



Azure Virtual Desktop L300 Presentation

Sven Langenfeld

Table of contents

What's new	New Azure Virtual Desktop feature updates
Concepts	What is Azure Virtual Desktop? Azure Virtual Desktop key concepts Azure Virtual Desktop architecture
Building your cloud VDI foundation	Performance requirements & sizing guidelines User experience
Securing, managing, and optimizing Azure Virtual Desktop	Security approach Management & monitoring Availability & resilience Cost & performance optimization Azure Virtual Desktop for Azure Stack HCI
Partners and migration	Migration considerations Citrix & VMware capabilities ISV partners
Positioning and competitive overview	Azure Virtual Desktop or Windows 365? Competitive solutions



Azure Virtual Desktop new updates

[Back to table of contents](#)

Windows App (preview)

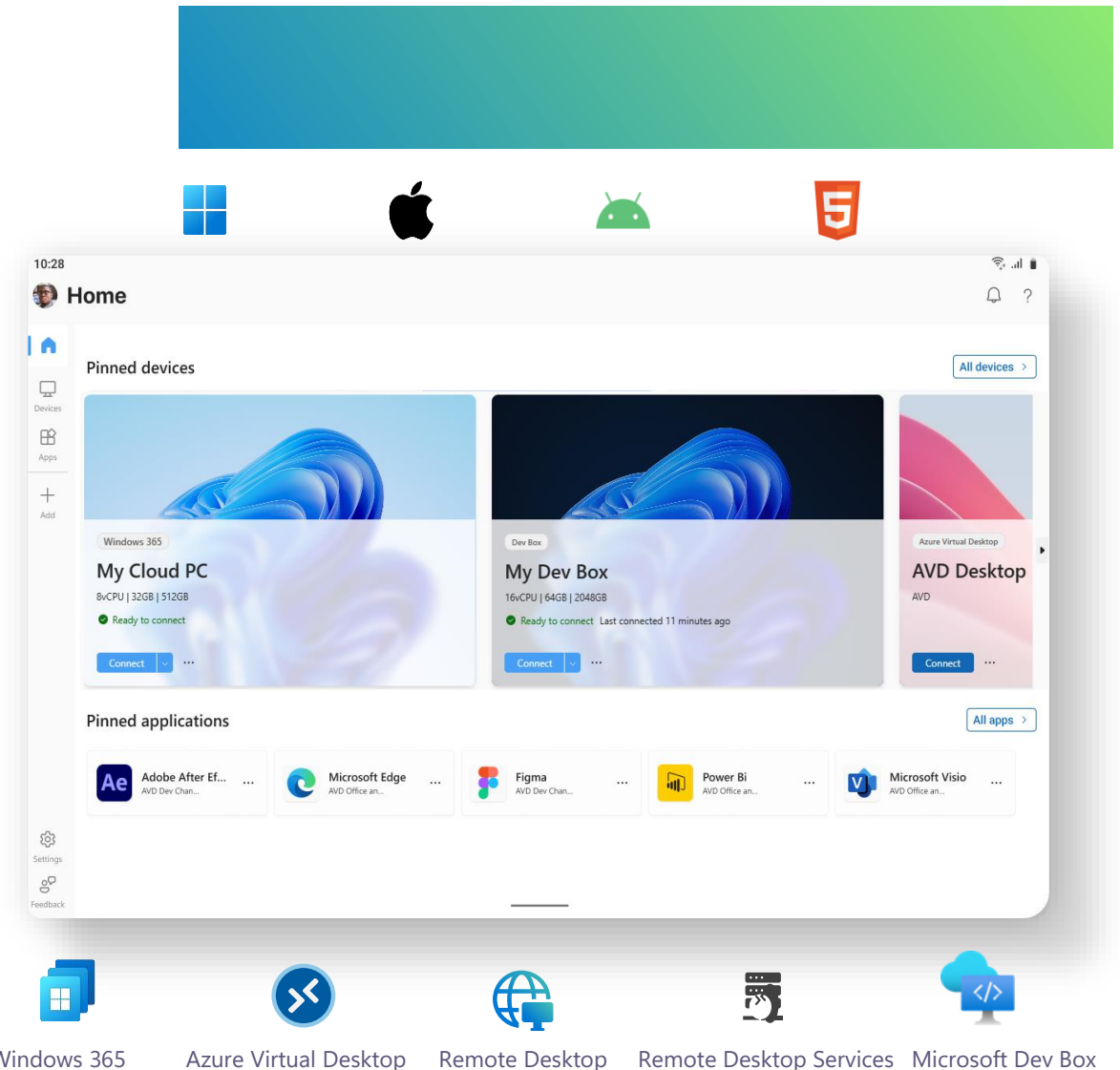
Windows App is a unified client on Windows, iOS, Android, Mac, and Web that can access Windows 365, Azure Virtual Desktop, Remote Desktop Services, Remote Desktop, Microsoft Dev Box, and more.

Windows App allows easy access to multiple services across client platforms with a simple and unified experience.

Windows and Web public preview access

Windows 365 app users: A preview toggle is on the app which, if enabled, turns on the Windows App experiences and, if disabled, returns them to the current Windows 365 app experiences.

Windows 365 users on the web: A banner will redirect to the new Windows App web portal and can return to the Windows 365 web portal by going to windows365.com.



Azure Virtual Desktop: App attach (preview)

Applications can be assigned to any host pool or VM within a region, including desktop and RemoteApp sessions.

Users in any host pool can have unique application combinations without requiring a maintenance window or session interruption, thus helping separate the application lifecycle from image lifecycle, resulting in fewer gold images.

Steps to configure:

- Expand your MSIX package to disk image
- Import to Azure Virtual Desktop
- Assign to users and hostpools

The screenshot displays two overlapping panels from the Azure Virtual Desktop console. The top panel, titled 'Terminal Preview | Host pools', shows an 'App attach package' configuration page. It includes a search bar, '+ Assign', 'Refresh', and 'Remove' buttons. A table lists the assigned host pools:

Host pool ↑	Location
DesktopWin11	UK South

The bottom panel, titled 'Terminal Preview | Users', shows the 'App attach package' configuration for users. It includes a search bar, '+ Add', 'Refresh', and 'Remove' buttons. A table lists the assigned users:

Filter by Name	Display name
	User2

Both panels feature a left-hand navigation menu with sections for 'Settings' (Locks, Configuration, Properties) and 'Manage' (Host pools, Users).

FSLogix enhancements

Enhancement 1 (generally available)

FSLogix configuration settings are available from Microsoft Intune Settings Catalog, which simplify configuration and management for Azure Virtual Desktop in the Microsoft Cloud.

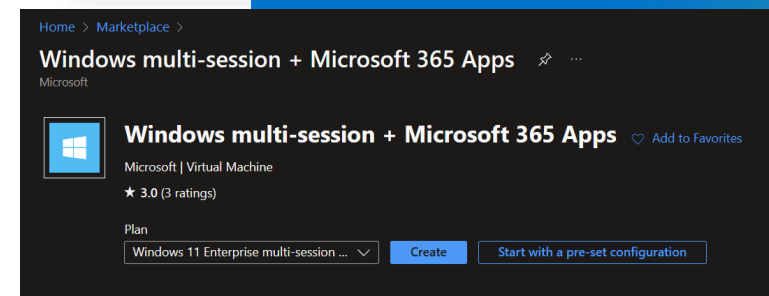
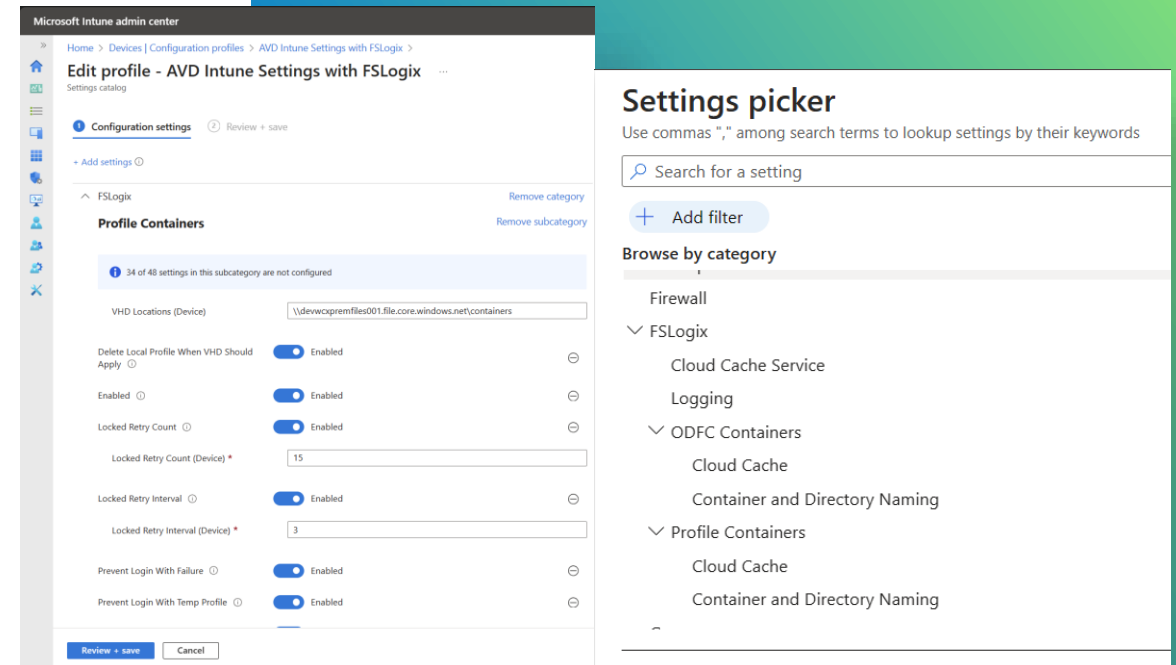
Enablement requirement:

Create new configuration policy

- Platform: Windows 10 or later
- Type: Settings Catalog
- Add settings (FSLogix)

Enhancement 2 (generally available)

Azure Marketplace Windows multi-session images contain the latest version of FSLogix.



What is Azure Virtual Desktop?

[Back to table of contents](#)

Azure Virtual Desktop is a cloud VDI solution designed to meet the challenges of remote work

Enable a secure,
remote desktop
experience
from anywhere



Access Windows 11 and Windows 10 from anywhere



Maintain full control over configuration and management



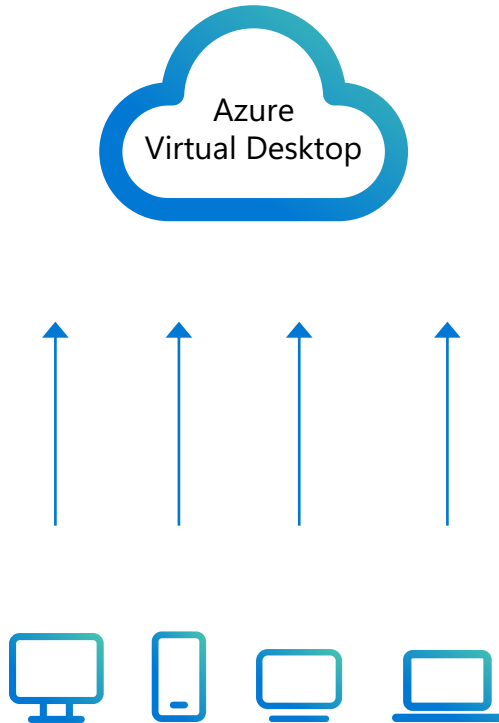
Get the security and reliability of Azure



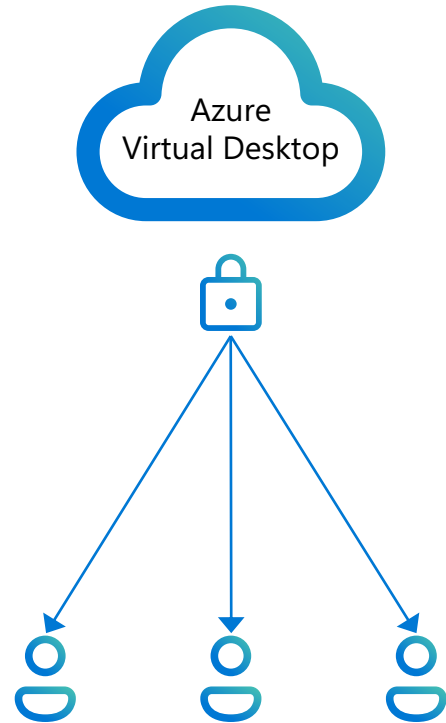
Optimize cost with multi-session and pay for only what you use

Here's what you can do when you run Azure Virtual Desktop on Azure

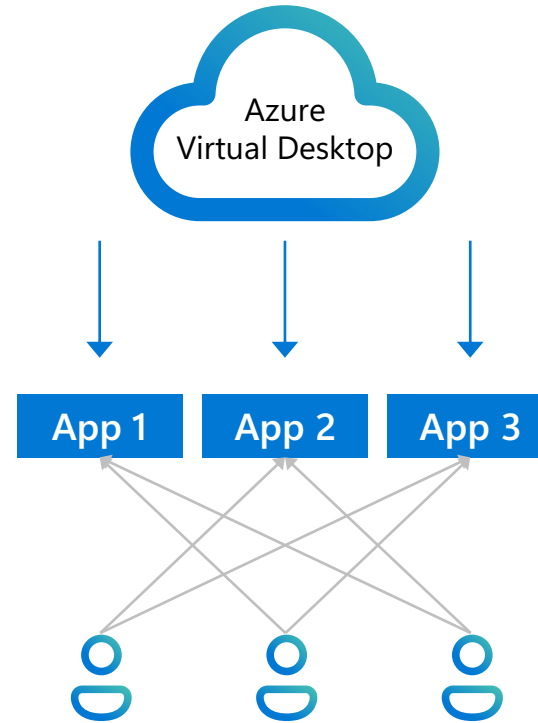
Access your org's apps from anywhere on any device



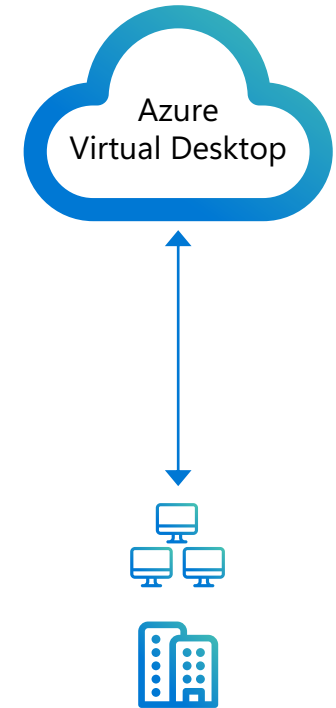
Create secure, customized PC experiences for every user



"SaaSify" your custom apps and stream them to users



Gain efficiencies by migrating existing VDI to the cloud



Azure Virtual Desktop

Provide your employees with a full desktop and access to remote apps.

Focus on policies and controls rather than managing infrastructure.


Connect from any device of your choice.


Desktops & remote apps


 Full desktop

 Remote app

Management & policies

 Image, app, and profile management

 User density, VM sizing, and scaling policies

 User management and identity

 Networking policies



Azure Virtual Desktop service

Azure Virtual Desktop simplifies VDI management

- Microsoft and Azure manage the entire infrastructure for you.
- Focus only on the users, apps, and OS images you need to use.
- Use Azure portal or automate deployment using ARM template.
- Easily scale by adding any number of hosts to a host pool.
- Use built-in monitoring with Azure Monitor and Log Analytics.

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

Virtual machine location

Virtual machine size *
2 vCPU's, 8 GiB memory
[Change size](#)

Number of VMs *

Name prefix *

i Session host name must be unique within the Resource Group.

Image type

Azure Virtual Desktop unlocks hybrid work scenarios



Data security

Improve regulatory compliance and IP protection via data centralization and a reduced threat surface.



High-capacity computing

Get cloud-scale compute and storage to support specialized workloads such as design and development.



BYOPC programs

Enable secure virtual desktops, even on personal devices.



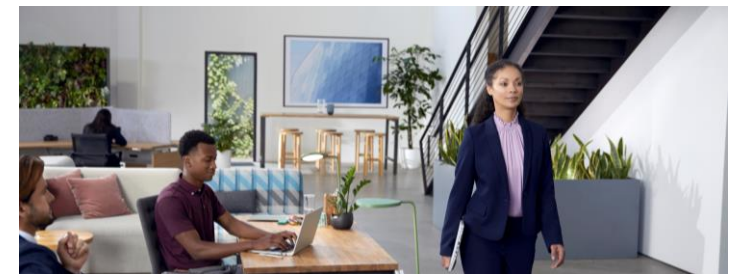
Disaster recovery

Help ensure continuity and access for your workforce and company data even in the most challenging circumstances.



Temporary workforces

Simplify and accelerate the onboarding and offboarding process for elastic workforces.



Mergers & acquisitions

Provide seamless transitions and access for growing businesses.

Azure Virtual Desktop uses innovative technology to deliver a more secure and cost-effective user experience



[Windows 11 and Windows 10 multi-session](#) enables you to add more users per virtual machine (VM)



[FSLogix](#) optimizations for user profiles gives you a consistent, seamless local-desktop-like experience.



[Single sign-on and passwordless authentication](#) provides a safer and simpler sign-in experience for users.



[Multimedia redirection](#) enables you to use [Microsoft Teams](#) for video and audio.

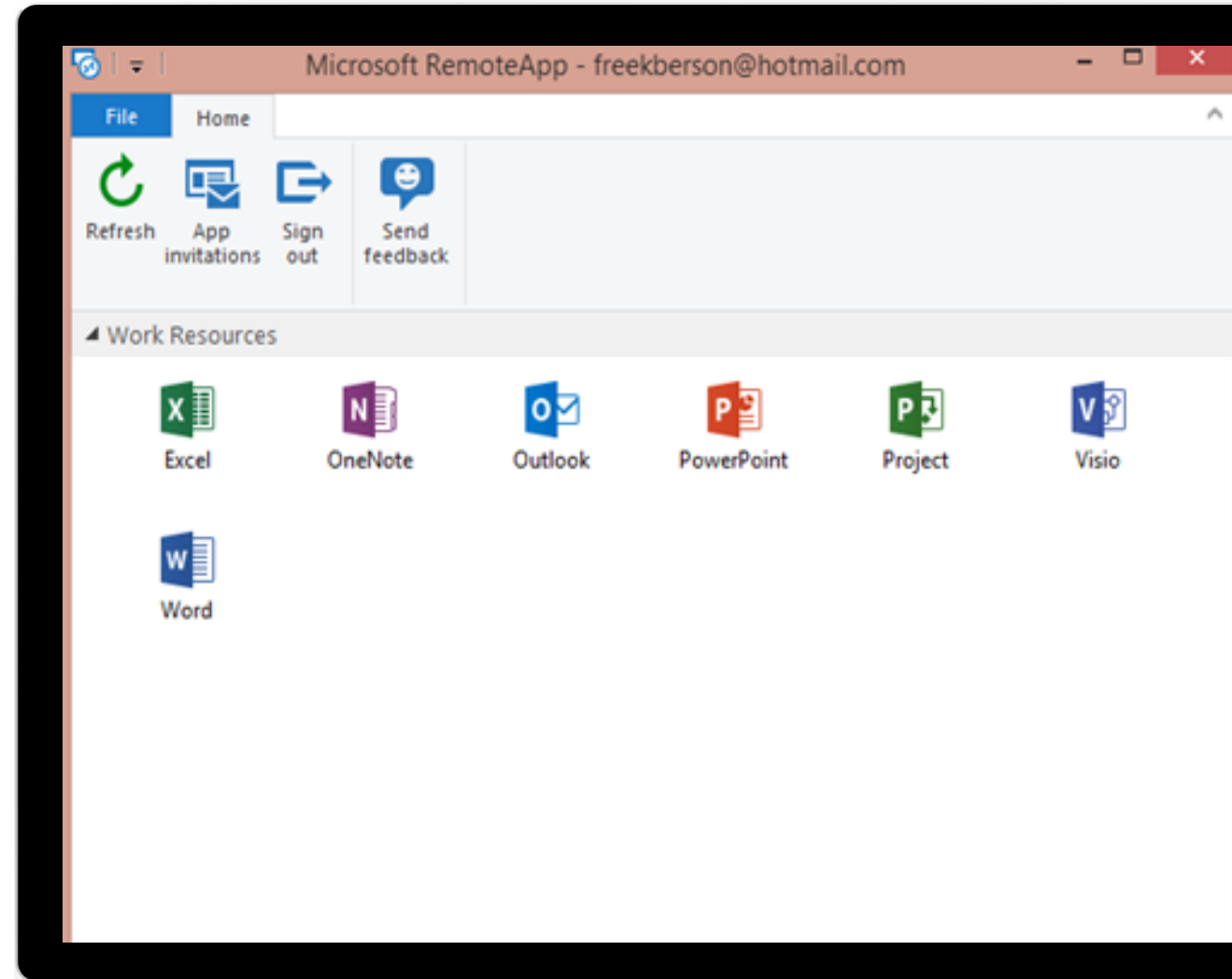
Azure Virtual Desktop key concepts

[Back to table of contents](#)

Azure Virtual Desktop key concepts - 1

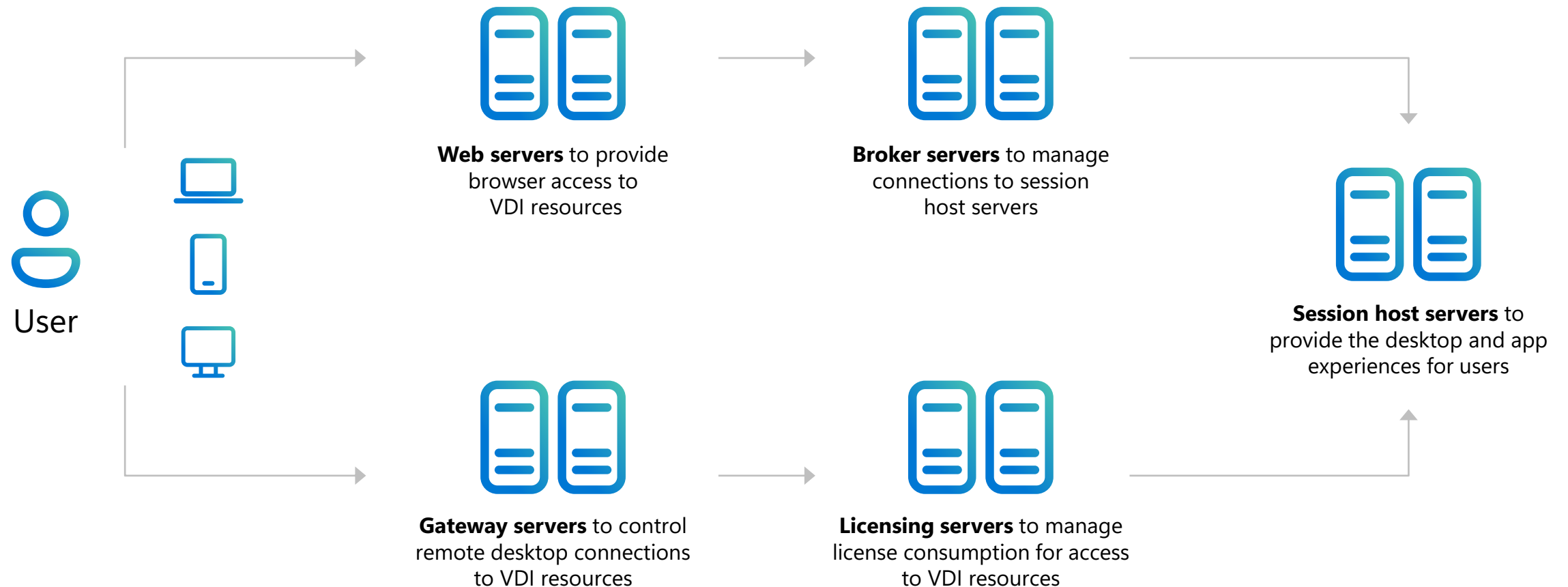


Azure Virtual Desktop can deliver users a full desktop environment and access to designated apps using a variety of clients and from any location.


















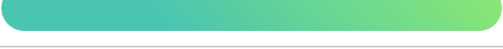

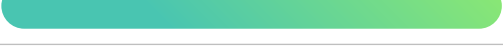

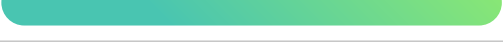
Azure Virtual Desktop key concepts - 2

Configuring and managing the on-prem infrastructure to deliver remote desktop and app experiences requires investment and management of a diverse set of hardware and software.



Azure Virtual Desktop key concepts - 3

Azure Virtual Desktop shifts the management of the physical resources necessary for delivering virtual desktop and app experiences to Microsoft.

Responsibility	Traditional on-prem VDI	Azure Virtual Desktop
Identity		
End-user devices (mobile and PCs)		
Application security		
Operating systems		
Deployment configuration		
Network controls		
Virtualization control plane		
Physical hosts		
Physical network		
Physical datacenter		

CUSTOMER

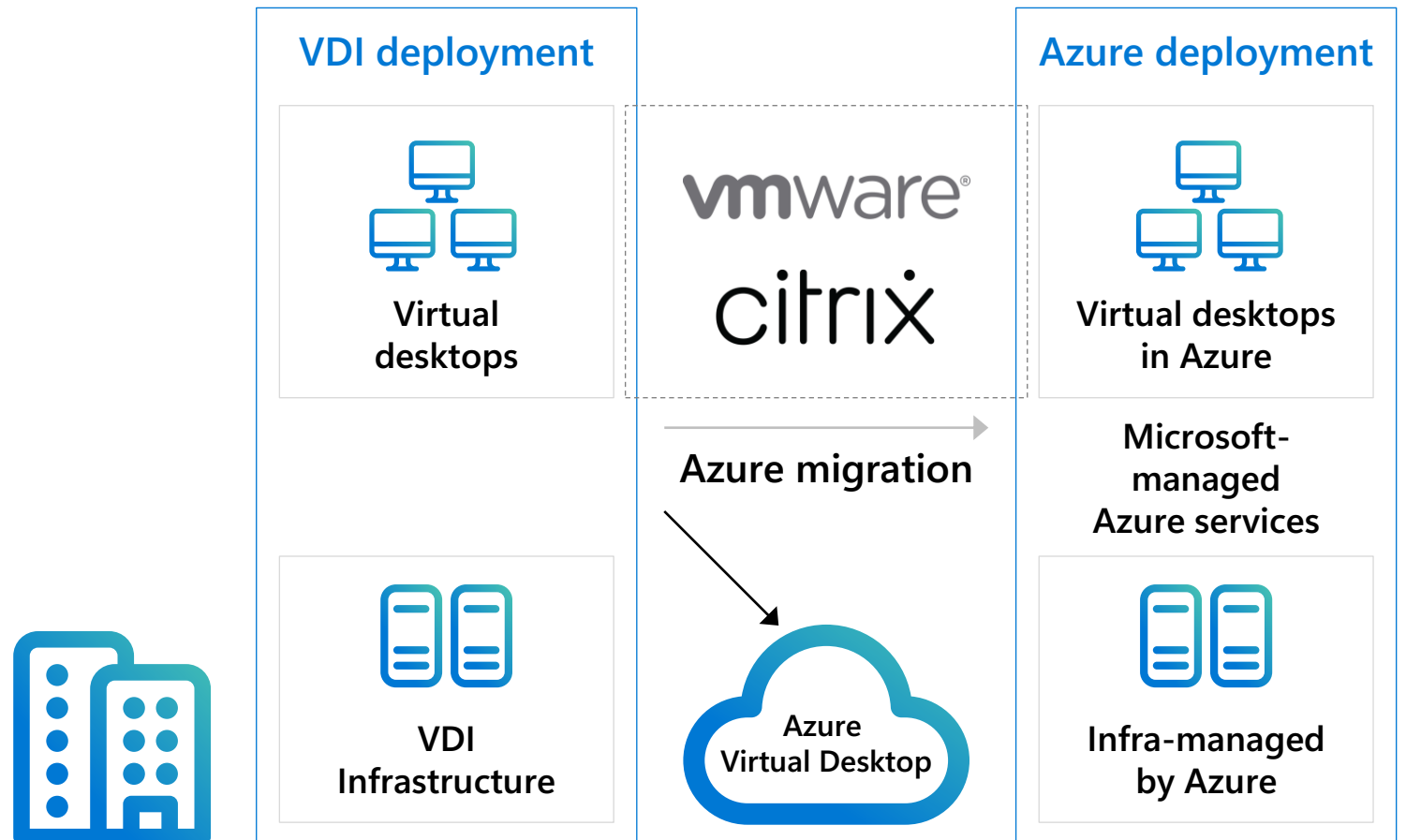
MICROSOFT

Azure Virtual Desktop key concepts - 4

Azure Virtual Desktop provides a migration path for on-prem VDI implementations using partner control planes.

VDI migration

- Azure Virtual Desktop
- Citrix + Azure
- VMware + Azure



What you need to get started with Azure Virtual Desktop

Azure Portal	Microsoft Entra ID Active Directory	Windows 11/10 Enterprise Windows Server 2012 R2 and up Windows 11/10 Enterprise multi-session	Azure ExpressRoute	Microsoft 365	Azure Virtual Desktop
An Azure account with an active subscription	An identity provider	A supported operating system	Network connectivity	Appropriate licenses	A remote desktop client
<p>Azure Virtual Desktop configuration, monitoring, and management happens in the Azure Portal.</p> <p>Admins need an account with the necessary privileges to start an Azure Virtual Desktop implementation.</p>	<p>Identity providers allow for granular control of user access to Azure Virtual Desktop resources.</p> <p>Microsoft Entra ID provides identity management for Azure Virtual Desktop.</p>	<p>Azure Virtual Desktop resources are delivered through virtual machines running Windows operating systems. You can choose from a broad set of available OS images or create your own.</p>	<p>Users can connect to Azure Virtual Desktop from anywhere. Customers can also use Azure ExpressRoute to link on-prem infrastructure to Azure Virtual Desktop services.</p>	<p>Many customers are already entitled to access Azure Virtual Desktop resources through existing eligible licenses.</p>	<p>Users can access Azure Virtual Desktop resources through a variety of remote desktop clients.</p>

Pricing for Azure Virtual Desktop

 Pay only for the virtual machines (VMs), storage, and networking consumed when the service is in use.



Calculating your costs

An Azure user account and subscription are required to deploy and manage a virtual machine.

Pricing factors include:

- Virtual machines and operating system (OS) storage
- Data disk (personal desktop only)
- User profile storage
- Networking



Making it work for you

- We offer pricing options such as [one-year or three-year Azure Reserved Virtual Machine Instances](#), for savings of up to 72 percent versus the pay-as-you-go plan,
- [Monthly payment plan is now available upon request.](#)
- Reserved virtual machines can be exchanged or returned.



Only infrastructure cost with BYOL

Azure Virtual Desktop session host virtual machines (including Citrix Cloud and VMWare Horizon Cloud on Azure deployments) are charged at Linux compute rates for Windows 11 or 10 single, Windows 11 or 10 multi-session, and Windows Server.

Customer only needs to bring appropriate Windows license.

All Azure discounts and benefits apply to Azure Virtual Desktop

Virtualization endpoints

New environment

Azure Virtual Desktop

Burst to Azure (cloud)

Lift and shift

Lift, shift, and modernize



Azure incentive programs



Reserved instances



Cloud Service Provider margins and rebates



Digital Partner of Record

Many customers are already eligible for Azure Virtual Desktop

Azure Virtual Desktop licensing requirements



Client

Customers are eligible to access Windows 11 and Windows 10 single and multi-session and Windows 7 with Azure Virtual Desktop if they have one of the following licenses*:

- Microsoft 365 E3/E5
- Microsoft 365 A3/A5/Student Use Benefits
- Microsoft 365 F3
- Microsoft 365 Business Premium
- Windows 11 and Windows 10 Enterprise E3/E5
- Windows 11 and Windows 10 Education A3/A5
- Windows 11 and Windows 10 VDA E3/E5



Server

Customers are eligible to access Server workloads with Azure Virtual Desktop if they have one of the following licenses:

- RDS CAL license with active Software Assurance (SA) or RDS User Subscription Licenses

Customers pay for the virtual machines (VMs), storage, and networking consumed when the users are using the service.

