

E-book series

Insight[®]

Microsoft
Azure

Quickstart Guide to

Windows Virtual Desktop

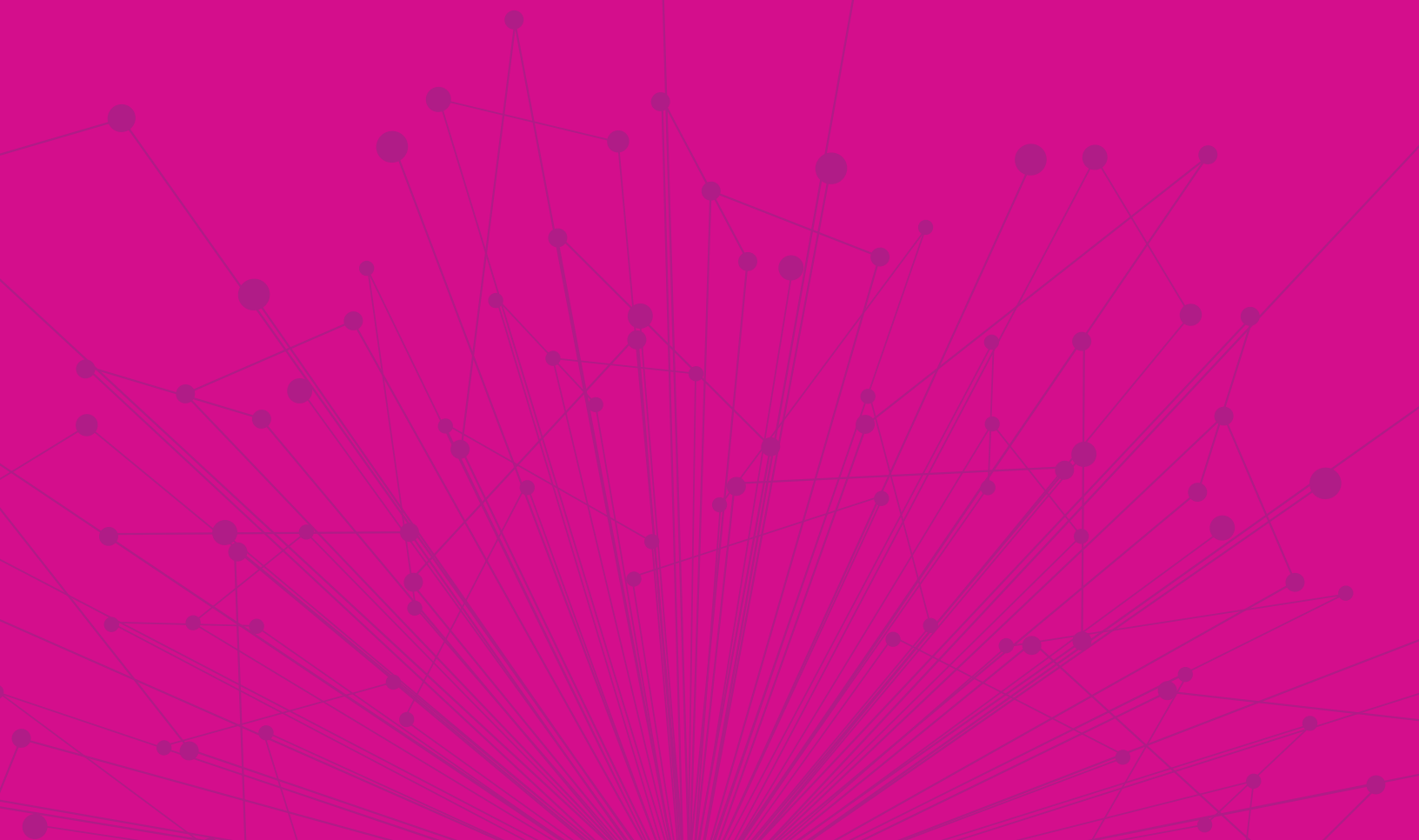


Table of contents

Section 1:

Introduction to Windows Virtual Desktop

Introduction	4
Virtual desktop infrastructure	4
What is Windows Virtual Desktop?	5
Business benefits of Windows Virtual Desktop	7

Section 2:

Windows Virtual Desktop deployment and prerequisites

How do you successfully deploy Windows Virtual Desktop?	11
Phase 1: Plan for Windows Virtual Desktop deployment	13
Phase 2: Prepare a Windows Virtual Desktop environment	17
Phase 3: Deploy the Windows Virtual Desktop workspace	19

Section 3:

Windows Virtual Desktop optimization

Phase 4: Optimize your Windows Virtual Desktop environments—recommendations and best practices	30
Security capabilities and best practices for Windows Virtual Desktop	33
Troubleshooting tips	36

Section 4

Conclusion

Summary and resources	39
Glossary	40



Section 1:

Introduction to Windows Virtual Desktop

Introduction

In today's environment, it's vital for businesses to implement remote working strategies for their teams, while enhancing security, reducing infrastructure costs, and simplifying IT management. Windows Virtual Desktop enables users to continue to work from any location using the latest desktop and application virtualization cloud technology, empowering companies to provide a secure, productive experience in an ever-changing world.

To help prepare you for successful Windows Virtual Desktop deployment, this e-book shares the essentials of desktop virtualization, the unique benefits of Windows Virtual Desktop will bring to your organization, and scenarios that will help you meet your business needs.

We will then explain how to deploy Windows Virtual Desktop and share some best practices to help you optimize your deployment.

We hope you enjoy your tour of Windows Virtual Desktop. After reading this e-book, you will be prepared to embark on your Windows Virtual Desktop journey! If you have any questions about the technical requirements or need advice on short- and long-term solutions for enabling remote work, you can talk to an [Azure sales specialist](#).

Virtual desktop infrastructure

Virtual desktop infrastructure (VDI) refers to the use of virtualization and virtual machines to provide and manage virtual desktops. Users can access these virtual machines remotely from supported devices and remote locations, and all the processing is completed on the host server. Users typically connect to their desktop instances through a connection broker. This broker is essentially a software layer that acts as the intermediary between the user and server, enabling the orchestration of sessions to virtual desktops or published applications. VDI is usually deployed in an organization's datacenter and managed by their IT department. Typical on-premises providers include Citrix, VMware, and Microsoft (Remote Desktop Services). VDI can be hosted on-premises or in the cloud. Cloud-based VDI can offer reduced infrastructure investments with all the core benefits that the cloud provides.

What is Windows Virtual Desktop?

Windows Virtual Desktop is a desktop and app virtualization service that runs on Microsoft Azure. Windows Virtual Desktop can be accessed from any device—Windows, Mac, iOS, Android, and Linux—with applications that you can use to access remote desktops and applications, including multi-session Windows 10 and Microsoft 365 Apps for enterprise. You can also use most modern browsers to access Windows Virtual Desktop–hosted experiences.

Typically, Windows Virtual Desktop is easier to deploy and manage than traditional Remote Desktop Services (RDS) or VDI environments. You don't have to provision and manage servers and server roles such as the gateway, connection broker, diagnostics, load balancing, and licensing.

Figure 1 depicts a simple example of a Windows Virtual Desktop workspace with two host pools. Host pool A has two application groups: Desktop and RemoteApp. These resources are shared (pooled) across the sales team. Host pool B has a Desktop application group with personal desktops for an engineering team:

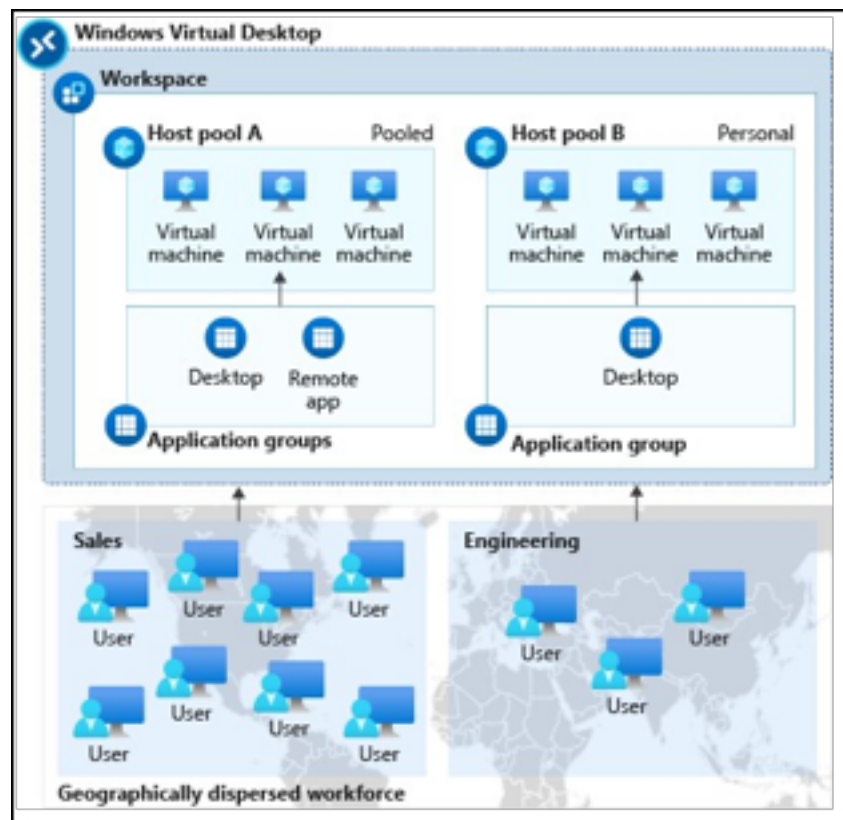


Figure 1: Windows Virtual Desktop workspace with two host pools

Building on this simple example, here is a typical enterprise deployment of Windows Virtual Desktop that provides an insight into its overall architecture and deployment capabilities. As you will also note, there are multiple subscriptions in use, as well as virtual network peering and a VPN to the customer's on-premises network:

