Microsoft

Migrating from RDS to Windows Virtual Desktop (WVD): Technical Guide

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

Contents

1. Introduction

The ***primary intent of this guide is to illustrate transitioning from an on-premise RDS 2016 deployment to WVD Session Host in Azure***. It is intended to be used by Customer & Partners to help familiarize themselves with the processes, methodologies and tools required to migrate their on-premise RDS workloads into Azure and integrate with the WVD service/platform.

2. Target Audience

This document is ***Level 400+ technical migration 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 on-premise to Azure (WVD) migrations. 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 migration process and is NOT a primer for the technologies afore mentioned.

3. Prerequisites/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.***

- ✓ Presence of an on-premises datacenter / dev-test environment where you currently have an active RDS deployments.
- ✓ Need admin level access and in-depth knowledge to manage infrastructure level services like Active Directory, GPO management, DNS, Networking ETC.
- ✓ Admin level access to all the components in the on-premises RDS deployments is required along with in-depth knowledge of how RDS deployments are configured, user access, ETC.
- ✓ Knowledge and comfortability in managing Azure services like:
    - o Azure Compute (VMs/Availability Sets)
    - o Azure Storage (disks/storage accounts)
    - o Azure Networking (VNET/Subnets/NIC/NSGs)

  - Azure Migrate & Azure Site Recovery
  - Azure Active Directory & Azure AD Connect
- ✓ 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.
- ✓ The WVD requirements must be satisfied.
- ✓ Knowledge of how UPD (User profile Disks) work with RDS.
- ✓ Knowledge of FSlogix Profile Containers
- ✓ 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.

NOTE:

- Always open PowerShell in administrator mode
- The screenshots in this document are for reference only. There might be instances where the instructions and the details in the screenshot are different so, ***always ensure to clearly read & follow the instructions***

4. Planning & Design

4.1. General Best Practices

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

- Standard naming Conventions
    - Skip this section if you are already following a standard naming convention for resources on-prem and in Azure. If not, please follow the guidance in the link to maintain a consistent naming convention across your resources
- Azure security best practices and patterns
- Azure Active Directory Hybrid Identity best practices
    - Azure identity management and access control security best practices
- Azure Networking & security Best Practices
    - Implementing a secure hybrid network architecture in Azure
- Azure Storage security overview
- Best practices for Azure VM security

4.2. Discovery & Assessment of on-prem RDS infrastructure

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.

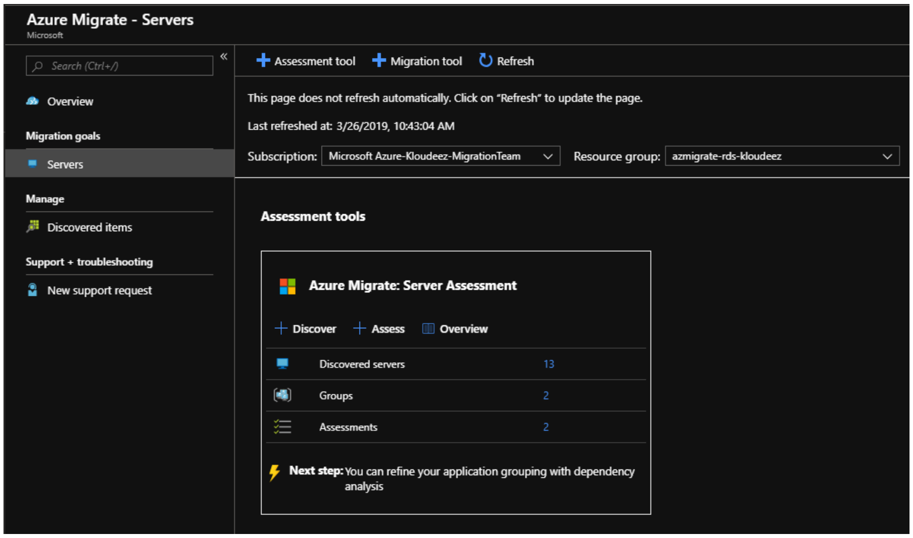
  NOTE: If your end goal is to migrate to WVD, the recommendation is to assess the session hosts and exclude the core services (Connection Broker/Gateway/Web/SQL) which will not be migrated to Azure. Alternatively, if the business driver today is to just migrate everything to Azure (But not migrate to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

4.2.1. Access & Export the 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.



This page does not refresh automatically. Click on "Refresh" to update the page.

Last refreshed at: 3/26/2019, 10:43:04 AM

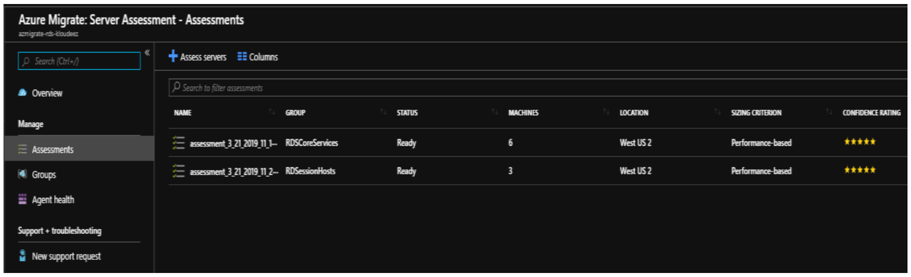
Subscription: Microsoft Azure-Kloudeez-MigrationTeam

Resource group: azmigrate-rds-kloudeez

Discovered servers	13
Groups	2
Assessments	2

Next step: You can refine your application grouping with dependency analysis

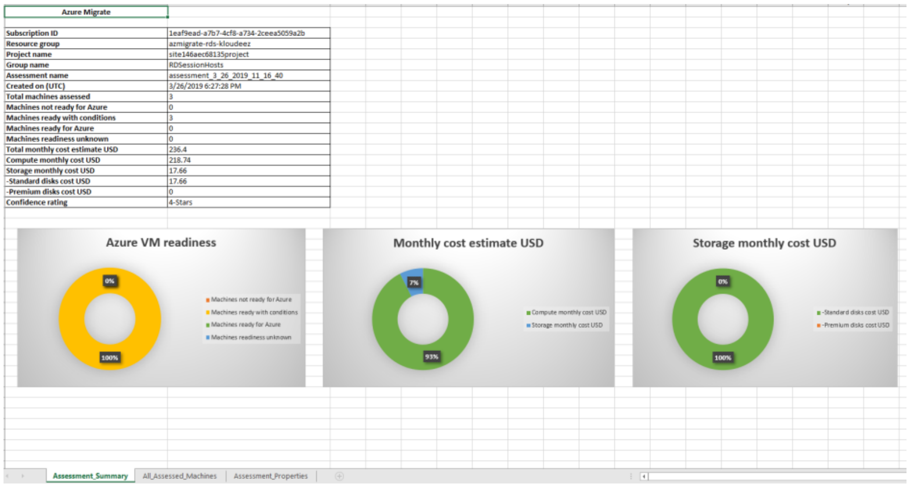
2. Click on the Assessments to open them.



Azure Migrate: Server Assessment - Assessments
azmigrate-rds-kloudeez

NAME	GROUP	STATUS	MACHINES	LOCATION	SIZING CRITERION	CONFIDENCE RATING
assessment_3_21_2019_11_1...	RDSCoreServices	Ready	6	West US 2	Performance-based	★★★★★
assessment_3_21_2019_11_2...	RDSessionHosts	Ready	3	West US 2	Performance-based	★★★★★

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.*



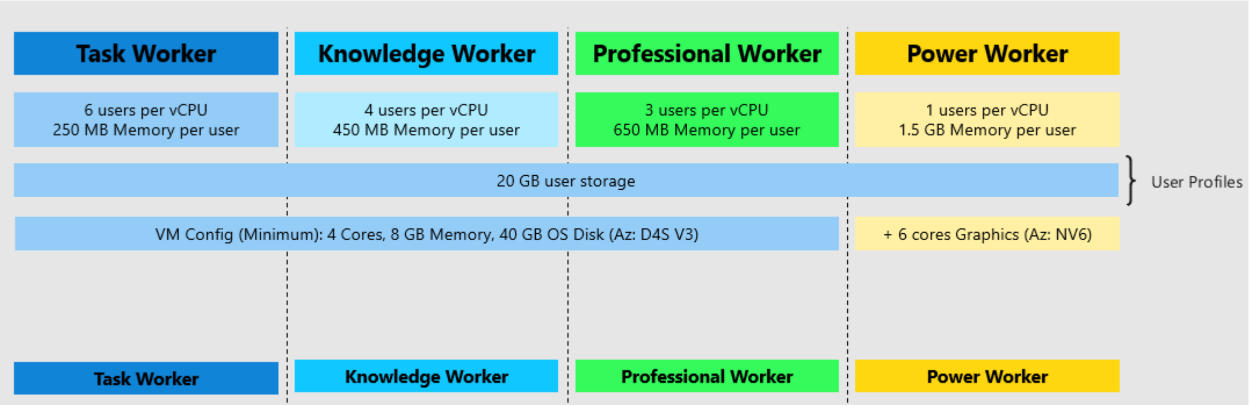
Azure Migrate	
Subscription ID	1eaf9ead-a7b7-4cf8-a734-2ceea5059a2b
Resource group	azmigrate-rds-kloudeez
Project name	site146aec68135project
Group name	RDSessionHosts
Assessment name	assessment_3_26_2019_11_16_40
Created on (UTC)	3/26/2019 6:27:28 PM
Total machines assessed	3
Machines not ready for Azure	0
Machines ready with conditions	3
Machines ready for Azure	0
Machines readiness unknown	0
Total monthly cost estimate USD	236.4
Compute monthly cost USD	218.74
Storage monthly cost USD	17.66
-Standard disks cost USD	17.66
-Premium disks cost USD	0
Confidence rating	4-Stars

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)

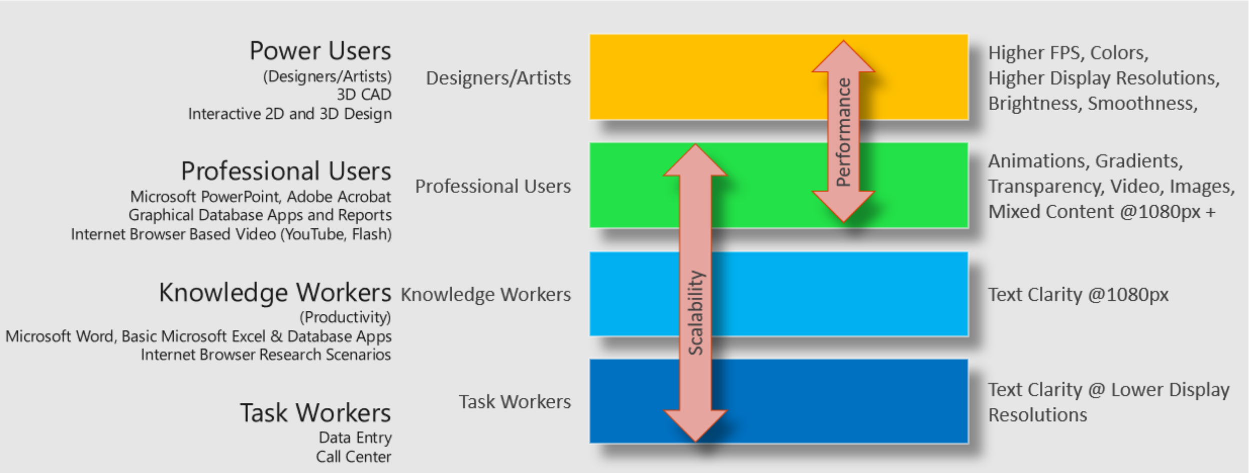
4.2.2. WVD Session Host VM & Storage SKU Guidance

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.



