azure-virtual-desktop-architecture

Thursday, December 22, 2022 10:11 AM

Components microsoftmanages:

- Web access(accessing desktops,remote apps through browser)
- Gateway(connects remote users with azure cirtual desktop apps,desktops from any intenret connected device that can run azure virtual desktop client
- Connection broker(load balancing , reconnection to existing sesions)
- Diagnostics(event based aggregator that marks each user or adminsitrator action on AVD deployment as success or failure,can query)
- Extensibility components(manage using powershell,REST api,thrid party tools)

Components we manage:

- Azure VNET(virtual network)
- Azure AD
- AD DS
- Azure virtual desktop session hosts(host pool(windows 7,10,server etc..)
- Azure Virtual Desktop workspace: The Azure Virtual Desktop workspace or tenant is a management construct to manage and publish host pool resources.

Host pools are collection of one or more vm's withing AVD env

Each host pool can contain an app group that users can interact with as they would on a physical desktop.

Users obtain access to host pools by being allocated to a host pool using an assigned Application Group:

- Pooled((multi session)many users sharing a VM,(can also use custom image))
- Personal(dedicated VM for each user)

Updating virtual desktop desktops:

- Microsoft endpoint configuration manager
- Windowsupdate for business
- Azure update for business
- Azure log analaytics
- Deploy a new image to session hosts every month for latest window updates

Limitations:

- 200 app groups
- 50 app per app group
- 5000 vms per subscription

Architect your Azure Virtual Desktop solution to realize cost savings. Here are five different options to help manage costs for enterprises:

- Windows 10 multi-session: By delivering a multi-session desktop experience for users that have identical compute requirements, you can let more users log onto a single VM at once, resulting in considerable cost savings.
- Azure Hybrid Benefit: If you have Software Assurance, you can use Azure Hybrid Benefit for Windows Server to save on the cost of your Azure infrastructure.
- Azure Reserved Instances: You can prepay for your VM usage and save money. Combine Azure Reserved Instances with Azure Hybrid Benefit for up to 80 percent savings over list prices.
- Session host load-balancing: When setting up session hosts, Breadth-first is the standard

default mode, which spreads users randomly across session hosts. Depth-first mode fills up a session host server with the maximum number of users before it moves on to the next session host. You can adjust this setting for maximum cost benefits.

Use the Azure Virtual Desktop Experience Estimator to determine the connection round-trip time (RTT) from your current location, through the Azure Virtual Desktop service, to the Azure region where you deploy virtual machines.

You can access Azure Virtual Desktop resources on devices with Windows 10, Windows 10 IoT Enterprise, and Windows 7 using the Windows Desktop client.

The client doesn't support Window 8 or Windows 8.1.
Once installed, the client can be launched from the Start menu by searching for Remote Desktop.

Azure Virtual Desktop doesn't support the RemoteApp and Desktop Connections (RADC) client or the Remote Desktop Connection (MSTSC) client.

Session host<=> a VM

Breadth-first load balancing allows you to evenly distribute user sessions across the session hosts in a host pool.
Depth-first load balancing allows you to saturate a session host with user sessions in a host pool. Once the first session reaches its session limit threshold, the load balancer directs any new user connections to the next session host in the host pool until it reaches its limit, and so on.

Each host pool can only configure one type of load-balancing specific to it. However, both load-balancing methods share the following behaviors no matter which host pool they're in:

If a user already has a session in the host pool and is reconnecting to that session, the load balancer will successfully redirect them to the session host with their existing session. This behavior applies even if that session host's AllowNewConnections property is set to False.
If a user doesn't already have a session in the host pool, then the load balancer won't consider session hosts whose AllowNewConnections property is set to False during load balancing.

Azure AD and Azure resources are secured independently from one another.

Azure AD role assignments do not grant access to Azure resources, and Azure role assignments do not grant access to Azure AD. However, if you are a Global Administrator in Azure AD, you can assign yourself access to all Azure subscriptions and management groups in your directory. Use this capability if you don't have access to Azure subscription resources. For example, for virtual machines or storage accounts, and you want to use your Global Administrator privilege to gain access to those resources.