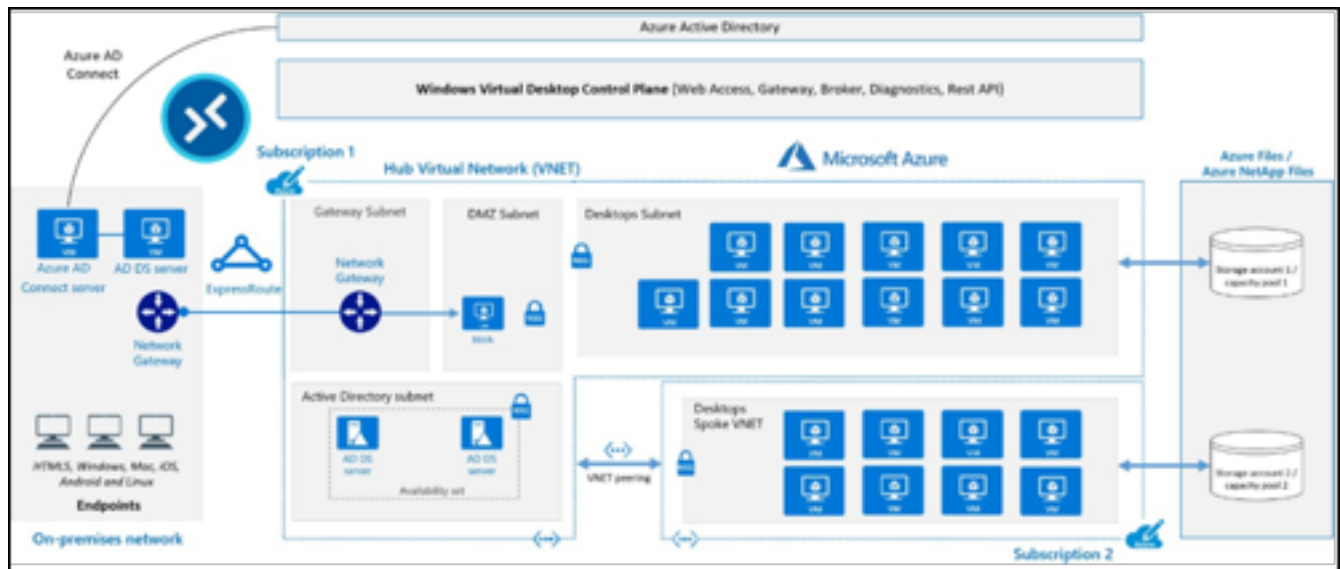


Figure 2: A typical architectural setup for Windows Virtual Desktop

In summary, Windows Virtual Desktop provides a managed VDI that is easy to manage, secure, cost-effective, and offers a seamless experience that is comparable to a laptop or local desktop. In the upcoming sections, we'll talk more about the benefits Windows Virtual Desktop brings to your business, and then dive into deployment prerequisites.

While the guidance in this e-book focuses on native VDI deployment, Windows Virtual Desktop is also integrated into partner solutions such as Citrix and VMware, making it easy to modernize your existing VDI investments. [Learn more](#) about Windows Virtual Desktop partner integrations.

Business benefits of Windows Virtual Desktop

There are many benefits that Windows Virtual Desktop will bring to your organization. Let's have a look at a few of these benefits in detail.

Provide the best user experience

- Windows Virtual Desktop provides full Windows 10 and Windows Server desktop, and application virtualization, including seamless integration with Microsoft Teams and Microsoft 365 Apps for enterprise, helping users to be productive and stay connected with the desktop experience that they're used to.
- Some organizations are concerned about cloud application latency. Azure supports over 60 regions worldwide (the most compared to any cloud provider), meaning that you can get a desktop close to any user's location and establish a fast connection. This enables users to stay productive and mitigate long load times.
- Additionally, user sign-in to Windows Virtual Desktop is extremely fast because user profiles are containerized by using FSLogix. At sign-in, the user profile container is dynamically attached to the computing environment. The user profile is immediately available and appears on the system exactly like a typical native user profile.

Improve your security posture

- Windows Virtual Desktop includes many features that help keep applications and data secure. For example, the data and applications are separated from the local hardware and are run on the remote server, reducing the risk of confidential data being left on a personal device. It also isolates user sessions in both single and multi-session environments. This provides better security than a VPN because it doesn't give users access to a full subnet.
- Windows Virtual Desktop also improves security by using reverse connect (RC) technology, which is a more secure connection type as compared to the traditional Remote Desktop Protocol (RDP). It is not necessary to open the inbound ports to the session host VMs, as this is not required when using Windows Virtual Desktop.

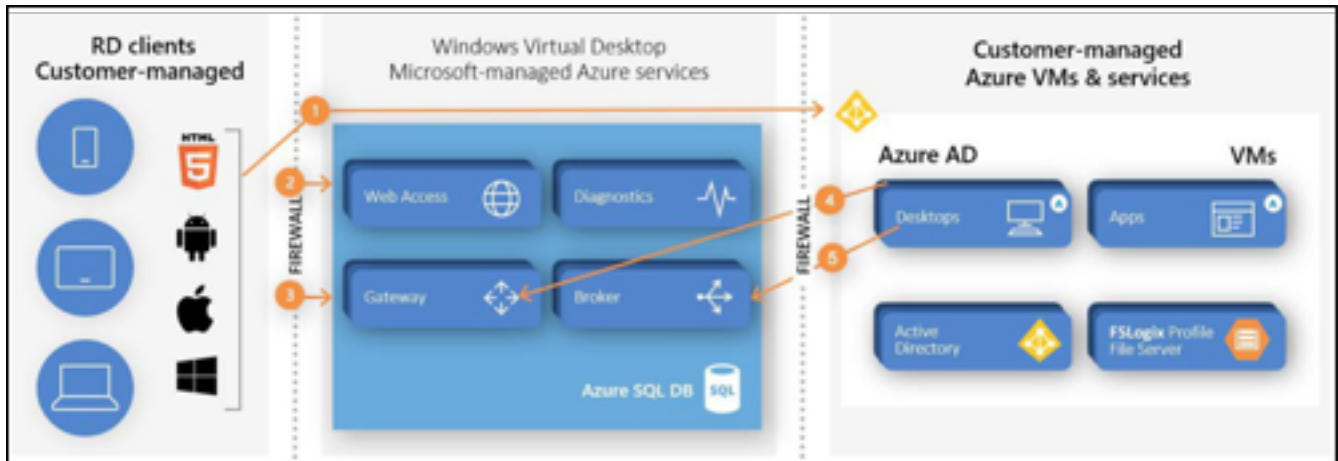


Figure 3: The connection flow process of Windows Virtual Desktop

- As an Azure Service, Windows Virtual Desktop uses industry-leading security and compliance offering to protect user data, including solutions such as Azure Security Center and Microsoft Endpoint Manager. This helps to protect your infrastructure, and Azure Active Directory, which allows you to enable conditional access policies and role-based access control. You can read more about security best practices for Windows Virtual Desktop [here](#).

Simplify deployment and management

- Since Windows Virtual Desktop manages the entire VDI for you, you can focus on the user, the apps, and the operating system images you need to use, instead of hardware inventory and maintenance.
- With the features of the cloud, you'll be able to quickly and securely get your users up and running, with limitless scale and full automation that you control based on your business needs. For example, you can automate VM deployments by using the Azure portal or an Azure Resource Manager (ARM) template, and easily scale by adding any number of hosts to the host pool. Windows Virtual Desktop also provides tools to automatically provision additional VMs when an incoming demand exceeds a specified threshold.
- With Windows Virtual Desktop, you'll have access to other monitoring services, such as Azure Monitor, which allows admins to identify issues and get alerted through a single interface; and Azure Service Health, which provides personalized guidance to help mitigate downtime and prepare for planned maintenance.

Reduce the costs of licensing and infrastructure

- Upgrading and refreshing infrastructure can be expensive. With Windows Virtual Desktop, you can reduce large capital expenditure and infrastructure costs by taking advantage of cloud-based capabilities, paying only for what you use. Learn more about pricing and licensing eligibility [here](#).
- The unique Windows 10 multi-session capability enables multiple concurrent users, maximizing your VM utilization. You also have the flexibility to choose the VM you want to use and tune it how you would like to meet your business and budget needs.
- Purchasing a one-year or three-year Azure Reserved VM Instance (RI) term on Windows and Linux VMs could save you up to 72 percent versus pay-as-you-go pricing. You can read more about Azure RIs [here](#).

In summary, Windows Virtual Desktop will bring numerous benefits to your business, including enabling more secure remote work for your end users, quick deployment and simplified IT management, and reduced licensing and infrastructure costs.

See [customer stories](#) to get real-life examples of how others have used Windows Virtual Desktop to help their business.

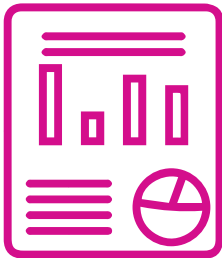


Section 2:

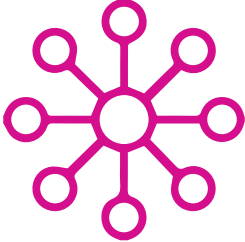
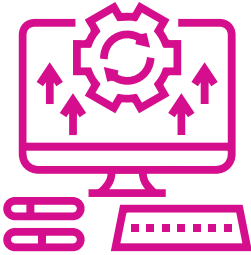
Windows Virtual Desktop deployment and prerequisites

How do you successfully deploy Windows Virtual Desktop?

There are four areas of a Windows Virtual Desktop deployment: plan, prepare, deploy, and optimize. The following table provides a high-level view of the key steps for each phase:

Windows Virtual Desktop Deployment Checklist	
Phase	Steps
 Plan	<p>The following steps should be completed in the Plan section before you deploy Windows Virtual Desktop:</p> <ul style="list-style-type: none">▪ Networking considerations▪ Number of VMs, including limits and sizing▪ Image types▪ Domain joining▪ Application groups▪ Device clients
 Prepare	<p>The following steps should be completed in the Prepare section before you deploy Windows Virtual Desktop:</p> <ul style="list-style-type: none">▪ Set up Azure Active Directory (Azure AD).▪ Integrate with Active Directory Domain Services.▪ Create Azure resources.▪ Assign administrator roles.▪ Assign licenses to Windows Virtual Desktop users.▪ Register the DesktopVirtualization provider with your subscription.

