VDS Components and Permissions

Virtual Desktop Service

NetApp
June 09, 2021

This PDF was generated from https://docs.netapp.com/us-en/virtual-desktop-service/Deploying.Azure.AVD.vds_v5.4_components_and_permissions.html on September 12, 2021. Always check docs.netapp.com for the latest.

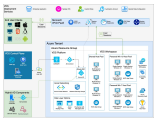
Table of Contents

VDS Components and Permissions

AVD and VDS security entities and services

Azure Virtual Desktop (AVD) requires security accounts and components in both Azure AD and the local Active Directory to perform automated actions. NetApp's Virtual Desktop Service (VDS) creates components and security settings during the deployment process that allow administrators to control the AVD environment. This document describes the relevant VDS accounts, components, and security settings in both environments.

The components and permissions of the deployment automation process are mostly distinct from the components of the final deployed environment. Therefore this article is constructed in two major sections, the deployment automation section and the deployed environment section.



AVD deployment automation components & permissions

VDS deployment leverages multiple Azure and NetApp components and security permissions to implement both deployments and workspaces.

VDS Deployment Services

Enterprise applications

VDS leverages Enterprise Applications and App Registrations in a tenant's Azure AD domain. The Enterprise Applications are the conduit for the calls against the Azure Resource Manager, Azure Graph and (if using the AVD Fall Release) AVD API endpoints from the Azure AD instance security context using the delegated roles and permissions granted to the associated Service Principal. App registrations may be created depending on initialization state of AVD services for the tenant through VDS.

To enable the creation and management of these VMs, VDS creates several supporting components in the Azure Subscription:

Cloud Workspace

This is the initial Enterprise Application admins grant consent to and is used during VDS Setup Wizard's deployment process.

The Cloud Workspace Enterprise Application requests a specific set of permissions during the VDS Setup Process. These permissions are:

- Access Directory as the Signed In User (Delegated)
- Read and Write Directory Data (Delegated)
- Sign In and Read User Profile (Delegated)
- Sign Users in (Delegated)
- View Users' Basic Profile (Delegated)
- Access Azure Service Management as Organization Users (Delegated)

Cloud Workspace API

Handles general management calls for Azure PaaS functions. Examples of Azure PaaS functions are Azure Compute, Azure Backup, Azure Files, etc. This Service Principal requires Owner rights to the target Azure subscription during initial deployment, and Contributor rights for ongoing management (note: Use of Azure Files requires subscription Owner rights in order to set per user permissions on Azure File objects).

The Cloud Workspace API Enterprise Application requests a specific set of permissions during the VDS Setup Process. These permissions are:

- Subscription Contributor (or Subscription Owner if Azure Files is used)
- Azure AD Graph
  - Read and Write All Applications (Application)
  - Manage Apps That This App Creates or Owns (Application)
  - Read and Write Devices (Application)
  - Access the Directory as the Signed In User (Delegated)
  - Read Directory Data (Application)
  - Read Directory Data (Delegated)
  - Read and Write Directory Data (Application)
  - Read and Write Directory Data (Delegated)
  - Read and Write Domains (Application)
  - Read All Groups (Delegated)
  - Read and Write All Groups (Delegated)
  - Read All Hidden Memberships (Application)
  - Read Hidden Memberships (Delegated)
  - Sign In and Read User Profile (Delegated)
  - Read All Users' Full Profiles (Delegated)
  - Read All Users' Basic Profiles (Delegated)
- Azure Service Management
  - Access Azure Service Management as Organization Users (Delegated)

NetApp VDS

NetApp VDS components are used via the VDS control plane to automate the deployment and configuration of AVD roles, services and resources.

Custom role

The Automation Contributor role is created to facilitate deployments via least privileged methodologies. This role allows the CWMGR1 VM to access the Azure automation account.

Automation account

An Automation account is created during deployment and is a required component during the provisioning process. The Automation account contains variables, credentials, modules and Desired State Configurations

and references the Key Vault.

