Azure Virtual Desktop

Agenda:

Section 1:

1. Introduction to Azure Virtual Desktop
2. Virtual desktop infrastructure
3. What is Azure Virtual Desktop?
4. Azure Virtual Desktop Architecture
5. Azure Virtual Desktop components
6. Benefits of Azure Virtual Desktop
7. Azure limitations for Azure Virtual Desktop

1. Introduction of AVD:

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

2. Virtual desktop infrastructure:

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

3. What is Azure Virtual Desktop?

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

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

Azure Virtual Desktop is a desktop and app virtualization service that runs on Azure. Here's some of the key highlights:

- Deliver a full Windows experience with Windows 11, Windows 10, or Windows Server. Use single-session to assign devices to a single user, or use multi-session for scalability.
- Offer full desktops or use RemoteApp to deliver individual apps.
- Present Microsoft 365 Apps for enterprise and optimize it to run in multi-user virtual scenarios.
- Install your line-of-business or custom apps you can run from anywhere, including apps in the formats Win32, MSIX, and Appx.
- Deliver Software-as-a-service (SaaS) for external usage.
- Replace existing Remote Desktop Services (RDS) deployments.
- Manage desktops and apps from different Windows and Windows Server operating systems with a unified management experience.
- Host desktops and apps on-premises in a hybrid configuration with Azure Stack HCI.

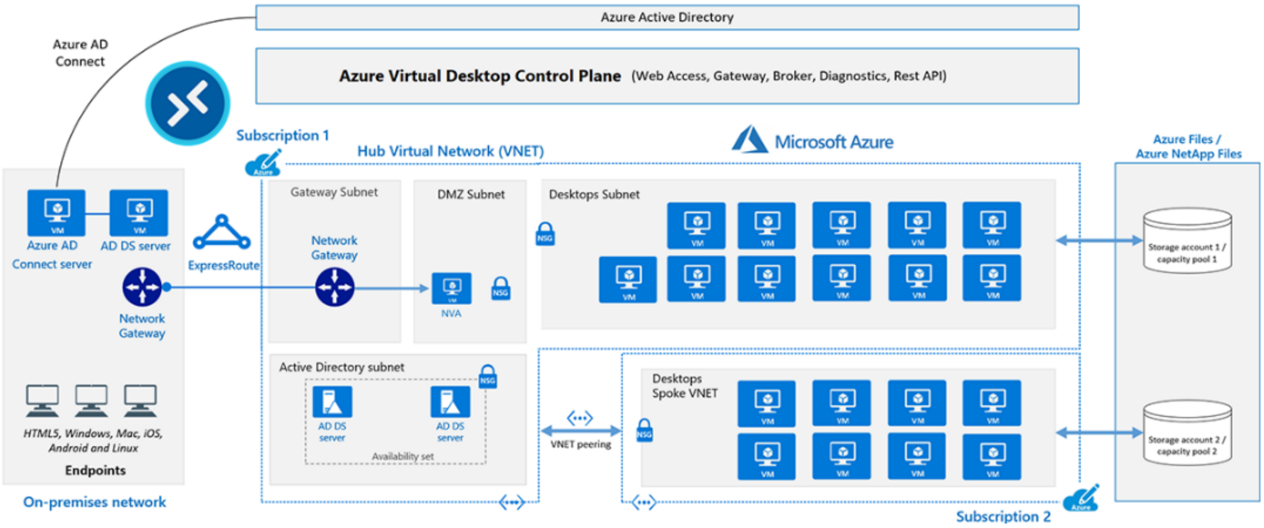
Key capabilities
With Azure Virtual Desktop, you can set up a scalable and flexible environment:

- Create a full desktop virtualization environment in your Azure subscription without running any gateway servers.
- Flexible configurations to accommodate your diverse workloads.
- Bring your own image for production workloads or test from the Azure Gallery.
- Reduce costs with pooled, multi-session resources. With the new Windows 11 and Windows 10 Enterprise multi-session capability, exclusive to Azure Virtual Desktop, or Windows Server, you can greatly reduce the number of virtual machines and operating system overhead while still providing the same resources to your users.
- Provide individual ownership through personal (persistent) desktops.
- Automatically increase or decrease capacity based on time of day, specific days of the week, or as demand changes with auto scale, helping to manage cost.