*Customers can access Azure Virtual Desktop from their non-Windows Pro endpoints if they have a Microsoft 365 E3/E5/F3, Microsoft 365 A3/A5 or Windows 11 and Windows 10 VDA per user license. Source: [Azure Virtual Desktop Prerequisites](#)

Azure Virtual Desktop architecture

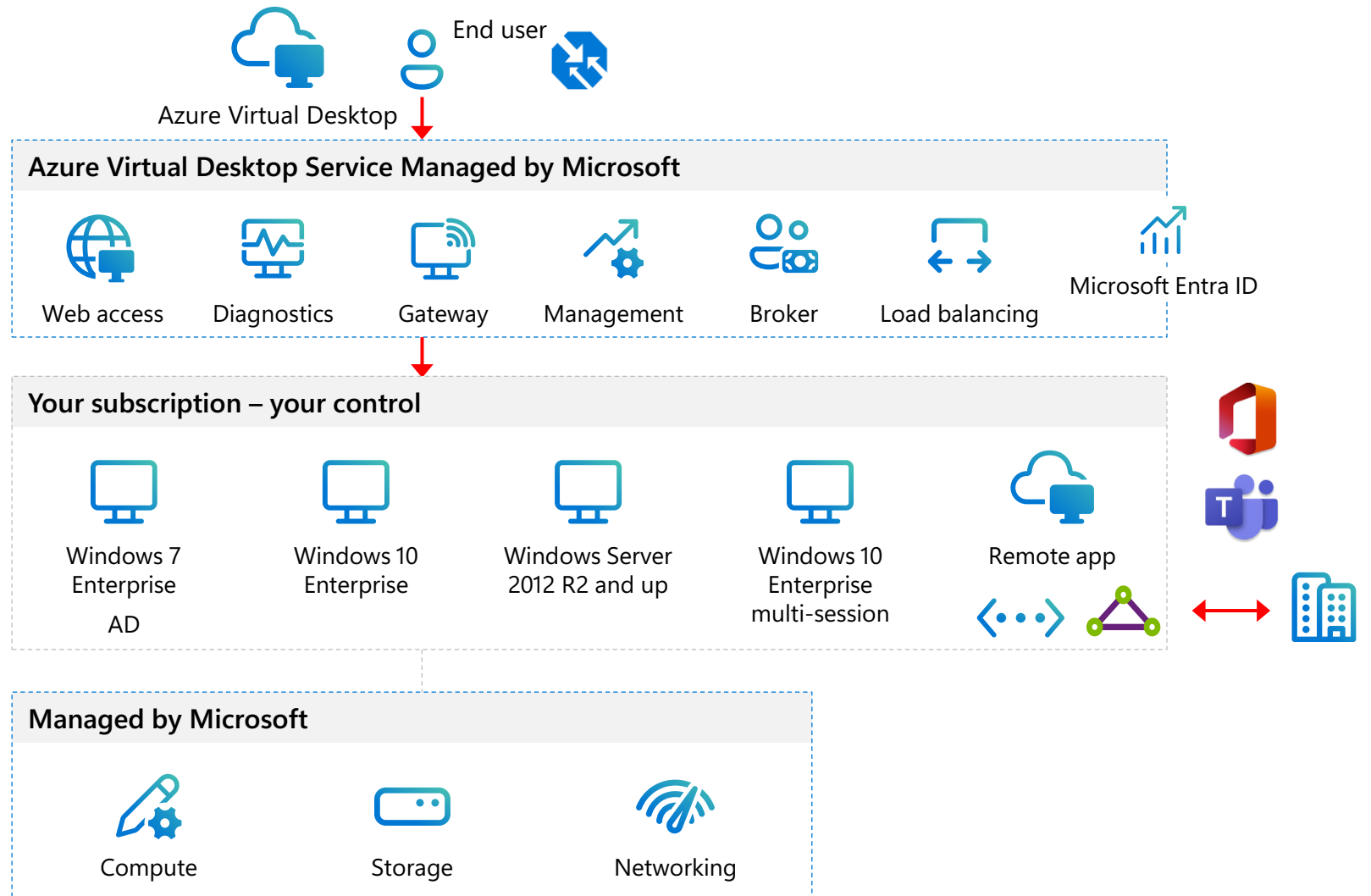
[Back to table of contents](#)

Azure Virtual Desktop architecture

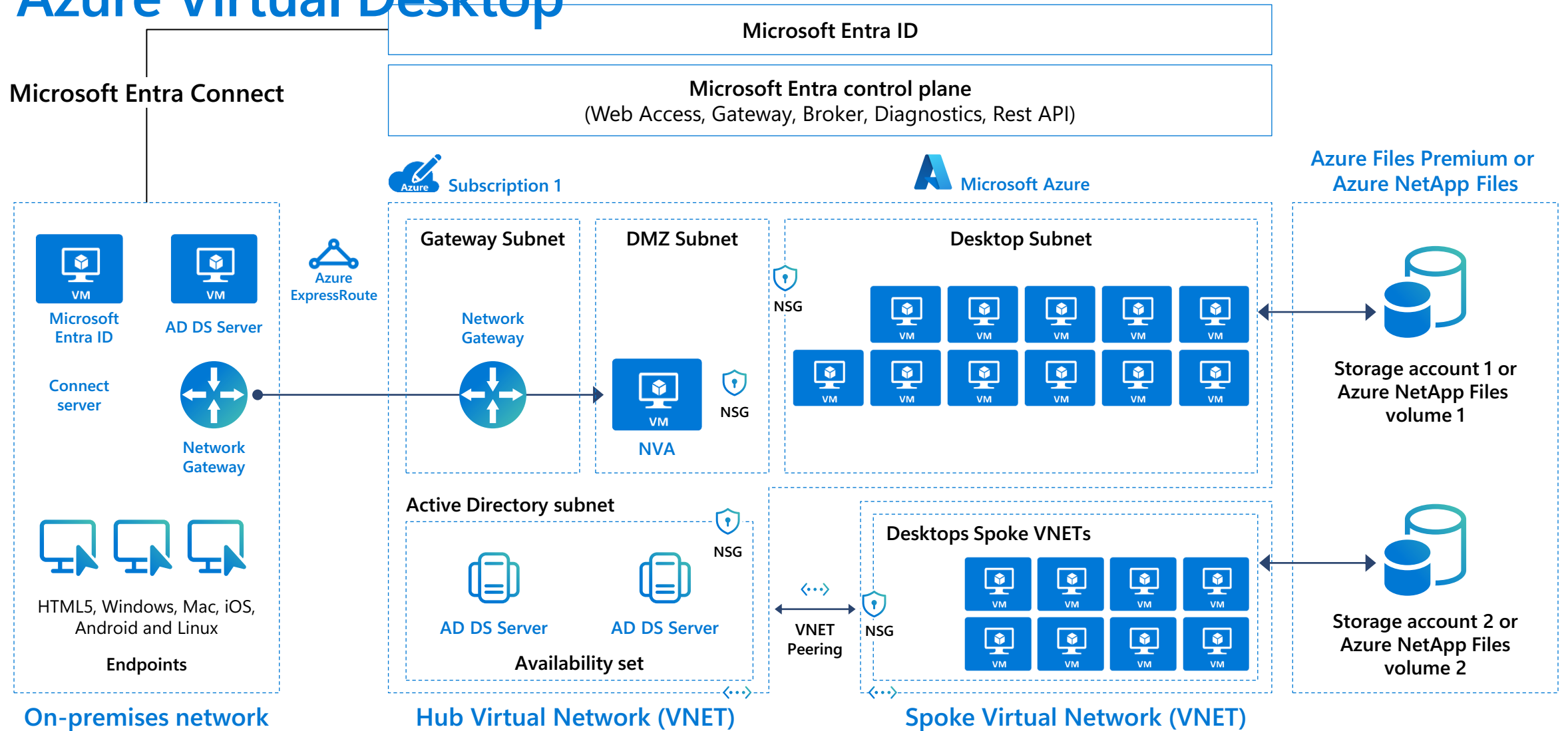
Provide your employees with a secure, remote desktop experience.

Connect from any device of your choice.

Focus on the right policies and controls rather than managing infrastructure.



Example enterprise architecture diagram – Azure Virtual Desktop



Creating the foundation for your Azure Virtual Desktop environment

[Back to table of contents](#)

Creating the foundation for your Azure Virtual Desktop environment - 1



Performance requirements and sizing

- Virtual machine (VM) recommendations
- Multi-session and sizing guidelines
- Storage for your VMs
- Storage for your FSLogix profiles
- GPU VMs
- Networking
- New features



User experience

- Host pools and session hosts
- Personal or pooled host pools
- User profile management (FSLogix)
- Remote App Streaming
- New features:
 - Personal desktop unassignment and reassignment
 - Storage cost savings with FSLogix



Networking and connectivity

- Networking considerations
- On-prem to Azure connectivity
- Inter-Azure traffic management
- New features:
 - RDP Shortpath

Creating the foundation for your Azure Virtual Desktop environment

Performance requirements
& sizing guidelines

[Back to table of contents](#)

Performance requirements & sizing guidelines



One of the fundamental benefits of implementing Cloud VDI with Azure Virtual Desktop is the ability to tailor the remote compute experience to meet the needs of users whether they're performing their duties as call center agents, designing a next generation video game, or providing temporary consulting services for a multinational client.



Azure Virtual Desktop provides this flexibility by using the foundational compute, storage, and networking components of the Azure service.



The following slides give an overview of:

- Virtual machine sizing
- Pooled sizing and multi-session sizing
- Disk type recommendations
- Profile storage recommendations
- GPU Capabilities
- Networking design and best practices

Configuring Azure Virtual Desktop



Azure Virtual Desktop provides a simple, clean interface for configuring and customizing a VDI environment.

The screenshot displays the Azure Virtual Desktop management console. The interface is clean and modern, with a left-hand navigation pane and a main content area. The navigation pane includes sections for Overview, Getting started, Manage (Host pools, Application groups, Workspaces, Scaling plans, Users), Monitoring (Insights, Insights (Preview), Workbooks), and Licensing (Per-user access pricing). The main content area features a prominent call to action: "Donald, create a host pool!" with a "Create a host pool" button. Below this, there are several informational cards under "Documentation and help", including "Getting started", "Create your own image", "Cost calculator", and "Profile containers". At the bottom, there is a "Community" section with links to the Azure Virtual Desktop forums and a Twitter handle @AzureSupport.

Virtual machines - 1

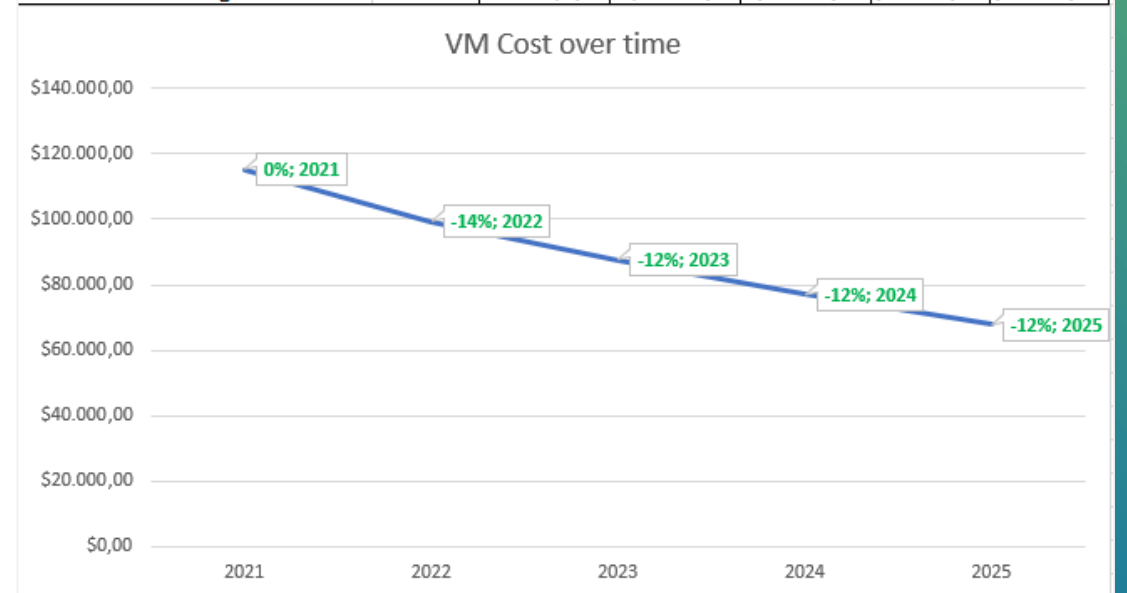
Virtual machine (VM) type

- Azure resources can be optimized with scale to offer cost savings.
- In the case of Azure Virtual Desktop, the most important resource is the VM (compute).
- If we start by looking at a popular VM series for Azure Virtual Desktop, the D-series, VMs get more powerful and could be optimized to become cheaper.
- Over time it can offer [great cost savings](https://aka.ms/AzureMakesAVDCheaperOverTime) (aka.ms/AzureMakesAVDCheaperOverTime).



Select the newest VM families to help get the optimal price/performance ratio.

		Ds8 v3	Ds8 v4	Ds8 v5	Ds8 v6?	Ds8 v7?
Number of users	1000					
Number of users per VM	11					
ACU increase (worst case)		0%	10%	10%	10%	10%
Number of hosts (VMs) required		91	82	74	66	60
Running hours	220					
Cost of VM per hour		\$0,48	\$0,46	\$0,45	\$0,44	\$0,43
Cost per month		\$9.600,00	\$8.280,00	\$7.290,00	\$6.415,20	\$5.642,46
Cost per year		\$115.200,00	\$99.360,00	\$87.480,00	\$76.982,40	\$67.709,52
Savings\$ per year		\$0,00	\$15.840,00	\$11.880,00	\$10.497,60	\$9.272,88
Savings% per year		0%	-14%	-12%	-12%	-12%
		2021	2022	2023	2024	2025
Cummulative savings		\$0,00	\$15.840,00	\$27.720,00	\$38.217,60	\$47.490,48



Virtual machines - 2

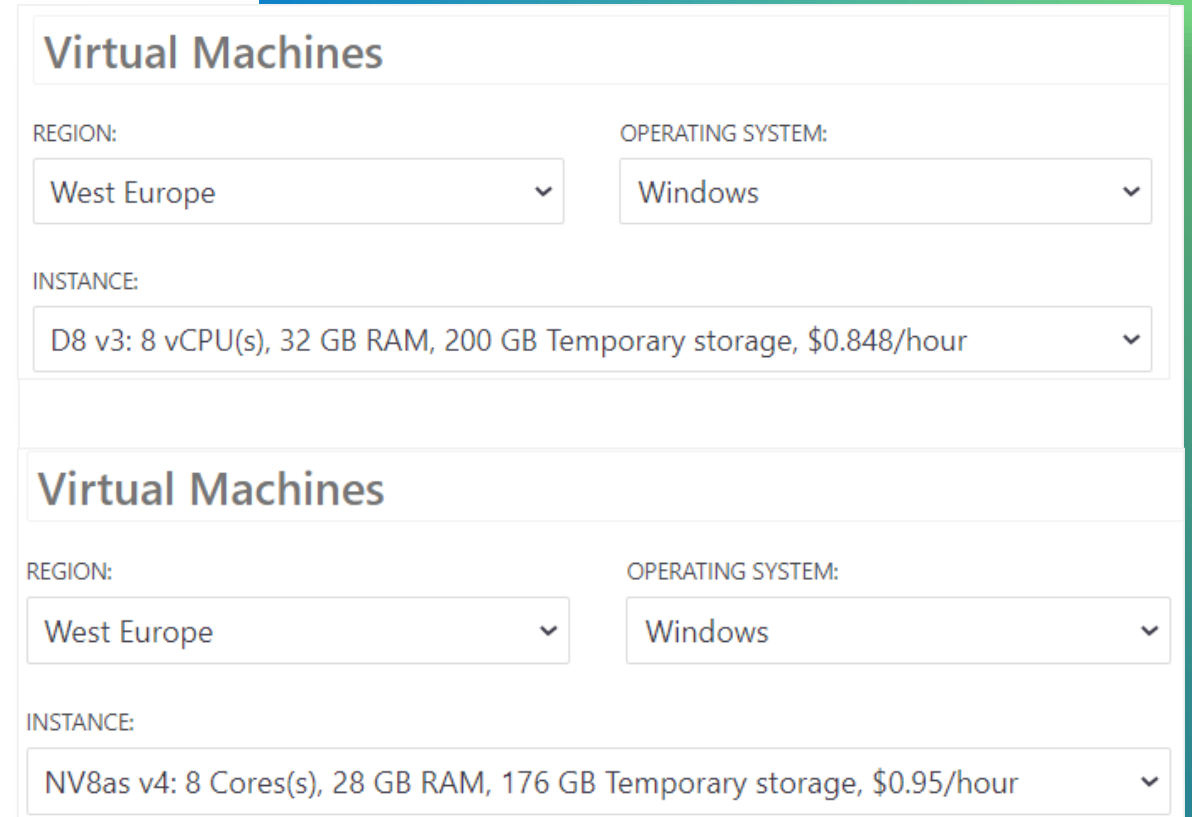
Virtual machine (VM) type (continued)

Azure offers many different virtual machine types, where the D, F, and N (with GPU) series are the most used with Azure Virtual Desktop.

Because the [N series VMsm](#) (aka.ms/GPUOptimizedVMSizes) have a GPU, they not only offer better graphical performance, but also offload the CPU significantly. Even if you have a moderately graphically intense workload, it'll help increase your density with a minimal increment in cost.



Investigate if the N series lowers the average cost per user for your workload.

The image shows two screenshots of the Azure Virtual Machines configuration interface. The top screenshot shows the configuration for a VM in the West Europe region with a Windows operating system and an instance type of D8 v3: 8 vCPU(s), 32 GB RAM, 200 GB Temporary storage, \$0.848/hour. The bottom screenshot shows the configuration for a VM in the West Europe region with a Windows operating system and an instance type of NV8as v4: 8 Cores(s), 28 GB RAM, 176 GB Temporary storage, \$0.95/hour. Both screenshots have a blue and green gradient background.

Virtual Machines

REGION: West Europe

OPERATING SYSTEM: Windows

INSTANCE: D8 v3: 8 vCPU(s), 32 GB RAM, 200 GB Temporary storage, \$0.848/hour

Virtual Machines

REGION: West Europe

OPERATING SYSTEM: Windows

INSTANCE: NV8as v4: 8 Cores(s), 28 GB RAM, 176 GB Temporary storage, \$0.95/hour

Virtual machines - 3

Azure region



Usually, the single most important thing for the user experience is to have the VMs as close to the user as possible, but it's important to be aware of the [different prices](#) (aka.ms/AzureVMPriceComparison) of VMs in the different Azure regions.



Investigate if you can run a VM cheaper in another Azure region without impacting the end user experience.

Azure VM Comparison

Find and compare Azure Virtual machines specs and pricing on a one page. Check column **Best region price**, it will help you to find in what region that VM. Know that the price in different currencies is different, sometimes the difference is significant, check this [page](#). The data updated daily from Azure API and is not related to Microsoft or Azure. Last update was: 2020-12-04 10:08:11Z GMT

Euro (€) UK South Cost per hour Standard Priority nv

Cores: RAM:

VM name	# Cores	Memory (GiB)	Max # disks	Linux price	Windows price	Best region price
Standard_NV24	24	224	64	3.040096	5.918279	
Standard_NV12	12	112	48	2.532429	1.985971	
Standard_NV6	6	56	24	1.266636	0.992564	
Standard_NV48s_v3	48	448	32	4.80681	6.668816	
Standard_NV24s_v3	24	224	24	2.403405	3.334408	
Standard_NV12s_v3	12	112	12	1.201702	1.667204	
Standard_NV32as_v4	32	112	32	1.964889	3.206226	
Standard_NV16as_v4	16	56	32	0.982444	1.603113	
Standard_NV8as_v4	8	28	16	0.4908	0.801978	
Standard_NV4as_v4	4	14	8	0.2454	0.400567	

Multi-session is an exclusive feature for Azure Virtual Desktop and drives cost efficiency without impacting user experience

Multi-session allows administrators to place multiple users in the same virtual machine (VM).

Azure Virtual Desktop multi-session can share resources across users and place many users into the VM.

Multi-session is available with pooled desktops and requires FSLogix for user profile roaming.

User	Status	40% CPU	62% Memory
chitturs		8.8%	866.5 MB
jbruner		0.2%	394.3 MB
jesmith		1.2%	1,742.3 MB
markma		0.3%	388.2 MB
mattandr		0%	719.9 MB
sprabhu		0.1%	1,012.7 MB
stdowns		0.9%	694.1 MB
> timmck (66)		1.3%	1,632.9 MB

Azure Virtual Desktop host sizing recommendations (multi-session and single session)

Multi-session recommendations

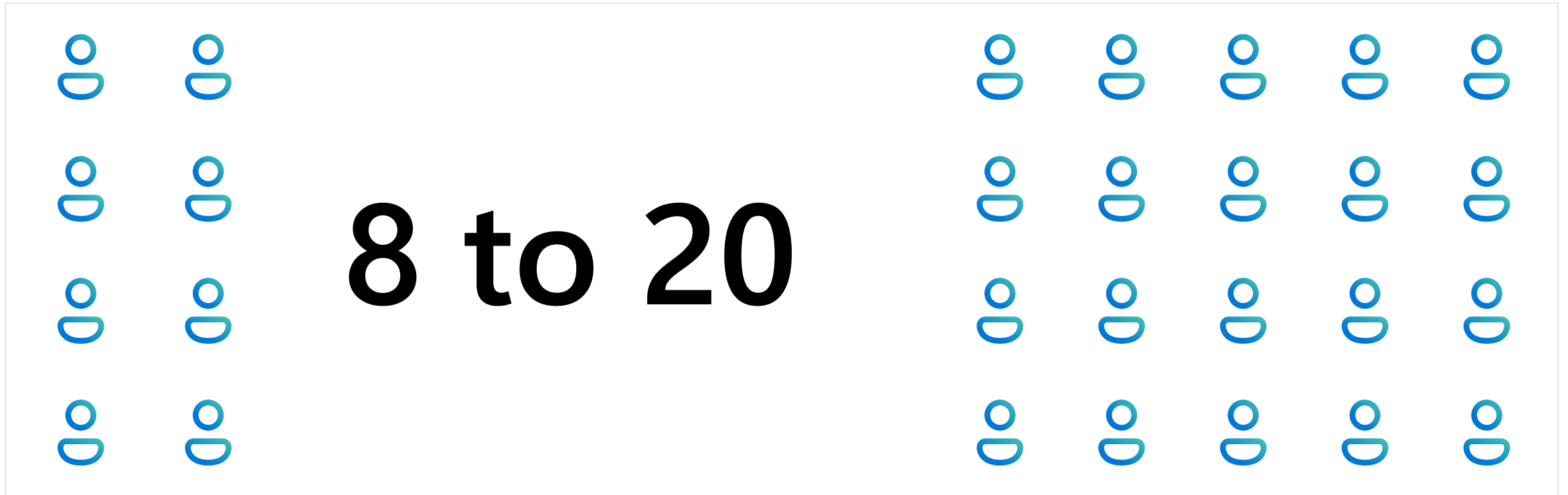
The following table lists the maximum suggested number of users per virtual central processing unit (vCPU) and the minimum virtual machine (VM) configuration for each workload. These recommendations are based on [Remote Desktop workloads](#).

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	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

Single-session/personal desktop recommendations

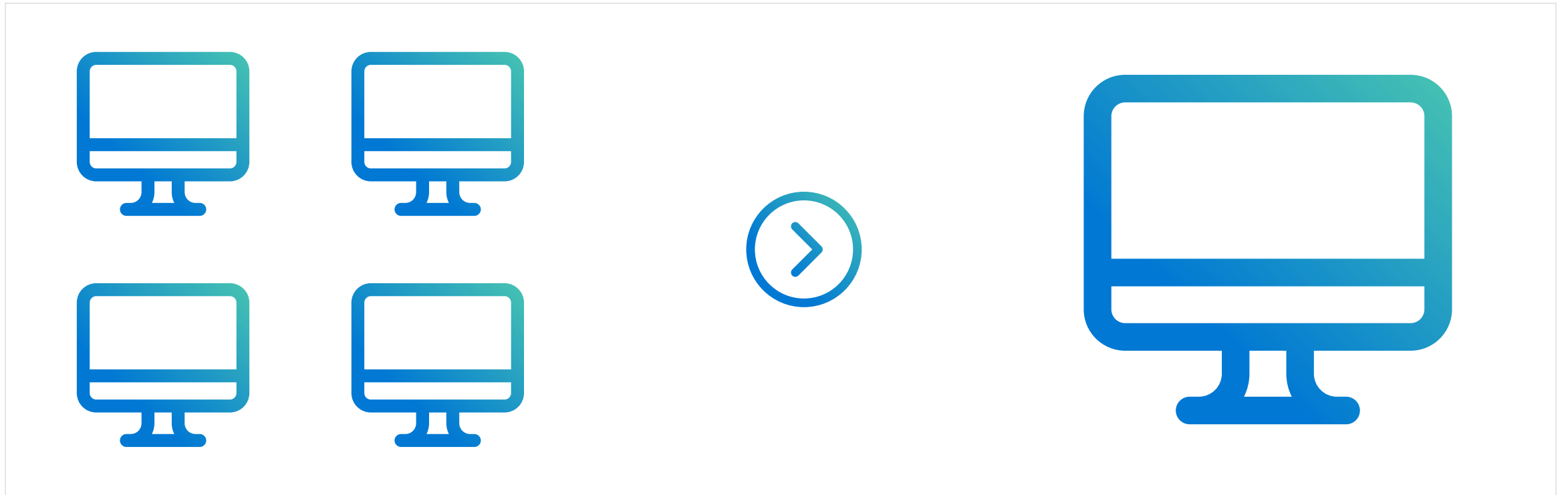
- Sizing largely dependent on the workload, apps deployed, and user type.
- We recommend at least two physical CPU cores per VM (typically four vCPUs with hyperthreading).
- If you need more specific VM sizing recommendations for single-session scenarios, check with your software vendors specific to your workload .
- VM sizing for single-session VMs will likely align with physical device guidelines .
- Use other tools to get granular level sizing and scaling recommendations.

Pooled sizing guidelines for determining user density per VM



Maximum number of people per VM (density)

Pooled multi-session sizing guidelines



Some small are better than one large
Most common SKU: Standard_D8_v4

Azure Virtual Desktop storage considerations – OS disk choice

OS disk type

Each Azure Virtual Desktop VM needs an OS disk. The disc type can be configured by the system admin during set up or at any point.

The table below compares the different options at a high level (more details [here](https://aka.ms/AzureManagedDiskTypes) (aka.ms/AzureManagedDiskTypes)).

	Premium SSD	SSD	HDD	<u>Ephemeral Disk</u>
SLA + HA	● ● ●	● ●	● ●	●
IOPS & throughput	● ●	● ●	●	● ● ●
Flexibility	● ● ●	● ●	● ●	●
Low cost	●	● ●	● ● ●	● ● ● ● ●



Use Ephemeral disks (free) to save costs if your scenario allows it

Azure Virtual Desktop storage considerations – FSLogix profile storage

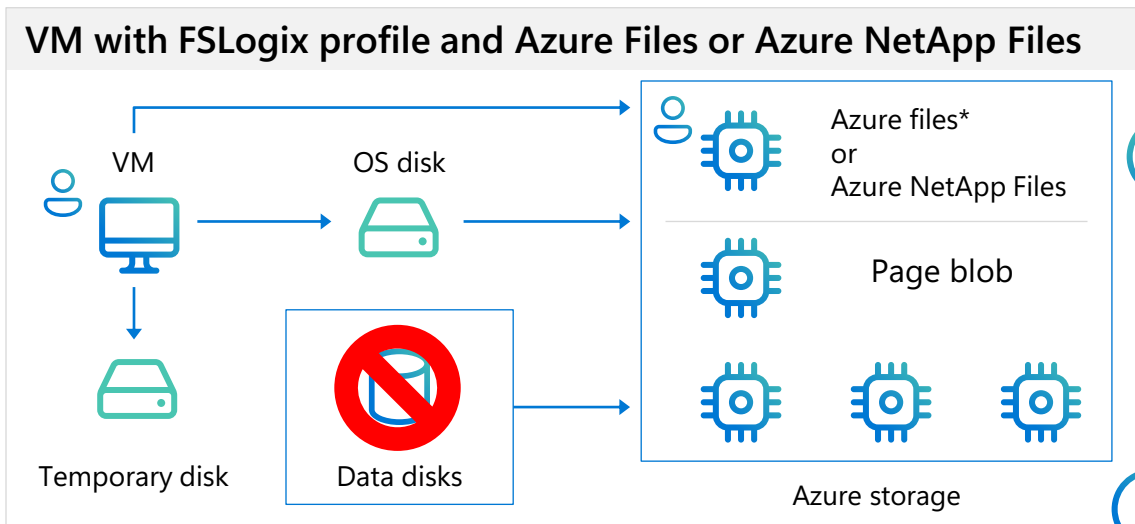
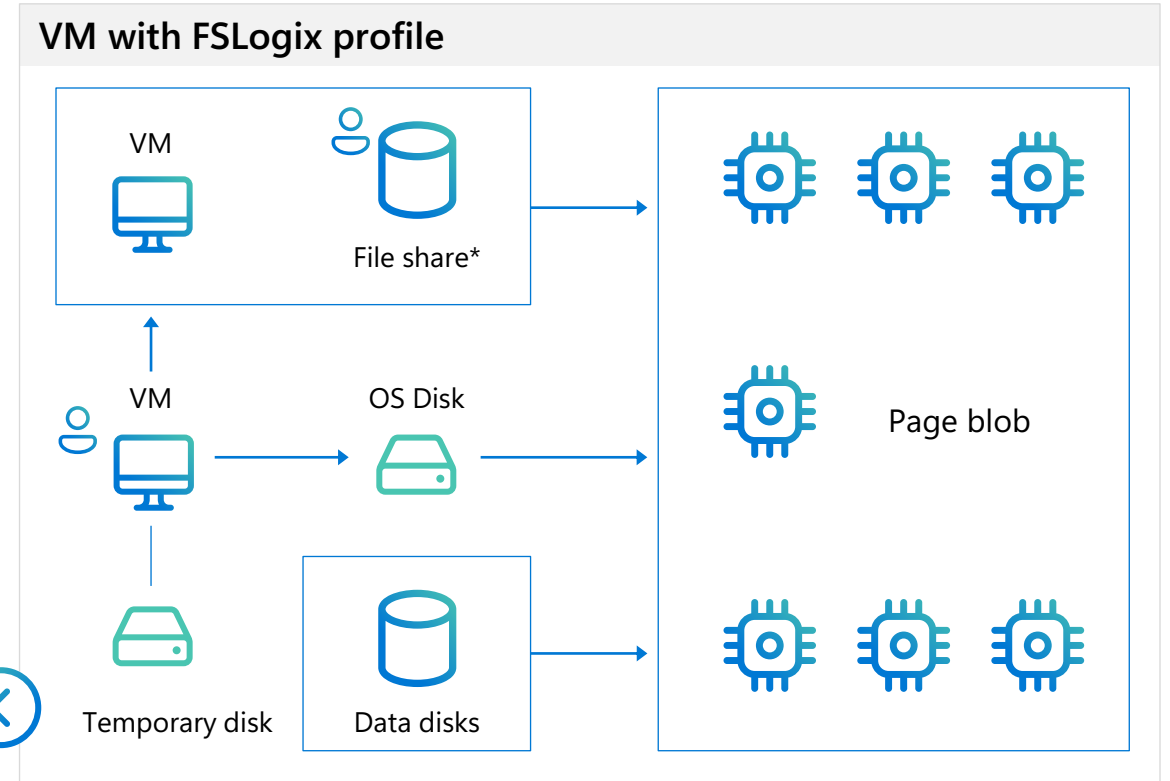
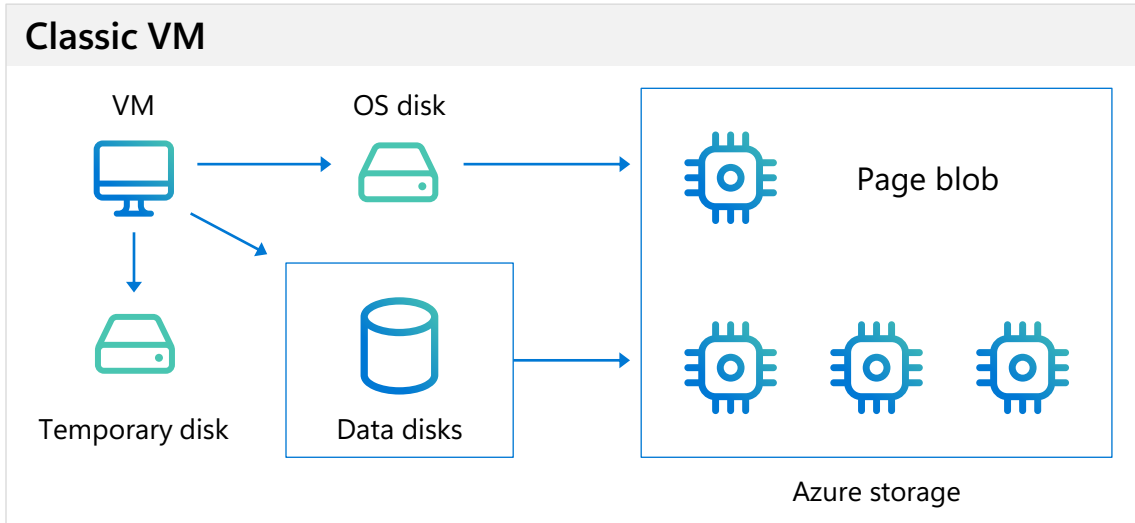
FSLogix profile storage

Azure offers multiple solutions that you can use to store your FSLogix profile containers.

The table below compares the different options at a high level (more details [here](#)).