Windows Virtual Desktop Deployment Checklist

Phase	Steps
 Deploy	<p>The following steps should be completed during the Deploy section of the process before moving on to the fourth step:</p> <ul style="list-style-type: none">▪ Create a Windows Virtual Desktop workspace and host pool.▪ Make the desktop and remote apps available to users by using application groups.▪ Customize the workspace, apps, desktop, and protocol.▪ Connect to the workspace by using the Windows Virtual Desktop client.
 Optimize	<p>The final phase, Optimize, lists the configuration of FSLogix, Azure files and Azure automation, if required:</p> <ul style="list-style-type: none">▪ Set up roaming and stateful user profiles by using Azure File Storage and FSLogix.▪ Configure Azure Files Sync to sync on-premises files or user profile data to Azure Storage.▪ Scale session hosts by using the scaling tool built on Azure Automation and Azure Logic Apps.

In Section 2 of this e-book, we'll go through the plan, prepare, and deployment prerequisites and key steps in more detail. In Section 3, we'll move on to best practices and troubleshooting tips to help with the optimize phase.

Phase 1: Plan for Windows Virtual Desktop deployment

To plan for the deployment, you'll need to review some of the key requirements for designing a Windows Virtual Desktop deployment. You can find an overview of these requirements [here](#). We'll go through a few tips to help you along the way.

Tip 1: Before you can deploy any VMs, you need to set up a network

Select the virtual network and subnet where you want to put the VMs you create. The virtual network you specify for the host pool provisioning process must be connected to the organization's domain, and the Azure virtual network must allow outbound access to the URLs that support Windows Virtual Desktop.

You'll also need to join the VMs inside the virtual network to the domain, on a different virtual network using peering or a different network as long as the hosts can communicate with the domain controller.

If you're using Azure Active Directory Domain Services (Azure AD DS), it's suggested that an Azure AD DS-managed domain is deployed into its own dedicated subnet. It is also advised not to deploy your VM in the same subnet as your Azure AD DS-managed domain. To deploy your VM and connect to an appropriate virtual network subnet, select one of the following options:

- Create or select an existing subnet in the same virtual network as your Azure AD DS-managed domain is deployed.
- Select a subnet in an Azure virtual network that is connected to it using Azure virtual network peering.

IMPORTANT

Ensure that you have configured DNS correctly because if the session hosts cannot see the domain controller (DC), the provisioning process will fail on the next step. You should ensure that the virtual network is configured with Active Directory as a DNS server.

Tip 2: Ensure you've set up firewall and other network requirements

Windows Virtual Desktop requires a specific set of firewall rules to function correctly. Failing to ensure these rules are applied to the VM, Azure Firewall, or a third-party firewall could lead to networking communication issues with Windows Virtual Desktop. One example of this is Windows Activation failing because the outbound port TCP 1688 for kms.core.windows.net is blocked.

[Learn more](#) about the required firewall rules.

Tip 3: Ensure you've got the right number and size of VMs you need to support your business requirements

Number of VMS

You can create up to 159 VMs when you first create your host pool. You can see them in your resource group, including some additional ARM objects. There is a hard limit of 10,000 VMs per host pool. However, it is recommended to limit a host pool to 5,000 VMs. These session hosts can be active in different subscriptions. There is a 399 VMs maximum host pool enrolment limitation without availability sets being used, and a hard limit of 400 host pools per tenant.

You can quickly reach the 800 Azure resources per deployment limit. You can also add more VMs after you finish creating your host pool. Check the Azure VM and API limits for your resource group and subscription.

For recommendations in the design phase to avoid having to make changes in the scaling phase, see [Azure limitations](#).

VM sizing

For single-session scenarios, it is recommended that there are at least two physical CPU cores per VM. It is recommended to check with your application software vendor(s) to get sizing recommendations that are specific to your workload. VM sizing for single-session VMs likely align with physical device guidelines.

For multi-session VM sizing recommendations, see [Virtual machine sizing guidelines](#).

Tip 4: Select your required image type

Azure uses two image types to create VMs, Gallery and Storage blob. You'll also need to choose what kind of operating system disks you want your VMs to use: Standard SSD, Premium SSD, or Standard HDD.

Image Type	Description
Gallery	With the Gallery image type, you can select one of the recommended images from the drop-down menu, such as Windows 10 Enterprise multi-session and Microsoft 365. If you don't see the image you want, select Browse all images and disks. This lets you select another Azure Managed Image in your gallery (My Items) or a Shared image from the Shared Image Gallery. It is also possible to use one image provided by Microsoft and other publishers (Marketplace).
Storage blob	The Storage blob image type enables you to use your own image built through Hyper-V or on an Azure VM. You can use this option when you have an image that you're using on-premises and want to upload it and start using it in Azure immediately. When you select this option, there are some additional fields you need to complete.

Tip 5: Ensure that you prepare for domain join VMs

To domain join the VMs you create, you need to specify the full Active Directory domain name to join, such as northwindtraders.com. If you've set up a test environment with Azure AD DS, use the DNS domain name that's on the properties page for Azure AD DS, such as adds-northwindtraders.onmicrosoft.com.

You will also need to specify an Administrator account so the provisioning process can join the VMs to the domain. This account must be assigned to the Active Directory domain administrator role.

Tip 6: Assign the required application groups

You can assign a user or group to both a remote desktop application group and a RemoteApp application group in the same host pool. However, users can only launch one type of application group per session.

If a user or group is assigned to multiple RemoteApp application groups within the same host pool, they'll see all the applications published to those application groups. It is recommended to split RemoteApp and Remote Desktop workloads to separate host pools where possible.

Tip 7: Decide how you want to connect to a workspace with a web or desktop client

You can access a Windows Virtual Desktop workspace either from a web browser or by using a client on your device. The browser option enables you to connect using any device when you need to access a desktop and don't have your primary device with you. For the best experience, it is recommended that you run the Windows Virtual Desktop client directly from your device. The following list of client device types support Windows Virtual Desktop:

- Windows
- Android
- macOS
- iOS
- Linux, provided by Linux thin client partners; [read more here](#)

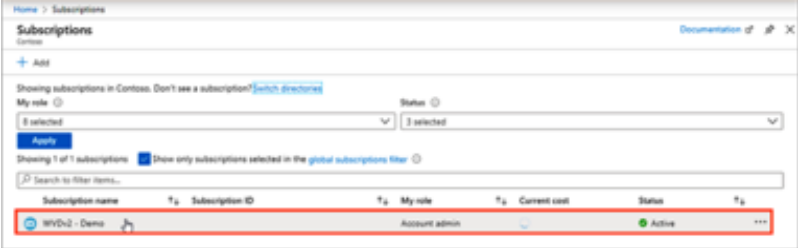
Phase 2: Prepare a Windows Virtual Desktop environment

To prepare for deployment, you'll need to make sure you have the right licensing, an Azure subscription, and the correct Azure Active Directory and VM configuration. The following table steps through these requirements.

Resources	Requirements
Licenses and subscriptions	<ul style="list-style-type: none">▪ Access Windows Virtual Desktop for free with an eligible^[1] Windows license, M365 license, or RDS Client Access License (CAL) with Software Assurance, depending on the operating system you want to deploy.▪ You must also have an Azure subscription^[2] that contains a virtual network that either contains or is connected to the Windows Server Active Directory or Azure AD DS instance. This subscription must also be parented to the same Azure AD tenant. If you need an Azure subscription, you can sign up for a free trial. If you're using the free trial version of Azure, you should use Azure AD DS to keep your Windows Server Active Directory in sync with Azure AD.▪ Assign Users for Windows Virtual Desktop.
Create Azure resources	<ul style="list-style-type: none">▪ Create the Azure network.▪ Configure connectivity to Active Directory via a VPN, local host, or using▪ Azure virtual network peering.

[1] More information on eligible licenses at <https://azure.microsoft.com/pricing/details/virtual-desktop/>.

[2] Read about Azure subscriptions at <https://azure.microsoft.com/pricing/purchase-options/pay-as-you-go/>.

Resources	Requirements
Azure AD	<ul style="list-style-type: none"> ▪ An Azure AD ▪ A domain controller (DC) that's synced with Azure AD <p>You can configure this DC with one of the following:</p> <ul style="list-style-type: none"> ▪ The user must be sourced from the same Active Directory that's connected to Azure AD via Azure AD Connect. ▪ The UPN you use to subscribe to Windows Virtual Desktop must exist in the Active Directory domain the VM is joined to. ▪ Azure AD DS. ▪ A VM in Azure acting as a DC. ▪ An Azure subscription that contains a virtual network that either contains or is connected to the Windows Server Active Directory or AD DS. ▪ Assign administrator roles for Windows Virtual Desktop.
Virtual Machines (VMs)	<ul style="list-style-type: none"> ▪ VMs must be standard domain-joined or Hybrid AD-joined. VMs can't be Azure AD-joined. ▪ VMs must be running one of the supported operating system images.
User requirements	<p>Register the required subscription(s) with the Microsoft. DesktopVirtualization resource provider. Do this by going into the Azure Services subscription menu, finding the subscriptions you want to register, searching for the Microsoft.DesktopVirtualization provider, and clicking Register:</p> 

Once you've met the prerequisites in the plan and prepare section, you're ready to move on to the first step of deployment.

Phase 3: Deploy the Windows Virtual Desktop workspace

In this section, we'll provide a high-level overview of how to deploy your Windows Virtual Desktop workspace. You can also refer to step-by-step guidance on how to deploy your Windows Virtual Desktop workspace [here](#).

