

Windows Virtual Desktop Scenario (WVD) Enablement Kit Aligned to

Azure Cloud Adoption Framework

**Table of Contents**

[1. Introduction 4](#_Toc44021468)

[2. WVD - Cloud Adoption Framework 4](#_Toc44021469)

[2.1 Strategy Phase 4](#_Toc44021474)

[2.1.1 Understanding Business Motivations 4](#_Toc44021475)

[2.1.2 Business Outcomes of WVD 7](#_Toc44021476)

[2.1.3 Quantifying Business Justification for WVD 8](#_Toc44021477)

[2.1.4 WVD First Project 8](#_Toc44021478)

[2.2 Plan Phase 8](#_Toc44021479)

[2.2.1 Digital Estate 9](#_Toc44021480)

[2.2.2 Cloud Adoption Plan 11](#_Toc44021481)

[2.2.3 Skill Readiness 15](#_Toc44021482)

[2.2.4 Azure Environment Assessment 15](#_Toc44021483)

[2.3 Ready Phase 15](#_Toc44021484)

[2.3.1 First Landing Zone 16](#_Toc44021485)

[2.3.2 Create a Tenant in Windows Virtual Desktop: 19](#_Toc44021486)

[2.3.3 Build VM Image 19](#_Toc44021487)

[2.4 Adopt 20](#_Toc44021488)

[2.4.1 Host Pool Setup 20](#_Toc44021489)

[2.4.2 Innovate - Greenfield (new) Deployments 22](#_Toc44021490)

[2.4.3 Migrate – RDS workload to WVD 24](#_Toc44021491)

[2.5 Governance 29](#_Toc44021492)

[2.5.1 Security Baseline 33](#_Toc44021493)

[2.5.2 Identity and Access Management 35](#_Toc44021494)

[2.5.3 Cost Management 36](#_Toc44021495)

[2.6 Manage 36](#_Toc44021496)

[2.6.1 WVD Management and Monitoring 36](#_Toc44021497)

[2.6.2 Patch Management 37](#_Toc44021498)

[3. Appendix A – Technical References 38](#_Toc44021499)

[4. Deleted Content 38](#_Toc44021500)

Version history

|  |  |  |
| --- | --- | --- |
| Version | Changes | Date |
| V0 | Initial Release | April 2020 |
| V1 | Final Release | June 2020 |

Disclaimer

© 2020 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. Microsoft customers and partners may copy, use and share these materials for planning, deployment and adoption of Microsoft Cloud Adoption Methodology.

**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.

We look forward to your feedback!

Thank you for your continued trust and partnership. The resources within this toolkit will be iteratively improved upon based on product releases as well as direct feedback from delivered engagements. We encourage you to provide feedback to help us improve our products and toolkits.

# Introduction

This document will provide partners and customers guidance to deploy and manage Windows Virtual Desktop deployment in Azure in alignment to Cloud Adoption Framework (CAF). This guide is structured according to the phases of Cloud Adoption Framework; detailing the work that needs to happen in each CAF phase for a successful WVD deployment. In this section, we will discuss the audience intended to refer this document, a brief on WVD deployment and CAF introduction.

**Audience**

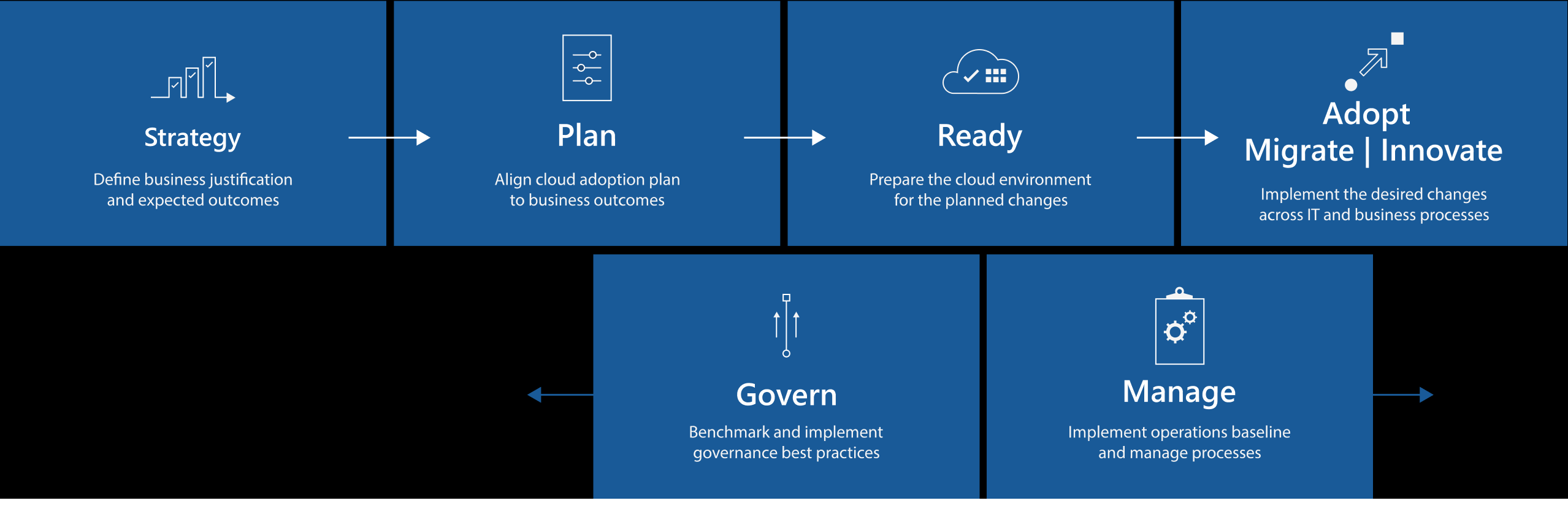
This document is primarily intended for Azure Specialists, Cloud Solution Architects, Technical Pre-Sales Teams and related stakeholders, primarily form Partner and Customer Organizations who are going to build adopt or migration Windows Virtual Desktop. This document helps them with the key phases in CAF framework that needs to be consider and follow based on their business needs and customer requirements necessary to successfully implement the WVD.

**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. This 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.

**Cloud Adoption Framework**

Let’s start by understanding what is Cloud Adoption Framework. Cloud Adoption Framework is a collection of documentation, implementation guidance, best practices, and tools that are proven guidance from Microsoft designed to accelerate your cloud adoption journey. Below is the outline of the key tasks typically required/recommended to successfully implement and execute the WVD engagement. Below diagram shows the different phases of Cloud Adoption Framework Journey. In this document we explain what needs to happen for WVD deployment and management in each phase of the cloud adoption framework.



# WVD - Cloud Adoption Framework



## Strategy Phase

Documenting WVD Strategy will assist business stakeholders and technicians in understanding the organizational benefits that entail adopting WVD. This section will specifically discuss the following:

* Business Motivations
* Business Outcomes
* Business Justifications associated with WVD adoption
* WVD First Project

### Understanding Business Motivations

Outlining the motivations for a business is crucial in order to construct an appropriate strategy. Business stakeholders should be included in the discussion and outlining of relevant business motivations. Business motivations for WVD adoption are categorized into the following four general pillars:

* Critical Business Events
* Changes in Workforce
* End-user Computing Migration & Secure Access
* Innovation Motivations

The above categories are meant as a source of inspiration and are not an exhaustive list of all existing business motivations. However, overall motivations can be broken down further for WVD as below:

|  |  |  |  |
| --- | --- | --- | --- |
| **COST** | **SECURITY** | **SCALE** | **INNOVATION** |
| Underwriting of desktop digital estate  Datacenter exit/adopting Commercial cloud  Bringing the overall IT cost of managing, maintain and secure down  Thin Client and Mobile Desktop adoption  Cost management of VDI Infrastructure | BYOD Deployment & Governance  Compliance/regulatory protocols  End of Support for Windows 7  Data sovereignty requirements  Endpoint management  Desktop computing Threat Protection | On-demand resources onboarding  Meeting market demands  Business agility – proactive vs. reactive  Mergers & Acquisitions, Geo expansion  Varying workforces  Workforce consolidation | Building new technical capabilities  Improve customer experience  Market disruption – new services and products  Transforming products and services  Frontline workforce empowerment  Changes in Communication & Collaboration License |

All the above motivations are described in detail below:

#### Cost

One of the most consistent business motivations when adopting or migrating to a new technology is **COST**. We cannot maintain and operate a secure desktop and end user computing environment in on-prem data center in a cost-effective manner. There are certain drawbacks while maintaining end user computing environment. These drawbacks are:

* Operational and Capital expenses are quite steep
* Owning enough labor to continuously monitor and manage the infrastructure
* Acquisition of new hardware or hardware refresh

**Solution to above Drawbacks**: Migrating to WVD and adopting a cloud-based desktop computing will make things more cost-effective.

**Benefits**:

* Adopting WVD’s Windows 10 Multi-Session Technology significantly reduces average cost, per user, per month (up to 70% in reserved instances use), compared to the traditional Windows 10 Single-Session.
* For High Performance workloads WVD’s Personal Computing provide a choice of hardware options to choose when need arises to scale and make a right fit.
* WVD eliminates the cost of RDS Client licensing.
* No VDI management infrastructure cost.
* WVD also eliminates the need for deploying your own management infrastructure, RDS Client licensing since it is provided by WVD.
* Microsoft 365– this significantly reduces the required labor cost and additional overhead fees.

All in all, WVD brings down the overall TCO drastically (running Windows Server at Linux VM cost) for managing and maintaining your virtualized desktop workloads.

#### Security

Security protocols and compliance issues regarding data or applications are a very common scenario in regulated industries. As such, the need to be quickly assessed but finding a solution is often complex and time consuming. Keeping your data secure, regardless of end computing devices, is one of WVDs many strengths.

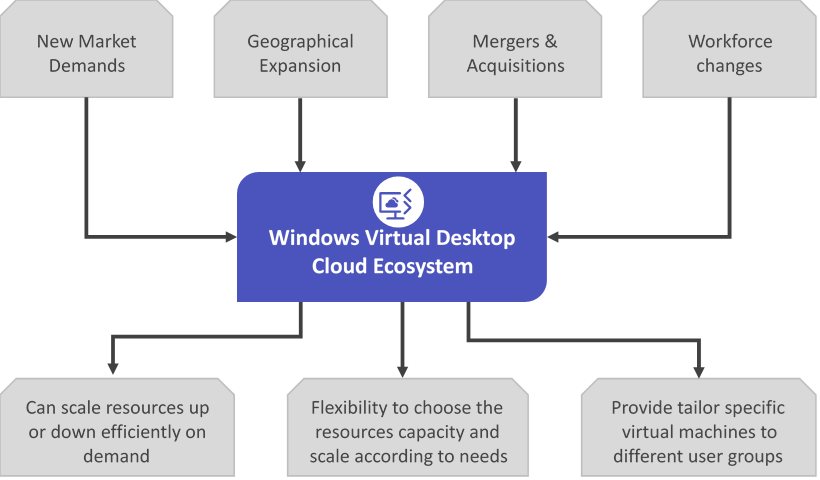
* WVD has “reverse connect,” which literally negates the need for inbound traffic and reduces the overall attack surface of your ecosystem.
* Azure Active Directory authentication makes sure that all connections and user data is isolated for valid users within your ecosystem, making data sovereignty requirements easy to handle.
* WVD and Azure have more compliance certifications than any other cloud provider

More recently, Windows 7 End of Support for all desktop computing needs, resulting in a wide variety of compliance issues for many businesses. However, WVD allows businesses to continue utilizing their legacy applications on a fully supported Windows 7 Operating System for the next three years, cost free.

