Windows Virtual Desktop (WVD)

- SoW Checklist Document



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

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation. Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. The descriptions of other companies’ products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers. © 2019 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

[1. Introductions 4](#_Toc19024522)

[2. What this document is not 4](#_Toc19024523)

[3. Target Audience 4](#_Toc19024524)

[4. Pre-requisites/Requirements 4](#_Toc19024525)

[5. WVD Deployments 4](#_Toc19024526)

[5.1. Greenfield (new) Deployments 4](#_Toc19024527)

[5.2. Migrate to WVD 6](#_Toc19024528)

[6. WVD Implementation Steps 7](#_Toc19024529)

[6.1. Azure Environment Assessment 7](#_Toc19024530)

[6.2. Application Assessment 8](#_Toc19024531)

[6.3. Networking 8](#_Toc19024532)

[6.4. Identity and Access Management 9](#_Toc19024533)

[6.5. Security and Compliance 9](#_Toc19024534)

[6.6. Licensing and Entitlements 10](#_Toc19024535)

[6.7. Image Management 10](#_Toc19024536)

[6.8. Deploy and Configure Storage for User Profile(s) 11](#_Toc19024537)

[6.9. Windows Virtual Desktop Environment 11](#_Toc19024538)

[6.10. Windows Virtual Desktop Deployment 12](#_Toc19024539)

[6.11. Migrate Existing RDS/VDI Infrastructure 12](#_Toc19024540)

[6.12. Convert and Migrate User Profiles 13](#_Toc19024541)

[6.13. FSLogix Setup and Configuration for WVD User Profiles 13](#_Toc19024542)

[6.14. Application and Desktop Management 13](#_Toc19024543)

[6.15. WVD Management and Monitoring 14](#_Toc19024544)

[6.16. Patch Management 14](#_Toc19024545)

[6.17. Business Continuity and Disaster Recovery 14](#_Toc19024546)

# Introductions

Welcome to the Windows Virtual Desktop Lighthouse Program. The primary goal of this document is to provide partners (and customers) a helper document they can leverage to build their Statement of Work (SoW) for each Lighthouse program engagement. The singed SoW is required to participate in the program and this SoW must describe the key steps partners (and customers) will follow to successfully implement & manage a Windows Virtual Desktop deployment in Azure, as part of the WVD Lighthouse program.

# What this document is not

This document is not a

* Detailed WVD implementation, execution guide
* Citrix + WVD deployment guide

# Target Audience

This document is primarily intended for Azure Specialists, Cloud Solution Architects, Technical Pre-Sales Teams and related stakeholders, primarily form Partner (and or Customer) Organizations who are going to build a SoW for their customers for the WVD Lighthouse program. It is assumed that the Partner (and their Customer) already has their standard SoW Template they use to describe their work (services), and this document merely helps them with the key WVD implementation steps that they need to consider and follow based on their customer requirements necessary to successfully execute the WVD program.

# Pre-requisites/Requirements

* Agreement with Customer to implement WVD and build a SoW.
* SOW Template with all the legal/required terms.

# WVD Deployments

A successful WVD engagement should consider the various implementation details like Networking, WVD Setup, Application Assessment, User Profile Management, Migration Scenarios (in case of migrating existing RDS implementations), Licensing Options, Management & Monitoring Capabilities and Identity & Security. This is by no means a complete list of all the implementation details, as each implementation is unique to the customer’s environment and needs. The document is only intended as a checklist and a starting point for the partner (or customer) team to customize the engagement as they see fit. Below is the outline of the key tasks typically required/recommended to successfully implement and execute the WVD engagement.

# Greenfield (new) Deployments

For Customers deploying WVD Service as a new or greenfield deployment, please follow the list of links below to complete the execution.

