E-book series

Microsoft Azure

Quickstart Guide to Azure Virtual Desktop

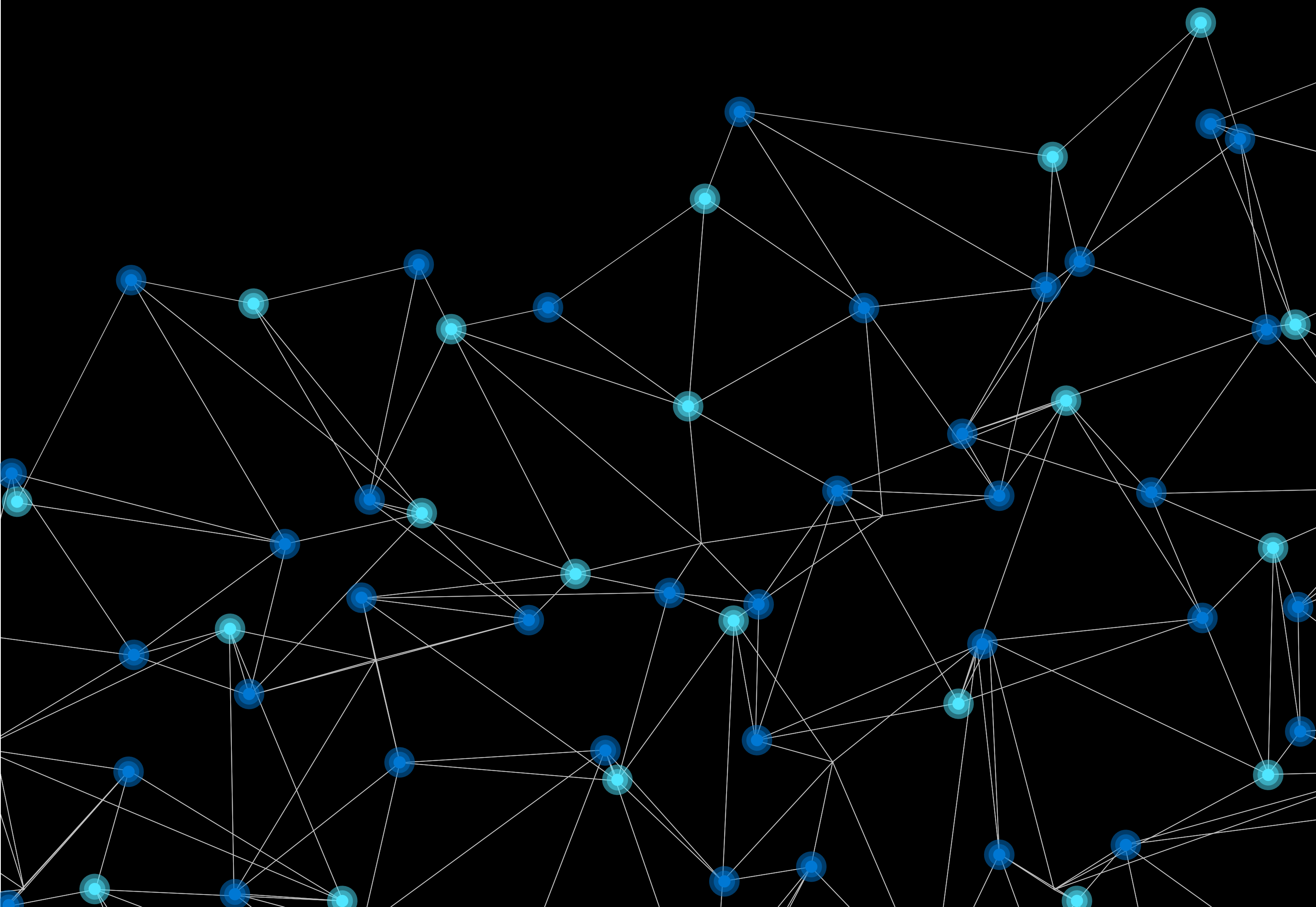
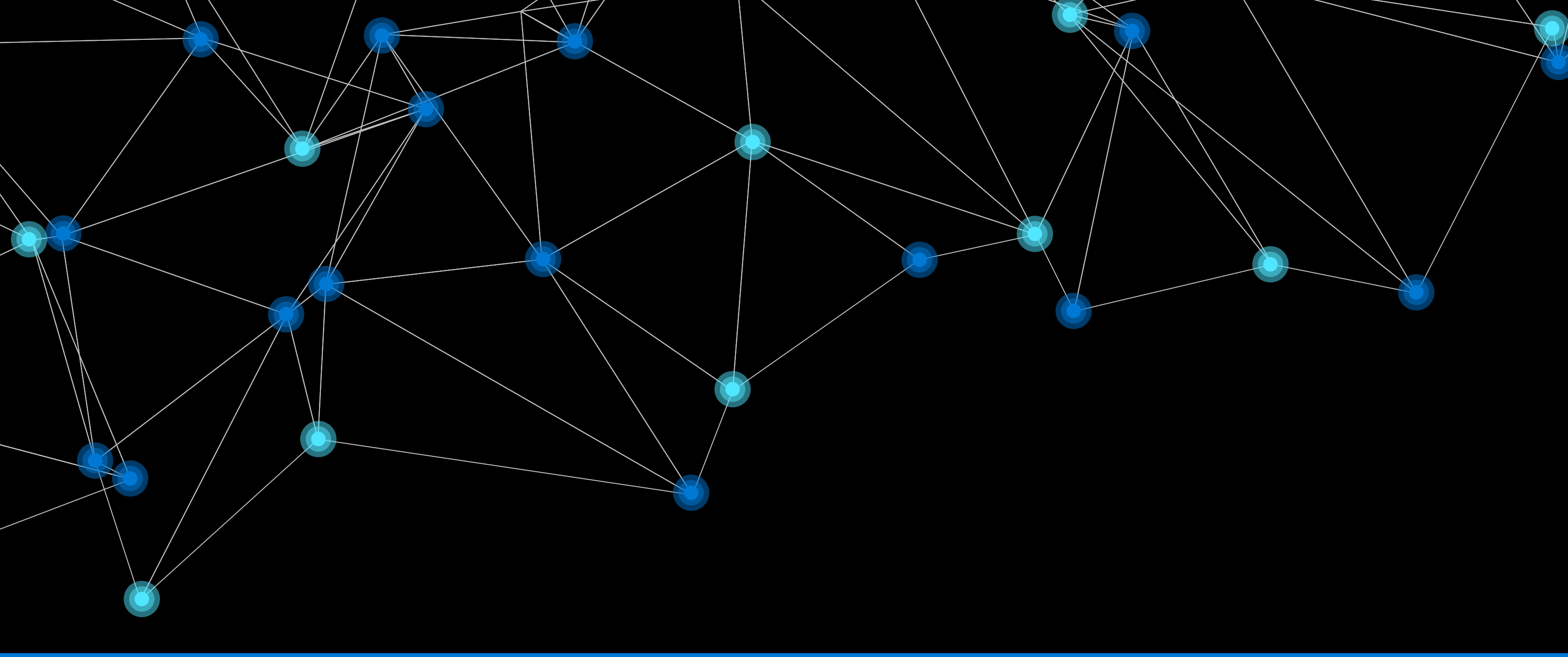


Table of contents

Section 1:
Introduction to Azure Virtual Desktop

Section 2:
Azure Virtual Desktop deployment and prerequisites

Section 3:
Azure Virtual Desktop optimization



Section 1: Introduction to Azure Virtual Desktop

Introduction

As organizations around the world evolve to modern and hybrid working scenarios, it has become vital for businesses to implement remote working strategies that increase business resilience, including desktop and app virtualization. Azure Virtual Desktop is a flexible cloud virtual desktop infrastructure (VDI) platform that helps enable users to work securely and productively from virtually any location, while also simplifying IT management and reducing infrastructure costs.

As you plan your adoption of Azure Virtual Desktop, it's good to understand the benefits you can realize, as well as the key steps and practices to get started successfully. To help prepare you for successful Azure Virtual Desktop deployment, this e-book shares the essentials of desktop virtualization and the unique benefits that Azure Virtual Desktop will bring to your organization.

It will then outline the Azure Virtual Desktop deployment steps along with best practices to help you optimize your environment.

We hope you enjoy your tour of Azure Virtual Desktop. After reading this e-book, you will be prepared to embark on your Azure 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 get in touch with an Azure sales specialist.

Virtual desktop infrastructure

Virtual desktop infrastructure (VDI) refers to the use of virtualization and virtual machines (VMs) to provide and manage virtual desktops and remote apps. Users can access these VMs 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 Azure Virtual Desktop?

Azure Virtual Desktop is a desktop and app virtualization service that runs on Microsoft Azure. Azure 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 Azure Virtual Desktop–hosted experiences.

Typically, Azure 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 an Azure 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:

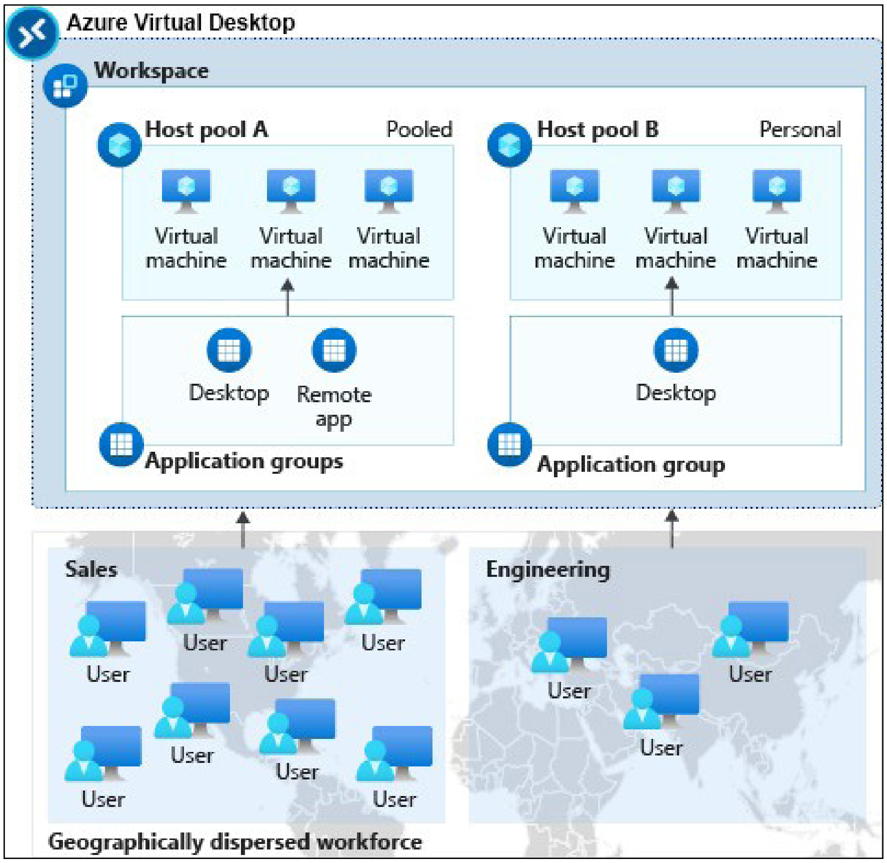


Figure 1: Azure Virtual Desktop workspace with two host pools

Building on this simple example, here is a typical enterprise deployment of Azure 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:

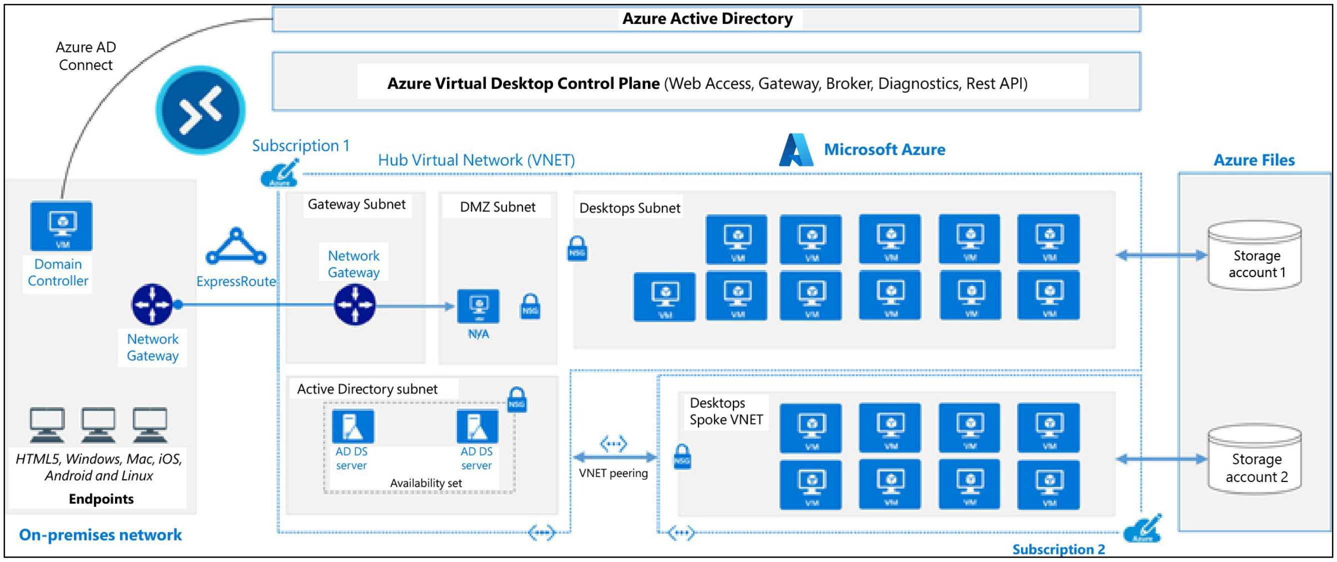


Figure 2: A typical architectural setup for Azure Virtual Desktop

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

While the guidance in this e-book focuses on native VDI deployment, Azure 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 Azure Virtual Desktop partner integrations.

Business benefits of Azure Virtual Desktop

There are many benefits that Azure 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

- Azure Virtual Desktop provides full Windows 10, Windows 11 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, so 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 Azure Virtual Desktop is seamless 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

- Azure 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.
- Azure Virtual Desktop also isolates user sessions in multi-session environments. This provides better security than a VPN because it doesn't give users access to a full subnet.
- Azure 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). Session host VMs use secure outbound connectivity to the Azure Virtual Desktop infrastructure over the HTTPS connection.

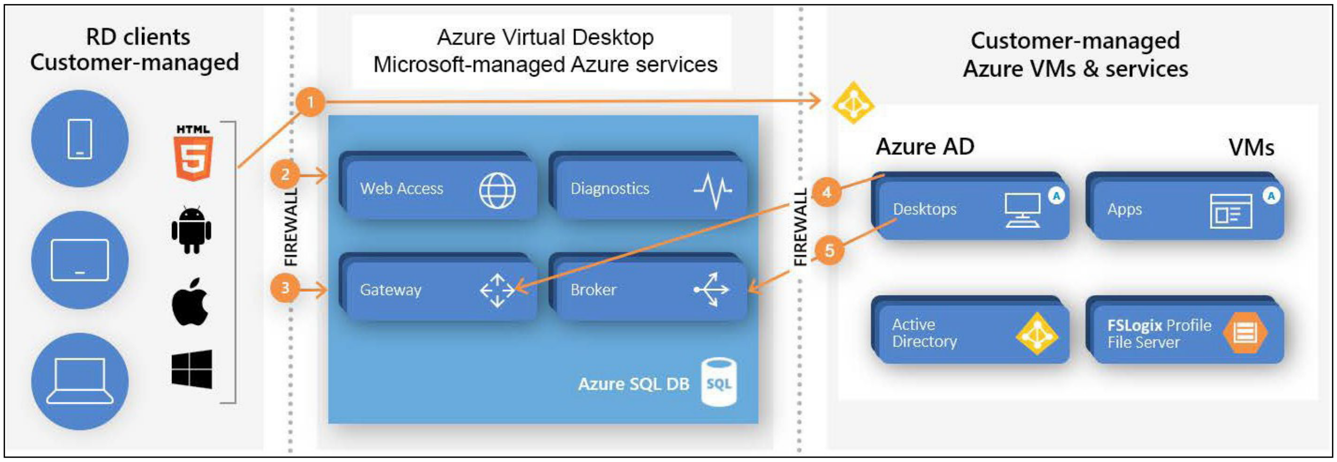


Figure 3: The connection flow process of Azure Virtual Desktop

- As an Azure service, Azure Virtual Desktop uses industry-leading security and compliance offerings 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 allows you to enable conditional access policies and role-based access control. You can read more about security best practices for Azure Virtual Desktop here.

