



Virtual Desktop Service Documentation

Virtual Desktop Service

NetApp
September 12, 2021

This PDF was generated from <https://docs.netapp.com/us-en/virtual-desktop-service/index.html> on September 12, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Virtual Desktop Service Documentation	1
Overview	1
Getting Support	1
Additional resources	1
Deploying with VDS	3
Azure	3
Google	70
Architectural	102
Redirecting Storage Platform	102
Data Migration Considerations	121
Wildcard SSL Certificate Renewal Process	123
AVD Teardown Guide	131
Management	134
Deployments	134
Applications	145
Scripted Events	158
Command Center	163
Resource Optimization	168
User Administration	175
System Administration	198
Troubleshooting	216
Troubleshooting Failed VDS Actions	216
Internet Connection Quality Troubleshooting	221
Enable Desktop Wallpaper for User Sessions	224
Troubleshooting Printing Issues	226
Azure vCPU Core Quota	227
Unlocking User Accounts	230
Troubleshooting Virtual Machine Performance	232
DNS Forwards for Azure ADDS & SSO via O365 identity	243
Troubleshooting Application Issues	249
Reference	251
Release notes	251
End User Requirements	323
VDS Change Environments	331
Script Library Documentation	332
Advanced	358
NetApp VDS v5.4 videos	359
VDS Content on NetApp TV	359
Deploy AVD or RDS Into Azure with NetApp VDS v5.4	359
Create a AVD Host Pool with NetApp VDS v5.4	360
Add and Manage AVD Users and App Groups in Azure with NetApp VDS v5.4	361
Optimize Azure Resource Consumption in VDS 5.4	361
Day to Day Administration of RDS and AVD with NetApp VDS v5.4	362

Update AVD host pool from v1 (Fall 2019) to v2 (Spring 2020)	362
--	-----

Virtual Desktop Service Documentation

Overview

NetApp's Virtual Desktop Service (VDS) solves the complexity of deploying and managing virtual desktops in the public cloud, delivered both as a flexible software service to manage your Virtual Desktop Infrastructure (VDI), or as a fully managed VDI as a Service platform. The Virtual Desktop Service removes the complexity of deploying desktops in the cloud taking the hundreds of tasks that took 2-3 days to deploy into just a few hours.

Virtual Desktop Service Benefits:

- **Reduce Infrastructure Costs**

Our customizable resource scheduling system optimizes infrastructure spending by up to 50%.

- **Reduce Risk**

Deploy desktops into logical workflows per cloud best practices; Such as Microsoft best practice standards for Azure Virtual Desktop (AVD).

- **Custom Automation**

Event driven automation and orchestration engine leveraging your current scripts, making management so easy, general IT administrators can manage your cloud desktops!

- **Multi-Cloud**

Control multiple tenants across AWS, Azure and Google with a single graphical user interface.

- **Flexible Control**

Maximize business flexibility with a single portal to control every layer of your technology stack.

Learn more: <https://cloud.netapp.com/virtual-desktop-service>

Getting Support

Email Support: VDSsupport@netapp.com

Phone Support: 844.645.6789

[VDS Support Portal](#)

Normal support business hours: Monday-Friday, 7:00am-7:00pm Central Time.

- After hours (on-call) support available via phone only.

Additional resources

Cost Calculators

Azure

- <https://manage.vds.netapp.com/azure-cost-estimator>

Google Cloud

- <https://manage.vds.netapp.com/google-cost-estimator>

Downloads

Remote Desktop Services (RDS) Clients

- [VDS RDS client for Windows](#)
- [VDS Web Client](#)
- [Microsoft RD Client](#)

Azure Virtual Desktop (AVD) Clients

- [Microsoft AVD for Windows Client](#)
- [Microsoft AVD Web Client](#)
- [Microsoft AVD for Android Client](#)
- [Microsoft AVD for macOS Client](#)
- [Microsoft AVD for iOS Client](#)

Other Downloads

- [RemoteScan Client](#)
- [VDS RDS Windows Client Designer](#)

Deploying with VDS

Azure

Azure Virtual Desktop

AVD Deployment Guide

Overview

This guide will provide the step by step instructions to create a Azure Virtual Desktop (AVD) deployment utilizing NetApp Virtual Desktop Service (VDS) in Azure.

The guide starts at: <https://cwasetup.cloudworkspace.com/>

This Proof of Concept (POC) guide is designed to help you quickly deploy and configure AVD in your own test Azure Subscription. This guide assumes a green-field deployment into a clean, non-production Azure Active Directory tenant.

Production deployments, especially into existing AD or Azure AD environments are very common however that process is not considered in this POC Guide. Complex POCs and production deployments should be initiated with the NetApp VDS Sales/Services teams and not performed in a self-service fashion.

This POC document will take you thru the entire AVD deployment and provide a brief tour of the major areas of post-deployment configuration available in the VDS platform. Once completed you'll have a fully deployed and functional AVD environment, complete with host pools, app groups and users. Optionally you'll have the option to configure automated application delivery, security groups, file share permissions, Azure Cloud Backup, intelligent cost optimization. VDS deploys a set of best practice settings via GPO. Instructions on how to optionally disable those controls are also included, in the event your POC needs to have no security controls, similar to an unmanaged local device environment.

AVD basics

Azure Virtual Desktop is a comprehensive desktop and app virtualization service that runs in the cloud. Here is a quick list of some of the key features and functionality:

- Platform services including gateways, brokering, licensing, and login and included as a service from Microsoft. This minimized infrastructure requiring hosting and management.
- Azure Active Directory can be leveraged as the identity provider, allowing for the layering of additional Azure security services such as conditional access.
- Users experience single sign-on experience for Microsoft services.
- User sessions connect to the session host via a proprietary reverse-connect technology. This means that no inbound ports need to be open, instead an agent creates and outbound connection to the AVD management plane which in turn connects to the end user device.
- Reverse connect even allows virtual machines to run without being exposed to the public internet enabling isolated workloads even while maintaining remote connectivity.
- AVD includes access to Windows 10 Multi Session, allowing a Windows 10 Enterprise experience with the efficiency of high density user sessions.
- FSLogix profile containerization technology is included, enhancing user session performance, storage efficiency and enhancing the Office experience in non-persistent environments.

- AVD supports full desktop and RemoteApp access. Both persistent or non-persistent, and both dedicated and multi-session experiences.
- Organizations can save on Windows licensing because AVD can leverage "Windows 10 Enterprise E3 Per User" which replaces the need for RDS CALs and significantly reduces the per-hour cost of session host VMs in Azure.

Guide scope

This guide walks you through the deployment of AVD using NetApp VDS technology from the perspective of an Azure and VDS administrator. You bring the Azure tenant and subscription with zero pre-configuration and this guide helps you setup AVD end-to-end.

This guide covers the following steps:

1. Confirm prerequisites of the Azure tenant, Azure subscription and Azure admin account permissions
2. Collect required discovery details
3. Build the Azure environment using the purpose-built VDS for Azure Setup wizard
4. Create the first host pool with a standard Windows 10 EVD image
5. Assigning virtual desktops to Azure AD user(s)
6. Add users to the default app group for delivering the desktop environment to users. Optionally, create additional host pool(s) for delivering RemoteApp services
7. Connect as an end user via client software and/or web client
8. Connect to the platform and client services as local and domain admin
9. Optionally enable VDS' multi-factor authentication for VDS admins & AVD end users
10. Optionally walk through the entire application entitlement workflow including populating the app library, app install automation, app masking by users and security groups
11. Optionally create and manage Active Directory security groups, folder permissions and application entitlement by group.
12. Optionally configure cost optimization technologies including Workload Scheduling and Live Scaling
13. Optionally create, update and Sysprep a virtual machine image for future deployments
14. Optionally configure Azure Cloud Backup
15. Optionally disable default security control group policies

Azure prerequisites

VDS uses native Azure security context to deploy the AVD instance. Before starting the VDS Setup wizard, there are a few Azure prerequisites that need to be established.

During the deployment, service accounts and permissions are granted to VDS via authentication of an existing admin account from within the Azure tenant.

Quick prerequisites checklist

- Azure Tenant with Azure AD instance (can be Microsoft 365 instance)
- Azure Subscription
- Available Azure Quota for Azure virtual machines
- Azure Admin Account with Global Admin and Subscription Ownership Roles



Detailed prerequisites are documented on [this PDF](#)

Azure administrator in Azure AD

This existing Azure admin must be an Azure AD account in the target tenant. Windows Server AD accounts can be deployed with the VDS Setup but additional steps are required to setup a sync with Azure AD (out of scope for this guide)

This can be confirmed by finding the user account in the Azure Management Portal under Users > All Users.

The screenshot shows the Azure Management Portal's 'Users - All users' page. On the left, there's a sidebar with options like 'All users', 'Deleted users', 'Password reset', etc. The main area has a search bar and filters for 'Name or email', 'Search attributes', and 'Show'. A table lists users with columns for Name, User name, User type, and Source. One row for 'Toby vanRoojen' is highlighted with a yellow circle, and this entire row is also circled in red. The details for Toby vanRoojen show the name, user name (admin@...), source (Azure Active Directory), and user type (Member).

Name	User name	User type	Source
Toby vanRoojen	admin@...onmicrosoft.com	Member	Azure Active Directory

Global administrator role

The Azure Administrator must be assigned the Global administrator role in the Azure tenant.

To check your role in Azure AD, follow these steps:

1. Log in to the Azure Portal at <https://portal.azure.com/>
2. Search for and select Azure Active Directory
3. In the next pane to the right, click on the Users option in the Manage section
4. Click on the name of the Administrator user that you are checking
5. Click on Directory Role. In the far-right pane the Global administrator role should be listed

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various navigation options like 'Diagnose and solve problems', 'Manage', 'Profile', and 'Assigned roles'. Under 'Assigned roles', several categories are listed: Groups, Applications, Licenses, Devices, Azure resources, Authentication methods, Activity, Sign-ins, Audit logs, Troubleshooting + Support, and New support request. The main content area is titled 'Toby vanRoojen - Assigned roles' and shows a table of assigned roles. The table has columns for Role, Description, Resource Name, Organization, and Type. One row is highlighted with a yellow circle: 'Global administrator' (Role), 'Can manage all aspects of Azure AD and Microsoft services th...' (Description), 'Directory' (Resource Name), 'Organization' (Organization), and 'Built-in' (Type). There are also buttons at the top for '+ Add assignment' and 'Remove assignment'.

If this user does not have the Global administrator role, you can perform the following steps to add it (Note that the logged in account must be a Global administrator to perform these steps):

1. From the user Directory Role detail page in step 5 above, click the Add Assignment button at the top of the detail page.
2. Click on Global administrator in the list of roles. Click the Add button.

This screenshot shows the same 'Assigned roles' section as the previous one, but with a different focus. The 'Add assignment' button at the top left is circled in yellow. In the list of roles, the 'Global administrator' option is selected and highlighted with a yellow circle. At the bottom right of the list, there is a large blue 'Add' button, which is also circled in yellow.

Azure subscription ownership

The Azure Administrator must also be a Subscription Owner on the subscription that will contain the deployment.

To check that the Administrator is a Subscription Owner, follow these steps:

1. Log in to the Azure Portal at <https://portal.azure.com/>
2. Search for, and select Subscriptions

3. In the next pane to the right, click on the name of the subscription to see the subscription details
4. Click on the Access Control (IAM) menu item in the pane second from the left
5. Click on the Role Assignments tab. The Azure Administrator should be listed in the Owner section.

The screenshot shows the Azure portal interface for managing access control. The left sidebar lists various service categories like Overview, Activity log, and Access control (IAM). The main content area is titled 'Azure subscription 1 - Access control (IAM)' and shows the 'Role assignments' tab selected. It displays a table of role assignments for the current subscription. One row is highlighted, showing a user named 'Toby vanRoojen' with the role 'Owner' assigned to 'This resource'. Both the 'Role assignments' tab and the 'Owner' role entry are circled in yellow to indicate they are the focus of the instructions.

If the Azure Administrator is not listed, you can add the account as a subscription owner by following these steps:

1. Click the Add button at the top of the page and choose the Add Role Assignment option
2. A dialog will appear to the right. Choose “Owner” in the role drop down, then start typing the username of the Administrator in the Select box. When the full name of the Administrator appears, select it
3. Click the Save button at the bottom of the dialog

This screenshot shows the 'Add role assignment' dialog box overlaid on the main Azure portal page. The 'Role' dropdown is set to 'Owner'. The 'Select' dropdown shows two options: 'AAD DC Administrators' and 'CloudWorkspace'. Below these, the 'Selected members' list contains a single entry: 'Toby vanRoojen'. At the bottom of the dialog, there are 'Save' and 'Discard' buttons, with the 'Save' button being the one currently being interacted with, as indicated by the mouse cursor.

Azure compute core quota

The CWA Setup wizard and VDS portal will create new virtual machines and the Azure subscription must have available quota to successfully run

To check quota follow these steps:

1. Navigate to the Subscriptions module and click “Usage + Quotas”
2. Select all providers in the “providers” drop-down, select “Microsoft.Compute” in the “Providers” drop-down
3. Select the target Region in the “Locations” drop-down
4. A list of available quotas by virtual machine family should be shown

The screenshot shows the Azure portal interface with the URL [https://portal.azure.com/#blade/Microsoft_Azure_Billing/UsageQuotaBlade/SubscriptionId/00000000-0000-0000-0000-000000000000/resourceGroup/00000000-0000-0000-0000-000000000000/resourceType/Microsoft.Compute/resourceName/00000000-0000-0000-0000-000000000000/quotaId/00000000-0000-0000-0000-000000000000](#). The left sidebar is collapsed. The main content area is titled "Azure subscription 1 - Usage + quotas". It displays a table of service quotas for the provider "Microsoft.Compute" in the location "East US 2". The table has columns for Quota, provider, location, and Usage. Most quotas show 0% usage and 0 of the quota limit. One quota for "Standard DS Family vCPUs" shows 0% usage and 0 of 8. The top right of the table has a "Request Increase" button, which is highlighted with a yellow oval. The top bar includes a search bar, navigation icons, and a user profile.

Quota	provider	location	Usage
Availability Sets	Microsoft.Compute	East US 2	0 % 0 of 2000
Basic A Family vCPUs	Microsoft.Compute	East US 2	0 % 0 of 250
Premium Storage Managed Disks	Microsoft.Compute	East US 2	0 % 0 of 50000
PremiumStorageSnapshots	Microsoft.Compute	East US 2	0 % 0 of 50000
Standard A0-A7 Family vCPUs	Microsoft.Compute	East US 2	0 % 0 of 250
Standard A8-A11 Family vCPUs	Microsoft.Compute	East US 2	0 % 0 of 350
Standard A1c2 Family vCPUs	Microsoft.Compute	East US 2	0 % 0 of 350
Standard B5 Family vCPUs	Microsoft.Compute	East US 2	0 % 0 of 250
Standard D Family vCPUs	Microsoft.Compute	East US 2	0 % 0 of 350
Standard D4S4 Family vCPUs	Microsoft.Compute	East US 2	0 % 0 of 0
Standard D4v2 Family vCPUs	Microsoft.Compute	East US 2	0 % 0 of 0
Standard DCS Family vCPUs	Microsoft.Compute	East US 2	0 % 0 of 8
Standard DS Family vCPUs	Microsoft.Compute	East US 2	0 % 0 of 350
Standard DSv2 Family vCPUs	Microsoft.Compute	East US 2	0 % 0 of 250

If you need to increase quota, click Request Increase and follow the prompts to add additional capacity. For the initial deployment specifically request increased quote for the “Standard DSv3 Family vCPUs”

Collect discovery details

Once working through the CWA Setup wizard there are several questions that need to be answered. NetApp VDS has provided a linked PDF that can be used to record these selections prior to deployment. Item include:

Item	Description
VDS admin credentials	Collect the existing VDS admin credentials if you already have them. Otherwise a new admin account will be created during deployment.
Azure Region	Determine the target Azure Region based on performance and availability of services. This Microsoft Tool can estimate end user experienced based on region.
Active Directory type	The VMs will need to join a domain but can't directly join Azure AD. The VDS deployment can build a new virtual machine or use an existing domain controller.

Item	Description
File Management	Performance is highly dependent on disk speed, particularly as related to user profile storage. The VDS setup wizard can deploy a simple file server or configure Azure NetApp Files (ANF). For nearly any production environment ANF is recommended however for a POC the file server option provides sufficient performance. Storage options can be revised post-deployment, including using existing storage resources in Azure. Consult ANF pricing for details: https://azure.microsoft.com/en-us/pricing/details/netapp/
Virtual Network Scope	A routable /20 network range is required for the deployment. the VDS setup wizard will allow you to define this range. It is important that this range does not overlap with any existing vNets in Azure or on-premises (if the two networks will be connected via a VPN or ExpressRoute).

VDS setup sections

Login to <https://cwasetup.cloudworkspace.com/> with your Azure admin credentials found in the prerequisites section.

IaaS and platform

Azure AD domain name

The Azure AD domain name is inherited by the selected tenant.

Location

Select an appropriate **Azure Region**. This [Microsoft Tool](#) can estimate end user experienced based on region.

Active Directory type

VDS can be provisioned with a **new virtual machine** for the Domain Controller function or setup to leverage an existing Domain Controller.

In this guide we will select New Windows Server Active Directory, which will create one or two VMs (based on choices made during this process) under the subscription.

A detailed article covering an existing AD deployment is found [here](#).

Active Directory domain name

Enter a **domain name**. Mirroring the Azure AD Domain Name from above is recommended.

File management

VDS can provision a simple file server virtual machine or setup and configure Azure NetApp Files. In production Microsoft recommends allocating 30gb per user and we've observed that allocating 5-15 IOPS per user is required for optimal performance.

In a POC (non-production) environment the file server is a low-cost and simple deployment option however the available performance of Azure Managed Disks can be overwhelmed by the IOPS consumption of even a small production deployment.

For example, a 4TB Standard SSD disk in azure supports up to 500 IOPS, which could only support a maximum of 100 total users at 5 IOPS/user. With ANF Premium the same sized storage setup would support 16,000 IOPS posting 32x more IOPS.

For production AVD deployments, **Azure NetApp Files is Microsoft's recommendation**.



Azure NetApp Files needs to be made available to the subscription you wish to deploy into - please contact your NetApp account rep or use this xref:/ <https://aka.ms/azurenappfiles>

It is also required that you register NetApp as a provider to your subscription. This can be done by doing the following:

- Navigate to Subscriptions in the Azure portal
 - Click Resource Providers
 - Filter for NetApp
 - Select the provider and click Register

RDS license number

NetApp VDS can be used to deploy RDS and/or AVD environments. When deploying AVD, this field can **remain empty**.

Thinprint

NetApp VDS can be used to deploy RDS and/or AVD environments. When deploying AVD, this toggle can remain **off** (toggle left).

Notification email

VDS will send deployment notifications and ongoing health reports to the **email provided**. This can be

changed later.

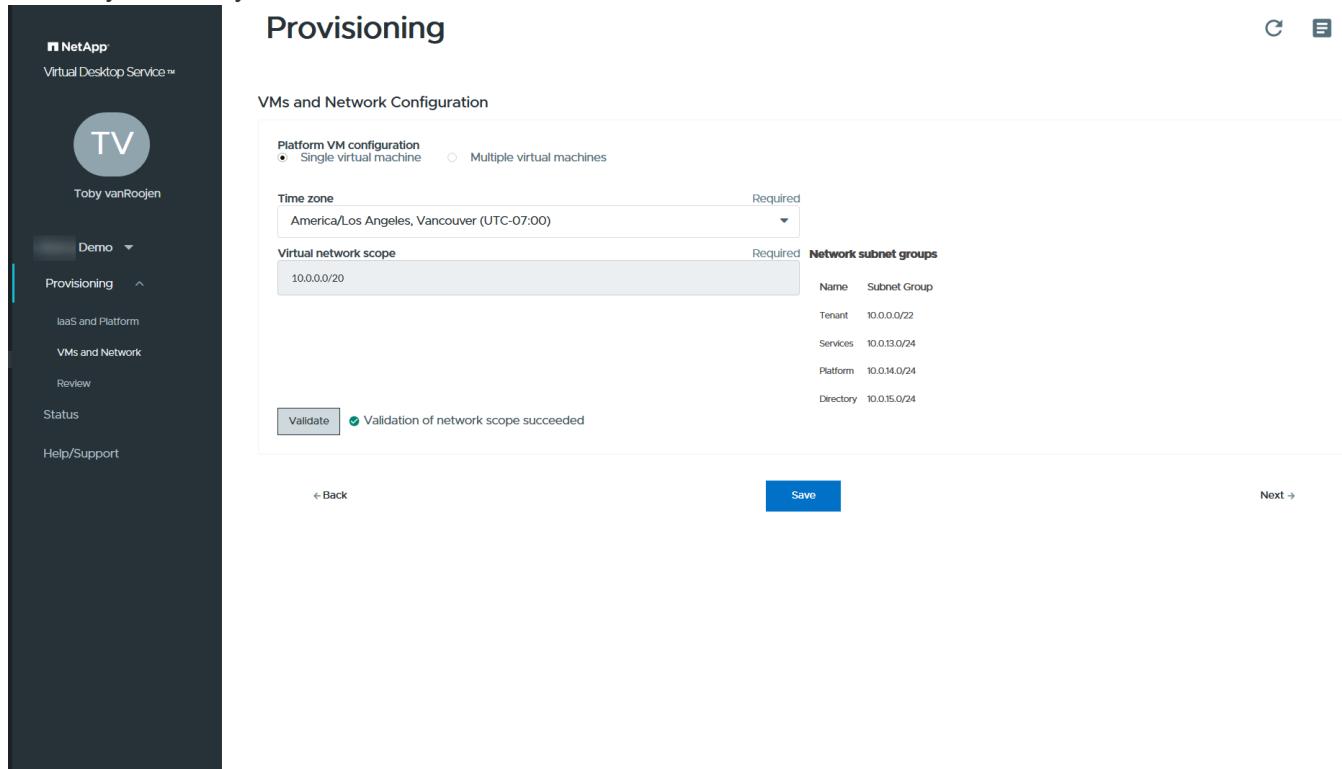
VMs and network

There are a variety of services that need to run in order to support a VDS environment – these are collectively referred to as the “VDS platform”.

Depending on the configuration these can include CWMGR, one or two RDS Gateways, one or two HTML5 Gateways, an FTPS server, and one or two Active Directory VMs.

Most AVD deployments leverage the Single virtual machine option, as Microsoft manages the AVD Gateways as a PaaS service.

For smaller and simpler environments that will include RDS use cases, all of these services can be condensed into the Single virtual machine option to reducing VM costs (with limited scalability). For RDS uses cases with more than 100 users the Multiple virtual machines option is advised in order to facilitate RDS and/or HTML5 Gateway scalability



Platform VM configuration

NetApp VDS can be used to deploy RDS and/or AVD environments. When deploying AVD the Single virtual machine selection is recommended. For RDS deployments you need to deploy and manage additional components such as Brokers and Gateways, in production these services should be run on dedicated and redundant virtual machines. For AVD, all of these services are provided by Azure as an included service and thus, the **single virtual machine** configuration is recommended.

Single virtual machine

This is the recommended selection for deployments that will exclusively use AVD (and not RDS or a combination of the two). In a Single virtual machine deployment the following roles are all hosted on a single VM in Azure:

- CW Manager

- HTML5 Gateway
- RDS Gateway
- Remote App
- FTPS Server (Optional)
- Domain Controller role

The maximum advised user count for RDS use cases in this configuration is 100 users. Load balanced RDS/HTML5 gateways are not an option in this configuration, limiting the redundancy and options for increasing scale in the future. Again, this limit does not apply to AVD deployments, since Microsoft manages the Gateways as a PaaS service.



If this environment is being designed for multi-tenancy, a Single virtual machine configuration is not supported - neither is AVD or AD Connect.

Multiple virtual machines

When splitting the VDS Platform into Multiple virtual machines the following roles are hosted on dedicated VMs in Azure:

- Remote Desktop Gateway

VDS Setup can be used to deploy and configure one or two RDS Gateways. These gateways relay the RDS user session from the open internet to the session host VMs within the deployment. RDS Gateways handle an important function, protecting RDS from direct attacks from the open internet and to encrypt all RDS traffic in/out of the environment. When two Remote Desktop Gateways are selected, VDS Setup deploys 2 VMs and configures them to load balance incoming RDS user sessions.

- HTML5 Gateway

VDS Setup can be used to deploy and configure one or two HTML5 Gateways. These gateways host the HTML5 services used by the *Connect to Server* feature in VDS and the web-based VDS Client (H5 Portal). When two HTML5 Portals are selected, VDS Setup deploys 2 VMs and configures them to load balance incoming HTML5 user sessions.



When using Multiple server option (even if users will only connect via the installed VDS Client) at least one HTML5 gateway is highly recommended to enable *Connect to Server* functionality from VDS.

- Gateway Scalability Notes

For RDS use cases, the maximum size of the environment can be scaled out with additional Gateway VMs, with each RDS or HTML5 Gateway supporting roughly 500 users. Additional Gateways can be added later with minimal NetApp professional services assistance

If this environment is being designed for multi-tenancy then the Multiple virtual machines selection is required.

Time zone

While the end users' experience will reflect their local time zone, a default time zone needs to be selected. Select the time zone from where the **primary administration** of the environment will be performed.

Virtual network scope

It is a best practice to isolate VMs to different subnets according to their purpose. First, define the network scope and add a /20 range.

VDS Setup detects and suggests a range that should prove successful. Per best practices, the subnet IP addresses must fall into a private IP address range.

These ranges are:

- 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

Review and adjust if needed, then click Validate to identify subnets for each of the following:

- Tenant: this is the range that session host servers and database servers will reside in
- Services: this is the range that PaaS services like Azure NetApp Files will reside in
- Platform: this is the range that Platform servers will reside in
- Directory: this is the range that AD servers will reside in

Review

The final page provides an opportunity to review your choices. When you have completed that review, click the Validate button. VDS Setup will review all the entries and verify that the deployment can proceed with the information provided. This validation can take 2-10 minutes. To follow the progress, you can click the log logo (upper right) to see the validation activity.

Once validation is complete the green Provision button will appear in place of the Validate button. Click on Provision to start the provisioning process for your deployment.

Status

The provisioning process takes between 2-4 hours depending on Azure workload and the choices you made. You can follow the progress in the log by clicking the Status page or wait for the email that will tell you the deployment process has completed. Deployment builds the virtual machines and Azure components required to support both VDS and a Remote Desktop or a AVD implementation. This includes a single virtual machine that can act as both a Remote Desktop session host and a file server. In a AVD implementation this virtual machine will act only as a file server.

Install and configure AD Connect

Immediately after the install is successful, AD Connect needs to be installed and configured on the Domain Controller. In a singe platform VM setup the CWMGR1 machine is the DC. The users in AD need to sync between Azure AD and the local domain.

To install and configure AD Connect, follow these steps:

1. Connect to the domain controller as a domain admin.
 - a. Get credentials from the Azure Key Vault (See [Key Vault instructions here](#))
2. Install AD Connect, login with the domain admin (with Enterprise Admin role permissions) and the Azure AD Global Admin.

Activating AVD services

Once the deployment is complete, the next step is to enable the AVD functionality. The AVD enablement process requires the Azure Administrator to perform several steps to register their Azure AD domain and subscription for access using the Azure AVD services. Similarly, Microsoft requires VDS to request the same permissions for our automation application in Azure. The steps below walk you through that process.

Create AVD host pool

End User access to AVD virtual machines is managed by host pools , which contain the virtual machines, and app groups, which in-turn contain the users and type of user access.

To build your first host pool

1. Click the Add button in the right hand side of the AVD host pools section header.

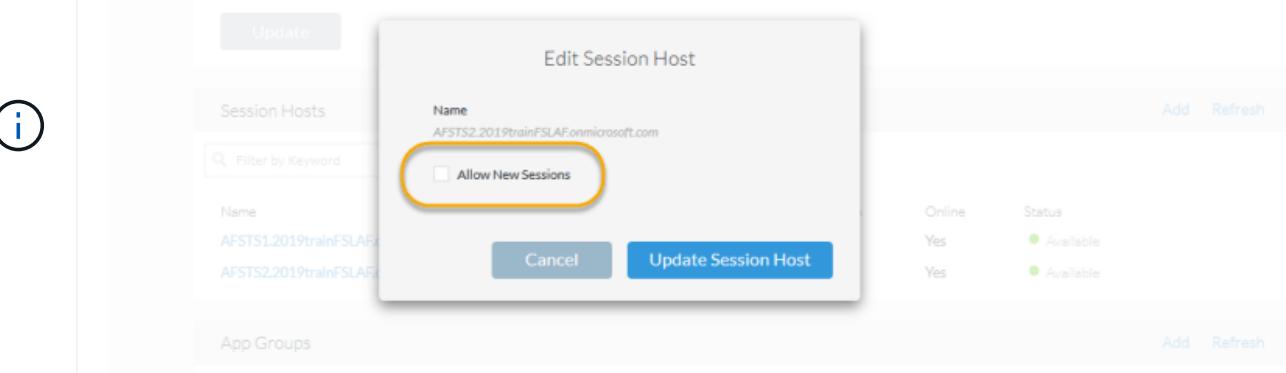
The screenshot shows the 'Cloud Workspaces' interface with the 'Workspaces' menu item selected. In the center, there's a 'WVD Details' section with tenant ID and HTML5 URL information. Below it is a table titled 'WVD Host Pools' containing one row for 'hostpool1'. A large black arrow points to the 'Add' button located at the top right of the host pool table area.

Name	Description	Type	Session Hosts
hostpool1	First Host Pool	Shared	2

2. Enter a name and description for your host pool.
3. Choose a host pool type
 - a. **Pooled** means multiple users will access the same pool of virtual machines with the same applications installed.
 - b. **Personal** creates a host pool where users are assigned their own session host VM.
4. Select the Load Balancer type
 - a. **Depth First** will fill the first shared virtual machine to the max number of users before starting on the second virtual machine in the pool
 - b. **Breadth First** will distribute users to all the virtual machines in the pool in a round robin fashion
5. Select an Azure virtual machines template for creating the virtual machines in this pool. While VDS will show all templates available in the subscription, we recommend selecting the most recent Windows 10 multi-user build for the best experience. The current build is Windows-10-20h1-evd. (Optionally create a Gold Image using the Provisioning Collection functionality to build hosts from a custom virtual machine image)

6. Select the Azure machine size. For evaluation purposes, NetApp recommends the D series (standard machine type for multi-user) or E series (enhanced memory configuration for heavier duty multi-user scenarios). The machine sizes can be changed later in VDS if you want to experiment with different series and sizes
7. Select a compatible storage type for the virtual machines' Managed Disk instances from the drop down list
8. Select the number of virtual machines you want created as part of the host pool creation process. You can add virtual machines to the pool later, but VDS will build the number of virtual machines you request and add them to the host pool once its created
9. Click the Add host pool button to start the creation process. You can track progress on the AVD page, or you can see the details of the process log on the Deployments/Deployment name page in the Tasks section
10. Once the host pool is created it will appear in the host pool list on the AVD page. Click on the name of the host pool to see its detail page, which includes a list of its virtual machines , app groups, and active users

AVD Hosts in VDS are created with a setting that disallows user sessions to connect. This is by design to allow for customization prior to accepting user connections. This setting can be changed by editing the session host's settings.



Enable VDS desktops for users

As noted above, VDS creates all the elements required to support end user workspaces during deployment. Once the deployment has completed, the next step is to enable workspace access for each user you want introduced to the AVD environment. This step creates the profile configuration and end user data layer access that is the default for a virtual desktop. VDS reuses this configuration to link Azure AD end users to the AVD App Pools.

To enable workspaces for end users follow these steps:

1. Log in to VDS at <https://manage.cloudworkspace.com> using the VDS primary administrator account you created during provisioning. If you don't remember your account information, please contact NetApp VDS for assistance in retrieving it
2. Click on the Workspaces menu item, then click on the name of the Workspace that was created automatically during provisioning
3. Click on the Users and Groups tab

Cloud Workspace

All Workspaces TrainWVD2's Workspace (rs6a)

Overview Users & Groups VM Resource Workload Schedule WVD Delete Client

Groups

Groups

Add

Filter by Keyword

Group Users

risk-all-users 1

Users

Add/Import Refresh

You have 1 user(s) pending Cloud Workspace approval.

Filter by Keyword

Name	Username	Status	Connection Status
Toby vanRoojen	Toby vanRoojen	Pending (Pending Cloud Workspace)	Offline
WVD User1	WVDUser1@r...	Available	Offline

©2019 Privacy / Terms of Use / Cookies

-
4. For each user that you want to enable, scroll over the username and then click on the Gear icon
 5. Choose the “Enable Cloud Workspace” option

Cloud Workspace

All Workspaces TrainWVD2's Workspace (rs6a)

Overview Users & Groups VM Resource Workload Schedule WVD Delete Client

Groups

Groups

Add

Filter by Keyword

Group Users

risk-all-users 1

Users

Add/Import Refresh

You have 1 user(s) pending Cloud Workspace approval.

Filter by Keyword

Name	Username	Status	Connection Status
Toby vanRoojen	Toby vanRoojen	Pending (Pending Cloud Workspace)	Offline
WVD User1	WVDUser1@r...	Available	Offline

Enable Cloud Workspace

©2019 Privacy / Terms of Use / Cookies

-
6. It takes about 30-90 seconds for the enablement process to complete. Note that the user status will change from Pending to Available



Activating Azure AD Domain Services creates a managed domain in Azure, and each AVD virtual machine that is created will be joined to that domain. In order for traditional login to the virtual machines to work, the password hash for Azure AD users must be synced to support NTLM and Kerberos authentication. The easiest way to accomplish this task is to change the user password in Office.com or the Azure portal, which will force the password hash sync to occur. The sync cycle for Domain Service servers can take up to 20 minutes.

Enable user sessions

By default, session hosts are unable to accept user connections. This setting is commonly called “drain mode” as it can be used in production to prevent new user sessions, allowing the host to eventually remove all user sessions. When new user sessions are allowed on a host this action is commonly referred to as placing the session host “into rotation.”

In production it makes sense to start new hosts in drain mode because there are typically configuration tasks that need to be completed before the host is ready for production workloads.

In testing and evaluation you can immediately take the hosts out of drain mode to enable user connects and to confirm functionality.

To Enable user sessions on the session host(s) follow these steps:

1. Navigate to the AVD Section of the workspace page.
2. Click on the host pool name under “AVD host pools” .

The screenshot shows the Microsoft Cloud Workspaces interface for a workspace named "2019 Training Step 3 - WVD Activated's Workspace (z58b)". The left sidebar has a "Workspaces" tab selected. The main area shows "WVD Details" with fields for Tenant ID and HTML5 URL. Below this is the "WVD Host Pools" section, which contains a table with two rows:

Name	Description	Tenant	Type	Session Hosts
apps	apps	z58b	Shared	1
Desktop Users	Hostpool for Desktop Users	z58b	Shared	4

3. Click on the name of the Session host(s) and check the box “Allow New Sessions”, Click “Update Session Host”. Repeat for all hosts that need to be placed into rotation.

The screenshot shows the 'WVD Host Pool Desktop Users' page. On the left, there's a sidebar with options like Dashboard, Organizations, Deployments, Workspaces (selected), App Services, Service Board, Scripted Events, Admins, and Reports. The main area shows 'Host Pool Details' for 'Desktop Users' with a description 'Hostpool for Desktop Users' and tenant 'z58b'. Below this is a 'Session Hosts' table with four entries: Z58BTS1, Z58BTS2, Z58BTS3, and Z58BTS4, all from 'onmicrosoft.com'. A yellow arrow points from the 'Allow New Sessions' checkbox in the 'Edit Session Host' dialog to the 'Allow New Session' column in the table. Another yellow arrow points from the 'Edit Session Host' dialog to the table.

Name	Allow New Session	Sessions	Online	Status
Z58BTS1.onmicrosoft.com	Yes	0	Yes	Available
Z58BTS2.onmicrosoft.com	Yes	0	No	NoHeartbeat
Z58BTS3.onmicrosoft.com	Yes	0	No	NoHeartbeat
Z58BTS4.onmicrosoft.com	Yes	0	No	NoHeartbeat

4. The current stats of “Allow New Session” is also displayed on the main AVD page for each host line item.

Default app group

Note that the Desktop Application Group is created by default as part of the host pool creation process. This group provides interactive desktop access to all group members.

To add members to the group:

1. Click on the name of the App Group

The screenshot shows the 'WVD Host Pool hostpool1' page. It has sections for 'Host Pool Details', 'Session Hosts', and 'App Groups'. In the 'App Groups' section, there is one entry: 'Desktop Application Group'. A black arrow points to this link. Below it is a 'Active Users' section with the message 'No active users found.'

Name	Description	Resource	Users	Remote Apps
Desktop Application Group	Desktop Application Group	Desktop	1	-

2. Click on the link that shows the number of Users Added

3. Select the users you wish to add to the app group by checking the box next to their name
4. Click the Select Users button
5. Click the Update app group button

Create additional AVD app group(s)

Additional app groups can be added to the host pool. These app groups will publish specific applications from the host pool virtual machines to the App Group users using RemoteApp.



AVD only allows end users to be assigned to the Desktop App Group type or RemoteApp App Group type but not both in the same host pool, so make sure you segregate your users accordingly. If users need access to a desktop and streaming apps, a 2nd host pool is required to host the app(s).

To create a new App Group:

1. Click the Add button in the app groups section header

Cloud Workspace

WVD Host Pool hostpool1

Host Pool Details

Name	Description	Host Pool Type
hostpool1	First Host Pool	Shared

Session Hosts

Name	Allow New Session	Sessions	Online	Status
RS6AT51.trainwvd2.azmonsoft.com	Yes	0	Yes	Available
RS6AT52.trainwvd2.azmonsoft.com	Yes	0	Yes	Available

App Groups

Name	Description	Resource	Users	Remote Apps
Desktop Application Group	Desktop Application Group	Desktop	1	-

Active Users

No active users found.

2. Enter a name and description for the App Group
3. Select users to add to the group by clicking on the Add Users link. Select each user by clicking the check box next to their name, then click the Select Users button

WVD Host Pool hostpool1

Select Remote Apps

Name
<input checked="" type="checkbox"/> 7-Zip File Manager
<input type="checkbox"/> Character Map
<input type="checkbox"/> dcmd
<input type="checkbox"/> Disk Cleanup
<input checked="" type="checkbox"/> Internet Explorer
<input type="checkbox"/> iSCSI Initiator
<input type="checkbox"/> 1 2 3 4 5 > >

Cancel Select Remote Apps

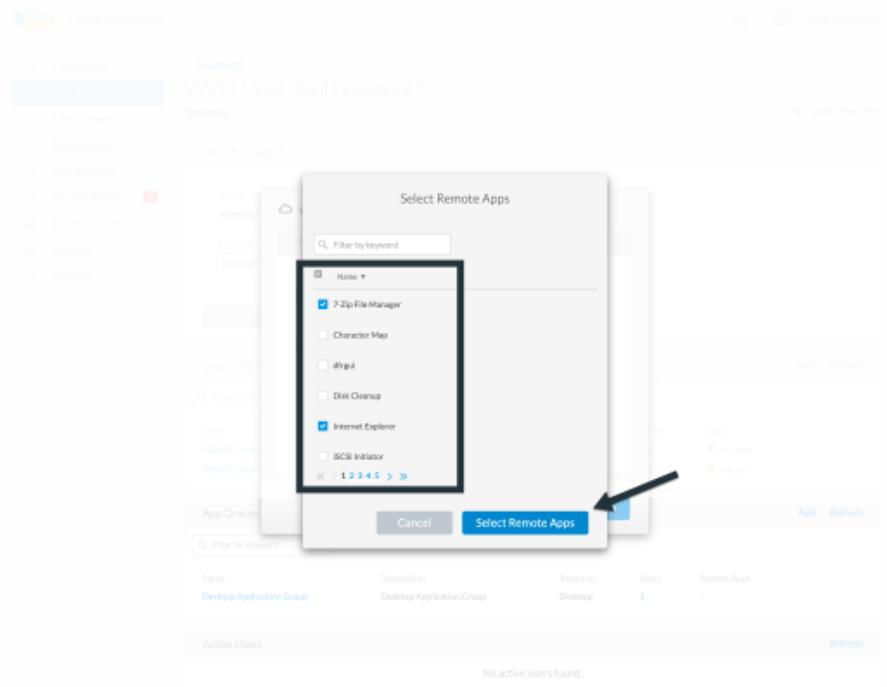
App Groups

Name	Description	Resource	Users	Remote Apps
Desktop Application Group	Desktop Application Group	Desktop	1	-

Active Users

No active users found.

4. Click the Add RemoteApps link to add applications to this App Group. AVD automatically generates the list of possible applications by scanning the list of applications installed on the virtual machine . Select the application by clicking on the check box next to the application name, then click the Select RemoteApps button.



5. Click the Add App Group button to create the App Group

End user AVD access

End users can access AVD environments using the Web Client or an installed client on a variety of platforms

- Web Client: <https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-web>
- Web Client Login URL: <http://aka.ms/AVDweb>
- Windows Client: <https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-windows-7-and-10>
- Android Client: <https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-android>
- macOS Client: <https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-macos>
- iOS Client: <https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-ios>
- IGEL Thin Client: <https://www.igel.com/igel-solution-family/windows-virtual-desktop/>

Log in using the end user username and password. Note that Remote App and Desktop Connections (RADC), Remote Desktop Connection (mstsc), and the CloudWorksapce Client for Windows application do not currently support the ability to log in to AVD instances.

Monitor user logins

The host pool detail page will also display a list of active users when they log in to a AVD session.

Admin connection options

VDS Admins are able to connect to virtual machines in the environment in a variety of ways.

Connect to server

Throughout the portal, VDS Admins will find the “Connect to Server” option. By default, this function connects the admin to the virtual machine by dynamically generating local admin credentials and injecting them into a

web client connection. The Admin does not need to know (and is never provided with) credentials in order to connect.

This default behavior can be disabled on a per-Admin basis as described in the next section.

.tech/Level 3 admin accounts

In the CWA Setup process there is a “Level III” admin account created. The user name is formatted as username.tech@domain.xyz

These accounts, commonly called a “.tech” account, are named domain-level administrator accounts. VDS Admins can use their .tech account when connecting to a CWMGR1 (platform) server and optionally when connecting to all other virtual machines in the environment.

To disable the automatic local admin login function and force the Level III account to be used, change this setting. Navigate to VDS > Admins > Admin Name > Check “Tech Account Enabled.” With this box checked, the VDS admin will not be automatically logged into virtual machines as a local admin and rather be prompted to enter their .tech credentials.

These credentials, and other relevant credentials, are automatically stored in the *Azure Key Vault* and can be accessed from within the Azure Management Portal at <https://portal.azure.com/>.

Optional post-deployment actions

Multi-factor authentication (MFA)

NetApp VDS includes SMS/Email MFA at no charge. This feature can be used to secure VDS Admin accounts and/or End User accounts.

[MFA Article](#)

Application entitlement workflow

VDS provides a mechanism to assign end users access to applications from a pre-defined list of applications called the Application Catalog. The Application catalog spans all managed deployments.



The automatically deployed TSD1 server must remain as-is to support application entitlement. Specifically, do not run the “convert to data” function against this virtual machine.

Application Management is detailed in this Article: https://docs.netapp.com/us-en/virtual-desktop-service/Management.Applications.application_entitlement_workflow.html

Azure AD security groups

VDS includes functionality to create, populate and delete user groups which are backed by Azure AD Security Groups. These groups can be used outside of VDS just like any other Security Group. In VDS these groups can be used to assign folder permissions and application entitlement.

Create user groups

Creating user groups is performed on the Users & Groups tab within a workspace.

Assign folder permissions by group

Permissions to view and edit folders in the company share can be assigned to users or groups.

https://docs.netapp.com/us-en/virtual-desktop-service/Management.User_Administration.manage_folders_and_permissions.html

Assign applications by group

In addition to assigning applications to users individually, applications can be provisioned to groups.

1. Navigate to the Users and Groups Detail.

The screenshot shows the 'Cloud Workspace' interface with the 'All Workspaces' view. The 'TrainWVD2's Workspace (rs6a)' is selected. In the left sidebar, 'Workspaces' is highlighted with a blue box. On the main page, the 'Users & Groups' tab is active. The 'Groups' section shows a table with one row ('role-all-users') and two users. An 'Add' button is located above the table. To the right, a 'Users' table lists three entries: 'Toby vanRooijen' (admin@trainwvd2), 'WVDUser1' (WVDUser1@trainwvd2), and 'WVDUser1@trainwvd2'. The 'Add/Import' and 'Refresh' buttons are at the top of the user table.

2. Add a new group or edit an existing group.

This screenshot is identical to the previous one, showing the 'Cloud Workspace' interface with the 'All Workspaces' view and the 'TrainWVD2's Workspace (rs6a)' selected. The 'Workspaces' menu item in the sidebar is highlighted with a blue box. A large black arrow labeled 'add' points to the 'Add' button in the 'Groups' section. A blue arrow labeled 'edit' points to the 'role-all-users' group entry in the 'Groups' table. The 'Users' table on the right shows the same three entries as before.

3. Assign user(s) and application(s) to the group.

The screenshot shows the Cloud Workspace interface with the 'Users & Groups' tab selected for the workspace 'TrainWVD2 (rs6a)'. On the left, the 'Organizations' menu is open, showing options like Deployments, Workspaces, App Services, Service Board, Scripted Events, Admins, and Reports. The main area displays a 'Groups' section with a table for 'rs6a-all-users' containing 2 users: 'Toby vanRooyen' and 'WVD User1'. Below this is a 'Users' section listing the same two users with their status (Available) and connection status (Offline). A large double-headed arrow between the 'Groups' and 'Users' sections is labeled 'choose users'. To the right, another table lists 'Applications' such as 'Local Drive Access' and 'Delete'. A large double-headed arrow between the 'Applications' table and the 'Users' section is labeled 'assign applications'. Below these tables are two callout boxes: one for 'choose users' pointing to the 'rs6a-all-users' group table, and another for 'assign applications' pointing to the 'Applications' table. At the bottom, there are two modal dialogs: 'Update Group' showing users 'WVD User1' and 'Toby vanRooyen' with checkboxes checked, and 'TrainWVD2' showing applications like '7zip - Current Version (v16.0)' and 'Calculator' with checkboxes checked.

Configure cost optimization options

Workspace management also extends to managing the Azure resources that support the AVD implementation. VDS allows you to configure both Workload Schedules and Live Scaling to turn Azure virtual machines on and off based on end user activities. These features result in matching Azure resource utilization and spending to the actual usage pattern of end users. In addition, if you have configured a proof of concept AVD implementation you can turn the whole Deployment from the VDS interface.

Workload scheduling

Workload Scheduling is a feature that allows the Administrator to create a set schedule for the Workspace virtual machines to be on to support end user sessions. When the end of the scheduled time period is reached for a specific day of the week, VDS Stops/Deallocates the virtual machines in Azure so that hourly charges stop.

To enable Workload Scheduling:

1. Log in to VDS at <https://manage.cloudworkspace.com> using your VDS credentials.
2. Click on the Workspace menu item and then click on the name of the Workspace in the list.

3. Click on the Workload Schedule tab.

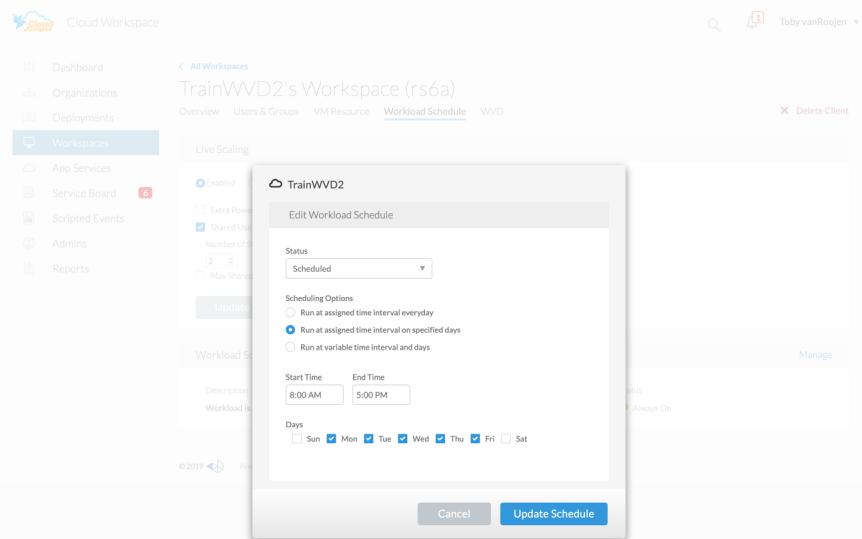
4. Click the Manage link in the Workload Schedule header.

5. Choose a default state from the Status drop down: Always On (default), Always Off, or Scheduled.

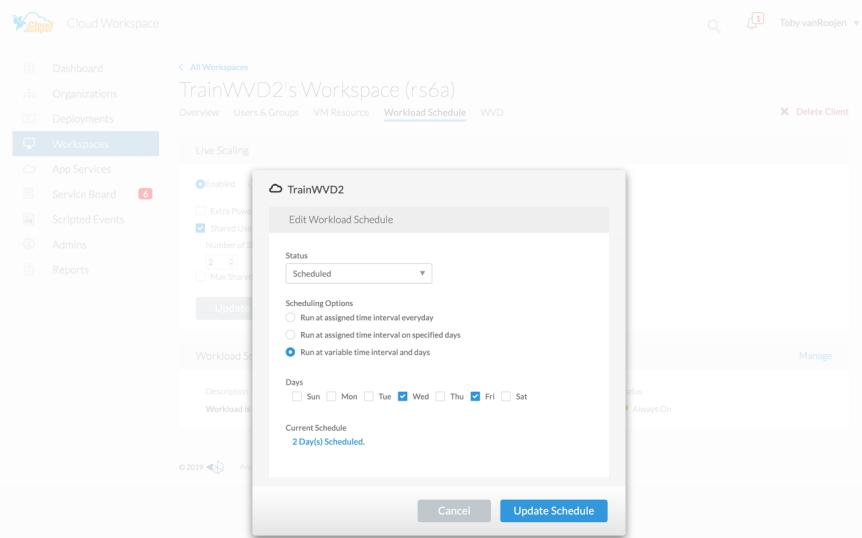
6. If you choose Scheduled, the Scheduling options include:

- Run at Assigned Interval every day. This option sets the schedule to be the same Start Time and End Time for all seven days of the week.

- Run at Assigned Interval for Specified Days. This option sets the schedule to the same Start Tie and End Time only for selected days of the week. Non-selected days of the week will cause VDS to not turn the virtual machines on for those days.



- c. Run at variable time intervals and days. This option sets the schedule to different Start Times and End Times for each selected day.



- d. Click the Update schedule button when finished setting the schedule.

The screenshot shows the Cloud Workspace interface with the 'Workspaces' menu item selected. In the center, a modal window titled 'Edit Workload Schedule' for 'TrainWVD2' is open. The modal contains fields for 'Status' (set to 'Scheduled'), 'Scheduling Options' (radio button selected for 'Run at variable time interval and days'), and a 'Days' section where Wednesday and Friday are checked. Below this, it says 'Current Schedule' with '2 Day(s) Scheduled'. At the bottom right of the modal is a prominent blue 'Update Schedule' button, which is highlighted by a large black arrow.

Live Scaling

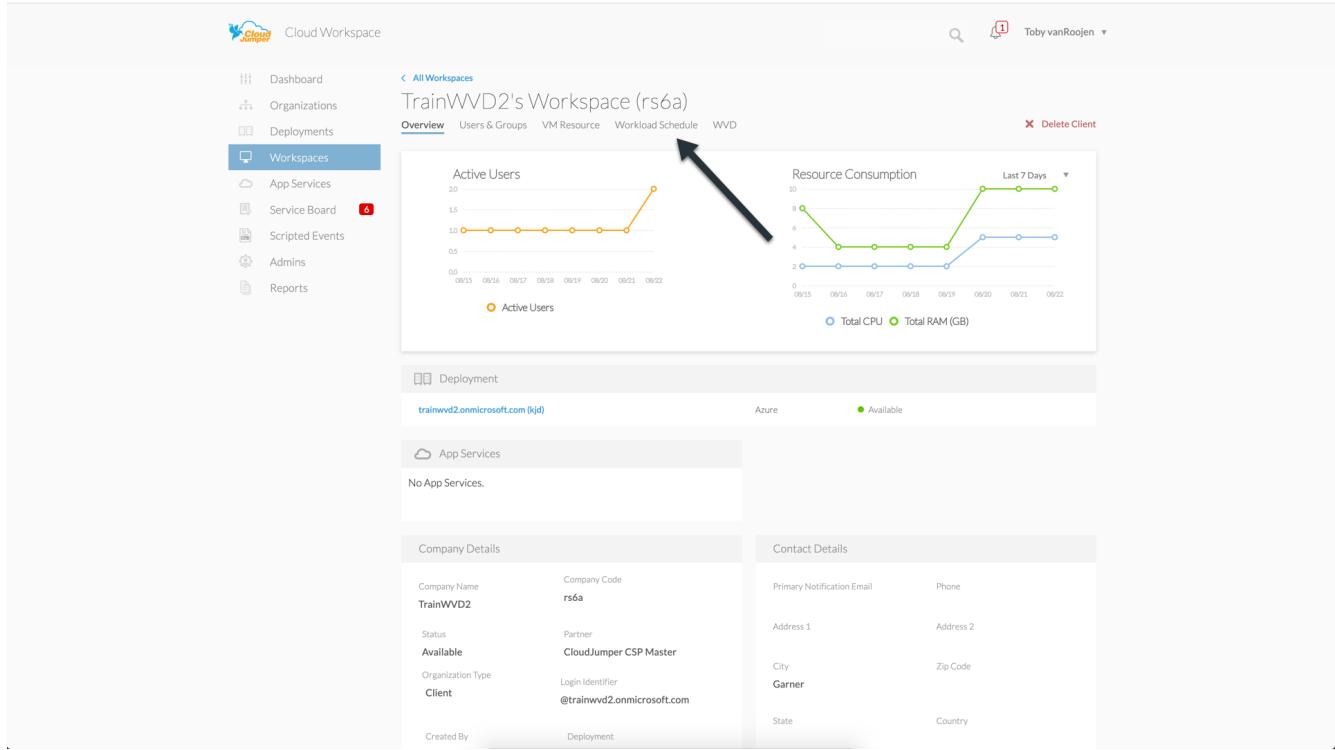
Live Scaling automatically turns virtual machines in a shared host pool on and off depending on concurrent user load. As each server fills up, an additional server is turned on so that its ready when the host pool load balancer sends user session requests. For effective use of Live Scaling, choose “Depth First” as the load balancer type.

To enable Live Scaling:

1. Log in to VDS at <https://manage.cloudworkspace.com> using your VDS credentials.
2. Click on the Workspace menu item and then click on the name of the Workspace in the list.

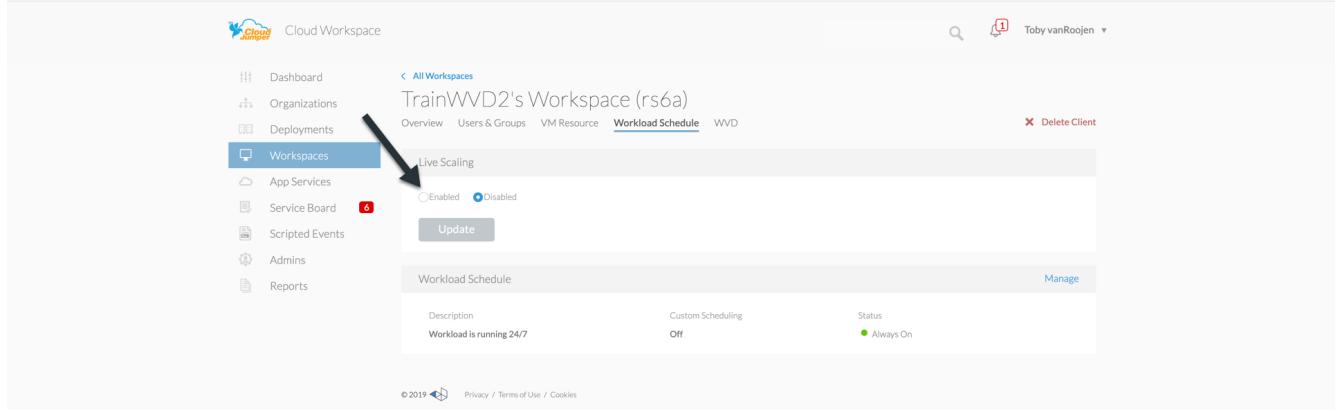
The screenshot shows the Cloud Workspace interface with the 'Workspaces' menu item selected. On the left, there is a sidebar with various menu items: Dashboard, Organizations, Deployments, Workspaces (which is currently selected and highlighted in blue), App Services, Service Board, Scripted Events, Admins, and Reports. On the right, a table lists workspaces. The first workspace listed is 'zJDR Test Wvd's Workspace' (Code: zwn, Deployment: lpm, Users: 0, Status: Available). The second workspace listed is 'TrainWVD2's Workspace' (Code: rs6a, Deployment: kjd, Users: 2, Status: Available). A large black arrow points to the 'TrainWVD2's Workspace' entry in the list.

3. Click on the Workload Schedule tab.



The screenshot shows the Cloud Workspace interface for 'TrainWVD2's Workspace (rs6a)'. The 'Workload Schedule' tab is highlighted with a blue border. On the left, a sidebar menu has 'Workspaces' selected. The main area displays two line charts: 'Active Users' (orange line) and 'Resource Consumption' (blue line for Total CPU, green line for Total RAM (GB)). Below the charts, there are sections for 'Deployment' (trainwvd2.onmicrosoft.com), 'App Services' (No App Services), 'Company Details', and 'Contact Details'. A large black arrow points from the text in step 3 to the 'Workload Schedule' tab.

4. Click the Enabled radio button in the Live Scaling section.



The screenshot shows the Cloud Workspace interface for 'TrainWVD2's Workspace (rs6a)'. The 'Workload Schedule' tab is selected. In the 'Live Scaling' section, there is a radio button group with 'Enabled' (unchecked) and 'Disabled' (checked). A large black arrow points from the text in step 4 to the 'Enabled' radio button. Below this, there is a 'Workload Schedule' section with a 'Manage' button. At the bottom, there is a footer with copyright information and links to Privacy, Terms of Use, and Cookies.

5. Click the Max Number of Users Per Server and enter the max number. Depending on virtual machine size, this number is typically between 4 and 20.

The screenshot shows the 'Workload Schedule' tab for a workspace named 'TrainWVD2's Workspace (rs6a)'. In the 'Live Scaling' section, the 'Shared Users Per Server Enabled' checkbox is checked, and the value '10' is entered in the 'Number of Shared Users Per Server' input field. A black arrow points to this checkbox.

6. OPTIONAL – Click the Extra Powered On Servers Enabled and enter a number of additional servers that you want on for the host pool. This setting activates the specified number of servers in addition to the actively filling server to act as a buffer for large groups of users logging on in the same time window.

The screenshot shows the 'Workload Schedule' tab for a workspace named 'TrainWVD2's Workspace (rs6a)'. In the 'Live Scaling' section, the 'Extra Powered On Servers Enabled' checkbox is checked, and the value '10' is entered in the 'Number of Shared Users Per Server' input field. A black box highlights this section.

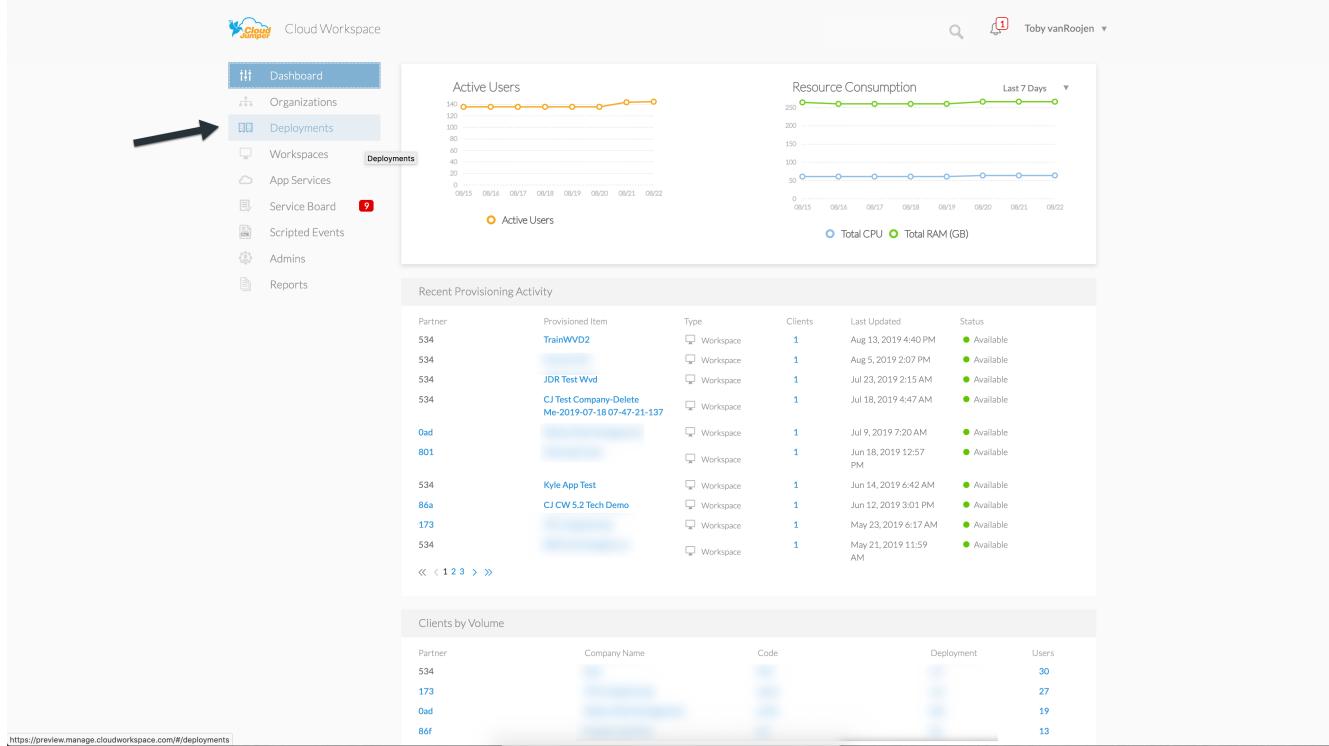
 Live Scaling currently applies to all Shared resource pools. In the near future each pool will have independent Live Scaling options.

Power down the entire deployment

If you plan to only use your evaluation deployment on a sporadic, non-production basis you can turn off all the virtual machines in the deployment when you are not using them.

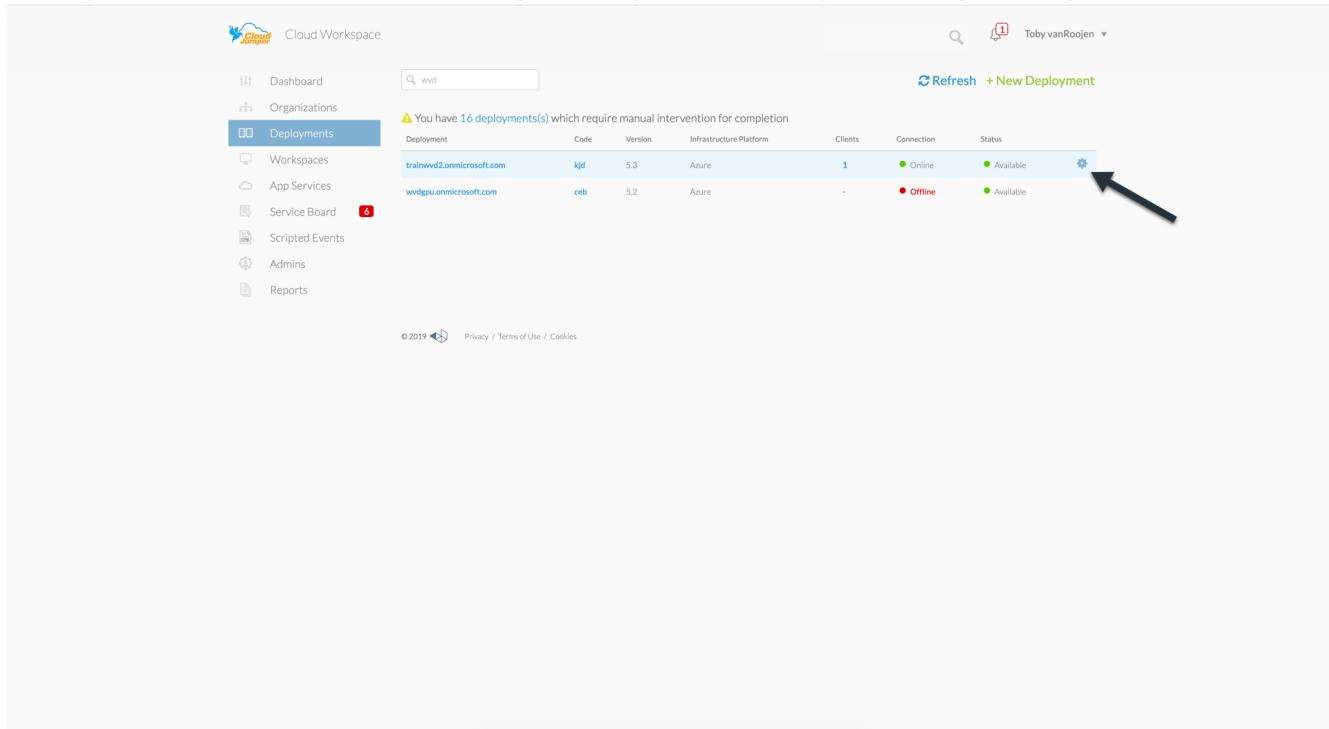
To turn the Deployment on or off (i.e. turn off the virtual machines in the deployment), follow these steps:

1. Log in to VDS at <https://manage.cloudworkspace.com> using your VDS credentials.
2. Click on the Deployments menu item.



The screenshot shows the Cloud Workspace dashboard. On the left, there is a navigation sidebar with the following items: Dashboard (highlighted with a black arrow), Organizations, Deployments (highlighted with a black arrow), Workspaces, App Services, Service Board (with a red notification badge), Scripted Events, Admins, and Reports. To the right of the sidebar are two line charts: 'Active Users' (orange line) and 'Resource Consumption' (blue line for Total CPU and green line for Total RAM GB). Below the charts is a section titled 'Recent Provisioning Activity' with a table of data. At the bottom of this section is a pagination control with links <<, < 1 2 3 > >>. Further down is a section titled 'Clients by Volume' with another table of data. At the very bottom of the page, there is a URL bar showing 'https://preview.manage.cloudworkspace.com/#/deployments'.

Scroll your cursor over the line for the target Deployment to display the Configuration gear icon.



The screenshot shows the Cloud Workspace dashboard with the 'Deployments' menu item selected. A search bar contains the text 'wvd'. A warning message says '⚠ You have 16 deployment(s) which require manual intervention for completion'. Below this is a table of deployments with columns: Deployment, Code, Version, Infrastructure Platform, Clients, Connection, and Status. The first deployment listed is 'trainwvd2.onmicrosoft.com' with code 'kjd', version 5.3, Azure platform, 1 client (online), and available status. The second deployment is 'wvdgpu.onmicrosoft.com' with code 'ceb', version 5.2, Azure platform, 1 client (offline), and available status. A large black arrow points to the gear icon in the 'Status' column for the 'trainwvd2.onmicrosoft.com' row.

3. Click on the gear, then choose Stop.

The screenshot shows the 'Deployments' section of the Cloud Workspace interface. A search bar at the top contains the text 'wvd'. Below it, a message states 'You have 16 deployment(s) which require manual intervention for completion'. A table lists two deployments:

Deployment	Code	Version	Infrastructure Platform	Clients	Connection	Status
trainwvd2.onmicrosoft.com	kjd	5.3	Azure	1	● Online	● Available
wvdgpu.onmicrosoft.com	ceb	5.2	Azure	-	● Offline	● Available

On the far right of the table, there are 'Delete' and 'Stop' buttons for each row. The 'Stop' button for the first row is highlighted with a blue box and a black arrow pointing to it.

4. To restart or Start, follow steps 1-3 and then choose Start.

This screenshot shows the same 'Deployments' section as the previous one, but with a different focus. The 'Start' button for the second deployment, 'wvdgpu.onmicrosoft.com', is highlighted with a blue box and a black arrow pointing to it.



It may take several minutes for all the virtual machines in the deployment to stop or start.

Create and manage VM images

VDS contains functionality for creating and managing virtual machine images for future deployments. To reach this functionality, navigate to: VDS > Deployments > Deployment Name > Provisioning Collections. The "VDI Image Collection" features are documented here: https://docs.netapp.com/us-en/virtual-desktop-service/Management.Deployments.provisioning_collections.html

Configure Azure cloud backup service

VDS can natively configure and manage Azure Cloud Backup, an Azure PaaS service for backing up virtual machines. Backup Policies can be assigned to individual machines or groups of machine by type or host pool. Details are found here: https://docs.netapp.com/us-en/virtual-desktop-service/Management.System_Administration.configure_backup.html

Select app management/policy mode

By default, VDS implements a number of Group Policy Objects (GPO) that lock down the end user workspace. These policies prevent access to both core data layer locations (ex: c:\) and the ability to perform application installations as an end user.

This evaluation is intended to demonstrate the capabilities of Window Virtual Desktop, so you have the option to remove the GPOs so that you can implement a “basic workspace” that provides the same functionality and access as a physical workspace. To do this, follow the steps in the “Basic Workspace” option.

You can also choose to utilize the full Virtual Desktop management feature set to implement a “Controlled Workspace”. These steps include creating and managing an application catalog for end user application entitlement and using Administrator level permissions to manage access to both applications and data folders. Follow the steps in the “Controlled Workspace” section to implement this type of workspace on your AVD host pools.

Controlled AVD workspace (default policies)

Using a controlled workspace is the default mode for VDS deployments. The polices are applied automatically. This mode requires VDS Administrators to install applications and then end users are granted access to the application via a shortcut on the session desktop. In a similar fashion, access to the data folders are assigned to end users by creating mapped shared folders and setting up permissions to see only those mapped drive letters instead of the standard boot and/or data drives. To manage this environment, follow the steps below to install applications and provide end user access.

Reverting to basic AVD workspace

Creating a basic workspace requires disabling the default GPO policies that are created by default.

To do this, follow this one-time process:

1. Log in to VDS at <https://manage.cloudworkspace.com> using your primary admin credentials.
2. Click on the Deployments menu item on the left.

Cloud Workspace

Dashboard Deployments Workspaces App Services Service Board Scripted Events Admins Reports

Active Users

Resource Consumption

Recent Provisioning Activity

Partner	Provisioned Item	Type	Clients	Last Updated	Status
534	TrainWVD2	Workspace	1	Aug 13, 2019 4:40 PM	Available
534		Workspace	1	Aug 5, 2019 2:07 PM	Available
534	JDR Test Wvd	Workspace	1	Jul 23, 2019 2:15 AM	Available
534	CJ Test Company-Delete Me-2019-07-18 07:47:21-137	Workspace	1	Jul 18, 2019 4:47 AM	Available
Oad		Workspace	1	Jul 9, 2019 7:20 AM	Available
801		Workspace	1	Jun 18, 2019 12:57 PM	Available
534	Kyle App Test	Workspace	1	Jun 14, 2019 6:42 AM	Available
86a	CJ CW 5.2 Tech Demo	Workspace	1	Jun 12, 2019 3:01 PM	Available
173		Workspace	1	May 23, 2019 6:17 AM	Available
534		Workspace	1	May 21, 2019 11:59 AM	Available

<< < 1 2 3 > >>

Clients by Volume

Partner	Company Name	Code	Deployment	Users
534				30
173				27
Oad				19
86f				13

<https://preview.manage.cloudworkspace.com/#/deployments>

3. Click on the name of your Deployment.

Cloud Workspace

Dashboard Deployments Workspaces App Services Service Board Scripted Events Admins Reports

wvd

You have 1.6 deployment(s) which require manual intervention for completion

Deployment	Code	Version	Infrastructure Platform	Clients	Connection	Status
trainwvd2.onmicrosoft.com	kjd	5.3	Azure	1	Online	Available
wvdgpu.onmicrosoft.com	ceb	5.2	Azure	-	Offline	Available

Refresh + New Deployment

© 2019 Privacy / Terms of Use / Cookies

4. Under the Platform Servers section (mid page on right), scroll to the right of the line for CWMGR1 until the gear appears.

Cloud Workspace

All Deployments

trainwvd2.onmicrosoft.com (kjd)

Deployment Details

Workloads

Profile Server

Platform Servers

Platform Processes

Name	CPU	RAM (GB)	Status
CWMGR1	2	4	Online

Refresh

5. Click on the gear and choose Connect.

Cloud Workspace

All Deployments

trainwvd2.onmicrosoft.com (kjd)

Deployment Details

Workloads

Profile Server

Platform Servers

Platform Processes

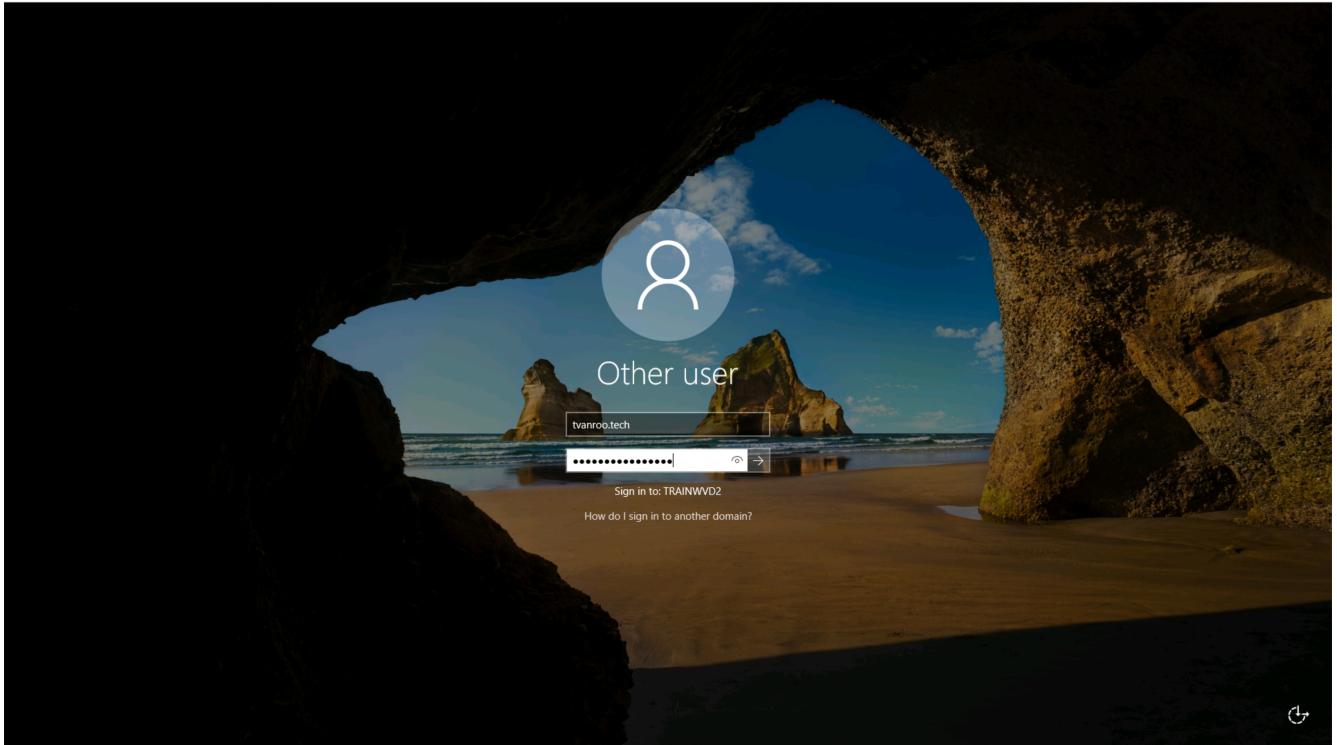
Name	CPU	RAM (GB)	Status
CWMGR1	2	4	Online

Backup

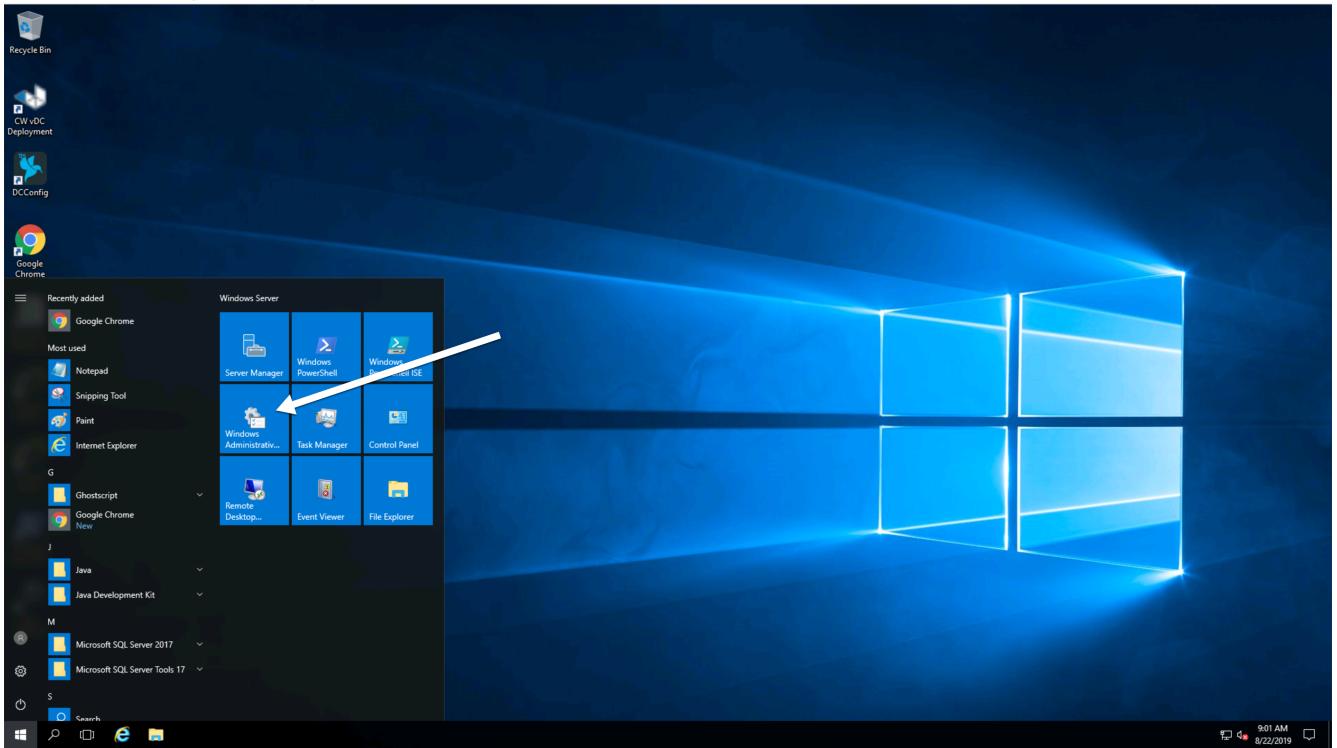
Connect

Refresh

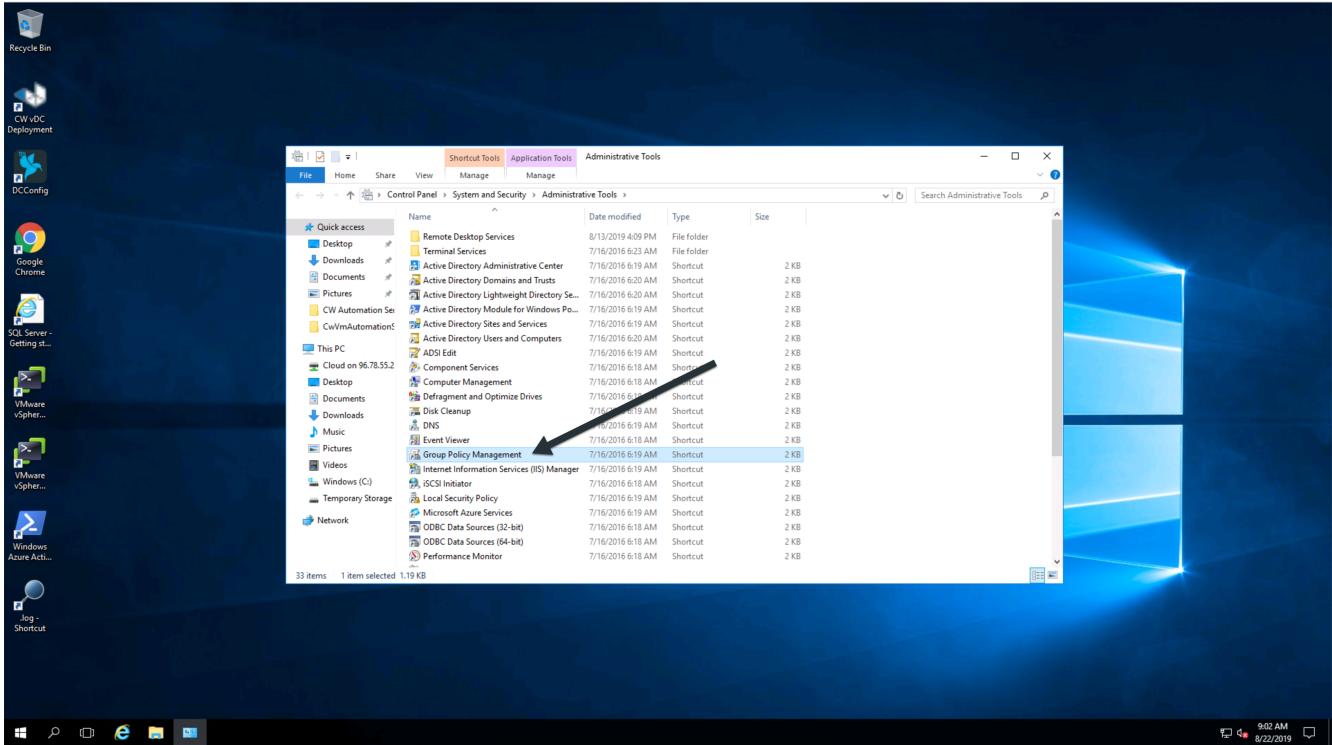
6. Enter the “Tech” credentials you created during provisioning to log on to the CWMGR1 server using HTML5 access.



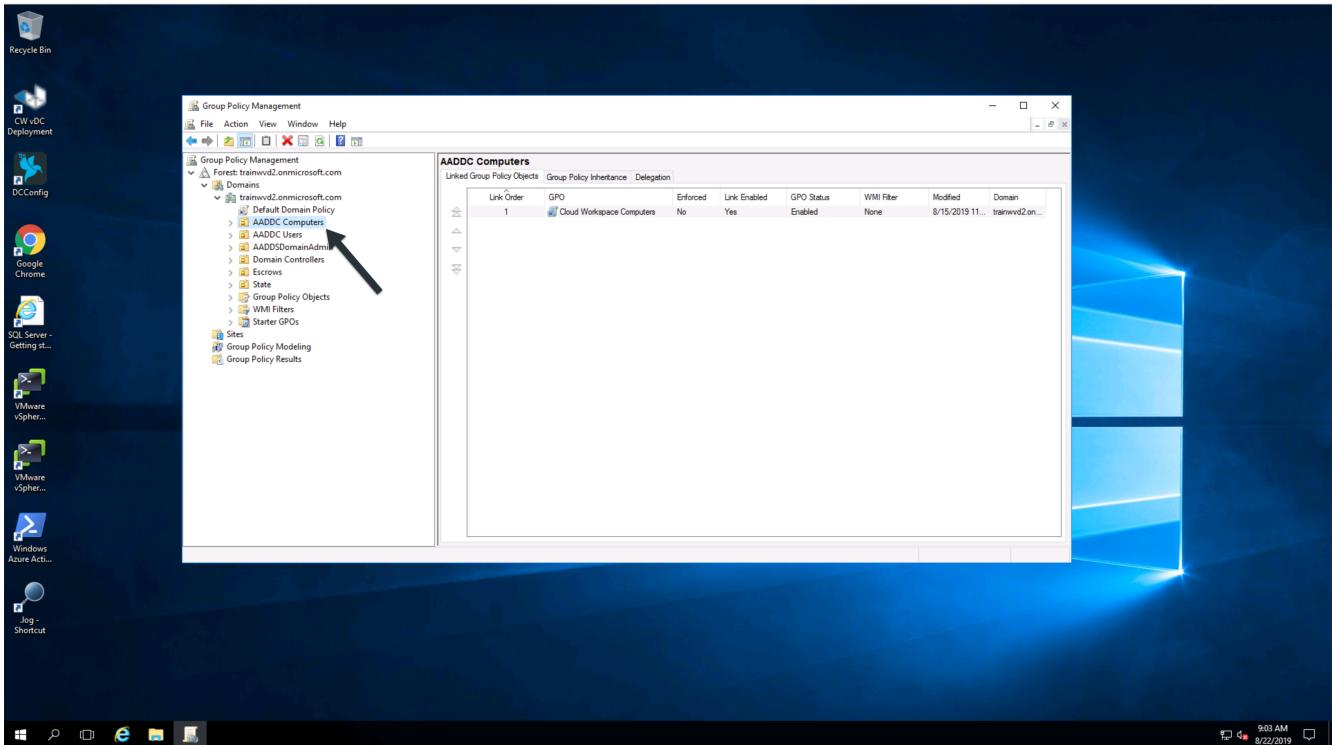
7. Click the Start (Windows) menu, choose Windows Administrative Tools.



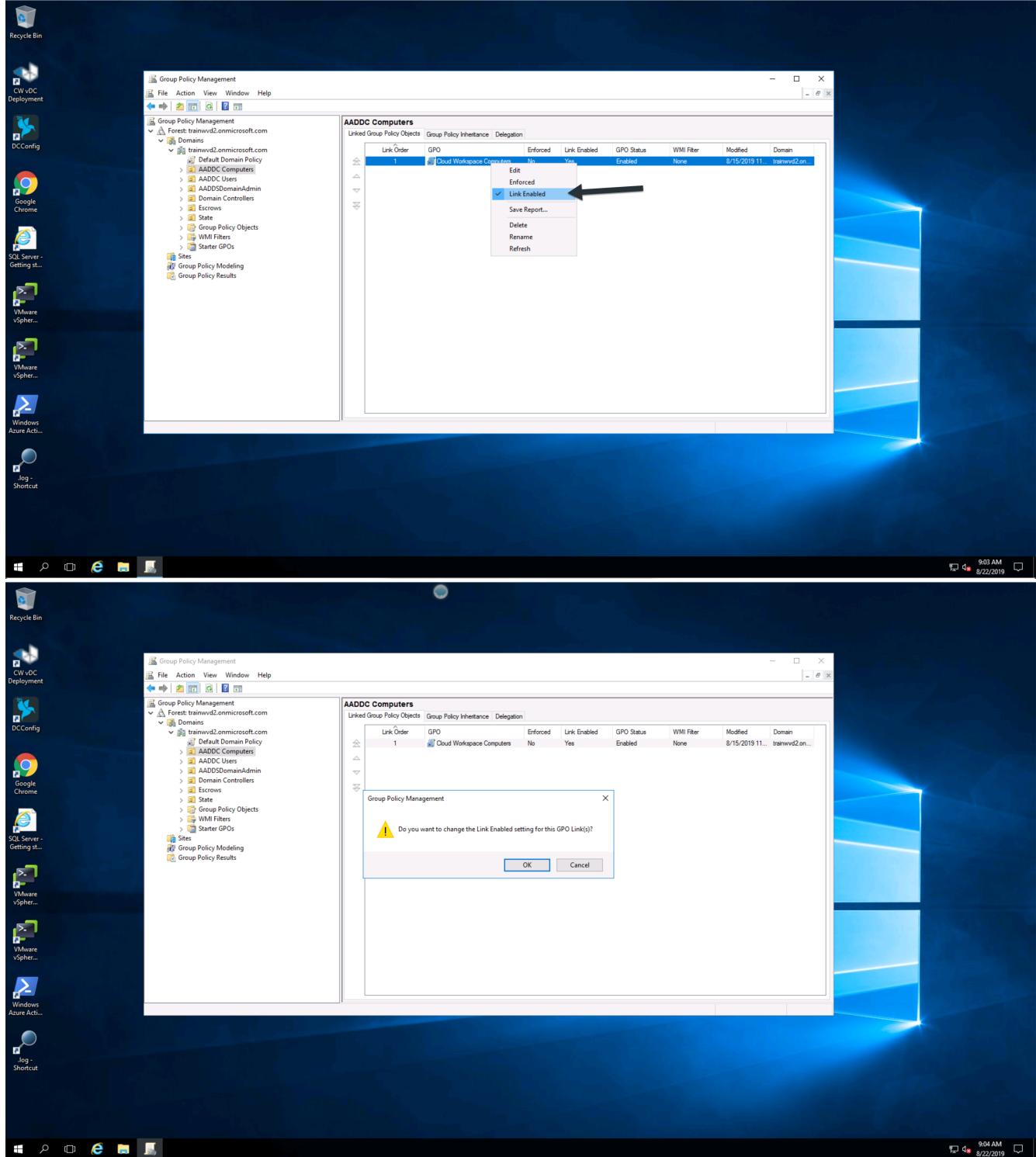
8. Click the Group Policy Management icon.