We enable the elavted access in the properties of the directory and toggling access check to yes

Azure Virtual Desktop stores global metadata information like tenant names, host pool names, app group names, and user principal names in a datacenter. Whenever a customer creates a service object, they must enter a location for the service object. The location they enter determines where the metadata for the object will be stored. The customer will choose an Azure region and the metadata will be stored in the related geography.

There is currently support for storing metadata in the following geographies:

United States (US) (Generally available)
Europe (EU) (Public preview)

Virtual machine host
Virtual machines in Azure provide information for the virtual machine host as described in Monitoring data.

Platform metrics - Numerical values that are automatically collected at regular intervals and describe some aspect of a resource at a particular time. Platform metrics are collected for the virtual machine host, but you require the diagnostics extension to collect metrics for the guest operating system.
Activity log - Provides insight for each Azure resource in the subscription from the outside (the management plane). For a virtual machine, such information as when it was started and any configuration changes.
Guest operating system
To collect data from the guest operating system of a virtual machine, and agent running on each virtual machine sends data to Azure Monitor. Agents are available for Azure Monitor with each collecting different data and writing data to different locations.

Log Analytics agent - Available for virtual machines in Azure, other cloud environments, and on-premises. Collects data to Azure Monitor Logs. Supports Azure Monitor for VMs and monitoring solutions. The same agent used for System Center Operations Manager.
Dependency agent - Collects data about the processes running on the virtual machine and their dependencies. Relies on the Log Analytics agent to transmit data into Azure and supports Azure Monitor for VMs, Service Map, and Wire Data 2.0 solutions.
Azure Diagnostic extension - Available for Azure Monitor virtual machines only. Can collect data to multiple locations but primarily used to collect guest performance data into Azure Monitor Metrics for Windows virtual machines.
Telegraf agent - Collect performance data from Linux VMs into Azure Monitor Metrics.

You can access Windows 10 Enterprise and Windows 7 Enterprise desktops and apps at no extra cost if you have an eligible Windows or Microsoft 365 license.

Windows Server Remote Desktop Service is available at no cost if you have an eligible Microsoft Remote Desktop Services (RDS) Client Access License (CAL).

Reserved Virtual Machine Instances are flexible and can be exchanged or returned.

Single session(personal desktop),multi-session desktop are two scenarios

Azure Virtual Desktop offers FSLogix profile containers as the recommended user profile solution. FSLogix is designed to roam profiles in remote computing environments, such as Azure Virtual Desktop.

When a user signs in the container is dynamically attached to the environment using a natively supported Virtual Hard Disk (VHD) and a Hyper-V Virtual Hard Disk (VHDX). The user profile is immediately available and appears exactly like a native user profile.

Azure file,Azure Netapp files,storage spaces(self0manaaged(low capacity per disk)) direct can be used for user profile storage

Get the list of managed resources you can access, such as apps and desktops, by subscribing to the Workspace your admin provided you. When you subscribe, the resources become available on your local PC. The Windows Desktop client currently supports resources published from Azure Virtual Desktop.

(REMOTE DESKTOP CLIENT)

Subscribe to a Workspace

There are methods you can subscribe to a Workspace. The client can try to discover the resources available to you from your work or school account or you can directly specify the URL where your resources are for cases where the client is unable to find them. Once you've subscribed to a Workspace, you can launch resources with one of the following methods:

- Go to the Connection Center and double-click a resource to launch it.
- You can also go to the Start menu and look for a folder with the Workspace name or enter the resource name in the search bar.

Subscribe with a user account

1. From the main page of the client, tap Subscribe.
2. Sign in with your user account when prompted.
3. The resources will appear in the Connection Center grouped by Workspace.

Subscribe with URL

1. From the main page of the client, tap Subscribe with URL.
2. Enter the Workspace URL or your email address:
   Note
   To use email, enter your email address. This tells the client to search for a URL associated with your email address if your admin has setup email discovery.
3. Tap Next.
4. Sign in with your user account when prompted.
5. The resources will appear in the Connection Center grouped by Workspace.

(REMOTE DESKTOP WEB CLIENT)

Once your admin sets up your remote resources all you need are your domain, user name, password, the URL your admin sent you, and web browser.
(NO MOBILE OS SUPPORT)

For the web client, you'll need a PC running Windows, macOS, ChromeOS, or Linux.
A modern browser like Microsoft Edge, Internet Explorer 11, Google Chrome, Safari, or Mozilla Firefox (v55.0 and later).
The URL your admin sent you.

