AVD and VDS v5.4 Prerequisites

Virtual Desktop Service

NetApp
June 09, 2021

Table of Contents

AVD and VDS v5.4 Prerequisites

AVD and VDS requirements and notes

This document describes the required elements for deploying Azure Virtual Desktop (AVD) using NetApp Virtual Desktop Service (VDS). The “Quick Checklist” provides a brief list of required components and pre-deployment steps to take to ensure an efficient deployment. The rest of the guide provides greater detail for each element, depending on the configuration choices that are made.

Quick checklist

Azure requirements

- Azure AD Tenant
- Microsoft 365 Licensing to support AVD
- Azure Subscription
- Available Azure Quota for Azure virtual machines
- Azure Admin Account with Global Admin and Subscription Ownership Roles
- Domain admin account with 'Enterprise Admin' role for AD Connect setup

Pre-deployment information

- Determine total number of users
- Determine Azure Region
- Determine Active Directory Type
- Determine Storage Type
- Identify session host VM image or requirements
- Assess existing Azure and on-premises networking configuration

VDS deployment detailed requirements

End user connection requirements

The following Remote Desktop clients support Azure Virtual Desktop:

- Windows Desktop
- Web
- macOS
- iOS
- IGEL Think Client (Linux)
- Android (Preview)

Azure Virtual Desktop does not support the RemoteApp and Desktop Connections (RADC) client or the Remote Desktop Connection (MSTSC) client.

Azure Virtual Desktop does not currently support the Remote Desktop client from the Windows Store. Support for this client will be added in a future release.

The Remote Desktop clients must have access to the following URLs:

Address	Outbound TCP Port	Purpose	Client(s)
*.AVD.microsoft.com	443	Service traffic	All
*.servicebus.windows.net 443 Troubleshooting data	All	go.microsoft.com	443
Microsoft FWLinks	All	aka.ms	443
Microsoft URL shortener	All	docs.microsoft.com	443
Documentation	All	privacy.microsoft.com	443
Privacy statement	All	query.prod.cms.rt.microsoft.com	443

Opening these URLs is essential for a reliable client experience. Blocking access to these URLs is unsupported and will affect service functionality. These URLs only correspond to the client sites and resources, and do not include URLs for other services like Azure Active Directory.

VDS setup wizard starting point

The VDS setup wizard can handle much of the prerequisite setup required for a successful AVD deployment. The setup wizard (https://cwasetup.cloudworkspace.com) either creates or uses the following components.

Azure tenant

Required: An Azure tenant and Azure Active Directory

AVD activation in Azure is a tenant-wide setting. VDS supports running one AVD instance per tenant.

Azure subscription

Required: An Azure subscription (note the subscription ID that you want to use)

All the deployed Azure resources should be setup in one dedicated subscription. This makes cost tracking for AVD much easier and simplifies the deployment process.
NOTE: Azure free trials are not supported as they do not have enough credits to deploy a functional AVD deployment.

Azure core quota

Enough quota for the VM families you will use - specifically at least 10 cores of the Ds v3 family for the initial platform deployment (as few as 2 cores can be used, but 10 covers every initial deployment possibility).

Azure admin account

Required: An Azure global administrator account.

The VDS setup wizard requests that the Azure admin grant delegated permissions to the VDS service principal

and install the VDS Azure Enterprise application. The admin must have the following Azure roles assigned:

- Global Administrator on the tenant
- Owner role on the subscription

VM image

Required: An Azure image that supports multi-session Windows 10.

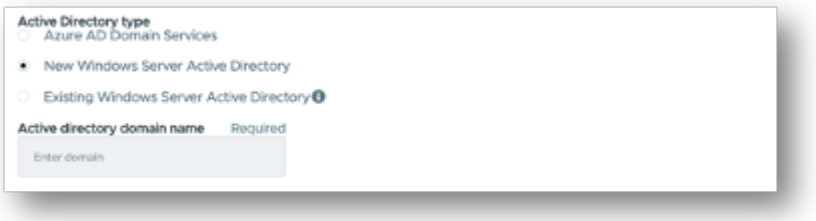
The Azure Marketplace provides the most recent versions of their base Windows 10 image and all Azure subscriptions have access to those automatically. If you want to use a different image or a custom image, want the VDS team to provide advice about creating or modifying other images or have general questions about Azure images let us know and we can schedule a conversation.