You can deploy and manage virtual desktops and applications:

- Use the Azure portal, Azure CLI, PowerShell and REST API to configure the host pools, create application groups, assign users, and publish resources.
- Publish a full desktop or individual applications from a single host pool, create individual application groups for different sets of users, or even assign users to multiple application groups to reduce the number of images.
- As you manage your environment, use built-in delegated access to assign roles and collect diagnostics to understand various configuration or user errors.
- Use the new diagnostics service to troubleshoot errors.
- Only manage the image and virtual machines, not the infrastructure. You don't need to personally manage the Remote Desktop roles like you do with Remote Desktop Services, just the virtual machines in your Azure subscription.

4. Azure Virtual Desktop Architectural:



The diagram above shows a typical architectural setup for Azure Virtual Desktop.

- The application endpoints are in the customer's on-premises network. ExpressRoute extends the on-premises network into the Azure cloud, and Microsoft Entra Connect integrates the customer's Active Directory Domain Services (AD DS) with Microsoft Entra ID.
- The Azure Virtual Desktop control plane handles Web Access, Gateway, Broker, Diagnostics, and extensibility components like REST APIs.
- The customer manages AD DS and Microsoft Entra ID, Azure subscriptions, virtual networks, Azure Files or Azure NetApp Files, and the Azure Virtual Desktop host pools and workspaces.
- To increase capacity, the customer uses two Azure subscriptions in a hub-spoke architecture, and connects them via virtual network peering.

Let's delve into the details of each component and their interactions:

1. On-Premises Application Endpoints:

- The customer's applications are hosted on-premises, forming the initial point of interaction for end-users with the system.

2. ExpressRoute:

- ExpressRoute serves as a dedicated, high-throughput connection between the customer's on-premises network and the Azure cloud. This ensures a reliable and secure link, minimizing latency and optimizing data transfer between on-premises resources and Azure.

3. Microsoft Entra Connect:

- Microsoft Entra Connect plays a crucial role in integrating the customer's on-premises Active Directory Domain Services (AD DS) with Microsoft Entra ID. This integration enables a unified identity management system, ensuring seamless authentication and authorization processes for users accessing Azure resources.

4. Azure Virtual Desktop Control Plane:

The control plane is responsible for managing various components, including:

- Web Access: Provides a web-based interface for users to access virtual desktops and applications.
- Gateway: Serves as an entry point for remote users to connect securely to the Azure Virtual Desktop infrastructure.
- Broker: Manages the assignment of virtual desktops to users and ensures optimal resource utilization.
- Diagnostics: Monitors and collects data for troubleshooting and performance optimization.
- Extensibility Components: Such as REST APIs, allowing customization and integration with external tools and systems.

5. Customer Management Responsibilities:

The customer retains control and management over several aspects, including:

- AD DS and Microsoft Entra ID: Ensures that user identities and access are administered in accordance with the organization's policies.
- Azure Subscriptions: Manages Azure subscription plans and resources to meet organizational requirements.
- Virtual Networks: Configures and maintains the virtual networks necessary for connecting on-premises and Azure resources.
- Azure Files or Azure NetApp Files: Manages the storage solutions for data and files associated with the virtual desktop infrastructure.
- Azure Virtual Desktop Host Pools and Workspaces: Controls the deployment and scaling of virtual desktops based on user requirements.