If you already have an Azure subscription, you can also try the [Windows Virtual Desktop quickstart deployment tool](#), which will guide you through each step of deployment using the Azure portal and your existing account subscription

Creating your first host pool (desktop)

There are two ways to deploy host pools in Windows Virtual Desktop: with or without adding VMs. In this section, both types of deployment will be covered. If you select the option to not add VMs, you will need to configure the session hosts manually so that the host agent can communicate with Windows Virtual Desktop. You can also use custom ARM templates to deploy and add session hosts to your existing host pool. This manual process is the same process for migrating Remote Desktop Services (server) session hosts to Windows Virtual Desktop.

Don't have an Azure subscription?
You can sign up for an Azure free account [here](#).

Creating your first host pool (desktop)—manual deployment

This section details the steps to add session hosts to Windows Virtual Desktop without using the provision feature when adding a host pool:

1. Search for Windows Virtual Desktop in the Azure search panel and select **Create a host pool**:

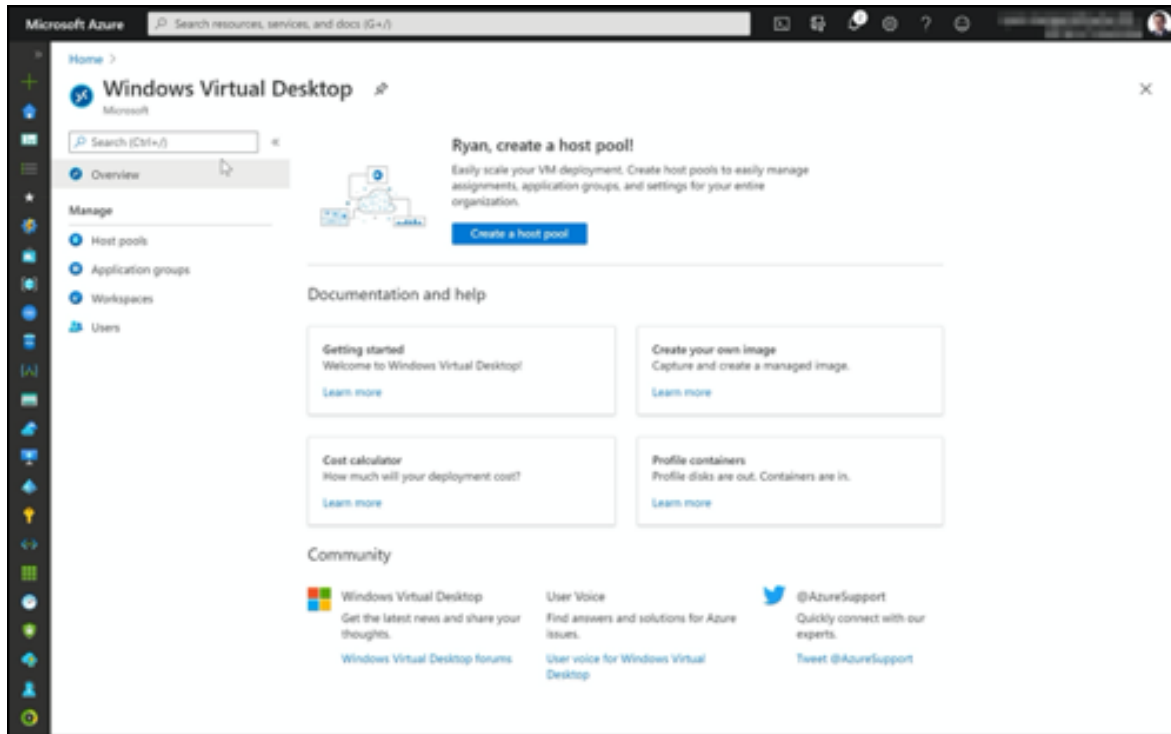


Figure 4: Creating a host pool

2. Select the subscription, metadata location, and **host pool properties**:

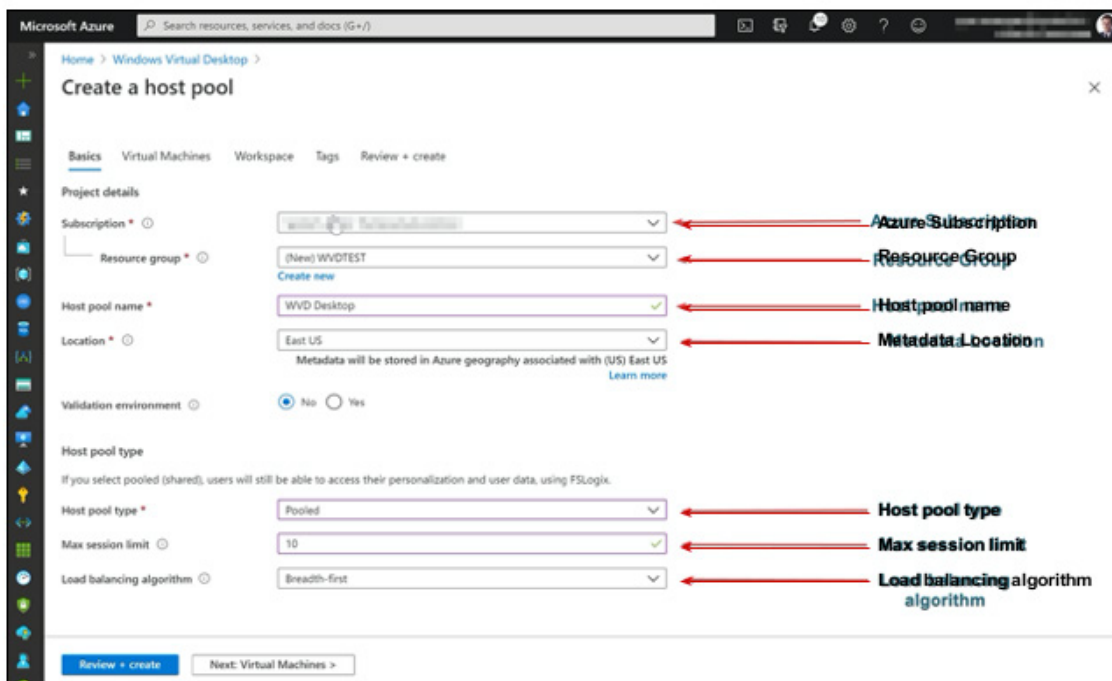


Figure 5: Configuring the host pool properties

Validation host pools are useful for testing changes that could result in downtime for your standard environment. [Learn more here.](#)

3. Select **Next Virtual Machines** and select **No** to add VMs. Next, select an existing workspace or create a new one, and finally, select **Review + create** and then select **Create**.

Once the deployment is complete, navigate to the Windows Virtual Desktop Service page in the ARM console:

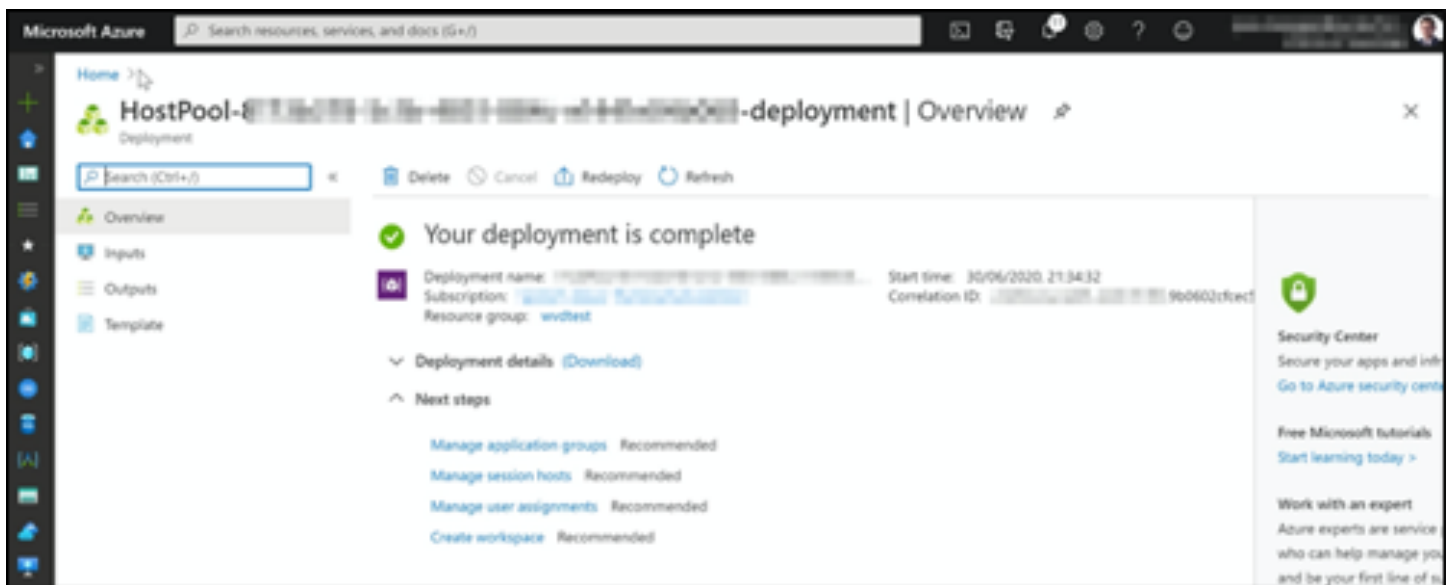


Figure 6: The deployment overview

Note that in order to add session hosts manually, you will need a registration key. This is optional and common in automation scenarios. Also, in order to register session hosts manually, you will need to download and install both the Windows Virtual Desktop Agent, which requires the registration key, and the Windows Virtual Desktop Agent Bootloader.