Simplify deployment and management

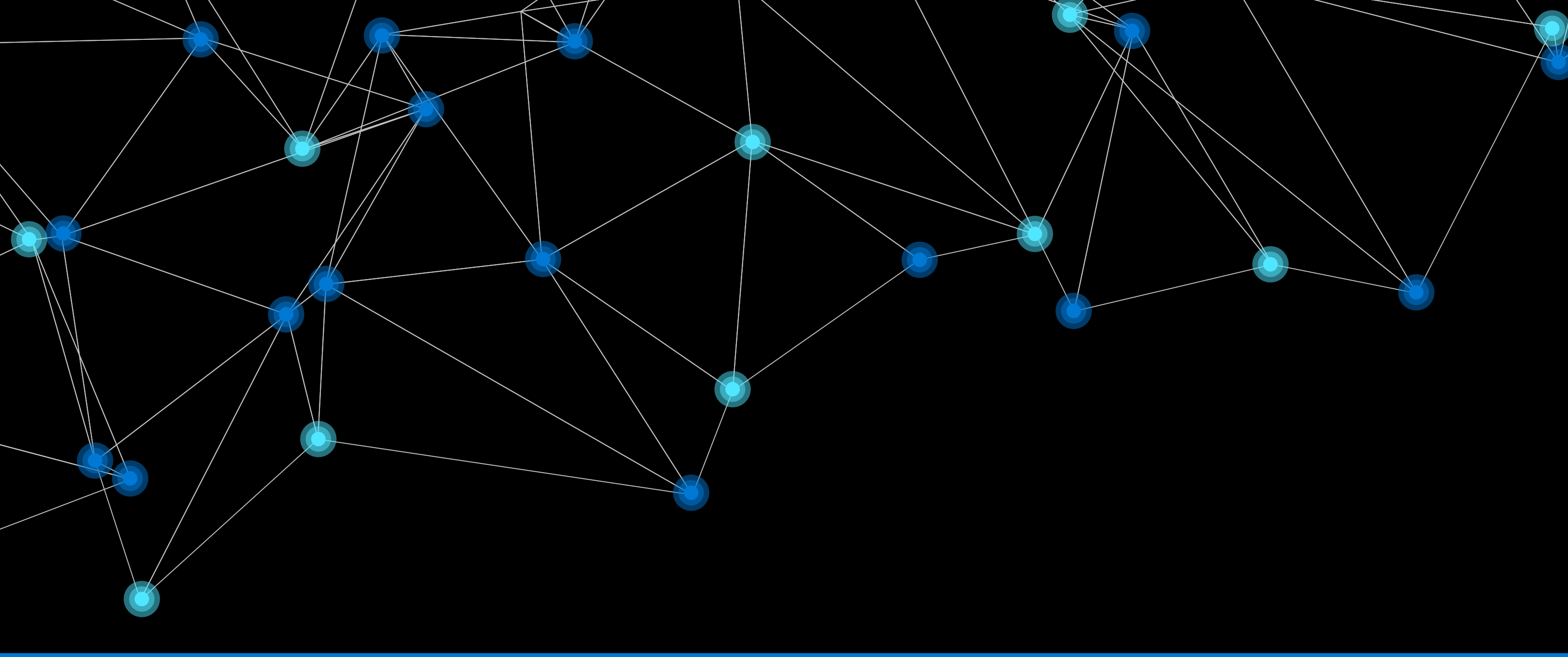
- Since Azure Virtual Desktop manages the entire VDI for you, you can focus on the user and the apps and operating system images you need to use, instead of hardware inventory and maintenance.
- With the features of the cloud, you'll be able to quickly and securely get your users up and running, with 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. Azure Virtual Desktop also provides tools to automatically provision additional VMs when an incoming demand exceeds a specified threshold.
- With Azure 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 Azure 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, Azure Virtual Desktop will bring numerous benefits to your business, including more secure remote work for your end users, quick deployment, simplified IT management, and reduced licensing and infrastructure costs.

See customer stories to get real-life examples of how others have used Azure Virtual Desktop to help their business.



Section 2: Azure Virtual Desktop deployment and prerequisites

Azure Virtual Desktop deployment checklist

As a reference, here is an overview of the four stages of Azure Virtual Desktop deployment along with the key steps of each phase:

Phase	Steps
Plan	Gather your organization's current and future virtual desktop requirements: • Determine the appropriate networking considerations • Assess current user requirements and motivations • Decide on the user experience, personal or pooled (multi-session) • Choose your deployment and configuration strategy
Prepare	Ready your Microsoft Azure subscription for Azure Virtual Desktop: • Establish connectivity to Microsoft Azure subscription • Set up your chosen Active Directory configuration • Create resources, roles, assign licenses, and register the desktop virtualization provider
Deploy	Create the Azure Virtual Desktop workspace and configure it for usage: • Use the Azure Virtual Desktop Getting started feature • Configure the required workspace and host pool(s) • Assign desktop and remote apps via application groups • Customize the workspace for desktops, apps, and protocols
Optimize	Adjust and scale your environment to meet your needs: • Deliver a true roaming profile using FSLogix • Configure Azure File Sync to sync files and user profiles to Azure storage • Enhance application delivery using MSIX app attach • Simplify business changes using Azure's automation tools

In *Section 2* of this e-book, we'll go through the planning, preparation, 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 Azure Virtual Desktop deployment

To plan for the deployment, you'll need to review some of the key requirements for designing an Azure Virtual Desktop deployment. You can find an overview of these requirements here. We'll go through a few considerations to help you along the way.

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 Azure Virtual Desktop.

When using domain-joined or hybrid Azure AD–joined VMs, you'll need to join the VMs to the domain. To do this, the VMs should be able to communicate with the domain controller. This can be accomplished with the VMs being on the same virtual network, on a different virtual network using peering, or by using ExpressRoute or site-to-site VPN to an on-premises 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 where 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 the Active Directory Domain Controller as a DNS server.

2. Ensure you've set up firewall rules and other network requirements

Azure 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 Azure 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.

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 create a 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 limit 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. The sizing for single-session VMs will likely align with physical device guidelines.

For multi-session VM sizing recommendations, see Virtual machine sizing guidelines.

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 dropdown 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.

5. Ensure that you prepare for domain-joined VMs

Azure Virtual Desktop supports joining the VMs to Active Directory or Azure AD. When joining to Active Directory, you can specify the domain and organizational unit. When using 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'll also need to specify a Domain 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.

When joining to Azure AD, the VMs will automatically be joined to the same Azure AD tenant as the subscription. You'll also have the option to automatically enroll the VMs in Intune for easy management.

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.

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

You can access Azure Virtual Desktop workspaces 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 Azure Virtual Desktop client directly from your device. The following client device types support Azure Virtual Desktop:

- Windows
- Android
- macOS
- iOS
- Linux, provided by Linux thin client partners; read more here

Phase 2: Prepare an Azure 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 AD and VM configuration. The following table walks through these requirements.

Resource	Requirements
Licenses and subscriptions	• Access Azure 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]. 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.
Create Azure resources	• Create the Azure virtual network. • Configure connectivity to Active Directory if needed via a VPN, localhost, or Azure virtual network peering.

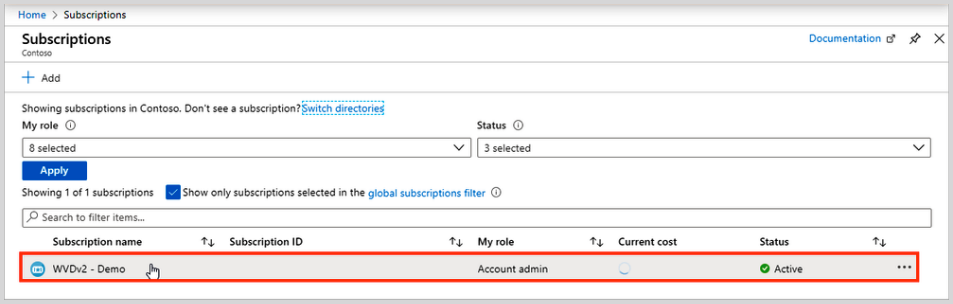
[1] More information on eligible licenses at https://azure.microsoft.com/pricing/details/virtual-desktop/.

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

Resource	Requirements
Azure AD	• Azure AD • A domain controller (DC) that's synced with Azure AD when deploying domain-joined or Hybrid Azure AD–joined VMs You can configure this DC with one of the following: • On-premises DC with ExpressRoute or site-to-site VPN to the same Azure Virtual Network as the VMs • Windows Server VMs in Azure configured as DCs • Azure AD DS The following restrictions also apply: • The users must be sourced from the same Active Directory that's connected to Azure AD via Azure AD Connect. • The UPN and/or SID of the users you use to subscribe to Azure Virtual Desktop must exist in the Active Directory domain the VM is joined to.
Virtual Machines (VMs)	• VMs can be standard domain-joined, Hybrid Azure AD–joined, or Azure AD–joined. • VMs must be running one of the supported operating system images.

<table>
<tr><th>Resource</th><th>Requirements</th></tr>
<tr><td>Tenant requirements</td><td>

- 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:



Subscriptions
Contoso

Showing subscriptions in Contoso. Don't see a subscription? Switch directories

My role: 8 selected
Status: 3 selected

Showing 1 of 1 subscriptions ☑ Show only subscriptions selected in the global subscriptions filter

Search to filter items...

<table>
<tr><th>Subscription name</th><th>Subscription ID</th><th>My role</th><th>Current cost</th><th>Status</th></tr>
<tr><td>WVDv2 - Demo</td><td></td><td>Account admin</td><td></td><td>Active</td></tr>
</table>

</td></tr>
<tr><td>Azure Virtual Desktop Getting started requirements

(Optional)</td><td>

- An Azure AD tenant
- An account with global admin permissions on Azure AD
- An active Azure subscription
- An account with Owner permissions to the subscription

</td></tr>
</table>

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 Azure Virtual Desktop workspace

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

If you already have an Azure subscription, you can also try the Getting started functionality, which will guide you through each step of deployment using the Azure portal and your existing account subscription.

Azure Virtual Desktop's Getting started feature

The new Getting started feature in the Azure portal provides a quick and easy way to deploy and configure an Azure Virtual Desktop environment. This feature offers simplicity for those who want to get started with Azure Virtual Desktop quickly by removing complex multi-step processes, including some of the following:

- FSLogix profiles setup, Azure Files Storage account creation, and domain join.
- Creation of session hosts and configuration of Azure Virtual Desktop (host pool, workspaces, desktop groups, and validation user)
- Validating user input
- Validating the environment (DNS, firewall/NSG configuration requirements for Azure Virtual Desktop, permission on Azure AD and subscriptions)

The new functionality offers several benefits, including:

- Optimizing the time to production for Azure Virtual Desktop deployments.
- Completing Azure Virtual Desktop deployment in less than a couple of hours.
- Reducing the complexity of the Azure Virtual Desktop deployment experience, making the platform more accessible by automating the deployment process.
- Increasing the deployment success rate.

We will now take a look at deploying an Azure Virtual Desktop environment using the Azure Virtual Desktop Getting started feature.

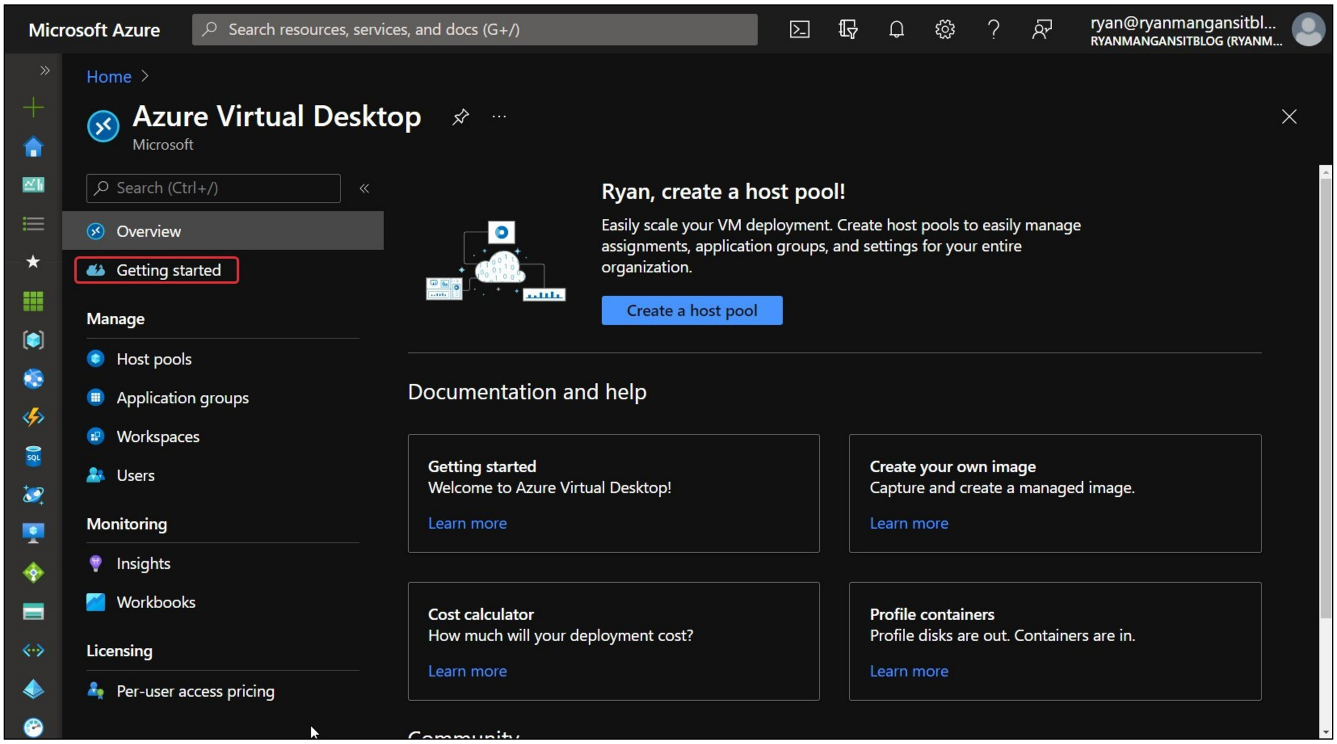
Getting started:

Before we look at the steps for configuring Azure Virtual Desktop Getting started, it is important to note that there are two deployment options available to you:

1. **Existing active directory**: This option uses an existing Active Directory or Azure AD DS setup for your Azure subscription.
2. **No identity provider**: This provisions Azure AD DS as the identity provider and any required Azure resources, such as networking.

The following steps detail what you need to do to create your first Azure Virtual Desktop Getting started deployment:

1. Sign in to Azure, open Azure Virtual Desktop management, and select **Getting started**, as shown here:



Ryan, create a host pool!

Easily scale your VM deployment. Create host pools to easily manage assignments, application groups, and settings for your entire organization.

Documentation and help

Getting started
Welcome to Azure Virtual Desktop!

Create your own image
Capture and create a managed image.