In order to deploy to multiple devices or multiple users then we can run cli silently through group policies or microsoft endpoint configuration manager

Insider group(early version),public groups(stable) are groups where we can confgure the client

For hybrid identities we can use azure ad for inprem,cloud connectivity(authentcateautorize)
(AD CONNECT)

implement-manage-networking-azure-virtual-desktop

Thursday, December 22, 2022 12:58 PM

Five-step connection flow for AVD:

1. When authenticated in Azure Active Directory, a token is returned to the Remote Desktop Services client.
2. The gateway checks the token with the connection broker.
3. The broker queries the Azure SQL database for resources assigned to the user.
4. The gateway and the broker select the session host for the connected client.
5. The session host creates a reverse connection to the client by using the Azure Virtual Desktop gateway.

Client connection sequence described below:

1. Using supported Azure Virtual Desktop client user subscribes to the Azure Virtual Desktop Workspace.
2. Azure Active Directory authenticates the user and returns the token used to enumerate resources available to a user.
3. Client passes token to the Azure Virtual Desktop feed subscription service.
4. Azure Virtual Desktop feed subscription service validates the token.
5. Azure Virtual Desktop feed subscription service passes the list of available desktops and RemoteApps back to the client with a digitally signed connection.
6. Client stores the connection configuration for each available resource in a set of rdp files.
7. When a user selects the resource to connect, the client uses the associated rdp file and establishes the secure TLS 1.2 connection to the closest Azure Virtual Desktop gateway instance.
8. Azure Virtual Desktop gateway validates the request and asks the Azure Virtual Desktop broker to orchestrate the connection.
9. Azure Virtual Desktop broker identifies the session host and uses the previously established persistent communication channel to initialize the connection.
10. Remote Desktop stack initiates the TLS 1.2 connection to the same Azure Virtual Desktop gateway instance as used by the client..
11. After both client and session host connected to the gateway, the gateway starts relaying the raw data between both endpoints. Establishing the base reverse connect transport for the RDP.
12. After the base transport is set, the client starts the RDP handshake.

Connection security is through TLS with RDP

RDP Shortpath for managed networks is a feature of Azure Virtual Desktop that establishes a direct UDP-based transport between Remote Desktop Client and Session host. RDP uses this transport to deliver Remote Desktop and RemoteApp while offering better reliability and consistent latency.

- RDP Shortpath transport is based on the Universal Rate Control Protocol (URCP). URCP enhances UDP with active monitoring of the network conditions and provides fair and full link utilization. URCP operates at low delay and loss levels as needed by Remote Desktop.
- RDP Shortpath establishes the direct connectivity between the Remote Desktop client and the session host. Direct connectivity reduces dependency on the Azure Virtual Desktop gateways, improves the connection's reliability, and increases available bandwidth for each user session.
- The removal of extra relay reduces round-trip time, which improves user experience with latency-sensitive applications and input methods.
- RDP Shortpath brings support for configuring Quality of Service (QoS) priority for RDP

connections through Differentiated Services Code Point (DSCP) marks.

- RDP Shortpath transport allows limiting outbound network traffic by specifying a throttle rate for each session.

Create a network rule collection add the following rules:
Allow DNS. Traffic from your AD DS private IP address to * for TCP and UDP ports 53.
Allow KMS. Traffic from your Azure Virtual Desktop virtual machines to Windows Activation Service TCP port 1688.

We can also configure bastion host vm for connecting to the vm's securely and when connecitng to the vm specify the bastion host tyoe and the rdp sesion willl happen in the browser itself

Azure Network Watcher(ip flow,packet capture,next hop,security group vieww) provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network.

Network Watcher is designed to monitor and repair the network health of IaaS (Infrastructure-as-a-Service) including virtual machines, virtual networks, application gateways, and load balancers.

Connection Monitor 2.0 monitors for availability, latency, and network topology changes between the virtual machine and the endpoint.

If an endpoint becomes unreachable, Connection Monitor informs you. Potential issues are DNS name resolution problems, CPU, memory, or firewall within the operating system of a virtual machine.