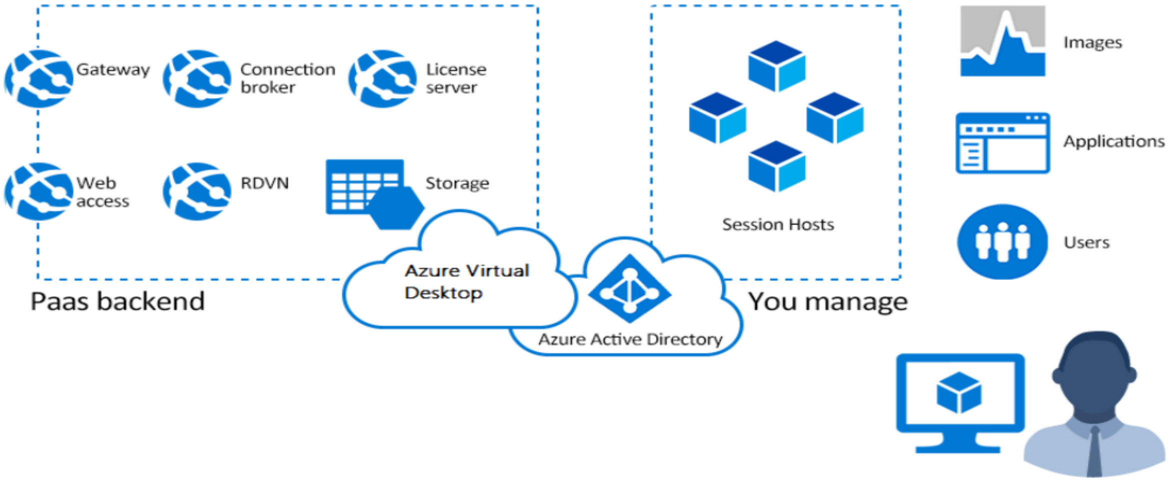
6. Hub-Spoke Architecture with Virtual Network Peering:

To enhance capacity and optimize resource management, the customer employs a hub-spoke architecture with two Azure subscriptions. This allows for the segregation of resources into hubs (centralized components) and spokes (specific workload or business units). Virtual network peering connects these subscriptions, enabling seamless communication and resource sharing between them.

5. Azure Virtual Desktop components:

Azure Virtual Desktop service architecture is similar to Windows Server Remote Desktop Services. Microsoft manages the infrastructure and brokering components, while enterprise customers manage their own desktop host virtual machines (VMs), data, and clients.

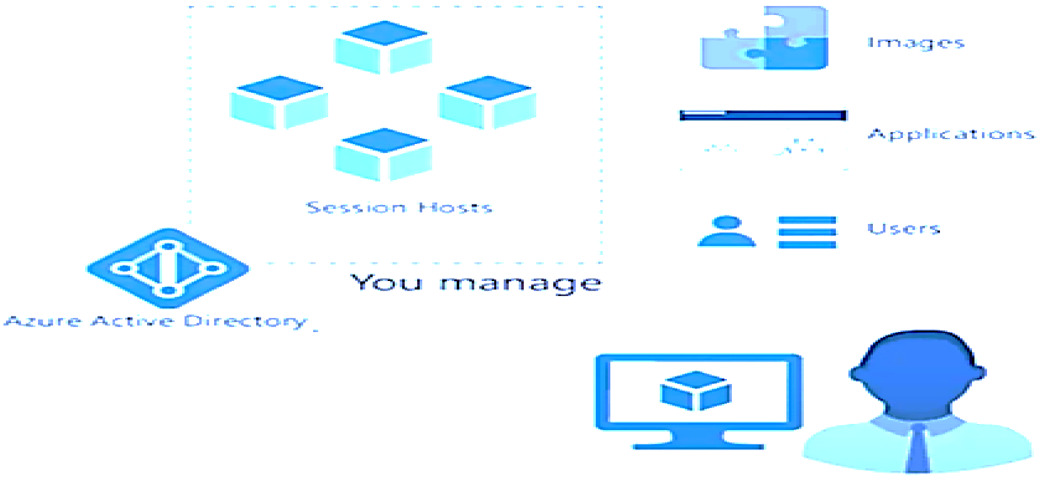
Section 1: Azure Virtual Desktop Architecture



