



Windows 365 vs. Azure Virtual Desktop (AVD) – Comparing Two DaaS Products

Find more:
getnerdio.com

The recently released Microsoft Windows 365 service and Azure Virtual Desktop (AVD) are both Desktop-as-a-Service solutions from Microsoft but there are several important differences between them. In this article, we'll take a deep dive into the similarities and differences between the services. We'll compare AVD and Windows 365 across several dimensions in detail and then summarize it all together in a side-by-side chart. Let's take a look at the two services across 5 primary areas:

1. [Technical Architecture](#)
2. [IT Admin Experience](#)
3. [End-user Experience](#)
4. [Licensing and Infrastructure Costs](#)
5. [Cloud PC License Cost vs. AVD Azure Consumption](#)

1 – Technical architecture

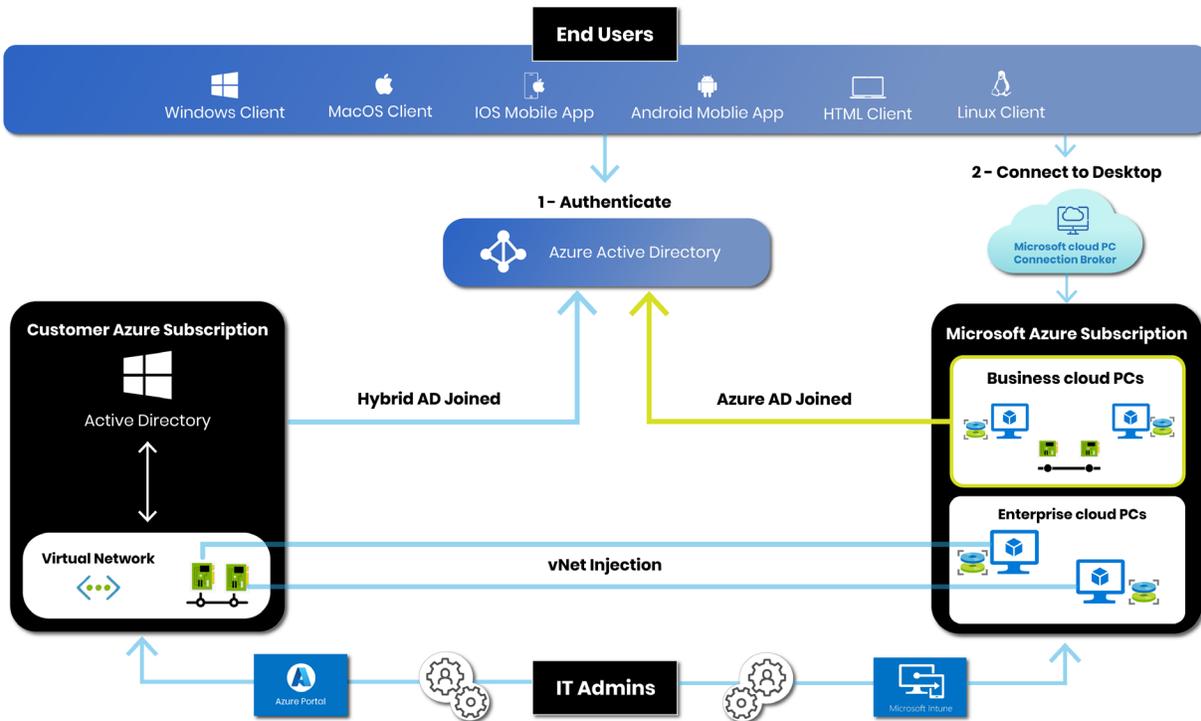
Under-the-hood, both AVD and Windows 365 leverage a similar set of Microsoft cloud technologies. Technically, Windows 365 is built on top of existing AVD components but has a different transactional model (fixed price vs. consumption-based).

There are two versions of cloud PCs: **Enterprise** and **Business**.

Enterprise cloud PCs are designed for organizations who have invested into Microsoft Endpoint Manager and are using this powerful platform to manage their existing, physical Windows 10 desktops. Enterprise cloud PCs require an Intune license for each user who is assigned a cloud PC M365 SKU.

Business cloud PCs are designed for individual users and very small businesses who typically go to their local Best Buy when they need a new PC. Now, instead of visiting Best Buy, they can go to Microsoft and subscribe to a new cloud PC and have it ready to use in an hour. Business cloud PCs do not require an Intune license and are managed entirely by the user, similar to a standalone physical PC.

The diagram below depicts the deployment architecture of both Enterprise and Business cloud PCs.



Enterprise Cloud PC Architecture

Enterprise cloud PCs are Azure and Active Directory dependent. An Azure subscription with a properly configured network is required with access to Active Directory that has [Azure AD Hybrid](#) Join enabled. Azure AD DS is not currently supported and cloud-only, Azure AD join is not currently supported either.

The VM itself runs in a Microsoft-managed Azure subscription, which means admins don't have access to it directly and are not incurring the cost of this VM in their own Azure subscription. However, the VM's network interface card (NIC) is "injected" into a vNet in a

customer's Azure subscription. All network traffic enters and leaves the VM via the customer-managed vNet. Egress transfer costs are incurred by the customer.

Since admins don't have direct access to the VM running in Microsoft's Azure subscription, all management tasks (e.g. software installation, patching, policies) are performed through the Microsoft Endpoint Manager portal.

Enterprise cloud PC pre-requisites:

- Azure subscription with vNet
- Azure vNet can access Active Directory domain controller (i.e. a PC can be joined to the domain). Custom DNS servers, necessary routing, and firewall access to AD.
- Azure AD Connect configured and running within Active Directory with AAD Hybrid Join enabled
- Intune enabled on Azure AD tenant (each cloud PC user needs an Intune license assigned)
- Admin setting up the initial deployment must be an Owner of this Azure subscription
- Azure AD DS is NOT supported

Enterprise cloud PC high-level setup steps (without Nerdio Manager):

- In Microsoft Endpoint Manager create an **“on-premises network connection”** pointing at the vNet and provide AD credentials to join new VMs. The network connection and AD credentials will be validated automatically. This process may take a while to complete.
- Upload an existing custom Windows 10 Enterprise image or use a clean Microsoft-provided gallery image
- Create a cloud PC **“provisioning policy”** that combines an **“on-premises network connection”** with a desktop image. Assign this provisioning policy to an Azure AD security group.
- Add users to the Azure AD security group that the provisioning policy is assigned to

Enterprise cloud PC user entitlement

- Once the above pre-requisites and setup steps are completed, entitling a user to a cloud PC is very easy. Simply assign a cloud PC license to the user via the Windows 365 Admin portal.