Desired state configuration

This is the method used to build the configuration of CWMGR1 The configuration file is downloaded to the VM and applied via Local Configuration Manager on the VM. Examples of configuration elements include:

- Installing Windows features
- Installing software
- Applying software configurations
- Ensuring the proper permission sets are applied
- Applying the Let's Encrypt certificate
- Ensuring DNS records are correct
- Ensuring that CWMGR1 is joined to the domain

Modules:

- ActiveDirectoryDsc: Desired state configuration resource for deployment and configuration of Active Directory. These resources allow you to configure new domains, child domains and high availability domain controllers, establish cross-domain trusts and manage users, groups and OUs.
- Az.Accounts: A Microsoft provided module used for managing credentials and common configuration elements for Azure modules
- Az.Automation: A Microsoft provided module for Azure Automation commandlets
- Az.Compute:A Microsoft provided module for Azure Compute commandlets
- Az.KeyVault: A Microsoft provided module for Azure Key Vault commandlets
- Az.Resources: A Microsoft provided module for Azure Resource Manager commandlets
- cChoco: Desired state configuration resource for downloading and installing packages using Chocolatey
- cjAz: this NetApp-created module provides automation tools to the Azure automation module
- cjAzACS: this NetApp-created module contains environment automation functions and PowerShell processes that run from within the user context.
- cjAzBuild: this NetApp-created module contains build and maintenance automation and PowerShell processes that run from the system context.
- cNtfsAccessControl: Desired state configuration resource for NTFS access control management
- ComputerManagementDsc: Desired state configuration resource that allow computer management tasks such as joining a domain and scheduling tasks as well as configuring items such as virtual memory, event logs, time zones and power settings.
- cUserRightsAssignment: Desired state configuration resource that allow management of user rights such as logon rights and privileges
- NetworkingDsc: t Desired state configuration resource for networking
- xCertificate: Desired state configuration resource to simplify management of certificates on Windows Server.
- xDnsServer: Desired state configuration resource for configuration and management of Windows Server DNS Server
- xNetworking: Desired state configuration resource related to networking.

- xRemoteDesktopAdmin: this module utilizes a repository that contains desired state configuration resources for configuring remote desktop settings and Windows firewall on a local or remote machine.
- xRemoteDesktopSessionHost: Desired state configuration resource (xRDSessionDeployment, xRDSessionCollection, xRDSessionCollectionConfiguration and xRDRemoteApp) enabling the creation and configuration of a Remote Desktop Session Host (RDSH) instance
- xSmbShare: Desired state configuration resource for configuration and managing an SMB share
- xSystemSecurity: Desired state configuration resource for managing UAC and IE Esc

Azure Virtual Desktop also installs Azure components, including Enterprise Applications and App Registrations for Azure Virtual Desktop and Azure Virtual Desktop Client, the AVD Tenant, AVD Host Pools, AVD App Groups, and AVD registered Virtual Machines. While VDS Automation components manage these components, AVD controls their default configuration and attribute set so refer to the AVD documentation for details.

Hybrid AD components

To facilitate integration with existing AD either on-remises or running in the public cloud, additional components and permissions are required in the existing AD environment.

Domain Controller

The existing domain controller can be integrated into a AVD deployment via AD Connect and/or a site-to-site VPN (or Azure ExpressRoute).

AD Connect

To facilitate successful user authentication through the AVD PaaS-services, AD connect can be used to sync the domain controller with Azure AD.

Security Group

VDS uses a Active Directory Security Group called CW-Infrastructure to contain the permissions required for automating the Active Directory dependent tasks such as domain join and GPO policy attachment.

Service Account

VDS uses an Active Directory service account called CloudworkspaceSVC that is used as the identity for the VDS Windows services and the IIS application service. This account is non-interactive (does not allow RDP login) and is the primary member of the CW-Infrastructure account

VPN or ExpressRoute

A site-to-site VPN or Azure ExpressRoute can be used to directly join Azure VMs with the existing domain. This is an optional configuration available when project requirements dictate it.

Local AD permission delegation

NetApp provides an optional tool that can streamline the hybrid AD process. If using NetApp's optional tool, it must:

- Run on a server OS as opposed to a Workstation OS

- Run on a server that is joined to the domain or is a domain controller
- Have PowerShell 5.0 or greater in place on both the server running the tool (if not run on the Domain Controller) and the Domain Controller
- Be run by a user with Domain Admin privileges OR be run by a user with local administrator permissions and ability to supply a Domain Administrator credential (for use with RunAs)

Whether created manually or applied by NetApp's tool, the permissions required are:

- CW-Infrastructure group
  - The Cloud Workspace Infrastructure (**CW-Infrastructure**) security group is granted Full Control to the Cloud Workspace OU level and all descendent objects
  - <deployment code>.cloudworkspace.app DNS Zone – CW-Infrastructure group granted CreateChild, DeleteChild, ListChildren, ReadProperty, DeleteTree, ExtendedRight, Delete, GenericWrite
  - DNS Server – CW-Infrastructure Group granted ReadProperty, GenericExecute
  - Local admin access for VMs created (CWMGR1, AVD session VMs) (done by group policy on the managed AVD systems)
- CW-CWMGRAccess group This group provides local administrative rights to CWMGR1 on all templates, the single server, new native Active Directory template utilizes the built-in groups Server Operators Remote Desktop Users, and Network Configuration Operators.