Task Worker	Knowledge Worker	Professional Worker	Power Worker	
6 users per vCPU 250 MB Memory per user	4 users per vCPU 450 MB Memory per user	3 users per vCPU 650 MB Memory per user	1 users per vCPU 1.5 GB Memory per user	User Profiles
20 GB user storage				
VM Config (Minimum): 4 Cores, 8 GB Memory, 40 GB OS Disk (Az: D4S V3)			+ 6 cores Graphics (Az: NV6)	
Task Worker	Knowledge Worker	Professional Worker	Power Worker	



Power Users
(Designers/Artists)
3D CAD
Interactive 2D and 3D Design

Professional Users
Microsoft PowerPoint, Adobe Acrobat
Graphical Database Apps and Reports
Internet Browser Based Video (YouTube, Flash)

Knowledge Workers
(Productivity)
Microsoft Word, Basic Microsoft Excel & Database Apps
Internet Browser Research Scenarios

Task Workers
Data Entry
Call Center

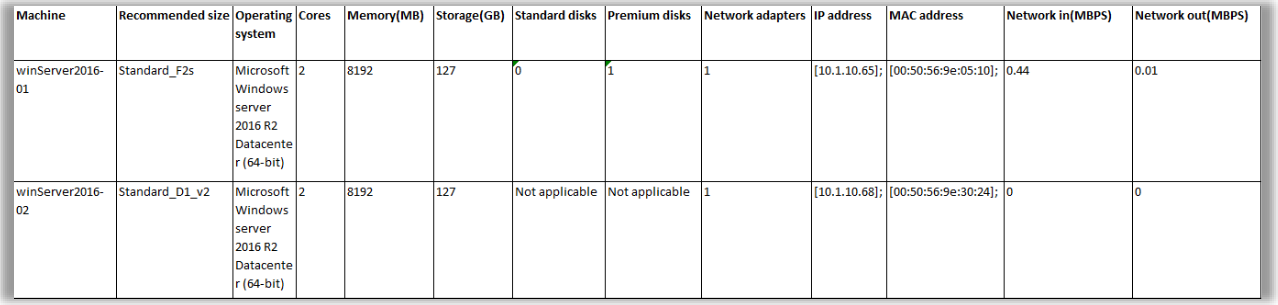
Designers/Artists
Professional Users
Knowledge Workers
Task Workers
Performance
Scalability
Higher FPS, Colors, Higher Display Resolutions, Brightness, Smoothness,
Animations, Gradients, Transparency, Video, Images, Mixed Content @1080px +
Text Clarity @1080px
Text Clarity @ Lower Display Resolutions

- 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.), 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]
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)	
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. Use the VM SKU & storage recommendations by Azure Migrate in the Assessment as seen below.



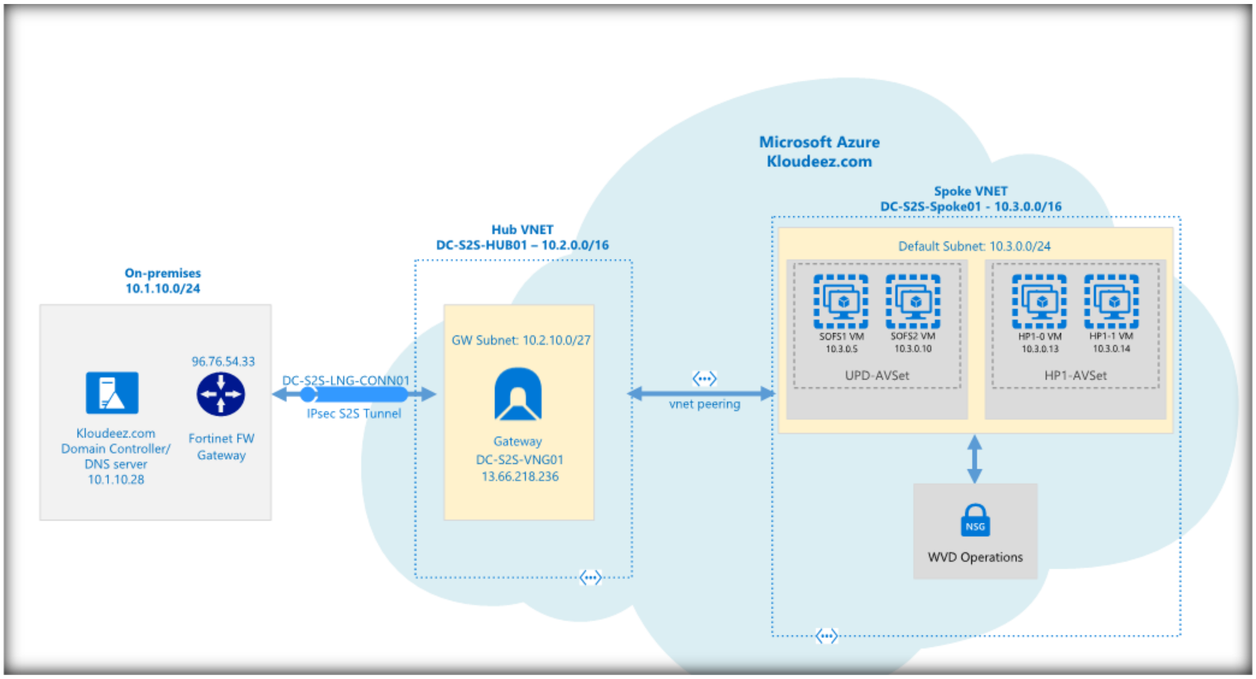
Machine	Recommended size	Operating system	Cores	Memory(MB)	Storage(GB)	Standard disks	Premium disks	Network adapters	IP address	MAC address	Network in(MBPS)	Network out(MBPS)
winServer2016-01	Standard_F2s	Microsoft Windows server 2016 R2 Datacenter (64-bit)	2	8192	127	0	1	1	[10.1.10.65];	[00:50:56:9e:05:10];	0.44	0.01
winServer2016-02	Standard_D1_v2	Microsoft Windows server 2016 R2 Datacenter (64-bit)	2	8192	127	Not applicable	Not applicable	1	[10.1.10.68];	[00:50:56:9e:30:24];	0	0

3. 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.

4.3. 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 Network 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.***

1.1. Azure Virtual Networks (VNET)

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

1.1.1. HUB

- VNET Name: DC-S2S-Hub01
- CIDR: 10.2.0.0/16 *or anything else which does not overlap/conflict with any existing networks*
- Create a subnet called "GatewaySubnet" (this is cannot change and will host the Virtual Network Gateway)
- Based on your requirements, choose an Azure virtual Network Gateway using the specifications from Gateway SKU and deploy it to the "GatewaySubnet"

1.1.2. Spoke

- VNET Name: DC-S2S-Spoke01
- CIDR: 10.3.0.0/16 *or anything else which does not overlap/conflict with any existing networks.*

- Create a subnet called “Default” (or make it specific based on how you want to isolate & manage servers)

1.1.3. VNET Peering

- Configure Peering across the HUB & Spoke VNETs so that resources in networks Hub (10.2.0.0/16) & Spoke (10.3.0.0/16) can communicate with each other.

1.1.4. 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. Please consult your networking team to understand and implement steps in 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
        - *Like shown in the above diagram, an 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 and complete the connectivity to azure.
        - *From the architecture diagram, 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
        - *For both the HUB & SPOKE VNETs the DNS servers has been updated to 10.1.10.28(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.

4.4. Identity & Access Management

Please ensure that the Active Directory Requirements mentioned at **WVD requirements** are completed only after which steps in the below section can be accomplished.

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.

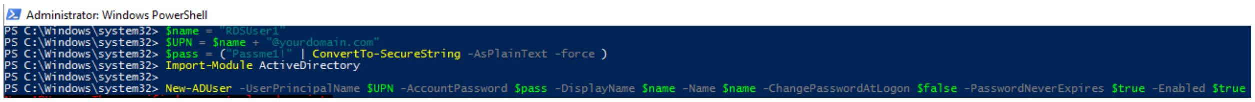
1.1. Create Test Users and AD Security Groups

For the sake of implementing a WVD PoC, we will be creating some test 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
```



Administrator: Windows PowerShell

```
PS C:\Windows\system32> $name = "RDSUser1"
PS C:\Windows\system32> $UPN = $name + "@yourdomain.com"
PS C:\Windows\system32> $pass = ("Passme1!" | ConvertTo-SecureString -AsPlainText -force )
PS C:\Windows\system32> Import-Module ActiveDirectory
PS C:\Windows\system32>
PS C:\Windows\system32> New-ADUser -UserPrincipalName $UPN -AccountPassword $pass -DisplayName $name -Name $name -ChangePasswordAtLogon $false -PasswordNeverExpires $true -Enabled $true
```

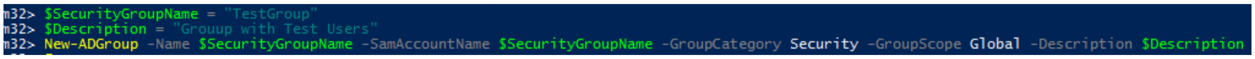
Update the values and Repeat the command for as many users you like to test with.

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
```



```
m32> $SecurityGroupName = "TestGroup"
m32> $Description = "Grouup with Test Users"
m32> 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")
```

