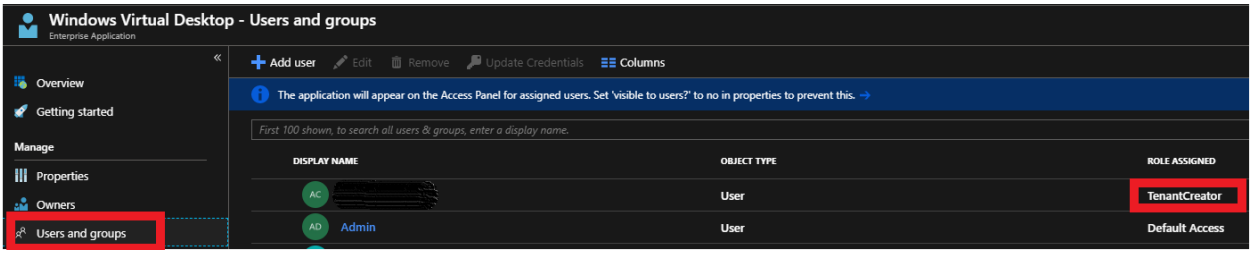
1. Open a browser and connect to the Windows Virtual Desktop consent page.
2. For **Consent Option** > **Server App**, enter the Azure Active Directory tenant name or Directory ID (from the Azure portal), then select **Submit**.
   - For Cloud Solution Provider customers, the ID is the customer's Microsoft 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** > wait for one minute.
5. Navigate back to the Windows Virtual Desktop consent page.
6. Go to **Consent Option** > **Client App**, enter the same Azure AD tenant name or Directory ID, then select **Submit**.
7. Sign into the Windows Virtual Desktop consent page as global administrator like you did back in step 3. Select **Accept**.

4.9.2. Assign the Tenant Creator Application role to a user in your Azure Active Directory.

1. Open a browser and connect to the Azure Portal with your global administrator account.
   a. If you're working with multiple Azure AD tenants, it's best practice to open a private browser session and copy and paste URLs into the address.
2. Select Enterprise applications, search for Windows Virtual Desktop and select the application.
3. Select Users and groups, then select Add user.

4. Select Users and groups in the Add Assignment blade. *Ensure that this is either a service or a user account that does not have MFA/CA enabled*

5. Search for a user account that will create your Windows Virtual Desktop tenant.
    a. For simplicity, this can be the global administrator account.
6. Select the user account, click the Select button > now click Assign at the bottom



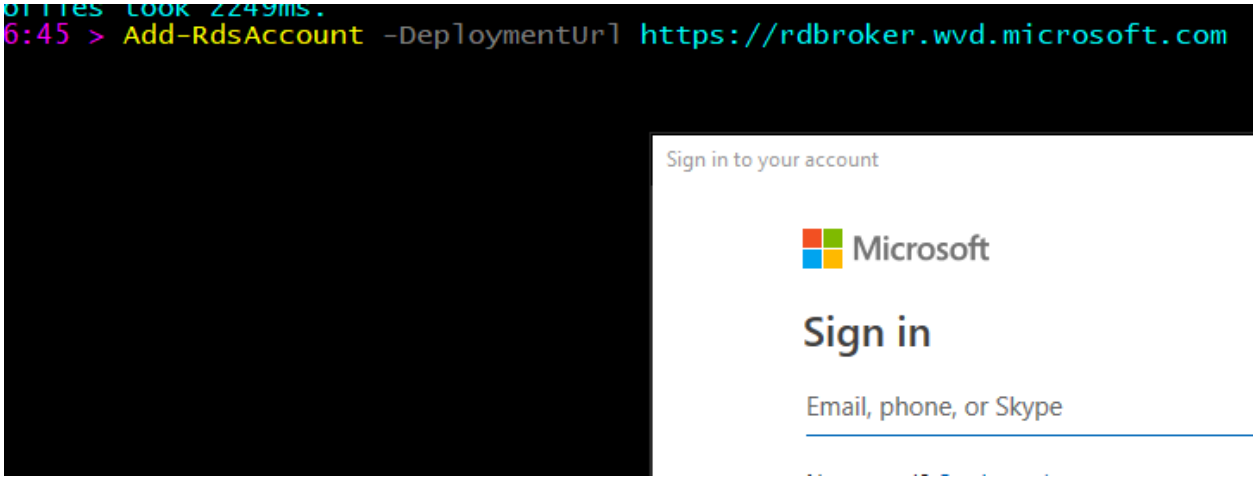
4.9.3. Download the WVD PowerShell Module

1. Download the Windows Virtual Desktop module and save the package in a known location on your computer.
2. Find the downloaded package. Right-click the zip file, select Properties, select Unblock, then select OK. This will allow your system to trust the module.
3. Right-click the zip file, select Extract all..., choose a file location, then select Extract.
4. First, run this cmdlet to save the file location of the extracted .zip file into a variable:
    `$module = "<extracted-module-location>"`
5. Second, run this cmdlet to import the DLL for the module:
    `Import-Module $module\Microsoft.RDInfra.RDPowershell.dll`
6. You can now run Windows Virtual Desktop cmdlets in your PowerShell window. If you close your PowerShell session, you'll have to import the module into your session again.

4.9.4. Create the WVD Tenant

1. In the PowerShell session, login as a Tenant Creator using the command below

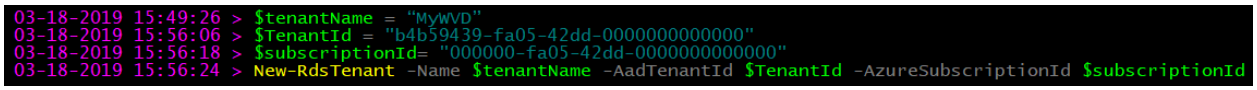
    `Add-RdsAccount -DeploymentUrl https://rdbroker.wvd.microsoft.com`

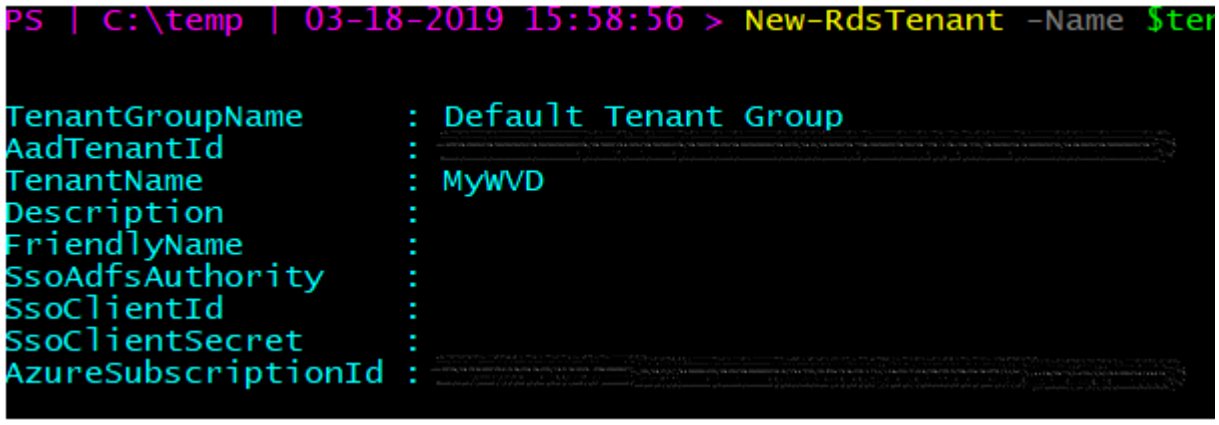


2. Now run the below commands to create a new WVD Tenant

```
#Setting Variables. Update the demo values within " " based on your specifics
$tenantName = "MyWVD"
$TenantId = "0000000-0000-0000-0000000000000"
$subscriptionId= "0000000-0000-0000-0000000000000"


New-RdsTenant -Name $tenantName -AadTenantId $TenantId -AzureSubscriptionId $subscriptionId
```





4.9.5. Deploy the WVD Host Pools

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

Follow the steps in this article to create a host pool within a Windows Virtual Desktop tenant. 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.

Very important to note that at this time, WVD only supports the OS versions listed at Requirements

Deploy VMs with Client Operating System

1. **Windows 10 Multi-Session**

   Choose any deployment style from below based on your preference (GUI Vs command line)

   a. For deploying using the Azure portal (GUI) refer the section Deploy HostPool using Azure Portal (Marketplace)
   b. For deploying using the ARM template (GitHub) refer section Deploy HostPool using ARM template

Deploy VMs with Server Operating System

1. **Windows Server 2016**

   Choose any deployment style from below based on your preference (GUI Vs command line)

   c. For deploying using the Azure portal (GUI) refer the section Deploy HostPool using Azure Portal (Marketplace)
   d. For deploying using the ARM template (GitHub) refer section Deploy HostPool using ARM template

2. **Windows Server 2012 R2 and Windows Server 2019**

   Currently, the Azure Portal (GUI) or existing ARM templates (GitHub) do not support deploying these Operating Systems. So, to deploy VMs with this OS refer steps from Deploy HostPool using modified ARM template

4.9.6. Validate the new Host Pools

1. Now, we will validate this newly created host pool
1. Open PowerShell and first connect to the WVD tenant using below commands.

```
#UPDATE THESE VALUES FIRST
$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
```

```
PS | C:\temp | 03-19-2019 16:56:52 > Add-RdsAccount -DeploymentUrl $brokerURL

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

2. Check for the new Host Pool using below command

```
#UPDATE THESE VALUES FIRST
$TenantName = “MyWVD”

Get-RdsHostPool -TenantName $tenantName
```

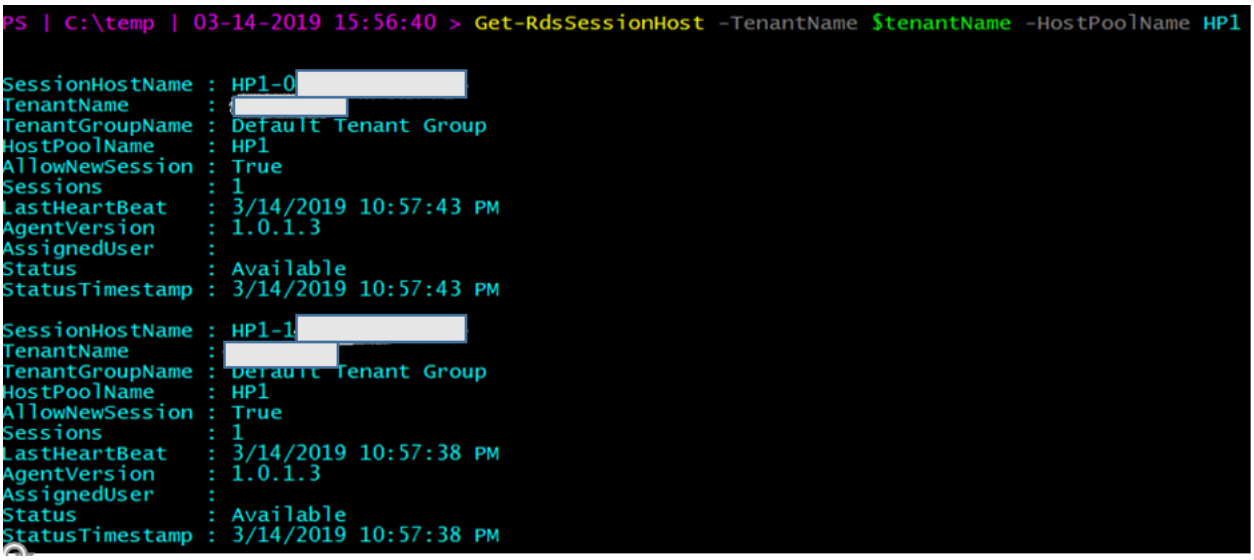
```
PS | C:\temp | 03-14-2019 15:50:59 > Get-RdsHostPool -TenantName $tenantName


TenantName            :
TenantGroupName       : Default Tenant Group
HostPoolName          : HP1
FriendlyName          : HP1
Description           : Created through ARM template
Persistent            : False
DiskPath              :
EnableUserProfileDisk : False
ExcludeFolderPath     :
ExcludeFilePath       :
IncludeFilePath       :
IncludeFolderPath     :
```

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