	Azure Files Premium	Azure NetApp Files	Storage Spaces Direct
Workload type	Medium user, low-concurrency	All user types, high-concurrency	Light user, low-concurrency
SLA + HA	● ●	● ● ●	●
IOPS & throughput	● ●	● ●	●
Low latency	● ●	● ● ●	●
Flexibility	● ● ●	● ● ●	● ●
Low cost	● ●	● ●	●
Data protection	● ●	● ● ●	● ●

Extend your storage options with Azure Virtual Desktop



Dependencies

- On-prem AD integration (Coming soon)
- ✓ Premium Files rollout (overlap in hero regions)
- ✓ AADS integration

Azure Virtual Desktop on Azure

Optimize end user experience with Azure NetApp Files (ANF)

Simple to manage

- Native Azure service for easy deployment and scalability
- Single shared platform for FSLogix profile, MSIX App Attach containers, and generic file shares

Lower TCO

- PaaS service
- No VMs resources required on Azure IaaS
- Integrated Snapshot Backup & DR

Enterprise performance

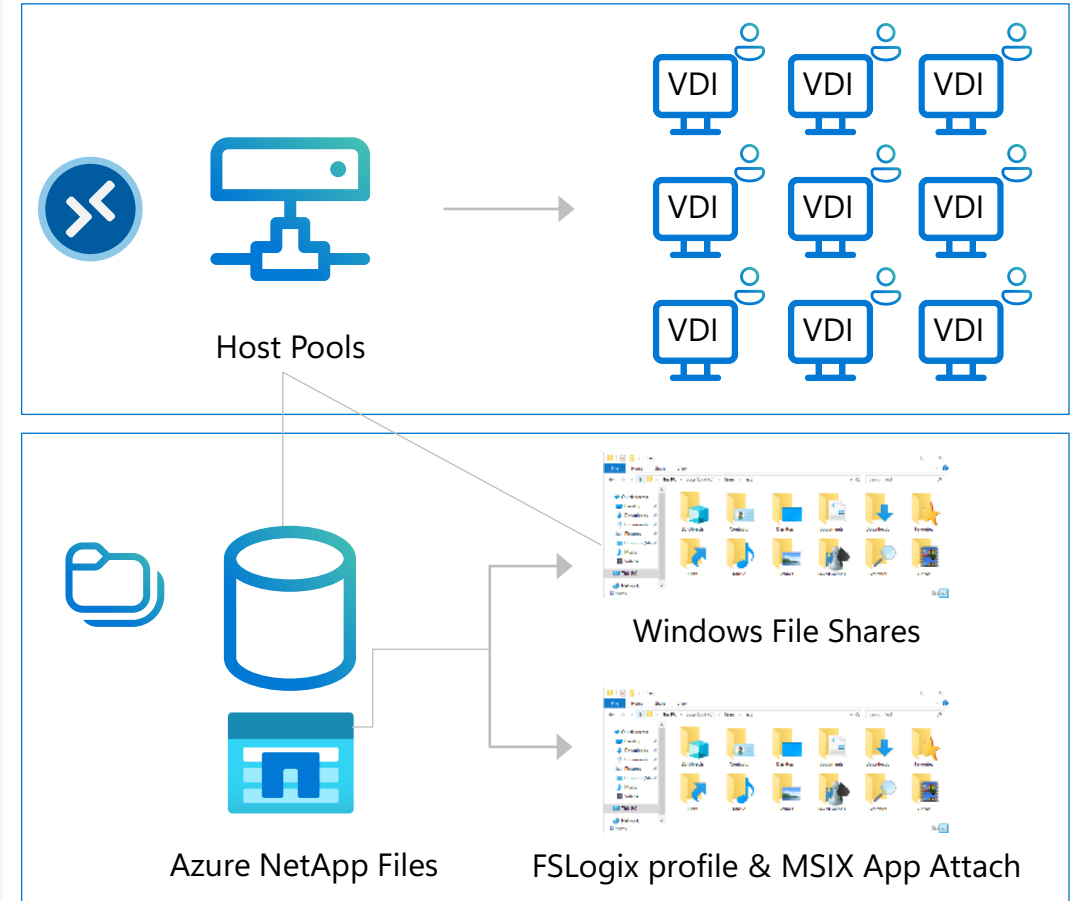
- High IOPs w/ low latency
- Online scalability of capacity and performance (e.g., burst for login storms)

Maximum compatibility

- SMB (all versions) support
- Native Active Directory Domain Services (non-AAD) support
- Full NTFS ACLs support



Azure Virtual Desktop on Azure Architecture



Azure Virtual Desktop

GPU use cases

GPUs for Visualization – Architects, designers, graphic artists

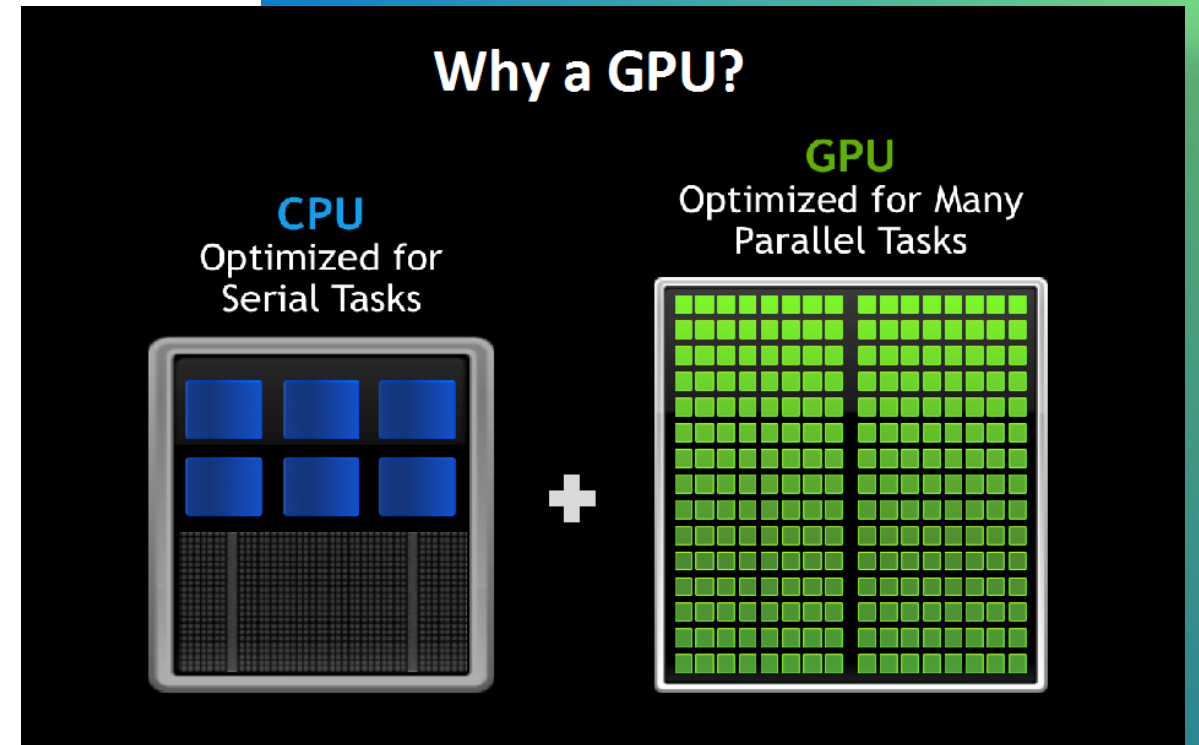
CAD/CAE

GPU for HPC – Developers, scientists

Supercomputers for high-end simulations

GPU for AI – Data scientists

Supercomputing training deep learning models



Azure Virtual Desktop GPU processor options



NC Series

HPC workloads such as reservoir modeling, DNA sequencing, protein analysis, Monte Carlo simulations, and others.



NCasT4 (NC4asT4 [4 CPU 1 GPU] to NC64asT4 [64 CPU and 4 GPUs])

Ideal for deploying AI services, such as real-time inferencing of user-generated requests, or for interactive graphics and visualization workloads using NVIDIA's GRID driver and virtual GPU technology.



ND Series

- Built for both computationally intense scale-up (harnessing 8 GPUs per VM) and scale-out (harnessing multiple VMs working together) workloads. The NDv2 series now supports 100-Gigabit InfiniBand EDR backend networking, like that available on the HB series of HPC VM, to allow high-performance clustering for parallel scenarios including distributed training for AI and ML.
- ND A100 v4 – 96 AMD Epyc CPUs and 8 A100 40GiB Tensor Core GPUs
- NDm A100 v4 – 96 AMD Epyc CPUs and 8 A100 80Gib Tensor Core GPUs



NV Series

- NVv1 (NV6)
- NVv3 (NV12 [1 GPU] to NV48 [GPUs])
- NVv4 (NV4asv4 [4 CPUs 1/8 GPU] to NV32asv4 [32 CPUs 1 full GPU])

Azure Virtual Desktop GPU performance

GPU Rendering cost for 4K image on Azure VMs

VM Name	# GPUs on VM	Azure VM hourly cost (\$)	4K Image Render time	Total Azure consumption
NC64as_T4_v4	4	\$8.60	11min 47 sec	\$1.69
NV24s_v3	2	\$4.29	1 hr 23 min 53 sec	\$6.00

CPU Rendering cost for 4K image on Azure VMs

VM Name	No. of CPU cores	Azure VM hourly cost (\$)	4K Image Render time	Total Azure consumption
NC64as_T4_v4	64	\$8.60	21 min 13 sec	\$3.04
NV24s_v3	24	\$4.29	1 hr 41 min 43 sec	\$7.27

Configuring Azure Virtual Desktop networking



Networking options for Azure Virtual Desktop let you specify security and active directory model.

Network and security

Use Azure Firewall to secure your VNET and host pool resources. [Learn more](#)

Virtual network * ⓘ

Network security group ⓘ

Public inbound ports ⓘ Yes No

Inbound ports to allow
i All traffic from the internet will be blocked by default.

Domain to join

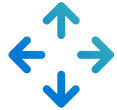
Select which directory you would like to join

AD domain join UPN * ⓘ

Password * ⓘ

Specify domain or unit ⓘ Yes No

Network requirements & considerations



How to connect

	Connectivity type	Special considerations
Azure ExpressRoute	Hybrid	Dedicated network through service provider
Site-to-Site VPN	Hybrid	Limited bandwidth compared to Azure ExpressRoute
Microsoft Entra Domain Services	Isolated	Must synchronize password hashes to Microsoft Entra ID



Identity strategy options

- Spin up a domain controller in your Azure subscription.
- For cloud-based organizations, use Microsoft Entra Domain Services.
- For hybrid organizations, use VPN or Azure ExpressRoute and make sure your on-premises domain controllers can be found in Azure.

Recommended networking and identity setup for hybrid organizations



With this setup, you are managing identities from the on-premises Active Directory instance.

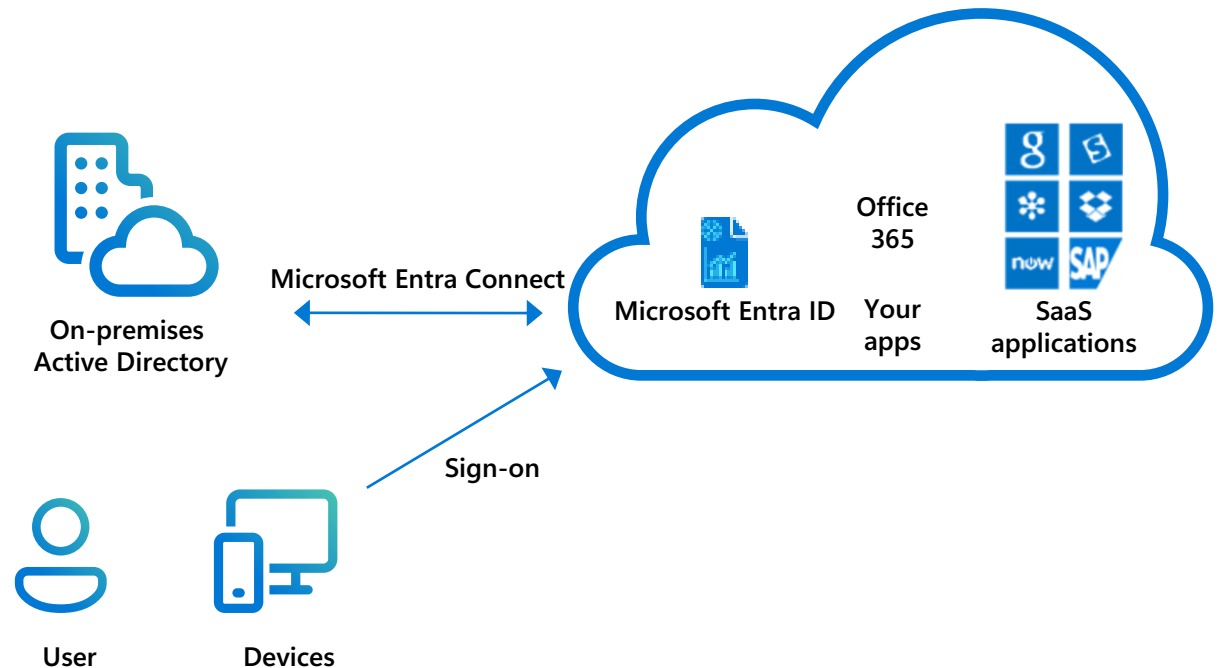


Microsoft Entra ID



Windows Server AD on-premises, connected to Azure

- Azure ExpressRoute or site-to-site Virtual Private Network (VPN) to Azure
- Microsoft Entra Connect synchronizes identities



Networking

Inter-Azure traffic



If possible, try to place VMs in an Azure region with an Azure Virtual Desktop control plane.



Investigate if you can meet your security requirements without forced tunneling to an on-premises environment.



For large deployments, [calculate](https://aka.ms/AzureExpressRoutePricing) (aka.ms/AzureExpressRoutePricing) if an unlimited Azure ExpressRoute is cheaper.

A screenshot of the Azure Bandwidth calculator interface. The title is "Bandwidth". It features three dropdown menus: "DATA TRANSFER TYPE:" set to "Inter Region", "SOURCE REGION:" set to "UK South", and "DESTINATION REGION:" set to "North Europe". Below these is a section for "Outbound Data Transfer" with a value of "50 TB". A price tag in the bottom right corner shows "= \$921.60".

DATA TRANSFER TYPE:	SOURCE REGION:	DESTINATION REGION:
Inter Region	UK South	North Europe

Outbound Data Transfer ⓘ

50 TB

= \$921.60

Creating the foundation for your Azure Virtual Desktop environment

User experience

[Back to table of contents](#)

Azure Virtual Desktop user experience



Azure Virtual Desktop provides many options for customizing the virtual desktop and remote app experience for users.



Administrators can create environments that deliver a remote desktop experience that's deeply personal.



Administrators can create application groups that make an organization's custom apps available to a select set of users.

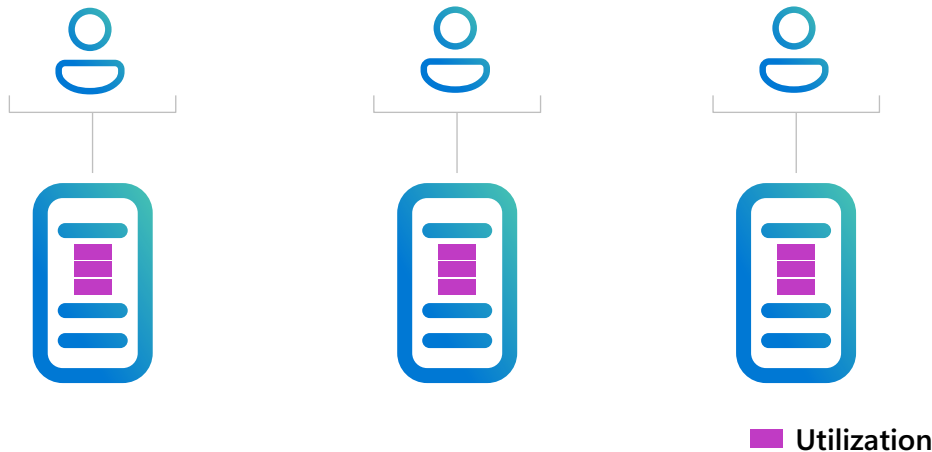


The following slides give an overview of:

- Host pools & session hosts
- Multi-session
- FSLogix
- Remote app streaming
- New features

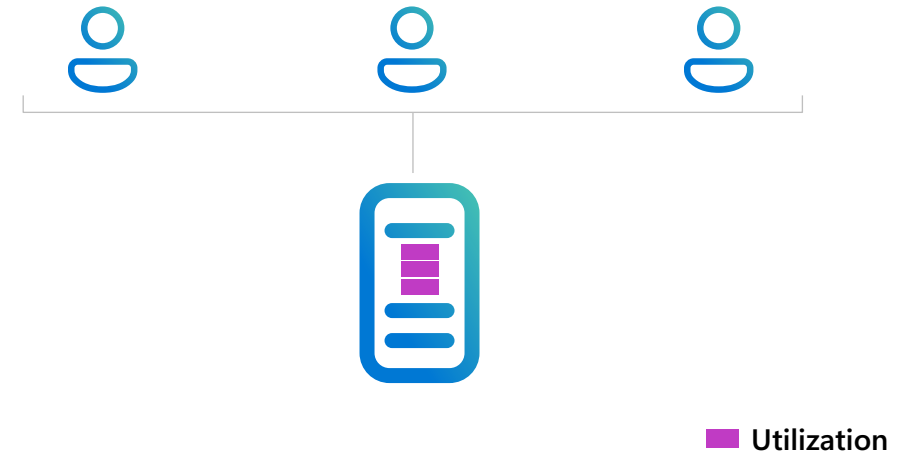
Choose the right configuration to meet your user requirements

Personal desktops



- Ideal for **single-session** users with **heavy performance** requirements
- Choose the right VM to run robust business apps such as CAD, SAP and others
- Always-on experience and single state retention

Pooled desktops



- Ideal for **multi-session** users and certain **single-session** with **light – medium** workloads with basic business requirements
- Choose the right VM to run most business apps

Azure automation – Automate your Azure management tasks and orchestrate actions across external systems from within Azure

Pay only for the virtual machines (VMs), storage, and networking consumed when the service is in use

Host pools & session hosts



Host pools are groupings of session host virtual machines that have the same image and configuration.

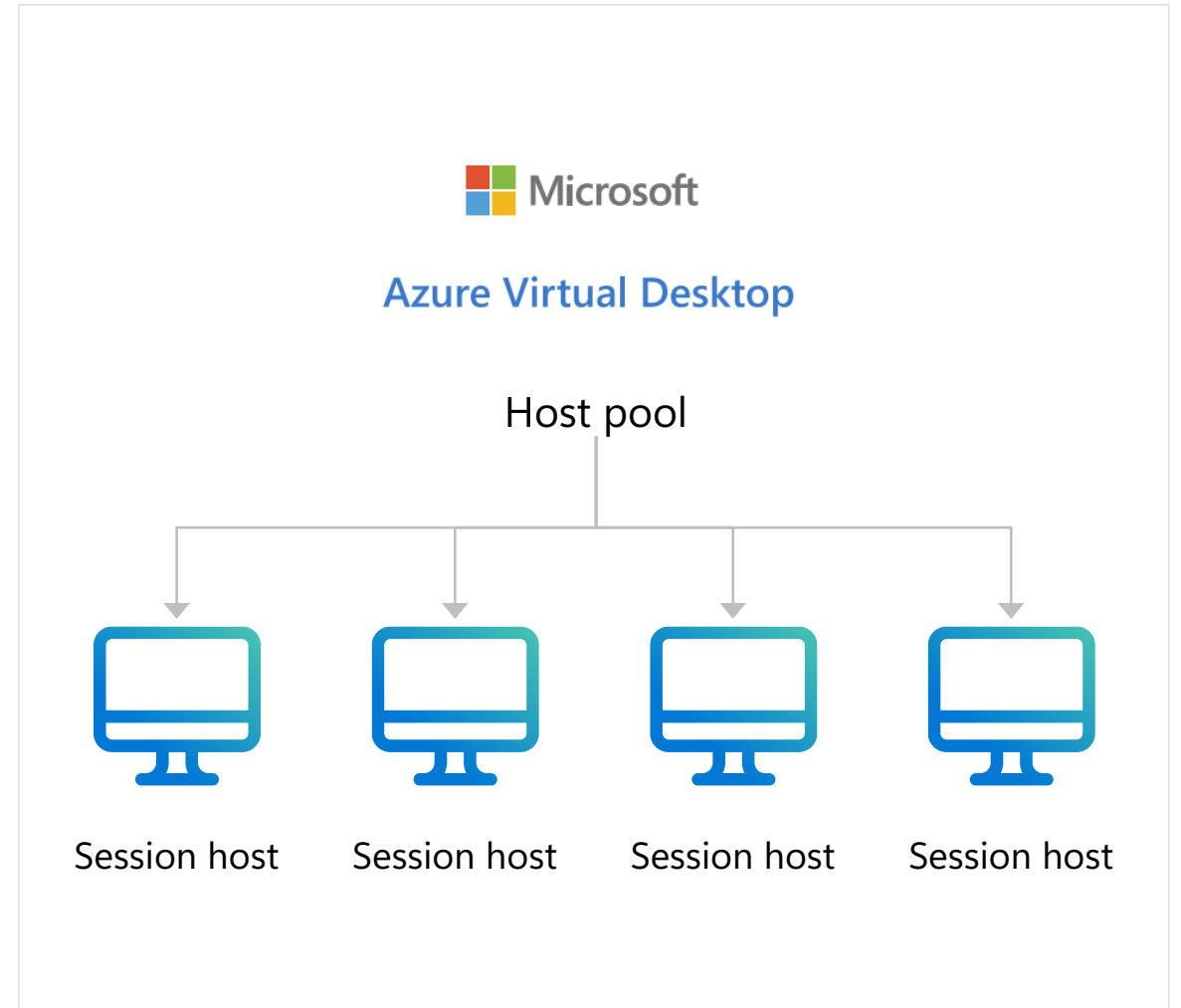


Host pools can either be pooled or personal:

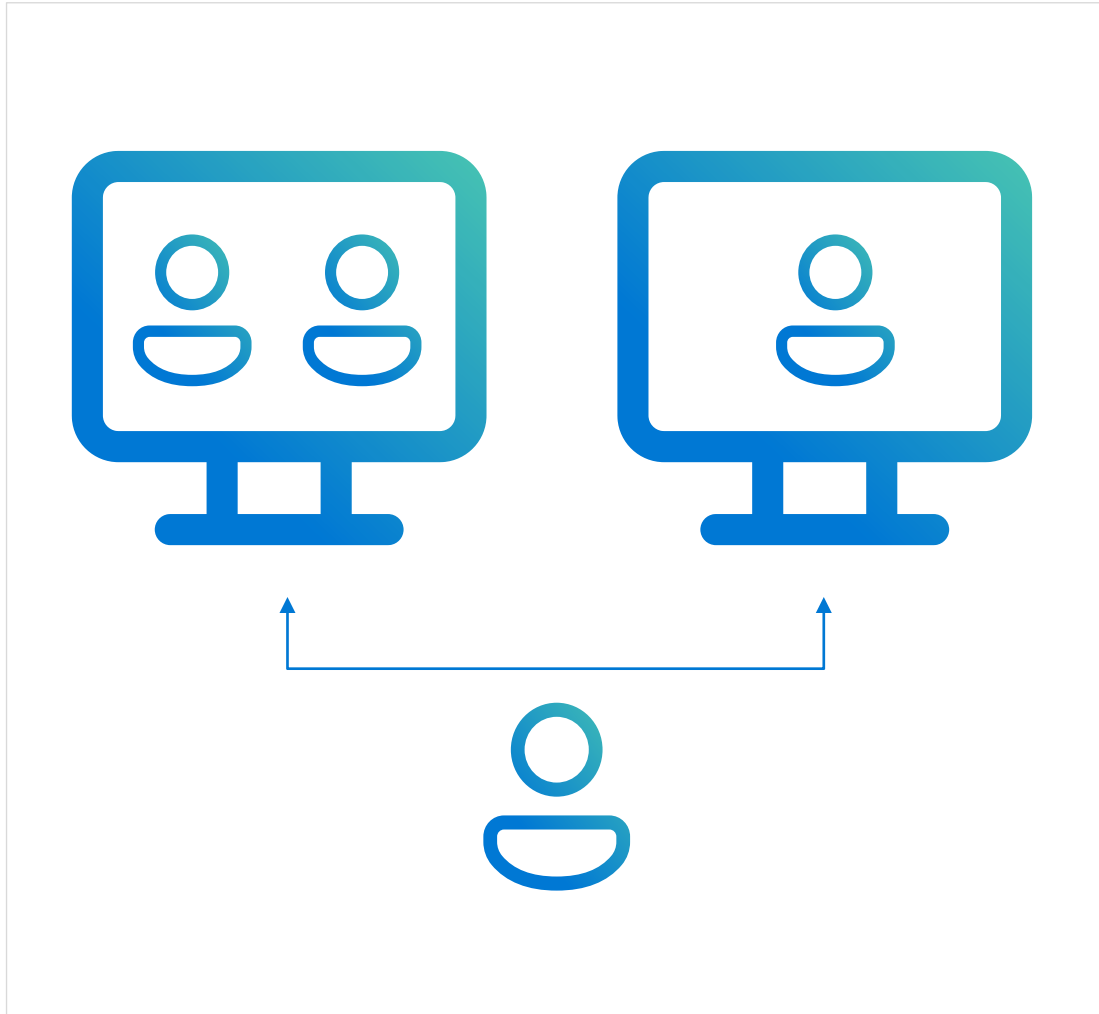
- In pooled host pools, one session host can host many user sessions (multi-session).
- In personal host pools, each user is assigned to one session host and that user always logs into the same session host.



Session hosts are domain joined virtual machines that have the Azure Virtual Desktop agent installed on them.



Pooled host pools



Users can sign in to any virtual machine (VM)



One or more users can sign in to the VM



More automation needed



Requires more effort to set up

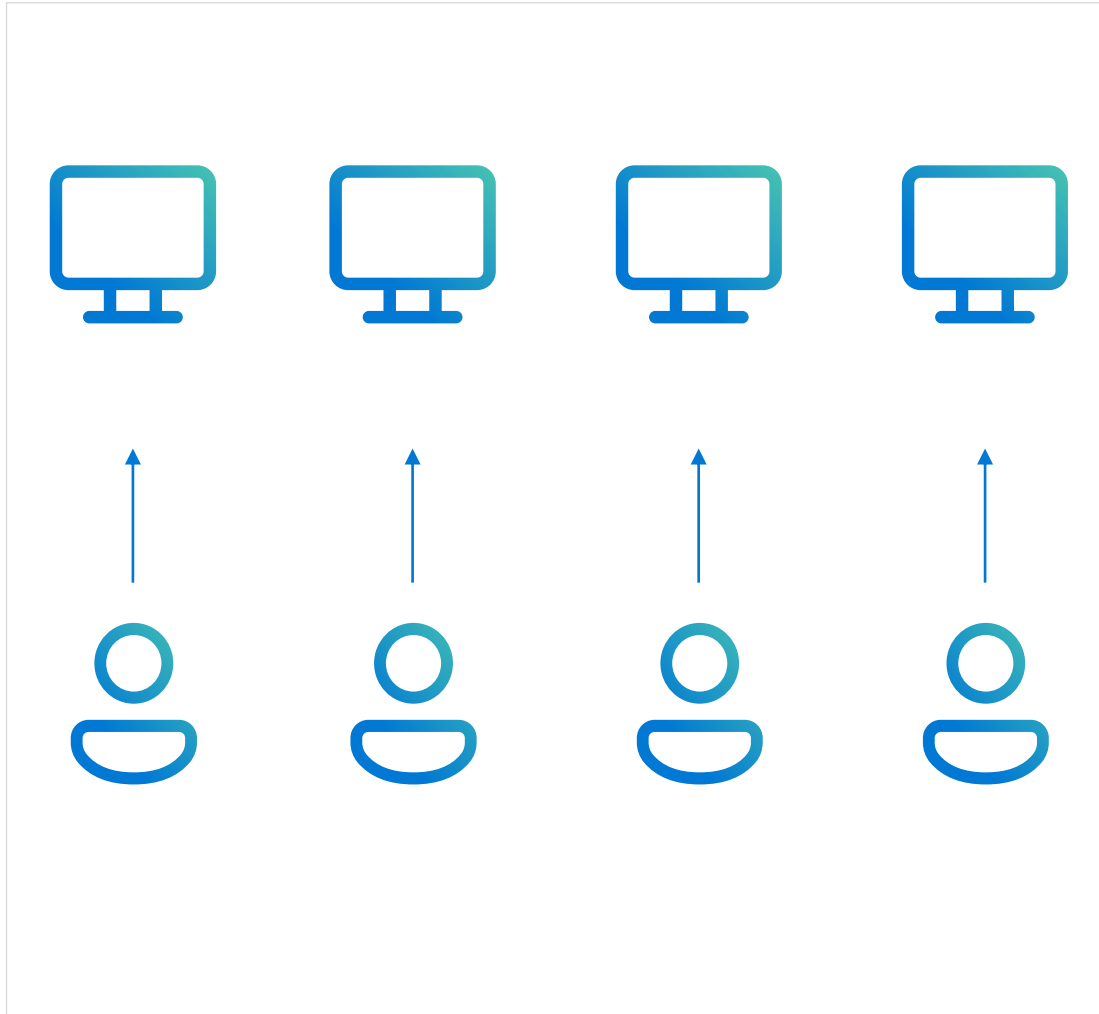


Better management if done right



Tends to be about half the cost of personal host pools

Personal host pools



Each virtual machine (VM) is assigned to a single user



The user will always sign in to that VM



Use existing tools and methodology to manage the estate



Simple to set up

Personal desktop unassignment/reassignment



Personal desktop unassignment/reassignment is a feature that allows you to remove or change the end user assignment for personal desktops.



With this added capability, you no longer need to delete and recreate a session host to remove a user assignment. Instead, you can simply select *Unassign user* or *Assign to a different user* in the portal.



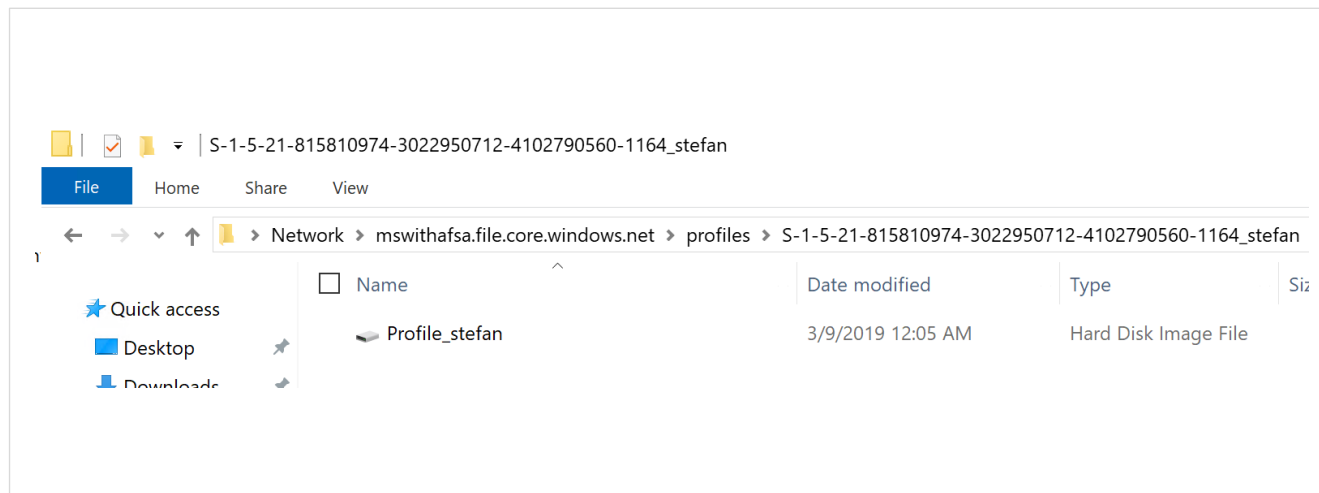
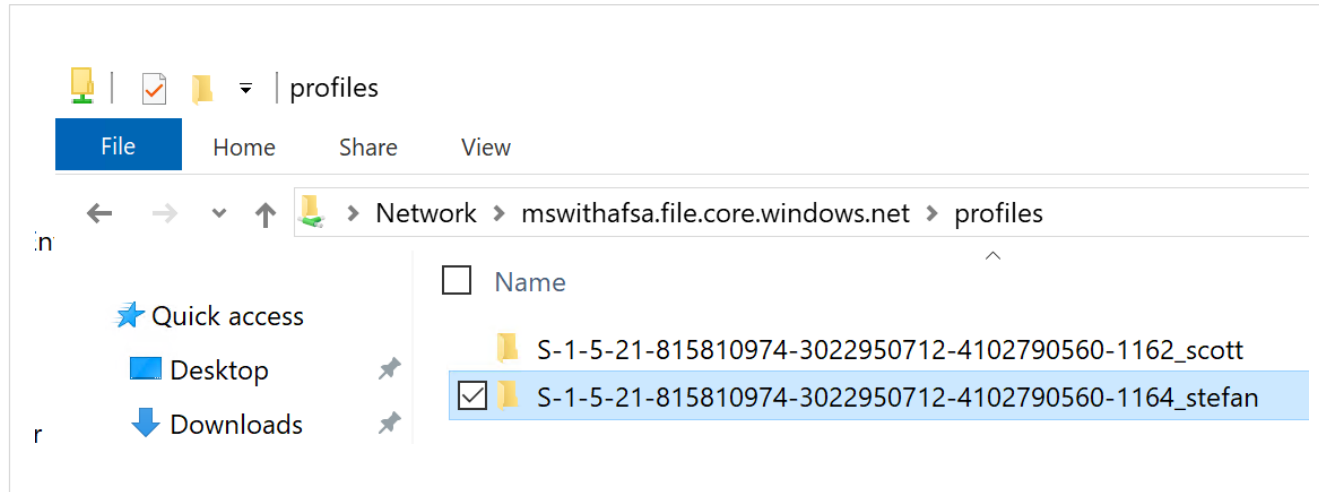
This is useful for temporary/shift-based workloads or scenarios where customers may have high end-user turnover.

The screenshot shows the Azure portal interface for managing personal desktops. At the top, there are navigation buttons: '+ Add', 'Refresh', 'Assignment', 'Export to CSV', and 'Turn drain mode on'. Below this, there is an information icon and a note: 'If you have assigned VMs to all of them. Group, all members of that group will see the VM'. A dropdown menu is open under 'Assignment', showing two options: 'Assign to a different user' and 'Unassign user', both of which are highlighted with red boxes. Below the menu, there is a search bar 'Filter by Name', a status filter 'Status: 12 selected', and a 'Drain mode' button. A table lists the personal desktops:

Name	Status	Drain mode	Assigned User
pd-0	Available	Off	(Assign)
pd-1	Available	Off	tstestuser1

The table has columns for 'Name', 'Status', 'Drain mode', and 'Assigned User'. The 'pd-1' row is selected, indicated by a blue checkmark in the first column. The 'Assigned User' for 'pd-1' is 'tstestuser1', while 'pd-0' is '(Assign)'. The 'Status' for both is 'Available' with a green checkmark, and 'Drain mode' is 'Off'.

Azure Virtual Desktop with FSLogix



Admins assign users to session hosts



End-users sign in



Profiles are assigned

User profile management with FSLogix



Persistent desktop experience

Users can customize their desktop and have a persistent experience every time they sign in.



Faster login and application launch

Optimized profile containers have much shorter launch times than roaming profiles and folder redirection. Consider Azure NetApp Files for the fastest launch times for larger, enterprise scale environments.



Multiple storage options available

Store profile containers in Azure files/Azure NetApp Files/file server clusters. Consider Azure NetApp Files for increased performance and better user experience at enterprise scale.



Migrate existing user profiles

Perform mass conversions of user profiles from various types to FSLogix-based profile containers at scale.

Apps with FSLogix & MSIX

Minimize number of master images by creating a single image with all applications



Why App Masking with FSLogix?

- Excellent app compatibility with no packaging, sequencing, backend infrastructure, or virtualization
- Control app licensing costs by limiting access to specific users
- Reduce the amount of host pools



Why MSIX?

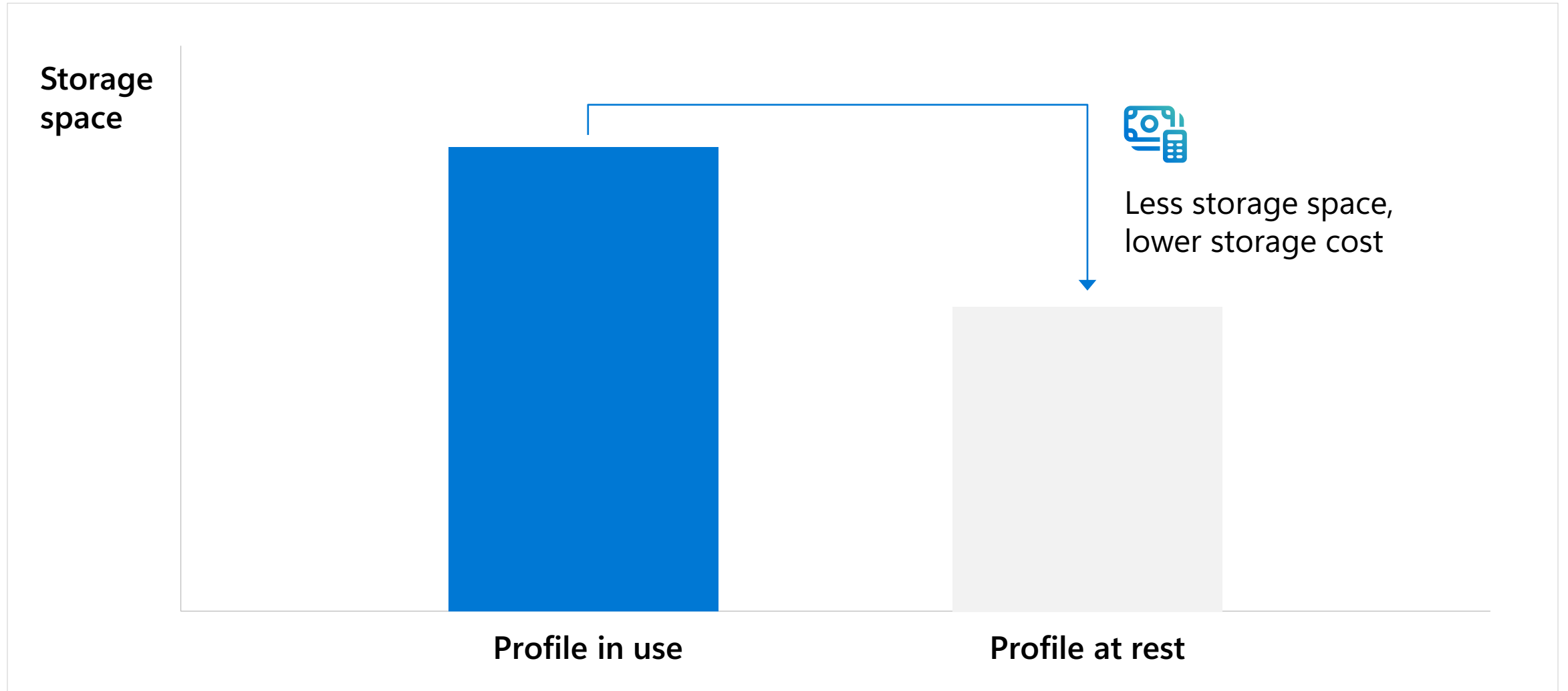
- Single format for physical and virtual environments
- Doesn't require packaging to be delivered
- Clean install/uninstall
- Secured by default
- Optimized storage and network bandwidth



Why MSIX app attach?