Active Directory

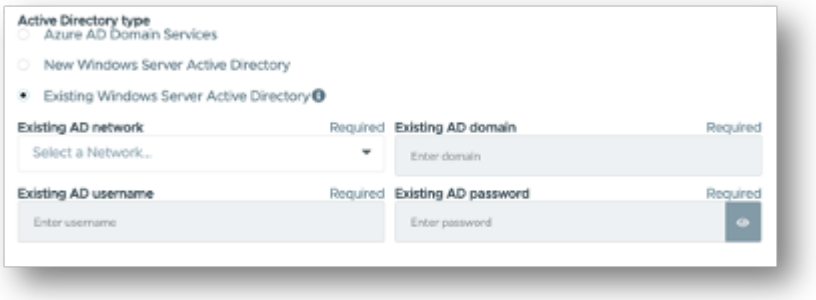
AVD requires that the user identity be a part of Azure AD and that the VMs are joined to an Active Directory domain that is synced with that same Azure AD instance. VMs cannot be attached directly to the Azure AD instance so a domain controller needs to be configured and in-sync with Azure AD.

These supported options include:

- The automated build of an Active Directory instance within the subscription. The AD instance is typically created by VDS on the VDS control VM (CWMGR1) for Azure Virtual Desktop deployments that use this option. AD Connect must be setup and configured to sync with Azure AD as part of the setup process.



- Integration into an existing Active Directory domain that is accessible from the Azure subscription (typically via Azure VPN or Express Route) and has its user list synced with Azure AD using AD Connect or a 3rd party product.



Storage layer

In AVD the storage strategy is designed so that no persistent user/company data resides on the AVD session VMs. Persistent data for user profiles, user files and folders, and corporate/application data are hosted on one

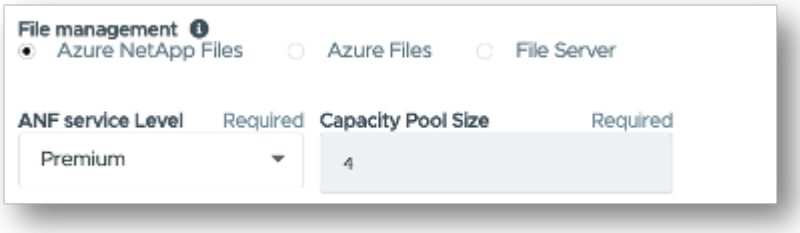
or more data volume(s) hosted on an independent data layer.

FSLogix is a profile containerization technology that solves many user profile issues (like data sprawl and slow logins) by mounting a user profile container (VHD or VHDX format) to the session host at session initialization.

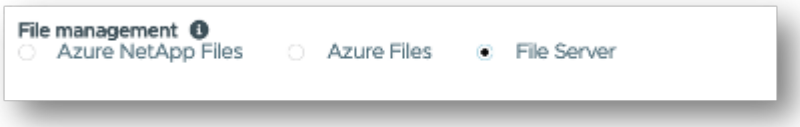
Due to this architecture a data storage function is required. This function must be able to handle the data transfer required each morning/afternoon when a significant portion of the users login/logoff at the same time. Even moderately sized environments can have significant data transfer requirements. The disk performance of the data storage layer is one of the primary end user performance variables and special care must be taken to appropriately size the performance of this storage, not just the amount of storage. Generally, the storage layer should be sized to support 5-15 IOPS per user.

The VDS Setup wizard supports the following configurations:

- Setup and configuration of Azure NetApp Files (ANF) (Recommended). *ANF standard service level supports up to 150 users, while environments of 150-500 users ANF Premium is recommended. For 500+ users ANF Ultra is recommended.*



- Setup and configuration of a File Server VM



Networking

Required: An inventory of all existing network subnets including any subnets visible to the Azure subscription via an Azure Express Route or VPN. The deployment needs to avoid overlapping subnets.

The VDS setup wizard allows you to define the network scope in case there is a range that is required, or must be avoided, as part of the planned integration with existing networks.

Determine an IP range to user during your deployment. Per Azure best practices, only IP addresses in a private range are supported.

Supported choices include the following but default to a /20 range:

- 192.168.0.0 through 192.168.255.255
- 172.16.0.0 through 172.31.255.255
- 10.0.0.0 through 10.255.255.255

CWMGR1

Some of the unique capabilities of VDS such as the cost saving Workload Scheduling and Live Scaling functionality require an administrative presence within the tenant and subscription. Therefore, an administrative VM called CWMGR1 is deployed as part of the VDS setup wizard automation. In addition to VDS automation tasks this VM also holds VDS configuration in a SQL express database, local log files and an advanced configuration utility called DCConfig.