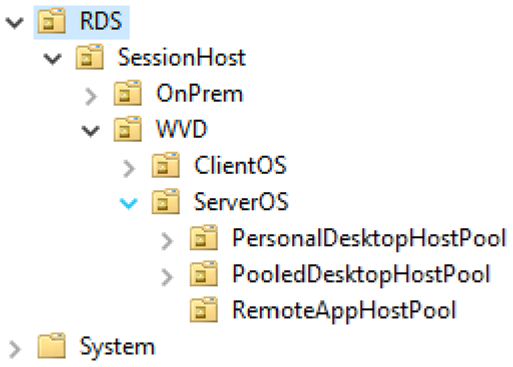
```
#adding users to RemoteDesktop group

$Identity = “RDS-PooledDesktopUsers”

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

1.2. 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 have an already 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.*

4.5. Azure Storage and Disks

Please refer the storage assessment results to finalize the Azure storage / Disk options required for your VM's. As a baseline recommendation, it would be advised to choose the following for production workloads. We are NOT going to deploy anything at this time and will be handled in the subsequent sections.

- **Azure Storage Account**

  Azure Storage account would be primarily be utilized for hosting the diagnostic logging information across ALL your VMs.

  - Choose SKU = Standard for low-Pri (Dev/Test) workloads/servers
  - Choose SKU = Premium for High Pri (Production) workloads/servers

- **Azure Disks**

  For better management and efficiency, the recommended storage solution for all VMs in Azure must be ***Managed Disks*** and it is highly encouraged to avoid using ***un-managed disks (blob VHD on a Storage Account)*** unless there is a very strong business requirement.

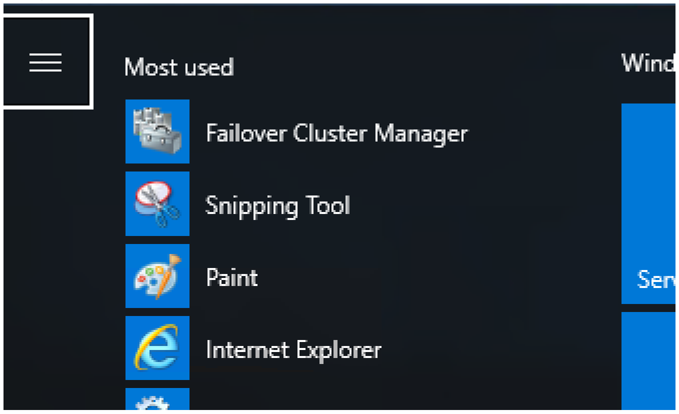
  - Choose SKU = Standard for low-Pri (Dev/Test) workloads/servers
  - Choose SKU = Premium for High Pri (Production) workloads/servers

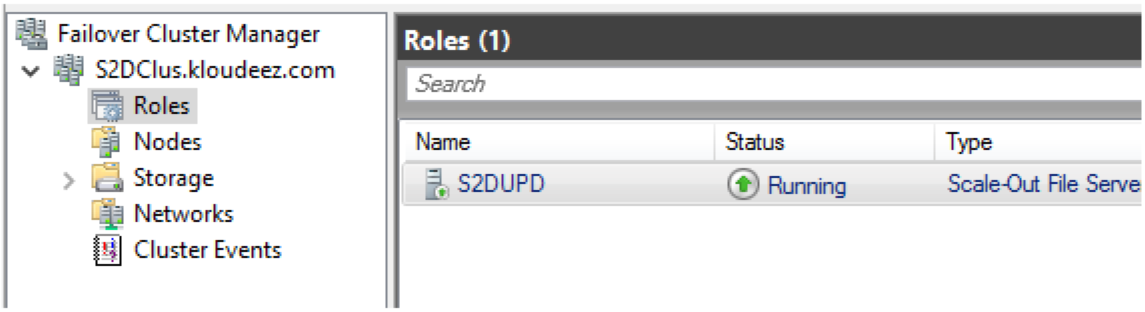
4.6. Scale Out File Server (SOFS) with Storage Spaces Direct (S2D)

If you already have (or planning) to use either roaming profiles or FSlogix solutions for your users` profile data in Azure, then a Scale out File server (SOFS) with Storage Spaces Direct (S2D) is the recommended storage solution in Azure to host those user profiles.

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

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





Failover Cluster Manager
S2DClus.kloudeez.com
Roles
Nodes
Storage
Networks
Cluster Events

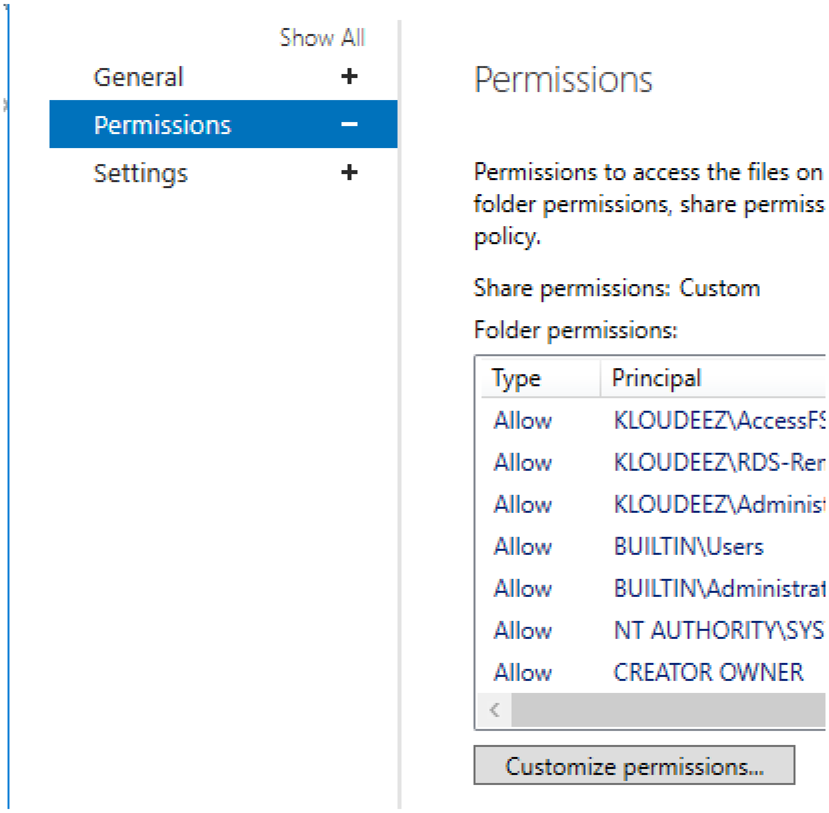
Roles (1)

Search

Name	Status	Type
S2DUPD	Running	Scale-Out File Serve

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

III. In the new window > click permissions > customize permissions



Permissions

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

Share permissions: Custom

Folder permissions:

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

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

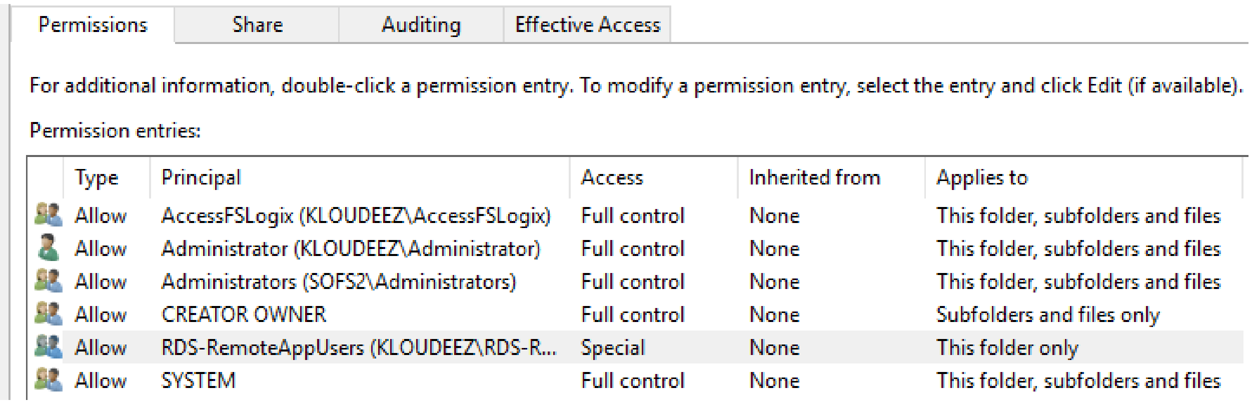
V. Click Select a principal > Select the respective AD object we want to set permissions > click ok > Set Type = Allow > Applies To = value under Folder in the table below > Click Show advanced permissions and select respective values from Permissions column below

User Account	Description	Folder	Permissions

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

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

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



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

Permission entries:

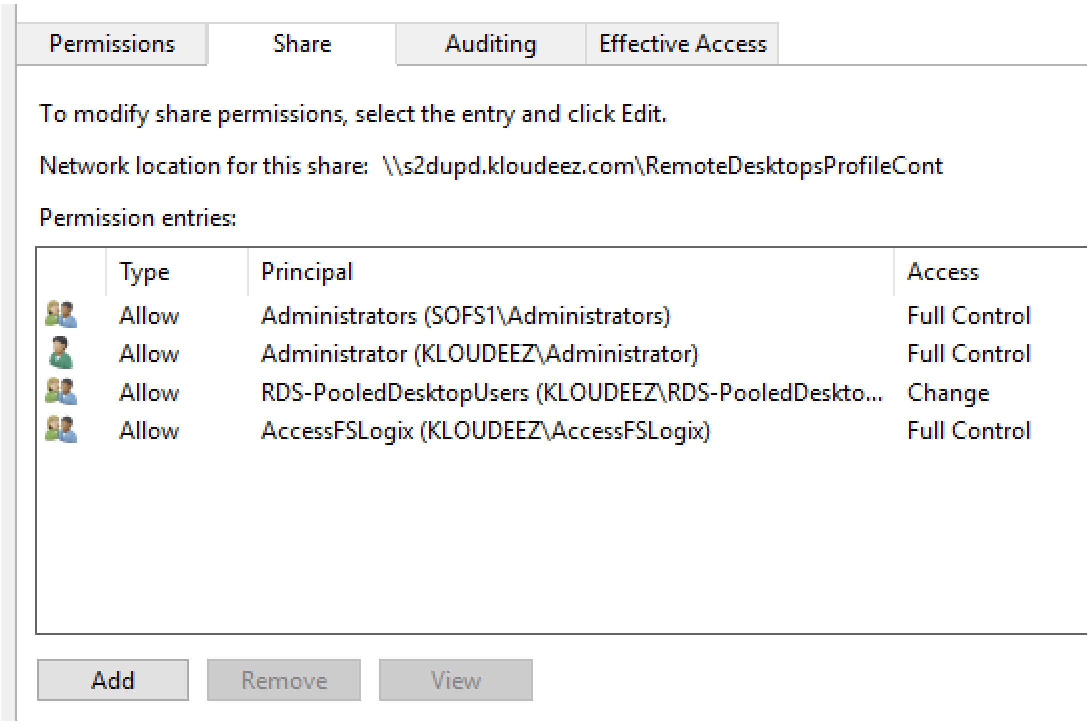
Type	Principal	Access	Inherited from	Applies to
Allow	AccessFSLogix (KLOUDEEZ\AccessFSLogix)	Full control	None	This folder, subfolders and files
Allow	Administrator (KLOUDEEZ\Administrator)	Full control	None	This folder, subfolders and files
Allow	Administrators (SOFS2\Administrators)	Full control	None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

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

IX. 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

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



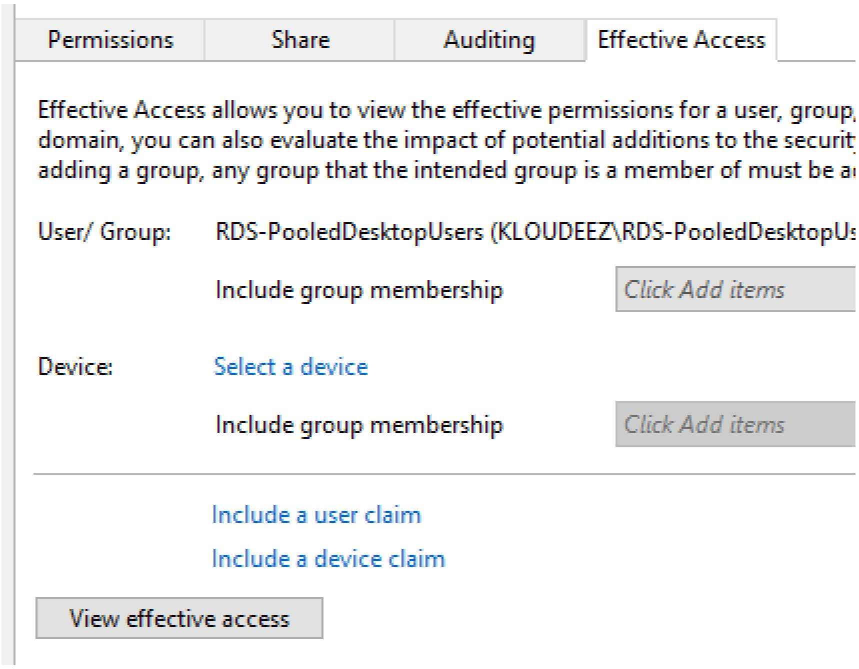
To modify share permissions, select the entry and click Edit.

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

Permission entries:

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

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



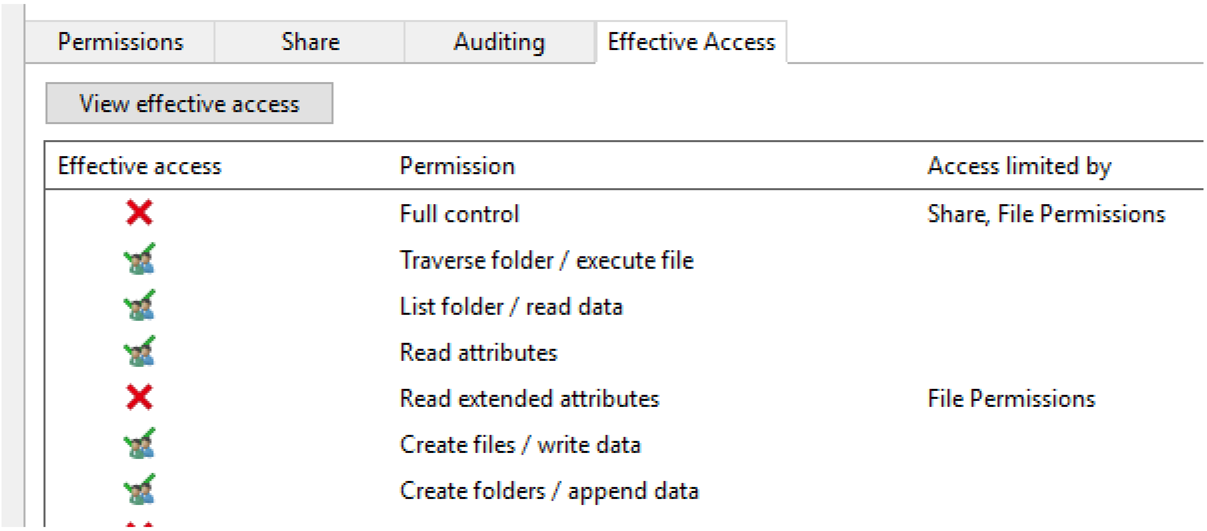
Effective Access allows you to view the effective permissions for a user, group, domain, you can also evaluate the impact of potential additions to the securit adding a group, any group that the intended group is a member of must be a

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

Include group membership: Click Add items

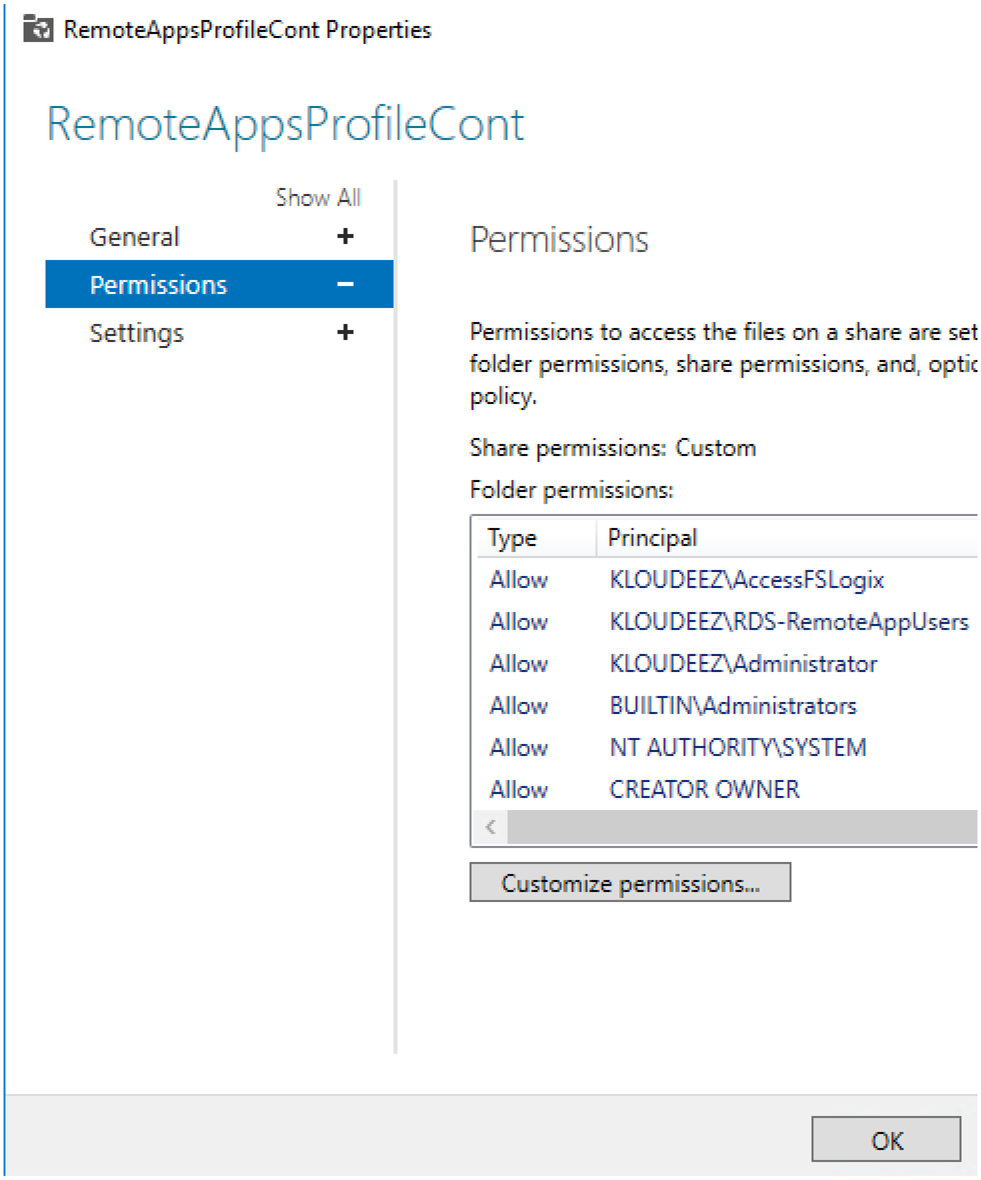
Device: Select a device

Include group membership: Click Add items



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

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



RemoteAppsProfileCont Properties

RemoteAppsProfileCont

Permissions

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

Share permissions: Custom

Folder permissions:

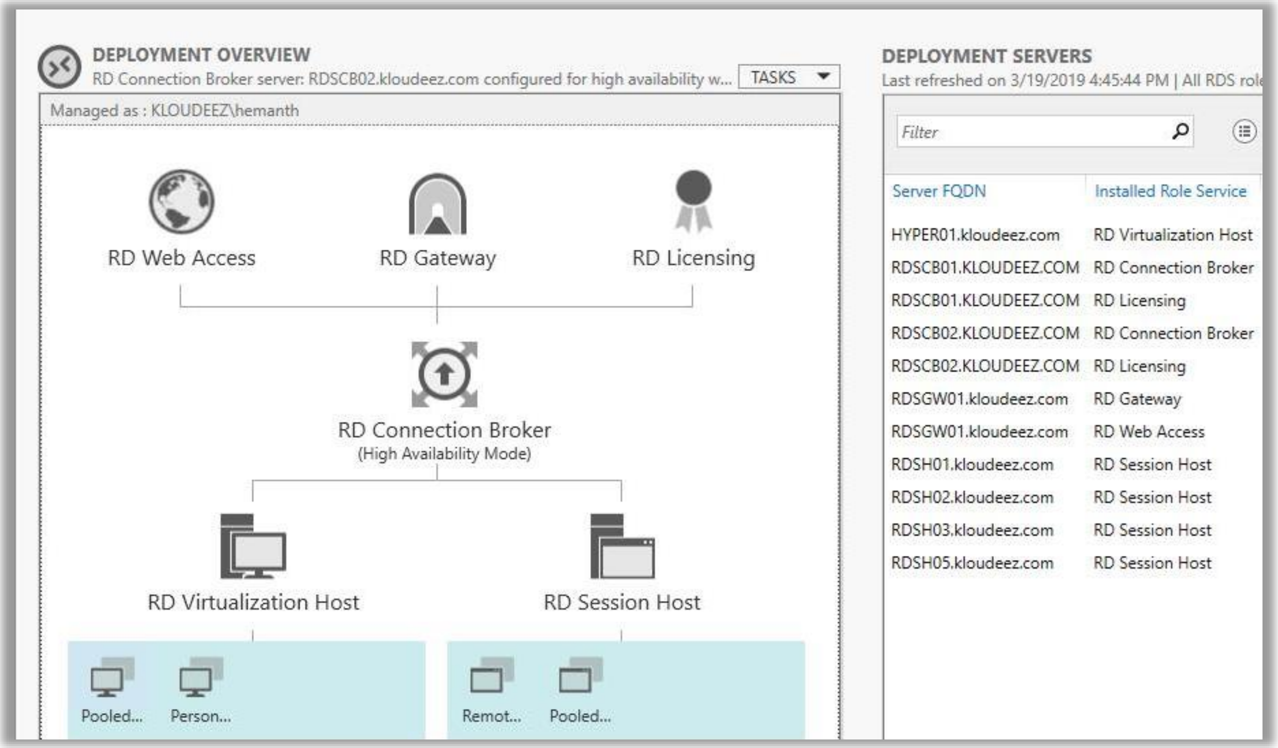
Type	Principal
Allow	KLOUDEEZ\AccessFSLogix
Allow	KLOUDEEZ\RDS-RemoteAppUsers
Allow	KLOUDEEZ\Administrator
Allow	BUILTIN\Administrators
Allow	NT AUTHORITY\SYSTEM
Allow	CREATOR OWNER

XIII. Now, repeat step 3 for all the other shares you wish to use for storing user profile data in Azure.

5. RDS Setup (on-premises)

This section describes a ***typical RDS on-premises configuration*** to simulate an existing enterprise architecture setup that will eventually be migrated to Azure. Please be advised this baseline configuration is to help understand/summarize the standard migration process and your enterprises` implementation may contain additional customizations and/or settings that ***might not*** be covered in this document.

Below is the on-premises RDS deployment overview and the breakdown of the different server roles being used in the environment.


DEPLOYMENT OVERVIEW

RD Connection Broker server: RDSCB02.kloudeez.com configured for high availability w...

Managed as : KLOUDEEZ\hemanth

DEPLOYMENT SERVERS

Last refreshed on 3/19/2019 4:45:44 PM | All RDS rol

Server FQDN	Installed Role Service
HYPER01.kloudeez.com	RD Virtualization Host
RDSCB01.KLOUDEEZ.COM	RD Connection Broker
RDSCB01.KLOUDEEZ.COM	RD Licensing
RDSCB02.KLOUDEEZ.COM	RD Connection Broker
RDSCB02.KLOUDEEZ.COM	RD Licensing
RDSGW01.kloudeez.com	RD Gateway
RDSGW01.kloudeez.com	RD Web Access
RDSH01.kloudeez.com	RD Session Host
RDSH02.kloudeez.com	RD Session Host
RDSH03.kloudeez.com	RD Session Host
RDSH05.kloudeez.com	RD Session Host

On-premises RDS Deployment

- Active Directory
    - All servers listed above are domain joined. For the sake of this document, we are using a fictitious single forest/domain called Kloudeez.com *(like contoso.com OR fabrikam.com references found in any Microsoft public documentation)*
    - There is a single domain controller called ADC01 that also doubles up as the DNS server.
- Connection Broker

    - 2 connection brokers RDSCB01 & RDSCB02 are configured in a highly available (HA) configuration
    - The broker configuration data is stored on a standalone SQL server RDSSQL01 that both brokers can access.
- RD Gateway & Web Access
    - A standalone server RDSGW01 has both the RD-Gateway and Web Access roles installed
- RD-Licensing
    - The RD-licensing role is also installed on RDSCB01 & RDSCB02 (connection broker)
    - The licensing mode configured is per-user
- RD-Session Hosts
    - We have a total of 4 Session hosts servers (RDSH01/02/03/05)
    - These are the servers where session-based RemoteApp & RemoteDesktop(pooled) collections are hosted.
- RD-Virtualization Host
    - A Hyper-V host HYPER01 is being used for VDI collections.