- If the user is a member of a security group that's assigned to a cloud PC provisioning policy and the network connection is "healthy," a new cloud PC will start provisioning. It will take up to an hour for the cloud PC to be ready for the user to log into.

Business Cloud PC Architecture

Business cloud PCs are VMs that run entirely in Microsoft's Azure subscription, including the network interface cards. The customer does not need to provide an Azure subscription. There is no Active Directory dependency since Business cloud PCs natively join Azure AD. There is also no requirement of an Intune license.

Business cloud PCs route all traffic through Microsoft-controlled network infrastructure and there is no way for admins to control the inbound or outbound connectivity to/from these VMs. There is currently no way to assign static IPs to Business cloud PCs. Since these cloud PCs run in Microsoft's Azure subscription and are not enrolled in Intune, there is no admin interface to manage them. They can only be managed directly by the user, just like a standalone physical Windows device.

There are no pre-requisites and no setup steps needed for Business cloud PCs. Simply assign a Business cloud PC license to a user in the Windows 365 Admin portal and the new desktop gets provisioned within an hour. The user will get an email notification with login instructions to start using their new cloud PC.

1a – Control Plane

Azure Virtual Desktop and Windows 365 share the same global control plane running in Azure. The control plane consists of things such as the web portal, gateway, connection broker, licensing, and diagnostics service. All components are hosted and managed by Microsoft and admins interact with them via a portal or API while end users interact with them via the AVD and cloud PC client apps.

An agent application runs on each virtual desktop – AVD session hosts and Windows 365 cloud PCs. This agent is responsible for communication with the Microsoft-managed control plane. Microsoft manages the agent and updates it automatically. The agent for both AVD and Windows 365 appear to be the same..

1b – Azure Subscriptions

Azure Virtual Desktop requires all session host VMs, FSLogix profile storage, and networking to be contained in a customer's Azure subscription. Microsoft manages the control plane components, while the customer is fully responsible for everything related to the session host VMs. Costs are also incurred for all components based on usage at the customer subscription level.

With Windows 365, all compute (i.e. VMs) is contained in a Microsoft-managed Azure subscription. This means that customers don't have direct access to manage the VM resources, as they do with AVD, since these resources are not accessible in their Azure subscription. They also don't incur the costs associated with running cloud PC VMs at the Azure subscription level (more on this below).

There is a significant difference between Windows 365 **Enterprise** cloud PCs and **Business** cloud PCs. Enterprise cloud PCs run in Microsoft's Azure subscription, but their network interface cards (virtual NICs) are "injected" into the customer's Azure subscription. Business cloud PC VMs reside entirely within Microsoft's Azure subscription with no components connected to any customer Azure subscription.

1c – Compute

Azure Virtual Desktop session hosts are regular VMs and can be deployed and used in a very flexible way with all the power of Azure. These session hosts can serve up personal desktops, where a VM is dedicated to a single user, or pooled desktops where a VM can be used by multiple users who move between such VMs daily. The cost of compute is incurred by the customer since these VMs run in the customer's Azure subscription. Since pricing for Azure compute is based on usage, auto-scaling can be used to significantly reduce the cost of VMs in an AVD environment. Reserved Instances can also be used with AVD session host VMs.

A Windows 365 cloud PC is a VM that's dedicated to a single user via permanent assignment (like personal desktops in AVD). These VMs run in Microsoft's Azure subscription, which means the customer is not responsible for the compute costs. They are licensed via a Windows 365 cloud PC license and are based on a fixed per-user-per-month price. Since IT admins don't

have access to these VMs directly from the Azure portal and the cost doesn't depend on usage, concepts like auto-scaling and reserved instances don't apply to cloud PCs.

1d – Storage

Azure Virtual Desktop session host VMs must have an OS disk attached to them. These disks can be any Azure managed disk type (e.g. Premium SSD, Standard SSD or Standard HDD) and even an Ephemeral OS disk. IT admins have full flexibility when it comes to the size and type of OS disk to use. Auto-scaling can be leveraged to convert SSD disks to cheaper HDD disks while VMs are powered off.

FLogix profiles are typically stored in Azure Files shares, Azure NetApp Files volumes, or file server VMs. Here too, IT admins have full flexibility around the type of storage and the size of storage to use in the AVD deployment, including what to back up and how. All storage costs associated with session host OS disks and FLogix profile storage are incurred by the customer via the Azure subscription.

Each Windows 365 cloud PC comes with a pre-defined amount of local SSD storage. The cost of this storage is included in the cloud PC M365 license, and the OS disk object is located within Microsoft's Azure subscription, which means the customer is not responsible for any Azure storage costs. There is no flexibility around what type of storage to use and using auto-scaling is not possible since the cost is fixed. FLogix is not used with Windows 365 cloud PCs and user profiles are "native" and reside fully on the C: drive of the desktop. This means that no additional Azure Files, Azure NetApp Files, or file server VMs are needed. There are limited backup and DR options available for now with cloud PCs..

1e – Networking

Azure Virtual Desktop network routing and security is fully under the control of IT admins. Session hosts are regular VMs that can be created on any virtual network in the customer's Azure subscription and this vNet can be configured with all the flexibility of Azure networking. This means that customers have full control of how ingress and egress traffic is routed, what IP addresses are used, VPN connectivity, etc. They are also responsible for any costs associated with egress bandwidth usage.

