VDS AND WVD COMPONENTS AND PERMISSIONS

VDS SECURITY ENTITIES AND SERVICES

Windows Virtual Desktop (WVD) requires security accounts and components in both Azure AD and the local Active Directory to perform automated actions. Virtual Desktop Service (VDS) creates components and security settings during the deployment process that allows administrators to control the WVD environment without needing to re-authenticate for each action. This document describes the relevant VDS accounts, components, and security settings in both environments.

AZURE COMPONENTS AND SECURITY SETTINGS

WVD requires that the user session Virtual Machines (VM) be created in an Azure subscription. To enable the creation and management of these VMs, VDS creates several supporting components in the Azure Subscription:

- **Azure AD 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 ARM and WVD API endpoints from the Azure AD instance security context using the delegated rights granted to the associated Service Principal. App registrations may be created depending on initialization state of WVD services for the tenant through VDS:
    - **Cloud Workspace** – initial Enterprise Application used during Cloud Workspace for Azure Deployment process.
    - **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).
    - Cloud Workspace Management – used during WVD initialization process to grant VDS components access to the WVD Tenant and its components.
    - **Cloud Workspace WVD** – handles WVD specific management functions (creating and managing host pools) and is granted RD Owner rights to the WVD tenant object(s) in the WVD control plane when initializing WVD via the WVD consent page.
- **Azure Resource Group** – VDS creates a single Azure Resource Group to contain the other WVD components, including VMs, network subnets, network security groups, and either Azure Files containers or Azure NetApp Files capacity pools.
- **Azure Virtual Network and Subnets** – VDS creates an Azure Virtual Network and supporting subnets. VDS requires a separate subnet for CWMGR1, WVD 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.
- **CWMGR1** – CMWGR1 is the VDS control VM for each Deployment. By default, it is created as a Windows 2016 Server VM in the target Azure subscription. See the Local Deployment section for the list of VDS and 3rd party components installed on CWMGR1.

CONFIDENTIALITY: This document and any analysis, language and proposed concepts or models contained herein remain the exclusive intellectual property of NetApp Corporation ("NetApp"). This document may not be disclosed, reproduced in part or full or otherwise presented to any party but the expressed intended audience and for the expressed purpose without written consent of NetApp.

- **Network Security Group (NSG**) – a network security group is created to control access to the CWMGR1 VM.
- **Azure NetApp Files Capacity Pool (Optional) –** 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 CWA Setup. The Volume hosts the shared filed storage for user profiles (via FSLogix containers), user personal folders, and the corporate data share folder.
- **File Server VM (Optional)** – a Windows Server VM is created with a Managed Disk if you choose File Server as the Data Layer option in CWA 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 File Share (Optional)** – 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.
- **Recovery Service Vault (Optional)** – a Recovery Service Vault is created by VDS Automation if you choose to use Azure Backup in the Deployment.

Note: Conditional Access policies and Multi Factor Authentication (MFA) will prevent an account that has Global Administrator permissions that is created (and subsequently deleted) during the deployment automation from fulfilling its purpose. The functionality of this account is in the process of being converted to the Service Principal.

For the time being, if any Conditional Access or MFA is applied to accounts with the Global Administrator role then VDS requires an exclusion from that policy for a single account - cloudworkpace@<domain>.onmicrosoft.com. This account can also be created ahead of time as long as it is granted the Global Administrator role on the tenant and the Owner role on the subscription. This account will automatically be created after the deployment process, so the exclusion will no longer be relevant and can then be deleted as well.