* [Azure Environment Assessment](#_Azure_Environment_Assessment) - For Customers with existing Azure deployments, the assessment phase can help identify resources that can be repurposed or utilized and narrow down the list of new services required for deploying WVD.
* [Licensing and Entitlements](#_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.
* [Application Assessment](#_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 the Users can perform this to get detailed insights into their applications.
* [Azure Networking](#_Networking) – As networking plays a crucial role in any cloud service, designing it to satisfy all the requirements is important.
* [Identity and Access Management](#_Identity_and_Access) - 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).
* [Security and Compliance](#_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.).
* [Image Management](#_Image_Management) - Organizations use Custom Images to implement their security controls and configurations, pre-install their IT applications for users.
* [Deploy and Configure Storage for User Profile(s)](#_Deploy_and_Configure) - 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.
* [WVD Environment](#_Windows_Virtual_Desktop) - Windows Virtual Desktop is a service that gives users easy and secure access to their virtualized desktops and RemoteApps. This section describes the WVD Environment.
* [WVD Deployment](#_Windows_Virtual_Desktop_1) – This section describes the steps required to deploy the WVD service.
* [FSLogix Setup and Configuration for WVD User Profiles](#_FSLogix_Setup_and) - 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.
* [Application and Desktop Management](#_Application_and_Desktop) – Manage publishing applications and desktops in WVD.
* [WVD Management and Monitoring](#_WVD_Management_and) - 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.
* [Patch Management](#_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.
* [Business Continuity and Disaster Recovery](#_Business_Continuity_and) - Customers can implement BCDR for their Session hosts using ASR. This would protect the VMs and provide faster recovery from disasters.

# Migrate to WVD

For Customers migrating from their existing RDS/VDI environment on-premise to WVD in Azure Service, please follow the links below to complete the execution

* [Azure Environment Assessment](#_Azure_Environment_Assessment) - For Customers with existing Azure deployments, the assessment phase can help identify resources that can be repurposed or utilized and narrow down the list of new services required for deploying WVD.
* [Licensing and Entitlements](#_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.
* [Application Assessment](#_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 the Users can perform this to get detailed insights into their applications.
* [Azure Networking](#_Networking) – As networking plays a crucial role in any cloud service, designing it to satisfy all the requirements is important.
* [Identity and Access Management](#_Identity_and_Access) - 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).
* [Security and Compliance](#_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.).
* [Image Management](#_Image_Management) - Organizations use Custom Images to implement their security controls and configurations, pre-install their IT applications for users.
* [Deploy and Configure Storage for User Profile(s)](#_Deploy_and_Configure) - 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.
* [WVD Environment](#_Windows_Virtual_Desktop) - Windows Virtual Desktop is a service that gives users easy and secure access to their virtualized desktops and RemoteApps. This section describes the WVD Environment.
* [WVD Deployment](#_Windows_Virtual_Desktop_1) – This section describes the steps required to deploy the WVD service.
* [Migrate Existing RDS/VDI Infrastructure](#_Migrate_Existing_RDS/VDI) – 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.
* [Convert and Migrate User Profiles](#_Convert_and_Migrate) – Customers running an existing RDS/VDI Infrastructure and migrating to WVD may also want to move their User’s profile data to WVD.
* [FSLogix Setup and Configuration for WVD User Profiles](#_FSLogix_Setup_and) - 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.
* [Application and Desktop Management](#_Application_and_Desktop) – Manage publishing applications and desktops in WVD.
* [WVD Management and Monitoring](#_WVD_Management_and) - 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.
* [Patch Management](#_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.
* [Business Continuity and Disaster Recovery](#_Business_Continuity_and) - Customers can implement BCDR for their Session hosts using ASR. This would protect the VMs and provide faster recovery from disasters.

# WVD Implementation Steps

# Azure Environment Assessment

As part of the Azure environment assessment phase, check for the following services to see if they already exist and can be utilized to deploy WVD.

The SoW should include this section to describe what steps are done to assess the existing environment.

* + Network
    - Verify if the CIDR block for the VNET/subnet has enough IP addresses for deploying new session hosts.
    - If utilizing a hybrid architecture, verify if a S2S VPN tunnel or Express Route exists between your On-prem network to Azure VNET.
  + Identity and Access Management
    - Verify Active Directory Domain Services are available in the Azure
    - If the Customer is using Hybrid Architecture, verify that you have
      * Connectivity to a Domain Controller from on-prem/Azure
      * AD Connect configured to sync objects between Domain Controllers and Azure Active Directory
    - If the Customer is cloud native, verify that
      * Azure Active Directory Domain Services is deployed to an Azure VNET.
      * the VNET is peered with the AAD DS VNET if the Session hosts are deployed in a different VNET.
  + Storage
    - Verify if there is a storage solution (Azure Files, NetApp, SOFS Cluster) already in place for user profile data.
  + Licensing/Entitlements
    - Verify if the Customer has required licenses/entitlements.
    - For accessing Windows Server deployments verify if the customer has required number of CALs/SALs.
  + Image and Patch Management
    - Verify if the Customer has any existing management solutions such as SCCM that they would like to utilize for Image and Patch management for WVD Session hosts.