The network configuration of cloud PCs depends on whether they are Enterprise or Business. Enterprise cloud PCs have the same capabilities, from a networking perspective, as AVD session hosts. The vNet that they attach to resides within the customer's Azure subscription and is fully controlled by the IT admin. Network interfaces of cloud PCs are "injected" into the customer's Azure subscription even though the VM resources they are attached to are in a different subscription. Just like with AVD, all costs associated with networking are incurred by the customer.

Business cloud PCs don't have the same network flexibility as Enterprise ones. Their network interfaces are not injected into a vNet in the customer's Azure subscription but are part of a Microsoft-managed network. This means that routing, firewall security, VPN connectivity, and IP addressing cannot be controlled by the customer. The costs of egress bandwidth usage are not customer's responsibility and are included in the cost of licensing a cloud PC (more on this below).

If – User profiles

Azure Virtual Desktop leverages FSLogix profile container technology. This allows users to roam from one session host VM to another while their user profile (contents of `c:\users\username` folder) follows them seamlessly. FSLogix provides lots of flexibility but comes at the cost of having to deploy at least one SMB file share to host the profile container VHD(X) files. This is typically done with Azure Files, Azure NetApp Files, or file server VMs.

Because Windows 365 cloud PCs are single-session desktops dedicated to individual users, Microsoft removed FSLogix from the picture. A user's Windows profile is "native", meaning that it is stored directly on the C: drive of the cloud PC, exactly as is with traditional, physical Windows computers. This removes the complexity of having to configure and manage FSLogix and the associated overhead of having a SMB file share to store profiles centrally. It also introduces some unique challenges in protecting users' data (e.g. Documents and Desktop folders) and moving users from one desktop to another without losing settings.

1g – Identity

Azure Virtual Desktop currently requires Active Directory Domain Services. This requirement can be fulfilled by using an existing Windows AD environment or by using the Azure AD DS PaaS service. Native Azure AD join isn't yet supported, but upcoming support was [recently announced](#).

Windows 365 Enterprise cloud PCs require [Hybrid Azure AD join](#). This means that you need traditional Windows AD synched to Azure AD with Hybrid Join enabled. Azure AD DS is not currently supported.

Business cloud PCs are natively Azure AD joined and do not require (or support) Windows AD or Azure AD DS.

Summary (Technical Architecture)

	Windows 365		Azure Virtual Desktop	
	Enterprise	Business	Personal	Pooled
Control plane	Azure Virtual Desktop		Azure Virtual Desktop	
Azure subscriptions	Microsoft-managed, except networking	Fully Microsoft-managed	Customer-managed	
Compute	Microsoft-managed, fixed cost, no direct admin access to VMs		Customer-managed, usage-based cost, flexible	
Storage	Microsoft-managed, fixed cost, multiple storage sizes, service-level DR		OS disks, FSLogix, customer-managed, usage-based cost, flexible, easy to back up	
Networking	Customer-managed, usage-based cost, flexible routing, IPs, and security	Microsoft-managed, fixed cost, no direct admin access, no flexibility	Customer-managed, usage-based cost, flexible routing, IPs, and security	
User profiles	Local profiles		FSLogix optional	FSLogix mandatory
Identity	Hybrid AD join required. Azure AD join coming soon. Azure AD DS is not supported.	Azure AD join only. No AD DS option.	AD DS is required. Windows AD or Azure AD DS supported. Native Azure AD join coming soon.	

2 – IT Admin Experience

The IT admin experience varies greatly between Windows 365 and Azure Virtual Desktop. AVD relies heavily on Azure management concepts and provides maximum flexibility while Windows 365 aims to simplify management by making it (close to) identical to managing existing physical desktop assets and leveraging the same set of Microsoft tools to manage physical and virtual PCs.

2a – Management Portal

All components of Azure Virtual Desktop are managed via the Azure portal, PowerShell, or third-party tools like the Nerdio Manager.

Enterprise cloud PCs are managed via Microsoft Endpoint Manager (MEM) and via the Azure portal for all networking. Administration of Enterprise cloud PCs can also be unified via a single portal like the Nerdio Manager. MEM allows management of cloud PCs at the OS level and above. This means that admins do not have access to make changes to the underlying VM resources, they can only make changes to Windows and applications. Virtual networking is managed via the Azure portal.

Business cloud PCs are not integrated with Endpoint Manager and do not have a dedicated management portal. They can only be managed by the end user assigned to the desktop while logged into it. Actions such as PC restarts can be performed by the user from the cloud PC web portal. Admins can manage Business cloud PC license assignment with Windows 365 Admin portal and third-party tools like the Nerdio Manager.

2b – Operating System

Azure Virtual Desktop supports all current versions of Windows, including Windows 10 Enterprise (single session), EVD (multi-session) and Server 2012/2016/2019.

Windows 365 cloud PCs only support Windows 10 Enterprise (single session) since they are dedicated, non-multi-user desktops..

2c – Desktop Image Management

Azure Virtual Desktop can leverage all image types. These include Azure Marketplace images, custom images, and shared image gallery images. Session host VMs can be created from these images and be kept up to date by updating the image and then re-imaging session hosts to the latest version. Images can be stored in one or more Azure regions for geographic distribution and resilience. Images can use any supported operating system and be both Gen1 and Gen2 VM hardware. There is no limit on the number of Azure images that can be used in an AVD environment.

Enterprise cloud PC images support Microsoft-provided Windows 10 Enterprise OS or custom images stored in a customer's subscription. These images must be Gen1 VM hardware. There is a limit of 20 custom images per Azure AD tenant.

Business cloud PCs don't support custom images and must be deployed from Microsoft provided Windows 10 Enterprise OS.

2d – Applications and Updates

Azure Virtual Desktop session hosts can be updated via Microsoft Endpoint Manager, through a golden image, or manually. Applications can be delivered to session hosts via image updates, manual installation on host VMs, or using MSIX app attach. The update and application delivery process in AVD is very flexible and can be fully automated.

Enterprise cloud PCs can be updated via MEM or manual methods. Image-based software deployments are not typical without third-party tools like Nerdio Manager. Also, MSIX app attach application delivery is not currently supported with cloud PCs.

Business cloud PCs can be updated with Windows update, manually by the user, or by using third-party management tools.