Components Microsoft manages

Microsoft manages the following Azure Virtual Desktop services as part of Azure:

- Web Access: The Web Access service within Window Virtual Desktop lets users access virtual desktops and remote apps through an HTML5-compatible web browser as they would with a local PC, from anywhere on any device. You can secure Web Access using multifactor authentication in Microsoft Entra ID.
- Gateway: The Remote Connection Gateway service connects remote users to Azure Virtual Desktop apps and desktops from any internet-connected device that can run an Azure Virtual Desktop client. The client connects to a gateway, which then orchestrates a connection from a VM back to the same gateway.
- Connection Broker: The Connection Broker service manages user connections to virtual desktops and remote apps. The Connection Broker provides load balancing and reconnection to existing sessions.
- Diagnostics: Remote Desktop Diagnostics is an event-based aggregator that marks each user or administrator action on the Azure Virtual Desktop deployment as a success or failure. Administrators can query the event aggregation to identify failing components.
- Extensibility components: Azure Virtual Desktop includes several extensibility components. You can manage Azure Virtual Desktop using Windows PowerShell or with the provided REST APIs, which also enable support from third-party tools



- Azure Virtual Network: Connect an Azure Virtual Desktop to an on-premises network using a VPN or Azure ExpressRoute.
- Azure AD: Azure Virtual Desktop uses Azure AD for identity and access management.
- AD DS: Azure Virtual Desktop VMs must domain-join an AD DS service, and the AD DS must be in sync with Azure AD to associate users between the two services.
- Azure Virtual Desktop session hosts: A host pool can run the operating systems.

Components you manage
Customers manage these components of Azure Virtual Desktop solutions:

Azure Virtual Network: Azure Virtual Network lets Azure resources like VMs communicate privately with each other and with the internet. By connecting Azure Virtual Desktop host pools to an Active Directory domain, you can define network topology to access virtual desktops and virtual apps from the intranet or internet, based on organizational policy. You can connect an Azure Virtual Desktop to an on-premises network using a virtual private network (VPN), or use Azure ExpressRoute to extend the on-premises network into the Azure cloud over a private connection.

- Microsoft Entra ID: Azure Virtual Desktop uses Microsoft Entra ID for identity and access management. Microsoft Entra integration applies Microsoft Entra security features like conditional access, multifactor authentication, and the Intelligent Security Graph, and helps maintain app compatibility in domain-joined VMs.
- AD DS: Azure Virtual Desktop VMs must domain-join an AD DS service. You can use Microsoft Entra Connect to associate AD DS with Microsoft Entra ID.
- Azure Virtual Desktop session hosts: A host pool can run the following operating systems:
  - Windows 10 Enterprise and Windows 11 Enterprise
  - Windows 10 Enterprise Multi-session
  - Windows Server 2012 R2 and above
  - Custom Windows system images with pre-loaded apps, group policies, or other customizations

You can choose VM sizes, including GPU-enabled VMs. Each session host has an Azure Virtual Desktop host agent, which registers the VM as part of the Azure Virtual Desktop workspace or tenant. Each host pool can have one or more app groups, which are collections of remote applications or desktop sessions that users can access.

- Azure Virtual Desktop workspace: The Azure Virtual Desktop workspace or tenant is a management construct to manage and publish host pool resources.