We can enabel the rdp shotpth (quality of service)managed netowrk in the windows by going to services

```
New-NetFirewallRule -DisplayName 'Remote Desktop - Shortpath (UDP-In)'  -Action Allow -Description 'Inbound rule for the Remote Desktop service to allow RDP traffic. [UDP 3390]' -Group '@FirewallAPI.dll,-28752' -Name 'RemoteDesktop-UserMode-In-Shortpath-UDP'  -PolicyStore PersistentStore -Profile Domain, Private -Service TermService -Protocol udp -LocalPort 3390 -Program '%SystemRoot%\system32\svchost.exe' -Enabled:True
```

Azure Virtual Desktop service recommends FSLogix profile containers as a user profile solution. FSLogix is designed to roam profiles in remote computing environments, such as Azure Virtual Desktop. It stores a complete user profile in a single container. At sign-in, this container is dynamically attached to the computing environment using natively supported Virtual Hard Disk (VHD) and Hyper-V Virtual Hard disk (VHDX).

The VHD or VHDX files are stored to this location and attached to users the next time they sign in.

We can create a azure file share storage account and for the file share we can give the premium or standard on eiwth necessary quotas on storage and tiers(transaction optimized,hot,cold)

We can attach disk to the vm that is running the apps

Creation of AVD host poolowershell:

```
New-AzWvdHostPool -ResourceGroupName <resourcegroupname> -Name <hostpoolname> -WorkspaceName <workspacename> -HostPoolType <Pooled|Personal> -LoadBalancerType <BreadthFirst|DepthFirst|Persistent> -Location <region> -DesktopAppGroupName <appgroupname>
```

```
New-AzWvdRegistrationInfo -ResourceGroupName <resourcegroupname> -HostPoolName <hostpoolname> -ExpirationTime $((get-date).ToUniversalTime().AddDays(1).ToString('yyyy-MM-ddTHH:mm:ss.fffffffZ'))
```

```
New-AzWvdRegistrationInfo -ResourceGroupName <resourcegroupname> -HostPoolName <hostpoolname> -ExpirationTime $((get-date).ToUniversalTime().AddHours(2).ToString('yyyy-MM-ddTHH:mm:ss.fffffffZ'))
```

```
New-AzRoleAssignment -SignInName <userupn> -RoleDefinitionName "Desktop Virtualization User" -ResourceName <hostpoolname+"-DAG"> -ResourceGroupName <resourcegroupname> -ResourceType 'Microsoft.DesktopVirtualization/applicationGroups'
```

```
$token = Get-AzWvdRegistrationInfo -ResourceGroupName <resourcegroupname> -HostPoolName <hostpoolname>
```

Preparing the vm's for ACD agent installations

- Domain join the virtual machine(connect to it and in the control panel annd change the computer name to the domain of AD domain and authenticate with the account that has sufficient privelegfes)
- Install the remote desktop session host role

Register the vm's to host pool

- Downlaod the agent inside the each vm and run it (https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWrmXv)
- When asking for a token specify the one we got from the cmdlet(Get-AzWvdRegistrationInfo)
- Donwnload and install the AVD agent bootloader(https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWrxrH)
- Run it

Assignment type for host pool:

- automatic

To automatically assign users, first assign them to the personal desktop host pool so that they can view the desktop in their feed.

~~~~
Update-AzWvdHostPool -ResourceGroupName <resourcegroupname> -Name <hostpoolname> -PersonalDesktopAssignmentType Automatic```
~~~~

```
New-AzRoleAssignment -SignInName <userupn> -RoleDefinitionName "Desktop Virtualization User" -ResourceName <appgroupname> -ResourceGroupName <resourcegroupname> -ResourceType 'Microsoft.DesktopVirtualization/applicationGroups'
```

- Direct

you must assign the user to both the personal desktop host pool and a specific session host before they can connect to their personal desktop. If the user is only assigned to a host pool without a session host assignment, they won't be able to access resources.

```
Update-AzWvdHostPool -ResourceGroupName <resourcegroupname> -Name <hostpoolname> -PersonalDesktopAssignmentType Direct
```

```
New-AzRoleAssignment -SignInName <userupn> -RoleDefinitionName "Desktop Virtualization
```

```
User" -ResourceName <appgroupname> -ResourceGroupName <resourcegroupname> -
ResourceType 'Microsoft.DesktopVirtualization/applicationGroups'
```

```
Update-AzWvdSessionHost -HostPoolName <hostpoolname> -Name <sessionhostname> -
ResourceGroupName <resourcegroupname> -AssignedUser <userupn>
```

For directly assinging users to session host we can go to app groups of the host pool and assignments > add > assign VM

We can edit rdp propertiesd of a host pool

Azure Virtual Desktop licensing allows you to apply a license to any Windows or Windows Server virtual machine that is registered as a session host in a host pool receiving user connections.