```
#UPDATE THESE VALUES FIRST
$HostPoolName = “HP1”
```

```
Get-RdsSessionHost -TenantName $tenantName -HostPoolName
$HostPoolName
```



4.10. FSLogix Setup & Configuration for WVD User Profiles

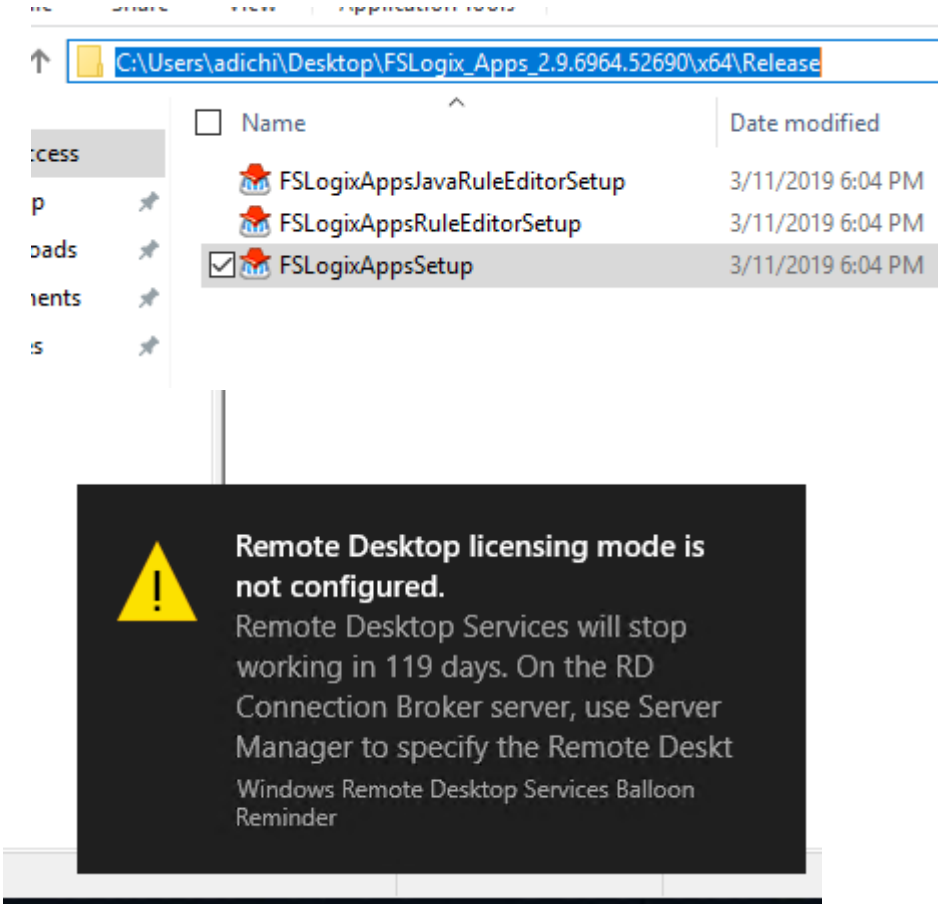
The Windows Virtual Desktop service offers FSLogix containers as the recommended user profile solution. The traditional windows user profile disk (UPD) solution is not recommended and will be deprecated in future versions of Windows Virtual Desktop.

For any reason, if you have NOT already completed provisioning a storage solution, please complete Deploy & Configure Storage for User Profiles first.

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.

4.10.1. Install FSLogix on Session Hosts

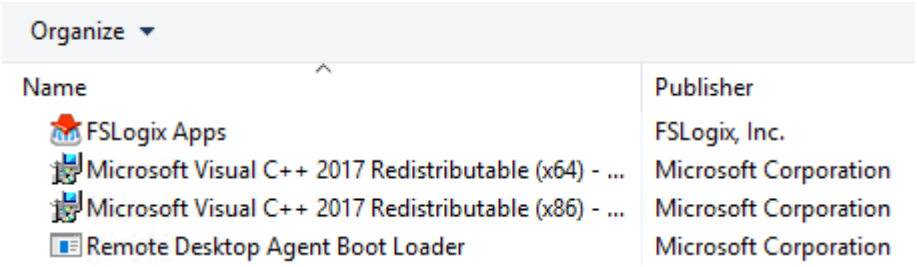
1. Use this link to download FSLogix.
2. From your WVD Host pool in Azure, login to one of the session hosts using an administrator account and copy the FSLogix bits locally. *Please ignore the RDLicensing warning at this time.*



3. CD to the path where you copied > open PowerShell > run the below command. ***Please ignore the trial key in the screenshot which is not required anymore.***

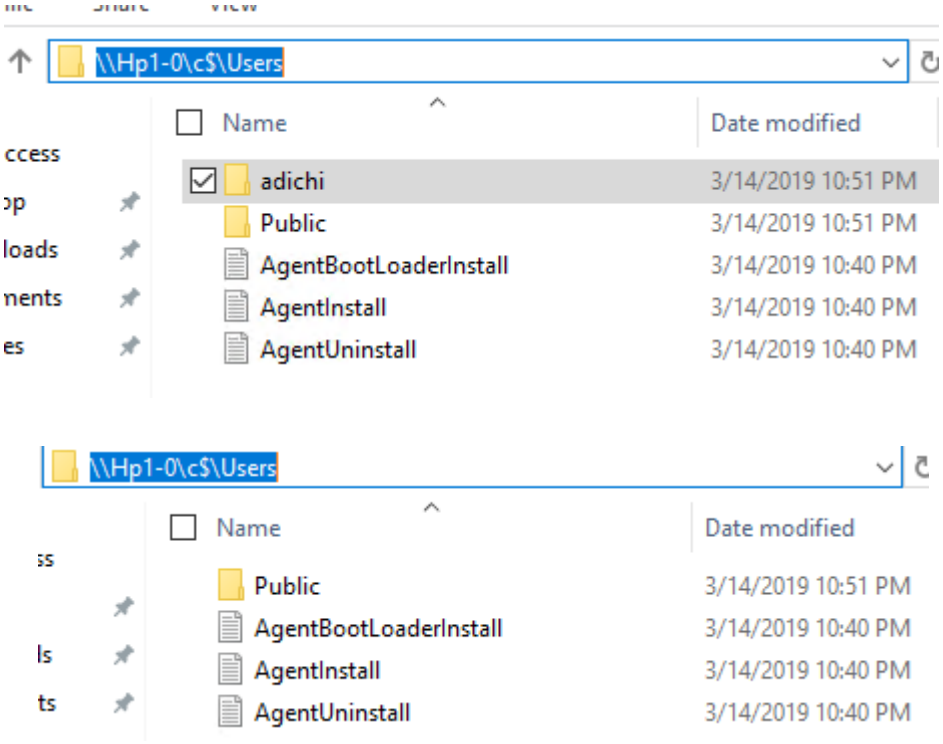
   .\fslogixappssetup.exe /install /quiet

4. After couple of minutes > goto control Panel and see that FSLogix is now installed.



5. **Logoff (not disconnect/close session)** from this Session host
6. Now repeat steps 2-5 for the other Session Host(s) in the HostPool.
7. RDP to one of the server nodes of the SOFS cluster (EX: SOFS1) > open Windows explorer > and goto path \\SessionHost\C$\Users > delete the

Admin profile that you just logged with after which you should only see the Public folder and the Agent* text files

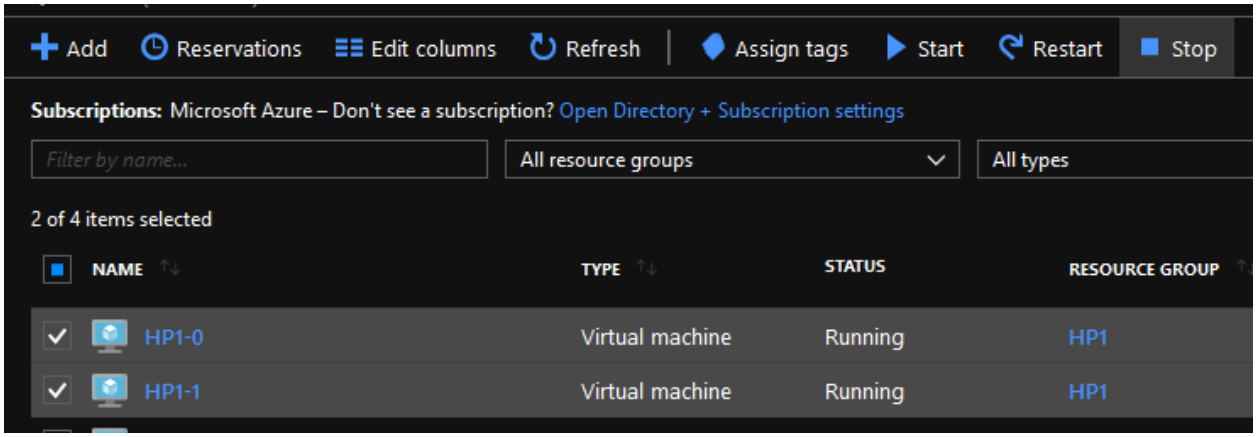


8. Repeat Step 7 for ALL other session hosts in your host pool.

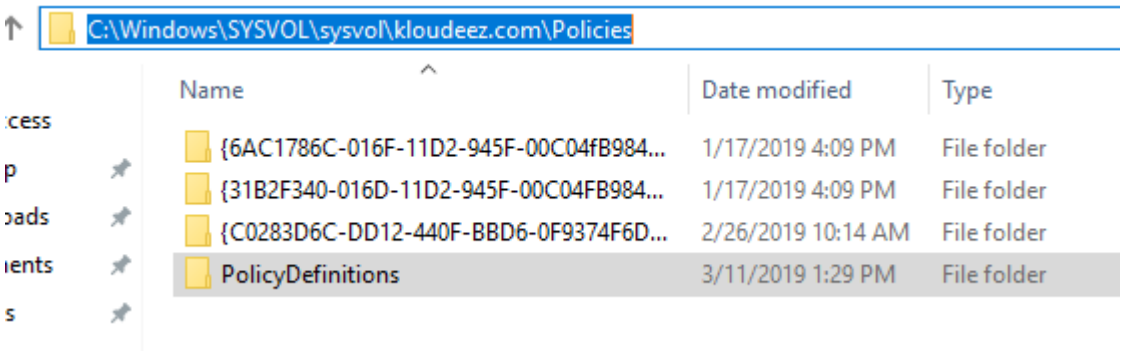
4.10.2. Configure FSLogix GPO Settings

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.

1. Login to the Azure Portal > goto Virtual Machines and STOP the session hosts

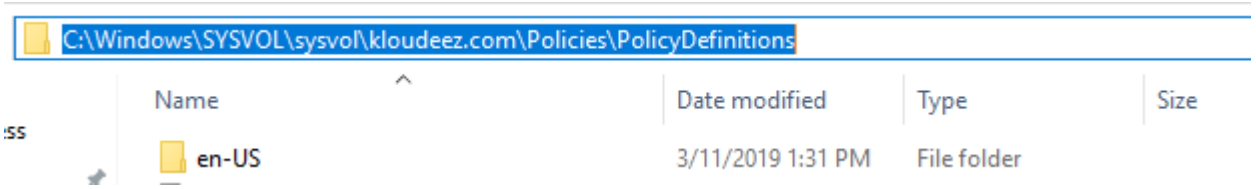


2. Now RDP to your domain controller > goto C:\Windows\SYSVOL\sysvol\<<YourDomain>>\Policies and create a folder called **PolicyDefinitions**

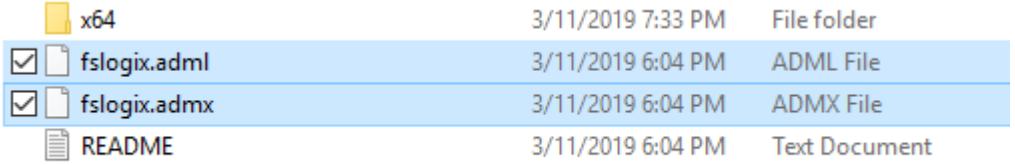


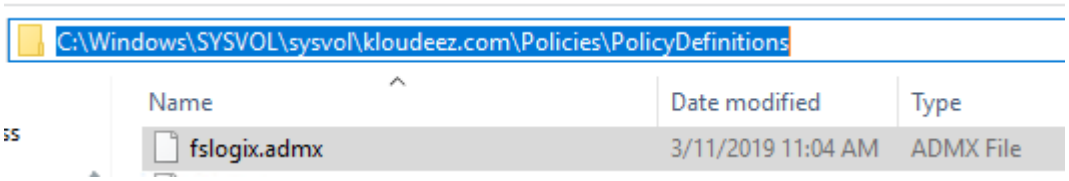
3. Go into the above folder and create another folder called “en-US”

s

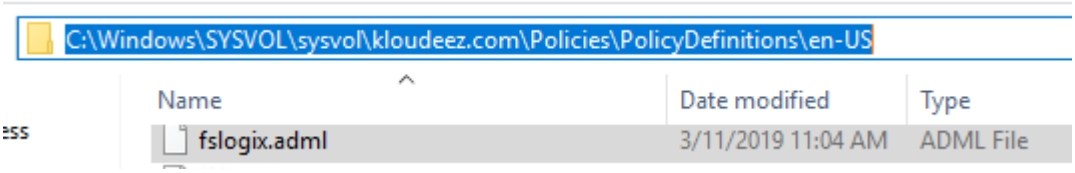


4. From the FSlogix installation folder in the section Install FSLogix on Session Hosts copy the **fslogix.ADMX** file to C:\Windows\SYSVOL\sysvol\<<YourDomain>>\Policies**PoliciesDefinition** folder on the domain controller

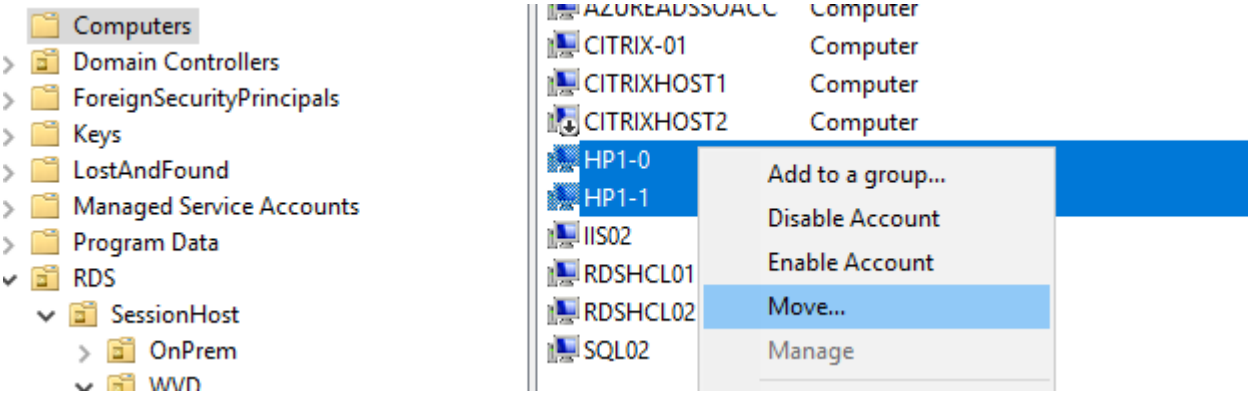


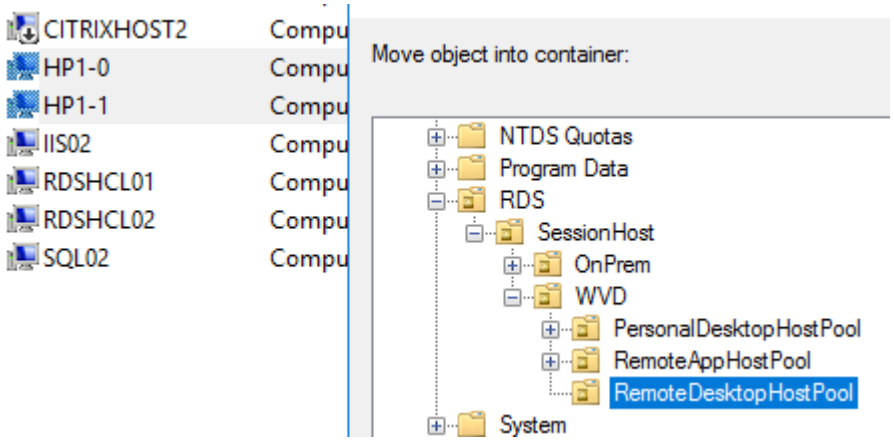


5. Similarly, copy the **fslogix.ADML** file to C:\Windows\SYSVOL\sysvol\<<YourDomain>>\Policies**PoliciesDefinition\en-US** folder on the domain controller

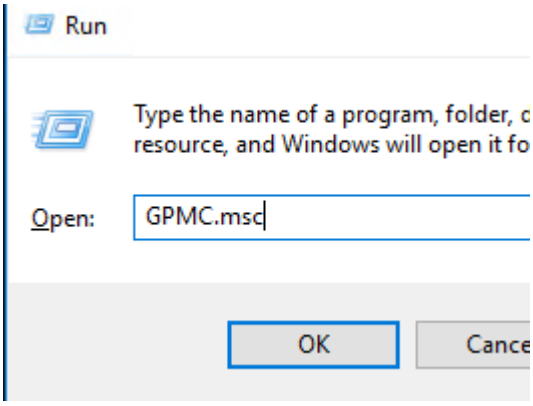


6. Open Active directory users & computers (dsa.msc)
7. Goto the Container/OU where your session hosts are present > CTRL + select the WVD session hosts > right click > move > and move them to the Respective WVD OU > Click OK

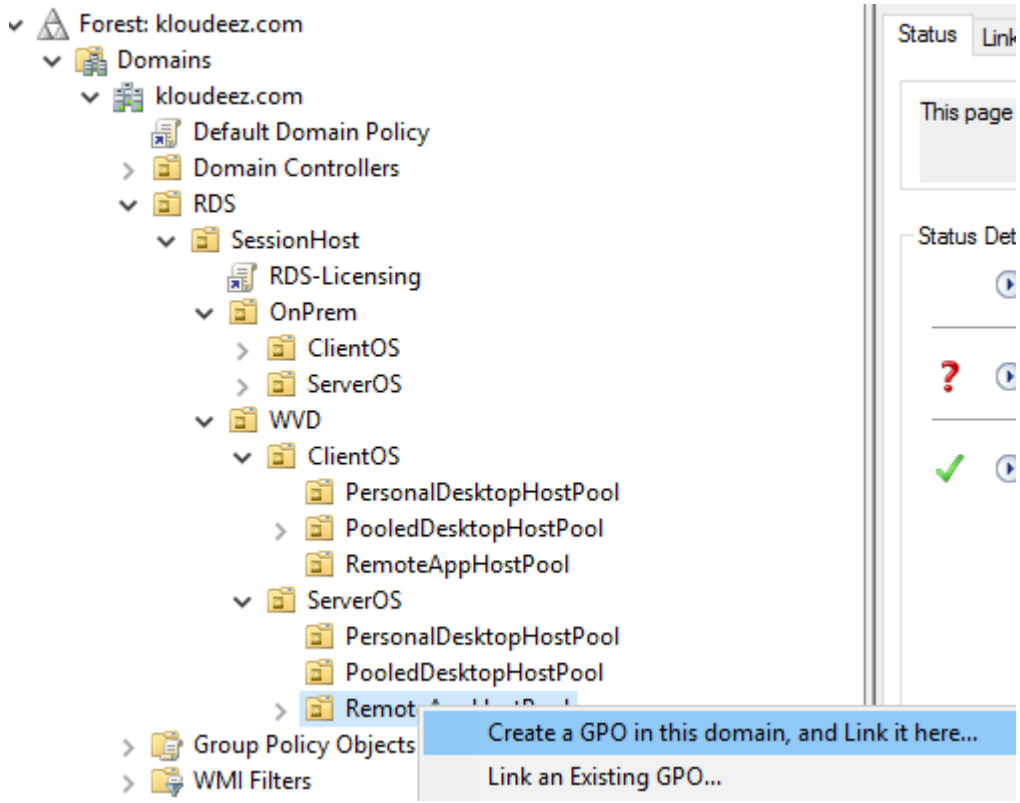




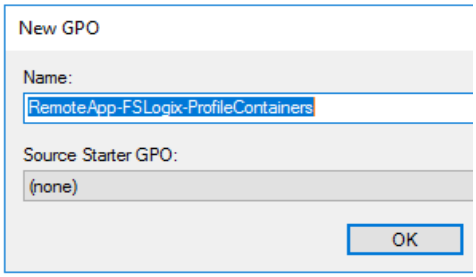
8. Hold Windows key + R > type GPMC.msc to open the group policy management console



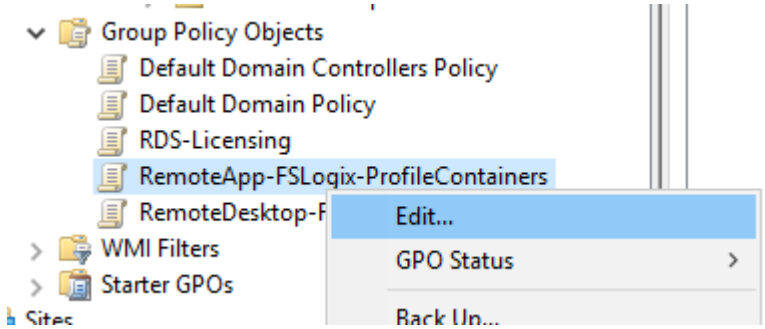
9. Expand the domain and get to the OU where your session hosts exist to create and link a new GPO that will deploy FSlogix container settings



10. Provide a meaningful name for the GPO > OK

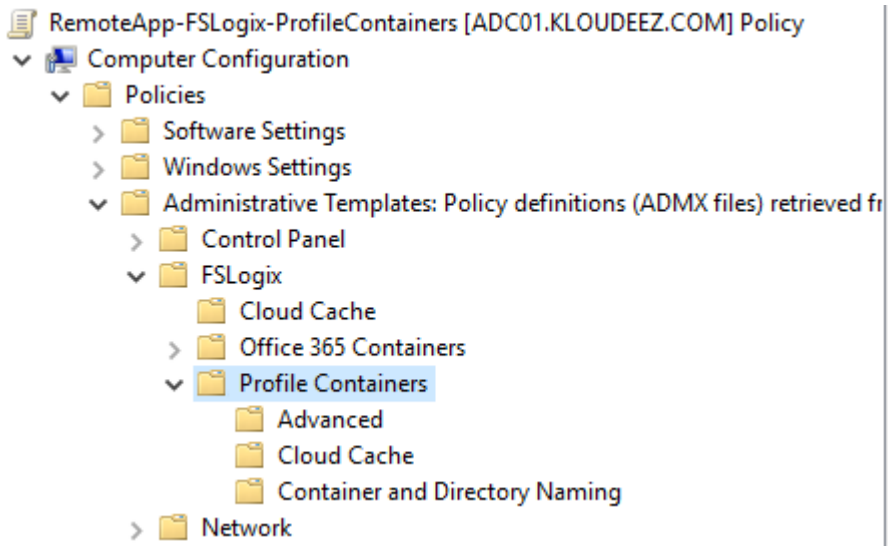


11. Expand the OU to see the new GPO > right click > Edit



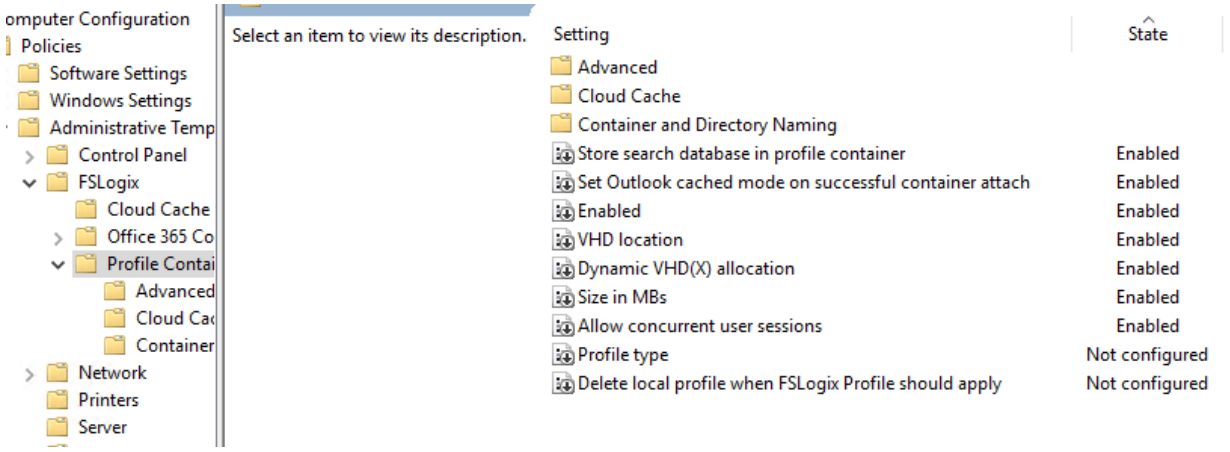
12. This should open the GPO editor

13. Expand Computer Configuration > Policies > Administrative Templates > FSLogix > Profile Containers



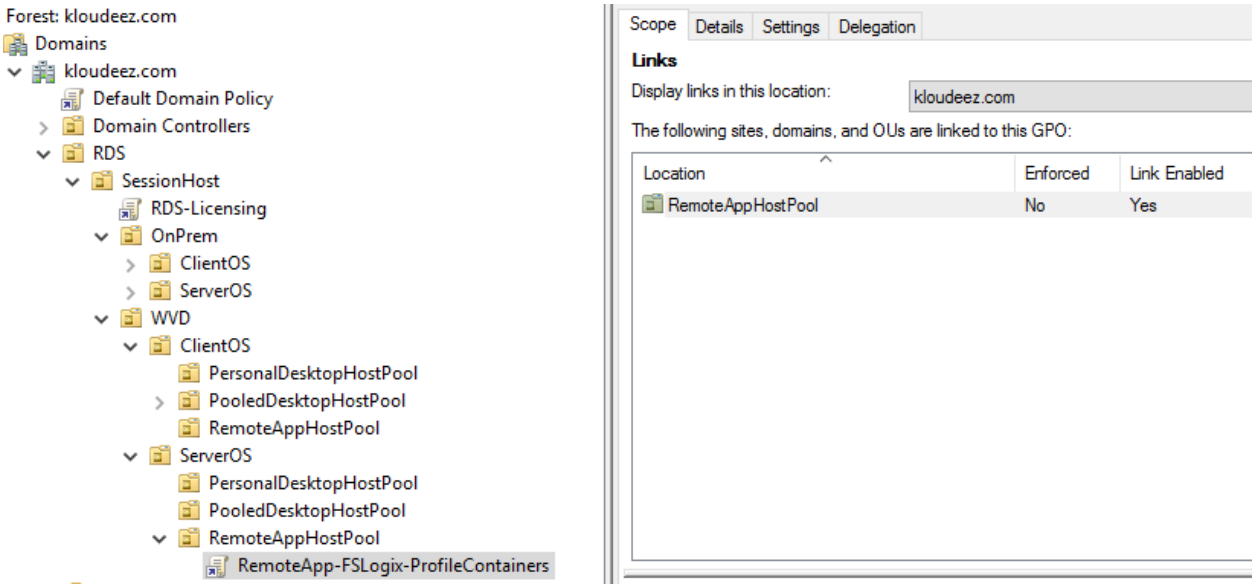
14. Now, using the list below, double click on the respective setting and Enable it so that the session hosts with FSLogix installed will have the same settings updated
    - **Core Settings (These MUST be enabled for FSLogix to function)**
        - Enabled
        - Size in MBs
            - Provide Size in MBs for each user profile (Ex: 10000MB / 10GB)
        - VHD location
            - Use the respective share path you created in section Deploy & Configure Storage for User Profiles (EX: \\S2DUPD\RemoteAppsProfileCont)

    - *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

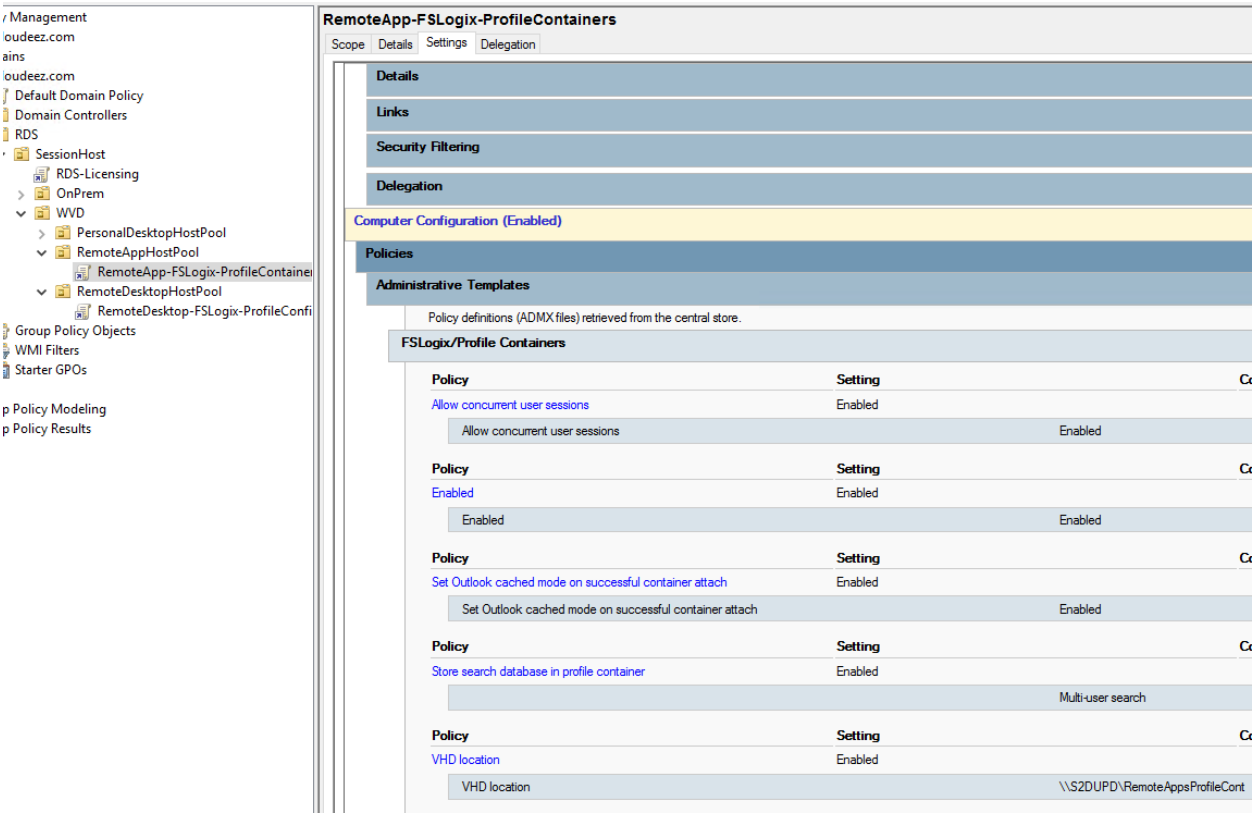


15. Now close the GPO editor and get back to GPMC
16. Select the GPO > on the right under scope ensure that Link Enabled = Yes

ss



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



4.11. Application & Desktop Management

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

4.11.1. Publish Apps & Desktops

1. Check the Default Desktop Application Group is automatically 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      : [redacted]
HostPoolName    : HP1
AppGroupName    : Desktop Application Group
Description     : The default desktop application group for the session host pool
FriendlyName    : Desktop Application Group
ResourceType    : Desktop
```