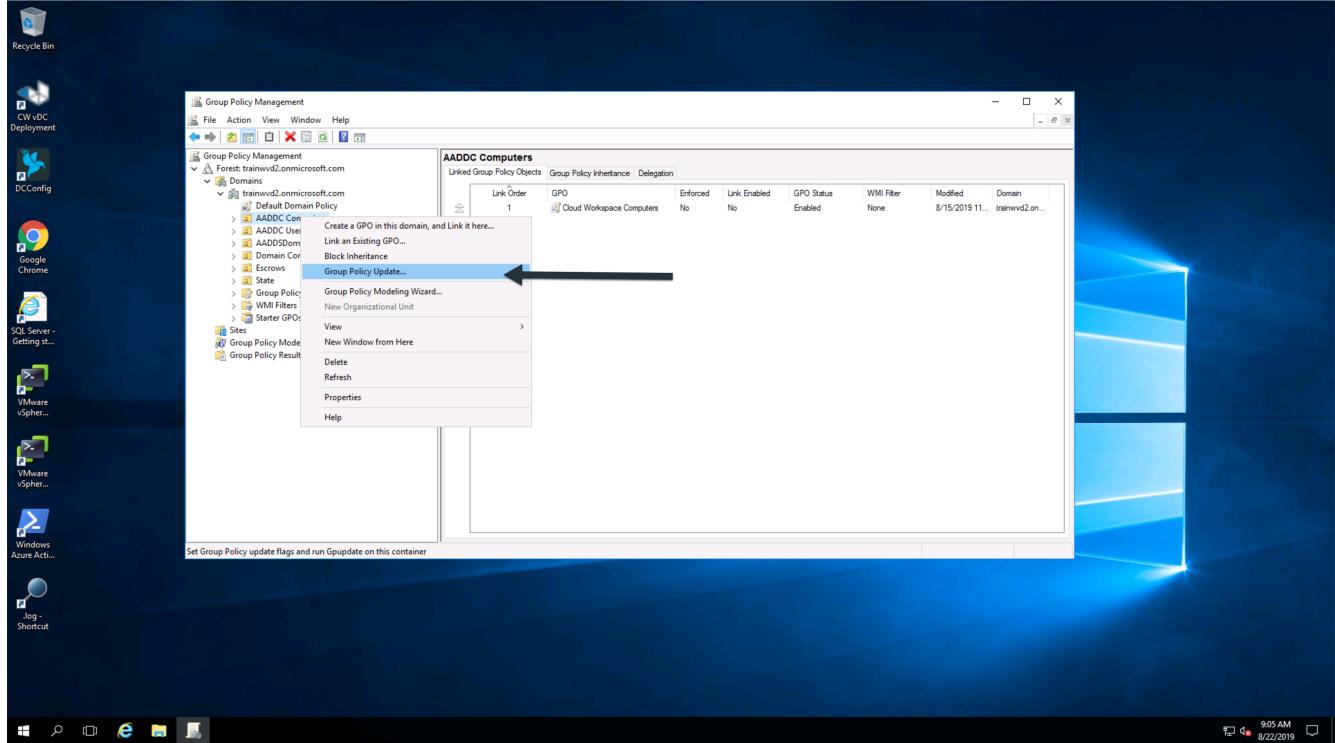
9. Click on the AADDC Users item in the list in the left pane.



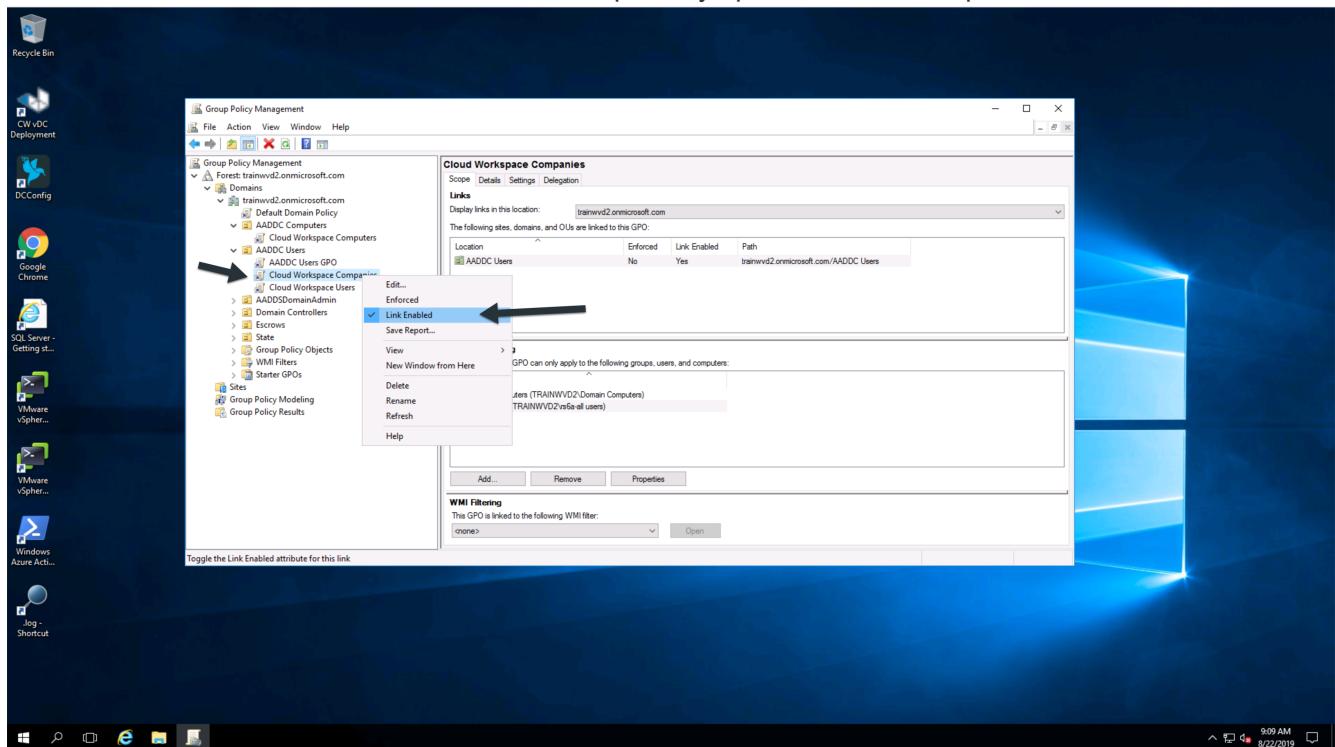
10. Right click on the "Cloud Workspace Users" policy in the list on the right pane, then deselect the "Link Enabled" option. Click OK to confirm this action.

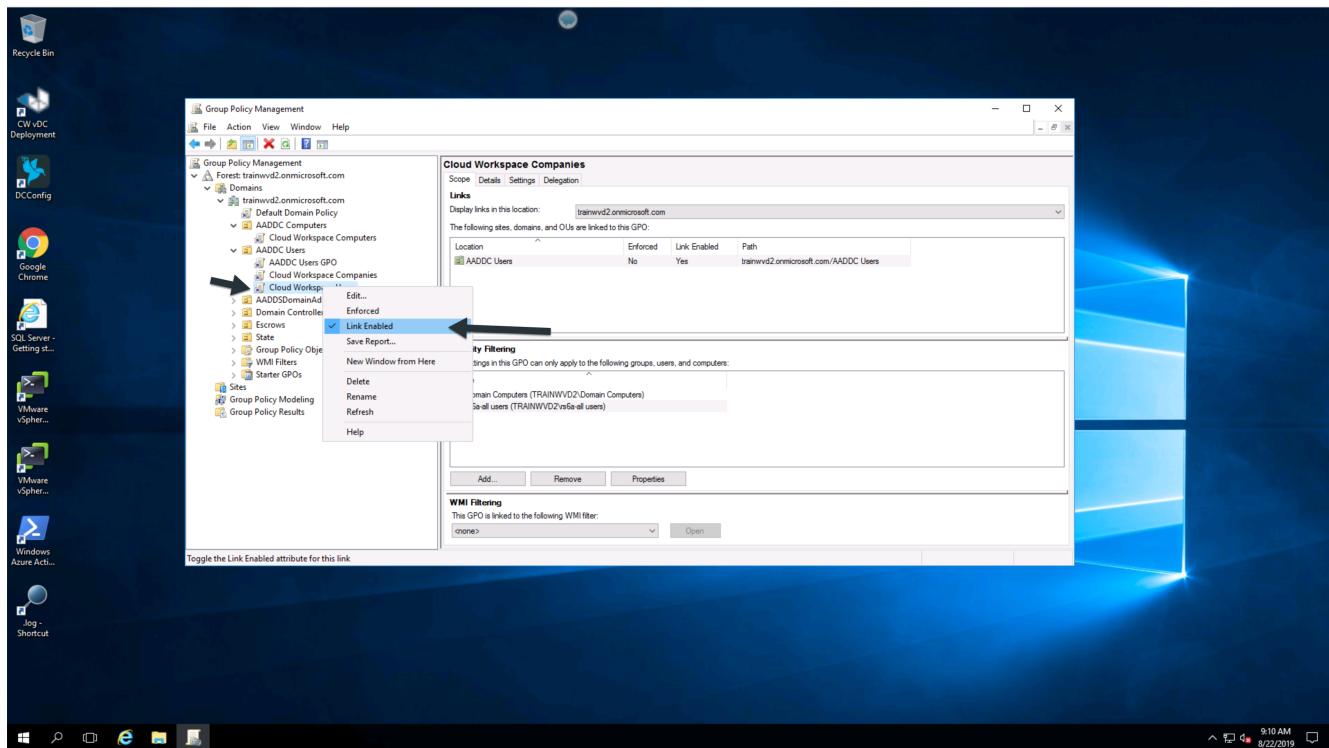


11. Select Action, Group Policy Update from the menu, then confirm that you want to force a policy update on those computers.

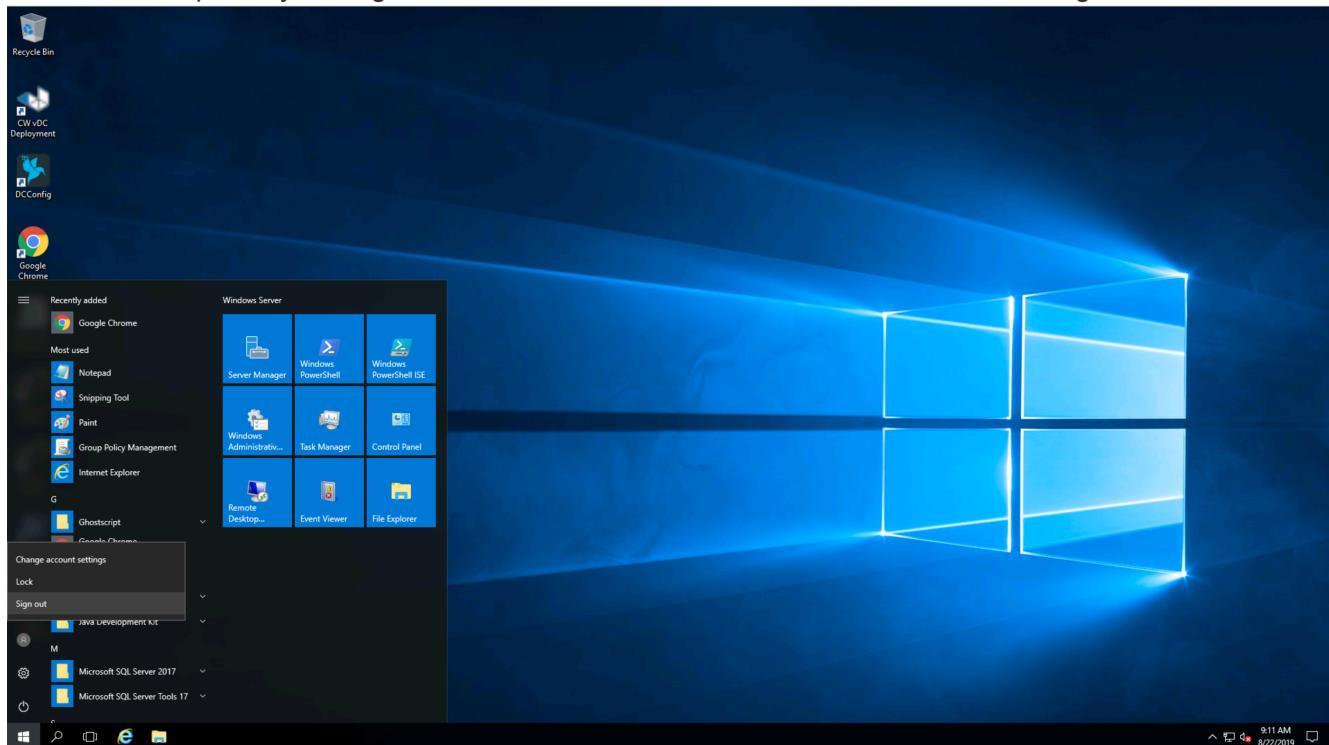


12. Repeat steps 9 and 10 but select “AADDC Users” and “Cloud Workspace Companies” as the policy to disable the Link. You do not need to force a Group Policy update after this step.





13. Close the Group Policy Management editor and Administrative Tools windows, then Log Off.



These steps will provide a basic workspace environment for end users. To confirm, log in as one of your end user accounts – the session environment should not have any of the Controlled Workspace restrictions like hidden Start menu, locked down access to the C:\ drive, and hidden Control Panel.

 The .tech account that was created during deployment has full access to install applications and change security on folders independent of VDS. However, if you want end users from the Azure AD domain to have similar full access, you should add them to the Local Administrators group on each virtual machine.

AVD Deployment Guide - Existing AD Supplemental

Overview

VDS Setup has the ability to connect a new deployment to an existing AD structure. These instruction cover that option in detail.

This article does not stand-alone, rather it is a detailed explanation of an alternative to the New AD option covered in the [AVD Deployment Guide](#)

Active Directory type

The next section defines the Active Directory deployment type for the VDS deployment. In this guide we will select Existing Windows Server Active Directory, which will leverage an AD structure that already exists.

Existing AD network

VDS Setup will display a list of vNets that could represent the connection between the existing AD structure and Azure AD. The vNet that you select should have the an Azure-hosted DC that you have configured in Azure. In addition, the vNet will have Custom DNS settings pointed at the Azure-hosted DC.

The screenshot shows the Microsoft Azure portal interface. The URL in the address bar is <https://portal.azure.com/#@trainingpulliam.onmicrosoft.com/resources>. The page title is "rzq | DNS servers". On the left, there's a sidebar with navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, and Address space. The main content area shows a list of "DNS servers". There are two options: "Default (Azure-provided)" (unchecked) and "Custom" (checked). Below the list, the IP address "10.0.0.4" is shown, followed by an "Add DNS server" button and three dots. At the top right, there are "Save" and "Discard" buttons.

Existing Active Directory domain name

Enter the existing domain name that will be used. Note: you do not want to use the domain that is found in the Azure Portal under the Active Directory module, as it can cause DNS issues. The primary example of this is that users will not be able to access the that website (<yourdomain>.com, for example) from inside their desktop.

Existing AD username and password

There are three ways to provide the credentials necessary to facilitate a deployment using an existing AD structure.

1. Provide Active Directory Domain Admin Username and Password

This is the easiest method – providing domain admin credential that are used to facilitate the deployment.



This account can be created for a one-time purpose and be deleted once the deployment process is complete.

2. Create Account Matching Required Permissions

This method involves customer administrators manually creating the permission structure here, then entering the credentials for the CloudWorkspaceSVC account here and proceeding.

3. Manual Deployment Process

Contact NetApp VDS Support for assistance configuring AD access with least privileged account principals.

Next Steps

This article covers the unique steps to deploy into an existing AD environment. With these steps complete, you can return to the standard deployment guide [here](#).

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-premises 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 with the VDS application via the VDS web app. This web portal is at: <https://manage.cloudworkspace.com>

Control plane database

VDS data and settings 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 Resource 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 manage 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

CWMGR1 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 file 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 file 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 file 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 join 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

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.

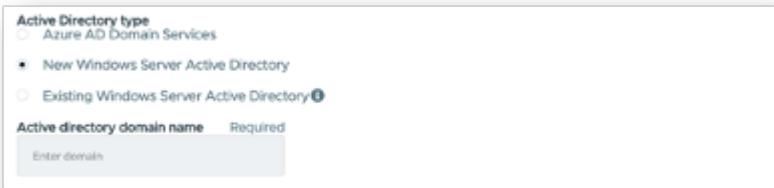
The Azure Marketplace provides the most recent versions of their base Windows 10 image and all Azure subscriptions have access to those automatically. If you want to use a different image or a custom image, want the VDS team to provide advice about creating or modifying other images or have general questions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

Active Directory

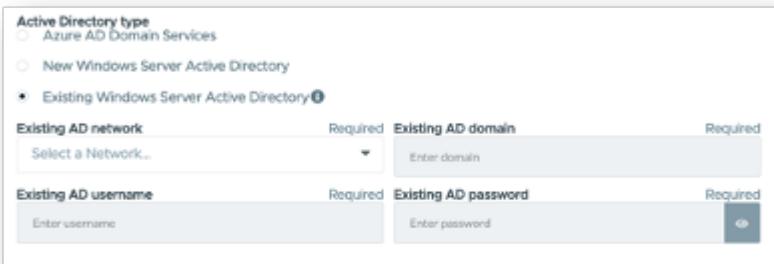
AVD requires that the user identity be a part of Azure AD and that the VMs are joined to an Active Directory domain that is synced with that same Azure AD instance. VMs cannot be attached directly to the Azure AD instance so a domain controller needs to be configured and in-sync with Azure AD.

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

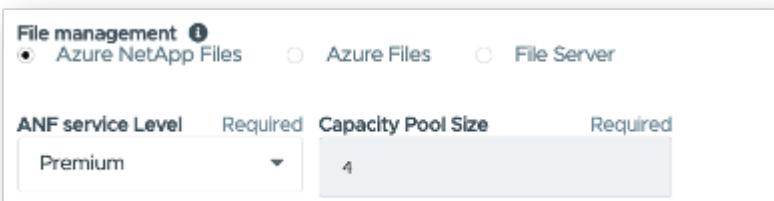
In AVD the storage strategy is designed so that no persistent user/company data resides on the AVD session VMs. Persistent data for user profiles, user files and folders, and corporate/application data are hosted on one or more data volume(s) hosted on an independent data layer.

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.

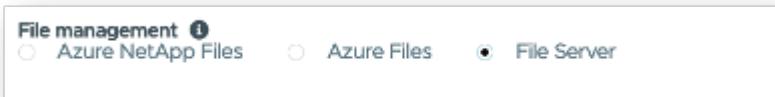
Due to this architecture a data storage function is required. This function must be able to handle the data transfer required each morning/afternoon when a significant portion of the users login/logoff at the same time. Even moderately sized environments can have significant data transfer requirements. 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 DCCConfig.

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 it in 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 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

Address	Outbound TCP Port	Purpose	Service Tag
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
*.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

AVD and VDS v6.0 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.

Active Directory type

- Azure AD Domain Services
- New Windows Server Active Directory
- Existing Windows Server Active Directory ?

Active directory domain name Required

Enter domain

- 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.

Active Directory type

- Azure AD Domain Services
- New Windows Server Active Directory
- Existing Windows Server Active Directory ?

Existing AD network Required

Select a Network...

Existing AD domain Required

Enter domain

Existing AD username Required

Enter username

Existing AD password Required

Enter password

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.*

File management ?

- Azure NetApp Files
- Azure Files
- File Server

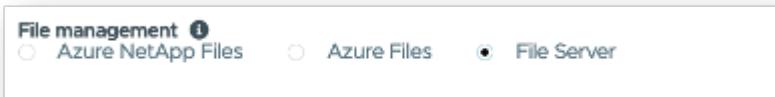
ANF service Level Required

Premium

Capacity Pool Size Required

4

- 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 DCCConfig.

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 it in 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 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/vdctoolsapiprimary.azurewebsites.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

Address	Outbound TCP Port	Purpose	Service Tag
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
*.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

Google

RDS Deployment Guide for Google Cloud (GCP)

Overview

This guide will provide the step by step instructions to create a Remote Desktop Service (RDS) deployment utilizing NetApp Virtual Desktop Service (VDS) in Google Cloud.

This Proof of Concept (POC) guide is designed to help you quickly deploy and configure RDS in your own test GCP Project.

Production deployments, especially into existing AD environments are very common however that process is not considered in this POC Guide. Complex POCs and production deployments should be initiated with the NetApp VDS Sales/Services teams and not performed in a self-service fashion.

This POC document will take you thru the entire RDS deployment and provide a brief tour of the major areas of post-deployment configuration available in the VDS platform. Once completed you'll have a fully deployed and functional RDS environment, complete with session hosts, applications and users. Optionally you'll have the option to configure automated application delivery, security groups, file share permissions, Cloud Backup, intelligent cost optimization. VDS deploys a set of best practice settings via GPO. Instructions on how to optionally disable those controls are also included, in the event your POC needs to have no security controls, similar to an unmanaged local device environment.

Deployment architecture



RDS basics

VDS deploys a fully functional RDS environment, with all necessary supporting services from scratch. This functionality can include:

- RDS gateway server(s)
- Web client access server(s)
- Domain controller server(s)
- RDS licensing service
- ThinPrint licensing service
- Filezilla FTPS server service

Guide scope

This guide walks you through the deployment of RDS using NetApp VDS technology from the perspective of a GCP and VDS administrator. You bring the GCP project with zero pre-configuration and this guide helps you setup RDS end-to-end.

Create service account

1. In GCP, navigate to (or search for) *IAM & Admin > Service Accounts*

The screenshot shows the Google Cloud Platform dashboard for a project named 'VDS Sandbox G6'. The left sidebar navigation includes sections for Home, Recent, Marketplace, Billing, APIs & Services, Support, IAM & Admin (selected), Getting started, Security, Anthos, Compute (App Engine, Compute Engine, Kubernetes Engine, Cloud Functions, Cloud Run, VMware Engine), Storage (Bigtable, Datastore), and a link to https://console.cloud.google.com/iam-admin/serviceaccounts?authuser=2&project=vds-sandbox-g6. The main dashboard area displays 'Project info' (Project name: VDS Sandbox G6, Project ID: vds-sandbox-g6, Project number: 967069066092), 'APIs' (Requests (requests/sec) chart showing no data available), 'Google Cloud Platform status' (All services normal), 'Billing' (Estimated charges USD \$0.00 for Sep 1 - 29, 2020), 'Monitoring' (Set up alerting policies, Create uptime checks, View all dashboards, Go to Monitoring), 'Error Reporting' (No sign of any errors, Learn how to set up Error Reporting), and 'News'.

2. Click + CREATE SERVICE ACCOUNT

Service accounts for project "VDS Sandbox G6"
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more about service accounts.](#)
Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. [Learn more about service account organization policies.](#)

3. Enter a unique service account name, click **CREATE**. Make a note of the service account's email address which will be used in a later step.

Create service account

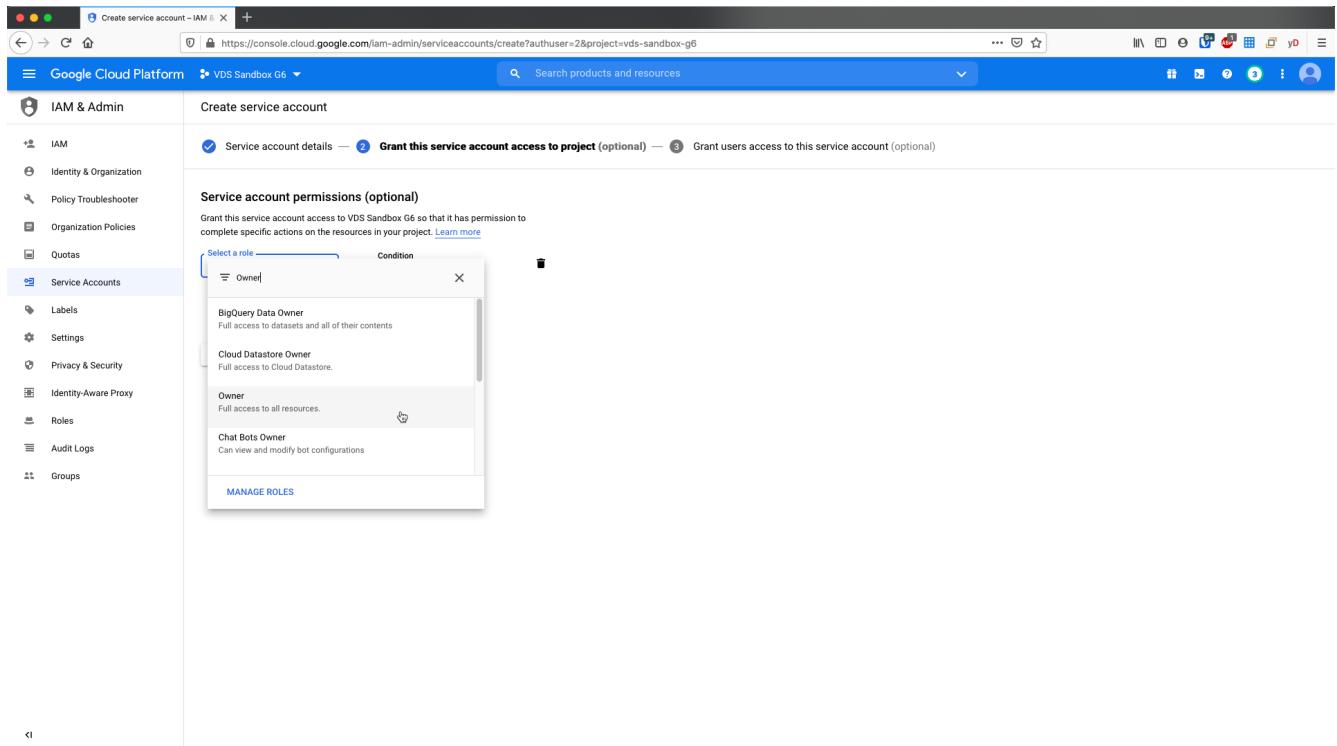
1 Service account details — 2 Grant this service account access to project (optional) — 3 Grant users access to this service account (optional)

Service account details

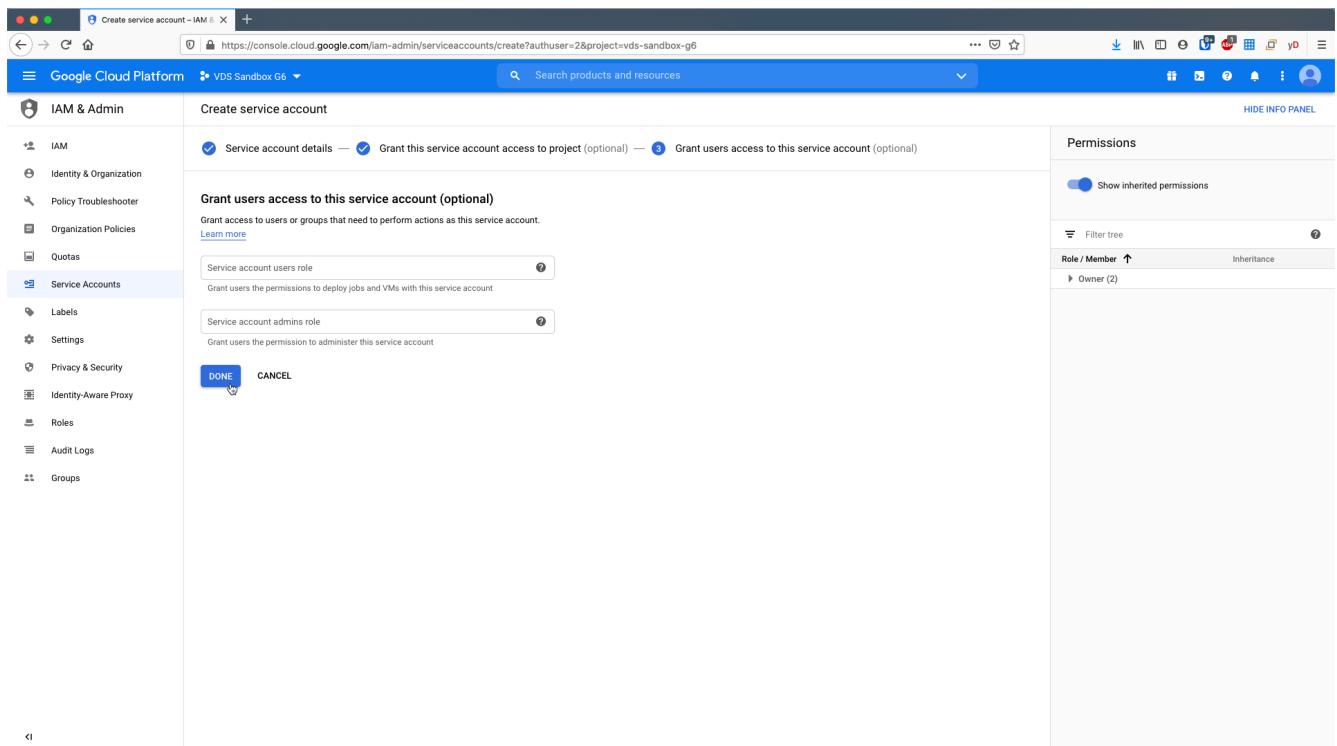
Service account name: novavelocity
Display name for this service account
Service account ID: novavelocity @vds-sandbox-g6.iam.gserviceaccount.com
Service account description: VDS deploy for Toby
Describe what this service account will do

CREATE CANCEL

4. Select the **Owner** role for the service account, click **CONTINUE**



5. No changes are necessary on the next page (*Grant users access to this service account(optional)*), click **DONE**



6. From the *Service accounts* page, click the action menu and select *Create key*

Service accounts for project "VDS Sandbox G6"

Email	Status	Name	Description	Key ID	Key creation date	Actions
novavelocity@vds-sandbox-g6.iam.gserviceaccount.com	Green	novavelocity	VDS deploy for Toby	No keys		⋮

7. Select P12, click CREATE

Create private key for "novavelocity"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

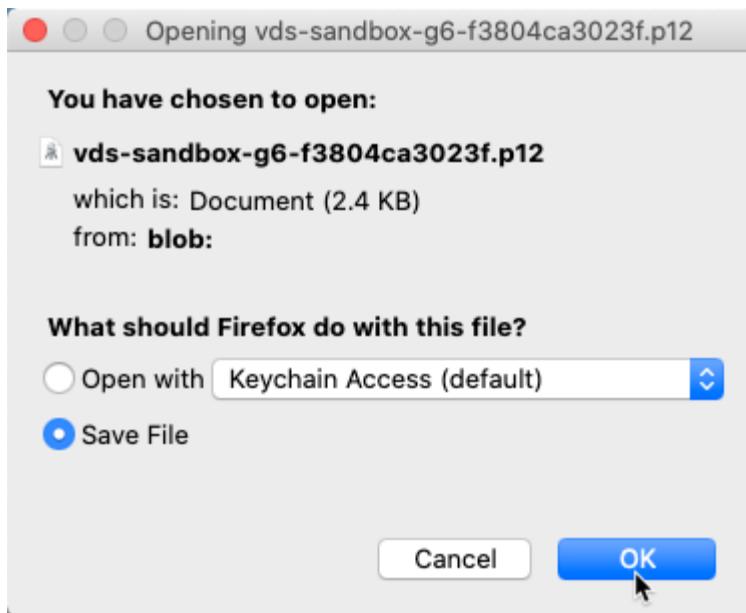
Key type

JSON
Recommended

P12
For backward compatibility with code using the P12 format

CANCEL CREATE

8. Download the .P12 file and save it to your computer. Leaved the *Private key password* unchanged.



Enable Google compute API

1. In GCP, navigate to (or search for) *APIs & Services > Library*

Google Cloud Platform - VDS Sandbox G6

IAM & Admin

Service accounts

CREATE SERVICE ACCOUNT

Service accounts for project "VDS Sandbox G6"

A service account represents a Google Cloud service identity, such as code running in Google Compute Engine.

Organization policies can be used to secure service accounts and block risky service accounts.

Filter table

Email novelocity@vds-sandbox-g6.iam.gserviceaccount.com

LIBRARY

APIs & Services

RPI RxNorm National Library of Medicine

RPI Library Agent API NIH LINCS Program

RPI Photos Library API

RPI AbanteCart Certified by Bitnami Bitnami

RPI AISE PyTorch CPU Notebook Jetware

RPI AISE PyTorch CPU Production Jetware

RPI AISE PyTorch Nvidia GPU Production Jetware

RPI AISE TensorFlow CPU Notebook Jetware

RPI AISE TensorFlow Nvidia GPU Notebook Jetware

RPI Caffe Python 3.6 Nvidia GPU Production Jetware

RPI CanvasJS for Data Visualization & Analytics Fenopix

RPI Coppermine Mini Infotech

RPI Coppermine on Ubuntu 16.04 LTS Cognosys Inc.

RPI Custom Governance Custom Governance

Manage resources

<https://console.cloud.google.com/apis/library?authuser=2&project=vds-sandbox-g6>

2. In the GCP API Library, navigate to (or search for) *Compute Engine API*, Click *ENABLE*

Google Cloud Platform - VDS Sandbox G6

Search products and resources

Search

comput engine

Filter by

CATEGORY

Big data (1)

Compute (5)

Developer tools (1)

Financial services (1)

Google Cloud APIs (2)

Networking (1)

Storage (1)

Other (3)

10 results

Compute Engine API

Google Compute Engine API

Compute Engine Instance Group Manager API

Google Compute Engine Instance Group Manager API provides services for creating and...

App Engine Admin API

Google Provisions and manages developers' App Engine applications.

Kubernetes Engine API

Google Builds and manages container-based applications, powered by the open source Kubernetes tec...

Google App Engine Flexible Environment

Google This service enables App Engine's Flexible Environment, which gives you the benefits of App...

Compute Engine Instance Group Updater API

Google The Google Compute Engine Instance Group Updater API provides services for updating groups...

Compute Engine Instance Groups API

Google Google Compute Engine Instance Groups API provides services for grouping together cloud inst...

Web Security Scanner API

Google

<https://console.cloud.google.com/apis/library/compute.googleapis.com?q=compute+engine&id=a08439d8-80d6-43f1-a72e-6878251018d&project=vds-sandbox-g6&authuser=2>

Create new VDS deployment

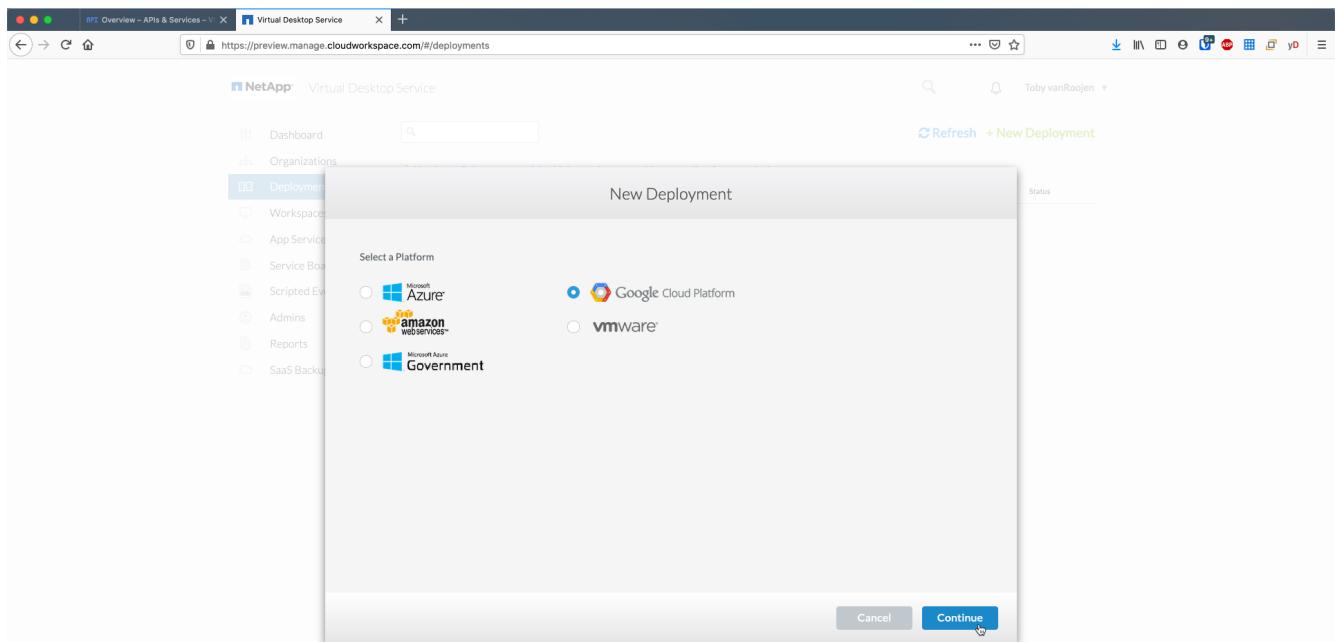
1. In VDS, navigate to *Deployments* and click *+ New Deployment*

The screenshot shows the NetApp Virtual Desktop Service interface. The left sidebar has a 'Deployments' section selected. A warning message at the top right says, '⚠ You have 5 deployment(s) which require manual intervention for completion'. The main area displays tabs for Deployment, Code, Version, Infrastructure Platform, Clients, Connection, and Status.

2. Enter a name for the deployment

The screenshot shows the 'New Deployment' dialog box. It contains a 'Deployment Name' field with the value 'GCP Deploy Demo'. There are 'Cancel' and 'Continue' buttons at the bottom. The background shows the same interface as the previous screenshot, with the 'Deployments' tab selected.

3. Select Google Cloud Platform

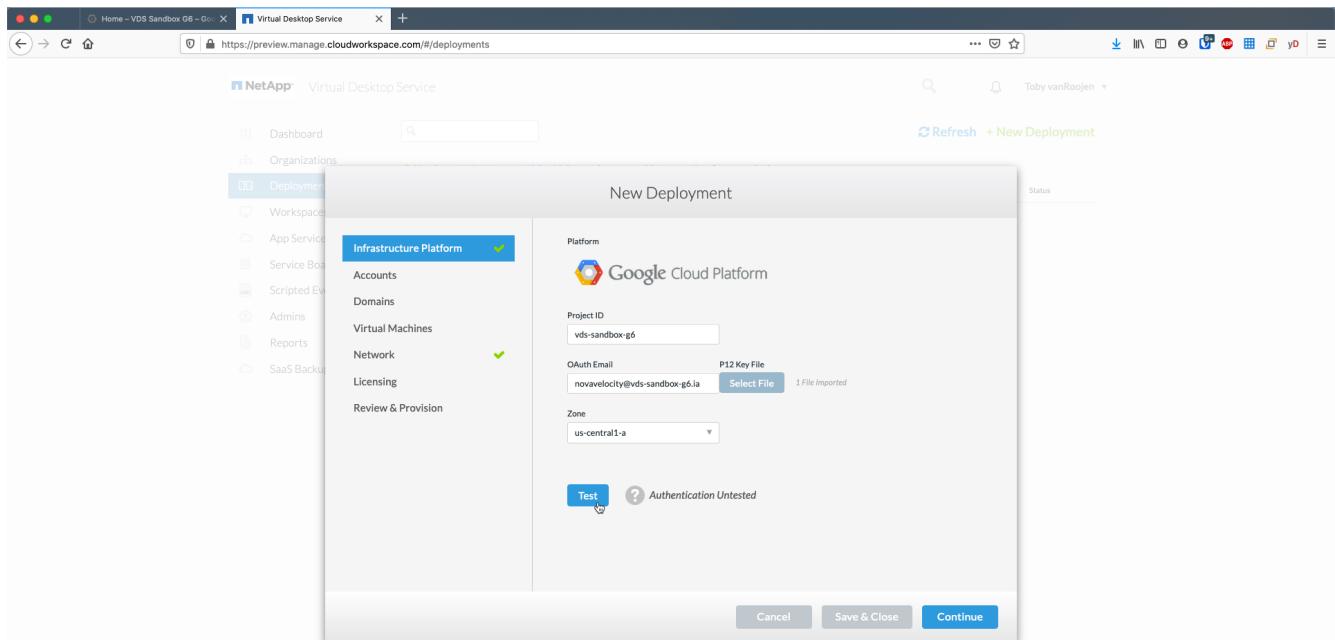


Infrastructure platform

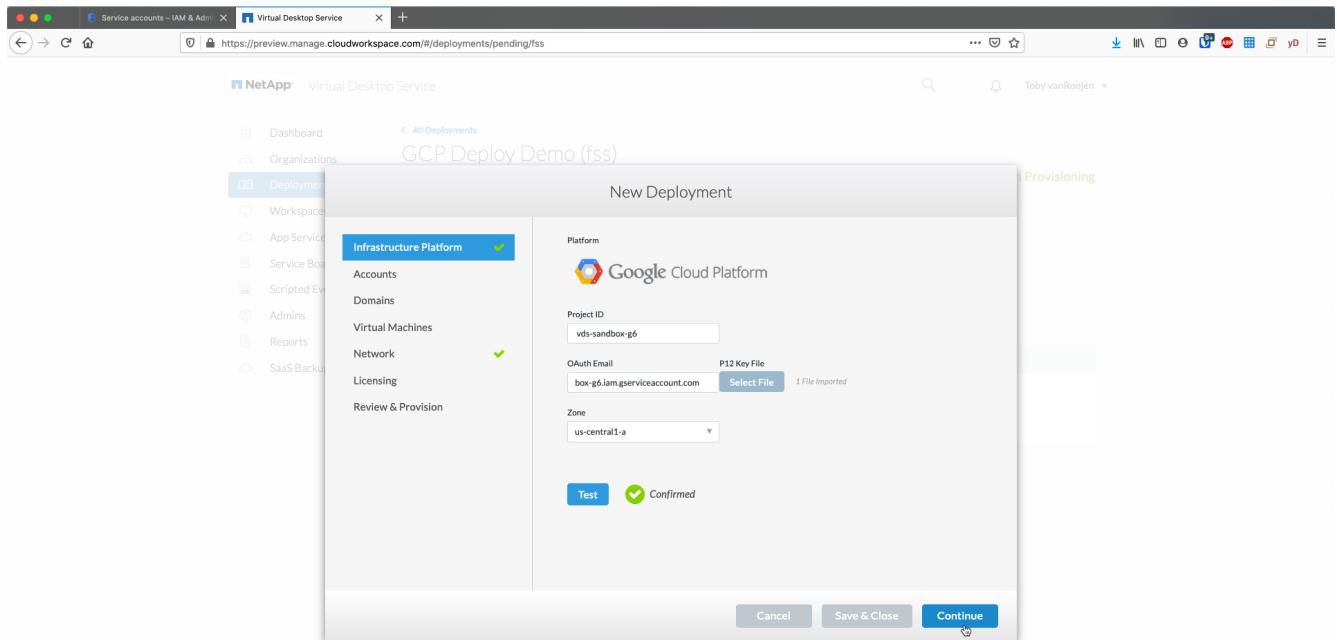
1. Enter the *Project ID* and OAuth Email address. Upload the .P12 file from earlier in this guide and select the appropriate zone for this deployment. Click *Test* to confirm the entries are correct and the appropriate permissions have been set.



The OAuth email is the address of the service account created earlier in this guide.



2. Once confirmed, click *Continue*



Accounts

Local VM accounts

1. Provide a password for the local Administrator account. Document this password for later use.
2. Provide a password for the SQL SA account. Document this password for later use.

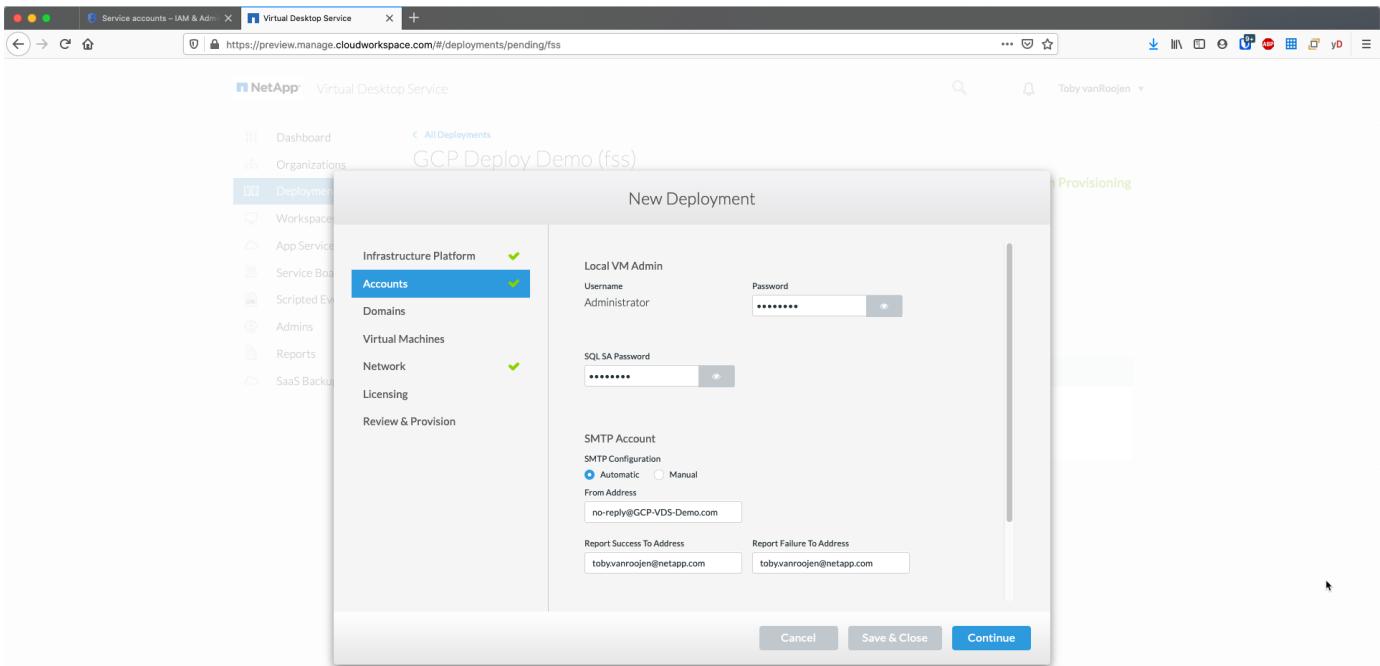


Password complexity requires an 8 character minimum with 3 of the 4 following character types: uppercase, lowercase, number, special character

SMTP account

VDS can send email notifications via custom SMTP settings or the built-in SMTP service can be used by selecting *Automatic*.

1. Enter an email address to be used as the *From* address when email notification are sent by VDS. *no-reply@<your-domain>.com* is a common format.
2. Enter an email address where success reports should be directed.
3. Enter an email address where failure reports should be directed.



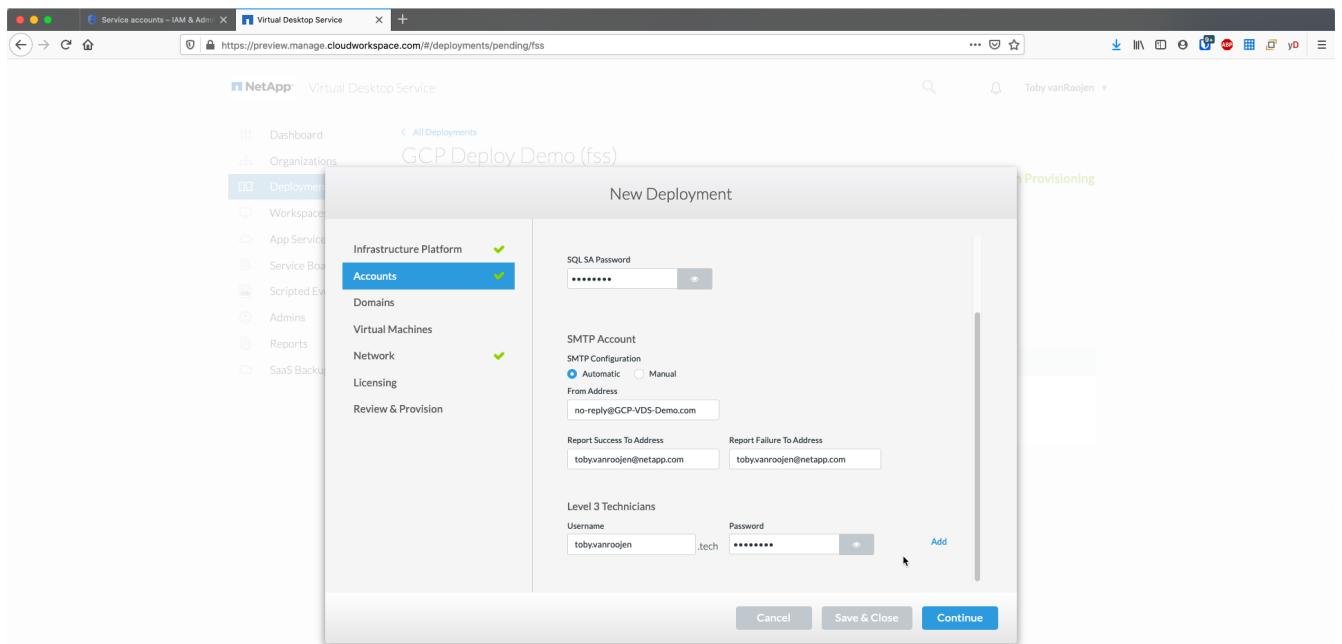
Level 3 technicians

Level 3 technician accounts (aka. *.tech accounts*) are domain-level accounts for VDS admins to use when performing administrative tasks on the VMs in the VDS environment. Additional accounts can be created on this step and/or later.

1. Enter the username and password for the Level 3 admin account(s). ".tech" will be appended to the user name you enter to help differentiate between end users and tech accounts. Document these credentials for later use.



The best practice is to define named accounts for all VDS admins that should have domain-level credentials to the environment. VDS admins without this type of account can still have VM-level admin access via the *Connect to server* functionality built into VDS.



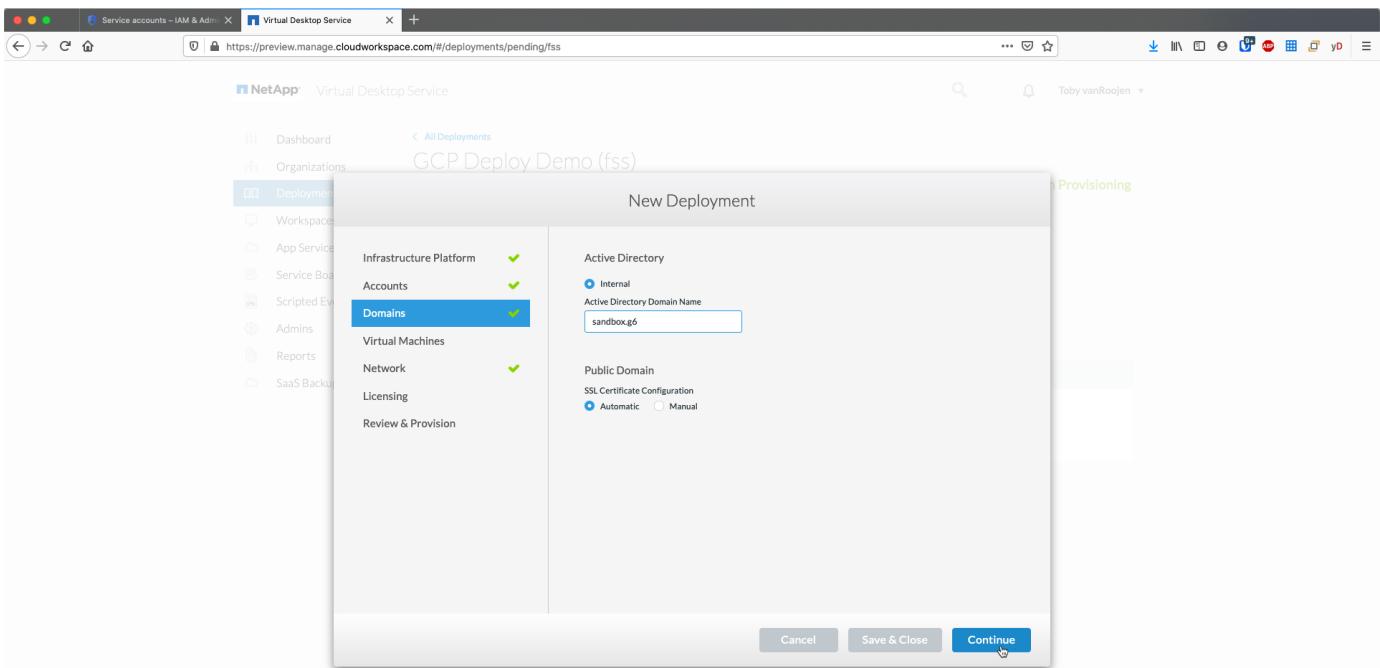
Domains

Active directory

Enter the desired AD domain name.

Public domain

External access is secured via an SSL certificate. This can be customized with your own domain and a self-managed SSL certificate. Alternatively, selecting *Automatic* allows VDS to manage the SSL certificate including an automatic 90-day refresh of the certificate. When using automatic, each deployment uses a unique sub-domain of *cloudworkspace.app*.



Virtual machines

For RDS deployments the required components such as domain controllers, RDS brokers and RDS gateways need to be installed on platform server(s). In production these services should be run on dedicated and redundant virtual machines. For proof of concept deployments a single VM can be used to host all of these services.

Platform VM configuration

Single virtual machine

This is the recommended selection for POC deployments. In a Single virtual machine deployment the following roles are all hosted on a single VM:

- CW Manager
- HTML5 Gateway
- RDS Gateway
- Remote App
- FTPS Server (Optional)
- Domain Controller

The maximum advised user count for RDS use cases in this configuration is 100 users. Load balanced RDS/HTML5 gateways are not an option in this configuration, limiting the redundancy and options for increasing scale in the future.



If this environment is being designed for multi-tenancy, a Single virtual machine configuration is not supported.

Multiple servers

When splitting the VDS Platform into Multiple virtual machines the following roles are hosted on dedicated VMs:

- Remote Desktop Gateway

VDS Setup can be used to deploy and configure one or two RDS Gateways. These gateways relay the RDS user session from the open internet to the session host VMs within the deployment. RDS Gateways handle an important function, protecting RDS from direct attacks from the open internet and to encrypt all RDS traffic in/out of the environment. When two Remote Desktop Gateways are selected, VDS Setup deploys 2 VMs and configures them to load balance incoming RDS user sessions.

- HTML5 Gateway

VDS Setup can be used to deploy and configure one or two HTML5 Gateways. These gateways host the HTML5 services used by the *Connect to Server* feature in VDS and the web-based VDS Client (H5 Portal). When two HTML5 Portals are selected, VDS Setup deploys 2 VMs and configures them to load balance incoming HTML5 user sessions.



When using Multiple server option (even if users will only connect via the installed VDS Client) at least one HTML5 gateway is highly recommended to enable *Connect to Server* functionality from VDS.

- Gateway Scalability Notes

For RDS use cases, the maximum size of the environment can be scaled out with additional Gateway VMs, with each RDS or HTML5 Gateway supporting roughly 500 users. Additional Gateways can be added later with minimal NetApp professional services assistance

If this environment is being designed for multi-tenancy then the *Multiple servers* selection is required.

Service roles

- Cwmgr1

This VM is the NetApp VDS administrative VM. It runs the SQL Express database, helper utilities and other administrative services. In a *single server* deployment this VM can also host the other services but in a *multiple server* configuration those services are moved to different VMs.

- CWPortal1(2)

The first HTML5 gateway is named *CWPortal1*, the second is *CWPortal2*. One or two can be created at deployment. Additional servers can be added post-deployment for increased capacity (~500 connections per server).

- CWRDSGateway1(2)

The first RDS gateway is named *CWRDSGateway1*, the second is *CWRDSGateway2*. One or two can be created at deployment. Additional servers can be added post-deployment for increased capacity (~500 connections per server).

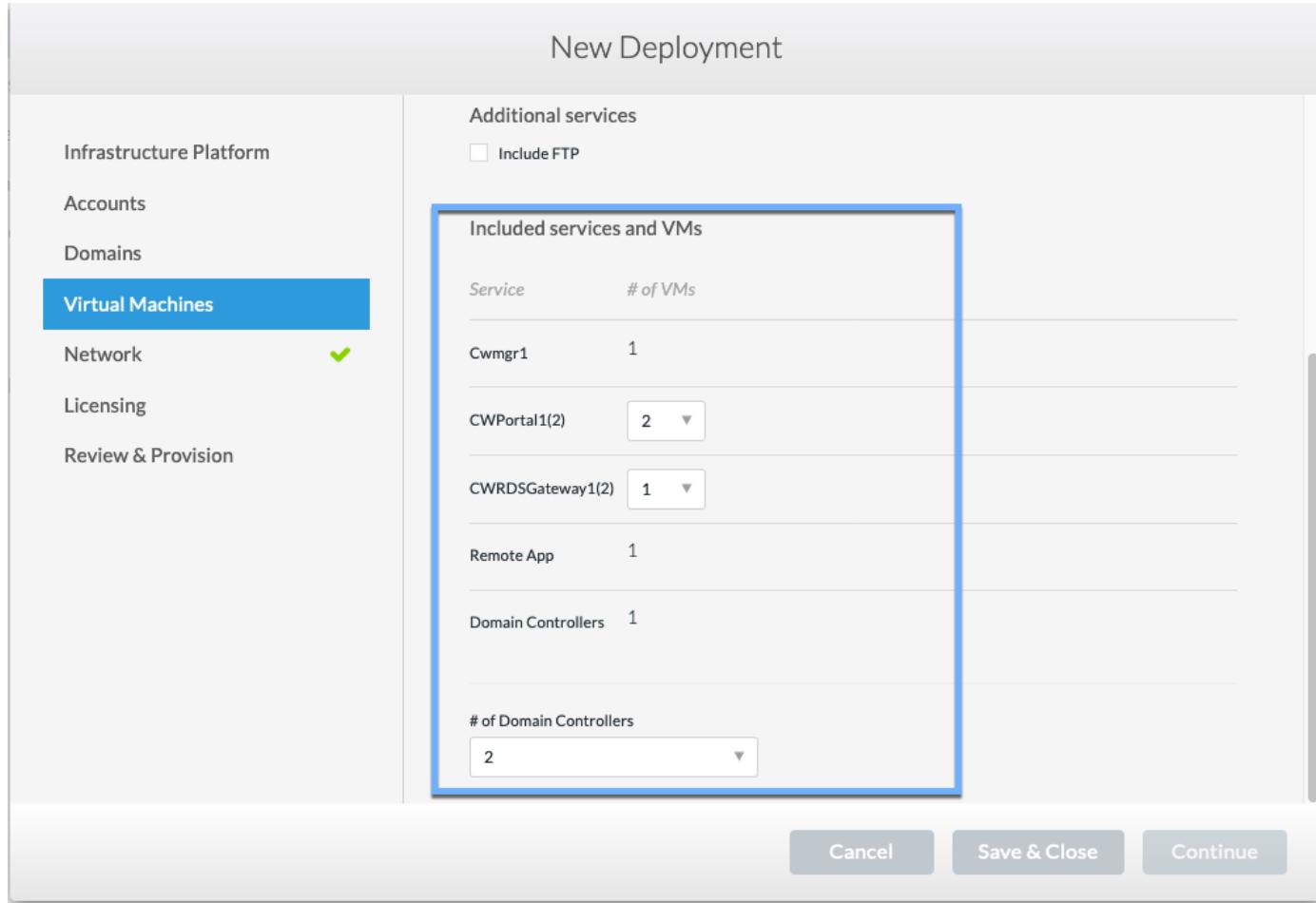
- Remote App

App Service is a dedicated collection for hosting RemotApp applications, but uses the RDS Gateways and

their RDWeb roles for routing end user session requests and hosting the RDWeb application subscription list. No VM dedicated vm is deployed for this service role.

- Domain Controllers

At deployment one or two domain controllers can be automatically built and configured to work with VDS.



Operating system

Select the desired server operating system to be deployed for the platform servers.

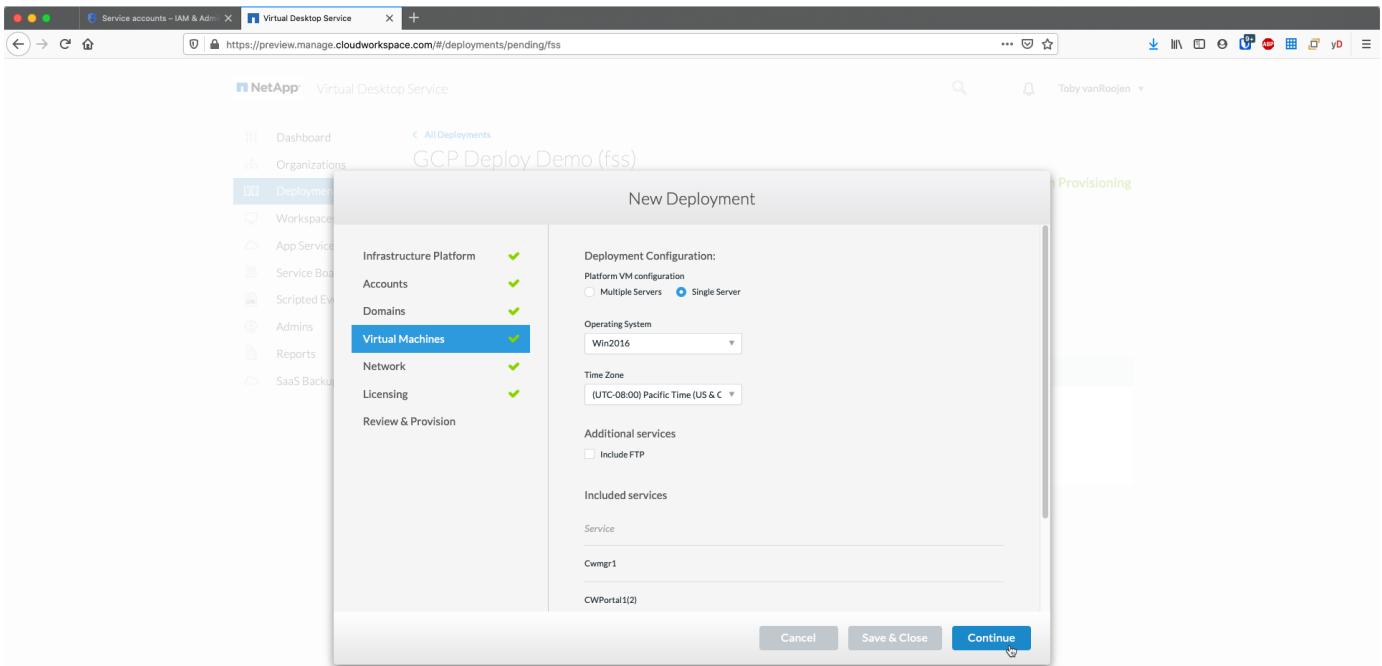
Time zone

Select the desired timezone. The platform servers will be configured to this time and log files will reflect this timezone. End user session will still reflect their own timezone, regardless of this setting.

Additional services

FTP

VDS can optional install and configure Filezilla to run an FTPS server for moving data in and out of the environment. This technology is older and more modern data transfer methods (like Google Drive) are recommended.



Network

It is a best practice to isolate VMs to different subnets according to their purpose.

Define the network scope and add a /20 range.

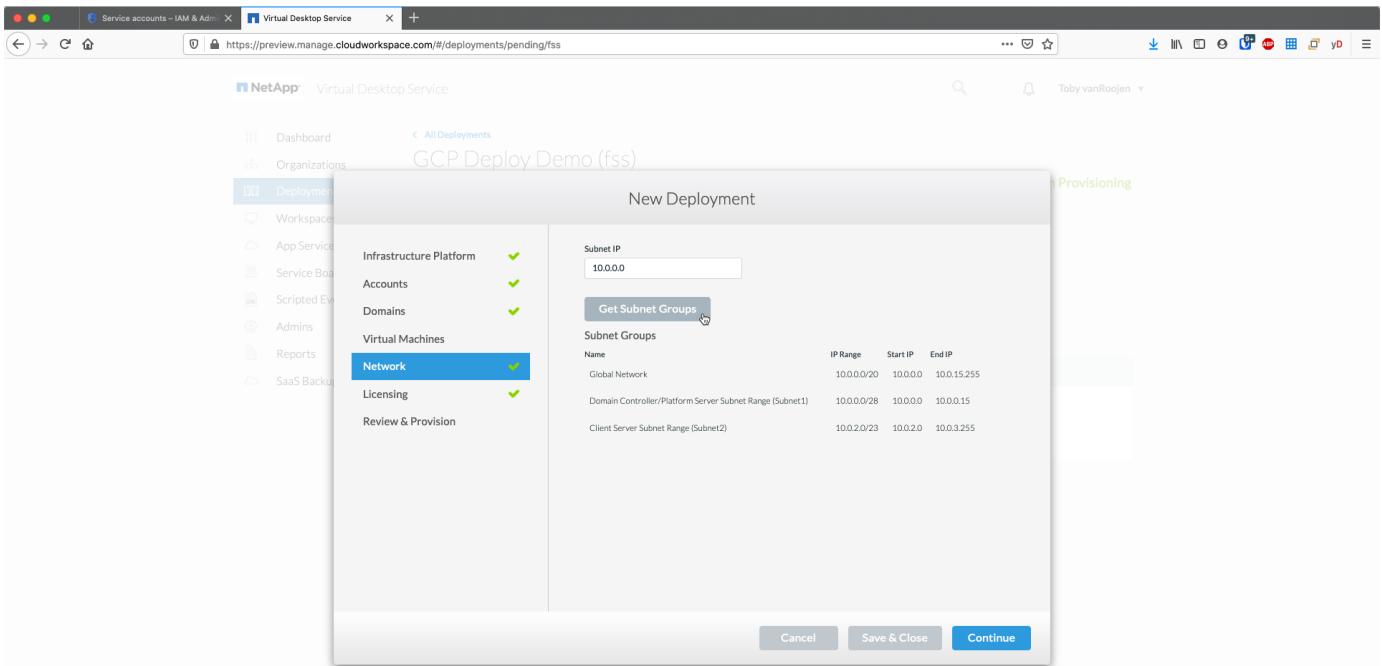
VDS Setup detects and suggests a range that should prove successful. Per best practices, the subnet IP addresses must fall into a private IP address range.

These ranges are:

- 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

Review and adjust if needed, then click Validate to identify subnets for each of the following:

- Tenant: this is the range in which session host servers and database servers will reside
- Services: this is the range in which PaaS services like Cloud Volumes Service will reside
- Platform: this is the range in which Platform servers will reside
- Directory: this is the range in which AD servers will reside



Licensing

SPLA

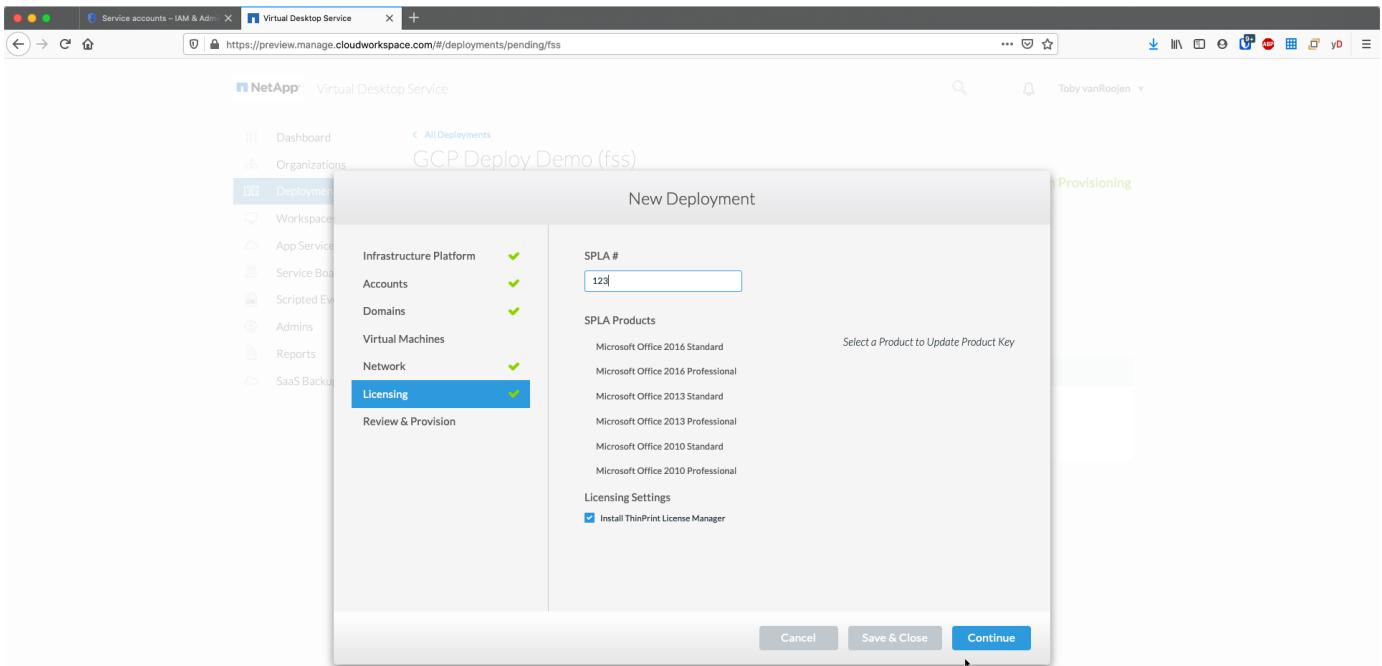
Enter your SPLA number so VDS can configure the RDS licensing service for easier SPLA RDS CAL reporting. A temporary number (such as 12345) can be entered for a POC deployment but after a trial period (~120 days) the RDS sessions will stop connecting.

SPLA products

Enter the MAK license codes for any Office products licensed via SPLA to enable simplified SPLA reporting from within VDS reports.

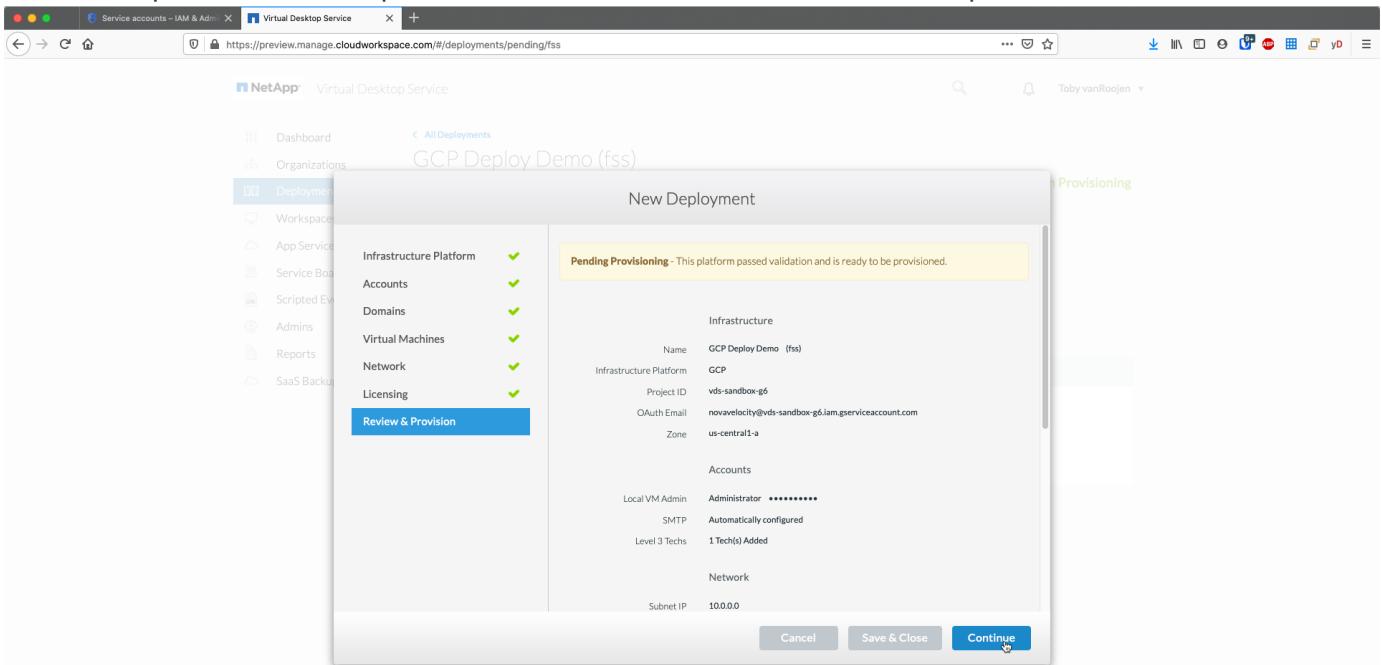
ThinPrint

Choose to install the included ThinPrint licensing server and license to simplify end user printer redirection.



Review & provision

Once all steps have been completed, review the selections, then validate and provision the environment.



Next steps

The deployment automation process will now deploy a new RDS environment with the options you selected throughout the deployment wizard.

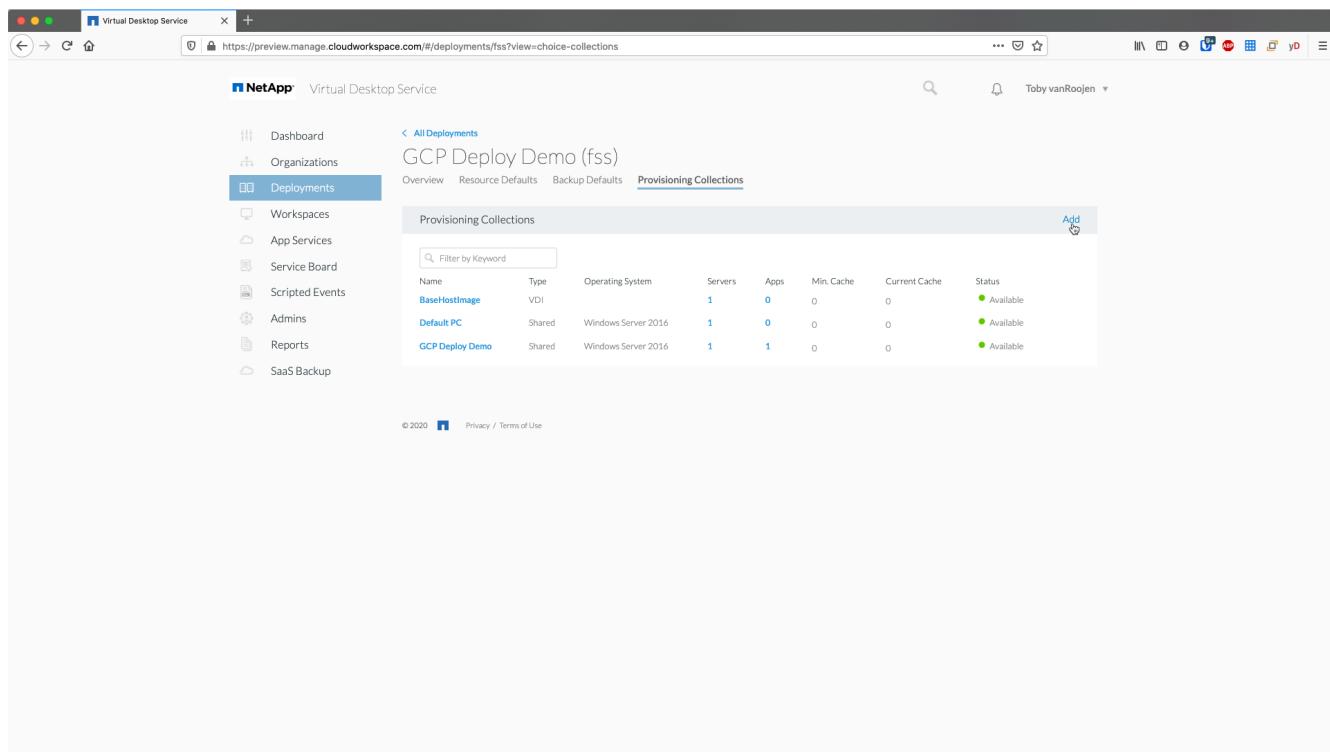
You'll receive multiple emails as the deployment completes. Once complete you'll have an environment ready for your first workspace. A workspace will contain the session hosts and data servers needed to support the end users. Come back to this guide to follow the next steps once the deployment automation completes in 1-2 hours.

Create a new provisioning collection

Provisioning collections is functionality in VDS that allows for the creation, customization and SysPrep of VM images. Once we get into the workplace deployment, we'll need an image to deploy and the following steps will guide you thru creating a VM image.

Follow these steps to create a basic image for deployment:

1. Navigate to *Deployments > Provisioning Collections*, click *Add*



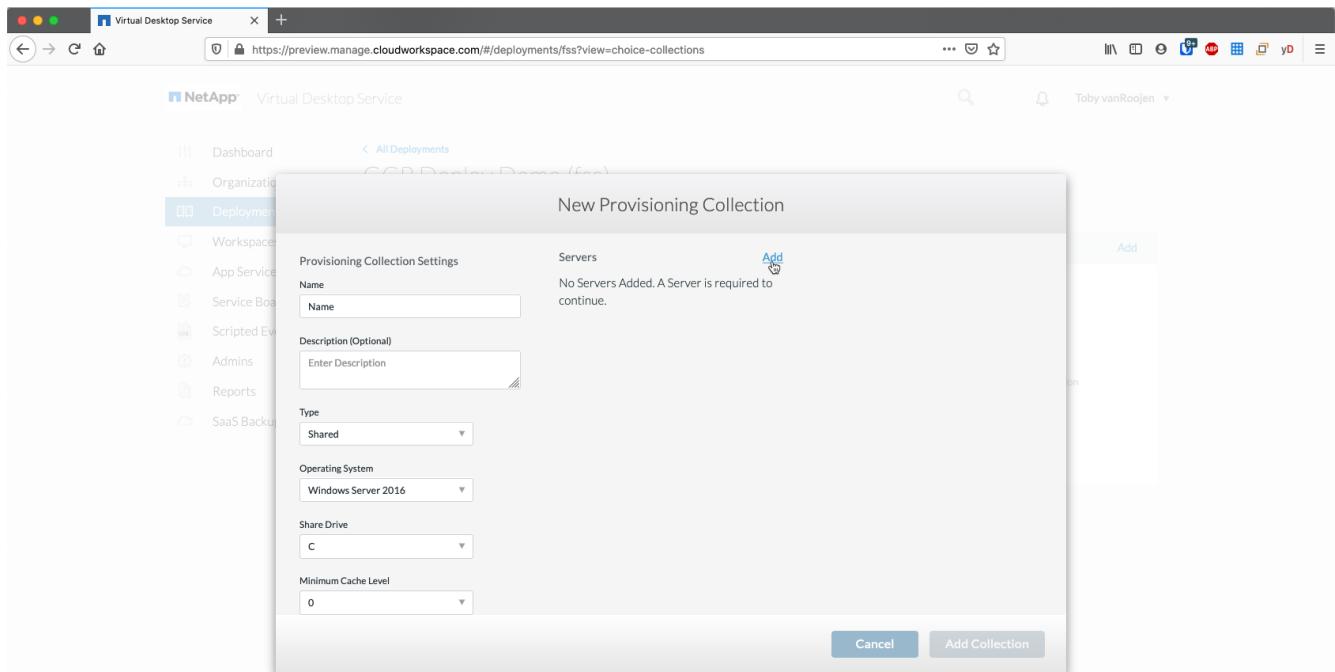
The screenshot shows the 'Virtual Desktop Service' interface. On the left, there's a sidebar with options like Dashboard, Organizations, Deployments (which is selected), Workspaces, App Services, Service Board, Scripted Events, Admins, Reports, and SaaS Backup. The main area is titled 'GCP Deploy Demo (fss)' and shows a table of 'Provisioning Collections'. The table has columns: Name, Type, Operating System, Servers, Apps, Min. Cache, Current Cache, and Status. It lists three items: 'BaseHostImage' (VDI, Windows Server 2016, 1 server, 0 apps, 0 cache, Available), 'Default PC' (Shared, Windows Server 2016, 1 server, 0 apps, 0 cache, Available), and 'GCP Deploy Demo' (Shared, Windows Server 2016, 1 server, 1 app, 0 cache, Available). At the top right of the main area, there's an 'Add' button with a cursor icon pointing at it. The URL in the browser bar is https://preview.manage.cloudworkspace.com/#/deployments/fss?view=choice-collections.

2. Enter a Name and Description. Choose *Type: Shared*.

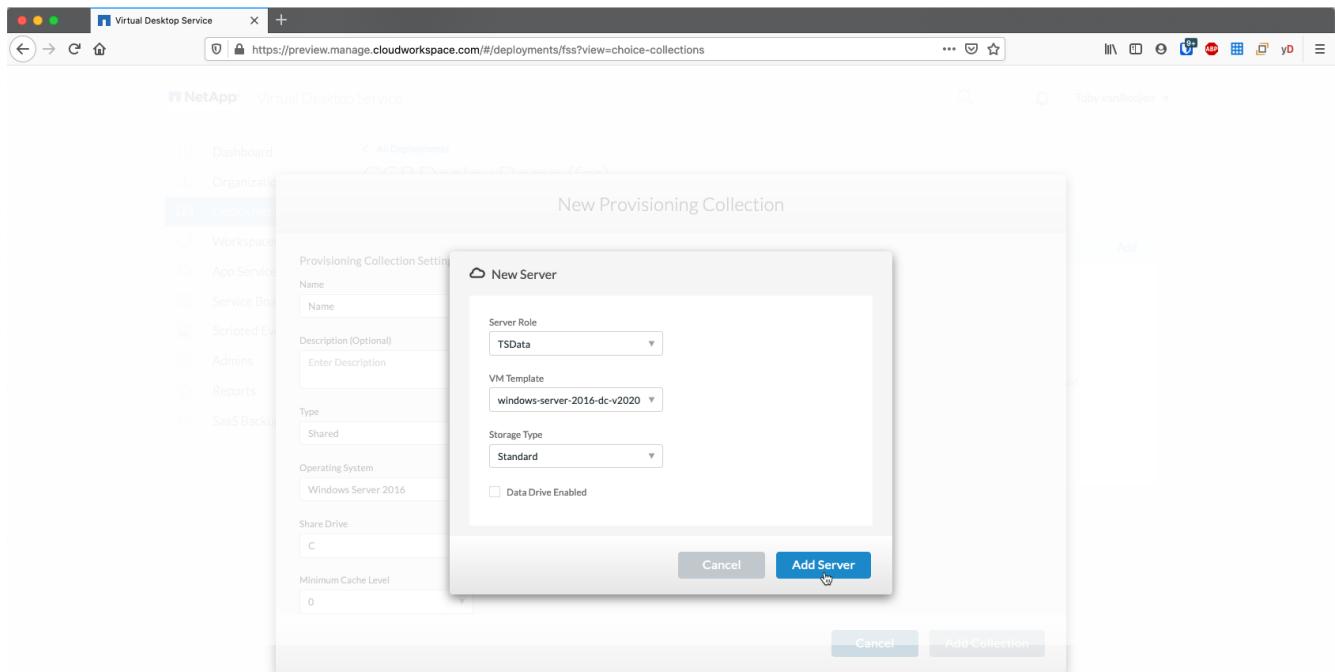


You can choose Shared or VDI. Shared will support a session server plus (optionally) a business server for applications like a database. VDI is a single VM image for VMs that will be dedicated to individual users.

3. Click *Add* to define the type of server image to build.



4. Select TSData as the **server role**, the appropriate VM image (Server 2016 in this case) and the desired storage type. Click **Add Server**



5. Optionally select the applications that will be installed on this image.

- a. The list of applications available is populated from the App Library that can be accessed by clicking the admin name menu in the upper right corner, under the *Settings > App Catalog* page.

VDS 5.4 Preview (6e2)

Company Overview App Catalog PAM Requests CWAutoPro API Contact Info

Application Catalog

App Catalog Type: Standard (radio button) Custom (radio button)

Application Visible To All

Toby vanRoojen ▾

My Account

Settings (selected)

Help

Sign Out

6. Click *Add Collection* and wait for the VM to be built. VDS will build a Vm that can be accessed and customized.
7. Once the VM build has completed, connect to the server and make the desired changes.
 - a. Once the status shows *Collection Validation*, click the collection name.