Find out more about [registering VMs to the Windows Virtual Desktop host pool.](#)

Creating your first host pool (desktop)—Adding VMs to a deployment

This section shows you how to deploy a Windows Virtual Desktop host pool and add VMs using the wizard:

1. Search for Windows Virtual Desktop service in the Azure search panel and select **Create a host pool**:

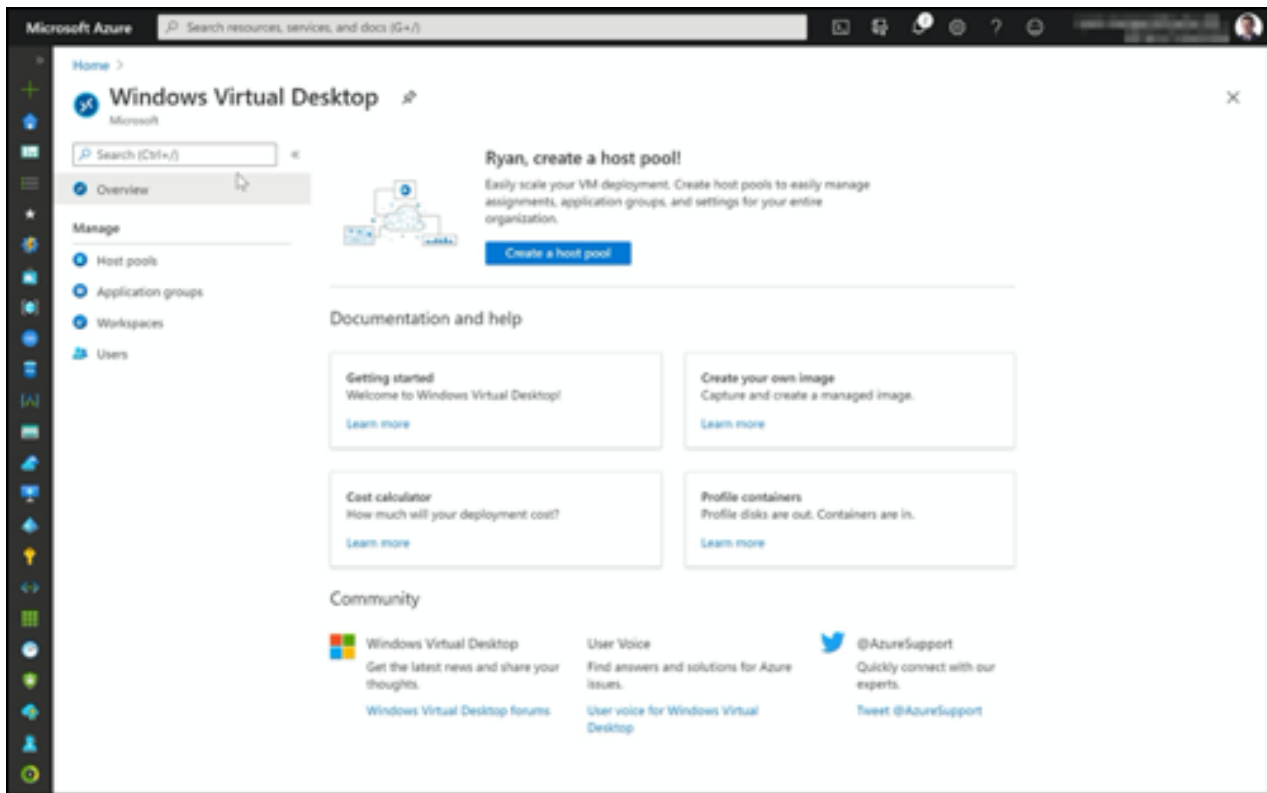


Figure 7: Create a new host pool

2. Select the subscription, metadata location, and host pool properties. If you're using Windows 10 single-session, ensure that you select the **Personal Host pool** type:

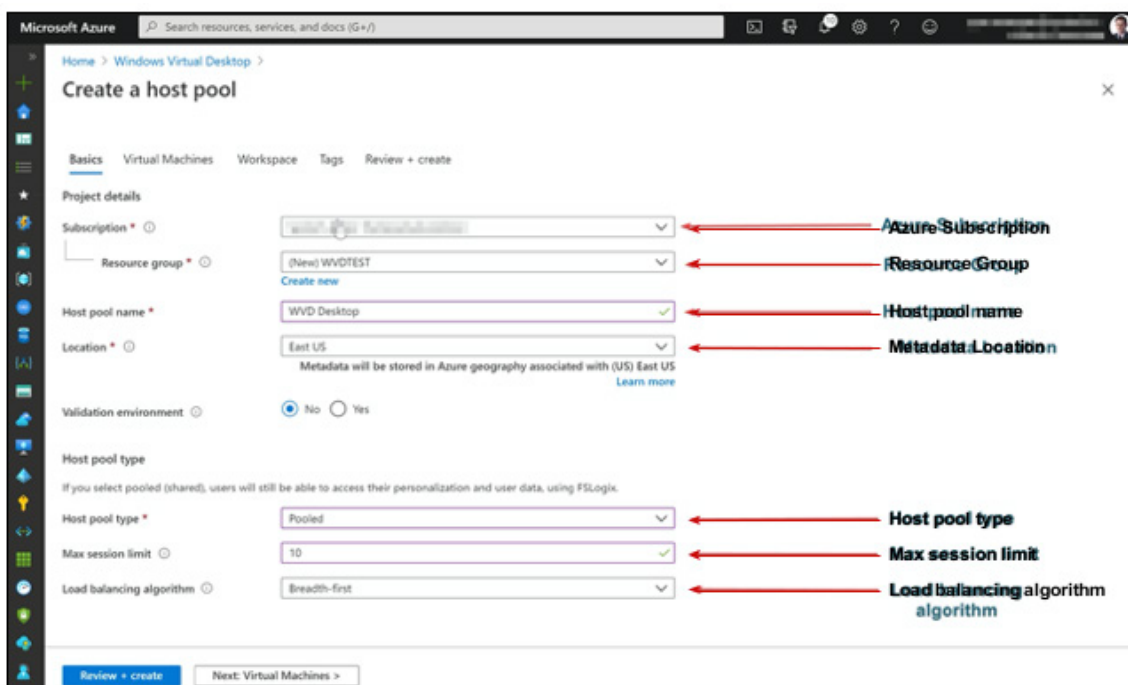


Figure 8: Configuring the host pool properties

3. Select **Add Virtual Machines**, then **Yes**, then complete the VM details, including the size and the image you would like to deploy. When you're finished, select **Review + create** and then **Create**:

The screenshot shows the 'Create a host pool' wizard in the Microsoft Azure portal, specifically the 'Virtual Machines' tab. The form is titled 'Create a host pool' and has tabs for 'Basics', 'Virtual Machines', 'Workspace', 'Tags', and 'Review + create'. Below the tabs, there is a description of host pools. The 'Add virtual machines' section has a radio button set to 'Yes'. The 'Resource group' is 'wvdtest', 'Virtual machine location' is 'UK South', 'Virtual machine size' is 'Standard D2s v3' (2 vCPUs, 8 GiB memory), 'Number of VMs' is '2', 'Name prefix' is 'WVDTEST', 'Image type' is 'Gallery', and 'Image' is 'Windows 10 Enterprise multi-session, Version 1909 + Microsoft 365 Apps'. Red arrows point to these fields with labels: 'Resource Group', 'Azure Data Center Region', 'Virtual Machine Size', 'Number of Session hosts per pool', 'Computer Account', and 'Marketplace image'. The 'OS disk type' is also visible but not labeled. The 'Review + create' button is at the bottom left.

Figure 9: Adding the VM and the VM details

IMPORTANT

Azure VM session host name prefixes can't exceed 11 characters due to the auto-assigning of instance names and the NetBIOS limit of 15 characters per computer account. When you have fewer than 999 VMs, the prefix can be one character longer; the same applies when you have fewer than 100 VMs.

4. Select an existing workspace or select Create new, then select **Review + create**:

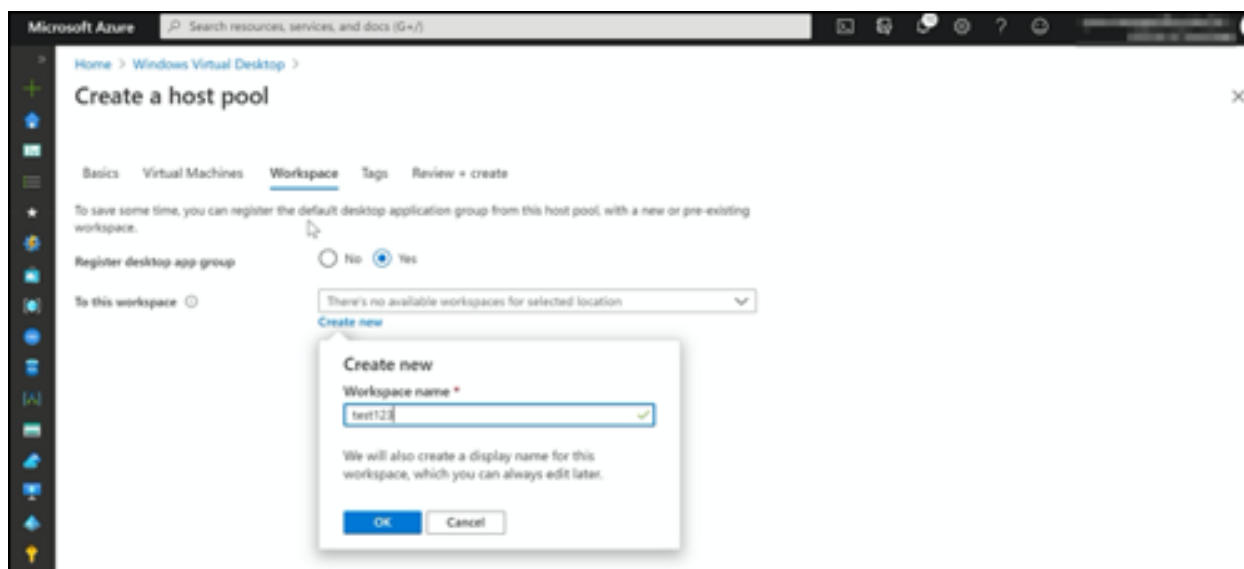


Figure 10: Creating a workspace and deployment

The final step is to assign a desktop application group to the user.