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

```
#UPDATE THESE VALUES FIRST
$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      : [redacted]
HostPoolName    : HP1
AppGroupName    : MyRemoteApps
Description     :
FriendlyName    :
ResourceType    : RemoteApp


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

3. Run the following cmdlet to get a list of start menu apps on the host pool's virtual machine image. Write down the values for FilePath, IconPath, IconIndex, and other important information for the application you want to publish.

```
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
```

4. Run the following cmdlet to publish a new RemoteApp to the application group and you will need the values from the above command to be used here.

```
#updates these variables with corresponding values form above command that you saved.
$name = "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 $name -Filepath $filepath -IconPath $IconPath -IconIndex $IconIndex
```

```
PS | C:\temp | 03-20-2019 11:13:46 > $appalias = "wordpad"
PS | C:\temp | 03-20-2019 11:14:16 > $filepath="C:\Program Files\Windows NT\Accessories\wordpad.exe"
PS | C:\temp | 03-20-2019 11:14:16 > $IconPath = "C:\Program Files\Windows NT\Accessories\wordpad.exe"
PS | C:\temp | 03-20-2019 11:14:16 > $IconIndex = 0
PS | C:\temp | 03-20-2019 11:14:16 >
PS | C:\temp | 03-20-2019 11:14:16 > New-RdsRemoteApp -TenantName $tenantName -HostPoolName $hostpoolNam
  -IconIndex $IconIndex


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

Now, update the variables and repeat the above commands for any other applications you want to publish. As an example, we are publishing Paint & Snipping Tool in addition to WordPad.

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

```
Get-RdsRemoteApp -TenantName $tenantName -HostPoolName $hostpoolName -AppGroupName $appgroupname | FT
```

```
TenantName,HostPoolName,AppGroupName,RemoteAppName,ShowInWebFe
ed,FilePath,IconPath,IconIndex
```

```
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
```

6. Run the following cmdlet to grant users access to the RemoteApps in the app group

```
#UPDATE THESE VALUES FIRST
$appgroupname = "MyRemoteApps"
$upn = "rdsuser1@domain.com" #this should be the user that
will access WVD resources from your domain

Add-RdsAppGroupUser -TenantName $tenantName -HostPoolName
$HostPoolName -AppGroupName $appgroupname -UserPrincipalName
$upn
```

```
29:24 > $appgroupname = "MyRemoteApps"
29:46 > $upn = "rdsuser1@kloudeez.com"
29:54 > Add-RdsAppGroupUser -TenantName $tenantName -HostPoolName $HostPoolName -AppGroupName $appgroupname -UserPrincipalName $upn
```

```
#check 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@kloudeez.com
TenantName        : [redacted]
TenantGroupName   : Default Tenant Group
HostPoolName      : HP1
AppGroupName      : MyRemoteApps
```

Publish Apps & Desktops

4.11.2. Setup & Configure App Masking

Use Application Masking to manage user access of installed components. Application Masking may be used in both physical and virtual environments. Application Masking is most often applied to manage non-persistent, virtual environments, such as Virtual Desktops.

Please follow the steps below to setup and configure App Masking using FSLogix.