* The VDI Infrastructure and Public Facing IP are maintained by Microsoft so businesses do not have to be concerned with gateways or connection brokers.
* If you connect WVD to your existing Microsoft ecosystem, you can take advantage of Conditional Access, Multi-Factor Authentication and Role-based Access Control present in M365, and combine it with Azure’s compliance offerings and extensive team cybersecurity experts – effectively making WVD one of the most secure VDI platforms on the market.

#### Scale

Scaling your business to accommodate below requirements:

Currently, Microsoft Azure boasts the largest geographical footprint of any cloud provider with more than 54 Azure Regions. This expansive footprint, in turn, enables an easy transition with new mergers and acquisitions, as well as enabling your remote workforce, irrespective of geographical location.

If a business’s virtual desktop journey requires the reuse of existing investments, such as Citrix, VMWare environments, or other solution providers, WVD has the inherent ability to support both persistent and non-persistent environments, while retaining the profile structure of previous environments.

#### Innovation

* WVD offers a business unparalleled agility with its demand driven scaling potential that can accommodate nearly any workload significantly faster than acquiring the equivalent hardware.
* WVD offers the only multi-session Windows 10 user experience, while, at the same time, keeping cost considerably lower compared to any single session VM infrastructure due to high CPU utilization.
* With WVD, businesses have access to the highest quality value-adding partner network. These value-adding partners, who work in tandem with Microsoft, make it possible for businesses to constantly have the ability to reach out and obtain professional guidance, with the assistance of third-party applications in Azure Marketplace ecosystem as well. The third-party applications have all been catered to the Microsoft APIs so you can tailor WVD workloads in any way.
* Leveraging WVD also enables any business the capacity to utilize WVDs end-to-end diagnostic services. These services make the identification of root causes efficient and fast compared to an infrastructure, where logs can be dispersed across multiple clients, RDS servers, and VMs.

### Business Outcomes of WVD

The next step for creating a comprehensive WVD adoption strategy is to take the business motivations and figure out what business outcome are likely to transpire.

The categories of business outcomes vary between five general buckets. It is important for anticipated business outcomes to be ranked according to priority: from high, to mid, to low priority. They include stakeholders, the business drivers behind a specific outcome, and associate what KPIs and capabilities are required in order to achieve the desired outcome.

The following categories as displayed in figure are used to identify and categorize desired business outcomes.

### Quantifying Business Justification for WVD

Justifying the decision to migrate or adopt WVD will require somewhat complex calculations. In its basic form, the calculations needed to justify WVD are:

|  |
| --- |
| **Initial investment** is the capital expense and operating expense required to complete the WVD initiative.  **Gain from investment** include revenue deltas and cost deltas. |

### WVD First Project

By considering all the motivations, outcomes, and justifications, you should be able to pinpoint a business strategy that supports your initial project. It is important that the outlined motivations are aligned with the new WVD engagement. The criteria should be able to demonstrate progress towards a defined business outcome.

* **First project expectation**

First project expectations are mainly used to test the waters and thus create a learning platform. Acknowledging the possibility of a first project may necessitate more effort than originally anticipated to properly gauge production deployments. Starting fresh is typically difficult and that is why a first project objective should be to create a clear set of requirements for a long-term production solution.

* **Greenfield scenario for WVD pilot project**

The greenfield deployment scenario - for any WVD pilot project - has a standard setup that both enables most scenarios and tests various capabilities associated with each setup.

|  |  |  |
| --- | --- | --- |
| **WVD Pilot Configuration** | **Host pool 1** | **Host pool 2** |
| WVD (W7, W10, W10 MS, WS) | Windows 10 Multi-session | Windows 10 |
| **Customer Environment / User Requirements** |  |  |
| User Type | Medium | Medium |
| App group | Desktop app group | Remote app group |
| Named (total) users | 75 | 25 |
| Peak Concurrency | 80% | 100% |
| Pooled / Personal | Pooled | Personal |
| Azure Region (Example of one potential region) | US-East | US-East |

## Plan Phase

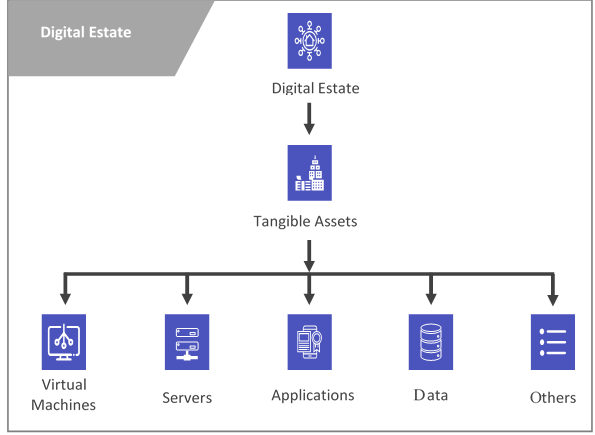
Planning is a crucial step which aids to build a roadmap to transform the strategy goals and business motivation into actionable items in alignment with the technical efforts.

The following subsections cover the plan phase:

* Digital Estate
* Cloud Adoption Plan
* Skill Readiness
* Azure Environment Assessment

This approach captures important tasks to drive adoption efforts. The derived plan then maps to the metrics and motivations defined in the cloud adoption strategy.

### Digital Estate

The initial part of planning is understanding your digital estate and your need and based on that understanding – a plan can be constructed. In other words, a digital estate is the collection of IT assets that power your business processes and supporting operations. From a WVD perspective, it is imperative to quantify the complex digital workplace that end users navigate day to day to stay productive. We must assess the distinct services, devices & form factors, applications (desktop, remote and SaaS apps) and other assistive workloads that you wish to use in the cloud.

Microsoft Monitoring Agent can be deployed on both physical and virtual end computing devices, which in turn gathers, analyses the telemetry of the workloads and also help to build heuristics of end user usage patterns. All of this information, whether it is On-premise or cloud is collected in a centralized Log Analytics database. Realization of this telemetry data makes it possible to visualize and leverage insights thus proactively solve the problems before they can occur.

With the aid of Azure Monitor, this information can be analyzed further in real-time, proactively documenting the key decision drivers for the adaption of WVD.

The processes which drive the adaption of WVD are detailed below:

#### Cloud Rationalization

Cloud rationalization is the process of evaluating applications and strategically identifying assets within the cloud that needs to be replaced or modernized. It is an on-going process of transforming assets to facilitate changes in the cloud. This can be done in 3 ways as described below:

**Rehost scenario**

Also known as a lift and shift migration, a rehost effort moves a current state asset to the chosen cloud provider, with minimal change to overall architecture.

Lifting and shifting in cloud:

* Migration of Win7 workload to Azure WVD
* Migration of Win 7 Virtual Desktop Infrastructure to Win 10 VDI Single session

**Rearchitect scenario**

Some aging applications aren't compatible with cloud providers because of the architectural decisions that were made when the application was built. In these cases, the application might need to be rearchitected before transformation.

Scenarios that are considered as Rearchitect Scenarios:

* Migrating workload from RDS to Windows Virtual Desktop: Customers who need to migrate their existing on-prem RDS deployments to Azure and host them as Session hosts in WVD need this section.

This section shall 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 that 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

**Rebuild scenario**

In this scenario, original coding is discarded. Rebuilding the application allows us to take advantage of more advanced and innovative features and improve the application even further. The new cloud-native application would be inexpensive to operate and it is usually done for applications which are now unsupported or misaligned with the current business processes.

#### Documentation of Digital Estate

Assessing the environment help us establish a “Privilege Vantage point” for end user computing needs, as we derive *“Where the business of productivity happens within our digital workplace estate?”* (i.e. laptop, endpoint, virtual machine). For WVD, continuous assessment helps us to define the drivers listed below:

* **Core Applications & Data**

A quantitative inventory of desktop applications, SaaS apps, data storage, and system performance metrics that helps us to rationalize and document ideal candidates of apps & services to be hosted on WVD environment

* **Important Digital Workplace Features**

A qualitative analysis of features and capabilities are to be identified by business stakeholders as these are unique to the organization and solution identified and can only be answered by business stakeholders and power users. For WVD, this helps to map the end user experience to multi-session offerings of the platform

* **Identity and Data Access**

A thorough understanding of how current physical and virtual endpoint devices manage the user identity, nature of access to local data, data stored by application (desktop, web, SaaS) and identity federation requirements helps to derive domain connectivity and Azure AD synchronization and thus lays the foundation of user access in WVD

With adequate quantification of digital workplace and continuous assessment of the above drivers helps to transform the needs to informed decisions for multi session desktop infrastructure.

#### Application Assessment

Application assessment provides:

* Current performance and usage details of 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

It is important to understand the required compute of your core applications & data in order to size your VMs, use the correct Operating System, etc. However, to understand the importance of your user groups or Personas, we need to classify them as below.

**Groups of Users / Personas**

There are many types of workers within the same departments and it is of vast importance to classify them correctly if you plan to successfully deploy optimized WVD workloads. Furthermore, we can begin with an easy step by outlining the number of seats that is required based on your User Groups. Examples of user groups could be:

* Frontline workers
* Core Engineers
* Office Staff
* Remote Workers

Then you analyze the core application and data usage that is required by the user groups in order to remain productive in their individual positions. Foremost requirement could be data security if they are handling sensitive data and then it is important to take the necessary security precautions. Taking all of these requirements into consideration it is time to decide how each group of users connect to their sessions.

### Cloud Adoption Plan

Cloud adoption plans start with a well-defined strategy. The strategy initiates by defining WVD workloads and then mapping them to technical work. Skilled people in a proper organizational structure can execute this technical work and so, the skilled people are identified along with the assessment environment.

#### Define WVD Workloads

Basically, a collection of IT assets (servers, VMs, applications, data, or appliances) is a workload and these workloads can support more than one process. This section of the document will guide us in understanding the different WVD scenarios or options available and navigate us to Decision tree that help to come up with a Cloud Adoption plan.