Creating your first host pool (desktop)—Creating and assigning remote applications

To enable the use of RemoteApp as your resource type, you first need to create an application group and select RemoteApp. If you would like to use both RemoteApp and desktops as one specific user, it's recommended that you create two host pools; however, only one is required. A Desktop Application Group (DAG) is automatically created when you create a host pool through the wizard. The default DAG is for desktops, and the following steps explain how to configure RemoteApps:

1. Navigate to the **Application groups** panel and select the host pool you want to configure the application group with:

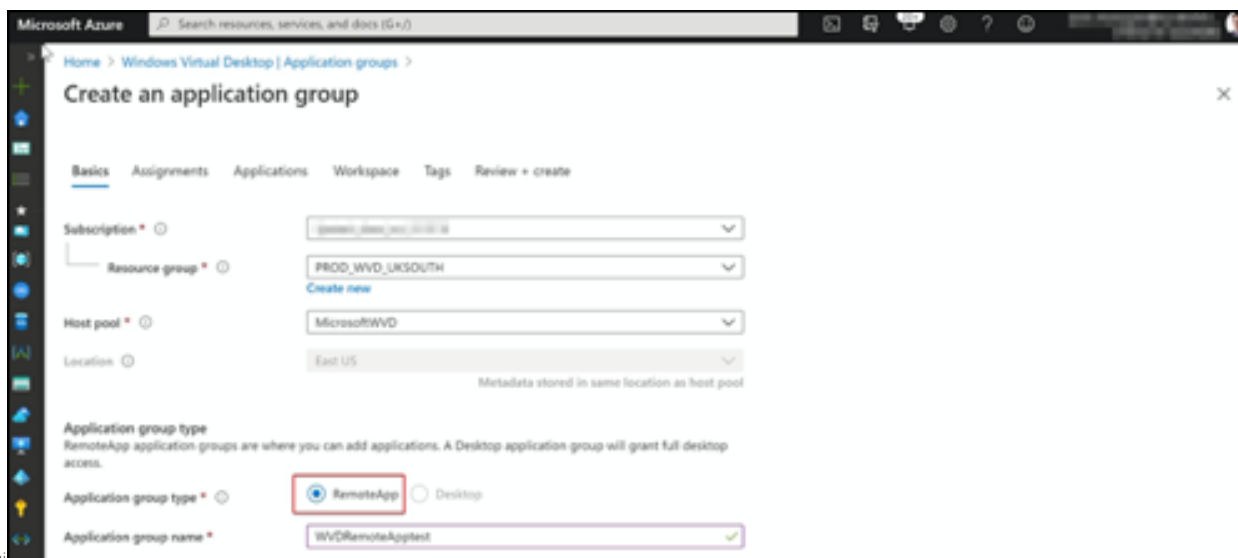


Figure 11: Configuring the application group and the host pool

2. Add the Azure AD users or groups to the application group:



Figure 12: Adding an Azure AD user to the application group

3. Add the remote applications you require. You can also deploy remote applications using the application source **File path**:

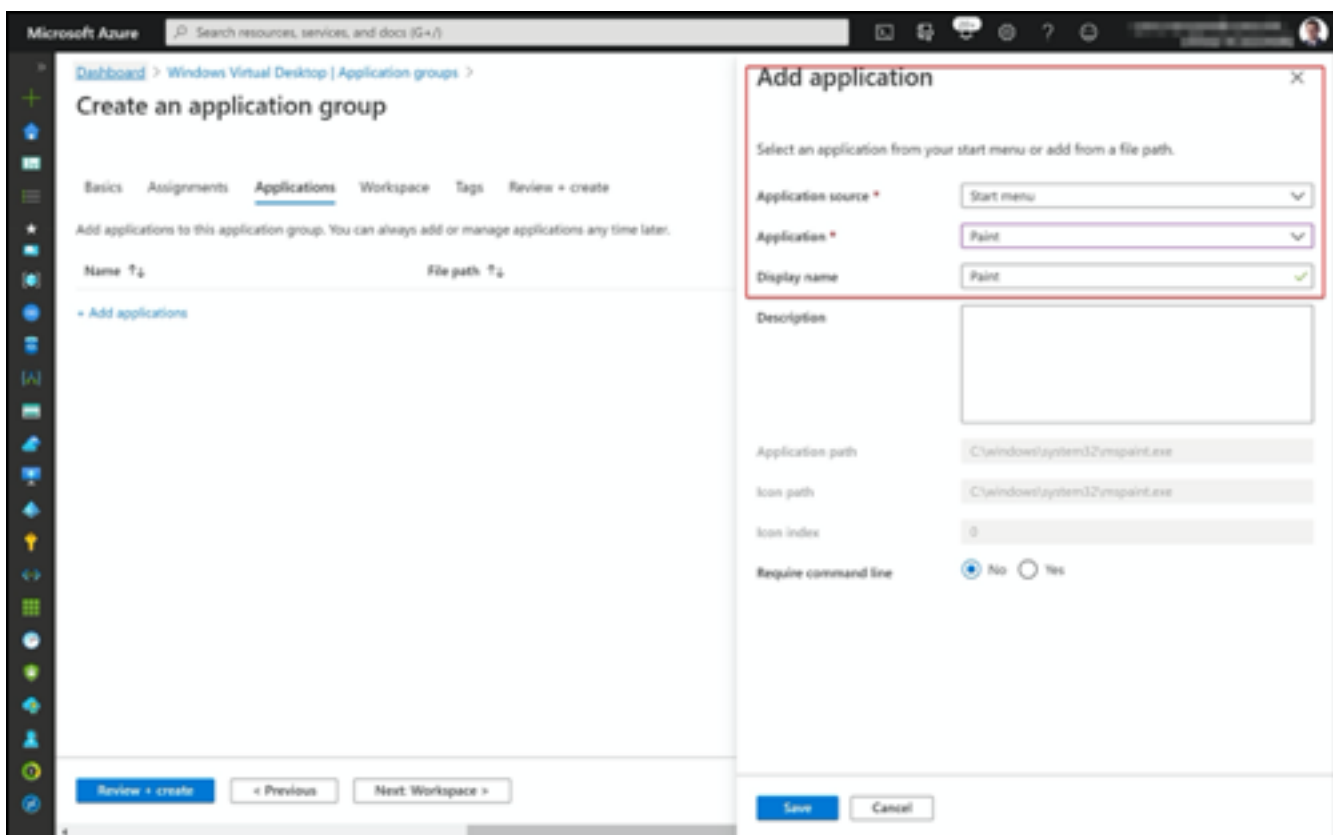


Figure 13: Adding remote applications

4. Register the application group with a workgroup:



Figure 14: Registering the application group

5. Select **Review + create** and then select **create**. When it's finished, you can add, edit, and remove applications from the application group as required:



Figure 15: Reviewing the applications

Getting started with the Windows Virtual Desktop client

To access Windows Virtual Desktop from the client/Start menu, you first need to download and install the Windows Virtual Desktop client.

[Click here](#) to download the Windows Virtual Desktop client.