Cost calculator
How much will your deployment cost?

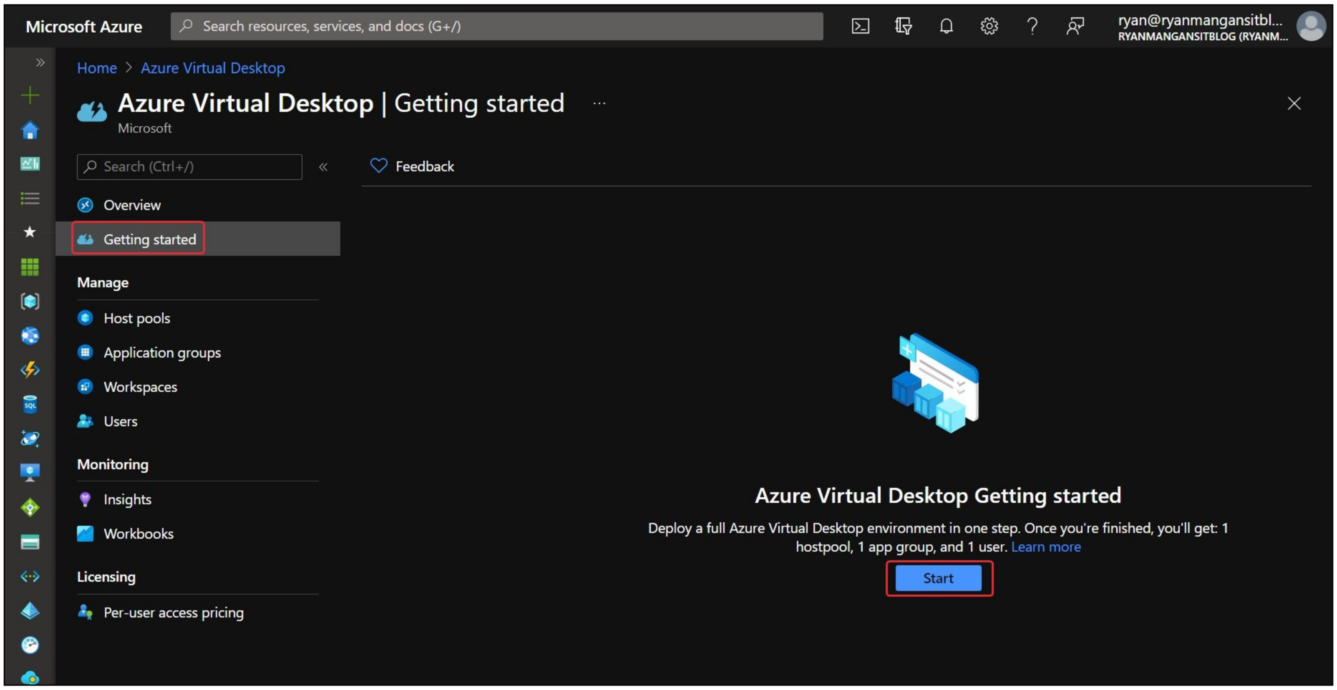
Profile containers
Profile disks are out. Containers are in.

Community

Figure 4: The Getting started feature

Once on the Azure Virtual Desktop page, you will see the **Getting started** icon just below the **Overview** icon.

2. This will open the landing page for the wizard. Click **Start:**



Azure Virtual Desktop Getting started

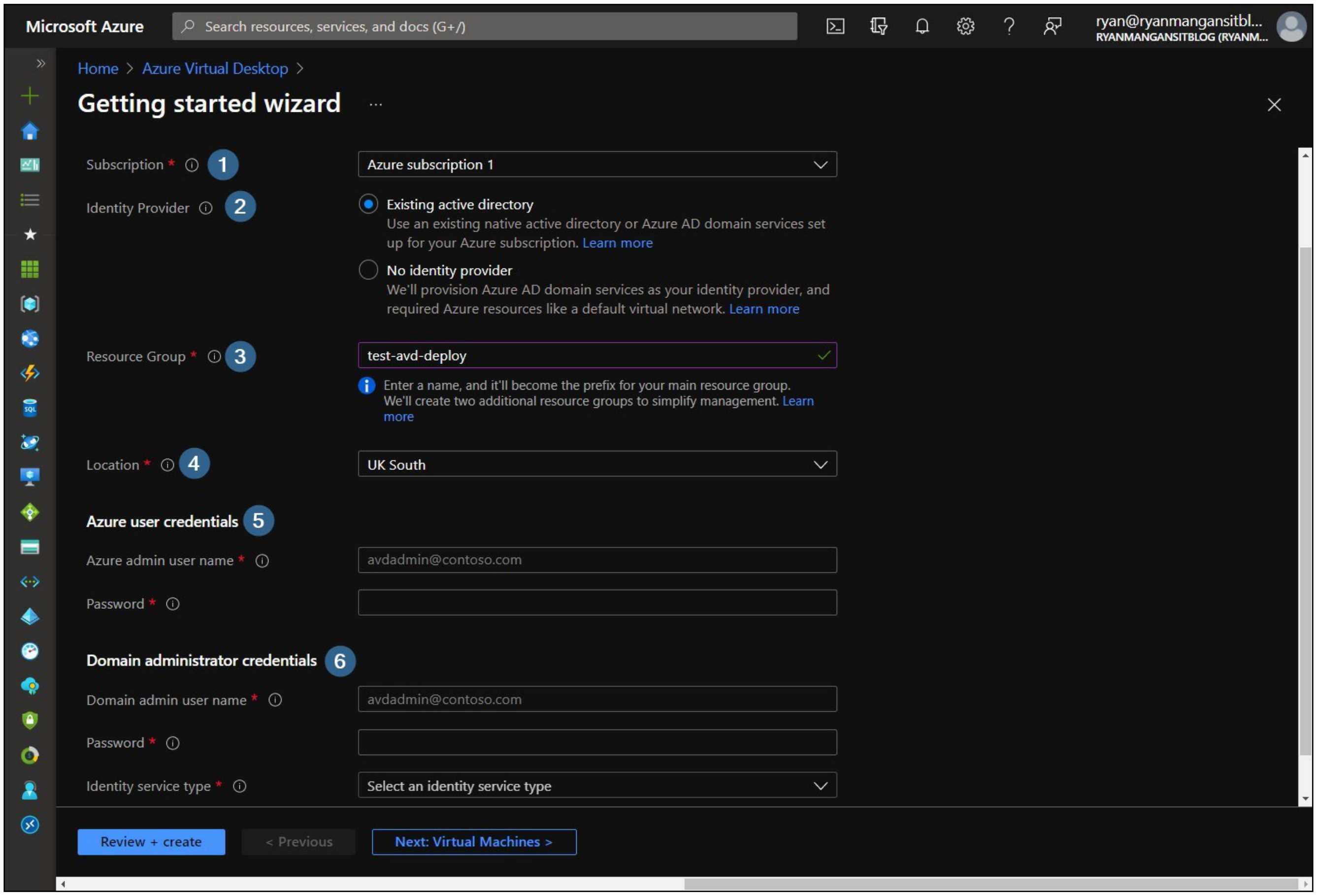
Deploy a full Azure Virtual Desktop environment in one step. Once you're finished, you'll get: 1 hostpool, 1 app group, and 1 user. Learn more

Figure 5: The Getting started page

3. In the **Basic** panel, you will need to configure the following:

    1. **Subscription**: Allows you to select a subscription to which the wizard is going to deploy.
    2. **Identity provider**: Select either **Existing active directory** or **No identity provider**. The **No identity provider** option is used to deploy a full Azure Virtual Desktop infrastructure, including networking. If you already have the fundamentals configured, choose **Existing active directory**.
    3. **Resource group**: Specify a resource group you want for this Azure Virtual Desktop deployment.
    4. **Location**: Select an Azure region you would like to deploy to.
    5. **Azure user credentials**: The full user principal name (UPN) for an account that has admin permissions on Azure AD and owner permission on the subscription.
    6. **Domain administrator credentials**: The full UPN for an account that has permissions and will be used to join the VMs to your domain.

Figure 6 shows the **Basic** panel with each section numbered one to six.


Microsoft Azure
Search resources, services, and docs (G+/)
ryan@ryanmangansitbl...
RYANMANGANSITBLOG (RYANM...
Home > Azure Virtual Desktop >
Review + create
< Previous
Next: Virtual Machines >

Getting started wizard

Subscription * 1: Azure subscription 1

Identity Provider 2:

● Existing active directory
Use an existing native active directory or Azure AD domain services set up for your Azure subscription. Learn more

○ No identity provider
We'll provision Azure AD domain services as your identity provider, and required Azure resources like a default virtual network. Learn more

Resource Group * 3: test-avd-deploy
Enter a name, and it'll become the prefix for your main resource group. We'll create two additional resource groups to simplify management. Learn more

Location * 4: UK South

Azure user credentials 5

Azure admin user name *: avdadmin@contoso.com

Password *:

Domain administrator credentials 6

Domain admin user name *: avdadmin@contoso.com

Password *:

Identity service type *: Select an identity service type

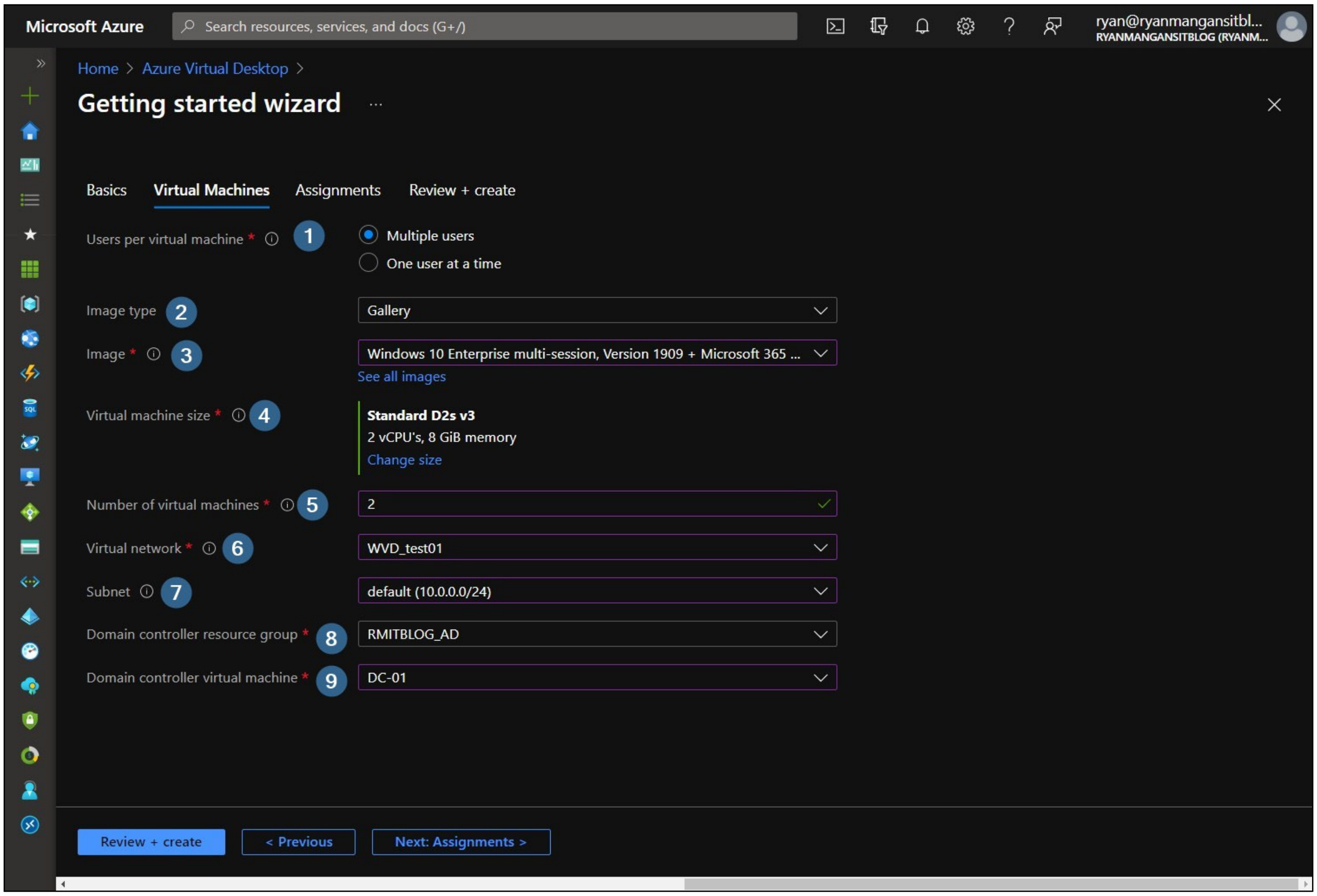
Figure 6: The Basic settings page

We now move on to the **Virtual Machines** tab where we will configure the type of user session deployment (personal or multi-session) and enter further information, including the image, VM size, and number of VMs to be deployed.

4. On the **Virtual Machines** page, the options are as follows:
    1. **Users per virtual machine**: This option determines if a single session (personal) or multi-session (pooled) host pool will be configured. When selecting **Multiple users**, this will also trigger the creation of an Azure Files storage account that will be joined to either Azure AD DS or AD DS.
    2. **Image type**: This allows you to select an image from the image gallery, custom images, or VHDs from storage blobs.
    3. **Image**: Select your chosen image.

4. **Virtual machine size**: This allows selecting size and SKU for the VMs that are going to be deployed.
5. **Number of virtual machines**: This defines how many VMs are to be provisioned in the host pool.
6. **Virtual network**: Choose the required virtual network.
7. **Subnet**: Select your subnet.
8. **Domain controller resource group**: Select the domain controller resource group
9. **Domain controller virtual machine**: Select the domain controller virtual machine.

Figure 7, with numbers one to nine, details the configuration steps we just covered.



Getting started wizard

Users per virtual machine * 1
● Multiple users
○ One user at a time

Image type 2: Gallery

Image * 3: Windows 10 Enterprise multi-session, Version 1909 + Microsoft 365 ...
See all images

Virtual machine size * 4: Standard D2s v3
2 vCPU's, 8 GiB memory
Change size

Number of virtual machines * 5: 2

Virtual network * 6: WVD_test01

Subnet 7: default (10.0.0.0/24)

Domain controller resource group * 8: RMITBLOG_AD

Domain controller virtual machine * 9: DC-01

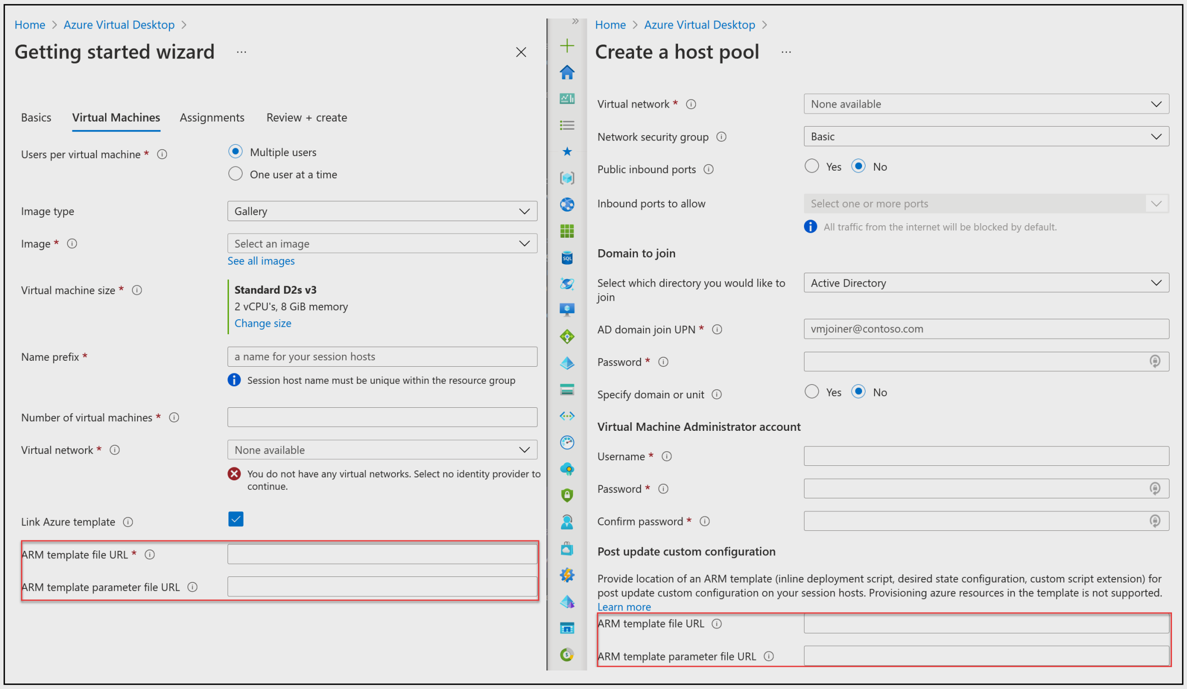
Figure 7: The Virtual Machines tab

We now look at assignments that can be configured or left unticked.