You can create a host pool and its session host virtual machines using the Azure Marketplace offering. Virtual machines created this way automatically have the license applied.
You can create a host pool and its session host virtual machines using the GitHub Azure Resource Manager template. Virtual machines created this way automatically have the license applied.
You can apply a license to an existing session host virtual machine. Follow the instructions in Create a host pool with PowerShell to create a host pool and associated virtual machines.

For creating a vm use managed images available in azure or download the image and open hyper-v manager and customize it or changing an existing aVHD to a fixed disk or if you have the masteri image then convert it into a fixed image and upload it to blob container and create image swith it

Inside the vm we can apply local grouppolicy to disable automatic updates,specify start layour,setup time zone redirection,disable storage sense etc..

Azure Compute Gallery as a repository for images,app stuffs,etc for sharing across all within an organization
We can share directly or through rbac or publicly share(community gallery)

We can configure languagaes,create images using vm iage builder,install microsoft 365 apps in it

We can enable screen capture protection by copying the policy template file to a policydefinitions folder and in the computer configuration>>AVD> enable screen captuere protection along with rdp shortpath will be h=there

manage-user-environments-apps

Thursday, December 22, 2022 3:08 PM

Install fslogix in each vm to activate or something

Profile Container is used to redirect the full user profile. Profile Container is used in non-persistent, virtual environments, such as Virtual Desktops. When using Profile Container, the entire user profile is included in the profile container except for data that is excluded using the redirections.xml.

Office Container is implemented with another profile solution, and is designed to improve the performance of Microsoft Office in non-persistent environments. As opposed to Profile Container, Office Container redirects only the local user files for Microsoft Office. When configuring Office Container, each Office component is independently included based on the selected settings to include data for specific office components.

Cloud Cache is an optional add-on to Profile Container and Office Container.

Application Masking manages access to Applications, Fonts, and other items based on criteria. The Application Rules Editor is used to Describe the item, such as application, to be managed.

Configure netapp files with capacity pools

Fslogix supports 4 rule types:

- Hiding rule
- Redirect rule
- App container rule
- Specify value rule

Can configure user policies using microsoft endpoint manager

You run msrdcw.exe to remove your user data, restore default settings and unsubscribe from all Workspaces.

MSIX is a Windows app package format that provides a modern packaging experience to all Windows apps. The MSIX package format preserves the functionality of existing app packages and/or installs files in addition to enabling new, modern packaging and deployment features to Win32, WPF, and Windows Forms apps.

MSIX app attach is a way to deliver MSIX applications to both physical and virtual machines. However, MSIX app attach is different from regular MSIX because it's made especially for Azure Virtual Desktop. This unit will describe what MSIX app attach is and what it can do for you.

Configure the FSLogix agent with a path to the secondary location in the main region. Once the primary location shuts down, the FLogix agent will replicate as part of the VM Azure Site Recovery replication. Once the replicated VMs are ready, the agent will automatically attempt to path to the secondary region.

Run the Qwinsta command for finding the session name in a multi-session virtual machine (VM) host session. Additionally, for a session hosted on a virtual machine supporting virtual Graphics Processing Units (vGPU).

Configure a Group Policy Object (GPO) and set the LimitSecondsToForceLogOffUser parameter to zero. This allows the session configuration setting in specified group policies to handle signing off user sessions.

The scaling tool in Azure Automation account provides start and stop based on Peak and Off-Peak business hours.

The scaling tool uses a combination of an Azure Automation account, a PowerShell runbook, a webhook, and the Azure Logic App to function. When the tool runs, Azure Logic App calls a webhook to start the Azure Automation runbook. The runbook then creates a job.