- Dynamic application delivery
- Only authorized users can see or access apps running on multiple user instances
- MSIX apps behave like natively installed apps

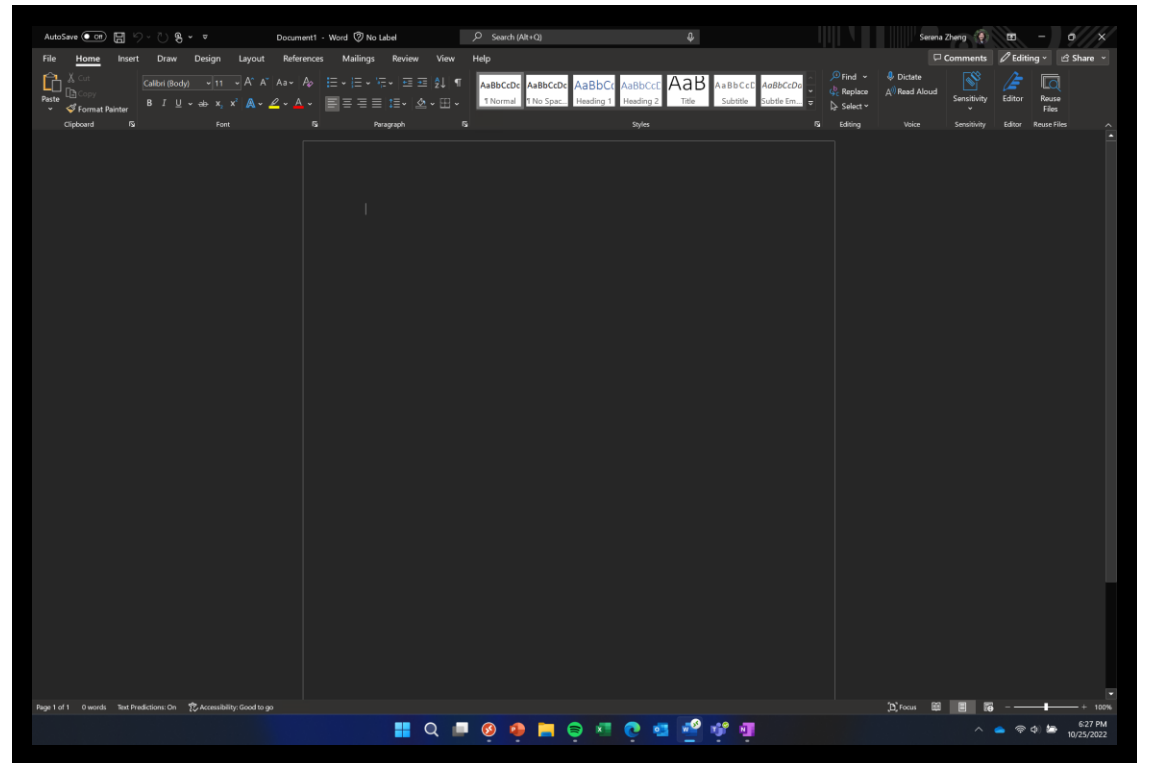
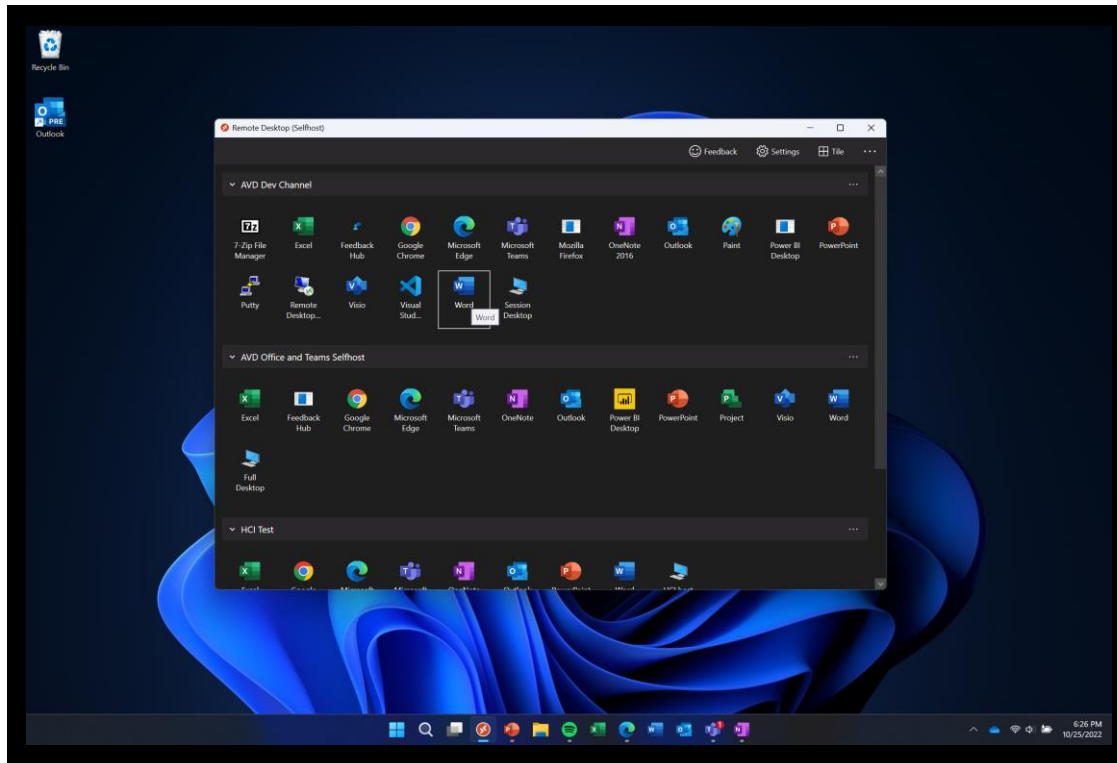
Storage cost savings with FSLogix



Azure Virtual Desktop remote app streaming



Migrate Windows apps to Azure and remotely stream them to your employees or customers with Azure Virtual Desktop



Benefits of streaming apps on Azure



Migrate your Windows apps to Azure, where you gain cloud scale, security, and agility, while giving users access from any device, from anywhere.



Reduce the complexity to run a traditional SaaS infrastructure by abstracting gateways, brokers, and other resources typically found in a Remote Desktop Service Remote Application deployment.



Modernize your legacy apps by enabling all types of applications to run consistently well across the breadth of Windows and other devices, with minimal rewrite and hardware requirements.



Enable new business models, such as time-based subscriptions or demos, without requiring complex Digital Rights Management (DRM) solutions to safeguard your intellectual property.



Expand globally and sell on Marketplace with newly reduced fees of 3% on Marketplace to reach customers everywhere.



Reduce support and validation costs by becoming platform agnostic across different customer architectures and use cases.

Securing, managing, & optimizing Azure Virtual Desktop

Overview

[Back to table of contents](#)

Securing, managing, & optimizing Azure Virtual Desktop

Security, management, and monitoring work together to create a resilient, cost- and performance-optimized Azure Virtual Desktop deployment.



Security

- Azure security approach
- Azure Virtual Desktop security model
- Security Best Practices:
 - Zero Trust and Conditional Access
 - Multifactor Authentication
 - Endpoint security
 - Networking security
- New features
 - SSO and Passwordless Authentication
 - Confidential VMs
 - FSLogix profiles on Microsoft Entra ID-joined VMs for hybrid users
 - Azure Private Link
 - Watermarking



Management & monitoring

- Microsoft Intune
- Multi-session configuration
- Azure Virtual Desktop Insights
- Azure Monitor and Azure Log Analytics
- Patch and Image Management
- Custom images
- Portal-integrated session host
- New features
 - Windows 11 Multi-session Monitoring
 - Microsoft Intune user configuration for multi-session



Availability & resilience

- Azure global footprint
- Business continuity & disaster recovery (BCDR) considerations and best practices
- New features:
 - Availability zones for Azure Virtual Desktop



Cost & performance optimization

- Deployment cost estimation
- Windows 11 and Windows 10 multi-session cost optimization
- Autoscale
- Azure Stack HCI
- New features
 - Windows 11 multi-session performance improvements
 - Group costs by host pool
 - Autoscale for grouped host pools
 - Personal Desktop Autoscale

Securing, managing, & optimizing Azure Virtual Desktop

Security approach

[Back to table of contents](#)

Optimizing the Azure Virtual Desktop security approach



The Azure Platform provides many features that enable admins to customize security for virtual desktop users.



Admins can use Multifactor Authentication, disk encryption, firewalls, endpoint protection, and monitoring to create a security regimen for Azure Virtual Desktop that's flexible and powerful without slowing or obscuring the day-to-day virtualization experience for users.



The following slides give an overview of security configuration and best practices:

- Zero Trust and Conditional Access
- Multifactor Authentication
- Endpoint security
- Network security
- Confidential computing

Azure security is...



Built-in

Simplified and streamlined security, built directly into Azure:

- All cloud resources, all layers of architecture
- Native controls for DevOps, scalable experiences for SecOps
- Broad policy support and actionable best practices



Modern

Protect, detect, and respond with AI and cloud scale:

- Reduces false positives with AI trained on trillions of signals
- Streamlines common tasks with automation
- Scale quickly and optimize costs with the cloud



Holistic

Secures your entire organization and works with what you have:

- Unified visibility, centrally managed
- Security across hybrid resources
- Multi-cloud posture management and threat protection with EASM and XDR

Azure security relies on multi-layered security controls across hybrid environments



Identity & access

Unify identity management and secure identities to implement Zero Trust.



App & data security

Encrypt data, and protect keys and secrets used by apps.



Network security

Enhance the protection of your virtual networks/



Threat protection

Access cloud-native SIEM and AI-driven security analytics.



Security management

Manage security state of hybrid workloads with a single view.

Azure Sentinel

Azure Security Center

Microsoft Entra ID

Azure Key Vault

Azure Firewall & DDoS

Azure Virtual Desktop delivers end-to-end security for your virtual desktops



Identity

- Conditional Access
- Microsoft Intune support
- MFA



Operating systems

- Microsoft Defender for Endpoint
- Policies



Apps

- Application Control
- AppLocker



Network

- Reverse connect
- Encryption
- Service tags
- Azure Firewall



Infrastructure

- Microsoft Defender for Cloud
- Secure score
- Best practices



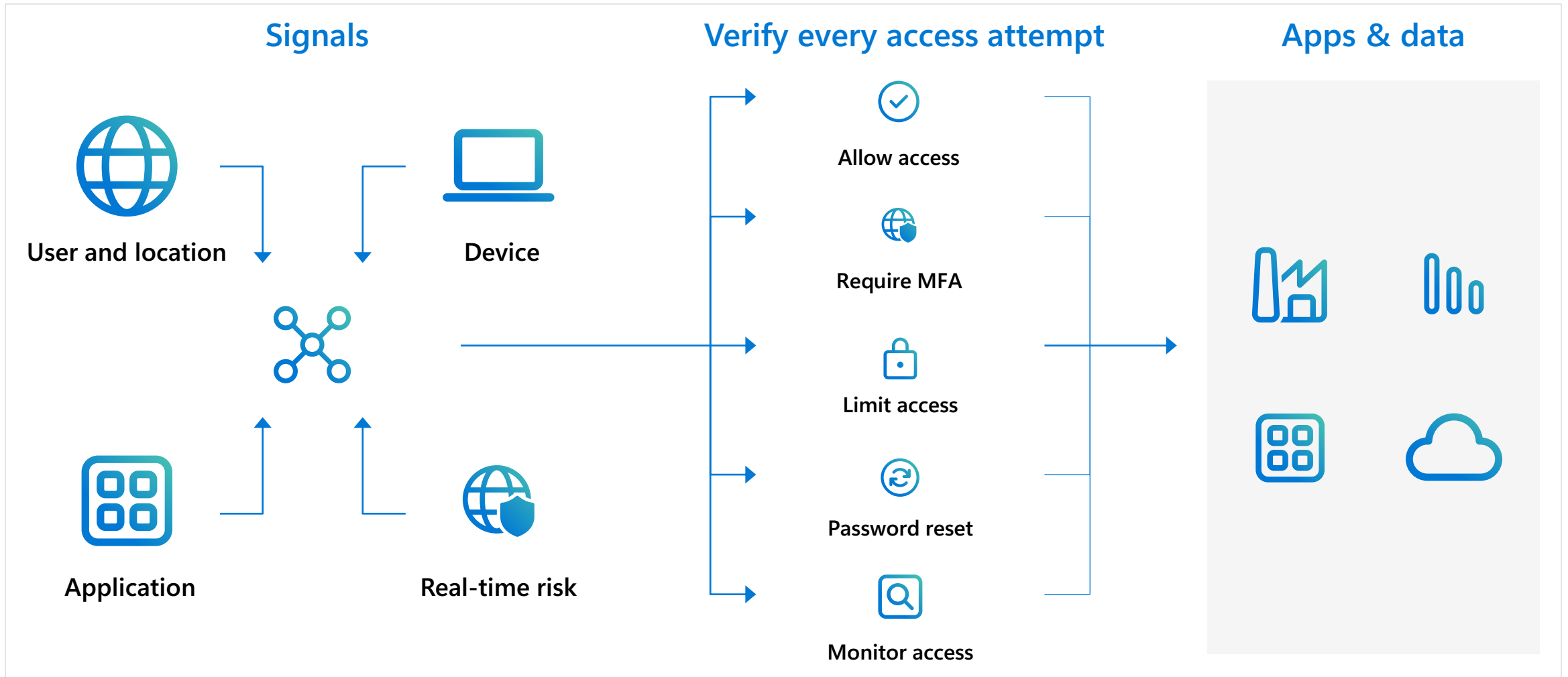
Data

- Information protection
- Azure Disk Encryption



Protect resources with Conditional Access

Enable Zero Trust with strong authentication and adaptive policies



Security controls & best practices for Azure Virtual Desktop - 1



Require Multifactor Authentication (MFA)

Activate Azure MFA for Microsoft Entra ID accounts



Enable Conditional Access

Configure a Conditional Access policy and target Azure Virtual Desktop



 Microsoft

demo@cspieter.com

Approve sign in request

 We've sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond.

Having trouble? [Sign in another way](#)

[More information](#)

Security controls & best practices for Azure Virtual Desktop - 2



Patch software vulnerabilities

Update live host/redeploy using latest gallery image



Control device redirection

Look into disabling smart card, port, drives, or camera redirection



Windows security baseline

Apply Windows 11/10 Enterprise Security baselines

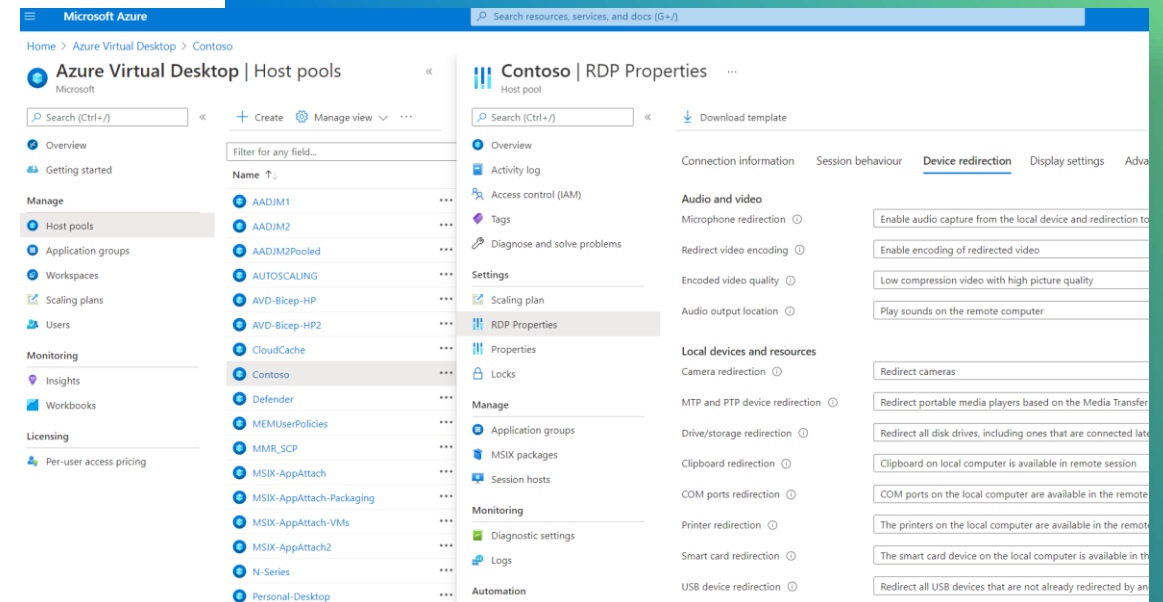


Define group policies

Set time limit for active but idle Remote Desktop Services sessions



Set time limit for disconnected sessions



Security controls & best practices for Azure Virtual Desktop - 3



Enable Azure Defender and Microsoft Defender for Cloud (formerly Azure Security Center)

Provides threat and vulnerability management assessments



Operationalize your Secure Score

Secure Score provides recommendations and best practice advice for increasing your security posture



Follow Azure best practices

Secure surrounding infrastructure with documented best practices

aka.ms/AzureSecureBP

Infrastructure



The screenshot shows the Azure Security best practices and patterns page. The page title is "Azure security best practices and patterns" with a date of 05/03/2019 and a reading time of 2 minutes. The page content includes an introduction stating that the articles below contain security best practices for designing, deploying, and managing cloud solutions. It also mentions that the best practices are intended to be a resource for IT pros. A list of best practices is provided, including Azure boundary security, Azure database security, Azure data security and encryption, Azure identity management and access control, Azure network security, Azure operational security, Azure PaaS Best Practices, Azure Service Fabric security, Best practices for Azure VM security, Implementing a secure hybrid network architecture in Azure, Internet of Things security, Securing PaaS databases in Azure, Securing PaaS web and mobile applications using Azure App Service, Securing PaaS web and mobile applications using Azure Storage, and Security best practices for IaaS workloads in Azure. The page also includes a "Is this page helpful?" section with "Yes" and "No" options.

Security controls & best practices for Azure Virtual Desktop - 4



Application Control (WDAC)

Control what drivers and applications can run



AppLocker

Control what applications users can run

The screenshot shows a web browser window displaying the Microsoft Docs page for 'WDAC and AppLocker Overview'. The page title is 'WDAC and AppLocker Overview' and the URL is 'https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/wdac...'. The page content includes a navigation menu on the left with items like 'Application Control for Windows', 'WDAC and AppLocker Overview', 'WDAC and AppLocker Feature Availability', 'WDAC design guide', 'Windows Defender Application Control deployment guide', 'Windows Defender Application Control operational guide', and 'AppLocker'. The main content area discusses the factors for choosing between WDAC and AppLocker. It states that although either AppLocker or WDAC can be used to control application execution on Windows 10 clients, the following factors can help decide when to use each technology.

WDAC is best when:

- You are adopting application control primarily for security reasons.
- Your application control policy can be applied to all users on the managed computers.
- All of the devices you wish to manage are running Windows 10.

AppLocker is best when:

- You have a mixed Windows operating system (OS) environment and need to apply the same policy controls to Windows 10 and earlier versions of the OS.
- You need to apply different policies for different users or groups on a shared computer.
- You are using application control to help users avoid running unapproved software, but you do not require a solution designed as a security feature.
- You do not wish to enforce application control on application files such as DLLs or drivers.

When to use both WDAC and AppLocker together

AppLocker can also be deployed as a complement to WDAC to add user- or group-specific rules for shared device scenarios where its important to prevent some users from running specific apps. As a best practice, you should enforce WDAC at the most restrictive level possible for your organization, and then you can use AppLocker to fine-tune the restrictions to an even lower level.

Security controls & best practices for Azure Virtual Desktop – 5

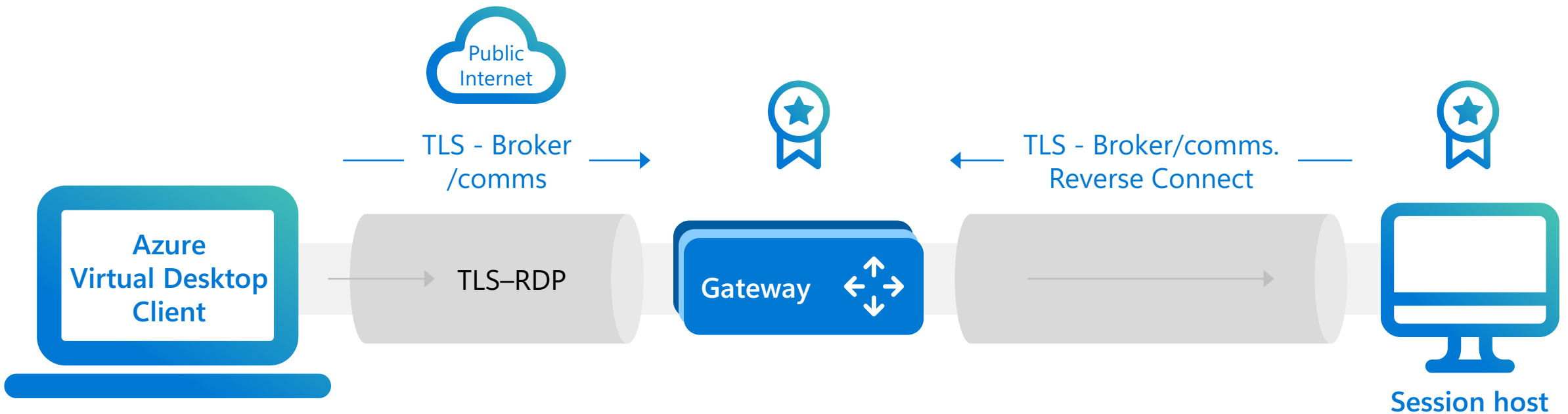
Reverse Connect

Disable all inbound traffic



Encryption

Secures all traffic



Security controls & best practices for Azure Virtual Desktop - 6



Microsoft Information Protection (MIP)

Discover, classify, and protect sensitive information wherever it lives or travels.



Azure Disk Encryption

Helps protect and safeguard your data.

ft Information Protection: x +

https://www.microsoft.com/en-us/security/business/information-protection

Microsoft | Security Solutions Products Operations Partners Resources Trust Center

All Microsoft Search Sign in

Protect your sensitive information

Learn how our solutions help you discover, classify, and protect sensitive information wherever it lives or travels.

[Read the white paper](#)

[Learn about information protection solutions >](#)

[Comprehensive data protection](#) [More information protection solutions](#) [Customer stories](#) [Blogs and white papers](#) [Additional resources](#)

Security controls & best practices for Azure Virtual Desktop - 7



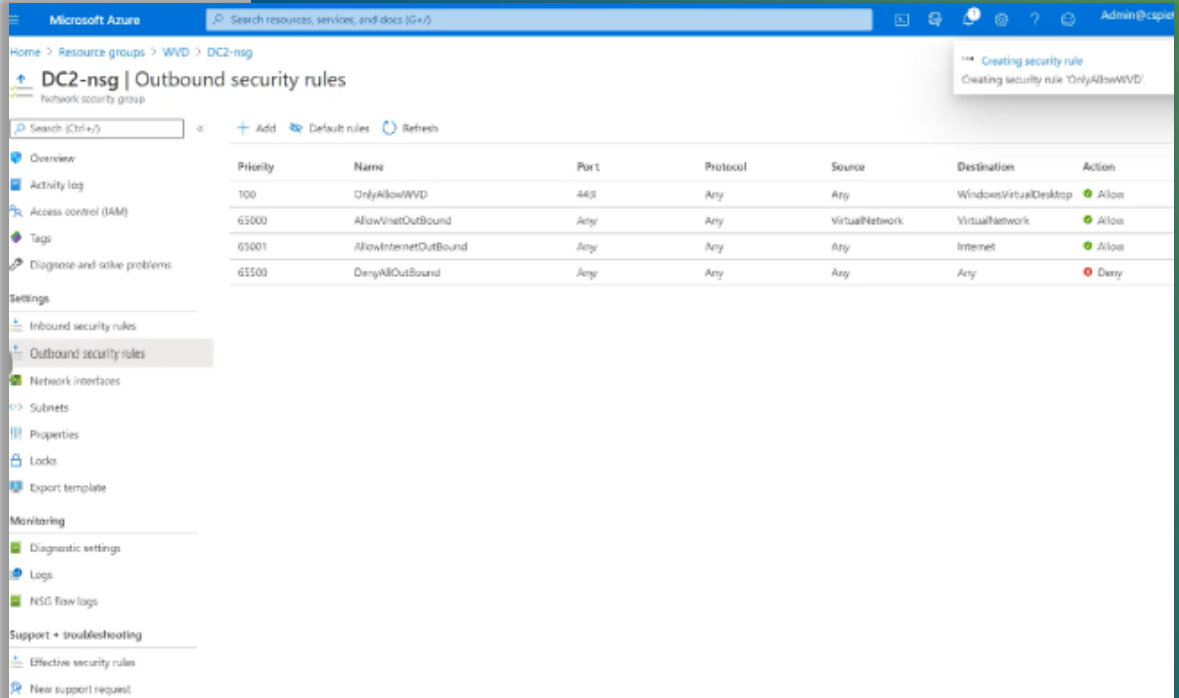
NSG Firewall service tags

Limit network-level traffic Azure Virtual Desktop traffic with service tags.



Azure Firewall

Consider Azure Firewall for application-level protection with Azure Virtual Desktop FQDN tag.



Microsoft Azure | Search resources, services, and docs (G+V) | Admin@corp

Home > Resource groups > WVD > DC2-nsg

DC2-nsg | Outbound security rules

Network security group

Search (Ctrl+F) | Add | Default rules | Refresh

Priority	Name	Port	Protocol	Source	Destination	Action
100	OnlyAllowWVD	443	Any	Any	WindowsVirtualDesktop	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces
- Subnets
- Properties
- Locks
- Export template

Monitoring

- Diagnostic settings
- Logs
- NSG flow logs

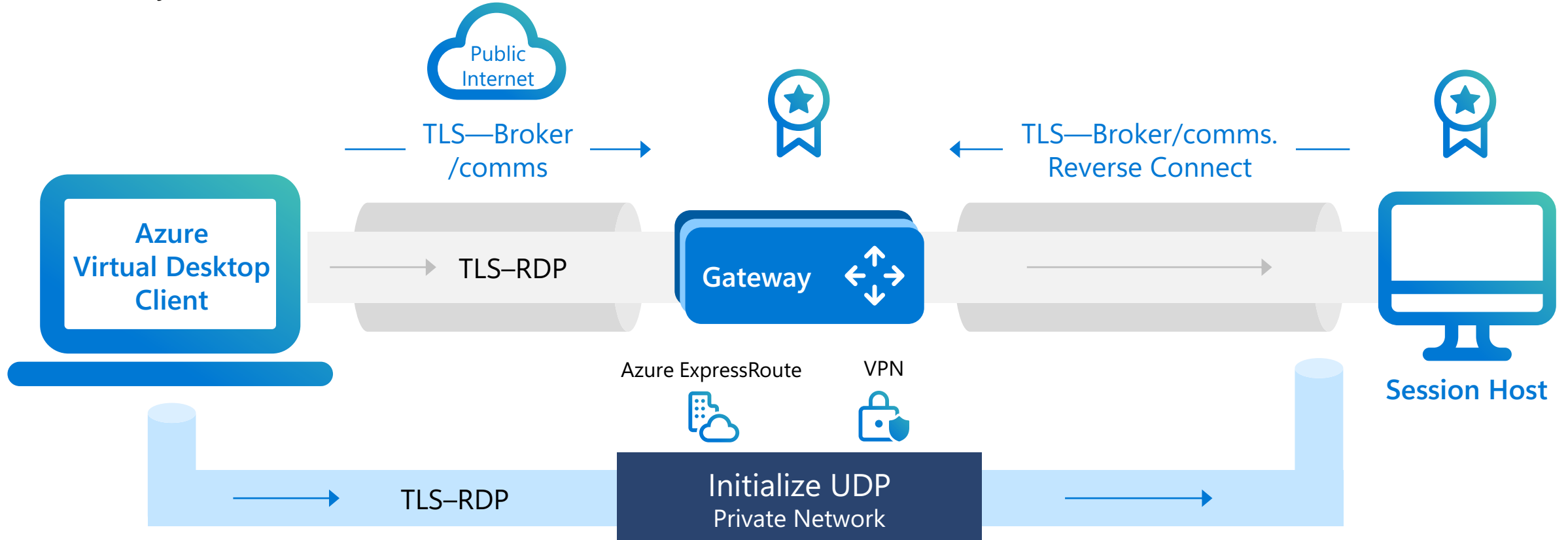
Support + troubleshooting

- Effective security rules
- New support request

Security controls & best practices for Azure Virtual Desktop – 8

RDP Shortpath for managed networks

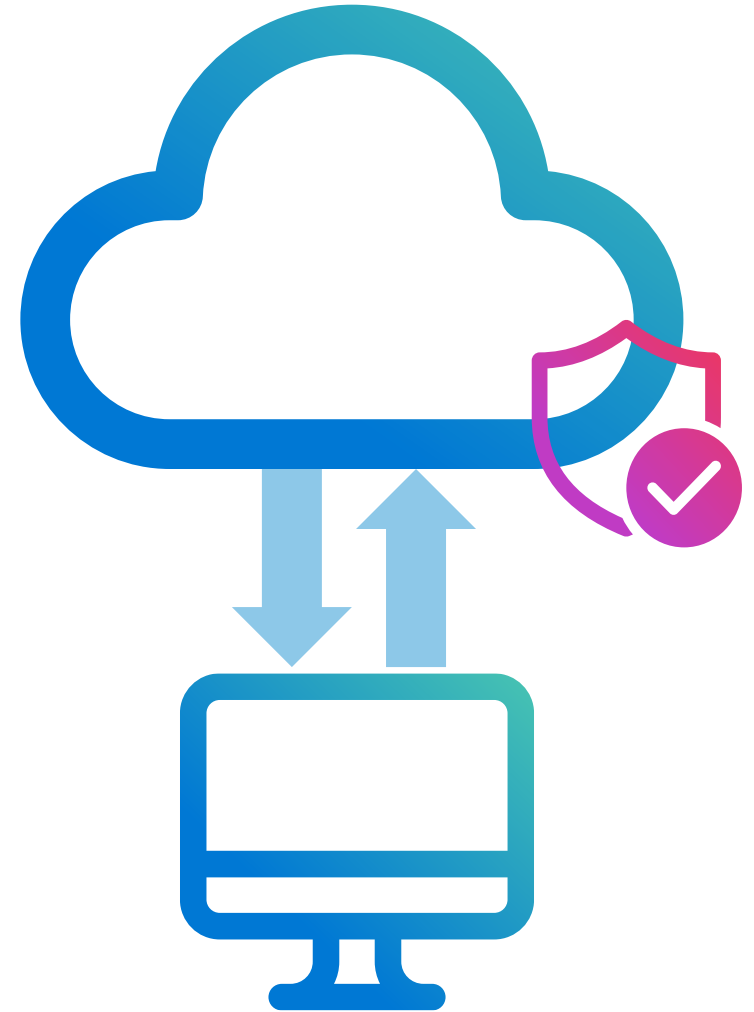
Redirects just the RDP traffic across your managed network directly and privately to the Azure Virtual Desktop VMs on your Virtual Network



Azure Virtual Desktop: Remote Desktop Protocol (RDP)

RDP is a collection of services that streams from the cloud to a local client.

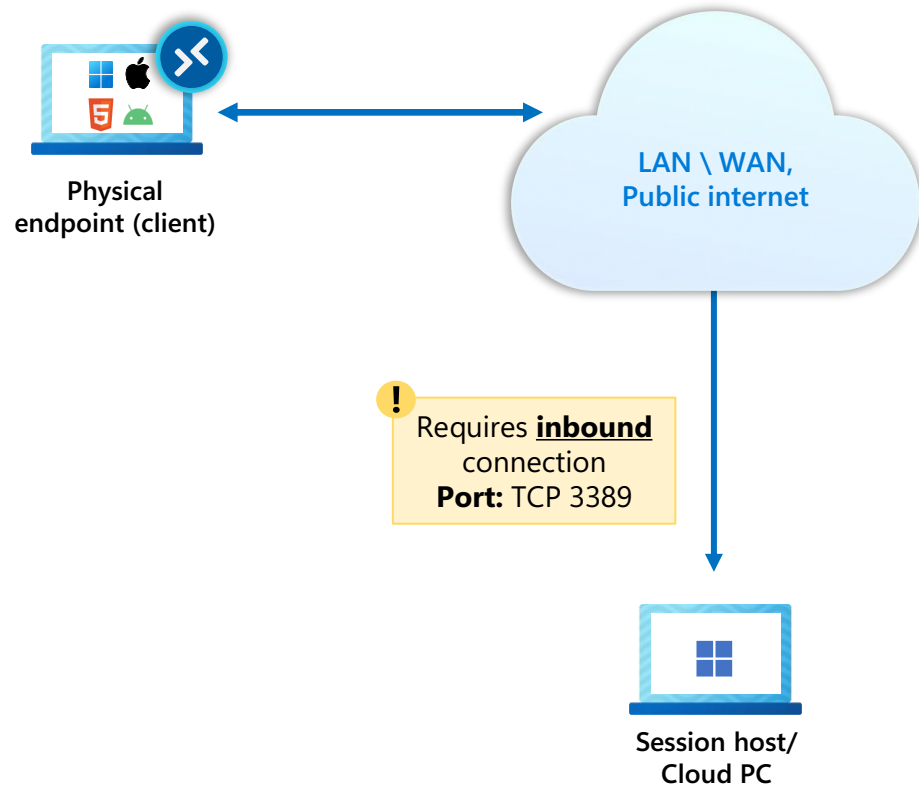
RDP supports various scenarios across connection reliability, remote content streaming, local input & device redirections (USB, mouse, location, etc.), media streaming optimizations, security features (single sign-on, passwordless authentication, watermarking, etc.) and more.