Depending on the selections made in the VDS setup wizard, this VM can be used to host additional functionality including:

- An RDS gateway (only used in RDS deployments)
- An HTML 5 gateway (only used in RDS deployments)
- An RDS license server (only used in RDS deployments)
- A Domain Controller (if chosen)

Decision tree in the Deployment Wizard

As part of the initial deployment a series of questions are answered to customize the settings for the new environment. Below is an outline of the major decisions to be made.

Azure region

Decide which Azure region or regions will host your AVD Virtual Machines. Note that Azure NetApp Files and certain VM families (GPU enabled VMs, for example) have a defined Azure region support list while AVD is available in most regions.

- This link can be used to identify Azure product availability by region

Active Directory type

Decide which Active Directory type you want to use:

- Existing on-prem Active Directory
- Refer to the AVD VDS Components and Permissions document for an explanation of the required permissions and components in both Azure and the local Active Directory environment
- New Azure subscription based Active Directory instance
- Azure Active Directory Domain Services

Data Storage

Decide where the data for user profiles, individual files, and corporate shares will be placed. Choices include:

- Azure NetApp Files
- Azure Files
- Traditional File Server (Azure VM with Managed Disk)

NetApp VDS Deployment Requirements for Existing Components

NetApp VDS Deployment with Existing Active Directory Domain Controllers

This configuration type extends an existing Active Directory domain to support the AVD instance. In this case VDS deploys a limited set of components into the domain to support automated provisioning and management tasks for the AVD components.

This configuration requires:

- An existing Active Directory domain controller that can be accessed by VMs on the Azure VNet, typically via either Azure VPN or Express Route OR a domain controller that has been created in Azure.
- Addition of VDS components and permissions required for VDS management of AVD host pools and data volumes as they are joined to the domain. The AVD VDS Components and Permissions guide defines the required components and permissions and the deployment process requires a Domain user with domain privileges to run the script that will create the needed elements.
- Note that the VDS deployment creates a VNet by default for VDS created VMs. The VNet can be either peered with existing Azure network VNets or the CWMGR1 VM can be moved to an existing VNet with the required subnets pre-defined.

Credentials and domain preparation tool

Administrators must provide a Domain Administrator credential at some point in the deployment process. A temporary Domain Administrator credential can be created, used and deleted later (once the deployment process completes).
Alternatively, customers who require assistance in building out the pre-requisites can leverage the Domain Preparation Tool.

NetApp VDS deployment with existing file system

VDS creates Windows shares that allow user profile, personal folders, and corporate data to be accessed from AVD session VMs. VDS will deploy either the File Server or Azure NetApp File options by default, but if you have an existing file storage component VDS can point the shares to that component once the VDS deployment is complete.

The requirements for using and existing storage component:

- The component must support SMB v3
- The component must be joined to the same Active Directory domain as the AVD session hosts
- The component must be able to expose a UNC path for use in the VDS configuration – one path can be used for all three shares or separate paths may be specified for each. Note that VDS will set user level permissions on these shares so refer to the VDS AVD Components and Permissions document to ensure the appropriate permissions have been granted to the VDS Automation Services.

NetApp VDS deployment with existing Azure AD Domain Services

This configuration requires a process to identify the attributes of the existing Azure Active Directory Domain services instance. Contact your account manager to request a deployment of this type.
NetApp VDS Deployment with Existing AVD deployment
This configuration type assumes that the necessary Azure VNet, Active Directory, and AVD components already exist. The VDS deployment is performed in the same manner as the “NetApp VDS Deployment with

Existing AD” configuration, but adds the following requirements:

- RD Owner role to the AVD Tenant needs to be granted to the VDS Enterprise Applications in the Azure
- AVD Host Pool and AVD Host Pool VMs need to be imported into VDS using the VDS Import function in the VDS Web App. This process collects the AVD host pool and session VM metadata and stores in it VDS so that these elements can be managed by VDS
- AVD User data needs to be imported into the VDS User section using the CRA tool. This process inserts metadata about each user into the VDS control plane so their AVD App Group membership and session information can be managed by VDS

APPENDIX A: VDS control plane URLs and IP addresses

VDS components in the Azure subscription communicate with the VDS global control plane components such as the the VDS Web Application and the VDS API endpoints. For access, the following base URI addresses need to be safelisted for bi-directional access on port 443:

https://docs.netapp.com/us-en/virtual-desktop-service/api.cloudworkspace.com
https://docs.netapp.com/us-en/virtual-desktop-service/autoprodb.database.windows.net
https://docs.netapp.com/us-en/virtual-desktop-service/vdctoolsapi.trafficmanager.net
https://docs.netapp.com/us-en/virtual-desktop-service/cjbootstrap3.cjautomate.net
https://cjdownload3.file.core.windows.net/media