2e – Backup and DR

Azure Virtual Desktop session hosts can be backed up and protected in several different ways including Azure Site Recovery and Azure Backup. This allows organizations to create a robust backup, DR, and business continuity strategy for their virtual desktop environment.

There is currently no native backup method for Windows 365 cloud PCs since they are not accessible to admins at the storage or hypervisor level. Third-party, agent-based, OS-level backup methods can be used to protect cloud PCs.

2f – Monitoring

Azure Virtual Desktop includes robust logging, diagnostics, monitoring, and reporting capabilities. Logs are generated by the AVD service and AVD agent running on session host VMs. This information is streamed to Azure Log Analytics where it is captured and visualized with Azure Monitor workbooks. Many third-party monitoring tools are available for AVD.

Due to the lack of hypervisor-level access to cloud PC VMs, monitoring is possible only via [Endpoint Analytics](#), which is the same tool that can be used for monitoring physical endpoints. Business cloud PCs do not currently have a monitoring interface.

2g – User profiles

Azure Virtual Desktop leverages FSLogix for user profile encapsulation. This allows users to easily roam between session host VMs without losing their user state between sessions. Personal AVD desktops can be deployed without FSLogix, but even in persistent scenarios FSLogix profiles provide a valuable profile backup capability and make it easier to manage session host updates through images. A SMB file share is required to host the FSLogix profile containers. This can be an Azure Files share, Azure NetApp Files volume, or a file server VM.

Windows 365 cloud PCs do not leverage FSLogix and all profiles are natively stored on the C: drive. This allows for simplified management since no additional SMB storage or profile configuration is required. Without profile data redirection it is important to consider ways to back up user data. One such strategy can leverage OneDrive to protect user data.

2h – Networking

IT admins fully control all aspects of Azure Virtual Desktop networking since it runs in a customer-managed Azure subscription. Static IP addresses can be assigned, VPN tunnels configured, and firewall rules enforced.

Enterprise cloud PCs have the same network flexibility as in AVD deployments. Business cloud PCs, on the other hand, do not have any network flexibility. Microsoft fully controls the IP addressing, traffic flow, and security of Business cloud PC networking.

2i – Auto-scaling

Azure Virtual Desktop greatly benefits from usage-based Azure pricing model and auto-scale can be used to drastically reduce Azure compute and storage costs – up to 75% of peak demand. It is also possible to use Azure Reserved Instances to reduce costs and guarantee available capacity.

Windows 365 cloud PCs are priced on a fixed monthly basis. Even if a user does not log into their desktop at all during the month, the desktop will cost the same as if the user logged into their desktop every day. Therefore, the concept of auto-scaling does not apply to cloud PCs. This has significant impact on cost efficiency in different use-cases.

See summary table on next page:

Summary (IT Admin Experience)

	Windows 365		Azure Virtual Desktop	
	Enterprise	Business	Personal	Pooled
Management portal	Microsoft Endpoint Manager	No admin portal	Azure Portal	
Operating system	Windows 10/11 Enterprise (single session)		Windows 10/11 Enterprise (Single session, multi-session), Windows Server	
Desktop images management	Custom and Microsoft-provided. No image based management due to persistent VMs.	Microsoft-provided only	Custom and Microsoft-provided. Image-based management possible with FSLogix.	Custom and Microsoft-provided. Image-based management.
Applications and updates	Delivered via MEM or manually installed	Manually installed only	Delivered via MEM, image updates or MSIX app attach	
Backup and DR	No hypervisor-level backups at this time		Full backup and DR flexibility of Azure	
Monitoring	Endpoint Analytics	Not available	Azure Monitor	
User profiles	Local profiles stored on C: drive		Native stored on C: drive or FSLogix stored on SMB file share	FSLogix stored on Azure Files, Azure NetApp Files or file server VM
Networking	Flexible, customer-managed	Not configurable, Microsoft-managed	Flexible, customer-managed	
Auto-scaling	Not applicable due to fixed monthly cost		Flexible and can save up to 75% of peak Azure costs	

3 – End-user Experience

The end-user experience is almost identical in Windows 365 and AVD. Users connect to AVD sessions and cloud PCs using the same client app, which is available for Windows, MacOS, iOS, Android and as a HTML client.

Windows 365 is built on top of Azure Virtual Desktop global infrastructure and will be familiar to those with AVD experience. When connecting to a cloud PC, a user authenticates to Azure AD using the AVD client and all cloud PCs that the user is entitled to appear in the feed.

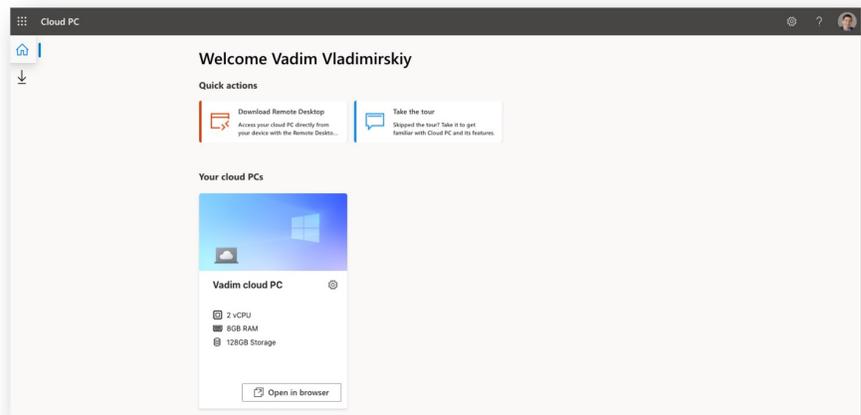
Leveraging the same infrastructure as AVD provides users the advantage of a unified experience across Windows 365 and Azure Virtual Desktop. Admins can control the resources visible to individual end-users and the user will see everything in a single feed using the same app. The authentication and multi-factor experience will also be very familiar since it leverages Azure AD, which is used for M365 and AVD authentication.

