Microsoft

Windows Virtual Desktop Architecture Guide

Designing virtual desktop infrastructure solutions with the best virtual desktop experience, delivered on Azure

Contents

Who should read this guide?

This architecture guide is for Desktop Infrastructure Architects, Cloud Architects, Desktop Administrators, or System Administrators who are exploring the Windows Virtual Desktop public preview. The aim of this guide is to help you understand how Windows Virtual Desktop works, while providing architectural considerations for building virtual desktop infrastructure solutions with it.

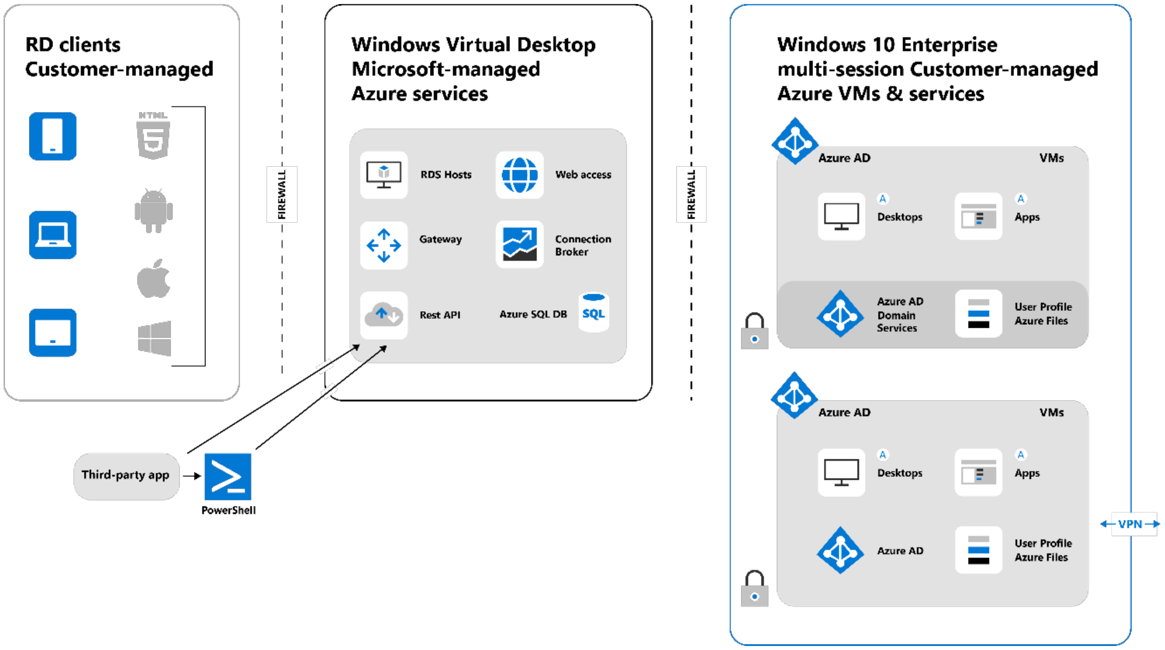
Service architecture

As you might expect, the architecture of the Windows Virtual Desktop service is like that of Windows Server Remote Desktop Services. Microsoft manages the infrastructure and brokering components, while you manage the desktop host virtual machines, data, and clients.

Microsoft-managed components

The following Windows Virtual Desktop services are managed by Microsoft as part of Azure:

- **Web Access.** The Web Access service within Window Virtual Desktop lets users access virtual desktops and remote apps through an HTML5-compatible web browser like they would with a local PC—from anywhere and any device. You can secure Web Access using multifactor authentication in Azure Active Directory.
- **Remote Connection Gateway.** The Remote Connection Gateway service grants remote users access to Windows Virtual Desktop remote apps and desktops from any internet-connected device that can run a Windows Virtual Desktop client. It allows access to a Windows Virtual Desktop client over port 443 using reverse-connect. This means you don't need inbound ports on the desktop hosts—and the inbound attack surface is smaller.
- **Connection Broker.** The Connection Broker service manages user connections to virtual desktops and remote apps. It provides load balancing and reconnection to existing sessions along with starting or stopping host virtual machines.
- **Remote Desktop Diagnostics.** Remote Desktop Diagnostics is an event-based aggregator that marks each user or administrator action on the Windows Virtual Desktop deployment as a success or failure. Administrators can query the aggregation of events to identify failing components.
- **Extensibility components.** Windows Virtual Desktop includes several extensibility components. You can manage Windows Virtual Desktop using Windows PowerShell or with the provided REST APIs, which also enable support from third-party tools.



Components you manage

You manage these components of your Windows Virtual Desktop solution:

Azure services

- **Azure Virtual Network.** A virtual network (vNET) enables Azure resources, such as virtual machines, to communicate privately with each other and with the internet. By connecting Windows Virtual Desktop host pools to the Azure Active Directory domain, you can define network topology to access virtual desktop and virtual apps from the intranet or internet based on organizational policy. Connect your Windows Virtual Desktop vNET to your on-premises network using a virtual private network. Or use Azure ExpressRoute to extend your on-premises networks into the Microsoft cloud platform over a private connection, facilitated by a connectivity provider.
- **Azure Active Directory.** Windows Virtual Desktop uses Azure Active Directory for identity and access management. This lets you take advantage of Azure Active Directory security features, such as conditional access, Multi-Factor Authentication, and the Intelligent Security Graph. It also helps you maintain app compatibility in your environment when your virtual machines are Active Directory domain.
- **Windows Virtual Desktop session hosts.** Windows Virtual Desktop *session hosts* are Azure virtual machines that can be grouped for identical session hosts into *host pools*. Each session host has a Windows Virtual Desktop host agent installed, which registers the virtual machine as part of your Windows Virtual Desktop *tenant*. And each host pool can have one or more *app groups*, which are collections of remote applications or desktop sessions that users can access.

Azure virtual machines in a host pool can run one of several operating systems—including Windows 7 Enterprise, Windows 10 Enterprise, Windows 10 Enterprise Multi-session, Windows Server 2012 R2 and above, including custom Windows system images with pre-loaded apps, group policies, or any other customizations. You also have your choice of virtual machine sizes, including GPU-enabled virtual machines.

- **Windows Virtual Desktop tenant.** Your Windows Virtual Desktop tenant is a management plane to manage host pools, app groups, users, and other related services that provide your users access to them.

Clients applications

Windows Virtual Desktop gives you the flexibility to connect to remote desktops and remote apps from almost anywhere using just about any device. Microsoft will support the following remote desktop clients with general availability (GA):

- Remote desktop client on Windows
- Remote desktop web client
- Remote desktop client on Android
- Remote desktop client on iOS
- Remote desktop client on Mac

Other service features

The Windows Virtual Desktop service architecture also supports:

- **Diagnostics, monitoring, and alerts.** Track the health and performance of your Windows Virtual Desktop environment with Azure Monitor, Log Analytics, and Application Insights.
- **Conditional access.** As mentioned earlier, deep integration with Azure Active Directory enables you to enforce security policies for remote apps and virtual desktops. You can even restrict access to remote desktops based on the risk profile of the user.
- **Role-based access controls.** Windows Virtual Desktop uses a role-based access controls model to manage access to the tenant environment. These include the following built-in roles:
    - *RDS Owner*. Can manage everything, including access to resources.
    - *RDS Contributor*. Can manage everything except access to resources.
    - *RDS Reader*. Can view everything but can't make any changes.
    - *RDS Operator*. Can view diagnostic activities.