Customizing Host Pool Deployments

You can also chain a custom **Azure Resource Manager** (**ARM**) template. This allows you to insert customizations into the deployment process. You can download the example ARM template customization here.

The following screenshot shows the Link Azure template:



Home > Azure Virtual Desktop >

Getting started wizard ...

Basics | Virtual Machines | Assignments | Review + create

Users per virtual machine *: ● Multiple users ○ One user at a time

Image type: Gallery

Image *: Select an image
See all images

Virtual machine size *: Standard D2s v3
2 vCPU's, 8 GiB memory
Change size

Name prefix *: a name for your session hosts
Session host name must be unique within the resource group

Number of virtual machines *:

Virtual network *: None available
You do not have any virtual networks. Select no identity provider to continue.

Link Azure template: ☑

ARM template file URL *:

ARM template parameter file URL:

Home > Azure Virtual Desktop >

Create a host pool ...

Virtual network *: None available

Network security group: Basic

Public inbound ports: ○ Yes ● No

Inbound ports to allow: Select one or more ports
All traffic from the internet will be blocked by default.

Domain to join

Select which directory you would like to join: Active Directory

AD domain join UPN *: vmjoiner@contoso.com

Password *:

Specify domain or unit: ○ Yes ● No

Virtual Machine Administrator account

Username *:

Password *:

Confirm password *:

Post update custom configuration

Provide location of an ARM template (inline deployment script, desired state configuration, custom script extension) for post update custom configuration on your session hosts. Provisioning azure resources in the template is not supported.
Learn more

ARM template file URL:

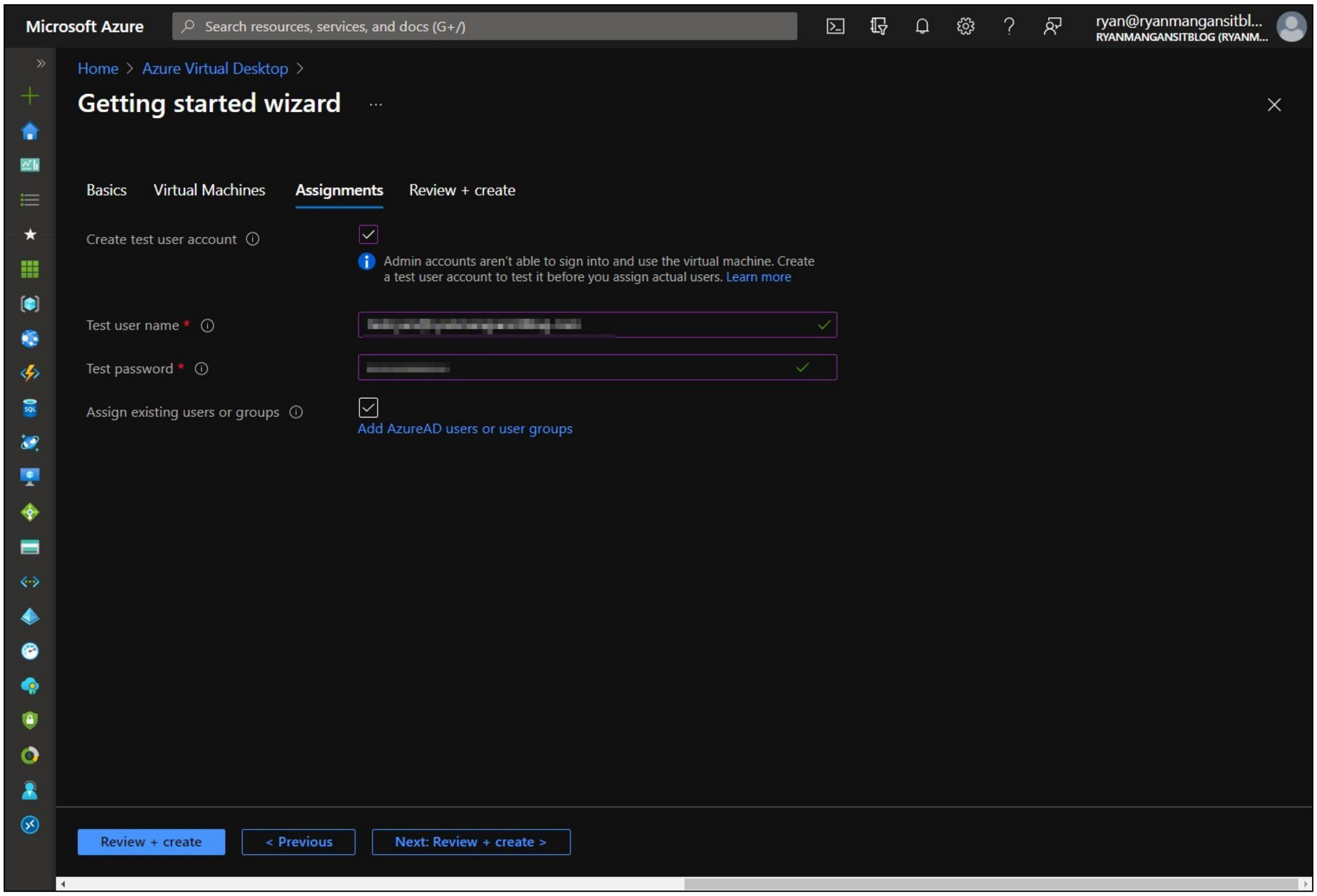
ARM template parameter file URL:

The location for linking a custom ARM template

5. The **Assignments** panel allows you to specify the creation of a validation user that is going to be assigned to test the deployment.
    1. **Create test user account**: When checked, this will open two fields—**Validation user username** and **Validation user password**.
    2. **Assign existing users or groups**: The option to assign users/groups automatically.
    3. Click **Review + create**.

Tip: *Getting started will create the validation user group in the "USERS" container. You must make sure your validation group is synced to Azure AD. If the sync doesn't work, then pre-create the Azure Virtual Desktop Validation Users group in an organization unit that is being synced to Azure AD.*

Figure 8 shows the assignments tab with options for a test user and assigning existing users or groups.



Getting started wizard

Create test user account ⓘ ☑

Admin accounts aren't able to sign into and use the virtual machine. Create a test user account to test it before you assign actual users. Learn more

Test user name * ⓘ [redacted] ✓

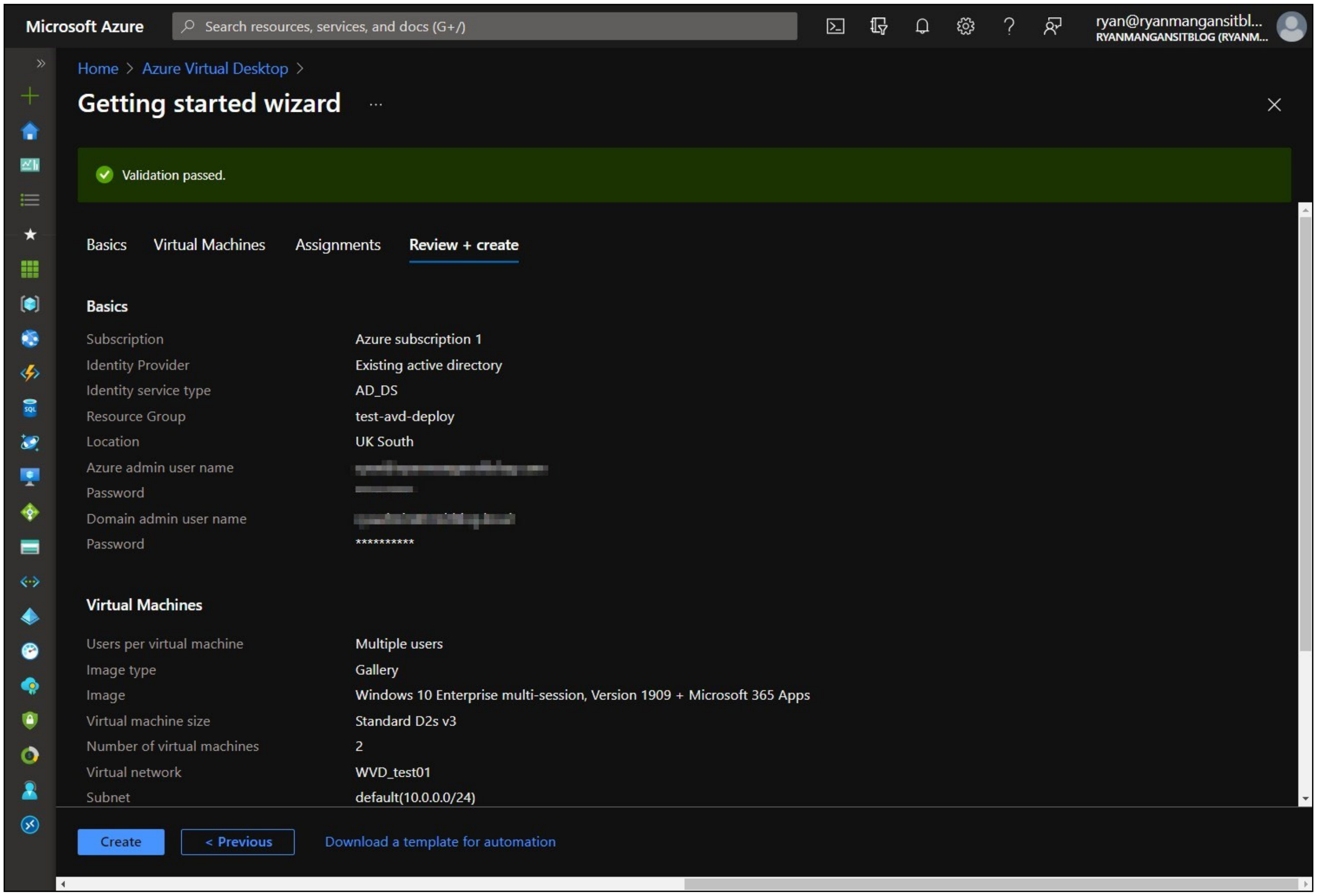
Test password * ⓘ [redacted] ✓

Assign existing users or groups ⓘ ☑

Add AzureAD users or user groups

Figure 8: The Assignments tab

The final tab is **Review + create**, where you should check the configurations before you start your deployment.


Microsoft Azure
Search resources, services, and docs (G+/)
ryan@ryanmangansitbl...
RYANMANGANSITBLOG (RYANM...
Home > Azure Virtual Desktop >
Basics
Virtual Machines
Assignments
Review + create
Create
< Previous
Download a template for automation

Getting started wizard

Validation passed.

Basics

Subscription	Azure subscription 1
Identity Provider	Existing active directory
Identity service type	AD_DS
Resource Group	test-avd-deploy
Location	UK South
Azure admin user name	[redacted]
Password	[redacted]
Domain admin user name	[redacted]
Password	**********

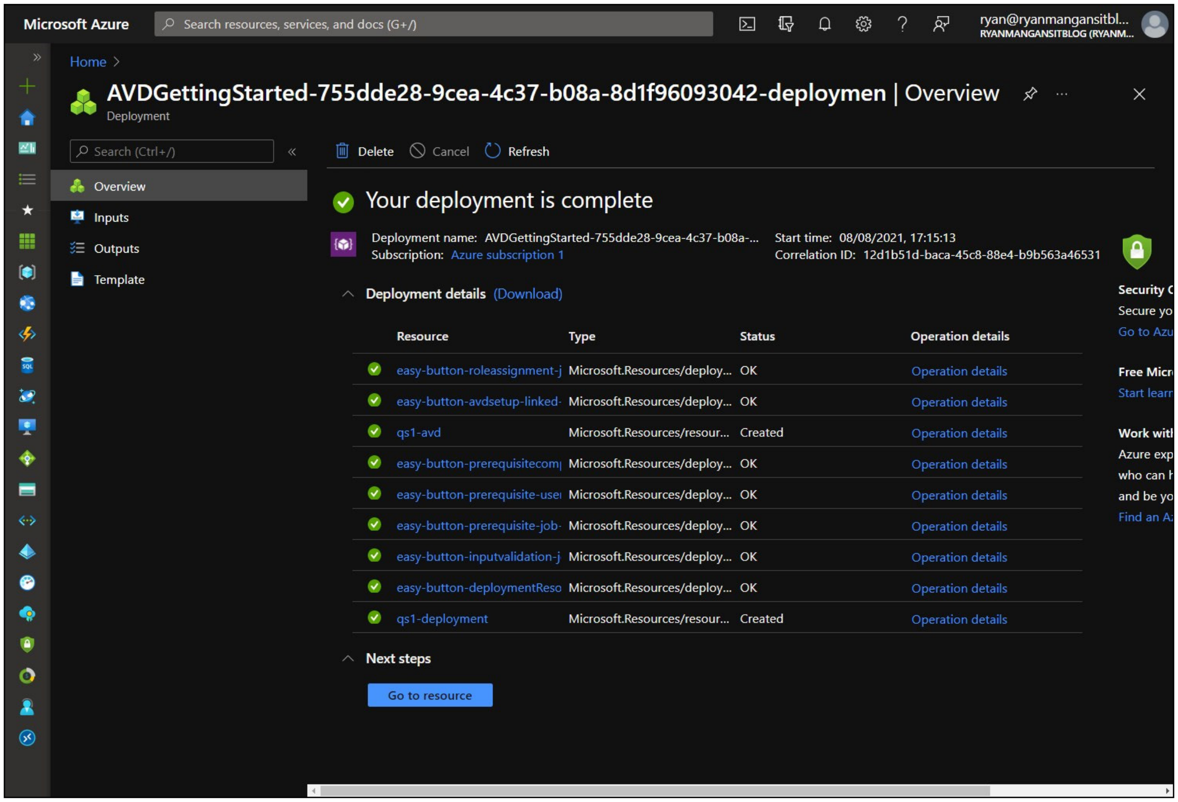
Virtual Machines

Users per virtual machine	Multiple users
Image type	Gallery
Image	Windows 10 Enterprise multi-session, Version 1909 + Microsoft 365 Apps
Virtual machine size	Standard D2s v3
Number of virtual machines	2
Virtual network	WVD_test01
Subnet	default(10.0.0.0/24)

Figure 9: The Review + create Getting started wizard tab

Once you have checked over the configurations you specified earlier, proceed with the creation by clicking the **Create** button.

On completion of the deployment, you should see something similar to *Figure 10*.