3a – Connecting to Desktop

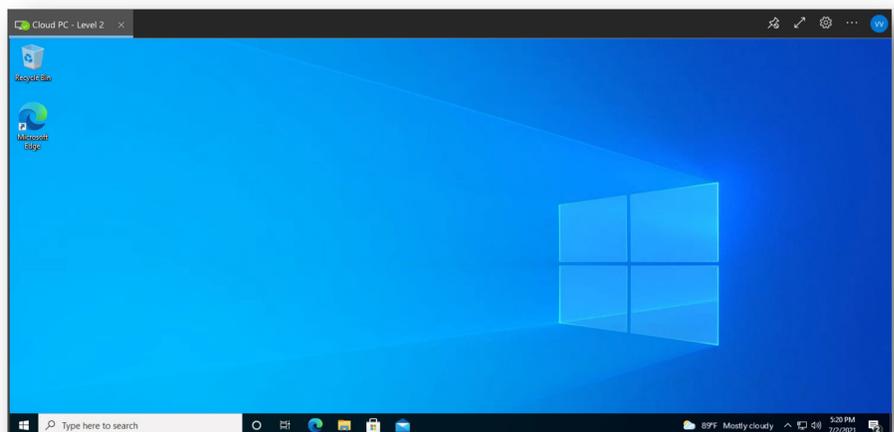
With Azure Virtual Desktop, users navigate to <https://aka.ms/wvdwebarm> or download a client app from <https://aka.ms/wvdclients>.

Windows 365 cloud PC users go navigate to <https://cloudpc.microsoft.com> and connect in the same way as AVD.

Step 1: Go to <https://cloudpc.microsoft.com> and log in



Step 2: Connect to cloud PC in browser or download the Remote Desktop client app



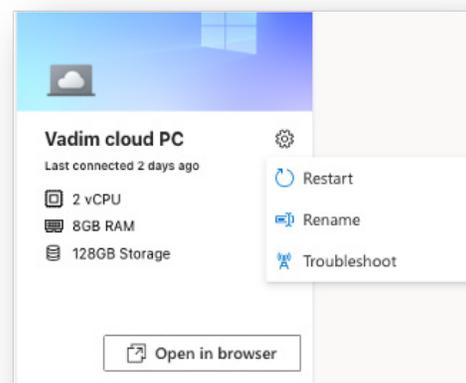
3b – Printing and Scanning

Both Azure Virtual Desktop and Windows 365 cloud PCs support printer and scanner redirection via the Remote Desktop client app. With AVD and Enterprise cloud PCs it is possible to configure network-based printing and scanning with a site-to-site VPN tunnel between the Azure vNet and local network that hosts the printers and scanners. It is not possible to use network-based printing and scanning with Business cloud PCs since IT admins do not have control of the network where the cloud PCs reside. [Universal Print](#) is Microsoft's new cloud-based print solution that can be used with AVD and Windows 365 cloud PCs. Several third-party products exist that help simplify printing and scanning.

3c – User Self-Service

Azure Virtual Desktop has limited self-service capabilities for end-users. For example, users cannot restart their own desktop VM or log off a hung session with the AVD client app. Third-party tools, like Nerdio Manager, provide users with a self-service portal where such actions can be performed.

Windows 365 cloud PCs can be restarted by the end-user without the need to contact support. A restart button is built into the cloud PC web portal.



Summary (End-user Experience)

	Windows 365		Azure Virtual Desktop	
	Enterprise	Business	Personal	Pooled
End-user connectivity	HTML, Windows, MacOS, iOS, Android, Linux (https://cloudpc.microsoft.com)		HTML, Windows, MacOS, iOS, Android, Linux (https://aka.ms/wvdwebarm)	
Printing and scanning	Redirected via client, Universal Print, and network-based	Redirected via client only	Redirected via client, Universal Print, and network-based	
User self-service (e.g. restart)	Yes, within HTML portal		No, only with third-party tools like Nerdio Manager	

4 – Licensing and Infrastructure Costs

4a – Windows10 Enterprise

Azure Virtual Desktop requires the user connecting to an AVD session to have an assigned Windows 10 Enterprise subscription license. Windows 10 Enterprise can be purchased as a standalone subscription (e.g. Windows 10 Ent E3/E5/VDA) or be included as part of a Windows 365 suite subscription (e.g. M365 E3/E5 and Business Premium). This Windows subscription license includes the usage rights of the AVD control plane and entitles the user to connect to Windows 10 desktops hosted in Azure. All other costs are part of Azure infrastructure consumption (e.g. compute, storage, networking).

Both Enterprise and Business Windows 365 cloud PCs require a Windows 10 Enterprise subscription just like AVD desktops. However, the compute costs are not purchased as usage-based Azure resources but rather as a M365 license SKU.

4b – Compute and Storage

Azure Virtual Desktop infrastructure costs are based on Azure consumption. This includes the compute costs of running AVD session host VMs, the cost of OS disks and the usage of Azure Files for FSLogix storage. All costs are based on actual usage. If a VM is powered off, there is no compute charge.

Windows 365 cloud PCs are not purchased as Azure usage-based infrastructure. Rather, they are purchased as licenses through Windows 365. Each cloud PC license provides the user with a certain amount of compute, RAM, and storage capacity. At general availability there will be 12 cloud PC sizes ranging from 1 vCPU to 8 vCPUs, 2 GB to 32 GB of RAM, and 64 GB to 512 GB of storage.

4c – Networking

Azure Virtual Desktop networking costs are incurred at the Azure subscription level where session host VMs run. These charges typically include egress bandwidth, NAT gateway, VPNs, and Firewalls.

Enterprise cloud PCs require the customer to provide a network infrastructure within a customer-managed Azure subscription. Therefore, all network costs are the same as with AVD.

Business cloud PCs do not leverage a customer-managed Azure network. Therefore, all network related costs are incurred by Microsoft and are included in the monthly cloud PC license.

4d – Intune

Intune can be optionally used to manage Azure Virtual Desktop session hosts. However, Intune is not required for an AVD deployment, and most environments are managed via images.