- Verify the prerequisites are met
- Create a rule set
- Test the rule set
- Assign users to the rule set
- Deploy rule sets

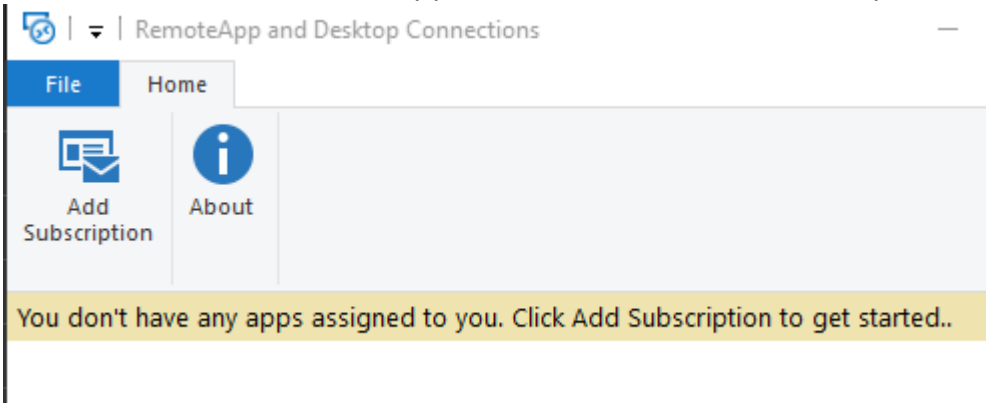
4.11.3. Setup & Configure App Layering

Refer to Liquidware's Flexapp for guidance on App Layering

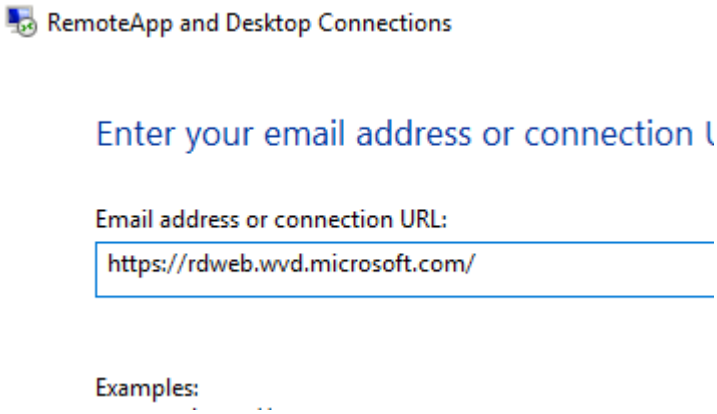
4.12. Validate End User Experience

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. A downloadable client is available that provides access to Windows Virtual Desktop resources from devices running Windows 7 and Windows 10 OR there is also a web client that can be used.

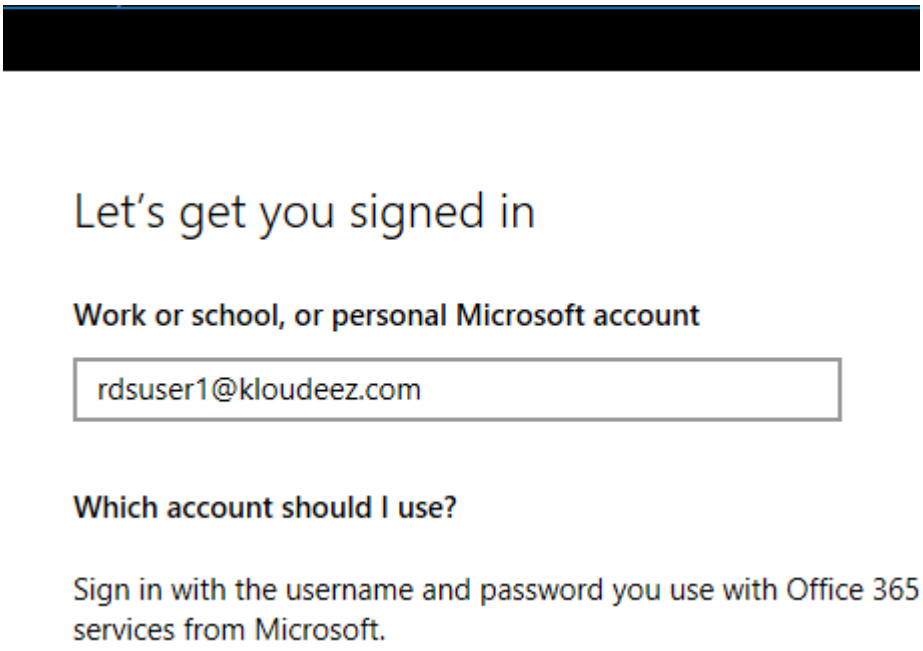
1. Download the client and run the MSI to complete the installation.
2. Start the client from the All Apps List, look for Remote Desktop.

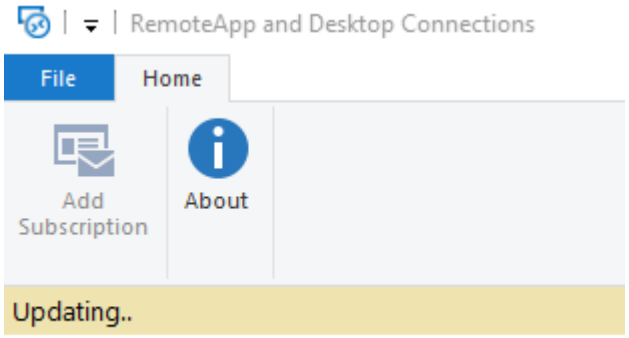


3. Click Add Subscription > provide URL = https://rdweb.wvd.microsoft.com/ > Next > Next Again

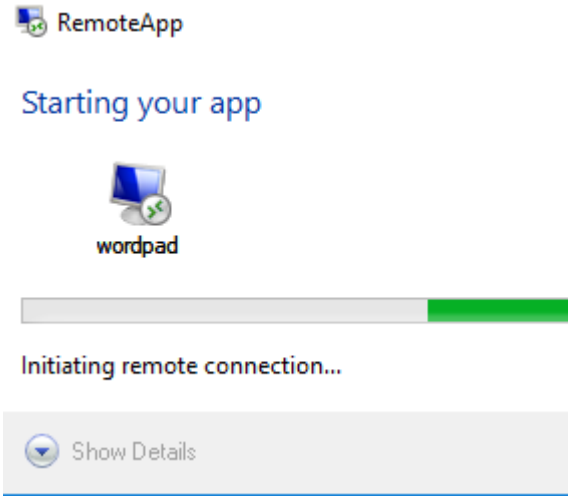


4. Sign in with you're the user account that was granted access to the WVD-RemoteApps in the earlier section > Next



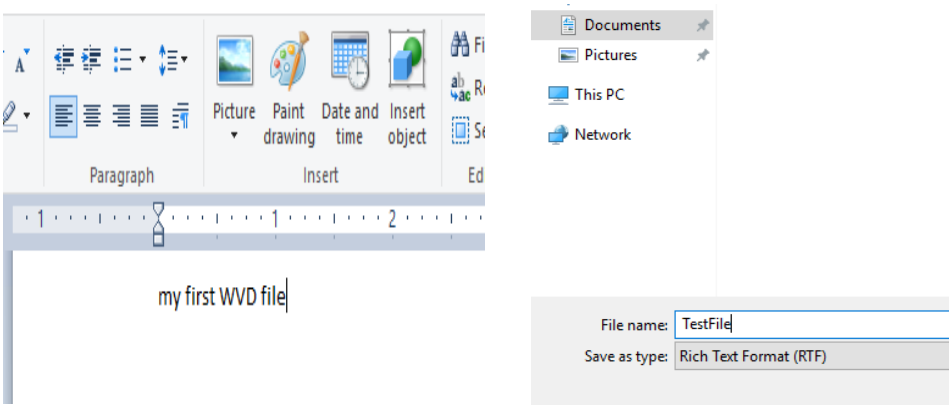


5. After successfully authenticating, you should now see a list of resources available to you.
6. Please launch any of the resources (EX: Wordpad). *please be advised that the first launch may be slow as your user profile is being created.*

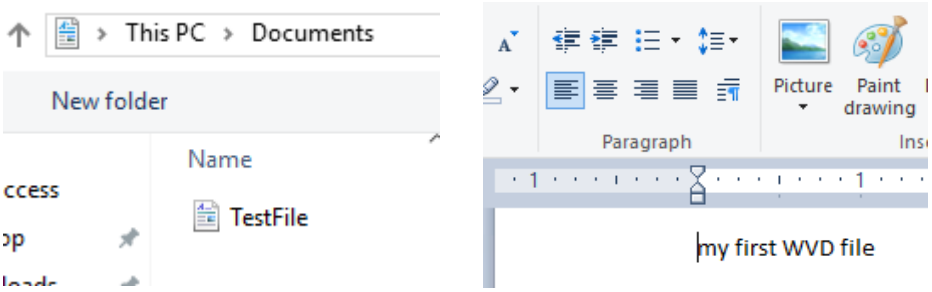


7. Once launched, you can see the icon in your taskbar

8. Now type something > save your file > close WordPad



9. Once again launch WordPad from the WVD client > Ctrl +O > to see you document present.



10. If you are trying to launch O365 applications and hit errors for any reason, please refer to ***WVD-FAQ.docx***

11. 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 ones include latest versions of IE/Edge/Safari/Firefox/Chrome

    - Going to https://rdweb.wvd.microsoft.com
    - Login with user domain credentials
    - Access Apps & Desktops

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

```
#for all AppGroups in a HostPool
Get-RdsUserSession -TenantName $tenantName
```

```
#Filter to a specific for all AppGroup in a HostPool
Get-RdsUserSession -TenantName $tenantName -HostPoolName
$hostpoolName -Verbose
```

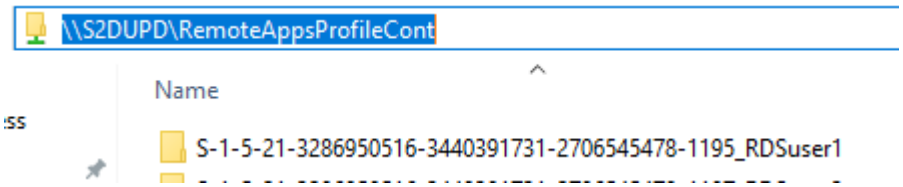
```
PS | C:\temp | 03-15-2019 11:20:06 > Get-RdsUserSession -Ten

TenantGroupName    : Default Tenant Group
TenantName         : [redacted]
HostPoolName       : HP1
SessionHostName    : HP1-1.kloudeez.com
UserPrincipalName  : RDSuser1@kloudeez.com
AdUserName         : KLOUDEEZ\RDSuser1
CreateTime         : 3/15/2019 6:14:14 PM
SessionId          : 3
ApplicationType    : Desktop
SessionState       : Active
```

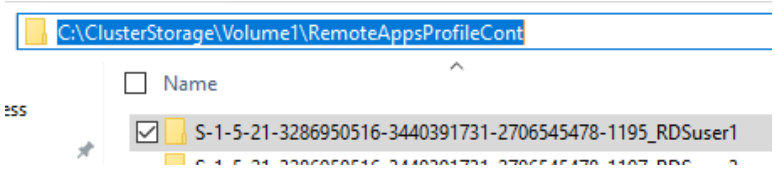
4.13. Validate FSlogix Profile container creation

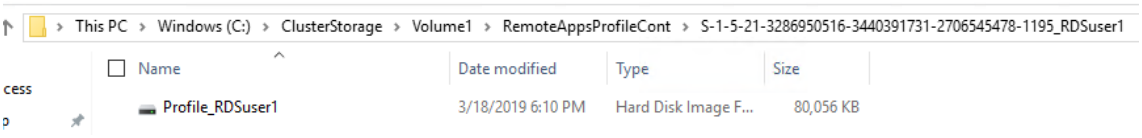
Since we had FSLogix configured on the session hosts for user profile management, all user profiles are saved as FSlogix Profile Containers (VHDx). This section will provide the steps to validate if and where the FSLogix Profile containers are being created.

1. From the Domain controller > open windows explorer
2. In the address bar type the S2D cluster share path [EX: \\S2DUPD\RemoteAppsProfileCont] to see the Profile Container for RDSUSER1



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





4.14. WVD Patch Management

Please refer to Update Management solution in Azure for detailed guidance on how to update WVD Session Hosts.

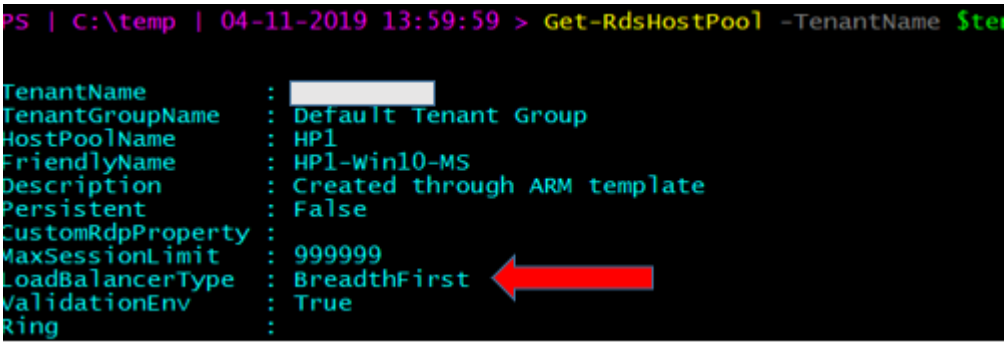
4.15. WVD Management & monitoring

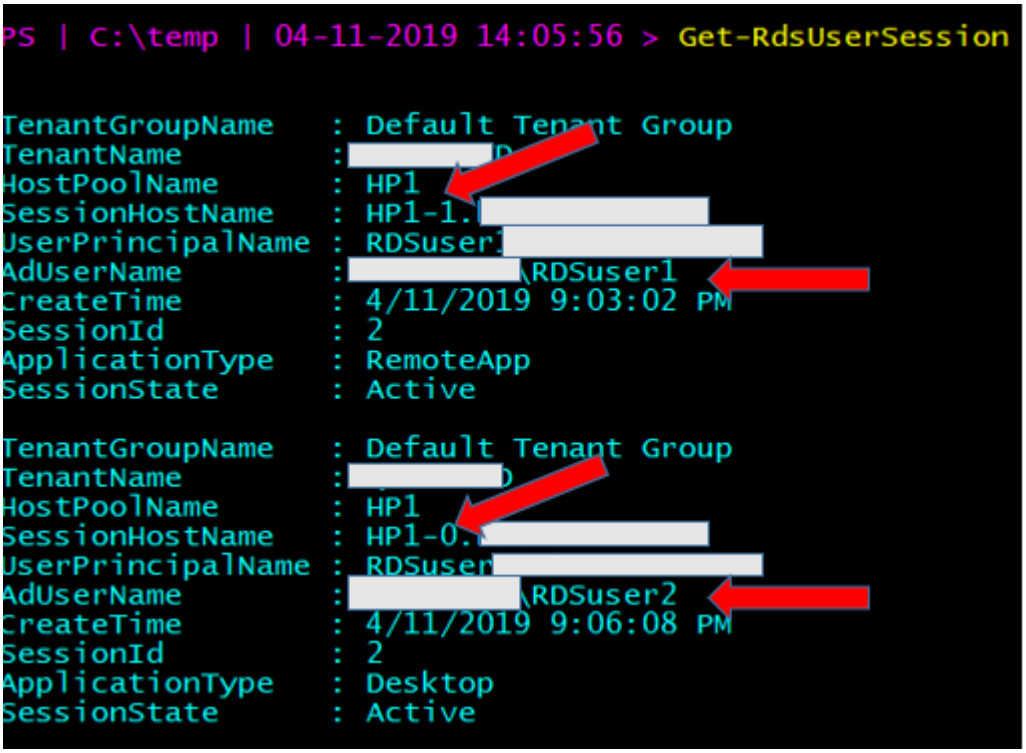
4.15.1. Configure the Load balancing Method

Explanation about the different LB methods is found at Configure the Windows Virtual Desktop load-balancing method . Below are a couple of screenshots that confirm how the session allocation across the session hosts changes with the Load balancing configuration.