AVD environmental components & permissions

Once the deployment automation process is complete the ongoing use and administration of deployments and workspaces a distinct set of components and permissions are required as defined below. Many of the components and permissions from above remain relevant but this section is focused on defining the structure of a deployed.

The components of VDS deployments and workspaces can be organized into several logical categories:

- End user clients
- VDS control plane components
- Microsoft Azure AVD-PaaS components
- VDS platform components
- VDS workspace components in Azure Tenant
- Hybrid AD Components

End user clients

Users can connect to their AVD desktop and/or from a variety of endpoint types. Microsoft has published client applications for Windows, macOS, Android and iOS. Additionally, a web client is available for client-less access.

There are some Linux thin-client vendors who have published endpoint client for AVD. These are listed at https://docs.microsoft.com/en-us/azure/virtual-desktop/linux-overview

VDS control plane components

VDS REST API

VDS is built on fully documented REST APIs so that all actions available in the web app are also available via the API. Documentation for the API is here: https://api.cloudworkspace.com/5.4/swagger/ui/index#

VDS web app

VDS admins can interact the ADS application via the VDS web app. This web portal is at: https://manage.cloudworkspace.com

Control plane database

VDS data and setting are stored in the control plane SQL database, hosted and managed by NetApp.

VDS Comms

Azure tenant components

VDS deployment automation creates a single Azure Resource Group to contain the other AVD components, including VMs, network subnets, network security groups, and either Azure Files containers or Azure NetApp Files capacity pools. Note – the default is a single resource group, but VDS has tools to create resources in additional Resources Groups if desired.

Microsoft Azure AVD-PaaS components

AVD REST API

Microsoft AVD can be managed via API. VDS leveraged these APIs extensively to automate and managed AVD environments. Documentation is at: https://docs.microsoft.com/en-us/rest/api/desktopvirtualization/

Session broker

The broker determines the resources authorized for the user and orchestrates the connection of the user to the gateway.

Azure diagnostics

Azure Diagnostics has been specially built to support AVD deployments.

AVD web client

Microsoft has provided a web client for users to connect to their AVD resources without a locally installed client.

Session gateway

The locally installed RD client connects to the gateway to securely communicate into the AVD environment.

VDS platform components

CWMGR1

CMWGR1 is the VDS control VM for each Deployment. By default, it is created as a Windows 2019 Server VM in the target Azure subscription. See the Local Deployment section for the list of VDS and 3rd party components installed on CWMGR1.

AVD requires the AVD VMs be joined to an Active Directory domain. To facilitate this process and to provide the automation tools for managing the VDS environment several components are installed on the CWMGR1 VM described above and several components are added to the AD instance. The components include:

- **Windows Services** - VDS uses Windows services to perform automation and management actions from within a deployment:
  - **CW Automation Service** is a Windows Service deployed on CWMGR1 in each AVD deployment that performs many of the user-facing automation tasks in the environment. This service runs under the **CloudWorkspaceSVC** AD account.
  - **CW VM Automation Service** is a Windows Service deployed on CWMGR1 in each AVD deployment that performs the virtual machine management functions. This service runs under the **CloudWorkspaceSVC** AD account.
  - **CW Agent Service** is a Windows Service deployed to each virtual machine under VDS management, including CWMGR1. This service runs under the **LocalSystem** context on the virtual machine.
  - **CWManagerX API** is an IIS app pool-based listener installed on CWMGR1 in each AVD deployment. This handles inbound requests from the global control plane and is run under the **CloudWorkspaceSVC** AD account.
- **SQL Server 2017 Express** – VDS creates a SQL Server Express instance on the CWMGR1 VM to manage the metadata generated by the automation components.
- **Internet Information Services (IIS)** – IIS is enabled on CWMGR1 to host the CWManagerX and CWApps IIS application (only if RDS RemoteApp functionality is enabled). VDS requires IIS version 7.5 or greater.
- **HTML5 Portal (Optional)** – VDS installs the Spark Gateway service to provide HTML5 access to the VMs in the Deployment and from the VDS web application. This is a Java based application and can be disabled and removed if this method of access is not desired.
- **RD Gateway (Optional)** – VDS enables the RD Gateway role on CWMGR1 to provide RDP access to RDS Collection based Resource Pools. This role can be disabled/uninstalled if only AVD Reverse Connect access is desired.
- **RD Web (Optional)** – VDS enables the RD Web role and creates the CWApps IIS web application. This role can be disabled if only AVD access is desired.
- **DC Config** – a Windows application used to perform Deployment and VDS Site specific configuration and advanced configuration tasks.
- **Test VDC Tools** – a Windows application that supports direct task execution for Virtual Machine and client level configuration changes used in the rare case where API or Web Application tasks need to be modified for troubleshooting purposes.
- **Let's Encrypt Wildcard Certificate (Optional)** – created and managed by VDS – all VMs that require HTTPS traffic over TLS are updated with the certificate nightly. Renewal is also handled by automated task (certificates are 90 day so renewal starts shortly before). Customer can provide their own wildcard certificate if desired.
  VDS also requires several Active Directory components to support the Automation tasks. The design intent is to utilize a minimum number of AD component and permission additions while still supporting the environment for automated management. These components include:
- **Cloud Workspace Organizational Unit (OU)** – this Organization Unit will act as the primary AD container for the required child components. Permissions for the CW-Infrastructure and Client DHP Access groups will be set at this level and its child components. See Appendix A for sub-OUs that are created in this OU.
- **Cloud Workspace Infrastructure Group (CW-Infrastructure)** is a security group created in the local AD to allow required delegated permissions to be assigned to the VDS service account (**CloudWorkspaceSVC**)