Enterprise cloud PCs require an Intune license. Since Intune is the management interface for these cloud PCs, the Azure AD tenant must have an Intune license and each user who is assigned to an Enterprise cloud PC must have an Intune license assigned. Intune licenses can be purchased standalone or as part of a Windows 365 package like E3/E5 and Business Premium.

Business cloud PCs are not managed through MEM and therefore do not require an Intune license.

4e – Microsoft 365 Apps (Office)

Azure Virtual Desktop requires a subscription to Windows 365 Apps with Shared Computer Activation entitlement. All Windows 365 packages that include Office Apps have Shared Computer Activation. Windows 365 Business standalone does not and, therefore, cannot be used in AVD.

Windows 365 cloud PCs are dedicated VMs and therefore do not require Shared Computer Activation. Any subscription to Windows 365 is sufficient.

Summary (Licensing and Infrastructure Costs)

	Windows 365		Azure Virtual Desktop	
	Enterprise	Business	Personal	Pooled
Windows 10 Enterprise	Any subscription to Windows 10 Enterprise or Microsoft 365 suite that includes Windows 10 Enterprise		Any subscription to Windows 10 Enterprise or Microsoft 365 suite that includes Windows 10 Enterprise	
Compute and storage	Windows 365 cloud PC license		Azure consumption	
Networking	Azure consumption	Included in Windows 365 license	Azure consumption	
Intune	Required	Optional	Optional	
Office	Any Office subscription		Office subscription with SCA rights	

5 – Comparing Windows 365 Cloud PC License Costs vs. AVD Azure Consumption

There are several considerations that come into play when deciding on the right virtual desktop technology for your organization. Microsoft provides customers with ample choice and meets customers where they are in terms of admin tooling, existing licenses, and Azure expertise. In this section we'll explore the cost efficiency of different virtual desktop use-cases and determine when Windows 365 fixed-price licenses are more cost-efficient than usage-based AVD infrastructure costs. For this discussion, we'll assume that Windows OS licensing costs are the same in both AVD and Windows 365 scenarios and focus exclusively on the cost of the infrastructure.

Windows 365 license costs depend on the hardware specs that a user needs. Each desktop comes with a certain number of vCPUs, GB of RAM, and SSD storage. If we align the vCPU and RAM configuration of each cloud PC license with a comparable Azure VM size and managed disk we can then compare their costs side-by-side.

Since cloud PCs are dedicated, persistent desktops they are most similar to AVD personal desktops. If we compare cloud PCs with equivalently sized personal AVD desktops, using a VM on a 3-year reserved instance, we'll see that the prices are very similar and cloud PC is slightly less expensive for some sizes and much more cost effective for the largest VMs. On average, Windows 365 is **11%** cheaper than a comparably sized Azure VM and managed disk running 24/7 on a 3-year reserved instance.

Windows 365			Azure Virtual Desktop Personal Host Pool (3-year reserved instance)			
vCPU and RAM	SSD Storage (GB)	User Price (monthly)	Compute	SSD Storage	Monthly Cost	\$ Savings (%) (relative to Windows 365)
Light user 1 vCPU / 2 GB RAM	64	\$20	\$27	\$5	\$32	\$-12
Basic user 2 vCPU / 4 GB RAM	64	\$28	\$27	\$5	\$32	\$-4
	128	\$31	\$27	\$10	\$37	\$-6
Standard user 2 vCPU / 8 GB RAM	256	\$40	\$27	\$19	\$46	\$-6
	128	\$41	\$32	\$10	\$42	\$-1
Premium user 4 vCPU / 16 GB RAM	256	\$50	\$32	\$19	\$51	\$-1
	128	\$66	\$64	\$10	\$74	\$-8
Super user 8 vCPU / 32 GB RAM	256	\$75	\$64	\$19	\$83	\$-8
	512	\$101	\$64	\$38	\$102	\$-1
Super user 8 vCPU / 32 GB RAM	128	\$123	\$132	\$10	\$142	\$-19
	256	\$132	\$132	\$19	\$151	\$-19
	512	\$158	\$132	\$38	\$170	\$-12
AVERAGE AVD SAVINGS (as compared to Windows 365)						-11%

If we assume that users are using their personal AVD desktops 50 hours per week (10 hours X 5 weekdays) and the VMs are stopped the rest of the time, then there will be a cost savings by using personal AVD desktops with pay-as-you-go VM pricing and powering them off outside of the 50 work hours (70% of the time). There are a few scenarios when Cloud PC is about the same cost as an AVD personal desktop, but on average, Azure Virtual Desktop personal desktop is **9%** cheaper than a cloud PC in this use-case.

Windows 365			Azure Virtual Desktop Personal Host Pool (Pay-as-you-go with auto-scaling)				
vCPU and RAM	SSD Storage (GB)	User Price (monthly)	Compute	SSD Storage	Monthly Cost	\$ Savings (%) (relative to Windows 365)	
Light user 1 vCPU / 2 GB RAM	64	\$20	\$22	\$5	\$27	\$-7	
Basic user 2 vCPU / 4 GB RAM	64	\$28	\$22	\$5	\$27	\$1 (3%)	
	128	\$31	\$22	\$10	\$32	\$-1	
Standard user 2 vCPU / 8 GB RAM	256	\$40	\$22	\$19	\$41	\$-1	
	128	\$41	\$25	\$10	\$35	\$6 (15%)	
Premium user 4 vCPU / 16 GB RAM	256	\$50	\$25	\$19	\$44	\$6 (12%)	
	128	\$66	\$50	\$10	\$60	\$6 (9%)	
Super user 8 vCPU / 32 GB RAM	256	\$75	\$50	\$19	\$69	\$6 (8%)	
	512	\$101	\$50	\$38	\$88	\$13 (13%)	
Super user 8 vCPU / 32 GB RAM	128	\$123	\$100	\$10	\$110	\$13 (11%)	
	256	\$132	\$100	\$19	\$119	\$13 (10%)	
512	\$158	\$100	\$100	\$38	\$138	\$20 (13%)	
Assumptions: • Average work week: 50 hours					AVERAGE AVD SAVINGS (as compared to Windows 365)		9%

Let's take this a step further and assume that not all users need a dedicated personal desktop and groups of users can be pooled together on multi-session AVD session hosts. We can see that there is significant per-user savings with AVD pooled desktops using reserved instances (RI). On average, the cost of a pooled Azure Virtual Desktop user on VMs that run 24/7 using 3-year reserved instances is **53%** lower than Windows 365.