**WVD Decision Tree**

**Host Pool Type**

**Compute Needs**

**Apps & Services**

**User Profile Storage**

**Auto Scale**

**Windows Virtual Desktop**

Pooled

Breadth first load balance

Depth first load balance

Light

Medium

Heavy

Heavy Graphics

File Server

Azure Files

Azure NetApp files

Full Session Desktop

User Access & Security

App Only

The components of the above decision tree are further described in detail as below:

**Host Pool Type**

WVD brings in a novel concept called Host pools. Host pools manage users, compute and applications collectively and lays to foundation of cost centers. Analysis of the telemetry data with the measures such as workstyle, common characteristics, groups of users; helps to classify the users and their needs into personas like Frontline workers, Core Engineers, Office Staff, Remote Workers etc. These personas also help to determine the security boundaries which aren’t visible generally. These personas determine requirements and realignment of these users to Host pools.

WVD, caters to the needs of these personas with its scalable offering to its desktop infrastructure namely:

* **Personal:** Dedicated 1:1 user to desktop environment where the needs of data isolation, security and computing are similar yet varied.
* **Pooled:** A truly scalable and cost optimized environment allowing multi session experience on Windows 10 for groups of users who have identical yet sparse computing needs.

**Compute Needs**

Once the Host pool sizing is ascertained, the next step is to determine the computing needs for each host pool. Nature of devices used, telemetry data of the system, resource usage of physical and virtual endpoint devices and comparative analysis of the data yield us to make more informed decision on the actual computing needs for WVD.

WVD make this decision process simple by aligning the computing needs for pooled and personal host pools as detailed below

* **Light**: For all general and office productivity computing needs, Ideal for frontline and information workers or users of web-based app and services.

For basic usage users you can select Light usage profile.

Ex: For 100 users with Standard D4s v3 it will create 5x session hosts (VM's)

* **Medium**: For power users, data analysts and decision makers whose usage of apps and services requires peak bursts of the CPU and memory needs multiple times a day.

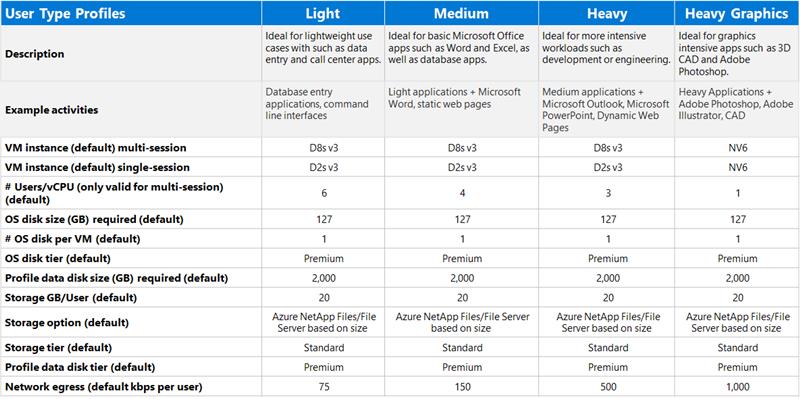
For Standard usage users you can select Medium usage profile.

Ex: For 100 users with Standard D4s v3 it will create 7x session hosts (VM's)

* **Heavy**: For Power user and advanced users who needs more dedicated computer or memory usage needs and they cannot be catered with bursts in peak use of CPU or memory

For heavely usage users you can select Heavy usage profile.

Ex: For 100 users with Standard D4s v3 it will create 13x session hosts (VM's)

* **Heavy Graphics**: For users who need specialized graphics card along with the peak usage of compute and memory. Especially for users in Game designing, Scientific modelling and visualization tools etc.

While the above categories are guidelines, with plethora of compute SKU’s available in Azure, the computing needs can be personalized for the right experience.

**Apps & Services Provisioning**

Enabling the right end user experience is depended on the app and services catered to the personas. The personas help us to ascertain the app usage, hardware and software load, usage patterns with help of the telemetry data. While these decisions help us to classify the app and services usage in to two broad end user experience.

* Full Session desktop
* App Only

WVD caters to both the experiences and aide to deliver the experience with help of Desktop and Remote App groups. App groups also provide the additional layer of security to enable access to a predefined set of published apps right from the start menu. Both experiences take advantage of the FSLogix app masking and containerized profiles with low latency. Based on the user needs and use case, App groups can be published within the host pool to cater a diverse set of users without the need of additional VM provisioning.

*User Access & Security*

User Identity, federation, data security and access to the resources on cloud are crucial decisions during the plan to WVD adaption. There are various factors that influence the decision and key metric such as the ability to extend and govern the existing Active Directory environment for WVD resources. The other factors include; how conditional access to remote resources are managed and how RDP sessions are established on the multi session environment.

* + WVD backed with Azure provides a safe and secure multi session desktop environment with Windows 10. WVD leverages reverse connect to securely enable remote access to the session hosts without the need of public IP’s or tunneling.
  + With Azure AD and ADFS federation portions, WVD provide a seamless single sign-on experience with added benefits of MFA and conditional access to all while extending the local AD users, groups and polices.

**User profile Storage Needs**

The continuous assessment of the physical and virtual endpoint devices also reveals vital characteristics of disk usage, usage of cloud storage, network bandwidth and other allied parameters which aid to make this decision better. WVD coupled with FSLogix employs containerized profiles and provides the best multi session experience for Windows 10.

The key decision drivers to define an ideal strategy of the user profile storage are

* Size of the user disk,
* Throughput of the IOPS
* Reliability of storage platform

WVD provides guidance here to make the right decision,

* **File Server:** The Local Shared network drives can be replaced with running a dedicated file server and choosing a right storage disk SKU’s. File server are flexible and adept to change based on the varying compute demands. With the use of Premium storage and GRS, file server can provide the same or better reliability of local fiber storage. File servers are limited to the IOPS and compute of the server configured.
* **Azure Files:** Azure Files is a PaaS based offering on top of azure storage layer allowing the user to eliminate the needs of the cost of managing the compute and operational overheads of file server. Azure Files are indeed ideal for the
* **Azure NetApp Files:** NetApp Files is also an additional PaaS storage offering for large data workloads or for desktop computing needs where the storage performance is critical for the user needs

**Auto scale**

Running desktop resources on cloud is indeed an expensive affair. While WVD provides the benefit of running multi session desktop experiences on a single VM, Operation costs are direct result of the compute, bandwidth usage of session hosts. With a consistent digital experience monitoring and leveraging the use of azure monitor on the multi session experience, usage patterns can help you tailor the WVD deployments.

* Auto scale is one of the important decisions to be made during WVD adaption as Auto scale helps to efficiently drive the WVD adaption during peak hours, non-peaks hours and period of burst usage.
* The scaling mechanism can be personalized to each of the host pool workloads to reduce the operation cost further.

### Skill Readiness

These are the following roles needed for successfully managing and deploying WVD environment:

* Azure Cloud Engineer
* Azure Solution Architect
* Network Engineer/System Engineer
* Azure Security Engineer

### Azure Environment Assessment

As part of the Azure environment assessment phase, we need to check for the following services to see if they already exist and can be utilized to deploy WVD. This section also describes what steps need to be taken for assessing 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 if 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 our environment assessment, we need to re-use any existing resources/services, and create other required services as detailed in further sections of this document. For example, if we already have a S2S VPN Tunnel or Express Route in place then we need to skip this part in the networking section.**

## Ready Phase

This is the phase where we need to define support needs, address current gaps and ensure that the business and IT employees are prepared for the planned changes. We need to prepare our cloud environment for any new technologies. To set up the floor, we will be discussing Landing zone and how to create tenant and build VM image.

### First Landing Zone

The principle purpose of the landing zone is to ensure that when an application lands on Azure, the required "plumbing" is already in place. To achieve this purpose, we follow the following setup process:

**Organize Azure Resources**

**Network Setup**

**Hybrid Network Setup**

**Domain Control Setup**

**Identity Setup**

#### Organize Azure Resources

Organizing your cloud-based resources is critical to securing, managing, and tracking the costs related to your workloads. Azure provides four levels of management scope: management groups, subscriptions, resource groups, and resources.

* **Create Management groups:** These groups are containers that help you manage access, policy, and compliance for multiple subscriptions. All subscriptions in a management group automatically inherit the conditions applied to the management group.
* **Create Subscription:** Start your Azure adoption by creating an initial set of subscriptions. A subscription logically associates user accounts and the resources that were created by those user accounts. Each subscription has limits or quotas on the amount of resources you can create and use. Organizations can use subscriptions to manage costs and the resources that are created by users, teams, or projects.
* **Create Resource groups:** A resource group is a logical container into which Azure resources like web apps, databases, and storage accounts are deployed and managed.

#### Network Setup

This section describes the different options to setup a network

**Virtual Network / Subnet**

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure.

VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but it brings with itself additional benefits of Azure's infrastructure such as scale, availability, and isolation. Remember, you do not configure DHCP in Azure virtual networks. IP addressing is dynamic based on the assigned subnet.

**Subnet**: Subnets enable you to segment the virtual network into one or more sub-networks and allocate a portion of the virtual network's address space to each subnet. You can then deploy Azure resources in a specific subnet. Just like in a traditional network, subnets allow you to segment your VNet address space into segments that are appropriate for the organization's internal network. This also improves address allocation efficiency. You can secure resources within subnets using Network Security Groups.

**Network Security Group:**

You can use Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.

For each rule, you can specify source and destination, port, and protocol.

Azure Bastion is a relatively new Azure service that can simplify as well as improve remote connectivity – as a secure better alternative for steppingstone servers to your Windows Virtual Desktop – and infrastructure Virtual Machines on Microsoft Azure. Azure Bastion is completely web-based and works via SSL. In some simple configuration clicks – and most importantly without exposing any RDP (or SSH) ports to the outside internet – you can access your

Windows Virtual Desktop Virtual Machines in Azure.

**Azure Firewalls**

When you deploy a new Pool, the VM’s in that pool will need access to some URLs and internal IP’s for the deployment to complete.

* First, the VM’s will be joined to your domain, which means they will need the standard ports open to the domain controllers and DNS servers.
* Secondly, an agent is deployed that allows the VM to login to AAD and with that login token, it registers themselves to the WVD service.
* That last part is done through “public” internet. In a “normal” deployment, the VM’s (and the users logging into the VM’s) would have full internet access. Even if you configure a proxy server, nothing stops a user from opening a command prompt or PowerShell and bypass the proxy.

Let us completely lock down internet access for the VM’s but allow them to deploy by using URL whitelisting on an Azure Firewall. The Azure Firewall is a standard service available in almost all regions.

It is a fully L3 firewall but also adds the possibility to whitelist based on URLs. To deploy it, you will need a separate subnet called **AzureFirewallSubnet** with at least a /26 address space.

#### Hybrid Network setup

This is an optional setup for organizations who wants to connect their on-premise network to Azure cloud. Here are the available options to connect to Azure cloud:

**Express Routes:**

* ExpressRoute gives you a fast and reliable connection to Azure with bandwidths up to 100 Gbps, which makes it excellent for scenarios like periodic data migration, replication for business continuity, disaster recovery and other high-availability strategies.
* It can be a cost-effective option for transferring large amounts of data, such as datasets for high-performance computing applications or moving large virtual machines between your dev-test environment in an Azure virtual private cloud and your on-premises production environments.
* Use ExpressRoute to both connect and add compute and storage capacity to your existing datacenters. With high throughput and fast latencies, Azure will feel like a natural extension to or between your datacenters, so you can enjoy the scale and economics of the public cloud without having to compromise on network performance.
* With predictable, reliable, and high-throughput connections offered by ExpressRoute, you can build applications that span on-premises infrastructure and Azure without compromising privacy or performance. For example, run a corporate intranet application in Azure that authenticates your customers with an on-premises Active Directory service and serve all of your corporate customers without traffic ever routing through the public Internet.