**NOTE: Based on your environment assessment, re-use any existing resources/services and create other required services as detailed in further sections of this document. For example, if you already have a S2S VPN Tunnel or Express Route in place then skip this part in the networking section.**

# Application Assessment

The SoW may contain this section to articulate the steps taken by a Partner (or Customer) to assess their Applications.

* + Lakeside
    - One of the preferred/recommended tools to do an assessment is from ISV partner Lakeside. Use Lakeside for a deep application level assessment where it generates User Personas, Performance reports, VM SKU recommendations for the VDI Infrastructure that can be used to build out the WVD environment.
    - Register with Lakeside [here](https://partners.lakesidesoftware.com/engage/wvd-assessment/) and follow their instructions to download and setup Assessment agents in your current infrastructure.
    - Lakeside generates reports after running the assessment for a minimum of 2 weeks.
  + Azure Migrate
    - Use Azure Migrate for quick TCO and Infrastructure level assessments.
    - Azure Migrate helps with
      * Azure Sizing
      * Azure Cost
      * Azure Readiness for migrating On-prem VMs into Azure

# Networking

The SoW should contain implementation details on how the partner (or customer) will design and build out the networking topology for the deployment***.*** The recommendation is to design your Azure Networking using a [Hub-Spoke topology](https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke). Consider the HUB like a DMZ deployed with your Virtual Network Gateways and other security/edge appliances like Firewalls, AAD-DS Etc. while the Spoke will act as the backend zone where your Session hosts servers are deployed and is peered with the HUB.

* + Gather networking requirements and setup a Virtual Network (VNET) using Hub-Spoke Topology in Azure for deploying resources.
    - Deploy a Hub VNET
    - Deploy and configure Network Gateways, Firewalls or any Network Virtual Appliances in the Hub VNET
    - Deploy a Spoke VNET and establish peering with the Hub VNET
    - Configure User Defined Routes (if required) to route all traffic from the Spoke VNET via the Hub VNET to avoid any traffic directly traversing from the Spoke VNET
    - Configure Network Security Groups (NSG) to allow/deny access to your Session hosts.
    - All Session hosts and any other infrastructure will be deployed into the Spoke VNET
  + If utilizing a hybrid architecture, setup one of the following
    - Site to Site VPN
      * Implement S2S VPN for encrypted traffic over the internet
      * Setup S2S VPN with the Hub VNET
    - Express Route
      * Implement Express Route if the Customers want a Private Peering directly into Azure instead of traversing the Internet
      * Setup S2S VPN with the Hub VNET
  + For Migrations to WVD, create an isolated VNET to perform Test Failovers (this VNET should not have any connectivity/dependencies to Production resources such as Domain Controllers etc.).

# Identity and Access Management

The SoW must articulate the steps each partner (or customer) will take to setup the identity and access management aspects for the WVD deployment.

Please ensure that the Active Directory requirements mentioned in [**WVD requirements**](https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements) are completed before the additional steps in the below section can be accomplished.

* + Deploy/utilize one of the following for AD Domain Services presence in the VNET where Session Hosts are deployed
    - Utilize a hybrid architecture with S2S VPN or Express Route
      * Have an on-prem AD server sync with Azure AD using AD Connect or
      * Have an on-prem AD server sync with an IaaS AD VM in Azure and install AD Connect on the IaaS VM to sync with Azure AD
    - Deploy Azure AD Domain Services for Cloud Native deployments
  + Create AD Organization Unit (OU) structure for WVD Session Hosts
  + Create GPOs to manage access and security on the WVD Session Hosts
  + Create Users and AD Security Groups as required

# Security and Compliance

The SoW should consider the design and implementation of the following services to WVD setup and configuration.