Windows 365			Azure Virtual Desktop Pooled Host Pool (3-year reserved instances)					
vCPU and RAM	SSD Storage (GB)	User Price (monthly)	Compute	SSD Storage	Monthly Cost	\$ Savings (%) (relative to Windows 365)		
Light user 1 vCPU / 2 GB RAM	64	\$20	\$5	\$1	\$6	\$14 (70%)		
Basic user 2 vCPU / 4 GB RAM	64	\$28	\$6	\$1	\$7	\$21 (73%)		
	128	\$31	\$6	\$7	\$14	\$17 (56%)		
Standard user 2 vCPU / 8 GB RAM	256	\$40	\$6	\$20	\$26	\$14 (36%)		
	128	\$41	\$9	\$7	\$17	\$24 (59%)		
Premium user 4 vCPU / 16 GB RAM	256	\$50	\$9	\$20	\$29	\$21 (42%)		
	128	\$66	\$19	\$7	\$26	\$40 (61%)		
Super user 8 vCPU / 32 GB RAM	256	\$75	\$19	\$20	\$38	\$37 (49%)		
	512	\$101	\$19	\$44	\$62	\$39 (38%)		
Super user 8 vCPU / 32 GB RAM	128	\$123	\$37	\$7	\$44	\$79 (64%)		
	256	\$132	\$37	\$20	\$57	\$75 (57%)		
512	\$158	\$37	\$37	\$44	\$81	\$77 (49%)		
Assumptions: • AVD pooled desktop minimum: 10 users • Average work week: 50 hours • Disk space used for OS and apps: 50 GB • Average disk space usage: 50% • Pooled session host VM OS disk: E10 (128 GB Std SSD)			Pooled user/vCPU density: • Light: 4 users / vCPU • Basic: 3 users / vCPU • Standard: 2 users / vCPU • Premium: 1 users / vCPU • Super: 0.5 users / vCPU			AVERAGE AVD SAVINGS (as compared to Windows 365)		53%

Combining pooled AVD desktops with auto-scaling provides the deepest savings when using Azure Virtual Desktop as compared to Windows 365. Assuming that users are working 10 hours/day, 5 days/week the average savings is **58%** when using pay-as-you-go VMs with auto-scaling.

Windows 365			Azure Virtual Desktop Pooled Host Pool (Pay-as-you-go with auto-scaling)			
vCPU and RAM	SSD Storage (GB)	User Price (monthly)	Compute	SSD Storage	Monthly Cost	\$ Savings (%) (relative to Windows 365)
Light user 1 vCPU / 2 GB RAM	64	\$20	\$4	\$1	\$5	\$15 (75%)
	128	\$28	\$5	\$1	\$6	\$22 (77%)
Basic user 2 vCPU / 4 GB RAM	128	\$31	\$5	\$7	\$12	\$19 (60%)
	256	\$40	\$5	\$20	\$25	\$15 (39%)
Standard user 2 vCPU / 8 GB RAM	128	\$41	\$8	\$7	\$15	\$26 (64%)
	256	\$50	\$8	\$20	\$27	\$23 (46%)
Premium user 4 vCPU / 16 GB RAM	128	\$66	\$15	\$7	\$22	\$44 (66%)
	256	\$75	\$15	\$20	\$35	\$40 (54%)
	512	\$101	\$15	\$44	\$59	\$42 (42%)
Super user 8 vCPU / 32 GB RAM	128	\$123	\$30	\$7	\$37	\$86 (70%)
	256	\$132	\$30	\$20	\$50	\$82 (62%)
	512	\$158	\$30	\$44	\$74	\$84 (53%)

Assumptions:

- AVD pooled desktop minimum: **10 users**
- Average work week: **50 hours**
- Disk space used for OS and apps: **50 GB**
- Average disk space usage: **50%**
- Pooled session host VM OS disk: **E10 (128 GB Std SSD)**

Pooled user/vCPU:

- Light: **4 users / vCPU**
- Basic: **3 users / vCPU**
- Standard: **2 users / vCPU**
- Premium: **1 users / vCPU**
- Super: **0.5 users / vCPU**

AVERAGE AVD SAVINGS (as compared to Windows 365)

58%

Another important consideration is that Cloud PCs and personal AVD desktops are priced per-**named** user. Meaning that a license or VM is consumed for every user to whom the Cloud PC license or AVD personal desktop VM is assigned – regardless of whether this user ever connects to the desktop. Pooled desktops, on the other hand, only consume infrastructure when **concurrent** users are logged in. If no users are connected, no session host VMs need to be powered on. As more users log in, more infrastructure is brought online to accommodate the demand.

In most environments, user concurrency is a fraction of the total named users at any given time – often 50% or less. This means that the cost savings in a pooled desktop environment will be even greater, when concurrency is considered, than presented in the table above.

By putting it all together, we see that Windows 365 Cloud PCs are most cost effective when users need dedicated, persistent desktops and will be using them more than 50 hours per week. With users who can be pooled together into AVD host pools, there is significant infrastructure cost savings to be realized by using auto-scaling.