6. Benefits of Azure Virtual Desktop:

1. Flexibility and Scalability:

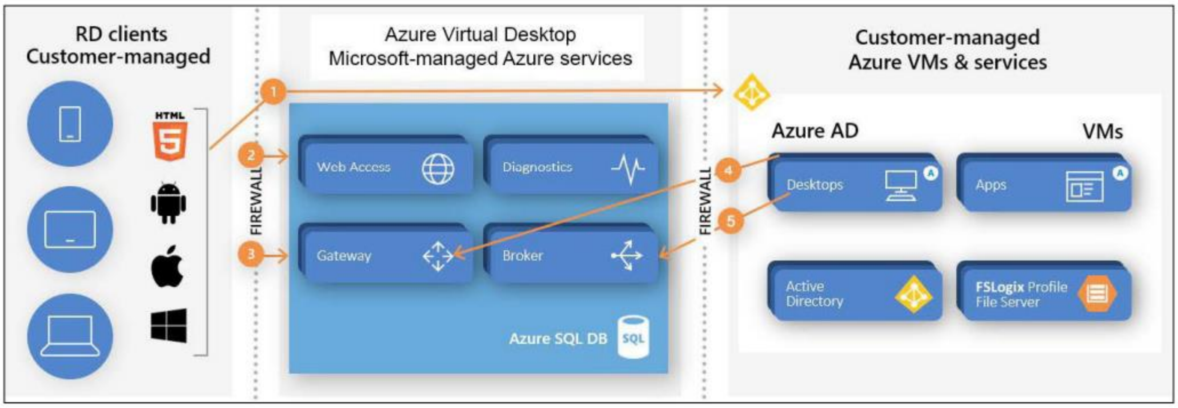
AVD allows organizations to scale their virtual desktop infrastructure based on demand. Whether you need to add new users, deploy additional applications, or expand resources, AVD provides flexibility to adapt to changing business requirements.

2. Resource Optimization:

With AVD, resources are allocated dynamically, ensuring efficient utilization. Users can access virtual desktops and applications from various devices, and administrators can adjust resources to match specific workloads, enhancing overall resource optimization.

3. Improve your security posture

• Azure Virtual Desktop includes many features that help keep applications and data secure. For example, the data and applications are separated from the local hardware and are run on the remote server, reducing the risk of confidential data being left on a personal device.
• Azure Virtual Desktop also isolates user sessions in multi-session environments. This provides better security than a VPN because it doesn't give users access to a full subnet.
• Azure Virtual Desktop also improves security by using reverse connect (RC) technology, which is a more secure connection type as compared to the traditional Remote Desktop Protocol (RDP). Session host VMs use secure outbound connectivity to the Azure Virtual Desktop infrastructure over the HTTPS connection.



The connection flow process of Azure Virtual Desktop

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

4. Anywhere Access:

Users can access their virtual desktops and applications from anywhere with an internet connection. This enables remote and mobile work scenarios, providing flexibility for employees and contributing to business continuity during unforeseen events or disruptions.

5. Integrated with Microsoft 365:

AVD integrates seamlessly with Microsoft 365 applications, providing a familiar environment for users. This integration ensures compatibility with popular productivity tools and simplifies the user experience.

6. Cost Savings:

AVD operates on a pay-as-you-go model, allowing organizations to pay for the resources they use. This can result in cost savings compared to traditional on-premises infrastructure, as it eliminates the need for upfront hardware investments and allows for more efficient resource allocation.

7. Support for Legacy Applications:

AVD enables organizations to run legacy applications on modern operating systems. This is particularly beneficial for businesses that rely on older software, as AVD provides a platform to host and deliver these applications without the need for legacy hardware.

8. Centralized Management:

AVD offers centralized management through the Azure portal, allowing administrators to monitor, configure, and update virtual desktops and applications from a single interface. This simplifies the management tasks associated with maintaining a virtualized environment.

9. Automated Updates and Patch Management:

AVD streamlines the process of updates and patch management. Microsoft takes care of maintaining the underlying infrastructure, ensuring that the virtual desktops are running on the latest software versions and security patches.

10. Disaster Recovery and Business Continuity:

AVD contributes to disaster recovery and business continuity strategies. By hosting desktops and applications in the cloud, organizations can quickly recover from disruptions, and users can access their virtual desktops from alternative locations in the event of a disaster.