RDP client connectivity

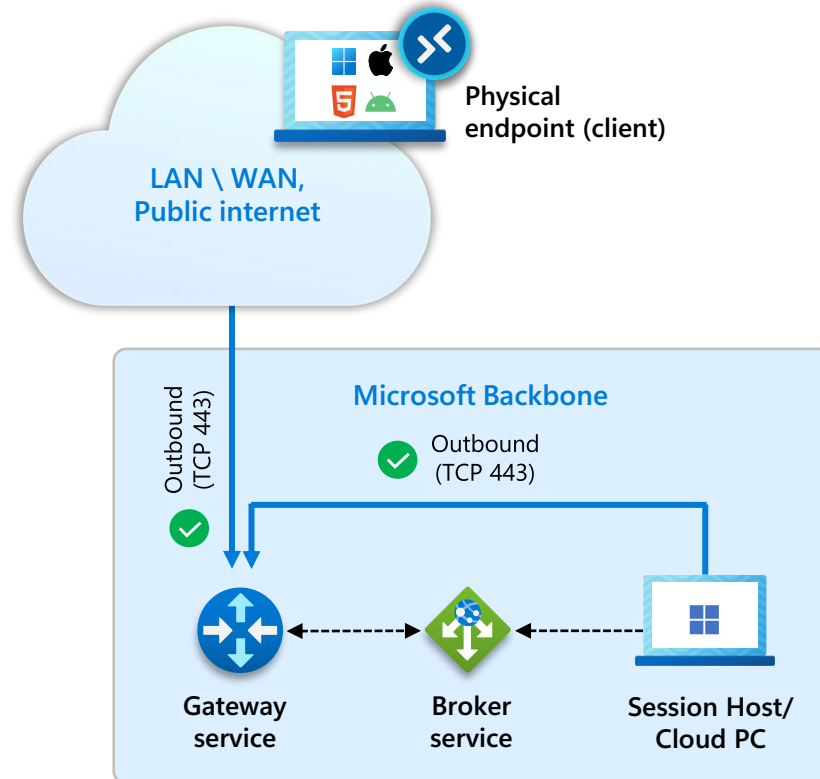
Traditional RDP connection (3389)

By default, an RDP connection to a client / server uses **inbound** port 3389 to enable users to access remote computers



Outbound connection (reverse connect)

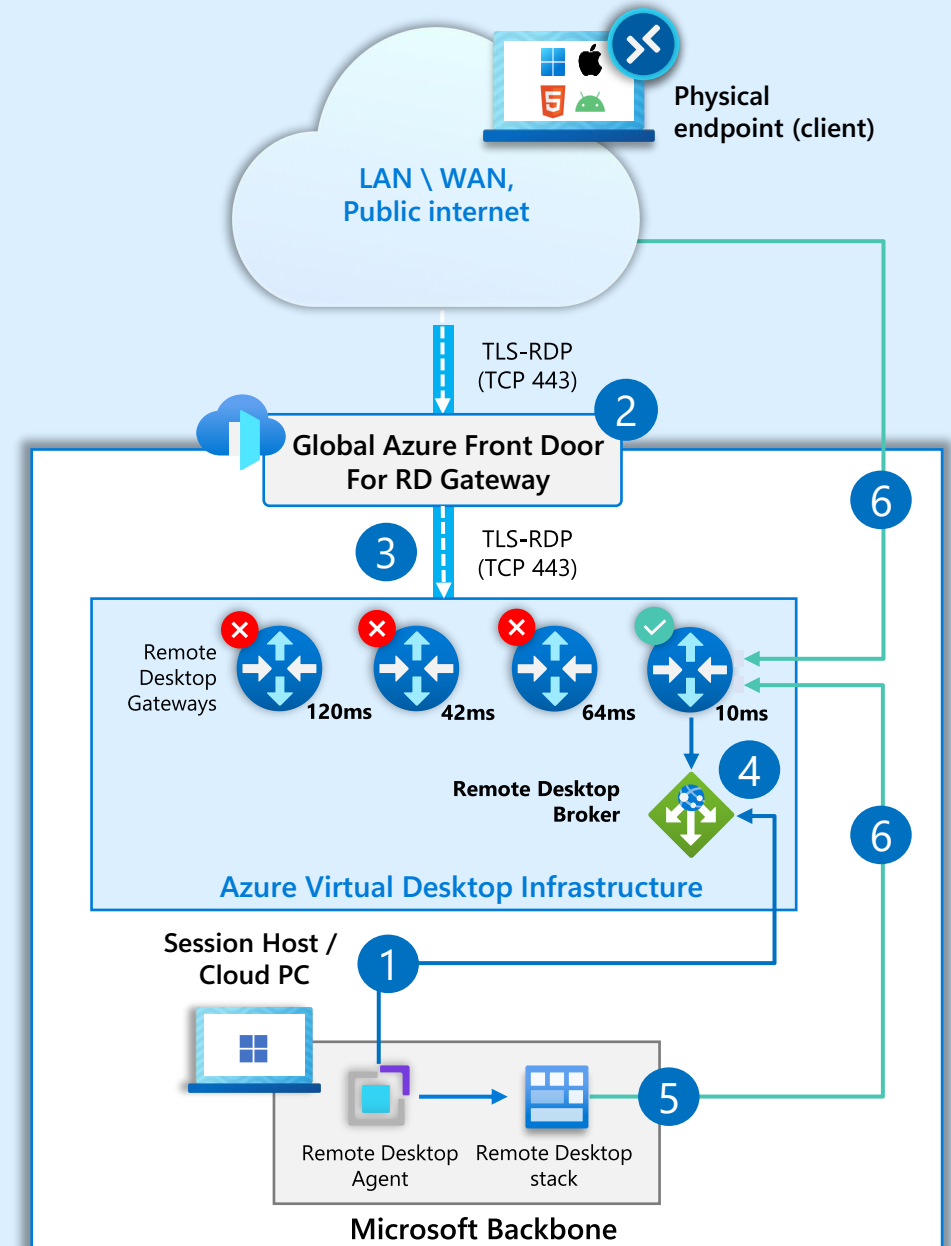
With Azure Virtual Desktop and Windows 365 an encrypted (TLS 1.2) outbound connection is used (TCP 443), meaning no inbound connectivity is required



RDP connection flow

1. Session Host / Cloud PC establishes outbound connection (**reverse connect**) with the Azure Virtual Desktop (AVD) Infra via Remote Desktop Agent / SxS Stack.
2. Client establishes a **secure TLS 1.2 connection** to an Azure Virtual Desktop Gateway instance with the help of [Azure Front Door](#).
3. Client is told to connect to a Gateway with the **lowest latency** and lowest number of connections.
4. Gateway validates the request and asks the Broker to **orchestrate the connection**. Broker identifies the Session Host / Cloud PC and uses the previously established persistent communication channel to initialize the connection.
5. Remote Desktop stack initiates the **TLS 1.2 connection** to the same Gateway instance as used by the client.
6. After both client and session host connected to the Gateway, the gateway starts relaying the raw data between both endpoints, this establishes the base **reverse connect transport** for the RDP

[Understanding Azure Virtual Desktop network connectivity - Azure | Microsoft Learn](#)



Connection performance – RDP Shortpath

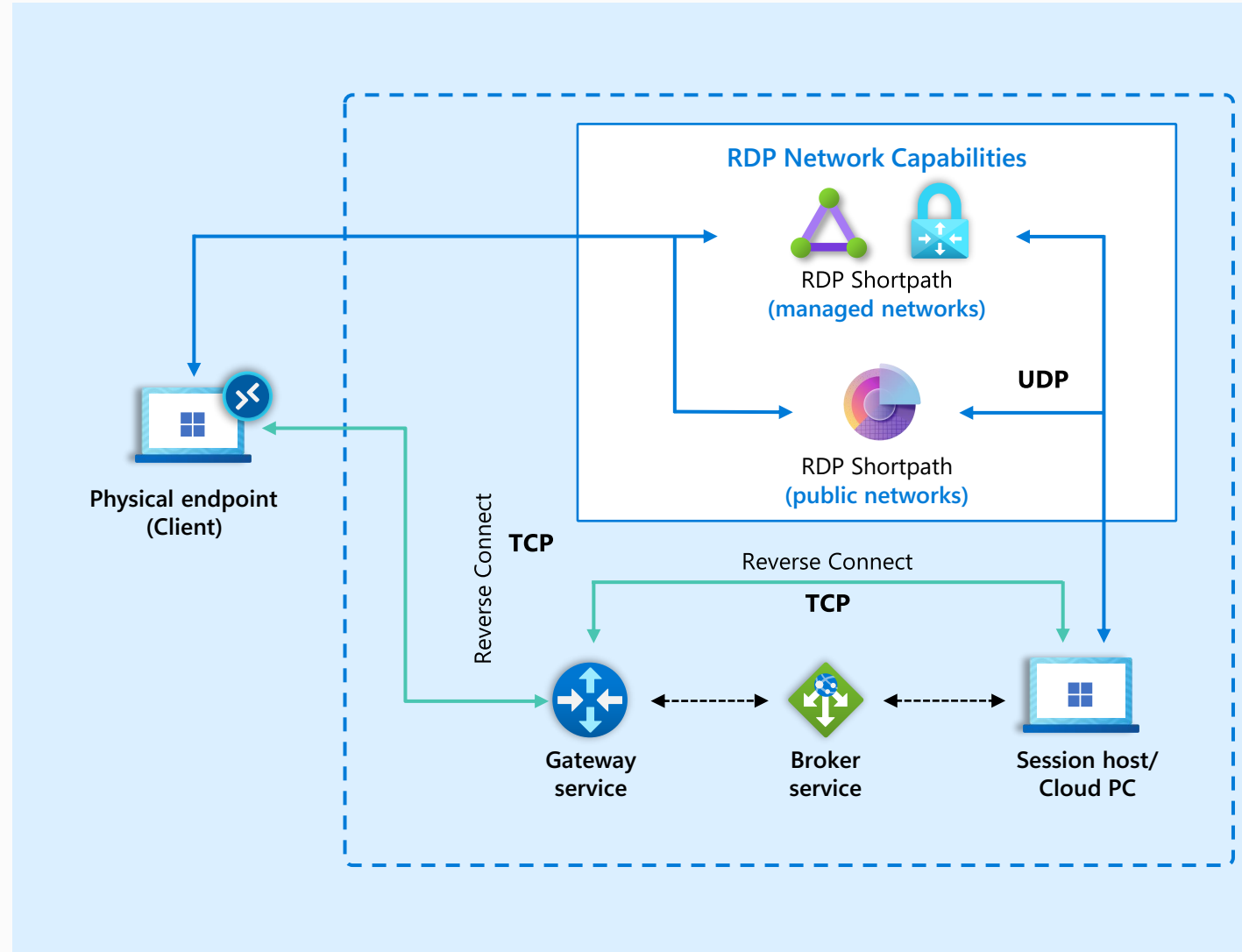
Connection performance is a collection of **protocol transport improvements** that fit under the umbrella of the evolved RDP experience.

RDP Shortpath establishes **reliable UDP-based transport** with the goal of improving the **connection reliability and reducing overall latency**.

Previously all connections were made via **TCP (reverse connect)** which allowed retransmission of packets at the cost of latency.

RDP Shortpath ensures that RDP connections have **high connectivity** and **lower latency than TCP** based connections.

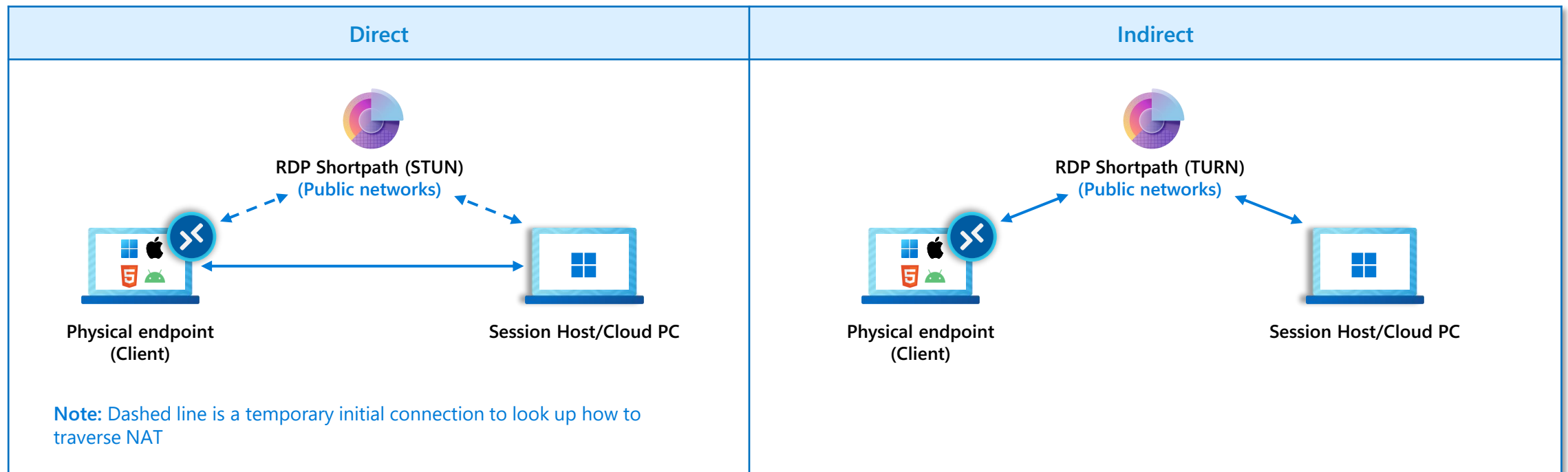
[RDP Shortpath - Azure Virtual Desktop | Microsoft Learn](#)



RDP ShortPath – public networks -2

When direct connectivity is established between the client and the session host / Cloud PC, there are two connection types when using a public connection, which are listed here in order of preference:

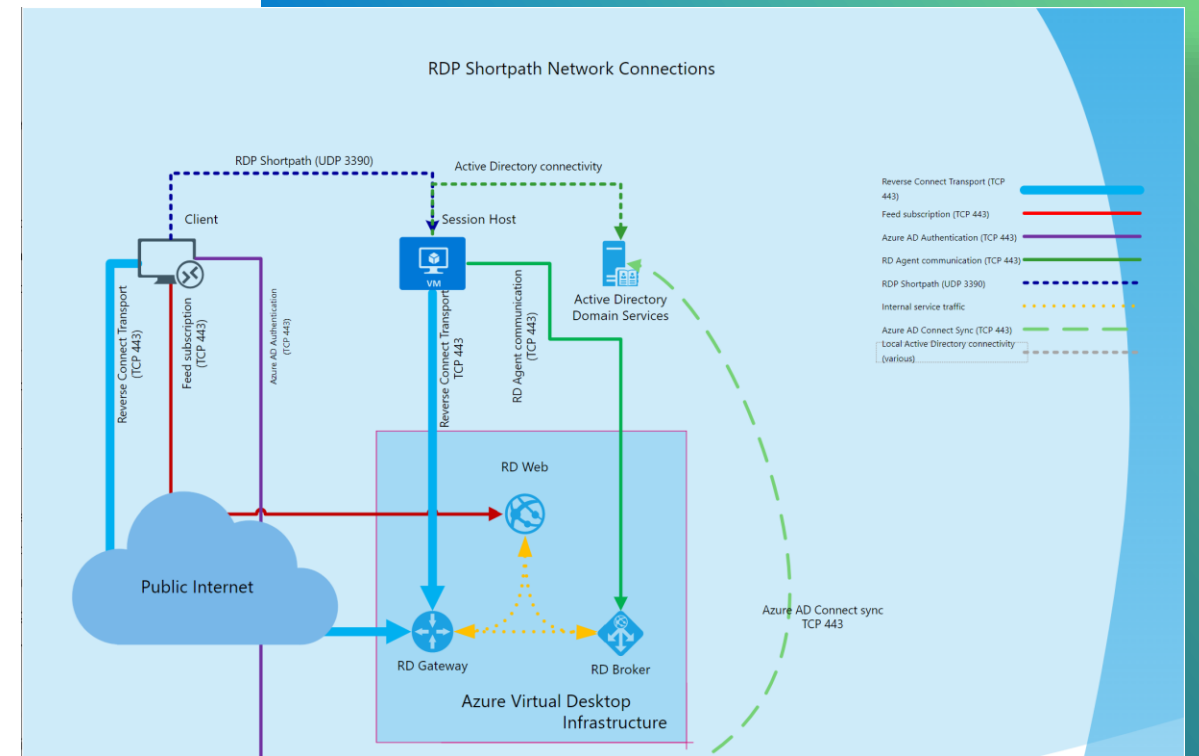
1. A **direct** UDP connection using the **Simple Traversal Underneath NAT (STUN)** protocol between a client and session host.
2. An **indirect** UDP connection using the **Traversal Using Relay NAT (TURN)** protocol with a relay between a client and session host. This is currently in public preview.



RDP Shortpath for managed networks



RDP Shortpath also works with managed networks using the private network (VPN) to establish a User Datagram Protocol (UDP) flow between client and session host.



Single sign-on & passwordless authentication for Azure Virtual Desktop

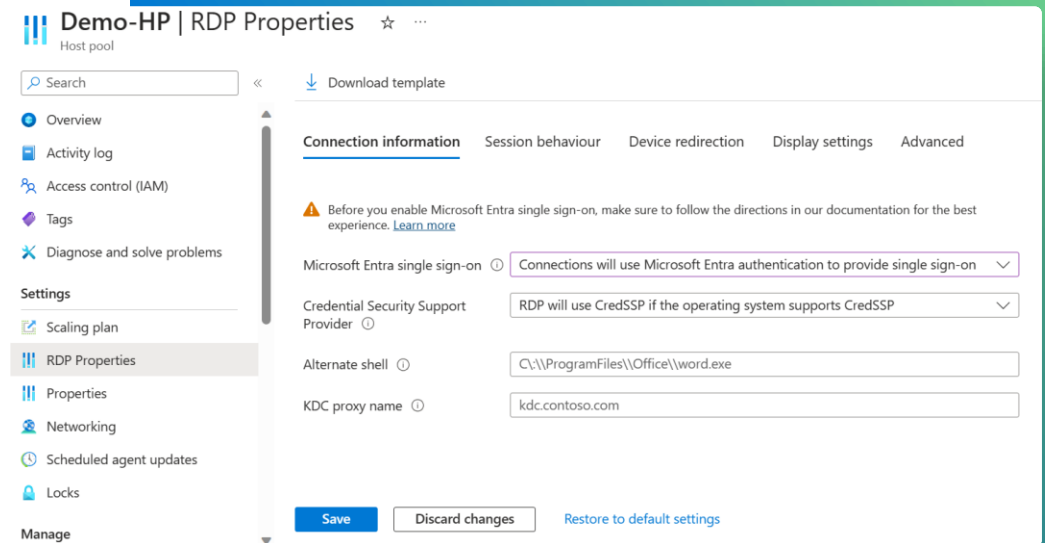
Leverage Microsoft Entra authentication to provide single sign-on, passwordless authentication, and support for 3rd-party Identity Providers.

It is a more secure and user-friendly authentication option that:

- Provides a single sign-on experience when connecting to a remote desktop or app
- Enables end-to-end passwordless support
- Enables support for 3rd-party Identity Providers.

Enablement requirement:

- Single sign-on can be enabled through Windows 365 provisioning policies and Azure Virtual Desktop host pool RDP properties.
- WebAuthn redirection is enabled by default.

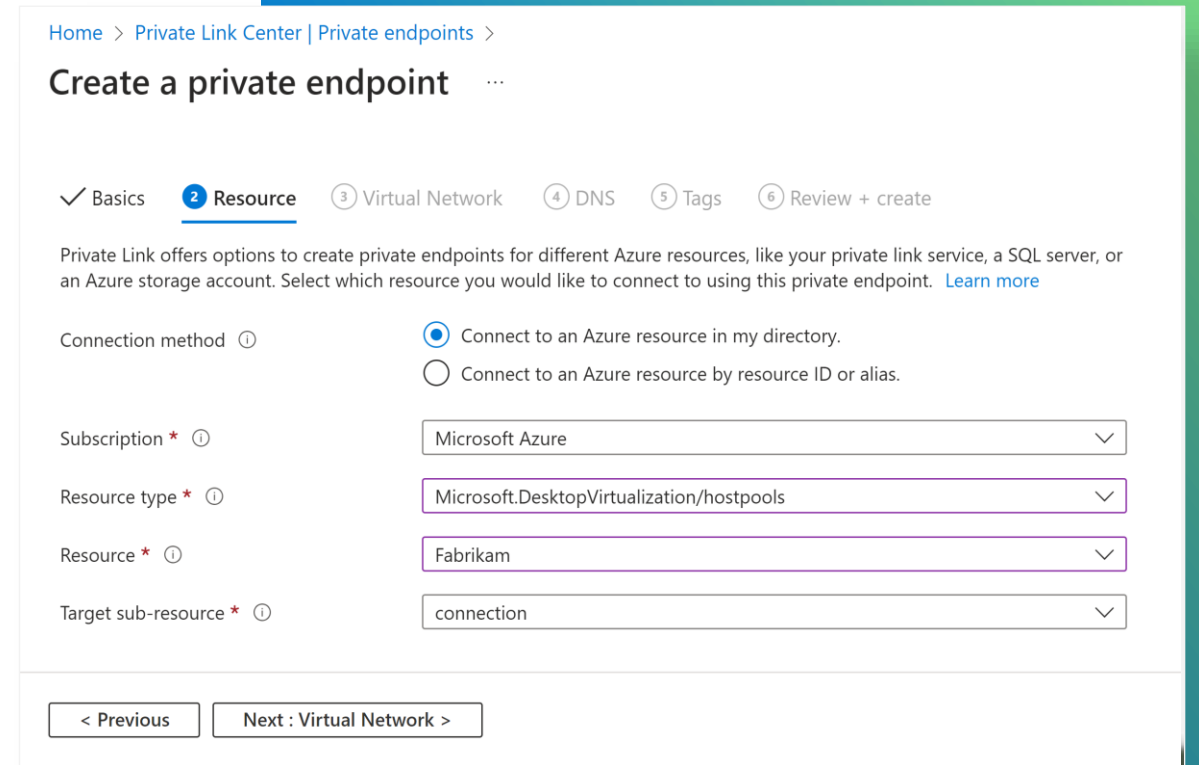


Azure Private Link

Private Link for Azure Virtual Desktop allows users to establish secure connections to remote resources by using private endpoints.

Private Link gives customers added security, allowing access to remote resources via private endpoints within the protected Microsoft Backbone network.

Follow these steps to [configure Private Link for Azure Virtual Desktop](https://learn.microsoft.com/azure/virtual-desktop/private-link-setup) (learn.microsoft.com/azure/virtual-desktop/private-link-setup)



Home > Private Link Center | Private endpoints >

Create a private endpoint

✓ Basics **2 Resource** ③ Virtual Network ④ DNS ⑤ Tags ⑥ Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Connection method ⓘ

Connect to an Azure resource in my directory.

Connect to an Azure resource by resource ID or alias.

Subscription * ⓘ

Resource type * ⓘ

Resource * ⓘ

Target sub-resource * ⓘ

< Previous Next : Virtual Network >

FSLogix profiles on Microsoft Entra joined VMs for hybrid users

The screenshot displays the Microsoft Azure portal interface for configuring identity-based access on a file share named 'azstgfileshare001'. The main content area is titled 'azstgfileshare001 | Identity-based access' and includes a 'Refresh' button. It outlines two steps: 'Step 1: Enable an identity source' and 'Step 2: Set share-level permissions'. Under Step 1, three options are shown: 'Active Directory Domain Services (AD DS)' (already configured), 'Microsoft Entra Domain Services' (already configured), and 'Microsoft Entra Kerberos' (Enabled, with a 'Configure' link). A note states that Microsoft Entra ID is not a domain controller. Step 2 involves setting permissions for all authenticated users and groups, with the 'Storage File Data SMB Share Contributor' role selected. A right-hand sidebar titled 'Microsoft Entra Kerberos' provides additional context, a confirmation checkbox, and a warning about granting admin consent. Below this, 'Domain services' configuration fields are shown with 'contoso.com' for the domain name and a GUID for the domain GUID. 'Save' and 'Discard' buttons are located at the bottom of the main panel and the sidebar.

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

Home > azstgfileshare001 | File shares >

azstgfileshare001 | Identity-based access

File shares

Refresh

Identity-based access can be enabled in two steps for a particular share in this storage account. This allows individual users to use their Active Directory or Microsoft Entra account to access the share.

Step 1: Enable an identity source

Choose the identity source that contains the user accounts that will access a share in this storage account. You can set up identity-based access control for user accounts located in either of the following identity sources:

- Active Directory Domain Services (AD DS) you host on a Windows Server (generally referred to as "on-premises AD" even though you might host these servers in Azure)
- Microsoft Entra Domain Services (Microsoft Entra DS), a platform as a service, hosted directory service and domain controller in Azure
- Microsoft Entra Kerberos allows using Kerberos authentication from Microsoft Entra ID joined clients. In order to use Microsoft Entra Kerberos, user accounts must be hybrid identities.

Active Directory Domain Services (AD DS)
Another access method is already configured

Microsoft Entra Domain Services
Another access method is already configured

Microsoft Entra Kerberos
Enabled
[Configure](#)

Microsoft Entra ID is not a domain controller, only a directory service. User accounts solely based in Microsoft Entra ID are currently not supported.

Step 2: Set share-level permissions

Once you have enabled Active Directory or Microsoft Entra source on your storage account, you must configure share-level permissions in order to get access to your file shares. The permissions you assign to all authenticated identities as a default share level permission and you can assign them to specific Microsoft Entra users/user group. [Learn more](#)

Permissions for all authenticated users and groups

Default share-level permissions

Disable permissions and no access is allowed to file shares

Enable permissions for all authenticated users and groups

Select appropriate role *

Storage File Data SMB Share Contributor

Save Discard

Microsoft Entra Kerberos

Identity-based access

Microsoft Entra Kerberos authentication allows users to connect to Azure Files over the internet without requiring a line-of-sight to domain controllers. In order to use Microsoft Entra Kerberos, user accounts must be hybrid identities. [Learn more](#)

Microsoft Entra Kerberos

After enabling Microsoft Entra Kerberos authentication, you will need to explicitly grant admin consent to the new Microsoft Entra ID application registered in your Microsoft Entra tenant. [Learn more](#)

Domain services

To configure directory and file level permissions through Windows File explorer, you also need to specify domain name and domain GUID for your on-premises AD. You can get this information from your domain admin or from an on-premises AD-joined client. If you prefer to configure using icacls, this step is not required. [Learn more](#)

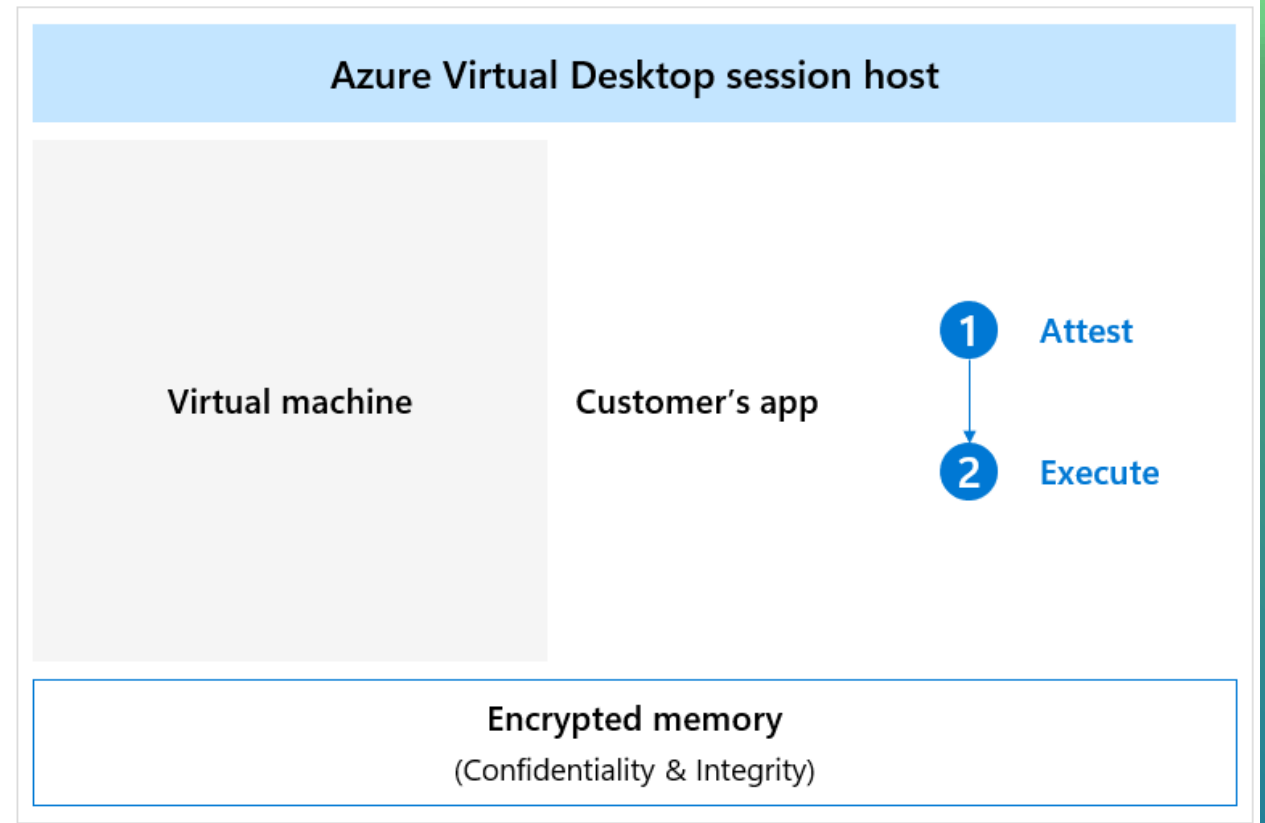
Domain name

Domain GUID

Save Discard

Confidential Virtual Machines for Azure Virtual Desktop - 1

Confidential Virtual Machines (CVMs) is a more secure VM offering that possesses memory encryption with integrity protection, leveraging AMD SEV-SNP security features.



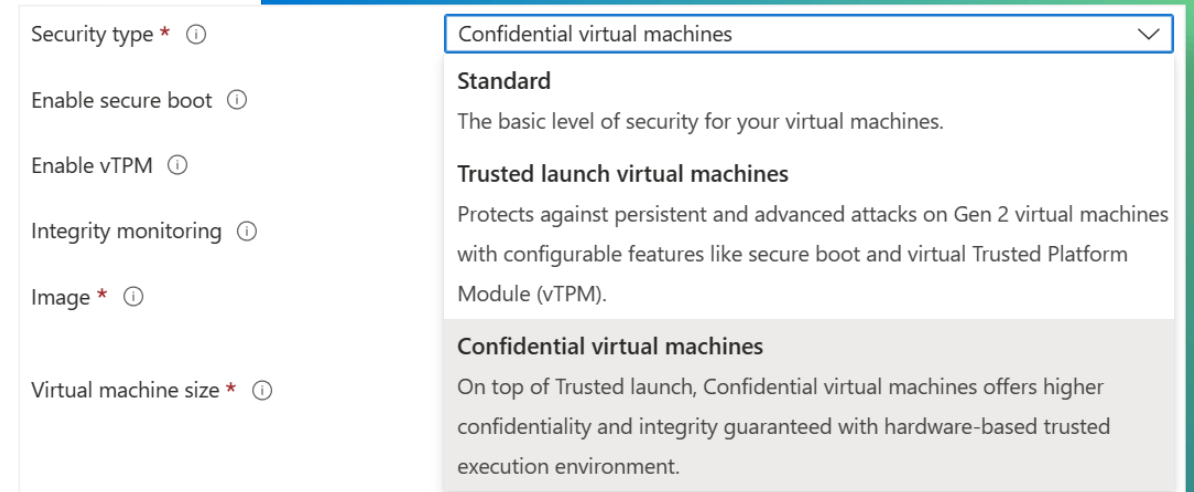
Confidential Virtual Machines for Azure Virtual Desktop -2

Confidential Virtual Machines (CVMs) ensure workloads running on a user's virtual desktop are encrypted in memory, protected in use, and backed by hardware root of trust.

Confidential Virtual Machines help to strengthen guest protections to deny the hypervisor and other host management components code access to the VM memory and state.

Select "Create a host pool" in the Azure Virtual Desktop section of the Azure Portal.

- Select *Confidential Virtual Machines* from the *Security Type* dropdown in the Azure Virtual Desktop Host Pool Virtual Machine blade.



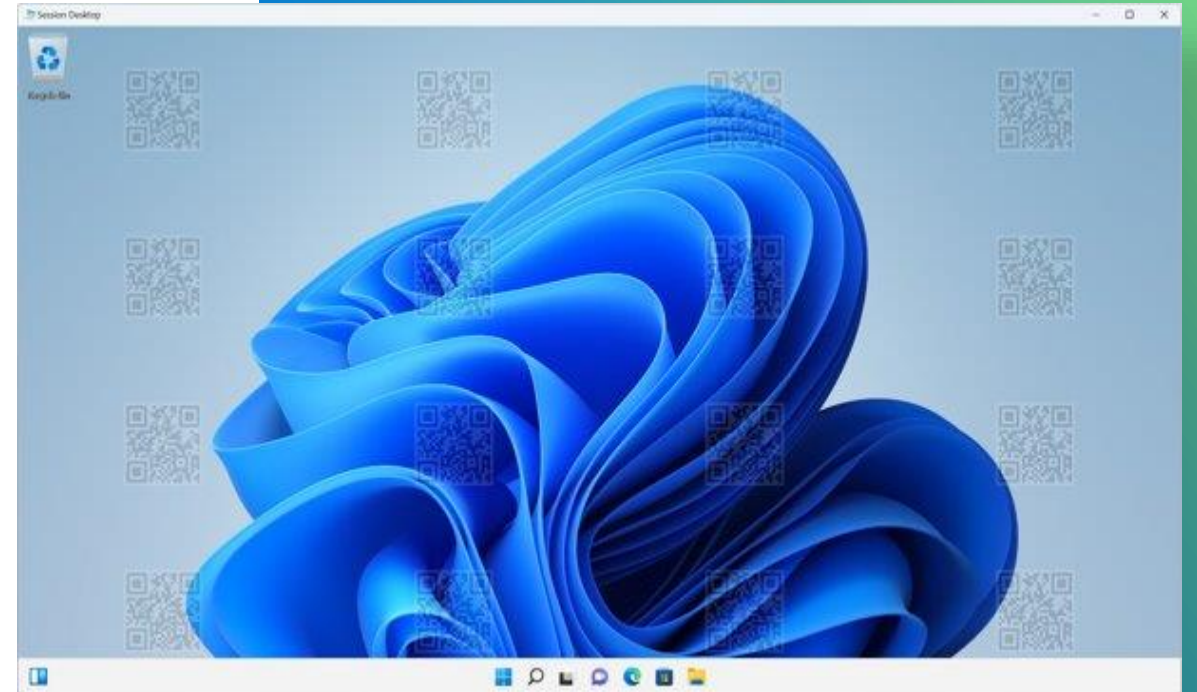
Watermarking

Watermarking support enables QR codes which are displayed on the session desktop.