    - This Host will deliver Windows client based Personal Desktops to users (1:1).
- File Server
    - A standalone file server called RDSFS01 is used as an SMB share endpoint to store profile data using UPD (User Profile Disks).

6. Migrate Server based RDS resources to Azure-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.

5.1. Choose the Migration Models

The migration approach and guidance greatly vary based on your end goals with WVD. Hence, the first and important step is to choose a migration model based on your requirements and the LOE (level of effort) it takes to execute the migrations.

5.1.1. Burst to Azure (Deploy parallel infra on Azure)

- **When to choose?**
    - If you like to migrate at a moderate pace to WVD

        - Do not have an imminent business need to refactor to Win 10 MS.
        - Already have generalized golden and/or custom images (with apps pre-installed) that can be readily deployed in Azure.
        - Would/can operate in a hybrid model managing both RDS on-prem & WVD as separate service endpoints.
    - **100 Ft Migration Process overview**
        - Provision Session hosts in Azure registered with WVD using any of the deployment models
            - Deploy using Azure Gallery
            - Deploy using custom Azure Image
            - Deploy using custom VHD from Azure Storage
        - If roaming user profile management is required, implement FSlogix on the session hosts.
        - Replicate/migrate the user profile data from on-premises to Azure.
        - Cutover users from on-prem to WVD endpoint.

5.1.2. 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.
- **100 Ft Migration overview**
    - Plan & Implement ASR infrastructure either on-prem or Azure
    - Replicate session hosts into Azure.
    - Initiate Test Failovers and validate user experience
        - If user profile management is required, implement FSlogix on the session hosts.
        - Integrate Pre-Post Failover tasks to create Availability sets, create & register with WVD HostPool
    - Complete Final Failovers

        - If user profile management is required, implement FSlogix on the session hosts.
        - Integrate Pre-Post Failover tasks to create Availability sets, create & register with WVD HostPool
    - Replicate/migrate the user profile data from on-premises to Azure.
    - Cutover users from on-prem to WVD endpoint.

5.2. Burst to Azure - Detailed Migration Steps

This steps in this section are like the PoC steps for deploying WVD session hosts in Azure. Please follow each step below and get back to this section for guidance.

1. Create a production specific WVD tenant using the steps in the section Create the WVD Tenant.
2. Deploy the HostPool using the ARM template using either of the below deployment models
   2.1. For deploying using the Azure portal (GUI) refer the section Deploy HostPool using Azure Portal (Marketplace)
   2.2. For deploying using the ARM template, refer section Deploy HostPool using ARM template
   2.3. For deploying nonstandard OS like Server 2010R2 and/or Server 2019, refer section Deploy HostPool using modified ARM template
3. Deploy the respective AppGroup (RemoteApps OR RemoteDesktop) and ACL users that need access using instructions from Manage App Groups
4. Complete the FSLogix configuration on the WVD session hosts using instructions from all the below sections
   4.1. Install FSLogix on Session Hosts
   4.2. Configure FSLogix GPO Settings

5. Complete the steps in the section Convert user profiles to FSLogix Containers for a few test users that can be validated during the subsequent Test Failovers – ***Please not this is a stop-gap solution and is not fully supported at this time.***

6. After it has been verified, that on-prem profile data has been replicated/migrated to Azure, you can prepare for cutting over traffic from on-prem to the new WVD endpoint
   6.1. Stop accepting connections on the on-premises session hosts

6.2. Optionally if required, make any DNS updates to redirect old URLs to the new WVD endpoint.

6.3. Please prepare/communicate the users/client by providing the latest WVD endpoint.

7. Since typically each HostPool will likely be dedicated for a specific collection (RemoteApps OR RemoteDesktop). If you have additional collections on-premises that need to be migrated to Azure, repeat steps 2 – 6 for those as well.

5.3. 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 (VMWare Migrations in Preview).

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 Server 2016	AZ Migrate	AZ Migrate	Supported
Hyper-V	Windows Server 2012 R2	AZ Migrate	ASR	Supported
Hyper-V	Windows Server 2016	AZ Migrate	ASR	Supported

For example: Based on the above table, if you have client and/or server VM's operating on VMware, then Azure Migrate would be the correct fit Vs the VM's operating on Hyper-V have to use Azure Site Recovery (ASR). The next sections include guidance to help with the lift-n-shift operations using either scenario.

5.3.1. Hyper-V

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 in ASR.

2. Once the Azure environment is setup as directed above, also prepare the on-premises Hyper-V by following the guidelines here.
    i. An ASR agent needs to be installed on the Hyper-V VM. Ensure you have appropriate permissions to perform the installation.
    ii. Enable RDP on the VM to ensure connectivity after failover.
3. Depending on how you manage your VMs in Hyper-V, follow the guidelines below.
    i. Managed by SCVMM – Follow guidelines here to setup VMs for Replication.
    ii. NOT Managed by SCVMM - Follow guidelines here to setup VMs for Replication.
4. Complete the steps in the section Convert user profiles to FSLogix Containers for a few test users that can be validated during the subsequent Test Failovers – ***Please not this is a stop-gap solution and is not fully supported at this time.***
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.
    i. Ensure you select a VNET, resource group that is separate from your primary/production environment.
    ii. You will also need AD connectivity and will require to failover your on-prem AD server as well.
    iii. 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. After a successful Test Failover, complete the steps in the section Convert user profiles to FSLogix Containers for all your users – ***Please note this is a stop-gap solution and is not fully supported at this time.***

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

5.3.2. VMWare

Azure Migrate now supports lift-and-shift migrations on VMWare environment. At the time of writing this document, the migration support is in preview. So before starting with the instructions in this section, you must first whitelist your subscriptions to use this service, using instructions at the link here.

Users can continue using ASR to perform lift-and-shift migrations from VMWare environments. Please see the guidelines below.

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 in ASR.
2. Once the Azure environment is setup as directed above, also prepare the on-premises VMWare by following the guidelines here.
    i. A VM needs to be imported when setting up replication. Ensure you have appropriate permissions to perform the installation.
3. Setup Replication on your VMs by following the guidelines here.