All Deployments < GCP Deploy Demo (fss)

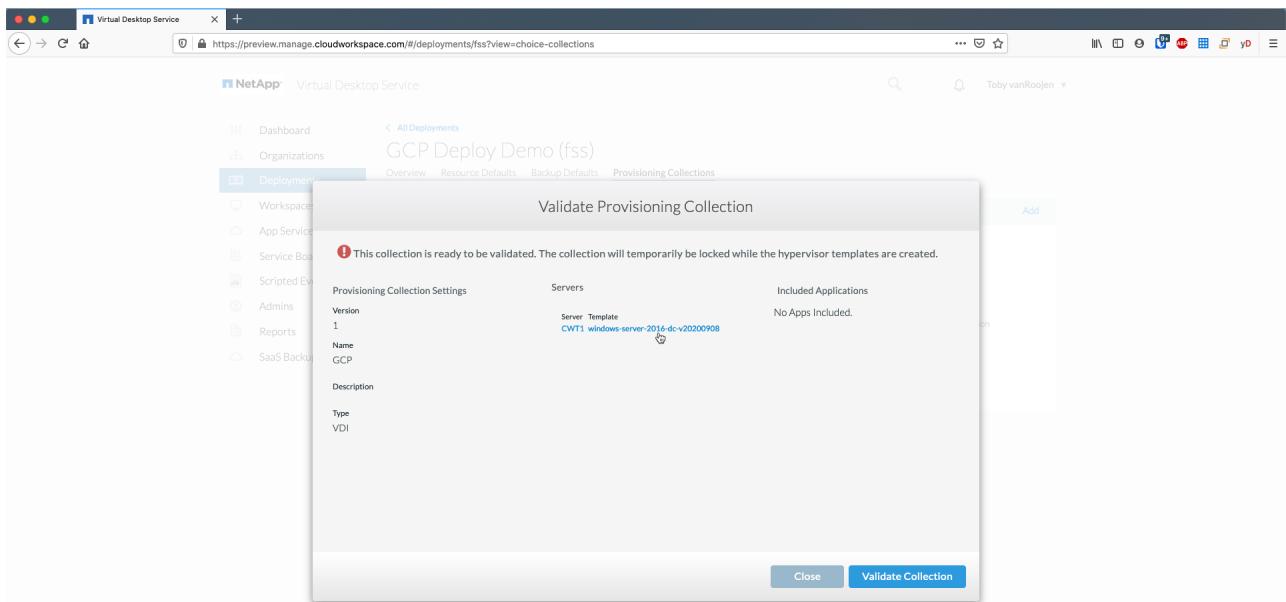
Overview Resource Defaults Backup Defaults Provisioning Collections

Provisioning Collections Add

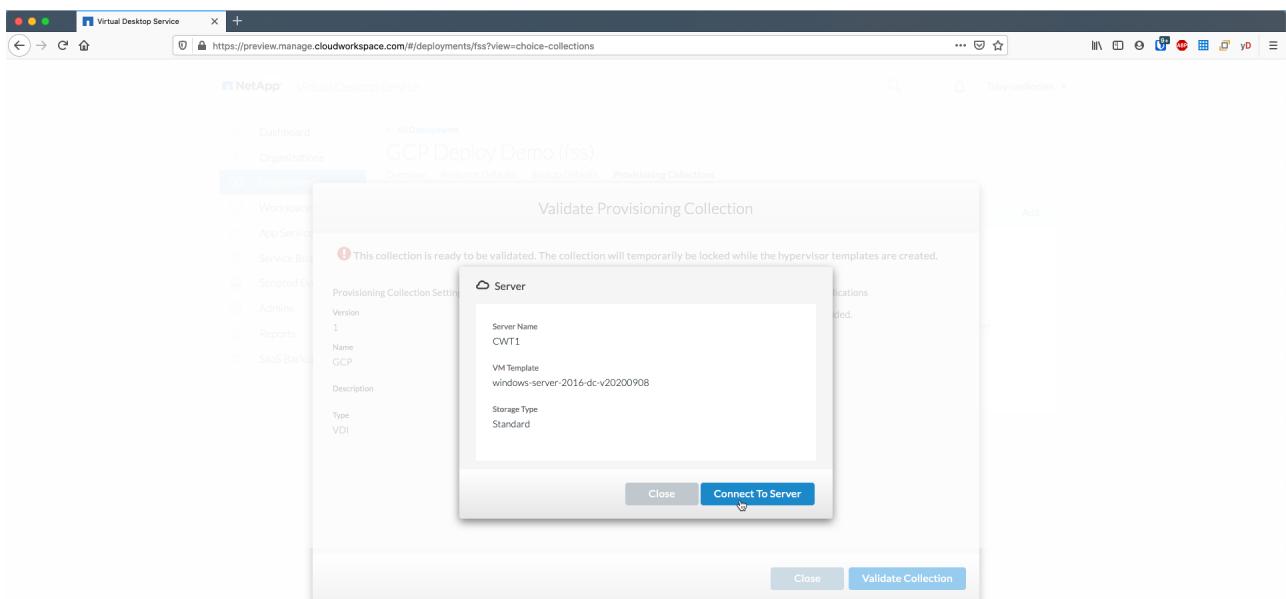
You have 1 collection(s) which require manual intervention for completion

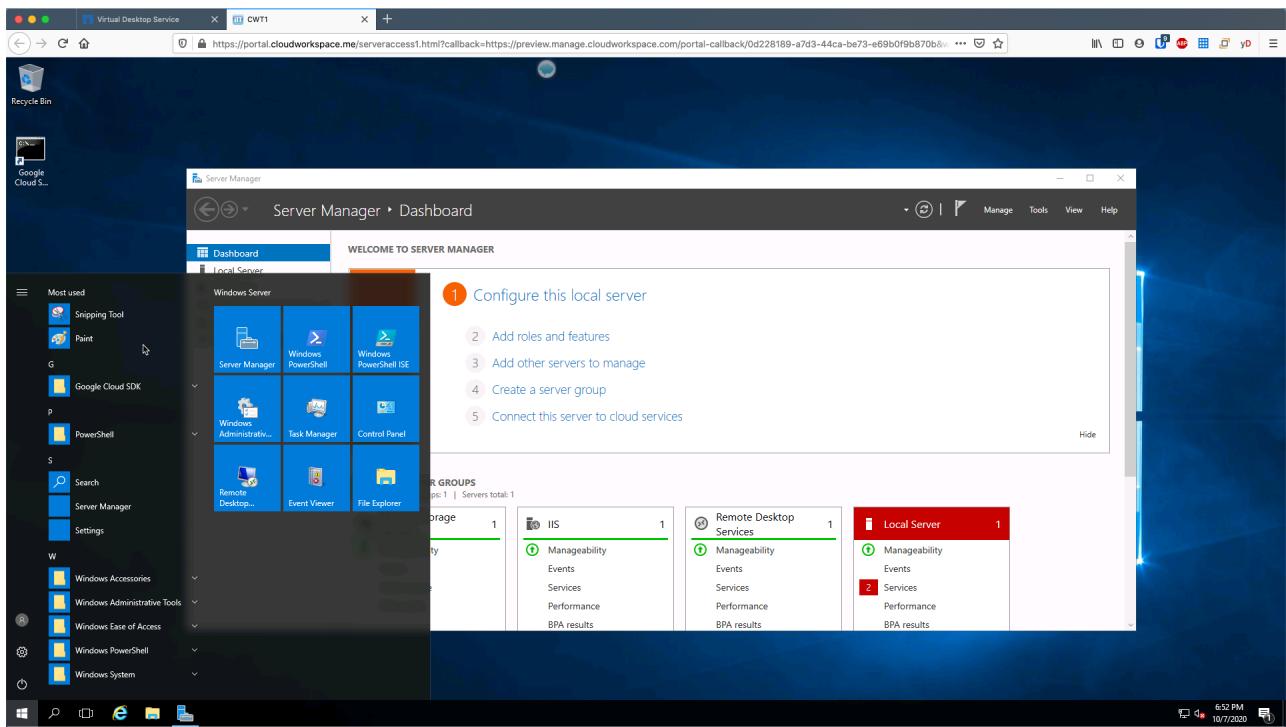
Name	Type	Operating System	Servers	Apps	Min. Cache	Current Cache	Status
GCP	VDI		1	0	0	0	● Collection Validation
BaseImage	VDI		1	0	0	0	● Available
Default PC	Shared	Windows Server 2016	1	0	0	0	● Available
GCP Deploy Demo	Shared	Windows Server 2016	1	1	0	0	● Available

- b. Then, click the *server template name*

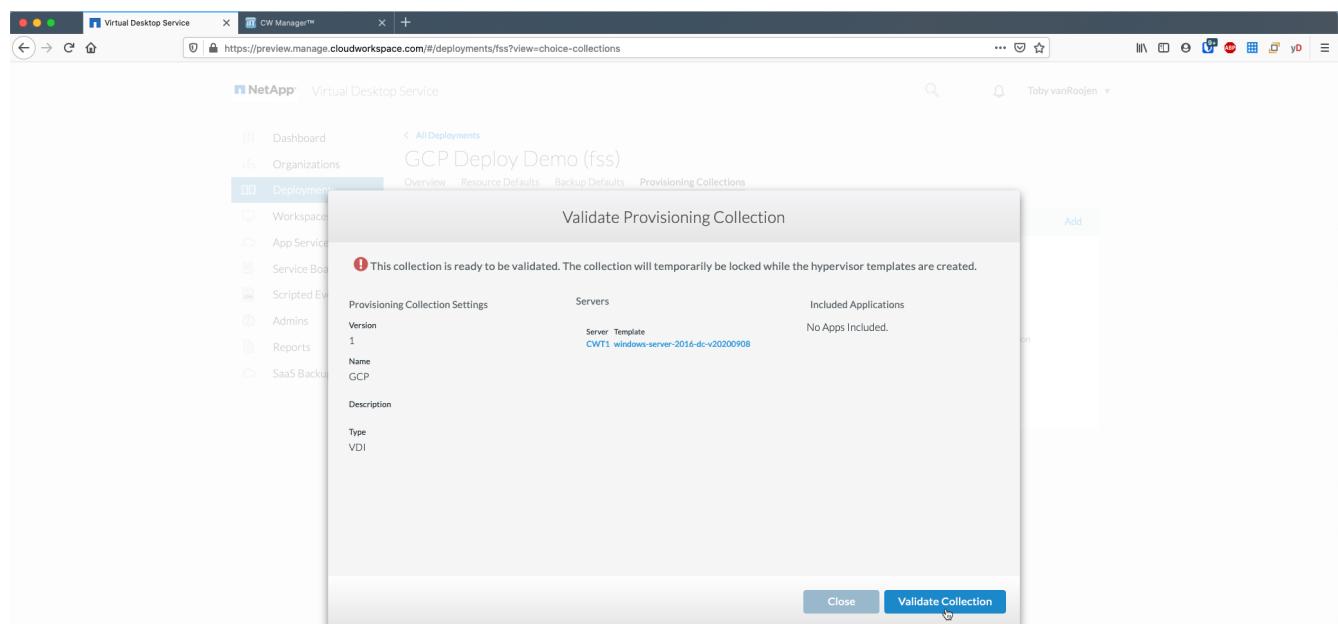


- c. Finally, click the **Connect to Server** button to be connected and automatically logged into the VM with local admin credentials.





8. Once all customizations have been completed, click *Validate Collection* so VDS can sysprep and finalize the image. Once complete, the VM will be deleted and the image will be available for deployment from within VDS deployment wizards.



5

Create new workspace

A workspace is a collection of session hosts and data servers that support a group of users. A deployment can contain a single workspace (single-tenant) or multiple workspaces (multi-tenant).

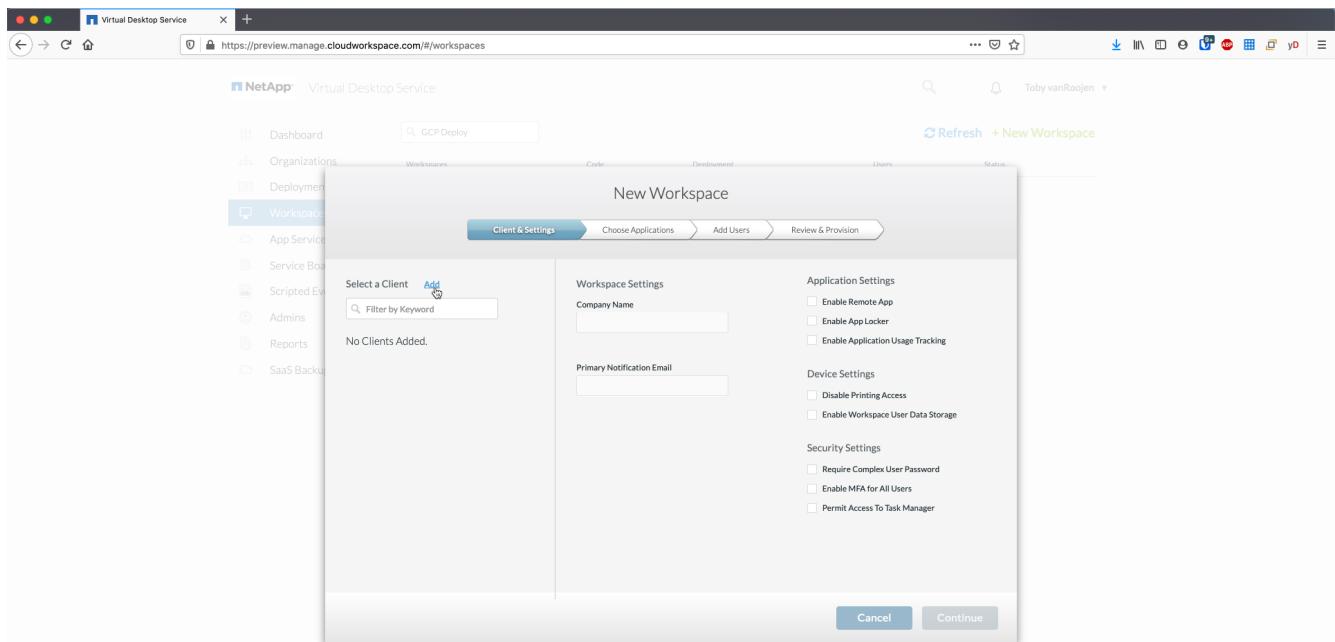
Workspaces define the RDS server collection for a specific group. In this example, we will deploy a single collection to demonstrate the virtual desktop capability. However, the model can be extended to multiple workspaces/ RDS collections to support different groups and different locations within the same Active Directory domain space. Optionally, administrators can restrict access between the workspaces/collections to support use cases that require limited access to applications and data.

Client & settings

1. In NetApp VDS, navigate to *Workspaces* and click *+ New Workspace*

The screenshot shows the NetApp Virtual Desktop Service (VDS) web interface. The browser title bar reads "Virtual Desktop Service". The URL is "https://preview.manage.cloudworkspace.com/#/workspaces". The main navigation menu on the left includes "Dashboard", "Organizations", "Deployments", "Workspaces" (which is selected and highlighted in blue), "App Services", "Service Board", "Scripted Events", "Admins", "Reports", and "SaaS Backup". The top right features a search bar with "GCP Deploy", a refresh button, and a "Toby vanRoojen" user profile. Below the menu, there are tabs for "Workspaces", "Code", "Deployment", "Users", and "Status". A prominent green button at the top right says "+ New Workspace". The bottom of the screen displays copyright information: "© 2020 NetApp Privacy / Terms of Use".

2. click *Add* to create a new client. The client details typically represent either the company information or the information for a specific location/department.



- Enter company details and select the deployment into which this workspace will be deployed.
- Data Drive:** Define the drive letter to be used for the company share mapped drive.
- User Home Drive:** Define the drive letter to be used for the individual's mapped drive.
- Additional Settings**

The following settings can be defined at deployment and/or selected post-deployment.

- Enable Remote App:* Remote app presents applications as streaming applications instead of (or in addition to) presenting a full remote desktop session.
- Enable App Locker:* VDS contains applications deployment and entitlement functionality, by default the system will show/hide applications to the end users. Enabling App Locker will enforce application access via a GPO safelist.
- Enable Workspace User Data Storage:* Determine if end users have a need to have data storage access in their virtual desktop. For RDS deployments, this setting should always be checked to enable data access for user profiles.
- Disable Printer Access:* VDS can block access to local printers.
- Permit Access to Task Manager:* VDS can enable/disable end user access to the Task Manager in Windows.
- Require Complex User Password:* Requiring complex passwords enables the native Windows Server complex password rules. It also disables the time-delayed automatic unlock of locked user accounts. Thus, when enabled, admin intervention is required when end users lock their accounts with multiple failed password attempts.
- Enable MFA for All Users:* VDS includes a no-cost email/SMS MFA service that can be used to secure end user and/or VDS admin account access. Enabling this will require all end users in this workspace authenticate with MFA to access their desktop and/or apps.

Choose applications

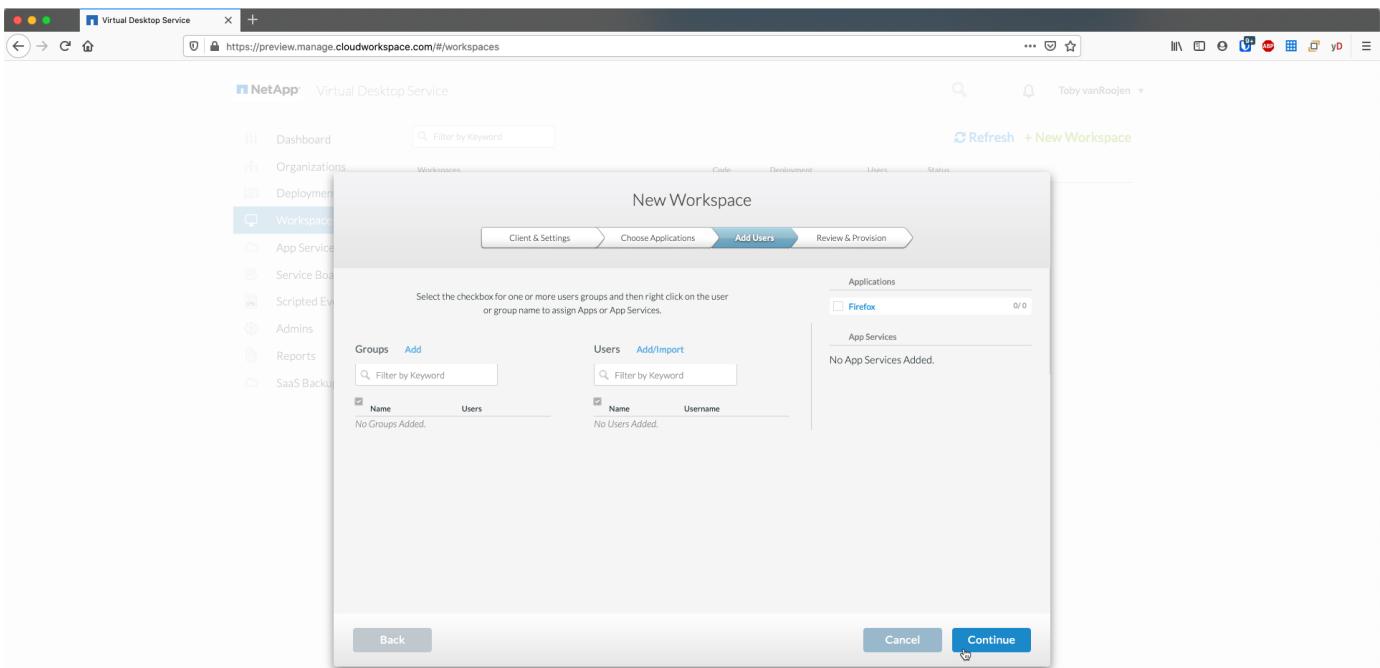
Select the Windows OS version and Provisioning collection created earlier in this guide.

Additional applications can be added at this point but for this POC we'll address application entitlement post-deployment.

The screenshot shows the 'New Workspace' configuration interface. On the left, a sidebar lists various service categories like Dashboard, Organizations, Deployments, Workspaces, App Services, Service Boards, Scripted Environments, Admins, Reports, and SaaS Backups. The 'Workspaces' icon is highlighted. The main panel has tabs for Client & Settings, Choose Applications (which is selected), Add Users, and Review & Provision. Under 'Choose Applications', there's a section titled 'Select a Provisioning Collection' showing 'Deployment fss' and a dropdown menu set to 'Windows Server 2016'. Another section lists 'Included with collection' with 'Firefox' checked. A third section, 'App Services', displays the message 'No App Services Available for the Selected Provisioning Collection.' At the bottom, there are 'Back', '(1) Applications Selected View', 'Cancel', and 'Continue' buttons.

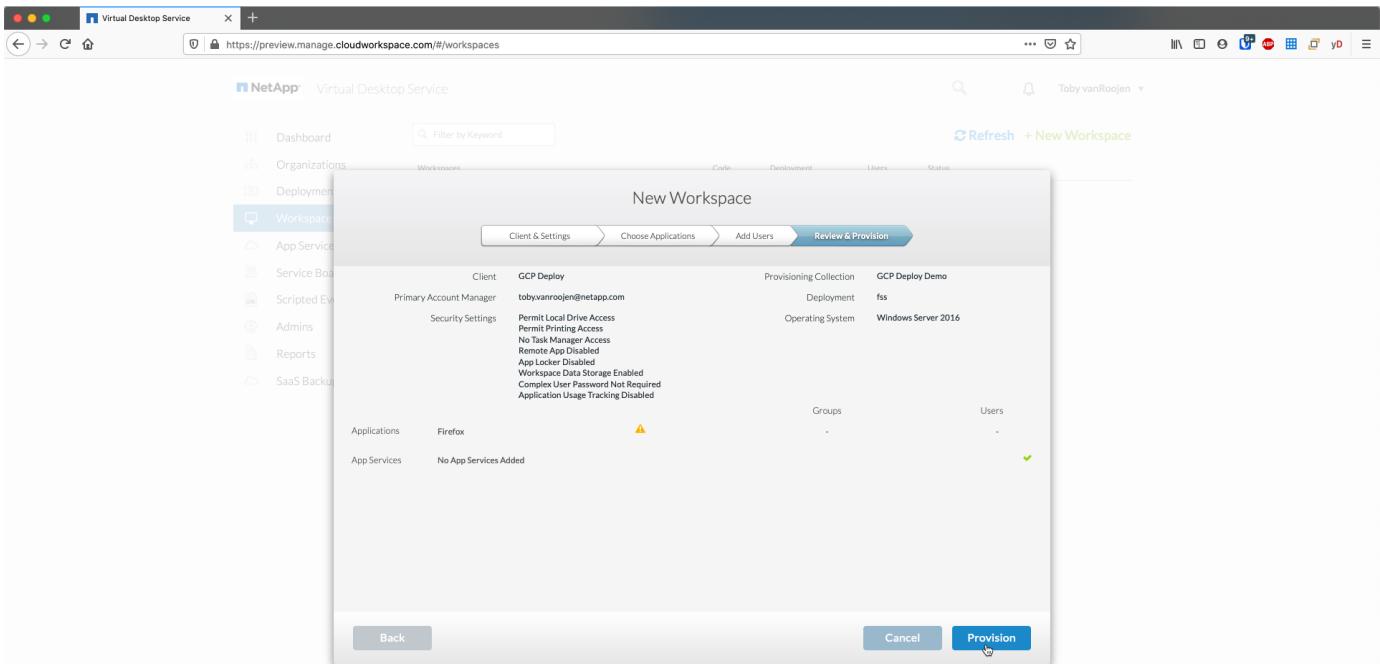
Add Users

Users can be added by selecting an existing AD security groups or individual users. In this POC guide we'll add users post-deployment.



Review & provision

On the final page, review the chosen options and click *Provision* to start the automated build of the RDS resources.





During the deployment process, logs are created and can be accessed under *Task History* near the bottom of the Deployment details page. Accessible by navigating to *VDS > Deployments > Deployment Name*

Next steps

The workplace automation process will now deploy a new RDS resources with the options you selected throughout the deployment wizard.

Once complete, there are several common workflows you'll follow to customize the typical RDS deployment.

- [Add Users](#)
- [End User Access](#)
- [Application Entitlement](#)
- [Cost Optimization](#)

Google Compute Platform (GCP) and VDS Prerequisites

GCP and VDS requirements and notes

This document describes the required elements for deploying Remote Desktop Services (RDS) 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

GCP requirements

- GCP tenant
- GCP project
- Service Account with Owner role assigned

Pre-deployment information

- Determine total number of users
- Determine GCP region and zone
- Determine active directory type
- Determine storage type
- Identify session host VM image or requirements
- Assess existing GCP and on-premises networking configuration

VDS deployment detailed requirements

End user connection requirements

The following Remote Desktop clients support RDS in GCP:

- [NetApp VDS Client for Windows](#)
 - NetApp VDS Client for Windows outbound url safelisting requirements
 - api.cloudworkspace.com
 - vdsclient.app
 - api.vdsclient.app
 - bin.vdsclient.app
 - Enhanced features:
 - VDS Wake on Demand
 - ThinPrint client and licensing
 - Self-service password reset
 - Automatic server and gateway address negotiation
 - Full desktop & streaming application support
 - Available custom branding
 - Installer switches for automated deployment and configuration
 - Built-in troubleshooting tools
- [NetApp VDS web client](#)
- [Microsoft RD Client](#)
 - Windows
 - MacOS
 - iSO
 - Android
- 3rd party software and/or thin clients
 - Requirement: Support RD gateway configuration

Storage layer

In RDS deployed by VDS, 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.

Networking

Required: An inventory of all existing network subnets including any subnets visible to the GCP project via a 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 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 organization and project. 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
- An HTML 5 gateway
- An RDS license server
- A Domain Controller

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.

GCP region

Decide which GCP region or regions will host your VDS virtual machines. Note that the region should be selected based on the proximity to end users and available services.

Data Storage

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

- Cloud Volumes Service for GCP
- Traditional File Server

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 RDS instance. In this case VDS deploys a limited set of components into the domain to support automated provisioning and management tasks for the RDS components.

This configuration requires:

- An existing Active Directory domain controller that can be accessed by VMs on the GCP VPC network, typically via VPN or a domain controller that has been created in GCP.
- Addition of VDS components and permissions required for VDS management of RDS hosts and data volumes as they are joined to the domain. 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 VPC network by default for VDS created VMs. The VPC network can be either peered with existing VPC networks or the CWMGR1 VM can be moved to an existing VPC network 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 RDS session hosts. VDS will deploy either the File Server 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 RDS session host(s)
- 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, ensure the appropriate permissions have been granted to the VDS Automation Services.

APPENDIX A: VDS control plane URLs and IP addresses

VDS components in the GCP project communicate with the VDS global control plane components that are hosted in Azure, including 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>

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 a load balancer with redundant public IP addresses, 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

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 GCP region where session hosts 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 region as the management service.

Supported virtual machine OS images

RDS session hosts, deployed by VDS, support the following x64 operating system images:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Architectural

Redirecting Storage Platform

Overview

Virtual Desktop Service deployment technologies allow for a variety of storage options depending on the underlying infrastructure, this guide addresses how to make a change post-deployment.

Virtual desktop performance depends on a variety of key resources, storage performance is one of the primary variables. As requirements change and workloads evolve, the need to change the storage infrastructure is a common task. In nearly all cases this involves migrating from a file server platform to NetApp storage technology (such as Azure NetApp Files, NetApp Cloud Volumes Service in Google or NetApp Cloud Volumes ONTAP in AWS) since these technologies typically offer the best performance profile for end user computing environments.

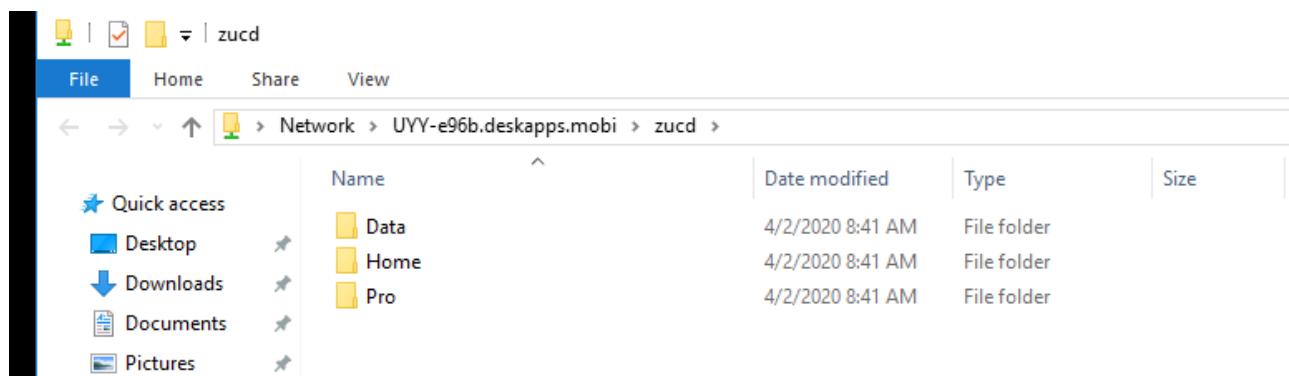
Creating the new storage layer

Due to the wide variety of potential storage services across a wide variety of cloud and HCI infrastructure providers, this guide assumes a new storage service has already been established and with the SMB path(s) known.

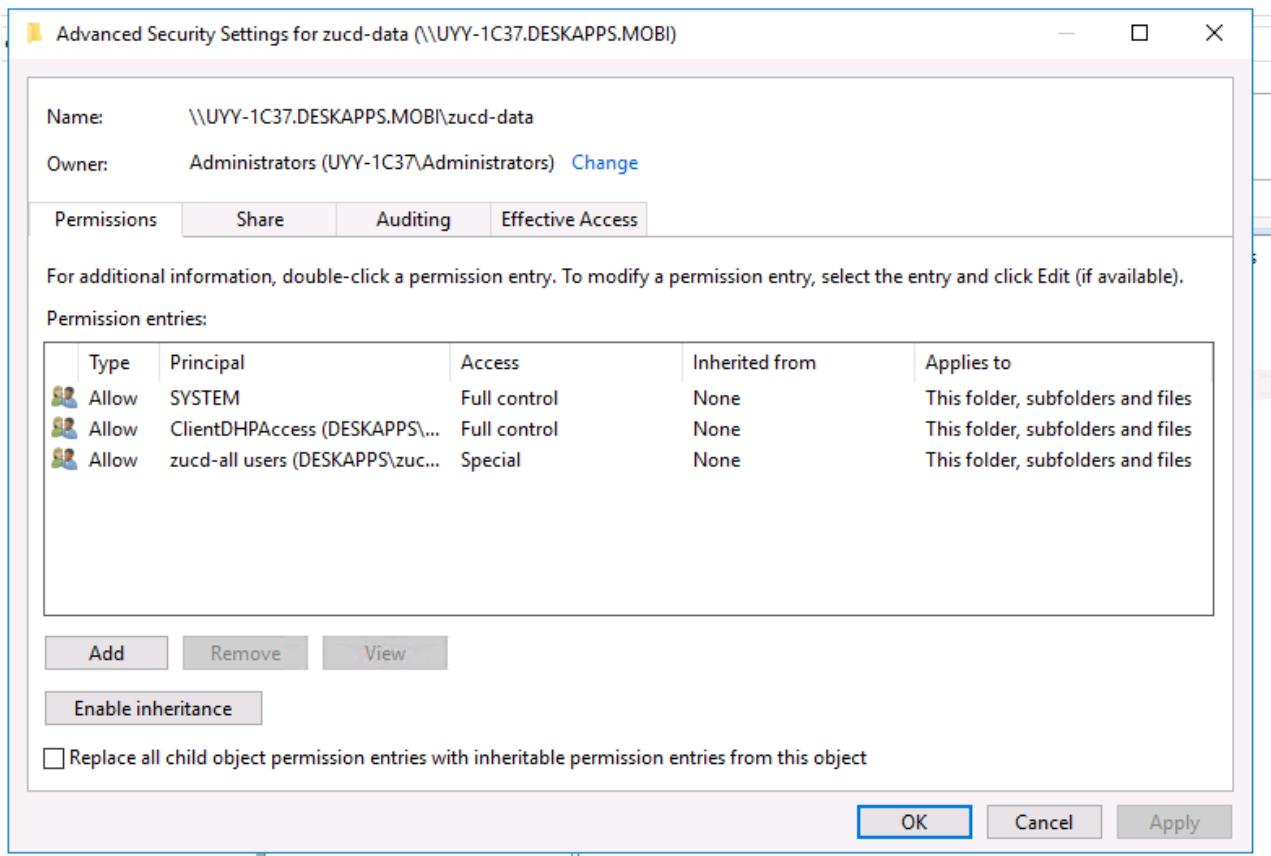
Create storage folders

1. In the new storage service, create three folders:

- /Data
- /Home
- /Pro



2. Set Folder Permissions
 - a. On Folder Properties, select *Security*, >*Advanced* > *Disable Inheritance*



- b. Adjust the remaining settings to match the settings on the original storage layer as originally created by the deployment automation.

Moving data

The directories, data, files and security settings can be moved a variety of ways. The following robocopy syntax will achieve the necessary changes. The paths need to be changed to match your environment.

```
robocopy c:\data\zucd \\uyy-1c37.deskapps.mobi\zucd-data /xd ~snapshot
/MIR /CopyAll /R:1 /W:1 /tee /log:C:\temp\roboitD.txt
```

Redirecting the SMB path at cutover

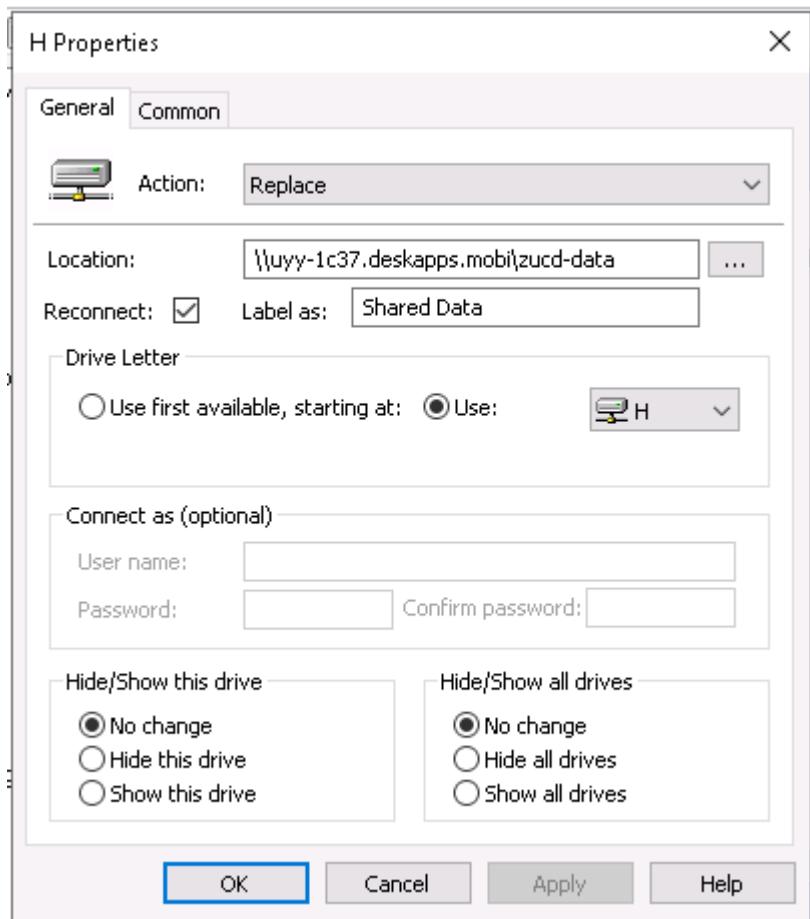
When the time for cutover comes, a few changes will redirect all the storage functionality across the VDS environment.

Update GPOs

1. The Users GPO (named <company-code>-users) needs to be updated with the new share path. Select *User Configuration > Windows Settings > Preferences > Drive Maps*

	3/9/2
	3/29/
	3/29/
	2/27/
	1/31/
	1/31/
	1/31/
	1/31/
	1/31/
	1/31/
	3/19/
	3/26/

2. Right Click on H:, select Properties > Edit > Action: Replace and enter the new Path



3. With Classic or Hybrid AD update the share defined in ADUC in the company OU. This is reflected in VDS folder management.



Update FSLogix profile paths

1. Open Regedit on the original file server and any other provisioned Session Hosts.



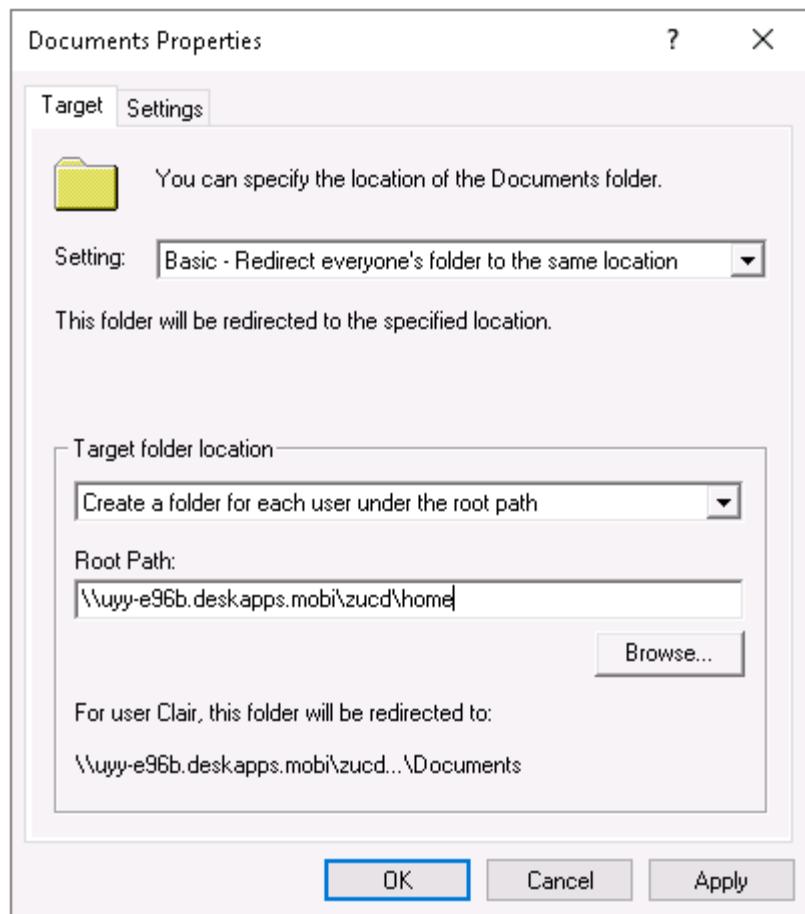
This can also be set via a GPO policy if desired.

2. Edit the *VHDLocations* value with the new value. This should be the new SMB path plus *pro/profilecontainers* as shown in the screenshot below.

Registry Editor			
File	Edit	View	Favorites
..	cj	Name	Type
..	Classes	(Default)	REG_SZ
..	Clients	ConcurrentUser...	REG_DWORD
..	CloudWorkspace	Enabled	REG_DWORD
..	FSLogix	FlipFlopProfileD...	REG_DWORD
..	Apps	FoldersToRemove	REG_MULTI_SZ
..	Logging	ProfileType	REG_DWORD
..	Profiles	ReAttachInterva...	REG_DWORD
..	Sessions	ReAttachRetryC...	REG_DWORD
..	SystemInfo	RoamSearch	REG_DWORD
..	Telemetry	VHDLocations	REG_SZ
..	UserModeDLL	VolumeType	REG_SZ
..	Intel		
..	Macromedia		

Update the folder redirection settings for the home directories

1. Open Group Policy Management, select Users GPO linked to DC=domain,DC=mobi/Cloud Workspace/Cloud Workspace Companies/<company-code>/<company-code>-desktop users.
2. Edit folder redirection paths under User Configuration>Policies>Windows Settings>Folder Redirection.
3. Only Desktop and Documents needs updated and the paths should match the new SMB path mount point for Home volume.

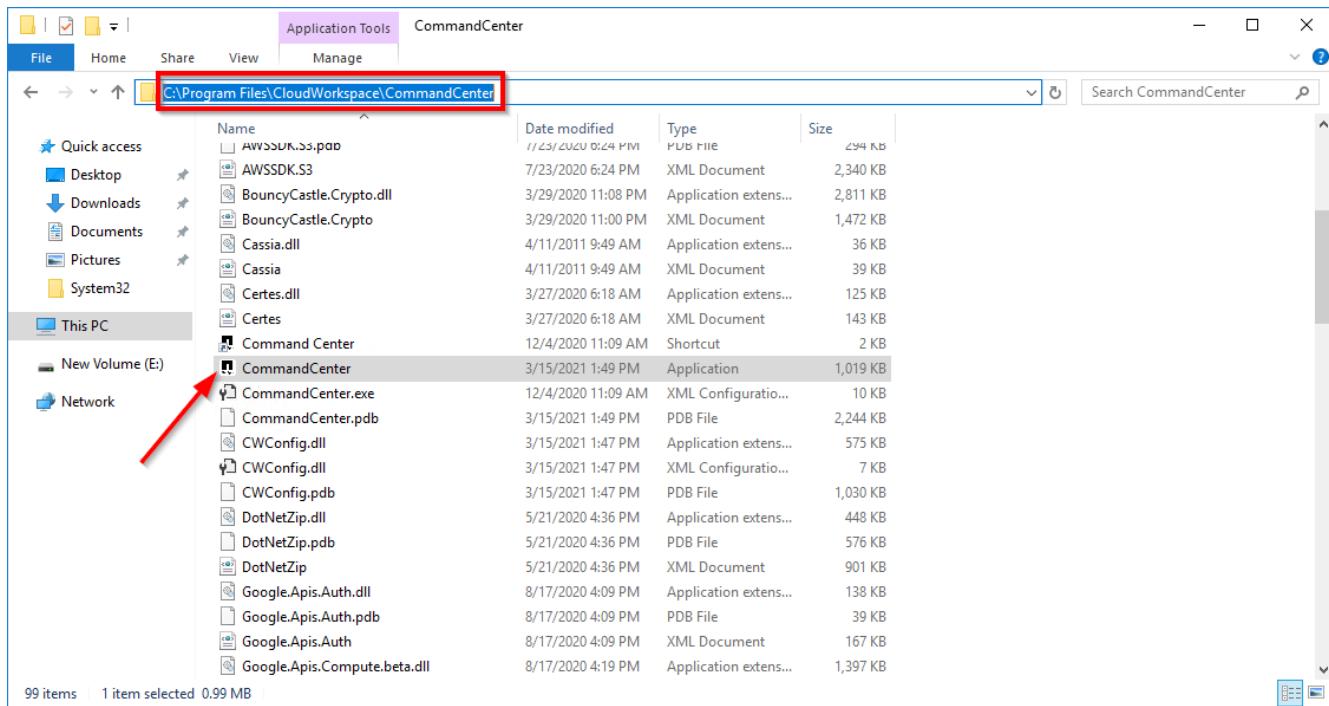


Update the VDS SQL database with Command Center

CWMGR1 contains a helper utility applications called Command Center which can bulk update the VDS database.

To make the final database updates:

1. Connect to CWMGR1, navigate and run CommandCenter.exe



2. Navigate to the *Operations* tab, click *Load Data* to populate the Company Code drop down, select the company code, and enter the new storage paths(s) for the storage layer then click *Execute Command*.

Command Center 5.4.21074.1747

Operations Hypervisor

Command **1** Change Data/Home/Pro Folders **2** Load Data

Company Code **3**

Resource Pool

Data **4** Home Pro

Is Windows Server Is Windows Server Is Windows Server

5 Execute Command

View All Logs **Clear Log**

1 Change Data/Home/Pro Folders
2 Load Data
3 Company Code
4 Data, Home, Pro
5 Execute Command

Redirecting Storage Platform to Azure Files

Overview

Virtual Desktop Service deployment technologies allow for a variety of storage options depending on the underlying infrastructure. This guide addresses how to make a change to using Azure Files post-deployment.

Pre-requisites

- AD Connect installed and set up
- Azure global admin account
- AZFilesHybrid PowerShell module <https://github.com/Azure-Samples/azure-files-samples/releases>
- AZ PowerShell module
- ActiveDirectory PowerShell module

Create the new storage layer

1. Log in to Azure with the global admin account
2. Create a new Storage Account in the same location and resource group as the workspace

Create storage account

Basics Networking Data protection Advanced Tags Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below.

[Learn more about Azure storage accounts](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Azure subscription 1

Resource group *

vrg

[Create new](#)

Instance details

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

Storage account name * ⓘ

azfskift

Location *

(US) East US

Performance ⓘ

Standard Premium

Account kind ⓘ

StorageV2 (general purpose v2)

Replication ⓘ

Read-access geo-redundant storage (RA-GRS)

3. Create the data, home, and pro file shares under the storage account

New file share

Name * home

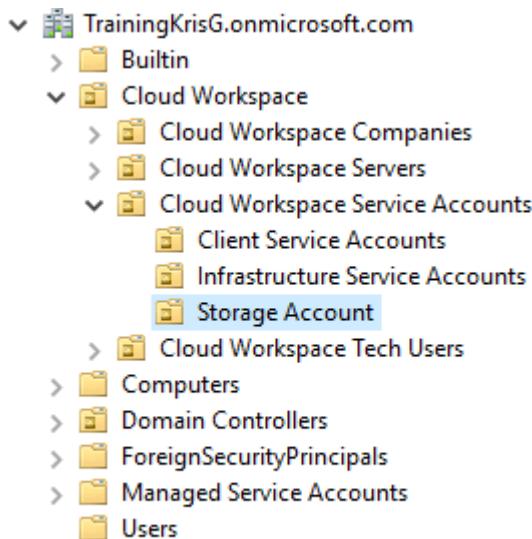
Quota 5120 GiB Set to maximum

Tiers Premium, Transaction optimized, Hot, Cool

Create Discard

Set Up Active Directory

1. Create a new Organization Unit named “Storage Account” under the Cloud Workspace > Cloud Worksapce Service Accounts OU



2. Enable AD DS authentication (must be done using PowerShell) <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-enable>

- a. DomainAccountType should be “ServiceLogonAccount”
- b. OraganizationalUnitDistinguishedName is the distinguished name of the OU created in the previous step (ie “OU=Storage Account,OU=Cloud Workspace Service Accounts,OU=Cloud Workspace,DC=TrainingKrisG,DC=onmicrosoft,DC=com”)

Set the Roles for the Shares

1. In the Azure portal, give "Storage File Data SMB Share Elevated Contributor" role to CloudWorkspaceSVC and Level3 Technicians

The screenshot shows the Azure portal's Access Control (IAM) blade for a file share named 'home'. The left sidebar includes links for Overview, Diagnose and solve problems, Access Control (IAM), Properties, Operations, Snapshots, and Backup. The main area displays sections for 'Check access' (My access, Check access), 'Grant access to this resource' (Add role assignments, View), 'View deny assignments' (View), and 'View access to this resource' (View). A modal window titled 'Add role assignment' is open on the right, allowing the selection of a role (Storage File Data SMB Share Contributor), the target (User, group, or service principal), and the members (Level3 Technicians and CloudWorkspace Service Account). Save and Discard buttons are at the bottom of the modal.

2. Give "Storage File Data SMB Share Contributor" role to the "<company code>-all users" group

Add role assignment

X

Role ⓘ

Storage File Data SMB Share Contributor ⓘ



Assign access to ⓘ

User, group, or service principal



Select ⓘ

kift-all

No users, groups, or service principals found.

Selected members:

KU

kift-all users

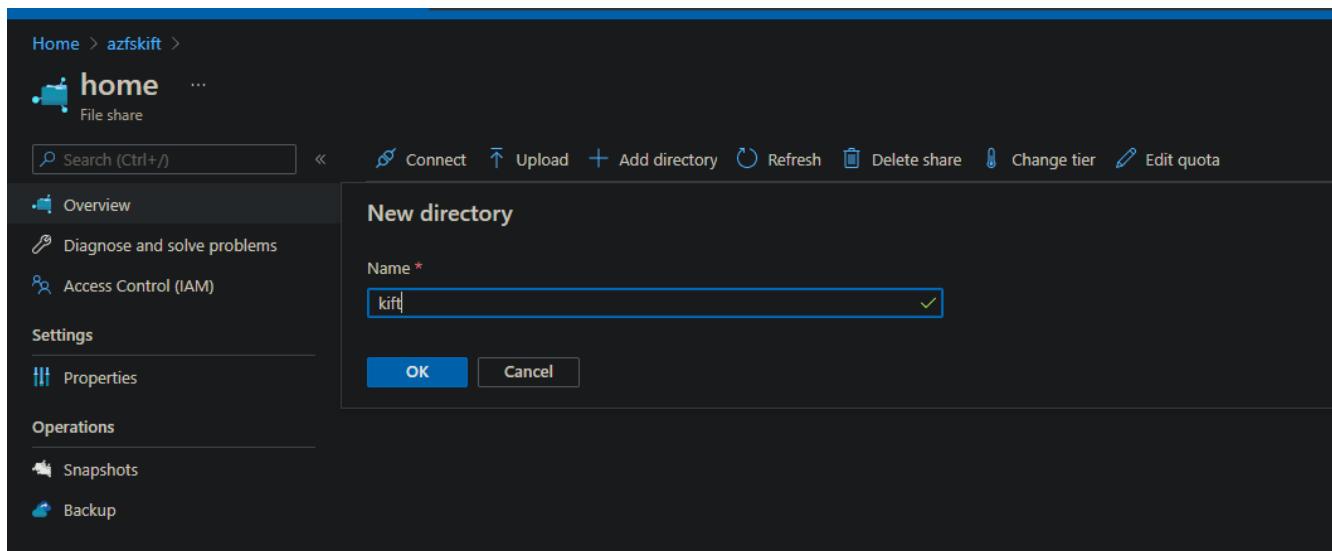
Remove

Save

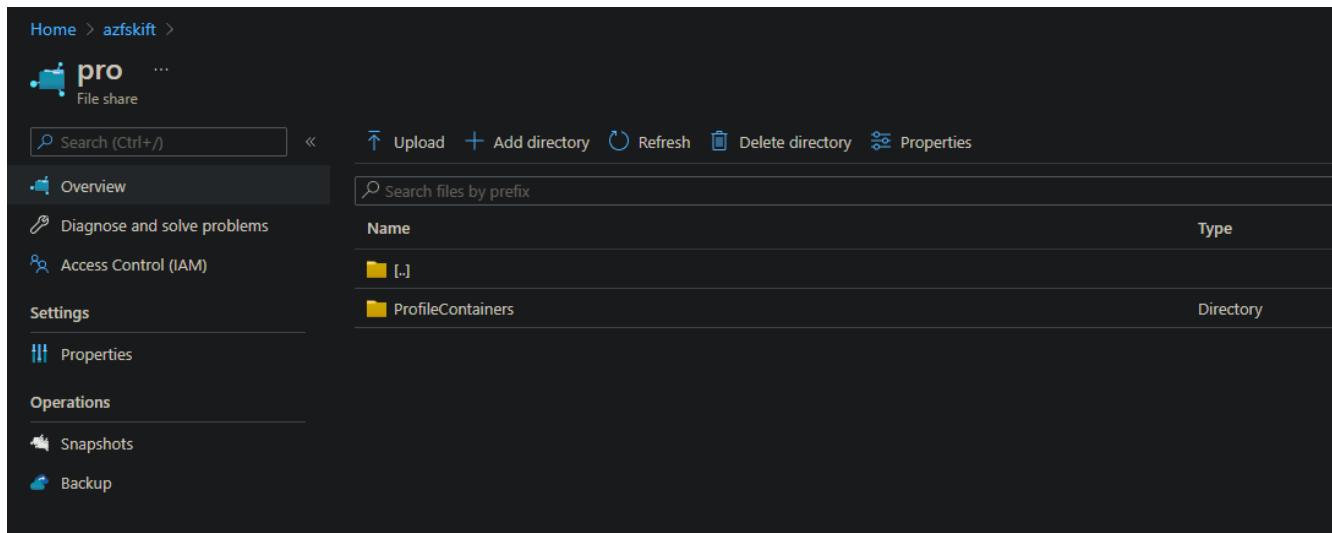
Discard

Create the directories

1. Create a directory in each share (data, home, pro) using the company code as the name (In this example, the company code is "kift")



2. In the <company code> directory of the pro share, create a "ProfileContainers" directory



Set the NTFS Permissions

1. Connect to the shares
 - a. Navigate to the share under the storage account in the Azure portal, click the three dots, then click Connect

The screenshot shows the Azure Storage File shares blade for the 'azfskift' storage account. On the left, there's a navigation sidebar with options like Home, Storage accounts, File service, Table service, Queue service, Monitoring, Insights, Alerts, Metrics, Workbooks, and Diagnostic settings (preview). The main area displays 'File share settings' with Active Directory set to 'Configured', Soft delete set to '7 days', and Share capacity set to '5 TiB'. Below this is a search bar and a 'Show deleted shares' toggle. A table lists three file shares: 'data' (modified 4/13/2021, 4:13:34 PM), 'home' (modified 4/13/2021, 4:02:21 PM), and 'pro' (modified 4/2/2021, 4:56:41 PM). To the right of the 'pro' share, a context menu is open, with the 'Connect' option highlighted.

Name	Modified	Tier	Quota
data	4/13/2021, 4:13:34 PM	Transaction optimized	5 TiB
home	4/13/2021, 4:02:21 PM	Transaction optimized	5 TiB
pro	4/2/2021, 4:56:41 PM	Transaction optimized	

- b. Choose Active Directory for Authentication method and click the Copy to clipboard icon in the lower right corner of the code

Connect

X

pro

! 'Secure transfer required' is enabled on the storage account. SMB clients connecting to this share must support SMB protocol version 3 or higher in order to handle the encryption requirement. [Click here to learn more.](#)

[Windows](#) [Linux](#) [macOS](#)

To connect to this Azure file share from Windows, choose from the following authentication methods and run the PowerShell commands from a normal (not elevated) PowerShell terminal:

Drive letter

Z



Authentication method

Active Directory

Storage account key

Identity-based access is configured for this storage account. Ensure the account used with the following command has permissions to this share. [Learn more](#)

```
$connectTestResult = Test-NetConnection -ComputerName  
azfskift.file.core.windows.net -Port 445  
if ($connectTestResult.TcpTestSucceeded) {  
    # Mount the drive  
    New-PSDrive -Name Z -PSProvider FileSystem -Root  
    "\\azfskift.file.core.windows.net\pro" -Persist  
} else {
```

[Copy to clipboard](#)



This script will check to see if this storage account is accessible via TCP port 445, which is the port SMB uses. If port 445 is available, your Azure file share will be persistently mounted. Your organization or internet service provider (ISP) may block port 445, however you may use Azure [Point-to-Site \(P2S\) VPN](#), Azure [Site-to-Site \(S2S\) VPN](#), or [ExpressRoute](#) to tunnel SMB traffic to your Azure file share over a different port.

[Learn how to circumvent the port 445 problem \(VPN\)](#)

- c. Log in to the CWMGR1 server with an account that is a member of the Level3 Technicians group
- d. Run the copied code in PowerShell to map the drive
- e. Do the same for each share while choosing a different drive letter for each

2. Disable inheritance on the <company code> directories
3. System and the AD Group ClientDHPAccess should have Full Control to the <company code> directories
4. Domain Computers should have Full Control to the <company code> directory in the pro share as well as the ProfileContainers directory within
5. The <company code>-all users AD group should have List folder/read data permissions to the <company code> directories in the home and pro shares
6. The <company code>-all users AD group should have the below Special permissions for the directory in the data share

The screenshot shows the Windows File Explorer security settings dialog for a folder named "Data Share".

General Tab:

- Principal: kift-all users (TRAININGKRISG\kift-all users) [Select a principal](#)
- Type: Allow
- Applies to: This folder, subfolders and files

Advanced permissions:

<input type="checkbox"/> Full control	<input checked="" type="checkbox"/> Write attributes
<input checked="" type="checkbox"/> Traverse folder / execute file	<input checked="" type="checkbox"/> Write extended attributes
<input checked="" type="checkbox"/> List folder / read data	<input checked="" type="checkbox"/> Delete subfolders and files
<input checked="" type="checkbox"/> Read attributes	<input checked="" type="checkbox"/> Delete
<input checked="" type="checkbox"/> Read extended attributes	<input checked="" type="checkbox"/> Read permissions
<input checked="" type="checkbox"/> Create files / write data	<input type="checkbox"/> Change permissions
<input checked="" type="checkbox"/> Create folders / append data	<input type="checkbox"/> Take ownership

[Show basic permissions](#)

Only apply these permissions to objects and/or containers within this container [Clear all](#)

Conditions Tab:

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

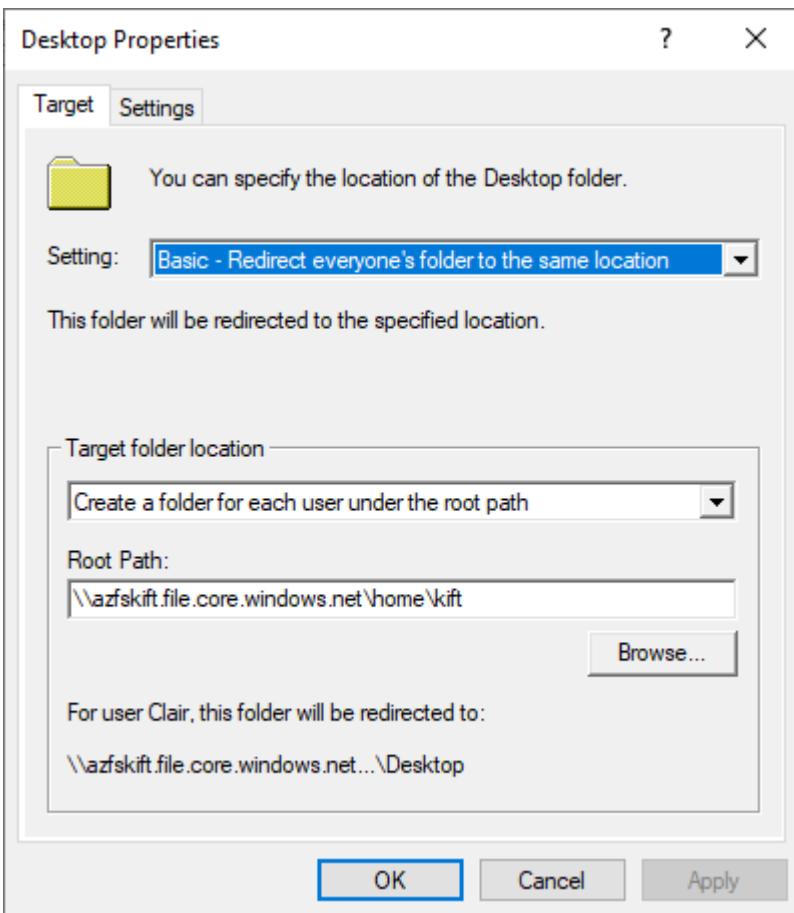
[Add a condition](#)

7. The <company code>-all users AD group should have the Modify permission on the ProfileContainers directory

Update Group Policy Objects

1. Update the GPO <company code> users located under Cloud Workspace > Cloud Workspace Companies > <company code> > <company code>-desktop users
 - a. Change the Home drive mapping to point the new home share

- b. Change the Folder Redirection to point the home share for Desktop and Documents



The screenshot shows the Group Policy Management console. On the left, the navigation pane shows the forest 'TrainingKrisG.onmicrosoft.com' with various domains and objects. The main pane displays the 'kift users' GPO under 'kift'. The 'Policies' section is selected, showing 'Windows Settings' and 'Folder Redirection' configurations for the 'kift' and 'kift-groups' groups.

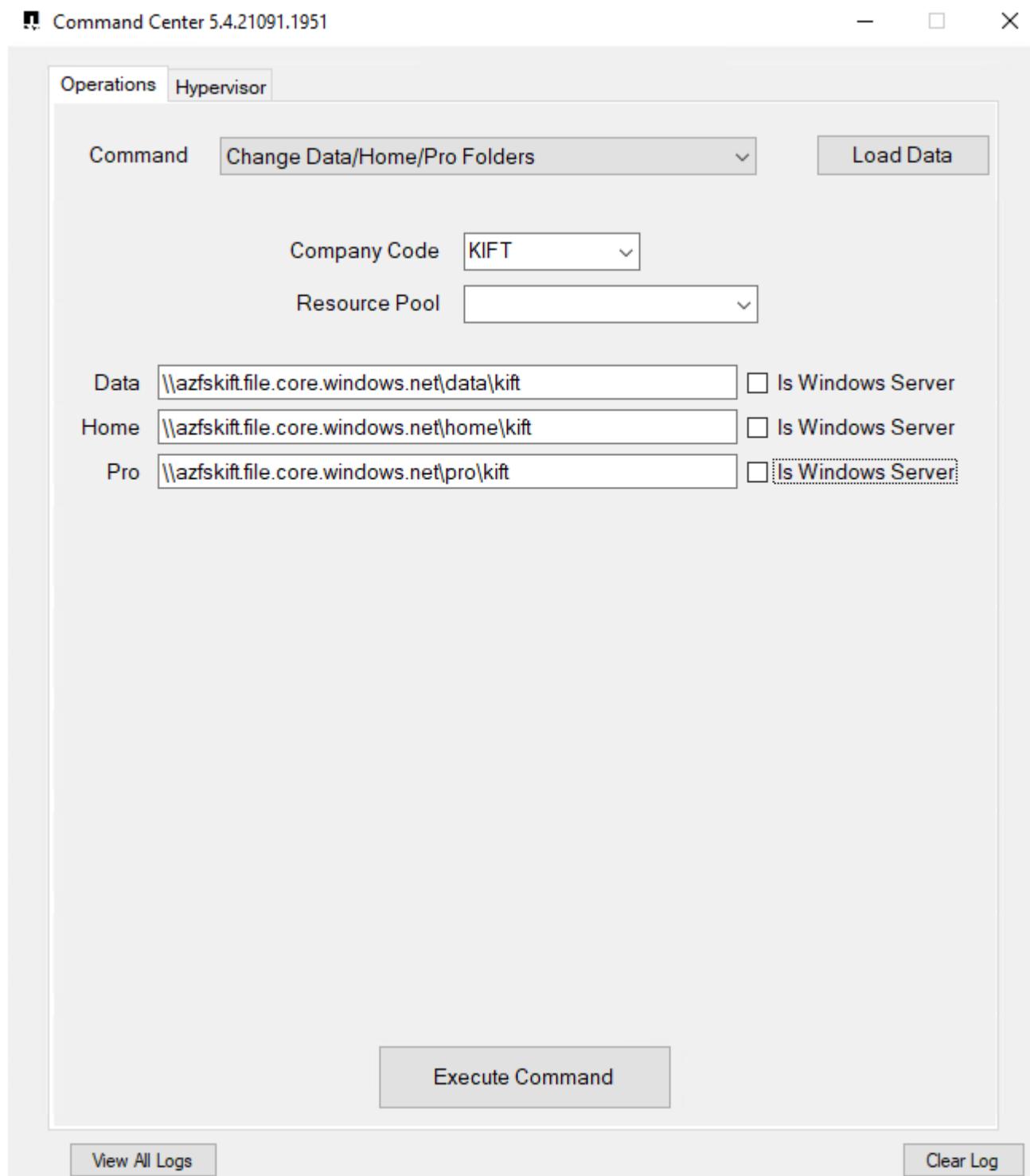
Update the share in Active Directory Users and Computers

- With classic or hybrid AD, the share in the company code OU needs to be updated to the new location

The screenshot shows the Active Directory Users and Computers (ADUC) interface. On the left, the navigation pane shows the 'TrainingKrisG.onmicrosoft.com' domain with various containers like 'Saved Queries', 'Builtin', and 'Cloud Workspace'. The 'Cloud Workspace' container is expanded, showing 'Cloud Workspace Companies' and 'kift'. The 'kift' folder is selected. On the right, the 'Properties' dialog box for 'kift' is open, showing the 'General' tab. The 'Type' is listed as 'Shared Folder' and the 'Description' is 'H:\'. The 'UNC name:' field contains '\\azfskift.file.core.windows.net\home\kift'. The dialog box includes 'OK', 'Cancel', and 'Apply' buttons at the bottom.

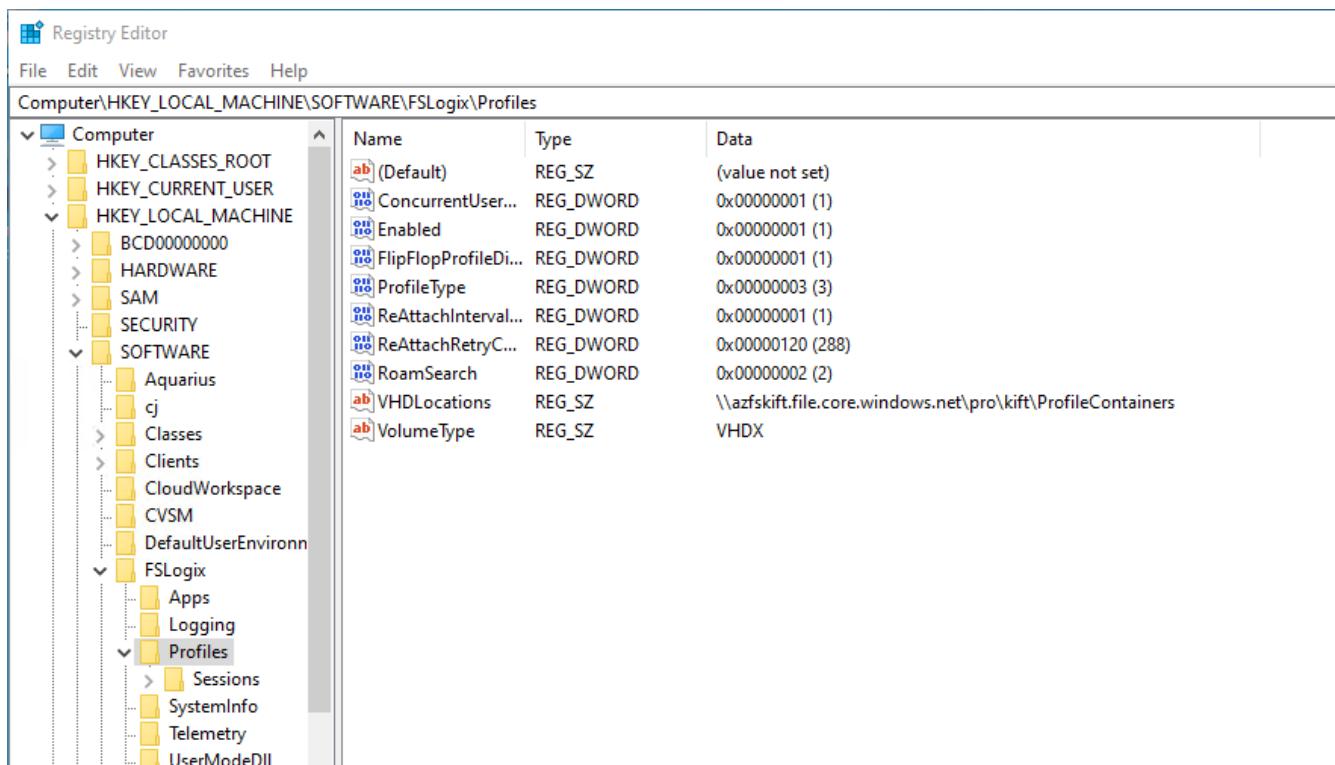
Update Data/Home/Pro paths in VDS

1. Log in to CWMGR1 with an account in the Level3 Technicians group and launch Command Center
2. In the Command drop down, select Change Data/Home/Pro Folders
3. Click the Load Data button, then be sure the proper company code is selected from the drop down
4. Enter the new path for the data, home, and pro locations
5. Uncheck the Is Windows Server box
6. Click the Execute Command button



Update FSLogix profile paths

1. Open registry editor on the session hosts
2. Edit the VHDLocations entry at HKLM\SOFTWARE\FSLogix\Profiles to be the UNC path to the new ProfileContainers directory



Configure Backups

1. It is recommended to set up and configure a backup policy for the new shares
2. Create a new Recovery Services Vault in the same resource group
3. Navigate to the vault and select Backup under Getting Started
4. Choose Azure for where the workload is running and Azure file share for what you want to back up then click Backups
5. Select the storage account used to create the shares
6. Add the shares to back up
7. Edit and Create a backup policy that fits your needs

Data Migration Considerations

Overview

Migrating data is a near-universal requirement when migrating to a cloud solution of any type. While Admins are responsible for migrating data into their Virtual Desktops, NetApp's experience is available and has proven invaluable for innumerable Customer migrations. The Virtual Desktop environment is simply a hosted Windows environment, so any methods desired can likely be accommodated.

Data that is typically migrated:

- User profiles (Desktop, Documents, Favorites, etc...)
- File Server Shares
- Data Shares (App data, databases, backup caches)

In the Virtual Desktop environment there are two primary places where data is stored and organized:

- The User (typically H:\) drive: This is the mapped drive visible for each User.
 - This is mapped back to the <DRIVE>:\home\CustomerCode\user.name\ path
 - Each user has their own H:\ drive and can not see another User
- The Shared (typically I:\) drive: This is the shared mapped drive visible for all users
 - This is mapped back to the <DRIVE>:\data\CustomerCode\ path
 - All users can access this drive. Their level of access to contained folders/file is managed in the Folders section of VDS.

Generic migration process

1. Replicate data to the Cloud Environment
2. Move data to the appropriate path for H:\ and I:\ drives
3. Assign appropriate permissions in the Virtual Desktop environment

FTPS transfers & considerations

Migration with FTPS

1. If the FTPS server role was enabled during the CWA deployment process, gather FTPS credentials by logging into VDS, navigating to Reports and running the Master Client Report for your organization
2. Upload data
3. Move data to the appropriate path for the H:\ and I:\ drives
4. Assign appropriate permissions in the Virtual Desktop environment via the Folders module

 When transferring data via FTPS, any interruption will prevent the data from being transferred as intended. Since servers managed by Virtual Desktop Services are rebooted nightly, the standard overnight transmission strategy will likely be interrupted. To get around this, admins can enable Migration Mode to prevent VMs from being rebooted for 1 week.

Enabling Migration Mode is easy – navigate to the organization, then scroll down to the Virtual Desktop Settings section and check the box for Migration Mode, then click Update.

 NetApp recommends that Admins enable a compliance setting that helps organizations meet PCI, HIPAA and NIST controls via hardening the deployment's gateways, etc. This also disallows the default FTP server role, if enabled, from accepting default, unencrypted transmissions via port 21. FileZilla does not allow SFTP, which means that connections should be made using FTPS over port 990.

To enable that setting, connect to CWMGR1 and navigate to the CwVmAutomationService program, then enable PCI v3 compliance.

Sync tools and considerations

Enterprise File Sync and Share, often referred to as EFSS or sync tools, can be extremely useful in migrating data, as the tool will capture changes on each side until cutover. Tools like OneDrive, which comes with Office 365, can help you sync fileserver data. It is also useful for VDI User deployments as well, where there is a 1:1 relationship between the User and the VM, as long as the User doesn't attempt to sync shared content onto their VDI Server when shared data can be deployed once to the Shared (typically I:\) drive for the whole organization to use.

Migrating SQL and Similar Data (Open Files)

Common sync and/or migration solutions do not transfer open files, which includes file types like:

- Mailbox (.ost) files
- QuickBooks files
- Microsoft Access files
- SQL databases

This means that if one single element of the entire file (1 new email appears, for example) or database (1 new record is entered into a app's system) then the entire file is different and standard sync tools (Dropbox, for example) will think it is an entirely new file and needs to be moved again. There are specialized tools available for purchase from 3rd party providers, if desired.

Another common way these migrations are handled is via providing access to a 3rd party VAR, who often have streamlined of importing/exporting databases.

Shipping drives

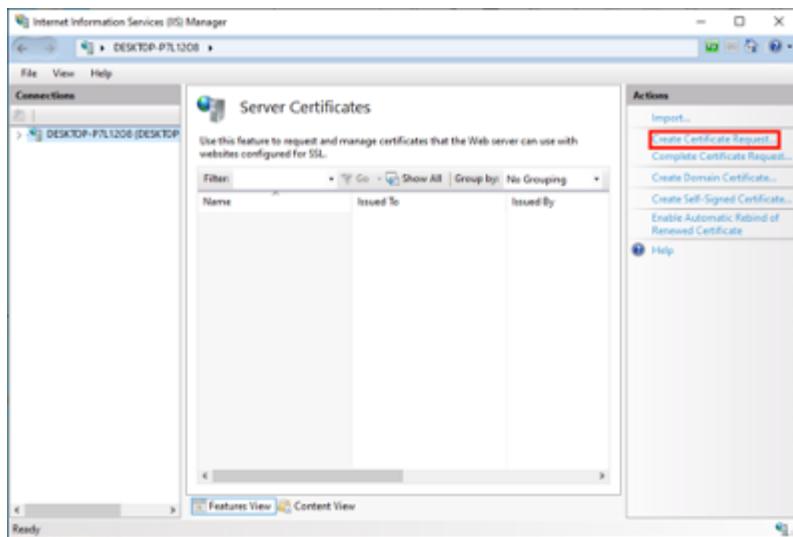
Many data center providers no longer ship hard drives – either that, or they require you to follow their specific policies and procedures.

Microsoft Azure is enabling organizations to use Azure Data Box, which Admins can take advantage of by coordinating with their Microsoft representatives.

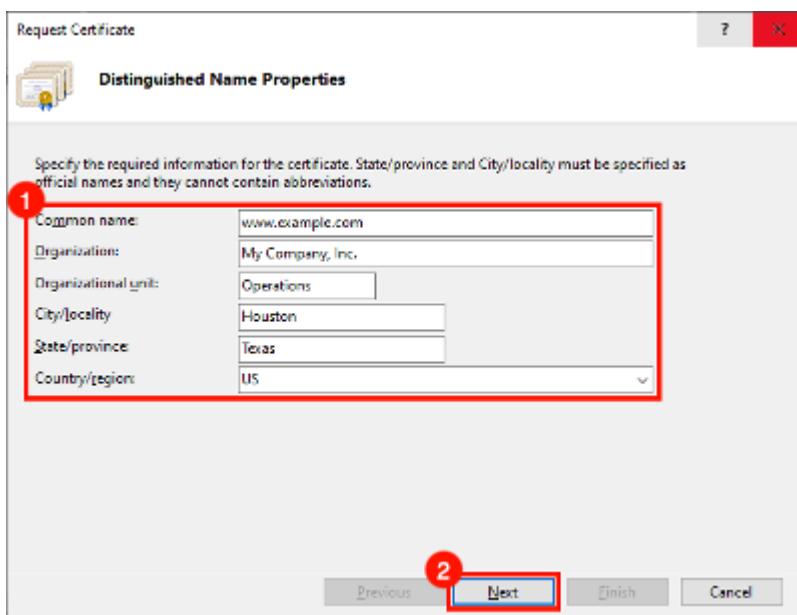
Wildcard SSL Certificate Renewal Process

Create a certificate signing request (CSR):

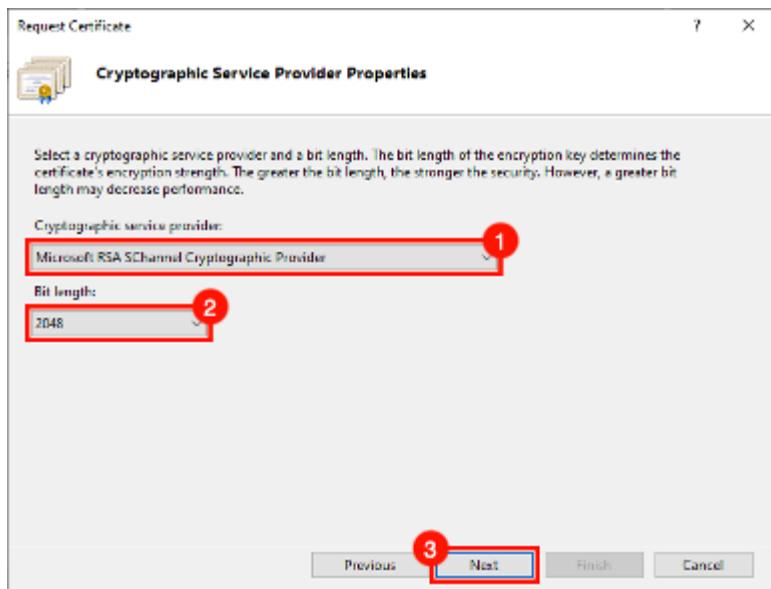
1. Connect to CWMGR1
2. Open IIS Manager from Administrator Tools
3. Select CWMGR1 and open Server Certificates
4. Click on Create Certificate Request in the Actions pane



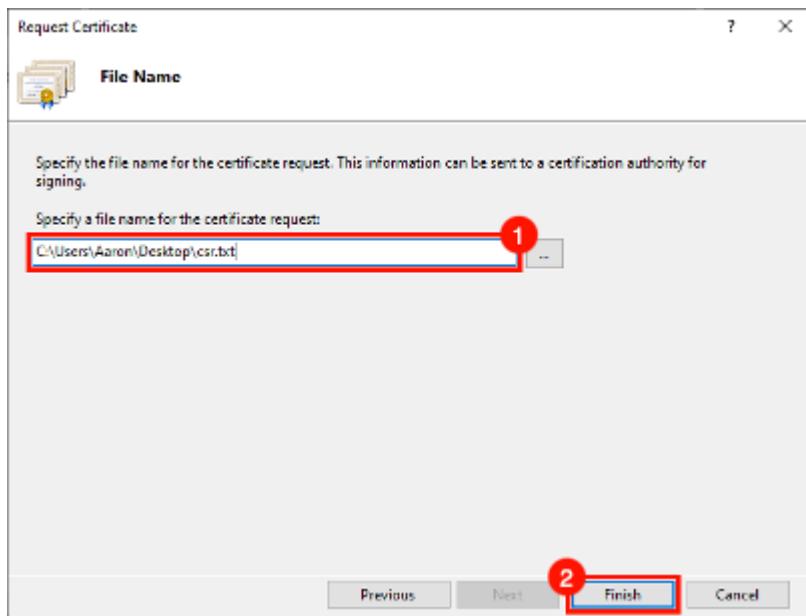
5. Fill out the Distinguished Name Properties in the Request Certificate Wizard and click Next:
- Common Name: FQDN of Wildcard - *.domain.com
 - Organization: Your company's legally registered name
 - Organizational unit: 'IT' works fine
 - City: City where company is located
 - State: State where company is located
 - Country: Country where company is located



6. On the Cryptographic Service Provider Properties page, verify the below appears and click Next:



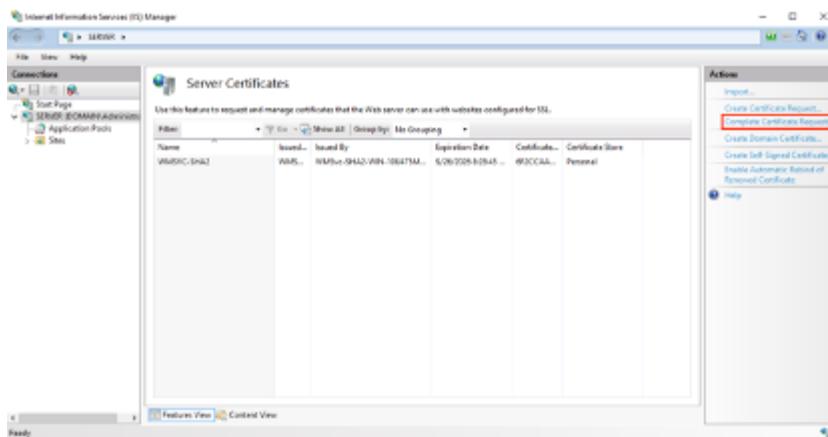
7. Specify a file name and browse to a location where you want to save the CSR. If you do not specify a location, the CSR will be in C:\Windows\System32:



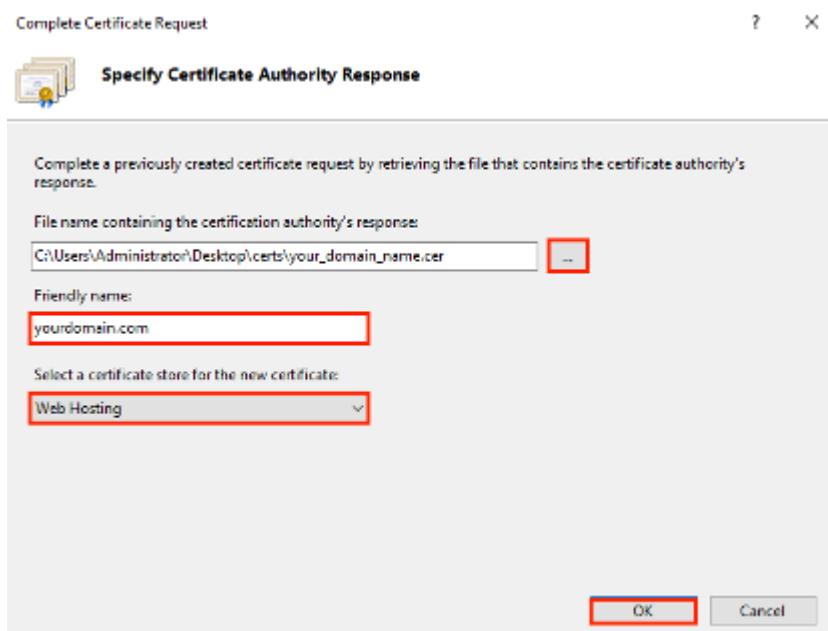
8. Click Finish when completed. You will use this text file to submit your order to certificate registrar
9. Reach out to registrar support to purchase a new Wildcard SSL for your certificate: *.domain.com
10. After receiving your SSL certificate, save the SSL certificate .cer file in a location on CWMGR1 and follow the below steps.

Installing and configuring CSR:

1. Connect to CWMGR1
2. Open IIS Manager from Administrator Tools
3. Select CWMGR1 and open 'Server Certificates'
4. Click on Complete Certificate Request in the Actions pane



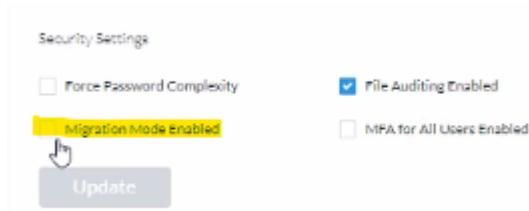
5. Complete the below fields in the Complete Certificate Request and click OK:



- File Name: Select .cer file that was saved previously
- Friendly name: *.domain.com
- Certificate store: Select either Web Hosting or Personal

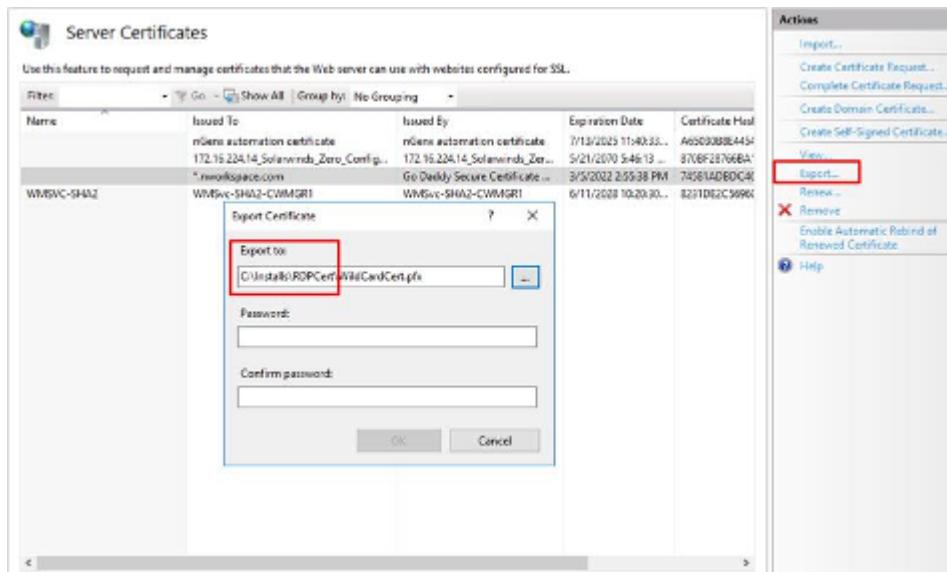
Assigning SSL certificate:

- Verify that Migration Mode is not enabled. This can be found on the Workspace Overview page under Security Settings in VDS.

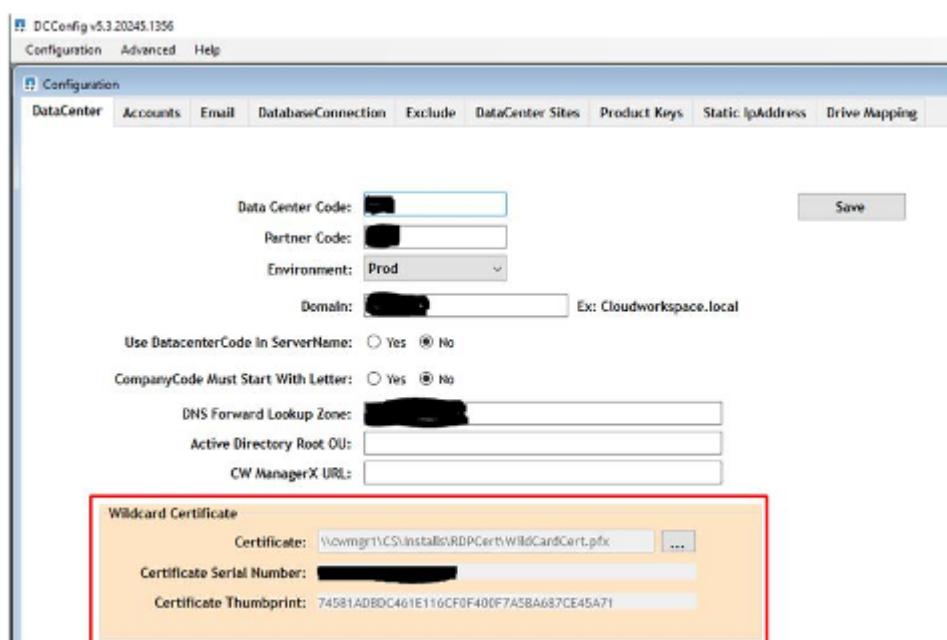


- Connect to CWMGR1

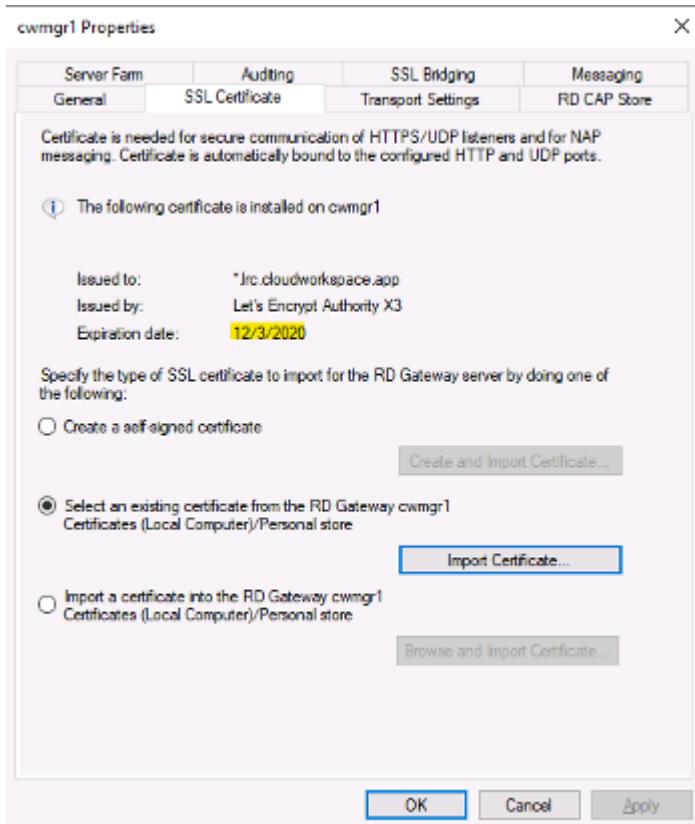
3. Open IIS Manager from Administrator Tools
4. Select CWMGR1 and open 'Server Certificates'
5. Click on Export in the Actions pane
6. Export the certificate in .pfx format
7. Create a password. Store password as it will be needed to import or re-use .pfx file in the future
8. Save .pfx file to the C:\installs\RDPcert directory
9. Click OK and close IIS Manager



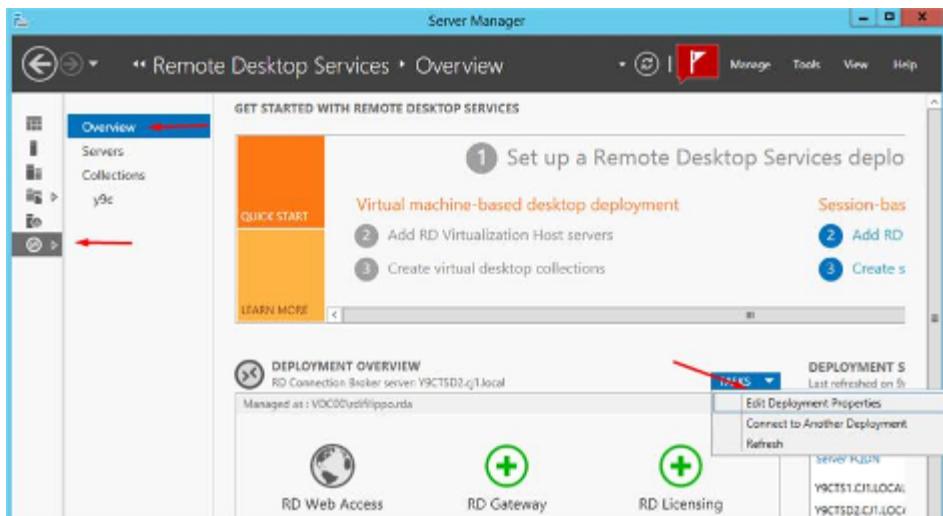
10. Open DCConfig
11. Under Wildcard Certificate, update the Certificate path to new .pfx file
12. Enter .pfx password when prompted
13. Click Save



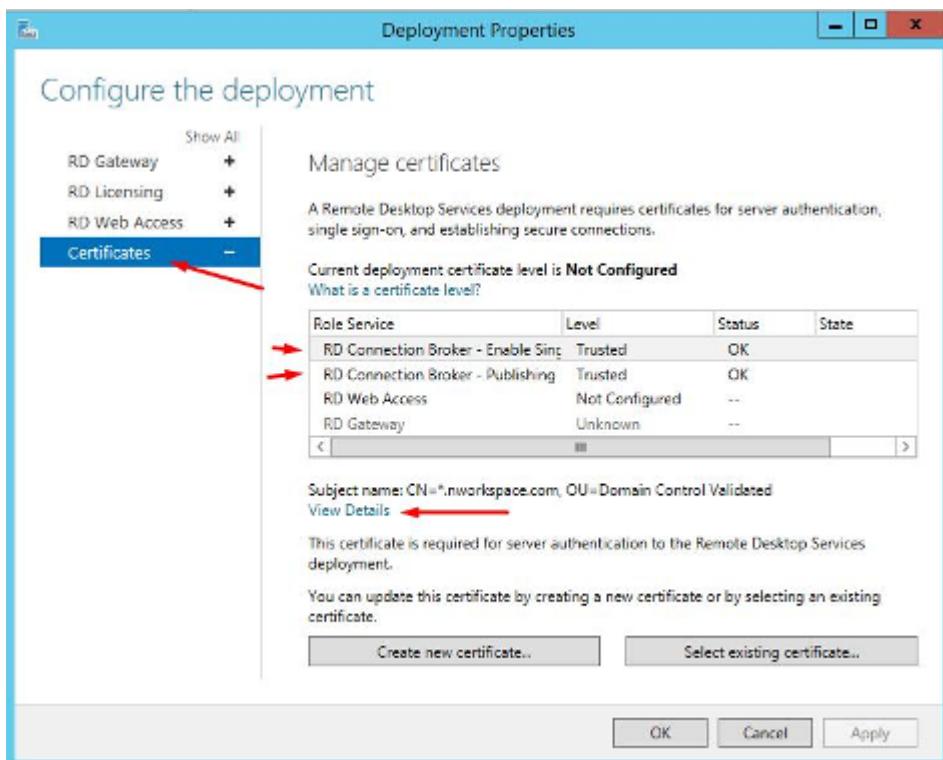
14. If the certificate is valid for 30 more days, allow automation to apply the new certificate during the morning Daily Actions task throughout the week
15. Periodically check the Platform servers to verify that the new certificate has propagated. Validate and test user connectivity to confirm.
 - a. On the server, go to Admin Tools
 - b. Select Remote Desktop Services > Remote Desktop Gateway Manager
 - c. Right click on gateway server name, select Properties. Click on the SSL Certificate tab to review expiration date

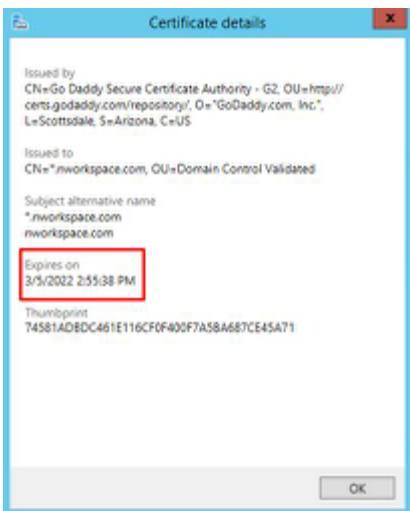


16. Periodically check the client VMs that are running the Connection Broker role
 - a. Go to Server Manager > Remote Desktop Services
 - b. Under Deployment Overview, select Tasks dropdown and choose Edit Deployment Properties

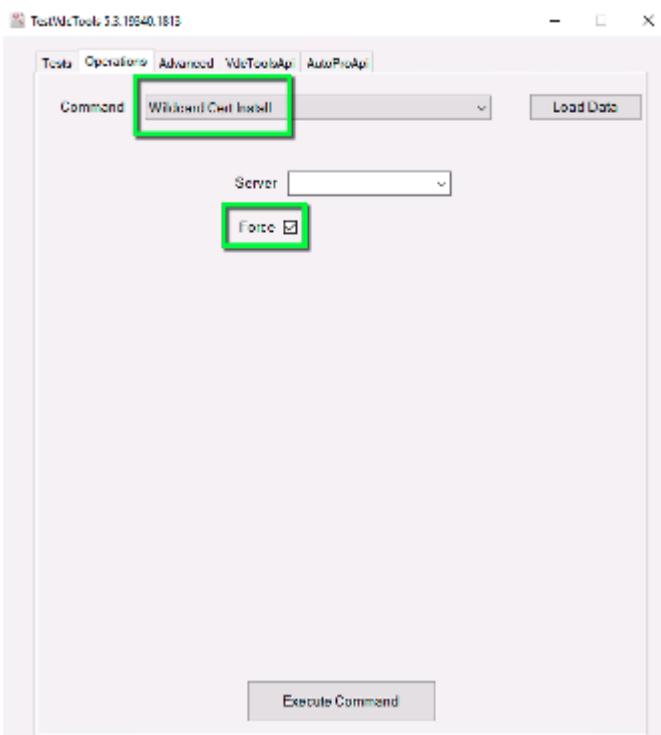


- c. Click on Certificates, select certificate and click View Details. Expiration date will be listed.





