Windows Virtual Desktop (WVD) SoW



Table of Contents

[1. Introductions 3](#_Toc35784409)

[Example Architecture 3](#_Toc35784410)

[2. Project Overview 3](#_Toc35784411)

[3. High-Level Solution Approach 3](#_Toc35784412)

[4. Scope of Work 4](#_Toc35784413)

[5. Key Engagement Activates 5](#_Toc35784414)

[Azure Environment Assessment: 5](#_Toc35784415)

[Licensing and Entitlements: 6](#_Toc35784416)

[Desktop Application Assessment: 7](#_Toc35784417)

[Azure Networking: 8](#_Toc35784418)

[Identity and Access Management: 9](#_Toc35784419)

[Security and Compliance: 10](#_Toc35784420)

[Image Management: 10](#_Toc35784421)

[Deploy and Configure Storage infrastructure for User Profile(s): 11](#_Toc35784422)

[Windows Virtual Desktop Service Deployment: 11](#_Toc35784423)

[Application and Desktop Management and Delivery: 11](#_Toc35784424)

[Business Continuity and Disaster Recovery (Azure to Azure): 13](#_Toc35784425)

[WVD Service Monitoring: 13](#_Toc35784426)

[Migrate Existing RDS/VDI Infrastructure: 14](#_Toc35784427)

[Convert and Migrate User Profiles: 14](#_Toc35784428)

[6. Assumptions: *List all of the assumptions:* 15](#_Toc35784429)

[7. Dependencies 16](#_Toc35784430)

[8. Out of Scope 16](#_Toc35784431)

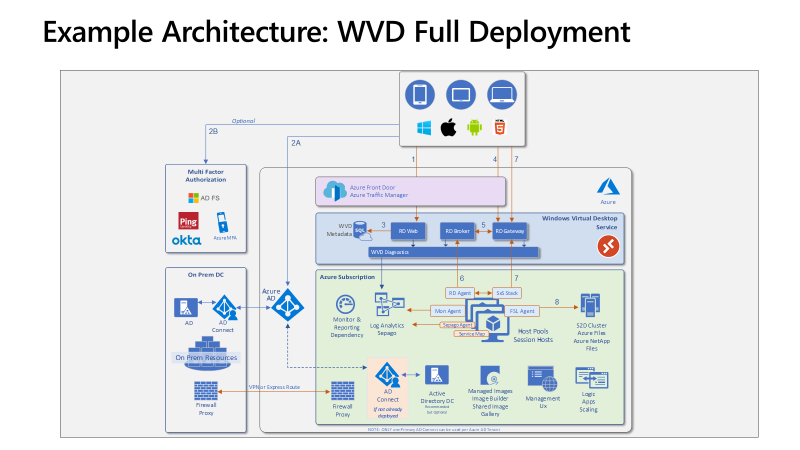
[9. Customer Acceptance Criteria 18](#_Toc35784432)

[10. Commercials 18](#_Toc35784433)

# Introductions

* Introduction to the Partner
* Experience with WVD & Azure
* Specialization (Security, VDI, ..)

## Example Architecture



# Project Overview

To be provided by the partner

# High-Level Solution Approach

*A successful WVD engagement should carefully consider the several key implementation details like Networking, WVD Setup/Configuration, Application Assessment, User Profile Management, Migration Scenarios (in case of migrating existing RDS implementations), Licensing Options, Management & Monitoring Capabilities, Identity and Security. This is by no means a complete list of all the implementation steps, as each deployment 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 specific engagement as needed. Below is the outline of the key tasks typically required/recommended to successfully implement and execute the WVD engagement.*

# Scope of Work

During this project, Partner will be deploying Windows Virtual Desktop by provisioning XX users up to YY VMs (at least 25 users up to 250 VMs) into a Windows Virtual Desktop Pool, and the project is expected to be delivered in X Days.

WVD Assessment and Design:

* **Customer Requirements:** Gather customer requirements for the WVD solution
* **Environment Assessments:**
  + Assess Azure Platform requirements to deploy WVD
  + Assess Licensing and Entitlement
  + Assess Application requirements
  + Assess Storage requirements
  + Assess Image Management requirements
  + Assess Network topology and requirements
  + Assess Identity and Access Management
  + Assess Security & Compliance requirements
  + Assess Monitoring requirements
  + Assess WVD Management requirements
  + Assess BCDR requirements
* **Design & Architecture:** Design WVD Desktops architecture and solution
* **Enablement:** Customer & End User Enablement.