It is a deterrent, preventing sensitive information from being captured and shared on Azure Virtual Desktop client endpoints.

Download administrative templates:

- Enable Group Policy (Watermark, Screen Cap Protection)
- Scan the QR code to show the Activity ID GUID
- Admin uses log analytics WVDConnection table to investigate the image origination



Securing, managing, & optimizing Azure Virtual Desktop

Management & monitoring

[Back to table of contents](#)

Managing & monitoring Azure Virtual Desktop



Developing a management regimen for Azure Virtual Desktop is critical for providing a secure, reliable virtual computing experience for users.



Azure Virtual Desktop makes it easy.



Admins can customize Azure services such as Microsoft Intune, Log Analytics, and Monitor to help admins do everything from provisioning and managing virtual machines to surfacing insights that can help better explain performance anomalies.



The following slides give an overview of:

- Microsoft Intune
- Multi-session configuration
- Azure Virtual Desktop Insights
- Azure Virtual Desktop Monitor

Azure Virtual Desktop & Microsoft Intune

Microsoft Intune provides a familiar and powerful interface for configuring secure and compliant session host VMs.

The screenshot displays the Microsoft Intune console interface. The main window is titled 'Create profile' and shows the 'Configuration settings' step of the wizard. The settings are organized into categories: System, Control Panel, Microsoft Edge, SmartScreen settings, and Microsoft Office 2016. Each category has a 'Remove category' link and a summary of settings not configured. The 'System' category shows 'Prevent access to registry editing tools' and 'Disable regedit from running silently?' both enabled. The 'Control Panel' category shows 'Prohibit access to Control Panel and PC settings' enabled. The 'Microsoft Edge' category shows 'Configure Microsoft Defender SmartScreen' enabled. The 'Microsoft Office 2016' category shows 'First Run' settings.

On the right, the 'Settings picker' pane is open, showing a search bar and a list of settings. The 'First Run' subcategory is selected, showing two results: 'Disable First Run Movie (User)' and 'Disable Office First Run on application boot (User)'. A 'Select all these settings' button is visible. Below the settings picker, the 'Create filter' pane is open, showing a rule builder with the following configuration:

And/Or	Property	Operator	Value
	operatingSyste...	Equals	ServerRdsh (Wind...

The 'Create filter' pane also shows the 'Rules' step of the wizard and a link to 'Learn more about creating filters'.

Microsoft Intune support for multi-session

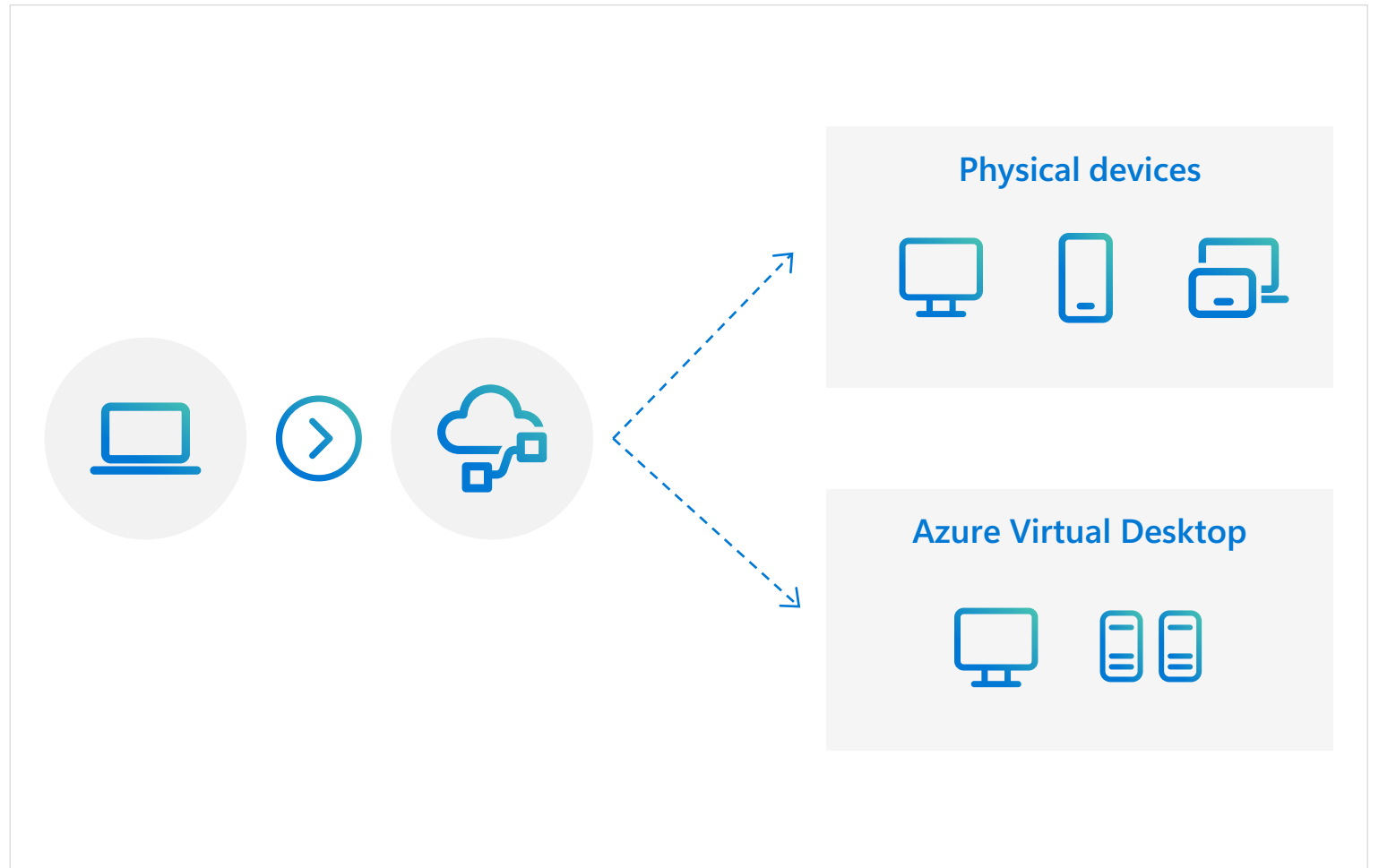
Manage both virtual and physical assets



Microsoft Intune gives admins a single tool to manage physical devices and virtual desktops integrated with Azure Virtual Desktop.

Windows 11 and 10 multi-session device configuration is generally available:

- Enroll Azure Virtual Machines in Microsoft Intune
- Manage using the settings catalog
- Use Microsoft 365 security features such as Conditional Access.



Microsoft Intune user configuration support for multi-session

Microsoft Endpoint Manager admin center

Home > Devices >

PKCS certificate

Windows 10 and later

Key storage provider (KSP) *

Certification authority *

Certification authority name *

Certificate template name *

Certificate type *

Subject name format *

Attribute	Value
<input type="text"/>	Not configured

Extended key usage

Export

Name	Object Identifier	Predefined values
Not configured	Not configured	Not configured

Previous Next

Microsoft Endpoint Manager admin center

Home > Endpoint security >

Endpoint security | Antivirus

Summary Unhealthy endpoints Active malware

Search (Ctrl+F)

Overview

Overview

All devices

Security baselines

Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

Monitor

- Assignment failures (preview)

Setup

- Microsoft Defender for Endpoint

Help and support

- Help and support

Last refreshed on: 4/11/2022, 5:41:22 PM

Unhealthy endpoints

- Pending update: 0
- Pending full scan: 0
- Pending restart: 0
- Pending manual steps: 0
- Pending offline scan: 0
- Critical failures: 0
- Inactive agent: 0
- Unknown status: 0

Active malware across categories (Top 8)

✓ No devices with active malware

AV policies

+ Create Policy Refresh Export

Search by column value

Policy name	Policy type	Assigned	Platform
zhluo-AntivirusTest	Microsoft Defender Antivirus	Yes	Windows 10 and later

Create a profile

Platform

Windows 10, Windows 11, and Windows Server

Profile

Microsoft Defender Antivirus

Microsoft Defender Antivirus

Windows Defender Antivirus is the next-generation protection component of Microsoft Defender for Endpoint. Next-generation protection brings together machine learning, big-data analysis, in-depth threat resistance research, and cloud infrastructure to protect devices in your enterprise organization.

Create

Patch management for Azure Virtual Desktop VMs



Use one host pool as a pilot group before updating all host pools.



Update VMs with existing Azure management solutions and all VMs in a host pool.



Updates can be staged in a maintenance window to keep systems available after sign in.



All VMs must be at the same update level after maintenance window is completed.



Use Microsoft Intune to manage your images.

Master image management for Azure Virtual Desktop VMs



The master image can be managed by already existing processes and technologies, including:

- Azure Update Management
- Microsoft Intune
- Third-party



A “best practices” document helps to configure a golden image for Azure Virtual Desktop.

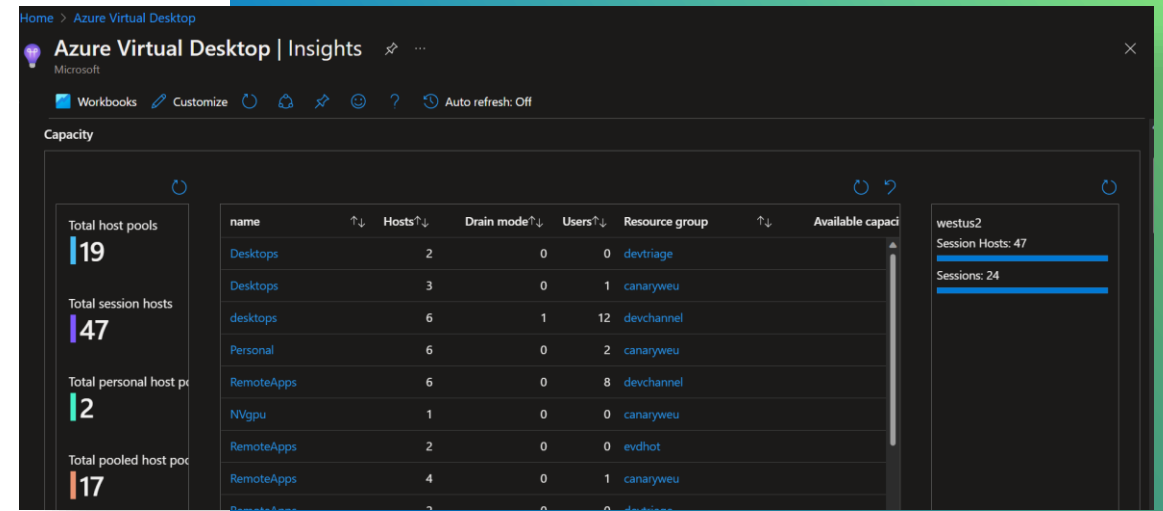


Application-masking technology helps to minimize the number of golden images and simplify app image management.

[Preparing a Master Image](#)

Azure Virtual Desktop Insights

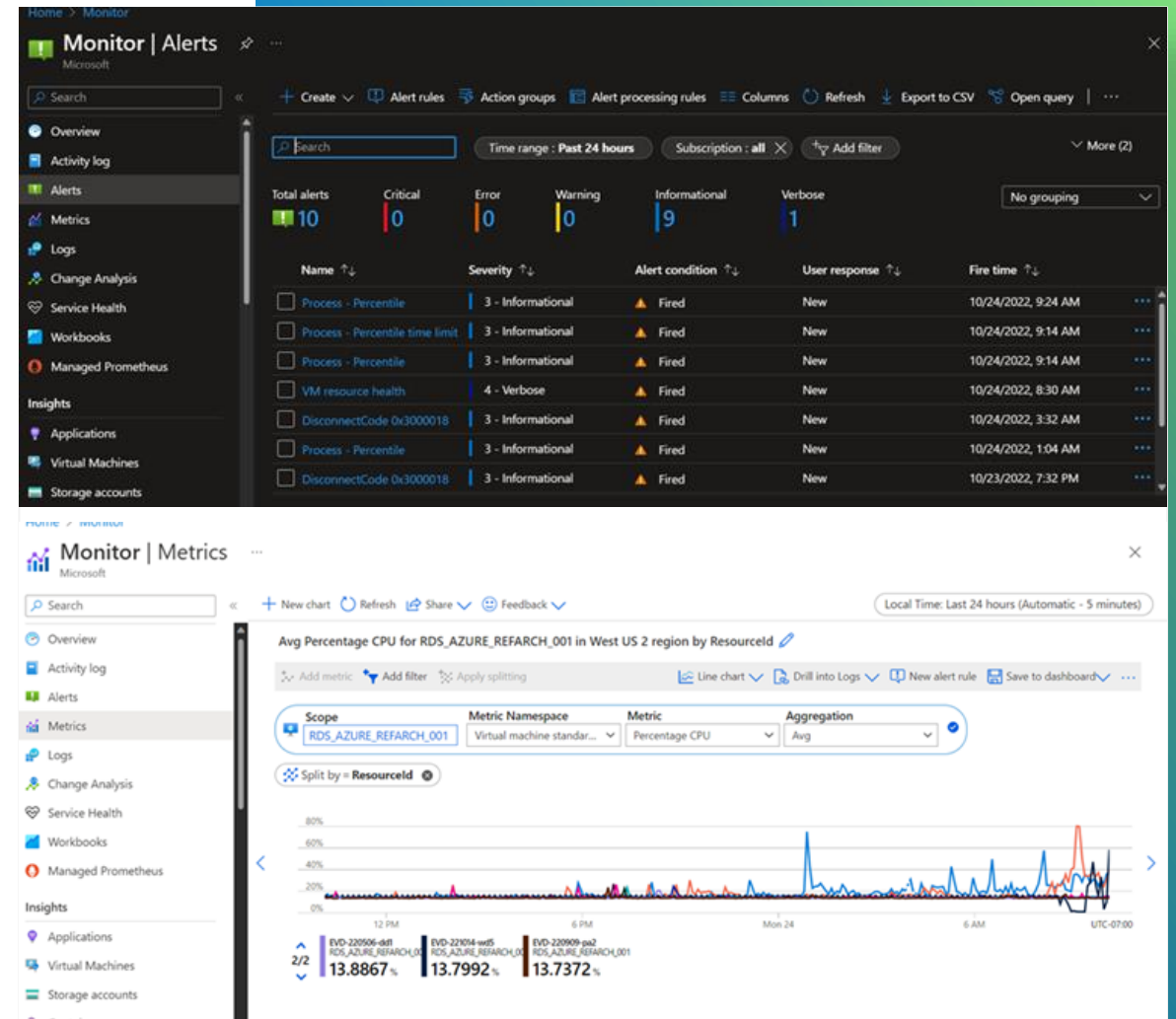
- Provides native monitoring for Azure Virtual Desktop deployments.
- Allows IT administrators and other users to understand the user experience and diagnostic output in their environment.
- Provides visibility into performance characteristics of Azure Virtual Desktop without requiring an investment in third-party monitoring software.
- Exposes diagnostic output from Log Analytics that would otherwise require manual querying or data extraction.



Azure Monitor and Log Analytics



Azure Monitor allows customers to configure native log and performance metric collection with the ability to set up alerts based on user-defined thresholds with customizable visualization options.



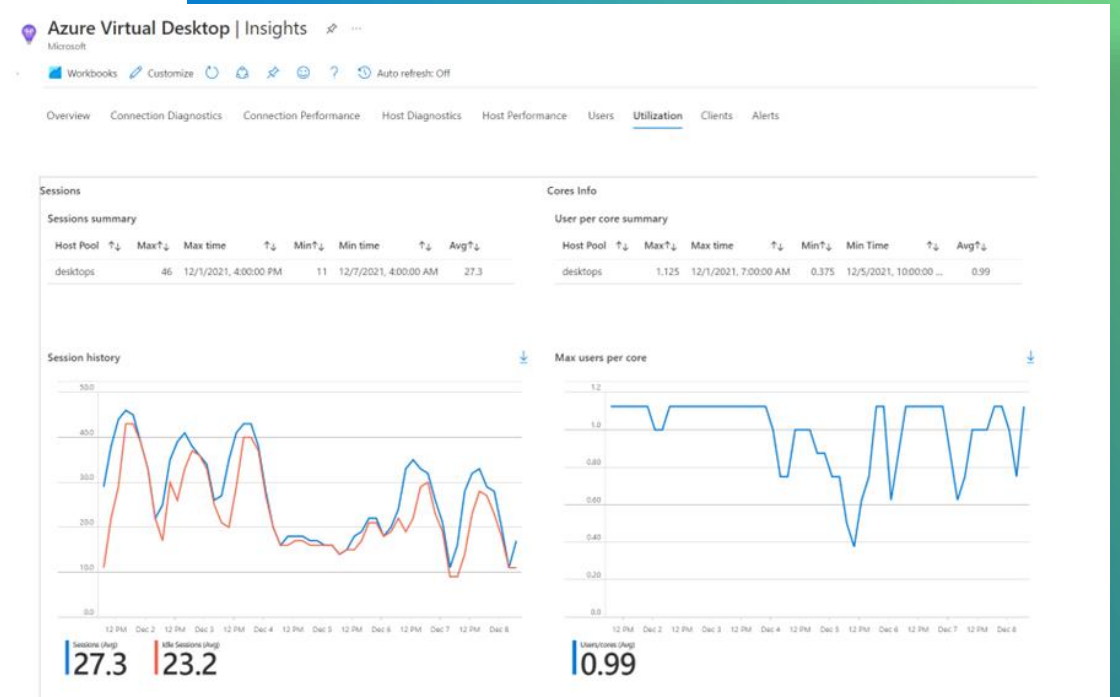
Use Azure Monitor for Azure Virtual Desktop

Azure Monitor for Azure Virtual Desktop (Insights) is a dashboard built on Azure Monitor Workbooks that helps you understand your Azure Virtual Desktop environment.

It can help save cost directly and indirectly.

Here are just some of the examples:

- Showing how (under)utilized your VMs are
- Allowing you to spot usage patterns so you can optimize scaling and load balancing
- Determining if there are session hosts that are unhealthy but are powered on (incurring cost)
- Informing you about a bad user experience (which is an indirect support cost)



Multi-select for Azure Virtual Desktop Insights

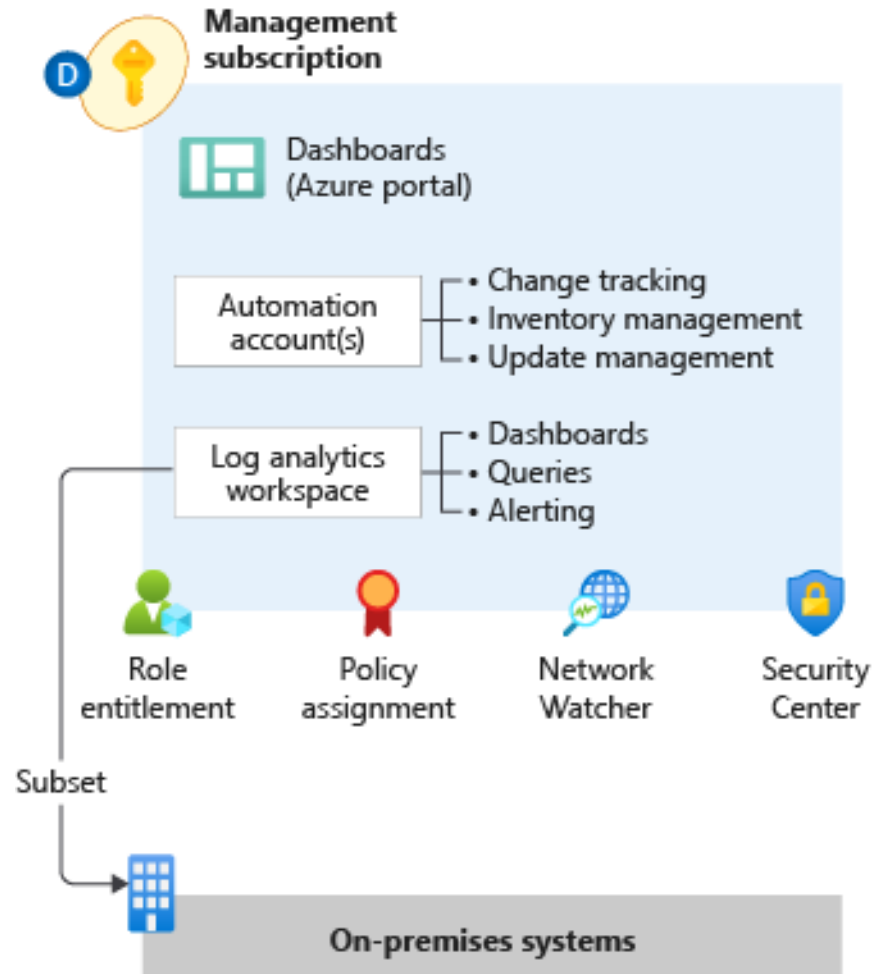
The screenshot displays the Azure Virtual Desktop Insights dashboard. The top navigation bar includes 'Home > Azure Virtual Desktop' and 'Azure Virtual Desktop | Insights'. Below this, there are filters for 'Subscriptions: RDS_AZURE_REFARCH_001', 'Resource Groups: devchannel, pltest (and 6 more)', 'Host Pools: 19 selected', and 'TimeRange: Last 48 hours'. The left sidebar contains navigation options like 'Overview', 'Getting started', 'Manage', 'Monitoring', and 'Licensing'. The main content area is divided into several sections:

- Capacity:** A summary card on the left shows 'Total host pools: 19', 'Total session hosts: 48', 'Total personal host pools: 2', and 'Total pooled host pools: 17'. To its right is a table with columns for 'name', 'Hosts', and 'Drain mode'. A multi-select dropdown menu is open over this table, listing various host pool names and their types (e.g., Desktops, RemoteApps, NVgpu, Win7dev).
- Connection diagnostics:** A line chart titled '% of users able to connect' shows a fluctuating line near 100% over a 48-hour period. To the right of the chart are three summary cards: 'Users with potential issues: 7', 'Hosts with potential issues: 3', and 'Clients with potential issues: 2'.
- Connection performance:** A line chart titled 'Time to connect (new sessions)' shows a fluctuating line over the same period. To the right are three summary cards: 'Min Time to connect: 13s', 'Median Time to connect: 32s', and 'Average Time to connect: 37s'.

Management & monitoring



Planning for platform & application management & monitoring



Design considerations

- Use Azure Monitor Log Analytics workspaces as the administrative boundary of logs.
- Collect telemetry from the platform services workspaces and HostPools.
- Performance counters should be collected.
- Azure event logs should be collected.
- Create a dashboard from the platform logs to centralize visuals for reporting operation.



Design recommendations

- Use a separate dedicated Azure Monitor Log Analytics workspace for Azure Virtual Desktop.
- Centralize your Azure Monitor Log Analytics workspace in the region of your Azure Virtual Desktop deployment.
- Export diagnostic settings to a storage account if there's a need to go beyond the two-year retention period.

Securing, managing, & optimizing Azure Virtual Desktop

Availability & resilience

[Back to table of contents](#)

Maximizing availability & resilience



Azure has more than 50 global regions and multiple features to ensure VDI availability across time zones, and resilience to eliminate single points of failure.



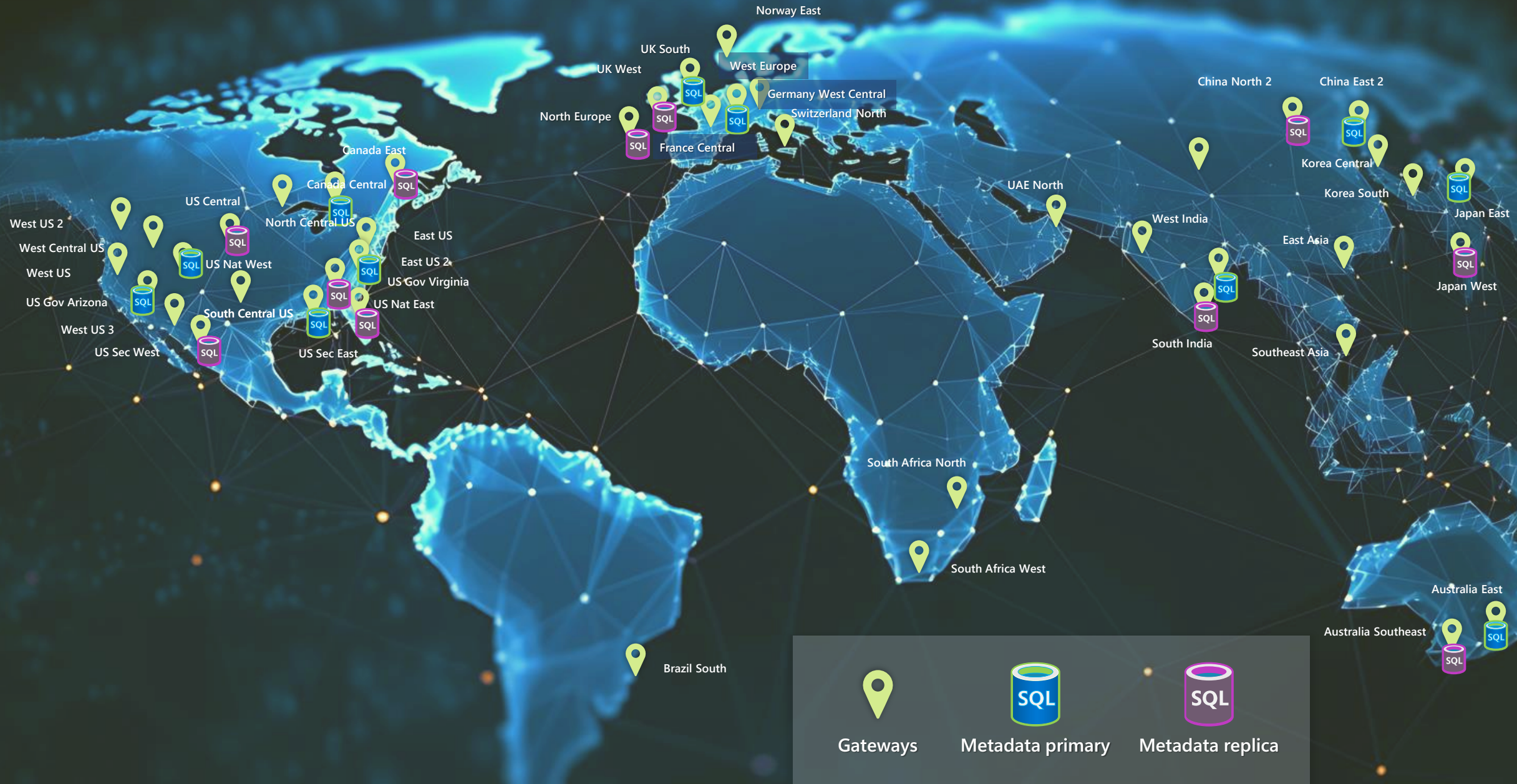
Azure Virtual Desktop takes advantage of these features and helps admins build a business continuity and disaster recovery (BCDR) regimen to provide powerful and cost-effective cloud-based protection of their computing assets.



The following slides give an overview of:

- Azure global footprint
- Business continuity & disaster recovery (BCDR) considerations and best practices
- Availability zones

Azure Virtual Desktop global footprint

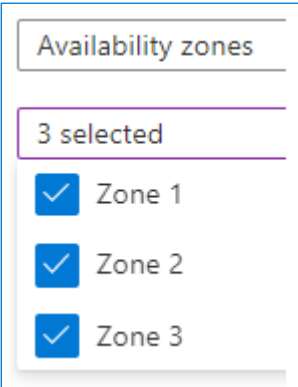


Availability zones (AZs) for Azure Virtual Desktop

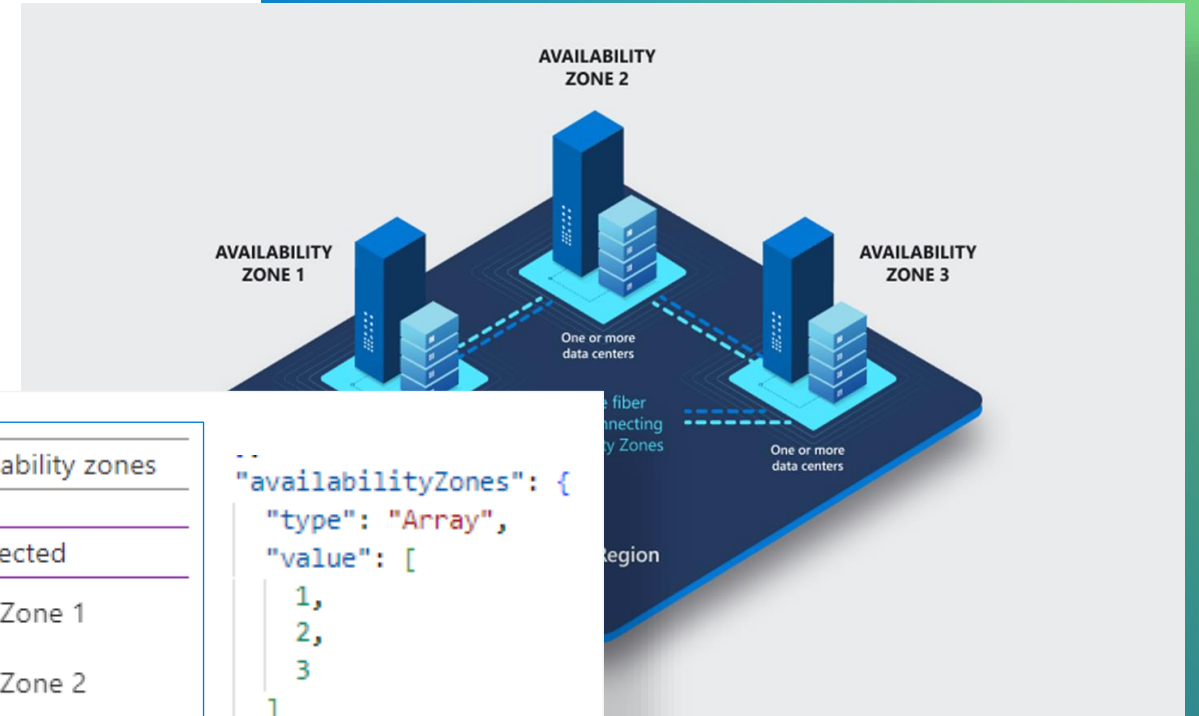
- Ability to equally distribute session hosts across all availability zones selected (in regions where AZ's are supported)
- Supports both new host pool creation and adding session hosts to host pools
- Increases resiliency of overall host pool and reduces the blast radius of an AZ outage

Deployment

- In portal select any number of AZ's
- In JSON define the AZ's required in the new array



```
--  
"availabilityZones": {  
  "type": "Array",  
  "value": [  
    1,  
    2,  
    3  
  ]  
},
```



Personal BCDR (business continuity and disaster recovery)



Use Azure Site Recovery



Keep profiles local



User-installed apps



Pooled BCDR – Administrator recommendations



Replicate images using Azure Compute galleries.



Backup and/or replicate FSLogix Profile disks.



Don't protect Microsoft 365 disks.



Have cold VMs ready in secondary location.



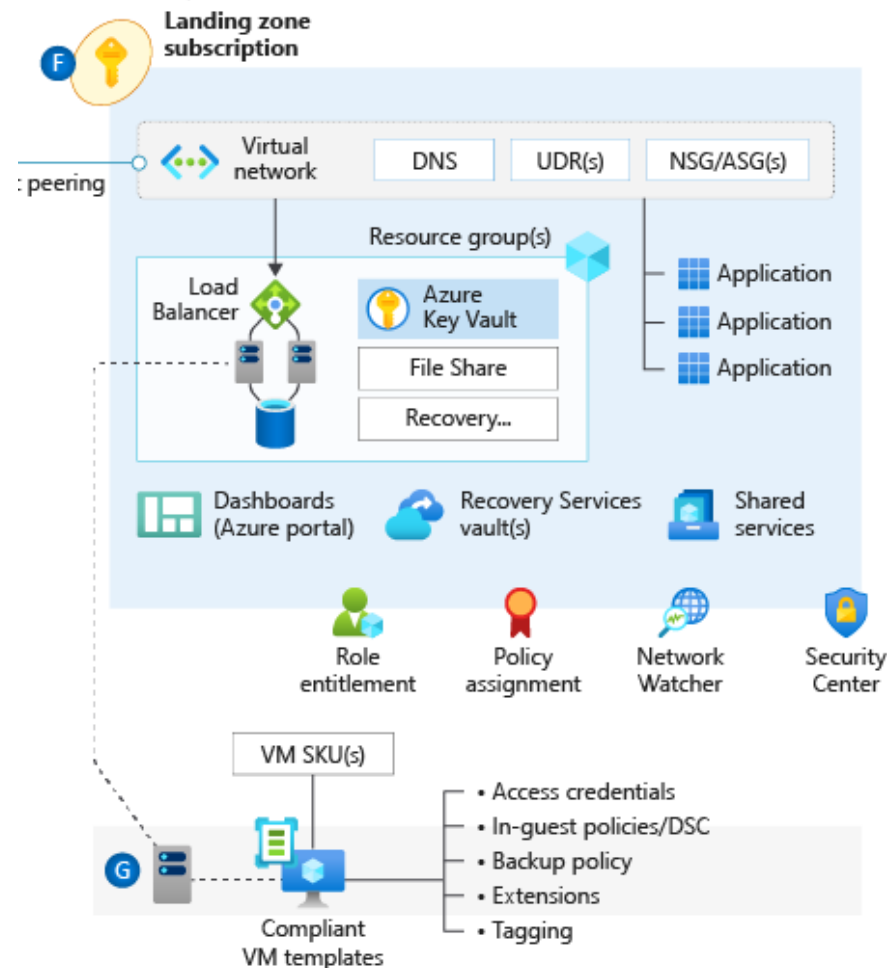
Automate all the things.