17. If less than 30 days or you prefer to push out the new certificate immediately, force the update with TestVdcTools. This should be done during a maintenance window as connectivity for any users logged in and your connection to CWMGR1 will be lost.
- Go to C:\Program Files\CloudWorkspace\TestVdcTools, click the Operations tab and select the Wildcard Cert-Install command
 - Leave the server field blank
 - Check the Force box
 - Click Execute Command
 - Verify certificate propagates using the steps listed above



AVD Teardown Guide

Overview

This article covers the removal of VDS and NetApp control while maintaining AVD end user access. Going forward management would be with native Azure/Windows administration tools. After this process is complete it is recommended to contact VDSsupport@netapp.com so that NetApp can clean up our back-end and billing systems.

Initial state

- AVD Deployment
- TDS1 is FS Logix Fileshare
- TS1 is Session Host
- User has logged in and FS Logix disk was created in:

```
\\\*\*\*TSD1\\*\*\*-Pro$\ProfileContainers (\*\*\* = Unique Company Code)
```

Delete CW Agent service

The CW Agent runs on every machine in the environment. The service that starts this process should be uninstalled with the following command on every VM in the environment. CWMGR1 can be skipped as that VM will be shut down and eventually deleted in most cases. Ideally this action would be run via scripted automation. The video below shows it done manually.

```
C:\Program files\CloudWorkspace\CwAgent\CwAgent.exe -u
```

Delete CW Agent service video

 | <https://img.youtube.com/vi/l9ASmM5aap0/maxresdefault.jpg>

Delete CW agent directory

The previous uninstall removed the service that launches CW Agent but the files remain. Delete the directory:

```
"C:\Program Files\CloudWorkspace"
```

Delete CW Agent directory video

 | https://img.youtube.com/vi/hMM_z4K2-iI/maxresdefault.jpg

Remove startup shortcuts

The startup items directory contains two shortcuts to files deleted in the previous step. To avoid end user error messages, these files should be deleted.

```
"C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Pen.lnk"  
"C:\ProgramData\Microsoft\Windows\Start  
Menu\Programs\StartUp\CwRemoteApps.lnk"
```

Remove startup shortcuts video

 | <https://img.youtube.com/vi/U0YLZ3Qfu9w/maxresdefault.jpg>

Unlink ‘Users’ and ‘Companies’ GPOs

There are three GPOs implemented by VDS. We recommend un-linking two of them and reviewing the content of the third.

Unlink:

- AADDC Users > Cloud Workspace Companies
- AADDC Users > Cloud Workspace Users

Review:

- AADDC Computers > Cloud Workspace Computers

Unlink ‘Users’ and ‘Companies’ GPOs video

 | <https://img.youtube.com/vi/cb68ri3HKUw/maxresdefault.jpg>

Shutdown CWMGR1

With the GPO Changes applied we can now shut down the CWMGR1 VM. Once continued AVD functionality is confirmed this VM can be deleted permanently.

In extremely rare cases there is a need to maintain this VM if another server role is running (e.g. DC, FTP Server...). In that event, three services can be disabled to disable the VDS functionality on CWMGR1:

- CW Agent (See Above)
- CW Automation Service
- CW VM Automation

Shutdown CWMGR1 video

 | https://img.youtube.com/vi/avk9HyliC_s/maxresdefault.jpg

Delete NetApp VDS service accounts

The Azure AD service accounts used by VDS can be removed. Login in the Azure Management Portal and delete the users:

- CloudWorkspaceSVC
- CloudWorkspaceCASVC

Other user accounts can be retained:

- End users
- Azure administrator
- .tech domain admins

Delete NetApp VDS service accounts video

 | https://img.youtube.com/vi/_VToVNp49cg/maxresdefault.jpg

Delete app registrations

Two App Registrations are made when deploying VDS. These can be deleted:

- Cloud Workspace API
- Cloud Workspace AVD

Delete app registrations video

 | <https://img.youtube.com/vi/iARz2nw1Oks/maxresdefault.jpg>

Delete enterprise applications

Two Enterprise Applications are deployed when deploying VDS. These can be deleted:

- Cloud Workspace
- Cloud Workspace Management API

Delete enterprise applications video

 | <https://img.youtube.com/vi/3eQzTPdilWk/maxresdefault.jpg>

Confirm CWMGR1 is stopped

Before testing that the end users can still connect, confirm the CWMGR1 is stopped for a realistic test.

Confirm CWMGR1 is stopped video

 | <https://img.youtube.com/vi/Ux9nkDk5IU4/maxresdefault.jpg>

Login and end user

To confirm success, login as an end user and confirm functionality is maintained.

Login and end user video

 | <https://img.youtube.com/vi/SuS-OTHJz7Y/maxresdefault.jpg>

Management

Deployments

Provisioning Collections

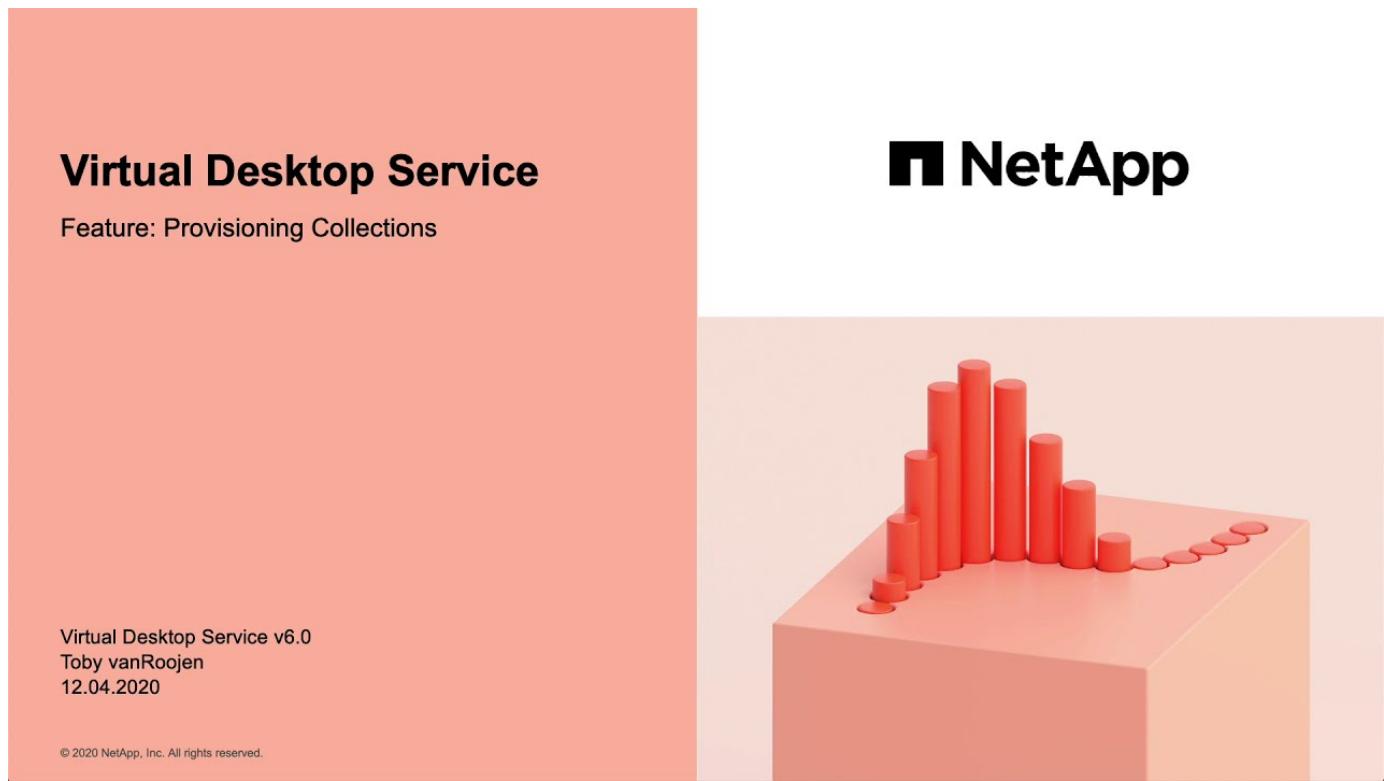
Overview

Provisioning Collections is a function of VDS related to the creation and management of VM images.

At a high level, the Provisioning Collection workflow is as follows:

1. A temporary VM (e.g. "CWT1") is built based on an existing image (either a stock image or a previously saved Provisioning Collection).
2. The VDS Administrator customizes the temporary VM to match their requirements using [Scripted Events](#), [Connect to Server](#) and/or 3rd party management tools.
3. Once customized, the VDS Admin click **Validate** and triggers a validation process that automates finalizing the image, running SysPrep, deleting the temporary VM and making the image available for deployment throughout VDS.

[Video Demo - Managing VM images for VDI Session Hosts](#)



Provisioning Collection Types

There are two distinct types of collection with specific use cases, **Shared** and **VDI**.

Shared

The **Shared** type is a collection of VM images(s) designed to deploy an entire environment with multiple,

distinct VM images and VM roles.

VDI

The **VDI** type is a single VM image designed to be used and reused to deploy multiple identical VMs, typically used for hosting user sessions. For all types of AVD session hosts, the **VDI** type should be selected, even for hosts that run multiple sessions per VM.

Creating a new Provisioning Collection

Provisioning Collections are found in the VDS interface within each deployment, under the **Provisioning Collections** sub-tab.



To create a new collection

1. Click the **+ Add Collection** button.
2. Complete the following fields:
 - a. **Name**
 - b. **Description**(Optional)
 - c. **Type** - Shared or VDI
 - d. **Operating System**
 - e. **Share Drive** - If this VM will be used to host users profiles or company share data, pick the drive letter on which it will be hosted. If not, leave as "C"
 - f. **Minimum Cache** - If you and VDS to create VMs to hold for instant deployment, specify the minimum number of cached VMs that should be maintained. If deploying new VMs can wait for as long as it takes the hypervisor to build a VM, this can be set to "0" to save costs.
 - g. **Add Servers**
 - i. **Role** (If "Shared" type is selected)
 - A. **TS** - This VM will act only as a session host
 - B. **Data** - This VM will not host any user sessions
 - C. **TSDATA** - This VM will be both the session host and the storage host (Maximum: one TSDATA per workspace)
 - ii. **VM Template** - Select from the available list, both stock hypervisor images and previously saved Provisioning Collections are available to select.
 - A. NOTE: Windows 7 images from the Azure Marketplace do not have PowerShell Remoting enabled. To use a Windows 7 image, you'll need to provide a custom image in your shared image gallery with PowerShell Remoting enabled.
 - B. NOTE: By using an existing Provisioning Collection you can update and re-deploy existing images as part of a planned image upgrade process.
 - iii. **Storage Type** - Select the speed of the OS disk considering cost and performance
 - iv. **Data Drive** - Optionally enable a 2nd disk attached to this image, typically for the data storage layer referenced above in 2.e.

- A. **Data Drive Type** - Select the speed of the 2nd (data) disk considering cost and performance
- B. **Data Drive Size (GB)** - Define the size of the 2nd (data) disk considering capacity, cost and performance
- h. **Add Applications** - Select any application from the Application Library that will be (1) installed on this image and (2) managed by VDS application entitlement. (This is only applicable to RDS deployments. It should remain empty for AVD workspaces)

Customizing the Temporary VM

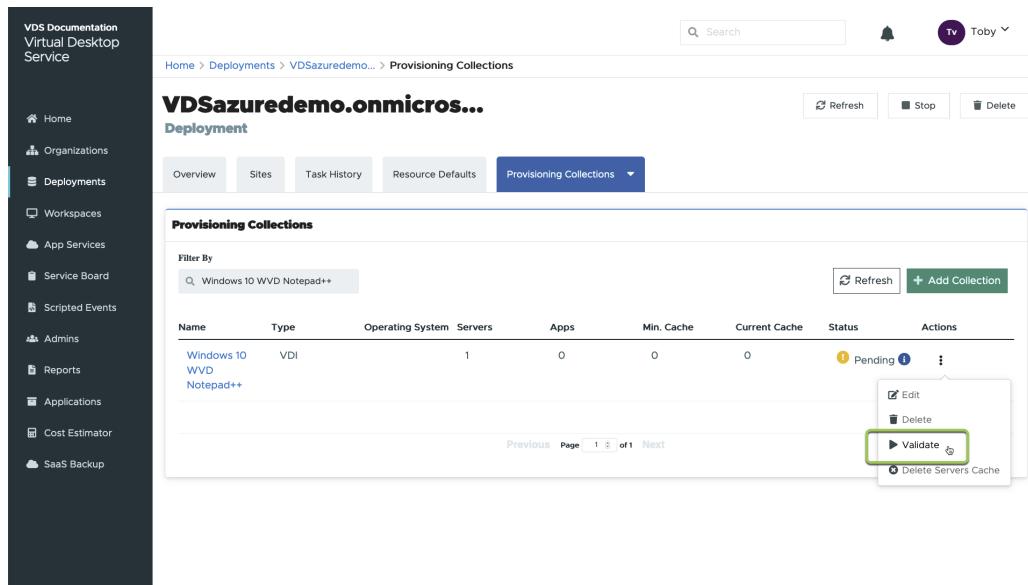
VDS includes functionality that will allow remove VM access from within the VDS web interface. By default a local Windows admin account is created with a rotating password and passed through to the VM allowing the VDS admin local admin access without needing to know local admin credentials.

 The Connect to Server function has an alternative setting where the VDS admin will be prompted for credentials with each connection. This setting can be enabled/disabled by editing the VDS admin account from within the "Admin" section of VDS. The functionality is called *Tech Account* and checking the box will require credential to be entered when using Connect to Server, unchecking this box will enable the automatic injection of local Windows admin credentials at each connection.

The VDS Admin simply needs to connect to the temporary VM using Connect to Server or another process and make the changes required to meet their requirements.

Validating the Collection

Once customization is complete, the VDS Admin can close the image and SysPrep it by clicking **Validate** from the Actions icon.



Name	Type	Operating System	Servers	Apps	Min. Cache	Current Cache	Status	Actions
Windows 10 WVD Notepad++	VDI		1	0	0	0	Pending	Edit Delete Validate Delete Servers Cache

Using the Collection

After validation has completed, the Status of the Provisioning Collection will change to **Available**. From within the Provisioning Collection the VDS Admin can identify the **VM Template** name which is used to identify this provisioning collection throughout VDS.

Name	Role	VM Template	Storage Type	Actions
TS		windows10e vDWi3500ve r1	StandardSSD_LRS	:

Previous Page 1 of 1 Next

New Server

From the Workspace > Servers page, a new server can be created and the dialog box will prompt for the VM Template. The template name from above will be found on this list:



VDS provides for an easy way to update session hosts in an RDS environment by using Provisioning Collections and the **Add Server** functionality. This process can be done without impacting end users and repeated over and over with subsequent image updates, building on previous image iterations. For a detailed workflow on this process, see the [RDS Session Host Update Process](#) section below.

New AVD Host Pool

From the Workspace > AVD > Host Pools page, new AVD Host Pool can be created by clicking **+ Add Host Pool** and the dialog box will prompt for the VM Template. The template name from above will be found on this list:

Add Host Pool

Basic Info

Name	Required	Friendly Name
Name...		Friendly Name...
Site	Required	Workspace
Select a site...		Select a site first
Host Pool Type	Required	Custom Profile Path
Select a host pool type...		Custom Profile Path...

Validation Environment

Included Session Hosts

OS Disk Type
 Ephemeral Persistent

VM Template	Required	Machine Size Type	Required
windows10	x	Select machine size type...	
Windows10EVD3497ver1			
Windows10EVDwi3500ver1			

Number of Instances
1

Cancel **Save**

New AVD Session Host(s)

From the Workspace > AVD > Host Pool > Session Hosts page, new AVD session host(s) can be created by clicking **+ Add Session Host** and the dialog box will prompt for the VM Template. The template name from above will be found on this list:

Shared WVD Pool

Host Pool

Session Hosts

Add Session Host

OS Disk Type
 Ephemeral Persistent

VM Template	Required	Machine Size Type	Required
Windows10	x	Standard_E2as_v4	x
Windows10EVD3497ver1			
Windows10EVDwi3500ver1			

Number of Instances
1

Cancel **Save**

VDS provides for an easy way to update session hosts in a AVD Host Pool by using Provisioning Collections and the **Add Session Host** functionality. This process can be done without impacting end users and repeated over and over with subsequent image updates, building on previous image iterations. For a detailed workflow on this process, see the [AVD Session Host Update Process](#) section below.



New Workspace

From the Workspaces page, a new workspace can be created by clicking **+ New Workspace** and the dialog box will prompt for the Provisioning Collection. The Shared Provisioning Collection name will be found on this list.

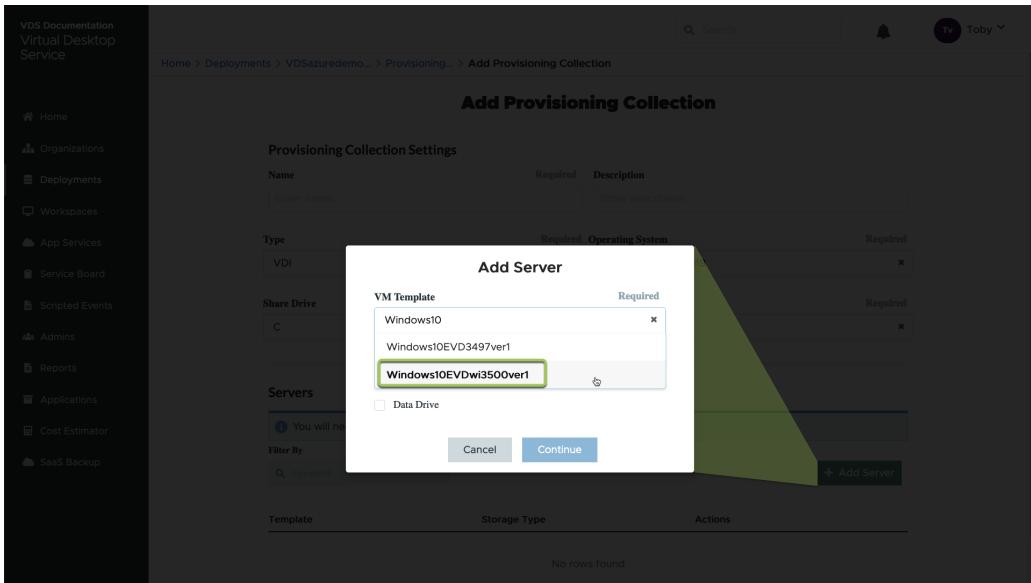
The screenshot shows the 'Add Workspace' dialog box with the 'Configure' tab selected. The top navigation bar includes a search bar, a bell icon, and a user profile for 'Toby'. The main form fields are as follows:

- Is this a new client?**: A radio button group where 'Yes' is selected.
- Company Name**: Omega Fuel
- Login Identifier**: @omegafuel
- Notification Email**: notify@omegafuel.abc
- Phone Number**: 5555555555
- Country**: United States
- Address 1**: 555 Main St
- Address 2**: Address 2...
- City**: Olympia
- State**: Washington
- Zip Code**: 98501
- Website**: Website...
- Internal Customer Number**: Customer number...
- Provisioning Info**
 - Deployment**: VDSGCPDemo (kxx)
 - Operating System**: Windows Server 2019
 - Provisioning Collection**: Default PC
 - Application Settings**:
 - Enable Remote App
 - Enable App Locker
 - Enable Application Usage Tracking
 - Device Settings**:
 - Disable Printing Access
 - Enable User Profile Disk
 - Enable User Workspace Data Storage
 - Permit Access to Task Manager
- Security Settings**:
 - Require Complex User Password
 - File Auditing Enabled
 - Migration Mode Enabled
 - Enable MFA for All Users

At the bottom are 'Cancel' and 'Next' buttons.

New Provisioning Collection

From the Deployment > Provisioning Collection page, a new Provisioning Collection can be created by clicking **+ Add Collection**. When adding servers to this collection the dialog box will prompt for the VM Template. The template name from above will be found on this list:



Addendum 1 - RDS Session Hosts

RDS Session Host Update Process

VDS provides for an easy way to update session hosts in a RDS environment by using Provisioning Collections and the **Add Server** functionality. This process can be done without impacting end users and repeated over and over with subsequent image updates, building on previous image iterations.

The RDS Session Host update process is as follows:

1. Build a new VDI Provisioning Collection, customize and validate the collection per the instructions above.
 - a. Generally this Provisioning Collection will be built on the previous VM Template, emulating an "Open, Save As" process.
2. Once the Provisioning Collection has validated, navigate to the *Workspace > Servers* page, click **+ Add Server**

3. Select **TS** as the **Server Role**
4. Select the latest **VM Template**. Make the appropriate **Machine Size** and **Storage Type** selections based on your requirements. Leave **Data Drive** unchecked.
5. Repeat this for the total number of Session Hosts required for the environment.
6. Click **Add Server**, the session hosts will build based on the selected VM Template and starting coming online in as soon as 10-15 minutes (depending on the hypervisor).

- a. Note that the Session Hosts currently in the environment will ultimately be decommissioned after these new host come online. Plan to build enough new hosts to be sufficient to support the entire workload in this environment.
7. When a new host comes online, the default setting is to stay in **Disallow New Sessions**. For each session host, the **Allow New Sessions** toggle can be used to manage which hosts can receive new user sessions. This setting is accessed by editing the settings of each individual session host server. Once sufficient new hosts have been built and functionality has been confirmed, this setting can be managed on both the new and old hosts to route all new sessions to the new hosts. The old hosts, with **Allow New Sessions** set to **disabled**, can continue to run and host existing user sessions.

The screenshot shows the 'Server Details' section for server 5Z5WTS8. It includes fields for Name (5Z5WTS8), Type (Shared), Connection (Offline), Status (Available), CPU (2), RAM (16GB), IP Addresses (N/A), and Uptime (N/A). Below this is the 'Connections' section, which contains a checkbox labeled 'Allow New Connections'. This checkbox is highlighted with a green rectangular box. At the bottom right of the 'Connections' section are 'Cancel' and 'Save' buttons.

8. As users log off of the old host(s), and with no new user sessions joining the old host(s), the old host(s) where **Sessions = 0** can be deleted by clicking the **Actions** icon and selecting **delete**.

The screenshot shows the 'Servers' table in the Azure WVD workspace. The table has columns for Name, Type, Machine Size, RAM, CPU, Online status (Offline), Status (Available), and Actions. The 'Actions' column for server 5Z5WTS6 shows a context menu with options: Backup, Start, Clone, and Delete. The 'Delete' option is highlighted with a green rectangular box. Other servers listed include 5Z5WTSD1, 5Z5WTSB, 5Z5WTS7, 5Z5WTS5, and 5Z5WTS4.

Addendum 2 - AVD Session Hosts

AVD Session Host Update Process

VDS provides for an easy way to update session hosts in a AVD Host Pool by using Provisioning Collections and the **Add Session Host** functionality. This process can be done without impacting end users and repeated

over and over with subsequent image updates, building on previous image iterations.

The AVD Session Host update process is as follows:

1. Build a new VDI Provisioning Collection, customize and validate the collection per the instructions above.
 - a. Generally this Provisioning Collection will be built on the previous VM Template, emulating an "Open, Save As" process.
2. Once the Provisioning Collection has validated, navigate to the *Workspace > AVD > Host Pools* page and click the name of the Host Pool
3. From within the *Host Pool > Session Hosts* page, click **+ Add Session Host**

The screenshot shows the 'Add Session Host' dialog box. At the top, it says 'Add Session Host'. Below that, under 'OS Disk Type', there are two options: 'Ephemeral' (radio button) and 'Persistent' (radio button, which is selected). There are four main configuration sections arranged in a grid-like layout. The first row contains 'VM Template' (dropdown menu showing 'Windows10EVDr3500ver1') and 'Machine Size Type' (dropdown menu showing 'Standard_E8as_v4'). Both have a red 'Required' label above them. The second row contains 'Machine Storage Type' (dropdown menu showing 'StandardSSD_LRS') and 'Number of Instances' (input field containing '12'). Both also have a red 'Required' label above them. At the bottom right of the dialog are two buttons: 'Cancel' and 'Save' (which is highlighted with a blue background).

4. Select the latest **VM Template**. Make the appropriate **Machine Size** and **Storage Type** selections based on your requirements.
5. Enter the **Number of Instances** equal to the total number of required Session Hosts. Typically this will be the same number as are currently in the Host Pool but it can be any number.
 - a. Note that the Session Hosts currently in the Host pool will ultimately be decommissioned after these new host come online. Plan for the **Number of Instances** entered to be sufficient to support the entire workload in this Host Pool.
6. Click **Save**, the session hosts will build based on the selected VM Template and starting coming online in as soon as 10-15 minutes (depending on the hypervisor).
7. When a new host comes online, the default setting is to stay in **Disallow New Sessions**. For each session host, the **Allow New Sessions** toggle can be used to manage which hosts can receive new user sessions. Once sufficient new hosts have been built and functionality has been confirmed, this setting can be managed on both the new and old hosts to route all new sessions to the new hosts. The old hosts, with **Allow New Sessions** set to **disabled**, can continue to run and host existing user sessions.

The screenshot shows the 'Session Hosts' tab selected in the 'Shared WVD Pool' section. The table lists four session hosts, all of which have 0 sessions and are online. The 'Actions' column for the first host has a context menu open, with the 'Disallow New Session' option highlighted.

Name	Allow New Session	Sessions	Online	Managed	Entity Status	Actions
5Z5WTS1.VDSazuredemo.onmicrosoft.com	✓	0	● Online	✓	Available	⋮
5Z5WTS10.VDSazuredemo.onmicrosoft.com	✓	0	● Online	✓	Available	⋮
5Z5WTS11.VDSazuredemo.onmicrosoft.com	✓	0	● Online	✓	Available	⋮
5Z5WTS12.VDSazuredemo.onmicrosoft.com	✓	0	● Online	✓	Available	⋮

- As users log off of the old host(s), and with no new user sessions joining the old host(s), the old host(s) where **Sessions = 0** can be deleted by clicking the **Actions** icon and selecting **delete**.

The screenshot shows the 'Session Hosts' tab selected in the 'Shared WVD Pool' section. The table lists four session hosts, with the first host's 'Allow New Session' checkbox now crossed out. The 'Actions' column for the first host has a context menu open, with the 'Delete' option highlighted.

Name	Allow New Session	Sessions	Online	Managed	Entity Status	Actions
5Z5WTS1.VDSazuredemo.onmicrosoft.com	✗	0	● Online	✓	Available	⋮
5Z5WTS10.VDSazuredemo.onmicrosoft.com	✓	0	● Online	✓	Available	⋮
5Z5WTS11.VDSazuredemo.onmicrosoft.com	✓	0	● Online	✓	Available	⋮
5Z5WTS12.VDSazuredemo.onmicrosoft.com	✓	0	● Online	✓	Available	⋮

VDS Logical Hierarchy Overview

Overview

VDS organizes concepts into various layers of a logical hierarchy. This article helps to outline how they fit together.

VDS Organizational Scheme

The VDS management portal is found at <https://manage.vds.netapp.com>. This web interface is a single pane of glass for managing all VDS-related objects. Within the VDS web UI, the following hierarchy of components and logical containers exist.

VDS Deployment

The *Deployment* is a VDS concept that organized and contains *VDS Workspace(s)*. In certain deployment

architectures a deployment can contain multiple VDS Workspaces.



Running multiple VDS Workspaces within a single Deployment is called "Multi-Tenancy" and is only an option in RDS deployments, AVD deployments do not support this approach.

A deployment is defined by its Active Directory domain and there is a 1:1 relationship between the AD domain and a Deployment.

There are certain VM resources that are deployed to support a deployment that are shared across all VDS Workspaces in the deployment. E.g. every Deployment contains a VM named "CWMGR1" which is a server that run VDS applications, a SQL Express database and facilitates management of the VDS Workspace(s) (and the contained resources) within the Deployment.

VDS Workspace



There is a difference between a "**VDS Workspace**" and a "**AVD Workspace**".

A VDS Workspace is a logical container inside the deployment for the client (end user) resources. These resources include Virtual Machines (for session hosts, application servers, database servers, file servers etc.), virtual networking, storage and other hypervisor infrastructure.

The VDS Workspace also contains management functionality to manage Users, Security Groups, Workload Scheduling, Applications, Automation, VMs, and AVD configuration.

Typically a VDS Workspace is aligned with a single company, or (in enterprise deployments), a business unit.

VDS Sites

Within a deployment, multiple Sites can be created to represent different infrastructure providers, all managed within a single deployment.

This is helpful when a single company or business unit needs to host users and apps across multiple physical locations (e.g North America and EMEA), hypervisor subscriptions (to align costs to business units) and even hypervisors (E.g. users in Azure, Google Compute and on-premises HCI on vSphere).

AVD Workspaces



There is a difference between a "**VDS Workspace**" and a "**AVD Workspace**".

A AVD Workspace is a logical container that sits inside a VDS Workspace and VDS Site. It that can be used similarly to a VDS Site for segmenting management and operational policies in the same deployment.

AVD Host Pools

AVD Host Pools are logical container that sit inside a AVD Workspace and hold the Session Hosts and App Groups users to server the user sessions and control access to individual resources.

AVD App Groups

Each AVD Host Pool starts with a single "Desktop" App Group. Users and/or groups can be assigned to this (or other) App Group to allow access to the resources in the App Group to the assigned users.

Additional App Groups can be created within a host pool in VDS. All Additional App Groups are "RemoteApp"

App Groups and serve RemoteApp resources as opposed to a full windows desktop experience.

Applications

Application Entitlement

Overview

VDS has a robust application automation and entitlement functionality built-in. This functionality allows users to have access to different applications while connecting to the same session host(s). This is accomplished by some custom GPOs hiding shortcuts along with automation selectively placing shortcuts on the users' desktops.



This workflow only applies to RDS deployments. For AVD application entitlement documentation, please see [Application Entitlement Workflow for AVD](#)

Applications can be assigned to users directly or via Security groups managed in VDS.

At a high level, the application provisioning process follows these steps.

1. Add App(s) to App Catalog
2. Add App(s) to the workspace
3. Install the Application on all Session Hosts
4. Select the Shortcut path
5. Assign apps to users and/or groups



Steps 3 & 4 can be fully automated with Scripted Events as illustrated below

NetApp

NetApp Virtual Desktop Service

Application Management

Toby vanRoojen
Product Marketing Manager
June, 2020

[Video Walkthrough](#)

Add applications to the App Catalog

VDS Application Entitlement starts with the App Catalog, this is a listing of all the applications available for deployment to end user environments.

To add applications to the catalog, follow these steps

1. Log in to VDS at <https://manage.cloudworkspace.com> using your primary admin credentials.
2. In the upper right, click the arrow icon next to your User Name and select Settings.
3. Click the App Catalog tab.
4. Click the Add App option in the Application Catalog title bar.
5. To add a group of applications, choose the Import Apps option.
 - a. A dialog will appear that provides an Excel template to download that creates the correct format for the application list.
 - b. For this evaluation NetApp VDS has created a sample application list for import it can be found [here](#).
 - c. Click on the Upload area and choose the application template file, click the Import button.
6. To add individual applications, choose the Add App button and a dialog box will appear.
 - a. Enter the name of the application.
 - b. External ID can be used to enter an internal tracking identifier such as a product SKU or billing tracking code (optional).
 - c. Check the Subscription box if you want to report on the applications as a Subscription product (optional).
 - d. If the product does not install by version (for example Chrome) check the Version Not Required checkbox. This allows “continuous update” products to be installed without tracking their versions.
 - e. Conversely, if a product supports multiple named versions (ex: Quickbooks) you need to check this box so that you can install multiple versions and have VDS specific each available version in the list of applications that can be entitled for and end user.
 - f. Check “No User Desktop Icon” if you don’t want VDS to provision a desktop icon for this product. This is used for “backend” products like SQL Server since end users don’t have an application to access.
 - g. “App Must be Associated” enforces the need for an associated app to be installed. For example, a client server application may require SQL Server or mySQL to be installed as well.
 - h. Checking the License Required box indicates that VDS should request a license file to be uploaded for an installation of this application before it sets the application status to active. This step is performed on the Application detail page of VDS.
 - i. Visible to All – application entitlement can be limited to specific subpartners in a multi-channel hierarchy. For evaluation purposes, click the Check Box so that all users can see it in their available application list.

Add the application to the Workspace

To start the deployment process you’ll add the app to the workspace.

To do this, follow these steps

1. Click Workspaces
2. Scroll down to Apps
3. Click Add

4. Check box the application(s), enter required information, click Add Application, click Add Apps.

Manually install the application

Once the application has been added to the Workspace you'll need to get that application installed on all session hosts. This can be done manually and/or it can be automated.

To manually install applications on session hosts, follow these steps

1. Navigate to Service Board.
2. Click on the Service Board Task.
3. Click on the Server Name(s) to connect as a local admin.
4. Install the app(s), confirm the shortcut to this app is found in the Start Menu path.
 - a. For Server 2016 and Windows 10: C:\ProgramData\Microsoft\Windows\Start Menu\Programs.
5. Go back to the Service Board Task, click Browse and choose either the shortcut or a folder containing shortcuts.
6. Whichever you select is what will be displayed on the end user desktop when assigned the app.
7. Folders are great when an app is actually multiple applications. e.g "Microsoft Office" is easier to deploy as a folder with each app as a shortcut inside the folder.
8. Click Complete Installation.
9. If required, open the created Icon Add Service Board Task and confirm the icon has been added.

Assign applications to users

Application entitlement is handled by VDS and application can be assigned to users in three ways

Assign Applications to Users

1. Navigate to the User Detail page.
2. Navigate to the Applications section.
3. Check the box next to all applications required by this user.

Assign users to an application

1. Navigate to the Applications section on the Workspace Detail page.
2. Click on the name of the application.
3. Check the box next to the users the application.

Assign applications and users to user groups

1. Navigate to the Users and Groups Detail.
2. Add a new group or edit an existing group.
3. Assign user(s) and application(s) to the group.

Application Entitlement Workflow for AVD

Overview

In a Azure Virtual Desktop (AVD) environment, application access is managed by app group membership.



This workflow only applies to AVD deployments. For RDS application entitlement documentation, please see [Application Entitlement Workflow for RDS](#)



AVD is a well documented service and there are many [public resources for information](#). VDS does not supersede the standard way that AVD operates. Rather, this article is designed to illustrate how VDS approaches the standard concept found across all AVD deployments.



Reviewing the [VDS Logical Hierarchy Overview](#) article may be useful before or while reviewing this article.

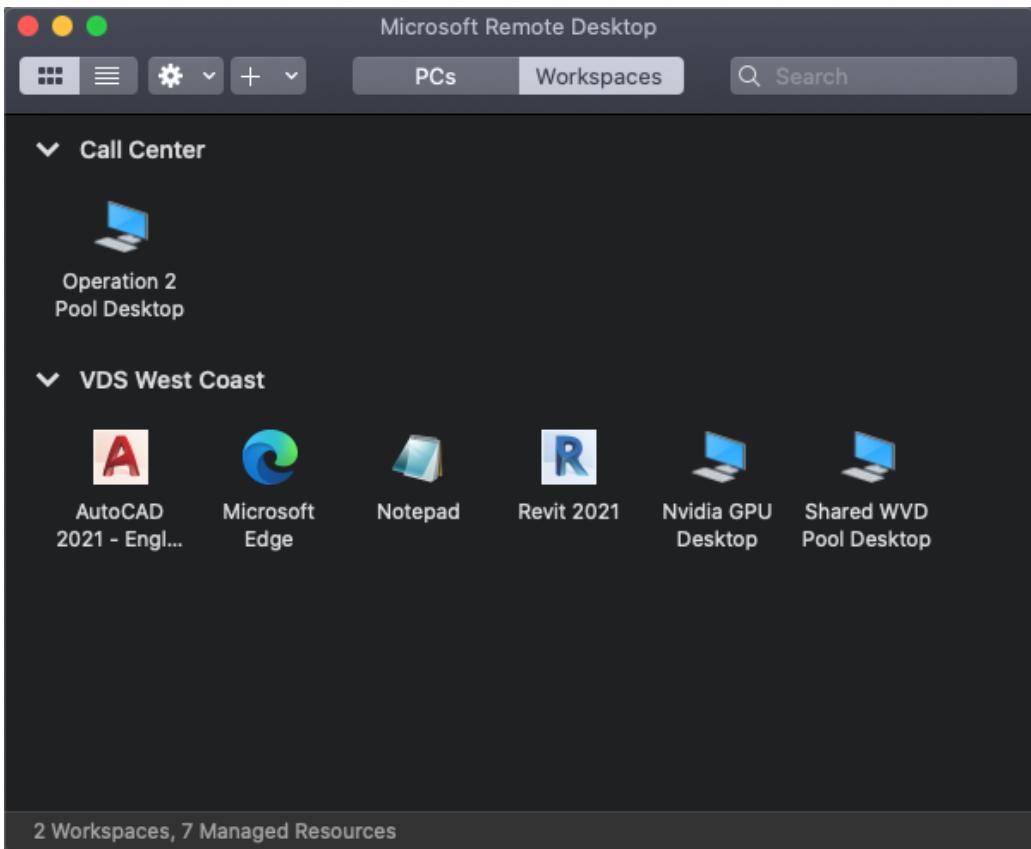
The End User View

In Azure Virtual Desktop, each end user is assigned access to RemoteApp(s) and/or Desktop(s) by their AVD administrator. This is accomplished via App Group assignment in VDS.

RemoteApp refers to an application that runs remotely on the session host but is presented on the local device without the desktop context. Commonly referred to as a "streaming app", these applications look like local applications on the local device but run in the security context, and on the storage and compute layer of the session host.

Desktop refers to the full Windows experience running on the session host and presented on the local device, typically in a full screen window. Commonly referred to as "remote desktop", this desktop itself will contain any applications installed on that session host which can be launched by the user from within the desktop session window.

At login, the end user is presented with the resources assigned to them by their administrator. Below is an example of the view an end user may see when logging in with their AVD client. This is a more complex example, often an end user will only have a single desktop or RemoteApp assigned to them. The end user can double click on any of these resources to launch that application/desktop.

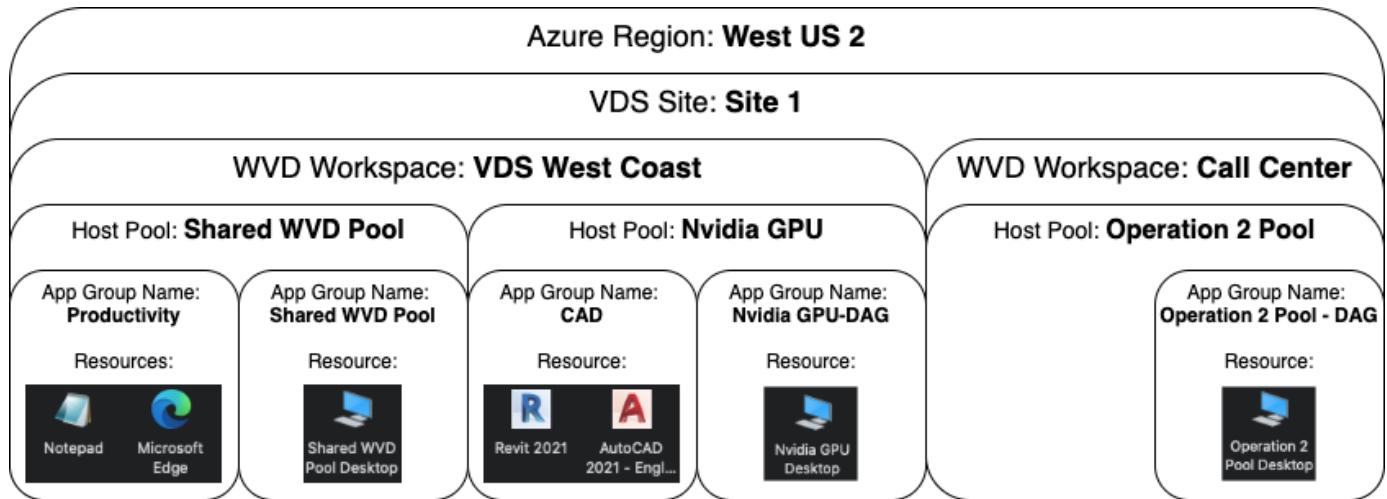


In this more complex example, this user has access to two different desktop sessions and 4 different streaming applications:

- **Available Desktops**
 - Nvidia GPU Desktop
 - Shared AVD Pool Desktop
 - Operation 2 Pool Desktop
- **Available RemoteApps**
 - AutoCAD 2021
 - Revit 2021
 - Microsoft Edge
 - Notepad

Behind the scenes these applications and desktops are hosted across a variety of session hosts, AVD workspaces and could even be hosted in different Azure regions.

Here is a diagram illustrating where each of these resources are hosted and how they got assigned to this end user.



As shown above, the various resources available to this end user are hosted in different session hosts, in different host pools, and potentially managed by different IT organizations in different AVD Workspaces. While not showing in this example, these resources could also be hosted in different Azure regions and/or subscriptions using the VDS Sites feature.

Providing Desktop Access

By default every host pool starts with a single app group, used to assign access to the Windows desktop experience. All applications installed on these session hosts will be accessible to the end users assigned to this app group.

To enable the Desktop resource for users in VDS:

1. Navigate to the Workspaces > AVD > Host Pool > App Groups page and click on the App group for the "Desktop" resource.

[Management.Applications.AVD application entitlement workflow 349fe] |

Management.Applications.AVD_application_entitlement_workflow-349fe.png

2. Once inside the App Group, click Edit

[Management.Applications.AVD application entitlement workflow 3bcfc] |

Management.Applications.AVD_application_entitlement_workflow-3bcfc.png

3. From the edit dialog, you can add or remove users to this App Group by User and/or by Groups.

[Management.Applications.AVD application entitlement workflow 07ff0] |

Providing RemoteApp Access

In order to provision access to RemoteApps, a new app group needs to be created within the host pool. Once created, the appropriate apps need to be assigned to this app group.



Any applications on these sessions hosts will already be available to any users assigned to this host pool's "Desktop" AppGroup. It is not necessary to also provision access via a RemoteApp app group simply to provide access to apps. A RemoteApp app group is only necessary to enable access to apps that run as-if on the local device as a streaming app.

Create a New App Group

1. Navigate to the Workspaces > AVD > Host Pool > App Groups page and click on the *+ Add App Group* button

[Management.Applications.AVD application entitlement workflow d33da] |

Management.Applications.AVD_application_entitlement_workflow-d33da.png

2. Enter the Name, Workspace and Friendly Name for this app group. Select the users and/or groups that should be assigned and click Save

[Management.Applications.AVD application entitlement workflow 242eb] |

Add Applications to the App Group

1. Navigate to the Workspaces > AVD > Host Pool > App Groups page and click on the App group for the "RemoteApp" resource.

[Management.Applications.AVD application entitlement workflow 3dcde] |

Management.Applications.AVD_application_entitlement_workflow-3dcde.png

2. Once inside the App Group, click Edit

[Management.Applications.AVD application entitlement workflow 27a41] |

Management.Applications.AVD_application_entitlement_workflow-27a41.png

3. Scroll down to the "Remote Apps" section. This section may take a moment to populate as VDS is directly querying the session hosts to show available apps for streaming.

[Management.Applications.AVD application entitlement workflow 1e9f2] |

4. Search and select any apps that the users in this app groups should have access to as a RemoteApp resource.

Scripted Events

Scripted Events

Overview

Scripted Events provides the advanced administrator with a mechanism to create custom automation for system maintenance, user alerts, group policy management, or other events. Scripts can be designated to run as an executable process with arguments, or can be used as arguments for a different executable program. This functionality allows for scripts to be combined and nested to support complex customization and integration needs.

A detailed example of scripted events in action is found in the [Application Entitlement Guide](#).

Additionally, Scripted Events allows for the creation of automation that does not require a script to process, rather the automation flow is launched by a system trigger and runs an existing program or system utility with optional arguments.

Scripted Events contains both a **repository** of scripts and **activities**. Scripts contain the instructions on **what** to do while activities link the scripts with the appropriate trigger and target (**when and where**) for the script.

Repository

The Repository Tab shows a list of all scripts available to be deployed from within your VDS account. This is a custom repository that is shared by all administrators in your VDS instance. Access to Scripted Events can be managed on the *VDS > Admins > Permissions page*.

The screenshot shows the NetApp Virtual Desktop Service interface. On the left, there's a sidebar with links: Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events (which is highlighted), and Admins. The main area has a header with 'Home > Scripted Events' and a search bar. Below that is a 'Scripted Events' section with tabs for 'Repository' (which is selected and highlighted with a green box) and 'Activities'. There's a 'Filter By' section with a keyword search input and checkboxes for 'Customer' and 'Global'. At the bottom are buttons for 'Refresh' and '+ Add Script'. A table lists two scripts: 'Install Adobe Reader' and 'Install Microsoft Office 365'. The table columns are Name, Script, Type, Created on, and Actions (with three dots). The 'Install Microsoft Office 365' row also has a 'Customer' checkbox next to it.

Name	Script	Type	Created on	Actions
Install Adobe Reader	InstallAdobeReader.ps1	Customer	Dec 4, 2020, 12:39 PM	⋮
Install Microsoft Office 365	InstallMicrosoftOffice365.ps1	Customer	Dec 8, 2020, 9:57 AM	⋮

Customer Filter

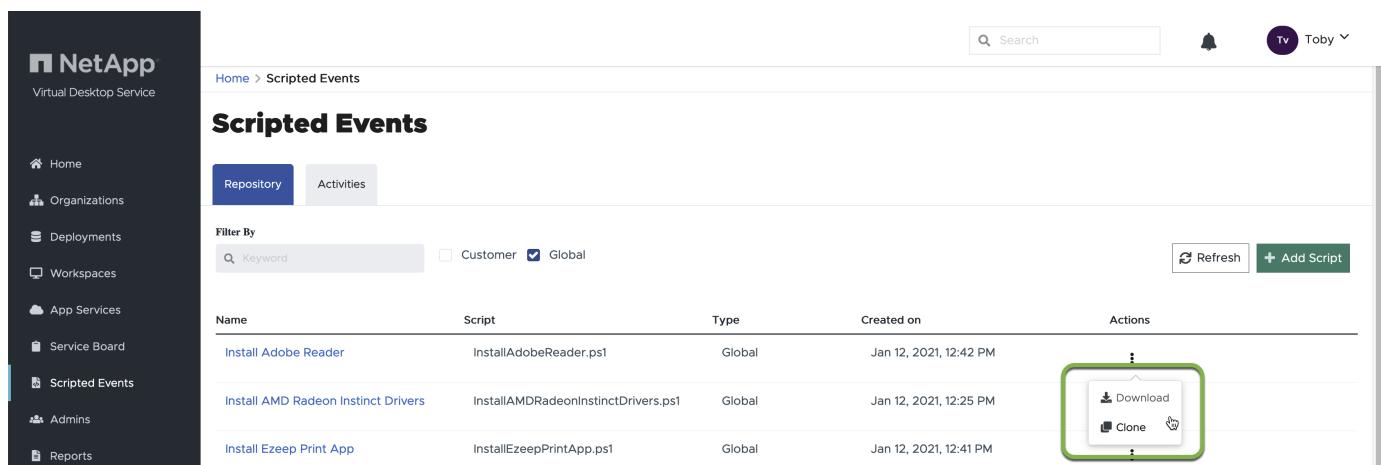
Each VDS administrator organization has a private library of scripts created and/or customized by their organization. These scripts are defined as Script Type "Customer." Customer scripts can be deleted and edited by any VDS administrator with appropriate admin permissions to the Scripted Events section.

Global Filter

NetApp also publishes and maintains a library of "Global" scripts that is the same across all VDS administrator organizations. These scripts are defined as Script type "Global." Global scripts can not be edited or deleted by any VDS administrator. Rather, Global scripts can be "Cloned" and the resulting script is a "Customer" script that can be edited and used.

Download Script

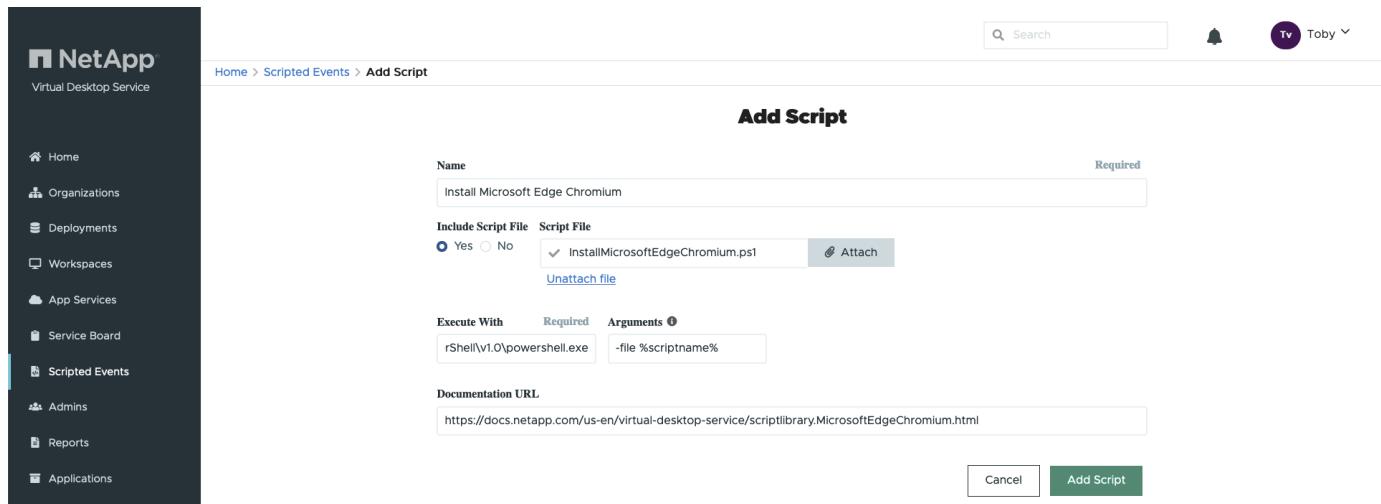
The ability to download the script file associated with a Scripted Event allows the VDS Administrator to review and edit the underlying script file prior to deployment. Running a script that you don't fully understand is never advisable.



The screenshot shows the 'Scripted Events' page. On the left is a sidebar with links like Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events (which is selected), Admins, and Reports. The main area has tabs for 'Repository' (selected) and 'Activities'. A 'Filter By' section includes a keyword search field, 'Customer' and 'Global' checkboxes (the latter is checked), a 'Refresh' button, and a '+ Add Script' button. Below is a table with columns: Name, Script, Type, Created on, and Actions. Three scripts are listed: 'Install Adobe Reader', 'Install AMD Radeon Instinct Drivers', and 'Install Ezeep Print App'. The third row's Actions column has a context menu with 'Download' and 'Clone' options, both of which are highlighted with a green rounded rectangle.

Add Script

Clicking on the **+ Add Script** button opens a new page for creating a script and saving it to the repository.



The screenshot shows the 'Add Script' form. The sidebar on the left is identical to the previous one. The main form has fields for 'Name' (containing 'Install Microsoft Edge Chromium'), 'Include Script File' (radio button for 'Yes' selected, pointing to 'InstallMicrosoftEdgeChromium.ps1'), 'Execute With' (containing 'rShell\vl1.0\powershell.exe -file %scriptname%'), and 'Documentation URL' (containing 'https://docs.netapp.com/us-en/virtual-desktop-service/scriptlibrary/MicrosoftEdgeChromium.html'). At the bottom are 'Cancel' and 'Add Script' buttons, with 'Add Script' being the active one.

The following fields need to be completed to create a new script:

- **Name**
- **Include Script File**
 - Yes - Allows for a script file (e.g. a .ps1 file) to be uploaded and run by the "Execute With" executable.
 - No - Removes the "Script File" field (below) and simply runs the "Execute With" and "Arguments" command

- **Script File**

- If *Include Script File* = Yes this field is visible and allows for the upload of a script file.

- **Execute With**

- Defines the path of the executable that is used to run the script file or the command that is run.
- For example, to run with PowerShell the "Execute With" value would be
C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe

- **Arguments**

- Defines any additional arguments that are run against the "Executes With" command.
- VDS offers some context aware variables that can be used including:
 - %companycode% - Company code at runtime
 - %servername% - VM name at runtime
 - %samaccountname% - <username>.<companycode>
 - %applicationname% - Requested application name at runtime
 - %scriptname% - Script name at runtime
 - %username% - username@loginidentifier at runtime

- **Documentation URL**

- This field allows the writer of the script to link it to documentation found outside of VDS such as a Knowledge Base system used by the VDS admins' organization.

Edit Script

Clicking the name of a script in the repository opens a new page with details about the script and an action button to **edit**.

When editing a script the same fields are editable as documented above in the [Add Script](#) section.

On this script detail page, you can also **delete** the script and **download** any uploaded script file.

The screenshot shows the NetApp Virtual Desktop Service web interface. On the left is a dark sidebar with various navigation options like Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events, Admins, Reports, Applications, Cost Estimator, and SaaS Backup. The main content area has a header with 'Home > Scripted Events > Install Microsoft Office 365'. Below the header, the title 'Install Microsoft Off...' is displayed, followed by a 'Script' tag and an 'Overview' tab. The main content is a 'Script Details' table with the following data:

Script Details			
Name	Install Microsoft Office 365	Type	Customer Script
Script	InstallMicrosoftOffice365.ps1	Execute With	C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe
Created By	toby.vanrooijen@vdsdocsdemo	Created On	Dec 8, 2020, 9:57 AM
Updated By	None	Updated On	None
Documentation URL	https://docs.netapp.com/us-en/virtual-desktop-service/scriptlibrary/MicrosoftOffice365.html		

At the top right of the main content area, there are buttons for Refresh, Download (highlighted with a green border), Edit, and a more options menu. A search bar and a user profile for 'Toby' are also at the top right.

Activities

Activities link a script from the repository to a Deployment, a subset of VMs and a trigger event.

The screenshot shows the 'Scripted Events' section of the NetApp Virtual Desktop Service. On the left is a sidebar with links like Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events (which is selected and highlighted in blue), and Admins. The main area has a header 'Scripted Events' with tabs for 'Repository' and 'Activities'. A green box highlights the 'Activities' tab. Below it is a search bar with 'Filter By Keyword' and a 'Refresh' button. A table lists two activities: 'InstallAdobeReader' and 'UninstallAdobeReader'. Each row includes columns for Name, Script, Deployment, Event, Clients, App Services, Enabled (with a checkmark), and Actions (with a three-dot menu icon). The 'InstallAdobeReader' row also has a small green checkmark icon.

Add Activity

Clicking on the **+ Add Activity** button opens a new page for creating an Activity.

The screenshot shows the 'Add Activity' page. The left sidebar is identical to the previous one. The main area has a header 'Add Activity'. It contains several sections: 'Activity Settings' (Name: 'Install Chrome', Description: 'Install Chrome'), 'Deployment' (Deployment: 'VDSGCPDemo (kxk)', Script: 'InstallGoogleChrome', Arguments: 'Enter arguments...'), an 'Enabled' checkbox which is checked, 'Event Settings' (Event Type: 'Application Install'), 'Target Settings' (Application: 'Google Chrome', Shortcut Path: '\\shortcuts\\Google Chrome.lnk'), and a 'Cancel' and 'Add Activity' button at the bottom. The 'Add Activity' button is highlighted with a green box.

The following fields need to be completed to create a new activity:

- **Name**
- **Description (Optional)**
- **Deployment**
- **Script**
- **Arguments**
- **Enabled** checkbox
- **Event Settings**

Activity Triggers

The screenshot shows the 'Add Activity' page in the NetApp Virtual Desktop Service. On the left is a dark sidebar with navigation links like Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events, Admins, Reports, Applications, Cost Estimator, and SaaS Backup. The main area has a header with a search bar, a bell icon, and a user profile for 'Toby'. Below the header, the 'Add Activity' title is centered. Underneath it is the 'Activity Settings' section with fields for 'Name' (Required) and 'Description'. The 'Deployment' section includes tabs for 'Script' (Required), 'Script' (Required), and 'Arguments'. A checkbox for 'Enabled' is checked. The 'Event Settings' section is highlighted with a green oval. It contains a dropdown menu titled 'Event Type' with options: Application Install, Application Uninstall, Clone Server, Create Cache, Create Client, Create Server, Create User, Delete User, Manual, Manual Application Update, Scheduled, and Start Server. The 'Required' label is visible at the top right of the dropdown. At the bottom of the page, there's a footer with a copyright notice and links to Privacy and Terms of Use.

• Application Install

- This is triggered when the VDS Admin clicks "+ Add..." from the *Workspace > Applications* page.
- This selection allows you to select an application from the Application Library and to pre-define the shortcut of the application.
- Detailed instructions for this trigger are highlighted in the [Install Adobe Reader DC script documentation](#).

• Application Uninstall

- This is triggered when the VDS Admin clicks **Actions > Uninstall** from the *Workspace > Applications* page.
- This selection allows you to select an application from the Application Library and to pre-define the shortcut of the application.
- Detailed instructions for this trigger are highlighted in the [Uninstall Adobe Reader DC script documentation](#).

• Clone Server

- This is triggered when the Clone function is performed against an existing VM

• Create Cache

- This is triggered anytime a new VM is built by VDS for a provisioning collection cache

• Create Client

- This is triggered anytime a new Client organization is added to VDS

• Create Server

- This is triggered anytime a new VM is built by VDS

- **Create User**

- This is triggered anytime a new user is added via VDS

- **Delete User**

- This is triggered anytime a new user is deleted via VDS

- **Manual**

- This is triggered by a VDS admin manually from within the **Scripted Events > Activity** page

- **Manual Application Update**

- **Scheduled**

- This is triggered when the defined date/time is reached

- **Start Server**

- This is triggered on a VM each time it boots up

Clicking on the *Name* opens a dialog box where the activity can be edited.

Command Center

Command Center Command: Overview

Overview

The Command Center is an executable that runs on the CWMGR1 Platform Server in the Deployment. It is accessed by connecting to the CWMGR1 VM and executing it locally on that VM.

This application was designed for troubleshooting, diagnostic and advanced management functions. This application is primarily used by NetApp's internal development and support teams however some functions are occasionally used by customer admins. This documentation is provided to support the use of selection functions. Use of these commands should be done with care and in collaboration with the NetApp support team.

Running Command Center

To run the Command Center application:

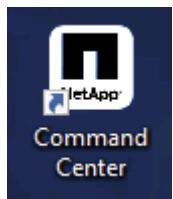
1. Connect to the server from the *VDS > Deployment > Platform Servers* page click the *Actions* icon and select "Connect"

Name	CPU	RAM (GB)	Online	Actions
CWMGR1	2	8	Online	

2. When prompted for credentials enter domain admin credentials
 - a. The user will need to be a member of the "CW-Infrastructure" security group. For consistency sake we recommend adding this membership by making the user a member fo the "Level 3 Technicians" group in AD > Cloud Workspace > Cloud Workspace Tech Users > Groups

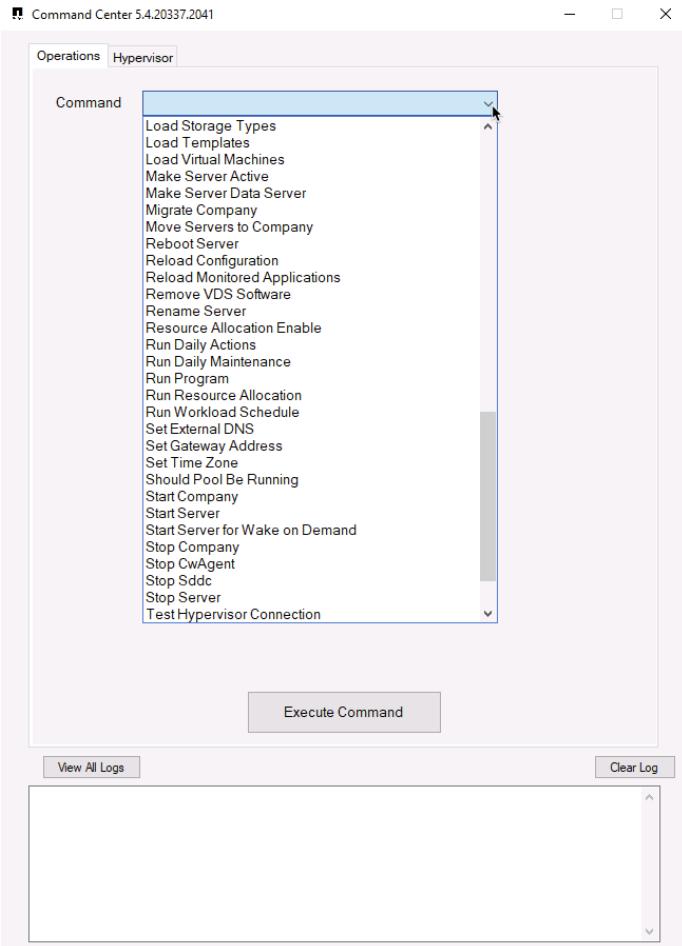
Name	Type	Description
CW-CWMGRAccess	Security Group...	CW-CWMGRAccess - en...
Level3 Technicians	Security Group...	Level 3 technicians - en...

3. Locate the desktop icon for *Command Center* and run it



- a. To enable the advanced tab, launch the application with the "-showadvancedtab" switch.

Operations Tab



From the **Command** menu you can select from a list of actions (listed below).

Once a command is selected, data can be populated with deployment data from the **Load Data** button. The Load Data button is also used to query the hypervisor for data once earlier selections are made (e.g. Loading a list of available backup dates after selecting a specific VM from a dropdown)



After making selections on a command, clicking **Execute Command** will run the selected process.

To review logs, click the **View All Logs** button. The raw text file will open, with newest entries at the bottom.

Command List

- Copy Template to Gallery

Operations

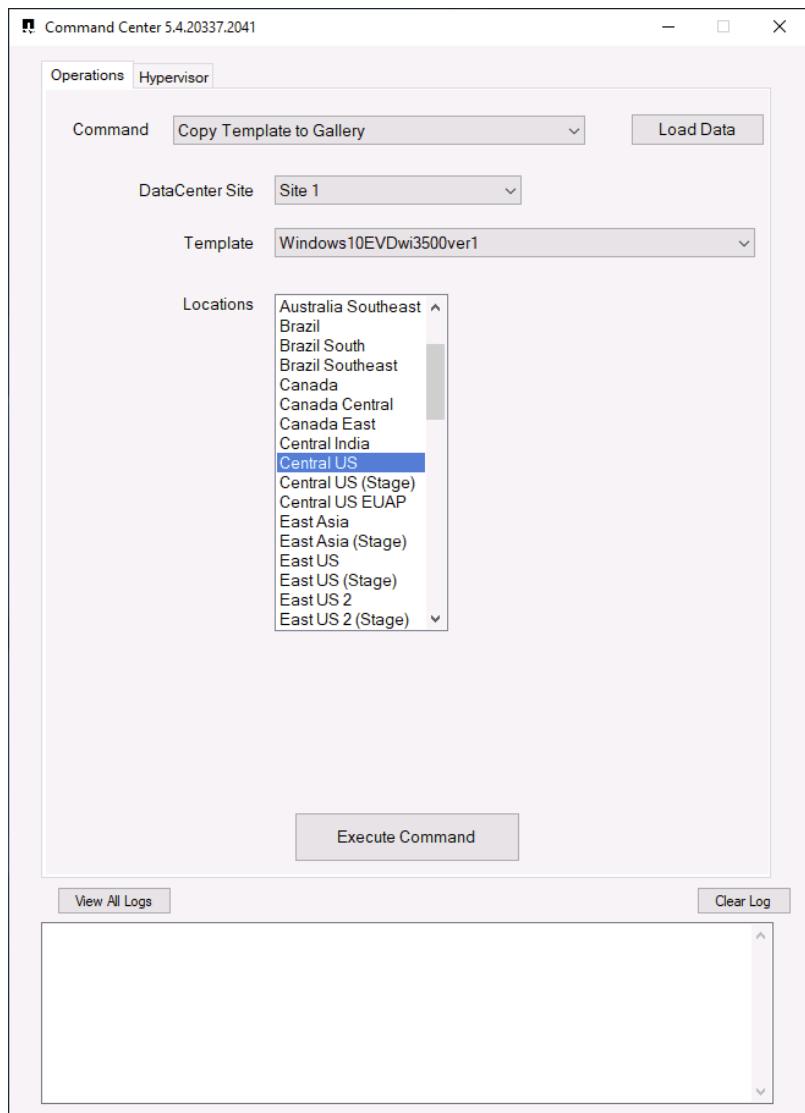
Command Center Command: Copy Template to Gallery

Command Center Warning



The Command Center is an application that runs on the CWMGR1 Platform Server in the Deployment. This application was designed for troubleshooting, diagnostic and advanced management functions. This application is primarily used by NetApp's internal development and support teams however some functions are occasionally used by customer admins. This documentation is provided to support the use of selection functions. Use of these commands should be done with care and in collaboration with the NetApp support team. More information can be found in the [Command Center Overview](#) article.

Copy Template to Gallery Overview



When a VDI Provisioning Collection is finalized the image is stored in Azure as an Image and can be deployed within the same VDS Site. In order to make the image available for deployment in another Azure region within the same Subscription the "Copy Template to Gallery" function is used. This action will copy the VM image to the Shared gallery and replicate it to all the selected regions.

VM Template Availability in VDS Dropdown

Once the replication has completed, the image will show in VDS in the dropdown for selecting VM Templates when deploying new VMs. The shared image will be available for deployment into any region that is selected when copying.

The screenshot shows the Azure portal interface for a shared image gallery named 'YBY_Site1'. The main pane displays the details for the image 'Windows10WVDNo3503ver1'. The 'Essentials' section includes fields like Resource group (yby), Status (Succeeded), Location (West US 2), Subscription (Azure subscription 1), and SKU (Windows10WVDNo3503ver1). The 'Image versions' section shows a single version entry: Name (1.0.0), Provisioning state (Creating), Source image (Windows10WVDNo3503ver1), Target regions (2), Storage account type (Standard HDD), and Replication status (InProgress). The left sidebar lists other sections such as Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Image versions, Configuration, Properties, Locks, Automation, Tasks (preview), Export template, Support + troubleshooting, and New support request.

VM Images stored in the Shared Gallery are appended with their version in the form of "-x.x.x" where the version matches the image version within the Azure Portal.

VM Template	Required
3500	
Windows10EVDwi3500ver1-1.0.0	
Windows10EVDwi3500ver1	



The replication of the image can take a while (depending on the size of the image) and the status can be seen by clicking on the version (e.g. 1.0.0) in the "Name" column as highlighted in the screenshot above.

Regional Availability

Deployments can only be performed into the regions where the image has been replicated. This can be checked in the Azure portal by clicking on the 1.x.x and then on *Update Replication* as shown here:

Microsoft Azure Search resources, services, and docs (G+ /) admin@VDSazuredemo... VDS SALES DEMO

Home > Shared image galleries > YBY_Site1 > Windows10EVD3497ver1 (YBY_Site1/Windows10EVD3497ver1) > 1.0.0 (YBY_Site1/Windows10EVD3497ver1/1.0.0)

1.0.0 (YBY_Site1/Windows10EVD3497ver1/1.0.0) | Update replication

Image version

Search (Cmd+/) Save Discard Refresh

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Update replication Configuration Properties Locks Automation Tasks (preview) Export template Support + troubleshooting New support request

Target regions Target region repl... Storage account type Replication status

Target regions	Target region repl...	Storage account type	Replication status
(US) Central US	1	Standard HDD	Completed
(US) West Cent...	1	Standard HDD	Completed
(US) West US 2	1	Standard HDD	Completed
		Standard HDD	-

Resource Optimization

Workload scheduling

Workload Scheduling is a feature that can schedule the time window in which the environment is active.

Workload scheduling can be set to "Always On", "Always Off" or "Scheduled". When set to "Scheduled" the on and off times can be set as granularly as a different time window for each day of the week.

5.4 Preview

Edit Workload Schedule

Status

Scheduled

Scheduling Options

- Run at assigned time interval everyday
- Run at assigned time interval on specified days
- Run at variable time interval and days

Days

Sun Mon Tue Wed Thu Fri Sat

Current Schedule

4 Day(s) Scheduled.

Cancel Update Schedule

When scheduled to be off, either via "Always Off" or "Scheduled", all tenant virtual machines will shut down. Platform servers (such as CWMGR1) will remain active to facilitate functionality such as wake on demand.

Workload Schedule works in conjunction with other resource optimization features including Live Scaling and Wake on Demand.

Wake on demand

Wake on Demand (WoD) is patent-pending technology that can wake the appropriate VM resources for an end user in order to facilitate unattended access 24/7, even when resources are scheduled to be inactive.

WoD for Remote Desktop Services

In RDS, the VDS Windows Client has built-in Wake on Demand integration and can wake the appropriate resources without any additional end-user actions. They simply need to initiate their normal login and the client will notify them of a short delay which the VM(s) are activated. This client (and thus this automate wake on demand functionality) is only available when connecting from a Windows device to an RDS environment.

Similar Functionality is built into the VDS Web client for RDS deployments. The VDS Web Client is found at: <https://login.cloudworkspace.com>

Wake on Demand functionality is not built into the Microsoft RD client (for Windows or any other platform) nor

any other 3rd party RD clients.

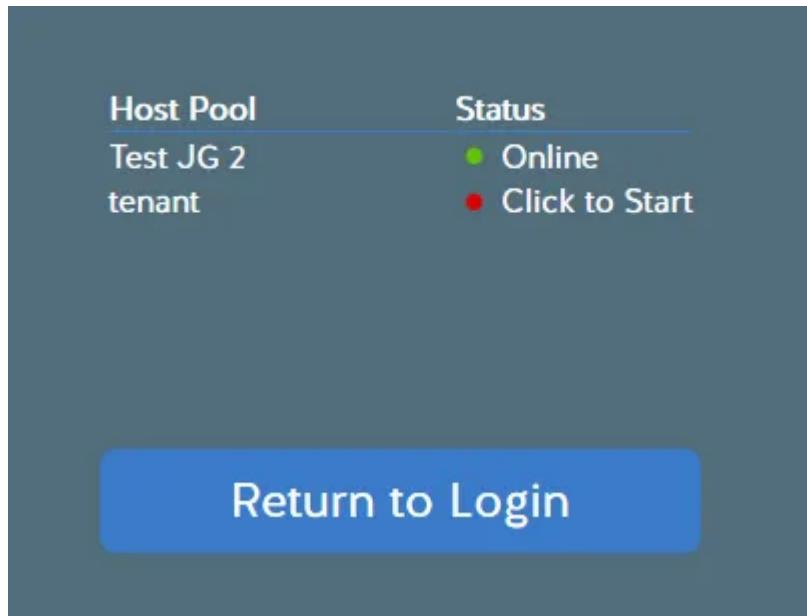
Wake on demand for Azure Virtual Desktop

In AVD, the only clients that can be used to connect are Microsoft provided and thus do not contain the Wake on Demand functionality.

VDS does include a self-service Wake on Demand function for AVD via the VDS Web Client. The web client can be used to wake the appropriate resources, then the connection can be initiated via the standard AVD client.

To wake VM resources in AVD:

1. Connect to the VDS Web Client at <https://login.cloudworkspace.com>
2. Login with the user AVD credentials
 - A warning message will prompt "*You have Microsoft's AVD services available. Click HERE to view the status and start offline Host Pools.*"
3. After clicking "*HERE*" you'll see a list of available Host Pools along with a link to "Click to Start" link under the status column



4. *Click to Start* the link and wait 1-5 minutes for the status to change to "Online" and show a green status icon
5. Connect to AVD using your normal process

Live Scaling

Live Scaling works in conjunction with Workload Scheduling by managing the number of online session hosts during the scheduled active time as configured in Workload Scheduling. When scheduled to be offline, Live Scaling won't control session host availability. Live scaling only impacts Shared Users and Shared Servers in RDS and AVD environments, VDI Users and VDI VMs are excluded from these calculations. All other VM types are unaffected.



The AVD *load balancer type* setting interacts with this configuration, so care should be taken in choosing that setting as well. Cost savings are maximized with a depth-first type while end user performance is maximized with a breadth-first type.

Enabling Live Scaling with no options checked, the automation engine will automatically select values for the Number of Extra Powered on Servers, Shared Users Per Server, and Max Shared Users Per Server.

- The *Number of Extra Powered on Servers* defaults to 0, meaning 1 server will run 24/7.
- The *Shared Users Per Server* defaults to the number users in the company divided by the number of servers.
- The *Max Shared Users Per Server* defaults to infinite.

Live Scaling turns the servers on as users log on and turns them off as users log off.

Powering an additional server is automatically triggered once the total active users reaches the number of Shared Users per Server multiplied by the total number of Powered On Servers.

e.g. With 5 Shared Users per Server set (this is the default # we'll use for all examples in this article) and 2 servers running, a 3rd server won't be powered up until server 1 & 2 both have 5 or more active users. Until that 3rd server is available, new connections will be load balanced all available servers. In RDS and AVD Breadth mode, Load balancing sends users to the server with the fewest active users (like water flowing to the lowest point). In AVD Depth mode, Load balancing sends users to servers in a sequential order, incrementing when the Max Shared Users number is reached.

Live Scaling will also turn off servers to save costs. When a server has 0 active users, and another server has available capacity below *Shared Users per Server* the empty server will be powered down.

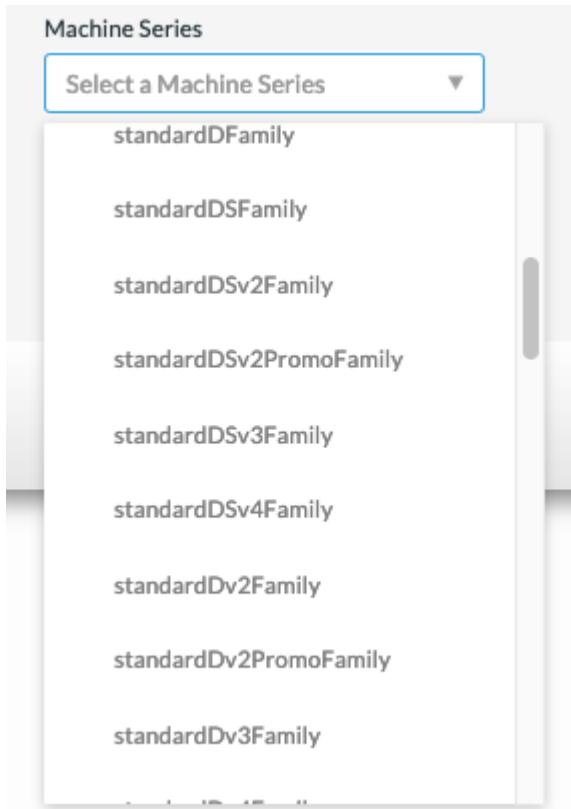
Powering on the next server can take a few minutes. In certain situations the speed of logins can outpace the availability of new servers. For example, if 15 people login in 5 minutes they'll all land on the first server (or be denied a session) while a 2nd and 3rd power up. There are two strategies that can be used to mitigate overloading a single server in this scenario:

1. Enable *Number of Extra Powered on Servers* so that the additional server(s) will be on and available to accept connections and allow time for the platform to spin up additional servers.
 - a. When activated, the number is added to the calculated need. For example, if set to 1 extra server (and with 6 users connected) two servers would be active because of the users count, plus a 3rd due to the *Extra Powered on Servers* setting.
2. Enable *Max Shared Users Per Server* to place a hard limit on the number of users allowed per server. New connections that would exceed this limit will be refused, the end user will get an error message and need to try again in a couple minutes once the additional server is available. If set, this number also defines the depth of AVD Shared servers.
 - a. Assuming the delta between *Shared Users Per Server* and *Max Shared Users Per Server* is appropriate, the new servers should become available before the max is reached in all but the most extreme situations (unusually large login storms).

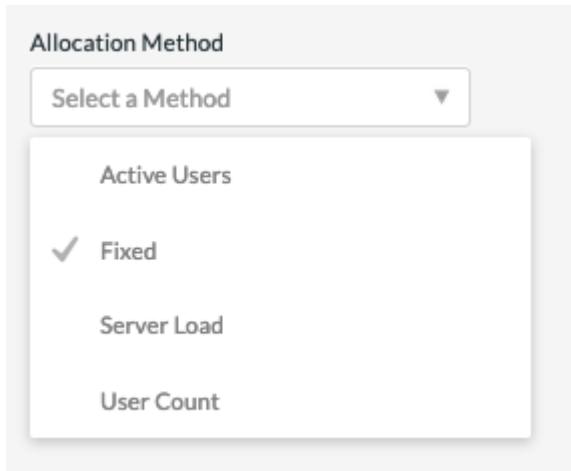
VM resource scaling

VM Resource scaling is an optional feature that can change the size and quantity of session host VMs in an environment.

When activated, VDS will calculate the appropriate size and quantity of session host VMs based on your selected criteria. These options include: Active Users, Named Users, Server Load, and Fixed.



The size of the VMs is contained within the family of VMs selected in the UI which can be changed by dropdown.
(e.g. Standard Dv3 Family in Azure)



Scaling based on users



The function below behaves the same for either "Active Users" or "User Count". User Count is a simply count of all users activated with a VDS desktop. Active Users is a calculated variable based on the previous 2 weeks of user session data.

When calculating based on users, the size (and quantity) of the session host VMs is calculated based on the defined RAM and CPU requirements. The administrator can define the GB of RAM, and number of vCPU cores per user along with additional non-variable resources.

In the screenshot below, each user is allocated 2GB RAM and 1/2 of a vCPU core. Additionally, the server starts with 2 vCPU cores and 8GB RAM.

The screenshot shows two main sections: 'Per User Settings' and 'Additional Resources per Server'.
Per User Settings:

- RAM per User (GB):** A text input field containing '2' with up and down arrow buttons.
- CPU Per User:** A text input field containing '.5' with up and down arrow buttons.

Additional Resources per Server:

- Additional RAM (GB):** A text input field containing '8' with up and down arrow buttons.
- Additional CPUs:** A text input field containing '2' with up and down arrow buttons.

Additionally, the administrator can define the maximum size a VM can reach. When reached, environments will scale horizontally by adding additional VM session hosts.

In the screenshot below, each VM is limited to 32GB Ram and 8vCPU cores.

The screenshot shows the 'Server Capacity' settings section.
Max RAM (GB): A slider with a current value of 1 and a maximum of 240, and a text input field showing 'Current Value: 32' with up and down arrow buttons.
Max CPU: A slider with a current value of 1 and a maximum of 64, and a text input field showing 'Current Value: 8' with up and down arrow buttons.

With all of these variables defined, VDS can calculate the appropriate size and quantity of session host VMs, greatly simplifying the process of maintaining appropriate resource allotment, even as users are added and removed.

Scaling based on server load

When calculating based on server load, the size (and quantity) of session host VMs is calculated based on the average CPU/RAM utilization rates as observed by VDS over the previous 2-week period.

When the maximum threshold is exceeded, VDS will increase the size or increment the quantity to bring average usage back within range.

Like user based scaling, the VM Family and the maximum VM size can be defined.

Manage Resource Pool

Basic Resource Info Name Primary Host Pool Status <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Server Load Settings Peak Hourly Resource Usage RAM CPU 0% 0%	Server Capacity Max RAM (GB) 1 <input type="range"/> 240 Current Value: 32
Use Default Deployment Settings <input type="radio"/> Yes <input checked="" type="radio"/> No	Increase Resource Threshold RAM 70 <input type="button" value="↑"/> CPU 70 <input type="button" value="↑"/>	Decrease Resource Threshold RAM 25 <input type="button" value="↓"/>
Allocation Method Server Load	Machine Series standardDSv2Family	
Total Shared Servers 2		Cancel Apply to Servers

Other active resources

Workload Scheduling does not control the platform servers such as CWMGR1 as they are needed to trigger the Wake on Demand functionality and facilitate other platform tasks and should run 24/7 for normal environmental operation.

Additional saving can be achieved by deactivating the entire environment but is only recommended for non-production environments. This is a manual action that can be performed in the Deployments section of VDS. Returning the environment to a normal status also requires a manual step on the same page.

Deployment URL	VDS	Azure	VM Progress (Provisioning)	Actions
bw54deploy.onmicrosoft.com	skk	5.4	Azure	1 ● Offline Available Delete
cjdevmherr2.onmicrosoft.com	pht	5.4	Azure	1 ● Online Available Stop Gear

							Delete
bw54deploy.onmicrosoft.com	skk	5.4	Azure	1	● Offline	● Available	Start
cjdevmherr2.onmicrosoft.com	pht	5.4	Azure	1	● Online	● Available	Start

User Administration

Managing User Accounts

Create New User(s)

Admins can add Users by clicking Workspaces > Users and Groups > Add/import

Users can be added individually or with a bulk import.



Including accurate email and mobile phone # at this stage greatly improves the process of enabling MFA later.

Once you have created Users, you can click on their name to see details like when they were created, their connection status (whether they're currently logged in or not) and what their specific settings are.

Activating the Virtual Desktop for existing AD users

If users are already present in AD, you can simple activate the users' Virtual Desktop by clicking on the gear next to their name and then enabling their desktop.



For Azure AD Domain Service only: In order for logins to work, the password hash for Azure AD users must be synced to support NTLM and Kerberos authentication. The easiest way to accomplish this task is to change the user password in Office.com or the Azure portal, which will force the password hash sync to occur. The sync cycle for Domain Service servers can take up to 20 minutes so changes to passwords in Azure AD typically take 20 minutes to be reflected in AADDS and thus in the VDS environment.

Delete user account(s)

Edit user info

On the user detail page changes can be made the the user details such as username and contact details. The email and phone values are used for the Self Service Password Reset (SSPR) process.

User Details

Username	TFranklin
Phone	Email
	
Login Identifier	Partner VDS Sales

Edit user security settings

- VDI User Enabled – an RDS Setting that, when enabled, builds a dedicated VM session host and assigned this user as the only user that connect to it. As part of activating this checkbox the CWMS administrator is prompted to select the VM Image, Size and Storage Type.
 - AVD VDI users should be managed on the AVD page as a VDI host pool.
- Account Expiration Enabled – allows the CWMS administrator to set an expiration date on the end user account.
- Force Password Reset at Next Login – Prompts the end user to change their password at next login.
- Multi-Factor Auth Enabled – Enables MFA for the end user and prompts them to setup MFA at next login.
- Mobile Drive Enabled – A legacy feature not used in current deployments of RDS or AVD.
- Local Drive Access Enabled – Allows the end user to access their local device storage from the cloud environment including Copy/Paste, USB Mass storage and system drives.
- Wake on Demand Enabled – For RDS users connecting via the CW Client for Windows, enabling this will give the end user permission to take their environment when connecting outside of normal working hours as defined by Workload Schedule.

Locked Account

By default, five failed login attempts will lock the user account. The user account will unlock after 30 minutes unless *Enable Password Complexity* is enabled. With password complexity enabled, the account will not automatically be unlocked. In either case, the VDS admin can manually unlock the user account from the Users/Groups page in VDS.

Reset user password

Resets the user password.

Note: When resetting Azure AD user passwords (or unlocking an account) there can be a delay of up to 20 minutes as the reset propagates through Azure AD.