WVD Deployment:

* Implement a Windows Virtual Desktop Host Pool for Personal Desktops
* Implement WVD design architecture components
  + Implement Azure Platform requirements to deploy WVD
  + Deploy Applications
  + Deploy Storage
  + Deploy Image Management solution
  + Deploy Network topology
  + Deploy Identity and Access Management
  + Deploy Security & Compliance solutions
  + Deploy Monitoring solutions
  + Deploy WVD Management tools
  + Deploy BCDR solution

The details of the assessment, design, and implementation for each item are listed in the follow sections.

## Key Deliverables

* Customer Requirements Documentation
* Environment Assessments Report
* Design & Architecture Document
* Customer & End User Training.
* WVD Solutions Implementation as per the approved Design & Architecture

PLEASE ADD / REMOVE TO THE ITEMS LISTED AS PER YOUR CUSTOMER’S REQUIREMENTS!

# Key Engagement Activities

Azure Environment Assessment:  
*Evaluate the current Azure footprint to drive efficiency and reuse services. For Customers with existing Azure deployments, the assessment phase can help identify resources that can be repurposed or utilized and reduce the number of new Azure services required for deploying WVD.*   
Insert details of the Customer’s current Azure environment and how WVD will be integrated (or not) to their existing Azure infrastructure.

| Description | Action (Delete as appropriate + add details) |
| --- | --- |
| * Network Assessment | * Verify if the CIDR block * Ensure the VNET/subnets have suitable IP addresses for deploying 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 Assessment | * Verify if Customer has Azure AD Connect deployed * If Hybrid Setup required, Customer has S2S VPN or ExpressRoute enabled between Azure and Customer Datacenter * 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 Assessment | * Verify Active Directory Domain Services are available   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 * VNET is peered with the AAD DS VNET if the Session hosts are deployed in a different VNET |
| * Storage Assessment | * Verify if there is a storage solution (Azure Files/ NetApp Files/ SOFS Cluster/ Standalone File server) already in place for re-using it for user profile data   NOTE: If you choose Azure NetApp Files as the storage option, remember it has regional limitations. Check to ensure the service is available in a region closer to you for better performance. |
| * Licensing / Entitlements Assessments | * Verify if the Customer has the 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 OR azure native solutions like update-management and image-builder-overview can be leveraged. |

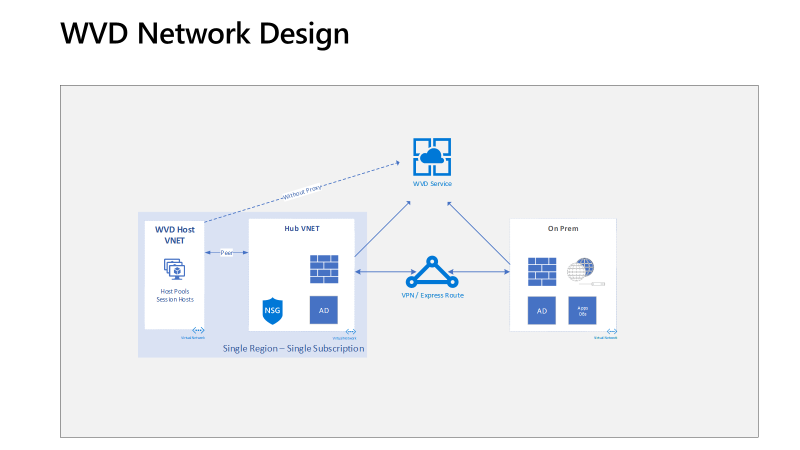
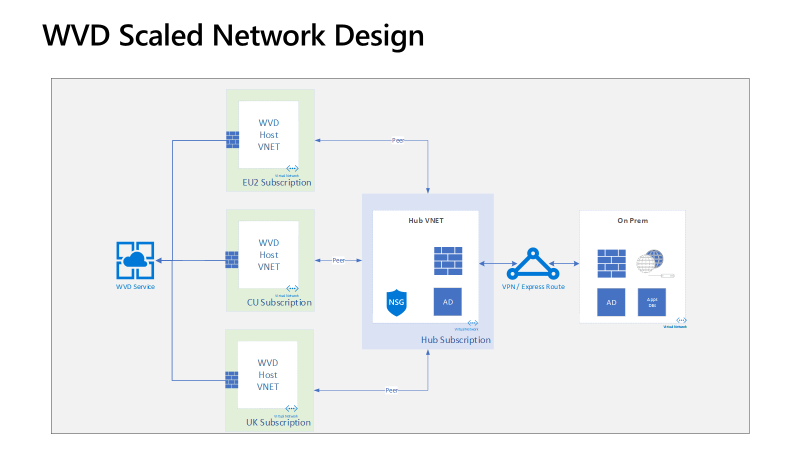
Licensing and Entitlements:  
*Ensure there is a licensing plan in place to run the appropriate apps or desktops in Azure WVD. Access Windows 10 Enterprise and Windows 7 Enterprise desktops and apps at no additional cost if you have an eligible Windows or Microsoft 365 license. For accessing Windows Server based deployments, you need to have an RDS CAL with SA.*   
  