1. Launch the Remote Desktop client by selecting **Remote Desktop**.

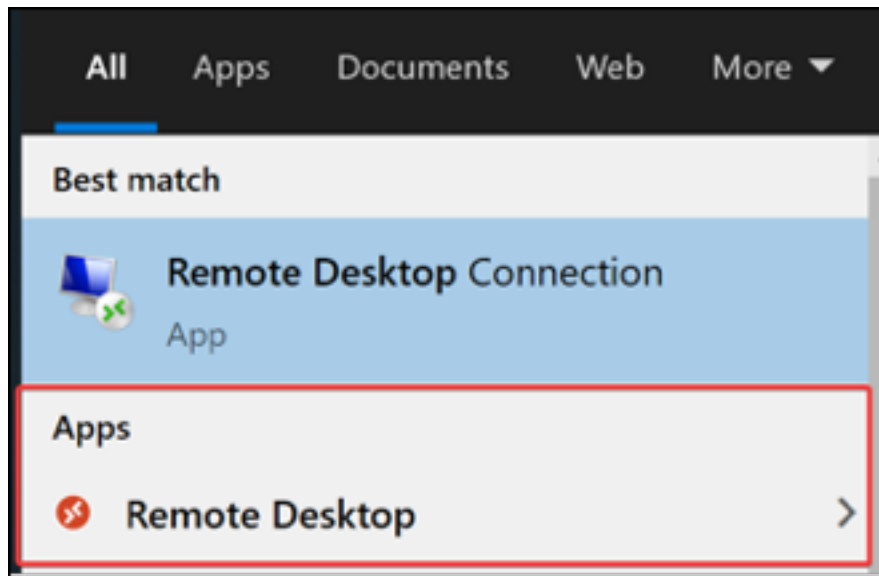


Figure 16: The Remote Desktop icon in the Start menu

2. Select **Subscribe with URL**:

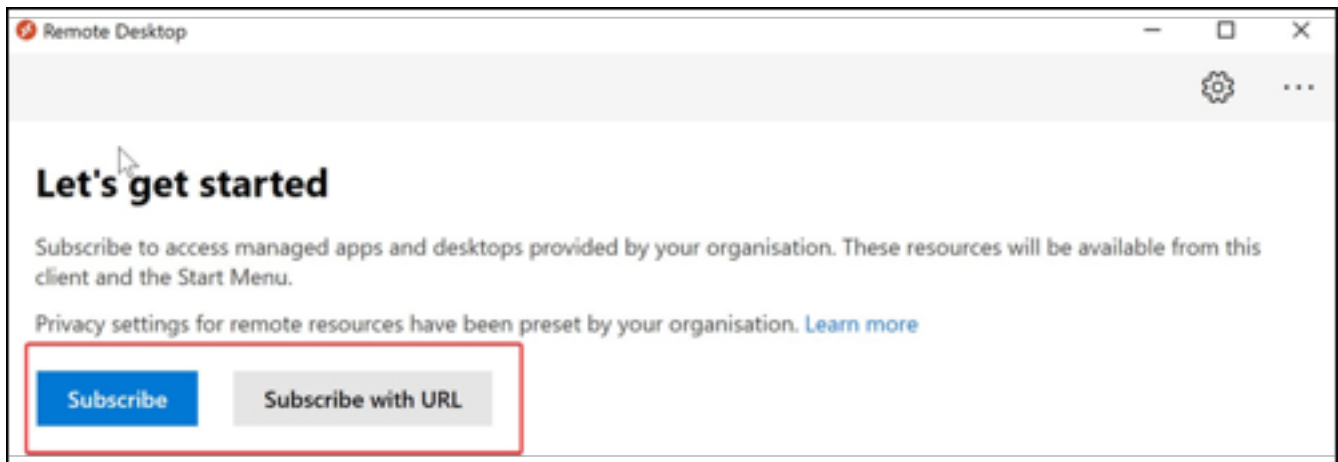


Figure 17: Choosing the option for subscription

3. Enter the Azure Resource Manager Feed,
<https://rdweb.wvd.microsoft.com/api/arm/feeddiscovery>:

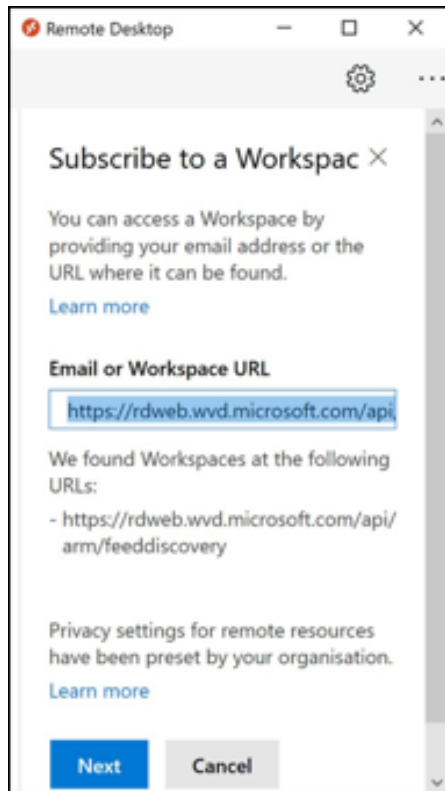


Figure 18: The Subscribe to a Workspace section

4. You will see a Microsoft authentication prompt appear. Enter your sign-in credentials.
5. Verify your identity if you're using Azure multifactor authentication (MFA).
Read more about MFA [here](#).
6. Your apps will and desktop resources will now appear in the Remote Desktop client:

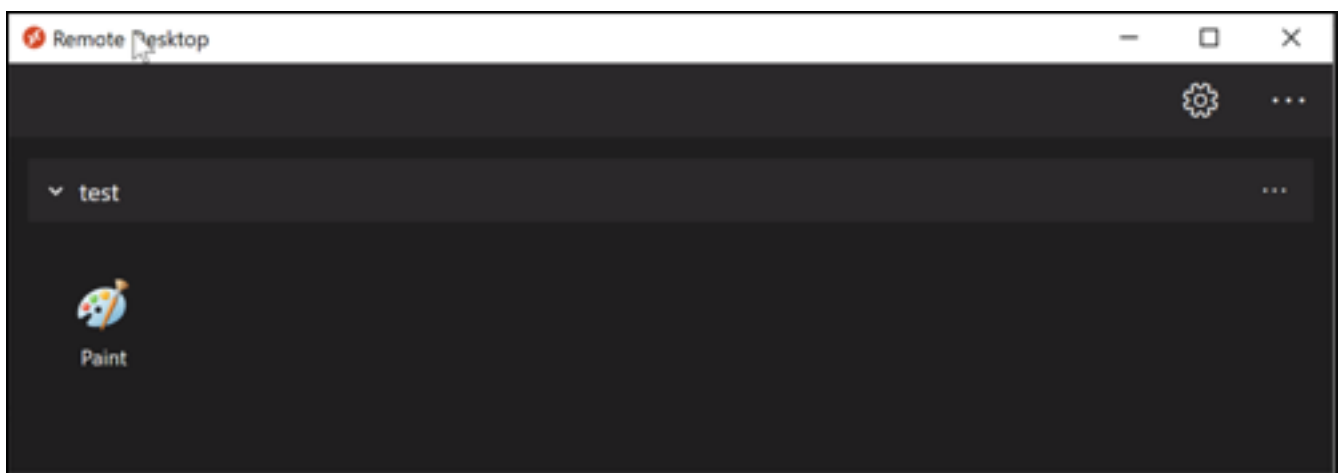


Figure 19: The Remote Desktop client



Section 3:

Windows Virtual Desktop optimization

Phase 4: Optimize your Windows Virtual Desktop environments—recommendations and best practices

After you deploy your Windows Virtual Desktop environment, there are several areas you can choose to optimize. This section provides best practices, recommendations, and troubleshooting tips you can use. Windows Virtual Desktop offers full control over the size, type, and count of VMs being used by customers.

These are some Windows Virtual Desktop general best practices:

- The Azure Files storage account should be in the same region as the session host VMs.
- Azure Files permissions should match those described in [Requirements—Profile Containers](#).
- Each host pool VM must be the same type and size and based on the same master image.
- Host pool VMs must be in the same resource group to aid management, scaling, and updating.
- For optimal performance, the storage solution and the FSLogix profile container should be in the same datacenter.
- The storage account containing the master image must be in the same region and subscription where the VMs are being provisioned.

Infrastructure strategies and VM recommendations

- For VM requirements to run the operating system, see [Virtual machine sizing guidelines](#).
- It is recommended that you use Premium SSD storage in your operating system disk for production workloads that require a service level agreement (SLA). For more details, see the [SLA for virtual machines](#).
- Graphics processing units (GPUs) are recommended for users who regularly use graphics-intensive programs, and non-graphics-intensive applications can also benefit from a GPU. To learn more about graphics acceleration, see [Choose your graphics rendering technology](#). Azure has several GPU deployment options and GPU VM sizes.

Learn more at [GPU optimized virtual machinesizes](#).

VM sizing recommendations for single- and multi-session VMs

Please note that these sizing recommendations are a guideline, and it is recommended that an assessment is carried out to ensure the best possible experience when using Windows Virtual Desktop.

Single-session recommendations

In terms of VM sizing recommendations for single-session scenarios, it is recommended that you use at least two physical CPU cores per VM (typically four vCPUs with hyperthreading). If you need more specific recommendations, ask the software vendors handling your workload. VM sizing for single-session VMs will likely align with physical device guidelines. It is recommended to use at least **two physical CPU cores per VM (typically four vCPUs with hyperthreading)**. For RAM, 8 GB is the standard in virtual desktop environments. A D2s_v3 instance could be a good start.

Multi-session recommendations

The following table lists the maximum suggested number of users per virtual central processing unit (vCPU) and the minimum VM configurations for each workload. These recommendations are based on [Remote Desktop workloads](#).

Workload type	Maximum users per vCPU	vCPU/RAM/OS storage minimum	Example Azure instances	Profile container storage minimum
Light	6	2 vCPUs, 8 GB RAM, 16 GB storage	D2s_v3, F2s_v2	30 GB
Medium	4–16 user per host	4 vCPUs, 16 GB RAM, 32 GB storage	D4s_v3, F4s_v2	30 GB
Heavy	2	4 vCPUs, 16 GB RAM, 32 GB storage	D4s_v3, F4s_v2	30 GB
Power	1	6 vCPUs, 56 GB RAM, 340 GB storage	D4s_v3, F4s_v2, NV6	30 GB

For a typical deployment, it's recommended that a medium workload type is used, as highlighted in the preceding table.

Identity strategies

The following identity strategies could apply for your Windows Virtual Desktop and Azure infrastructure. Choosing the right identity strategy will help you align with your immediate and future cloud requirements:

Option	Pros	Cons
Spin up a domain controller (DC) in your Azure subscription.	<p>Can sync with on-premises DCs if a</p> <p>All familiar AD Group Policies can be used.</p> <p>VMs can be paused or stopped when needed to reduce costs.</p>	<p>Adds additional management of a VM and Active Directory in Azure.</p>
For cloud-based organizations, use Azure AD DS.	<p>Great for test or isolated environments that do not need connectivity to on-premises resources.</p> <p>Azure AD will be your leading source for identities.</p>	<p>AD DS will always be running month.</p>
For hybrid organizations, use VPN or ExpressRoute and make sure your on- premises DCs can be found in Azure.	<p>Adds additional management of a VM and Active Directory in Azure.</p> <p>No AD DS or DC is required in Azure.</p>	<p>Latency could increase, adding delays during user authentication to VMs.</p> <p>This assumes you have an on-premises environment; it's not suitable for cloud-only tests.</p>

Security capabilities and best practices for Windows Virtual Desktop

Windows Virtual Desktop includes many security capabilities that help keep your data and users safe. An important point to note is that cloud services are different from traditional on-premises virtual desktop infrastructures, and there is a subtle difference in how security responsibilities are handled. Essentially, the responsibility for security is split between the cloud provider and the customer. Here is the list of security needs you're responsible for in your Windows Virtual Desktop deployment:

Security Need	Is the customer responsible for this?
Identity	YES
User devices (mobile and PC)	YES
App security	YES
Session host operating system	YES
Deployment configuration	YES
Network controls	YES
Virtualization control plane	NO
Physical hosts	NO
Physical network	NO
Physical datacenter	NO

Windows Virtual Desktop security capabilities

Microsoft invests more than USD1 billion annually in cybersecurity research and development, and Azure has more compliance certifications than any other cloud provider. Here are a few integrated security features you can use in your Windows Virtual Desktop environment:

- [Azure Security Center](#) supports Windows Virtual Desktop and helps you manage vulnerabilities, assess compliance with common frameworks such as PCI, and strengthen the overall security of your environment.
- [Multifactor authentication](#) on Windows Virtual Desktop improves the security of your entire deployment for access inside and outside your organization.
- [Conditional Access](#) provides the ability to manage risk and decide which users to grant access to, who the user is, how they sign in, and what device they're using.
- [RemoteApps](#) provide a seamless experience as the user works with applications on their virtual desktop. RemoteApps reduce risk by only letting the user work with a subset of the remote machine exposed by the application.