Breadth First

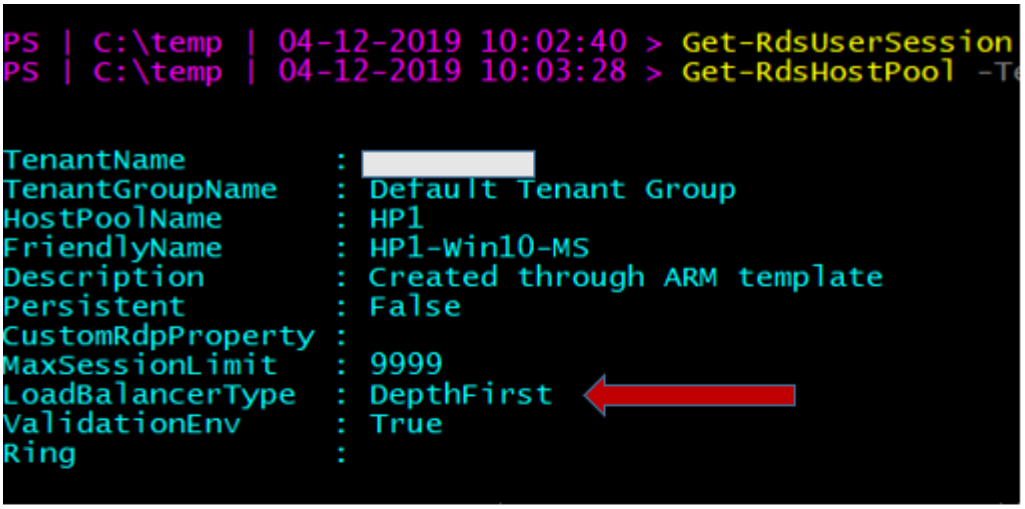
Session Allocation using Breadth-First for a HostPool with 2 VM's. RDSUser1 & RDSUser2 are scattered across the VM's for better using experience.

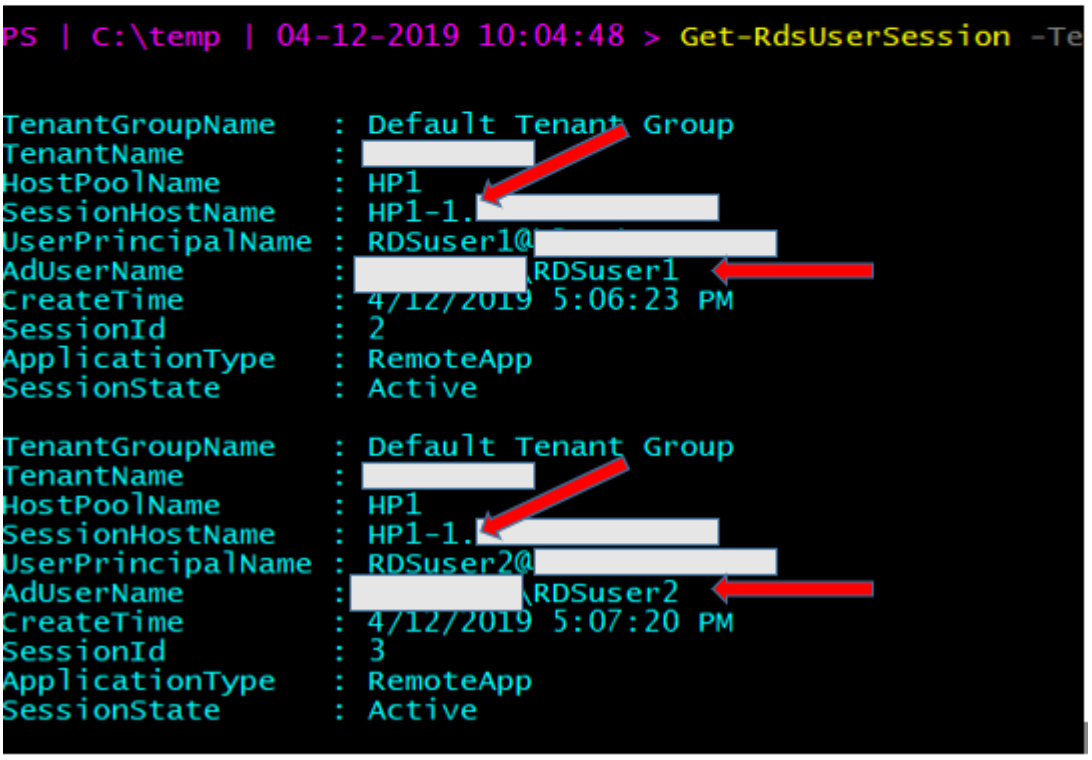




Depth First

Session Allocation using Depth-First for a HostPool with 2 VM's. RDSUser1 & RDSUser2 are logged onto the same VM till the HostPool session limit threshold is met.

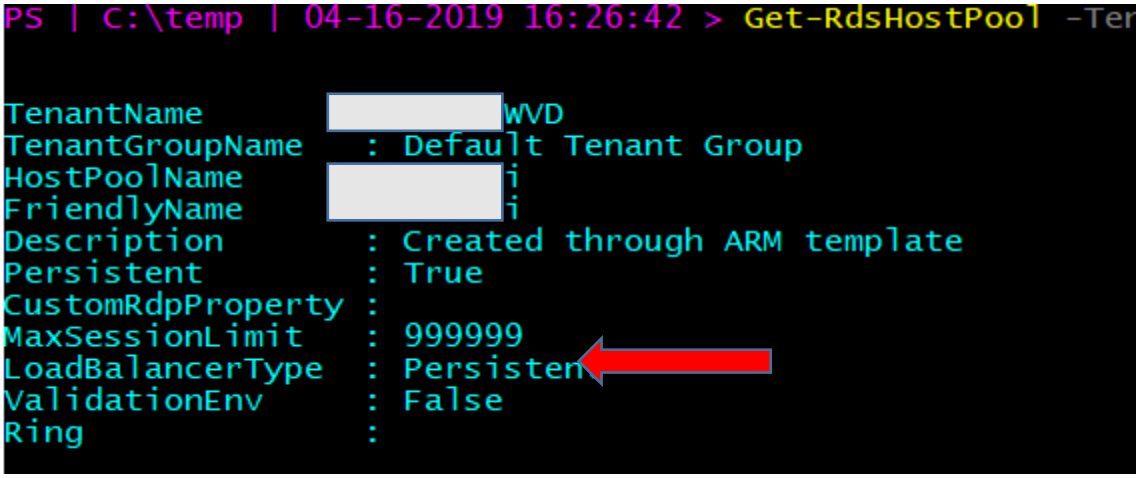


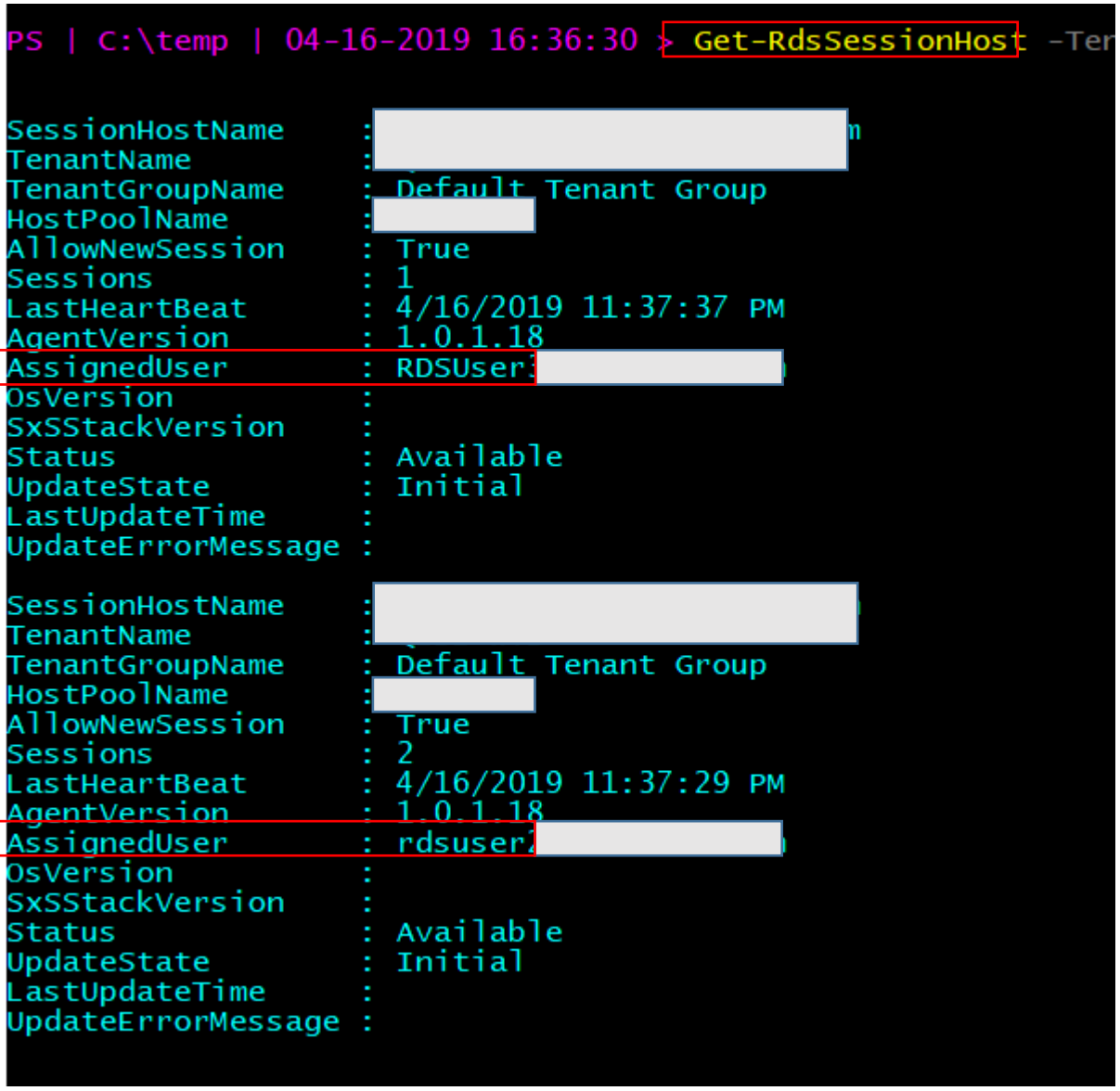


Persistent Desktops

Persistent desktops can only be created at deployment time. A typical use case scenario would be a VDI like environment. Here, users are auto-assigned an available session host during the first logon and any subsequent logins are directed to the same VM.

Unlike multi user session, persistence follows a 1:1 mapping between users → session hosts. For Example: if the HostPool has 5 VM's, they will be assigned to the first 5 users and the 6'th user will get an error that enough resources (VMs) are unavailable.


PS | C:\temp | 04-16-2019 16:26:42 > Get-RdsHostPool -Ter
TenantName : WVD
TenantGroupName : Default Tenant Group
HostPoolName :
FriendlyName :
Description : Created through ARM template
Persistent : True
CustomRdpProperty :
MaxSessionLimit : 999999
LoadBalancerType : Persisten
ValidationEnv : False
Ring :


PS | C:\temp | 04-16-2019 16:36:30 > Get-RdsSessionHost -Ter
SessionHostName :
TenantName :
TenantGroupName : Default Tenant Group
HostPoolName :
AllowNewSession : True
Sessions : 1
LastHeartBeat : 4/16/2019 11:37:37 PM
AgentVersion : 1.0.1.18
AssignedUser : RDSUser
OsVersion :
SxSStackVersion :
Status : Available
UpdateState : Initial
LastUpdateTime :
UpdateErrorMessage :
SessionHostName :
TenantName :
TenantGroupName : Default Tenant Group
HostPoolName :
AllowNewSession : True
Sessions : 2
LastHeartBeat : 4/16/2019 11:37:29 PM
AgentVersion : 1.0.1.18
AssignedUser : rdsuser
OsVersion :
SxSStackVersion :
Status : Available
UpdateState : Initial
LastUpdateTime :
UpdateErrorMessage :

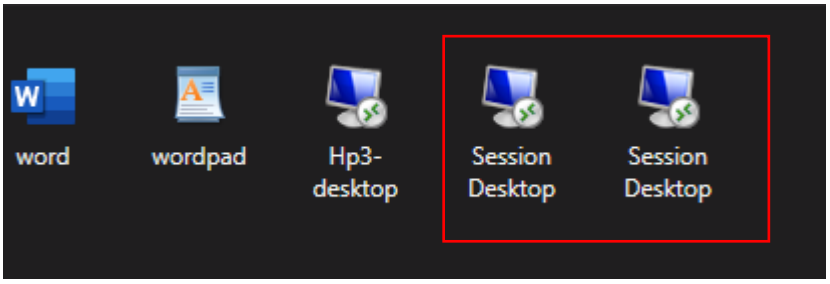
4.15.2. Customize feed for Windows Virtual Desktop users

Using the below command, you can set friendly names to uniquely identify multiple desktops published to a user.

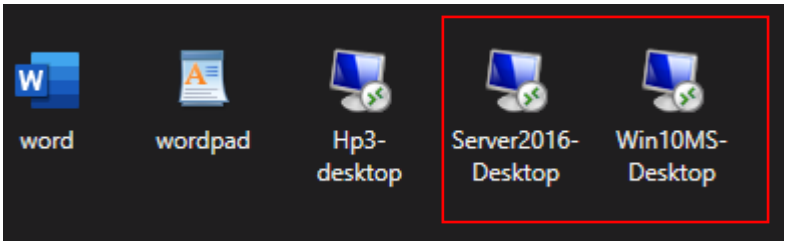
```
#Update the respective $variables first and then execute command

Set-RdsRemoteDesktop -TenantName $tenantName -HostPoolName $
HostPoolName -AppGroupName $AppGroupName -FriendlyName "My custom
Desktop"
```

Before



After



For all other customizations, follow instructions at [Customize feed for Windows Virtual Desktop users]

4.15.3. Customize RDP Properties

Run the Following commands to enable Audio and Camera redirection.

#Camera redirection works only for Windows Client OS.

Set-RdsHostPool -TenantName <tenantname> -Name <hostpool> -CustomRdpProperty camerastoredirect:s:*

Set-RdsHostPool - TenantName <tenantname> -Name <hostpool> -CustomRdpProperty audiomode:i:0

Set-RdsHostPool - TenantName <tenantname> -Name <hostpool> -CustomRdpProperty audiocapturemode:i:1

```
PS C:\Users\Hemanth> Set-RdsHostPool -TenantName qlbl-wvd -Name hp0 -CustomRdpProperty camerastoredirect:s:*


TenantName         : qlbl-wvd
TenantGroupName    : Default Tenant Group
HostPoolName       : HP0
FriendlyName       : HP0
Description        : Created through ARM template
Persistent         : False
CustomRdpProperty  : audiomode:i:0;audiocapturemode:i:1;camerastoredirect:s:*;
MaxSessionLimit    : 999999
LoadBalancerType   : BreadthFirst
ValidationEnv      : False
Ring               :
```

For all other customizations, follow instructions at customize-rdp-properties

4.15.4. Automatically scale Session Hosts

Please follow instructions at Automatically scale session hosts

4.15.5. Deploy the Management UI

Please follow instructions at Deploy a management tool

4.15.6. Check Diagnostic data

Please follow instructions at Identify issues with the diagnostics feature

4.15.7. Check VM Health & Performance

- Please follow the instructions at Enable Azure Monitor for VMs to collect VM health and performance metrics.
- Please follow the instructions at health of your Azure virtual machines to understand your VM Health data.