**Hub-n-spoke**

The hub is a virtual network in Azure that acts as a central point of connectivity to your on-premises network. The spokes are virtual networks that peer with the hub and can be used to isolate workloads. Traffic flows between the on-premises datacenter and the hub through an ExpressRoute or VPN gateway connection.

**Forced Tunneling**

Forced tunneling lets you redirect or "force" all Internet-bound traffic back to your on-premises location via a Site-to-Site VPN tunnel for inspection and auditing. This is a critical security requirement for most enterprise IT policies. Without forced tunneling, Internet-bound traffic from your VMs in Azure always traverses from Azure network infrastructure directly out to the Internet, without the option to allow you to inspect or audit the traffic. Unauthorized Internet access can potentially lead to information disclosure or other types of security breaches. Azure currently works with two deployment models: Resource Manager and classic. The two models are not completely compatible with each other. Before you begin, you need to know which model that you want to work in.

**Note:** For information about the deployment models, see Understanding deployment models. If you are new to Azure, we recommend that you use the Resource Manager deployment model.

#### Domain Controller setup

The Azure virtual machines you create for Windows Virtual Desktop must be:

* [Standard domain-joined](https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-comparison)
* [Hybrid AD-joined](https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-plan).

**Note**: Virtual machines can't be Azure AD-joined.

#### Identity Setup

**Active Directory configuration:**

Your infrastructure needs the following things to support Windows Virtual Desktop:

* An Azure Active Directory
* A Windows Server Active Directory in sync with Azure Active Directory. You can configure this with one of the following:
  + Azure AD Connect (for hybrid organizations)
  + Azure AD Domain Services (for hybrid or cloud organizations)
* An Azure subscription that contains a virtual network that either contains or is connected to the Windows Server Active Directory
* AAD Multifactor authentication
* AAD Conditional Access

**Azure MFA (Multi-Factor Authentication) for Windows Virtual Desktop**:

The Windows client for Windows Virtual Desktop is an excellent option for integrating Windows Virtual Desktop with your local machine. However, when you configure your Windows Virtual Desktop account into the Windows Client, there are certain measures you'll need to take to keep yourself and your users safe.

* When you first sign in, the client asks for your username, password, and Azure MFA. After that, the next time you sign in, the client will remember your token from your Azure Active Directory (AD) Enterprise Application.
* When you select Remember me, your users can sign in after restarting the client without needing to reenter their credentials. While remembering credentials is convenient, it can also make deployments on Enterprise scenarios or personal devices less secure.

To protect your users, you'll need to make sure the client keeps asking for Azure Multi-Factor Authentication (MFA) credentials. To enable Azure MFA for your users [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-mfa)

### Create a Tenant in Windows Virtual Desktop:

* Pre-Requisite to Tenant Setup. [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/virtual-desktop-fall-2019/tenant-setup-azure-active-directory#what-you-need-to-set-up-a-tenant)
* Grant permissions to Windows Virtual Desktop. [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/virtual-desktop-fall-2019/tenant-setup-azure-active-directory#grant-permissions-to-windows-virtual-desktop)
* Assign the TenantCreator application role. [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/virtual-desktop-fall-2019/tenant-setup-azure-active-directory#assign-the-tenantcreator-application-role)
* Create a service principal in Azure Active Directory (Optional step – Recommended). [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/virtual-desktop-fall-2019/create-service-principal-role-powershell#create-a-service-principal-in-azure-active-directory)
* Assign WVD Tenant Owner role to Azure Service Principal/Azure AD User

### Build VM Image

This section tells us how to create a custom image. In Azure, we create VM to install our business apps. With the help of custom image, we can create multiple session hosts. Below are some of the approaches to create custom images:

#### Azure Image Builder (AIB)

Azure Image Builder (AIB) allows you to take a source image, which can be any of the following:

* RHEL ISO
* Marketplace image
* Managed image
* Shared Image Gallery image version

It can then customize that specific image to your needs in an automated way.

And as a final step AIB can distribute your image to any or combination of the following:

* Managed image
* Shared Image Gallery
* VHD in a storage account

#### Prepare and customize a master VHD image

Install Language Packs: When you set up Windows Virtual Desktop deployments internationally, it's a good idea to make sure your deployment supports multiple languages. You can install language packs on a Windows 10 Enterprise multi-session virtual machine (VM) image to support as many languages as your organization needs. To install language pack [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/language-packs#install-a-language-pack)

Prepare a master virtual hard disk (VHD) image for upload to Azure, including how to create virtual machines (VMs) and install software on them. [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-customize-master-image)

#### Install Office on a master VHD image

Install Office 365 ProPlus, OneDrive, and other common applications on a master virtual hard disk (VHD) image for upload to Azure. If your users need to access certain line of business (LOB) applications, we recommend you install them.

Install Office in shared computer activation mode. Shared computer activation lets you to deploy Office 365 ProPlus to a computer in your organization that is accessed by multiple users. To configure install office on a master VHD image. [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/install-office-on-wvd-master-image)

## Adopt

### Host Pool Setup

Host pools are a collection of one or more identical virtual machines (VMs) within Windows Virtual Desktop environments. Each host pool can contain an app group that users can interact with, as they would on a physical desktop. A host pool can be one of two types:

* **Personal/Persistent**: Where each session host is assigned to individual users. You can configure the assignment type of your personal desktop host pool to adjust your Windows Virtual Desktop environment to better suit your needs. To configure assignment of automatic or direct [click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/configure-host-pool-personal-desktop-assignment-type)
  + **Configure automatic assignment**: Automatic assignment is the default assignment type for new personal desktop host pools created in your Windows Virtual Desktop environment. Automatically assigning users does not require a specific session host. To automatically assign users, first assign them to the personal desktop host pool so that they can see the desktop in their feed. When an assigned user launches the desktop in their feed, they will claim an available session host if they have not already connected to the host pool, which completes the assignment process.
  + **Configure direct assignment**: Unlike automatic assignment, when you use direct assignment, you must assign the user to both the personal desktop host pool and a specific session host before they can connect to their personal desktop. If the user is only assigned to a host pool without a session host assignment, they won't be able to access resources.
* **Pooled/Shared/Non-Persistent:** Where session hosts can accept connections from any user authorized to an app group within the host pool. Windows Virtual Desktop (WVD) offers two flavors of Load balancing known as Breadth-First and Depth-First in pooled Host Pools. We can set additional properties on the host pool to change its load-balancing behavior. How many sessions each session host can take, and what the user can do to session hosts in the host pool while signed in to their Windows Virtual Desktop sessions. We can control the resources published to users through app groups. To configure load balancing for a host pool [click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/configure-host-pool-load-balancing)
  + **Breadth-first load-balancing:** The breadth-first load-balancing mechanism is essentially a method which uses an algorithm to determine the least number of sessions on a session host for placement of new sessions. For example, a user connects to a Windows Virtual Desktop (WVD) Host pool which is Breadth-first configured. During the login process, a query is run against the available session hosts within the host pool. The load balancing method selects the session host with the least number of sessions. If there are two or more session hosts with the same number of sessions active, then the method selects the first session host identified in the query.
  + **Depth-first load-balancing:** The depth-first load-balancing method maximizes session utilization of a session host before loading sessions on to the next available session host. It is suggested that this algorithm is for organizations who want to operate an active/passive WVD Deployment or to reduce costs. The depth-first method queries the available session hosts to establish where to place new sessions. If a session host has exceeded the maximum session limit specified against the host pool, new sessions will be loaded on to the next available session host. Again, if there are two session hosts with the same number of sessions, then the first is selected in the query.

#### Host Pool Creation

Host Pool (either personal or pooled) can be created using source as Custom Image or Gallery or CustomVHD.

[Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/create-host-pools-azure-marketplace)

#### Customize RDP (Remote Desktop Protocol) properties for a host pool

Customizing a host pool's Remote Desktop Protocol (RDP) properties, such as multi-monitor experience and audio redirection, lets you deliver an optimal experience for your users based on their needs. To customize RDP properties for a host pool [click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/customize-rdp-properties)

#### App groups

In the host pool, an app group is a logical grouping of applications installed on session hosts. An app group can be one of two types:

**RemoteApp**: where users access the RemoteApps, we individually select and publish to the app group

**Desktop**: where users access the full desktop

By default, a desktop app group (named "Desktop Application Group") is automatically created whenever you create a host pool. You can remove this app group at any time. However, you can't create another desktop app group in the host pool while a desktop app group exists. To publish RemoteApps, you must create a RemoteApp app group. You can create multiple RemoteApp app groups to accommodate different worker scenarios. Different RemoteApp app groups can also contain overlapping RemoteApps.

To publish resources to users, you must assign them to app groups. When assigning users to app groups, consider the following things:

* A user can be assigned to both a desktop app group and a RemoteApp app group in the same host pool. However, users can only launch one type of app group per session. Users cannot launch both types of app groups at the same time in a single session.
* A user can be assigned to multiple app groups within the same host pool, and their feed will be an accumulation of both app groups.

**Feed customization for WVD users:** You can customize the feed, so the RemoteApp and remote desktop resources appear in a recognizable way for your users. To customize feed for WVD users [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/customize-feed-for-virtual-desktop-users)

**MSIX App Attach for WVD users:** Microsoft provides MSIX app attach for Windows Virtual desktop. MSIX app attach gives you the possibility to only have a few images and connect your application to them - without installing. That sounds a little bit like App-V, and from a user perspective, this is slightly comparable.

When MSIX is launched, the application files are accessed from a virtual hard disk (VHD) and the user is not even aware that the application is remote because the app functions like any local application. You cannot see the application in the file system from outside the app. If you open the app and if you browse to the application folder, you can see this folder. The attaching and links in the start menu “feels” like the use of modern apps from the marketplace. And indeed, the application links in the start menu did not refer to the exe-files in the program folder. [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/app-attach)

#### User Profile Container Configuration

While setting up host pool, the Windows Virtual Desktop service offers FSLogix profile containers as the recommended user profile solution. We don't recommend using the User Profile Disk (UPD) solution, which will be deprecated in future versions of Windows Virtual Desktop.