You can collect Windows Virtual Desktop service and availability information with Azure Monitor. You can also create service health alerts for the Windows Virtual Desktop service to receive notifications whenever an event occurs that affects your services.

You should aim to collect audit logs related to Windows Virtual Desktop, including the following:

- Azure Activity logs
- Azure Active Directory Activity logs
- Azure Active Directory
- Session hosts
- Windows Virtual Desktop Diagnostic logs
- Key Vault logs

Learn more about Azure security [here](#).

Four security tips for your Windows Virtual Desktop Environment

Use these additional security tips to help keep your customers' Windows Virtual Desktop deployments secure.

Security tip 1: Enable endpoint protection and install an endpoint detection and response product

Ensure you enable endpoint protection on all session hosts. You can use Windows Defender or a third-party program of choice. It is also recommended that you install an endpoint detection and response (EDR) product to provide advanced detection and response capabilities on Windows Virtual Desktop. For server operating systems with Azure Security Center enabled, installing an EDR product will deploy Defender ATP. For client operating systems, you can deploy Defender ATP or a third-party product to those endpoints.

Security tip 2: Manage Microsoft 365 Apps for Enterprise Security

To improve the security of your Office deployment, it is recommended that you use the [Security Policy Advisor for Microsoft 365 Apps for enterprise](#). This tool enables you to identify policies that you can apply to your deployment for more security. Security Policy Advisor also recommends policies based on their impact on your security and productivity.

Security tip 3: Establish maximum inactive time and disconnection policies

It is recommended that timeouts balance user productivity as well as resource usage. For users that interact with stateless applications, it is recommended that you consider more aggressive policies that turn off machines and preserve resources. Take care when configuring these policies, because disconnecting long-running applications that continue to run if a user is idle, such as a simulation or CAD rendering, can interrupt the user's work and may even require restarting the computer.

Security tip 4: Lock screens for idle sessions

Set up idle session screen locks to prevent unwanted system access by configuring Windows Virtual Desktop to lock after a period of idle time and require authentication to unlock the session.

Session host security recommendations

Strengthen the security of your session hosts by restricting operating system capabilities:

- **Device redirection:** Control device redirection by redirecting drives, printers, and USB devices to a user's local device in a remote desktop session. We recommend that you evaluate your security requirements and check whether these features ought to be disabled or not.

- **Restrict Windows Explorer access:** Hide local and remote drive mappings. This prevents users from discovering confidential information about system configuration and users.
- **Minimize direct RDP access to session hosts:** Avoid direct RDP access to session hosts in your environment. If you need direct RDP access for administration or troubleshooting, enable just-in-time access to limit the potential attack surface on a session host.
- **Limit access to local and remote file systems:** Grant users limited permissions when they access local and remote file systems. You can restrict permissions by making sure your local and remote file systems use access control lists with least privilege. This way, users can only access what they need and can't change or delete critical resources.
- **Enable App Locker:** Prevent unwanted software from running on session hosts. You can enable App Locker for additional security on session hosts, ensuring that only the apps you allow can run on the host.

Troubleshooting tips

Identifying issues

As mentioned in the previous section, Windows Virtual Desktop provides a diagnostic feature as a part of the management service that allows the administrator to identify issues through a single interface.

To find out more about the diagnostic capabilities of Windows Virtual Desktop, see [Use Log Analytics for the diagnostics feature](#).

Any connections that don't reach Windows Virtual Desktop won't show up in diagnostics results because the diagnostics role service itself is part of Windows Virtual Desktop, and you would need to use additional tools to identify the issue. Typically, Windows Virtual Desktop connection issues happen when the user is experiencing network connectivity issues. The first step should be for the user to check their connection.

Please use [this article](#) to find out more about the different methods to identify and diagnose Windows Virtual Desktop issues.

Common errors and suggested solutions

The following table lists some of the errors and messages that pop up if there are issues with the VM communicating with the management service:

Error message	Suggested solution
Failed to create registration key	Registration token couldn't be created. Try creating it again with a shorter expiry time (between 1 hour and 1 month).
Failed to delete registration key	Registration token couldn't be deleted. Try deleting it again. If it still doesn't work, use PowerShell to check if the token is still there. If it's there, delete it with PowerShell.
Failed to change session host drain mode	Couldn't change drain mode on the VM. Check the VM status. If the VM is unavailable, drain mode can't be changed.
Failed to disconnect user sessions	Couldn't disconnect the user from the VM. Check the VM status. If the VM is unavailable, the user session can't be disconnected. If the VM is available, check the user session status to see if it's disconnected.
Failed to log off all user(s) within the session host	Could not sign users out of the VM. Check the VM status. If it's unavailable, users can't be signed out. Check user session status to see if they're already signed out. You can force sign out with PowerShell.
Failed to unassign user from application group	Could not unpublish an app group for a user. Check if the user is available on Azure AD. Check if the user is part of a user group that the app group is published to.
There was an error retrieving the available locations	Check the location of the VM used in the Add virtual machines to a host pool wizard. If an image is not available in that location, add an image in that location or choose a different VM location.

[Read more](#) on the common error codes for Windows Virtual Desktop.



Section 4:

Conclusion

Summary and resources

In Section 1, we've detailed desktop and app virtualization and provided an overview of how Windows Virtual Desktop helps enable secure remote work for your business.

In Section 2, we provided references to step-by-step deployment guidance and provided tips and guidance to help you set up your Windows Virtual Desktop workspace.

Finally, in Section 3, we highlighted some best practices and recommendations to help you optimize your Windows Virtual Desktop environment.

We hope you enjoyed the tour and feel more prepared to start your journey with Windows Virtual Desktop! There are a lot of other resources and support to help—here are a few key references:

1. [Read](#) more Windows Virtual Desktop documentation to get the latest technical guidance.
2. [Take](#) a tutorial on getting started with Windows Virtual Desktop.
3. [Watch](#) this on-demand Windows Virtual Desktop webinar to see a demo.
4. [Sign up](#) for an Azure free account to try deploying your virtualized Windows desktops and apps.
5. [Get hands-on deployment](#) guidance if you already have an Azure subscription.
6. [Contact sales](#) to discuss pricing, technical requirements, and short- and long-term solutions for enabling secure remote work.



Glossary

Whether you're new to VDIs or an expert at desktop virtualization, there may be some terms you're not familiar with. The following are key terms introduced by Windows Virtual Desktop:

Application groups: An application group is a mechanism for grouping remote resources and assigning them to users. An application group can be one of two types:

- **RemoteApp:** This is a resource type that allows users to access the applications you individually publish to the application group. You can create multiple RemoteApp application groups to accommodate different user scenarios. It is recommended that you use RemoteApp to virtualize an application that runs on a legacy operating system or one that needs secured access to corporate resources.
- **Remote Desktop:** This is a resource that provides users with access to the full desktop. By default, the Desktop application group is automatically created when you create a host pool.

Broker: The Connection Broker service manages user connections to virtual desktops and remote apps. It provides load balancing and reconnection to existing sessions.

Diagnostics: Remote Desktop Diagnostics is an event-based aggregator that marks each user or administrator action in a Windows Virtual Desktop deployment as a success or failure. Administrators can query the aggregation of events to identify failing components.

Gateway: The Remote Connection Gateway service connects remote users to Windows Virtual Desktop remote apps and desktops from any internet-connected device that can run a Windows Virtual Desktop client or HTML5 browser. The client connects to a gateway, which then orchestrates a connection from the VM back to the same gateway.

Host pool: A host pool is a collection of Azure VMs that act as session hosts for Windows Virtual Desktop. Users obtain access to host pools by being allocated to a host pool via an assigned Application Group:

- **Pooled:** You can configure a pooled host pool where several users sign in and share a VM. Typically, none of those users would be a local administrator on the pooled VM. With pooled, you can use one of the recommended images that includes Windows 10 Enterprise multi-session. This operating system is exclusive to Windows Virtual Desktop. You can also use your own custom image.
- **Personal:** A personal host pool is where each user has their own dedicated VM. Those users would typically be local administrators for the VM. This enables the user to install or uninstall apps without impacting other users.

Load balancing: Session host load balancing is achieved by depth-first or breadth-first algorithms. The broker decides how new incoming sessions are to be distributed across the VMs in a host pool.

Load-balancing options:

- **Breadth-first:** This is the default configuration for new non-persistent host pools. Distributes new user sessions across all available session hosts in the host pool. When you configure breadth-first load balancing, you may set a maximum session limit per session host in the host pool.
- **Depth-first:** Distributes new user sessions to an available session host with the highest number of connections but that has not reached its maximum session limit threshold. When you configure depth-first load balancing, you must set a maximum session limit per session host in the host pool.

Web client: The Web Access service within Windows Virtual Desktop enables users to access virtual desktops and remote apps through an HTML5-compatible web browser like you would with a local PC—from anywhere and any device. You can secure Web Access by using MFA in Azure AD.

Workspace: A workspace is a logical grouping of application groups in Windows Virtual Desktop. When a user signs in to Windows Virtual Desktop, the user can see both a desktop and applications when a member of multiple application groups coming from different host pools.

About the author

Ryan Mangan is an end-user computing specialist. He is a speaker and presenter who has helped customers and technical communities with end-user computing solutions, ranging from small to global 30,000-user enterprise deployments in various fields. Ryan is the owner and author of ryanmangansitblog.com, which has over 3 million visitors and over 70 articles on Remote Desktop Services and Windows Virtual Desktop. Some of Ryan's community and technical awards include:

- VMware vExpert***** seven years running
- Parallels RAS VIPP 19/20
- LoginVSI Technology Advocate
- Technical person of the year 2017 KEMP Technologies
- Parallels RAS EMEA Technical Champion 2018
- Microsoft Community Speaker
- Experts Exchange Verified Expert
- Top 50 IT Blogs 2020—Feed spot
- Top 50 Azure Blogs 2020—Feed spot

GitHub: <https://github.com/RMITBLOG>