Admin Access

Enabling this give the end user limited access to the management portal for their tenant. Common uses include providing an on-site employee access to reset peers' passwords, assign application or allow manual server

wakeup access. Permissions controlling what areas of the console can be seen is set here as well.

Logoff user(s)

Logged on users can be logged off by the VDS admin from the Users/Groups page in VDS.

Applications

Displays the application deployed in this workspace. The check box provisions the apps to this specific user. Complete Application Management documentation can be found here. Access to applications can also be granted from the App interface or to Security Groups.

View/kill user processes

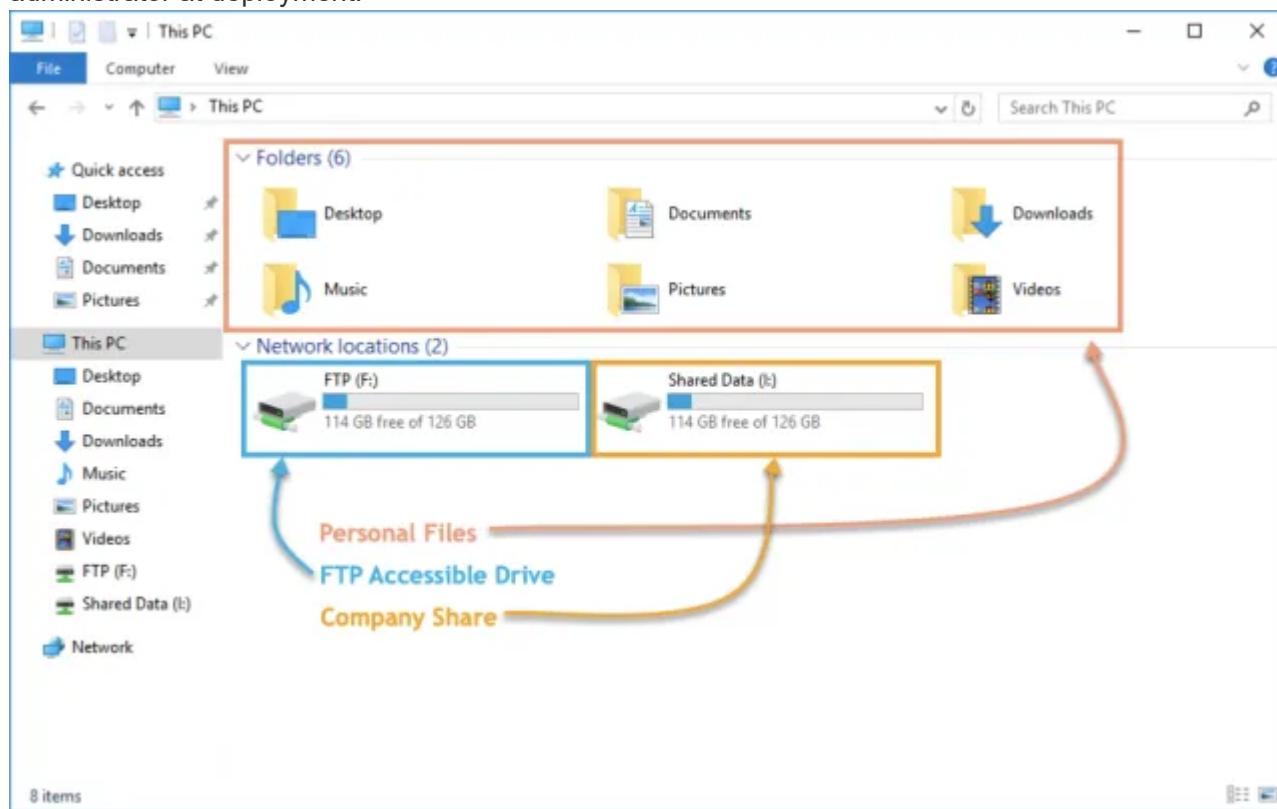
Displays the processes currently running in that user's session. Processes can be ended from this interface as well.

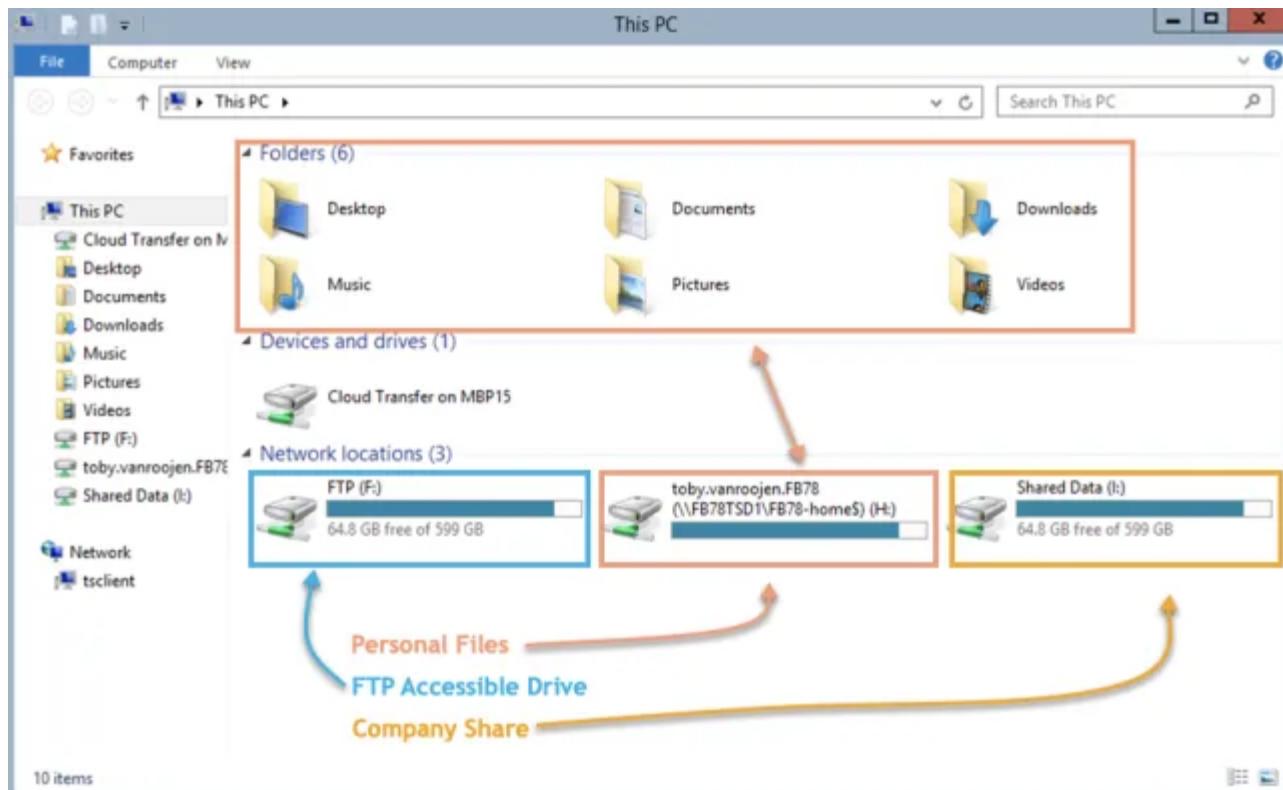
Managing Data Permissions

End user perspective

Virtual Desktop end users can have access to several mapped drives. These drives includes an FTPs accessible team share, a Company File Share and their Home drive (for their documents, desktop, etc...) . All of these mapped drives reference back to a central storage layer on either a storage services (such as Azure NetApp Files) or on a file server VM.

Depending on the configuration the user may or may not have the H: or F: drives exposed, they may only see their Desktop, Documents, etc... folders. Additionally, different Drive letters are occasionally set by the VDS administrator at deployment.





Managing permissions

VDS allows admins to edit security groups and folder permissions, all from within the VDS portal.

Security groups

Security groups are managed by clicking: Workspaces > Tenant Name > Users & Groups > under the Groups Section

In this section you can:

1. Create new security groups
2. Add/Remove users to the groups
3. Assign applications to groups
4. Enable/Disable Local Drive access to groups

Folder permissions

Folder Permissions are managed by clicking: Workspaces > Tenant Name > Manage (in the Folders section).

In this section you can:

1. Add/Delete Folders
2. Assign permissions to user or groups
3. Customize permissions to Read Only, Full Control & None



Application Entitlement

Overview

VDS has a robust application automation and entitlement functionality built-in. This functionality allows users to have access to different applications while connecting to the same session host(s). This is accomplished by some custom GPOs hiding shortcuts along with automation selectively placing shortcuts on the users' desktops.



This workflow only applies to RDS deployments. For AVD application entitlement documentation, please see [Application Entitlement Workflow for AVD](#)

Applications can be assigned to users directly or via Security groups managed in VDS.

At a high level, the application provisioning process follows these steps.

1. Add App(s) to App Catalog
2. Add App(s) to the workspace
3. Install the Application on all Session Hosts
4. Select the Shortcut path
5. Assign apps to users and/or groups



Steps 3 & 4 can be fully automated with Scripted Events as illustrated below



NetApp Virtual Desktop Service

Application Management

Toby vanRoojen
Product Marketing Manager
June, 2020

Video Walkthrough

Add applications to the App Catalog

VDS Application Entitlement starts with the App Catalog, this is a listing of all the applications available for deployment to end user environments.

To add applications to the catalog, follow these steps

1. Log in to VDS at <https://manage.cloudworkspace.com> using your primary admin credentials.
2. In the upper right, click the arrow icon next to your User Name and select Settings.
3. Click the App Catalog tab.
4. Click the Add App option in the Application Catalog title bar.
5. To add a group of applications, choose the Import Apps option.
 - a. A dialog will appear that provides an Excel template to download that creates the correct format for the application list.
 - b. For this evaluation NetApp VDS has created a sample application list for import it can be found [here](#).
 - c. Click on the Upload area and choose the application template file, click the Import button.
6. To add individual applications, choose the Add App button and a dialog box will appear.
 - a. Enter the name of the application.
 - b. External ID can be used to enter an internal tracking identifier such as a product SKU or billing tracking code (optional).
 - c. Check the Subscription box if you want to report on the applications as a Subscription product (optional).
 - d. If the product does not install by version (for example Chrome) check the Version Not Required checkbox. This allows “continuous update” products to be installed without tracking their versions.

- e. Conversely, if a product supports multiple named versions (ex: Quickbooks) you need to check this box so that you can install multiple versions and have VDS specific each available version in the list of applications that can be entitled for and end user.
- f. Check “No User Desktop Icon” if you don’t want VDS to provision a desktop icon for this product. This is used for “backend” products like SQL Server since end users don’t have an application to access.
- g. “App Must be Associated” enforces the need for an associated app to be installed. For example, a client server application may require SQL Server or mySQL to be installed as well.
- h. Checking the License Required box indicates that VDS should request a license file to be uploaded for an installation of this application before it sets the application status to active. This step is performed on the Application detail page of VDS.
- i. Visible to All – application entitlement can be limited to specific subpartners in a multi-channel hierarchy. For evaluation purposes, click the Check Box so that all users can see it in their available application list.

Add the application to the Workspace

To start the deployment process you’ll add the app to the workspace.

To do this, follow these steps

1. Click Workspaces
2. Scroll down to Apps
3. Click Add
4. Check box the application(s), enter required information, click Add Application, click Add Apps.

Manually install the application

Once the application has been added to the Workspace you’ll need to get that application installed on all session hosts. This can be done manually and/or it can be automated.

To manually install applications on session hosts, follow these steps

1. Navigate to Service Board.
2. Click on the Service Board Task.
3. Click on the Server Name(s) to connect as a local admin.
4. Install the app(s), confirm the shortcut to this app is found in the Start Menu path.
 - a. For Server 2016 and Windows 10: C:\ProgramData\Microsoft\Windows\Start Menu\Programs.
5. Go back to the Service Board Task, click Browse and choose either the shortcut or a folder containing shortcuts.
6. Whichever you select is what will be displayed on the end user desktop when assigned the app.
7. Folders are great when an app is actually multiple applications. e.g “Microsoft Office” is easier to deploy as a folder with each app as a shortcut inside the folder.
8. Click Complete Installation.
9. If required, open the created Icon Add Service Board Task and confirm the icon has been added.

Assign applications to users

Application entitlement is handled by VDS and application can be assigned to users in three ways

Assign Applications to Users

1. Navigate to the User Detail page.
2. Navigate to the Applications section.
3. Check the box next to all applications required by this user.

Assign users to an application

1. Navigate to the Applications section on the Workspace Detail page.
2. Click on the name of the application.
3. Check the box next to the users the application.

Assign applications and users to user groups

1. Navigate to the Users and Groups Detail.
2. Add a new group or edit an existing group.
3. Assign user(s) and application(s) to the group.

Reset User Password

Reset user password steps

1. Navigate to the Used Detail page in VDS

The screenshot shows the 'TrainWVD2's Workspace (rs6a)' page in the Microsoft Cloud Adoption Toolkit. The left sidebar has a 'Workspaces' menu item highlighted with a blue arrow. The top navigation bar has a 'Users & Groups' tab highlighted with a blue arrow. The main content area displays a table of users:

Name	Username	Status	Connection Status
Toby vanRoojen	admin@trainwv...	Available	Offline
WVD User1	WVDUser1@tr...	Available	Offline

2. Find the Password Section, enter the new PW twice and click

The screenshot shows the CloudJumper Cloud Workspace interface. On the left, a sidebar lists 'Dashboard', 'Organizations' (selected), 'Deployments', 'Workspaces', 'App Services', 'Service Board' (with a red notification badge), 'Scripted Events', 'Admins', and 'Reports'. The main area shows a user overview for 'WVD User1 (WVDUser1@trainwvd2.onmicrosoft.com)'. The 'User Details' tab is selected, displaying information such as Username (WVDUser1), Connection Status (Offline), Status (Available), Phone (3609996751), Email (toby.vanroojen@cloudjumper.com), Login Identifier (trainwvd2.onmicrosoft.com), Partner (CloudJumper CSP Master), First Name (WVD), Last Name (User1), Created By (toby@cjcsp), and Created On (8/14/2019 3:09 pm). Below this is a 'Security Settings' section with checkboxes for VDI User Enabled, Account Expiration Enabled, Force Password Reset at Next Login, Multi-factor Auth Enabled, Mobile Drive Enabled, Local Drive Access Enabled, Wake On Demand Enabled, and Admin Access Enabled (checked). A large black arrow points down to a 'Password Reset' dialog box. This dialog box contains fields for 'Password' and 'Confirm Password', both filled with '*****', and a 'Reset Password' button. To the right of the dialog box is an 'Admin Access' section with a checked checkbox for 'Admin Access Enabled'. The bottom of the page shows sections for 'Applications' (listing '7zip - Current Version (v. Latest)' and 'Calculator') and 'Processes' (listing 'No Processes Running').

Time to take effect

- For environments running an “Internal” AD on VMs in the environment the password change should take effect immediately.
- For environments running Azure AD Domain Services (AADDS) the password change should take about 20 minutes to take effect.
- The AD type can be determined on the Deployment Details Page:

The screenshot shows the Cloud Workspace interface. On the left, there's a sidebar with icons for Dashboard, Organizations, Deployments (which is highlighted with a red arrow), Workspaces, App Services, Service Board (with a red notification dot), Scripted Events, Admins, and Reports. The main content area has a header 'All Deployments' and 'trainwvd2.onmicrosoft.com (kjd)'. It includes tabs for Overview, Resource Defaults, Backup Defaults, and Provisioning Collections. Below this is a 'Deployment Details' card for 'trainwvd2.onmicrosoft.com (kjd)' with fields like Description, Deployment Code, Version, Hypervisor, Resource Allocation Type, MachineSize, h5 Gateway, RDP Gateway, FTP Server Address, and Directory Type (set to AADDS). To the right is a 'Workloads' section showing 'Workspaces' (1) and 'App Services'. Below these are sections for Profile Server and Platform Servers, which lists a single server named 'CWMGR1' with 2 CPU cores and 4 GB RAM, marked as online. At the bottom is a 'Platform Processes' table with rows for New Client, Update Client, Delete Client, and Server Cache, all listed as Idle.

Self service password reset (SSRP)

The NetApp VDS Windows client and the NetApp VDS web client will provide a prompt for users that enter an incorrect password when logging into a v5.2 (or later) virtual desktop deployment. In the event that the user has locked their account, this process will unlock a user's account as well.

Note: users must have already entered a mobile phone number or an email address for this process to work.

SSPR is supported with:

- NetApp VDS Window Client
- NetApp VDS Web Client

In this set of instructions, you will walk through the process of using SSPR as a simple means to enable users to reset their passwords and unlock their accounts.

NetApp VDS Windows client

1. As an end user, click the Forgot Password link to continue.



Welcome to Cloud Workspace®

Sign into your workspace

Please check your username and password and try again.

Username

recording@wvdrecording.onmicrosoft.com

Password

••••••••

[Forgot Password](#)

Save Username

[Sign In](#)

2. Select whether to receive your code via your mobile phone or via email.



Welcome to Cloud Workspace®

Sign into your workspace

Username

recording@wvdrecording.onmicrosoft.com

Send Code Using:

Email

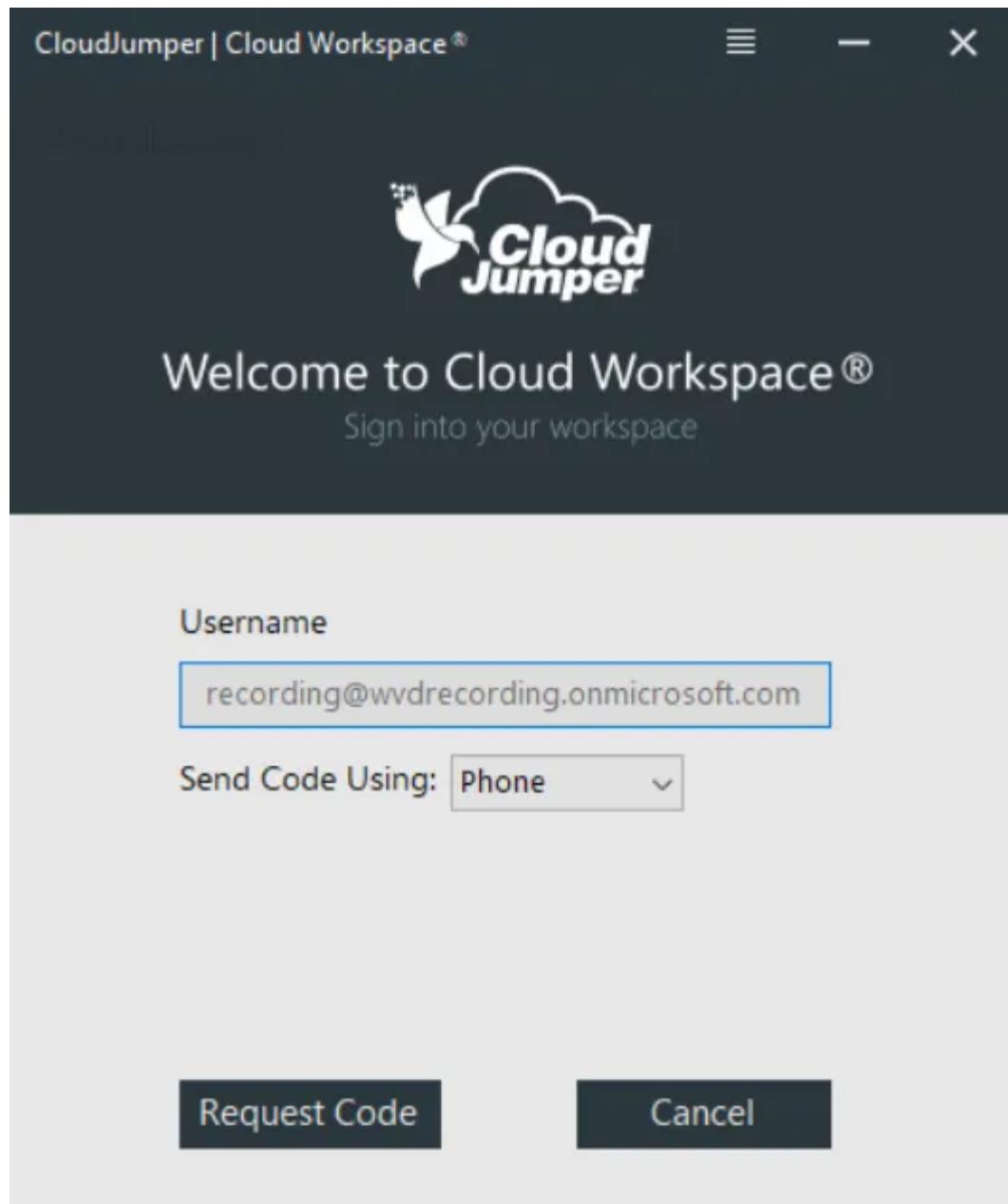
Email

Phone

Request Code

Cancel

3. If an end user has only provided one of those contact methods, that will be the only method displayed.



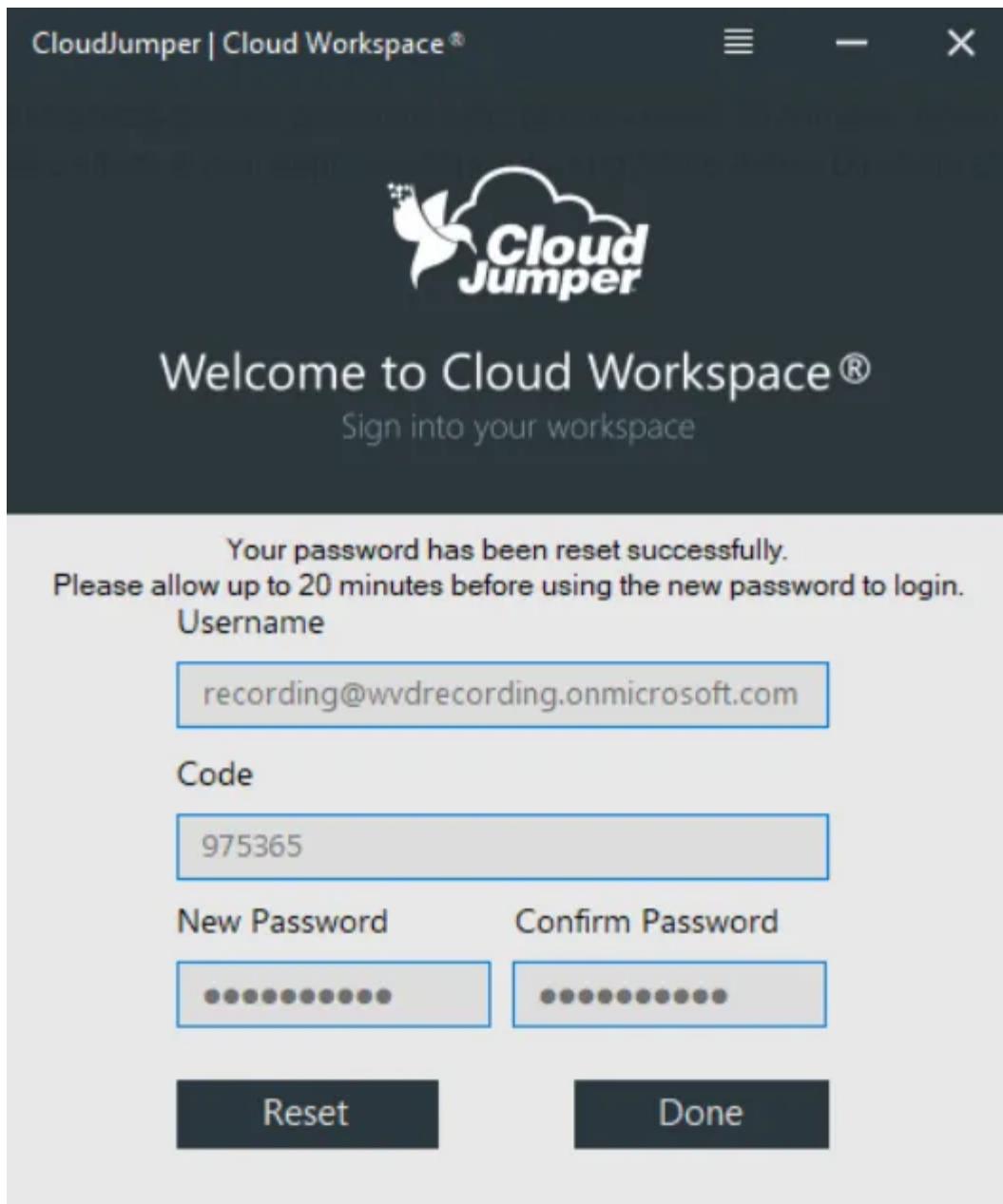
4. After this step, users will be presented with a Code field where they should enter the numeric value received either on their mobile device or in their inbox (depending which was selected). Enter that code followed by the new password and click Reset to proceed.



5. Users will see a prompt informing them that their password reset has been completed successfully – click Done to proceed to complete the logon process.

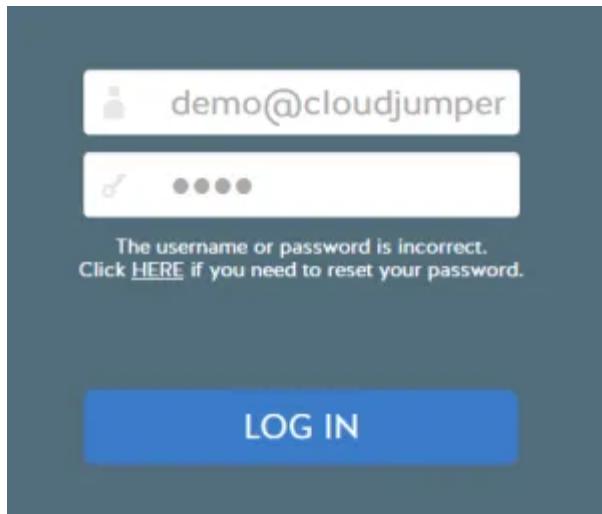


If your deployment is using Azure Active Directory Domain Services, there is a Microsoft-defined password sync period – every 20 minutes. Again, this is controlled by Microsoft and cannot be changed. With this in mind, VDS displays that the user should wait for up to 20 minutes for their new password to take effect. If your deployment is not using Azure Active Directory Domain Services, the user will be able to log in again in seconds.

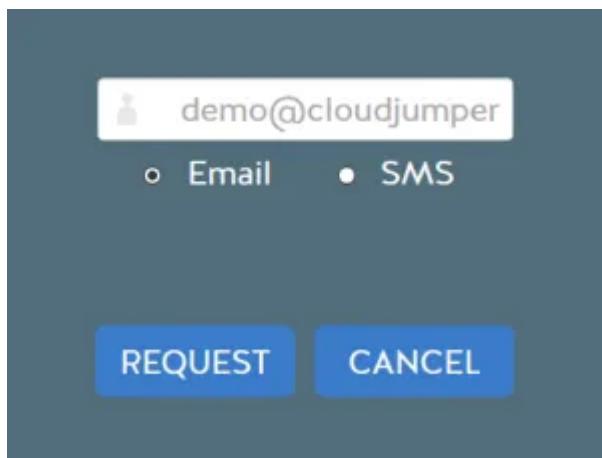


HTML5 portal

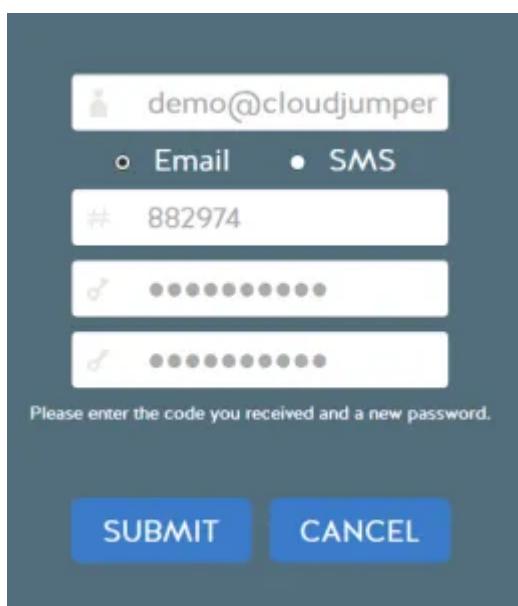
1. If the user fails to enter the correct password when attempting to login through the HTML5, they will now be presented with an option to reset the password:



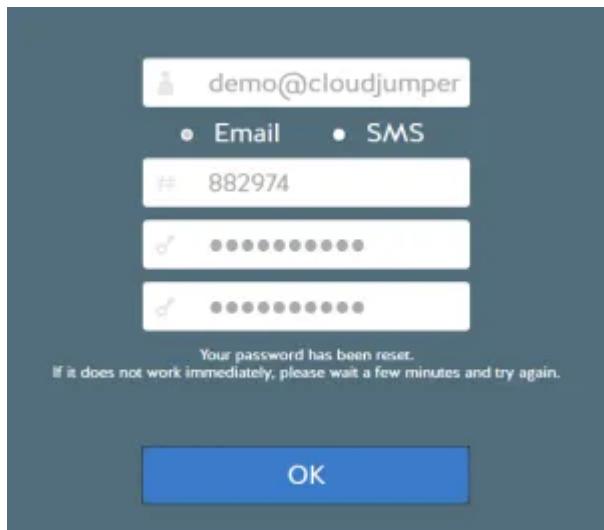
2. After clicking on the option to reset their password, they will be presented with their reset options:



3. The 'Request' button will send a generated code to the option selected (in this case the user's email). The code is valid for 15 minutes.



4. The password has now been reset! It is important to remember that Windows Active Directory will often need a moment to propagate the change so if the new password does not work immediately, just wait a few minutes and try again. This is particularly relevant for users residing in an Azure Active Directory Domain Services deployment, where a password reset could take up to 20 minutes to propagate.



Enabling self service password reset (SSPR) for users

To use Self Service Password Reset (SSPR), administrators must first enter a mobile phone number and/or an email account for an end user. There are two ways to enter a mobile number and email addresses for a virtual desktop user as detailed below.

In this set of instructions, you will walk through the process of configuring SSPR as a simple means for end users to reset their passwords.

Bulk importing users via VDS

Start by navigating to the Workspaces module, then Users & Groups and then clicking Add/Import.

You can enter these values for users when creating them one by one:

 Add User

First Name
 

Last Name

Username

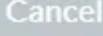
Phone

Email

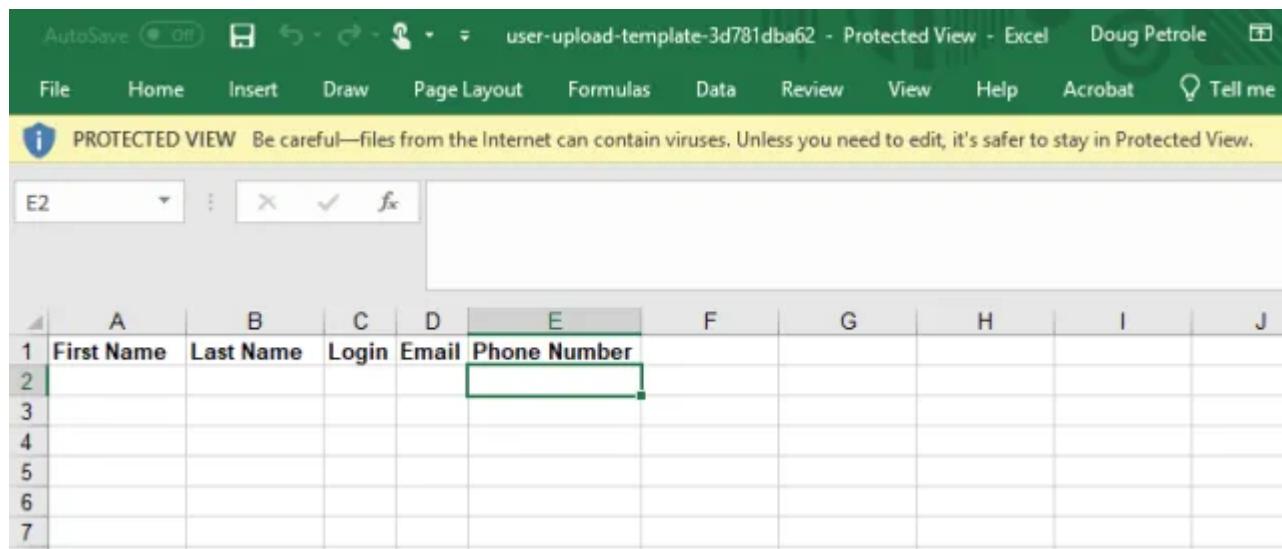
Mobile Drive Enabled

Multi-Factor Auth Enabled

Local Drive Access Enabled

Or you can include these when bulk-importing users downloading and uploading the preconfigured Excel XLSX file in with this content filled out:



A	B	C	D	E	F	G	H	I	J
1	First Name	Last Name	Login	Email	Phone Number				
2									
3									
4									
5									
6									
7									

Supplying the data via the VDS API

NetApp VDS API – specifically this call https://api.cloudworkspace.com/5.4/swagger/ui/index#!/User/User_PutUser – provides the ability to update this information.

Updating existing user phone

Update the users' phone number on the User Detail Overview page in VDS.

The screenshot shows the Cloud Jumper DEV WVD Cloud Workspace interface. On the left, there is a navigation sidebar with the following items:

- Dashboard
- Organizations** (highlighted in blue)
- Data Centers
- Workspaces
- App Services
- Service Board
- Scripted Events
- Admins
- Reports

The main content area shows a user overview for "Doug Petrole (DPetrole@cjdevshivok1.com)". The "Overview" tab is selected. The user details shown are:

Username	Phone	Email
DPetrole		

Using other consoles

Note: you currently cannot provide a phone number for a user via the Azure Console, Partner Center or from the Office 365 Admin console.

Customize SSPR sending address

NetApp VDS can be configured to send the confirmation email *from* a custom address. This is a service provided to our service provider partners who wish for their end users to receive the reset password email to be sent from their own customized email domain.

This customization requires some additional steps to verify the sending address. To start this process, please open a support case with VDS support requesting a custom "Self Service Password Reset Source Address". Please define the following:

- Your partner code (this can be found by clicking on *settings* under the upper-right down arrow menu. See screenshot below)

- Desired "from" address (which must be valid)
- To which clients the setting should apply (or all)

Opening a support case can be done by emailing: VDSsupport@netapp.com

Once received, VDS support will work to validate the address with our SMTP service and activate this setting. Ideally you'll have the ability to update public DNS records on the source address domain to maximize email deliverability.

Password complexity

VDS can be configured to enforce password complexity. The setting for this is on the Workspace Detail Page in the Cloud Workspace Settings section.

Workspaces

Active Users

Date	Active Users
08/16	1.0
08/17	1.0
08/18	1.0
08/19	1.0
08/20	1.0
08/21	2.0
08/22	2.0
08/23	2.0

Resource Consumption

Date	Total CPU	Total RAM (GB)
08/16	2.0	4.0
08/17	2.0	4.0
08/18	2.0	4.0
08/19	2.0	4.0
08/20	4.0	10.0
08/21	4.0	10.0
08/22	4.0	10.0
08/23	4.0	10.0

Deployment

trainwvd2.onmicrosoft.com (kjd)

Azure Available

Company Details

Company Name	TrainWVD2	Company Code	rs6a
Status	Available	Partner	CloudJumper CSP Master
Organization Type	Client	Login Identifier	@trainwvd2.onmicrosoft.com
Created By	Deployment	Address 1	Address 2
		City	Zip Code
		Garner	
		State	Country

Contact Details

The screenshot shows the CloudJumper CSP Master dashboard. At the top, there are basic account details: Available (Client), Organization Type (CloudJumper CSP Master), Login Identifier (@trainwvd2.onmicrosoft.com), City (Garner), Zip Code, Created By (kjd), Deployment (kjd), State, Country, Website (rs6a.kjd.cloudworkspace.app), and Server Address. Below this is the 'Cloud Workspace Settings' section, which includes 'App Settings' (Remote App Access, Enable Application Usage Tracking, Enable App Locker), 'Device Settings' (Disable Printing Access, User Data Storage, User Profile Disk, Enable Task Manager), and 'Security Settings' (Force Password Complexity, Migration Mode Enabled, File Auditing Enabled, MFA for All Users Enabled). The 'Force Password Complexity' checkbox is checked. There are 'Update' buttons for each section. Below the settings are sections for 'Audit Reports' (Report dropdown) and 'Apps' (Add button, search bar, filter by keyword).

Password complexity: Off

Policy	Guideline
Minimum Password Length	8 characters
Maximum Password Age	110 days
Minimum Password Age	0 days
Enforce Password History	24 passwords remembered
Password Lock	Automatically lockout will occur after 5 incorrect entries
Lock Duration	30 minutes

Password complexity: On

Policy	Guideline
Minimum Password Length	8 characters Not contain the user's account name or parts of the user's full name that exceed two consecutive characters Contain characters from three of the following four categories: English uppercase characters (A through Z) English lowercase characters (a through z) Base 10 digits (0 through 9) Non-alphabetic characters (for example, !, \$, #, %) Complexity requirements are enforced when passwords are changed or created.
Maximum Password Age	110 days

Policy	Guideline
Minimum Password Age	0 days
Enforce Password History	24 passwords remembered
Password Lock	Automatically lock will occur after 5 incorrect entries
Lock Duration	Remains locked until administrator unlocks

Multi-Factor Authentication (MFA)

Overview

NetApp Virtual Desktop Service (VDS) includes an SMS/Email based MFA service at no additional charge. This service is independent of any other services (e.g. Azure Conditional Access) and can be used to secure administrator logins to VDS and user logins to virtual desktops.

MFA basics

- VDS MFA can be assigned to admin users, individual end users or applied to all end users
- VDS MFA can send SMS or Email notifications
- VDS MFA has a self-service initial setup and reset function

Guide scope

This guide walks you thru the setup of MFA along with an illustration of the end user experience

This guide covers the following subjects:

1. [Enabling MFA for Individual Users](#)
2. [Requiring MFA for All Users](#)
3. [Enabling MFA for Individual Administrators](#)
4. [End User Initial Setup](#)

Enabling MFA for individual users

MFA can be enabled for individual users on the user detail page by clicking *Multi-factor Auth Enabled*

Workspaces > Workspace Name > Users & Groups > User Name > Multi-factor Auth Enabled > Update

MFA can also be assigned to all users, if this setting is in place, the checkbox will be checked and (*via Client Settings*) will be appended to the checkbox label.

Requiring MFA for all users

MFA can be enabled and enforced across all users on the workspace detail page by clicking *MFA for All Users Enabled*

Workspaces > Workspace Name > MFA for All Users Enabled >Update

Enabling MFA for individual administrators

MFA is also available for administrator accounts accessing the VDS portal. This can be enabled per administrator on the admin detail page.

Admins > Admin Name > Multi-Factor Auth Required > Update

Initial setup

On the first login after enabling MFA, the user or admin will be prompted to enter an email address or mobile phone number. They'll receive a confirmation code to enter and confirm successful enrollment.

System Administration

Create a Domain Admin ("Level 3") Account

Overview

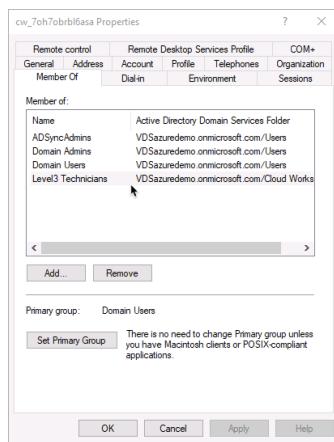
Occasionally VDS administrators will need domain-level credentials to manage the environment. In VDS these are called "Level 3" or ".tech" account.

These instructions show how these accounts can be created with the appropriate permissions.

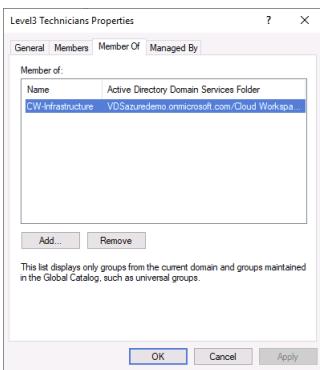
Windows Server Domain Controller

When running an internally hosted Domain Controller (or a local DC linked to Azure via a VPN/Express Route) managing .tech accounts can be done directly in Active Directory Manager.

1. Connect to the Domain Controller (CWMGR1, DC01 or the existing VM) with a domain admin (.tech) account.
2. Create a new user (if needed).
3. Add the user to the "Level3 Technicians" security group



- a. If the "Level3 Technicians" security group is missing, please create the group and make it a member of "CW-Infrastructure" security group.



Adding “.tech” to the end of the username is a recommended best practice to help delineate admin accounts from end user accounts.

Azure AD Domain Services

If running in Azure AD Domain Services or managing user in Azure AD, these accounts can be managed (i.e. password change) in the Azure Management Portal as a normal Azure AD user.

New accounts can be created, adding them to these roles should give them the permissions required:

1. AAD DC Administrators
2. ClientDHPAccess
3. Global Admin in the directory.



Adding “.tech” to the end of the username is a recommended best practice to help delineate admin accounts from end user accounts.

NAME	GROUP TYPE	MEMBERSHIP TYPE
AAD DC Administrators	Security	Assigned
ClientDHPAccess	Security	Assigned

Providing Temporary Access to 3rd Parties

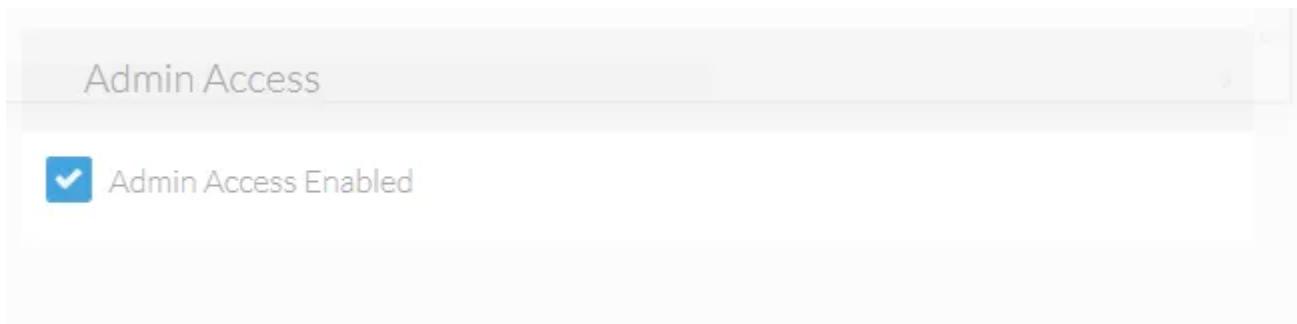
Overview

Providing access to 3rd parties is a common practice when migrating to any cloud solution.

VDS Admins often elect to not give these 3rd parties the same level of access that they have, to follow a “least required” security access policy.

To set up admin access for 3rd parties, log into VDS and navigate to the Organizations module, click into the organization and click Users & Groups.

Next, create a new User account for the 3rd party and scroll down until you see the Admin Access section and check the box to enable admin rights.



The VDS Admin is then presented with the Admin Access setup screen. There is no need to change user's name, login or password – just add phone number and/or email if you want to enforce Multi-Factor Authentication and select the level of access to grant.

For database administrators like a VAR or ISV, Servers is commonly the only access module required.

New Active Directory Admin

Basic Info <p>Username <input type="text" value="UOne@gputesting.onmicrosoft.com"/></p> <p>First Name <input type="text" value="User"/></p> <p>Last Name <input type="text" value="One"/></p> <p>Phone Number <input type="text" value="Enter Phone #"/></p> <p>Email <input type="text" value="Enter Email"/></p>	Security Settings <p><input type="checkbox"/> Multi-Factor Auth Required</p> <p><input type="checkbox"/> Tech Account Enabled</p> <p><input type="checkbox"/> User Support Only</p> <p><input type="checkbox"/> Shadow User Enabled</p>	Module Permissions <p>Module <input checked="" type="checkbox"/></p> <p>Audits <input type="checkbox"/></p> <p>Applications <input type="checkbox"/></p> <p>Groups <input type="checkbox"/></p> <p>Firewall <input type="checkbox"/></p> <p>Folders <input type="checkbox"/></p> <p>Servers <input type="checkbox"/></p> <p>Users <input type="checkbox"/></p>
<input type="button" value="Cancel"/> <input type="button" value="Add Admin"/>		

Once saved, the End User gains access to self-management functions by logging into VDS with their standard Virtual Desktop user credentials.

When the newly created User logs in, they will only see the modules you have assigned to them. They can select the organization, scroll down to the Servers section and connect to the server name you tell them to (say, <XYZ>D1, where XYZ is your company code and D1 designates that the server is a Data server. In the example below, we would tell them to connect to the TSD1 server to perform their assignments.

Servers							Add	Refresh
Name	Type	Machine Size	RAM	CPU	Online Status	Status		
[REDACTED]	Power User	Standard_B2s	4 GB	2	● Online	● Available		
[REDACTED]	Power User	Standard_B2s	4 GB	2	● Online	● Available		
[REDACTED]	Power User	Standard_B2s	4 GB	2	● Online	● Available		
[REDACTED]	Shared	Standard_B2s	4 GB	2	● Online	● Available		

Configure Backup Schedule

Overview

VDS has the ability to configure and manage native backup services in some infrastructure providers including Azure.

Azure

In Azure, VDS can automatically configure backups using native [Azure Cloud Backup](#) with locally redundant

storage (LRS). Geo-redundant storage (GRS) can be configured in the Azure Management Portal if needed.

- Individual backup policies can be defined for each Server Type (with default recommendations). Additionally, individual machines can be assigned a schedule independent (from their server type) from within the VDS UI, this setting can be applied by navigating to the Server Detail View by clicking on the Server name on the Workspace page (See Video Below: Setting Individual Backup Policies)
 - Data
 - Backup with 7 daily, 5 weekly & 2 monthly backups. Increase retention periods based on business requirements.
 - This is true for both a dedicated Data server and for add-on VPS VMs for Apps and Databases.
 - Infrastructure
 - CWMGR1 – Backup Daily and keep 7 daily, 5 weekly, 2 monthly.
 - RDS Gateway – Backup weekly and keep 4 weekly.
 - HTML5 Gateway – Backup weekly and keep 4 weekly.
 - PowerUser (aka VDI User)
 - Don't backup the VM as data should be stored on a D1 or TSD1 server.
 - Be aware that some applications do store data locally and special considerations should be taken if this is the case.
 - In the event of a VM failure, a new VM can be built via Cloning another. In the event there is only one VDI VM (or one unique VM build) it is advisable to back it up so that a complete rebuild of that VM is not required.
 - If needed, rather than backing up all VDI servers, costs can be minimized by manually configuring a single VM to backup directly in the Azure Management portal.
 - TS
 - Don't backup the VM as data should be stored on a D1 or TSD1 server.
 - Be aware that some applications do store data locally and special considerations should be taken if this is the case.
 - In the event of a VM failure, a new VM can be built via Cloning another. In the event there is only one TS VM it is advisable to back it up so that a complete rebuild of that VM is not required.
 - If needed, rather than backing up all TS servers, costs can be minimized by manually configuring a single VM to backup directly in the Azure Management portal.
 - TSData
 - Backup with 7 daily, 5 weekly & 2 monthly backups. Increase retention periods based on business requirements.
- Policies can be set to take backups daily or weekly, Azure does not support more frequent schedules.
- For daily schedules, enter the preferred time to take the backup. For weekly schedules, enter the preferred day and time to take the backup. Note: Setting the time to exactly 12:00 am can cause issues in Azure Backup so 12:01 am is recommended.
- Define how many daily, weekly, monthly and yearly backups should be retained.

Setting deployment defaults

In order to setup Azure backup for the entire deployment, follow these steps:

1. Navigate to the Deployments detail page, select Backup Defaults
2. Select a server type from the drop-down menu. The server types are:

Data: these are for LOB/database server types

Infrastructure: these are platform servers

Power User: these are for Users with a TS server dedicated solely to them

TS: these are terminal servers that Users launch sessions on

TSData: these are servers doubling as terminal and data servers.

- This will define the overarching backup settings for the entire Deployment. These can be overridden and set at a server-specific level later if desired.

3. Click the settings wheel, then the Edit popup that appears.
4. Select the following backup settings:

On or off

Daily or weekly

What time of day backups take place

How long each backup type (daily, weekly, etc.) should be retained

5. Finally, click Create (or Edit) Schedule to put these settings in place.

Setting individual backup policies

To apply server-specific integrated backup settings, navigate to a Workspace detail page.

1. Scroll down to the Servers section and click on a server's name
2. Click Add Schedule
3. Apply backup settings as desired and click Create Schedule

Restoring from backup

To restore backups of a given VM, begin by navigating to that Workspace detail page.

1. Scroll down to the Servers section and click on a server's name
2. Scroll down to the Backups section and click the wheel to expand your options, then select either
3. Restore to Server or Restore to Disk (attach a drive from the backup so that you can copy data from the backup to the existing version of the VM).
4. Proceed with your restore from this point on as you would in any other restore scenario.

 Costs depend on what schedule you want to maintain and is entirely driven by the Azure backup cost. Backup pricing for VMs is found on the Azure Cost Calculator: <https://azure.microsoft.com/en-us/pricing/calculator/>

Cloning Virtual Machines

Overview

Virtual Desktop Service (VDS) provides the ability to clone an existing virtual machine (VM). This functionality designed to automatically increase server unit count availability as defined user count grows OR additional servers to available resource pools.

Admins use cloning in VDS in two ways:

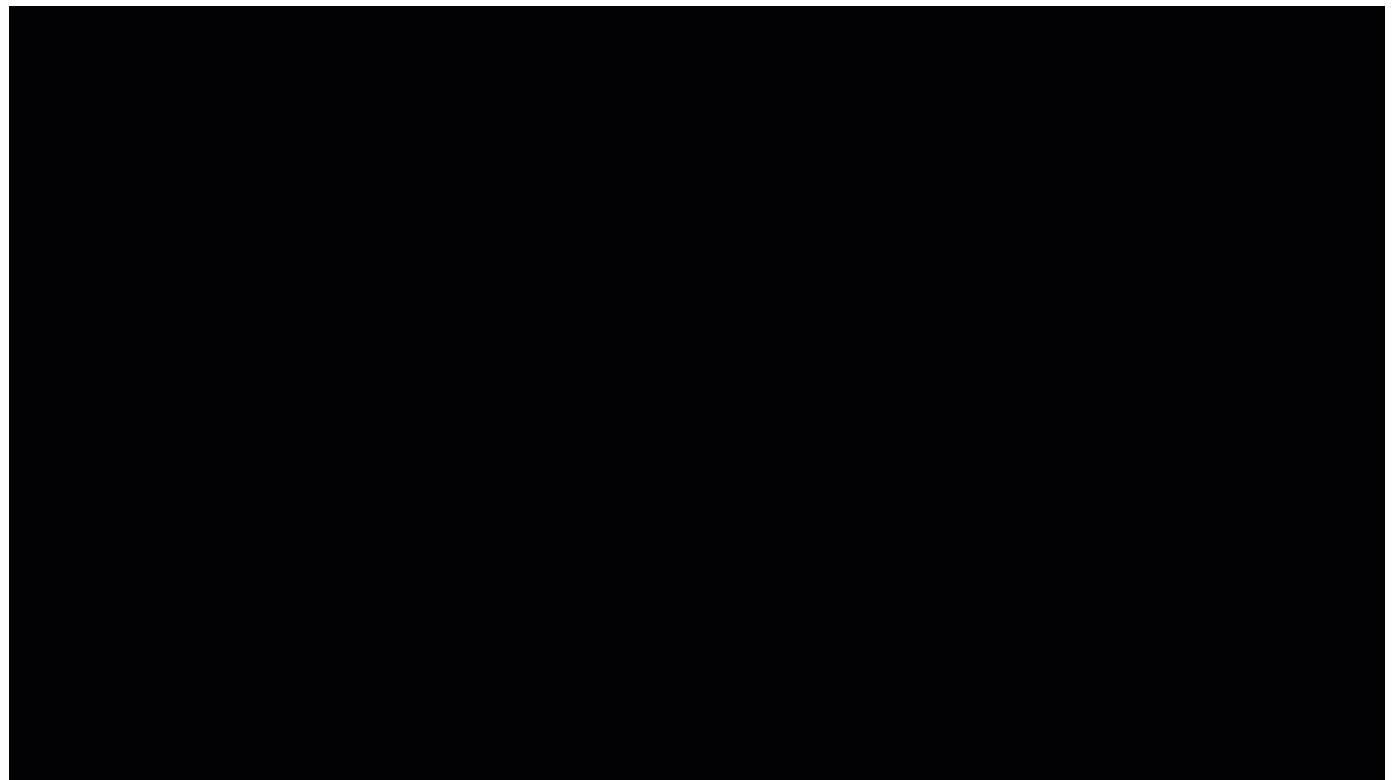
1. On demand automated creation of new server from an existing client server
2. Proactive automated creation of new client server(s) for auto-scaling of resources based-on rules defined and controlled by partners

Cloning to add additional shared servers

A clone is a copy of an existing virtual machine. Cloning functionality saves time and helps admins scale because installing a guest operating system and applications can be time consuming. With clones, you can make many copies of a virtual machine from a single installation and configuration process. This typically looks like:

1. Install all desired applications and settings onto a TS or TSD server
2. Navigate to: Workspaces > Servers Section > Gear Icon for the Source Server > Click Clone
3. Allow the clone process to run (typically 45-90 minutes)
4. The final step activate the cloned server, putting it into the RDS pool to accept new connections. Cloned servers may require individual configuration after being cloned so VDS waits for the Administrator to manually put the server into rotation.

Repeat as many times as necessary.



To increase the capacity for users in a shared session host environment, cloning a session host is an easy process requiring only a few steps.

1. Select a session host to clone, verify no users are currently logged in to the machine.
2. In VDS, navigate to the Workspace of the target client. Scroll to the Servers section, click the Gear Icon and select Clone. This process takes significant time and will take the source machine offline. Expect 30+ minutes to complete.

Name	Type	Machine Size	RAM	CPU	Online Status	Status
DVYTS1	Power User	Standard_B2s	4 GB	2	● Online	● Available
DVYTS2	Shared	Standard_B2s	4 GB	2	● Online	● Connect
DVYTS1	Shared	Standard_B2s	4 GB	2	● Online	● Convert To Data

Firewall Rules
No Rules Added.

Add Refresh

Filter by Keyword

Clone

Stop

Delete

Servers

Add Refresh

Filter by Keyword

Name	Type	Machine Size	RAM	CPU	Online Status	Status
DVYTS1	Power User	Standard_B2s	4 GB	2	● Online	● Available
DVYTS2	Shared	Standard_B2s	0 GB	0	● Offline	○ In Progress (Cloning)
DVYTSD1	Shared	Standard_B2s	4 GB	2	● Online	● Available

Firewall Rules

Add

No Rules Added.

- The process will shut down the server, clone the server to another image and SysPrep the image to the next TS# for the customer. The server shows as *Type=staged* and *Status=Activation Required* in the Servers list.

Servers

Add Refresh

Filter by Keyword

Name	Type	Machine Size	RAM	CPU	Online Status	Status
DVYTS1	Power User	Standard_B2s	4 GB	2	● Online	● Available
DVYTS2	Shared	Standard_B2s	4 GB	2	● Online	● Available
DVYTS3	Staged	Standard_DS2_v2	7 GB	2	● Online	Activation Required
DVYTSD1	Shared	Standard_B2s	4 GB	2	● Online	● Available

Firewall Rules

Add

No Rules Added.

- Logon to the server and verify that the server is ready for production.

Servers

Add Refresh

Filter by Keyword

Name	Type	Machine Size	RAM	CPU	Online Status	Status
DVYTS1	Power User	Standard_B2s	4 GB	2	● Online	● Available
DVYTS2	Shared	Standard_B2s	4 GB	2	● Online	● Available
DVYTS3	Staged	Standard_DS2_v2	7 GB	2	● Online	Activation Required
DVYTSD1	Shared	Standard_B2s	4 GB	2	● Online	● Available

Firewall Rules

Add

No Rules Added.

Connect

Activate

Clone

Stop

Delete

- When ready, click Activate to add the server into the session-host pool to start accepting user connections.

Servers							Add	Refresh
							<input type="text"/> Filter by Keyword	
Name	Type	Machine Size	RAM	CPU	Online Status	Status		
DVYTS1	Power User	Standard_B2s	4 GB	2	● Online	● Available	Connect	
DVYTS2	Shared	Standard_B2s	4 GB	2	● Online	● Available	Activate	
DVYTS3	Staged	Standard_DS2_v2	7 GB	2	● Online	Activation Required	Clone	
DVYTSD1	Shared	Standard_B2s	4 GB	2	● Online	● Available	Stop	

Firewall Rules

No Rules Added.

Connect Activate Clone Add Stop Delete

VDS cloning process definition

The step-by-step process is detailed in VDS > Deployment > Task History under any Clone Server operations. The process has 20+ steps, which start with accessing the hypervisor to start the clone process & ends with activating the cloned server. The cloning process includes key steps such as:

- Configure DNS & set server name
- Assign StaticIP
- Add to Domain
- Update Active Directory
- Update VDS DB (SQL instance on CWMGR1)
- Create Firewall rules for the clone

As well as Task History, the detail steps for any cloning process can be viewed in CwVmAutomationService log on CWMGR1 in each partner's Virtual Desktop Deployment. Reviewing these log files is documented [here](#).

Automated creation of new server(s)

This VDS functionality designed to automatically increase server unit count availability as defined user count grows.

The partner defines and manages via VDS (<https://manage.cloudworkspace.com>) > Client > Overview – VM Resources > Auto-Scaling. Several controls are exposed to allow partners to Enable/Disable Auto Scaling as well as create custom rules for each client such as: number/users/server, additional RAM per user & number of users per CPU.



Above assumes automated cloning is enabled for the entire Virtual Desktop Deployment. For example, to stop all automated cloning, use DCConfig, in the Advanced window, uncheck the Server Creation→Automated Cloning Enabled.

When does the automated clone process run?

The automated clone process runs when the daily maintenance is configured to run. The default is midnight, but this can be edited. Part of the daily maintenance is to run the Change Resources thread for each resource pool. The Change Resources thread determines the number of shared servers required based-on the number of users the pool's configuration (customizable; can be 10, 21, 30, etc users per server).

“On demand” automated creation of new server

This VDS functionality allows automated “on demand” cloning of additional servers to available resource pools.

The VDS Admin logs into VDS and under the Organizations or Workspaces Modules, finds the specific Client & opens the Overview tab. The Servers Tile lists all servers (TSD1, TS1, D1, etc). To clone any individual server, simply click on the cog to far-right of server name & select Clone option.

Typically, the process should take about an hour. However, the duration depends on the size of VM and the available resources of the underlying hypervisor. Please note the server being cloned will need to be rebooted, so partners typically perform after hours or during a scheduled maintenance window.

When cloning a TSDData server, one of the steps is deleting the c:\Home, c:\Data, and c:\Pro folders so they’re aren’t any duplicate files. In this case, the clone process failed there were problems deleting these files. This error is vague. Typically, this means the clone event failed because there was an open file or process. Next attempt, please disable any AV (because that might explain this error).

Auto-increase Disk Space Feature

Overview

NetApp recognizes the need to give Administrators an easy way to make sure that users always have space to access and save documents. This also ensures that VMs have enough free space to complete backups successfully, enabling and empowering Administrators and their Disaster Recovery and Business Continuity plans. With this in mind, we built a feature that automatically expands the managed disk in use to the next tier when a drive is running short on space.

This is a setting that is applied by default on all new VDS deployments in Azure, ensuring that all deployments protect users and the tenant’s backups by default.

Administrators can validate this is in place by navigating to the Deployments tab, then selecting a deployment and then connecting to their CWMGR1 server from there. Next, open the DCConfig shortcut on the desktop and click Advanced and scroll down to the bottom.

PropertyName	FriendlyName	Value
PEN	Logo	cloudworkspace-logo-med.png
PEN	NumNotifyDays	6
PEN	NotificationDay1	12
PEN	NotificationDay2	5
PEN	NotificationDay3	4
PEN	NotificationDay4	3
PEN	NotificationDay5	2
PEN	NotificationDay6	1
Monitoring	Enabled	<input checked="" type="checkbox"/>
Monitoring	Alert Server Down for Minutes	2
Monitoring	Alert Ram High for Minutes	60
Monitoring	Ram High %	95
Monitoring	Alert Cpu High for Minutes	60
Monitoring	CPU High %	95
Monitoring	Upload Data Every X Minutes	15
Delete Xml Delay	Minutes	90
Automatically Expand Drive	Enabled	<input checked="" type="checkbox"/>
Pci v3 Compliant	Enabled	<input type="checkbox"/>
Run CwAgent as Domain Admin	Enabled	<input checked="" type="checkbox"/>
Install WildCard Cert	On Infrastructure Servers	<input checked="" type="checkbox"/>

Administrators can change the amount of free space desired in either GB free or percent of the drive that

should be free before moving to the next tier of managed disks in the same Advanced section of DCCConfig.

FreeSpaceReport	MinFreeSpaceGB	10
FreeSpaceReport	MinFreeSpacePercent	10
MaxRebootTimeInHours	ClientServers	360

A few practical application examples:

- If you want to ensure that at least 50 GB is available on your drive, set MinFreeSpaceGB to 50
- If you want to ensure that at least 15% of your drive is free, set MinFreeSpacePercent from 10 to 15.

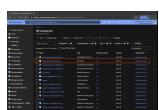
This action takes place at midnight on the server's time zone.

Accessing VDS credentials in Azure Key Vault

Overview

CWASetup 5.4 is a departure from previous Azure deployment methods. The configuration and validation process is streamlined to reduce the amount of information required to begin a deployment. Many of those removed prompts are for credentials or accounts such as Local VM Admin, SMTP account, Tech account, SQL SA, etc. These accounts are now automatically generated and stored in an Azure Key Vault. By default, accessing these automatically generated accounts requires an additional step, described below.

- Find the 'Key vault' resource and click into it:



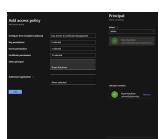
- Under 'Settings', click 'Secrets'. You'll see a message stating that you are unauthorized to view:



- Add an 'Access Policy' to grant an Azure AD account (like a Global Admin or System Administrator) access to these sensitive keys:



- A Global Admin is used in this example. After selecting the principal, click 'Select', then 'Add':



- Click 'Save':



- Access policy has been successfully added:



- Revisit the 'Secrets' to verify the account now has access to the deployment accounts:



- For example, if you required the Domain Administrator credential to login to CWMGR1 and update Group Policy, check the strings under cjDomainAdministratorName and cjDomainAdministratorPassword by clicking on each entry:



- Show or Copy the value:



Apply Monitoring and Antivirus

Overview

Virtual Desktop Service (VDS) Administrators are responsible for monitoring both their platform infrastructure (which will consist of CWMGR1 at minimum) and all other infrastructure and virtual machines (VMs). In most cases, Administrators arrange infrastructure (hypervisor/SAN) monitoring directly with their Data Center/IaaS provider. Administrators are responsible for monitoring terminal servers and data servers, typically by deploying their preferred Remote Management and Monitoring (RMM) solution.

Anti-Virus is the responsibility of the administrator (for both platform infrastructure and terminal/data server VMs). To streamline this process, VDS for Azure servers have Windows Defender applied by default.



When installing 3rd party solutions, be sure not to include Firewalls or any other components which might interfere with VDS automation.

More specifically, when very specific Anti-Virus policies are in place by default this can result in adverse effects when these Anti-Virus agents are installed on a server managed by Virtual Desktop Service.

Our overall guidance is that while VDS platform automation is generally not impacted by Anti-Virus or Anti-Malware products, it is a best practice to add exceptions/exclusions for the following processes on all platform servers (CWMGR1, RDGateways, HTML5Gateways, FTP, etc):

```
*\paexec.exe  
*\paexec_1_25.exe  
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe  
C:\Program Files\CloudWorkspace\CW Automation  
Service\cw.automation.service.exe  
C:\Program  
Files\CloudWorkspace\CwVmAutomationService\CwVmAutomationService.exe  
C:\Program Files (x86)\Myrtle\bin\Myrtle.Printer.exe  
C:\Program Files (x86)\Myrtle\bin\Myrtle.Services.exe
```

Additionally, we recommend safe-listing the following processes on client servers:

```
C:\Program Files\CloudWorkspace\CwAgent\paexec.exe  
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe  
C:\Program Files\CloudWorkspace\CwRemoteApps\cwra.exe  
C:\Program Files\CloudWorkspace\Pen\Pen.exe  
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgent.exe  
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgentMonitor.exe
```

Adding and Moving Mapped Drives

Overview

By default there are three shared folders exposed to end user sessions. These folders are found on the defined storage layer. This could be on the file server (TSD1 or D1) or a storage service such as Azure Files, Azure NetApp Files, NetApp CVO and NetApp CVS.

To assist with clarity, this article will use an example customer with the company code “NECA.” This example assumes a single TDS1 server has been deployed, named NECATSD1. We’ll work through the process of moving a folder to another VM (Named “NECAD1”). This strategy can be used to move between partition on the same machine or to another machine as shown in the following example...

Folders Starting Location:

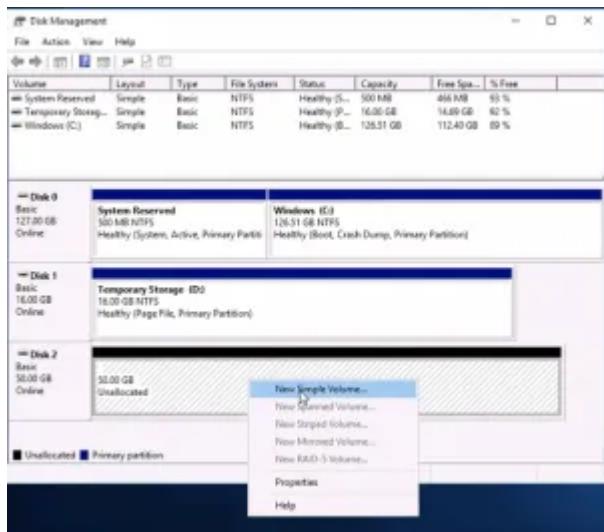
- Data: NECATSD1\C:\data\NECA\ (TSD1 means it is the first Terminal Server and also functions as the Data Server)
- FTP: NECATSD1\C:\ftp\NECA\
- Home: NECATSD1\C:\home\NECA\

Folders Ending Location:

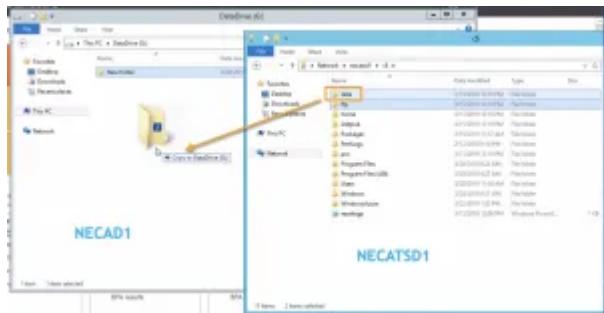
- Data: NECAD1\G:\data\NECA\ (the D1 means it is the 1st Data Server)
- FTP: The same process applies, no need to describe it 3x
- Home: The same process applies, no need to describe it 3x

Add disk for G: on NECAD1

1. In order to put the shared folder on the E: drive we'll need to add one via the hypervisor (e.g. Azure Management Portal), then initialize and format it

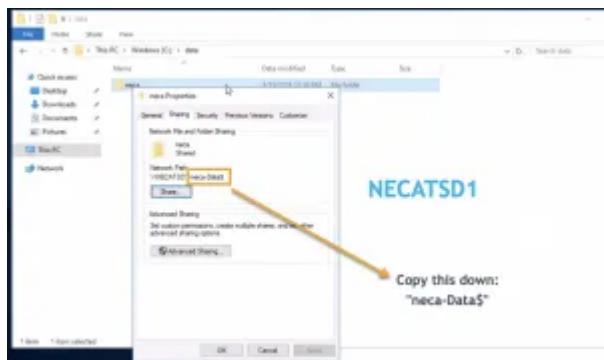


2. Copy the existing folder (on NECATSD1, C:\) path to the new location (on NECAD1, G:\)
3. Copy the folder(s) from the original location to the new location.

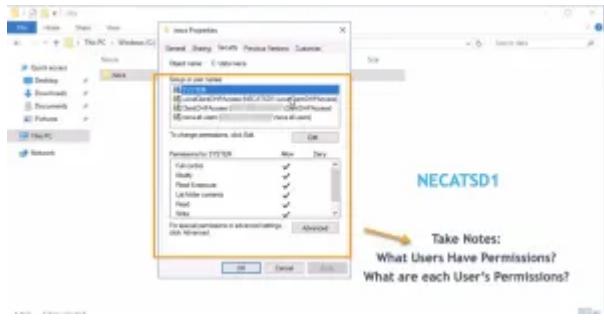


Gather Information From the Original Folder Share (NECATSD1, C:\data\NECA)

1. Share the new folder using the exact same path as the folder in the original location.
2. Open the new NECAD1, G:\data\ folder and you'll see a folder named the company code, "NECA" in our example.



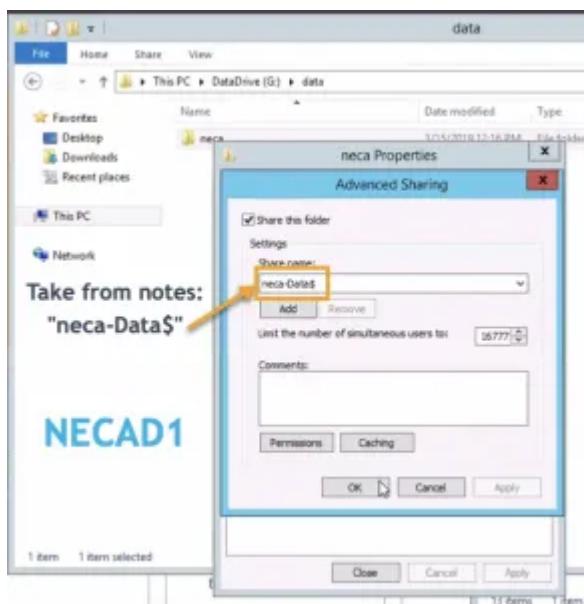
3. Note the security permissions of the original folder share:



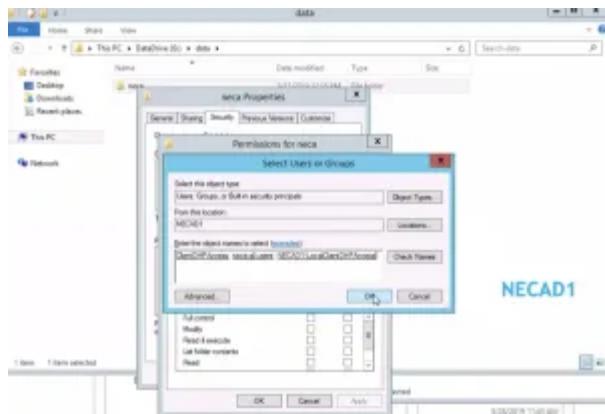
4. Here is the typical setup, however it is important to copy the original settings in case there are existing customizations we need to preserve. All other user/group permissions should be removed from the new folder share
 - SYSTEM:All permissions allowed
 - LocalClientDHPAccess (on the local machine):All permissions allowed
 - ClientDHPAccess (on the domain): All permissions allowed
 - NECA-all users (on the domain): All permissions except “Full Control” allowed

Replicate the Sharing Path and Security Permissions to the New Shared Folder

1. Go back to the new location (NECAD1, G:\data\NECA\ and share the NECA folder with the same network path (excluding the machine), in our example “neca-data\$”

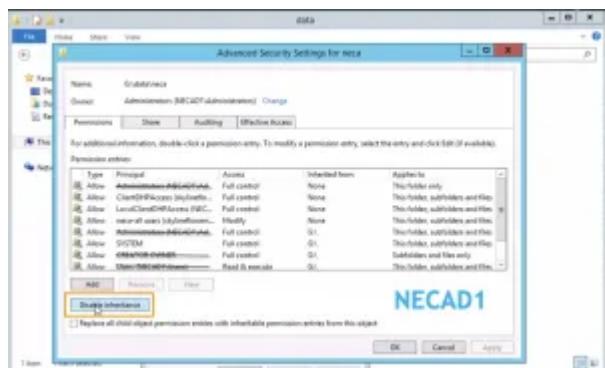


2. For user security add all the users, set their permissions to match.



NECAT1

3. Remove any other user/group permissions that may already exist.

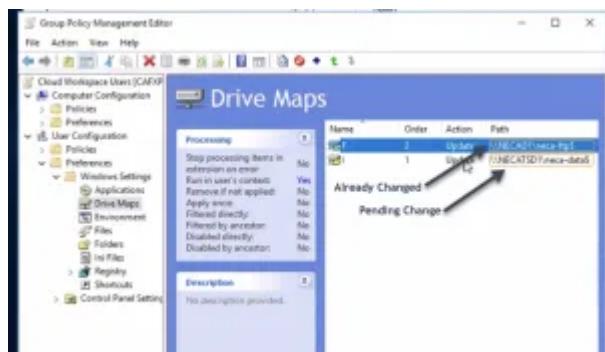


NECAT1

Edit Group Policy (Only if the folder moved to a new Machine)

1. Next you'll edit the Drive Maps in Group Policy Management Editor. For Azure AD Domain Services, the mapping is located in:

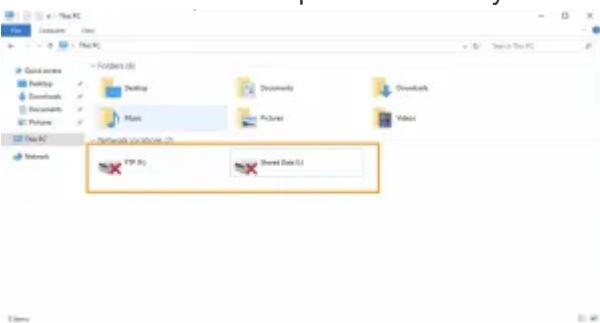
"Cloud Workspace Users > User Configuration > Preferences > Windows Settings> Drive Maps"



2. Once Group Policy updates, the next time each user connects, they'll see the mapped drives which are pointed back to the new location.
3. At this point you can delete the original folders, on NECATSD1, C:\.

Troubleshooting

If the end user sees the mapped drives with a red X, right click the drive and select disconnect. Log out and back in the drive will be present correctly.



Troubleshooting

Troubleshooting Failed VDS Actions

Overview

Much of the logging that happens in VDS is not exposed in the web UI due to the sheer volume of it. More detailed logs are found on the end point. These logs are described below.

In VDS v5.4+, the logs are found in the following folder path:

```
C:\programdata\cloudworkspace
```

In previous version of VDS, they can reside in the following paths:

```
C:\Program Files\CloudWorkspace\  
C:\Program Files\CloudJumper\  
C:\Program Files\IndependenceIT\
```



File type also varies by VDS version, log files are either .txt or .log files found in sub-folders of the above outlined path.

Automation logs

CW VM Automation Service log

```
CwVmAutomationService.log
```

The CW VM Automation service is a Windows Service that is responsible for the management of all Virtual Machines in the deployment. As a Windows Service it is always running in a deployment, but has two main modes of operation: Scheduled Task Mode and Event Mode.

Scheduled Task Mode consists of activities that are performed on the VMs as part of a schedule, including collection sizing and performance data, rebooting VMs, checking on state (on or off) vs rule sets generated by the Workload Schedule and Live Scaling features. The logs denote these action types in the 5th column with names like "Daily Actions", "Weekly Actions" and "Daily Maintenance". If you are troubleshooting questions like "Why did Server X reboot last night at 2:00 am" or "Why is this server on when I think it should be off" then the scheduled tasks for those specific VMs are usually the best place to look.

Event Mode is activated when a user or other VDS Service such as the CW Automation Service asks for a Task to be completed. Examples of this type of activity include a user request to Create a new Server or CW Automation requesting the sizing and state of servers to be checked because more users were added to the workspace. These events typically have log entries with both the event name "Create Server" and the actual name of the VM right next to it (ex: Create Server NNXTS2). When troubleshooting these types of events, its usually best to scroll to the bottom of the log and then to an upwards search for the VM name. You can then scroll up more rows to see where the process started.

CW Automation Service log

CWAutomationService.log

The CW Automation Service log is the primary Windows service for managing the components of a Workspace deployment. It runs the tasks required to manage users, applications, data devices, and policy. In addition, it can create tasks for the CW VM Automation Service when changes need to be made to size, count, or state of the VMs in the deployment.

Like the CW VM Automation Service, the CW Automation service executes both scheduled tasks and event driven tasks, with the latter being the more frequent type. The log for the CW Automation Service starts each line with the entity and action being worked on (ex: Start Server NNXTS1) so searching for the entity name from the bottom of the file is the quickest way to find the specific log lines that apply to the task.

CW Agent Service log

CwAgent.log

The CW Agent Service performs all the tasks that are local to a specific VM, including checking the resource levels and utilization for the VM, checking that the VM has a valid certificate for TLS traffic, and checking to see if the mandatory reboot period has been reached. Besides checking on detail information on these tasks, this log can also be used to check for unexpected VM restarts or unexpected network or resource activity.

CWManagerX log

CWManagerX.log

CWManagerX is a web service that provides the communication link between the local Deployment and the VDS global control plane. Tasks and data requests that originate in the VDS Web Application or VDS API are communicated to the local deployment through this web service. From there, the tasks and requests are directed to the appropriate web service (described above) or in rare cases directly to Active Directory. Since this is mostly a communications link there isn't much logging that occurs during normal communication, but this log will contain errors when the communication link is broken or performing incorrectly.

DC Config log

DCCConfig.log

DC Config is a Windows application that provides Deployment specific configuration parameters that are not exposed in the VDS Web Application interface. The DC Config log details the activities runs when configuration changes are made in DC Config.

CAVDCDeployment log

CAVDCDeployment.log

CW vDC Deployment is a Windows application that performs the tasks necessary to create a Deployment in Azure. The log tracks the configuration of the Cloud Workspace windows services, default GPOs, and routing and resource rules.

Miscellaneous logs

CwVmAutomationService-Installing.log

CwAgent-Installing.log

The remaining logs track the installation of the Windows Services and application described above. Since VDS services auto-update when a new version is targeted at that specific deployment, these logs track the upgrade process since the Service or application typically needs to be off while being upgraded. If you find the Services are consistently Stopped these logs can help identify if a failed upgrade to a specific service is the cause. In these cases, we would expect to see an error in these logs detailing why the upgrade failed.

Accessing logs and reviewing information

When requested actions like cloning a server, adding a user or restoring a backup you'll get feedback in the VDS UI.

+

Servers							Add	Refresh
							Filter by Keyword	
Name	Type	Machine Size	RAM	CPU	Online Status	Status		
DVYTS1	Power User	Standard_B2s	4 GB	2	● Online	● Failed (Restore Failed)		
DVYTSD1	Shared	Standard_B2s	4 GB	2	● Online	● Available		

1. VDS keeps detailed logs and exposes some of them on the Task History section of the Deployments page in VDS. Click on View can show details of the listed tasks.

Task History

Start: 01/29/2019 End: 02/06/2019 Filter by Keyword

Date / Time	Operation	Details	Code
Feb 5, 2019 11:38 AM	Start Server	Server Name: DVYTSD1 Requested By: toby@cjfsp	dvy
Feb 5, 2019 11:35 AM	Generate Server Access Credentials	See Extended Details	dvy
Feb 5, 2019 11:34 AM	Delete Server	Server Name: DVYTS3 Re	
Feb 5, 2019 11:33 AM	Stop Server	Server Name: DVYTS3 Re	
Feb 5, 2019 11:32 AM	Stop Server	Server Name: DVYTSD1 F	
Feb 5, 2019 11:29 AM	Restore Server	Server Name: DVYTS1 Re	
Feb 5, 2019 11:26 AM	Restore Server	Server Name: DVYTS1 R	
Feb 5, 2019 11:20 AM	Update Server Backup Schedule	Modified by: toby@cjfsp	
Feb 5, 2019 11:18 AM	Restore Server	Server Name: DVYTSD1 Requested by: toby@cjfsp	dvy
Feb 5, 2019 11:17 AM	Update Default Backup Schedule	Server Type: TS	lit
Feb 5, 2019 11:16 AM	Restore Server	Server Name: DVYTSD1 Requested by: toby@cjfsp	dvy
Feb 5, 2019 11:16 AM	Generate Server Access Credentials	See Extended Details	dvy
Jan 29, 2019 10:35 PM	Stop Server	Server Name: DVYTSD1 Requested By: toby@cjfsp	dvy
Jan 29, 2019 10:35 PM	Stop Server	Server Name: DVYTS1 Requested By: toby@cjfsp	dvy
Jan 29, 2019 10:35 PM	Stop Server	Server Name: DVYTS3 Requested By: toby@cjfsp	dvy

« < 1 2 3 > »

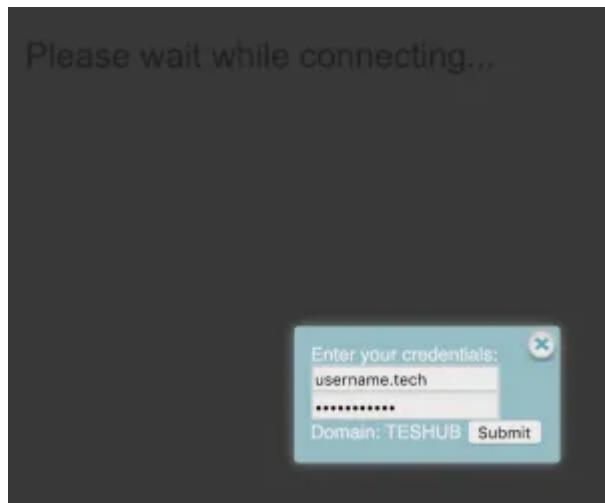
2. Sometimes the Task History does not contain enough details to identify the true root cause. In order to keep the Task History section usable and not overwhelmed by all logged events, only a subset of task information is presented here. For a deeper look the text log files referenced above can provide more details.

a. To access this log, navigate to the Deployments Section and click the Gear Icon next to the CWMGR1 VM, then click Connect (or in the case of the CwAgent log, connect to the appropriate VM)

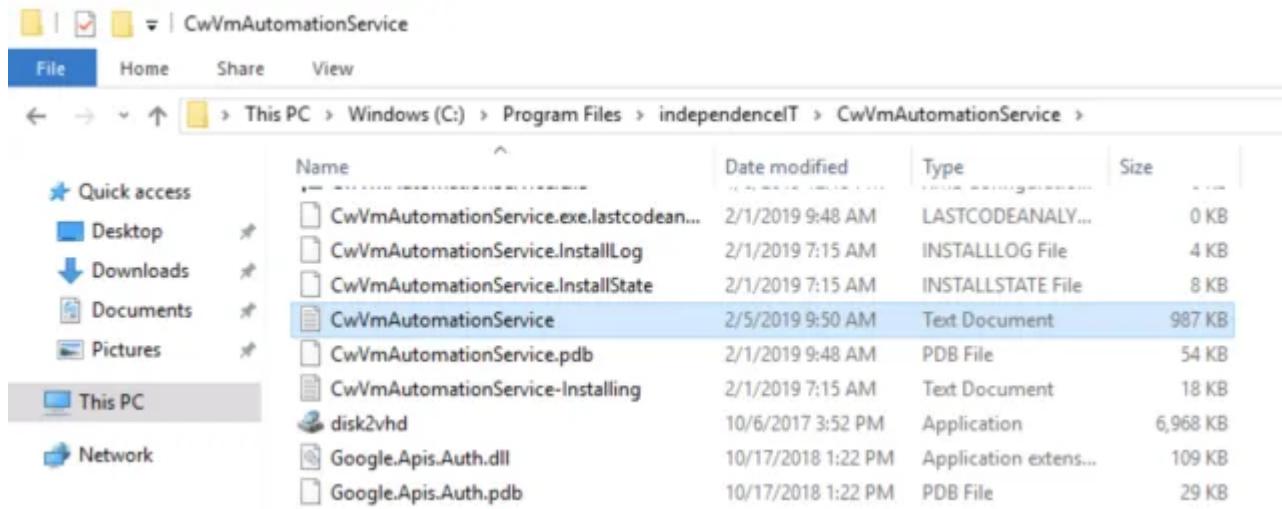
The screenshot shows the Microsoft Cloud Workload Management (CWM) interface. On the left, there's a navigation sidebar with options like Dashboard, Organizations, Data Centers (which is selected), Workspaces, App Services, Service Board (with 15 notifications), Scripted Events, Admins, and Reports. The main area is titled 'teshub.onmicrosoft.com (ada)' under 'All Data Centers'. It has tabs for Overview, Resource Defaults, Backup Defaults, and Provisioning Collections. The 'Overview' tab is active, showing 'Data Center Details' for 'teshub.onmicrosoft.com (ada)'. It includes sections for Description, Data Center Code, Hypervisor, Resource Allocation Type, Domain, and RDP Gateway. Below this is a 'Profile Server' table with one row for 'CWMGR1'. The table columns are Name, CPU, RAM (GB), Status, Backup, and Connect. The 'Status' column shows 'Up' with a green dot, and the 'Connect' button is highlighted in blue.

Name	CPU	RAM (GB)	Status	Backup	Connect
CWMGR1	2	4	Up		Connect

3. When connecting to a Platform Server (Like the CWMGR1) you will not be automatically logged into the server (unlike connecting to a server in the tenant). You'll need to login with a Level3 .tech account.