To setup a FSLogix profile container for host pool, we use below 3 approaches:

* **Use a VM-based file share** - You create the virtual machine, be sure to place it on either the same virtual network as the host pool virtual machines or on a virtual network that has connectivity to the host pool virtual machines. To configure VM-based file share [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/create-host-pools-user-profile)
* **Use Azure NetApp Files** - Windows Virtual Desktop team recommend using FSLogix profile containers as a user profile solution for the Windows Virtual Desktop service. FSLogix profile containers store a complete user profile in a single container and are designed to roam profiles in non-persistent remote computing environments like Windows Virtual Desktop. To configure Azure NetApp file share [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/create-fslogix-profile-container)
* **Use Azure files and Azure AD DS** - Create an FSLogix profile container with Azure Files and Azure Active Directory Domain Services (AD DS). To configure Azure file share [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/create-profile-container-adds)

### Innovate - 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 - 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 - 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 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 – As networking plays a crucial role in any cloud service, designing it to satisfy all the requirements is important.
* Identity and Access Management - WVD service in Azure requires authentication and Session host domain join using Windows Active Directory (AD), either from the on-premise environment or Azure AD Domain Services (AAD-DS).
* 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 - 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) - 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 is a service that gives users easy and secure access to their virtualized desktops and RemoteApps. This section describes the WVD Environment.
* WVD Deployment – This section describes the steps required to deploy the WVD service.
* FSLogix Setup and Configuration for WVD User Profiles - FSLogix is a set of solutions that enhance, enable, and simplify non-persistent Windows computing environments. FSLogix solutions are appropriate for Virtual environments in both public and private clouds. As part of WVD, we will utilize the FSLogix Profile Containers to manage User profile data.
* Application and Desktop Management – Manage publishing applications and desktops in WVD.
* WVD Management and Monitoring - Management of WVD plays a crucial role in how the users interact with the service. You can grant/revoke access to published applications or desktops through Management, debug any issues that users come across when they access the service.
* 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 - Customers can implement BCDR for their Session hosts using ASR. This would protect the VMs and provide faster recovery from disasters.

#### WVD Reference Architecture – ADDS

**Shared**

Pooled Host Pool

Desktop Application Group

Remote Application Group

Remote Apps

User Members

Personal Host Pool

**Dedicated**

**Dedicated**

Desktop Application Group

Desktops

Desktops

User Members

WVD Host Pool Setup

WVD Tenant

User Members

Windows Virtual Desktop Management Service

Laptop

Smart Phone

Work Stations

Conditional Access

Multi Factor Authentication

Azure

Azure Subscription

**File Services**

**Session Host Management**

**Active Directory Domain Services**

Azure File Share



File Server

Mapped

AD Domain Join

Personal Desktops

Pooled Desktops

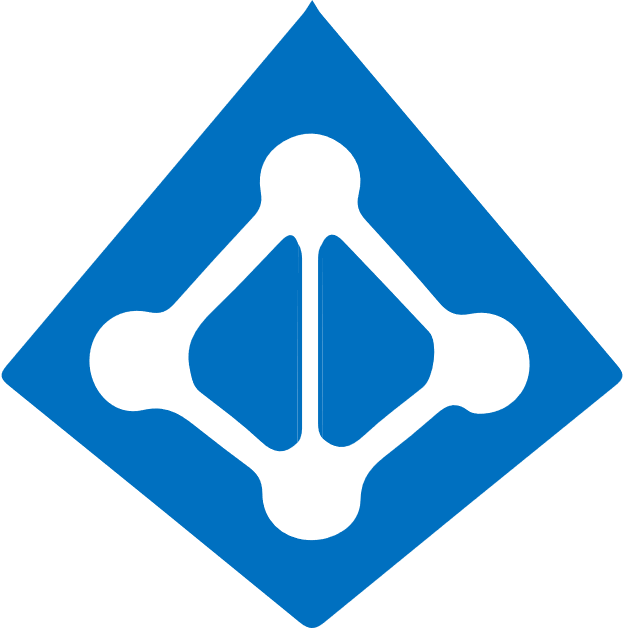
Customer managed ADDS on Domain controller VM

**or**

**or**

managed Azure

AD DS (AAD DS)



Users

WVD Agent reverse connect

WVD Agent reverse connect

**WVD Architecture**

#### WVD Reference Architecture – On-Premise AD Connect

Laptop

Smart Phone

Work Stations

**Shared**

Pooled Host Pool

Desktop Application Group

Remote Application Group

Remote Apps

User Members

Personal Host Pool

**Dedicated**

**Dedicated**

Desktop Application Group

Desktops

Desktops

User Members

WVD Host Pool Setup

WVD Tenant

User Members

Windows Virtual Desktop Management Service

Conditional Access

Multi Factor Authentication

Azure

Azure Subscription

**Session Host Management**

**File Service**

Azure File Share



File Server

Mapped

Personal Desktops

Pooled Desktops

**or**



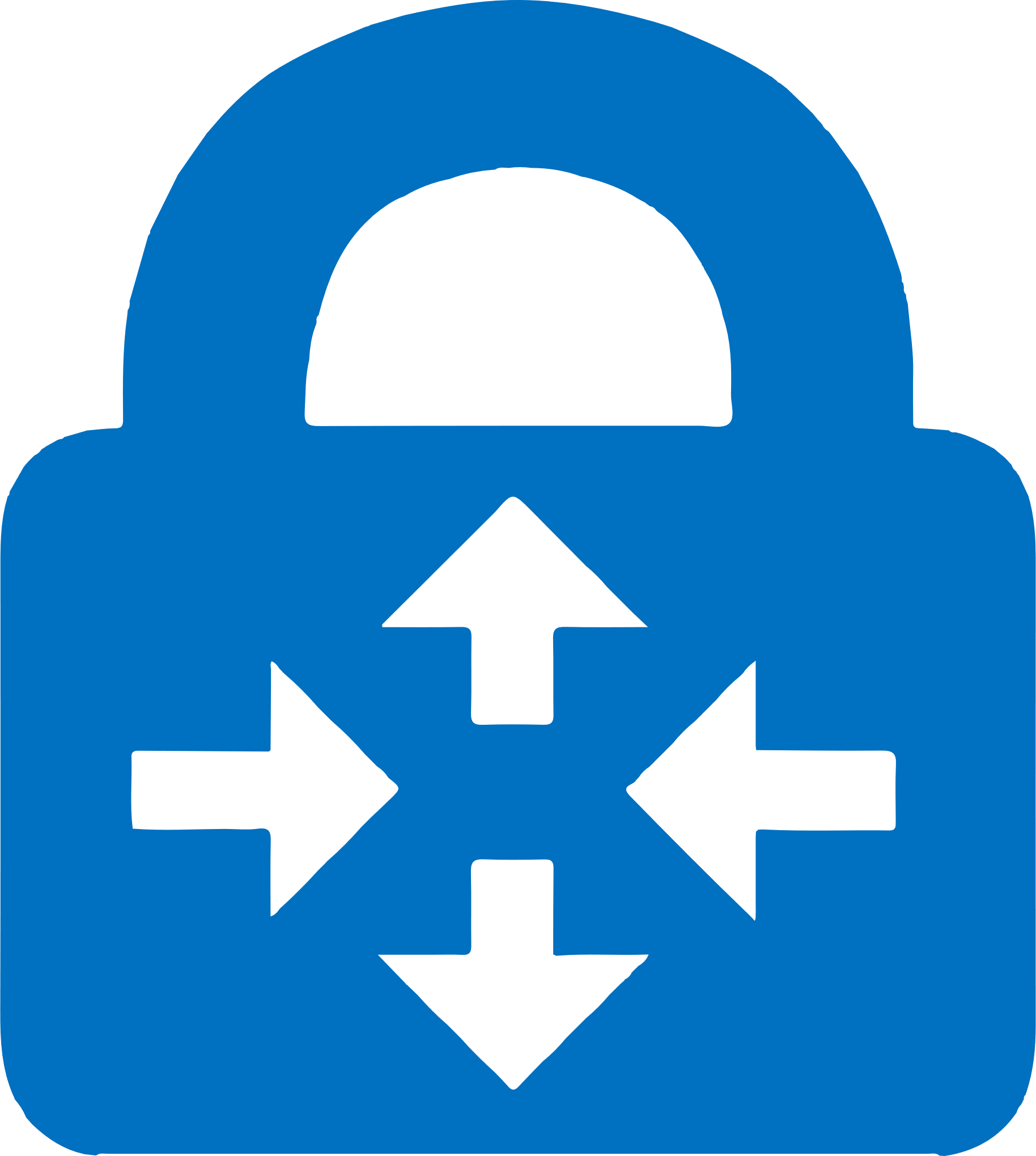
Users

WVD Agent reverse connect

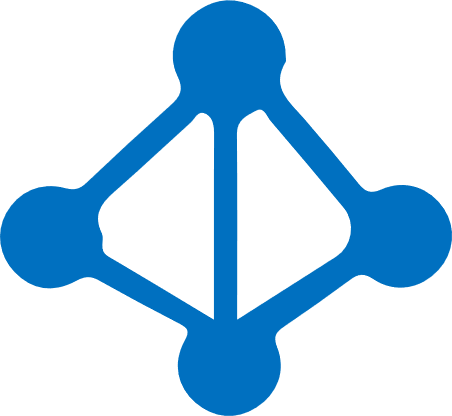
WVD Agent reverse connect

**WVD Architecture**

Virtual Network



Virtual Gateway

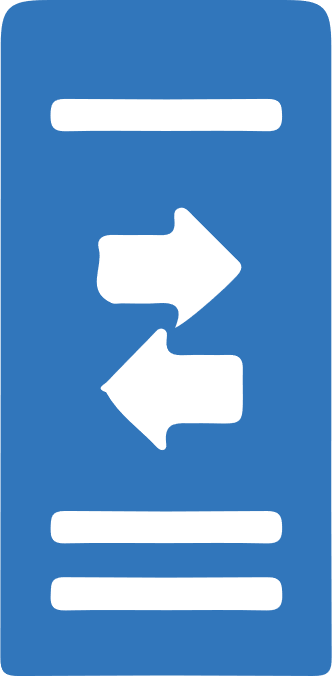


Azure Active Directive

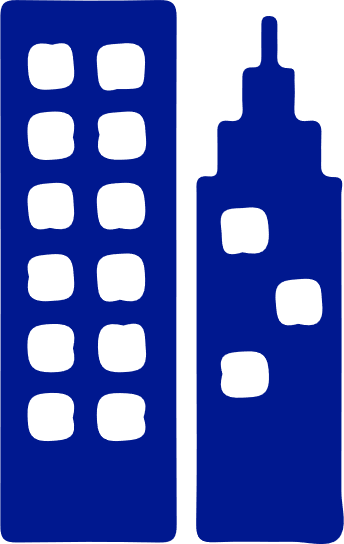
NSG

Azure Bastion

Azure Bastion Subnet



Azure AD Connect



Gateway

### Migrate – RDS workload to WVD

Whether it is migrating Remote Desktop Services (RDS) or Virtual Desktop Infrastructure (VDI) environments to Windows Virtual Desktop, Azure enables to migrate existing virtual desktop workloads to Microsoft Azure as part of Windows Virtual Desktop even if you are working with a greenfield scenario (i.e. building a new environment from the ground up) or a brownfield scenario (i.e. transforming existing RDS resources and Windows 10 single-session virtual machines). These migration processes are described below in this section.