- Please follow the instructions at VM Performance with Azure Monitor to understand how the VMs are performing.

4.16. Backup & Disaster Recovery (BCDR)

The Azure Site Recovery service contributes to your disaster recovery strategy by managing and orchestrating replication, failover, and failback of on-premises machines and Azure virtual machines (VMs).

Please follow the steps below to configure replication using ASR to protect your session hosts.

- Enable Replication
- Run a test failover
- Failover and reprotect your session hosts
- Failback to primary location

4.17. Migrate to WVD

The migration from a traditional RDS environment to WVD involves some changes w.r.t the fact that the core server roles (Broker/Gateway/Web/SQL) are not needed to be migrated and the focus would be on how to migrate the session hosts along with the user profile data to Azure.

Lift-n-Shift to Azure (Using ASR)

- **When to choose?**
  - If you have persistent VMs to be migrated to Azure
  - If you like to operate VMs with the same OS version as on-prem with WVD.
  - Like to migrate your entire infrastructure to Azure.
  - Do NOT have generalized and/or custom images (with apps pre-installed) that can be readily deployed in Azure.
  - Experienced with replication tools like Azure Migrate & Azure Site Recovery, failovers/failback process.

Lift-n-Shift to Azure - Detailed Migration Steps

First party tools from Azure are available to Lift-n-Shift your On-premise infrastructure to Azure, namely Azure Site Recovery (ASR) and Azure Migrate.

Based on the Hypervisor infrastructure used on-premises, the below table provides a reference point for the correct tool to be used for these operations

Infra	OS/Version	Assessment Tool	Migration Tool	WVD Connectivity
VMWare	Windows Server 2012 R2 +	AZ Migrate	AZ Migrate	Supported
VMWare	Windows 7 Ent	AZ Migrate	AZ Migrate	in-preview
VMWare	Windows 10 Ent	AZ Migrate	AZ Migrate	Supported
Hyper-V	Windows Server 2012 R2 +	AZ Migrate	AZ Migrate	Supported
Hyper-V	Windows 7 Ent	AZ Migrate	AZ Migrate	in-preview
Hyper-V	Windows 10 Ent	AZ Migrate	AZ Migrate	Supported

4.17.1. Migrate Server based RDS resources to Azure-WVD

Hyper-V

For migrating VMs from Hyper-V please follow the steps in the section Migrate Hyper-V VMs

VMWare

For migrating VMs from Hyper-V please follow the steps in the section Migrate VMWare VMs

4.17.2. Migrate Client based VDI resources to WVD.

Hyper-V

For migrating VMs from Hyper-V please follow the steps in the section Migrate Hyper-V VMs

VMWare

For migrating VMs from Hyper-V please follow the steps in the section Migrate VMWare VMs

4.17.3. Install WVD Agents

Once all the VMs are replicated and fail-over into Azure is successful, Please follow the steps in this section to add the VM as a session host to a new or an existing hostpool and publish a Desktop app group and assign users to it.

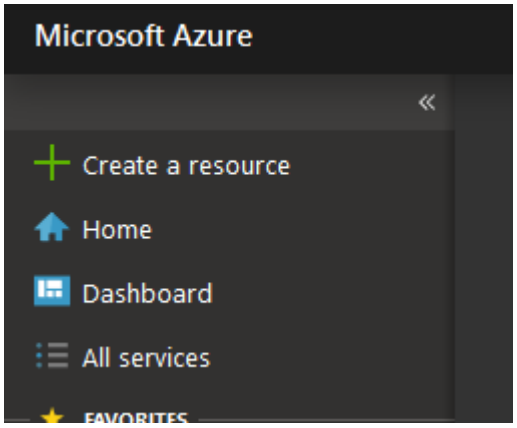
4.17.4. Convert and Migrate User Profiles

Please refer to Liquidware's ProfileUnity for migrating user profiles to WVD.

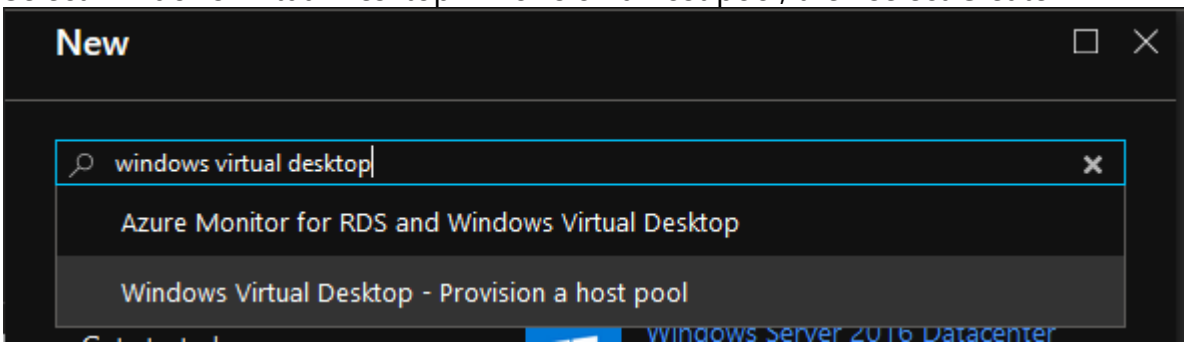
5. Appendix

5.1. Deploy HostPool using Azure Portal (Marketplace)

1. Login into the Azure portal
2. Select + or + Create a resource.

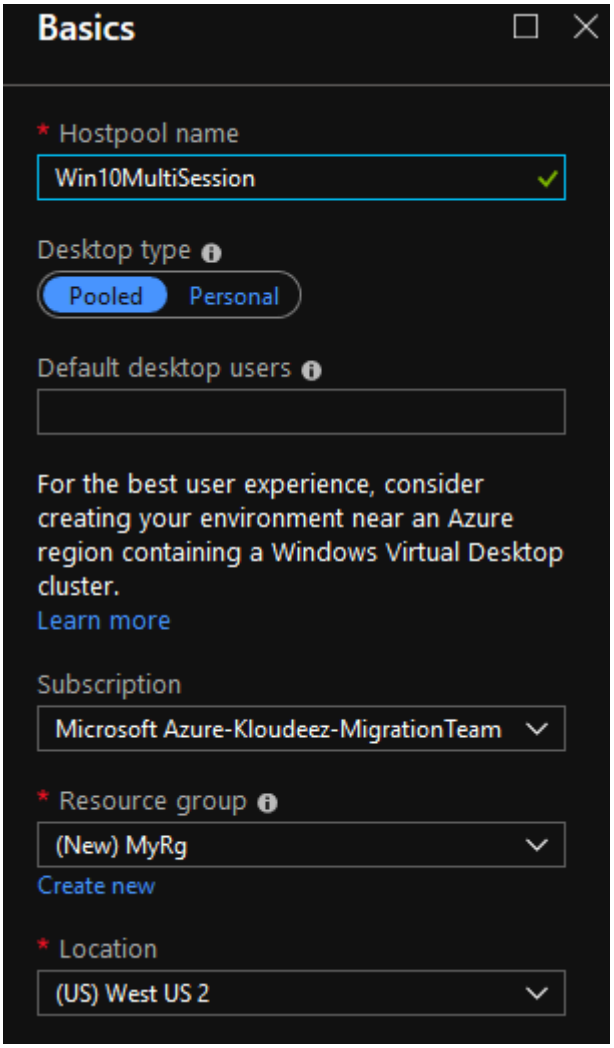


3. Enter Windows Virtual Desktop in the Marketplace search window.
4. Select Windows Virtual Desktop - Provision a host pool, then select Create



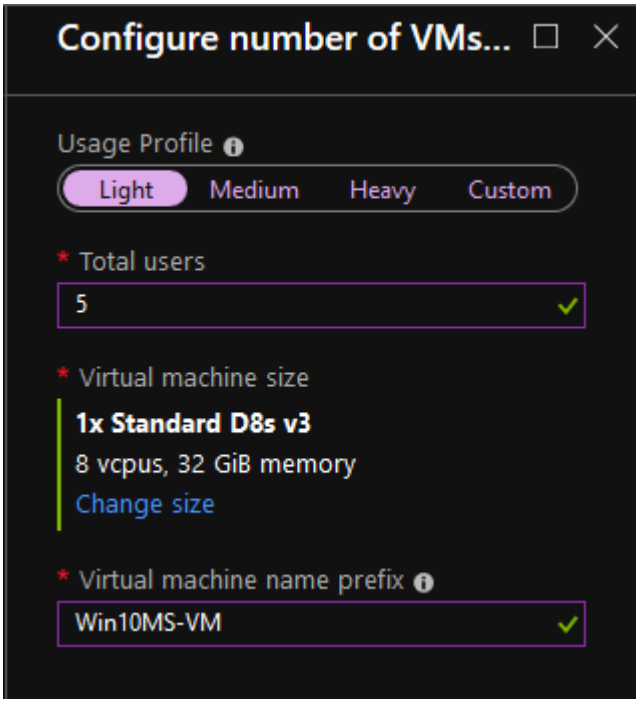
5. For Basic Settings, update as required
   - Enter a name for the host pool that's unique within the Windows Virtual Desktop tenant.

- Select the appropriate option for personal desktop. If you select Yes, each user that connects to this host pool will be permanently assigned to a virtual machine.
- (optional as this can be done later) Enter a comma-separated list of users who can sign in to the Windows Virtual Desktop clients and access a desktop after the Azure Marketplace offering completes. For example, if you'd like to assign user1@contoso.com and user2@contoso.com access, enter "user1@contoso.com,user2@contoso.com."
- Select Create new and provide a name for the new resource group
- For Location, select the same location as the virtual network that has connectivity to the Active Directory server.
- Select OK.

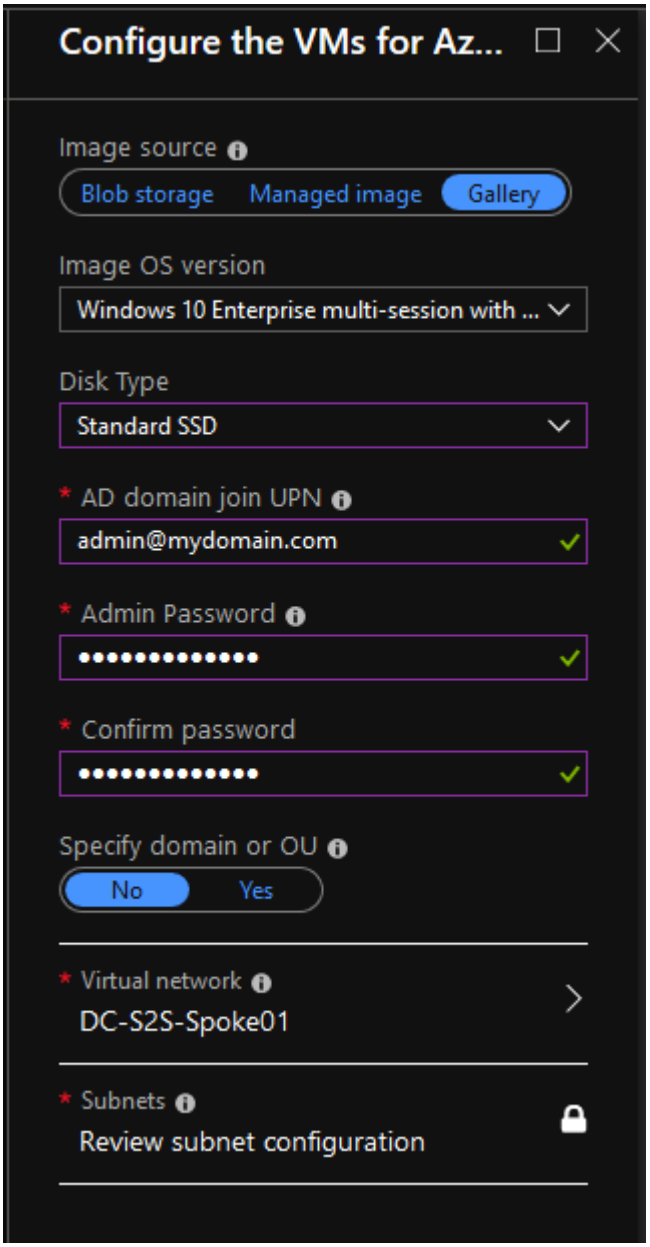


6. For Usage Profile & VM Count, update as required
   - Choose a usage profile and Provide the total # of users
   - You can change the VM size if required

- Enter a prefix for the names of the virtual machines. For example, if you enter the name "prefix," the virtual machines will be called "prefix-0," "prefix-1," and so on.
- Select ok



7. For VM Configuration, do the following
   - Select the Image source and enter the appropriate information on how to find and use it.
     - **Gallery** – Deploy using the approved images readily available from the gallery
     - **Managed Image** – Deploy an existing Azure Image (with your custom applications and configurations saved)
     - **Blob Storage** – If you choose not to use managed disks, select the storage account containing the .vhd file.
   - Enter the user principal name and password for the domain account that will join the VMs to the Active Directory domain. This same username and password will be created on the virtual machines as a local account. You can reset these local accounts later.
   - Select the virtual network that has connectivity to the Active Directory server, then choose a subnet to host the virtual machines.
   - Select OK.

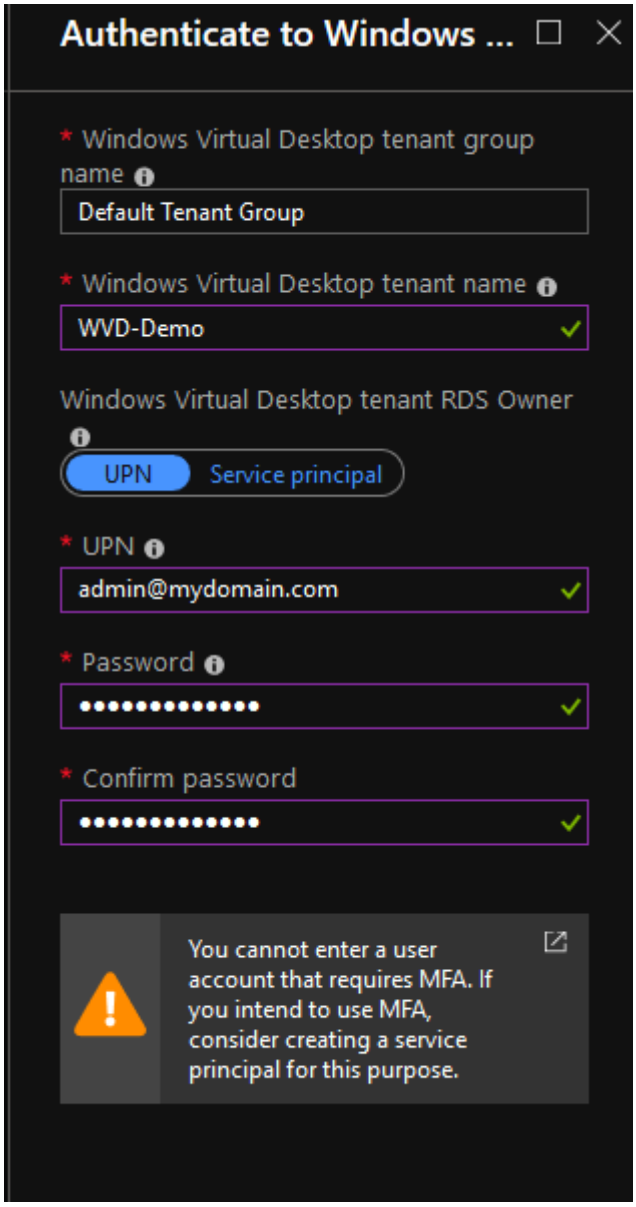


8. For the Windows Virtual Desktop tenant information blade

- Enter the Windows Virtual Desktop tenant group name for the tenant group that contains your tenant. Leave it as the default unless you were provided a specific tenant group name.
- Enter the Windows Virtual Desktop tenant name for the tenant you'll be creating this host pool in.
- Specify the type of credentials you want to use to authenticate as the Windows Virtual Desktop tenant RDS Owner. If you completed the Create service principals and role assignments with PowerShell tutorial, select Service principal.