Solution architecture

Personal desktops

Personal desktop solutions, sometimes called *persistent desktops*, allow users to connect to a specific session host each time they connect. Users can typically modify the desktop experience to meet their personal preferences and save files in the desktop environment. Personal desktop solutions are appropriate when you need to:

- Give users administrator access to the desktop for any reason, including installing or running apps.
- Allow users to customize the desktop environment, including saving files within the desktop environment.

Pooled desktops

Pooled desktop solutions, also called *non-persistent desktops*, assign users to whichever session host is currently available, depending on the load-balancing algorithm chosen. Because the user isn't always returned to the same session host each time they connect, they have limited ability to customize the desktop environment and are not typically given administrator access.

Remote apps

Remote app solutions deliver specific virtualized apps to the user on their local desktop. The user interacts with the app just like it's installed on their local desktop, but it runs on the remote desktop session host. Remote apps are commonly used when the user doesn't need a complete virtualized desktop environment or where control over the specific app is a high priority.

Architectural considerations

There are some key issues and requirements you should keep in mind when designing your Windows Virtual Desktop solution.

Azure service limits

An Azure subscription has a maximum number of vNETs, virtual machine cores, and cloud services that can be used by that subscription. If you need more than provided in the limits, you may need to create multiple subscriptions. See Azure subscription and service limits, quotas, and constraints for more information.

Desired operating system

Windows Virtual Desktop currently supports the following desktop operating systems:

- Windows 7 Enterprise

- Windows 10 Enterprise
- Windows 10 Enterprise Multi-session
- Windows Server 2012 R2 and above

Virtual machine size

Assess your current virtual desktop infrastructure workloads and perform capacity planning and right-sizing for the Azure virtual machines that will host your desktops. You can use Azure Migrate to help with this process.

Also consider whether you'll be using personal desktops or pooled desktops, and which provisioning rules you plan to use when planning virtual machine size. See Workloads for more information.

Location

Which Azure region you choose to locate your Windows Virtual Desktop solution depends on the following factors:

- **User location.** Locating your solution in a region that's physically closer to your users helps ensure they have a good connection experience.
- **Resource location.** If the applications your users access need low-latency connections to data, you should place your desktop hosts in a region physically close to the data or apps.
- **Compliance.** You may need to locate your solution in a specific region to meet compliance or regulatory requirements.

Security

To secure your Windows Virtual Desktop solutions—and *keep* them secure—you'll likely use a combination of these tools:

- **Azure Active Directory.** Control access to your remote apps and desktops through Azure Active Directory. Each Windows Virtual Desktop can be connected to a separate Azure Active Directory tenant. On-premises Active Directory can be synchronized with the Active Directory tenant to a common user identity for authentication and authorization to all resources. For more information, see Identity management.
- **Microsoft 365 security.** Use Microsoft 365 security and management capabilities to enhance the security posture for your Windows Virtual Desktop environment.
- **Azure Information Protection.** Secure data, documents, and email in your desktop environment.
- **Distributed Denial of Service (DDoS) Protection.** Protect your solution from denial of service threats through protection policies and monitoring of your vNET.
- **Network security.** Use network security groups within your Azure Virtual Network to control traffic in and out of your session-host virtual machines. You can also implement

your own network security and firewall appliances in Azure for advanced protection. Note that you need to open the outbound 443 port in the firewall of your session hosts.

- **Role-based access controls.** Use built-in or custom roles to enable a fine level of control over management permissions in Windows Virtual Desktop. As discussed previously under Other service features, pre-defined roles include:
  - RDS Owner
  - RDS Contributor
  - RDS Reader
  - RDS Operator
- **Conditional access policy.** Control how authorized users can access your remote apps and desktops based on the network location of a user, time of day, client device, client app, and risk profile.
- **Security Center.** Provide unified security management for your vNET and host virtual machines.
- **Virtual private network (VPN) gateway.** Create a secure connection from your on-premises environment to your Windows Virtual Desktop solution. You can also use ExpressRoute to create a dedicated secure connection between your environments.
- **Azure Multi-Factor Authentication.** Require two-step verification for user sign-ins.

Network

When designing your Windows Virtual Desktop solution, consider the following in terms of your network:

- **Capacity.** You'll need to perform network capacity planning based on the number of users, their expected usage pattern, and the types of applications they'll use in your Windows Virtual Desktop environment. Include both the traffic usage for the applications running inside user sessions and the usage for desktop input and output.

  For large deployments, consider a dedicated private connection from your on-premises environment or a co-located datacenter to Azure, using ExpressRoute.

- **App data transfer.** Depending on your application location, you will need to consider network capacity planning. If any of your application is residing on-premises or in another cloud and you want to access an application from Azure over the internet or ExpressRoute, you should plan for the required network bandwidth to negotiate app latency and cost management.

  While moving your existing business applications to the cloud, you should also consider network bandwidth and data to be consumed for transferring.

- **Topology.** Your network topology will also affect your solution. Many organizations have central network hubs that all traffic is routed through. These central hubs often include security devices that sniff network traffic. As you design cloud-based solutions, these centralized hubs can become a chokepoint for your network.

- **Latency.** Another important factor is network latency. Your choice of Azure region is an important factor in network latency, as is your network capacity. You can also add workloads that your Windows Virtual Desktop users will access to the same vNET you use for desktops.
- **Availability.** If your solution needs to be highly available, you should implement a network failover solution. For example, if you use ExpressRoute to create a dedicated secure connection, you can use a VPN gateway for backup connectivity.

Workloads

Consider the workloads your users will run on their desktops—and the experience you want them to have while running the workloads. Those workloads will determine if users need:

- **Administrative access to their desktop environment.** Requires deploying personal desktops.
- **Graphics-intensive applications.** Requires creating GPU-enabled session hosts.
- **Applications that run only on legacy operating systems.** Windows Virtual Desktop supports various legacy operating systems, and it offers extended support for Windows 7 Enterprise.
- **Persistent access to user profile data and personal files.** You can design your Windows Virtual Desktop solution based on personal desktops, or use FSLogix or other technologies to enable persistent access on multi-session desktops.

Workloads also influence what provisioning rule you choose:

- **Breadth mode.** Allocate desktops evenly across your pool of virtual desktop host virtual machines. With this rule, you ensure that each user has access to the maximum amount of available processing and memory resources.
- **Depth mode.** Allocate the maximum number of desktops to each host virtual machine before allocating any on the next machine in the pool. This rule ensures you get the most from each virtual machine, while minimizing the overall number of machines used.

Identity management

Selecting your identity management strategy depends on whether you use an on-premises environment, the cloud, or both.

- **Azure Active Directory identity management.** For this approach, you need to connect your Windows Virtual Desktop environment to your on-premises Azure Active Directory.
- **Cloud-only identity management.** If you don't have an on-premises Active Directory environment, a cloud-only approach lets you identify and manage users and groups only within Azure Active Directory.

- **Hybrid identity management.** Another option is a hybrid approach. With Azure Active Directory Connect, you can synchronize your on-premises Active Directory users and groups to an Azure Active Directory tenant. And even without a hybrid identity solution, you can still join Windows 10 desktops to both Azure Active Directory and your on-premises Active Directory domain, which makes signing into Azure easier.