* + Utilize [Azure Security Center](https://docs.microsoft.com/en-us/azure/security-center/security-center-intro) to strengthen the security and compliance posture of your infrastructure.
  + Integrate [Security Center with Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center) for proactive monitoring and threat mitigation.
  + Implement Single Sign-On with Active Directory Federation Services
  + Implement Multi Factor Authentication using Conditional Access for WVD
  + Implement Azure Firewall or a Network Appliance to restrict access only to WVD Resources

# Licensing and Entitlements

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

* + Ensure all users have one of the following Licenses/Entitlements or procure as required

| **OS** | **Required license** |
| --- | --- |
| Windows 10 Enterprise multi-session or Windows 10 Enterprise | Microsoft 365 E3, E5, A3, A5, F1, Business Windows E3, E5, A3, A5 |
| Windows 7 Enterprise | Microsoft 365 E3, E5, A3, A5, F1, Business Windows E3, E5, A3, A5 |
| Windows Server 2012 R2, 2016, 2019 | RDS Client Access License (CAL) with Software Assurance |
| FSLogix | Microsoft 365 E3, E5, A3, A5, Student User Benefits, F1, Business Windows E3, E5, A3, A5  Windows 10 VDS Per User  RDS CAL, RDS SAL |

# Image Management

Please follow the steps here to build your custom image for your Session hosts. Customers can also utilize any existing image management solutions.

The SoW should contain this section to describe how existing or new Image management solutions will be used along with WVD.

* + If you already have existing images that you would like to use with WVD, create and upload a [Master Image VHD](https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-customize-master-image) to Azure.
    - Create an Image from On-Prem VM
      * [Create a virtual machine in Hyper-V](https://docs.microsoft.com/windows-server/virtualization/hyper-v/get-started/create-a-virtual-machine-in-hyper-v)
      * Install and configure all required applications and settings.
      * [Prepare a Windows VHD or VHDX to upload to Azure](https://docs.microsoft.com/azure/virtual-machines/windows/prepare-for-upload-vhd-image)
      * If you're installing Office 365 ProPlus and OneDrive on your VM, see [Install Office on a master VHD image](https://docs.microsoft.com/en-us/azure/virtual-desktop/install-office-on-wvd-master-image)
      * [Upload the Image to Azure Storage Account and create an Image](https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-customize-master-image#upload-master-image-to-a-storage-account-in-azure)
    - Create an Image from VM in Azure
      * Provision a VM in Azure
      * Install and configure all required applications and settings.
      * [Generalize the Windows VM using Sysprep](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/capture-image-resource#generalize-the-windows-vm-using-sysprep)
      * [Create a Managed Image in the portal](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/capture-image-resource#create-a-managed-image-in-the-portal)
  + Use [Azure Image Builder (preview)](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Fvirtual-machines%2Flinux%2Fimage-builder-overview%3Ftoc%3D%252fazure%252fvirtual-machines%252fwindows%252ftoc.json&data=02%7C01%7CStefan.Georgiev%40microsoft.com%7Cb8a68cba8e9a411f361b08d72274c6b9%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637015757321685082&sdata=iQadU9OGjQ2Iro6PrG8J3CCdzqyVJsQM%2FSksnozdWoc%3D&reserved=0) or [Build image with Packer](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Fvirtual-machines%2Fwindows%2Fbuild-image-with-packer&data=02%7C01%7CStefan.Georgiev%40microsoft.com%7Cb8a68cba8e9a411f361b08d72274c6b9%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637015757321690070&sdata=RMJFwq1UT%2FbrDl4OMY95yfyD5nyVJhYpV9N6qM8z16g%3D&reserved=0) to manage images in Azure.
    - [Register the feature](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/image-builder-gallery#register-the-features)
    - [Set Variables and Permissions](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/image-builder-gallery#set-variables-and-permissions)
    - [Create an image definition and gallery](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/image-builder-gallery#create-an-image-definition-and-gallery)
    - [Customize image](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/image-builder-gallery#download-and-configure-the-json)
    - [Create image and build](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/image-builder-gallery#create-the-image-version)

# Deploy and Configure Storage for User Profile(s)

The Windows Virtual Desktop service recommends [FSLogix profile containers](https://docs.microsoft.com/en-us/azure/virtual-desktop/fslogix-containers-azure-files) as the default User Profile management solution. The SoW must articulate the steps each partner (or customer) will take to plan and setup the appropriate User Profile management solution for the WVD deployment.