- **Client DHP Access Group (ClientDHPAccess)** is a security group created in the local AD to allow VDS to govern the location in which the company shared, user home and profile data reside.
- **CloudWorkspaceSVC** service account (member of Cloud Workspace Infrastructure Group)
- **DNS zone for <deployment code>.cloudworkspace.app domain** (this domain manages the auto-created DNS names for session host VMs) – created by Deploy configuration.
- **NetApp-specific GPOs** linked to various child OUs of the Cloud Workspace Organizational Unit. These GPOs are:
  - **Cloud Workspace GPO (linked to Cloud Workspace OU)** – Defines access protocols and methods for members of the CW-Infrastructure Group. Also adds the group to the local Administrators Group on AVD session hosts.
  - **Cloud Workspace Firewall GPO** (linked to Dedicated Customers Servers, Remote Desktop and Staging OUs) - creates a policy that ensures and isolates connections to sessions hosts from Platform server(s).
  - **Cloud Workspace RDS** (Dedicated Customers Servers, Remote Desktop and Staging OUs) - policy set limits for session quality, reliability, disconnect timeout limits. For RDS sessions the TS licensing Server Value is defined.
  - **Cloud Workspace Companies** (NOT LINKED by default) – optional GPO to “lock down” a user session/ workspace by preventing access to administrative tools and areas. Can be linked/enabled to provide a restricted activity workspace.

Default Group Policy setting configurations can be provided on request.

VDS workspace components

Data layer

Azure NetApp Files

An Azure NetApp Files Capacity Pool and associated Volume(s) will be created if you choose Azure NetApp Files as the Data Layer option in VDS Setup. The Volume hosts the shared filed storage for user profiles (via FSLogix containers), user personal folders, and the corporate data share folder.

Azure Files

An Azure File Share and its associated Azure Storage Account will be created if you chose Azure Files as the Data Layer option in CWS Setup. The Azure File Share hosts the shared filed storage for user profiles (via FSLogix containers), user personal folders, and the corporate data share folder.

File server with Managed Disk

A Windows Server VM is created with a Managed Disk if you choose File Server as the Data Layer option in VDS Setup. The File Server hosts the shared filed storage for user profiles (via FSLogix containers), user personal folders, and the corporate data share folder.

Azure networking

Azure virtual network

VDS creates an Azure Virtual Network and supporting subnets. VDS requires a separate subnet for CWMGR1, AVD host machines, and Azure domain controllers and peering between the subnets. Note that the AD

controller subnet typically already exists so the VDS deployed subnets will need to be peered with the existing subnet.

Network security groups

A network security group is created to control access to the CWMGR1 VM.