4. Complete the steps in the section Convert user profiles to FSLogix Containers for a few test users that can be validated during the subsequent Test Failovers – ***Please note this is a stop-gap solution and is not fully supported at this time.***

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.
    i. Ensure you select a VNET, resource group that is separate from your primary/production environment.
    ii. 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.
8. After a successful Test Failover, complete the steps in the section Convert user profiles to FSLogix Containers for all your users – ***Please note this is a stop-gap solution and is not fully supported at this time.***

6. Perform a Final Failover to Azure to successfully cutover the VMWare VM and start using the Azure VM by following the guidelines here.

i. 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.

7. Migrate Client based VDI resources to WVD.

7.1. 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 (VMWare Migrations in Preview).

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 7 Ent	AZ Migrate	AZ Migrate	Not Supported at the moment
VMWare	Windows 10 Ent	AZ Migrate	AZ Migrate	Supported
Hyper-V	Windows 7 Ent	AZ Migrate	ASR	Not Supported at the moment
Hyper-V	Windows 10 Ent	AZ Migrate	ASR	Supported

For example: Based on the above table, if you have client and/or server VM's operating on VMware, then Azure Migrate would be the correct fit Vs the VM's operating on HyperV have to use Azure Site Recovery (ASR). The next sections include guidance to help with the lift-n-shift operations using either scenario.

7.1.1. Hyper-V

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 in ASR.
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. Depending on how you manage your VMs in Hyper-V, follow the guidelines below.

iv. Managed by SCVMM – Follow guidelines here to setup VMs for Replication.

v. NOT Managed by SCVMM - Follow guidelines here to setup VMs for Replication.

4. 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.

vi. Ensure you select a VNET, resource group that is separate from your primary/production environment.

vii. 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. After a successful Test Failover, perform a Final Failover to Azure to successfully cutover the Hyper-V VM and start using the Azure VM by following the guidelines here.

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

7.1.2. VMWare

Azure Migrate now support lift-and-shift migrations on VMWare environment. At the time of writing this document, the migration support is in **preview**. So before starting with the instructions in this section, you must first whitelist your subscriptions to use this service, using instructions at the link here.

Users can continue using ASR to perform lift-and-shift migrations from VMWare environments. Please see the guidelines below.

7. 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 in ASR.

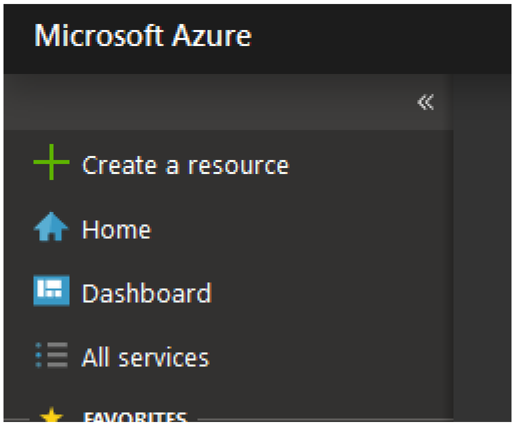
8. Once the Azure environment is setup as directed above, also prepare the on-premises VMWare by following the guidelines here.
    i. A VM needs to be imported when setting up replication. Ensure you have appropriate permissions to perform this step.
9. Setup Replication on your VMs by following the guidelines here.
10. 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.
    i. Ensure you select a VNET, resource group that is separate from your primary/production environment.
    ii. 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.
11. After a successful Test Failover, perform a Final Failover to Azure to successfully cutover the VMWare VM and start using the Azure VM by following the guidelines here.
    i. 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.

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.

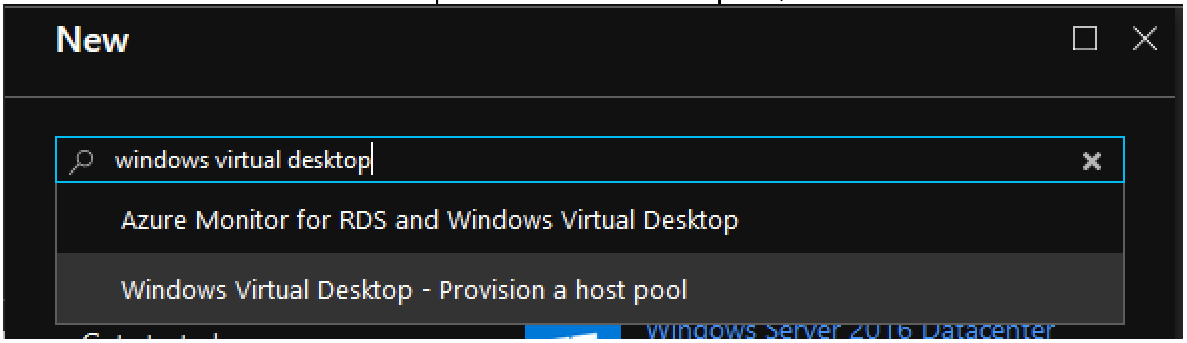
8. Appendix

8.1. Deploy HostPool using Azure Portal (Marketplace)

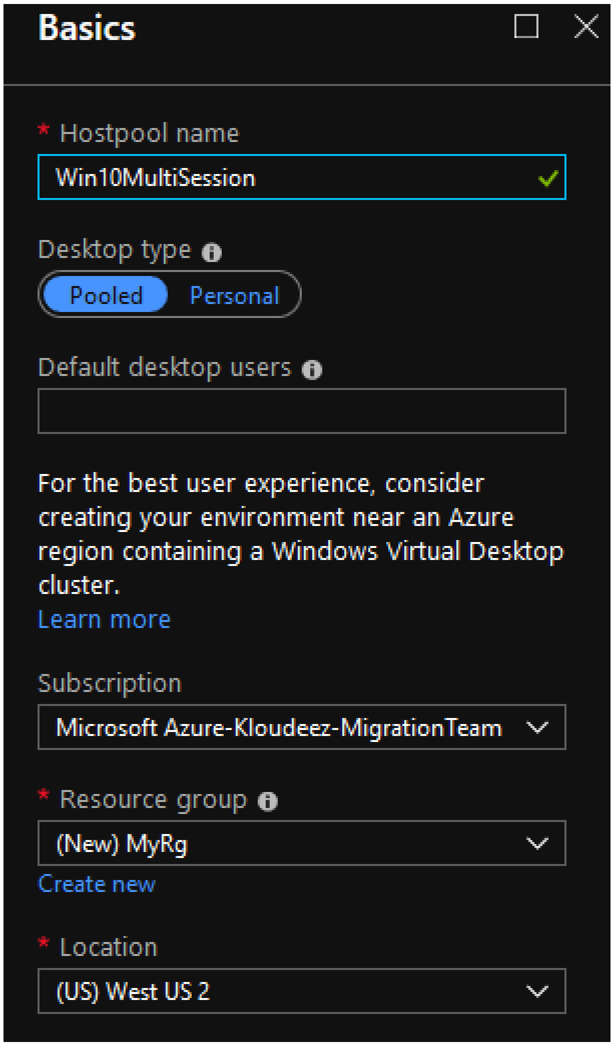
1. Login into the Azure portal
2. Select + or + Create a resource.



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


New
windows virtual desktop
Azure Monitor for RDS and Windows Virtual Desktop
Windows Virtual Desktop - Provision a host pool
Windows Server 2016 Datacenter

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.



Basics

* Hostpool name

Win10MultiSession

Desktop type

Default desktop users

For the best user experience, consider creating your environment near an Azure region containing a Windows Virtual Desktop cluster.

Subscription

Microsoft Azure-Kloudeez-MigrationTeam

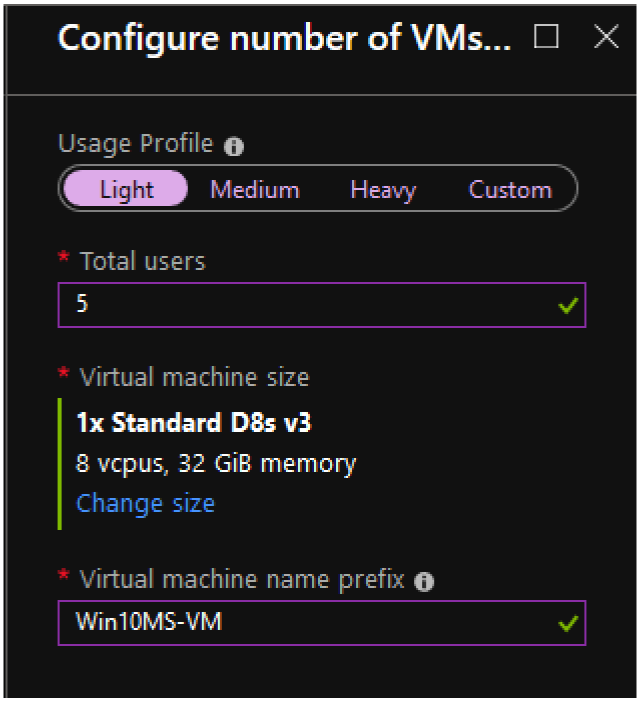
* Resource group

(New) MyRg

* Location

(US) West US 2

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



Configure number of VMs...

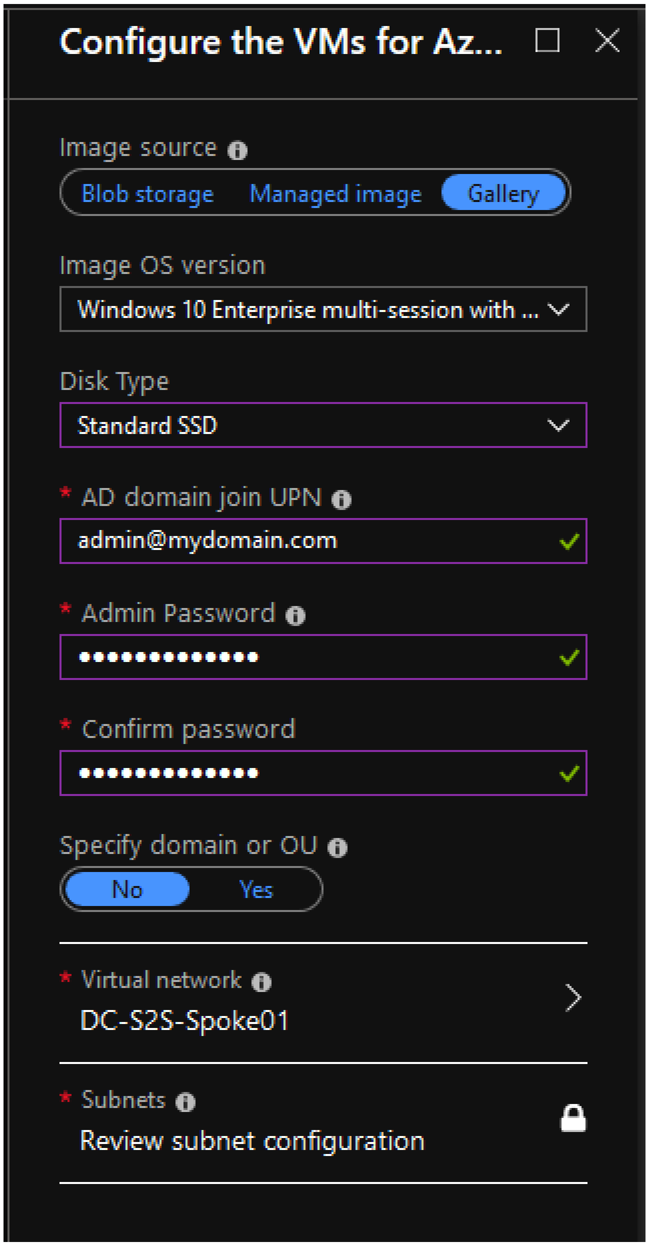
Usage Profile
Light | Medium | Heavy | Custom

* Total users
5 ✓

* Virtual machine size
1x Standard D8s v3
8 vcpus, 32 GiB memory
Change size

* Virtual machine name prefix
Win10MS-VM ✓

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.



Configure the VMs for Az...

Image source

Image source: Gallery

Image OS version: Windows 10 Enterprise multi-session with ...

Disk Type: Standard SSD

* AD domain join UPN: admin@mydomain.com

* Admin Password: ••••••••••••••

* Confirm password: ••••••••••••••

Specify domain or OU: No

* Virtual network: DC-S2S-Spoke01

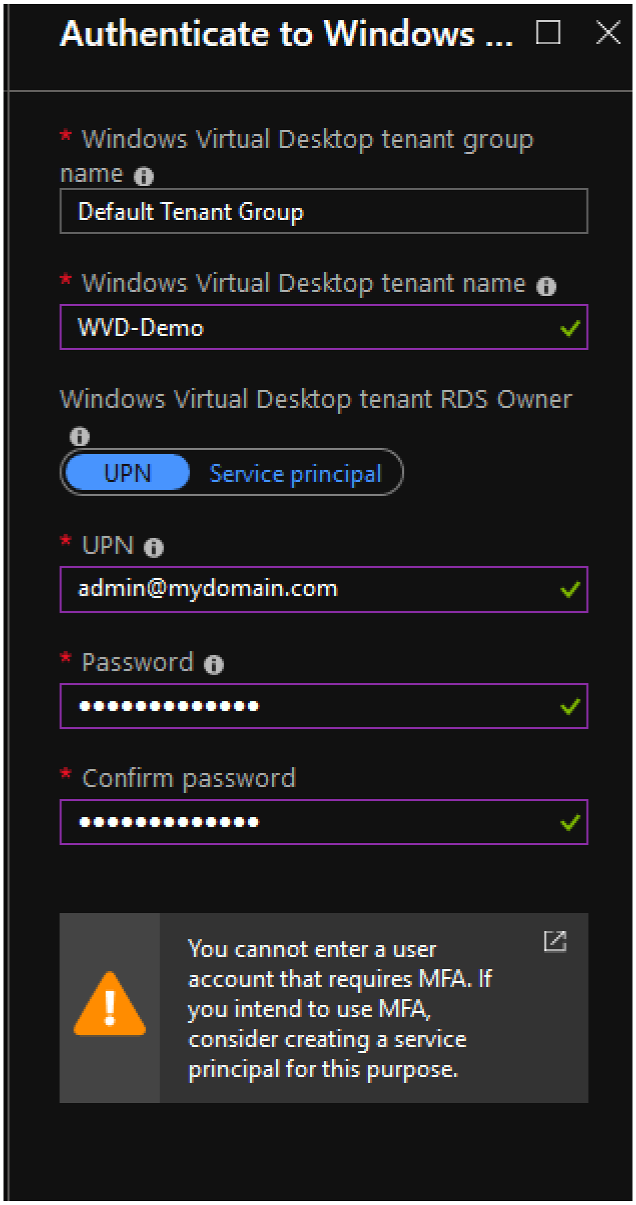
* Subnets: Review subnet configuration

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.



Authenticate to Windows ...

* Windows Virtual Desktop tenant group name: Default Tenant Group

* Windows Virtual Desktop tenant name: WVD-Demo ✓

Windows Virtual Desktop tenant RDS Owner: UPN | Service principal

* UPN: admin@mydomain.com ✓

* Password: ••••••••••••• ✓

* Confirm password: ••••••••••••• ✓

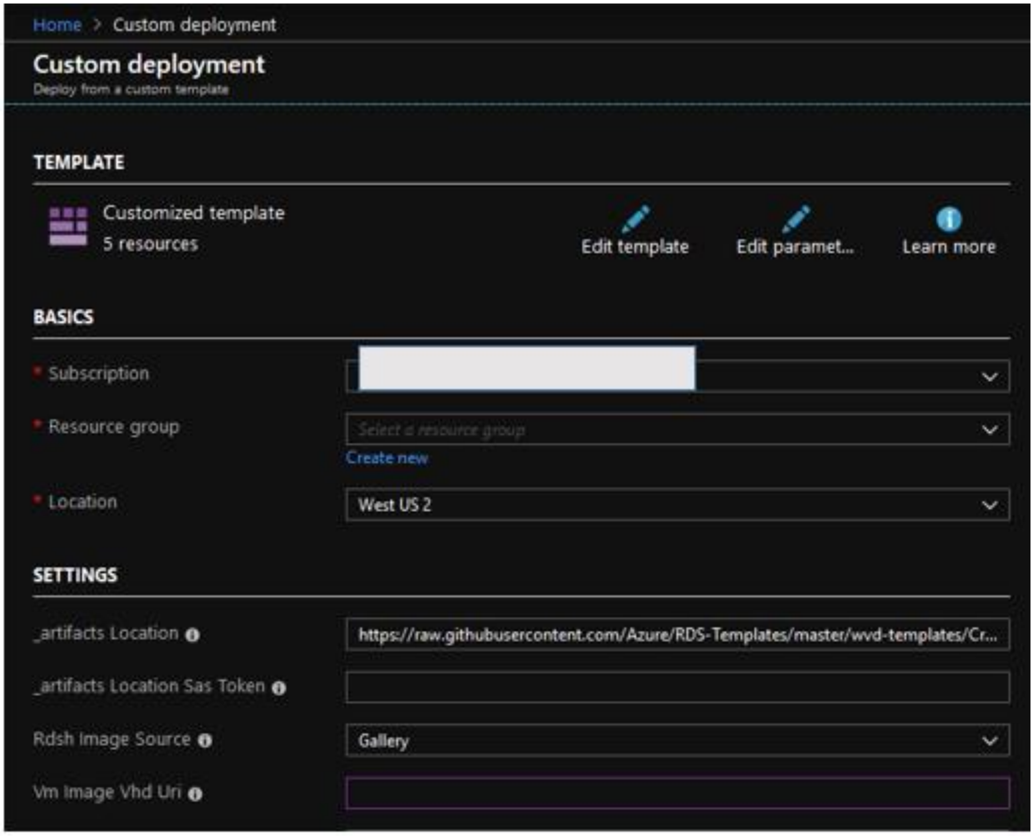
You cannot enter a user account that requires MFA. If you intend to use MFA, consider creating a service principal for this purpose.

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

8.2. 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



Custom deployment

Deploy from a custom template

TEMPLATE

Customized template
5 resources

BASICS

* Subscription	[redacted]
* Resource group	Select a resource group
* Location	West US 2

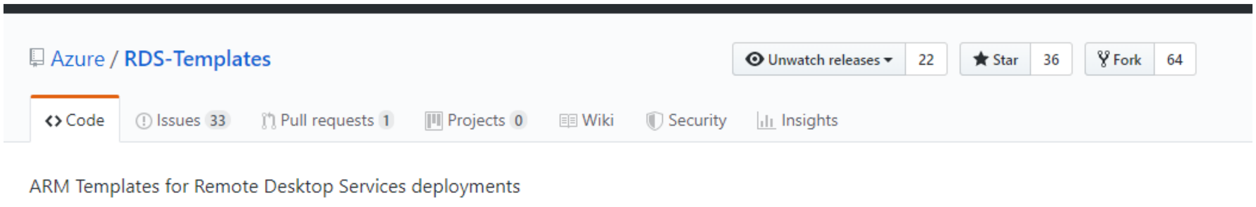
SETTINGS

_artifacts Location	https://raw.githubusercontent.com/Azure/RDS-Templates/master/wvd-templates/Cr...
_artifacts Location Sas Token	
Rdsh Image Source	Gallery
Vm Image Vhd Uri	

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**

8.3. Deploy HostPool using modified ARM template

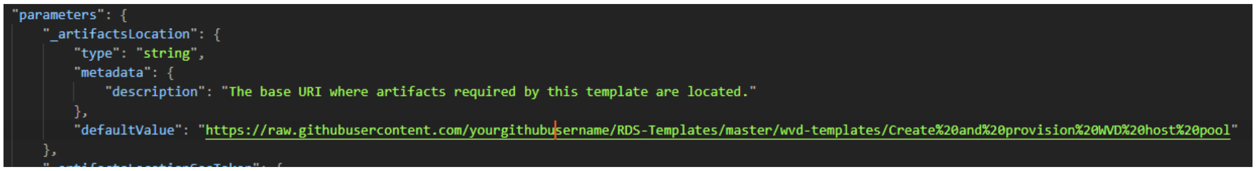
1. Firstly, you will need a GitHub account for this.
2. Goto here > click on Fork > to obtain the repo in your GitHub account



Azure / RDS-Templates

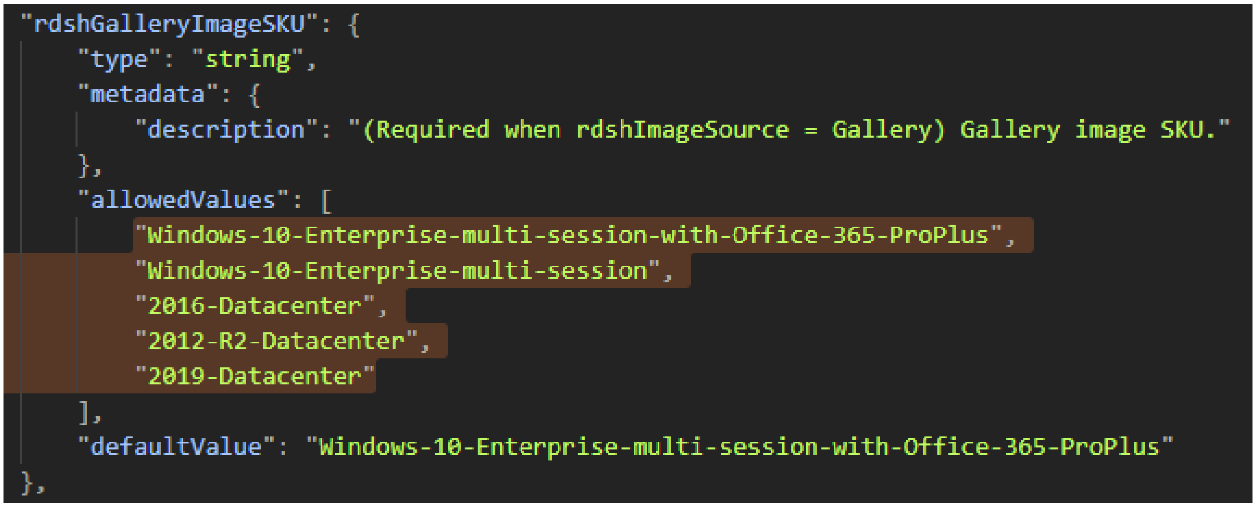
ARM Templates for Remote Desktop Services deployments

3. Once forking is complete, 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)



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

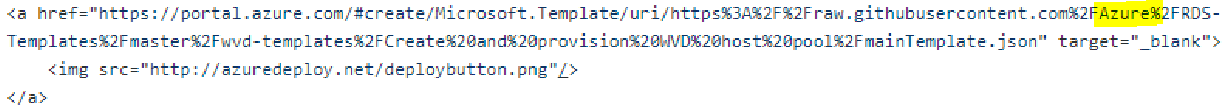
4. Update the rdshGalleryImageSKU parameter as per the below image in the files below:
    - ***Create and provision WVD host pool\mainTemplate.json***
    - ***Create and provision WVD host pool\nestedtemplates\managedDisks-galleryvm.json***
    - ***Create and provision WVD host pool\nestedtemplates\unmanagedDisks-galleryvm.json***