AVDGettingStarted-755dde28-9cea-4c37-b08a-8d1f96093042-deploymen | Overview

Deployment

Your deployment is complete

Deployment name: AVDGettingStarted-755dde28-9cea-4c37-b08a-...
Subscription: Azure subscription 1
Start time: 08/08/2021, 17:15:13
Correlation ID: 12d1b51d-baca-45c8-88e4-b9b563a46531

Deployment details (Download)

Resource	Type	Status	Operation details
easy-button-roleassignment-j	Microsoft.Resources/deploy...	OK	Operation details
easy-button-avdsetup-linked-	Microsoft.Resources/deploy...	OK	Operation details
qs1-avd	Microsoft.Resources/resour...	Created	Operation details
easy-button-prerequisitecom	Microsoft.Resources/deploy...	OK	Operation details
easy-button-prerequisite-user	Microsoft.Resources/deploy...	OK	Operation details
easy-button-prerequisite-job-	Microsoft.Resources/deploy...	OK	Operation details
easy-button-inputvalidation-j	Microsoft.Resources/deploy...	OK	Operation details
easy-button-deploymentReso	Microsoft.Resources/deploy...	OK	Operation details
qs1-deployment	Microsoft.Resources/resour...	Created	Operation details

Next steps

Figure 10: The Getting started feature deployed successfully

In this section, we ran through the deployment steps using the Azure Virtual Desktop Getting started feature to quickly deploy an Azure Virtual Desktop environment to an Azure subscription. We will next take a look at the deployment process in slightly more detail, where we will show you how to deploy a host pool.

Creating your first host pool manually (desktop)

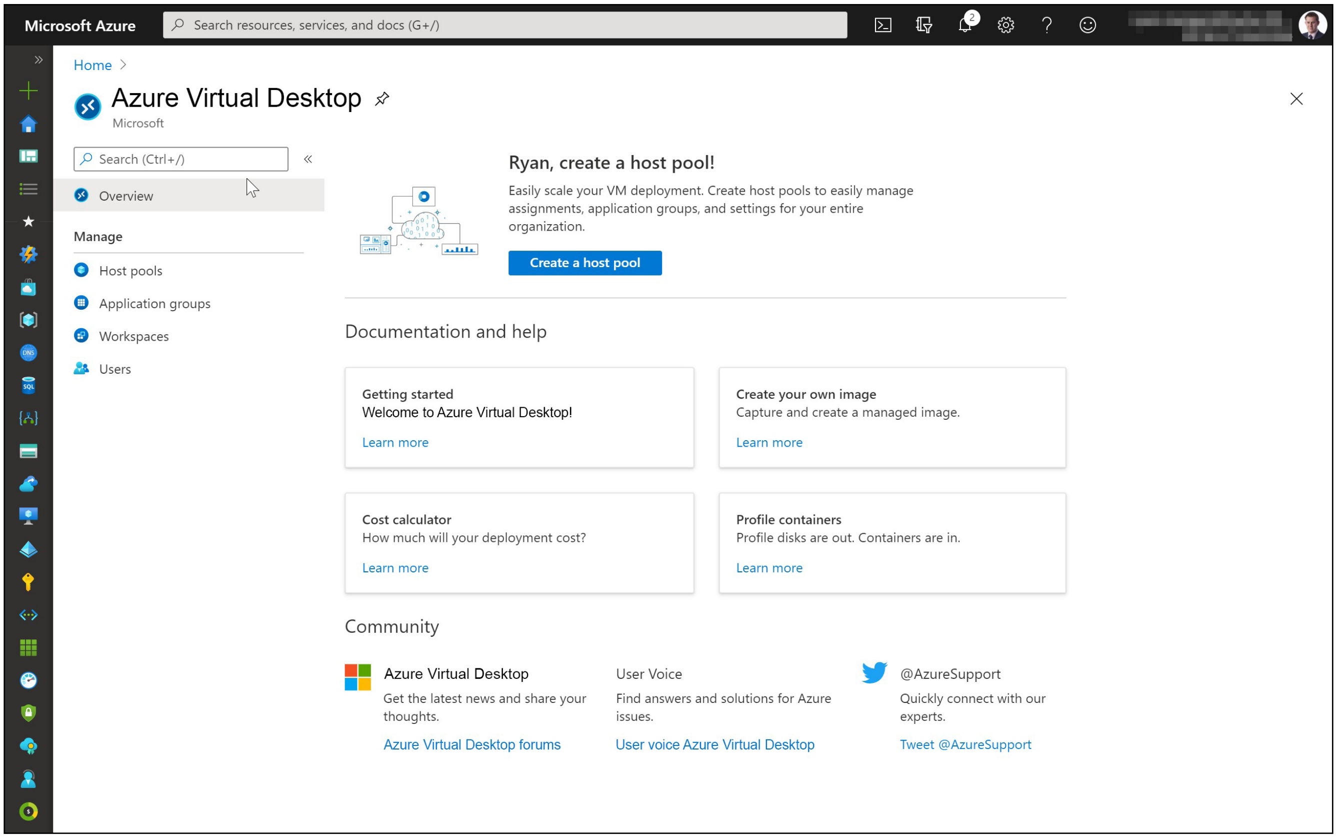
There are two ways to deploy host pools in Azure Virtual Desktop: with or without adding VMs. In this section, both types of deployment will be covered. If you select the option to not add VMs, you will need to configure the session hosts manually so that the host agent can communicate with Azure Virtual 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 Azure 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 Azure Virtual Desktop without using the provision feature when adding a host pool:

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



Microsoft Azure

Search resources, services, and docs (G+/)

[redacted]

Home >

Azure Virtual Desktop

Microsoft

Search (Ctrl+/)

Overview

Manage

Host pools

Application groups

Workspaces

Users

Ryan, create a host pool!

Easily scale your VM deployment. Create host pools to easily manage assignments, application groups, and settings for your entire organization.

Create a host pool

Documentation and help

Getting started
Welcome to Azure Virtual Desktop!
Learn more

Create your own image
Capture and create a managed image.
Learn more

Cost calculator
How much will your deployment cost?
Learn more

Profile containers
Profile disks are out. Containers are in.
Learn more

Community

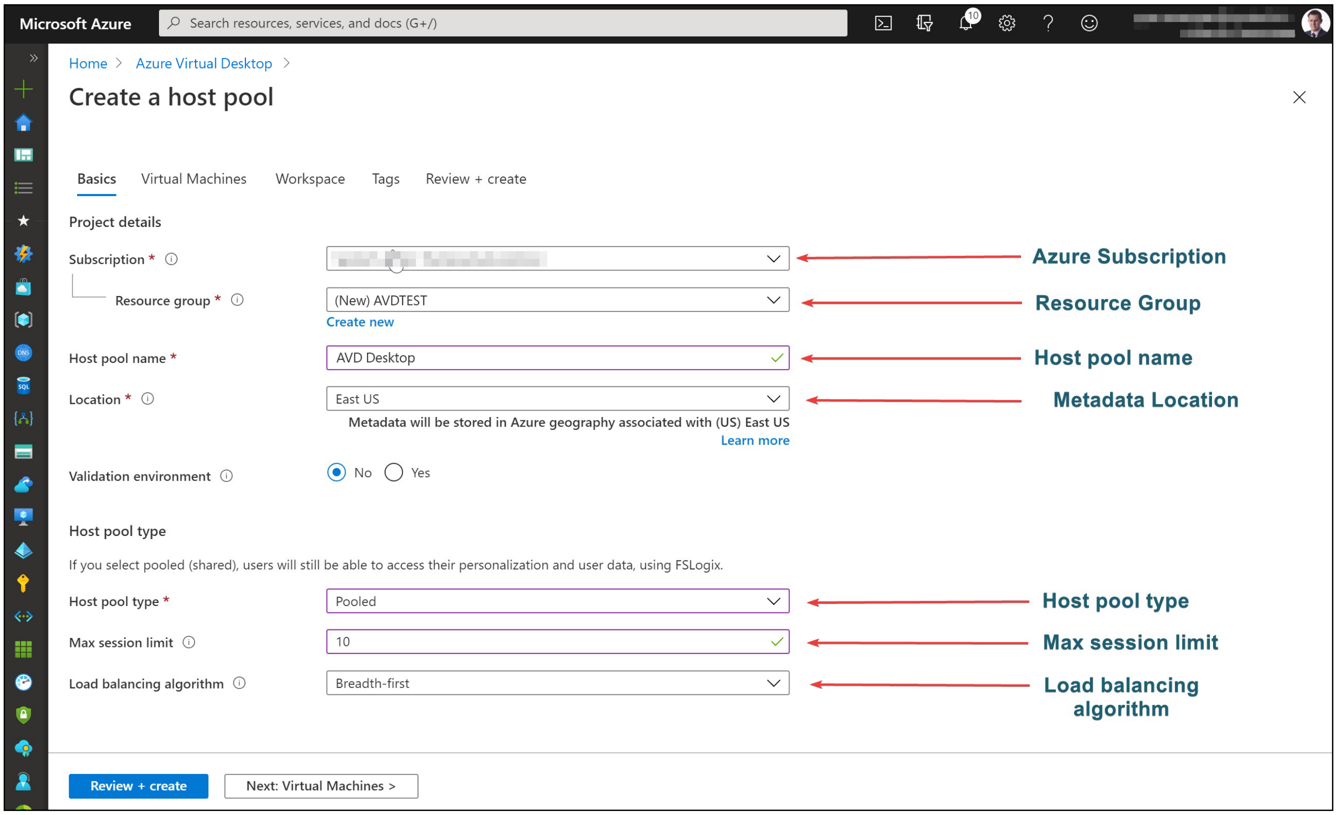
Azure Virtual Desktop
Get the latest news and share your thoughts.
Azure Virtual Desktop forums

User Voice
Find answers and solutions for Azure issues.
User voice Azure Virtual Desktop

@AzureSupport
Quickly connect with our experts.
Tweet @AzureSupport

Figure 11: Creating a host pool

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



Create a host pool

Project details

Subscription * [redacted]

Resource group * (New) AVDTEST

Host pool name * AVD Desktop

Location * East US

Metadata will be stored in Azure geography associated with (US) East US

Validation environment ● No ○ Yes

Host pool type

If you select pooled (shared), users will still be able to access their personalization and user data, using FSLogix.

Host pool type * Pooled

Max session limit 10

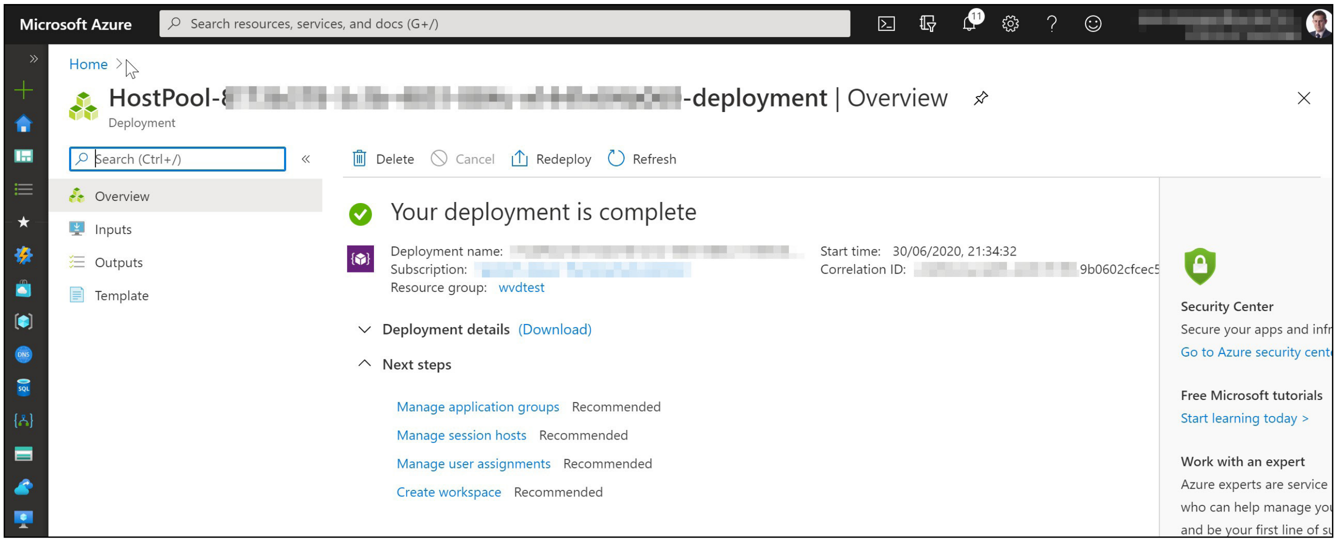
Load balancing algorithm Breadth-first

Figure 12: 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 **Create**.

Once the deployment is complete, navigate to the Azure Virtual Desktop service page in the Azure portal:



HostPool-[redacted]-deployment | Overview

Deployment

Your deployment is complete

Deployment name: [redacted]
Subscription: [redacted]
Resource group: wvdtest

Start time: 30/06/2020, 21:34:32
Correlation ID: [redacted]9b0602cfcec5

Deployment details (Download)

Next steps

Manage application groups Recommended
Manage session hosts Recommended
Manage user assignments Recommended
Create workspace Recommended

Security Center
Secure your apps and infr
Go to Azure security cent

Free Microsoft tutorials
Start learning today >

Work with an expert
Azure experts are service
who can help manage yo
and be your first line of s

Figure 13: The deployment overview

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

Find out more about registering VMs to the Azure Virtual Desktop host pool.

Deploy Azure AD–joined VMs in Azure Virtual Desktop

You can now deploy Azure AD–joined VMs within a host pool. This removes the need to have line-of-sight from the VM to an on-premises or virtualized AD DC or to deploy Azure AD DS. In some specific cases, it removes the need for a DC entirely, simplifying the overall deployment and management. You will also note that you can automatically enroll Azure AD–joined VMs in Intune for ease of management.

Supported configurations:

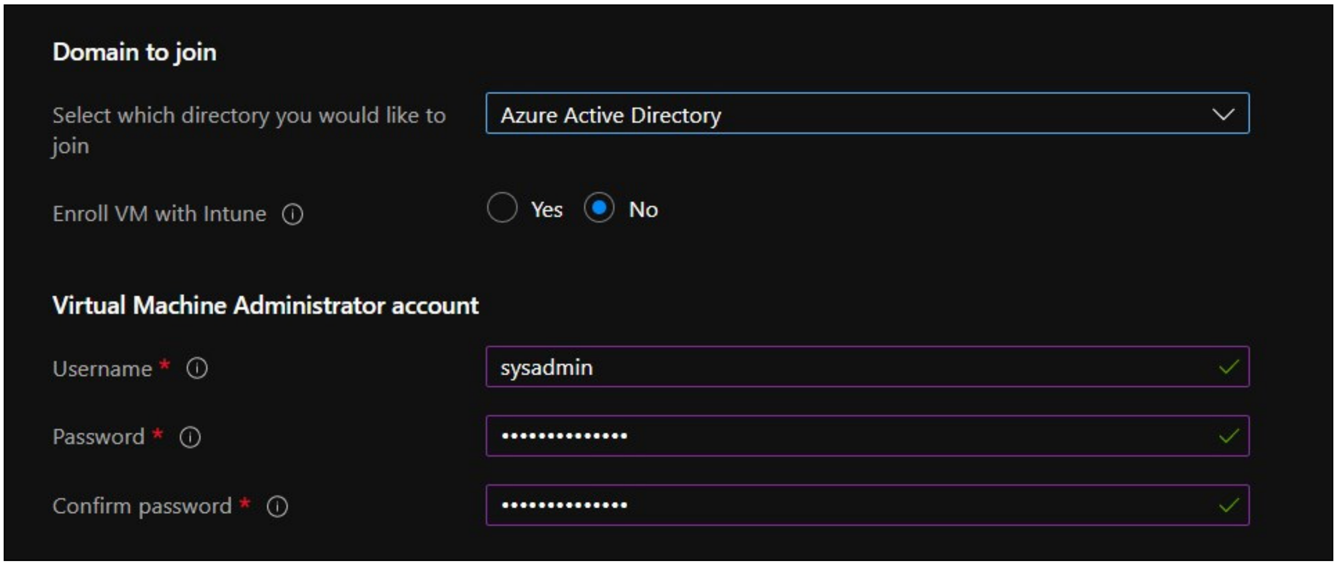
- Personal desktops with local user profiles.
- Pooled desktops used as a jump box. In this configuration, users first access the Azure Virtual Desktop VM before connecting to a different PC on the network. Users shouldn't save data on the VM.
- Pooled desktops or apps where users don't need to save data on the VM. For example, for applications that save data online or connect to a remote database.