Scale

How you scale your Windows Virtual Desktop depends heavily on your workloads and desired user experience. Once you decide, choosing the appropriate provisioning rule (discussed previously under Workloads) helps you carry this out.

With the Windows Virtual Desktop, there's no limit on how many virtual machines you provision. However, note that the current host pool can scale up to Azure subscription limits.

Costs

Architect your solution to realize cost savings with Azure for your Windows Virtual Desktop. Along with right-sizing your solution and architecting it to scale efficiently, other ways you can architect your management costs include:

- **Azure Hybrid Benefit.** If you have Software Assurance, you can use Azure Hybrid Benefit for Windows Server to save on the cost of your Azure infrastructure.
- **Azure Reserved Instances.** Prepay for your virtual machine usage and save money. Combine with Azure Hybrid benefit for up to 80 percent savings over list prices.
- **Multi-session remote experience.** By delivering a multi-session desktop experience, you can enable more than 500 users (with identical compute requirements) to log onto a single virtual machine at the same time, which can result in considerable cost savings.
- **On-demand infrastructure scaling.** Loadbalancing using breadth and depth mode helps you better control your variable costs and provision additional virtual machines as needed.

Licensing

Windows Virtual Desktop requires:

- Microsoft 365 E3, E5, A3, A5, F1, or Business
- Windows E3,[1] E5, A3, or A5

With any of the above licenses, you can access Windows Virtual Desktop at no cost. By setting up or using an Azure free account, you can start using Windows Virtual Desktop right away, deploying and managing your virtualization environment while paying only for the virtual machines you use.

[1] Access to FSLogix technology—including Office Containers, Profile Containers, and App Masking—are included in Windows E3+, Microsoft 365 E3+, and RDS CALs.

Running Windows Server 2012 R2, 2016, or 2019 requires a Remote Desktop Services (RDS)[2] Client Access License (CAL) with Software Assurance.

Migrating to Windows Virtual Desktop

Once you've decided to migrate to Windows Virtual Desktop, what's the best way to do it? It's helpful to break it down into phases: Assess, Prepare, Migrate, Optimize, and Secure/Manage. By organizing your efforts into these phases, you can solve the most pressing migration challenges and deliver the reliability, performance, and security you need.

Assess your existing virtual desktop infrastructure

Begin your Windows Virtual Desktop migration by discovering and assessing your apps, data, and current remote desktop service or other virtual desktop deployments and infrastructure. Map dependencies across applications and prioritize these for Windows Virtual Desktop migration. As you establish your migration priorities and business objectives, you can continually track to those as you discover more about your environment.

Technical and business planning for migration comes down to four straightforward procedures:

- **Discover remote desktop service workloads,** including remote desktop service components and remote desktop host servers. This procedure relies on interaction directly with the endpoint (using an agent) or managing hypervisor (such as Hyper-V). The goal is to discover existing virtual desktop infrastructure servers and applications deployed and accessed from remote desktop infrastructure—including type, configuration, and usage.
- **Identify application and server dependencies for remote desktop service environment.** This procedure helps in creating visual maps of all your applications and workloads. By mapping these together, you can understand their interaction as a single entity for costing, configuration analysis, and eventually migration.
- **Identify hardware or operating system dependencies.** Through configuration analysis, you can see which workloads can migrate with no modifications, those that may require basic modifications to comply, and any that are not compatible in their current formation.
- **Perform cost planning.** Through discovered resource usage reports—such as CPU, memory, and storage—and intelligent cost analysis tools, you can determine the actual usage of your workload. This analysis should suggest the best cloud infrastructure as a service (IaaS) virtual machine series to use.

[2] Access to FSLogix technology—including Office Containers, Profile Containers, and App Masking—are included in Windows E3+, Microsoft 365 E3+, and RDS CALs.

Microsoft provides migration assessment tools to inventory the physical and virtual servers for your remote desktop service environment. These tools also help you evaluate these servers for cloud compatibility. The tools include:

- **Azure Migrate.** This service helps you assess on-premises machines for migration to Azure. For more information, see Azure Migrate.
- **Microsoft Assessment and Planning (MAP) Toolkit.** This agentless, automated, multiproduct planning and assessment tool can lead to quicker and easier desktop, server, and cloud migrations. For more information, see Microsoft Assessment and Planning Toolkit.
- **Azure Site Recovery Deployment Planner.** This tool provides detailed assessment reports regarding cloud compatibilities and incompatibilities of workloads, network bandwidth requirements to meet target recovery point objectives, and recommendations on right-sizing Azure infrastructure deployment. For more information, see the Azure Site Recovery overview.
- **Microsoft Data Migration Assistant.** This tool assesses and detects compatibility issues that can impact database functionality in Azure. It also assesses feature parity between your SQL Server source and target, and it recommends performance and reliability improvements for your target environment. For more information, see Microsoft Data Migration Assistant.

Prepare your Azure and Windows Virtual Desktop environment

Preparing your Azure environment is a prerequisite for migration to Windows Virtual Desktop. Here’s how to go about it.

Prepare your Azure environment

If you’re new to Azure, you first need to sign up for an Azure account as an organization and add an Azure subscription. Then you can start preparing Azure resources for Windows Virtual Desktop through the following steps:

1. **Create and connect Azure Virtual Network.** Azure Virtual Network gives you an isolated and highly secure environment to run your virtual machines and applications in.
    a. **Create Azure Virtual Network.** By creating this network, you enable Azure resources, such as virtual machines, to communicate privately with each other, and with the internet. For more information about creating Azure Virtual Network, see Create a virtual network using the Azure portal.
    b. **Connect Azure Network to on-premises.** When users are connecting Windows Virtual Desktop over intranet only, you must define network topology to access virtual desktop and virtual apps from Windows Virtual Desktop over a private network. Azure offers two ways to connect your Azure Virtual Network to your on-premises network:

        i. **Azure Virtual Private Network (VPN).** Connects your on-premises networks to Azure through Site-to-Site VPNs. For more information, see Create a Site-to-Site connection using the Azure portal.
        ii. **Azure ExpressRoute.** ExpressRoute lets you extend your on-premises networks into the Microsoft cloud platform over a private connection facilitated by a connectivity provider, without going through public internet. For more information, see ExpressRoute circuits and peering.

2. **Set up Active Directory for Identity Management.** Windows Virtual Desktop uses Active Directory for services and user authentication. To best meet your identity management requirements, you have flexibility to set up Active Directory services in the following ways:
    a. **Standalone Azure Active Directory Domain Services.** Standalone or cloud-only Azure Active Directory tenants (often referred to as *managed tenants*) can be configured so you don’t have an on-premises identity footprint. You can keep these deployments standalone with their own identity service. For more information, see Enable Azure Active Directory Domain Services using the Azure portal.
    b. **Sync Azure Active Directory Domain Services with on-premises Azure Directory.** You can create a hybrid IT infrastructure that can consume a mix of cloud resources and on-premises resources. For organizations with hybrid cloud infrastructure, Azure Active Directory Domain Services can be used by synchronizing identity information from an on-premises directory to an Azure Active Directory tenant using Azure Active Directory Connect. For more information, see What is hybrid identity? and What is Azure AD Connect?
3. **Extend Active Directory Domain Services on an Azure Virtual Machine.** You may want to use hybrid applications with Windows Virtual Desktop, in which functionality is distributed between on-premises and Azure, and among applications and services that perform authentication using Active Directory. To do this, you can extend Active Directory Domain Services to Azure by deploying those services on an Azure Virtual Machine. You can also deploy Active Directory Domain Services on an Azure Virtual Machine manually, make it an additional domain controller, or use a GitHub script to deploy. For more information, see Install Active Directory Domain Services or Extend Active Directory Domain Services (AD DS) to Azure.