- Tenant: contains IP addresses for use by session host and data VMs
- Services: contains IP addresses for use by PaaS services (Azure NetApp Files, for example)
- Platform: contains IP addresses for use as NetApp platform VMs (CWMGR1 and any gateway servers)
- Directory: contains IP addresses for use as Active Directory VMs

Azure AD

The VDS automation and orchestration deploys virtual machines into a targeted Active Directory instance and then joins the machines to the designated host pool. AVD virtual machines are governed at a computer level by both the AD structure (organizational units, group policy, local computer administrator permissions etc.) and membership in the AVD structure (host pools, workspace app group membership), which are governed by Azure AD entities and permissions. VDS handles this “dual control” environment by using the VDS Enterprise application/Azure Service Principal for AVD actions and the local AD service account (CloudWorkspaceSVC) for local AD and local computer actions.

The specific steps for creating a AVD virtual machine and adding it to the AVD host pool include:

- Create Virtual Machine from Azure template visible to the Azure Subscription associated with AVD (uses Azure Service Principal permissions)
- Check/Configure DNS address for new Virtual Machine using the Azure VNet designated during VDS Deployment (requires local AD permissions (everything delegated to CW-Infrastructure above) Sets the Virtual Machine name using the standard VDS naming scheme ***{companycode}TS{sequencenumber}***. Example: XYZTS3. (Requires local AD permissions (placed into OU structure we have created on-prem (remote desktop/companycode/shared) (same permission/group description as above)
- Places virtual machine in designated Active Directory Organizational Unit (AD) (requires the delegated permissions to the OU structure (designated during manual process above))
- Update internal AD DNS directory with the new machine name/ IP address (requires local AD permissions)
- Join new virtual machine to local AD domain (requires local AD permissions)
- Update VDS local database with new server information (does not require additional permissions)
- Join VM to designated AVD Host Pool (requires AVD Service Principal permissions)
- Install Chocolatey components to the new Virtual Machine (requires local computer administrative privilege for the **CloudWorkspaceSVC** account)
- Install FSLogix components for the AVD instance (Requires local computer administrative permissions on the AVD OU in the local AD)
- Update AD Windows Firewall GPO to allow traffic to the new VM (Requires AD GPO create/modify for policies associated with the AVD OU and its associated virtual machines. Requires AD GPO policy create/modify on the AVD OU in the local AD. Can be turned off post-install if not managing VMs via VDS.)
- Set “Allow New Connections” flag on the new virtual machine (requires Azure Service Principal permissions)

Joining VMs to Azure AD

Virtual machines in the Azure tenant need to be joined to the domain however VMs cannot joining directly to Azure AD. Therefore, VDS deploys the domain controller role in the VDS platform and then we sync that DC with Azure AD using AD Connect. Alternative configuration options include using Azure AD Domain Services (AADDS), syncing to a hybrid DC (a VM on-premises or elsewhere) using AD Connect, or directly joining the VMs to a hybrid DC through a site-to-site VPN or Azure ExpressRoute.

AVD Host pools

Host pools are a collection of one or more identical virtual machines (VMs) within Azure Virtual Desktop environments. Each host pool can contain an app group that users can interact with as they would on a physical desktop.

Session hosts

Within any host pool is one or more identical virtual machines. These user sessions connecting to this host pool are load balanced by the AVD load balancer service.

App groups

By default, the *Desktop users* app group is created at deployment. All users within this app group are presented with a full Windows desktop experience. Additionally app groups can be created to serve streaming-app services.

Log analytics workspace

A Log Analytics workspace is created to store logs from the deployment and DSC processes and from other services. This can be deleted after deployment, but this isn't recommended as it enables other functionality. Logs are retained for 30 days by default, incurring no charges for retention.

Availability sets

An Availability Set is set up as a part of the deployment process to enable separation of shared VMs (shared AVD host pools, RDS resource pools) across fault domains. This can be deleted after deployment if desired but would disable the option to provide additional fault tolerance for shared VMs.

Azure recovery vault

A Recovery Service Vault is created by VDS Automation during deployment. This is currently activated by default, as Azure Backup is applied to CWMGR1 during the deployment process. This can be deactivated and removed if desired but will be recreated if Azure Backup is enabled in the environment.

Azure key vault

An Azure Key Vault is created during the deployment process and is used to store certificates, API keys and credentials that are used by Azure Automation Accounts during deployment.

Appendix A – Default Cloud Workspace organizational unit structure

- Cloud Workspace
  - Cloud Workspace Companies

    - Cloud Workspace Servers
        - Dedicated Customer Servers
        - Infrastructure
- CWMGR Servers
- Gateway Servers
- FTP Servers
- Template VMs
    - Remote Desktop
    - Staging
        - Cloud Workspace Service Accounts
    - Client Service Accounts
    - Infrastructure Service Accounts
        - Cloud Workspace Tech Users
    - Groups
    - Tech 3 Technicians

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.