Windows 365			Azure Virtual Desktop			
vCPU and RAM	SSD Storage (GB)	User Price (monthly)	Personal Desktop User Cost (3-year reserved instances)	Personal Desktop User Cost (% savings) (Pay-as-you-go & auto-scaling)	Pooled Desktop User Cost (% savings) (3-year reserved instances)	Pooled Desktop User Cost (% savings) (Pay-as-you-go & auto-scaling)
Light user 1 vCPU / 2 GB RAM	64	\$20	\$32	\$27 (0%)	\$6 (70%)	\$5 (75%)
	64	\$28	\$32	\$27 (3%)	\$7 (73%)	\$6 (77%)
Basic user 2 vCPU / 4 GB RAM	128	\$31	\$37	\$32 (0%)	\$14 (56%)	\$12 (60%)
	256	\$40	\$46	\$41 (0%)	\$26 (36%)	\$25 (39%)
Standard user 2 vCPU / 8 GB RAM	128	\$41	\$42	\$35 (15%)	\$17 (59%)	\$15 (64%)
	256	\$50	\$51	\$44 (12%)	\$29 (42%)	\$27 (46%)
Premium user 4 vCPU / 16 GB RAM	128	\$66	\$74	\$60 (9%)	\$26 (61%)	\$22 (66%)
	256	\$75	\$83	\$69 (8%)	\$38 (49%)	\$35 (54%)
	512	\$101	\$102	\$88 (13%)	\$62 (38%)	\$59 (42%)
Super user 8 vCPU / 32 GB RAM	128	\$123	\$142	\$110 (11%)	\$44 (64%)	\$37 (70%)
	256	\$132	\$151	\$119 (10%)	\$57 (57%)	\$50 (62%)
	512	\$158	\$170	\$138 (13%)	\$81 (49%)	\$74 (53%)
AVERAGE AVD SAVINGS (as compared to Windows 365)			-11%	9%	53%	58%

Assumptions:

- AVD pooled minimum: **10 users**
- Average work week: **50 hours**
- OS and apps used disk space: **50 GB**

- Average disk space usage: **50%**
- Pooled session host VM OS disk: **110 (128 GB Standard SSD)**

Pooled user/vCPU density:

- Light: **4 users / vCPU**
- Basic: **3 users / vCPU**
- Standard: **2 users / vCPU**
- Premium: **1 users / vCPU**
- Super: **0.5 users / vCPU**

View a complete comparative summary table on the next page.

TECHNICAL ARCHITECTURE				
	Windows 365		Azure Virtual Desktop	
	Enterprise	Business	Personal	Pooled
Control plane	Azure Virtual Desktop		Azure Virtual Desktop	
Azure subscriptions	Microsoft-managed, except networking	Fully Microsoft-managed	Customer-managed	
Compute	Microsoft-managed, fixed cost, no direct admin access to VMs		Customer-managed, usage-based cost, flexible	
Storage	Microsoft-managed, fixed cost, multiple storage sizes, service-level DR		OS disks, FSLogix, customer-managed, usage-based cost, flexible, easy to back up	
Networking	Customer-managed, usage-based cost, flexible routing, IPs, and security	Microsoft-managed, fixed cost, no direct admin access, no flexibility	Customer-managed, usage-based cost, flexible routing, IPs, and security	
User profiles	Local profiles		FSLogix optional	FSLogix mandatory
Identity	Hybrid AD join required. Azure AD join coming soon. Azure AD DS not supported.	Azure AD join only. No AD DS option.	AD DS is required. Windows AD or Azure AD DS supported. Native Azure AD join coming soon.	

IT ADMIN EXPERIENCE				
	Windows 365		Azure Virtual Desktop	
	Enterprise	Business	Personal	Pooled
Management portal	Microsoft Endpoint Manager	No admin portal	Azure Portal	
Operating system	Windows 10/11 Enterprise (single session)		Windows 10/11 Enterprise (Single session, multi-session), Windows Server	
Desktop images management	Custom and Microsoft-provided. No image based management due to persistent VMs.	Microsoft-provided only	Custom and Microsoft-provided. Image-based management possible with FSLogix.	Custom and Microsoft-provided. Image-based management.
Applications and updates	Delivered via MEM or manually installed	Manually installed only	Delivered via MEM, image updates or MSIX app attach	
Backup and DR	No hypervisor-level backups at this time		Full backup and DR flexibility of Azure	
Monitoring	Endpoint Analytics	Not available	Azure Monitor	
User profiles	Local profiles stored on C: drive		Native stored on C: drive or FSLogix stored on SMB file share	FSLogix stored on Azure Files, Azure NetApp Files or file server VM
Networking	Flexible, customer-managed	Not configurable, Microsoft-managed	Flexible, customer-managed	
Auto-scaling	Not applicable due to fixed monthly cost		Flexible and can save up to 75% of peak Azure costs	

END-USER EXPERIENCE				
	Windows 365		Azure Virtual Desktop	
	Enterprise	Business	Personal	Pooled
End-user connectivity	HTML, Windows, MacOS, iOS, Android, Linux (https://cloudpc.microsoft.com)		HTML, Windows, MacOS, iOS, Android, Linux (https://aka.ms/wvdwebarm)	
Printing and scanning	Redirected via client, Universal Print, and network-based	Redirected via client only	Redirected via client, Universal Print, and network-based	
User self-service (e.g. restart)	Yes, within HTML portal		No, only with third-party tools like Nerdio Manager	

LICENSING AND INFRASTRUCTURE COSTS				
	Windows 365		Azure Virtual Desktop	
	Enterprise	Business	Personal	Pooled
Windows 10 Enterprise	Any subscription to Windows 10 Enterprise or Microsoft 365 suite that includes Windows 10 Enterprise		Any subscription to Windows 10 Enterprise or Microsoft 365 suite that includes Windows 10 Enterprise	
Compute and storage	Windows 365 cloud PC license		Azure consumption	
Networking	Azure consumption	Included in Windows 365 license	Azure consumption	
Intune	Required	Optional	Optional	
Office	Any Office subscription		Office subscription with SCA rights	



Nerdio empowers IT professionals and Managed Service Providers (MSPs) to deploy, manage, and optimize virtual desktops in Microsoft Azure. Nerdio Manager for Enterprise is a packaged Azure application that runs in users' own tenant without compromising security and compliance by allowing third-party vendors access into the IT environment. Nerdio Manager for MSP is an Azure managed application that enables MSPs to automatically provision a complete virtual desktop environment in Azure in under an hour, connect to an existing deployment in minutes, manage all their clients in a single pane of glass admin portal, and optimize their virtual desktop environment with powerful auto-scaling. For more information, visit www.getnerdio.com.

Contact Us:

Email: hello@getnerdio.com

Website: getnerdio.com