Deploy and configure Windows Virtual Desktop for migration

Windows Virtual Desktop is a multi-tenant infrastructure hosted by Microsoft that manages connections between remote desktop clients and multiple isolated remote desktop tenant environments. Each tenant environment consists of one or more host pools, which in turn contain one or more identical session hosts. The session hosts are virtual machines running operating systems such as Windows 10 Enterprise Multi-session.

Use the following steps to create and configure a Windows Virtual Desktop tenant to migrate remote desktop services on Azure workloads:

1. **Give consent to have the Windows Virtual Desktop services access the Azure Active Directory.** You first need to give consent to allow Windows Virtual Desktop services and remote desktop clients to read your Azure Active Directory that you created in the first phase of migration.
    a. Grant Azure Active Directory consent for the Windows Virtual Desktop server app.
    b. Grant Azure Active Directory consent for the remote desktop client app.
2. **Create a Windows Virtual Desktop tenant.** After providing permission for Windows Virtual Desktop to query and read values from the Azure Active Directory, you should perform the onboarding process. This involves creating a Windows Virtual Desktop tenant, assigning Windows Virtual Desktop administrators to the RDS Owner role, and granting access to software packages. Multiple options are available to create host pools and manage app groups. You can use PowerShell cmdlets, a GitHub template, or Azure Marketplace offering (once available with preview) to create the tenant.
    a. **Create a host pool in remote desktop tenant using cmdlets.** Run the following cmdlets to create a new host pool and registration token, granting a user access to the default desktop app group. Replace the bracketed items with the relevant values:

```
New-RdsHostPool -TenantName <tenantname> -Name <hostpoolname>

New-RdsRegistrationInfo -TenantName <tenantname> -HostPoolName
<hostpoolname> - ExpirationHours <number of hours> | Select-Object
-ExpandProperty Token > <PathToRegFile>

Add-RdsAppGroupUser -TenantName <tenantname> -HostPoolName
<hostpoolname> -
AppGroupName “Desktop Application Group” -UserPrincipalName
<userupn>
```

    b. **Create a host pool in your remote desktop tenant using a GitHub template.** This template creates virtual machines and registers them as session hosts to a new or existing Windows Virtual Desktop host pool. There are multiple sets of parameters you must enter to successfully deploy the template:
        i. Virtual machine image
        ii. Virtual machine configuration
        iii. Domain and network properties
        iv. Authentication to Windows Virtual Desktop

    For more information, see RDS-Templates and follow the guidance for entering the appropriate parameters for your scenario.

c. **Create a host pool in your remote desktop tenant using Azure Marketplace.** You can use the Azure portal to create a host pool and registration token, granting a user access to the default desktop app group. Here's how:
   i. **Sign into the tenant's Azure subscription.** You can sign into the Azure subscription directly through the Azure portal. If you're a Cloud Solution Provider configuring a customer Azure subscription, you can sign in through the Cloud Solution Provider portal.
   ii. **Run the Azure Marketplace offering to create a tenant.** Once you're signed into the appropriate Azure subscription, run the Azure Marketplace offering and create a Windows Virtual Desktop tenant.
   iii. **Create a host pool.** Provision a new Windows Virtual Desktop host pool using operating system images from Azure Marketplace or a custom Windows image uploaded to Azure. Define the host pool name and resource group. Select the operating system image, size of pool, plus choose the vNET, subnets, and other configurations.
   iv. **Add a custom operating system image for host pool to your storage account.** To use a custom operating system image for your Windows Virtual Desktop host pool, you need to add a custom operating system image to your Azure Storage account.
   v. **Create an app group and assign users.** The default app group created automatically for a new host pool publishes the full desktop. You can also create one or more app groups to publish remote apps or desktops for users within the host pool using the PowerShell cmdlet. Assign end users who can access published remote apps and desktops.

Migrate to Windows Virtual Desktop

Once you complete these prerequisites for preparing your infrastructure on Azure, you have multiple options to migrate Windows remote desktop service workloads from on-premises, Azure, or third-party cloud providers to Windows Virtual Desktop. These workloads may comprise virtual machines, apps, and data.

Choose the most suitable migration path for you. These paths include migration from existing Windows remote desktop services on-premises, Azure, or another virtual desktop solution.

- **On-premises remote desktop service to Windows Virtual Desktop.** Migrate your existing Windows remote desktop service and app virtualization on-premises, whether hybrid or natively to Windows Virtual Desktop.
- **Remote desktop service on Azure to Windows Virtual Desktop.** Migrate your existing Windows remote desktop service and app virtualization on Azure to Windows Virtual Desktop.

- **Amazon WorkSpaces to Windows Virtual Desktop.** Migrate Windows desktop virtualization from Amazon WorkSpaces to Windows Virtual Desktop.

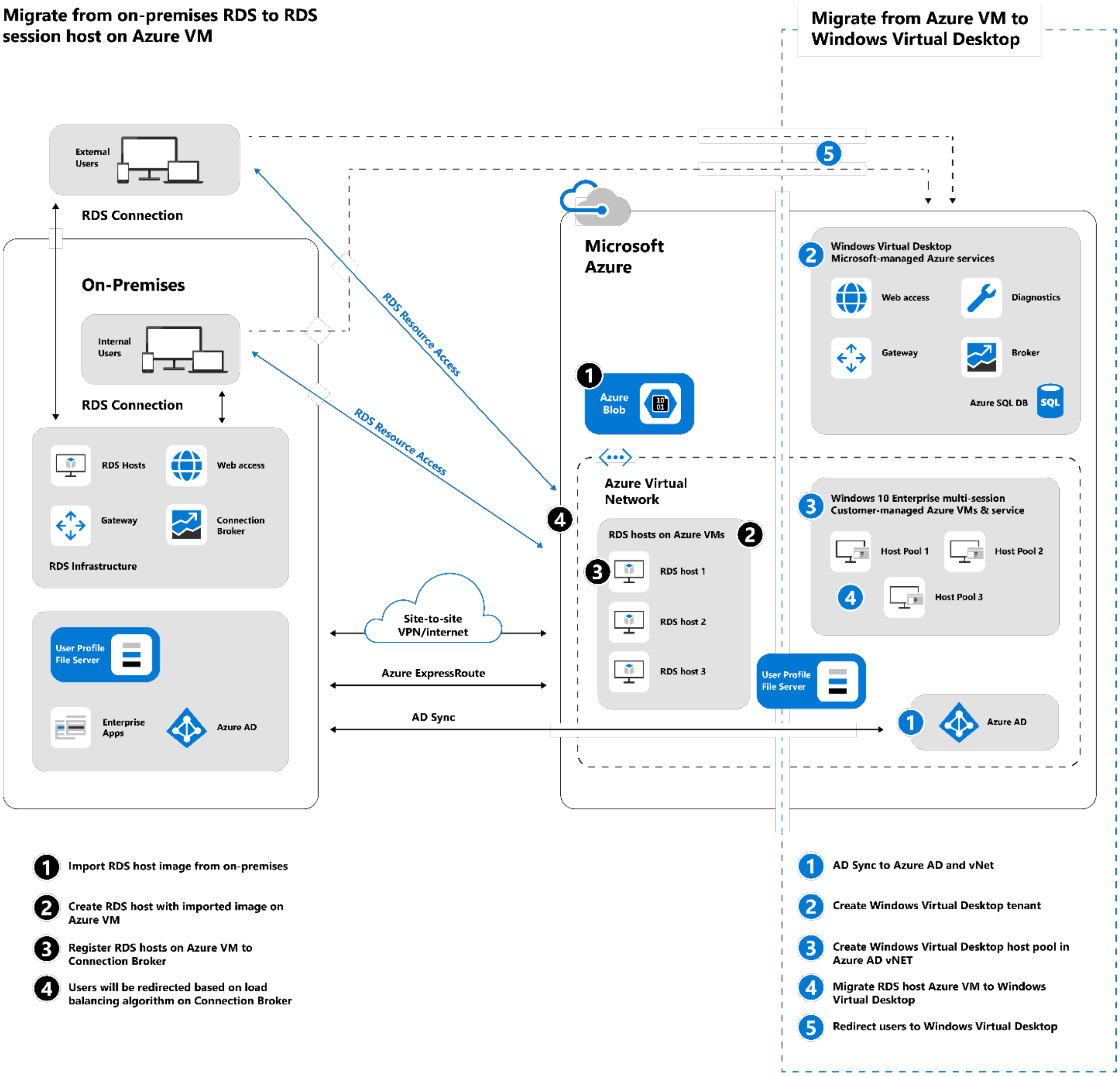
Migrate from on-premises remote desktop service to Windows Virtual Desktop