Insert the current licensing entitlements of the customer (E3, E5, etc) and whether new licenses such as RDS CALs will be required for this deployment.

| Description | Quantity |
| --- | --- |
| * Microsoft 365 E3, E5, A3, A5, F1, Business Windows E3, E5, A3, A5 |  |
| * RDS Client Access License (CAL) with Software Assurance |  |

Desktop Application Assessment:  
*Conduct an Application Landscape assessment. Application assessments provide the current performance and usage details like OS, Application Compatibility, CPU, memory etc., and aids in VM sizing recommendations by classifying users into Personas (task workers, power users, knowledge worker etc.) and related Azure costs. This is an optional step for greenfield deployments, but it is recommended that partners/customers perform this to get detailed insights into their applications needs.*  
Insert application assessment and list applications in/out of scope for the VDI implementation.

* + 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

| Description | Assessment Report |
| --- | --- |
| * Azure Migrate |  |
| * Lakeside (Or alternative 3rd Party) |  |

Azure Networking:  
*As networking plays a crucial role in any cloud service deployment, designing a robust network architecture to satisfy all the KPI requirements is important. This should be part of your services in the design.*   
Insert details of the to be Azure networking including connectivity to on-premise if required (VPN, Expressroute, etc). Your design should contain details on how the partner (or customer) will design and build out the networking topology for the WVD deployment. 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, 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.  
  
  


Identity and Access Management:  
*WVD Service in Azure requires Authentication and Session hosts to be domain joined using Windows Active Directory (AD). This can be done either from the on-premise environment or using Azure AD Domain Services (AAD-DS).*Insert the identity strategy for the deployment (AAD, IaaS +AD Connect, On-Premise +AD Connect).

| Description | Action (Delete as appropriate) |
| --- | --- |
| * Identity & Access Management Configuration | * Utilise a hybrid architecture with S2S VPN or Express Route * Deploy an on-prem AD server sync with Azure AD using AD Connect or * Deploy 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 host pools * Create GPOs to manage access and security on the WVD Session Hosts * Create Users and AD Security Groups as required |

Security and Compliance:  
*Customers need to strengthen the security and access mechanisms of their WVD deployments as they are governed by corporate policies (compliance, regulations etc.). This is a crucial step in the WVD implementation.*   
Insert security standards which are required for the customer, include which security solutions will be implemented to achieve the required level of security. (Security Centre, Azure Firewall, NGFW, Azure Sentinel, Logging, AAD Premium Conditional Access, RBAC, MFA, GPOs, Partner Solutions etc).

| Description | Action (Delete as appropriate + add details) |
| --- | --- |
| * Security Services Deployment | * Configure RBAC * Deploy & Configure AAD Premium * Configure Conditional Access * Configure Security Center * Deploy Azure Firewall * Deploy NGFW * Configure MFA * Configure GPOs * Deploy 3rd Party Solution.. |

Image Management:  
*Organizations use Custom Images to implement their desktops/apps including security controls and configurations, pre-install their IT applications for specific users. Ensure there is a good image management process is in place.*   
Insert details of the image management process, how images and software will be updated, how patches will be managed (SCCM, 3rd Party, Azure Image Builder, etc).

| Description | Action (Delete as appropriate + add details) |
| --- | --- |
| * Image Management Solution | * Deploy & Configure SCCM * Configure Azure Image Builder * Deploy 3rd Party Image Management Tool * Create an Azure Automation Account * Enable Update Management * View Update Assessment * Schedule an update deployment |

Deploy and Configure Storage infrastructure for User Profile(s):  
*User profile management is a key step in designing a successful WVD environment. 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. This section provides steps to create a storage infrastructure for User profiles.*  
Insert the profile storage details (Typically FSLogix+ Azure Files / NetApp Files / Storage Spaces Direct) 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 utilise the FSLogix Profile Containers to manage User profile data.