Important:

When using Azure AD–joined VMs, only local profiles are supported.

The feature to deploy Azure AD–joined VMs is found within the host pool deployment wizard. Within the host pool deployment wizard's **Virtual Machines** tab, under the **Domain to join** section, you will see a dropdown list where you can select which directory you would like to join. The dropdown list provides a choice of both Active Directory and Azure AD. You will see from *Figure 14* that Azure AD has been selected, and you have the option to enroll the VM with Intune.

Figure 14 shows the section where you add VMs to a host pool, specifically the **Domain to join** section. This is where you would choose Azure AD as the domain to join.



Domain to join

Select which directory you would like to join: Azure Active Directory

Enroll VM with Intune ⓘ ○ Yes ● No

Virtual Machine Administrator account

Username * ⓘ sysadmin ✓

Password * ⓘ •••••••••••••• ✓

Confirm password * ⓘ •••••••••••••• ✓

Figure 14: Choosing Azure AD when deploying VMs within a host pool

Tip: *Selecting Azure Active Directory gives you the option to enroll the VM with Intune automatically so you can easily manage Windows 10 Enterprise and Windows 10 Enterprise multi-session VMs.*

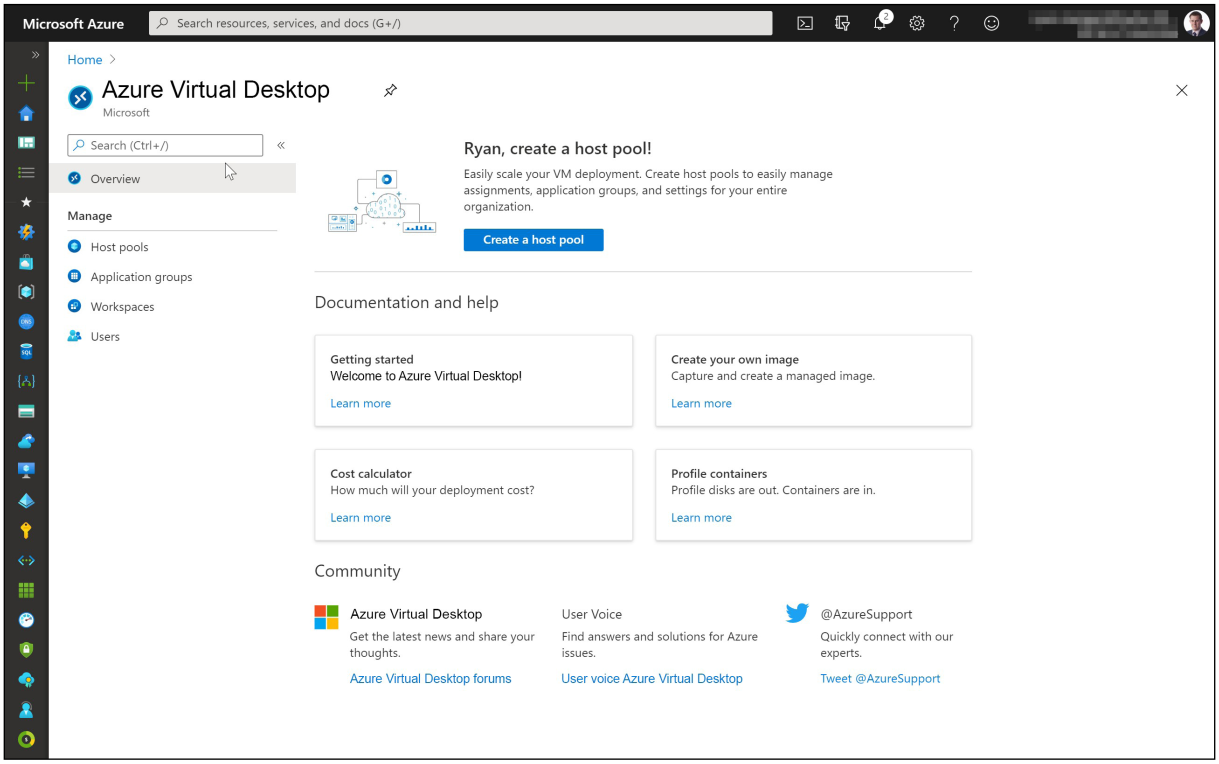
It is also important to note that if you are using Azure AD–joined VMs, you will need to configure a custom RDP property to the host pool "targetisaadjoined:i:1" for users using web, Android, macOS, and iOS clients. These connections are restricted to entering a username and password when signing in to the session host.

This section looked at deploying VMs using the Azure AD domain joined feature. We now move on to look at creating a host pool and adding VMs.

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

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

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



Ryan, create a host pool!

Easily scale your VM deployment. Create host pools to easily manage assignments, application groups, and settings for your entire organization.

Documentation and help

Getting started
Welcome to Azure Virtual Desktop!
Learn more

Create your own image
Capture and create a managed image.
Learn more

Cost calculator
How much will your deployment cost?
Learn more

Profile containers
Profile disks are out. Containers are in.
Learn more

Community

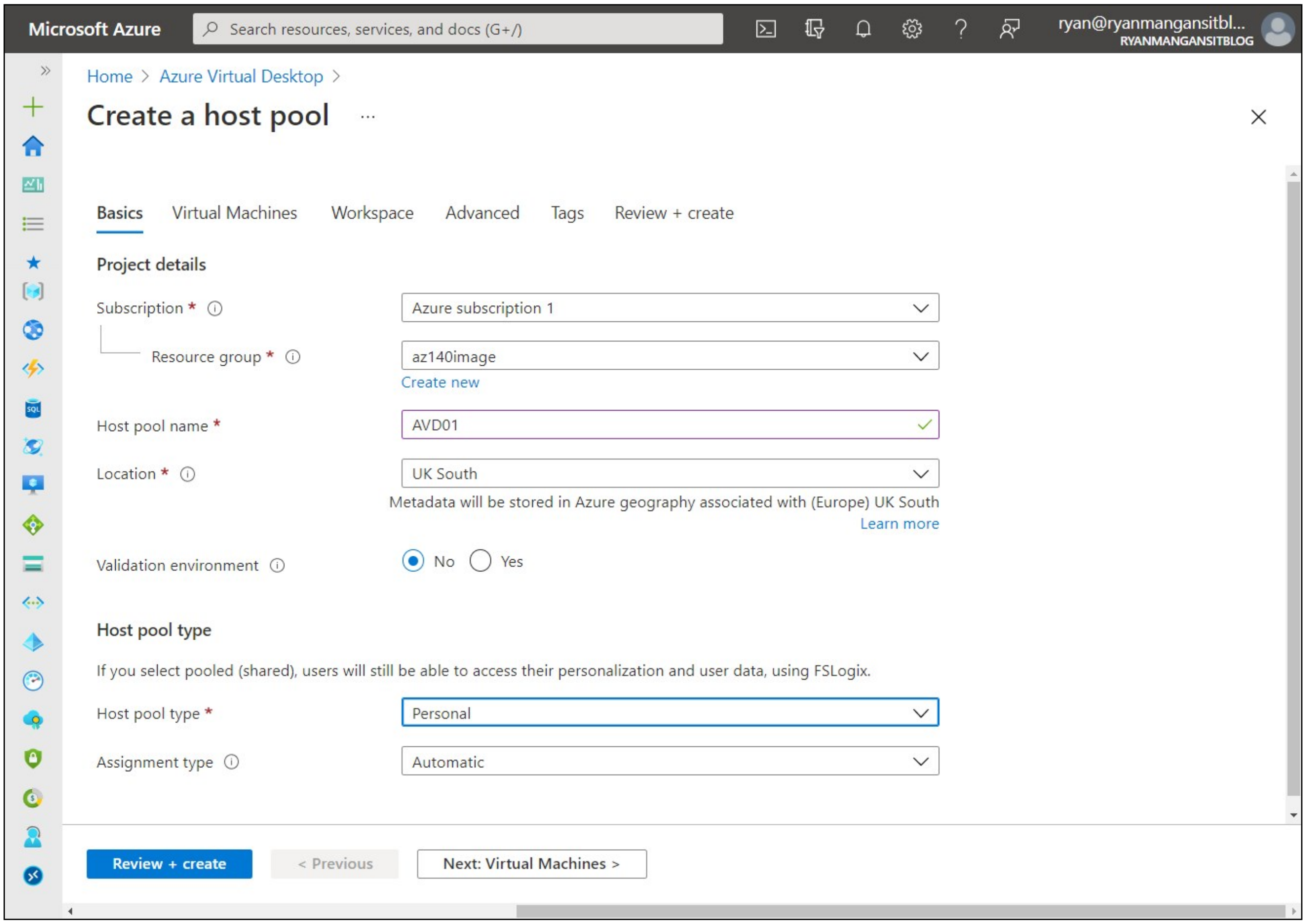
Azure Virtual Desktop
Get the latest news and share your thoughts.
Azure Virtual Desktop forums

User Voice
Find answers and solutions for Azure issues.
User voice Azure Virtual Desktop

@AzureSupport
Quickly connect with our experts.
Tweet @AzureSupport

Figure 15: 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 **Personal** for **Host pool type**:



Create a host pool

Project details

Subscription * : Azure subscription 1

Resource group * : az140image

Create new

Host pool name * : AVD01

Location * : UK South

Metadata will be stored in Azure geography associated with (Europe) UK South Learn more

Validation environment: ● No ○ Yes

Host pool type

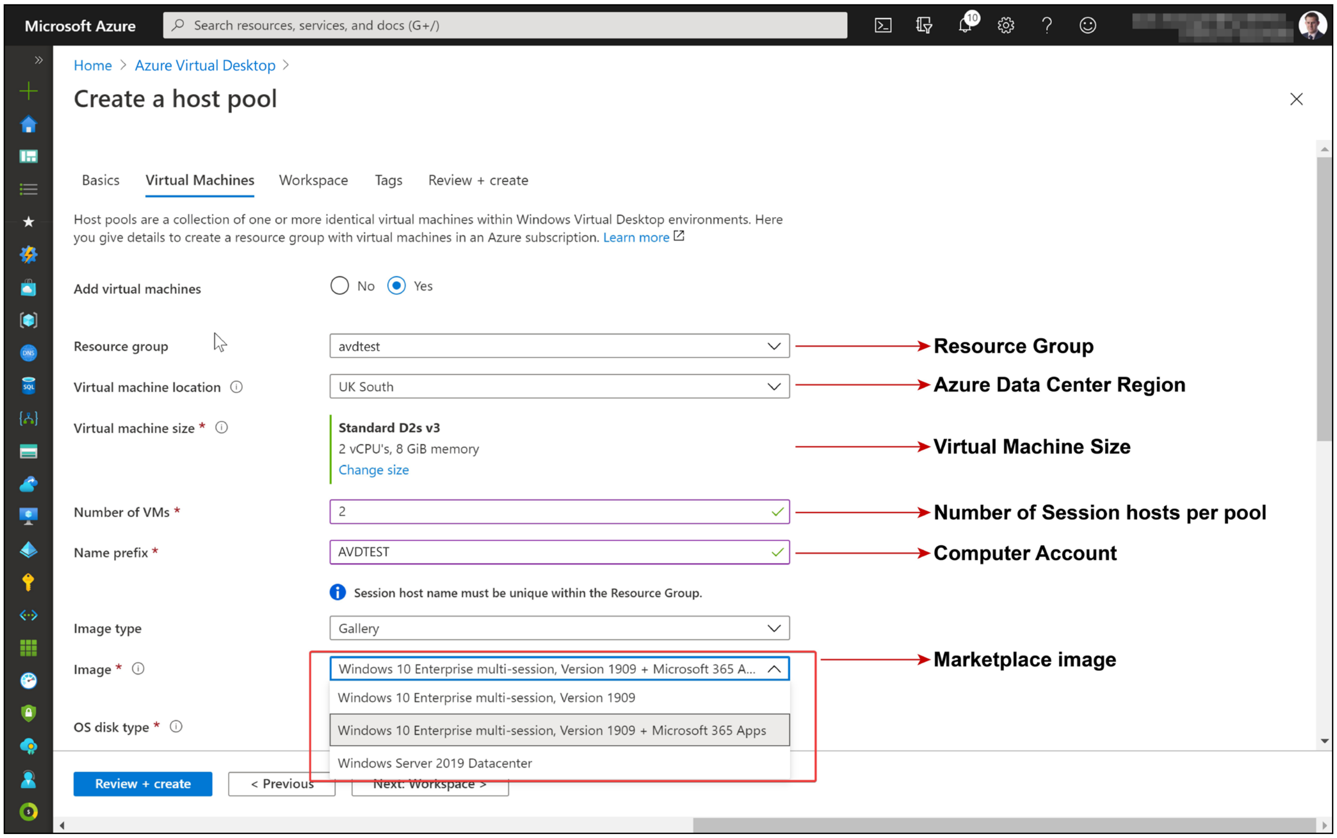
If you select pooled (shared), users will still be able to access their personalization and user data, using FSLogix.

Host pool type * : Personal

Assignment type: Automatic

Figure 16: 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 **Next: Workspace**:



Create a host pool

Host pools are a collection of one or more identical virtual machines within Windows Virtual Desktop environments. Here you give details to create a resource group with virtual machines in an Azure subscription. Learn more

Add virtual machines ○ No ● Yes

Resource group: avdtest

Virtual machine location: UK South

Virtual machine size *: Standard D2s v3, 2 vCPU's, 8 GiB memory, Change size

Number of VMs *: 2

Name prefix *: AVDTEST

Session host name must be unique within the Resource Group.

Image type: Gallery

Image *: Windows 10 Enterprise multi-session, Version 1909 + Microsoft 365 A...

- Windows 10 Enterprise multi-session, Version 1909
- Windows 10 Enterprise multi-session, Version 1909 + Microsoft 365 Apps
- Windows Server 2019 Datacenter

OS disk type *

Resource Group

Azure Data Center Region

Virtual Machine Size

Number of Session hosts per pool

Computer Account

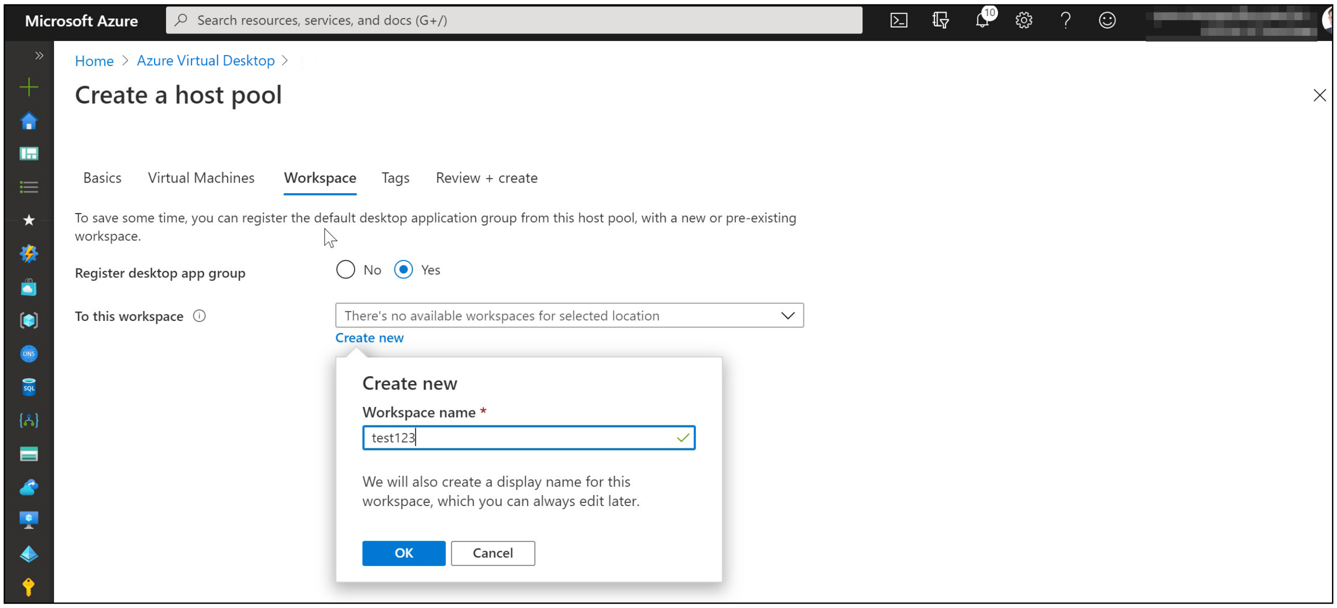
Marketplace image

Figure 17: 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 percomputer 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** and then **Create**:



To save some time, you can register the default desktop application group from this host pool, with a new or pre-existing workspace.