* + Gather requirements on User Profile Sizes and deploy one of the following to store the User Profiles
    - [Scale out File Server with Storage Spaces Direct (SOFS with S2D)](https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-storage-spaces-direct-deployment)
    - [Azure NetApp Files](https://docs.microsoft.com/en-us/azure/virtual-desktop/create-fslogix-profile-container)
    - [Azure Files with SMB authentication using Azure AD Domain Services.](https://docs.microsoft.com/en-us/azure/virtual-desktop/fslogix-containers-azure-files)

# Windows Virtual Desktop Environment

Designing the WVD environment to satisfy the Customer’s organizational requirements is crucial for deploying the service.

The SoW should contain this section to describe how a WVD environment will be created for the Customer.

Windows Virtual Desktop [environment](https://docs.microsoft.com/en-us/azure/virtual-desktop/environment-setup) is comprised of the following hierarchy

* + Tenants
  + Host pools
  + App groups
  + Tenant groups
  + End users

Customers can have multiple tenants created and associated with their AAD and use them for specific departments in their organization or use a single WVD tenant and create separate Host pools for each department.

# Windows Virtual Desktop Deployment

The SoW should include a section to Setup, Build and Configure the WVD service in Azure. Once setup, the WVD service will provide Host pools which encapsulate all the Session hosts running under them and provide access to the published applications and desktops to the user.

Please follow the steps below to perform the build out.

* + Give [AAD Admin Consent](https://docs.microsoft.com/en-us/azure/virtual-desktop/tenant-setup-azure-active-directory) to the WVD service.
  + Assign Tenant Creator role in AAD to required users/service principals.
  + Create a new WVD Tenant
  + For greenfield deployments follow the below steps and skip this for Migrations to WVD
    - Use [Azure Marketplace Deployment](https://docs.microsoft.com/en-us/azure/virtual-desktop/create-host-pools-azure-marketplace) or [GitHub ARM Template Deployment](https://github.com/Azure/RDS-Templates/tree/master/wvd-templates/Create%20and%20provision%20WVD%20host%20pool) to create a Host pool and deploy Session hosts into it.
      * Windows 10 Multi-Session Deployment
      * Windows Server 2016 Deployment

# Migrate Existing RDS/VDI Infrastructure

Customers who need to migrate their existing on-prem RDS deployments to Azure and host them as Session hosts in WVD need this section.

The SoW should include this section to describe how on-premises infrastructure will be migrated to Azure and integrated with WVD.

* + Deploy and configure ASR Agents on the Physical hosts
  + Configure replication to Azure Storage account
  + Perform a test failover to validate the VMs are fully replicated without any issues
  + Perform final failover to Migrate the VMs to Azure
  + Install WVD Agents on the VMs to create a Host pool and attach these VMs to the Host pool
  + Configure FSLogix on the VMs if they are non-persistent
  + Create and publish Remote Apps/Desktops and grant access to Users

# Convert and Migrate User Profiles

As part of the migration process, the Customer can use Microsoft’s partner [Liquidware](https://docs.microsoft.com/en-us/azure/virtual-desktop/partners#liquidware). Liquidware’s ProfileUnity if they would like to move their user profiles (UPDs, UPMs etc.) from their on-premises storage to Azure. ProfileUnity automates the migration process and the Users can see their profile data in WVD with near-zero downtime.

If migrating to WVD, the SoW should articulate how the User’s profile data is migrated and converted (if required) to be compatible with FSLogix.

# FSLogix Setup and Configuration for WVD User Profiles

The SoW should describe how FSLogix is installed and configured on Session hosts.