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

Azure Subscription Delegated Permissions

The Azure Enterprise Applications request a specific set of permissions during the CWA Setup Process. These permissions are:

- **Cloud Workspace Enterprise Application**
    - Access Azure Service Management
    - Access Directory
    - Read and Write Directory Data
    - Read Profile
- **Cloud Workspace API Enterprise Application**
    - Subscription Contributor (or Subscription Owner if Azure Files is used)
    - Azure AD Graph
        - Directory Access As User All (Delegated)

        - User Read (Delegated)
        - User Read All (Delegated)
        - User Read Basic All (Delegated)
    - Azure Service Management
        - User Impersonation (Delegated)
- **Cloud Workspace Management Enterprise Application**
    - Access Azure Service Management
    - Access Directory
    - Read and Write Directory Data
    - Read Profile
- **Windows Virtual Desktop**
        - Tenant Creator (Application)
        - User Impersonation (Delegated)
- **Cloud Workspace WVD Enterprise Application**
    - Azure Service Management
        - User Impersonation (Delegated)
    - Windows Virtual Desktop
        - Tenant Creator (Application)
        - User Impersonation (Delegated)

Local Deployment (Azure Subscription) Components

WVD requires the WVD 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 WVD 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 WVD 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 WVD deployment. This handles inbound requests from the global control plane and is run under the **CloudWorkspaceSVC** AD account.

VDS AND WVD COMPONENTS AND PERMISSIONS

- **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 WVD 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 WVD 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.

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 require 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 B for sub-OUs that are created in this OU.
- **Cloud Workspace Infrastructure Group** (**CW-Infrastructure**) - 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)** - 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** – a 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 VMs and supports the auto-generated Let's Encrypt certificates) – created by Deploy script
- **VDS-specific GPOs** - linked to various child OUs of the Cloud Workspace Organizational Unit. These GPOs are:

- **Cloudworkspace GPO (linked to Cloud Workspace GPO) –** defines access protocols and methods for members of the CW-Infrastructure Group. Also adds the group to the local Administrators Group on WVD Session hosts.
- **Cloud Workspace Firewall GPO (linked to Dedicated Customers Servers, Remote Desktop and Staging OUs) -** creates a connection policy that 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.

Note that the Default Group Policy setting configurations can be provided on request.

LOCAL AD PERMISSION DELEGATION

VDS provides an optional tool that can streamline this process. If using VDS'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 executed by a user with Domain Admin privileges OR be executed 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 VDS's tool, the permissions required and policies linked are:

- Group Policy Creator Group – add CW-Infrastructure as a member
- <data center 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

- Permissions to be delegated to the Cloud Workspace Infrastructure (**CW-Infrastructure**) security group at the Cloud Workspace OU level and below:
  - Child InetOrgPerson Objects (Read, Create, Delete)
  - Child Computer Objects (Read, Create, Delete)
  - Child Group Objects (Read, Create, Delete)
  - Child User Objects (Read, Create, Delete)
  - Child Organizational Units (Read, Create, Delete)
  - Child Organizational Unit Objects (Read, Create, Delete)
  - Descendent Computer Objects (Reset Password)
  - Descendent User Objects (Reset Password)

  - GPO object (Read, Create, Delete, Link)
  - Local admin access for VMs created (CWMGR1, WVD session VMs) (done by group policy on the managed WVD systems)
- Policy adjustments are:
  - Copy the following to the AD policy store as new objects
    - Cloudworkspace
    - Cloud Workspace Companies
    - Cloud Workspace Firewall
    - Cloud Workspace RDS
  - Link the Cloudworkspace policy object to the Cloudworkspace OU
  - Link the Cloudworkspace Firewall policy object to Dedicated Customers Servers, Remote Desktop and Staging OUs
  - Link the Cloudworkspace RDS policy object to Dedicated Customers Servers, Remoted Desktop and Staging OUs

APPENDIX A: WVD VIRTUAL MACHINE CREATION

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

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

- Create Virtual Machine from Azure template visible to the Azure Subscription associated with WVD (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 WVD Host Pool (requires WVD 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 WVD instance (Requires local computer administrative permissions on the WVD 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 WVD OU and its associated virtual machines. Requires AD GPO policy create/modify on the WVD 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)

APPENDIX B – DEFAULT CLOUD WORKSPACE ORGANIZATIONAL UNIT STRUCTURE

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