4. Then navigate to the path as shown above and open the log file.



5. This text file contains a log of all events, listed from oldest to newest:

```

CvVmAutomationService - Notepad
File Edit Format View Help
2019-01-08 18:19:23,883 DEBUG [IITServiceBaseProgram .Run :193 ] Main -Started CvVmAutomationService v5.2.18340.2212
2019-01-08 18:19:23,945 INFO [IITServiceBaseProgram .Run :193 ] Main -Arguments =
2019-01-08 18:19:25,898 DEBUG [Config .LoadConfig :388 ] CreateAndStartThreads -Loaded configuration from DB
2019-01-08 18:19:25,961 DEBUG [VmAutomationService .startAllInfrastructureServers:185 ] CreateAndStartThreads -Starting All Infrastructure Servers
2019-01-08 18:19:27,328 DEBUG [VmAutomationService .startAllInfrastructureServers:196 ] CreateAndStartThreads -Starting CMGR1
2019-01-08 18:19:27,335 DEBUG [VmAutomationService .startAllInfrastructureServers:207 ] CreateAndStartThreads -1 Infrastructure Servers Running
2019-01-08 18:19:27,336 DEBUG [HypervisorAzureRM .PowerOnVM :543 ] Main -VM CMGR1 is already powered on
2019-01-08 18:19:27,601 DEBUG [VmAutomationService .StartServiceHypervisor :362 ] CreateAndStartThreads -WCF Service Available at : http://localhost:871
2019-01-08 18:19:27,633 DEBUG [VmAutomationService .StartServiceVMActions :400 ] CreateAndStartThreads -WCF Service Available at : http://localhost:871
2019-01-08 18:19:27,742 DEBUG [VmAutomationService .ceCreateDeleteChangeServers:422 ] CreateAndStartThreads -WCF Service Available at : http://localhost:871
2019-01-08 18:19:27,859 DEBUG [VmAutomationService .StartServiceEveryServer :381 ] CreateAndStartThreads -WCF Service Available at : http://localhost:871
2019-01-08 18:19:27,915 INFO [ThreadBase .InitRunDone :118 ] Download vOC Tools -Starting Download vOC Tools Thread
2019-01-08 18:19:27,945 INFO [ThreadBase .InitRunDone :118 ] Monthly Actions -Starting Monthly Actions Thread
2019-01-08 18:19:27,961 INFO [ThreadBase .InitRunDone :118 ] Daily Actions -Starting Daily Actions Thread
2019-01-08 18:19:28,023 INFO [ThreadBase .InitRunDone :118 ] Daily Maintenance -Starting Daily Maintenance Thread
2019-01-08 18:19:28,023 DEBUG [ThreadActionMonthly .ComputeRunTime :38 ] Monthly Actions -Will Run in 2d:11h:40m:32s
2019-01-08 18:19:28,055 INFO [ThreadBase .InitRunDone :118 ] Maintenance Weekly -Starting Maintenance Weekly Thread
2019-01-08 18:19:28,055 DEBUG [ThreadActionDaily .ComputeRunTime :73 ] Daily Actions -Will Run in 8d:11h:40m:32s
2019-01-08 18:19:28,078 INFO [ThreadBase .InitRunDone :118 ] Reload Configuration -Starting Reload Configuration Thread
2019-01-08 18:19:28,078 DEBUG [ThreadBase .InitRunDone :118 ] Workload Scheduling -Starting Workload Scheduling Thread
2019-01-08 18:19:28,086 INFO [ThreadBase .InitRunDone :118 ] Monitor Server Up -Starting Monitor Server Up Thread
2019-01-08 18:19:28,195 INFO [ThreadBase .InitRunDone :118 ] Monitoring Ram -Starting Monitoring Ram Thread
2019-01-08 18:19:28,211 INFO [ThreadBase .InitRunDone :118 ] Monitoring Cpu -Starting Monitoring Cpu Thread
2019-01-08 18:19:28,228 DEBUG [ThreadDailyMaintenance .ComputeRunTime :44 ] Daily Maintenance -Will Run in 8d:1h:31m:31s
2019-01-08 18:19:28,242 INFO [ThreadBase .InitRunDone :118 ] Create Backups -Starting Create Backups Thread
2019-01-08 18:19:28,273 DEBUG [ThreadWeeklyMaintenance .ComputeRunTime :37 ] Maintenance Weekly -Will Run in 8d:5h:41m:31s at 1/13/2019 12:01 AM
2019-01-08 18:19:28,273 DEBUG [ThreadBase .RunNow :41 ] CreateAndStartThreads -Wake Up Thread-Daily Actions
2019-01-08 18:19:28,992 DEBUG [ThreadBase .RunNow :41 ] CreateAndStartThreads -Wake Up Thread-Download vOC Tools
2019-01-08 18:19:28,992 INFO [ThreadBase .Run :62 ] Daily Actions -Thread Daily Actions Requested to be Run
2019-01-08 18:19:28,992 INFO [ThreadBase .Run :62 ] Download vOC Tools -Thread Download vOC Tools Requested to be Run
2019-01-08 18:19:29,008 DEBUG [ThreadActionDaily .DoActions :81 ] Daily Actions -Started Daily Actions
2019-01-08 18:19:29,523 DEBUG [ActionSddOperations .SetSddCStatus :136 ] CreateAndStartThreads -Setting Status of ADA Primary to Available
2019-01-08 18:19:29,586 DEBUG [ActionInstallService .DoAction :67 ] Daily Actions -CMGR1-ActionInstallService-CvVmAutomationServ
2019-01-08 18:19:29,804 DEBUG [ActionInstallService .ShouldDoAction :302 ] Daily Actions -CMGR1-CvVmAutomationService v5.2.18340.2212 is
2019-01-08 18:19:29,929 DEBUG [VmAutomationService .CreateAndStartThreads :82 ] CreateAndStartThreads -Ended CreateAndStartThreads
2019-01-08 18:19:30,476 DEBUG [ActionInstallService .WriteDataToDatabase :375 ] Daily Actions -Wrote CvVmAutomationService data to database
2019-01-08 18:19:30,492 DEBUG [ThreadActionDaily .UpdateDataAgentOnAllServers :424 ] Daily Actions -Waiting for 1 Servers to be Updated

```

6. When opening a support case with NetApp VDS, being able to provide the errors found here will SIGNIFICANTLY accelerate the speed to resolution.

Internet Connection Quality Troubleshooting

Symptoms

Dropped users connections requiring a reconnect. Laggy interface response, general performance problems that don't appear to be related to resource (RAM/CPU) loads.

Cause

When users report performance issues, dropped user connections or a laggy interface, the most common cause is not resources at all but rather the network connections between the customer and the datacenter. These connections run through their ISP, various internet backbone carriers and ultimately into the datacenter. Along the way the data traverses multiple stops. Each of these hops can introduce network latency, lost packets and jitter, all of these can contribute to the perceived performance of the desktop computing environment in the virtual desktop.

Tier 1 triage and troubleshooting will include basic steps like confirming resources (RAM, CPU and HDD Space) are sufficient but once that is completed, testing the network connectivity is a great next step in the troubleshooting process.

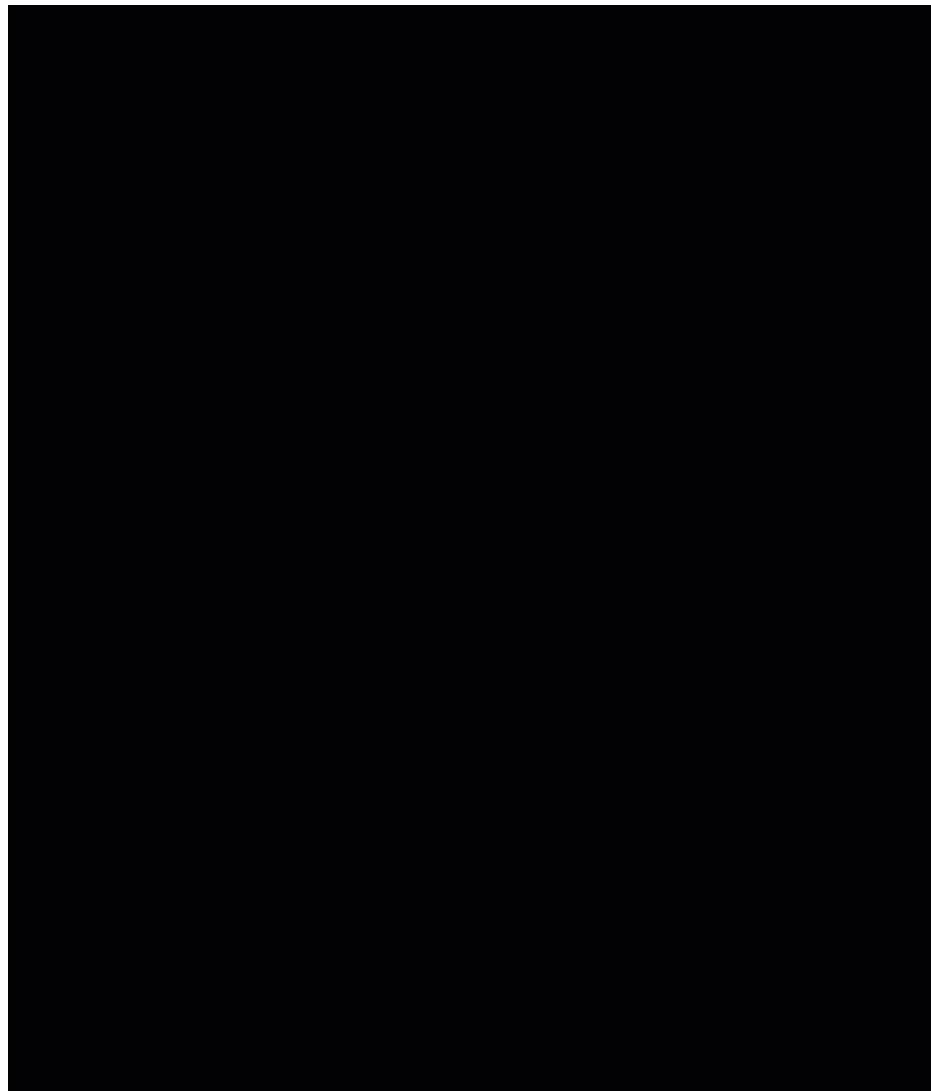
Resolution

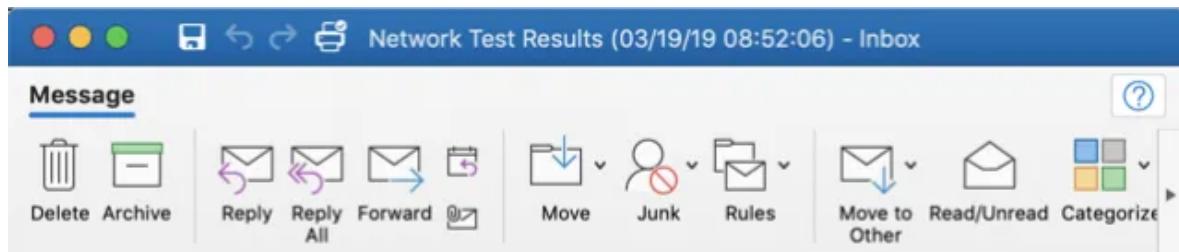
Primary option: NetApp VDS Windows client has built-in diagnostic tools

The diagnostic test can be run and delivered to your email, all from within the virtual desktop Client.

1. Click on the preferences icon (four horizontal lines on the top menu bar)
2. Click Help
3. Click Network Test

4. Enter the user name experiencing the issues, click Run
5. Once complete, enter your email address to receive an email report
6. Review the report to troubleshoot potential connection issues





Network Test Results (03/19/19 08:52:06)



cloudworkspaceclient

Toby vanRoojen

Tuesday, March 19, 2019 at 8:52 AM

[Show Details](#)

Network Test Results:

API address resolved successfully

API is reachable

Username: toby.vanroojen@cloudjumper.com

Gateway: fcf-rds.fcf.cloudworkspace.app

Tenant: rjb5.fcf.cloudworkspace.app

Gateway resolved to: 13.82.216.254

Gateway is reachable

fcf-rds.fcf.cloudworkspace.app	90.02ms
fcf-rds.fcf.cloudworkspace.app	96.65ms
fcf-rds.fcf.cloudworkspace.app	93.32ms
fcf-rds.fcf.cloudworkspace.app	90.35ms
fcf-rds.fcf.cloudworkspace.app	88.85ms
fcf-rds.fcf.cloudworkspace.app	91.81ms
fcf-rds.fcf.cloudworkspace.app	91.39ms
fcf-rds.fcf.cloudworkspace.app	95.21ms
fcf-rds.fcf.cloudworkspace.app	92.3ms
fcf-rds.fcf.cloudworkspace.app	92.2ms
fcf-rds.fcf.cloudworkspace.app	90.68ms
fcf-rds.fcf.cloudworkspace.app	93.51ms
fcf-rds.fcf.cloudworkspace.app	93.08ms
fcf-rds.fcf.cloudworkspace.app	1019.5ms
fcf-rds.fcf.cloudworkspace.app	90.74ms
fcf-rds.fcf.cloudworkspace.app	3109.41ms
fcf-rds.fcf.cloudworkspace.app	92.28ms
fcf-rds.fcf.cloudworkspace.app	90.4ms
fcf-rds.fcf.cloudworkspace.app	88.61ms
fcf-rds.fcf.cloudworkspace.app	90.88ms
fcf-rds.fcf.cloudworkspace.app	93.46ms
fcf-rds.fcf.cloudworkspace.app	92.99ms
fcf-rds.fcf.cloudworkspace.app	95.7ms
fcf-rds.fcf.cloudworkspace.app	90.11ms
fcf-rds.fcf.cloudworkspace.app	92.49ms
fcf-rds.fcf.cloudworkspace.app	94.54ms
fcf-rds.fcf.cloudworkspace.app	89.77ms
fcf-rds.fcf.cloudworkspace.app	94.84ms
fcf-rds.fcf.cloudworkspace.app	91.9ms
fcf-rds.fcf.cloudworkspace.app	91.62ms
fcf-rds.fcf.cloudworkspace.app	94.07ms
fcf-rds.fcf.cloudworkspace.app	92.1ms
fcf-rds.fcf.cloudworkspace.app	91.91ms
fcf-rds.fcf.cloudworkspace.app	99.07ms
fcf-rds.fcf.cloudworkspace.app	93.89ms
fcf-rds.fcf.cloudworkspace.app	89.78ms
fcf-rds.fcf.cloudworkspace.app	92.65ms
fcf-rds.fcf.cloudworkspace.app	92.26ms
fcf-rds.fcf.cloudworkspace.app	94.82ms
fcf-rds.fcf.cloudworkspace.app	92.64ms

Average Latency: 191.04ms

Secondary option: Manual analysis using PingPlotter

To confirm the client's network connection is the culprit you can run the free utility PingPlotter. This utility sends a ping every few seconds and reports on the speed (latency) of the round trip of that ping. It also notes the packet loss (PL) percentage at each hop along the route. When high latency and/or high packet loss is observed it is a good indication that the performance issues are caused by the quality of the internet connection at the hop that is displaying those issues.

1. Download and install [Ping Plotter](#) (Available for MacOS, Windows and iOS).
2. Enter the gateway of the data center in which the tenant is deployed.
3. Let it run for several minutes. Ideally while the performance issues or disconnections are being experienced.
4. Capture the data by choosing “Save Image...” from the File Menu if it is needed for additional troubleshooting.

Enable Desktop Wallpaper for User Sessions

Overview

By default remote sessions have Wallpaper display disabled to improve performance. The result is a black wallpaper that users often wish to customize. This setting can be changed with a simple GPO edit

Instructions:

1. Login to a platform server (e.g. CWMGR1) using level3 .tech account
2. Open Group Policy Management Console
3. Locate the rdsh GPO (labeled as “company code” rdsh (e.g. “xyz1 rdsh”)) Right click “xyz1 rdsh” GPO, choose edit
 - a. In Azure AD Domain Services the GPO is called “AADDC “Computers > Cloud Workspace Computers”
4. Modify the Policy: Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment > Remove remote desktop wallpaper set this to Disabled

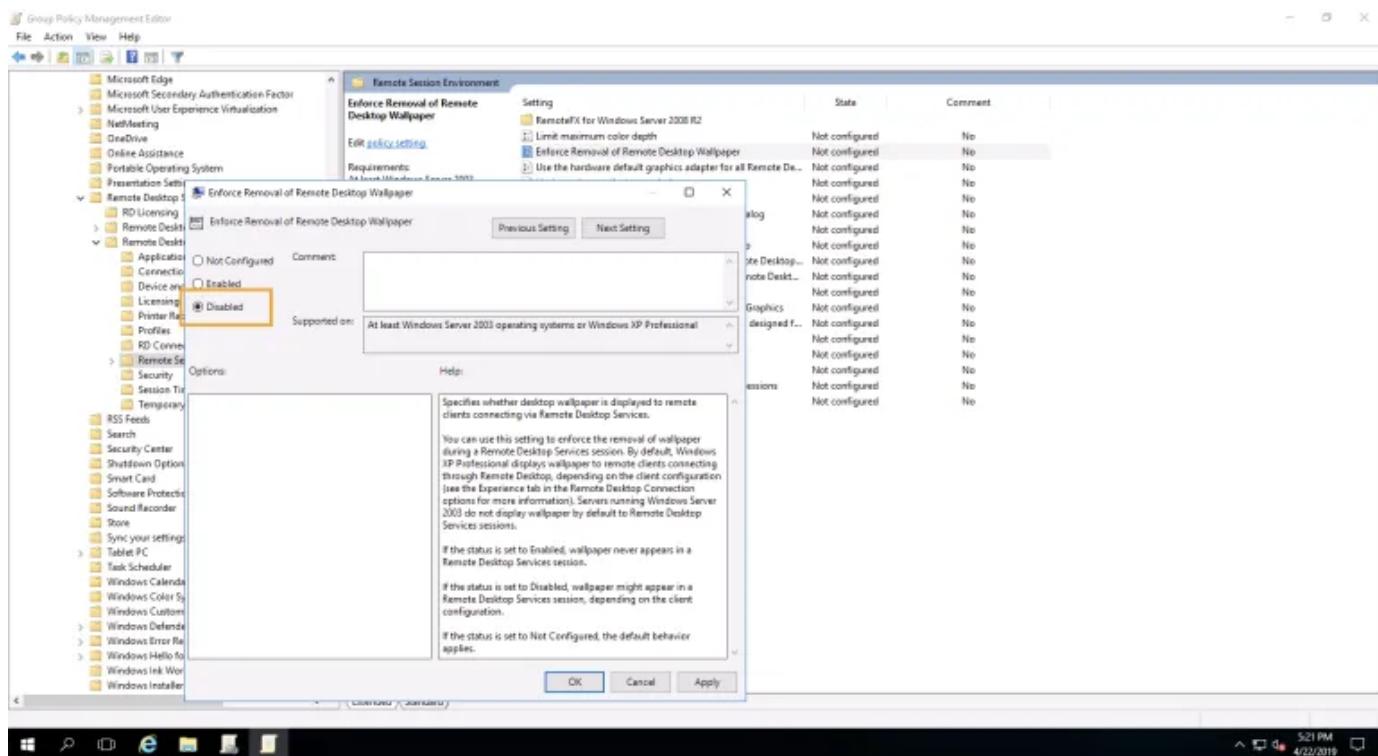
The figure consists of three side-by-side screenshots of the Group Policy Management Editor. All three screenshots show the 'Cloud Workspace Computers' GPO under the 'Cloud Workspace Computers' scope.

- Azure AD (Left):** Shows the 'Edit...' button highlighted in yellow. The 'User Configuration (Enabled)' section is visible.
- Internal AD (Middle):** Shows the 'Edit...' button highlighted in yellow. The 'User Configuration (Enabled)' section is visible.
- Internal AD (Right):** Shows the 'Edit...' button highlighted in yellow. The 'User Configuration (Enabled)' section is visible.

Bottom Screenshot:

This screenshot shows the 'Edit Administrative Templates policy setting' window for the 'Remote Session Environment' policy. A specific setting, 'Edit policy setting' for 'Force Removal of Remote Desktop Wallpaper', is selected and highlighted with a yellow box. The 'Edit' button for this setting is also highlighted with a yellow box.

Setting	Status	Comment
RemoteFX for Windows Server 2008 R2	Not configured	No
Force Removal of Remote Desktop Wallpaper	Not configured	No
Use the hardware default graphics adapter for	Not configured	No
Limit maximum display resolution	Not configured	No
Limit number of sessions	Not configured	No
Remove "Disconnected" option from Shut Down	Not configured	No
Remove Windows Security item from Start me	Not configured	No
Use advanced RemoteFX graphics for Remote	Not configured	No
Prioritize H.264/WF-4K graphics mode for Re	Not configured	No
Configure Luma compression for RemoteFX data	Not configured	No
Configure image quality for RemoteFX Adaptive Graphics	Not configured	No
Enable RemoteFX encoding for RemoteFX clients designed f...	Not configured	No
Configure RemoteFX Adaptive Graphics	Not configured	No
Start a program on connection	Not configured	No
Always show desktop on connection	Not configured	No
Allow desktop composition for remote desktop sessions	Not configured	No
Do not allow font smoothing	Not configured	No



Troubleshooting Printing Issues

Error

Printing to the local printer from the cloud desktop is not working.

Remote Desktop Services with ThinPrint

VDS optionally includes ThinPrint for Remote Desktop Services (RDS) deployments. The software and licensing are automatically configured at initial deployment. If ThinPrint is in use, the following sections can help troubleshooting issues with printing.

Cause

There are a variety of methods to connect to the cloud desktop. These method differ in how they perform printing functions and thus knowing which type of access is in use is necessary for troubleshooting:

1. Using CloudJumper's access client on a Windows device
 - a. ThinPrint runs on the local device and relays communication between the printer and the cloud desktop
2. Using the HTML5 browser on any device
 - a. The browser will present the printed document as a PDF to download and print locally
3. Using a manually configured RDP client (usually) on a Mac or Linux machine
 - a. Local printers are shared with the cloud desktop by manually configuring “Local Resources” in the RDP Client.

Resolution

1. Attempt to print a document from the local device to confirm that the local device is successfully connecting

to the printer.

2. Uninstall and re-install ThinPrint if using the Access Client on a Windows device. <https://www.thinprint.com/en/resources-support/software/clientsandtools/>
3. Make a note of the access type and the results of the first two steps in a new case with CloudJumper Support.

Azure Virtual Desktop

VDS does not implement any printing solution or unique printing configuration for AVD environments. Printing questions should be directed to Microsoft or (if one was implemented) the printing technology vendor.

Azure vCPU Core Quota

View Current Quota

1. Log into the Azure console and navigate to the Subscriptions module and click Quotas. Next, select all providers in the providers drop-down, select show all in the far-right drop down and select the Azure region in which your Cloud Workspace is deployed.

The screenshot shows the 'Microsoft Azure - Usage + quotas' page. In the left sidebar, 'Usage + quotas' is selected under 'Settings'. The main area displays a table with columns: QUOTA, PROVIDER, and LOCATION. A dropdown menu for 'LOCATION' is open, showing a list of Azure regions with checkboxes. Most regions have checkboxes checked, indicating they have quotas assigned. The regions listed are: Select all, Australia Central, Australia Central 2, Australia East, Australia Southeast, Brazil South, Canada Central, Canada East, Central India, Central US, East Asia, East US, East US 2, France Central, France South, Global, Japan East, Japan West, Korea Central, Korea South, and North Central US. A tooltip says 'No quotas & Select the provider in the dropdown'.

2. Then you'll see how much you're consuming vs. how much quota you have available. In the image below, CloudJumper is consuming 42 CPUs out of the 350 CPUs available for the BS family of VMs.
Increasing Quota

You can use each Microsoft Azure resource up to its quota. Each subscription has separate quotas and usage is tracked per subscription. If you reach a quota cap, you can request an increase via Help + Support. Learn more

[Request Increase](#)

QUOTA	PROVIDER	LOCATION	USAGE	
Standard B5 Family vCPUs	Microsoft.Compute	East US	<div style="width: 12%;"><div style="width: 12%;">12 %</div></div> 42 of 350	
Static Public IP Addresses	Microsoft.Network	East US	<div style="width: 1%;">1 %</div>	1 of 200
Public IP Addresses	Microsoft.Network	East US	<div style="width: 0%;">0 %</div>	2 of 1000
Load Balancers	Microsoft.Network	East US	<div style="width: 0%;">0 %</div>	1 of 1000
StandardSSDStorageDisks	Microsoft.Compute	East US	<div style="width: 0%;">0 %</div>	11 of 25000
Premium Storage Managed Disks	Microsoft.Compute	East US	<div style="width: 0%;">0 %</div>	1 of 25000
DDoS customized policies	Microsoft.Network	East US	<div style="width: 0%;">0 %</div>	0 of 200
DDoS Protection Plans	Microsoft.Network	East US	<div style="width: 0%;">0 %</div>	0 of 1
DirectDriveDisks	Microsoft.Compute	East US	<div style="width: 0%;">0 %</div>	0 of 20
DNS servers per Virtual Network	Microsoft.Network	East US	<div style="width: 0%;">0 %</div>	0 of 20
Frontend IP Configurations per Load B...	Microsoft.Network	East US	<div style="width: 0%;">0 %</div>	0 of 200
Inbound Rules per Load Balancer	Microsoft.Network	East US	<div style="width: 0%;">0 %</div>	0 of 250
Inbound rules per Network Interface	Microsoft.Network	East US	<div style="width: 0%;">0 %</div>	0 of 500

3. If you want to increase your quota, click Request Increase and tell it what you want to increase (99% of the time this will be compute/CPUs).

Home > Subscriptions > Microsoft Azure - Usage + quotas > New support request > Basics

New support request X

HELP + SUPPORT

1 Basics >

2 Problem >

3 Contact information >

Basics X

NEW SUPPORT REQUEST

Try our new case submission experience to submit your request →

* Issue type
Service and subscription limits (quotas)

* Subscription
Microsoft Azure (01d239c7-c2a9-494d-8a22-6c11afc3bc2d)

Can't find your subscription? [Show more](#) ⓘ

* Quota type
Compute/VM (cores/vCPUs) subscription limit increases

* Support plan
Cloud Solution Provider

Next

The screenshot shows the 'New support request' wizard in the Microsoft Azure portal. The current step is 'Basics'. The form contains several dropdown menus with selected values: 'Issue type' is 'Service and subscription limits (quotas)', 'Subscription' is 'Microsoft Azure (01d239c7-c2a9-494d-8a22-6c11afc3bc2d)', 'Quota type' is 'Compute/VM (cores/vCPUs) subscription limit increases', and 'Support plan' is 'Cloud Solution Provider'. A 'Next' button is visible at the bottom of the form.

4. Select the region your Cloud Workspace is deployed in and the VM family you want to increase quota for.

The screenshot shows the Microsoft Azure 'New support request' wizard at the 'Quota details' step. The left sidebar lists three steps: '1 Basics' (completed), '2 Problem' (selected), and '3 Contact information'. The main area is titled 'Problem NEW SUPPORT REQUEST' and contains sections for 'Severity' (set to 'C - Minimal impact'), 'Quota details' (with a note to 'Provide details for your quota request'), and 'File upload' (with a placeholder 'Select a file'). To the right, the 'Quota details' section is expanded, showing fields for 'Deployment model' (Resource Manager), 'Location' (East US), 'SKU family' (BS Series), and a table for 'SKU SERIES' with rows for 'BS Series' (CURRENT: 350, NEW LIMIT: 9001). A link to 'Learn about Compute (cores/vCPUs) quota increase requests' is also present. At the bottom are 'Next' and 'Save and continue' buttons.

- Enter your contact info and click Create to submit the request to Microsoft. They are usually VERY fast at increasing this.

Unlocking User Accounts

Overview

Unlocking a locked account for an End User is a simple process that resolves a moderately common issue that end users report.

After four failed login attempts the User will be locked out. The duration is 30 minutes unless the customer account has password complexity enabled, in which case the lockout can only be performed manually.

The user account can be unlocked from the list of users on the Users & Groups page in the Workspaces or from the User Detail page.

Users & Groups Page

Users				Add/Import	Refresh
<input type="text" value="toby"/>					
Name ▾	Username	Status	Connection Status		
Toby vanRoojen	toby.vanroojen...	● Available	● Account Locked		
« < 1 2 > »					

Users				Add/Import	Refresh
<input type="text" value="toby"/>					
Name ▾	Username	Status	Connection Status		
Toby vanRoojen	toby.vanroojen...	● Available	● Account Locked	Unlock	Locked
« < 1 2 > »				Delete	Unlock

User Detail Page

[NG6 Demo\(72q\)](#)

Toby vanRoojen (toby.vanroojen@ng6demo)

[Overview](#) [Delete User](#) [Unlock User](#)

User Details	Status & Connection Details	
Username toby.vanroojen	Connection Status Account Locked	Status Available
Phone	Email	
Login Identifier ng6demo	Partner Demo Customers	
First Name Toby	Last Name vanRoojen	
Created By toby.vanroojen@cloudjumper.net	Created On 11/10/2016 5:30 pm	

Troubleshooting Virtual Machine Performance

NetApp offers customers insight into troubleshooting server performance for users/apps. All companies consume resources differently based on the number of end users logged in at once, application use, if SQL Standard is installed vs. SQL Express, etc. so it is important to be able to review what is happening when a user reports performance issues.

Overview

Every app is different, and even the same software being run by the same number of users can have different resource consumption patterns. This is why it helps to understand the apps your users are running and what truly powers that app. Is it CPU, RAM or storage? These considerations will help focus your troubleshooting.

In our experience, these have proven to be generally true statements to help you begin:

CPU: this is usually the culprit/limiting factor if the app in question is home-grown and/or an Excel issue
 RAM: this is usually the culprit/limiting factor if SQL Standard is used
 Storage: this is usually a contributing factor if disk consumption is greater than 90%.



If SQL Express is used, it is likely a limiting factor – it limits RAM consumption to 1 GB, which will may be under the software vendor's required specs.

Using nightly resource reports

VDS sends nightly reports with information about each VM. There is a lot of useful information in that report, including recommendations on whether to increase or decrease resources. Here are a few excerpts:

This image shows whether you should increase or decrease CPU/RAM on VMs for a given workspace.

Company Code	Pool	Run Date PDT	Allocation Type	# Servers	# Users	Max Active Users	Ram GB Per User	CPU Per User	Max Ram %	Max CPU %	Recommended Change RAM	Recommended Change CPU	Ram GB	CPUs
[REDACTED]	D1	2018-07-30 09:12 AM	Unknown	0	0	0	N/A	N/A	N/A	N/A	No Change	No Change	0	0
[REDACTED]	D1	2018-07-30 09:12 AM	Unknown	0	0	0	N/A	N/A	N/A	N/A	No Change	No Change	0	0
[REDACTED]	SHARED	2018-07-30 09:12 AM	Fixed	0	0	0	N/A	N/A	N/A	N/A	Need More Data	Need More Data	6	2

In the image below, we can see that there is a column that shows how long it has been since the server has been rebooted.

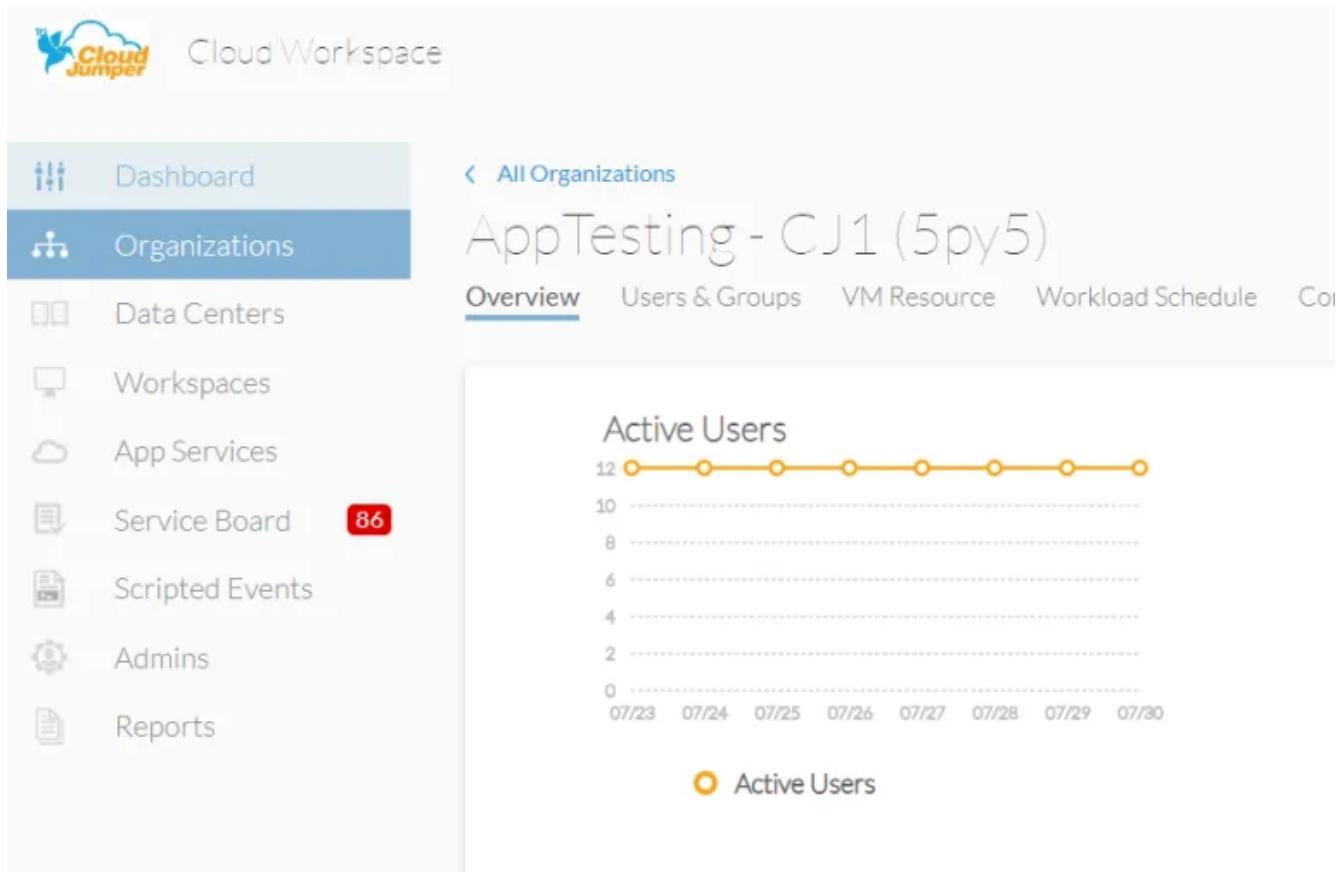
Time Since Last Reboot (dd:hh:mm)	Time Zone	RAM GB	CPUs
38:20:17	(UTC-08:00) Pacific Time (US & Canada)	4	2
146:00:46	(UTC-08:00) Pacific Time (US & Canada)	4	2

In this image we can see storage provisioned vs. consumed – this becomes a good topic to investigate briefly at first or once you have validated that CPU/RAM are not the issue.

Drive Total Space GB	Drive Used Space GB	Drive Free Space GB
63	15.63	47.82

Viewing CPU/RAM resource consumption in real-time

1. Log into VDS, then click the Organizations module and select the organization in question.



2. You can locate what server the user is logged into by locating them in the users section.

Overview **Users & Groups** VM Resource Workload Schedule Contact Info **X Delete Client**

Groups **Add** Users **Add/Import** Refresh

Filter by Keyword

Group	Users	Name	Username	Status	Connection Status
[REDACTED]	[REDACTED]	Test Doug	TestDoug@CJ1...	● Active	Offline
				● Active	Offline
				● Active	Offline
				● Active	Offline
				● Active	Offline
				● Active	Offline
				● Active	Offline

3. Next, scroll down until you see the Servers section – locate the server the user reporting the issue is logged into and click the settings wheel, then connect.

Servers **Add** Refresh

Filter by Keyword

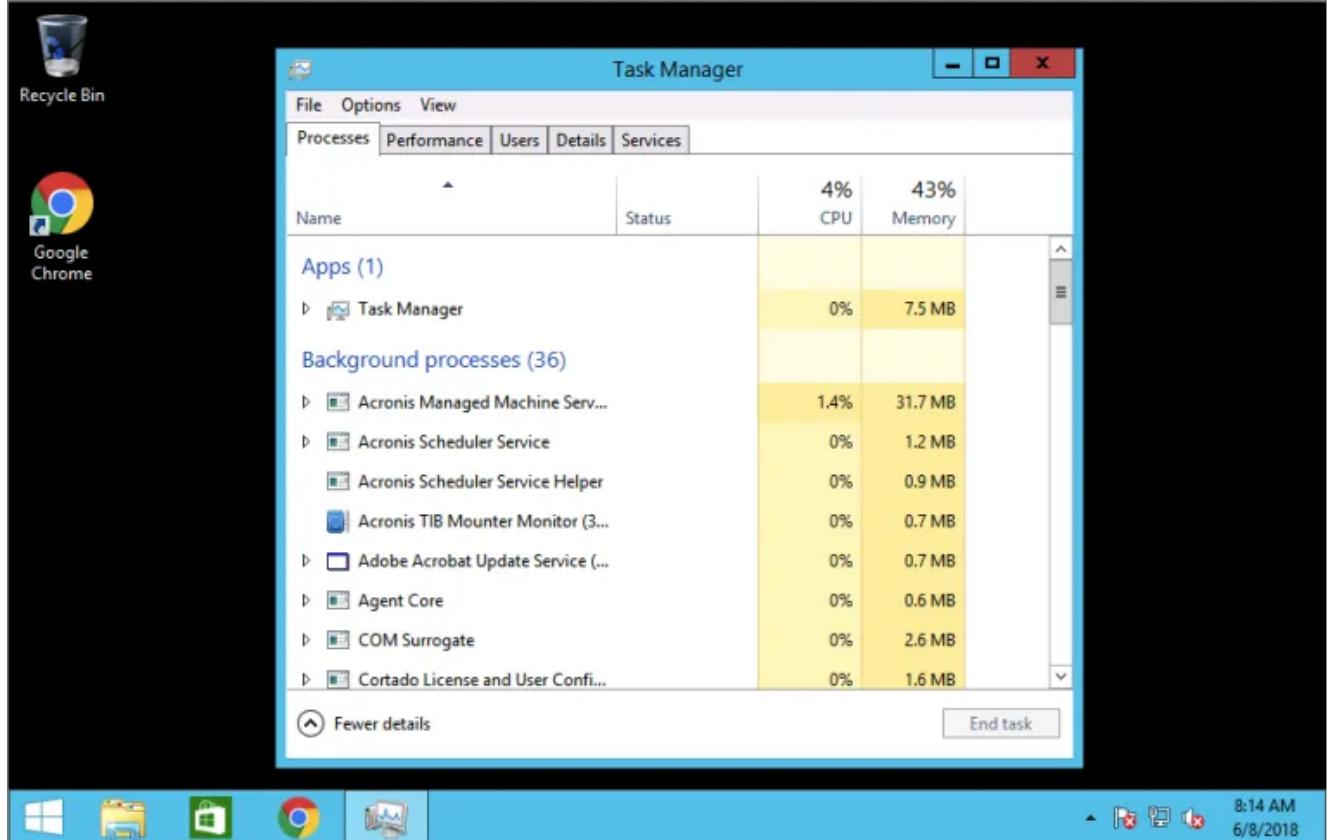
Name	Type	RAM	CPU	Online Status	Status
SPY5TSD1	Shared	8 GB	2	● Online	● Available

Connect

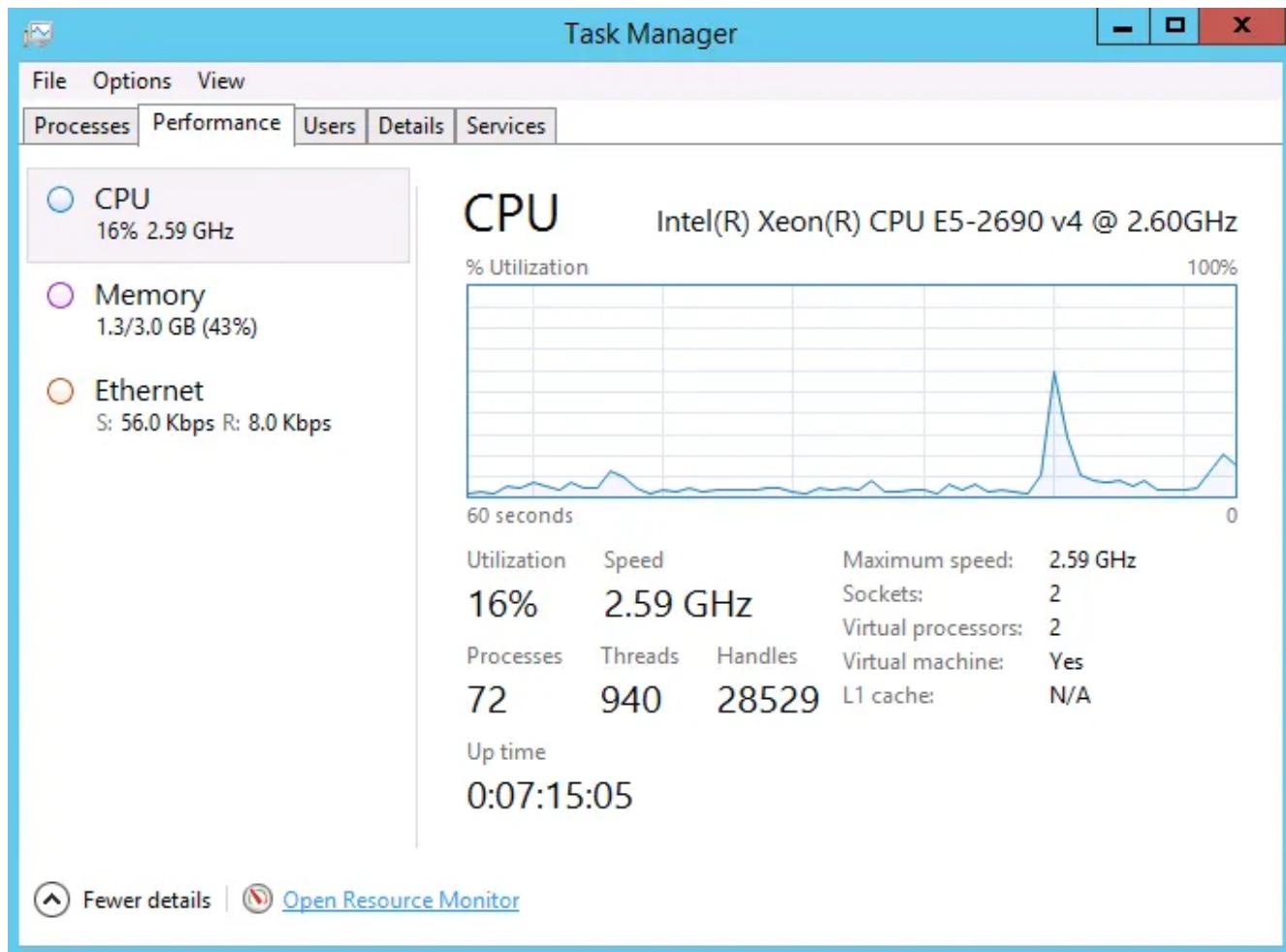
4. Once you've connected to the server, click the Start button. Next, click Task Manager.



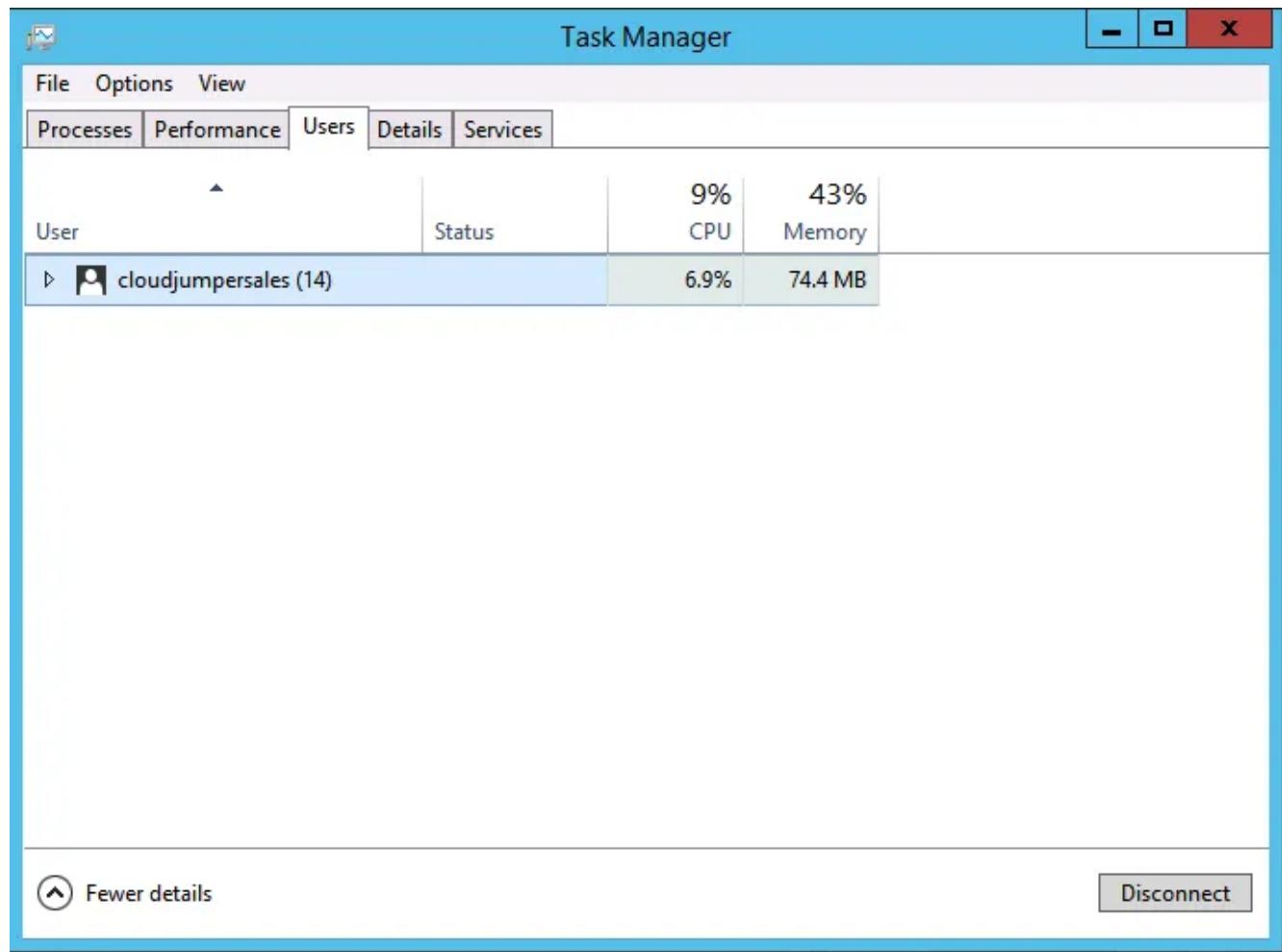
5. The Task Manager gives a wealth of insight into what's happening, right at that moment. This is the absolute best way to see what's affecting your users at the moment they report an issue to you.
6. You can review the processes running on the server, identify which if any are causing the issue and either communicate with the Customer or end the processes on the spot.



7. You can also view the Performance tab to show what's happening, live. This is a tremendous troubleshooting step – asking End users to repeat the steps they took to cause a performance issue, then seeing what happens. Similarly, if they follow general advice (close excess Chrome browser tabs, as Google Chrome tabs are a common resource consumer) you can see resource consumption decrease.



8. The users tab can show you which user, if any, is consuming the resources causing a spike in consumption.



9. You can expand each End user to see which specific processes they're running and how much each one is consuming.

The screenshot shows the Windows Task Manager window with the 'Users' tab selected. The main pane displays a list of processes running under the user 'cloudjumpersales'. The columns are labeled 'User', 'Status', 'CPU', and 'Memory'. The 'CPU' column shows usage percentages, and the 'Memory' column shows memory usage in MB. The 'Status' column indicates the process is running.

User	Status	4% CPU	43% Memory
cloudjumpersales (14)			
Acronis Scheduler Service ...		0%	0.9 MB
Acronis TIB Mounter Moni...		0%	0.7 MB
Client Server Runtime Proc...		0%	1.0 MB
Desktop Window Manager		0%	8.9 MB
Host Process for Windows ...		0%	1.9 MB
Java Update Checker (32 bit)		0%	2.1 MB
Java Update Scheduler (32 ...		0%	2.3 MB
PUAR v1.6 (32 bit)		0%	8.9 MB
RDP Clipboard Monitor		0%	1.3 MB
Resource and Performance...		0.7%	12.9 MB
SBAMTray Application (32 ...		0%	1.4 MB
Task Manager		0.7%	8.0 MB
Windows Explorer		0%	23.0 MB

More details Disconnect

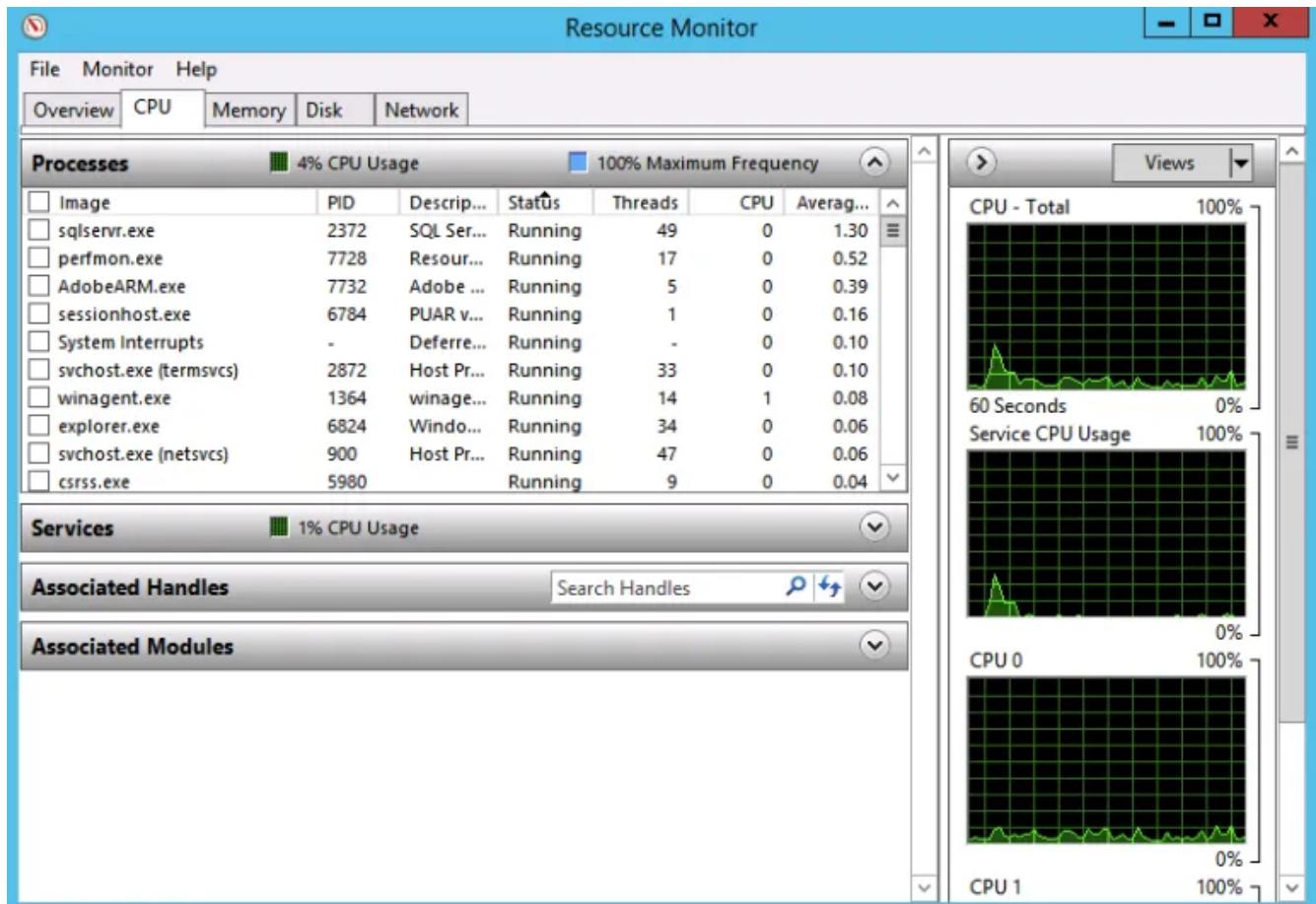
- Another option is viewing which services are running.

Task Manager

Name	PID	Description	Status	Group
WSearch	2420	Windows Search	Running	
wmiApSrv		WMI Performance Adapter	Stopped	
WIDWriter	1256	Windows Internal Database VSS Writer	Running	
VSS		Volume Shadow Copy	Stopped	
vmvss		VMware Snapshot Provider	Stopped	
VMTools	1644	VMTools	Running	
vds		Virtual Disk	Stopped	
VaultSvc		Credential Manager	Stopped	
UIODetect		Interactive Services Detection	Stopped	
Tssdis	2704	Remote Desktop Connection Broker	Running	
TrustedInstaller		Windows Modules Installer	Stopped	
TPVCGateway	2032	TP VC Gateway Service	Running	
TPTrackSvc	1988	TP Tracking Service	Running	
TPAutoConnSvc	1964	TP AutoConnect Service	Running	
TieringFngineService		Storage Tiers Management	Stopped	
sppsvc		Software Protection	Stopped	
Spooler	1200	Print Spooler	Running	
SNMPTRAP		SNMP Trap	Stopped	

More details |
 Open Services

11. Customers can also open the Resource Monitor to investigate in more detail.



Considering storage performance

One of the more common causes of VM performance issues is insufficient disk performance. Standard (and even SSD) disks are not designed to handle the high I/O load demanded by VDS workloads. User logins tend to happen in bunches and each one demands significant I/O as profiles and settings are loaded. NetApp's high performing storage technologies such as Azure NetApp Files, CVO and CVS are particularly well suited for this workload and should be considered the default option for VDS workloads.

Considering storage consumption

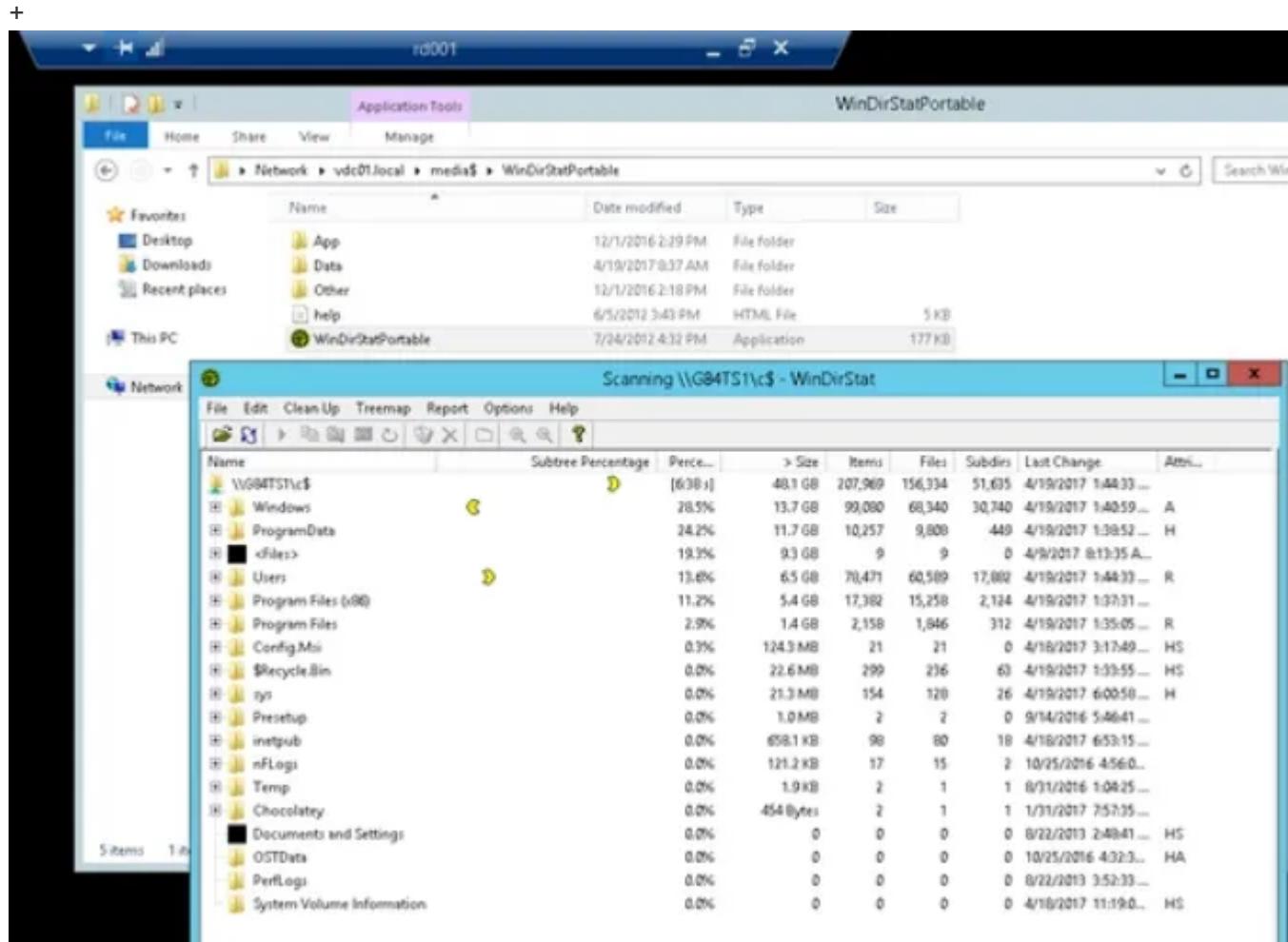
Microsoft has a long-held best practice against allowing disk consumption on any drive to exceed 90%. In their eyes, this causes performance to plummet and can cause a number of other challenges, such as not having enough storage for backups to complete and not allowing users to save their work.

RMM tools can offer storage monitoring services, including the ability to set thresholds and alerts. If storage becomes a challenge for you, working with your RMM vendor to enable these types of alerts is recommended.

For deeper investigation, install software to review drive consumption.

From conversations with customers, Windirstat or Treesize have proven to be the preferred applications for inspection of drive consumption.

Windirstat can inspect a full drive over the network if there is insufficient space to install/run an app locally or login is blocked:



DNS Forwards for Azure ADDS & SSO via O365 identity

Overview

Users can't access company websites on primary email domain.

For Example, NetApp employees in VDS workspaces can't access netapp.com if their SSO account is user@netapp.com

Dedicated VDS deployments use the internal domain of the Azure tenant.

Resolution

To resolve this, the Organization's team that manages DNS will need to create a DNS forward lookup zone for your internal domain to allow it to resolve the correct external IP (for NetApp's purpose, this would let NetApp employees browse to netapp.com from within their virtual desktop).

Step by Step Guide

1. Install the DNS Server Tools on CWMGR1 – this will allow you to manage DNS.

Server Manager

Server Manager • Dashboard

Manage Tools View Help

Dashboard Local Server All Servers File and Storage Services

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

5 Connect this server to cloud services

Hide

ROLES AND SERVER GROUPS

Roles: 1 | Server groups: 1 | Servers total: 1

File and Storage Services	Local Server	All Servers
Manageability	Manageability	Manageability
Events	Events	Events
Performance	Services	Services
BPA results	Performance	Performance
	BPA results	BPA results

Before you begin

DESTINATION SERVER
contoso100-test.contoso100.com

Before You Begin

[Installation Type](#)[Server Selection](#)[Server Roles](#)[Features](#)[Confirmation](#)[Results](#)

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:

[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

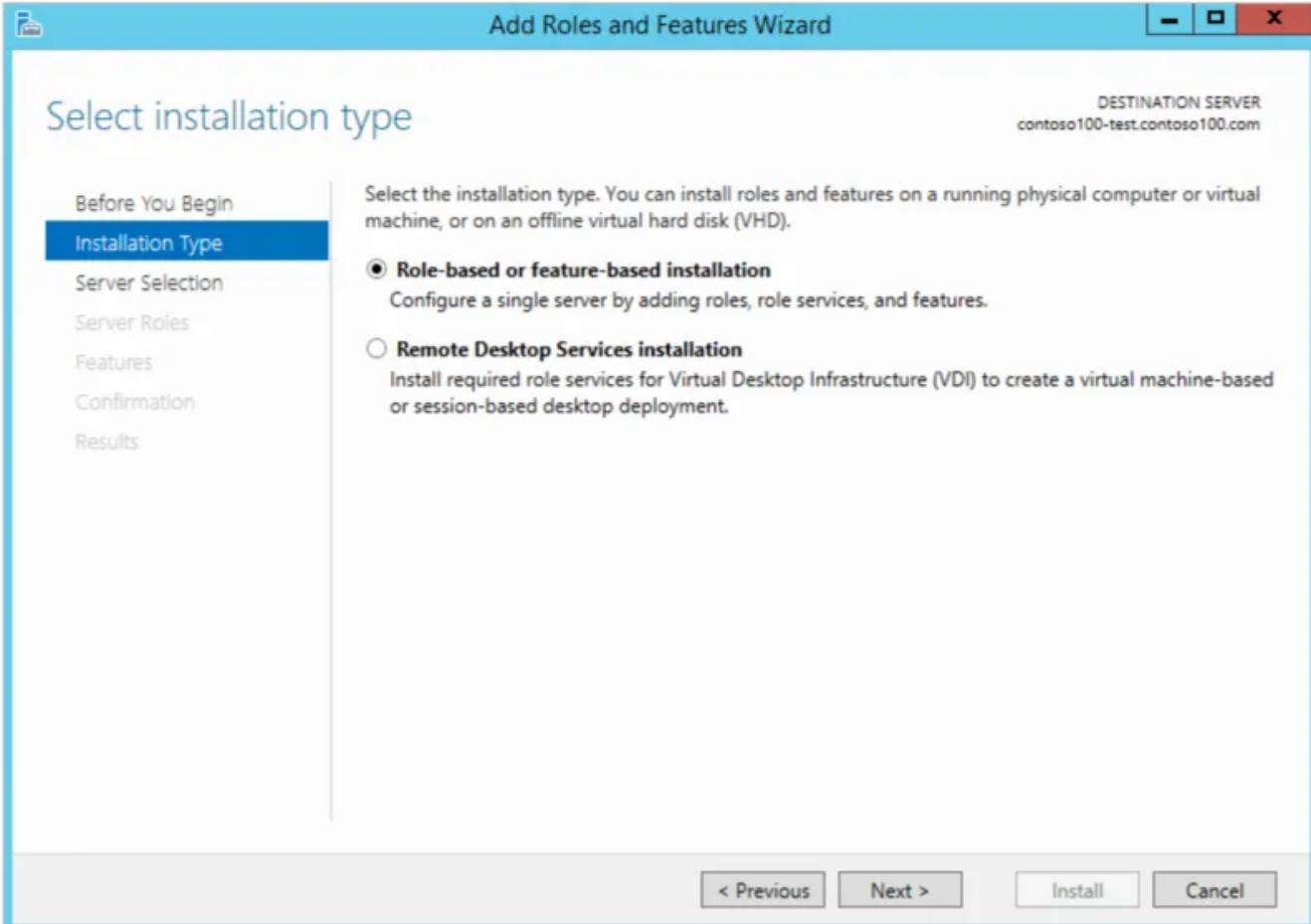
Skip this page by default

[< Previous](#)

[Next >](#)

[Install](#)

[Cancel](#)



Select destination server

DESTINATION SERVER
cwmgr1.cloudjumper.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select a server or a virtual hard disk on which to install roles and features.

- Select a server from the server pool
 Select a virtual hard disk

Server Pool

Filter:		
Name	IP Address	Operating System
cwmgr1.cloudjumper.com	10.0.0.12	Microsoft Windows Server 2016 Datacenter

1 Computer(s) found

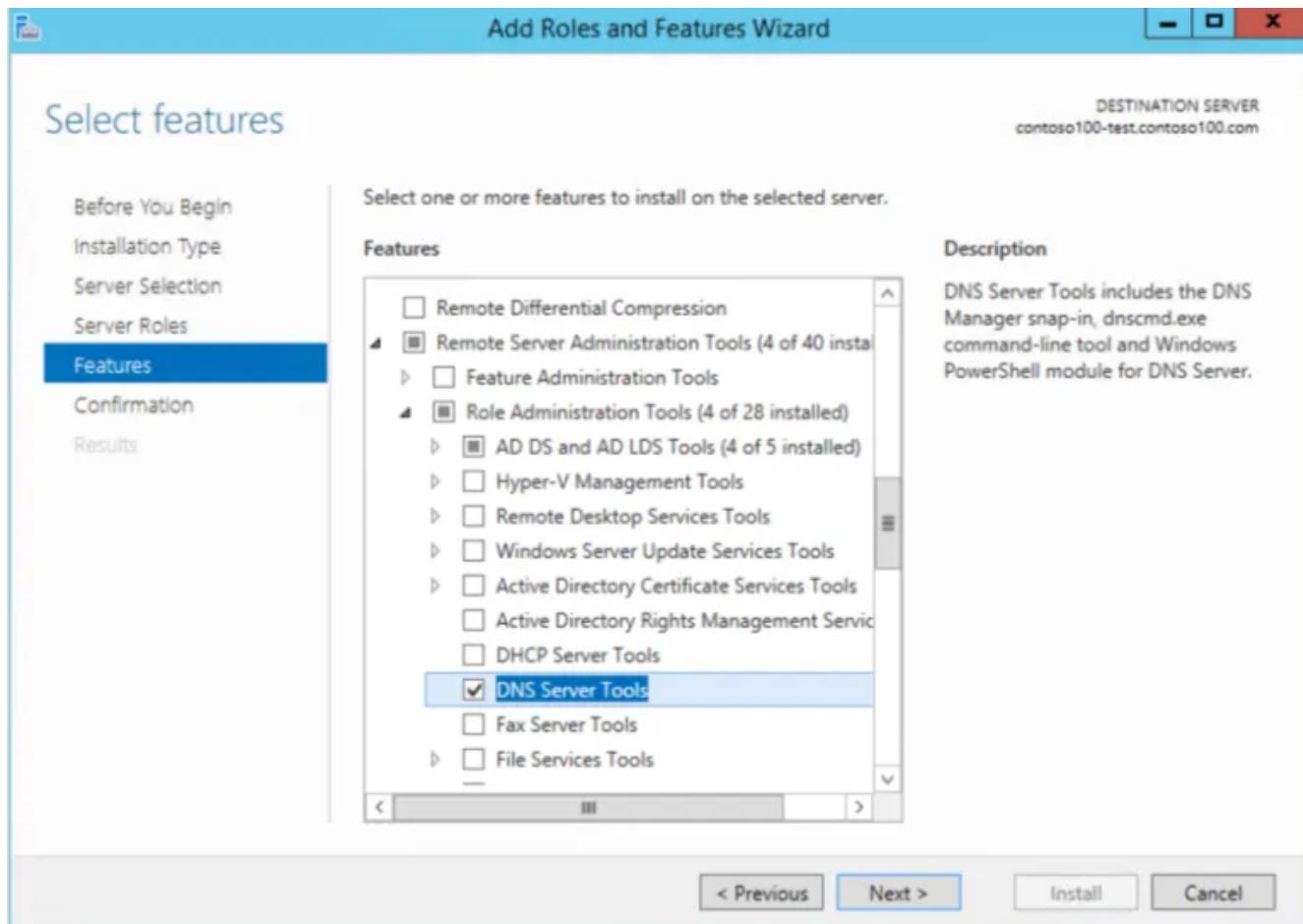
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous

Next >

Install

Cancel



- Once installed, you can go to Control Panel → System and Security → Administrative Tools and open up DNS.

The screenshot shows the Windows Control Panel with the path: Control Panel > System and Security > Administrative Tools. The 'Administrative Tools' tab is selected. On the left, there's a 'Quick access' sidebar with links to Desktop, Downloads, Documents, Pictures, This PC, Cloud on 64.141.18, Desktop, Documents, Downloads, Music, Pictures, Videos, Windows (C:), Temporary Storage, and Network. The main area lists various administrative tools as shortcuts, including Active Directory Administrative Center, Active Directory Domains and Trusts, Active Directory Lightweight Directory Se..., Active Directory Module for Windows Po..., Active Directory Sites and Services, Active Directory Users and Computers, ADSI Edit, Cassia.dll, Cassia, Component Services, Computer Management, Defragment and Optimize Drives, Disk Cleanup, DNS, Event Viewer, Group Policy Management, Internet Information Services (IIS) Manager, iSCSI Initiator, Local Security Policy, Microsoft Azure Services, and ODBC Data Sources (32-bit). The 'DNS' shortcut is highlighted with a blue selection bar.

Name	Date modified	Type	Size
Active Directory Administrative Center	7/16/2016 9:19 AM	Shortcut	2 KB
Active Directory Domains and Trusts	7/16/2016 9:20 AM	Shortcut	2 KB
Active Directory Lightweight Directory Se...	7/16/2016 9:20 AM	Shortcut	2 KB
Active Directory Module for Windows Po...	7/16/2016 9:19 AM	Shortcut	2 KB
Active Directory Sites and Services	7/16/2016 9:19 AM	Shortcut	2 KB
Active Directory Users and Computers	7/16/2016 9:20 AM	Shortcut	2 KB
ADSI Edit	7/16/2016 9:19 AM	Shortcut	2 KB
Cassia.dll	4/11/2011 1:49 PM	Application extens...	36 KB
Cassia	4/11/2011 1:49 PM	XML Document	39 KB
Component Services	7/16/2016 9:18 AM	Shortcut	2 KB
Computer Management	7/16/2016 9:18 AM	Shortcut	2 KB
Defragment and Optimize Drives	7/16/2016 9:18 AM	Shortcut	2 KB
Disk Cleanup	7/16/2016 9:19 AM	Shortcut	2 KB
DNS	7/16/2016 9:19 AM	Shortcut	2 KB
Event Viewer	7/16/2016 9:18 AM	Shortcut	2 KB
Group Policy Management	7/16/2016 9:19 AM	Shortcut	2 KB
Internet Information Services (IIS) Manager	7/16/2016 9:19 AM	Shortcut	2 KB
iSCSI Initiator	7/16/2016 9:18 AM	Shortcut	2 KB
Local Security Policy	7/16/2016 9:19 AM	Shortcut	2 KB
Microsoft Azure Services	7/16/2016 9:19 AM	Shortcut	2 KB
ODBC Data Sources (32-bit)	7/16/2016 9:18 AM	Shortcut	2 KB

3. When asked for the DNS server running DNS you will want to put in your domain name (in the example we've been using, this would be *netapp.com*).

Troubleshooting Application Issues

Overview

Troubleshooting an application error is a common administrative practice that doesn't involve VDS itself, but is greatly assisted by VDS and the level of control it provides administrators. While NetApp VDS does not troubleshoot these issues for Customers, our experience allows us to advise administrators after identifying some basic information like the following in order to dig deeper and troubleshoot with end users and/or third parties.

- Name of the user experiencing the issue
- Name of the application the user was working with
- The server the user's session was on
- Steps to reproduce the issue

Reviewing Your Tools

Monitoring

After identifying the server the User was using, check your monitoring solution to validate that resource (CPU and RAM) consumption is within normal levels. You can also validate that application-specific requirements (a special service that will cause issues if it isn't running) are functional. In situations like this, advanced settings like up/down monitoring of said services may have been triggered.

Anti-Virus

As an administrator with access to both the servers and Azure Active Directory, you have access to review what has been discovered and what policies are set. In the event something unforeseen is present, it could be affecting your application.

Additional Tools

Some applications require additional components, like a service account that remains logged in indefinitely or a VPN to a piece of physical equipment (say, an on-site network appliance or a piece of manufacturing equipment or diagnostic utility). In these situations, application-specific errors may be caused by something other than the way the application was installed or how its settings are configured.

Extending Access to Third Parties

Applications and/or their databases are often installed, configured and supported by either the software vendor (ISV) themselves or a third party expert in that software's configuration, management and integrations. In these situations you will want to extend temporary administrative access to a these steps: [Providing Temporary Access to 3rd Parties](#)

It is a best practice to shut down these third party accounts after the upgrade or update is completed or after the issue is resolved.

In many cases, this level of troubleshooting will require that a software maintenance contract with the ISV. If this is not in place, the ISV may not assist you until this is in place.

 It is also possible that the troubleshooting issue could be related to the hardware (desktops, laptops, thin clients, etc.) end users are working with. An example could be that upgrading a user's laptop could lock the machine in the eyes of a thin client configuration file, meaning that end users cannot access the tools that allow them to log into their virtual desktop. In this case, a maintenance contract for hardware may be required before the manufacturer will assist you.

Reference

Release notes

Virtual Desktop Service – v6.0 Release Notes

VDS v6 release: Thursday September 9th, 2021

Components: Virtual Desktop Service v6

When: Thursday September 9, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Assorted proactive security and performance enhancements

VDS v6 release: Thursday August 26th, 2021

Components: Virtual Desktop Service v6

When: Thursday August 26, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Update to the URL placed on a user's desktop when they are granted access to the VDS management UI

VDS v6 release: Thursday August 12th, 2021

Components: Virtual Desktop Service v6

When: Thursday August 12, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Enhancements to Cloud Insights functionality and context
- Improved backup schedule frequency handling
- Bug fix - resolve an issue for CwVmAutomation service checking config on service restart
- Bug fix - resolve an issue for DCConfig that did not allow saving configurations in certain scenarios
- Assorted proactive security and performance enhancements

VDS v6 hotfix: Tuesday July 30th, 2021

Components: Virtual Desktop Service v6

When: Friday July 30th, 2021 at 7pm – 8pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Deployment template update to facilitate automation improvements

VDS v6 release: Thursday July 29th, 2021

Components: Virtual Desktop Service v6

When: Thursday July 29th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Bug fix - resolve an issue for VMware deployments where CWAgent didn't get installed as intended
- Bug fix - resolve an issue for VMware deployments where creating a server with the Data role didn't function as intended

VDS v6 hotfix: Tuesday July 20th, 2021

Components: Virtual Desktop Service v6

When: Tuesday July 20th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Remediate an issue causing abnormally large amount of API traffic in a certain configuration

VDS 6.0 release: Thursday July 15th, 2021

Components: 6.0 Virtual Desktop Service

When: Thursday July 15th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Enhancement to Cloud Insights integration –capturing per-user performance metrics and displaying them in the User context
- Improvements to ANF provisioning automation – improved automated registration of NetApp as a provider in the customer's Azure tenant
- Phrasing adjustment when creating a new AVD Workspace
- Assorted proactive security and performance enhancements

VDS 6.0 release: Thursday June 24, 2021

Components: 6.0 Virtual Desktop Service

When: Thursday June 4th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.



Due to scheduling around the 4th of July, the next VDS release will be on Thursday 7/15.

Virtual Desktop Service

- Updates to reflect that Windows Virtual Desktop (WVD) is now Azure Virtual Desktop (AVD)
- Bug fix for username formatting in Excel exports
- Improved configurations for custom branded HTML5 login pages
- Assorted proactive security and performance enhancements

Cost Estimators

- Updates to reflect that Windows Virtual Desktop (WVD) is now Azure Virtual Desktop (AVD)
- Updates to reflect the more services/GPU VMs are available in new regions

VDS 6.0 release: Thursday June 10, 2021

Components: 6.0 Virtual Desktop Service

When: Thursday June 10th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Introduction of an additional HTML5 browser-based gateway/access point for VMs
- Improved user routing after deleting a host pool
- Bug fix for a scenario where importing an unmanaged host pool was not functioning as expected
- Assorted proactive security and performance enhancements

VDS 6.0 release: Thursday June 10, 2021

Components: 6.0 Virtual Desktop Service

When: Thursday June 10th, 2021 at 10pm eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Technical enhancements:

- Update the version of the .NET framework installed on each VM from v4.7.2 to v4.8.0
- Additional back-end enforcement of the use of https:// and TLS 1.2 or greater between the Local Control Plane team and any other entity
- Bug fix for the Delete Backup Operation in the Command Center – this now properly references the time zone of CWMGR1
- Rename the Command Center action from Azure File share to Azure Files share
- Naming convention updates in Azure Shared Image Gallery
- Improved concurrent user login count collection
- Update to outbound traffic allowed from CWMGR1, if restricting traffic outbound from the CWMGR1 VM
 - If you are not restricting outbound traffic from CWMGR1, you do not have to make any updates here
 - If you are restricting outbound traffic from CWMGR1, please allow access to vdctoolsapiprimary.azurewebsites.net. Note: you no longer need to allow access to vdctoolsapi.trafficmanager.net.

Deployment enhancements:

- Lay the foundation for future support of custom prefixes in server names
- Improved process automation and redundancies for Azure deployments
- Numerous deployment automation enhancements for Google Cloud Platform deployments
- Support for Windows Server 2019 in Google Cloud Platform deployments
- Bug fix for a subset of scenarios where the Windows 10 20H2 EVD image

Service delivery enhancements:

- Introduces Cloud Insights integration, delivering streaming performance data for User Experience, VM and Storage layers
- Introduces a function that allows you to quickly navigate to a VDS page visited recently
- Substantially improved list (Users, Groups, Servers, Applications, etc.) loading times for Azure deployments
- Introduces the ability to easily export lists of Users, Groups, Servers, Admins, Reports, etc.
- Introduces the ability to control what VDS MFA methods are available for customers (customer prefers email vs. SMS, for example)
- Introduces customizable “from” fields for VDS self-service password reset emails
- Introduces the option to only allow VDS self-service password reset emails to go to specified domains (company owned vs. personal, for example)
- Introduces an update that can prompt the user to add their email to their account so that they can use it or MFA/self-service password resets
- When starting a stopped deployment, start all VMs within the deployment as well
- Performance improvement for determining which IP address to assign to newly created Azure VMs

VDS 6.0 release: Thursday May 27, 2021

Components: 6.0 Virtual Desktop Service

When: Thursday May 27th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Introduce Start on Connect for Pooled session hosts in AVD host pools
- Introduce User performance metrics via Cloud Insights integration
- Display the Servers tab more prominently in the Workspaces module
- Allow the restoration of a VM via Azure Backup if the VM has been deleted from VDS
- Improved handling of Connect to Server functionality
- Improved handling of variables when creating and updating certificates automatically
- Bug fix for an issue where clicking an X in a drop-down menu didn't clear the selection as expected
- Improved reliability and automatic error handling for SMS message prompts
- Update to the User Support role – this can now terminate processes for a logged in user

- Assorted proactive security and performance enhancements

VDS 6.0 release: Thursday May 13, 2021

Components: 6.0 Virtual Desktop Service

When: Thursday May 13th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Introduction of additional AVD host pool properties
- Introduce additional automation resilience in Azure deployments in the event of back-end service issues
- Include the server name in the new browser tab when using the Connect to Server feature
- Display the quantity of users in each group
- Enhanced resilience for the Connect to Server feature in all deployments
- Additional enhancements to setting MFA options for organizations and end users
 - If SMS is set as the only MFA option available, require a phone number but not an email address
 - If email is set as the only MFA option available, require an email address but not a phone number
 - If both SMS and email are set as options for MFA, require both an email address and a phone number
- Clarity improvement - remove the size of an Azure Backup snapshot, as Azure doesn't return the size of the snapshot
- Add the ability to delete a snapshot in non-Azure environments
- Bug fix for AVD host pool creation when using special characters
- Bug fix for workload scheduling for host pool via the Resources tab
- Bug fix for an error prompt that appears when cancelling a bulk user import
- Bug fix for a possible scenario with settings of application added to a Provisioning Collection
- Update to the email address sending notifications/messages – messages will now be sent from noreply@vds.netapp.com
 - Customers safelisting inbound email addresses should add this email address

VDS 6.0 release: Thursday April 29, 2021

Components: 6.0 Virtual Desktop Service

When: Thursday April 29th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Introduce Start on Connect feature for Personal AVD host pools
- Introduce Storage context in the Workspace module
- Introduce Storage (Azure NetApp Files) monitoring via Cloud Insights integration
 - IOPs monitoring
 - Latency monitoring

- Capacity monitoring
- Improved logging for VM Cloning actions
- Bug fix for a specific workload scheduling scenario
- Bug fix for not displaying a VM's time zone in a certain scenario
- Bug fix for not logging out a AVD user in a certain scenario
- Updates to automatically generated emails to reflect NetApp branding

VDS 6.0 hotfix: Friday April 16th, 2021

Components: 6.0 Virtual Desktop Service

When: Friday April 16th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Resolve an issue with automated certificate creation that arose after last night's update that improved automated certificate management

VDS 6.0 release: Thursday April 15, 2021

Components: 6.0 Virtual Desktop Service

When: Thursday April 15th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Enhancements to the Cloud Insights integration:
 - Frames Skipped – Insufficient Network Resources
 - Frames Skipped – Insufficient Client Resources
 - Frame Skipped – Insufficient Server Resources
 - OS Disk – Read Bytes
 - OS Disk – Write Bytes
 - OS Disk – Read Bytes/second
 - OS Disk – Write Bytes/second
- Update to task history in the Deployments module – improved handling of task history
- Bug fix for an issue where an Azure Backup couldn't be restored to CWMGR1 from a disk in a subset of scenarios
- Bug fix for an issue where certificates weren't automatically being updated and created
- Bug fix for an issue where a stopped deployment didn't start quickly enough
- Update to the State drop-down list when creating a Workspace – remove the item "National" from the list
- Additional updates to reflect NetApp branding

VDS 6.0 hotfix: Wednesday April 7th, 2021

Components: 6.0 Virtual Desktop Service

When: Wednesday April 7th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Due to increasingly variable response times from Azure, we are increasing the amount of time we wait for a response when entering Azure credentials during the deployment wizard.

VDS 6.0 release: Thursday April 1, 2021

Components: 6.0 Virtual Desktop Service

When: Thursday April 1st, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Updates to the NetApp Cloud Insights integration – new streaming data points:
 - NVIDIA GPU performance data
 - Round Trip Time
 - User Input Delay
- Update the Connect to Server function to allow administrative connections to VMs even when VMs are set to disallow connections from end users
- API enhancements to enable theming & branding in a subsequent release
- Improved visibility of the actions menu available in HTML5 connections via Connect to Server or RDS user sessions via HTML5
- Increase the QTY of characters supported in the name of an activity Scripted Events
- Updated Provisioning Collections OS choices by type
 - For AVD and Windows 10, use the VDI collection type to ensure the Windows 10 OS is present
 - For a Windows Server OS, use the Shared collection type
- Assorted proactive security and performance enhancements

Virtual Desktop Service – v5.4 Release Notes

VDS 5.4 release: Thursday August 12, 2021

Components: 5.4 Virtual Desktop Service

When: Thursday August 12th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Updated AVD host pool links

VDS 5.4 release: Thursday May 13, 2021

Components: 5.4 Virtual Desktop Service

When: Thursday May 13th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Bug fix for AVD host pool creation when using special characters
- Automation enhancements for long domain names in the CWA Setup deployment wizard
- Bug fix for cloning servers in a subset of scenarios in GCP deployments
- Bug fix for a scenario where deleting a snapshot wasn't functioning as intended
- Update to the email address sending notifications/messages – messages will now be sent from noreply@vds.netapp.com
 - Customers safelisting inbound email addresses should add this email address

VDS 5.4 release: Thursday April 29, 2021

Components: 5.4 Virtual Desktop Service

When: Thursday April 29th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

(No updates this release)

VDS 5.4 hotfix: Friday April 16, 2021

Components: 5.4 Virtual Desktop Service

When: Friday April 16th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Resolve an issue with automated certificate creation that arose after last night's update that improved automated certificate management

VDS 5.4 release: Thursday April 15, 2021

Components: 5.4 Virtual Desktop Service

When: Thursday April 15th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Continuous, ongoing updates to improve connectivity and communication with the vSphere / vCloud hypervisor
- Bug fix for an individual scenario where a user couldn't clone a AVD session host

VDS 5.4 hotfix: Tuesday March 23, 2021

Components: 5.4 Virtual Desktop Service

When: Tuesday March 23rd, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Update to the displaying host pools – resolve an issue in a subset of scenarios where newly created host pools were completing successfully, but not promptly present in the VDS UI

VDS 5.4 release: Thursday March 18, 2021

Components: 5.4 Virtual Desktop Service

When: Thursday March 18th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

- Virtual Desktop Service
- Allow Connect to Server functionality when end user connections to a VM are disallowed
- Phrasing adjustment to PAM messages users receive via SMS
- Assorted proactive security and performance enhancements

VDS 5.4 hotfix: Tuesday March 9, 2021

Components: 5.4 Virtual Desktop Service

When: Tuesday March 9th, 2021 at 5pm – 5:15pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Apply an update to resolve a Connect to Server issue in a subset of scenarios

VDS 5.4 release: Thurs, Mar. 4, 2021

Components: 5.4 Virtual Desktop Service

When: Thursday March 4th, 2021 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Introduction of DSC-driven deployment model for Google Cloud Platform deployments
- Scripted Events update to prevent a script from being deleted while it is actively running
- Automation enhancements to the deployment wizard's handling of NetBIOS for existing Active Directory environments
- Support applying different backup schedules for individual platform servers
- Support changing a user's password to require them to reset their password at the next login in the same command

- Bug fix – allow individual VMs set to migration mode to override deployment-wide migration mode settings
- Bug fix for vSphere scenario where sending too many API commands at once caused a delay starting VMs
- Update new deployments to support .NET 4.8.0
- Assorted proactive security and performance enhancements

VDS 5.4 release: Thurs., Feb. 18, 2021

Components: 5.4 Virtual Desktop Service

When: Thursday February 18th, 2021 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Updates to the default install method for FSLogix per Microsoft best practices
- Proactive upgrades to platform components to support increased user activity
- Improved automation for handling certificate management variables
- Support forcing a reset of a User's MFA settings at next login when changing their password
- Remove VDS admin group from being managed within the Groups module VDS in AADDS deployments

Cost Estimators

- Updates to reflect that certain VMs no longer have Promo price points

VDS 5.4 release: Thurs., Feb. 4, 2021

Components: 5.4 Virtual Desktop Service

When: Thursday February 4th, 2021 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Improved variable handling when using Connect to Server functionality
- API – side functionality for reboot and multi-select reboot functionality
- Deployment automation enhancements in Google Cloud Platform
- Improved handling of Google Cloud Platform deployments that are powered off

VDS 5.4 release: Thurs., January 21, 2021

Components: 5.4 Virtual Desktop Service

When: Thursday January 21st, 2021 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Removal of TSD1 VMs from deployments selecting PaaS services for data management
- Assorted proactive security and performance enhancements

- Process streamlining for multi-server deployment configurations
- Bug fix for a specific configuration for a deployment in GCP
- Bug fix for creating Azure Files shares via the Command Center
- Update to provide Server 2019 as an OS in GCP

Cost Estimators

- Assorted proactive security and performance enhancements

VDS 5.4 hotfix: Mon. January 18, 2021

Components: 5.4 Virtual Desktop Service

When: Monday January 18th, 2021 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- VDS will be applying an update to deployments leveraging SendGrid for SMTP relay
- SendGrid is introducing a breaking change on Wednesday 1/20
- The VDS team had already been investigating upgrades to SendGrid
- We have been aware of this coming change and have tested and validated an alternative (Postmark)
- In addition to mitigating a breaking change, the VDS team has seen improved reliability and performance increases in deployments leveraging Postmark instead of SendGrid

VDS 5.4 hotfix: Fri. January 8, 2021

Components: 5.4 Virtual Desktop Service

When: Wednesday January 8th, 2021 at 12pm – 12:05pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Brief, subsequent update to ensure that VDCTools is current in all deployments
 - By design, updates to VDCTools are applied intelligently – the update waits until no actions are being taken, then automatically completes any actions taken during the brief update period

VDS 5.4 release: Thurs., January 7, 2021

Components: 5.4 Virtual Desktop Service

When: Thursday January 7th, 2021 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Assorted proactive security and performance enhancements
- Text update – change the Command Center action from Create Azure File Share to Create Azure Files Share

- Process enhancement for using Command Center to update Data/Home/Pro folders

Cost Estimators

- Assorted proactive security and performance enhancements

VDS 5.4 release: Thurs., December 17, 2020

Components: 5.4 Virtual Desktop Service

When: Thursday December 17th, 2020 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.



The next release will be on Thursday January 7th, 2021 instead of New Year's Eve 2020.