You will now need to enter the Azure AD tenant ID of the Azure Active Directory that contains the service principal.

- Enter either the credentials for the tenant admin account. Only service principals with a password credential are supported.
- Select OK.

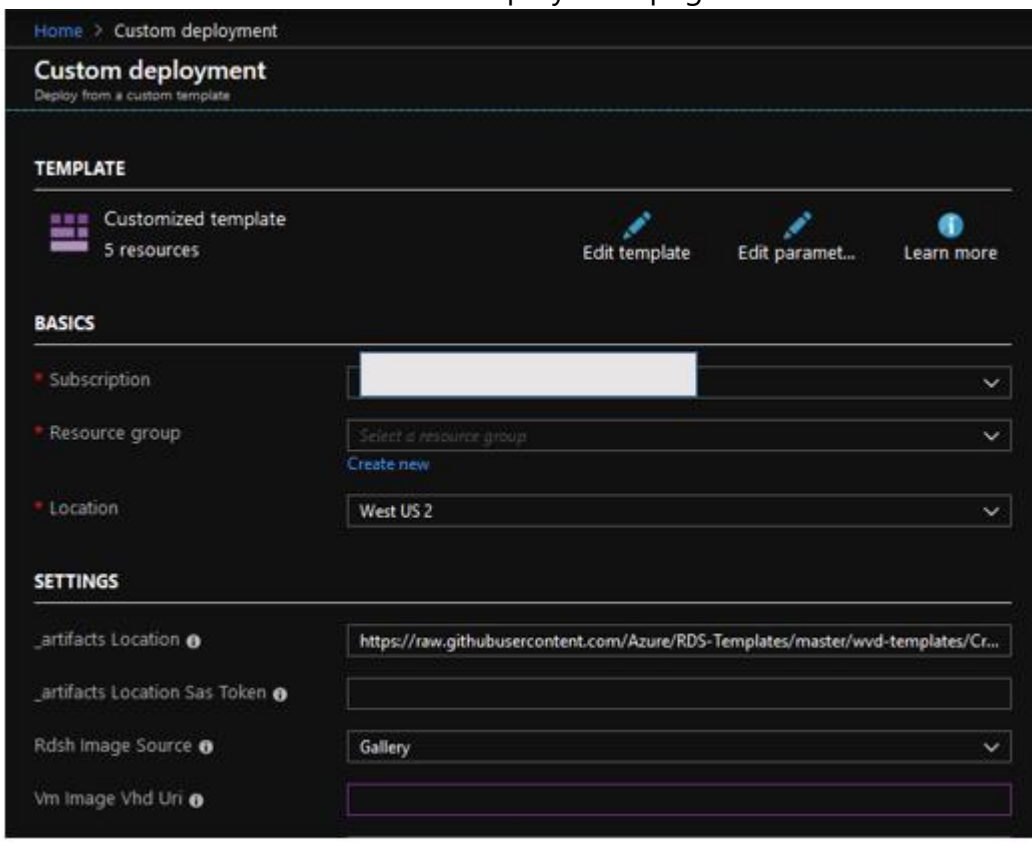


9. In the Summary blade, review the setup information. If you need to change something, go back to the appropriate blade and make your change before continuing. If the information looks right, select OK.
10. In the Buy blade, review the additional information about your purchase from Azure Marketplace.
11. Select Create to deploy your host pool

12. Follow the deployment progress under notifications and if you get any errors, please refer Tenant and host pool creation

5.2. Deploy HostPool using ARM template

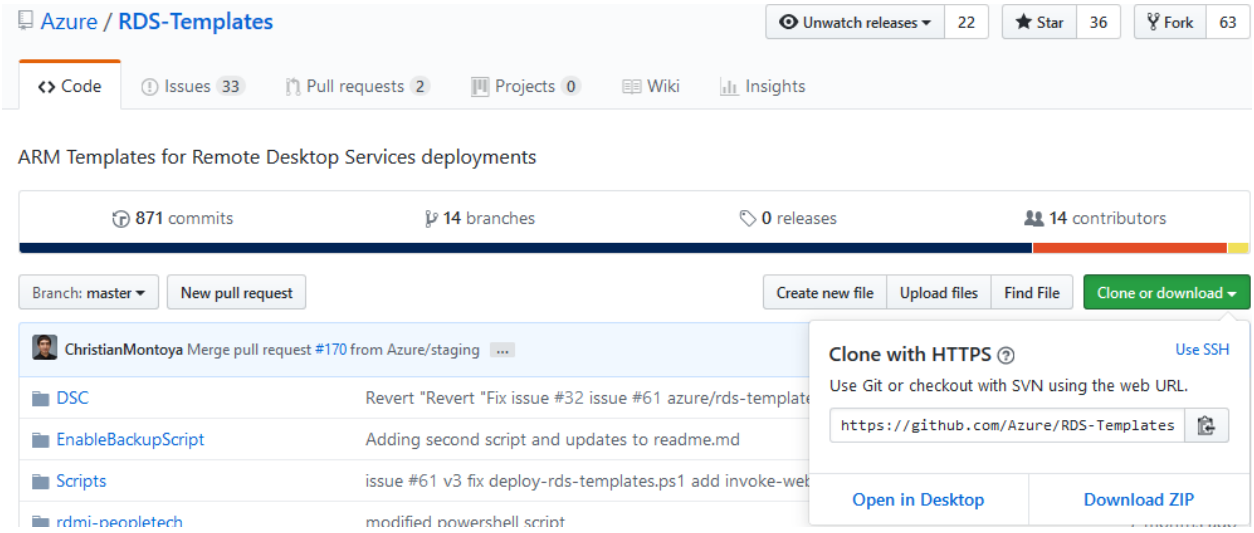
1. Goto here > scroll to the bottom and click on Deploy to Azure
2. If required, ensure you authenticate / login to azure using the correct credentials to land on the custom deployment page



3. On the custom deployment page, complete all the required fields (which are mostly self-explanatory). If there are default values in any of the fields, leave them for the most part unless you know if they need to be updated.
4. Once all required fields are completed > accept terms & conditions & click purchase
5. Wait for the deployment to complete and if there are any errors refer **here**

5.3. Deploy HostPool using modified ARM template

1. You will need a GitHub account for this.
2. Goto here > click on Fork > to obtain the repo



3. In your repo, update the _artifactsLocation parameter in **Create and provision WVD host pool\mainTemplate.json** to the raw URL of the file on GitHub (Ex: https://raw.githubusercontent.com/yourusername/RDS-Templates/master/wvd-templates/Create%20and%20provision%20WVD%20host%20pool/mainTemplate.json)

```
"parameters": {
    "_artifactsLocation": {
        "type": "string",
        "metadata": {
            "description": "The base URI where artifacts required by this template are located."
        },
        "defaultValue": "https://raw.githubusercontent.com/Azure/RDS-Templates/master/wvd-templates/Create%20and%20provision%20WVD%20host%20pool"
    },
```

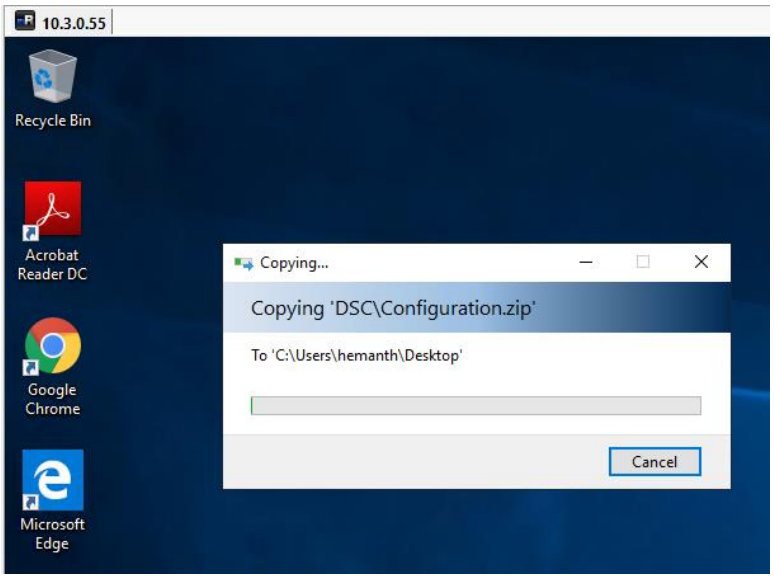
4. Update the rdshGalleryImageSKU parameter as per the below image in the files below:
   - ***Create and provision WVD host pool\mainTemplate.json***
   - ***Create and provision WVD host pool\nestedtemplates\managedDisks-galleryvm.json***
   - ***Create and provision WVD host pool\nestedtemplates\unmanagedDisks-galleryvm.json***

```
"rdshGalleryImageSKU": {
    "type": "string",
    "metadata": {
        "description": "(Required when rdshImageSource = Gallery) Gallery image SKU."
    },
    "allowedValues": [
        "Windows-10-Enterprise-multi-session-with-Office-365-ProPlus",
        "Windows-10-Enterprise-multi-session",
        "2016-Datacenter",
        "2012-R2-Datacenter",
        "2019-Datacenter"
    ],
    "defaultValue": "Windows-10-Enterprise-multi-session-with-Office-365-ProPlus"
},
```

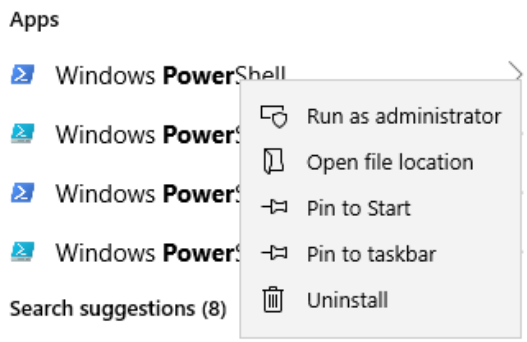
5. Now follow instructions here to deploy using a custom ARM template

5.4. Install WVD Agents manually

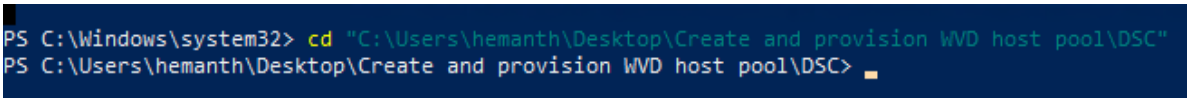
1. Download the template and DSC bits from here onto the VM in Azure. Extract the zip file.



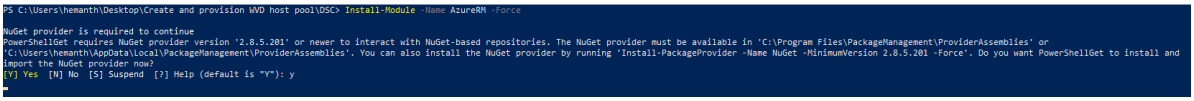
2. Run PowerShell as an Administrator.



3. CD into the DSC Folder you copied in the first step.



4. Run the following command to install the AzureRM Module.
    - Install-Module -Name AzureRM -Force

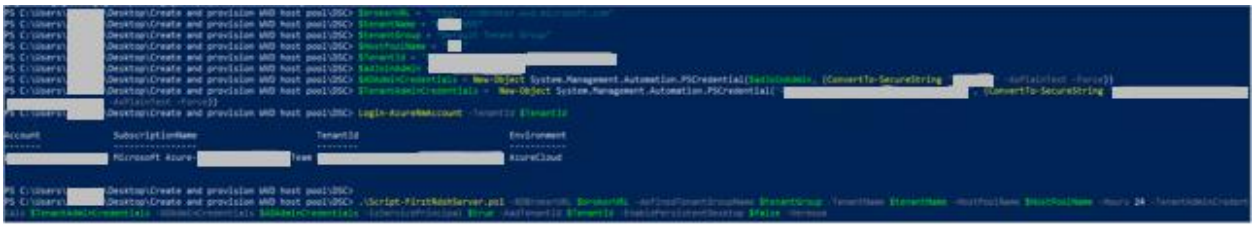


    - This step might take a while to install all required modules and sub-modules.

5. Copy the following script into a Notepad and modify the fields as required and run in PowerShell to install the WVD Agents and either register to an existing HostPool or create a new one.

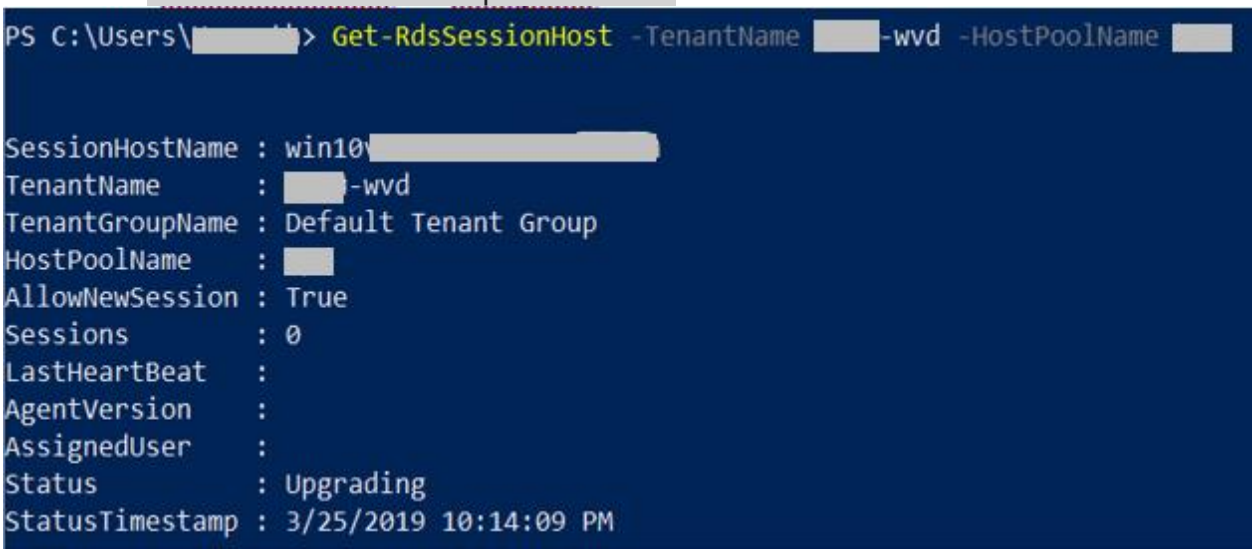
```
$brokerURL = "https://rdbroker.wvd.microsoft.com"
$tenantName = "<<WVD Tenant Name>>"
$tenantGroup = "<<WVD Tenant Group>>"
$HostPoolName = "<<HostPool Name>>"
$TenantId = "<<Tenant ID>>"
$adJoinAdmin = "<<Admin UPN>>"
$ADAdminCredentials = New-Object
System.Management.Automation.PSCredential($adJoinAdmin,
(ConvertTo-SecureString "<<Admin Password>>” -AsPlainText
-Force))
$TenantAdminCredentials =  New-Object
System.Management.Automation.PSCredential("<<Wvd tenant
admin UPN>>", (ConvertTo-SecureString "<<Admin
Password>>" -AsPlainText -Force))
Login-AzureRmAccount -TenantId $TenantId  --Login with
Global Admin Credentials
```

```
.\Script-FirstRdshServer.ps1 -RDBrokerURL $brokerURL -
definedTenantGroupName $tenantGroup -TenantName
$tenantName -HostPoolName $HostPoolName -Hours 24 -
TenantAdminCredentials $TenantAdminCredentials -
ADAdminCredentials $ADAdminCredentials -
isServicePrincipal $true -AadTenantId $TenantId -
EnablePersistentDesktop $false -Verbose
```



6. This will install all the required modules in the VM and if the Hostpool name specified in the parameters is new, a new HostPool will be created and the VM will be registered with it.
7. Check the status from Powershell by running the following command against WVD. The status should say available.

```
Get-RdsSessionHost -TenantName <<tenant name>> -
HostPoolName <<hostpool name>>
```



- The status in the above image should change to Available for us to be able to use the Session host to publish applications/desktops.

```
PS C:\Users\Hemanth> Get-RdsSessionHost -TenantName [redacted]-wvd -HostPoolName [redacted]

SessionHostName : win10[redacted]
TenantName      : [redacted]-wvd
TenantGroupName : Default Tenant Group
HostPoolName    : [redacted]
AllowNewSession : True
Sessions        : 1
LastHeartBeat   : 3/25/2019 10:24:24 PM
AgentVersion    : 1.0.1.8
AssignedUser    :
Status          : Available
StatusTimestamp : 3/25/2019 10:24:24 PM
```

8. Note: This process might take 10 to 15 minutes to complete.
9. Once the session hosts are available, follow the guidelines here to publish applications/desktops as required.