Register desktop app group ○ No ● Yes

To this workspace: There's no available workspaces for selected location

Create new

Create new

Workspace name *: test123

We will also create a display name for this workspace, which you can always edit later.

Figure 18: Creating a workspace and deployment

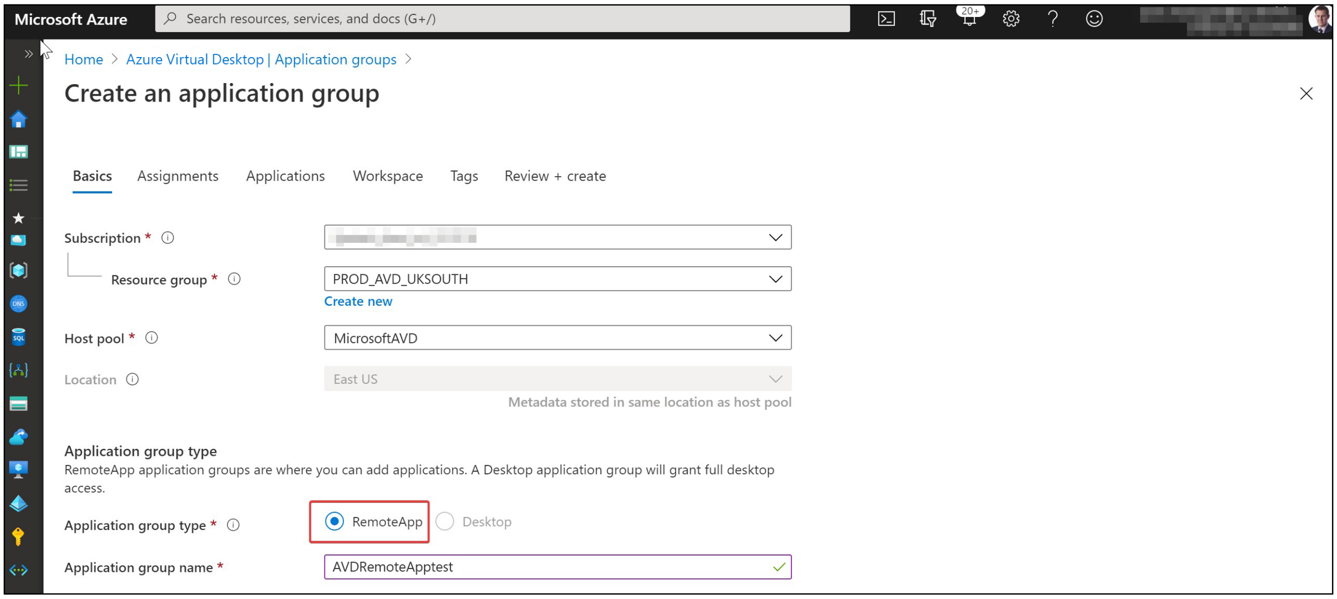
The final step is to assign a desktop application group to the user.

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 remote applications:

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



Home > Azure Virtual Desktop | Application groups >

Create an application group

Basics | Assignments | Applications | Workspace | Tags | Review + create

Subscription *

Resource group * PROD_AVD_UKSOUTH

Create new

Host pool * MicrosoftAVD

Location East US

Metadata stored in same location as host pool

Application group type

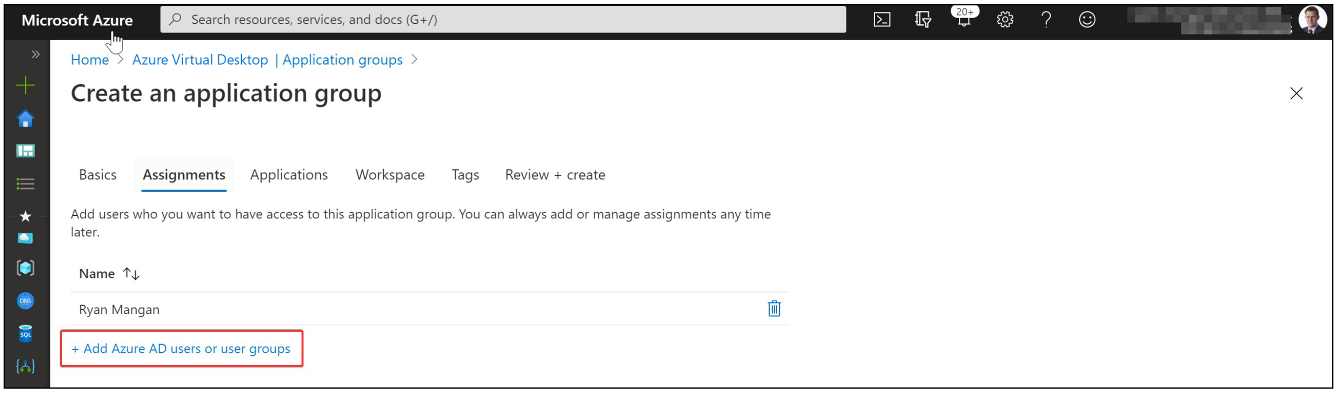
RemoteApp application groups are where you can add applications. A Desktop application group will grant full desktop access.

Application group type * ● RemoteApp ○ Desktop

Application group name * AVDRemoteApptest

Figure 19: Configuring the application group and the host pool

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



Home > Azure Virtual Desktop | Application groups >

Create an application group

Basics | Assignments | Applications | Workspace | Tags | Review + create

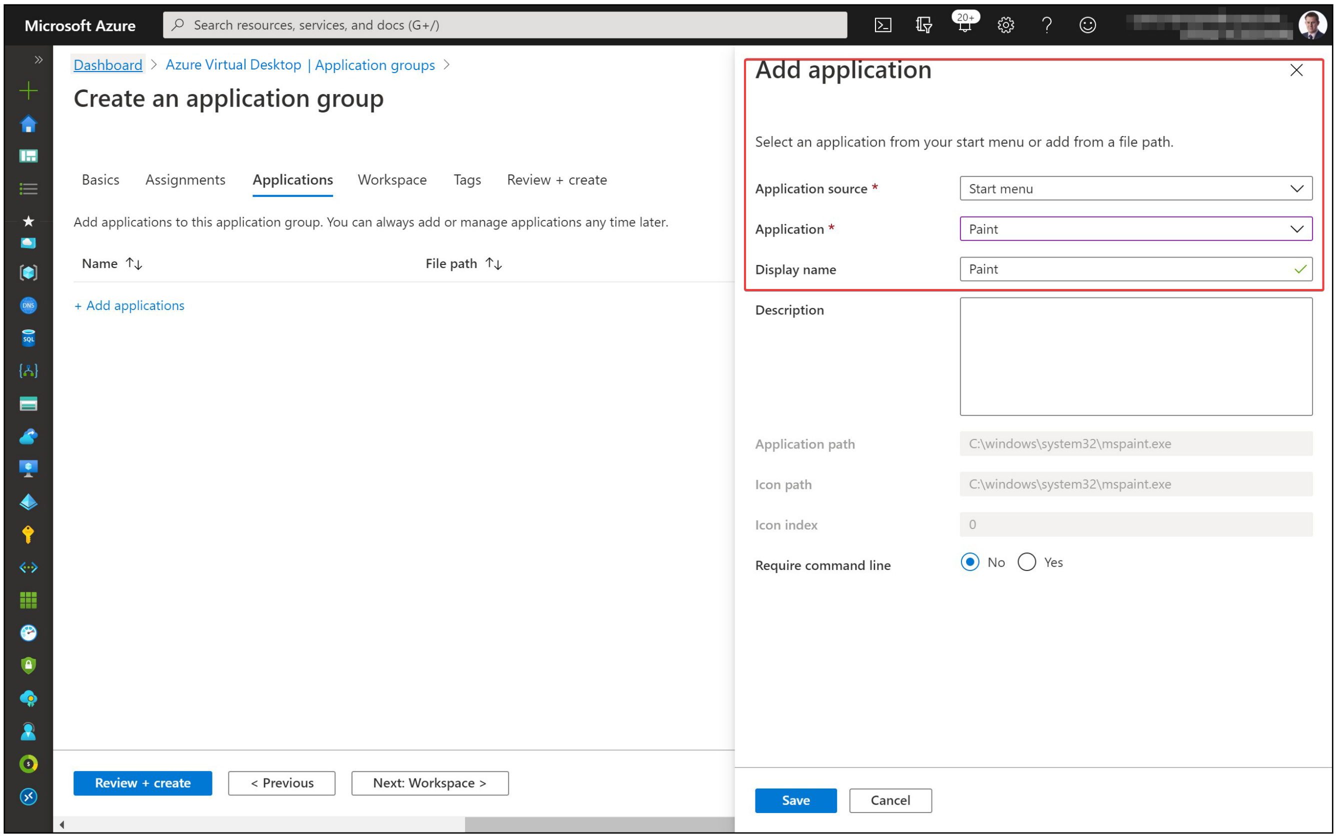
Add users who you want to have access to this application group. You can always add or manage assignments any time later.

Name ↑↓
Ryan Mangan

+ Add Azure AD users or user groups

Figure 20: 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:



Create an application group

Add applications to this application group. You can always add or manage applications any time later.

Add application

Select an application from your start menu or add from a file path.

Application source * : Start menu

Application * : Paint

Display name: Paint

Description:

Application path: C:\windows\system32\mspaint.exe

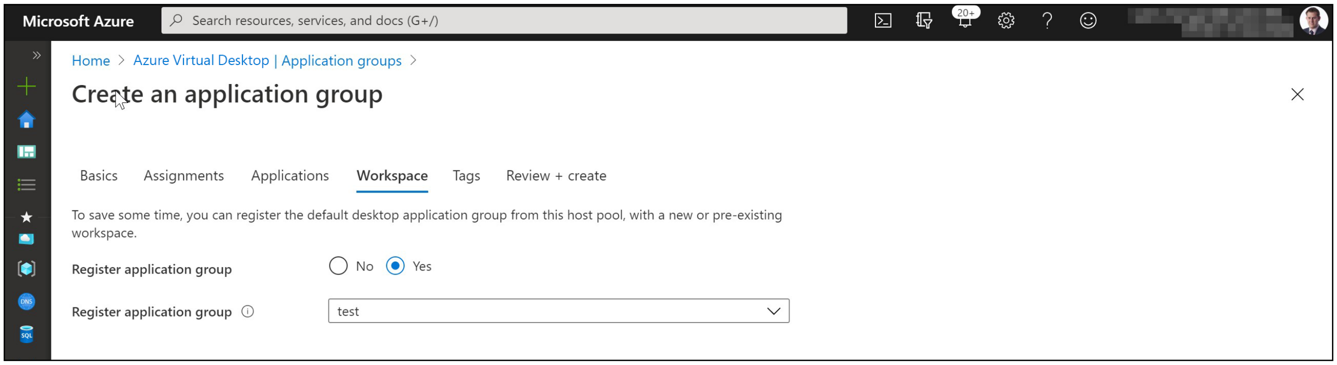
Icon path: C:\windows\system32\mspaint.exe

Icon index: 0

Require command line: ● No ○ Yes

Figure 21: Adding remote applications

4. Register the application group with a workgroup:


Microsoft Azure
Search resources, services, and docs (G+/)
20+
Home > Azure Virtual Desktop | Application groups >
Basics
Assignments
Applications
Workspace
Tags
Review + create

Create an application group

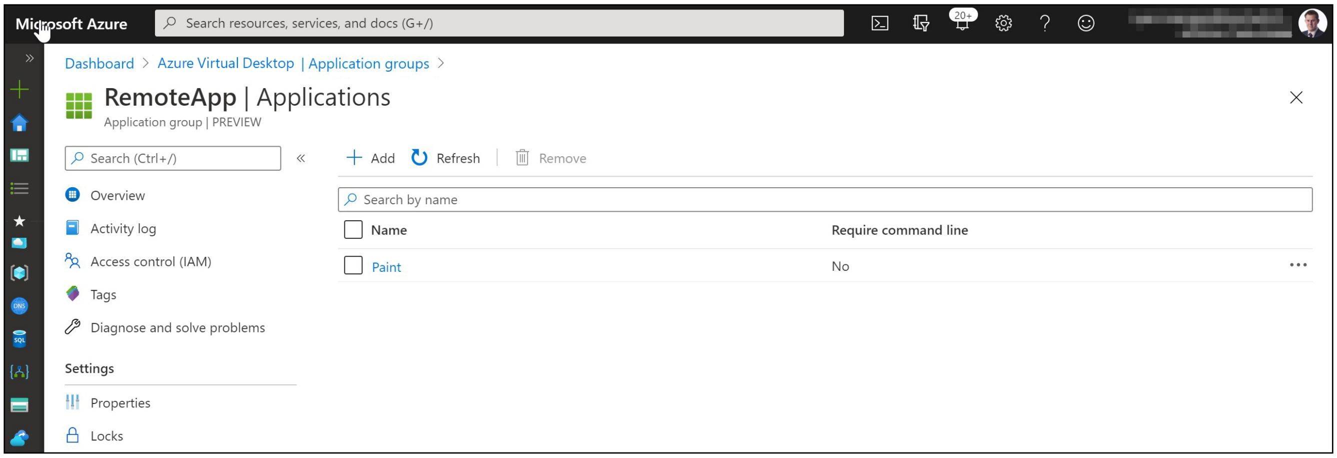
To save some time, you can register the default desktop application group from this host pool, with a new or pre-existing workspace.

Register application group: ○ No ● Yes

Register application group ⓘ: test

Figure 22: 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:



Name	Require command line
Paint	No

Figure 23: Reviewing the applications

Getting started with the Azure Virtual Desktop client

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

> **Important:**
>
> *Please note you have the option to* ***Subscribe*** *using either the Subscribe button for email or* ***Subscribing with URL****.*

Click here to download the Azure Virtual Desktop client for Windows.