BCDR – Strategy & design



Planning for BCDR



Design considerations

- User Data Replication.
- Use of active-passive availability pattern in a multi-region deployment.



Design recommendations

- For Personal (dedicated) host pools, it's recommended to use ASR to replicate host pool VMs in a secondary DR region (Active-Passive with Cold Stand-By). Region should be aligned with DR of the storage backend used by FSLogix.

Securing, managing, & optimizing Azure Virtual Desktop

Cost & performance
optimization

[Back to table of contents](#)

Cost & performance optimization for Azure Virtual Desktop



Azure Virtual Desktop provides features, processes, tools, and reporting to help admins create a cost-effective and high-performance cloud VDI experience.



Features such as autoscale and solutions such as Azure Stack HCI are two examples of capabilities that give admins cost-saving (autoscale) and performance-enhancing (latency reduction with Azure Stack HCI) controls for Azure Virtual Desktop.



The following slides give an overview of:

- Azure pricing calculator
- Cost savings of multi-session
- Autoscale
- Azure Stack HCI

Cost estimation & tracking for Azure Virtual Desktop

Before your deployment you can estimate your costs using the Azure pricing calculator. It has a dedicated calculator for Azure Virtual Desktop that includes VM, disks, and FSLogix storage and networking.

After (during) your deployment you should use [tagging](#) (aka.MS/TagAVDResources), so you can accurately track the costs of your deployment of Azure Virtual Desktop.



Use the Azure pricing calculator to make personal estimations for your Azure Virtual Desktop deployment(s)



Use the tagging to accurately track the cost of (the different components) of your Azure Virtual Desktop deployment

Pricing calculator

Configure and estimate the costs for Azure products

Products

Example Scenarios

Saved Estimates

FAQs

Select a product to include it in your estimate.

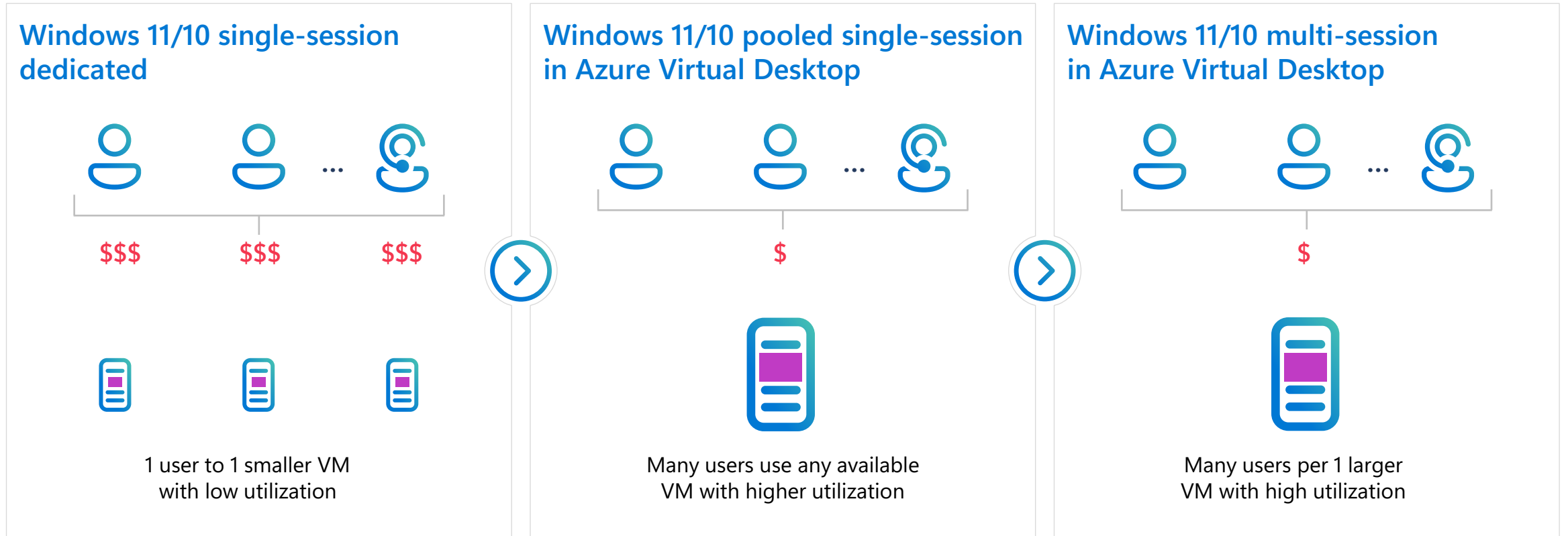
Azure Virtual Desktop



Azure Virtual Desktop

Enable a secure, remote desktop experience from anywhere

Reduce costs with exclusive Azure Virtual Desktop Windows 11 and Windows 10 multi-session



Cost models for on-prem vs. cloud VDI environments

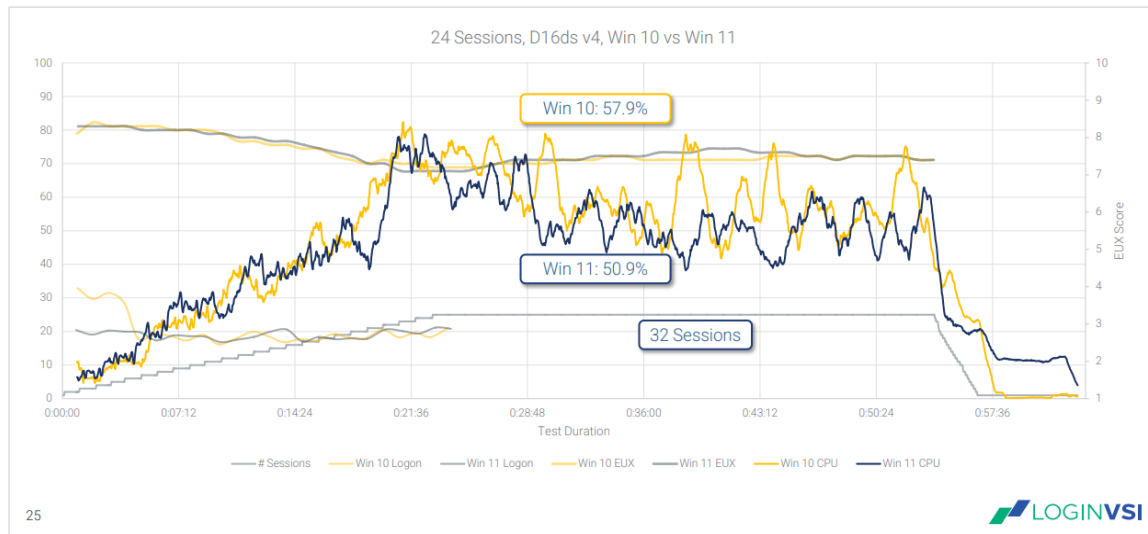
Scenarios	Sessions	On-prem hardware	Azure dedicated single-session	Azure pooled session	Azure multi-session (4 users per VM)	Azure multi-session (16 uses per VM)
		3.4GHz/8CPU	2.5GHz burst to 3.5Ghz/4 CPU	2.5GHz burst to 3.5Ghz/4CPU	2.5GHz burst to 3.5Ghz/16CPU	2.5GHz burst to 3.5Ghz/64CPU
		32GB RAM/T4-4G	110GB RAM/T4-16G GPU	110GB RAM/T4-16G GPU	110GB RAM/T4-16G GPU	440GB RAM/ 4X T4-16G 4 T4 GPUs
		C=250GB/D=50GB	C=250GB/D=360GB	C=250GB/D=360GB	C=250GB/D=360GB	C=250GB/D=360GB
1	1250	\$95,000	\$260,000	\$103,125	\$104,375	\$94,063
2	440	\$33,440	\$91,520	\$36,300	\$36,740	\$33,110
3	1180	\$89,680	\$245,440	\$97,350	\$98,530	\$88,795
4	570	\$43,320	\$118,560	\$47,025	\$47,595	\$42,893
5	300	\$22,800	\$62,400	\$24,750	\$25,050	\$22,575
6	90	\$6,840	\$18,720	\$7,425	\$7,515	\$6,773
Support		\$172,350	\$0	\$0	\$0	\$0
Monthly cost		\$463,430	\$796,640	\$315,975	\$319,805	\$288,208
Yearly cost		\$5,561,160	\$9,559,680	\$3,791,700	\$3,837,660	\$3,458,490

Many focus here
(on-prem hardware and Azure dedicated single-session)

When they should focus here
(Azure multi-session (4 users per VM))

Azure Virtual Desktop Windows 11 multi-session performance updates

24 User – Processor Utilization (Windows 10 vs Windows 11)



24 User (Windows 10 vs Windows 11)

	Windows 10	Windows 11
EUX Score	7.4	7.5
Average Logon	20.50	19.04
CPU % Util Steady State	57.93	50.89
Mem% Util Steady State	70.89	81.55
Disk Write IOPS Avg Steady State	210	213
User Input Delay Max Steady State	589	255
User Input Delay AvgMax Steady State	14.24	6.72

■ Better EUX score

Autoscale for Azure Virtual Desktop cost & performance optimization

Autoscale enables your Azure Virtual Desktop workloads to be performance- and cost-effective by starting and stopping session host virtual machines based on schedule and demand.



Optimizes compute costs by turning off session host virtual machines when not needed



Doesn't cost extra to use



Is easy to configure and doesn't require additional management overhead



Can be configured using the Azure Portal or REST API



Is completely supported by Microsoft

Azure Virtual Desktop autoscaling configuration

The Azure Virtual Desktop portal enables granular configuration & customization of a scaling plan.

Create a scaling plan

Basics Schedules Host pool assignments Tags Review + create

Scaling plan enables you to apply schedules and preset conditions under which the autoscaling should occur for a host pool. [Learn more](#)

Project details

Subscription *	115 - One Integration Service - NonProduction
Resource group *	Select a resource group Create new
Name *	
Location *	East US
Friendly name	
Description	
Time zone *	(UTC-05:00) Eastern Time (US & Canada)
Host pool type	Pooled
Exclusion tag	

Autoscale for pooled host pools

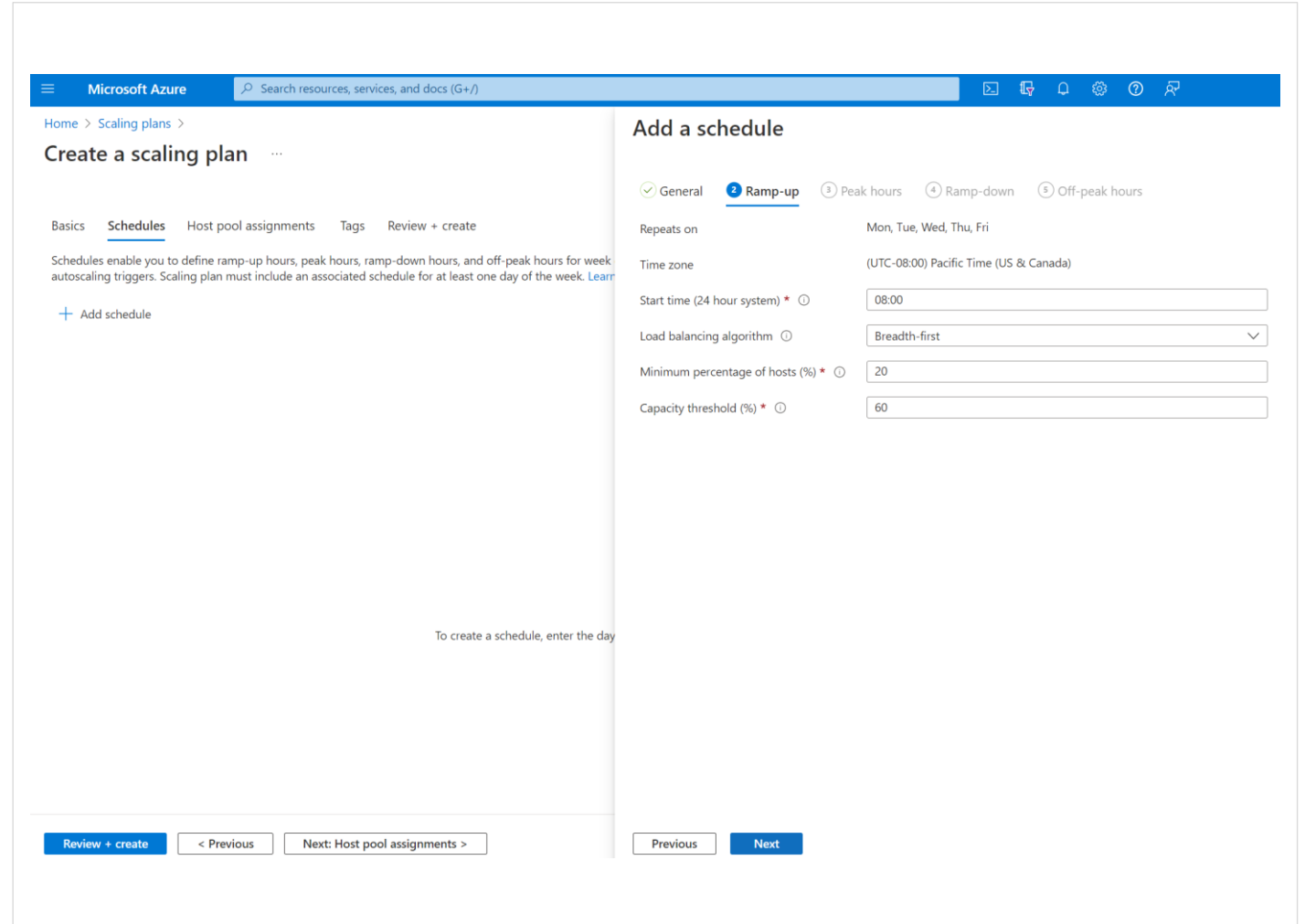


Autoscale automatically turns session host VMs on and off based on the capacity thresholds and schedules you define to match your workload

Using autoscale ensures that VMs are not running when they are not in use, which translates to optimized compute costs

To configure autoscale:

- Assign the Power On Off Contributor RBAC role to the Azure Virtual Desktop service principal.
- Create a scaling plan with schedules and assign it to your host pool(s).
- Enable autoscale on your host pool(s).



The screenshot displays the 'Add a schedule' configuration page in the Microsoft Azure portal. The page is part of a 'Create a scaling plan' workflow, with tabs for 'Basics', 'Schedules', 'Host pool assignments', 'Tags', and 'Review + create'. The 'Schedules' tab is active, showing a list of schedule types: 'General', 'Ramp-up' (selected), 'Peak hours', 'Ramp-down', and 'Off-peak hours'. The 'Ramp-up' configuration includes the following fields:

- Repeats on:** Mon, Tue, Wed, Thu, Fri
- Time zone:** (UTC-08:00) Pacific Time (US & Canada)
- Start time (24 hour system):** 08:00
- Load balancing algorithm:** Breadth-first
- Minimum percentage of hosts (%):** 20
- Capacity threshold (%):** 60

At the bottom of the page, there are navigation buttons: 'Review + create', '< Previous', 'Next: Host pool assignments >', 'Previous', and 'Next'.

Group costs by host pool with Microsoft Cost Management

Home > Cost Management: Visual Studio Enterprise Subscription

Cost Management: Visual Studio Enterprise Subscription | Cost analysis (preview)

Search (Ctrl+/)

Scope: Visual Studio Enterprise Subscription (change)

- Overview
- Access control
- Diagnose and solve problems
- Cost Management
 - Cost analysis (preview)
 - Cost analysis
 - Cost alerts
 - Budgets
 - Advisor recommendations

Resources

Customize Download

Filter rows < Aug 2022 >

Total (USD) Average Budget: None (create)

\$59.53 **\$2.39** / day --

Showing 9 resources [Check back tomorrow for cost anomaly insights](#) [See insights](#)

Name	Type	Resource group	Location	Subscription	Tags	Total ↓
▼ wvd-test2	Host pool	wvd-test2	US West	Visual Studio Enterprise Subscription	--	\$31.51
> wvd-test2	Host pool	wvd-test2	US West	Visual Studio Enterprise Subscription	--	\$15.50
> wvd-test2-1_osdisk_1_3...	Disk	wvd-test2	US West	Visual Studio Enterprise Subscription	costanalysis-parent: /subscriptions/1€	\$7.88
> wvd-test2-0_osdisk_1_7...	Disk	wvd-test2	US West	Visual Studio Enterprise Subscription	costanalysis-parent: /subscriptions/1€	\$7.87
> wvd-test2-1	Virtual machine	wvd-test2	Intercontinental, US West	Visual Studio Enterprise Subscription	costanalysis-parent: /subscriptions/1€	\$0.21
> wvd-test2-0	Virtual machine	wvd-test2	Intercontinental, US West	Visual Studio Enterprise Subscription	costanalysis-parent: /subscriptions/1€	\$0.06
> advm_osdisk	Disk	ad	US West	Visual Studio Enterprise Subscription	--	\$8.01
> wvd-test1-0_osdisk_1_8a6d6b...	Disk	wvd-test1	US West	Visual Studio Enterprise Subscription	wvd-test1: wvd-test1	\$7.83
> wvd-test1-1_osdisk_1_43cc4af...	Disk	wvd-test1	US West	Visual Studio Enterprise Subscription	wvd-test1: wvd-test1	\$7.82
> adpublicip	Public IP address	ad	US West	Visual Studio Enterprise Subscription	--	\$2.18

Personal Desktop Autoscale

Automatically starts session host VMs based on a schedule or "Start VM on Connect." It then deallocates session host VMs based when users sign off or disconnect.

Saves costs by shutting down idle session hosts. Session hosts can be started when needed.

To enable Personal Desktop Autoscale:

- Create a personal scaling plan.
- Define whether to enable "Start VM on Connect" and what action to perform after a user session has been disconnected/signed off for a configurable period of time.
- Assign personal scaling plan to one or more personal host pools

Add a schedule

General Ramp-up Peak hours **Ramp-down** Off-peak hours

Repeats on: Mon, Tue, Wed, Thu, Fri

Time zone: (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

Start time (24 hour system) * ⓘ: 18:00 ✓

Start VM on Connect ⓘ: Yes No

Disconnect settings

When disconnected for (min) * ⓘ: 30 ✓

Perform ⓘ: Hibernate ✓

Log off settings

When logged off for (min) * ⓘ: 10 ✓

Perform ⓘ: Shutdown None Shutdown Hibernate

Azure Virtual Desktop for Azure Stack HCI

[Back to table of contents](#)

Introduction to Azure Virtual Desktop for Azure Stack HCI



- Designed for customers who need **secure on-premises virtualized apps and desktops**
- Combines the **benefits of Azure Virtual Desktop and Azure Stack HCI**
- Customers can **deploy in their datacenters to extend their on-premises infrastructure** to Azure
- All while enjoying many of the **key benefits of Azure Virtual Desktop on Azure**, such as **Azure portal, Windows 11 and Windows 10 multi-session**

Azure Stack HCI provides a cloud native hybrid solution based on a modern subscription and an efficient hyper-converged infrastructure

Modern infrastructure to deploy cloud native solutions anywhere



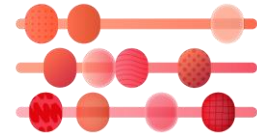
Cloud native
anywhere



Secured to run all
workloads from cloud
to edge



Familiar management
and operations



Flexible
options at the right price
and performance point

Azure Virtual Desktop for Azure Stack HCI extends the benefits of cloud VDI to on-premises



Secure anywhere

- Run virtualized desktops and apps securely with Entra ID, conditional access, and MFA
- Simplify VDI deployment
- No need to manage brokers, gateways, or underlying servers and storage



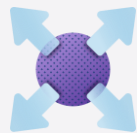
Windows 10 and 11 multi-session

- Windows 10 & 11 multi-session or single-session support
- Achieve high utilization & lower operation costs



Prime performance

- Enjoy optimized Microsoft 365/Teams/Windows App experiences
- Run graphic-intensive workloads with GPU support
- Built for sensitive low-latency workloads



Full control

- Satisfy data locality requirements
- On-premises storage and data residency



Scale cloud and on-premises

- Manage and scale deployments across both Azure and Azure Stack HCI through a single management experience
- Use the familiar Azure portal and admin experience



Optimize for cost

- Use existing eligible Windows licenses
- No need to manage overhead licenses for Remote Desktop Services (RDS)
- Save with Windows 10 & 11 multi-session support

Azure Virtual Desktop for Azure Stack HCI use cases



Security and compliance

Secure, high performance cloud platform for financial institutions that meets compliance requirements



Data sovereignty

Cloud functionality that can meet the data sovereignty and data gravity requirements for public sector entities



Low latency workloads

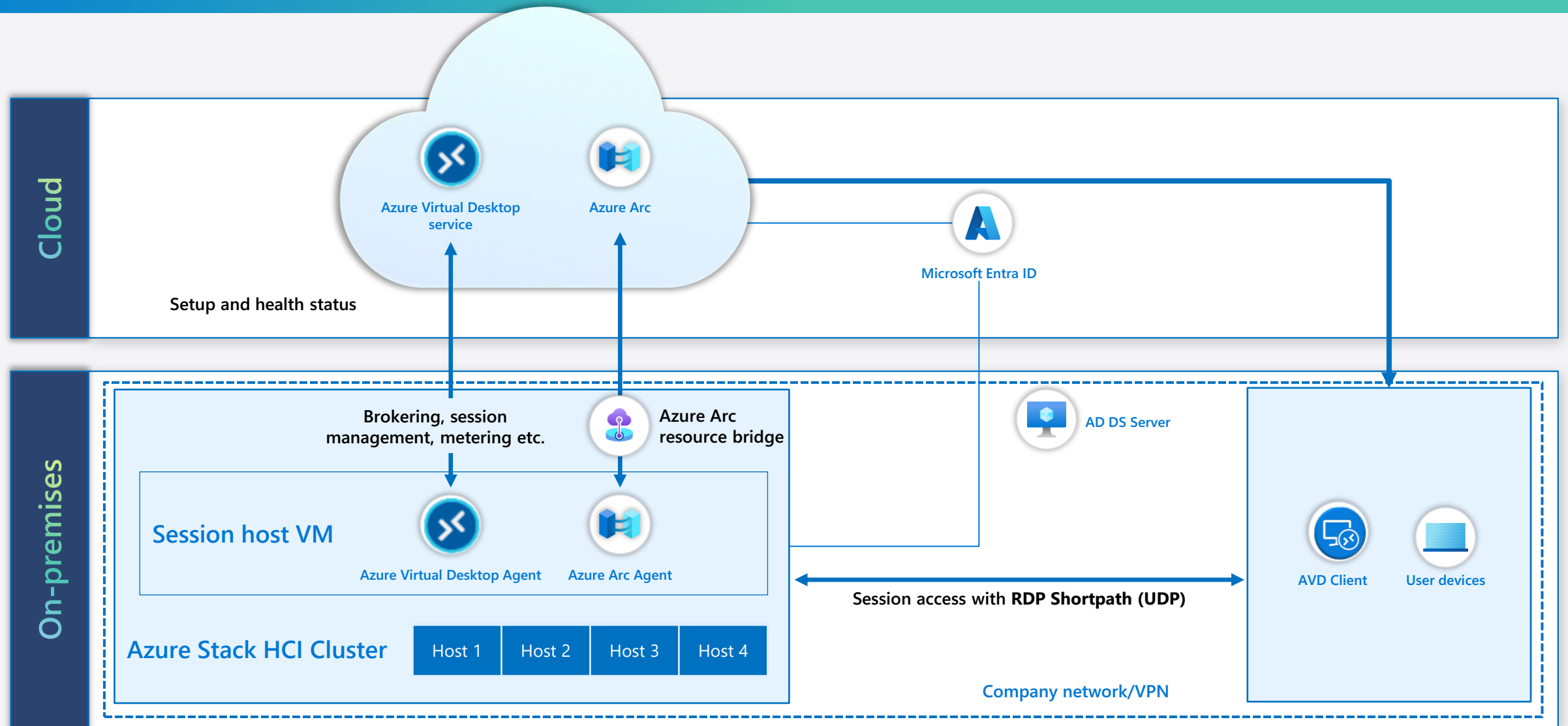
High performance and low latency cloud capabilities that can meet the compute requirements for the most demanding workloads



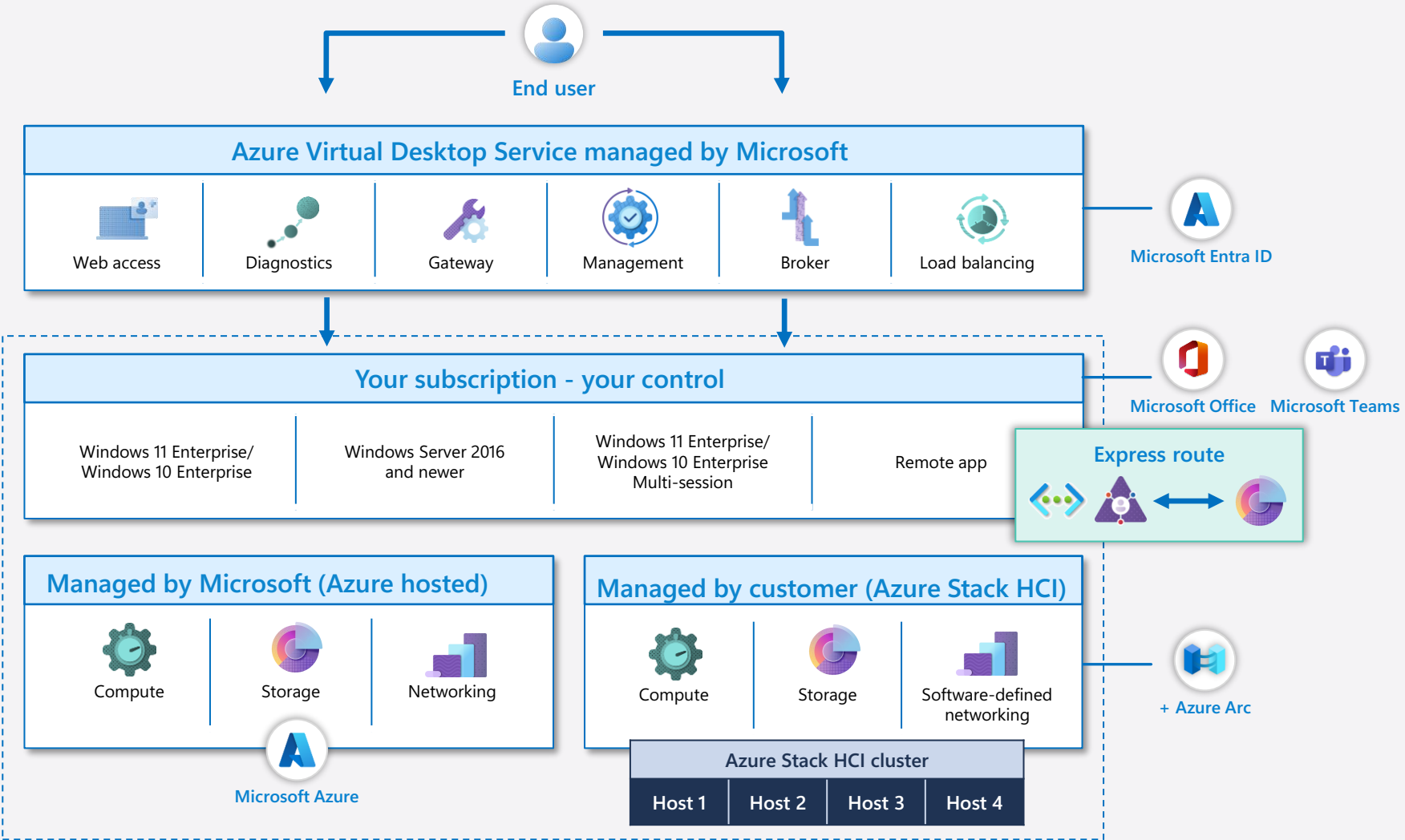
Virtual Desktop Infrastructure (VDI) modernization

Migrate existing VDI workloads to Azure using Azure Stack HCI

Azure Virtual Desktop for Azure Stack HCI high-level solution architecture



Azure Virtual Desktop architecture and Azure Stack HCI



Provide your employees with a secure, remote desktop experience.

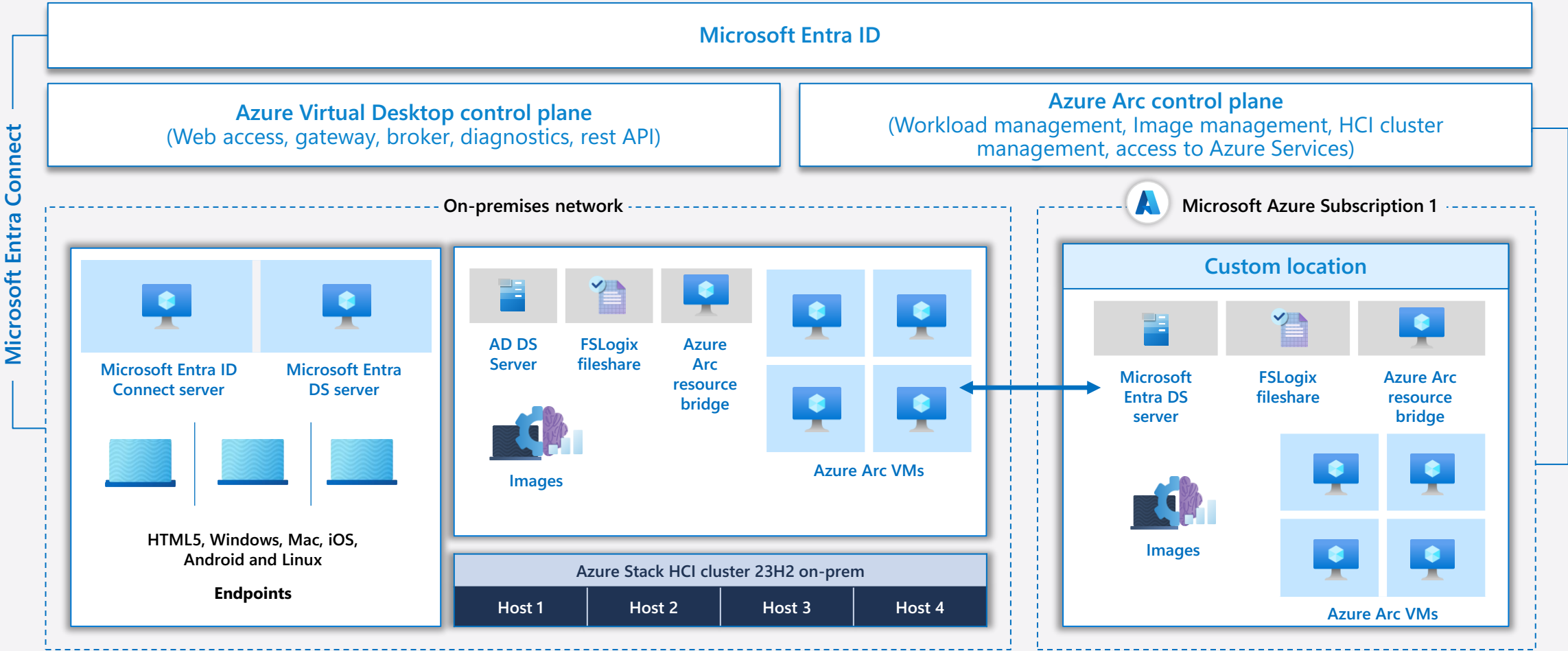


Connect from virtually any device of your choice.



Focus on the right policies and controls rather than managing infrastructure.

Sample customer architecture diagram



Admin experience

Fully integrated cloud-native deployment experience in Azure Portal, powered by Azure Stack HCI Fall 2023 release

Provisioning Azure Virtual Desktop session hosts on Azure Stack HCI clusters. Enablement requirement:

- Azure Stack HCI clusters have been added to the Azure Virtual Desktop portal.
- Azure Stack HCI clusters (Fall 2023) must be deployed first.

The screenshot shows the 'Create a host pool' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > Azure Virtual Desktop | Host pools >'. The page title is 'Create a host pool'. There are tabs for 'Basics', 'Virtual Machines' (which is selected), 'Workspace', 'Advanced', 'Tags', and 'Review + create'. A descriptive paragraph explains that a host pool is a collection of identical virtual machines within an Azure Virtual Desktop environment. Below this, there are several configuration options:

- 'Add Azure virtual machines' with radio buttons for 'No' and 'Yes' (selected).
- 'Resource group' dropdown menu set to 'Defaulted to same as host pool'.
- 'Name prefix *' text input field containing 'a name for your session hosts'. Below it is an information icon and the text 'Session host name must be unique within the Resource Group.'
- 'Virtual machine type' section with radio buttons for 'Azure region' and 'Azure Stack HCI' (selected). This section is highlighted with a green border.
- 'Custom location *' dropdown menu set to 'Location of ASZ cluster'.
- 'Images' dropdown menu set to 'Select an image' with a link to 'See all images'.
- 'Number of VMs *' empty text input field.
- 'Virtual processor count *' empty text input field.
- 'Memory type' with radio buttons for 'Static' (selected) and 'Dynamic'.
- 'Memory (GB) *' empty text input field.

Partners & migration

[Back to table of contents](#)

Microsoft provides access to a broad array of resources to help customers successfully migrate to Azure Virtual Desktop

Preparing for migration success



Migration considerations

- Migration drivers
- Planning guidance
- Cloud Adoption Framework
- Azure Migrate
- Azure landing zones and landing zone accelerators
- Best practices



Citrix solution overview

- Key benefits
- Architecture
- Playbook



VMware solution overview

- Key benefits
- Architecture
- Playbook



ISV partners

- ISV partner value add

Partners & migration

Migration considerations

[Back to table of contents](#)

Migration considerations for Azure Virtual Desktop



Migrating an on-premises VDI environment to the cloud can be a daunting proposition for customers. App compatibility, cost estimation, and security are just a few of the areas that customers must consider and solve before a migration can begin.