Virtual Desktop Service

- Improved deployment automation when using Azure NetApp Files
- Enhancement to Provisioning Collections with updated Windows 10 images
- Update to VCC to better support variables in multi-site configurations
- Minor proactive security enhancement to Sites functionality
- API enhancements to Peak Live Scaling functionality within Live Scaling
- General usability and text clarity improvements in DC Config
- Assorted behind the scenes bug fixes and security enhancements

VDS 5.4 release: Thurs., December 3, 2020

Components: 5.4 Virtual Desktop Service

When: Thursday December 3rd, 2020 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Update to the FSLogix installation method
- Ongoing proactive security measures

VDS Setup

- Update to Azure NetApp Files deployment automation – support creating:
 - 4 TB Capacity Pool/Volume at minimum
 - 500 TB Capacity Pool/100 TB Volume at maximum
- Improved variable handling for advanced deployment options

Cost Estimators

- Removal of disk operations from the Google Cost Estimator
- Updates reflecting new services available by region in the Azure Cost Estimator

VDS 5.4 release: Thurs., November 19, 2020

Components: 5.4 Virtual Desktop Service

When: Thursday November 19th, 2020 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

VDS

- Privileged Account Management (PAM) emails now include deployment code details
- Permissions streamlining for Azure Active Directory Domain Services (AADDS) deployments
- Improved clarity for admins looking to perform admin tasks in a deployment that is completely powered down
- Bug fix for an error prompt that appeared when a VDS admin viewing RemoteApp App Group details for a host pool that is powered down
- Phrasing update to API Users to reflect that they are VDS API Users
- Faster results for returning the Data Center Status report
- Improved handling of variables for daily actions (nightly reboots, for example) for VMs
- Bug fix for a scenario where IP Addresses entered in DC Config were not saving correctly
- Bug fix for a scenario where unlocking an admin account didn't function as intended

VDS Setup

- Form factor update – resolve a scenario where action buttons in the VDS Setup wizard were truncated

VDS 5.4 release: Thurs., November 5, 2020

Components: 5.4 Virtual Desktop Service

When: Thursday November 5th, 2020 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

VDS

- Introduction of scale-out mechanism for Sites in Command Center – use another Azure subscription with the same Tenant ID and Client ID
- Creation of VMs with the Data role now deploy as the VM selected in the VDS UI but will fall back to the default specified for the deployment if the VM selected is not available
- General enhancements to Workload Scheduling and Live Scaling
- Bug fix for Apply All checkbox for admin permissions
- Bug fix for a display issue when showing apps selected in a RemoteApp App Group
- Bug fix for an error prompt a subset of users see when accessing the Command Center
- Automated process improvements for manual certificate installs on HTML5 gateway VMs
- Ongoing proactive security measures

VDS Setup

- Improved Azure NetApp Files orchestration
- Ongoing enhancements to gracefully handle Azure deployment variables
- New Active Directory deployments will automatically have the Active Directory Recycle Bin feature enabled
- Improved deployment orchestration for Google Cloud Platform

VDS 5.4 hotfix: Wed. October 28, 2020

Components: 5.4 Virtual Desktop Service

When: Wednesday October 28th, 2020 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

VDS Setup

- Bug fix for a scenario where network details couldn't be entered properly in the deployment wizard

VDS 5.4 release: Thurs., October 22, 2020

Components: 5.4 Virtual Desktop Service

When: Thursday October 22nd, 2020 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

VDS

- If a VDS admin deletes a AVD host pool, automatically unassign users from that host pool
- Introduce improved, renamed automation driver – Command Center – in CWMGR1
- Bug fix for Workload Scheduling behavior in a Bug fix for updating site details when that resides in AWS
- Bug fix for Wake on Demand activation with specific Live Scaling settings applied
- Bug fix for creating a second site when incorrect settings were in place in the original site
- Ease of use improvements for Static IP details in DC Config
- Naming convention update to admin permissions – update Data Center permissions to Deployment permissions
- Update to reflect that fewer database entries are needed in single server deployment builds
- Update to manual AADDS deployment process update to streamline permissions
- Bug fix for reporting in VDS when changing the dates the report should return
- Bug fix for creating a Windows Server 2012 R2 template via Provisioning Collections
- Assorted performance improvements

VDS Setup

- Deployment automation enhancements for primary domain controller and DNS components of a deployment
- Assorted updates to support selecting from a list of available networks in a future release

Cost Estimators

- Improved handling of adding SQL to VMs

REST API

- New API call to identify which Azure regions are valid and available for a subscription
- New API call to identify if a customer has Cloud Insights access
- New API call to identify if a customer has Cloud Insights activated for their Cloud Workspace environment

VDS 5.4 hotfix: Wed., October 13, 2020

Components: 5.4 Virtual Desktop Service

When: Wednesday October 13th, 2020 at 10pm -11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Cost Estimators

- Bug fix for an issue where a scenario in the Azure Cost Estimator where RDS VMs applied OS pricing improperly
- Bug fix for a scenario where selecting storage PaaS services in the Azure Cost Estimator and Google Cost Estimator resulted in an inflated price per VDI user

VDS 5.4 release: Thurs., October 8, 2020

Components: 5.4 Virtual Desktop Service

When: Thursday October 8th, 2020 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

VDS

- Stability enhancements when creating a VM during hours in which Workload Scheduling is applied
- Bug fix for a display issue when creating new App Services
- Dynamically confirm the presences of .NET and ThinPrint for non-Azure deployments
- Bug fix for a display issue when reviewing the provisioning status of a Workspace
- Bug fix for creating a VM in vSphere with a specific combination of settings
- Bug fix for a checkbox error under a set of permissions
- Bug fix for a display issue where duplicate gateways were being displayed in DCConfig
- Branding updates

Cost Estimators

- Update to the display the CPU scaling details per workload type

VDS 5.4 hotfix: Wed., September 30, 2020

Components: 5.4 Virtual Desktop Service

When: Wednesday September 30th, 2020 at 9pm -10pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

VDS

- Bug fix for an issue where a subset of App Services VMs were improperly tagged as cache VMs
- Upgrade to underlying SMTP configuration to mitigate email relay account configuration issues
 - Note: as this is now a control plane service, this results in a slimmer deployment footprint with fewer permissions/components in a customer's tenant
- Bug fix to prevent an admin using DCConfig from resetting the a service account's password

VDS Setup

- Improved handling of environment variables for Azure NetApp Files deployments
- Enhanced deployment automation - improved handling of environment variables to ensure required PowerShell components are present

REST API

- Introduction of API support for Azure deployments to leverage an existing Resource Group
- Introduction of API support for existing AD deployments with different domain/NetBIOS names

VDS 5.4 release: Thurs., September 24, 2020

Components: 5.4 Virtual Desktop Service

When: Thursday September 24th, 2020 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

VDS

- Performance enhancement – the list of users for which Cloud Workspaces can be enabled will now populate faster
- Bug fix for handling site-specific AVD session host server imports
- Deployment automation enhancement - introducing an optional setting to direct AD requests to CWMGR1
- Improved handling of variables when importing servers to ensure that CWAgent is installed properly
- Introduce additional RBAC controls over TestVDCTools – require membership in the CW-Infrastructure group for access
- Fine tuning of permissions – grant admins in the CW-CWMGRAccess group access to registry entries for VDS settings
- Update for Wake on Demand for personal AVD host pools to reflect updates for the Spring Release – only power on the VM assigned to the user
- Update company code naming conventions in Azure deployments – this prevents an issue where Azure Backup cannot restore from a VM that starts with a number
- Replace deployment automation's use of Sendgrid for SMTP transmission with a global control plane to resolve an issue with SendGrid's back-end - this results in a slimmer deployment footprint with fewer permissions/components

VDS Setup

- Updates to VM quantity selections available in multi-server deployments

REST API

- Add Windows 2019 to GET /DataCenterProvisioning/OperatingSystems method
- Auto populate VDS admin first and last names when creating admins via the API method

Cost estimators

- Introduction of Google Cost Estimator and a prompt for which hyperscaler you want to use for your estimate - Azure or GCP
- Introduction of Reserved Instances in the Azure Cost Estimator
- Updated list of services available per updated Azure products available by region

VDS 5.4 release: Thurs., September 10, 2020

Components: 5.4 Virtual Desktop Service

When: Thursday September 10th, 2020 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Improved enforcement mechanism to confirm FSLogix is installed
- Support for multi-server configurations for Existing AD deployments
- Reduce the number of API calls used to return a list of Azure templates
- Improved management of users in AVD Spring Release / v2 host pools
- Referential link update in server resource nightly report
- Fix for changing administrative passwords to support improved, slimmer permission sets in AD
- Bug fix for creating VMs from a template via tools on CWMGR1
- Searches in VDS now point to content on docs.netapp.com
- Response time improvements for end users accessing the VDS admin interface with MFA enabled

VDS Setup

- Post-provisioning link now points to instructions here
- Updated choices for platform configuration for existing AD deployments
- Improvements to automated processes for Google Cloud Platform deployments

VDS 5.4 hotfix: Tues., September 1, 2020

Components: 5.4 Virtual Desktop Service

When: Tuesday September 1st, 2020 at 10pm -10:15pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

VDS Setup

- Bug fix for a referential link in the AVD tab

VDS 5.4 release: Thurs., August 27, 2020

Components: 5.4 Virtual Desktop Service

When: Thursday August 27th, 2020 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Introduction of the ability to use the VDS interface to automatically update AVD host pools from the Fall Release to the Spring release
- Streamlined automation to reflect recent updates resulting in a slimmer permission set required
- Deployment automation enhancements for GCP, AWS and vSphere deployments
- Bug fix for a Scripted Events scenario where date and time info was being displayed as current date and time
- Bug fix for deploying large quantities of AVD session host VMs at the same time
- Support for an increased amount of Azure VM types
- Support for an increased amount of GCP VM types
- Improved handling of variables during deployment
- Bug fix for vSphere deployment automation
- Bug fix for a scenario when disabling a Cloud Workspace for a user returned an unexpected result
- Bug fix for 3rd party apps and RemoteApp app use with MFA enabled
- Increased Service Board performance when a deployment is offline
- Updates to reflect NetApp logo/phrasing

VDS Setup

- Introduction of a multi-server deployment option for native/greenfield Active Directory deployments
- Further deployment automation enhancements

Azure Cost Estimator

- Release of Azure Hybrid Benefits functionality
- Bug fix for a display issue when entering custom name information into VM details
- Bug fix for adjusting storage details in a specific sequence

VDS 5.4 hotfix: Wed., August 19, 2020

Components: 5.4 Virtual Desktop Service

When: Wednesday August 19th, 2020 at 5:20pm – 5:25pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

VDS Setup

- Bug fix for variable handling to facilitate flexible automation
- Bug fix for DNS handling in a single deployment scenario
- Reduced membership requirements of CW-Infrastructure group

VDS 5.4 hotfix: Tues., August 18, 2020

Components: 5.4 Virtual Desktop Service

When: Tuesday August 18th, 2020 at 10pm – 10:15pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Azure Cost Estimator

- Bug fix for handling adding additional drives on certain VM types

VDS 5.4 release: Thurs., August 13, 2020

Components: 5.4 Virtual Desktop Service

When: Thursday August 13th, 2020 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Add Connect to Server option for AVD session hosts from AVD module
- Bug fix for a subset of scenarios where additional admin accounts cannot be created
- Update naming convention for resource defaults – change Power User to VDI User

VDS Setup

- Automatically validate pre-approved network settings, further streamlining deployment workflows
- Reduced permission set required for existing AD deployments
- Allow domain names longer than 15 characters
- Text layout fix for a unique combination of selections
- Allow Azure deployments to continue if the Sendgrid component presents a temporary error

VDS Tools and Services

- Proactive security enhancements behind the scenes
- Additional Live Scaling performance enhancements
- Enhanced support for hyperscaler deployments with hundreds of sites
- Bug fix for a scenario where deploying multiple VMs in a single command only partially succeeded
- Improved message prompts when assigning invalid paths as the target for Data, Home and Profile data locations
- Bug fix for a scenario where creating VMs via Azure Backup didn't function as intended
- Additional deployment validation steps added to GCP and AWS deployment process

- Additional options for managing external DNS entries
- Support for separate Resource Groups for VMs, VNETs, Services like Azure NetApp Files, Log Analytics Workspaces
- Minor back-end enhancements to the provisioning collection/image creation process

Azure Cost Estimator

- Add Ephemeral OS Disk support
- Improved tooltips for storage selections
- Disallow a scenario where a user became able to enter negative user counts
- Display the file server when using both AVD and File Server selections

VDS 5.4 hotfix: Mon., August 3, 2020

Components: 5.4 Virtual Desktop Service

When: Monday August 3rd, 2020 at 11pm – 11:05pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

VDS Tools and Services

- Improved handling of variables during deployment automation

VDS 5.4 release: Thurs., July 30, 2020

Components: 5.4 Virtual Desktop Service

When: Thursday July 30th, 2020 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Proactive security enhancements behind the scenes
- Improved performance monitoring behind the scenes
- Bug fix for a scenario where creating a new VDS admin presents a false positive alert

VDS Setup

- Reduced permission sets applied to administrative accounts during the deployment process in Azure
- Bug fix for a subset of trial account signups

VDS Tools and Services

- Improved handling of FSLogix install process
- Proactive security enhancements behind the scenes
- Improved data point collection for concurrent usage
- Improved handling of certificates for HTML5 connections
- Adjustment to DNS section layout for improved clarity

- Adjustment to Solarwinds monitoring workflow
- Updated handling of static IP addresses

Azure Cost Estimator

- Ask if the customer's data needs to be HA and if so, define if cost and labor savings are available by leveraging a PaaS service like Azure NetApp Files
 - Update and standardize default storage type for both AVD & RDS workloads to Premium SSD
 - Behind the scenes performance enhancements
 - *
- == VDS 5.4 hotfix: Thurs., July 23, 2020

Components: 5.4 Virtual Desktop Service

When: Thursday July 23rd, 2020 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

VDS Setup

- Automation enhancements for DNS settings in Azure deployments
- General deployment automation checks and improvements

VDS 5.4 release: Thurs., July 16, 2020

Components: 5.4 Virtual Desktop Service

When: Thursday July 16th, 2020 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Proactive security enhancements behind the scenes
- Streamlining the AVD App Group provisioning process by auto-selecting the AVD Workspace if only one AVD Workspace is present
- Performance improvements in the Workspace module via paginating Groups under the Users and Groups tab
- If VDS admins select Azure in the Deployments tab, direct the user to log into VDS Setup instead

VDS Setup

- Proactive security enhancements behind the scenes
- Improved layout to streamline the deployment workflow
- Enhanced descriptions for deployments using an existing Active Directory structure
- General enhancements and bug fixes for deployment automation

VDS Tools and Services

- Bug fix for TestVDCTools performance in single server deployments

REST API

- Usability enhancement for API consumption for Azure deployments – return usernames gathered even if first names are not defined on the user in Azure AD

HTML5 Login Experience

- Bug fix for Wake on Demand for session hosts leveraging the AVD Spring Release (AVD v2)
- Updates to reflect NetApp branding/phrasing

Azure Cost Estimator

- Display pricing dynamically by region
- Display whether relevant services are available in the region select to ensure that users understand whether the functionality desired will be available in that region. Those services are:
 - Azure NetApp Files
 - Azure Active Directory Domain Services
 - NV and NV v4 (GPU enabled) Virtual Machines

VDS 5.4 release: Fri., June 26, 2020

Components: 5.4 Virtual Desktop Service

When: Thursday June 26, 2020 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

As of Friday July 17th, 2020 the release of v5.4 is supported as a production release.

VDS Client for Windows Release Notes

Date: Thursday July 29th, 2020 at 11pm Eastern

Impact: Users will see the VDS Client for Windows update the next time they launch it

Improvements

- Streamline the installation process - new end users will no longer have to accept terms and conditions when installing the VDS Client for Windows
- Add a confirmation during the install process to confirm that the end user's device is able to access the location where auto-updates originate

Date: Thursday May 27, 2020 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

Bug Fixes

- Improved clarity in the error message displayed if the password provided is not long enough

Date: Thursday May 13, 2020 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Additional automation to ensure resource availability for end users

Updates

- The URL that is required for access to automatic updates is changing. If you are not actively safelisting inbound traffic you will not need to make any changes.
 - All end users will continue to have access to their desktops even if no changes are made
 - Organizations actively safelisting inbound traffic will need to ensure that end user devices have access to the new URLs above to ensure access to automatic updates
 - The current sources for updates are:
 - Primary: cwc.cloudworkspace.com
 - Secondary: cloudjumper.com
 - The new sources for updates will be:
 - Primary: bin.vdsclient.app
 - Secondary: cwc.cloudworkspace.com
 - New users installing the Cloud Workspace Client for Windows will still need access to the URLs listed [here](#)

Date: Thursday April 29, 2020 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

(No updates this release)

Date: Thursday April 15, 2020 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

Bug Fixes

- Resolve an issue where network test results wouldn't be sent as intended

Date: Thursday April 1, 2020 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Update to RemoteApp applications - no longer prompt for credentials when users launch individual apps
- Update to allow end users to toggle between using ThinPrint and Windows printer redirection for printing
- Update to allow the VDS Client for Windows Designer users to exclude printing redirection services

VDS 5.4 release: Thurs., January 21, 2021

Components: 5.4 Virtual Desktop Service

When: Thursday January 21st, 2021 at 10pm - 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Improved experience for end users – better handling of users imported from external domains

Date: Thursday June 11, 2020 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Update the latest AVD RDP Client available for installation

Date: Thursday May 28, 2020 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Updates to reflect NetApp branding/phrasing. Note – this new branding will be applied for:
 - New VDS Client downloads
 - Existing, unedited VDS Client for Windows installs
 - Existing custom-edited/branded clients will only receive a new banner image if it was never customized. If the banner image was customized, it will remain as-is. All other colors and phrasing will remain the same.

Date: Thursday May 14, 2020 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

- No updates this release cycle.

Date: Thursday April 30, 2020 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

Bug Fixes

- Bug fix for a subset of scenarios where self service password reset was not presented

Date: Thursday April 16, 2020 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

- No updates this release cycle.

Date: Thursday April 2, 2020 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

- No updates this release cycle.

Date: Thursday March 19, 2020 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

- No updates this release cycle.

Date: Thursday, March 5, 2020 at 10pm Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Graceful handling of a fringe bug with the RDP protocol where legacy credential types mixed with the most current patches on a RDS gateway results in an inability to connect to session hosts
 - If the end user's workstation is set up (whether by an external admin, internal customer admin or via the workstation's default settings) to use legacy credential types, there is a slim possibility this could have impacted users prior to this release
- Point the Info button in the Cloud Workspace Client Designer to an updated documentation source
- Improved auto-update process for the Cloud Workspace Client Designer

Date: Thursday, February 20, 2020 at 10pm Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Proactive enhancements to security, stability and scalability

Considerations

- The Cloud Workspace Client for Windows will continue to auto-update as long as a user launches it prior to 4/2. If a user does not launch the Cloud Workspace Client for Windows prior to 4/2 their connection to their desktop will still function, but they will need to uninstall and reinstall the Cloud Workspace Client for Windows to resume auto-update functionality.
- If your organization uses web filtering, please safelist access to cwc.cloudworkspace.com and cwc-cloud.cloudworkspace.com so that auto-update functionality remains in place

Date: Thursday January 9, 2020 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

- No updates this release cycle.

Date: Thursday December 19, 2019 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

- No updates this release cycle.

Date: Monday December 2, 2019 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

- No updates this release cycle.

Date: Thursday, November 14, 2019 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Improved clarity for the reason a user would see a 'your services are currently offline' message. The potential causes for a message appearing are:
 - Session host server is scheduled to be offline and user does not have Wake on Demand permissions.
 - If the user was using the Cloud Workspace Client, they would see: "Your services are currently scheduled to be offline, please contact your administrator if you need access."
 - If the user was using the HTML5 login portal, they would see: "Your services are currently scheduled to be offline. Please contact your administrator if you need access."
 - Session host server is scheduled to be online and user does not have Wake on Demand permissions.
 - If the user was using the Cloud Workspace Client, they would see: "Your services are currently offline, please contact your administrator if you need access."
 - If the user was using the HTML5 login portal, they would see: "Your services are currently offline. Please contact your administrator if you need access."
 - Session host server is scheduled to be offline and user has Wake on Demand permissions.
 - If the user was using the Cloud Workspace Client, they would see: "Your services are currently offline, please contact your administrator if you need access."
 - If the user was using the HTML5 login portal, they would see: "Your services are currently scheduled to be offline. Click START to bring them online and connect."
 - Session host server is scheduled to be online and user has Wake on Demand permissions.
 - If the user was using the Cloud Workspace Client, they would see: "Please allow 2-5 minutes for your Workspace to start."
 - If the user was using the HTML5 login portal, they would see: "Your services are currently offline. Click START to bring them online and connect."

Date: Thursday, October 31, 2019 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

- No updates this release cycle.

Date: Thursday, November 17, 2019 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Add AVD elements:

Date: Thursday October 3, 2019 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Improved handling of code signing certificates

Bug Fixes

- Fix an issue where Users accessing RemoteApp that didn't have any apps assigned to them saw an error
- Resolve an issue where a user loses their internet connection in the middle of logging into their virtual desktop

Date: Thursday September 19, 2019 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Add AVD elements:
 - If the end user has access to AVD resources, present a AVD tab
 - The AVD tab will provide options to:
 - Install the AVD RD Client, if it isn't already installed
 - If the AVD RD Client is installed, launch the RD Client
 - Launch Web Client to take the user to the AVD HTML5 login page
 - Click Done to go back to the prior page

Date: Thursday, September 5, 2019 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

- No updates this release cycle.

Date: Thursday, August 22, 2019 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

- No updates this release cycle.

Date: Thursday, August 8, 2019 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

- No updates this release cycle.

Date: Thursday, July 25, 2019 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

- No updates this release cycle.

Date: Thursday, July 11, 2019 at 11pm Eastern

Impact: Users will see the RDP client update the next time they launch it

- No updates this release cycle.

Date: Friday, June 21, 2019 at 4am Eastern

Impact: Users will see the RDP client update the next time they launch it

- No updates this release cycle.

Date: Friday, June 7, 2019 at 4am Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Enable Cloud Workspace Client to automatically launch RDP connections regardless of what the file type association for .rdp files is set to

Date: Friday, May 24, 2019 at 4am Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Improved performance during the sign in process
- Reduced load time on launch

Date: Friday, May 10, 2019 at 4am Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Improved performance during the sign in process
- Reduced load time on launch

Date: Friday, April 12, 2019 at 4am Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Enhanced login speed for Wake on Demand
- After the successful launch of the Cloud Workspace Client for Windows, we will be removing the Feedback button to free up space in the User interface

Bug Fixes

- Resolve an issue where the Sign In button was unresponsive after an unsuccessful Wake on Demand action

Date: Friday, March 15, 2019 at 4am Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- Allow for Admins using the Cloud Workspace Client for Windows to provide a Support email address OR a phone number, not to require both
- Ensure that the HTML5 URL provided in Cloud Workspace Client is a valid URL – if not, this will default to <https://login.cloudjumper.com>
- Streamlining the process of applying updates for End Users

Date: Friday, February 29, 2019 at 4am Eastern

Impact: Users will see the RDP client update the next time they launch it

Improvements

- The AppData folder has been moved for clarity from c:\users\<username>\appdata\local\RDPClient to c:\users\<username>\appdata\local\Cloud Workspace
- Implemented a mechanism to streamline upgrade paths if a User has not updated their client in multiple releases
- Enhanced log details has been enabled for Users working with the Beta version of the client

Bug Fixes

- There will no longer be multiple lines displayed during the update process

Date: Friday, February 15, 2019 at 4am Eastern

Impact: Users will see the RDP client update when they launch it

Improvements

- Enable Silent/Quiet installation options for remote installations
 - Install flags are as follows:
 - /s or /silent or /q or /quiet
 - These flags will install the client silently and in the background – the client will not launch after installation is complete
 - /p or /passive
 - Either of these will show the installation process, but not require any input and the client will launch after installation is complete
 - /nothinprint
 - Excludes ThinPrint from the installation process

- Registry entries have been added to HKLM\Software\CloudJumper\Cloud Workspace Client\Branding:
 - ClipboardSharingEnabled: True/False – allows or disallows clipboard redirection
 - RemoteAppEnabled: True/False – allows or disallows access to RemoteApp functionality
 - ShowCompanyNameInTitle: True/False – indicates whether or not the company name is displayed
- The following can be added to c:\Program Files (x86)\Cloud Workspace:
 - banner.jpg, banner.png, banner.gif or banner.bmp and this will be displayed in the client window.
 - These images should be in the 21:9 ratio

Bug Fixes

- The Registered symbol has been adjusted
- Empty phone and email entries on the Help page have been fixed

Previous versions

Virtual Desktop Service – Version 5.3



There will be no further recurring releases for v5.3 of VDS – all releases will be considered hotfixes.

VDS 5.3 release: Thurs., December 17, 2020

Components: 5.3 Virtual Desktop Service

When: Thursday December 17th, 2020 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.



The next release cycle will be on Thursday January 7th, 2021 instead of New Year's Eve 2020.

Virtual Desktop Service

- Update SMTP service to leverage Postmark

VDS 5.3 release: Thurs., October 22, 2020

Components: 5.3 Virtual Desktop Service

When: Thursday October 22nd, 2020 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

VDS

- Bug fix for scenarios where the MFA agent resides in a folder with legacy IIT naming conventions

VDS 5.3 release: Thurs., October 8, 2020

Components: 5.4 Virtual Desktop Service

When: Thursday October 8th, 2020 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

VDS

- Bug fix for Provisioning Collections – hypervisor template not auto-selected

VDS 5.3 release: Thurs., September 10, 2020

Components: 5.3 Virtual Desktop Service

When: Thursday September 10th, 2020 at 10pm - 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Reduce the number of API calls used to return a list of Azure templates
- Referential link update in server resource nightly report
- Fix for changing administrative passwords to support improved, slimmer permission sets in AD

VDS 5.3 release: Thurs., August 27, 2020

Components: 5.3 Virtual Desktop Service

When: Thursday August 13th, 2020 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Bug fix for a Scripted Events scenario where date and time info was being displayed as current date and time

Azure Cost Estimator

- Release of Azure Hybrid Benefits functionality
- Bug fix for a display issue when entering custom name information into VM details

VDS 5.3 release: Thurs., August 13, 2020

Components: 5.3 Virtual Desktop Service

When: Thursday August 13th, 2020 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Azure Cost Estimator

- Add Ephemeral OS Disk support
- Improved tooltips for storage selections
- Disallow a scenario where a user became able to enter negative user counts
- Display the file server when using both AVD and File Server selections

VDS 5.3 release: Thurs., July 30, 2020

Components: 5.3 Virtual Desktop Service

When: Thursday July 30th, 2020 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Bug fix for a subset of scenarios where AVD Diagnostics were not displaying properly

Azure Cost Estimator

- Ask if the customer's data needs to be HA and if so, define if cost and labor savings are available by leveraging a PaaS service like Azure NetApp Files
- Update and standardize default storage type for both AVD & RDS workloads to Premium SSD
- Behind the scenes performance enhancements

VDS 5.3 release: Thurs., July 16th, 2020

Components: 5.3 Virtual Desktop Service

When: Thursday July 16, 2020 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Proactive security enhancements behind the scenes
- Performance improvements in the Workspace module via paginating Groups under the Users and Groups tab

VDS Setup

- As new automation options are available, update for deployments selecting Azure Active Directory Domain Services (AADDS) to ensure the use of the Standard service tier
- Update to reflect a change to a Microsoft ARM API call

HTML5 Login Experience

- Updates to reflect NetApp branding/phrasing

Azure Cost Estimator

- Display pricing dynamically by region
- Display whether relevant services are available in the region select to ensure that users understand whether the functionality desired will be available in that region. Those services are:
 - Azure NetApp Files
 - Azure Active Directory Domain Services
 - NV and NV v4 (GPU enabled) Virtual Machines

VDS 5.3 release: Thurs., June 25, 2020

Components: 5.3 Virtual Desktop Service

When: Thursday June 25, 2020 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual

Desktop Service will remain available.

Virtual Desktop Service

- Updates to reflect NetApp branding/phrasing
- Bug fix for an isolated scenario where the list of users was not populating as expected
- Bug fix for a scenario where manual deployments were receiving a GPO configuration that was only partially correct

VDS Setup Wizard

- Support for American Express
- Updates to reflect NetApp branding/phrasing

REST API

- Ongoing enhancements to gather and display list data faster

VDS 5.3 release: Thurs., June 11, 2020

Components: 5.3 Virtual Desktop Service

When: Thursday June 11, 2020 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Proactive API processing enhancements
- Continued proactive hardening of platform elements

Cloud Workspace Tools and Services

- Ongoing improvements to Live Scaling triggers
- Improved auto-correction of issues identified when migrating a deployment from vCloud to vSphere

VDS 5.3 Hotfix: Thurs. May 7, 2020

Components: 5.3 Virtual Desktop Service

When: Wednesday June 3rd, 2020 at 10:00am – 10:30am Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Cloud Workspace Tools and Services

- Bug fix for an automated element of platform deployment automation. This only applies brand new deployments – there will be no impact to existing deployments.
- Bug fix for deployments into an existing Active Directory structure

VDS 5.3 release: Thurs., May 28, 2020

Components: 5.3 Virtual Desktop Service

When: Thursday May 28, 2020 at 10pm – 11pm Eastern

Impact: Access to desktops and application services for End Users will remain uninterrupted. Access to Virtual Desktop Service will remain available.

Virtual Desktop Service

- Updates to reflect NetApp branding/phrasing
- Performance improvements for the Workspace module
- Proactive stability enhancement VDS functions powered by frequently used API calls

Virtual Desktop Service Deployment

- Further streamlining of the footprint of the VDS platform in Azure deployments
- Bug fix for an optional scenario when deploying into an existing Active Directory Structure

Virtual Desktop Service Tools and Services

- Ongoing improvements to the way the number of users logged into a server is identified for Live Scaling

Virtual Desktop Service Web Client

- Updated branding to reflect NetApp branding/phrasing
- Support for shortening URLs saved as favorites that are longer than the default Web Client links to the default Web Client links (cloudworkspace.com/login/ to cloudworkspace.com, for example)

Azure Cost Estimator

- Add SQL Server options for more VM series/sizes
- Update to the way IP address pricing is displayed – don't display the IP address cost unless additional IP addresses are added

CWMS 5.3 release: Thurs., May 14, 2020

Components: 5.3 Cloud Workspace Management Suite

When: Thursday May 14, 2020 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Azure Cost Estimator

- Updated messaging to reflect NetApp branding/phrasing
- Updated platform server to reflect D2s v3 use
- Updated Windows 10 Enterprise E3 license details and price point
- Change default storage choice to Azure NetApp Files

CWMS 5.3 Hotfix: Thurs. May 7, 2020

Components: 5.3 Cloud Workspace Management Suite

When: Friday May 8th, 2020 at 10:15am – 10:30am Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Tools and Services

- Bug fix for the method in which DNS records are set for a specific combination of settings during the deployment process

CWMS 5.3 release: Thurs., April 30, 2020

Components: 5.3 Cloud Workspace Management Suite

When: Thursday April 30, 2020 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Improved session tracking to enable a future update – the option to preview future features
- Update to Scripted Events to allow for increased flexibility in applications and activities
- Bug fix for a specific combination of Provisioning Collections configurations

Cloud Workspace Tools and Services

- Enable the ability to set Workload Scheduling per AVD host pool
- Improved process of creating new deployments into an existing AD structure
- Enable the ability to assign Data/Home/Profile data paths for organizations using Azure Files
- Enable the ability to manage Resource Pools
- Improved handling of special characters in the deployment wizard process
- Adjustments to automated HTML5 components as a part of deployment for RDS (not AVD) workloads

REST API

- Updated list of Azure regions available for deployment
- Improved handling of Azure Backup integration for servers with the TSData role
- Resolve an issue in subset of scenarios where a failed login result in two failed login attempts being logged

CWA Setup

- Per Azure best practices, enforce that the Subnet IP details are within a Private IP address range.
Accepted Private IP ranges are:
 - 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

HTML5 Login Experience

- Behind the scenes hosting enhancements for <https://login.cloudworkspace.com> and <https://login.cloudjumper.com>. Note: there will be no impact for custom branded HTML5 login portals.
- Bug fix for a subset of scenarios where self service password reset was not presented

CWMS 5.3 Hotfix: Wedn. April 22, 2020

Components: 5.3 Cloud Workspace Management Suite

When: Wednesday April 22nd, 2020 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Performance upgrade to accommodate increased Customer use

CWMS 5.3 release: Thurs., April 16, 2020

Components: 5.3 Cloud Workspace Management Suite

When: Thursday April 16, 2020 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Continual enhancements to validation of AVD host pool VM creation (accounting for Azure process times due to surge in Azure activity due to COVID-19)
- AVD stability improvement when initializing AVD – if the AVD tenant name is not unique to AVD globally, CloudJumper will replace it with an updated string unique to the Deployment/tenant.
- Include support for special characters in email addresses in CWMS password reset functionality
- Bug fix for a subset of scenarios when adding apps to an AVD RemoteApp app group didn't pull apps from the Start menu
- Bug fix for a subset of the user activity report
- Remove the requirement for a description of a AVD host pool (remains as an optional field)
- Bug fix for a single fringe scenario where VMs in a shared host pool were tagged as VDI VMs

CWA Setup

- Additional support for order codes for Distributor workflows

Cloud Workspace Tools and Services

- Enhancements to unmanaging VMs that are managed by the Solarwinds Orion RMM tool to accommodate Workload Scheduling

CWMS 5.3 release: Thurs., April 2, 2020

Components: 5.3 Cloud Workspace Management Suite

When: Thursday April 2, 2020 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Activity History fix resolving a display issue for regional deployments where date localization prevented some Activity History from being visible in CWMS

- Provisioning collection enhancement to allow for images of any size
- Bug fix for AADDS deployments in Azure tenants with multiple domains – newly created users would previously use the primary Azure domain rather than matching the Workspace's login ID
- Bug fix for activity history when updating a username – the functionality is working as expected, but the previous username was not being displayed correctly

CWA Setup

- Improved handling of MFA on CWMS accounts used during registration
- Reduced permissions applied during deployment

Cloud Workspace Tools and Services

- Reduced permissions required for ongoing services/automation
- Process enhancements to reduce resource consumption on CWMGR1

REST API

- Bug fix for activity history when updating a username

CWMS 5.3 Hotfix: Tues. March 24, 2020

Components: 5.3 Cloud Workspace Management Suite

When: Tuesday March 24th, 2020 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Azure Cost Estimator

- Updated description of AVD User types and the programs they run per Microsoft documentation
- Increased clarity for CWMS licensing

CWMS 5.3 release: Thurs., March 19, 2020

Components: 5.3 Cloud Workspace Management Suite

When: Thursday March 19, 2020 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Connect to Server enhancement for multi-site deployments – automatically detect which site the CWMS admin is connecting to and process the connection
- Enabling migration mode now disables Live Scaling
- Bug fix for enabling new Cloud Workspace Services for an existing Client

CWA Setup

- Behind the scenes improvements to the deployment wizard

CWMS 5.3 release: Thurs., March 5, 2020

Components: 5.3 Cloud Workspace Management Suite

When: Thursday March 5, 2020 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Performance improvement for the Master Client Report
- Remove the delete function from a VM that didn't get properly created, as it cannot be deleted if it was never created

Cloud Workspace Tools and Services

- Bug fix for gracefully handling multi-site deployments where DC Config settings are not properly configured
- Bug fix for multi-site deployments where vSphere sites have resource allocation types set to Fixed

HTML 5 Portal

- Process enhancement for users logging in with AVD credentials

Azure Cost Estimator

- Clarity improvement for Live Scaling
- Phrasing adjustments to match Microsoft AVD messaging
- Bug fix for Workload Scheduling and Live Scaling savings details in heavily customized quotes

CWMS 5.3 release: Thurs., February 20, 2020

Components: 5.3 Cloud Workspace Management Suite

When: Thursday February 20, 2020 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Switch the word SDDC to Deployment in the VM Resource tab of the Workspaces module

CWA Setup

- Streamlining the process of applying policies during deployment
- Increased security for new deployments using Azure Active Directory Domain Services
- Increased security for new deployments – require defined subnet isolation (as opposed to flat subnets) during deployment
- Bug fix for RDS (non-AVD) deployments when applying ThinPrint licensing
- Bug fix for proper handling of whether ThinPrint is installed in DC Config
- Additional checks and validation for organizations opting to leverage FTP functionality

Cloud Workspace Tools and Services

- Bug fix for automated actions when a deployment with multiple sites has a site that is configured incorrectly
- Bug fix for an instance where deleting a VM didn't properly clear out the VM behind the scenes
- Functionality improvements and bug fixes when testing hypervisor connectivity in DC Config

REST API

- Performance improvements when displaying the list of users for an organization
- Performance improvements when displaying the list of applications for an organization
- Improved functionality when adding Users to AVD App Groups:
- Limit the number of users imported to 425
- If attempting to import more than 425 users, proceed with the import of the first 425 users and display that AVD's limit for user imports is 425 and that they can proceed with additional imports in 5 minutes
- Update to reflect that the number of users in a group is the number of Cloud Workspace users in a group as opposed to the total number of users in a group (which may be less when deploying into an existing Active Directory structure)
- Enable application assignments via security group for named users that are a member of the group (nested groups will not receive the app assignment)

Azure Cost Estimator

- Add a link at the bottom of the page so that users can request assistance
- Default Azure NetApp Files to the Premium tier
- Add Premium SSD to the choices for Fileserver storage type
- Update text for Azure Active Directory Domain Services – change from AADDS to Azure AD Domain Services
- Update text for Active Directory – change from Windows Active Directory VM(s) to Windows Server Active Directory

CWMS 5.3 Hotfix: Thurs., February 13, 2020

Components: 5.3 Cloud Workspace Management Suite

When: Thursday February 13, 2020 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Azure Cost Estimator

- Bug fix for pricing error when using E-series VMs in a subset of scenarios

CWMS 5.3 release: Thurs., February 6, 2020

Components: 5.3 Cloud Workspace Management Suite

When: Thursday February 6, 2020 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Improved provisioning status details during the VM creation process
- Improved handling of automation for newly created session host VMs that are part of a AVD host pool
- Performance improvement to the User Activity report when including “Only Server Access Users”

Cloud Workspace Tools and Services

- Bug fix for data path management when admins manually edit user accounts in traditional (non-Azure) Active Directory
- Improved Workload Scheduling stability in nuanced scenarios

Azure Cost Estimator

- Describe the specific savings achieved via Workload Scheduling and Live Scaling separately vs. combined
- Display the “S” versions of servers in order to support Premium (SSD) storage
- Improved layout for printed estimates
- Bug fix for an issue where SQL server pricing was not being calculated correctly

CWMS 5.3 release: Thurs., January 23, 2020

Components: 5.3 Cloud Workspace Management Suite

When: Thursday January 23, 2020 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Redirect the older <https://iit.hostwindow.net> site to the modern <https://manage.cloudworkspace.com>
- Bug fix for a subset of CWMS admins logging in via IE 11
- Correct a visual issue where deleting an API user correctly deleted them behind the scenes, but was were not showing as deleted in CWMS
- Streamline the process of clearing out Subscriptions so that you can re-provision a new/test environment
- Service board enhancement – only look at session host servers that are online for icons to place for application shortcuts

Cloud Resource App

- Support importing users from an OU or Active Directory security group via command line

Cloud Workspace Tools and Services

- Live Scaling enhancements behind the scenes

CWA Setup

- Improved handling for scenarios when the account used during the CWA Setup process has MFA applied

Azure Cost Estimator

- Update VM sizing defaults to mirror Microsoft's recommendations

CWMS 5.3 release: Thurs., January 9, 2020

Components: 5.3 Cloud Workspace Management Suite

When: Thursday January 9, 2020 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Updating phrasing in the email admins receive after creating a new Workspace to reflect updated links
- Bug fix for an issue where servers were not appearing in the Servers list if a series of folder permissions errors existed
- Bug fix for servers were not appearing in the Servers list if a resource pool was not present in the Resource Pools table in CWMGR1

Cloud Resource App

- Support importing users from an Active Directory security group.
- Enhanced validation – ensure the proper command line parameter is being used for command line argument/servers
- Enhanced validation – check for duplicate users when importing from command line
- Enhanced validation – ensure the servers being imported belong to the site specified when importing from command line

REST API

- Additional behind the scenes security enhancements

Cloud Workspace Tools and Services

- Enhanced command processing stability behind the scenes
- Workload Scheduling and Live Scaling enhancements behind the scenes
- Additional Workload Scheduling and Live Scaling stability behind the scenes
- Updates and improvements to FSLogix in new deployments – redirect Downloads and Favorites into Profile Container to match best practices
- Additional Host Pool VM creation stability enhancements
- Introduce the ability to specify the gateway for new sites
- Improved automation validation for VMs
- Improved automated database management
- Improved handling of user creation if the action takes place at the exact same time VMs are powered down
- Streamlined handling of temporary disks in Microsoft Azure deployments
- Improved handling of resource allocation type for GCP deployments
- Bug fix for drive expansion in ProfitBricks data centers

- Improved stability for App Services based client creation
- Bug fix and stability improvements after converting a server from one role to another

CWMS 5.3 release: Fri., December 20, 2019

Components: 5.3 Cloud Workspace Management Suite

When: Friday December 20, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Tools and Services

- Fix for scenario where user activity logging does not record data successfully

CWMS 5.3 release: Thurs., December 19, 2019

Components: 5.3 Cloud Workspace Management Suite

When: Thursday December 19, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Improvements for CWMS availability monitoring
- Fix for an issue with AVD app group user modal where the username is not always selected properly when it contains capital letters
- Fix for pagination in the Users list for ‘User Support Only’ admin role members
- Fix for alignment of radio buttons in MFA setup dialog
- Improvement for Dashboard/Overview page load by removing service board dependency
- Fix for issue where admin users cannot reset their own passwords if they don’t have edit admin permissions
- Improvements collecting debug logging for future troubleshooting

Cloud Resource App

- Feature Enhancement: Allow import of users based on AD group membership.
- Feature Enhancement: Allow default logon identifier to be specified during import

Azure Cost Estimator

- Improve text and tooltip for storage under VMs

CWA Setup

- Release deployment workflow improvements

Cloud Workspace Tools and Services

- Improvement handling locking of the data server during new user creation
- Fix for scenario where a client is incorrectly flagged as a cache company during workload scheduling

- Fix to correctly update the company table when a organization is created without a workspace
- Fix for invalid characters appended to the AVD host pool name in the local control plane database
- Fix for issue with workload scheduling when a VM is listed in the local control plane database, but not the hypervisor
- Fix for issue preventing some VMs from having drives expanded automatically in Azure hypervisor
- Fix for client provisioning error 'Supplied data drive not valid'
- Fix for CWAgent install failure in certain scenarios
- Improvement for TestVDCTools to allow assignment of RDS Gateway URL during new site creation
- Fix for workload scheduling failure in some scenarios where it is set to 'disabled'
- Fix for issues starting servers when in still in cache
- Fix for failure to power on some VMs after automatic drive expansion
- Fix for issue managing folders/permissions when using Azure files or Azure NetApp Files

CWMS 5.3 release: Mon. December 2, 2019

Components: 5.3 Cloud Workspace Management Suite

When: Monday December 2, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Enhancements to automated FSLogix installs
- Updates and fixes to Live Scaling
- Add AMD (non-GPU) VMs to the drop-down list in CWMS
- Support for multiple tenants in the same AVD deployment

CWA Setup

- Clarity improvements in the Help/Support section CWA Setup

Azure Cost Estimator

- Bug fix for a scenario where electing to not include Microsoft licensing in the estimate continues to include it

Cloud Resource App

- Additional validation when using the Data Center site command line functionality
- New command line argument – /listserversinsite
- Configuration enhancement – when importing a company, now set the RDSH deployment to use the RDHS Gateway configured for the site

Cloud Workspace Tools and Services

- Updated vCloud support elements in DC Config
- Enhancement to TestVDCTools to correctly detect the server type in more specific scenarios

Components: 5.3 Cloud Workspace Management Suite

When: Thursday November 14, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Additional redundancy/high availability added behind the scenes
- Drop-down menus in CWMS will become searchable
- Performance improvements when using the Workspaces module
- Performance improvements when using the Servers section of the Workspaces module
- Display host pool name in the Servers section of the Workspaces module
- The Servers section of the Workspaces module will now be paginated, displaying 15 servers at a time
- Bug fix for a scenario where a subset of admins creating a new host pool would not see VM templates
- Bug fix for a scenario where navigating to a host pool, then a second host pool would sometimes display information from the first host pool
- Bug fix where a subset of admins could not log into an older version of CWMS
- Bug fix where navigating to AVD Diagnostics and then back to Workspaces displayed ‘page not found’
- Change friendly name of a user’s desktop (what appears in the AVD RDP client and in the blue bar at the top of the user’s session) to match the name of the host pool
- Servers must be manually added to the pool with a checkbox “Allow New Sessions” which is unchecked by default. Checkbox was previously checked by default.

CWA Setup

- Deployments will now automatically use FSLogix
- Add Azure Files as an optional storage target for Data, Home and Profile storage if the deployment will use Azure Active Directory Domain Services
- Deploy a package to support deployment automation where Azure tenants have enabled RBAC
- Install the latest version of Java and HTML5 licensing with each deployment
- Bug fix for when a subnet range was incorrectly calculated, causing a validation error prior to deployment

HTML5 Login Experience

- Update default branding to reflect the branding of the Cloud Workspace Client for Windows. A preview is available [here](#).
- Apply in-place branding updates to additional branded HTML5 login pages

Azure Cost Estimator

- Update the default storage tier for D4s v3 VMs (the default VM type for AVD) to Premium SSD in order to match Microsoft’s default setting

Cloud Resource App

- Add ability to pre-allocate a company code for use during import

CWMS 5.3 release: Thurs., October 31, 2019

Components: 5.3 Cloud Workspace Management Suite

When: Thursday October 31, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Update for users logging into iit.hostwindow.net (the URL for the older v5.2 deployments, of which there are very few) will see a prompt indicating them to navigate to manage.cloudworkspace.com (the URL for v5.3 and future deployments)
- Allow users to delete AVD host pools via CWMS
- Enhancement that allows for future branding enhancements in CWMS
- Bug fix for an issue when validating a VDI Provisioning Collection

Deployment Automation

- Improvements in automated issue resolution and behind the scenes process streamlining

HTML5 Login Experience

- We will be making a series of user experience enhancements for end users logging into their virtual desktops from login.cloudjumper.com or login.cloudworkspace.com:
- Allow the user to view the AVD host pools the user has access to
- Enable Wake on Demand functionality for users with the proper permissions, allowing them to log in and work at a time which a AVD session host VM is scheduled to be offline
- Enable Self Service Password Reset for users that have an email or phone number set in their user account in CWMS

Azure Cost Estimator

- Allow users to select Windows Active Directory VM(s) after selecting AVD for AD Connect use cases
- Update the default storage quantity for all VMs to 128 GB in order to match Microsoft's default value
- Update the default setting for uptime hours to 220 in order to match Microsoft's default value
- Update the names of the workload types to match the names that Microsoft changed them to

CWMS 5.3 release: Thurs., October 17, 2019

Components: 5.3 Cloud Workspace Management Suite

When: Thursday October 17, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Support for Server 2019 as the OS for an organization's Workspace
- Update to improve showing active users in a AVD Host Pool
- Allow for multiple Organizations/Workspaces under a AVD deployment
- Add "Update" button for editing multiple fields associated with an Admin
- Add "Update" button for editing company details and contact info
- Updated search function to use Flight School
- Updated links in the bottom of CWMS
- Allow for the use of a Validation Host Pool in AVD deployments – this will provide earlier access to AVD features prior to them being GA (production release)
- Typo fix in a prompt responding to an action taken by an admin on an AADDS deployment
- Bug fix for a prompt for an admin that does not have App Services permissions

REST API

- Support for Server 2019 as the OS for an organization's Workspace
- Bug fix for a scenario where call would return a client's services as offline

Deployment Automation

- Bug fix for auto-generating Data Center site name
- Log files summarized and moved to c:\Program Files to c:\ProgramData

Cloud Workspace Tools and Services

- Support for accessing templates from the Azure Shared Image Gallery
- Security improvement – reduced use of administrative accounts by changing the location of log files from c:\Program Files to c:\ProgramData (also an updated Microsoft best practice)
- Enhancement for data center site creation in VDCTools – sites can be created with a space in the name
- Feature add for Automatic Data Center Site creation – now able to automatically select the address range
- Feature add – add the configuration option to use unmanaged VHD files as templates
- Support for assigning a VM series/size in the provisioning collection
- Bug fix for a subset of scenarios where a license server setting was applied improperly
- Bug fix – deleting temp folders post deployment as intended
- Bug fix for a scenario when creating a server in Azure that has the same IP address as a VM already in use

Azure Cost Estimator

- Update pricing to reflect that AVD customers pay for Linux OS VMs instead of Windows OS VMs
- Added an option to include relevant Microsoft licensing
- Update to storage defaults used according to Microsoft's updated calculator (flat vs. user count)
- Add SQL pricing for D4s v3 VMs

- Bug fix for a display issue when editing VMs

CWMS 5.3 release: Thurs., October 3, 2019

Components: 5.3 Cloud Workspace Management Suite

When: Thursday October 3, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Workflow enhancement where clicking “Back” will return Users to the Workspace tab instead of the Organizations tab
- When provisioning Cloud Workspaces in Azure via CWMS, confirm that AADDS is successfully validated during the Validation step
- Support for usernames up to 256 characters

CWA Setup

- System improvements to remember linked Partner accounts in the event that the user links their account to CWMS, but did not complete the provisioning of the deployment the first time around
- Bug fix for a javascript error appearing when selecting a tenant to provision a Cloud Workspace deployment during the CSP workflow

Azure Cost Estimator

- Add an option to display or not display Microsoft licensing in the Azure Cost Estimator
- Not enabling this (default behavior) assumes that the organization already owns Microsoft licensing via their EA or existing Microsoft/Office 365 licensing
- Enabling this provides a more complete, TCO-level understanding of the solution
- Bug fix where hours of uptime was very slightly off when users were toggling uptime by increments of 15 minutes
- Bug fix for a scenario where users set the day to start in the afternoon/evening (PM setting) and end in the morning (AM setting)

CWMS 5.3 release: Thurs., September 19, 2019

Components: 5.3 Cloud Workspace Management Suite

When: Thursday September 19, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Default an Azure deployment’s Resource Allocation Type to Fixed; with the VM series/size selected being the VM defined by the Administrator in CWMS
- Add search functionality for User Activity audit functionality
- Improvement to bulk user creation process – enable the “force password change at next logon” feature when importing users

- Bug fix for incorrectly displaying session inactivity timeout warning after 5 minutes instead of 55 minutes
- User Support role fix – a subset of Admins with this role were unable to see the list of Users for their organization
- User sorting fix – sorting by username works as intended instead of sorting by status
- Added Heartbeat function to the Overview section of the Deployments tab, indicating the last time the deployment was polled to see if it is online
- Workflow improvements – when clicking “back” in the AVD module, you will now be taken the Workspaces module instead of the Organizations module
- Ensure Master Client Report is present; hide the non-applicable SPLA report for non-Master Software Partners

Cloud Workspace Tools and Services

- Remove the standard ThinPrint agent from Azure Virtual Desktop (AVD) servers in host pools, as this is not the supported ThinPrint agent for AVD. Instead, organizations should contact ThinPrint about their ezeep solution.
- Enhanced password encryption behind the scenes
- Bug fix for Password Enforcement Notification (PEN) where using the “change password at next logon” feature wasn’t working as intended if password expiration dates were set to null by an administrator in CWMGR1

Cloud Workspace for Azure Setup App

- Fix for international administrators – this no longer requires a State if the Country is not the United States.
- Apply CloudJumper via Partner Admin Link (PAL) to present and future Azure deployments at the subscription level

CWMS 5.3 release: Thurs., September 5, 2019

Components: 5.3 Cloud Workspace Management Suite

When: Thursday September 5, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

- Updates to the User Support Only role:
- Add searching for/filtering Users functionality
- Include Connection Status column for Users and their connections
- Provide access to the Force Password Change at Next Login feature
- Remove visibility of the Delete Client function
- Enforce logout of CWMS after 1 hour of inactivity
- Fix for a display issue where VM series/sizes were displaying incorrectly when viewing VM roles whose Resource Allocation Type is set to Fixed
- Fix for a display issue where environments with Workload Scheduling set to Always Off were displaying improper settings in CWMS, despite being correctly set to Always Off behind the scenes
- Permissions update – remove Resource Scheduling tab if the CWMS admin does not have access to the

Resources function in CWMS

- Remove the ability to add more than one VM instance in a VDI User Host Pool
- Display fix for Max Users per Session Host in a AVD Host Pool – these values now match the values set in the Live Scaling section of the Workload Scheduling tab

Cloud Resource App

- Updated functionality – support for Command Line usage

Cloud Workspace Tools and Services

- Support for the vCloud Rest interface

CWMS 5.3 release: August 22, 2019

Components: 5.3 Cloud Workspace Management Suite

When: Thursday August 22, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

5.3 Cloud Workspace Management Suite

- Add a message to the AVD tab defining under which circumstances AVD is supported
- Workflow improvements when returning from the AVD tab to the Workspace
- Text edit in the instructions on the AVD module

5.3 Cloud Workspace for Azure Setup

- Remove the requirement for entering a state when the Customer registering is outside of the United States
- Now deploys CWMGR1 as a D series VM for initial deployment, then resizes to B2ms for cost purposes after initial deployment

Cloud Workspace Tools and Services

- Bug fix for SSL certificate management on Legacy (2008 R2) environments
- Additional health checks for certificate enforcement and lifecycle management

CWMS 5.3 release: August 8, 2019

Components: 5.3 Cloud Workspace Management Suite

When: Thursday August 8, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

5.3 Cloud Workspace Management Suite

- Bug fix for a subset of scenarios where connecting to CWMGR1 from CWMS was not functioning as expected

Cloud Workspace Management Suite – Version 5.2



There will be no further recurring releases for v5.2 of CWMS – all releases will be considered hotfixes.

CWMS 5.2 release: Mon., December 2, 2019

Components: 5.2 Cloud Workspace Management Suite

When: Monday December 2, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.

Access to Cloud Workspace Management Suite will remain available.

No updates this release cycle.

CWMS 5.2 release: Thurs., November 14, 2019

Components: 5.2 Cloud Workspace Management Suite

When: Thursday November 14, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.

Access to Cloud Workspace Management Suite will remain available.

No updates this release cycle.

CWMS 5.2 release: Thurs., October 31, 2019

Components: 5.2 Cloud Workspace Management Suite

When: Thursday October 31, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.

Access to Cloud Workspace Management Suite will remain available.

No updates this release cycle.

CWMS 5.2 release: Thurs., October 17, 2019

Components: 5.2 Cloud Workspace Management Suite

When: Thursday October 17, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.

Access to Cloud Workspace Management Suite will remain available.

No updates this release cycle.

CWMS 5.2 release: Thurs., October 3, 2019

Components: 5.2 Cloud Workspace Management Suite

When: Thursday October 3, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.

Access to Cloud Workspace Management Suite will remain available.

No updates this release cycle.

CWMS 5.2 release: Thurs., September 19, 2019

Components: 5.2 Cloud Workspace Management Suite

When: Thursday September 19, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.
Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

Default an Azure deployment's Resource Allocation Type to Fixed; with the VM series/size selected being the VM defined by the Administrator in CWMS

Add search functionality for User Activity audit functionality

Bug fix for incorrectly displaying session inactivity timeout warning after 5 minutes instead of 55 minutes

User Support role fix – a subset of Admins with this role were unable to see the list of Users for their organization

User sorting fix – sorting by username works as intended instead of sorting by status

Ensure Master Client Report is present; hide the non-applicable SPLA report for non-Master Software Partners

Cloud Workspace tools and services

Enhanced password encryption behind the scenes

Bug fix for Password Enforcement Notification (PEN) where using the "change password at next logon" feature wasn't working as intended if password expiration dates were set to null by an administrator in CWMGR1

Cloud Workspace for Azure setup app

Fix for international administrators – this no longer requires a State if the Country is not the United States.

Apply CloudJumper via Partner Admin Link (PAL) to present and future Azure deployments at the subscription level

CWMS 5.2 release: Thurs., September 5, 2019

Components: 5.2 Cloud Workspace Management Suite

When: Thursday September 5, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.
Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

Updates to the User Support Only role:

- * Add searching for/filtering Users functionality
- * Include Connection Status column for Users and their connections
- * Provide access to the Force Password Change at Next Login feature
- * Remove visibility of the Delete Client function

Enforce logout of CWMS after 1 hour of inactivity

Fix for a display issue where VM series/sizes were displaying incorrectly when viewing VM roles whose Resource Allocation Type is set to Fixed

Fix for a display issue where environments with Workload Scheduling set to Always Off were displaying improper settings in CWMS, despite being correctly set to Always Off behind the scenes

Permissions update – remove Resource Scheduling tab if the CWMS admin does not have access to the Resources function in CWMS

Cloud resource app

Updated functionality – support for Command Line usage

Cloud Workspace tools and services

Support for the vCloud Rest interface

CWMS 5.2 release: Thurs., August 22, 2019

Components: 5.2 Cloud Workspace Management Suite

When: Thursday August 22, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.

Access to Cloud Workspace Management Suite will remain available.

Cloud Workspace Management Suite

Fix a display issue in the User profile for some monitor sizes

Add clarifying message for non-dynamic App Services notifying admins that it may take a few minutes for changes to take effect

Add refresh button for non-dynamic App Services to make it easier to tell if new clients/users have been added

Cloud Workspace for Azure setup

Add support for MFA for the registration process when linking to an existing CWMS account

Improvement to post-provisioning instructions – link to new and improved Public KB

Improvement to post-provisioning instructions – link opens in a new tab

Cloud Workspace tools and services

Bug fix for SSL certificate management on Legacy (2008 R2) environments

Additional health checks for certificate enforcement and lifecycle management

CWMS 5.2 release: Thurs., August 8, 2019

Components: 5.2 Cloud Workspace Management Suite

When: Thursday August 8, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.

Access to Cloud Workspace Management Suite will remain available.

No updates this release.

CWMS 5.2 release: Thurs., July 25, 2019

Components: 5.2 Cloud Workspace Management Suite

When: Thursday July 25, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.

Access to Cloud Workspace Management Suite will remain available.

5.2 CWA Setup

Display a message post-provisioning that directs CWA Setup users to the CloudJumper Public KB where they can review next steps and how to refine their deployment

Improved handling of countries outside the United States during the registration process

Added a field to confirm the password of the newly created CWMS login during the CWA Setup process

Remove SPLA licensing section under circumstances where RDS licenses will not be required

5.2 Cloud Workspace Management Suite

Improved HTML5 connection handling for CWMS Admins in single server deployments
Bug fix for a scenario where restarting a user's processing (when it had failed previously) resulted in an "Internal Server Error" message
Remove SPLA licensing section under circumstances where RDS licenses will not be required
Include Automatic SSL certificate handling and Automatic SMTP to the provisioning wizard inside CWMS

5.2 Cloud Workspace tools and services

When a VDI user logs out of their VM at a time it is set to be powered off, power off that VM
Azure Backup enhancement – when restoring TSD1 servers as a VM, restore as a TS VM instead of an additional TSD VM
Streamlined preparation of Azure VMs for Azure Backup handling
Back end processing speed and security improvements

5.2 REST API

Improved handling of server information, enabling faster Wake-on-Demand server load times

CWMS 5.2 release: Thurs., July 11, 2019

Components: 5.2 Cloud Workspace Management Suite
When: Thursday July 11, 2019 at 10pm – 11pm Eastern
Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.
Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace tools and services

Ongoing behind the scenes security enhancements
Ongoing stability enhancements for auto-generated certificates
Least Privileged methodology improvement – adjustment to use an account with fewer permissions/less affected by generic lockdowns to perform nightly reboots
Improvements for integrated backups for Azure deployments
Improvements for integrated backups for GCP deployments
Bug fix to no longer unnecessarily reboot servers to apply resource adjustments when they were already correct
Process enhancement to allow for manual certificate management, if desired

CWMS 5.2 release: Thurs., June 20, 2019

Components: 5.2 Cloud Workspace Management Suite
When: Thursday June 20, 2019 at 10pm – 11pm Eastern
Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.
Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Management Suite

Improved handling of Users imported into CWMS via the CRA process
Correct storage displays in the Server section of the Workspace module for a subset of scenarios
Updated year at the bottom of the CWMS web interface

5.2 Cloud Workspace tools and services

Enhanced automated certificate automation

5.2 REST API

Display correction – display the correct values previously entered in the Live Scaling feature when opening the Live Scaling feature again
Allow for creation of a default backup schedule for the Power User role (VDI Users).

CWMS 5.2 release: Thurs., June 6, 2019

Components: 5.2 Cloud Workspace Management Suite
When: Thursday June 6, 2019 at 10pm – 11pm Eastern
Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.
Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace tools and services

Improved handling of multiple emails for platform notifications
Bug fix for a subset of scenarios where Workload Scheduling was not turning servers off correctly
Bug fix for a subset of scenarios where restoring servers from Azure Backup didn't restore the proper storage type vs. a default storage type

5.2 CWA Setup

Continued security enhancements during the CWA Setup Process
Improved automated handling of subnet and gateway settings
Improved behind-the-scenes process of handling user accounts during the registration process
Includes a process to refresh tokens in the event a user remains in the CWA Setup process for more than 1 hour

CWMS 5.2 release: Thurs., May 23, 2019

Components: 5.2 Cloud Workspace Management Suite
When: Thursday May 23, 2019 at 10pm – 11pm Eastern
Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.
Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Management Suite

Improved link in the AVD tab in the Workspaces module
Bug fix for a scenario where clicking a link to a Workspace from the Data Centers module wouldn't take you to that Workspace
Bug fix for a scenario where updating the contact info for a Primary Admin would remove their designation as Primary Admin

CWMS 5.2 release: Thurs., May 9, 2019

Components: 5.2 Cloud Workspace Management Suite
When: Thursday May 9, 2019 at 10pm – 11pm Eastern
Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.
Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace tools and services

Scalability improvements for deployments with several hundred to several thousand VMs

CWMS 5.2 release: Thurs., April 25, 2019

Components: 5.2 Cloud Workspace Management Suite

When: Thursday April 25, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.

Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Management Suite

Interface improvement – in the event backups are not enabled for a server in Azure or GCP, remove the size column from the Backup section of a server

5.2 Cloud Workspace tools and services

Bug fix for a scenario where changing resources for RDP and/or HTML5 gateway servers would not bring them back online after the resource change was complete

5.2 REST API

Improved handling of initial MFA configurations, regardless of scenario

5.2 CWA Setup

Support for existing CWMS accounts, empowering indirect CSPs to provision correctly and simplifying the process for existing Partners

Additional validation for Azure Active Directory Domain Services – display an error if Azure Active Directory Domain Services is selected, but is already in place

CWMS 5.2 release: Thurs., April 11, 2019

Components: 5.2 Cloud Workspace Management Suite

When: Thursday April 11, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.

Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Management Suite

Bug fix for Provisioning Collections – saving a Provisioning Collection with an app that does not have a desktop icon will no longer display an error in CWMS

Bug fix – resolve an issue where starting a stopped platform server from CWMS displayed an error because there was no Partner code attached

5.2 Cloud Workspace tools and services

Stability enhancement for deleting servers in vCloud deployments – in the event that multiple FMs are found in one vApps, only delete the VM instead of deleting the vApp

Add an option to not install wildcard certificates on infrastructure servers

Improvements for cloning TSD servers in AzureAD

Improvements for Server Resource Report – handling servers with multiple IP addresses

Bug fix for a subset of scenarios when a list of backups for a server didn't load for review in AzureRM

Bug fix when attempting to clone VMs with a prefix in Azure Classic (all new and recent deployments use AzureRM)

Bug fix for DNS errors not being reported correctly in the Server Resource Report for Server 2008 R2

Bug fix for not sending the Company Resource report in the event that a VM deleted from the hypervisor (but not from AD) and CWMS cannot find Azure backups in the hypervisor itself (only in AzureRM deployments)

5.2 CWA Setup

Adding a method to validate that the region selected to provision into has Azure Active Directory Domain Services available

Adding additional checks to resolve DNS timeout issues in a subset of scenarios

Remove B2s as a target for CMGR1 deployment, as it was slowing down the deployment process

CWMS 5.2 release: Thurs., March 28, 2019

Components: 5.2 Cloud Workspace Management Suite

When: Thursday March 28, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.

Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Management Suite

Add Azure Virtual Desktop section to the CWMS interface

Allow a CWMS Admin to not set a company logo under Settings → Logo

Add requirement for External ID when updating an app in a Custom App Catalog

5.2 Cloud Workspace tools and services

Further streamlining and improvements to the Cloud Workspace for Azure (CWA) deployment process

A Premium Storage account is no longer required to create VMs with Premium Storage in Azure RM deployments

Resolve an issue in a subset of scenarios where Application Usage Tracking reports did not capture usage data

Resolve an issue where updating certificates on HTML5 portal servers would result in an error as HTML5 portal server licensing was updated

Bug fix for Password Expiration Notifications not updating passwords when using Azure Active Directory Domain Services

Adjusted location to which Password Expiration Notifications writes log files

5.2 REST API

Bug fix for starting/stopping Platform servers (not Customer servers) in the Data Center module

5.2 CWA Setup

Improvements for FTP role settings during deployment

Improved mechanism to ensure Admins are seeing the latest release every time they access the CWA Setup process

Improved handling of elements that time out during deployment

Bug fix for a scenario where a deployment was incorrectly tagged as using Azure AD

CWMS 5.2 Minor Release: Thurs., March 14, 2019

Components: 5.2 Cloud Workspace Management Suite

When: Thursday March 14, 2019 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.

Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Management Suite

Change the name of the “Application Monitoring” feature to “Application Usage Tracking”
Apply a fix where refreshing a search for Scripted Events does not re-use selected start/end dates
Default File Audit to start with the date filter set to one day prior to the current date, streamlining the amount of data returned
Bug fix to Integrated Backups for Azure where restoring backups to a server was not functioning as intended in a subset of scenarios
Resolve an application error prompt when updating a Client that belongs to an App Service

5.2 REST API

Azure safeguard – when adding an Azure AD User, ensure that their email address is not already added to the account.
Bug fix – when adding an application for a Client and creating a Group at the same time, add the Users to the Group as intended
Add a validation step when disabling access to RDSH servers that ensures it is still applied after a server is rebooted
General improvements for CWA workflow automation
Bug fix for a subset of scenarios when adding an App to a Group affected other Users of that Group

5.2 CWA Setup

Add a refresh option for the list of subscriptions during the deployment process
Auto-set deployment flag for degraded, legacy MobileDrive service to False
Additional automation safeguards and checks in Azure

CWMS 5.2 Minor Release: Thurs., February 28, 2019

Components: 5.2 Cloud Workspace Management Suite
When: Thursday February 28, 2019 at 10pm – 11pm Eastern
Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Management Suite

Improved clarity and confirmation message for what happens when deselecting the “VDI User” checkbox for Users in the CWMS interface (deletes VDI User’s server) and how to proceed if you do not want to delete the server
Back-end improvements to timestamp handling

5.2 Cloud Workspace tools and services

Updated settings for the license server name in Azure Domain Services
Behind-the-scenes improvements to the process by which a User can change their own password after being logged into their Cloud Workspace
Updated native 2FA to reflect CloudJumper imagery
Bug fix for 2FA if a rare setting is enabled

5.2 CWA Setup

Additional Help/Support content in the CWA Setup wizard
Add agreement terms and pricing to the CWA Setup wizard
Improved mechanism for detecting a Subscription’s quota and permissions

Streamline deployments for Azure Active Directory Domain Services based deployments
Behind-the-scenes improvement to the storage account name format
Bug fix for FTP server settings in a subset of scenarios

CWMS 5.2 Minor Release: Thurs., February 14, 2019

Components: 5.2 Cloud Workspace Management Suite
When: Thursday February 14, 2019 at 10pm – 11pm Eastern
Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.
Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Management Suite

Performance improvement in User management actions
Additional logging enabled to display who requested a change on a Group in the Data Center task history
Resolve an issue in the Standard App Catalog where applications were not displaying in a subset of scenarios
Resolve an issue in App Services with Dynamic Provisioning where an error is displayed if two applications with the same name are
Remove the SDDC creation wizard from the CWMS 5.1 interface
* If you are running a SDDC that is on 5.1 and you wish to provision a new SDDC, please contact support@cloudjumper.com to schedule an upgrade to CWMS 5.2
Correct a spelling error in the API User creation screen of CWMS

5.2 Cloud Workspace tools and services

In vCloud based SDDCs, re-login to the hypervisor in the event the connection expires
In vCloud based SDDCs, increase the default timeout when waiting for servers to boot up
Improved limitations on CloudJumper's administrative access

5.2 REST API

When provisioning a new SDDC via the 5.1 interface of CWMS, the message displayed will be “New data center creation is only supported when using v5.2 of CWMS.”

5.2 CWA Setup

Improved automatic error handling

CWMS 5.2 Minor Release: Thurs., January 31, 2019

Components: 5.2 Cloud Workspace Management Suite
When: Thursday January 31, 2019 at 10pm – 11pm Eastern
Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.
Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Management Suite

Add the Cloud Workspace client server's connection info to the Cloud Workspace client's Overview section
Add an editable field in CWMS Account Settings that allows you to enter your Azure AD Tenant ID
Use the most modern version of Microsoft Standard Storage in new Azure deployments
Improved Azure integration, requiring Integrated Backups in Azure deployments to be retained for at least 1 day
Improved handling in Dynamic Provisioning for App Services deployments
Add the date at which server storage is inventoried to that section of the Servers module

Display that an app is provisioned to a User while the User's status is still Pending Cloud Workspace
If a User is a VDI User, display the VDI Server on the User page
If a server is for a VDI User, display the User on the Server page
Resolve an issue in certain scenarios where if a User has an open Service Board task associated with their username, remote access to the VM fails from CWMS

5.2 Cloud Workspace tools and services

Improved handling of Live Scaling as Users log in throughout the day
Add automation prerequisites for future Wake on Demand improvements
Add automation prerequisites for future Workload Scheduling improvements
Resolve an issue where using Windows 10 for VDI servers was not properly enabling the remote registry service in Azure Active Directory Domain Services deployments
Resolve an issue where using Windows 10 for VDI servers was not properly setting the security group for the local Remote Desktop Users group in Azure Active Directory Domain Services deployments
Modify PCI compliance setting feature to take no action when not enabled instead of enforcing default configuration settings
Resolve a issue in Workload Scheduling so that Users with Wake on Demand enabled that log out can power down servers if they are scheduled to be powered down
Fix a bug when cloning a server in ProfitBricks public cloud
Fix a bug where cloning servers checks server prefixes to that server names aren't duplicated in VDI User scenarios
Add a check in nightly reports for cached customer codes that are not using a valid provisioning collection
Improved handling of exceptions when both the VM is not in the hypervisor and CWAgent requires an update
Resolve issue resetting passwords via Password Expiration Notification to correctly enforce password history

CWA Setup

Implement option to automatically configure SMTP settings
Adding validation options for the location list to checks if the subscription has enough quota and enough permissions to create VMs in the selected Azure region
Added feature to remove unneeded Cloudworkspace and other service accounts with administrative permissions at the end of the provisioning process in Azure
Notify Users that manual DNS certificate uploads have been verified
Resolved an issue where ThinPrint installations don't install as intended in certain scenarios

CWMS 5.2 Minor Release: Thurs., January 17, 2019

Components: 5.2 Cloud Workspace Management Suite
When: Thursday January 17, 2019 at 10pm – 11pm Eastern
Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Management Suite

The Workload Scheduling interface will now display Description as the first column and change the name of Scheduling to Custom Scheduling
Bug fix for displaying backups of platform servers in Azure deployments
Bug fix for scenarios where End User self-administration for App Services use cases where the organization does not have any Cloud Workspace services set up

5.2 Cloud Workspace tools and services

Add Support for PCI v3 compliance

Security enhancement: new CWMS deployments will use a local admin vs. a domain admin to run the CWAgent processes.

Support for Windows Server 2019 in AzureRM deployments

* Note: Microsoft does not support Microsoft Office in this version yet

Improved handling of Wake on Demand Users – if their organization is scheduled to power VMs down but a User with Wake on Demand is still actively working, do not power down the organization's VMs

Stability improvement when cloning VMs – remove roles like Connection Broker from the newly created VM coming from the cloned VM.

Improved process for installing the ThinPrint license server role

Improved AzureRM template handling – return all templates available for a VM in Azure based on the hardware it runs on, not just templates available in the tenant's Azure region

Improved automated testing for vSphere deployments

Include a check in nightly email reports to see if ThinPrint license server is installed

Bug fix for Live Scaling in a limited subset of scenarios

Bug fix for cloning servers in certain scenarios in vCloud deployments

Bug fix for VM name prefixes in AzureRM deployments

Bug fix for reporting error when using custom machine sizes in Google Cloud Platform

Bug fix for reporting Users with ThinPrint functionality enabled

Excluded Chinese version of Windows from the list of templates available in AzureRM

CWA Setup

Fix a scenario where passwords that meet the minimum number of characters required were not accepted

Change the ID column to Customer Domain during the tenant selection process for CSPs

Update to the signup process that streamlines credit card entry

CWMS 5.2 Minor Release: Thurs., December 20, 2018

Components: 5.2 Cloud Workspace Management Suite

When: Thursday December 20, 2018 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.

Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Setup

Added a feature of FTP DNS Registration in the event of a single-server deployment and Automatic SSL is selected during the deployment process

Automated process for populating Azure AD info. (Tenantid, ClientId, Key) into back-end tables

The automated installation process will now install ThinPrint License Server 11 instead of 10

5.2 CWA Setup

Fix an issue where the registration process redirected admins to a sign in page when completed

CWMS 5.2 Minor Release: Thurs., December 6, 2018

Components: 5.2 Cloud Workspace Management Suite

When: Thursday December 6, 2018 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.

Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Tools and Service

Support for creating servers with Win10 OS

Improved speeds when loading a VM from the hypervisor
Return correct storage types available when creating servers in Azure
Add logging of daily reports to the back end of the control plane
Avoid a scenario where temp drives could expand automatically in Azure
Lay the foundation for a future change to display server OS when selecting a template for provisioning
Bug fix for not automatically expanding a drive in GCP
Bug fix for deployment automation when using Azure Active Directory Domain Services
If multiple MGR servers are configured, note an error in the nightly report
Bug fix for automated tests for public cloud (Azure, GCP) backups in VMware deployments
Bug fix for determining disk space on a new VM created via HyperV deployments
Bug fix for collecting server data when AD root OU is blank
Stability improvement when cloning servers based off of a mis-configured hypervisor

5.2 REST API

Enable support for machine series in public cloud deployments
Allow the Default Resource Allocation to be Disabled for an SDDC
Added DataCollectedDateUTC to storage details for a server
Add the ability to Compute resource values
Add a new method to get detailed user connection statuses
Display an error in CWMS when deleting a user that also had admin rights
Fixed issue with drive mapping for a data enabled app service not always appearing
Fixed issue updating a client and/or user via CWMS that was imported via CWA
Fixed issue when a new user was created and applications were assigned to the all users group, the new user would not receive the application shortcuts.

CWMS 5.2 Minor Release: Thurs., November 1, 2018

Components: 5.2 Cloud Workspace Management Suite
When: Thursday November 1, 2018 at 10pm – 11pm Eastern
Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.
Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Management Suite

Bug fix for integrated backups
Bug fix for a specific use case in a CRA deployment

5.2 Cloud Workspace tools and services

Enable the ability to return storage types available in Azure ARM deployments when creating servers
Support for multi-site Active Directory topology
Fix an issue with TestVDCTools when using Azure Active Directory Domain Service
Bug fix for nightly email reports when AD root OU is blank

5.2 REST API

Support unlocking Users when Azure Active Directory Domain Services. Note: please be aware that there may be a delay of up to 20 minutes due to replication.

CWMS 5.2 Minor Release: Thurs., October 18, 2018

Components: 5.2 Cloud Workspace Management Suite
When: Thursday October 18th, 2018 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.
Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Management Suite

in the Data Center wizard, enable validation of wildcard certificates

General behind-the-scenes improvements and bug fixes

Add a search function in the applications table

Improved sorting in the applications table

Add details for completing DNS registration in the Data Center provisioning process

Include all Sub Partner Users and groups in API call responses for Dynamic App Services

Fix a bug where migration mode didn't persist for a tenant in a specific instance

Add Extra Powered On Servers, Shared Users per Servers and Max Shared Users per Server to live scaling details

Add DNS validation to the wildcard certificate testing when provisioning via the new Data Center wizard

5.2 Cloud Workspace Tools and Service

Enable an option to return all VM sizes grouped by VM series

Return all VM sizes available from the hypervisor

Fix to Resource Allocation when calculating App Service Users

Enable option for automatic resource update for CWMGR1

Include wildcard cert status DataCenterResources Report

Enable future DNS enhancements

Bug fix – fix to automatic drive expansions in GCP deployments

5.2 REST API

Performance improvements when listing Clients/Users

Allow support for new Live Scaling features – configuring ExtraPoweredOnServers, SharedUsersPerServer and MaxSharedUsersPerServer

API now supports the ability to validate wildcard certificate domain when creating new Platform deployments

New API method available to get User activity data for all Partner Clients

Known issue: When using a the "Active Users" or "User Count" dynamic allocation method for resource pool sizing inside an Azure ARM deployment, the "Computed Resource Per Server" summary incorrectly displays the Machine Size as Basic A series type instead of the correct Standard D series type.

CWMS 5.2 Minor Release: Thurs., September 27, 2018

Components: 5.2 Cloud Workspace Management Suite

When: Thursday September 27th, 2018 at 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted.
Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Management Suite

Simplify the display of provisioning collection VMs in cache

Fix a display quirk when managing App Services

5.2 Cloud Workspace tools and services

Bug fix for an obscure use case for End User MFA

Update API to interface with the latest in Azure RM

Update Testing for Azure RM to use the latest API
Replace Power User terminology with VDI User
Update email report to include additional CPU and RAM for a server
Update the address reports come from – instead of dcnotifications@independenceit.com messages will come from dcnotifications@cloudjumper.com
Allow definition of Users per server and additional VMs to remain on via Live Scaling
Performance improvements when starting a stopped SDDC/deployment
Security enhancement – disallow Partners with multiple SDDCs/deployments from connecting from one to another
Stability improvement – in the event automation cannot return User count, do not make any changes to resource count
Minor cosmetic enhancements

CWMS 5.2 Minor Release: Thurs., September 6, 2018

Components: 5.2 Cloud Workspace Management Suite
When: Thursday September 6th, 2018 at 10pm – 11pm Eastern
Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Management Suite

Added the ability to search for Sub Partners in the Custom App Catalog
Fixed a bug where refreshing the screen in the Data Centers module causes an error prompt
Removing the restriction on max folder name size and making it easier to browse folders
Ensure that resource counts on VMs are never lower than the minimum specified CPU and RAM values
Rephrase Power User terminology to VDI User
Fixed an error where a generic error was displayed despite the back-end process completing successfully
Improved server name display in Data Center creation wizard
Fix account expiration not displaying saved expiration date in CWMS

5.2 Cloud Workspace tools and services

Fixed a bug with MFA where Users who selected Email sometimes didn't receive a code
Allow additional CPU and RAM to be entered for User Count resource allocation type
Fix a bug where the automation engine didn't power all machine types on
Fixed a timing issue that sometimes would cause cloning servers to err out
Automate the previously manual installation of a wildcard certificate on FTP server
Added a process to purge old certificates after updating wildcard certificates
Resolve an issue where when using Data Enabled Application Services, the X: drive would not always map for an end user.

CWMS 5.2 General Availability Release: Thurs., August 10, 2018

Components: 5.2 Cloud Workspace Management Suite
When: Thursday August 10th, 2018 at 10pm Eastern
Impact: Access to Cloud Workspace desktops and application services for End Users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

5.2 Cloud Workspace Management Suite

Release web interface components to enable the features found in the overview above

5.2 Cloud Workspace tools and services

Release back-end tools to enable the features found in the overview above

5.2 REST API

Release API to production to enable the features found in the overview above

Cloud Workspace Suite – Version 5.1



There will be no further recurring releases for v5.1 of CWMS – all releases will be considered hotfixes.

CWMS 5.1 minor release: Thursday, October 18th, 2018

Components: 5.1 Cloud Workspace Management Suite

When: Thursday October 18th, 2018 @ 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for end-users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

Workspace Management Suite

- Add a search function in the applications table
- Improved sorting in the applications table

CWMS 5.1 minor release: Thurs., September 6th, 2018

Components: 5.1 Cloud Workspace Management Suite

When: Thurs., September 6, 2018 @ 10pm – 11pm Eastern

Impact: Access to Cloud Workspace desktops and application services for end-users will remain uninterrupted. Access to Cloud Workspace Management Suite will remain available.

5.1 Cloud Workspace Management Suite

- Added the ability to search for Sub Partners in the Custom App Catalog
- Fixed a bug where refreshing the screen in the Data Centers module causes an error prompt
- Removing the restriction on max folder name size and making it easier to browse folders
- Ensure that resource counts on VMs are never lower than the minimum specified CPU and RAM values

5.1 Cloud Workspace tools and services

- Fixed a bug with MFA where Users who selected Email sometimes didn't receive a code
- Allow additional CPU and RAM to be entered for User Count resource allocation type
- Fixed a bug for Resource Allocation for Server Load allocation type where in some cases the number of servers required was off
- Add safeguard when automatically rebooting a server – if CwVmAutomationService is busy, retry in 20 minutes

- Improved handling of wildcard certificate installs on CWMGR1
- Fixed data in the Data Center Resource Report
- Improved handling of updating RAM resources
- Improved calculations on the available Hard Drive Resources
- Introduces support of v4 of ProfitBricks' API, allowing for setting of CPU family
- Fixed deleting old temporary templates in ProfitBricks used when creating a provisioning collection
- Increased the timeout when waiting for ProfitBricks' hypervisor to create a VM
- When installing new versions of VdcTools, Update VdcToolsVersionRunningAtVdc as soon as it is in process so that automation will run sooner
- Fixed a bug that would surface when installing wildcard certificates on RDP Gateway servers
- Automate the previously manual installation of a wildcard certificate on FTP server
- Fixed a bug where password expiration notices were not forcing Users to update their password
- Improved the File Audit process to reduce the frequency of the Unknown user error appearing
- Fixed a bug where the File Audit Report was not properly excluding folders
- Added a feature to install the wildcard certificate if the certificate on the connection broker is expired
- Fixed a bug where password expiration notices wouldn't appear if the password expiration notification shortcut is removed from the startup folder (it will be reinstalled)
- Fixed a bug where wildcard certificate didn't delay an update on HTML5 portal servers if a User was logged in
- Fixed a bug where wildcard certificate would show needing an update HTML5 portal servers when it was already current
- Fixed a bug found when installing wildcard certificates on connection broker servers
- Fixed a cloning issue where Local VM accounts have been removed
- Fixed an issue where cloning servers put the tenant in Migration Mode
- Fixed an error with cloning VMs in vCloud where the hypervisor took long than expected to create the VM
- Fixed a bug where deleting a VM in AzureRM would also always delete the associated managed disks
- Fixed a rare timing issue creating VMs in AzureRM to prevent two build operations from overlapping
- Updated list of machine sizes and types in AzureRM
- Fixed an error when configuring the subnet in the hypervisor for GCP during deployment
- Fixed an error storing monitoring data re: platform health by removing a timeout that caused data to not be written when a server is busy
- Added a feature to allow each server to have its time zone set individually, or not controlled by platform automation
- Fixed a bug when creating VMs at a secondary site would return static IP addresses from the primary site
- Fixed an error in capturing Username for the User Login Report
- Fixed a bug that failed to delete old monitoring data by making the call asynchronous so that it would not time out
- Automatically install wildcard certificates on all infrastructure servers

CWMS 5.1 minor release: Thurs., July 12, 2018

Components: 5.1 CWMS Tools and Services

When: Thursday July 12, 2018 @ 10-10:30 pm Eastern

Impact: Access to Cloud Workspace desktops and application services for end-users will remain uninterrupted.

5.1 CWMS web app

- Fix an issue regarding Global App Catalog settings persistence

CWMS 5.1 minor release: Thurs., May 17, 2018

Components: 5.1 CWMS Tools and Services

When: Thursday May 17, 2018 @ 10-11 pm EST

Impact: Access to Cloud Workspace desktops and application services for end-users will remain uninterrupted.

5.1 CWMS web app

- Fix an issue regarding summaries of Users for App Services groups
- Fix an issue with the Data Center wizard pre-populating Username and password
- Add Username validation for local VM Admins and Level 3 technicians in the Data Center wizard
- Improved session handling, including auto-logout of Users after a session timeout
- Fix an issue when deleting Admins if a primary Admin couldn't be detected
- Change placeholder in Data Center → Profile Server Changes from Enter Profile Name to Enter Profile and change Label from Profile Name to Server Name
- Fix enabling AD admin not working for non-Cloud Workspace Users
- Fix JavaScript error preventing adding new Users/Groups for a non-Cloud Workspace Customer
- Allow Master Partners to create Active Directory User Admins for Sub Partners
- Fix bug causing password resets of a Sub Partner's Primary Admin to err out

CWS 5.1 minor release: Wed., Feb. 21, 2018

Components: 5.1 CW Tools and Services

When: Wed., Feb. 21, 2018 @ 10-11 pm EST

Impact: Access to Cloud Workspace desktops and application services for end-users will remain uninterrupted.

5.1 CW web app

- Fix issue managing user folders via Admin Access role

5.1 CW tools and services

- Ensure failed server is not automatically deleted when upgrading a "no services" client with a Workspace
- Handle W2016 GPO updates to prevent notification pop-up from being briefly visible to user(s) logged into their RDS sessions on W2016 VMs

5.1 REST API

- Add new attributes (modify CWS' SPLA Report to consume new attributes) to better handle core licensing-based apps (specifically, SQL)

CWS 5.1 minor release: Wed., Feb. 7, 2018

Components: 5.1 CW Tools and Services

When: Wed., Feb. 7, 2018 @ 10-11 pm EST

Impact: Access to Cloud Workspace desktops and application services for end-users will remain uninterrupted.

5.1 CW web app

- None

5.1 CW tools and services

- Fix issue disabling App Locker on Windows 2016 (due to newly discovered internal Windows 2016 issue)
- Fix bug when IP incorrectly being reassigned based-on clone failure event

5.1 REST API

- Fix saving Storage Type when modifying a server in a Provisioning Collection
- When creating a Provisioning Collection with two Terminal Server (TS) servers, only one TS server should be built to validate collection

CWS 5.1 minor release: Wed., Jan. 31, 2018

Components: 5.1 CW Tools and Services

When: Wed., Jan. 31, 2018 @ 10-11 pm EST

Impact: Access to Cloud Workspace desktops and application services for end-users will remain uninterrupted.

5.1 CW web app

- Increase number of rows per table on top-level CWS Modules from 10 to 20
- Fix User Support Only Admin being unable delve into a client

5.1 CW tools and services

- Fix bug when template doesn't have .Net Framework v4.5.2 incorrectly fails the server creation
- Fix issue when cloning VMs in Hyper-V

CWS 5.1 minor release: Wed., Jan. 10, 2018

Components: 5.1 CW Tools and Services

When: Wed., Jan. 10, 2018 @ 10-11 pm EST

Impact: Access to Cloud Workspace desktops and application services for end-users will remain uninterrupted.

5.1 CW tools and services

CWS version 5.1 Tools and Services (including the CW Automation Service, VM Automation Service and the CWAgent service) will be updated to eliminate any authorization error that occurs for specific RemoteApp application delivery scenarios. Specifically, the services will be modified to:

- Change automatic deployment of the SSL Wildcard Certificate for session servers to only deploy to Remote Desktop (RD) Connection Broker servers and Power User servers. Non-Broker session servers will utilize the default certificate generated by Remote Desktop Services (RDS).

- Change the external DNS Forward Lookup Zone on Active Directory at the SDDC to only create one DNS record for client shared session servers. That record will point to the client's RDS Broker server (VM), which will in turn handle the load balancing between shared session servers. Power user servers will continue to have a separate DNS entries.

Note: Only end client configurations that utilize multiple shared session servers were impacted by this issue, but new and modified client configurations will be deployed using this configuration.

CWS 5.1 minor release: Wed., Jan. 3, 2018

Components: 5.1 CW Web App

When: Wed., Jan. 3, 2018 @ 10-10:30 pm EST

Impact: Access to Cloud Workspace desktops and application services for end-users will remain uninterrupted.

5.1 CW web app

- Fix sorting by company code in CWS' Workspaces module
- Fix Cloud Workspace Users → Force Password reset not reflecting changes (when navigating to another module and then back to the user)
- SDDC Self-Deploy Wizard: Add confirmation alert modal when unchecking ThinPrint installation (Licensing section)

CWS 5.1 minor release: Tues., Dec. 5, 2017

Components: 5.1 CW Web App

When: Tues., Dec. 5, 2017 @ 10-10:30 pm EST

Impact: Access to Cloud Workspace desktops and application services for end-users will remain uninterrupted.

5.1 CW web app

- Fix CWS Admin MFA error on Internet Explorer (IE) 11
- Fix CWS Groups → Local Drive Access returning 'not found'
- Data Center Self Deploy Wizard: add support for AzureRM (ARM) Azure Active Directory
- Applications Catalog: ensure Subscription option always available/propagates
- CWS Scripted Events Module > Script Activity → Add Application: fix incorrect application icon path
- Improve efficiency of Admin Access request to prevent error when redirecting to CWS v5.0
- Fix various errors when updating AppService details and/or managing application licenses for an AppService
- CWS Workspace Module > Add Workspace Wizard → fix AppServices incorrect format being sent to Global Control Plane
- CWS Workspace Module > Add Workspace Wizard → New Client → Step 3, fix Update Group to address JavaScript error to ensure update is processed

CWS 5.1 minor release: Sat., Nov. 11, 2017

Components: 5.1 CW Web App

When: Sat., Nov. 11, 2017 @ 10-11pm EST

Impact: Access to Cloud Workspace desktops and application services for end-users will remain uninterrupted.

5.1 CW web app

- As of 10pm EST on Nov. 11, all CWS 5.1 partners must use <https://it.hostwindow.net>. This URL is being retrofitted to support CWS 5.1 (as well as CWS 5.0). Partners are responsible for ensuring their CWS Admin and end-users with CWS Admin Access are aware of this change.