```
"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"
},
```

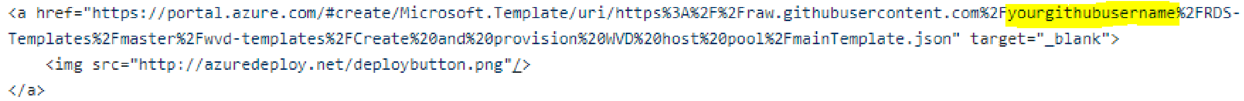
5. Now goto ***RDS-Templates/wvd-templates/Create and provision WVD host pool/*** and edit the readme.MD file to update your github username

   From:



```
<a href="https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2FAzure%2FRDS-
Templates%2Fmaster%2Fwvd-templates%2FCreate%20and%20provision%20WVD%20host%20pool%2FmainTemplate.json" target="_blank">
    <img src="http://azuredeploy.net/deploybutton.png"/>
</a>
```

   To:



```
<a href="https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2Fyourgithubusername%2FRDS-
Templates%2Fmaster%2Fwvd-templates%2FCreate%20and%20provision%20WVD%20host%20pool%2FmainTemplate.json" target="_blank">
    <img src="http://azuredeploy.net/deploybutton.png"/>
</a>
```

6. Once all your changes are committed, goto ***RDS-Templates/wvd-templates/Create and provision WVD host pool/*** scroll to the bottom of the page and click on "Deploy to Azure"

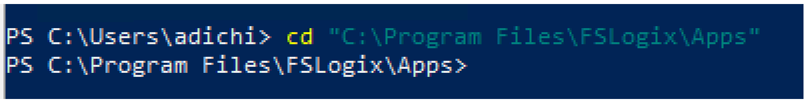
7. Now you can follow the same instructions like Deploy HostPool using ARM template

8.4. Convert user profiles to FSLogix Containers

Since FSLogix is the recommended solution for WVD, if you are currently using windows roaming profiles and/or UPD (User profile Disks), they need to be converted to ProfileContainers before cutting over users. The below steps provide that guidance to complete the same.

Please note this is a stop-gap solution and is not fully supported at this time.

1. Log onto any one of WVD session hosts (or any domain joined machine on the same network) where FSLogix is installed
2. Open PowerShell as an administrator and CD to the FSLogix installation path