If your access control device can only safe list by IP address, the following list of IP addresses should be safelisted. Note that VDS uses the Azure Traffic Manager service, so this list may change over time:

13.67.190.243
13.67.215.62
13.89.50.122
13.67.227.115
13.67.227.230
13.67.227.227
23.99.136.91
40.122.119.157
40.78.132.166
40.78.129.17
40.122.52.167
40.70.147.2
40.86.99.202
13.68.19.178
13.68.114.184
137.116.69.208
13.68.18.80
13.68.114.115
13.68.114.136
40.70.63.81
52.171.218.239
52.171.223.92
52.171.217.31
52.171.216.93
52.171.220.134
92.242.140.21

APPENDIX B: Microsoft AVD requirements

This Microsoft AVD Requirements section is a summary of AVD requirements from Microsoft. Complete and current AVD requirements can be found here:

https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements

Azure Virtual Desktop session host licensing

Azure Virtual Desktop supports the following operating systems, so make sure you have the appropriate licenses for your users based on the desktop and apps you plan to deploy:

OS	Required license
Windows 10 Enterprise multi-session or Windows 10 Enterprise	Microsoft 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5
Windows 7 Enterprise	Microsoft 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5
Windows Server 2012 R2, 2016, 2019	RDS Client Access License (CAL) with Software Assurance

URL Access for AVD machines

The Azure virtual machines you create for Azure Virtual Desktop must have access to the following URLs:

Address	Outbound TCP Port	Purpose	Service Tag
*.AVD.microsoft.com	443	Service traffic	WindowsVirtualDesktop
mrsglobalsteus2prod.blob.core.windows.net	443	Agent and SXS stack updates	AzureCloud
*.core.windows.net	443	Agent traffic	AzureCloud
*.servicebus.windows.net	443	Agent traffic	AzureCloud
prod.warmpath.msftcloudes.com	443	Agent traffic	AzureCloud
catalogartifact.azureedge.net	443	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Windows activation	Internet
AVDportalstorageblob.blob.core.windows.net	443	Azure portal support	AzureCloud

The following table lists optional URLs that your Azure virtual machines can have access to:

Address	Outbound TCP Port	Purpose	Service Tag
*.microsoftonline.com	443	Authentication to MS Online Services	None

Address	Outbound TCP Port	Purpose	Service Tag
*.events.data.microsoft.com	443	Telemetry Service	None
www.msftconnecttest.com	443	Detects if the OS is connected to the internet	None
*.prod.do.dsp.mp.microsoft.com	443	Windows Update	None
login.windows.net	443	Login to MS Online Services, Office 365	None
*.sfx.ms	443	Updates for OneDrive client software	None
*.digicert.com	443	Certificate revocation check	None

Optimal performance factors

For optimal performance, make sure your network meets the following requirements:

- Round-trip (RTT) latency from the client's network to the Azure region where host pools have been deployed should be less than 150ms.
- Network traffic may flow outside country/region borders when VMs that host desktops and apps connect to the management service.
- To optimize for network performance, we recommend that the session host's VMs are collocated in the same Azure region as the management service.

Supported virtual machine OS images

Azure Virtual Desktop supports the following x64 operating system images:

- Windows 10 Enterprise multi-session, version 1809 or later
- Windows 10 Enterprise, version 1809 or later
- Windows 7 Enterprise
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure Virtual Desktop does not support x86 (32-bit), Windows 10 Enterprise N, or Windows 10 Enterprise KN operating system images. Windows 7 also does not support any VHD or VHDX-based profile solutions hosted on managed Azure Storage due to a sector size limitation.

Available automation and deployment options depend on which OS and version you choose, as shown in the following table:

Operating System	Azure Image Gallery	Manual VM Deployment	ARM Template Integration	Provision Host Pools on Azure Marketplace
Windows 10 multi-session, version 1903	Yes	Yes	Yes	Yes
Windows 10 multi-session, version 1809	Yes	Yes	No	No
Windows 10 Enterprise, version 1903	Yes	Yes	Yes	Yes
Windows 10 Enterprise, version 1809	Yes	Yes	No	No
Windows 7 Enterprise	Yes	Yes	No	No
Windows Server 2019	Yes	Yes	No	No
Windows Server 2016	Yes	Yes	Yes	Yes
Windows Server 2012 R2	Yes	Yes	No	No