5.5. Check Group Policy updates remotely

ONLY if you have PowerShell remoting enabled on your session hosts, with PowerShell using the below commands you can remotely update the servers to get the latest group policy and check the latest ones were applied

```
#update these values first
$sessionhost = “HP1-0”

#update group policy
ICM -ComputerName $sessionhost -ScriptBlock { gpupdate /force}
```

```
PS C:\Windows\system32> ICM -ComputerName HP1-0 -ScriptBlock { gpupdate /force}
Updating policy...


Computer Policy update has completed successfully.

User Policy update has completed successfully.
```

```
#check if the new GPO was applied
ICM -ComputerName $sessionhost -ScriptBlock { gpresult /r /scope computer}
```

```
PS C:\Windows\system32> ICM -ComputerName HP1-0 -ScriptBlock { gpresult /r /scope computer}

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
c 2018 Microsoft Corporation. All rights reserved.

Created on ?3/?20/?2019 at 9:44:20 PM


RSOP data for  on HP1-0 : Logging Mode
-------------------------------------

OS Configuration:            Member Server
OS Version:                  10.0.17763
Site Name:                   Default-First-Site-Name
Roaming Profile:
Local Profile:
Connected over a slow link?: No


COMPUTER SETTINGS
------------------

    Last time Group Policy was applied: 3/20/2019 at 8:52:09 PM
    Group Policy was applied from:      ADC01.kloudeez.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        KLOUDEEZ
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        RemoteDesktop-FSLogix-ProfileConfiguration
        RDS-Licensing
        Default Domain Policy

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
```

5.6. Get the Object SID

1. Login to the domain controller > open PowerShell and type the below command

```
#update the value first
$identity = ”RDSuser1”

Get-ADUser -Identity $Identity | select Name,SID
```

```
PS C:\Windows\system32> $identity = "RDSuser1"
PS C:\Windows\system32> Get-ADUser -Identity $Identity | select Name,SID

Name      SID
----      ---
RDSuser1 S-1-5-21-3286950516-3440391731-2706545478-1195
```

5.7. Get error details to help investigations

If there are errors during the hostpool / Session host provisioning process, then please do the following to get the error details to help with any investigations

1. If the deployment fails half way through, In the Azure portal, goto the respective Resource Group > Deployments > Click the Error > click RAW ERRROR > copy that information

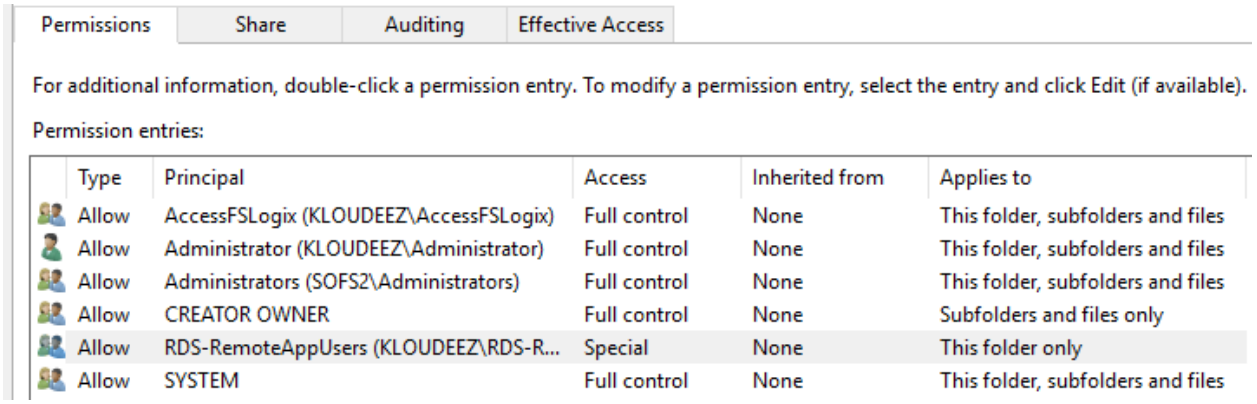
2. Assuming the deployment completes (session host has been created) but there are errors with the WVD-Agent installation phase using PowerShell DSC, then:
    a. RDP to the session host using the privateIP
    b. Goto C:\Windows\TEMP\scriptlogs.log to find any related errors
3. Share that information with an engineer that will help you.

5.8. Set NTFS & Share permissions

1. Right click on the volume > goto Security and click advanced at the bottom
    a) 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
local or File cluster Administrators	The local Administrator OR *File cluster administrators (if present)*	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 users that use RemoteApps	This Folder, Subfolders and Files	Create Folder/Write Data List Folder/Read Data Read Attributes Traverse Folder/Execute File

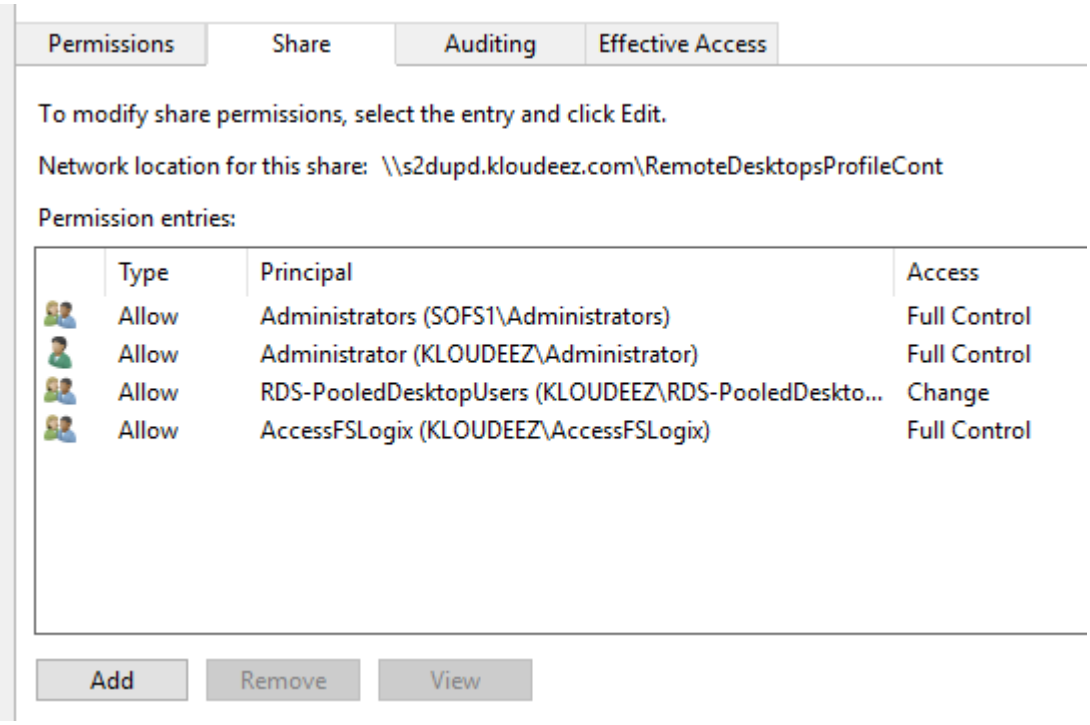
2. Repeat the above step for all other objects (in the above table) you need to set permissions for
    a) Once done, your NTFS permissions window should look relative to below. Now click Apply



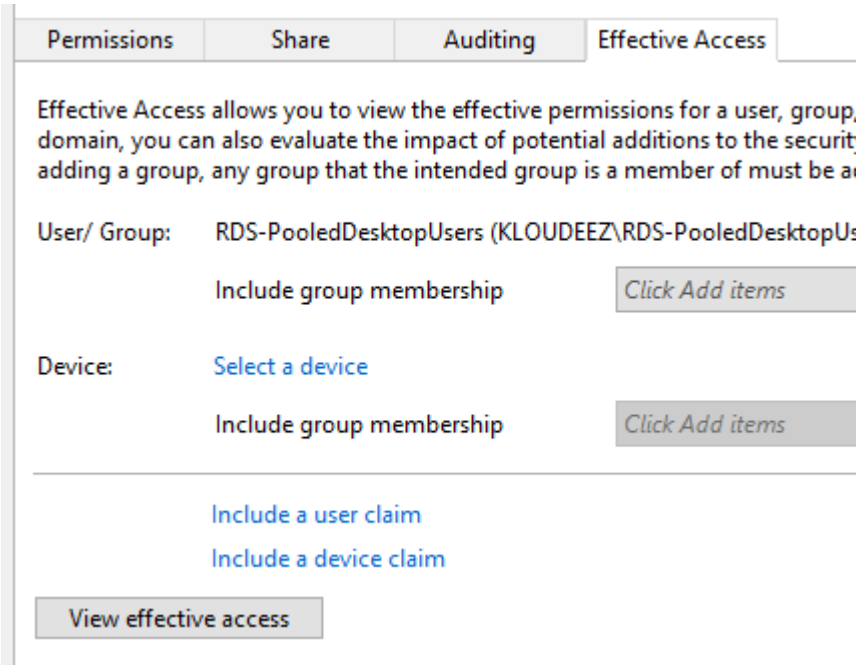
3. Now we will set Share permissions. Click on Share at the top > click Add
    a) Click Select a principal > Select the respective AD object we want to set permissions > click ok > Set Type = Allow > Permissions = value From Permissions column in the table below

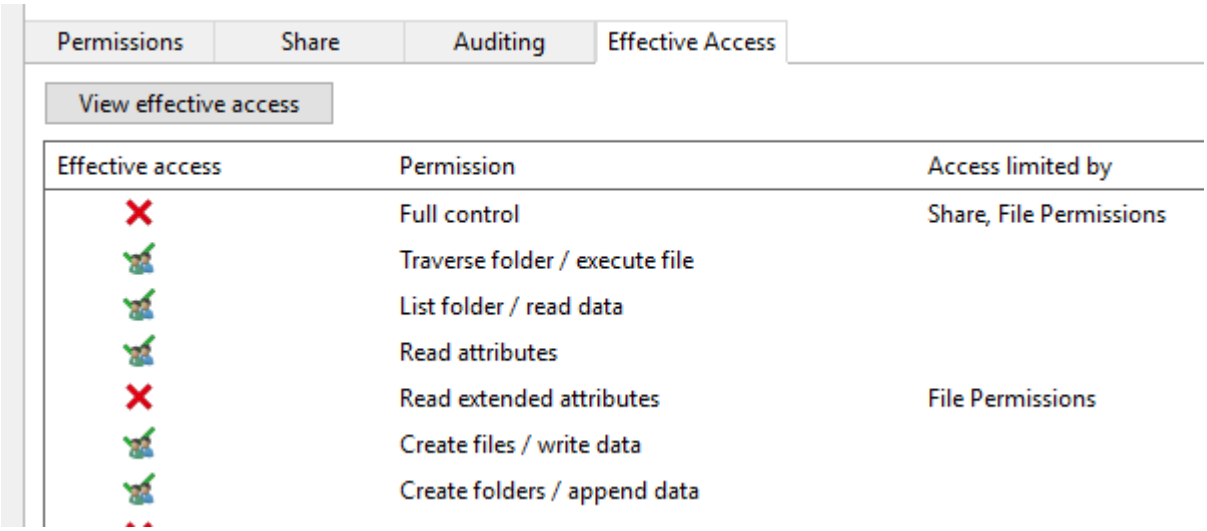
User Account	Description	Permissions
Domain Administrators	Your Domain Administrator AD Security Group	Full Control
File cluster Administrators	The local File cluster Administrator	Full Control
Domain\AccessFSLogix	AD Security group containing Session Host computer objects that can access/control these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

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



4. 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.





5. Click OK > again OK in the Properties window to save your changes

5.9. Migrate Hyper-V VMs

1. Prepare Azure environment/resources for replicating On-premise VMs by following the guidelines here.
    i. Ensure that a new VNET, Resource Group isolated from your primary/production environment are created for the purposes of testing.
2. Once the Azure environment is setup as directed above, also prepare the on-premises Hyper-V by following the guidelines here.
    ii. An ASR agent needs to be installed on the Hyper-V VM. Ensure you have appropriate permissions to perform the installation.
    iii. Enable RDP on the VM to ensure connectivity after failover.
3. Setup and configure Azure Migrate Tool and appliance. Please follow the guidelines here.
4. Perform a Test migration of the replicated VMs in Azure to ensure all the data is being replicated properly and the VMs are functioning as they should. Please follow the guidelines here.
    iv. Ensure you select a VNET, resource group that is separate from your primary/production environment.
    v. You will also need AD connectivity and will require to failover your on-prem AD server as well.

vi. Since this VM is now in an isolated environment, it needs a Public IP to be able to accessible. Assign a public IP to the Test NIC and then RDP using this IP.

5. Perform a Final migration to Azure to successfully cutover the Hyper-V VM and start using the Azure VM by following the guidelines here.

vii. When performing a Final Failover, the VM needs to be in the primary/production VNET to ensure the servers are talking to each other in your environment.

5.10. Migrate VMWare VMs

1. Azure Migrate can migrate VMWare VMs using both agent-based and agentless approaches. Choose the appropriate method based on your requirements. Refer to the comparison here.
2. Prepare Azure environment/resources for replicating On-premise VMs by following the guidelines here.
    a) Ensure that a new VNET, Resource Group isolated from your primary/production environment are created for the purposes of testing.
3. Once the Azure environment is setup as directed above, also prepare the on-premises VMWare
    a) Agentless
    b) Agent-based
    c) A VM needs to be imported when setting up replication. Ensure you have appropriate permissions to perform the installation.
4. Setup and configure Azure Migrate for replication. Below are the instructions for
    a) Agentless
    b) Agent-based
5. Perform a Test Failover of the replicated VMs in Azure to ensure all the data is being replicated properly and the VMs are functioning as they should. Please follow the guidelines here.
    a) Ensure you select a VNET, resource group that is separate from your primary/production environment.
    b) Since this VM is now in an isolated environment, it needs a Public IP to be able to accessible. Assign a public IP to the Test NIC and then RDP using this IP.
6. Perform a Final Failover to Azure to successfully cutover the VMWare VM and start using the Azure VM by following the guidelines here.

a) When performing a Final Failover, the VM needs to be in the primary/production VNET to ensure the servers are talking to each other in your environment.