You need to perform this migration in two parts, both of which follow the Assess and Prepare phases. The first part is to migrate your on-premises Windows remote desktop service workloads—including remote desktop service components, remote apps, remote desktop, virtual machines, and user data—to remote desktop service on Azure. In the second part, migrate your Azure remote desktop service session-host virtual machines to Windows Virtual Desktop.

Migrate from remote desktop service on Azure to Windows Virtual Desktop

Depending upon business and technical considerations of your on-premises Windows remote desktop service deployment, you can choose any of the following migration options for remote desktop service on Azure migration.

Hybrid Windows remote desktop service. Cloud bursting is a migration approach to remote desktop service on Azure, where hybrid deployment is configured between on-premises Windows remote desktop service and remote desktop session hosts deployed on Azure virtual machines. Cloud bursting is usually used to handle seasonal spikes by redirecting users to the remote desktop session host on Azure virtual machines. For migration to Windows Virtual Desktop, cloud bursting can be used to gradually redirect users to a remote desktop session host on Azure virtual machines and then move them to Windows Virtual Desktop. In this scenario, the remote desktop service components include Web Access, Gateway, Broker, and file server for profile data. Your database remains on-premises as you provision the remote desktop service host on Azure. This is an active-active configuration of on-premises and Azure remote desktop services.


Migrate from on-premises RDS to RDS session host on Azure VM
Migrate from Azure VM to Windows Virtual Desktop
External Users
RDS Connection
On-Premises
Internal Users
RDS Connection
RDS Hosts
Web access
Gateway
Connection Broker
RDS Infrastructure
User Profile File Server
Enterprise Apps
Azure AD
RDS Resource Access
RDS Resource Access
Site-to-site VPN/internet
Azure ExpressRoute
AD Sync
Microsoft Azure
Azure Blob
Azure Virtual Network
RDS hosts on Azure VMs
RDS host 1
RDS host 2
RDS host 3
User Profile File Server
Windows Virtual Desktop Microsoft-managed Azure services
Web access
Diagnostics
Gateway
Broker
Azure SQL DB
SQL
Windows 10 Enterprise multi-session Customer-managed Azure VMs & service
Host Pool 1
Host Pool 2
Host Pool 3
Azure AD
1 Import RDS host image from on-premises
2 Create RDS host with imported image on Azure VM
3 Register RDS hosts on Azure VM to Connection Broker
4 Users will be redirected based on load balancing algorithm on Connection Broker
1 AD Sync to Azure AD and vNet
2 Create Windows Virtual Desktop tenant
3 Create Windows Virtual Desktop host pool in Azure AD vNET
4 Migrate RDS host Azure VM to Windows Virtual Desktop
5 Redirect users to Windows Virtual Desktop

Once your Azure Virtual Network is in place with a secure tunnel to on-premises using site-to-site VPN or ExpressRoute, you can begin deploying remote desktop service virtualization endpoints (remote desktop session host and virtual machine) and configuring them to be part of remote desktop broker on-premises. Here are the steps to follow:

1. **Create virtual machines for virtualization endpoints.** Provision new Azure virtual machines for the remote desktop session host. These virtual machines will be part of the on-premises remote desktop service host pool and used to deliver session-based remote desktop and remote apps. The virtual machines must be the same images that you're using in the remote desktop service collection on-premises, as the remote desktop broker will look at all these virtual machines as one homogeneous unit. It will load

balance users across virtual machines on-premises and on Azure. First, you need to upgrade and update the virtual machine to an OS that Azure supports.

   a. **Prepare a Windows virtual hard disk to upload to Azure.** Before you upload a remote desktop session-host virtual machine from on-premises to Azure, you must prepare the virtual hard disk. Azure supports only first-generation virtual machines that are in the virtual hard disk file format and have a fixed-sized disk. For more information, see Prepare a Windows VHD or VHDX to upload to Azure.
   b. **Upload a generalized virtual hard disk to Azure Storage.** Once generalized, upload Windows virtual machine for remote desktop session host on Azure. For more information, see Upload a generalized VHD and use it to create new VMs in Azure.
   c. **Create the virtual machine.** From your uploaded remote desktop session-host virtual machine image on Azure, create one or more Azure virtual machines. For more information, see Create a managed image from the uploaded VHD.

2. **Add Azure virtual machines to an on-premises remote desktop service host farm.** After creating the remote desktop session host on the Azure virtual machine, make sure to add it to the remote desktop session host farm. That way the remote desktop broker can identify it and load balance sessions. For more information, see Scale out your Remote Desktop Services deployment by adding an RD Session Host farm.
3. **Redirect users to Azure virtual machines.** Once your remote desktop session host on Azure virtual machine is added to the host farm, you can configure the client redirects to the remote desktop session host on Azure for the user connection. These configurations are based on the remote desktop connection broker load balancing algorithm (for example: weight factor, fewest connections, and least utilized). In phases or by collection, you can move all users to the remote desktop session-host virtual machines on Azure.
4. **Get ready for Windows Virtual Desktop migration.** When all users are migrated to the remote desktop session host on Azure, prepare for the next migration phase, which is beginning to migrate Azure-hosted remote desktop service workloads to Windows Virtual Desktop.
   a. **Deploy and configure Windows Virtual Desktop for migration** to verify or create Windows Virtual Desktop tenant and host pools.
   b. **Register remote desktop service session-host Azure virtual machine to Windows Virtual Desktop.** To migrate the remote desktop service session-host Azure virtual machines currently part of the on-premises remote desktop service infrastructure, you can register these to the host pool. To do this, install the remote desktop agent on the session-host Azure virtual machine that you want to be part of the Windows Virtual Desktop host pool. Here are the steps:
      i. Install remote desktop agent on the session-host Azure virtual machine.
         1. Download the remote desktop agent from Windows Virtual Desktop services.
         2. Run the remote desktop agent installation wizard.