* + [Install](https://docs.microsoft.com/en-us/fslogix/install-ht) FSLogix
    - Download the bits from [here](https://aka.ms/fslogix_download)
    - Copy them onto the Session host
    - Install FSLogixAppsSetup.exe
  + [Configure](https://docs.microsoft.com/en-us/fslogix/configure-profile-container-tutorial) FSLogix on the non-persistent Session host VMs.
    - Configure FSLogix settings using GPO to centrally manage all VMs from a single policy
    - Customers can also configure these settings by modifying local registry settings although this is not recommended

# Application and Desktop Management

Once the WVD tenant is setup and a Host pool is deployed, Admins are required to publish remote applications and desktops for the users to access.

The SoW should include this section as this describes the steps to install and configure the required application and desktop management options.

* + Publish [Applications or Desktops](https://docs.microsoft.com/en-us/azure/virtual-desktop/manage-app-groups) in the Host pool.
    - Create a RemoteApp group and set type to RemoteApp or RemoteDesktop
    - For RemoteApps
      * Browse and add applications to the RemoteApp group
    - Assign users to the RemoteApp group in order to access the published applications or desktops
  + Implement [Application Masking from FSLogix](https://docs.microsoft.com/en-us/fslogix/implement-application-masking-tutorial) or any 3rd party service to block access to certain applications to users or to grant access to only a certain apps.
    - Create a Rule Set
    - Test the Rule Set
    - Assign users/groups to the Rule to either allow them or deny them from accessing applications
    - Deploy the Rule Set
  + Implement Application Layering using [Liquidware](https://docs.microsoft.com/en-us/azure/virtual-desktop/partners#liquidware) FlexApp. With application layering, administrators can separate Windows applications from the underlying infrastructure and send particular virtual apps to users, depending on given circumstances, without the need for installation.

# WVD Management and Monitoring

The SoW should include this section as this describes the steps to install and configure the required WVD management and monitoring options.

* + Install [WVD PowerShell](https://docs.microsoft.com/en-us/powershell/windows-virtual-desktop/overview) module.
  + Deploy [WVD Management UI](https://docs.microsoft.com/en-us/azure/virtual-desktop/manage-resources-using-ui) in the subscription using GitHub ARM Template
  + Deploy a [WVD Diagnostics Portal](https://docs.microsoft.com/en-us/azure/virtual-desktop/deploy-diagnostics) in the subscription using GitHub ARM Template
  + Deploy [Scaling Script](https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-scaling-script) to Auto On/Off Session host VMs based on the current user load
  + [Load Balancing strategies](https://docs.microsoft.com/en-us/azure/virtual-desktop/host-pool-load-balancing) – Depth First vs Breadth First vs Persistent
  + RBAC Roles and privileges available for WVD Access Control
  + Deploy and integrate a Log Analytics workspace to the WVD Tenant using PowerShell
  + Run queries in the workspace to gather data on CPU Usage trends etc., for the Session host VMs
  + Check [VM health and performance](https://docs.microsoft.com/en-us/azure/azure-monitor/insights/vminsights-performance) using Azure Monitor

# 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. Since the Session host VMs are in an Availability Set, it will automatically ensure that not all of them are down at the same time. Below instructions are for managing Windows updates using Azure Automation. Customers can also utilize their existing management services such as SCCM or any 3rd party services.

The SoW should have this section to describe how Patch Management in implemented in WVD Session hosts to avoid any security vulnerabilities.

* + Create an [Azure Automation Account](https://docs.microsoft.com/en-us/azure/automation/automation-quickstart-create-account)
  + [Enable Update Management](https://docs.microsoft.com/en-us/azure/automation/automation-tutorial-update-management#enable-update-management)
  + [View Update Assessment](https://docs.microsoft.com/en-us/azure/automation/automation-tutorial-update-management#view-update-assessment)
  + [Schedule an update deployment](https://docs.microsoft.com/en-us/azure/automation/automation-tutorial-update-management#view-update-assessment)

# Business Continuity and Disaster Recovery

The SoW should include this section as this describes the steps to replicate VMs using ASR to shield the Customer from any disasters.

* + Implement [Disaster Recovery of Session host VMs](https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-architecture#replication-process) to another geographic location using Azure Site Recovery (ASR).
    - Create a Recover Services Vault in a different region than where the Session hosts are deployed
    - Enable Replication
    - Failover to the target region in the event of a Disaster
    - Resynchronize the VMs once the source region is online
    - Failback once the resynchronization is successful