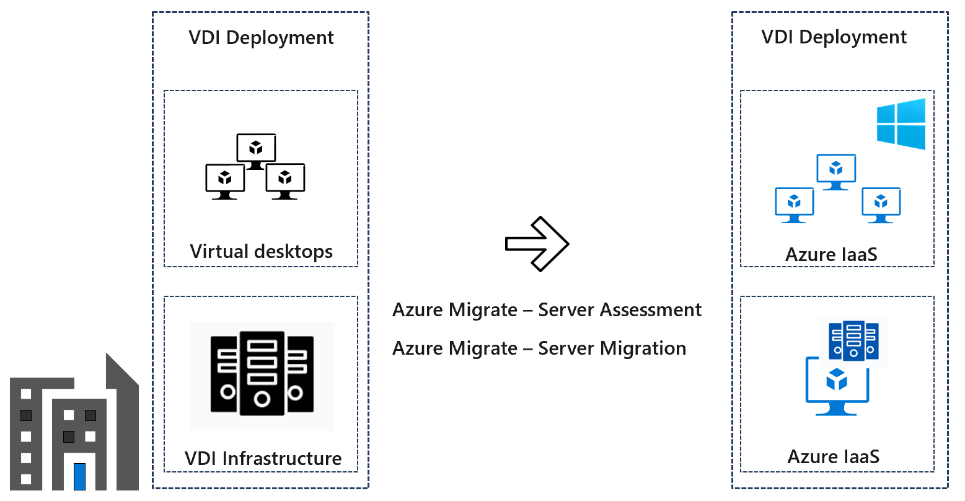
**Azure Migrate**

Azure Migrate is a free Azure service that helps you leverage Azure Infrastructure-as-a-service (IaaS) most efficiently.

It offers:

* Assessments for readiness, sizing, and cost estimation
* Migration with near-zero downtime
* An Integrated experience with end-to-end progress tracking
* Your choice of tools with ISV integration (Lakeside - SysTrack)

**Azure Migrate: Server Migration**

Server Migration uses a management server that remains a replication server in your on-premises, physical, or AWS/Google Cloud environment. The management server replicates the specific drives of the virtual machines to your Azure storage blob account. After you start the migration process, virtual machines in your Azure IaaS environment will be created. Click on hyperlinks for information on how to start with Azure Migrate for [VMware](https://docs.microsoft.com/en-us/azure/site-recovery/vmware-physical-large-deployment), [Physical](https://docs.microsoft.com/en-us/azure/site-recovery/vmware-physical-large-deployment) and [Hyper-V](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-manage-network-interfaces-on-premises-to-azure) on-premises workloads.

#### Migration Process

The standard process of migration is explained below:

* **Migration to Personal/Pooled Desktops**

Following are the important steps you need to take to ensure a successful migration to personal and pooled desktops in Windows Virtual Desktop:

* User identity
  + Sync user identities and password hash from on-premises Active Directory (AD) to Azure AD.
  + Set up an AD instance on Azure or continue using on-premises AD via VPN or ExpressRoute.
  + (Alternative) Set up Azure Active Directory Domain Services (Azure AD Domain Services).
* Virtual Machines
  + Lift and shift virtual machines from your on-premises environments with [Azure Migrate: Server Migration.](https://azure.microsoft.com/en-us/blog/introducing-the-new-azure-migrate-a-hub-for-your-migration-needs/" \t "_blank)
  + Bring your on-premises Windows Server or Desktop images and create new virtual machines on Azure.
  + Register your new virtual machines with the Windows Virtual Desktop brokering service.
* Networking
  + Configure your [Azure Virtual Network (VNet)](https://docs.microsoft.com/azure/virtual-network/virtual-networks-overview) and subnets.
* User and application data
  + Since UPDs are not supported on Windows Virtual Desktop, convert your UPD profiles into FSLogix Profile Containers.
  + Prepare your [Azure Files](https://techcommunity.microsoft.com/t5/Windows-IT-Pro-Blog/Getting-started-with-FSLogix-profile-containers-on-Azure-Files/ba-p/746477) or [Azure NetApp file](https://docs.microsoft.com/azure/virtual-desktop/create-fslogix-profile-container) shares to [store your profiles](https://docs.microsoft.com/azure/virtual-desktop/store-fslogix-profile).
* Client (end user) endpoint capabilities
  + Download and install the WVD Windows or MacOS client or use the HTML5 web client or use the mobile RD clients available through Google Play or Apple App Store. (Did you know that the [RD Client iOS](https://apps.apple.com/us/app/microsoft-remote-desktop/id714464092) app for Apple is now available?)
* **Migrate existing user profiles to FSLogix Profile Containers**

To provide a good migration path between your existing profile solution and Profile Container, we have created a migration script that is currently available as a Private Preview. To gain access to the Private Preview, complete this [registration form](https://forms.office.com/Pages/ResponsePage.aspx?id=v4j5cvGGr0GRqy180BHbR3HZFwpyCxVCngXplJaL78tUOUE0NEtBM0NDTU5DTTY0Qzg0NkRHWE85Si4u).

The migration script will allow you to perform mass conversions of user profiles from various (specified) types to FSLogix based Profile Containers at scale. Here are some details about the tool code base and structure of the code with the commands to be executed, as well as detailed examples.

* **Make existing RDS or VDI hosts available for Windows Virtual Desktop**

Use existing images as base image for the Azure Marketplace host pool enrolment process.

Now your image is being used as base for all your virtual machines as part of your Windows Virtual Desktop host pool! You can start [assigning desktops or remote apps](https://docs.microsoft.com/azure/virtual-desktop/create-host-pools-azure-marketplace#optional-assign-additional-users-to-the-desktop-application-group) to users, or performing other tasks.

* **Resize a Virtual Machine**

Virtual machines created or migrated using other methods, or in cases where your post-migration virtual machine requirements need adjustment, you may want to further refine your virtual machine sizing.

Resizing production virtual machines can cause service disruptions. Try to apply the correct sizing for your VMs before you promote them to production.

#### Application migration patterns

**Migration patterns**

Strategies for migration to the cloud fall into four broad patterns: rehost, refactor, rearchitect, or rebuild. The strategy you adopt depends on your business drivers and migration goals. You might adopt multiple patterns. For example, you could choose to rehost simple apps, or apps that aren't critical to your business, but rearchitect apps that are more complex and business-critical.

| **Pattern** | **Definition** | **When to use** |
| --- | --- | --- |
| **Rehost** | Often referred to as a lift and shift migration. This option doesn't require code changes, and allows you to migrate your existing apps to Azure quickly. Each app is migrated as is, to reap the benefits of the cloud, without the risk and cost associated with code changes. | * When you need to move apps quickly to the cloud. * When you want to move an app without modifying it. * When your apps are designed so that they can take advantage of [Azure IaaS](https://azure.microsoft.com/overview/what-is-iaas) scalability after migration. * When apps are important to your business, but you don't need immediate changes to app capabilities. |
| **Refactor** | Often referred to as "repackaging," refactoring requires minimal changes to apps, so that they can connect to [Azure PaaS](https://azure.microsoft.com/overview/what-is-paas), and use cloud offerings.  For example, you could migrate existing apps to Azure App Service or Azure Kubernetes Service (AKS).  Alternatively, you could refactor relational and nonrelational databases into options such as Azure SQL Database Managed Instance, Azure Database for MySQL, Azure Database for PostgreSQL, and Azure Cosmos DB. | * If your app can easily be repackaged to work in Azure. * If you want to apply innovative DevOps practices provided by Azure, or you're thinking about DevOps using a container strategy for workloads. * For refactoring, you need to think about the portability of your existing code base, and available development skills. |
| **Rearchitect** | Rearchitecting for migration focuses on modifying and extending app functionality and the code base to optimize the app architecture for cloud scalability.  For example, you could break down a monolithic application into a group of microservices that work together and scale easily.  Or, you could rearchitect relational and nonrelational databases to a fully managed database solution, such as Azure SQL Database Managed Instance, Azure Database for MySQL, Azure Database for PostgreSQL, and Azure Cosmos DB. | * When your apps need major revisions to incorporate new capabilities, or to work effectively on a cloud platform. * When you want to use existing application investments, meet scalability requirements, apply innovative DevOps practices, and minimize use of virtual machines. |
| **Rebuild** | Rebuild takes things a step further by rebuilding an app from scratch using Azure cloud technologies.  For example, you could build green-field apps with [cloud-native](https://azure.microsoft.com/overview/cloudnative) technologies like Azure Functions, Azure AI, Azure SQL Database Managed Instance, and Azure Cosmos DB. | When you want rapid development, and existing apps have limited functionality and lifespan.  When you're ready to expedite business innovation (including DevOps practices provided by Azure), build new applications using cloud-native technologies, and take advantage of advancements in AI, Blockchain, and IoT. |

#### Best practices for cloud migration

**Business driven scope expansion**

* Support global markets: The business operates in multiple geographic regions with disparate data sovereignty requirements. To meet those requirements, additional considerations should be factored into the prerequisite review and distribution of assets during migration.

**Technology driven scope expansion**

* *VMware migration*: Migrating VMware hosts can accelerate the overall migration process. Each migrated VMware host can move multiple workloads to the cloud using a lift and shift approach. After migration, those VMs and workloads can stay in VMware or be migrated to modern cloud capabilities.
* *SQL Server migration*: Migrating SQL Servers can accelerate the overall migration process. Each SQL Server migrated can move multiple databases and services, potentially accelerating multiple workloads.
* *Multiple datacenters*: Migrating multiple datacenters adds significant complexity. During the Assess, Migrate, Optimization, and Manage processes, additional considerations are discussed to prepare for more complex environments.
* *Data requirements exceed network capacity*: Companies frequently choose to migrate to the cloud because the capacity, speed, or stability of an existing datacenter is no longer satisfactory. Unfortunately, those same constraints add complexity to the migration process, requiring additional planning during the assessment and migration processes.
* *Governance or compliance strategy*: When governance and compliance are vital to the success of a migration, additional alignment between IT governance teams and the cloud adoption team is required.

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 - 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 - 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 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 – As networking plays a crucial role in any cloud service, designing it to satisfy all the requirements is important.
* Identity and Access Management - WVD service in Azure requires authentication and Session host domain join using Windows Active Directory (AD), either from the on-premise environment or Azure AD Domain Services (AAD-DS).
* 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 - 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) - 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 is a service that gives users easy and secure access to their virtualized desktops and RemoteApps. This section describes the WVD Environment.
* WVD Deployment – This section describes the steps required to deploy the WVD service.
* 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.
* Convert and Migrate User Profiles – Customers running an existing RDS/VDI Infrastructure and migrating to WVD may also want to move their User’s profile data to WVD.
* FSLogix Setup and Configuration for WVD User Profiles - FSLogix is a set of solutions that enhance, enable, and simplify non-persistent Windows computing environments. FSLogix solutions are appropriate for Virtual environments in both public and private clouds. As part of WVD, we will utilize the FSLogix Profile Containers to manage User profile data.
* Application and Desktop Management – Manage publishing applications and desktops in WVD.
* WVD Management and Monitoring - Management of WVD plays a crucial role in how the users interact with the service. You can grant/revoke access to published applications or desktops through Management, debug any issues that users come across when they access the service.
* 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 - Customers can implement BCDR for their Session hosts using ASR. This would protect the VMs and provide faster recovery from disasters.