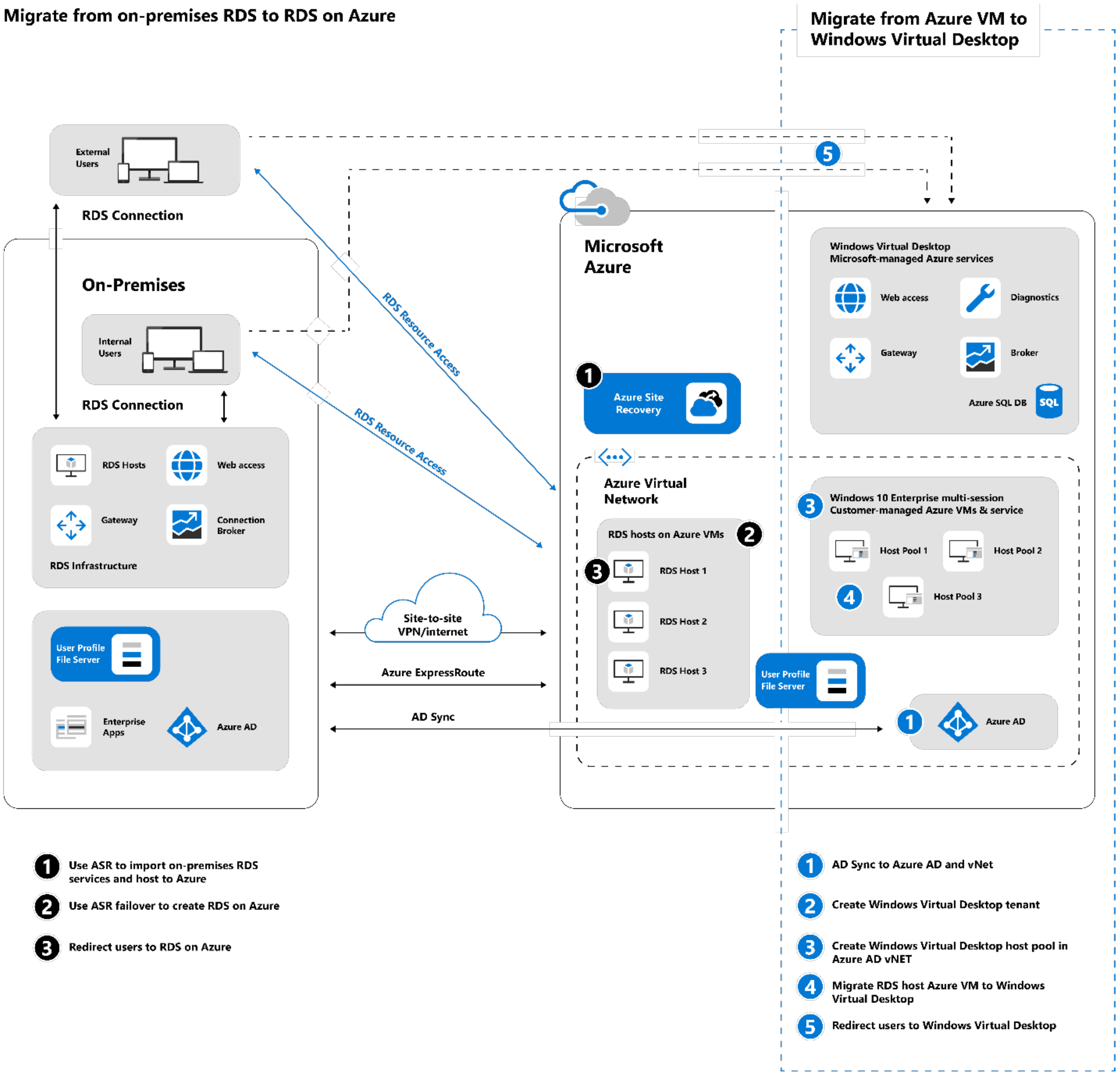
        3. Provide the secret received during the onboarding process for Windows Virtual Desktop.
        4. When the secret is confirmed, you can install the remote desktop agent on the virtual machine.
    ii. Follow these steps to install the remote desk agent bootloader to the same session-host virtual machine:
        1. Download remote desktop agent bootloader from Windows Virtual Desktop services.
        2. Run the remote desktop agent installation wizard.

    Once the remote desktop agent and bootloader are successfully installed, the machine will be automatically added to the existing Windows Virtual Desktop host pool.

5. **Publish app group in the Windows Virtual Desktop tenant.** The Azure virtual machines added to the Windows Virtual Desktop host pool can be used to define and publish the app group in Windows Virtual Desktop tenant. You can also create one or more remote desktops or remote app groups for the host pool.
6. **Redirect users to Windows Virtual Desktop.** Once your session-host virtual machines are migrated to Windows Virtual Desktop, you can deploy Windows Virtual Desktop clients. With these, your users can access remote desktop and apps hosted on Windows Virtual Desktop.

Note: This is the easiest option for migrating your existing session host and users to Azure. Before you do this, however, evaluate app dependencies between those running on Azure to the on-premises infrastructure, as there will be lot of data flow across this network.

Azure migration using Azure Site Recovery. You can also use Azure Site Recovery to migrate your remote desktop service workloads hosted on-premises to Azure virtual machines. This scenario enables active-passive configuration of your remote desktop services on-premises and on Azure. After migrating remote desktop service workloads to Azure, remote desktop service on Azure will be active while on-premises workloads will be passive.


Migrate from on-premises RDS to RDS on Azure
Migrate from Azure VM to Windows Virtual Desktop
External Users
RDS Connection
On-Premises
Internal Users
RDS Connection
RDS Hosts
Web access
Gateway
Connection Broker
RDS Infrastructure
User Profile File Server
Enterprise Apps
Azure AD
RDS Resource Access
RDS Resource Access
Site-to-site VPN/internet
Azure ExpressRoute
AD Sync
Microsoft Azure
1 Azure Site Recovery
Azure Virtual Network
RDS hosts on Azure VMs 2
3 RDS Host 1
RDS Host 2
RDS Host 3
User Profile File Server
5
Windows Virtual Desktop Microsoft-managed Azure services
Web access
Diagnostics
Gateway
Broker
Azure SQL DB
SQL
3 Windows 10 Enterprise multi-session Customer-managed Azure VMs & service
Host Pool 1
Host Pool 2
4 Host Pool 3
1 Azure AD
1 Use ASR to import on-premises RDS services and host to Azure
2 Use ASR failover to create RDS on Azure
3 Redirect users to RDS on Azure
1 AD Sync to Azure AD and vNet
2 Create Windows Virtual Desktop tenant
3 Create Windows Virtual Desktop host pool in Azure AD vNET
4 Migrate RDS host Azure VM to Windows Virtual Desktop
5 Redirect users to Windows Virtual Desktop

Here are the steps for Azure migration using Azure Site Recovery:

1. **Migrate your on-premises remote desktop service session-host virtual machines to Azure.**
   a. Create a Recovery Services vault on Azure.
   b. Configure the on-premises components of Azure Site Recovery.
   c. Configure the Azure components of Azure Site Recovery.
   d. Replicate your virtual machines to Azure.
   e. Perform failover and test your virtual machines.
   f. Perform a final failover.