```
PS C:\Users\adichi> cd "C:\Program Files\FSLogix\Apps"
PS C:\Program Files\FSLogix\Apps>
```

3. Based on the profile type being used on-prem follow instructions from the respective section

- **RoamingProfiles**

    1. In PS complete the below steps

    ```
    #set the variables first (update these values accordingly)

    $username = “RDSUser1”

    $userSID = “S-1-5-21-3286950516-3440391731-2706545478-1198”
    #this is the user objectSID of the user that can be obtained
    from AD. Follow the steps in the section Get the Object SID
    and continue

    $S2DShare = “\\server\share\RemoteAppProfileContainers”
    #this is the share path for the cluster in azure.

    $sourceProfile = “\\server\share\UserFolder” #the on-prem
    share path to the user profile folder


    #do not update these

    $userFolder = $userSID + “_” + $username

    $vhdName = “Profile”+”_”+ $username +”.vhd”

    $filename =  $S2DShare + “\” + $userfolder + “\” + $vhdName


    #convert the local profile to FSLogix Profile container and
    save it to Azure S2D cluster using the below command

    .\frx.exe copy-profile -filename $filename -username
    $username -profile-path $sourceProfile
    ```

    2. Now goto the path mentioned using $filename and you see the VHD created on the Azure S2D cluster.

    3. Repeat above steps to complete the same for other users.

- **UPD (User profile Disks)**

1. On the session host that you are logged on, Mount the user VHD from the on-prem SMB share so that the file system can be accessed locally.

2. Open PowerShell and complete the below steps

```
#set the variables first (update these values accordingly)

$username = “RDSUser1”

$userSID = “S-1-5-21-3286950516-3440391731-2706545478-1198” #this is the user objectSID of the user that can be obtained from AD. Follow the section Get the Object SID to get the SID details

$S2DShare = “\\server\share\RemoteAppProfileContainers” #this is the share path for the cluster in azure.

$sourceProfile = “X:\UserFolder” #the path where the user VHD was locally mounted


#do not update these

$userFolder = $userSID + “_” + $username

$vhdName = “Profile”+”_”+ $username +”.vhd”

$filename =  $S2DShare + “\” + $userfolder + “\” + $vhdName


#convert the user profile to FSLogix Profile container and save it to Azure S2D cluster using the below command

.\frx.exe copy-profile -filename $filename -username $username -profile-path $sourceProfile
```

4. Now goto the path mentioned using $filename and you see the VHD created on the Azure S2D cluster.

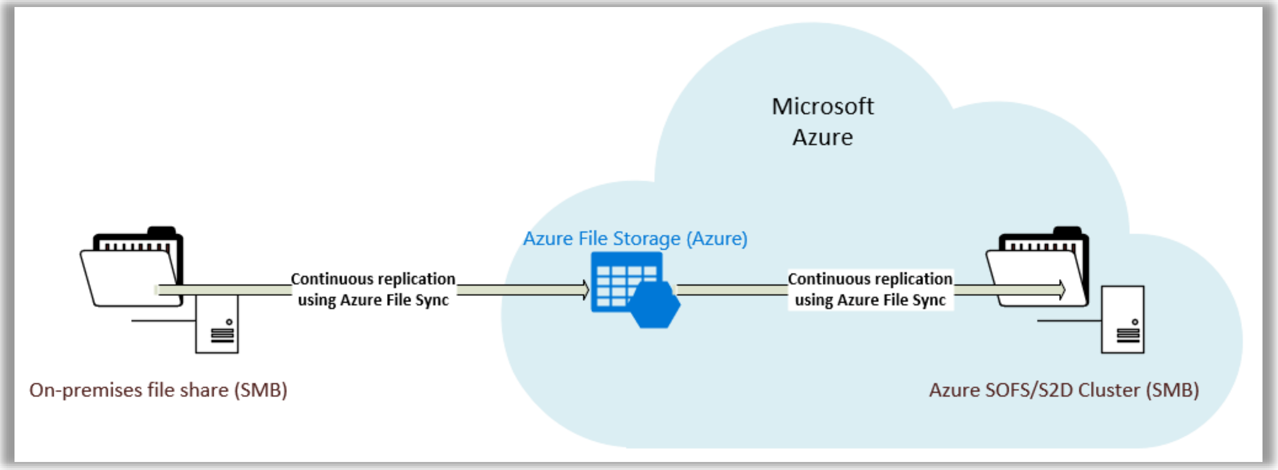
5. Repeat above steps to complete the same for other users.

8.5. Deploy Azure File Sync for Profile data replication

Using Azure File Sync, we will seamlessly synchronize the on-premises user profile data to the SOFS/S2D cluster that we plan to use to store FSlogix Profiles.

Essentially – the goal of this section is to show how to configure Azure File Sync to replicate files between “on-prem SMB share” and “Azure SOFS/S2D cluster” using

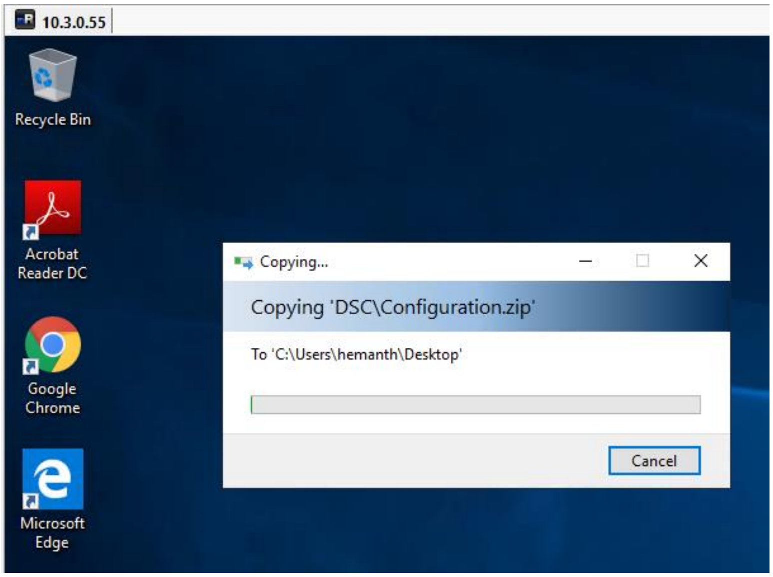
Azure Storage as the intermediary. The below architecture summarizes the 2-hop approach where data will first be replicated between the on-prem SMB share and Azure File share after which the SOFS/S2D cluster will be added as an additional endpoint to the existing sync group without impacting daily user operations.


Microsoft Azure
Azure File Storage (Azure)
Continuous replication using Azure File Sync
Continuous replication using Azure File Sync
On-premises file share (SMB)
Azure SOFS/S2D Cluster (SMB)

1. Follow steps in this Guide to complete replicating data from on-prem to Azure S2D cluster

8.6. Install WVD Agents manually

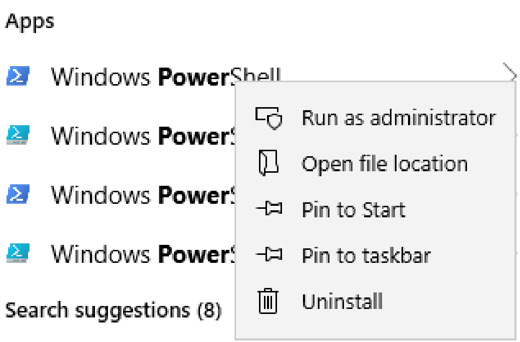
1. Download the template and DSC bits from here onto the VM in Azure. Extract the zip file.



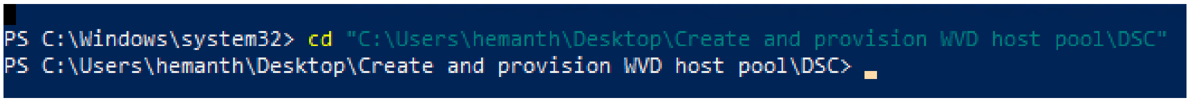
Copying 'DSC\Configuration.zip'

To 'C:\Users\hemanth\Desktop'

2. Run PowerShell as an Administrator.

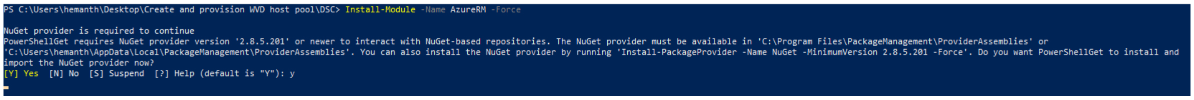


3. CD into the DSC Folder you copied in the first step.