| Description | Action (Delete as appropriate + add details) |
| --- | --- |
| * Profile Storage Solution | * Deploy & Configure FSLogix * Deploy Azure Files * Deploy Azure NetApp Files * Deploy S2D on Azure |

Windows Virtual Desktop Service Deployment:  
*This is one of the key steps in the WVD deployment. Windows Virtual Desktop is a service that gives users easy and secure access to their virtualized Desktops and RemoteApps. This section describes the various components of a WVD Environment, and the steps required to deploy, setup and configure the WVD service.*  
Insert details of how the WVD Tenant and Hostpools will be created and whether a partner solution will be used. Some partner solutions simplify the deployment of WVD and include additional features.

| Description | Action (Delete as appropriate + add details) |
| --- | --- |
| * WVD Deployment | * Configure WVD Tenant Roles * Create WVD Tenant(s) * Deploy 3rd Party Tenant Management Solution |

Application and Desktop Management and Delivery:  
*Once WVD elements are deployed, the applications and desktops need to be published and managed. Ensure this step is part of the implementation process.*   
Insert details of the application and desktop management and delivery if applicable, partner solutions from Citrix, VMware, Nerdio, and more can be included here.

| Description | Action (Delete as appropriate + add details) |
| --- | --- |
| * WVD Management Solution | * Configure WVD using Azure native tools * Mange the service configuration using PowerShell * Customize Feed for Windows Virtual Desktop * Customize RDP Properties * Load Balancing strategies – Depth First vs Breadth First vs Persistent * RBAC Roles and privileges available for WVD Access Control * Deploy Scaling Script or Azure Automation Runbook for PowerShell to Auto On/Off Session host VMs based on the current user load * Deploy WVD Management UI in the subscription using GitHub ARM Template * Publish Applications or Desktops 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 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 any one of the below solutions. With application layering, administrators can separate Windows applications from the underlying infrastructure and send selected virtual apps to users, depending on given circumstances, without the need for installation. * Deploy & Configure Liquidware / FlexApp * Deploy & Configure Microsoft App-V * Deploy & Configure Citrix Managed * Deploy & Configure VMware Horizon Cloud on Azure * Deploy & Configure 3rd Party WVD Management Tool |

### Business Continuity and Disaster Recovery (Azure to Azure):

*Customers sometimes may require a highly available WVD deployment. BCDR can be implemented for Session hosts using ASR. This would protect the VMs and provide faster recovery from disasters.*

Insert BCDR requirements and the solution(s) to be implemented (ASR, hot/cold standby, 3rd party, etc).

| Description | Action (Delete as appropriate + add details) |
| --- | --- |
| * WVD BCDR Solution | * Deploy ASR replication to secondary region * Implement Disaster Recovery of Session host VMs 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 * Configure WVD Hot / Cold Standby * Deploy & Configure 3rd party BCDR solution |

WVD Service Monitoring:  
*Ongoing monitoring of your WVD environment is required to deliver best performance to your users. This will provide you with insights into any issues or errors. Ensure that your WVD implementation has taken this into consideration.*   
Insert details whether this is a managed service or deployment only, SLAs, tools used to monitor infrastructure and user performance.

| Description | Action (Delete as appropriate + add details) |
| --- | --- |
| * WVD Monitoring Solution | * Configure Azure native monitoring * Investigate WVD activity log and errors using the PowerShell module * 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 using Azure Monitor * Deploy Azure Monitor for RDS and Windows Virtual Desktop by Sepago * Deploy a WVD Diagnostics Portal in the subscription using GitHub ARM Template * Configure 3rd Party monitoring solution |

Migrate Existing RDS/VDI Infrastructure:  
*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. ASR/Azure Migrate is the tool of choice for migrations and can migrate BOTH Windows Server and Client OS based machines.*  
Insert details of the existing VDI platform, tools to assess and migrate, assessment of the environment, existing licenses, migration approach, user transition, roll-back plan.