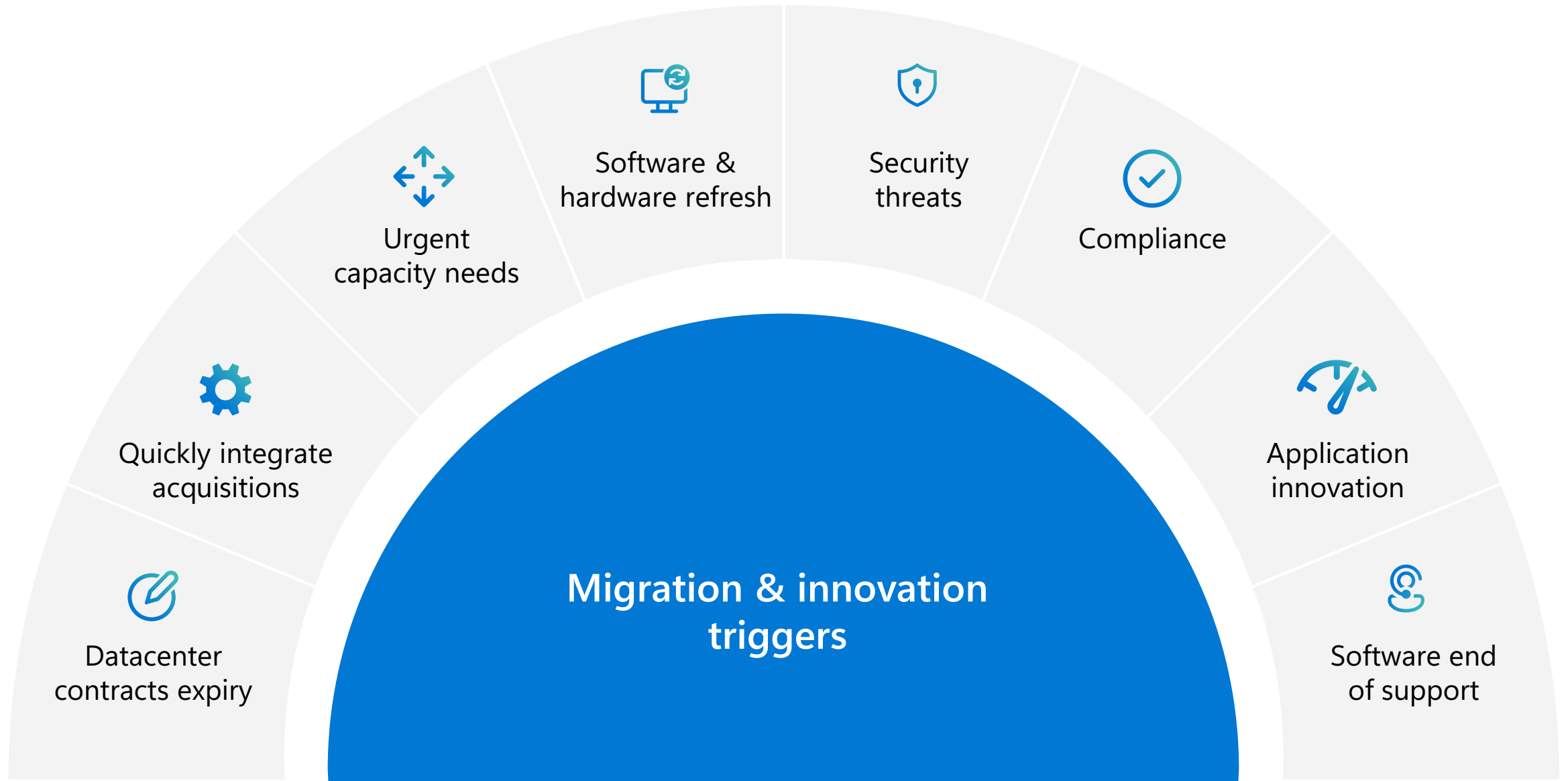
Azure Virtual Desktop uses tools like the Microsoft Cloud Adoption Framework and landing zone accelerators to take the guess work out of the migration process and provide a repeatable framework for success that has been used by many customers.



The following slides give an overview of:

- Migration planning and execution
- Azure landing zones and landing zone accelerator

What's driving migrations to Azure?



Migration planning and execution

A step-by-step approach

Migration plan

TCO | Target workloads | Approach (e.g., rehost) | Timelines



Assess



Migrate



Optimize

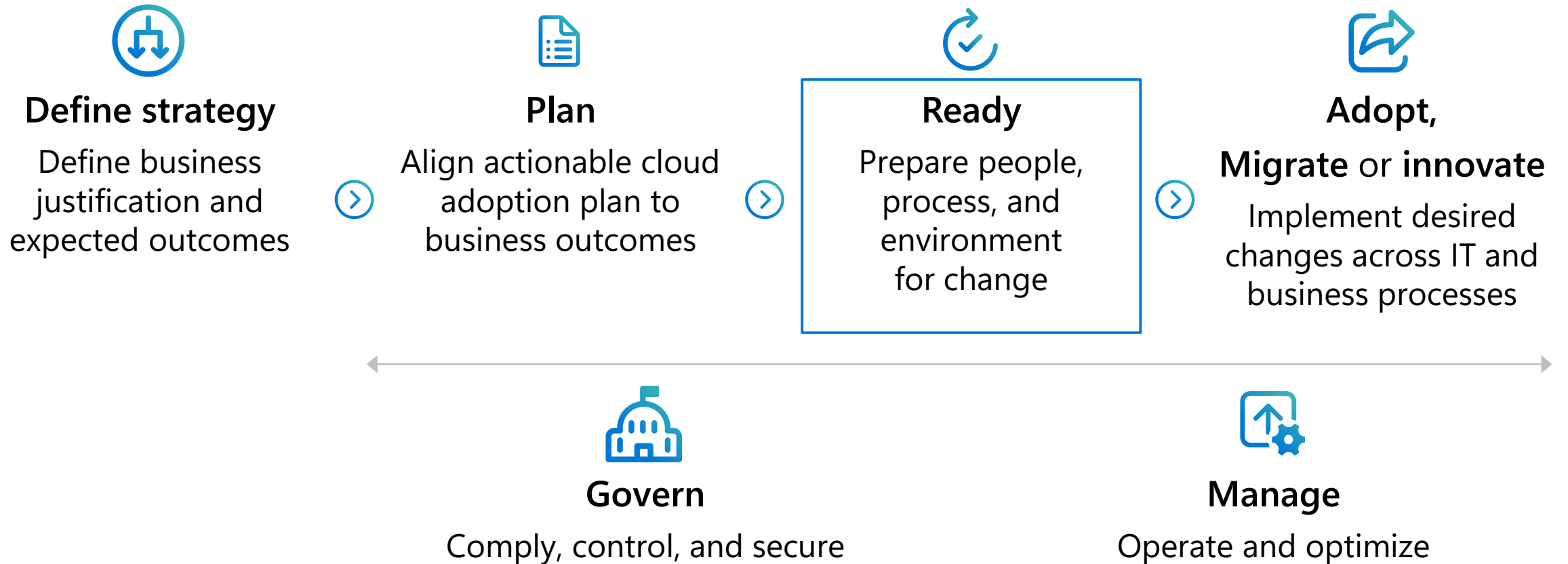


Secure & manage

Azure Migrate | Azure Cost Management | Azure Security & Management

Microsoft Cloud Adoption Framework for Azure

Proven business and technical guidance to help customers create and implement the business and technology strategies necessary to succeed in the cloud.



Azure landing zones



Azure landing zones help customers set up their Azure environment for scale, security, governance, networking, and identity.



Azure landing zones

- Enable migrations and net new apps
- Consider all platform resources
- Don't differentiate between IaaS or PaaS

Azure Virtual Desktop landing zone accelerator



Azure Virtual Desktop landing zone accelerator is an **architectural approach and reference implementation that enables effective workload and scenario operationalization** of landing zones on Azure, at scale and **aligned** with **Azure Roadmap** and **Microsoft Cloud Adoption Framework for Azure**



Authoritative

Provides holistic design decision framework for Azure Platform



Proven

Based on success of large-scale migration projects at-scale



Prescriptive

Apply it on clearly plan and design your Azure environment

Azure Virtual Desktop landing zone accelerator architecture

Landing zone accelerator design guidelines: Guidelines (decisions and recommendations) for the six components of the enterprise-scale architecture.

Azure Virtual Desktop landing zone reference implementation

A reference implementation of shared services containing network, security, identity, governance services required to construct and operationalize an enterprise-scale landing zone.

Azure Virtual Desktop landing zone accelerator design areas



Identity access management



Management & monitoring



Security, governance, & compliance



Network topology & connectivity



Business continuity & disaster recovery



Platform automation & DevOps



Azure Migrate Hub for all migration tools

Discover, assess, and migrate applications, infrastructure, and data with Azure Migrate.



Assessments for readiness, sizing, and cost estimation



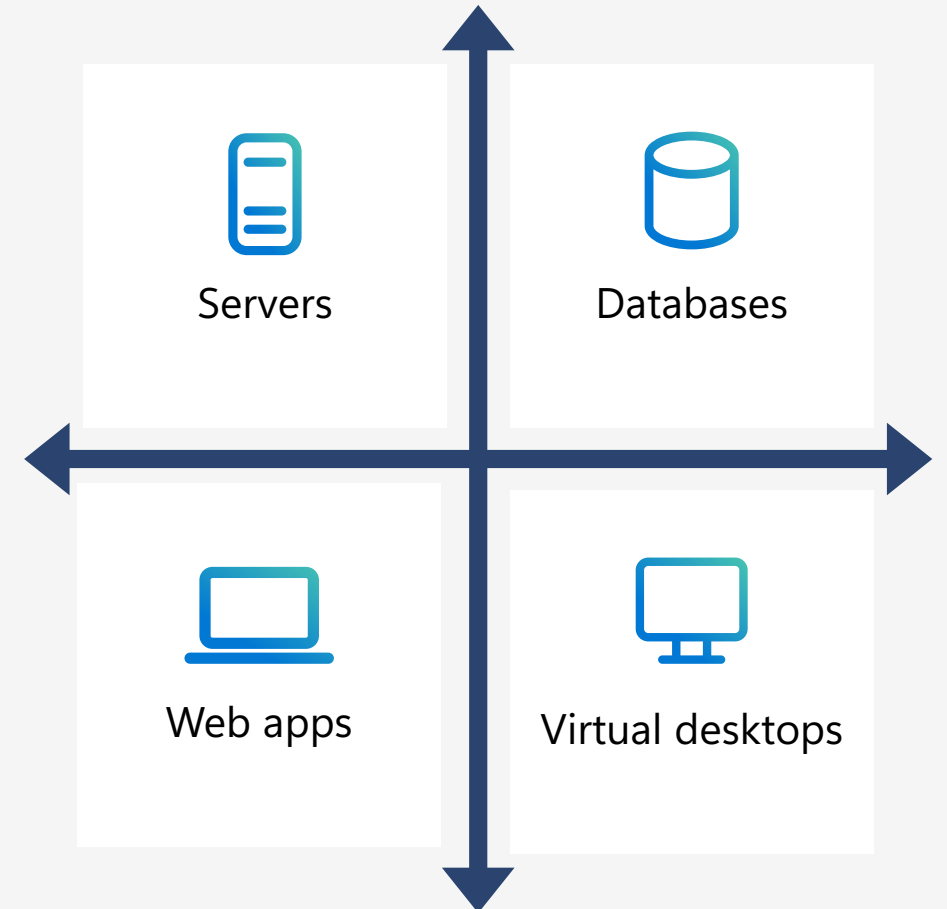
Migration with near-zero downtime




Integrated experience and end-to-end progress tracking



Choice of tools with ISV integration



Azure Migrate Hub

Microsoft Azure (Preview)  Search resources, services, and docs (G+)

Home > Azure Migrate

Azure Migrate


Microsoft

Search (Ctrl+/) <<

Get started

Migrate your on-premises datacenter to Azure


Discover, assess and migrate your on-premises applications using Microsoft or third-party tools, or [find an expert](#) to help with your migration. [Learn more](#)



Windows and Linux servers

Discover, assess and migrate your on-premises VMware and Hyper-V virtual machines or Physical servers to Azure.


[Assess and migrate servers](#)



SQL and other databases

Discover, assess and migrate your on-premises databases to Azure SQL Database Managed Instance or Azure SQL Database.

[Assess and migrate databases](#)



Web apps, data and Virtual Desktop Infrastructure

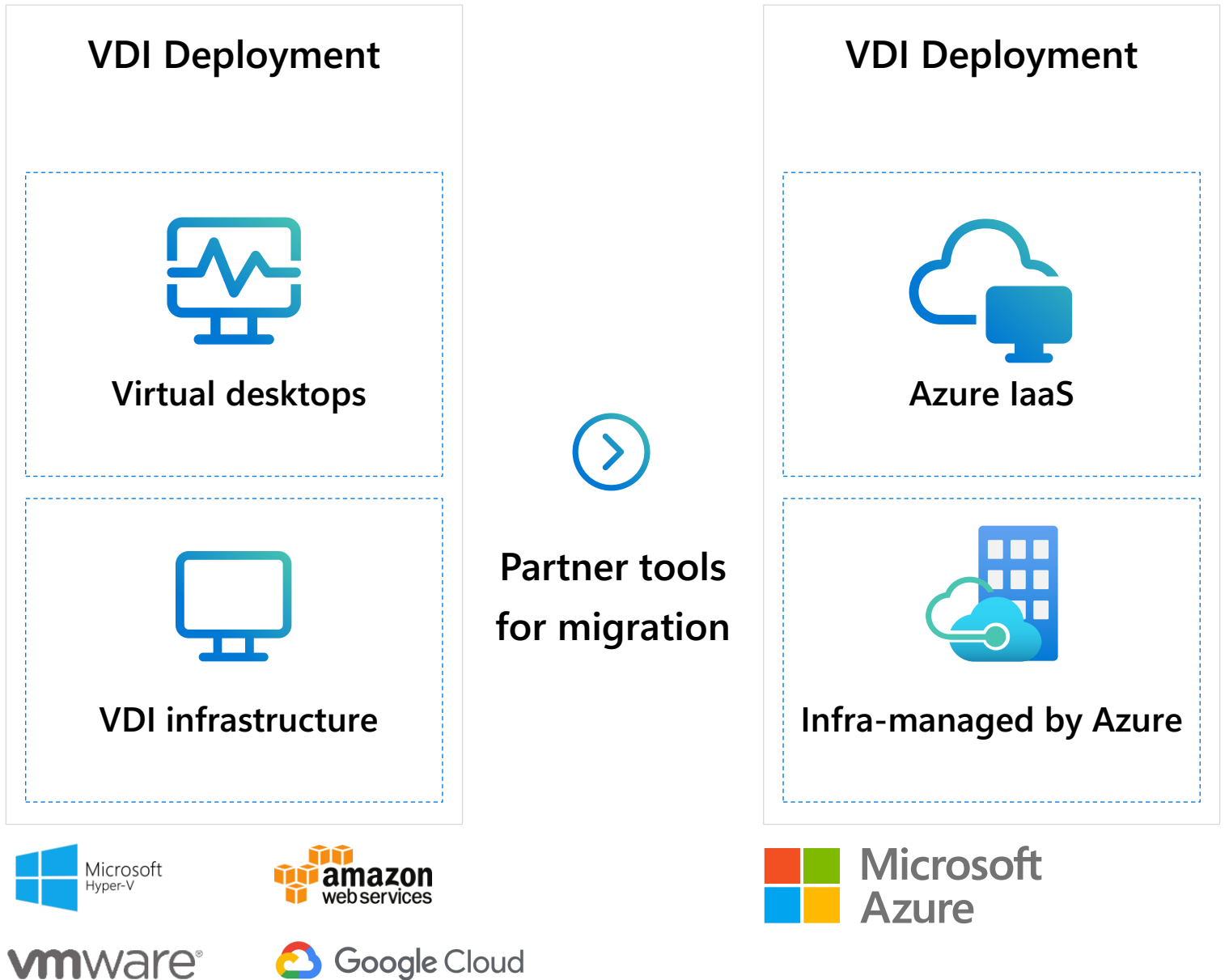
Assess and migrate web apps, migrate data and assess virtual desktop infrastructure (VDI).

[Assess and migrate web apps \(new\)](#)
[Assess virtual desktop infrastructure \(new\)](#)
[Migrate data](#)

Useful links

VDI migration

Azure Virtual Desktop



Azure Virtual Desktop migration

Pooled resources

Steps to migration

- 1 User identity**
 - Sync user identities and password hash from on-premises Active Directory (AD) to Microsoft Entra ID
 - Setup AD instance on Azure using ASR or continue using on-premises AD
- 2 Virtual machines**
 - Bring your own image from on-premises and create new VMs on Azure
 - Lift and shift VMs from on-premises
 - Register them with Azure Virtual Desktop infrastructure
- 3 User and app data**
 - UPDs not supported on Azure Virtual Desktop
 - Convert UPD into Profile Container—conversion tool available in GitHub soon
 - Sync to Azure using Azure file sync or file server replication
- 4 Client (end-user) capabilities**
 - Download Azure Virtual Desktop client for Windows or use the web client
 - Continue using existing RD clients available through app stores

Azure Virtual Desktop migration Personal desktop

Steps to migration

- 1 Virtual machines**
 - Lift and shift VMs from on-premises
 - Register them with Azure Virtual Desktop infrastructure
- 2 Client (end user) capabilities**
 - Download Azure Virtual Desktop client for Windows or use the web client Continue using existing RD clients available through App stores
- 3 End-user assignment**


Use Azure Virtual Desktop direct assignment capability to assign personal desktops to specific users


Partners & migration

Understanding Citrix & VMware
offers & capabilities

[Back to table of contents](#)

Understanding Citrix & VMware offers & capabilities

 Citrix and VMware provide on-premises VDI solutions that are used by customers around the world. These vendors provide virtualization capabilities that deliver unique value to VDI customers.

 Citrix and VMware play an important role in helping customers migrate to Azure Virtual Desktop while also providing the option to continue operating their VDI environment on-prem or with other vendors.



The following slides give an overview of migration planning and execution.

Citrix + Azure Virtual Desktop

Delivering enterprise value and unified management around Azure Virtual Desktop.



Workspace experience

Include Azure Virtual Desktop workloads within Citrix Workspace for central access to all apps, desktops, and files.



Image management

Simplify management by layering OS, apps, and user data on Azure Virtual Desktop resources and rapidly provisioning updates.



Hybrid cloud journey

Accelerate the move to Azure for on-prem customers by enabling management of on-prem and Azure Virtual Desktop workloads from one console.

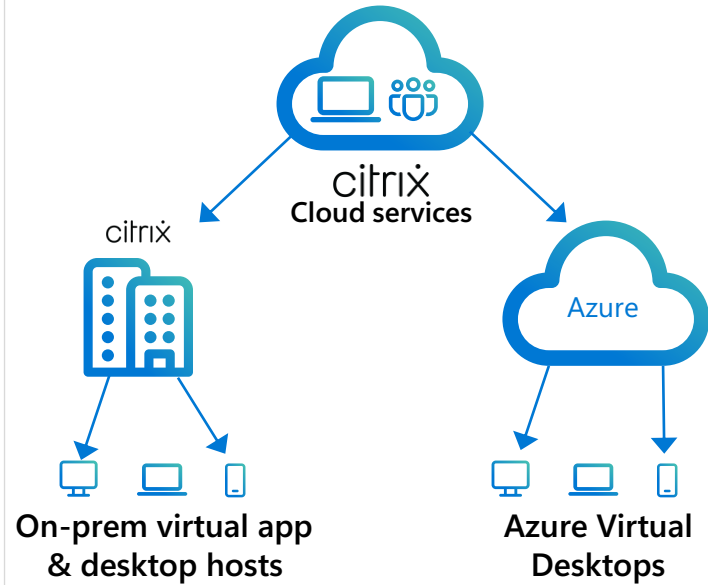


Environment management

Optimize host performance, accelerate application delivery, and enhance scalability for Azure Virtual Desktop.

Achieve business outcomes with Citrix & Microsoft

Enable hybrid multi-cloud



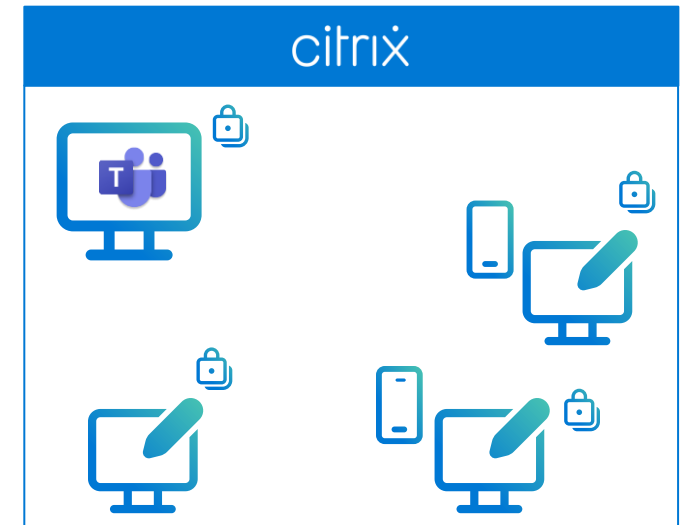
Mitigate risk

Optimize operations



Reduce cost

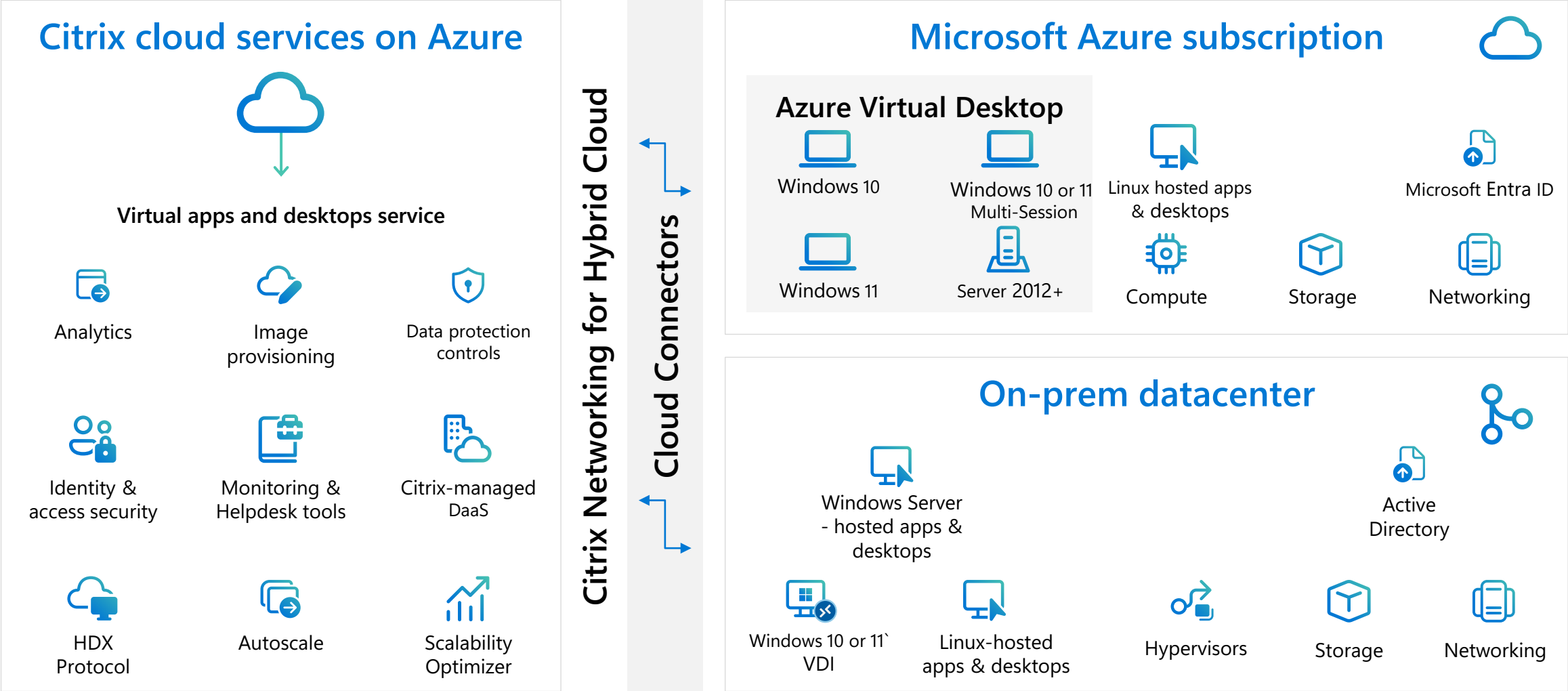
Deliver secure experiences



Improve UX

Reference: [Citrix TechZone – Enhancing Azure Virtual Desktop](https://aka.ms/CitrixTechZoneEnhancingAVD) (aka.ms/CitrixTechZoneEnhancingAVD)

Citrix and Azure Virtual Desktop architecture



Optimize performance

Plan



Workspace environment management

- Included in CVAD service (and Workspace Premium Plus)
- Actively monitors Azure Virtual Desktop resource utilization and dynamically adjusts based on user profiles, system policies, and resource consumption
- Intelligently adjust the way applications utilize systems resources such as RAM, CPU, and IOPS
- Simplifies the administration of Windows policies – which improves both user experience and application security

** Internal Citrix estimates*

Improve the number of users per server by

10-30%*

Server utilization up to

80%

Up to 65% with RDS/
Azure Virtual Desktop alone

Follow the playbook: Citrix



Suggest Azure Virtual Desktop when it's time to replace an existing virtualization solution or build a new one.

#1

Azure Virtual Desktop on Azure + on-premises deployments

- Pitch joint offerings with the Citrix Virtual Apps and Desktops service and Citrix Workspaces.
- Customers can manage hybrid scenarios with Citrix on-premises workloads under one management console.

#2

Migrate on-premises services to Azure Virtual Desktop

- Pitch Azure Virtual Desktop and/or Citrix joint offerings with Citrix Virtual Apps and Desktops service and Citrix Workspaces.
- Azure Virtual Desktop benefits – such as multi-session Windows 11 or 10 and Office 365 ProPlus optimization – are key drivers for moving to Azure Virtual Desktop on Azure

#3

Citrix Cloud: RDS/VDI on Azure only (not ready to onboard Azure Virtual Desktop)

- Pitch Citrix Virtual Apps and Desktops service running RDS/VDI on Azure

If moving to Azure isn't an option right now, customers can upgrade to the newest versions of Remote Desktop Services on-premises and Citrix for improved functionality and easier cloud migration later.

VMware Horizon Cloud on Microsoft Azure

Extending Azure Virtual Desktop capabilities to Horizon Cloud



Broad endpoint support with enhanced remote experience



Global brokering with cloud-optimized architecture



Real-time audio video and peripheral support



Enhanced user environment management



Flexible desktop options and configurations



Hybrid environment support

Azure Virtual Desktop

Follow the playbook: VMware Horizon Cloud



Suggest VMware when the customer has multiple independent on-premises servers

#1

Accelerate cloud adoption

- Customers can try Microsoft Azure on a use-case-by-use-case basis.
- Recommend hybrid environments with existing Horizon on-premises and Azure Virtual Desktop in Azure.
- Highlight the common management tools and skillsets for all environments.
- Customers get a single pane of glass for all workloads.

#2

Maximize cost savings

- Pitch the Azure Virtual Desktop entitlement, features, and simple pricing.
- Customers can optimize costs at scale with advanced power management that matches utilization and saves money.
- Support a broader Windows 10 or 11 migration to Azure Virtual Desktop with multiple deployment options.

#3

Exceptional user experience

- Pitch Workspace ONE Access and Intelligent Hub for highly secure access to apps and desktops.
- These offerings provide enterprise-class performance on a broad range of clients with dynamic remoting protocols.
- Users get a consistent experience across all devices.

Promote integrated Azure Virtual Desktop and VMware Horizon, including FSLogix and Dynamic Environment Manager, to accelerate customer time-to-value.

Partners & migration

ISV partners

[Back to table of contents](#)

Azure Virtual Desktop & ISV partners



The ISV community for Azure Virtual Desktop is large and diverse. ISVs exist to ensure that the apps running in a customers' on-prem environment will work in the cloud.



Other ISVs provide automated migration to Azure Virtual Desktop for customers that fit a certain profile. Other ISVs provide industry-specific enhancements for Azure Virtual Desktop.

↩ ↗ The following slide gives an overview of the Azure Virtual Desktop ISV partner
↙ ↘ environment.

Azure Virtual Desktop ISV partner environment

Rich ISV partner ecosystem allows you to further enhance your Azure Virtual Desktop experience

Category	Description
Customer environment assessment	Assess resource utilization of apps/users/OS, baseline user experiences, and recommend sizing for Azure Virtual Desktop <i>Example – Lakeside</i>
Diagnostics & end user experience monitoring	Assess, monitor, and manage end user experiences with GUI enabling reactive troubleshooting as well as predictive troubleshooting leveraging AI/ML <i>Example – Sepago</i>
Application layering	Enable dynamic provisioning of apps during boot/sign on time based on user profile <i>Example – Liquidware</i>
Management	Deployment and configuration <i>Example – Nerdio, NetApp (CloudJumper)</i>
Printing	Remove the need for print server infrastructure <i>Example – PrinterLogic</i>
App compatibility assessment/remediation	Assess app compatibility for layering new packaging <i>Example – PolicyPak</i>

Positioning Azure Virtual Desktop & Windows 365

[Back to table of contents](#)

Azure Virtual Desktop lets you create a purpose-built cloud VDI environment to meet your use case

Helping customers make the best choice for their use case



Azure Virtual Desktop & Windows 365

- VM recommendations
- Sizing guidelines
- Storage for your VMs
- GPU VMs



User experience

- Host pools and session hosts
- Personal or pooled host pools
- User profile management (FSLogix)
- Remote App Streaming

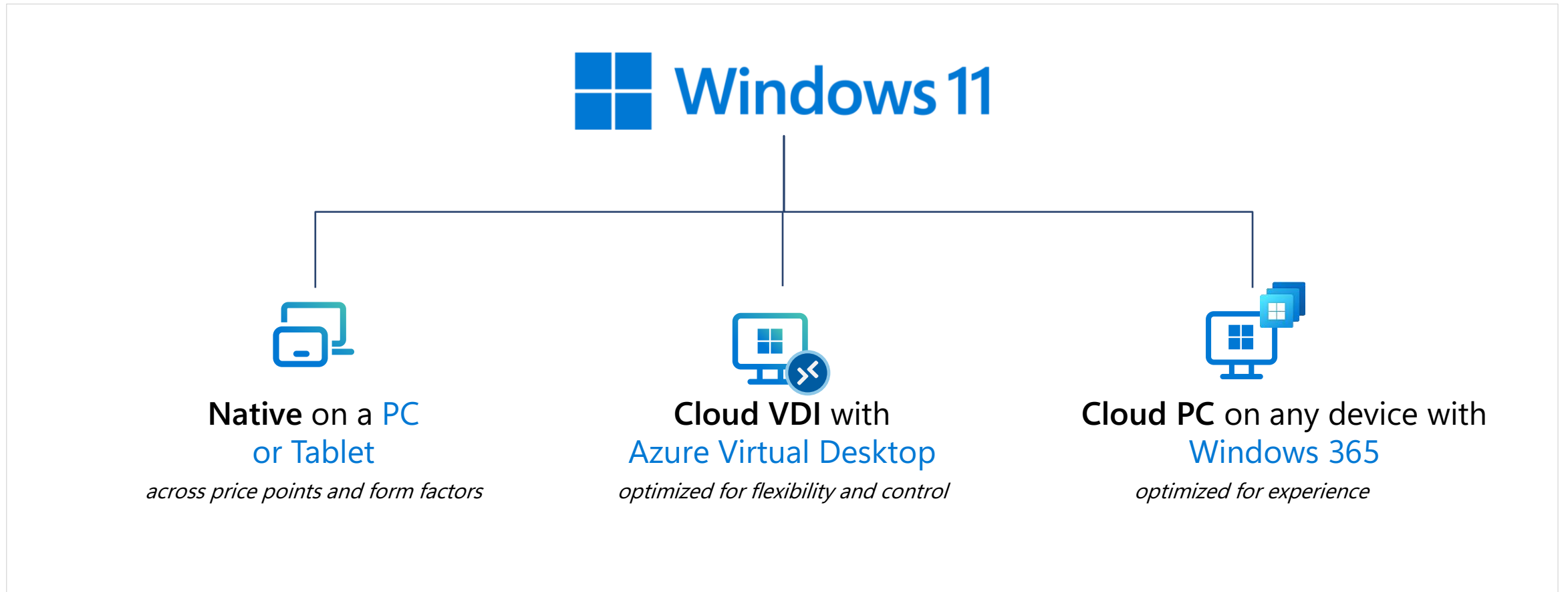


Networking & connectivity

- Networking considerations
- On-prem to Azure connectivity
- Inter-Azure traffic management
- RDP Shortpath

Different ways to deliver Windows

Options for maximum flexibility



Finding the right Microsoft solution for your needs



Windows 365



Secure work on personal PCs



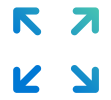
Onboard and offboard employees



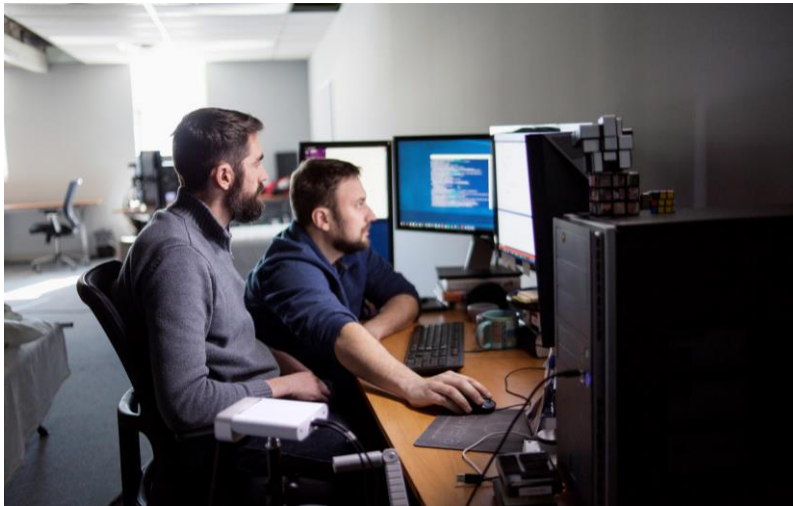
Simple to buy, deploy, and manage



No employee or IT special skills or training



Quickly scale and resize



Azure Virtual Desktop



Shift on-prem VDI to the cloud



Leverage existing VDI infra and expertise



Enable remote app streaming and non-persistent desktops

Microsoft cloud solution options



Windows 365

A complete SaaS service that securely streams your personalized Windows desktop, apps, settings, and content from the Microsoft cloud, to any device.



Azure Virtual Desktop

A cloud VDI platform that delivers hosted desktops and apps with maximum flexibility and control.

	Windows 365 Cloud PC	Azure Virtual Desktop Cloud VDI
OS Support	Windows 11 or Windows 10	Windows 11, Windows 10, single- or multi-session, Windows Server
Admin	<ul style="list-style-type: none">• Microsoft Intune• Web self-service (Business)	<ul style="list-style-type: none">• Azure Portal• VMware or Citrix management panel
Service	SaaS: complete end-to-end Microsoft service	PaaS: Granular controls over configuration and management
Pricing	Per-user, per-month	Consumption-based
Scale	Unlimited based on subscription	Unlimited based on consumption
End-user	Full Windows like-local experience	Single or multi-user, pooled, remote app





Thank you