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

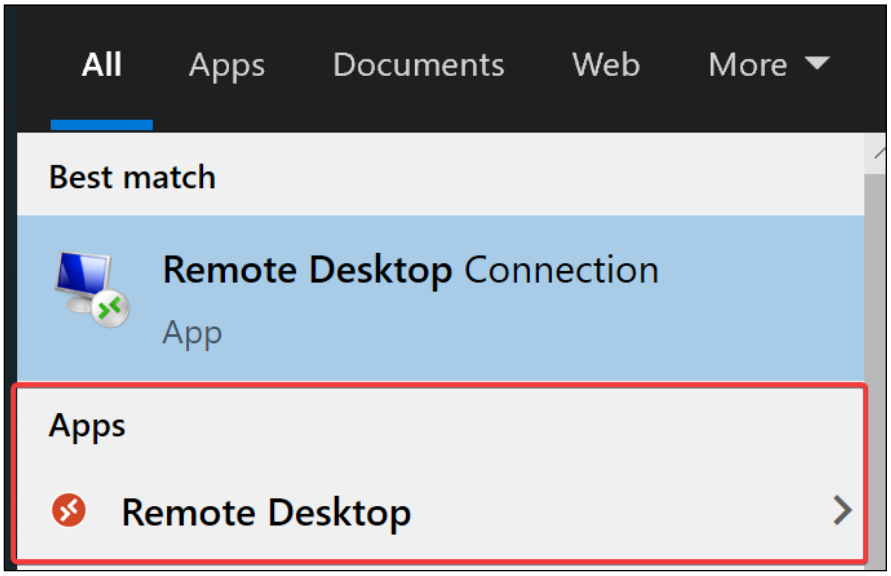
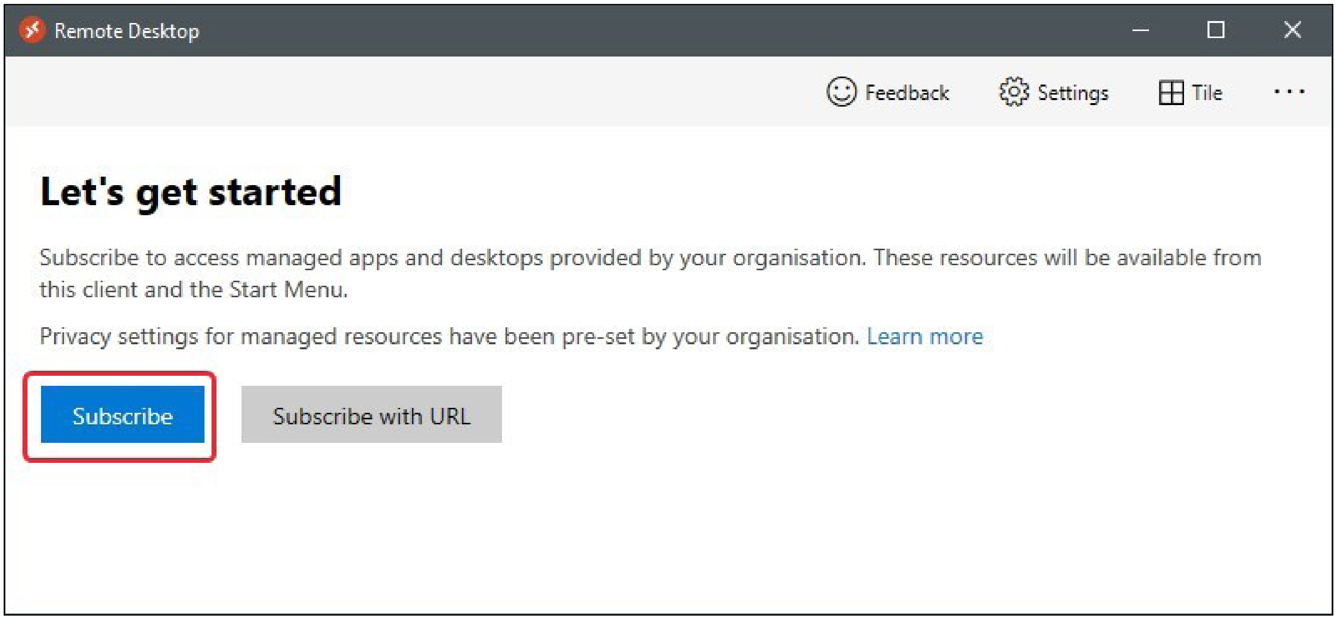


Figure 24: The Remote Desktop icon in the Start menu

2. Select **Subscribe**:



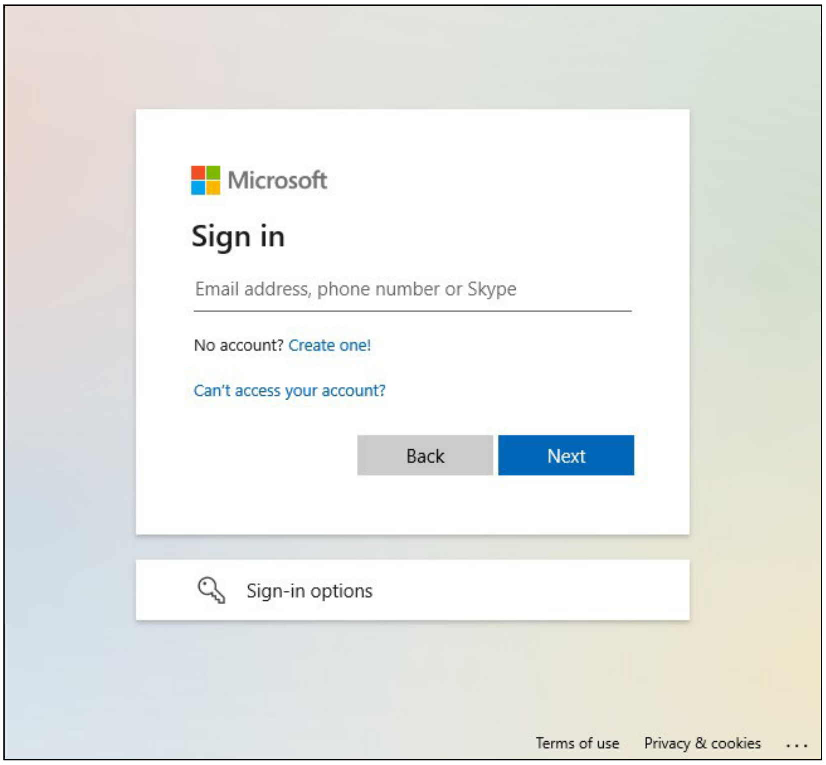
Let's get started

Subscribe to access managed apps and desktops provided by your organisation. These resources will be available from this client and the Start Menu.

Privacy settings for managed resources have been pre-set by your organisation. Learn more

Figure 25: Choosing the option for subscription

3. Enter your email address and password:



Microsoft

Sign in

Email address, phone number or Skype

No account? Create one!

Can't access your account?

Figure 26: The Sign in page

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 and desktop resources will now appear in the Remote Desktop client:

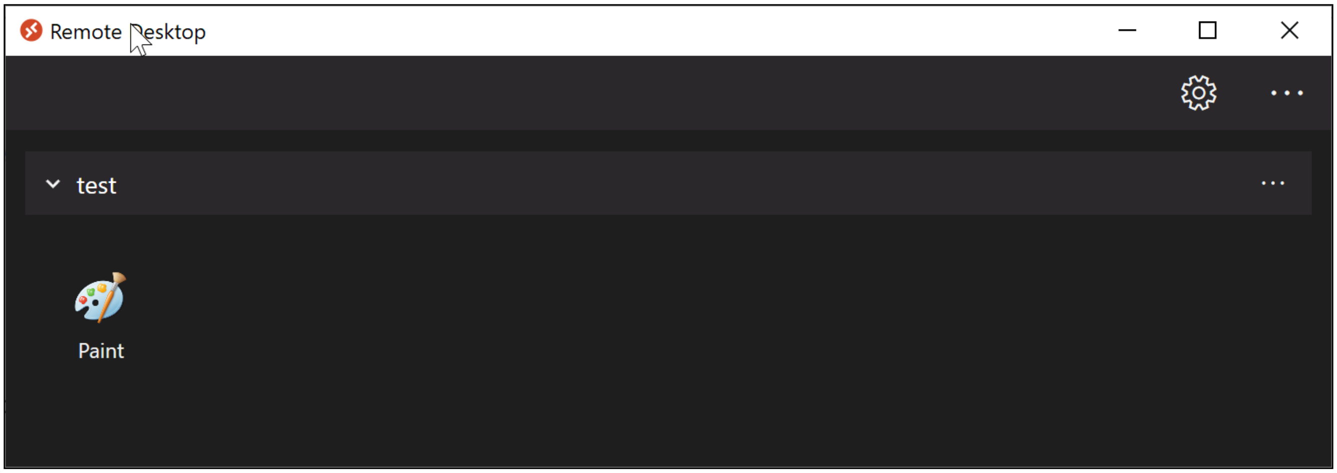
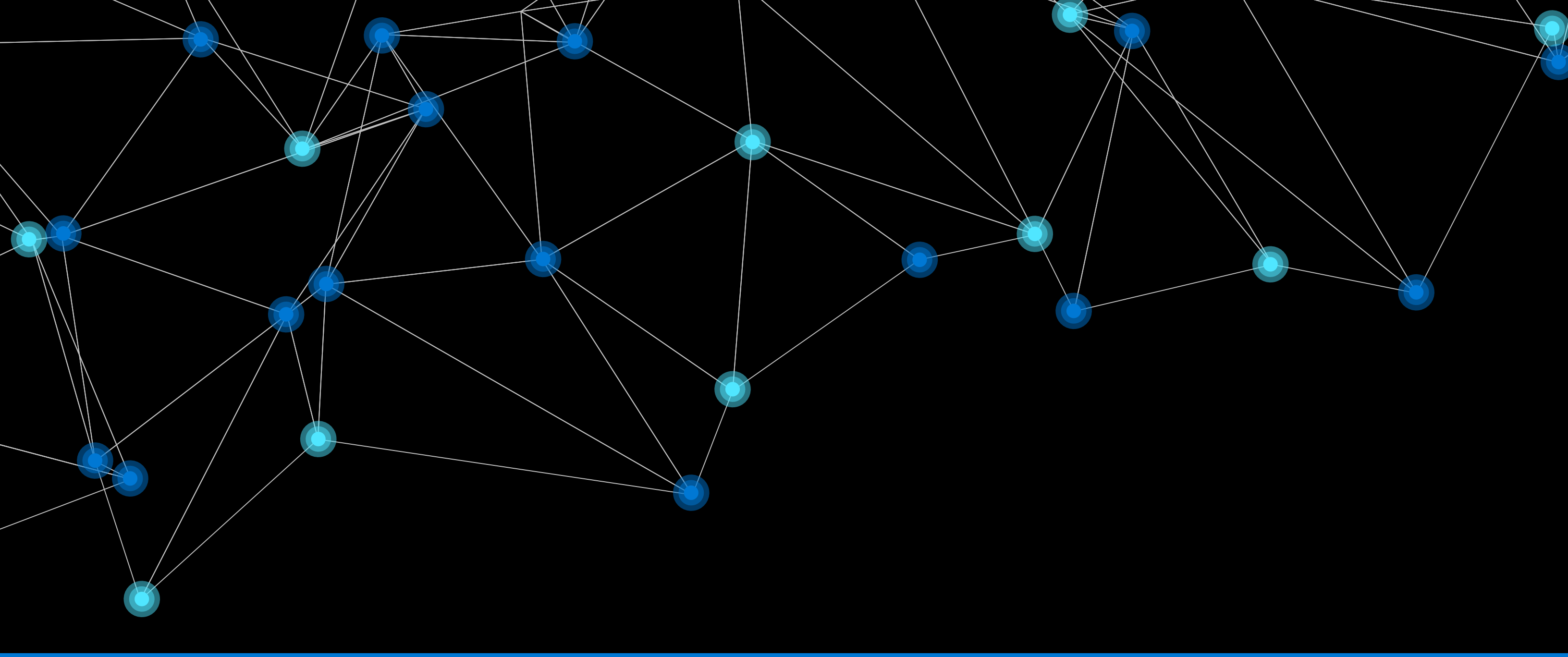


Figure 27: The Remote Desktop client



Section 3: Azure Virtual Desktop optimization

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

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

These are some Azure 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 VM sizes.

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 Azure 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.

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 suggested maximum 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 to your Azure 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.	Can sync with on-premises DCs if a VPN or ExpressRoute is configured All familiar Active Directory Group Policies can be used. VMs can be paused or stopped when needed to reduce costs.	Adds additional management of a VM and Active Directory in Azure.
For cloud-based organizations, use Azure AD DS.	Great for test or isolated environments that do not need connectivity to on-premises resources. Azure AD will be your leading source for identities.	Azure AD DS will always be running, resulting in a fixed change per month.
For hybrid organizations, use VPN or ExpressRoute and make sure your on-premises DCs can be found in Azure.	No management of a VM and Active Directory in Azure. No Azure AD DS or DC is required in Azure.	Latency could increase, adding delays during user authentication to VMs. This assumes you have an on-premises environment; it's not suitable for cloud-only tests.
Use Azure AD–joined VMs.	Reduced cost. Supports cloud-only users. No Azure AD DS or DCs required.	Currently only supports local profiles. May still require Active Directory for legacy Kerberos applications and SMB shares.

Security capabilities and best practices for Azure Virtual Desktop

Azure 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 Azure 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

Azure 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 Azure Virtual Desktop environment:

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

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

- Azure activity logs
- Azure AD activity logs
- Session hosts
- Azure Virtual Desktop diagnostic logs
- Key Vault logs

Learn more about Azure security here.

Four security tips for your Azure Virtual Desktop environment

Use these additional security tips to help keep your customers' Azure 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 your choice. It is also recommended that you install an endpoint detection and response (EDR) product to provide advanced detection and response capabilities on Azure 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 Azure 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, Azure Virtual Desktop provides a diagnostics 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 Azure Virtual Desktop, see Use Log Analytics for the diagnostics feature.

Any connections that don't reach Azure Virtual Desktop won't show up in diagnostics results because the diagnostics role service itself is part of Azure Virtual Desktop, and you would need to use additional tools to identify the issue.

Please use this article to find out more about the different methods to identify and diagnose Azure Virtual Desktop issues.

Typically, Azure 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.

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 users 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 Azure Virtual Desktop.

Summary and resources

Thank you for reading the Quickstart Guide to Azure Virtual Desktop, Second Edition. We hope you feel more prepared to start your journey with Azure Virtual Desktop! To help you get started, here are a few key references:

1. Read more Azure Virtual Desktop documentation to get the latest technical guidance.
2. Take a tutorial on getting started with Azure Virtual Desktop.
3. Sign up for an Azure free account to try deploying your virtualized Windows desktops and apps.
4. Get in touch with Azure sales to discuss pricing, technical requirements, and short- and long-term solutions for enabling secure remote work.
5. Join the Azure Migration and Modernization program for curated guidance and support to migrate your VDI.

Deploy and scale your virtualized Windows desktops and apps on Azure

Get started with 12 months of free services

assessment_2_13_2019_6_34_1

Assessment

Migration project : Demo

Group : contosopayroll

Status : Ready (Tuesday, February 19, 2019, 1:22:58 AM)

Confidence rating : *****

Target location : UK South

Sizing criterion : Performance-based

Azure Hybrid Benefit : Yes

Currency : US Dollar ($)

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 Azure 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 secure 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 an Azure 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 Azure Virtual Desktop remote apps and desktops from any internet-connected device that can run an Azure 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 VMs that act as session hosts for Azure Virtual Desktop. Users gain 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 host pools, you can use one of the recommended images that includes Windows 10 Enterprise multi-session. This operating system is exclusive to Azure 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. It 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 Azure 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 Azure Virtual Desktop. When a user signs in to Azure 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 Azure Virtual Desktop. Some of Ryan's community and technical awards include:

- Author of:
  -An Introduction to MSIX App Attach
  -Azure Virtual Desktop Migration Guides for RDS, Citrix, and VMware
  -Azure Virtual Desktop Technical Handbook series
- VMware vExpert******** eight 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—Feedspot
- Top 50 Azure Blogs 2020—Feedspot
- GitHub: https://github.com/RMITBLOG

This document is provided "as is." Information and views expressed in this document, including URL and other internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.