Convert and Migrate User Profiles:  
*Customers running an existing RDS/VDI Infrastructure and migrating to WVD are encouraged to migrate their user profiles to WVD.*  
Insert details of how the user profiles will be migrated, the tools used, consider the size of the profiles and required time to migrate

| Description | Action (Delete as appropriate + add details) |
| --- | --- |
| * Migration from on-premises VDI | * Deploy Azure Migrate * Deploy 3rd Party assessment & migration tool * 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 and ensure the VMs that will be part of a particular hostpool are in availability sets to avoid VMs going down for maintenance at the same time. * Verify that all security and governance policies are still intact * 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 & Migrate User Profiles | * Convert User Profiles * Migrate User Profiles to WVD Solution |

# Assumptions: *List all of the assumptions:*

| Description (Add and Remove are required) | Details |
| --- | --- |
| * Customer will attend workshops and share required information regarding identity, applications, networking and Azure Readiness * Customer will share scale requirements |  |
| * Customer has Azure AD Connect deployed * If Hybrid Setup required, Customer has S2S VPN or ExpressRoute enabled between Azure and Customer Datacenter * Customer has procured an Azure subscription and has provided access. * Active Directory is extended to Azure IaaS platform or a network connection is in place for authentication to occur to existing Active Directory servers. * Azure AD Domain Services will be deployed if required * If a custom image is required with LOB applications, the customer can upload to Azure and it can be used with WVD Deployment * Auto-Scaling is out of scope, however, sample scripts will be provided for customer to test if required. |  |

# Dependencies

*List all of the dependencies required:*

| Description | Details |
| --- | --- |
| * Dependencies |  |

# Out of Scope

*List all of the out-of-scope items:  
Please list all of the items you remove from the Scope of Work in this section along with any additional items which are Out of Scope for your project.*

| Description (Add and remove as required) | Details |
| --- | --- |
| * Azure Environment Assessment * Licensing and Entitlements * Desktop Application Assessment * Azure Networking * Identity and Access Management * Security and Compliance * Image Management * Deploy and Configure Storage infrastructure for User Profile(s) * Windows Virtual Desktop Service Deployment * Application and Desktop Management and Delivery * Business Continuity and Disaster Recovery (Azure to Azure) * WVD Service Monitoring * Migrate Existing RDS/VDI Infrastructure * Convert and Migrate User Profiles |  |
| * Product licenses | Product licenses will not be provided. The Customer is responsible for acquiring all necessary product licenses required as a result of this WO. |
| * Hardware | Hardware will not be provided under this WO. The Customer is responsible for acquiring and configuring all necessary hardware. |
| * Management of Windows servers | Management, operational process, backup/restore, disaster recovery, and decommissioning of Windows VMs is the Customer’s responsibility. |
| * Organizational change management | Design or redesign of the Customer’s functional organization unless specifically included in scope |
| * Training and training materials | Creation or delivery of training materials is not in scope. |
| * Azure subscription | Creating or configuration of an Azure subscription, if required, and establishing any required connectivity including the following configurations (native Azure or third-party) are not in scope:  Load balancer  Firewall  Network Virtual Appliance  Network Security Groups (NSG)  Application security groups  Global traffic manager  Application gateway |
| * Performance testing | Performance testing in comparison to source on target is not in scope. |
| * Application deployment | Manual or scripted deployment of applications on Azure virtual machines is out of scope. |
| * FSLogix | Profiles hosted on an external system off the VMs is not in scope. It is assumed for this deployment users will be allocated to personal desktops. |
| * Migration | Migration from current VDI is not in scope. |
| * Applications | Publishing Applications via app groups (remote apps) is out of scope. |
| * Image Management | A Windows 10 Image with Office Pro Plus will be deployed. Additional applications deployed are customer responsibility. If a custom image is preferred, the customer can upload to Azure and it can be used. |
| * Automation | Any automation such as auto scaling, or auto shutdown is considered out of scope. |
| * Networking | Any networking configuration such as forward proxies or firewalls is out of scope. |
| * Security | Any enablement of security policies is out of scope. Hardening should be provided via suggested OU or customer image. |

# Customer Acceptance Criteria

*Verify that the WVD Implementation is successful. This is a critical stage in the overall process.*   
Insert details of the User sign-off process, key stakeholders, success criteria, minimum requirements, key contacts.

| Description | Action (Delete as appropriate + add details) |
| --- | --- |
| * Service Validation | * Define validation criteria and align with key stakeholders * Validate WVD host pool configuration * Validate WVD application configuration * Validate connectivity to on-premises applications * Validate WVD performance * Validate WVD User profile solution * Validate WVD across clients |

# Commercials

| Description | Details |
| --- | --- |
| * Effort estimation with cost with breakup (Tasks/Resources/Hours) |  |
| * One-time charges (Network, Initial Setup, etc.) |  |
| * Recurring charges (Ongoing support, SW, etc.) |  |