```
PS C:\Windows\system32> cd "C:\Users\hemanth\Desktop\Create and provision WVD host pool\DSC"
PS C:\Users\hemanth\Desktop\Create and provision WVD host pool\DSC>
```

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



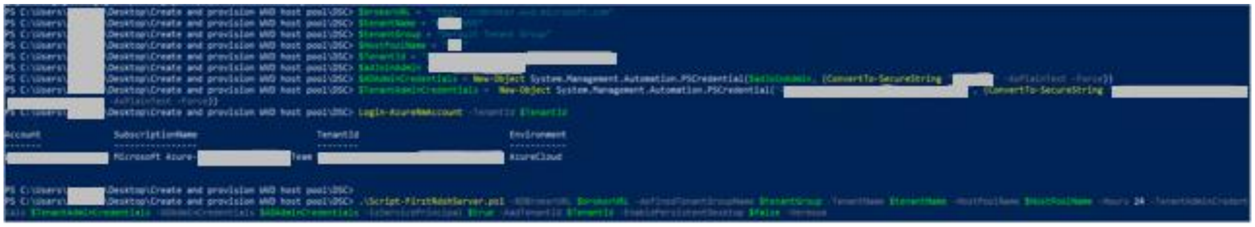
```
PS C:\Users\hemanth\Desktop\Create and provision WVD host pool\DSC> Install-Module -Name AzureRM -Force

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\hemanth\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and
import the NuGet provider now?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
```

    - 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
```

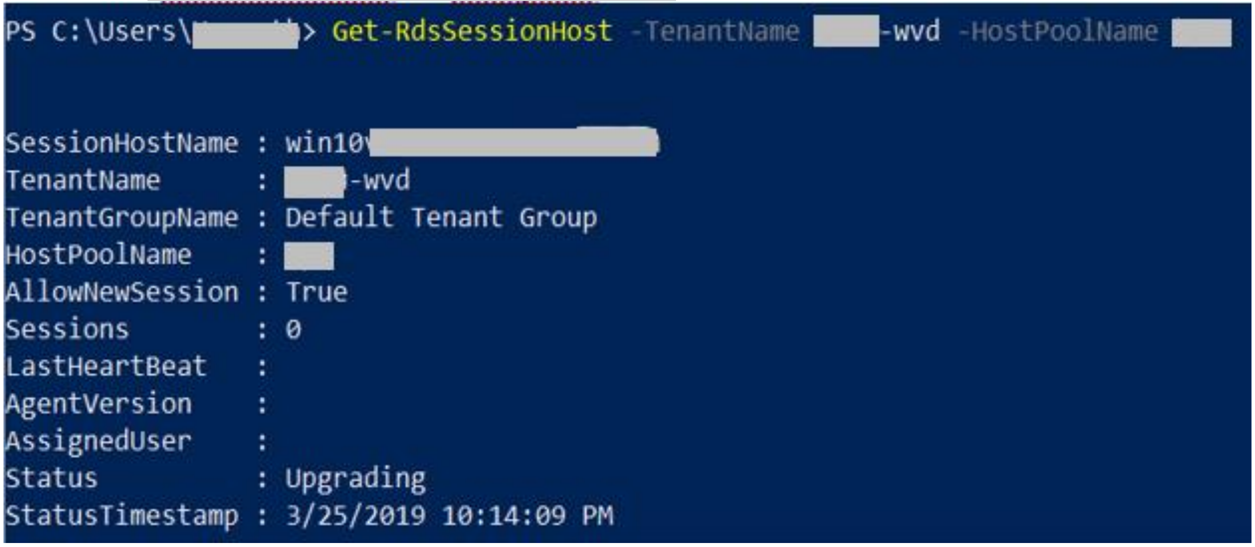
```
.\Script-FirstRdshServer.ps1 -RDBrokerURL $brokerURL -
definedTenantGroupName $tenantGroup -TenantName
$tenantName -HostPoolName $HostPoolName -Hours 24 -
TenantAdminCredentials $TenantAdminCredentials -
ADAdminCredentials $ADAdminCredentials -
isServicePrincipal $true -AadTenantId $TenantId -
EnablePersistentDesktop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



```
PS C:\Users\[redacted]\Desktop\Create and provision WVD host pool\DSC> $brokerURL = "https://rdbroker.wvd.microsoft.com"
PS C:\Users\[redacted]\Desktop\Create and provision WVD host pool\DSC> $tenantName = "[redacted]-wvd"
PS C:\Users\[redacted]\Desktop\Create and provision WVD host pool\DSC> $tenantGroup = "Default Tenant Group"
PS C:\Users\[redacted]\Desktop\Create and provision WVD host pool\DSC> $HostPoolName = "[redacted]"
PS C:\Users\[redacted]\Desktop\Create and provision WVD host pool\DSC> $TenantId = [redacted]
PS C:\Users\[redacted]\Desktop\Create and provision WVD host pool\DSC> $adJoinAdmin= [redacted]
PS C:\Users\[redacted]\Desktop\Create and provision WVD host pool\DSC> $ADAdminCredentials = New-Object System.Management.Automation.PSCredential($adJoinAdmin, (ConvertTo-SecureString [redacted] -AsPlainText -Force))
PS C:\Users\[redacted]\Desktop\Create and provision WVD host pool\DSC> $TenantAdminCredentials = New-Object System.Management.Automation.PSCredential([redacted], (ConvertTo-SecureString [redacted]
[redacted] -AsPlainText -Force))
PS C:\Users\[redacted]\Desktop\Create and provision WVD host pool\DSC> Login-AzureRmAccount -TenantId $TenantId

Account        SubscriptionName                TenantId                         Environment
-------        ----------------                --------                         -----------
[redacted]     Microsoft Azure-[redacted]Team  [redacted]                       AzureCloud

PS C:\Users\[redacted]\Desktop\Create and provision WVD host pool\DSC>
PS C:\Users\[redacted]\Desktop\Create and provision WVD host pool\DSC> .\Script-FirstRdshServer.ps1 -RDBrokerURL $brokerURL -definedTenantGroupName $tenantGroup -TenantName $tenantName -HostPoolName $HostPoolName -Hours 24 -TenantAdminCredent
ials $TenantAdminCredentials -ADAdminCredentials $ADAdminCredentials -isServicePrincipal $true -AadTenantId $TenantId -EnablePersistentDesktop $false -Verbose
```

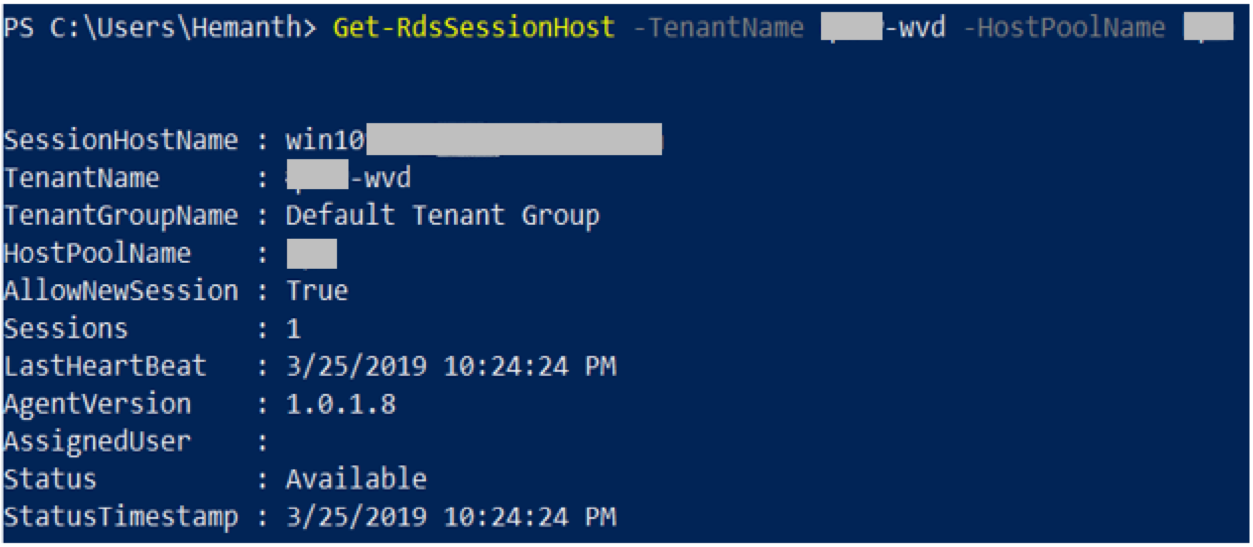
6. This will install all the required modules in the VM and if the Hostpool name specified in the parameters is new, a new HostPool will be created and the VM will be registered with it.
7. Check the status from Powershell by running the following command against WVD. The status should say available.

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



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


SessionHostName : win10[redacted]
TenantName      : [redacted]-wvd
TenantGroupName : Default Tenant Group
HostPoolName    : [redacted]
AllowNewSession : True
Sessions        : 0
LastHeartBeat   :
AgentVersion    :
AssignedUser    :
Status          : Upgrading
StatusTimestamp : 3/25/2019 10:14:09 PM
```

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



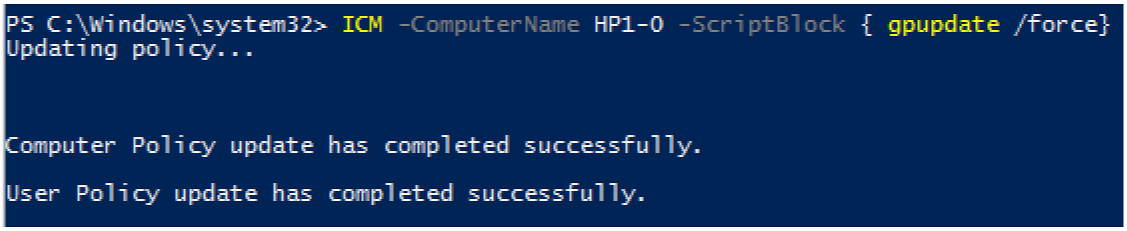
```
PS C:\Users\Hemanth> Get-RdsSessionHost -TenantName [redacted]-wvd -HostPoolName [redacted]


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.

8.7. Check Group Policy updates remotely

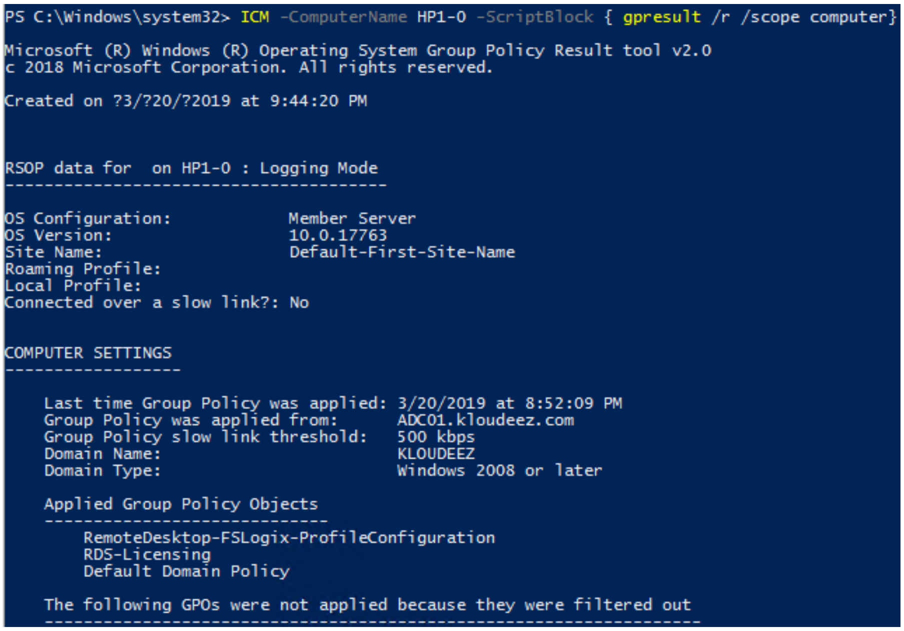
ONLY if you have PowerShell remoting enabled on your session hosts, with PowerShell using the below commands you can remotely update the servers to get the latest group policy and check the latest ones were applied

```
#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}
```

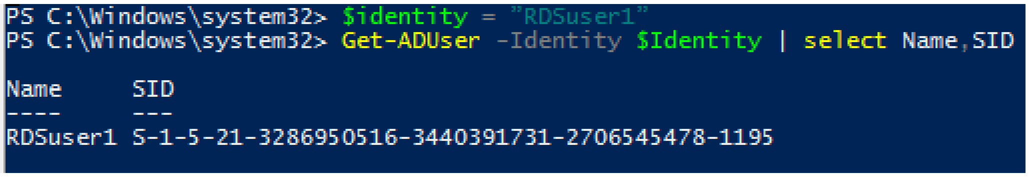


```
PS C:\Windows\system32> ICM -ComputerName HP1-0 -ScriptBlock { gpresult /r /scope computer}

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
    -------------------------------------------------------------------
```

8.8. 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
```

8.9. 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
    c. Share that information with an engineer that will help you.