## Governance

Governance creates guardrails that keep the company on a safe path throughout the journey. Governance guides that describe the experiences of fictional companies that are based on the experiences of real customers. Governance is an iterative process. For organizations with existing policies that govern on-premises IT environments, governance should complement those policies. The level of corporate policy integration between on-premises and the cloud varies depending on governance maturity and a digital estate in the cloud.

* **Govern - Cost Management** 
  + **Cost and Budget Management**: Azure Cost Management alerts to monitor your Azure usage and spending Or Dashboard configuration
  + **Risk**: Cost overrun alerts
* **Govern - Identity Baseline**
  + **Hybrid Identity**
  + azure ad connects
  + Password policy (Passthrough, password hash, Federation)
  + SAS (azure shared access signature)
  + **Identity requirements**
  + Conditional access policy (MFA, failed login)
  + Configure MFA
  + Creation of authentication and authorization Policy (application identity, Shared credentials, RBAC, MS365 App Security
  + **Identity requirements**
  + Azure Directory Service if needed
* **Govern - Security Baseline**
  + **Compliance and risk**
  + Compliance manager configuration, reporting, risk mitigation
  + Policy and Industry Standard controls configuration
  + Security Assessment - Secure score configuration
  + **Data encryption**
  + data at rest encryption is performed on the Azure platform
  + **Data Security - Encryption**
  + Azure Key Vault - Configure Bring your own keys configuration per policy (BYOK)
  + Azure Key Vault - Configure HSM per company standard and policy
  + Azure Key Vault - Configure Key rotation policy
  + Azure Key Vault - configure internal/External CA per company standard and policy
  + Azure Key Vault - Key management policies
  + Configuring customer-managed encryption keys for Azure Storage – Always encrypted
  + Data at rest - Configure Encrypting - VM Disks (Windows and Linux VMs Bit locker/DM Crypt
  + Data at rest - Configure Encrypting -Azure storage encryption
  + Data at rest - Configure Encrypting SQL DB - TDE
  + Data at rest - Configure Encrypting SQL DB -SQL Always Encrypted
  + Encrypting data in use - Azure Confidential computing for multi-tenant scenario
  + Encryption data in transit - Azure App Service - https://. azurewebsites.net - Custom domains and certificates
  + Encryption data in transit - Azure portal uses HTTPS
  + Encryption data in transit - Azure Storage REST endpoints - HTTPS is optional - SAS can enforce HTTPS
  + Encryption data in transit - Encryption of all public endpoints - VPN, Express routes encryption
  + Security center alerts configuration
  + Security documents and emails – Azure information Protection (labeling and classification)
  + **DDoS protection**
  + Use Azure DDoS Protection Standard to minimize disruptions caused by DDoS attacks.
  + **Deployment Acceleration**
  + all assets deployed to the cloud should be deployed using templates or automation scripts, where possible
  + Azure Blueprints
  + Azure DevOps Pipelines
  + **Hybrid Network security/Identity**
  + Redirect cloud authentication through on-premise firewall (if Azure AD connect environment is in place) i.e. Route and NSG configurations
  + **Infrastructure Security**
  + Develop an Azure Blueprint
  + Naming conventions and tags
  + Role-based access control model
  + Set up security and monitoring
  + **Monitoring alert, Audit/diagnostic Logs and alerting**
  + Azure Security Centre - Security Policy configuration
  + **Network Security**
  + Application Gateway
  + Creating user defined routes (UDR)
  + DDoS configuration for internet endpoints
  + Network access controls with NSGs and Azure Firewall
  + Network monitoring and threat detection
  + Policy templates for networking
  + The hub spoke model
  + **Network security - Internet connectivity Paths**
  + Autoscaling
  + Publish - IIS web servers, App Services, Azure Kubernetes Service clusters
  + Route based on host headers, URI path
  + SSL termination
  + Static virtual IP address
  + Web Application Firewall
  + Web traffic load balancer
  + **Network Security - Software defined networking models**
  + Cloud DMZ -DMZ traffic is audited
  + Cloud DMZ -Not using a dedicated WAN connection
  + Cloud Native - Using cloud-based identity
  + Hybrid - Access to services from cloud to on-prem - Application Proxy
  + Hybrid - Access to services in cloud from on-prem
  + Infrastructure as a Service resources - NSGs, Monitoring agent, encryption configuration
  + **Resource Consistency**
  + Develop resource template - ARM
  + Discoverable to IT operations - Tag, alerts based on tags for non-compliant resource
  + Included in recovery planning
  + Part of repeatable operations processes
* **Govern - Security Baseline** 
  + **Identity**
  + Ensure admin accounts are not licensed
  + Ensure all admin accounts are enabled for multi-factor authentication (MFA)
  + Ensure no service accounts are assigned admin role in the tenant
  + Ensure on-premise synchronized accounts are not assigned admin roles in the Tenant
  + Implement a process for disabling and deleting accounts that are no longer used
  + Implement Azure Active Directory (Azure AD) Privileged Identity Management
  + Implement privileged access management in Office 365
  + Reduce the number of global administrator accounts to less than five
  + Require multi-factor authentication for all users
  + Review and optimize your conditional access and related policies to align with your objectives for a zero-trust network.
  + Setup multi-factor authentication and use recommended conditional access policies, including sign-in risk policies
  + **Identity**
  + Implement Privileged Access Workstations (PAW)
  + **Information protection**
  + Configure data loss prevention policies for sensitive data
  + Disable Anonymous external calendar sharing policy
  + Disable external email forwarding
  + Implement data classification and information protection policies
  + Protect data in third-party apps and services by using Cloud App Security
  + Use AIP Scanner to identify and classify information across servers and file shares
  + Use Microsoft Defender ATP to identify if users store sensitive information on their desktops
  + **Monitoring**
  + Ensure the Office 365 audit log is turned on
  + Review risky logins weekly
  + Review Secure Score weekly
  + Review Top malware, spam users weekly
  + Use Microsoft Azure Sentinel or your current SIEM tool to monitor for threats across your environment.
  + Use Microsoft Cloud App Security to detect unusual behavior across cloud apps
  + Use Microsoft Defender ATP
  + Use Office 365 ATP tools
  + Use the Azure Security Center to monitor for threats across hybrid and cloud workloads.
  + **Threat protection**
  + Block connections from countries that you don't do business with
  + Disable POP, IMAP, and SMTP protocols
  + Protect against ransomware
  + Protect your email from targeted phishing attacks
  + Raise the level of protection against malware in mail
  + Retire servers and applications that are no longer used in your environment
  + **Threat protection**
  + Block access to the Microsoft Azure Management portal to all non-administrators
  + Configure Defender Advanced Threat Protection capabilities
  + Configure Office 365 Advanced Threat Protection (Office ATP)
  + Deploy Azure ATP to monitor and protect against threats targeted to your on-premises Active Directory environment.
  + Disable Remote PowerShell for all users
  + Do not whitelist sender domains, individual senders, or source IPs as this allows these to bypass spam and malware checks
  + Enable Outbound spam notifications
  + Open Teams Federation only to Partners you communicate with
  + Secure partner channel communications like emails using TLS
  + Use Microsoft Cloud App Security to discover and monitor SaaS apps
* **Governance – Resource Consistency**
  + **Asset classification**
  + Establish resource tagging standards and ensure IT staff apply them consistently to any deployed resources using Azure resource tags.
  + **Service discoverability and shadow IT**
  + Configure policy for resource tagging
  + **Service disturbance**
  + Microsoft Cloud services audit report and service alert configuration

### Security Baseline

**Networking**

This section contains 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.).

**Communications in general for WVD service (443) detailed flow – Reverse Connect**

One of the core differences between traditional Remote Desktop Services and Windows Virtual Desktop is the way clients connect to (RD/WVD) resources. Microsoft have introduced a new mechanism within Windows Virtual Desktop called Reverse Connect.

* Clients would typically connect to a RD Gateway for external access to RDS resources.
* The RD client would connect to the RD gateway over TCP 443, authenticate with Active Directory, and then the Gateway would establish a secure inbound session to the selected/chosen resource (RemoteApp/Desktop).
* In more recent versions of windows, the RDS Gateway can also use the UDP port 3391 (when configured) to enable dual transport for improved connection quality compared to the traditional TCP method.
* UDP provides significant improvements over higher latency/unreliable networks. There is no requirement for any inbound ports to be configured or opened on a VM to setup an RDP connection on WVD. This is essentially a reverse proxy security feature straight out of the box.
* Communication between the host pools and WVD core SaaS components is completed done using TCP https (443) only (at time of writing). That being said, for those using third party firewall’s/security appliances, you may need to double check rules allowing access to Azure services.

Reverse connect also provides new benefits like setting policies including conditional access policies. For example, Client time of day restrictions via IP address, controlling access via the Client IP address, time and/or other.

**Azure Bastion**:

Azure Bastion is a fully managed PaaS service that provides secure and seamless RDP and SSH access to your virtual machines directly through the Azure Portal. Azure Bastion is provisioned directly in your Virtual Network (VNet) and supports all VMs in your Virtual Network (VNet) using SSL without any exposure through public IP addresses.

Using a bastion host can help limit threats such as port scanning and other types of malware targeting your VMs. Azure Bastion provides an integrated platform alternative to manually deploying and managing jump servers to shield your virtual machines.

**Security and Compliance**

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
* Azure has the broadest [compliance coverage](https://aka.ms/AzureCompliance) in the industry, including key independent certifications and attestations such as ISO 27001, ISO 27017, ISO 27018, ISO 22301, ISO 9001, ISO 20000-1, SOC 1/2/3, PCI DSS Level 1, HITRUST, CSA STAR Certification, CSA STAR Attestation, US FedRAMP High, Australia IRAP, Germany C5, Japan CS Mark Gold, Singapore MTCS Level 3, Spain ENS High, UK G-Cloud and Cyber Essentials Plus, and many more.
* **Microsoft Intelligent Security Graph**: Microsoft Intelligent Security Graph uses advanced analytics to synthesize massive amounts of threat intelligence and security signals obtained across Microsoft products, services, and partners to combat cyberthreats. Millions of unique threat indicators across the most diverse set of sources are generated every day by Microsoft and its partners and shared across Microsoft products and services.
* **Azure Policy**: It enables effective governance of Azure resources by creating, assigning. and managing policies. These policies enforce various rules over provisioned Azure resources to keep them compliant with specific customer corporate security and privacy standards. For example, one of the built-in policies for Allowed Locations can be used to restrict available locations for new resources to enforce customer’s geo-compliance requirements. Azure Policy provides a comprehensive compliance view of all provisioned resources and enables cloud policy management and security at scale.
* **Microsoft Azure blueprint for Zero Trust**: Many of Microsoft customers in regulated industries are adopting a Zero Trust architecture, moving to a security model that more effectively adapts to the complexity of the modern environment, embraces the mobile workforce, and protects people, devices, applications, and data wherever they’re located. A Zero Trust approach should extend throughout the entire digital estate and serve as an integrated security philosophy and end-to-end strategy, across three primary principles: (1) verify explicitly, (2) enforce least privilege access, and (3) assume breach.