   For more information, see Prepare Azure for migration and Prepare on-premises Hyper-V Servers.

2. **Redirect users to Azure.** After you complete the migration process, you can redirect your end users to access remote apps and desktops hosted on the Azure remote desktop service environment.
3. **Get ready for Windows Virtual Desktop migration.** Once all users are migrated to remote desktop service on Azure, get prepared for the next migration phase where you begin migrating Azure-hosted remote desktop service workloads to Windows Virtual Desktop.
    a. **Deploy and configure Windows Virtual Desktop for migration** to verify or create Windows Virtual Desktop tenant and host pools.

    b. **Register remote desktop service session-host Azure virtual machine to Windows Virtual Desktop.** To migrate the remote desktop service session-host Azure virtual machines currently part of the on-premises remote desktop service infrastructure, register them to the host pool. To do this, install the remote desktop agent on the session host Azure virtual machine that you want to be part of the Windows Virtual Desktop host pool. Here are the steps:

        i. Install the remote desktop agent on the session-host Azure virtual machine.

        1. Download the remote desktop agent from Windows Virtual Desktop services.
        2. Run the remote desktop agent installation wizard.
        3. Provide the secret received during the onboarding process for Windows Virtual Desktop.
        4. When the secret is confirmed, you can install the remote desktop agent on the virtual machine.

        ii. Follow these steps to install the remote desk agent bootloader to the same session-host virtual machine:

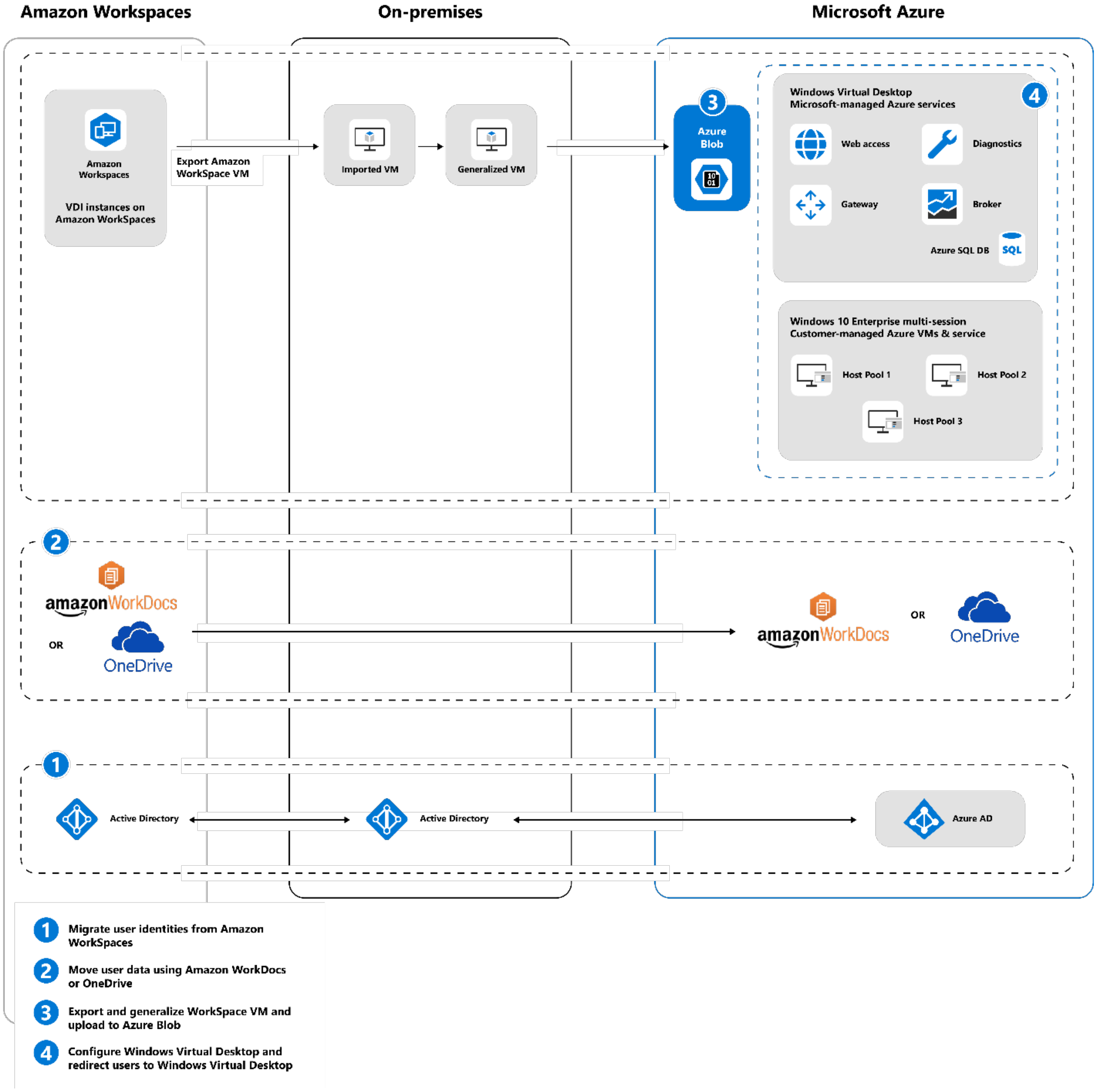
        1. Download the remote desktop agent bootloader from Windows Virtual Desktop services.
        2. Run the remote desktop agent installation wizard.

        Once the remote desktop agent and bootloader are successfully installed, the machine will be automatically added to the existing Windows Virtual Desktop host pool.
4. **Publish app group in the Windows Virtual Desktop Tenant.** The Azure virtual machines added to the Windows Virtual Desktop host pool can be used to define and publish the app group in Windows Virtual Desktop tenant. You can also create one or more remote desktops or remote app groups for the host pool.
5. **Redirect users to Windows Virtual Desktop.** Once your session-host virtual machines are migrated to Windows Virtual Desktop, you can deploy Windows Virtual Desktop clients. With these, your users can access remote desktop and apps hosted on Windows Virtual Desktop.

Migrate from Amazon WorkSpaces to Windows Virtual Desktop

Amazon WorkSpaces offers a cloud desktop service (personal desktop) for Windows or Linux desktop operating systems. On Amazon WorkSpaces, Windows desktop bundles are provided as Microsoft Windows 7 or Windows 10 desktop experiences, powered by Windows Server 2008 R2 and Windows Server 2016, respectively. Or you can import Windows 7, Windows 10 Enterprise, or Windows 10 Pro desktop images to your WorkSpaces if licenced with Microsoft.

The images you imported to Amazon WorkSpaces can only be migrated to Windows Virtual Desktop. For migrating from Amazon WorkSpaces, you may need to move identities, user data, and golden images (imported images) to Azure and use them in Windows Virtual Desktop.