CWS 5.1 minor release: Mon., Oct. 30, 2017

Components: 5.1 CW Web App and 5.1 CW Tools & Services

When: Mon., Oct. 30, 2017 @ 10-11pm EST

Impact: Access to Cloud Workspace desktops and application services for end-users will remain uninterrupted

5.1 CW web app

- CWS Admin MFA: pressing Enter submit code for MFA and fix bug which prevents re-sending MFA code
- SDDC Self Deploy Wizard: for GCP, have Administrator for Local VM name instead of just being disabled
- SDDC Self Deploy Wizard: increase width of drop-down for time zones
- Scripted Events: add Arguments field to script activity
- Scripted Events: add %applicationname% as an runtime variable for scripted events scripts

5.1 CW tools & services

- End-user email address: fix issue with email addresses not being saved to DB for existing end-users
- End-user logon status: fix issue getting UPN of end-user logged-in
- End-user logon status in AzureRM: support Azure Managed Disks
- Templates: fix workflow when templates not being deleted properly
- Resources: fix issue converting old Resource Pools to new allocation types
- File Audit Report: fix bug that causes user to be unknown
- Windows 2016: fix to ensure GPO to remove PowerShell icons from end-user Workspaces is applied properly
- Change Resources/Resource Allocation Report: fix error being incorrectly displayed
- Data Center Resources Report: if hypervisor not configured to return available Hard Drive Space or VM Quote, prevent report from showing error
- Infrastructure Server Monthly Reboots: address scenario when infrastructure servers not rebooting monthly as scheduled because they couldn't communicate to the CWMGR1 server due to this server being busy rebooting

5.1 minor release: Tues., Oct. 3, 2017

Components: 5.1 CW Web App and 5.1 CW Tools & Services

When: Tues., Oct. 3, 2017 @ 10-11pm EST

Impact: Access to Cloud Workspace desktops and application services for end-users will remain uninterrupted

5.1 CW web app

- AppServices: fix issue blocking add licenses functionality for AppService applications
- AppServices: ensure "Add New Instance" functionality always available for AppService applications

- Resource Pool Terminology: update terminology while always allowing applying resource pool configuration to servers even when there are no changes – “Update” changed to “Apply to Servers” and “Edit” has been changed to “Manage”
- Workload Schedule: ensure Edit modal always opens
- Workload Schedule: ensure arrows for selecting time always appear
- Scripted Events: allow for more granular time selection
- CWS Report ‘Admin Access’: fix issue causing IP column to have multiple IP addresses listed instead of just the client IP

5.1 CW tools & services

- File Audit Service: now disabled consistently
- Automation Service and new SSL Wildcard Certificate (RDP connections): update order of commands to ensure updated RDP certificate on RDS Gateway is always refreshed (i.e. not cached)

CWS® 5.1 initial release overview

Cloud Workspace Suite 5.1 is currently in Public Beta starting in Q3 2017. This release includes an update of both the CWS APIs and the Admin Control interface. The release is an update to CWS 5.0 (released Q4 2016) and is not “backward compatible” to version 4.x entities.

Once officially released in Q4 2017, there’s no upgrade fee or implementation cost to transition to CWS 5.1. The upgrades will be completed by CloudJumper in coordination with each Partner and will not interrupt existing services. CWS 5.1 continues to support all of the previous versions’ functionality, and extends new features that enhance both Administrator and End-User experience, and further improve the award winning automation and orchestration introduced with previous releases of Cloud Workspace Suite.

The CWS 5.1 upgrade is the fastest and easiest yet by extending and leveraging the updated architecture and REST API platform introduced in CWS 5.0. CWS 5.1 continues CloudJumper’s commitment for a friendlier environment to allow external developers to extend their services and products based on Cloud Workspace.



CWS 4.x will reach official end-of-life on 12.31.2017. Partners who remain on the CWS 4.x platform will no longer receive direct support for 4.x deployments and no further 4.x updates or bug fixes will be provided.

5.1 Highlights:

- Support for Windows 2016 Server
- Full Stack Support for Microsoft Azure Resource Manager
- Support for Office 365 Single Authentication
- MFA for CWS Portal Administrators
- Improved Provisioning Collection Management
- Administrator Defined Automation and Scripting
- Resource Sizing Management Schemes

Support for Windows 2016 Server

- Support Windows Server 2016 server versions for all supported platforms.

- Windows 2016 Server provides the “Windows 10” desktop experience for shared RDS session users and enables configuration options such as GPU assignment for graphics intensive applications*.

Full stack support for Microsoft Azure Resource Manager

- Microsoft requires migration from the traditional encryption key/delegated account user entitlement model to the Azure Resource Manager model.
- Microsoft Azure Resource Manager is a framework that enables users to work with the resources within a solution as a group.
- The required authentication attributes are collected once during software defined data center (SDDC) deployment and then reused for other Microsoft Azure activities without the need for re-entry or re-authentication.

Support for Office 365 single authentication

- Microsoft Office 365 utilizes an authentication model that requires end-users to enter credentials every time they use the office productivity suite on a new computer or device.
- CWS 5.1 Manages these credentials across the server farm so that end-users require authentication only on their first use of a new office 365 subscription.

Improved provisioning collection management

- Configuration and management of hypervisor templates for pre-defined workloads can be confusing, especially when working across multiple hypervisor platforms.
- CWS 5.1 introduces Automated hypervisor management functions that include the creation of server instances based on an existing template or Cloud Provider VM image; direct connection/login to the created server for installation of applications from CWS Web App; automatic template creation/Windows sysprep from the configured server instance, and validation of application paths and installs from within CWS to eliminate the need for accessing the hypervisor or cloud service dashboard directly.

MFA for CWS portal administrators

- CWS 5.1 includes a built-in multi-factor authentication (MFA) solution for CWS Administrators only
- Partners can implement their own MFA solution for end-users. Popular options include Duo, Auth-Anvil & Azure MF. CloudJumper will be releasing own built-in MFA for end-users in Q1 2018

Administrator defined automation

- CWS provides improved deployment/management automation for service providers with Administrator Defined Automation of tasks/script execution.
- With this enhancement, CWS 5.1 will significantly speed deployments, simplify management, and reduce overhead costs.
- CWS Administrator Defined Automation will allow for the installation or upgrading of applications based on events, allowing partners to trigger automated application installations/maintenance using this method.

Resource sizing management schemes

- CWS 5.1 resource functionality enhances ability to scale resources dynamically by adding three more resource schemas
- The existing Total Users schemas is now augmented by three more resource sizing schemes: Fixed, Active User & Activity-based

- Example: Fixed method supports exact specification of the CPU and RAM.
- All resource sizing schemes continue to allow for immediate/force change or nightly automated resource check/modification.

CWS – v5.0 Release Notes



There will be no further recurring releases for v5.0 of CWS – all releases will be considered hotfixes.

Overview

CloudJumper has released Cloud Workspace Suite 5.0 for general implementation starting in Q4 2016. This release includes an update of both the CWS APIs and the Admin Control interface. The release is a significant change and is not “backward compatible” to version 4.x entities.

Version 4.x will continue to be supported until all partner Software Defined Data Centers (SDDCs) have been upgraded to the 5.0 platform, upgrades will be completed by CloudJumper in coordination with each Partner and will not interrupt existing services. There is no upgrade fee or implementation cost to transition. CWS 5 continues to support all of the previous versions’ functionality, and extends new features that enhance both Administrator and End-User experience, and further improve the award winning automation and orchestration introduced with previous releases of Cloud Workspace Suite.

With CWS 5.0, CloudJumper has re-written all of the platforms APIs into REST API format and completely retired the earlier SOAP APIs. This updated architecture will make further enhancement by CloudJumper easier and faster, and creates an even friendlier environment for external developers to extend their services and products based on Cloud Workspace.

Highlights

- Complete UI/UX Rewrite
- Azure AD Integration
- Azure SDDC self service deploy
- App Services
- Resource Scheduling
- Live Server Scaling – Cross Platform
- Automated Server Cloning – Cross Platform
- Customize Drive Shares on a per client basis

Key features

Azure Active Directory (AD) Integration

- Build SDDC as Private Cloud Active Directory or use Microsoft Azure-AD-as-a-Service
- Combine CWS with Office365
- Support Azure-based SSO & MFA

Azure SDDC self service deploy

- Complete integration with Azure

- Rapidly deploy new SDDCs
- Deploy private enterprise Clouds within Azure for any workload including Cloud Workspace managed: WaaS, App Services, Private Web App & SharePoint

App services

- Deploy application silos for publishing applications as isolated service building blocks
- Apps delivered from 'public' app servers to many custom entities
- Apps installed in single app dedicated server pools
- Apps decoupled from user profile and data layer requirements
- Build hyper-scalable app services
- Multiple app services can be combined into user collections
- CWS license tracking and usage reporting

Live server scaling – cross platform

- Intelligent automated scaling of server resources/active servers
- Tightly manage server resources with dynamic increase/decrease while user load changes
- Automatically scale server resources up & down as workload varies

Automated server cloning – cross platform

- Automatically increase server until count availability as defined user count grows
- Adds additional servers to the available resource pools
- Combine with CWS Live Server Scaling capability to create fully automated solution

Resource scheduling

- Schedule service times on a per-customer basis
- Cost containment for Public Cloud
- Shut systems down when not in use and re-activate on pre-defined schedule

End User Requirements

Overview

NetApp VDS does not track or recommend different user endpoint devices. We do recommend some basics, but this does not exclude other possible endpoint choices.

Remote Desktop environments can be access from a variety of endpoint devices. Clients are available directly from Microsoft and 3rd party vendors. NetApp VDS offers a custom connection client for Windows devices (*NetApp VDS Client for Windows*) as well as a Web client compatible with HTML 5 browsers.

Azure Virtual Desktop environments can be accessed from a variety of endpoint devices. Unlike RDS, AVD environments can only be accessed by Microsoft native clients. Microsoft has published clients for Windows, MacOS, Android, iOS as well as a web client. Additionally they have partnered with IGEL to offer a Linux-based thin client offering.

End user connection options

Remote Desktop Services

NetApp VDS Client for Windows

The NetApp VDS Client for Windows is the best way for users to connect to their RDS environment. This simple installer allows the users to connect with just their user name and password. No server or gateway configuration is required. Printing and Local drive mapping are automatically enabled and this method has the highest performance.

VDS client url safelisting

In the event that outbound network connections are controller and in order to guarantee that they can continue to use the NetApp VDS Client for Windows for Windows, we recommend adding the following to the safelist:

- * api.cloudworkspace.com
- * vdsclient.app
- * api.vdsclient.app
- * bin.vdsclient.app

Upon request, a branded version of this application can be created with the Partner's logos and contact information. Please contact support to request this.

The NetApp VDS Client can be downloaded from here: <https://cwc.cloudworkspace.com/download/cwc-win-setup.exe>

Printing: When connecting with the NetApp VDS Client for Windows, printing is automatically setup using ThinPrint.

Local File Access: By default, the NetApp VDS Client for Windows shares the Local device drives (HDD, USB & Network) with the cloud user session. The user can browse and transfer data back and forth from the "This PC" location in Windows Explorer. This functionality can be disabled by editing the workspace or user in VDS.

VDS > Workspaces > Users & Groups > Security Settings

<input type="checkbox"/> VDI User Enabled	<input type="checkbox"/> Mobile Drive Enabled
<input type="checkbox"/> Account Expiration Enabled	<input checked="" type="checkbox"/> Local Drive Access Enabled
<input type="checkbox"/> Force Password Reset at Next Login	<input checked="" type="checkbox"/> Wake On Demand Enabled
<input type="checkbox"/> Multi-factor Auth Enabled	

Update

NetApp VDS web client

The NetApp VDS Web client can be accessed at <https://login.cloudworkspace.com/>

End users can also access their desktop via a webpage, as long as their browser supports HTML5. Browser

compatibility for HTML5 can be checked at <https://html5test.com/>

A fully branded version of this page can be created for NetApp VDS Partners. The partner is required to provide an SSL cert and there is a small professional services fee to implement. Please contact support to begin the process.

Printing: When connecting via HTML5, printing from the Virtual Desktop generates a PDF that is downloaded in the browser and can then be printed locally.

Local File Access: When connecting via HTML5, the user can upload files to the Cloud Drive. To do this the user will click the floating cloud icon, upload the file and then navigate to the “This PC > Cloud on...” location in Windows Explorer to access that file in the Virtual Desktop user session.

Manually configured RDS client

The second best connection method is to manually configure the Microsoft Remote Desktop application. This is ideal for MacOs, Linux, iOS, Android and ThinClients. The only requirement is that the device/software be able to connect via RDP and to configure an RDS Gateway.

The information needed to manually configure an RDP client is (Links go to where that information can be located):

- Username
- Password
- Server Address (a.k.a. PC Name)
- Gateway Address

Printing: When configuring a local RDP client, the user can optionally forward their printer to the cloud environment for printing.

Local File Access: When manually configuring an RDP client, the user can choose to share specific folders with the Virtual Desktop user session.

Locating the RDS gateway address

1. Navigate to VDS (<https://manage.cloudworkspace.com>)
2. Click Deployments
3. Click the name of the deployment
4. Locate RDP Gateway under Deployment Details

The screenshot shows the CloudJumper CSP Master interface. On the left, a sidebar menu includes options like Dashboard, Organizations, Data Centers, Workspaces, App Services, Service Board, Scripted Events, Admins, and Reports. The 'Data Centers' option is selected. In the main content area, a sub-menu for 'All Data Centers' shows 'trainwest3.onmicrosoft.com (afa)'. The 'Overview' tab is selected, displaying 'Data Center Details'. Key information shown includes:

- Description: trainwest3.onmicrosoft.com
- Data Center Code: afa
- Resource Allocation Type: MachineSize
- MachineSize: 4
- IP Gateway: afa
- IP address: afa.cloudworkspace.app:444
- HTTP Server Address: afa-htp.afa.cloudworkspace.app
- Port: 444

Below this, there are sections for Profile Servers, Platform Servers, and Platform Processes. The 'Profile Servers' section shows one server named 'CLOUD93' with 2 cores, 4 RAM GB, and an Online status. The 'Platform Servers' section shows two servers with similar specifications. The 'Platform Processes' section lists tasks like New Client, New User, New App Service, etc., all marked as Idle.

Locating the server address for users on a shared session host

Navigate to VDS (<https://manage.cloudworkspace.com>)

1. Click Workspaces
2. Click the name of the workspace
3. Locate Server Address under Company Details

The screenshot shows the 'TrainWest3's Workspace (d7)' overview page. The left sidebar includes 'Organizations', 'Data Centers', and 'Workspaces' (selected). The main content area has tabs for Overview, Users & Groups, VM Resource, Workload Schedule, and Contact Info. The 'Overview' tab is selected, displaying two charts:

- Active Users:** A line chart showing user activity over time. The Y-axis ranges from 0 to 100, and the X-axis shows dates from 2020-01-01 to 2020-01-07. The chart shows a sharp increase starting around January 4th.
- Resource Consumption:** A line chart showing resource usage over the last 7 days. The Y-axis ranges from 0 to 10. The X-axis shows dates from 2020-01-01 to 2020-01-07. It tracks 'Total CPU' (blue line with circles) and 'Total RAM [GB]' (green line with diamonds).

Below the charts, there are sections for 'Data Center' and 'App Services'. The 'Data Center' section shows 'trainwest3.onmicrosoft.com (afa)' with an 'Available' status. The 'App Services' section shows 'No App Services.'

Company Details:

Company Name: TrainWest3	Company Code: d7	Primary Notification Email: robbyennojen@cloudjumper.com	Phone: 3403905484
Status: Available	Person: Training West Demo	Address 1: 2667 50th CI SE	Address 2:
Organization Type: Client	Logon Identifier: @trainwest3.onmicrosoft.com	City: Olympia	Zip Code: 98501
Contact Email: robbyennojen@cloudjumper.com	Data Center: afa	State: WA	Country: United States
Website: d7.afa.cloudworkspace.app	Cloud Matrix: d7.afa.cloudworkspace.app		

Contact Details:

Primary Contact Name: Training West Demo	Primary Contact Email: robbyennojen@cloudjumper.com
Address 1: 2667 50th CI SE	Address 2:
City: Olympia	Zip Code: 98501
State: WA	Country: United States

Locating the server address for VDI users

1. Navigate to VDS (<https://manage.cloudworkspace.com>)
2. Click Workspaces
3. Click the name of the workspace
4. Locate Server Address under Company Details

The screenshot shows the CloudWorkspace management interface. At the top, there are navigation links for 'Admins' and 'Reports'. Below that is a dashboard with 'Active Users' and performance metrics for 'Total CPU' and 'Total RAM (GB)'. The main area is titled 'Data Center' and shows a workspace named 'teshub.cloudworkspace.com (dyv)'. The status is 'Available' with a green dot. Under 'App Services', it says 'No App Services.'.

Company Details

Company Name	Company Code	Contact Details
TechJumper Associates	dyv	Primary Notification Email: toby.vanrooijen@cloudjumper.com
Status	Owner:	Phone: 260-690-5484
Available	Surf Taco	Address 1: 361 Cleveland Crossing Drive
Organization Type	Login Identifier:	Address 2: Suite 133
Client:	@teshub.onmicrosoft.com	City: Garner
E-mail Address:	Data Center:	Zip Code: 27529
tobyv@cjxp.com	dyv	State: NC
Website:	Server Address: dyv.cloudworkspace.app	Country: United States

Cloud Workspace Settings

App Settings: Enable App Access, Enable Application Usage Tracking, Enable Application Lockdown.

Account Options

Account Lockout Notifications, Account Lockout Recovery.

Update

5. Click on the Users & Groups tab
6. Click on the user name
7. Locate the VDI Server address

The screenshot shows the CloudJumper CSP Master interface. The left sidebar has 'CloudJumper CSP Master' and 'Cloud Workspace' tabs, with 'Organizations' selected. The main area shows a user profile for 'Toby vanRoojen (toby.vanrooijen@teshub.onmicrosoft.com)'. The 'User Details' section includes fields like Username, Login Identifier, First Name, Last Name, and Availability. The 'Status & Connection Details' section shows Connection Status as 'Online' and VDI Server as 'DVYVTS3'. The 'Security Settings' section contains checkboxes for VDI User Enabled, Account Expiration Enabled, Force Password Reset at Next Login, Multi-Factor Auth Enabled, Multi-Drive Enabled, Local/Drive Access Enabled, and Web On-Demand Enabled. At the bottom, there are 'Password Reset' and 'Admin Access' sections.

8. The server address for this vdi user is the Server address: dvy.ada.cloudworkspace.app but with the company code (e.g. dvy) replaced with the VDI Server value (e.g. DVYTS1)...

e.g. DVYTS1.ada.cloudworkspace.app

RDS requirements matrix

Type	Operating System	RDS Client Access Method(s)	RDS Web Client
Windows PC	Windows 7 or later with Microsoft RDP 8 App	NetApp VDS Clients Manually Configure Client	https://login.cloudworkspace.com/
MacOS	MacOS 10.10 or later and Microsoft Remote Desktop 8 App	Manually Configure Client	https://login.cloudworkspace.com/
iOS	iOS 8.0 or Later and any Remote Desktop App that supports RD Gateways	Manually Configure Client	https://login.cloudworkspace.com/
Android	Android version capable of running Microsoft Remote Desktop app	Manually Configure Client	https://login.cloudworkspace.com/
Linux	Virtually all versions with any RDS application that supports RD Gateways	Manually Configure Client	https://login.cloudworkspace.com/
Thin Client	A wide variety of Thin Clients work, provided they support RD Gateways. Windows-based thin clients are recommended	Manually Configure Client	https://login.cloudworkspace.com/

Comparison matrix

Elements/Features	HTML5 Browser	VDS Client for Windows	MacOS RDP Client	RDP Client on mobile devices	HTML5 Client on mobile devices
Local Drive Access	Click the background, then the cloud icon that appears in the center of the top of the screen	Available in Windows Explorer	Right click edit the RDP. Go to the redirection tab. Then pick a folder that you would like to map. Log into the desktop and it will be displayed as a mapped drive.	N/A	N/A

Elements/Features	HTML5 Browser	VDS Client for Windows	MacOS RDP Client	RDP Client on mobile devices	HTML5 Client on mobile devices
Display Scaling	Can be resized, and will change based on how large the browser window is. This can never be larger than the resolution of the endpoint (primary, endpoint monitor in the event of multiple monitors)	Can be re-scaled, but will always be equal to the screen resolution of the endpoint (primary, endpoint monitor in the event of multiple monitors)	Can be re-scaled, but will always be equal to the screen resolution of the endpoint (primary, endpoint monitor in the event of multiple monitors)	N/A	N/A
Copy/Paste	Enabled through clipboard redirection.	Enabled through clipboard redirection.	Enabled through clipboard redirection. Inside virtual desktop, use control + C or V instead of command + C or V.	Enabled through clipboard redirection.	Enabled through clipboard redirection.
Printer Mapping	Printing handled via a PDF print driver that browsers are using to detect local and network printers	All local and network printers mapped via ThinPrint utility	All local and network printers mapped via ThinPrint utility	All local and network printers mapped via ThinPrint utility	Printing handled via a PDF print driver that browsers are using to detect local and network printers
Performance	RemoteFX (enhancement of audio and video) not enabled	RemoteFX enabled via RDP, enhancing audio/video performance	RemoteFX enabled via RDP, enhancing audio/video performance	RemoteFX enabled, enhancing audio/video performance	RemoteFX (enhancement of audio/video) not enabled
Use of mouse on mobile device	N/A	N/A	N/A	Tap the screen to move the mouse, click	Press and hold the screen and drag to move the mouse, tap to click

Peripheral devices

Printing

- The Virtual Desktop Client includes ThinPrint which passes local printers to the cloud desktop seamlessly.
- The HTML5 connection method downloads a PDF in the browser for local printing.
- The Microsoft Remote Desktop 8 App on MacOS allows the user to share printers into the cloud desktop

USB peripherals

Items such as scanners, cameras, card readers, audio devices have mix results. There is nothing unique about a Virtual Desktop deployment that will prevent this but the best choice is to test any devices that are required. Your Sales Rep can help setup test accounts if required.

Bandwidth

- NetApp recommends a minimum of 150kb bandwidth per user. Higher capacity will improve the user experience.
- Internet Latency under 100ms and very low Jitter are just as important. KB Article
- Additional bandwidth needs will be introduced by your company's use of VOIP, video streaming, audio streaming, and general Internet browsing.
- The amount of bandwidth consumed by the Virtual Desktop itself will be one of the smallest components when calculating user bandwidth requirements.

Microsoft bandwidth recommendations

<https://docs.microsoft.com/en-us/azure/virtual-desktop/bandwidth-recommendations>

App recommendations

Workload	Sample Applications	Recommended Bandwidth
Task worker	Microsoft Word, Outlook, Excel, Adobe Reader	1.5 Mbps
Office worker	Microsoft Word, Outlook, Excel, Adobe Reader, PowerPoint, Photo Viewer	3 Mbps
Knowledge worker	Microsoft Word, Outlook, Excel, Adobe Reader, PowerPoint, Photo Viewer, Java	5 Mbps
Power worker	Microsoft Word, Outlook, Excel, Adobe Reader, PowerPoint, Photo Viewer, Java, CAD/CAM, illustration/publishing	15 Mbps



These recommendations apply regardless of how many users are in the session.

Display resolution recommendations

Typical display resolutions at 30 fps	Recommended Bandwidth
About 1024 x 768 px	1.5 Mbps
About 1280 x 720 px	3 Mbps
About 1920 x 1080 px	5 Mbps
About 3840 x 2160 px (4K)	15 Mbps

Local device system resources

- Local system resources like RAM, CPU, Network Cards and Graphics capabilities will cause variation in the user experience.

- This is MOST true of network and Graphics capability.
- 1 GB of RAM and a low-power processor on an inexpensive Windows device. 2-4 GB RAM is a recommended minimum.

Azure Virtual Desktop

AVD Windows client

Download the Windows 7/10 client from <https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-windows-7-10> and log in using the end user username and password. Note that Remote App and Desktop Connections (RADC), Remote Desktop Connection (mstsc), and the NetApp VDS Client for Windows application does not currently support the ability to log in to AVD instances.

AVD web client

In a browser, navigate to the Azure Resource Manager-integrated version of the Azure Virtual Desktop web client at <https://rdweb.AVD.microsoft.com/arm/webclient> and sign in with your user account.



If you're using Azure Virtual Desktop (classic) without Azure Resource Manager integration, connect to your resources at <https://rdweb.AVD.microsoft.com/webclient> instead.

VDS Change Environments

Overview

NetApp's Virtual Desktop Service allows organizations to manage deployments on prior releases, to preview future releases and to manage environments running one version prior (N -1 methodology).

Virtual Desktop Service URLs

Virtual Desktop Service is the management console that administrators can use to manage VDS deployments on an ongoing basis.

Environment	Description	URL	Codebase	API Documentation
Preview	Preview version of the upcoming release	https://preview.manage.cloudworksace.com/	5.4	https://api.cloudworkspace.com/5.4/swagger/ui/index
Current	Current release	https://manage.vds.netapp.com/	6.0	https://api.cloudworkspace.com/6.0/swagger/ui/index
Previous	Previous release	https://manage.cloudworkspace.com/	5.4	https://api.cloudworkspace.com/5.4/swagger/ui/index

Virtual Desktop Service Deployment

VDS offers a wizard-driven deployment process that allows Administrators to drastically streamline the process of provisioning a AVD and/or virtual desktop environment.

Administrators cannot provision deployments to a Legacy environment – only into a Current or Preview

environment.

Environment	Description	URL	Codebase	Deployment Guide
Current	Current release	https://manage.vds.netapp.com/deployments/add	5.4	VDS v6.0 Deployment Guide
Previous	Previous release	https://cwasetup.cloudworkspace.com	5.4	Contact Support

VDS Cost Estimator

The VDS Cost Estimator is a purpose-built, value-added tool that allows organizations to estimate what their public cloud costs will be in either Azure or Google Cloud. The tool includes ways to vary and optimize budgets to deliver the solution needed within an organization's budget.

Environment	Description	URL
Validation	Preview of the upcoming release	https://val.manage.vds.netapp.com/cost-estimator
Current	Current release	https://manage.vds.netapp.com/cost-estimator

Script Library Documentation

Scripted Event Documentation - Adobe Reader DC

Global Scripts Overview

NetApp VDS includes a library of pre-defined scripted events that can be used directly in VDS environments and/or duplicated and used as the building blocks for custom scripted events.

For this application, this article covers both the install/enable and uninstall/disable action.

Global Script Use

Built-in scripted events such as this one are pre-populated, checking the "global" filter checkbox will display them.

Global Scripted Events such as this one are read-only. They can be used as-is or the "Clone" function can be used to create a customer copy for editing and use.

The Clone button is found in the action menu on the Scripted Events page.

The screenshot shows the 'Scripted Events' section of the VDS interface. On the left is a sidebar with various navigation options like Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events, Admins, Reports, Applications, Cost Estimator, and SaaS Backup. The main area is titled 'Scripted Events' and has tabs for 'Repository' (which is selected) and 'Activities'. A search bar at the top right contains the query 'Install Adobe'. Below the search bar are filter options: 'Customer' (unchecked), 'Global' (checked), and buttons for 'Refresh' and '+ Add Script'. A table lists the scripts with columns for Name, Script, Type, and Created on. The 'Install Adobe Reader' script was created on Jan 12, 2021, at 12:42 PM. The 'Uninstall Adobe Reader' script was created on Jan 12, 2021, at 12:43 PM. The 'Clone' button for the 'Uninstall Adobe Reader' script is highlighted with a green border.

Adobe Reader DC overview

This script package installs/uninstalls *Adobe Reader DC* using the Chocolatey package manager (<https://chocolatey.org/>) to do the deployment. Chocolatey is deployed by VDS when VMs are created but this script will also check and install Chocolatey as a prerequisite if it is missing.

Default shortcut path

The default shortcut path will be entered below, for this application the shortcut is: \\shortcuts\Acrobat Reader DC.lnk

Add activity dialog window screenshot

The screenshot shows the 'Add Activity' dialog. On the left is a sidebar with the same navigation options as the previous screenshot. The main area is titled 'Add Activity'. It has sections for 'Activity Settings' (Name: 'InstallAdobeReader', Required: checked, Description: empty), 'Deployment' (Script: 'InstallAdobeReader', Arguments: empty), and 'Event Settings' (Event Type: 'Application Install'). Under 'Target Settings', 'Application' is set to 'Adobe Reader' and 'Shortcut Path' is set to '\\shortcuts\Acrobat Reader DC.lnk'. At the bottom are 'Cancel' and 'Add Activity' buttons.

Add application install/uninstall activity

In order for a script in the repository to take any action, an activity must be created to associate that script with a selected trigger. In this example activity will install/uninstall this application when the app is added to or

removed from the workspace (from the *Workspace > Applications* page in VDS).

VDS scripted events offers many other types of activity triggers such as *Create Server* which could be used as an alternative to the *Application Install* (or *Application Uninstall*) event type. Using *Create Server* would simply run this app install against all newly created VMs in VDS. *Create Server* and other triggers are documented and can be explored [here](#).



This application will need to be present in the VDS application library. This [section](#) of the app entitlement for RDS article covers adding apps to the library.

To create an activity and link this script to an action:

1. Navigate to the *Scripted Events* section in VDS
2. Under *Activities* click **+ Add Activity**
3. In the opened dialog window enter the following information:
 - **Name:** Name this activity
 - **Description:** Optionally enter a description
 - **Deployment** Select the desired deployment from dropdown
 - **Script:** Select the install (or uninstall) script from the dropdown. This could be the global script or customer script you've cloned and customized.
 - **Arguments:** Leave blank
 - **Enabled checkbox:** Check the box
 - **Event Type:** Select *Application Install* (or *Application Uninstall*) from dropdown
 - **Application:** Select this application from dropdown
 - **Shortcut Path:** Enter the default shortcut path for this application (noted above)

Scripted Event Documentation - AMD Radeon Instinct Drivers

Global Scripts Overview

NetApp VDS includes a library of pre-defined scripted events that can be used directly in VDS environments and/or duplicated and used as the building blocks for custom scripted events.

For this application, this article covers both the install/enable and uninstall/disable action.

Global Script Use

Built-in scripted events such as this one are pre-populated, checking the "global" filter checkbox will display them.

Global Scripted Events such as this one are read-only. They can be used as-is or the "Clone" function can be used to create a customer copy for editing and use.

The Clone button is found in the action menu on the Scripted Events page.

The screenshot shows the VDS interface with the 'Scripted Events' repository selected. A search bar at the top has 'Install Adobe' entered. Below it, a table lists two scripts: 'Install Adobe Reader' and 'Uninstall Adobe Reader'. The 'Clone' button for the 'Uninstall Adobe Reader' script is highlighted with a green border.

AMD Radeon Instinct Drivers overview

This script package installs/uninstalls *AMD Radeon Instinct Drivers* using the Chocolatey package manager (<https://chocolatey.org/>) to do the deployment. Chocolatey is deployed by VDS when VMs are created but this script will also check and install Chocolatey as a prerequisite if it is missing.

Add activity dialog window screenshot

The screenshot shows the 'Add Activity' dialog. Under 'Activity Settings', the name is 'InstallAMDRadeonInstinctDrivers' and the description is 'Enter description...'. Under 'Deployment', the deployment is 'VDSGCPDemo (kxx)' and the script is 'InstallAMDRadeonInstinctDrivers'. The 'Arguments' field is empty. The 'Enabled' checkbox is checked. Under 'Event Settings', the event type is 'Manual'. Under 'Target Settings', the target type is 'Servers'. The 'Managed Servers' section shows four items selected: 'CWMGR1', 'CWT1', 'CWT2', and 'NYMMTSD1'. At the bottom right are 'Cancel' and 'Add Activity' buttons.

Add Manual activity

In order for a script in the repository to take any action, an activity must be created to associate that script with a selected trigger. In this example activity runs when the VDS admin manually triggers the script.

VDS scripted events offers many other types of activity triggers such as *Create Server* which could be used as an alternative to the *Manual* event type. Using *Create Server* would simply execute this script on all newly created VMs in VDS. *Create Server* and other triggers are documented and can be explored [here](#).

To create an Activity and link this script to an action:

1. Navigate to the Scripted Events section in VDS
2. Under *Activities* click + Add Activity
3. In the opened dialog window enter the following information:
 - **Name:** Name this activity
 - **Description:** Optionally enter a description
 - **Deployment** Select the desired deployment from dropdown
 - **Script:** Select the install (or uninstall) script from the dropdown. This could be the global script or customer script you've cloned and customized.
 - **Arguments:** Leave blank
 - **Enabled checkbox:** Check the box
 - **Event Type:** Select *Manual* from dropdown
 - **Target Type:** Select the *Servers* radio button
 - **Managed Servers:** Check the box for each VM that should receive this uninstall.

Scripted Event Documentation - Ezeep Print App

Global Scripts Overview

NetApp VDS includes a library of pre-defined scripted events that can be used directly in VDS environments and/or duplicated and used as the building blocks for custom scripted events.

For this application, this article covers both the install/enable and uninstall/disable action.

Global Script Use

Built-in scripted events such as this one are pre-populated, checking the "global" filter checkbox will display them.

Global Scripted Events such as this one are read-only. They can be used as-is or the "Clone" function can be used to create a customer copy for editing and use.

The Clone button is found in the action menu on the Scripted Events page.

Ezeep Print App overview

This script package installs/uninstalls *Ezeep Print App* using the Chocolatey package manager (<https://chocolatey.org/>) to do the deployment. Chocolatey is deployed by VDS when VMs are created but this script will also check and install Chocolatey as a prerequisite if it is missing.

Default shortcut path

The default shortcut path will be entered below, for this application the shortcut is: \\shortcuts\Printer Self Service.lnk

Add activity dialog window screenshot

Add application install/uninstall activity

In order for a script in the repository to take any action, an activity must be created to associate that script with a selected trigger. In this example activity will install/uninstall this application when the app is added to or

removed from the workspace (from the *Workspace > Applications* page in VDS).

VDS scripted events offers many other types of activity triggers such as *Create Server* which could be used as an alternative to the *Application Install* (or *Application Uninstall*) event type. Using *Create Server* would simply run this app install against all newly created VMs in VDS. *Create Server* and other triggers are documented and can be explored [here](#).



This application will need to be present in the VDS application library. This [section](#) of the app entitlement for RDS article covers adding apps to the library.

To create an activity and link this script to an action:

1. Navigate to the *Scripted Events* section in VDS
2. Under *Activities* click **+ Add Activity**
3. In the opened dialog window enter the following information:
 - **Name:** Name this activity
 - **Description:** Optionally enter a description
 - **Deployment** Select the desired deployment from dropdown
 - **Script:** Select the install (or uninstall) script from the dropdown. This could be the global script or customer script you've cloned and customized.
 - **Arguments:** Leave blank
 - **Enabled checkbox:** Check the box
 - **Event Type:** Select *Application Install* (or *Application Uninstall*) from dropdown
 - **Application:** Select this application from dropdown
 - **Shortcut Path:** Enter the default shortcut path for this application (noted above)

Scripted Event Documentation - Google Chrome

Global Scripts Overview

NetApp VDS includes a library of pre-defined scripted events that can be used directly in VDS environments and/or duplicated and used as the building blocks for custom scripted events.

For this application, this article covers both the install/enable and uninstall/disable action.

Global Script Use

Built-in scripted events such as this one are pre-populated, checking the "global" filter checkbox will display them.

Global Scripted Events such as this one are read-only. They can be used as-is or the "Clone" function can be used to create a customer copy for editing and use.

The Clone button is found in the action menu on the Scripted Events page.

Google Chrome overview

This script package installs/uninstalls *Google Chrome* using the Chocolatey package manager (<https://chocolatey.org/>) to do the deployment. Chocolatey is deployed by VDS when VMs are created but this script will also check and install Chocolatey as a prerequisite if it is missing.

Default shortcut path

The default shortcut path will be entered below, for this application the shortcut is: \\shortcuts\Google Chrome.lnk

Add activity dialog window screenshot

Add application install/uninstall activity

In order for a script in the repository to take any action, an activity must be created to associate that script with a selected trigger. In this example activity will install/uninstall this application when the app is added to or

removed from the workspace (from the *Workspace > Applications* page in VDS).

VDS scripted events offers many other types of activity triggers such as *Create Server* which could be used as an alternative to the *Application Install* (or *Application Uninstall*) event type. Using *Create Server* would simply run this app install against all newly created VMs in VDS. *Create Server* and other triggers are documented and can be explored [here](#).



This application will need to be present in the VDS application library. This [section](#) of the app entitlement for RDS article covers adding apps to the library.

To create an activity and link this script to an action:

1. Navigate to the *Scripted Events* section in VDS
2. Under *Activities* click **+ Add Activity**
3. In the opened dialog window enter the following information:
 - **Name:** Name this activity
 - **Description:** Optionally enter a description
 - **Deployment** Select the desired deployment from dropdown
 - **Script:** Select the install (or uninstall) script from the dropdown. This could be the global script or customer script you've cloned and customized.
 - **Arguments:** Leave blank
 - **Enabled checkbox:** Check the box
 - **Event Type:** Select *Application Install* (or *Application Uninstall*) from dropdown
 - **Application:** Select this application from dropdown
 - **Shortcut Path:** Enter the default shortcut path for this application (noted above)

Scripted Event Documentation - Microsoft Edge Chromium

Global Scripts Overview

NetApp VDS includes a library of pre-defined scripted events that can be used directly in VDS environments and/or duplicated and used as the building blocks for custom scripted events.

For this application, this article covers both the install/enable and uninstall/disable action.

Global Script Use

Built-in scripted events such as this one are pre-populated, checking the "global" filter checkbox will display them.

Global Scripted Events such as this one are read-only. They can be used as-is or the "Clone" function can be used to create a customer copy for editing and use.

The Clone button is found in the action menu on the Scripted Events page.

The screenshot shows the 'Scripted Events' section of the VDS interface. On the left is a sidebar with various navigation options like Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events (which is selected), Admins, Reports, Applications, Cost Estimator, and SaaS Backup. The main area has tabs for 'Repository' (selected) and 'Activities'. A search bar at the top right contains the query 'Install Adobe'. Below it is a table with columns: Name, Script, Type, Created on, and Actions. Two scripts are listed: 'Install Adobe Reader' (script file: InstallAdobeReader.ps1, Global, Jan 12, 2021, 12:42 PM) and 'Uninstall Adobe Reader' (script file: UninstallAdobeReader.ps1, Global, Jan 12, 2021, 12:43 PM). The 'Actions' column for the 'Uninstall Adobe Reader' row contains two buttons: 'Download' and 'Clone', with 'Clone' being highlighted with a green border.

Microsoft Edge Chromium overview

This script package installs/uninstalls *Microsoft Edge Chromium* using the Chocolatey package manager (<https://chocolatey.org/>) to do the deployment. Chocolatey is deployed by VDS when VMs are created but this script will also check and install Chocolatey as a prerequisite if it is missing.

Default shortcut path

The default shortcut path will be entered below, for this application the shortcut is: \\shortcuts\Microsoft Edge.lnk

Add activity dialog window screenshot

The screenshot shows the 'Add Activity' dialog. The left sidebar is identical to the one in the previous screenshot. The main area has a title 'Add Activity'. Under 'Activity Settings', there is a 'Name' field containing 'InstallMicrosoftEdgeChromium', a 'Required' field, and a 'Description' field with placeholder text 'Enter description...'. Under 'Deployment', there is a 'Deployment' dropdown set to 'VDSGCPDemo (xxx)', a 'Script' dropdown set to 'InstallMicrosoftEdgeChromium', and an 'Arguments' field with placeholder text 'Enter arguments...'. A checked checkbox labeled 'Enabled' is present. Under 'Event Settings', there is an 'Event Type' dropdown set to 'Application Install'. Under 'Target Settings', there is an 'Application' dropdown set to 'Microsoft Edge Chromium' and a 'Shortcut Path' field containing '\\shortcuts\Microsoft Edge.lnk'. At the bottom are 'Cancel' and 'Add Activity' buttons, with 'Add Activity' being highlighted with a green border.

Add application install/uninstall activity

In order for a script in the repository to take any action, an activity must be created to associate that script with a selected trigger. In this example activity will install/uninstall this application when the app is added to or

removed from the workspace (from the *Workspace > Applications* page in VDS).

VDS scripted events offers many other types of activity triggers such as *Create Server* which could be used as an alternative to the *Application Install* (or *Application Uninstall*) event type. Using *Create Server* would simply run this app install against all newly created VMs in VDS. *Create Server* and other triggers are documented and can be explored [here](#).



This application will need to be present in the VDS application library. This [section](#) of the app entitlement for RDS article covers adding apps to the library.

To create an activity and link this script to an action:

1. Navigate to the *Scripted Events* section in VDS
2. Under *Activities* click **+ Add Activity**
3. In the opened dialog window enter the following information:
 - **Name:** Name this activity
 - **Description:** Optionally enter a description
 - **Deployment** Select the desired deployment from dropdown
 - **Script:** Select the install (or uninstall) script from the dropdown. This could be the global script or customer script you've cloned and customized.
 - **Arguments:** Leave blank
 - **Enabled checkbox:** Check the box
 - **Event Type:** Select *Application Install* (or *Application Uninstall*) from dropdown
 - **Application:** Select this application from dropdown
 - **Shortcut Path:** Enter the default shortcut path for this application (noted above)

Scripted Event Documentation - Microsoft Office 365

Global Scripts Overview

NetApp VDS includes a library of pre-defined scripted events that can be used directly in VDS environments and/or duplicated and used as the building blocks for custom scripted events.

For this application, this article covers both the install/enable and uninstall/disable action.

Global Script Use

Built-in scripted events such as this one are pre-populated, checking the "global" filter checkbox will display them.

Global Scripted Events such as this one are read-only. They can be used as-is or the "Clone" function can be used to create a customer copy for editing and use.

The Clone button is found in the action menu on the Scripted Events page.

The screenshot shows the 'Scripted Events' section of the VDS interface. On the left is a sidebar with various navigation links like Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events (which is selected and highlighted in blue), Admins, Reports, Applications, Cost Estimator, and SaaS Backup. The main content area has a header 'Scripted Events' with tabs 'Repository' (selected) and 'Activities'. Below is a search bar with the query 'Install Adobe'. A table lists two scripts: 'Install Adobe Reader' and 'Uninstall Adobe Reader'. The 'Actions' column for 'Install Adobe Reader' contains 'Download', 'Clone' (with a green border around it), and 'Edit'. At the bottom of the table are pagination controls: Previous, Page 1 of 1, and Next.

Microsoft Office 365 overview

This script package installs/uninstalls *Microsoft Office* using the Chocolatey package manager (<https://chocolatey.org/>) to do the deployment. Chocolatey is deployed by VDS when VMs are created but this script will also check and install Chocolatey as a prerequisite if it is missing.

! This Microsoft Office 365 install script does not include Microsoft Teams or Microsoft One Drive. These are included as stand-alone automated scripts to allow for greater flexibility as some deployments do not require these applications. This deployment can be copied and edited to include them (or to change any other [Office Deployment Tool](#) settings) by cloning the Script from VDS and editing the InstallMicrosoftOffice365.ps1 to input different values into the xml config file.

Default shortcut path

The default shortcut path will be entered below, for this application the shortcut is: \\folders\Microsoft Office

Add activity dialog window screenshot

Add application install/uninstall activity

In order for a script in the repository to take any action, an activity must be created to associate that script with a selected trigger. In this example activity will install/uninstall this application when the app is added to or removed from the workspace (from the *Workspace > Applications* page in VDS).

VDS scripted events offers many other types of activity triggers such as *Create Server* which could be used as an alternative to the *Application Install* (or *Application Uninstall*) event type. Using *Create Server* would simply run this app install against all newly created VMs in VDS. *Create Server* and other triggers are documented and can be explored [here](#).



This application will need to be present in the VDS application library. This [section](#) of the app entitlement for RDS article covers adding apps to the library.

To create an activity and link this script to an action:

1. Navigate to the *Scripted Events* section in VDS
2. Under *Activities* click *+ Add Activity*
3. In the opened dialog window enter the following information:
 - **Name:** Name this activity
 - **Description:** Optionally enter a description
 - **Deployment** Select the desired deployment from dropdown
 - **Script:** Select the install (or uninstall) script from the dropdown. This could be the global script or customer script you've cloned and customized.
 - **Arguments:** Leave blank
 - **Enabled checkbox:** Check the box
 - **Event Type:** Select Application Install (or Application Uninstall) from dropdown
 - **Application:** Select this application from dropdown
 - **Shortcut Path:** Enter the default shortcut path for this application (noted above)

Scripted Event Documentation - Microsoft OneDrive

Global Scripts Overview

NetApp VDS includes a library of pre-defined scripted events that can be used directly in VDS environments and/or duplicated and used as the building blocks for custom scripted events.

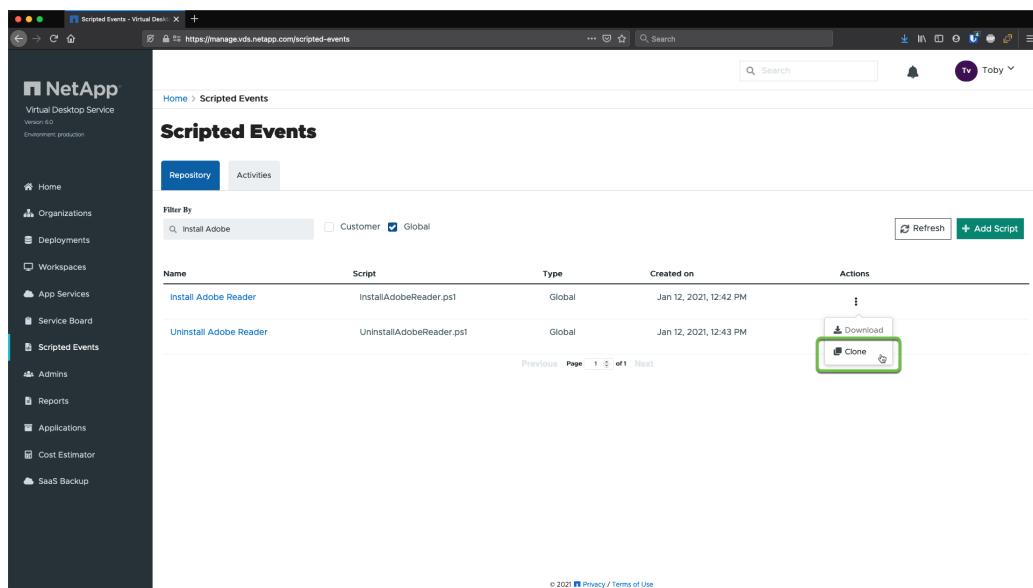
For this application, this article covers both the install/enable and uninstall/disable action.

Global Script Use

Built-in scripted events such as this one are pre-populated, checking the "global" filter checkbox will display them.

Global Scripted Events such as this one are read-only. They can be used as-is or the "Clone" function can be used to create a customer copy for editing and use.

The Clone button is found in the action menu on the Scripted Events page.



The screenshot shows the 'Scripted Events' page in the NetApp VDS interface. The left sidebar contains navigation links for Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events, Admins, Reports, Applications, Cost Estimator, and SaaS Backup. The main content area has a header 'Scripted Events' with tabs 'Repository' (selected) and 'Activities'. A search bar and a 'Toby' user icon are at the top right. Below is a 'Filter By' section with a search input 'Install Adobe', a 'Customer' checkbox (unchecked), and a 'Global' checkbox (checked). Buttons for 'Refresh' and '+ Add Script' are on the right. A table lists scripts with columns: Name, Script, Type, Created on, and Actions. Two rows are shown: 'Install Adobe Reader' (Script: InstallAdobeReader.ps1, Type: Global, Created on: Jan 12, 2021, 12:42 PM) and 'Uninstall Adobe Reader' (Script: UninstallAdobeReader.ps1, Type: Global, Created on: Jan 12, 2021, 12:43 PM). The 'Actions' column for the second row contains a 'Download' button and a 'Clone' button, which is highlighted with a green box. Navigation links 'Previous', 'Page 1 of 1', and 'Next' are at the bottom of the table.

Microsoft OneDrive overview

This script package installs/uninstalls *Microsoft OneDrive* using the Chocolatey package manager (<https://chocolatey.org/>) to do the deployment. Chocolatey is deployed by VDS when VMs are created but this script will also check and install Chocolatey as a prerequisite if it is missing.

Default shortcut path

The default shortcut path will be entered below, for this application the shortcut is:
\shortcuts\OneDrive.lnk

Add activity dialog window screenshot

Add application install/uninstall activity

In order for a script in the repository to take any action, an activity must be created to associate that script with a selected trigger. In this example activity will install/uninstall this application when the app is added to or removed from the workspace (from the *Workspace > Applications* page in VDS).

VDS scripted events offers many other types of activity triggers such as *Create Server* which could be used as an alternative to the *Application Install* (or *Application Uninstall*) event type. Using *Create Server* would simply run this app install against all newly created VMs in VDS. *Create Server* and other triggers are documented and can be explored [here](#).



This application will need to be present in the VDS application library. This [section](#) of the app entitlement for RDS article covers adding apps to the library.

To create an activity and link this script to an action:

1. Navigate to the *Scripted Events* section in VDS
2. Under *Activities* click *+ Add Activity*
3. In the opened dialog window enter the following information:
 - **Name:** Name this activity
 - **Description:** Optionally enter a description
 - **Deployment** Select the desired deployment from dropdown
 - **Script:** Select the install (or uninstall) script from the dropdown. This could be the global script or customer script you've cloned and customized.
 - **Arguments:** Leave blank
 - **Enabled checkbox:** Check the box
 - **Event Type:** Select Application Install (or Application Uninstall) from dropdown
 - **Application:** Select this application from dropdown
 - **Shortcut Path:** Enter the default shortcut path for this application (noted above)

Scripted Event Documentation - Microsoft Teams

Global Scripts Overview

NetApp VDS includes a library of pre-defined scripted events that can be used directly in VDS environments and/or duplicated and used as the building blocks for custom scripted events.

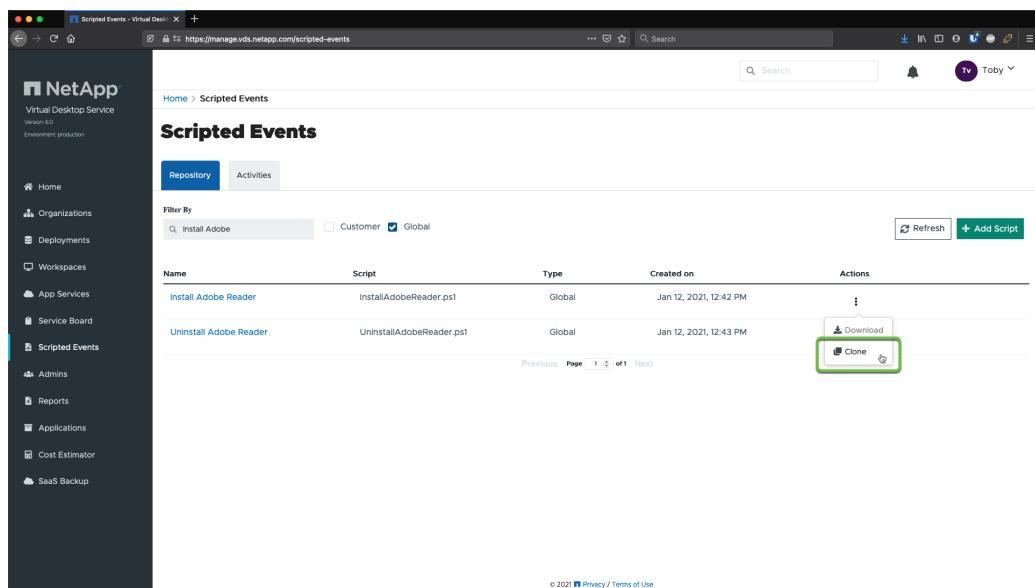
For this application, this article covers both the install/enable and uninstall/disable action.

Global Script Use

Built-in scripted events such as this one are pre-populated, checking the "global" filter checkbox will display them.

Global Scripted Events such as this one are read-only. They can be used as-is or the "Clone" function can be used to create a customer copy for editing and use.

The Clone button is found in the action menu on the Scripted Events page.



The screenshot shows the 'Scripted Events' page in the NetApp VDS interface. The left sidebar contains navigation links for Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events, Admins, Reports, Applications, Cost Estimator, and SaaS Backup. The main content area has a header 'Scripted Events' with tabs for 'Repository' (selected) and 'Activities'. A search bar and a 'Toby' user icon are at the top right. Below is a 'Filter By' section with a search input 'Install Adobe', a 'Customer' checkbox (unchecked), and a 'Global' checkbox (checked). Buttons for 'Refresh' and '+ Add Script' are on the right. A table lists scripts with columns: Name, Script, Type, Created on, and Actions. Two rows are shown: 'Install Adobe Reader' (Script: InstallAdobeReader.ps1, Type: Global, Created on: Jan 12, 2021, 12:42 PM) and 'Uninstall Adobe Reader' (Script: UninstallAdobeReader.ps1, Type: Global, Created on: Jan 12, 2021, 12:43 PM). The 'Actions' column for the second row contains a 'Download' button and a 'Clone' button, which is highlighted with a green box. Navigation links 'Previous', 'Page 1 of 1', and 'Next' are at the bottom of the table.

Microsoft Teams overview

This script package installs/uninstalls *Microsoft Teams* using the Chocolatey package manager (<https://chocolatey.org/>) to do the deployment. Chocolatey is deployed by VDS when VMs are created but this script will also check and install Chocolatey as a prerequisite if it is missing.



This Microsoft Teams install is specifically configured for deployments into an RDS environment. [A different Microsoft Teams script](#) is provided for AVD deployments.

Default shortcut path

The default shortcut path will be entered below, for this application the shortcut is: \\shortcut\Microsoft Teams.lnk

Add application install/uninstall activity

In order for a script in the repository to take any action, an activity must be created to associate that script with

a selected trigger. In this example activity will install/uninstall this application when the app is added to or removed from the workspace (from the *Workspace > Applications* page in VDS).

VDS scripted events offers many other types of activity triggers such as *Create Server* which could be used as an alternative to the *Application Install* (or *Application Uninstall*) event type. Using *Create Server* would simply run this app install against all newly created VMs in VDS. *Create Server* and other triggers are documented and can be explored [here](#).



This application will need to be present in the VDS application library. This [section](#) of the app entitlement for RDS article covers adding apps to the library.

To create an activity and link this script to an action:

1. Navigate to the *Scripted Events* section in VDS
2. Under *Activities* click *+ Add Activity*
3. In the opened dialog window enter the following information:
 - **Name:** Name this activity
 - **Description:** Optionally enter a description
 - **Deployment** Select the desired deployment from dropdown
 - **Script:** Select the install (or uninstall) script from the dropdown. This could be the global script or customer script you've cloned and customized.
 - **Arguments:** Leave blank
 - **Enabled checkbox:** Check the box
 - **Event Type:** Select *Application Install* (or *Application Uninstall*) from dropdown
 - **Application:** Select this application from dropdown
 - **Shortcut Path:** Enter the default shortcut path for this application (noted above)

Scripted Event Documentation - Microsoft Teams for AVD

Global Scripts Overview

NetApp VDS includes a library of pre-defined scripted events that can be used directly in VDS environments and/or duplicated and used as the building blocks for custom scripted events.

For this application, this article covers both the install/enable and uninstall/disable action.

Global Script Use

Built-in scripted events such as this one are pre-populated, checking the "global" filter checkbox will display them.

Global Scripted Events such as this one are read-only. They can be used as-is or the "Clone" function can be used to create a customer copy for editing and use.

The Clone button is found in the action menu on the Scripted Events page.

The screenshot shows the 'Scripted Events' section of the VDS interface. On the left is a sidebar with various navigation options like Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events (which is selected), Admins, Reports, Applications, Cost Estimator, and SaaS Backup. The main area has a header 'Scripted Events' with tabs 'Repository' (selected) and 'Activities'. A search bar at the top right contains the text 'Install Adobe'. Below it is a filter section with checkboxes for 'Customer' and 'Global', and a 'Refresh' and 'Add Script' button. A table lists two scripts:

Name	Script	Type	Created on	Actions
Install Adobe Reader	InstallAdobeReader.ps1	Global	Jan 12, 2021, 12:42 PM	⋮
Uninstall Adobe Reader	UninstallAdobeReader.ps1	Global	Jan 12, 2021, 12:43 PM	Download Clone ⋮

At the bottom of the page are links for 'Previous', 'Page 1 of 1', and 'Next'.

Microsoft Teams for AVD overview

This script package installs/uninstalls *Microsoft Teams AVD* using the Chocolatey package manager (<https://chocolatey.org/>) to do the deployment. Chocolatey is deployed by VDS when VMs are created but this script will also check and install Chocolatey as a prerequisite if it is missing.

! This Microsoft Teams install is specifically configured for deployments into a AVD environment with customizations and components specific to AVD in Azure. [A different Microsoft Teams script](#) is provided for RDS deployments.

Default shortcut path

The default shortcut path will be entered below, for this application the shortcut is: \\shortcut\Microsoft Teams AVD.lnk

Add activity dialog window screenshot

[scriptlibrary.activity.InstallMicrosoftTeamsAVD] | [scriptlibrary.activity.InstallMicrosoftTeamsAVD.png](#)

Add application install/uninstall activity

In order for a script in the repository to take any action, an activity must be created to associate that script with a selected trigger. In this example activity will install/uninstall this application when the app is added to or removed from the workspace (from the *Workspace > Applications* page in VDS).

VDS scripted events offers many other types of activity triggers such as *Create Server* which could be used as an alternative to the *Application Install* (or *Application Uninstall*) event type. Using *Create Server* would simply run this app install against all newly created VMs in VDS. *Create Server* and other triggers are documented and can be explored [here](#).

i This application will need to be present in the VDS application library. This [section](#) of the app entitlement for RDS article covers adding apps to the library.

To create an activity and link this script to an action:

1. Navigate to the *Scripted Events* section in VDS

2. Under *Activities* click + Add Activity

3. In the opened dialog window enter the following information:

- **Name:** Name this activity
- **Description:** Optionally enter a description
- **Deployment** Select the desired deployment from dropdown
- **Script:** Select the install (or uninstall) script from the dropdown. This could be the global script or customer script you've cloned and customized.
- **Arguments:** Leave blank
- **Enabled checkbox:** Check the box
- **Event Type:** Select Application Install (or Application Uninstall) from dropdown
- **Application:** Select this application from dropdown
- **Shortcut Path:** Enter the default shortcut path for this application (noted above)

Scripted Event Documentation - Nvidia Cuda Drivers

Global Scripts Overview

NetApp VDS includes a library of pre-defined scripted events that can be used directly in VDS environments and/or duplicated and used as the building blocks for custom scripted events.

For this application, this article covers both the install/enable and uninstall/disable action.

Global Script Use

Built-in scripted events such as this one are pre-populated, checking the "global" filter checkbox will display them.

Global Scripted Events such as this one are read-only. They can be used as-is or the "Clone" function can be used to create a customer copy for editing and use.

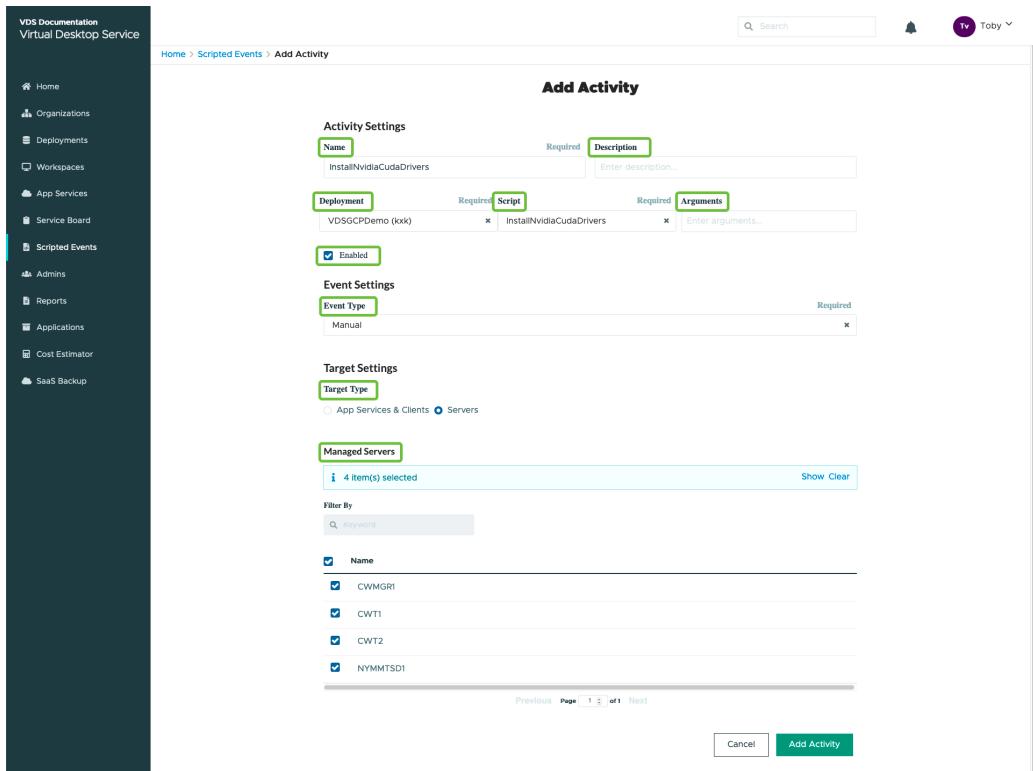
The Clone button is found in the action menu on the Scripted Events page.

The screenshot shows the 'Scripted Events' page in the NetApp VDS interface. The left sidebar contains navigation links for Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events, Admins, Reports, Applications, Cost Estimator, and SaaS Backup. The main content area has a header 'Scripted Events' with tabs for 'Repository' (selected) and 'Activities'. A search bar and a 'Refresh' button are at the top right. Below is a table with columns: Name, Script, Type, Created on, and Actions. Two rows are listed: 'Install Adobe Reader' (Script: InstallAdobeReader.ps1, Type: Global, Created on: Jan 12, 2021, 12:42 PM) and 'Uninstall Adobe Reader' (Script: UninstallAdobeReader.ps1, Type: Global, Created on: Jan 12, 2021, 12:43 PM). The 'Actions' column for the first row contains a 'Clone' button, which is highlighted with a green box.

Nvidia Cuda drivers overview

This script package installs/uninstalls *Nvidia Cuda Drivers* using the Chocolatey package manager (<https://chocolatey.org/>) to do the deployment. Chocolatey is deployed by VDS when VMs are created but this script will also check and install Chocolatey as a prerequisite if it is missing.

Add activity dialog window screenshot



Add Manual activity

In order for a script in the repository to take any action, an activity must be created to associate that script with a selected trigger. In this example activity runs when the VDS admin manually triggers the script.

VDS scripted events offers many other types of activity triggers such as *Create Server* which could be used as an alternative to the *Manual* event type. Using *Create Server* would simply execute this script on all newly created VMs in VDS. *Create Server* and other triggers are documented and can be explored [here](#).

To create an Activity and link this script to an action:

1. Navigate to the Scripted Events section in VDS
2. Under *Activities* click + Add Activity
3. In the opened dialog window enter the following information:
 - **Name:** Name this activity
 - **Description:** Optionally enter a description
 - **Deployment** Select the desired deployment from dropdown
 - **Script:** Select the install (or uninstall) script from the dropdown. This could be the global script or customer script you've cloned and customized.
 - **Arguments:** Leave blank

- **Enabled checkbox:** Check the box
- **Event Type:** Select Manual from dropdown
- **Target Type:** Select the Servers radio button
- **Managed Servers:** Check the box for each VM that should receive this uninstall.

Scripted Event Documentation - Nvidia GRID Drivers

Global Scripts Overview

NetApp VDS includes a library of pre-defined scripted events that can be used directly in VDS environments and/or duplicated and used as the building blocks for custom scripted events.

For this application, this article covers both the install/enable and uninstall/disable action.

Global Script Use

Built-in scripted events such as this one are pre-populated, checking the "global" filter checkbox will display them.

Global Scripted Events such as this one are read-only. They can be used as-is or the "Clone" function can be used to create a customer copy for editing and use.

The Clone button is found in the action menu on the Scripted Events page.

The screenshot shows the 'Scripted Events' page in the NetApp VDS interface. The left sidebar contains navigation links for Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events, Admins, Reports, Applications, Cost Estimator, and SaaS Backup. The main content area has a header 'Scripted Events' with tabs for 'Repository' (selected) and 'Activities'. A search bar and a 'Refresh' button are at the top right. Below is a table with columns: Name, Script, Type, Created on, and Actions. Two entries are listed: 'Install Adobe Reader' (Script: InstallAdobeReader.ps1, Type: Global, Created on: Jan 12, 2021, 12:42 PM) and 'Uninstall Adobe Reader' (Script: UninstallAdobeReader.ps1, Type: Global, Created on: Jan 12, 2021, 12:43 PM). The 'Actions' column for the second entry shows a 'Clone' button, which is highlighted with a green border. Navigation links 'Previous', 'Page 1 of 1', and 'Next' are at the bottom of the table.

Nvidia GRID drivers overview

This script package installs/uninstalls *Nvidia GRID Drivers* using the Chocolatey package manager (<https://chocolatey.org/>) to do the deployment. Chocolatey is deployed by VDS when VMs are created but this script will also check and install Chocolatey as a prerequisite if it is missing.

Add activity dialog window screenshot

The screenshot shows the 'Add Activity' dialog in the VDS Documentation Virtual Desktop Service. The 'Activity Settings' section includes fields for 'Name' (InstallNvidiaGridDrivers), 'Description' (Enter description...), 'Deployment' (VD5GCPDemo (okx)), 'Script' (InstallNvidiaGridDrivers), and 'Arguments' (Enter arguments...). The 'Event Settings' section has 'Event Type' set to 'Manual'. Under 'Target Settings', 'Target Type' is set to 'Servers'. In the 'Managed Servers' section, four items are selected: CWMGR1, CWT1, CWT2, and NYMMTS01. A 'Filter By' search bar is at the bottom left. At the bottom right are 'Cancel' and 'Add Activity' buttons.

Add Manual activity

In order for a script in the repository to take any action, an activity must be created to associate that script with a selected trigger. In this example activity runs when the VDS admin manually triggers the script.

VDS scripted events offers many other types of activity triggers such as *Create Server* which could be used as an alternative to the *Manual* event type. Using *Create Server* would simply execute this script on all newly created VMs in VDS. *Create Server* and other triggers are documented and can be explored [here](#).

To create an Activity and link this script to an action:

1. Navigate to the Scripted Events section in VDS
2. Under *Activities* click + Add Activity
3. In the opened dialog window enter the following information:
 - **Name:** Name this activity
 - **Description:** Optionally enter a description
 - **Deployment** Select the desired deployment from dropdown
 - **Script:** Select the install (or uninstall) script from the dropdown. This could be the global script or customer script you've cloned and customized.
 - **Arguments:** Leave blank
 - **Enabled checkbox:** Check the box
 - **Event Type:** Select Manual from dropdown
 - **Target Type:** Select the Servers radio button
 - **Managed Servers:** Check the box for each VM that should receive this uninstall.

Scripted Event Documentation - AVD Screen Capture Protection

Global Scripts Overview

NetApp VDS includes a library of pre-defined scripted events that can be used directly in VDS environments and/or duplicated and used as the building blocks for custom scripted events.

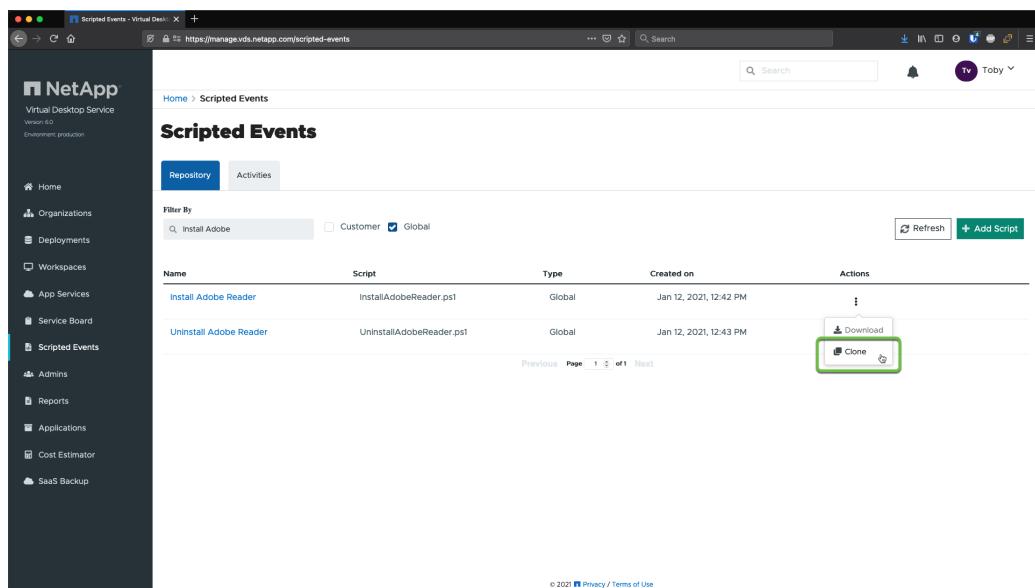
For this application, this article covers both the install/enable and uninstall/disable action.

Global Script Use

Built-in scripted events such as this one are pre-populated, checking the "global" filter checkbox will display them.

Global Scripted Events such as this one are read-only. They can be used as-is or the "Clone" function can be used to create a customer copy for editing and use.

The Clone button is found in the action menu on the Scripted Events page.



The screenshot shows the 'Scripted Events' page in the NetApp VDS web interface. The left sidebar contains navigation links for Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events, Admins, Reports, Applications, Cost Estimator, and SaaS Backup. The main content area has a title 'Scripted Events' with tabs for 'Repository' (selected) and 'Activities'. A search bar and a user profile for 'Toby' are at the top right. Below is a table with columns: Name, Script, Type, Created on, and Actions. Two rows are listed: 'Install Adobe Reader' (Script: InstallAdobeReader.ps1, Type: Global, Created on: Jan 12, 2021, 12:42 PM) and 'Uninstall Adobe Reader' (Script: UninstallAdobeReader.ps1, Type: Global, Created on: Jan 12, 2021, 12:43 PM). The 'Actions' column for the second row contains a 'Download' button and a 'Clone' button, which is highlighted with a green box.

AVD Screen Capture Protection overview

This script package enables/disables the native AVD feature *screen capture protection* by executing the (relevant) command with Powershell:

Enable:

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v fEnableScreenCaptureProtection /t REG_DWORD /d 1
```

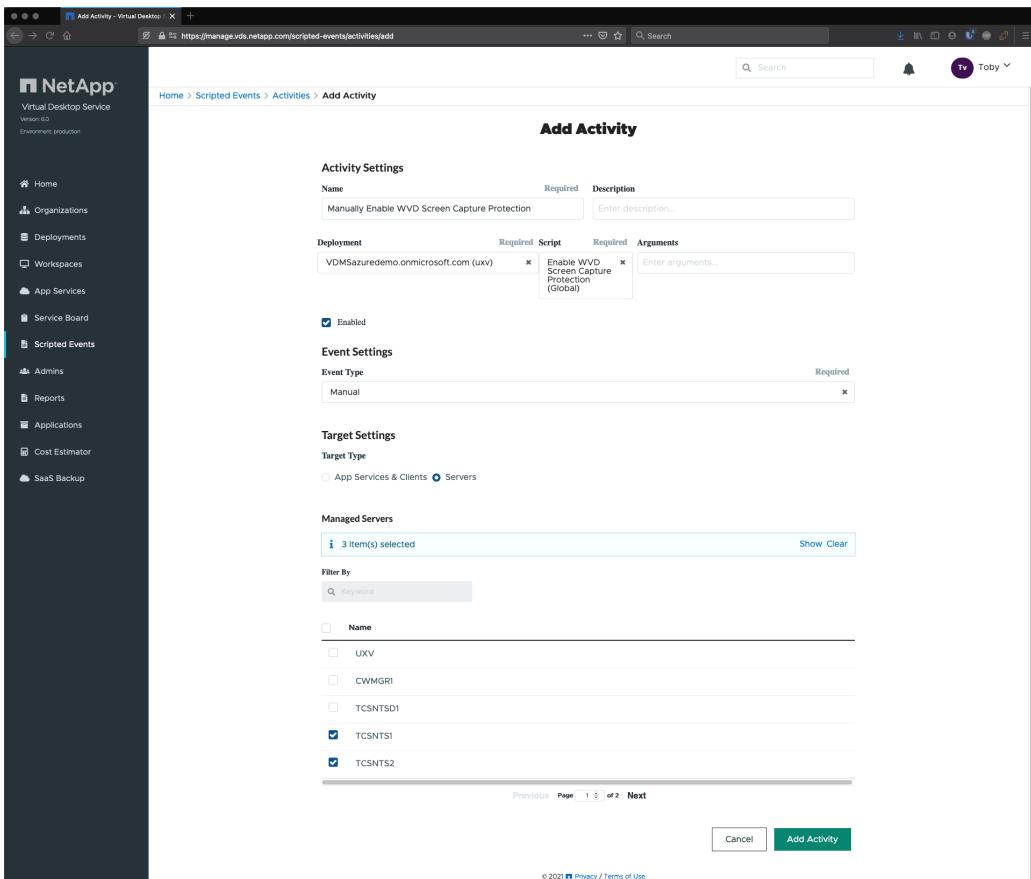
Disable:

```
reg delete "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v fEnableScreenCaptureProtection /f
```

Microsoft documentation on this AVD feature can be found here:

<https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide#session-host-security-best-practices>

Add activity dialog window screenshot



Add Manual activity

In order for a script in the repository to take any action, an activity must be created to associate that script with a selected trigger. In this example activity runs when the VDS admin manually triggers the script.

VDS scripted events offers many other types of activity triggers such as *Create Server* which could be used as an alternative to the *Manual* event type. Using *Create Server* would simply execute this script on all newly created VMs in VDS. *Create Server* and other triggers are documented and can be explored [here](#).

To create an Activity and link this script to an action:

1. Navigate to the Scripted Events section in VDS
2. Under *Activities* click + *Add Activity*
3. In the opened dialog window enter the following information:
 - **Name:** Name this activity
 - **Description:** Optionally enter a description
 - **Deployment** Select the desired deployment from dropdown
 - **Script:** Select the install (or uninstall) script from the dropdown. This could be the global script or customer script you've cloned and customized.
 - **Arguments:** Leave blank
 - **Enabled checkbox:** Check the box
 - **Event Type:** Select *Manual* from dropdown

- **Target Type:** Select the **Servers** radio button
- **Managed Servers:** Check the box for each VM that should receive this uninstall.

Scripted Event Documentation - Zoom VDI AVD

Global Scripts Overview

NetApp VDS includes a library of pre-defined scripted events that can be used directly in VDS environments and/or duplicated and used as the building blocks for custom scripted events.

For this application, this article covers both the install/enable and uninstall/disable action.

Global Script Use

Built-in scripted events such as this one are pre-populated, checking the "global" filter checkbox will display them.

Global Scripted Events such as this one are read-only. They can be used as-is or the "Clone" function can be used to create a customer copy for editing and use.

The Clone button is found in the action menu on the Scripted Events page.

Name	Script	Type	Created on	Actions
Install Adobe Reader	InstallAdobeReader.ps1	Global	Jan 12, 2021, 12:42 PM	⋮
Uninstall Adobe Reader	UninstallAdobeReader.ps1	Global	Jan 12, 2021, 12:43 PM	⋮ Download Clone

Zoom for VDI/AVD overview

This script package installs/uninstalls *Zoom VDI-AVD* using PowerShell to do the deployment.

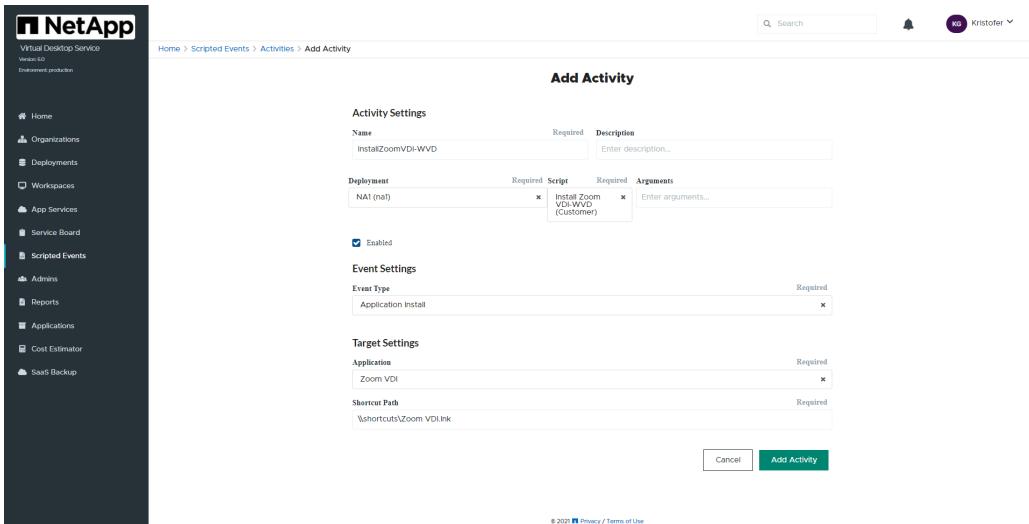


Zoom performance is improved if audio redirection is also enabled for the VDI/AVD environment.

Default shortcut path

The default shortcut path will be entered below, for this application the shortcut is: \\shortcuts\Zoom VDI.lnk

Add activity dialog window screenshot



Add application install/uninstall activity

In order for a script in the repository to take any action, an activity must be created to associate that script with a selected trigger. In this example activity will install/uninstall this application when the app is added to or removed from the workspace (from the *Workspace > Applications* page in VDS).

VDS scripted events offers many other types of activity triggers such as *Create Server* which could be used as an alternative to the *Application Install* (or *Application Uninstall*) event type. Using *Create Server* would simply run this app install against all newly created VMs in VDS. *Create Server* and other triggers are documented and can be explored [here](#).



This application will need to be present in the VDS application library. This [section](#) of the app entitlement for RDS article covers adding apps to the library.

To create an activity and link this script to an action:

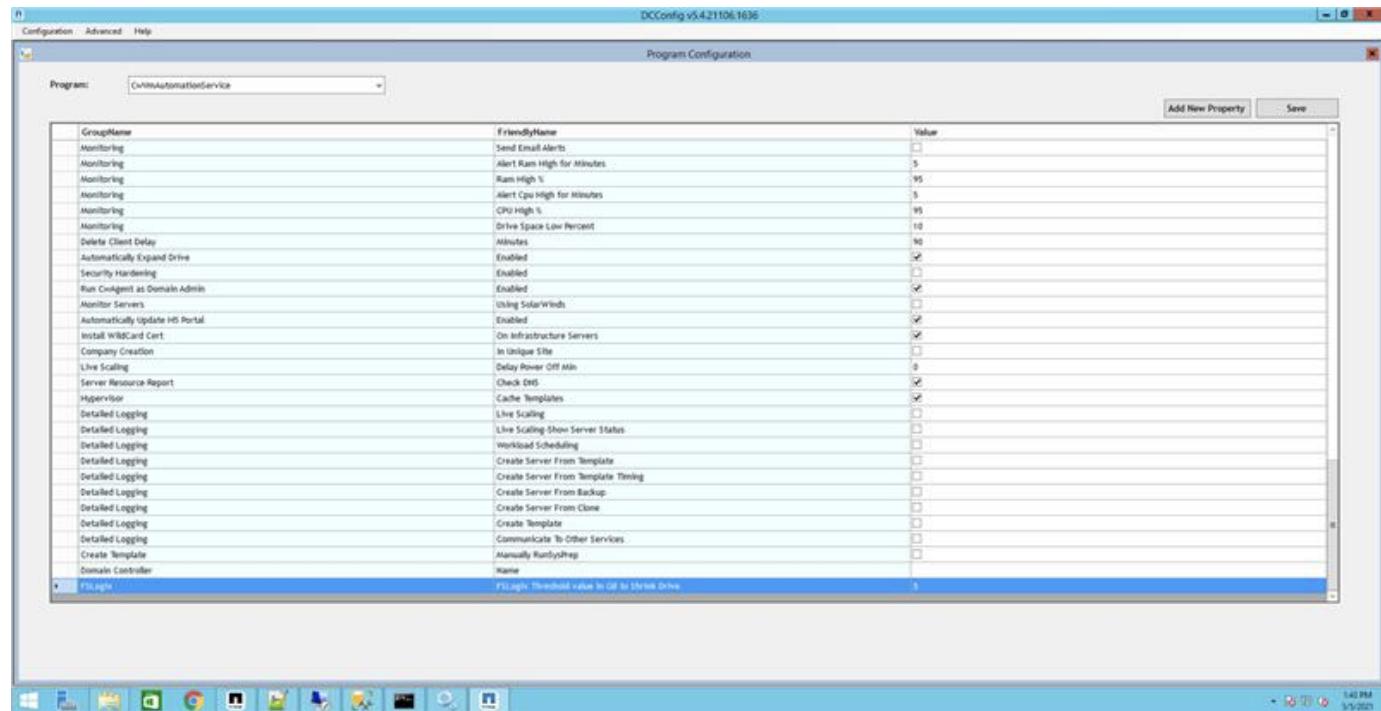
1. Navigate to the *Scripted Events* section in VDS
2. Under *Activities* click + *Add Activity*
3. In the opened dialog window enter the following information:
 - **Name:** Name this activity
 - **Description:** Optionally enter a description
 - **Deployment** Select the desired deployment from dropdown
 - **Script:** Select the install (or uninstall) script from the dropdown. This could be the global script or customer script you've cloned and customized.
 - **Arguments:** Leave blank
 - **Enabled checkbox:** Check the box
 - **Event Type:** Select *Application Install* (or *Application Uninstall*) from dropdown
 - **Application:** Select this application from dropdown
 - **Shortcut Path:** Enter the default shortcut path for this application (noted above)

Advanced

FSLogix Profile Shrink

Overview

VDS has a built-in profile shrink operation that runs nightly. This automation will automatically shrink the FSLogix container of a user's profile if 5GB or more can be saved. This automation runs nightly at 12:01am. The 5GB threshold is configurable in DCConfig, found on the CWMGR1 server.



NetApp VDS v5.4 videos

VDS Content on NetApp TV

VDS, GFC, and ANF - The Solution for Globally Deployed Cloud Desktops

Azure NetApp Files hosts high performance storage, while Virtual Desktop Service and Global File Cache manage workspaces and site regions from a single control panel for your globally deployed cloud desktops.



<https://tv.netapp.com/detail/video/6182654694001>

Deploy AVD or RDS Into Azure with NetApp VDS v5.4

Overview



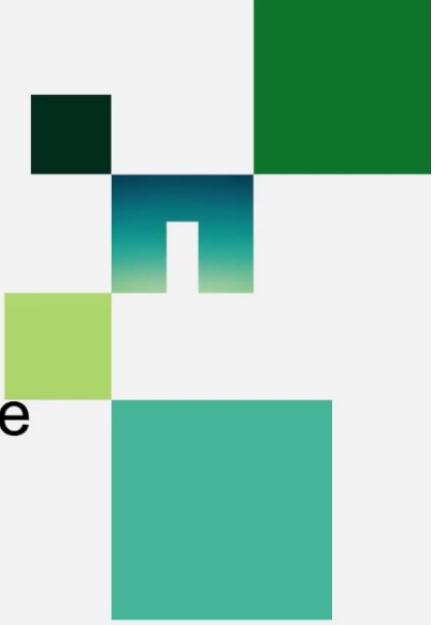
NetApp Virtual Desktop Service

Deployment & AD Connect

Toby vanRoojen
Product Marketing Manager
June, 2020

Create a AVD Host Pool with NetApp VDS v5.4

Overview



NetApp Virtual Desktop Service

Creating WVD Host Pools

Toby vanRoojen
Product Marketing Manager
June, 2020

Add and Manage AVD Users and App Groups in Azure with NetApp VDS v5.4

Overview



NetApp

NetApp Virtual Desktop Service

Managing Users and App Groups

Toby vanRoojen
Product Marketing Manager
June, 2020

Optimize Azure Resource Consumption in VDS 5.4

Overview



NetApp Virtual Desktop Service

Cost Containment and Optimization

Toby vanRoojen
Product Marketing Manager
June, 2020

=

Day to Day Administration of RDS and AVD with NetApp VDS v5.4

Overview

 | <https://img.youtube.com/vi/uGEgA3hFdM4/maxresdefault.jpg>

Update AVD host pool from v1 (Fall 2019) to v2 (Spring 2020)

Overview

This guide outlines the process of using the Virtual Desktop Service (VDS) interface to do an in-place upgrade of an existing AVD Fall Release (v1) host pool, resulting in a AVD Spring Release (v2) host pool. Without VDS, this transformation requires highly skilled architects to figure this out on their own or do a complete re-deployment of the environment.

Prerequisites

This guide assumes that the customer has the following:

- At least one Fall Release (v1) AVD host pool deployed
- A v5.4 (or greater) Virtual Desktop Service Deployment
- All VMs in the host pool must be online and running

It is worth noting that NetApp's Virtual Desktop Service can import existing host pools, so customers can

leverage VDS to perform in-place upgrades even if VDS was not used to deploy the host pool initially.



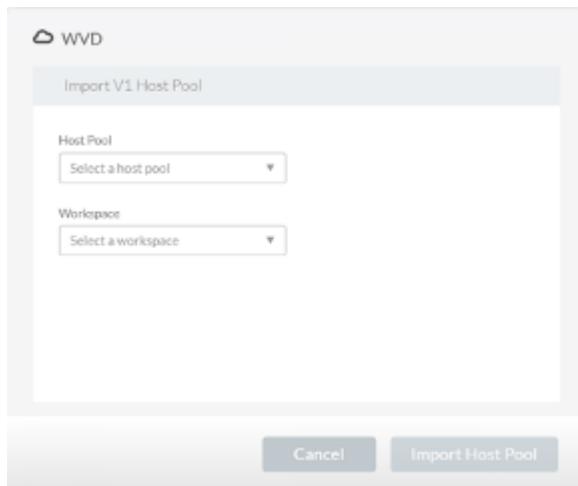
It is a best practice to perform this action during an established maintenance window in which end users are instructed not to log in (or the VMs are set to not allow user connections), as the end user desktops will not accessible while this action is performed.

Process steps

1. Navigate to the Workspaces module, then to the AVD tab. You will then see the Host Pools section, which now includes an option to leverage VDS' automation to upgrade a host pool.
2. Click on the link that reads Import V1 Host Pool to identify the Host Pool to be upgraded to V2 (the AVD Spring Release) to proceed.

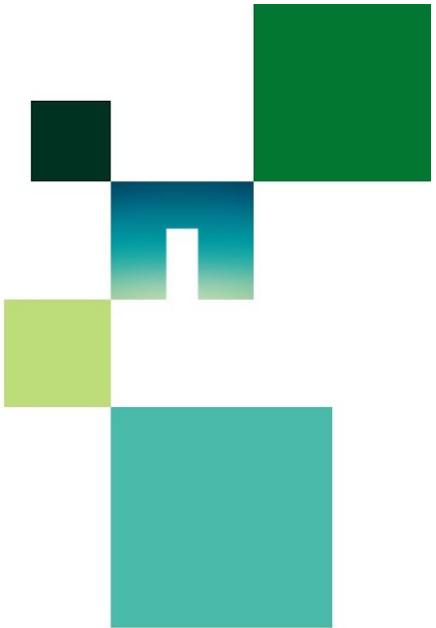


3. Next, select the host pool you want to upgrade from the drop-down menu and select the workspace to assign it to, then click Import Host Pool button to start the automated upgrade process.



4. Repeat this process for each host pool you want to upgrade. When the automation completes you will see your newly upgraded Spring Release (v2) host pool in the AVD tab of VDS.

Video demo



NetApp Virtual Desktop Service

Upgrading Spring (v1) WVD into Fall (v2)

Toby vanRoojen
Product Marketing Manager
September 2020

Please contact your service representatives with any additional questions you may have.

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.