**Business Continuity and Disaster Recovery**

Customers can implement BCDR for their Session hosts using ASR. This would protect the VMs and provide faster recovery from disasters.

### Identity and Access Management

Each partner (or customer) will take some time 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

**Common customer concerns, including**:

* Data residency and data sovereignty: Microsoft provides strong customer commitments regarding cloud services data residency and transfer policies
* Government access to customer data, including CLOUD Act related questions
* Data encryption, including customer control of encryption keys
* Access to customer data by Microsoft personnel
* Threat detection and prevention
* Private and hybrid cloud options
* Cloud compliance and certifications
* Conceptual architecture for classified workloads

**Windows Virtual Desktop RBAC:**

Windows Virtual Desktop has a delegated access model that lets you define the amount of access a particular user is allowed to have by assigning them a role. A role assignment has three components: security principal, role definition, and scope. The Windows Virtual Desktop delegated access model is based on the Azure RBAC model.

Windows Virtual Desktop delegated access supports the following values for each element of the role assignment:

* Security principal
* Users
* User groups
* Service principals
* Role definition
* Built-in roles
* Custom roles
* Scope
* Host pools
* App groups
* Workspaces

**Built-in roles**: Delegated access in Windows Virtual Desktop has several built-in role definitions you can assign to users and service principals.

* An RDS Owner can manage everything, including access to resources.
* An RDS Contributor can manage everything but cannot access resources.
* An RDS Reader can view everything but cannot make any changes.
* An RDS Operator can view diagnostic activities.

### Cost Management

**Azure Pricing Calculator**

Pay only for the virtual machines (VMs), storage, and networking consumed when your users are using the service

You have the flexibility to pick any VM and storage options to match your use cases.

Take advantage of options such as [one-year or three-year Azure Reserved Virtual Machine Instances](https://azure.microsoft.com/en-us/pricing/reserved-vm-instances/), which can save you up to 72 percent versus pay-as-you-go pricing. Reserved Virtual Machine Instances are flexible and can easily be exchanged or returned.

**WVD Solution Configurator - Simple**

This tool breaks down WVD requirements into a series of questions about users and user requirements and includes a short how-to guide. You can also watch Windows Virtual Desktop – Customer Targeting for an overview of the tool and various input fields. The output of this tool is estimated Azure Infrastructure costs. Microsoft recommends using this tool for WVD cost estimations.

**WVD Solution Configurator - Comprehensive**

The Comprehensive version of the WVD Solution Configurator allows you to incorporate licensing and management costs into your calculation for a more comprehensive estimate of total WVD costs

## Manage

Managing the ongoing operation of the digital assets that deliver business outcomes is a key to this process. Unless, we have a plan to manage the operations, the efforts put in planning, readiness and adoption will yield little value. The following details will help develop the business approach to provide cloud management.

### WVD Management and Monitoring

**Install WVD PowerShell Module:**

Windows virtual desktop cmdlets for Windows PowerShell: Here you will find the resources for PowerShell modules targeting Windows Virtual Desktop. [Click here](https://docs.microsoft.com/en-us/powershell/windows-virtual-desktop/overview)

PowerShell cmdlets for managing and interacting with Windows Virtual Desktop [Click here](https://docs.microsoft.com/en-us/powershell/module/windowsvirtualdesktop/)

**Deploy WVD Management UI:**

You can manage WVD with Management tool GUI. Deploy the management tool in your environment. To deploy management tool, follow any one of the below approaches.

* Azure Resource Manager Template. [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/virtual-desktop-fall-2019/manage-resources-using-ui)
* PowerShell. [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/virtual-desktop-fall-2019/manage-resources-using-ui-powershell)

**Deploy WVD Diagnostic Tool**:

You can manage diagnostic activities of users. To deploy diagnostic tool [click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/virtual-desktop-fall-2019/deploy-diagnostics). Here is what the diagnostics tool for Windows Virtual Desktop can do for you:

* Look up diagnostic activities (management, connection, or feed) for a single user over a period of one week.
* Gather session host information for connection activities from your Log Analytics workspace.
* Review virtual machine (VM) performance details for a particular host.
* See which users are signed into the session host.
* Send message to active users on a specific session host.
* Sign users out of a session host.

**Scale session hosts using Azure Automation:**

You can reduce your total Windows Virtual Desktop deployment cost by scaling your virtual machines (VMs). This means shutting down and deallocating session host VMs during off-peak usage hours, then turning them back on and reallocating them during peak hours. To configure scaling [Click here](https://docs.microsoft.com/en-us/azure/virtual-desktop/virtual-desktop-fall-2019/set-up-scaling-script)

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

The section describes how Patch Management is 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)

# Appendix A – Technical References

[C](https://docs.microsoft.com/en-us/azure/sentinel/)loud Adoption [Framework](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/)

# Deleted Content

**Licensing and Entitlements**

The details of auditing licenses for users to remain compliant with Microsoft licensing terms are given below. Ensure all users have one of the following Licenses/Entitlements or has procured 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 |

**Azure Virtual Machines NVv3-series:**

GPU optimized VM sizes are specialized virtual machines available with single or multiple NVIDIA GPUs. These sizes are designed for compute-intensive, graphics-intensive, and visualization workloads. NVv3-series sizes are optimized and designed for remote visualization, streaming, gaming, encoding, and VDI scenarios using frameworks such as OpenGL and DirectX.

Each GPU in NVv3 instance comes with a GRID license. This license gives you the flexibility to use an NV instance as a virtual workstation for a single user, or 25 concurrent users can connect to the VM for a virtual application scenario.

**Cosmos DB Data Migration Tool**

Azure Cosmos DB Data Migration tool can import data from various sources into Azure Cosmos DB collections and tables. You can import from JSON files, CSV files, SQL, MongoDB, Azure Table storage, Amazon DynamoDB, and even Azure Cosmos DB SQL API collections. The Data Migration tool can also be used when migrating from a single partition collection to a multipartition collection for the SQL API.



**Refactor scenario**

*Platform as a service (PaaS) options can reduce the operational costs that are associated with many applications. It is a good idea to slightly refactor an application to fit a PaaS-based model.*

*"Refactor" also refers to the application development process of refactoring code to enable an application for delivering on new business opportunities.*

**Replace scenario**

Solutions are typically implemented by using the best technology and approach available at the time. Sometimes software as a service (SaaS) applications can provide all the necessary functionality for the hosted application. In these scenarios, a workload can be scheduled for future replacement, effectively removing it from the transformation effort.

**Azure migration:**

* 1. **Before you start:**
* Assess each workload's technical fit: Validate the technical readiness and suitability for migration.
* Migrate your services: Perform the actual migration, by replicating on-premises resources to Azure.
* Manage costs and billing: Understand the tools required to control costs in Azure.
* Optimize and promote: Optimize for cost and performance balance before promoting your workload to production.
* Get assistance: Get help and support during your migration or post-migration activities.
  1. **Assess workloads and refine plans:**

Azure Migrate is the native tool for assessing **and** migrating to Azure.

Azure Migrate assesses on-premises infrastructure, applications, and data for migration to Azure. This service:

* Assesses the migration suitability of on-premises assets.
* Performs performance-based sizing.
* Provides cost estimates for running on-premises assets in Azure.
  1. **Deploy workloads and assets (infrastructure, apps, and data):**

In this phase of the journey, you use the output of the Assess phase to initiate the migration of the environment.

Azure Migrate provides the following functionality:

1. Enhanced assessment and migration capabilities:
   * Hyper-V assessments.
   * Improved VMware assessment.
   * Agentless migration of VMware virtual machines to Azure.
2. Unified assessment, migration, and progress tracking.
3. Extensible approach with ISV integration (such as Cloudamize).
   1. **Release workloads (test, optimize, and handoff):**

This phase is also an opportunity to optimize your environment and perform possible transformations of the environment. For example, you may have performed a "rehost" migration, and now that your services are running on Azure, you can revisit the solutions configuration or consumed services, and possibly perform some "refactoring" to modernize and increase the functionality of your solution.

* 1. **Migration-focused cost control mechanisms:**

Prior to migration of any asset (infrastructure, app, or data), there is an opportunity to estimate costs and refine sizing based on observed performance criteria for those assets.

Cost calculators: there are two handy calculators

* The [Azure pricing calculator](https://azure.microsoft.com/pricing/calculator) provides cost estimates for the Azure products you select.
* Sometimes decisions require a comparison of the future cloud costs and the current on-premises costs. The [Total Cost of Ownership (TCO) calculator](https://azure.microsoft.com/pricing/tco/calculator) can provide such a comparison.

**Azure Migrate calculations**: Azure Migrate calculates **monthly cost estimates** based on data captured by the collector and service map.

**Azure Database Migration Service:** The Azure Database Migration Service is a fully managed service that enables seamless migrations from multiple database sources to Azure data platforms, with minimal downtime (online migrations). The Azure Database Migration Service performs all of the required steps.

**Data Migration Assistant:** The **Data Migration Assistant (DMA)** helps you upgrade to a modern data platform by detecting compatibility issues that can affect database functionality in your new version of SQL Server or Azure SQL Database. DMA recommends performance and reliability improvements for your target environment and allows you to move your schema, data, and uncontained objects from your source server to your target server.

**SQL Server Migration Assistant**

**Microsoft SQL Server Migration Assistant (SSMA)** is a tool designed to automate database migration to SQL Server from Microsoft Access, DB2, MySQL, Oracle, and SAP ASE. we recommend reviewing the detailed [SQL Server Migration Assistant documentation](https://docs.microsoft.com/sql/ssma/sql-server-migration-assistant).

**Database Experimentation Assistant**

Database Experimentation Assistant (DEA) is a new A/B testing solution for SQL Server upgrades. It will assist in evaluating a targeted version of SQL for a given workload. Customers who are upgrading from previous SQL Server versions (SQL Server 2005 and above) to any new version of the SQL Server can use these analysis metrics.

The Database Experimentation Assistant contains the following workflow activities:

* **Capture:** The first step of SQL Server A/B testing is to capture a trace on your source server. The source server usually is the production server.
* **Replay:** The second step of SQL Server A/B testing is to replay the trace file that was captured to your target servers. Then, collect extensive traces from the replays for analysis.
* **Analysis:** The final step is to generate an analysis report by using the replay traces. The analysis report can help you gain insight about the performance implications of the proposed change.