Amazon Workspaces
On-premises
Microsoft Azure
Amazon Workspaces
VDI instances on Amazon WorkSpaces
Export Amazon WorkSpace VM
Imported VM
Generalized VM
3
Azure Blob
4
Windows Virtual Desktop
Microsoft-managed Azure services
Web access
Diagnostics
Gateway
Broker
Azure SQL DB
SQL
Windows 10 Enterprise multi-session
Customer-managed Azure VMs & service
Host Pool 1
Host Pool 2
Host Pool 3
2
amazonWorkDocs
OR
OneDrive
amazonWorkDocs
OR
OneDrive
1
Active Directory
Active Directory
Azure AD
1 Migrate user identities from Amazon WorkSpaces
2 Move user data using Amazon WorkDocs or OneDrive
3 Export and generalize WorkSpace VM and upload to Azure Blob
4 Configure Windows Virtual Desktop and redirect users to Windows Virtual Desktop

Here are the steps for migrating your Amazon WorkSpaces to Windows Virtual Desktop.

Active Directory migration. Amazon WorkSpaces uses a directory to store and manage information for your WorkSpaces and users. To export or sync identities from AWS Directory Service to Azure Active Directory, choose from the following options:

1. **Natively using AWS Directory Service.** If you're using AWS Directory Service for Amazon WorkSpaces, you can either export the identities to Azure Active Directory or manually create the user identities on Azure Active Directory. To migrate or export AWS Managed Microsoft Active Directory, use ADMT or CSVDE.
2. **Hybrid identity with on-premises Active Directory.** If you're using an existing on-premises Microsoft Active Directory for users to sign in to their WorkSpaces through Azure AD Connect, you can configure a similar hybrid identity scenario. To do this, use your on-premises Active Directory synchronization with Azure Active Directory for common user identity. For more information, see What is hybrid identity?

Migrate user data. In Amazon WorkSpaces, users either choose a local data storage option or Amazon WorkDocs Drive to stream their data on demand. To migrate this data, you can choose the best option for your scenario from the following:

1. **Amazon WorkDocs sync for data export.** If your users are using Amazon WorkDocs to sync their folders on Amazon WorkSpaces to Amazon WorkDocs Drive, you can use the same Amazon WorkDocs Sync Client to sync or export data to the Windows Virtual Desktop session host (personal desktop). For more information, see Using Amazon WorkDocs Sync Client.
2. **Use Microsoft OneDrive to export user data.** If your users are saving data to local storage on Amazon WorkSpaces, you can install the OneDrive client to sync data to Azure. Once migrated to Windows Virtual Desktop, the same OneDrive client can be installed to sync user data to the Windows Virtual Desktop session host (personal desktop). The Office 365 E3 or E5 plans you use with Windows Virtual Desktop include 1 TB of OneDrive file storage. For more information, see Sync files with the OneDrive sync client in Windows.

Windows image migration. To migrate your Amazon WorkSpaces virtual machines, you should export them as virtual hard disks and then upload them to Azure. To do this, follow these steps:

1. **Export instance from Amazon Web Services.**
    a. To export the EC2 instance from Amazon Web Services, you need to use VM Import/Export.
    Note: If you've previously used VM Import to import a virtual machine into Amazon EC2, then only you can export that EC2 instance.
    b. To export your instance, use the create-instance-export-task command. For more information, see Exporting an Instance as a VM Using VM Import/Export.

2. **Prepare virtual hard disk to upload to Azure.** Before you upload a Windows virtual machine from on-premises to Azure, you must prepare the virtual hard disk (VHD or VHDX).
   Note: Azure supports only first-generation virtual machines that are in the virtual hard disk file format and have a fixed-sized disk. For more information, see Prepare a Windows VHD or VHDX to upload to Azure.
3. **Generalize virtual hard disk to be uploaded on Azure.** For more information, see Create a managed image of a generalized VM in Azure.
4. **Upload a generalized virtual hard disk to Azure Storage.** For more information, see Upload a generalized VHD and use it to create new VMs in Azure.

Configure Windows Virtual Desktop. Once you've successfully uploaded your virtual hard disk to Azure Storage, you can use this image for configuring your Windows Virtual Desktop host pool. Here's how:

1. **Create Windows Virtual Desktop tenant and host pool.** Use the uploaded Windows image to create a Windows Virtual Desktop host pool. Or create multi-session host pools for users using Windows 10 multi-session or Windows Server images provided with Windows Virtual Desktop. See the earlier Deploy and configure Windows Virtual Desktop for migration section for more information on verifying or creating Windows Virtual Desktop tenant and host pools.
2. **Redirect users to Windows Virtual Desktop.** After you create your Windows Virtual Desktop infrastructure, you can deploy Windows Virtual Desktop clients. With these, your users can access remote desktop and apps hosted on Windows Virtual Desktop.

Optimize Windows Virtual Desktop resources on Azure

Azure helps you govern and manage your Windows Virtual Desktop resources and costs. While using Azure services, you can consistently optimize cloud experience to improve performance, maximize ROI, and stay compliant with organizational standards—all in Azure.

- **Analyze cloud spending.** With Azure built-in cost management services, you get recommendations for your remote desktop service virtual machine instances—such as right-sizing over-utilized virtual machines and up-sizing as needed to ensure performance SLAs. For more information, see Explore and analyze costs with cost analysis.
- **Lower cost of ownership.** For customers with Software Assurance, Azure Hybrid Benefit for Windows Server lets you use on-premises Windows Server licenses and run Windows virtual machines on Azure at a reduced cost. When you combine the cost savings gained from Azure Reserved Instances with the added value of the Azure Hybrid Benefit, you can save up to 80 percent. For more information, see Azure Hybrid Benefit and Azure Reserved VM Instances (RIs).

Secure and manage your Windows Virtual Desktop

Azure is built on a foundation of trust and security, compliance, privacy, and transparency. Azure provides a secure platform to host your infrastructure with built-in security controls and capabilities, helping you further protect your data and applications.

Here are some of the ways you can take advantage of Azure:

Keep your resources safe with Azure Security Center. Azure Security Center provides unified security management and advanced threat protection across your remote desktop service and Windows Virtual Desktop workloads, whether these are hosted on-premises or in Azure. For more information, see What is Azure Security Center?

Monitor your cloud health with Azure tools. As with any system, monitoring is important for driving both proactive and reactive analysis. Azure provides several monitoring services targeted at applications, workloads, and core service health. These services ensure you have full visibility into current status and access to important data when working with break-fix situations. In Azure, you can use utilize either basic or premium monitoring services.

- Azure Monitor. Enables full observability into your applications, infrastructure, and network. Offers sophisticated tools for collecting and analysing telemetry, allowing you to maximize the performance and availability of your cloud and on-premises resources and applications. In addition, Azure Monitor now includes Log Analytics and Application Insights.
- Azure Service Health. Identifies any issues with Azure services that might impact availability of your services. Service Health also helps you plan for scheduled maintenance.
- Azure Advisor. Constantly monitors your Windows Virtual Desktop resource configuration and usage telemetry. Provides personalized recommendations based on best practices.
- Network Watcher. Offers insight into your Azure Virtual Network to diagnose problems with traffic filtering and routing, and to monitor connections.

Learn more

Want further information about Windows Virtual Desktop? Check out these resources:

Visit the product page and get started.

Read the announcement from Microsoft Azure and Microsoft 365.

Watch Windows Virtual Desktop be introduced at the 2018 Microsoft Ignite.

View the Windows Virtual Desktop Dive deep dive at the 2018 Microsoft Ignite.