



AVD Deployment Guide

Virtual Desktop Service

NetApp

June 09, 2021

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

Table of Contents

AVD Deployment Guide	1
Overview	1
AVD basics	1
Guide scope	2
Azure prerequisites	2
VDS setup sections	7
Install and configure AD Connect	11
Activating AVD services	12
Create AVD host pool	12
Enable VDS desktops for users	13
End user AVD access	19
Monitor user logins	19
Admin connection options	19
Optional post-deployment actions	20

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 including, 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

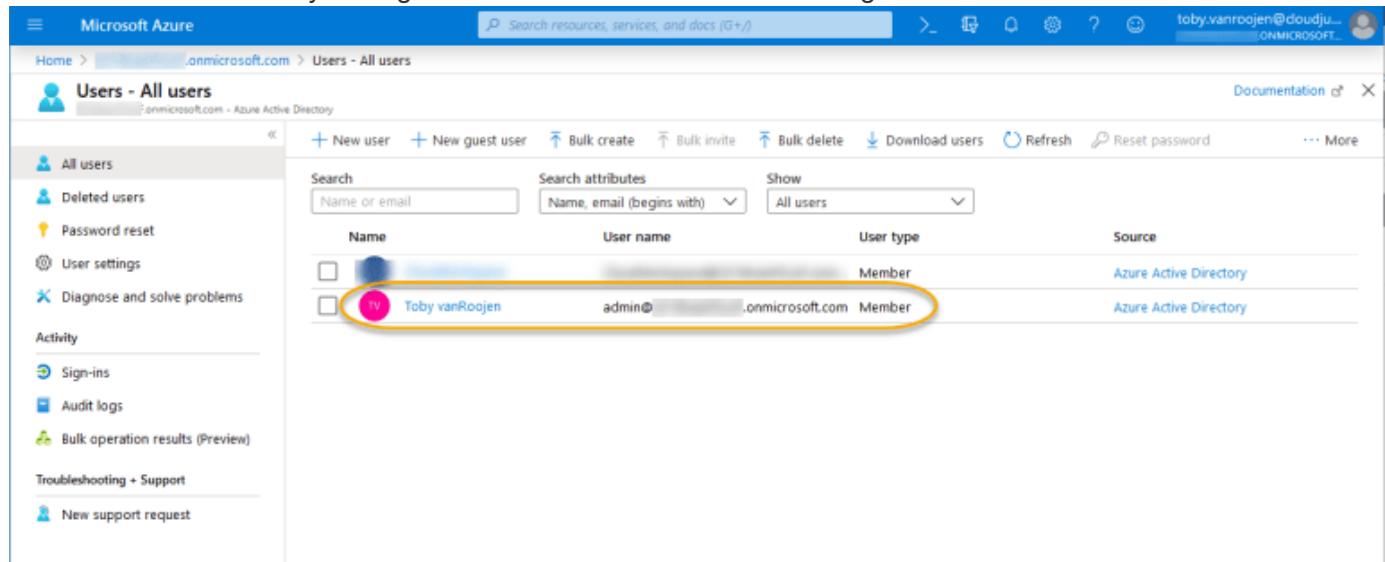


Detailed prerequisites are documented on [this PDF](#)

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 search filters for 'Name or email', 'Search attributes', and 'Show' (set to 'All users'). Below is a table with columns: Name, User name, User type, and Source. Two users are listed: one with a blue icon and one with a pink icon (Toby vanRoojen). Both are marked as 'Member' and come from 'Azure Active Directory'. The row for Toby vanRoojen is highlighted with a yellow oval, and his name is also circled in pink in the original image.

Name	User name	User type	Source
[Blue Icon]	[Redacted]	Member	Azure Active Directory
[Pink Icon] T	Toby vanRoojen	admin@.onmicrosoft.com	Member

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. The left sidebar has a 'Assigned roles' section selected. The main area displays a table of administrative roles. One row, 'Global administrator', is circled in yellow.

Role	Description	Resource Name	Type
Global administrator	Can manage all aspects of Azure AD and Microsoft services th...	Directory	Organization

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.

The screenshot shows the Microsoft Azure portal interface. The left sidebar has a 'Assigned roles' section selected. The main area shows a list of roles under 'Directory roles'. The 'Global administrator' role is selected and highlighted with a yellow circle. At the bottom right of the list, there is an 'Add' button, which is also highlighted with a yellow circle.

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. On the left, there's a sidebar with various navigation options like Overview, Activity log, and Access control (IAM). The main area is titled 'Azure subscription 1 - Access control (IAM)' and has tabs for 'Check access', 'Role assignments' (which is currently selected), 'Deny assignments', 'Classic administrators', and 'Roles'. Below the tabs, there's a search bar and filters for Name, Type, Role, and Scope. A table lists four items: two users, one group, and one service principal. The first user, 'Toby vanRoojen', is highlighted with a yellow circle around their 'Owner' role under the 'Role' column. The table also includes columns for 'Name', 'Type', 'Role', and 'Scope'.

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 dialog has a title 'Add role assignment' and a 'Role' dropdown set to 'Owner'. Below it, there's a 'Select' dropdown and a list of available identities. One identity, 'AAD DC Administrators', is selected. At the bottom of the dialog, there's a 'Selected members' section containing the account 'Toby vanRoojen'. The 'Save' button is highlighted with a blue border. The background shows the same 'Role assignments' table from the previous screenshot, but the 'Add' button in the header is now circled in yellow.

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

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 Aa2 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 DASv4 Family vCPUs	Microsoft.Compute	East US 2	0 % 0 of 0
Standard Dv1 Family vCPUs	Microsoft.Compute	East US 2	0 % 0 of 0
Standard DCv3 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

The screenshot shows the 'Provisioning' step of the VDS setup wizard. On the left, a sidebar menu includes 'TV', 'Demo', 'Provisioning' (which is expanded), 'IaaS and Platform' (selected), 'VMs and Network', 'Review', 'Status', and 'Help/Support'. The main area is titled 'Provisioning' and has a 'Save' button at the bottom right. The 'Infrastructure' section contains fields for 'Azure AD domain name' (set to 'demo.onmicrosoft.com'), 'Location' (set to 'West US 2'), 'Active Directory type' (set to 'New Windows Server Active Directory'), 'Active directory domain name' (set to 'demo.onmicrosoft.com'), 'File management' (set to 'Azure NetApp Files'), 'ANF service Level' (set to 'Premium'), 'Capacity Pool Size (TB)' (set to '4'), 'RDS license number (If using RDS)', 'Thinprint' (unchecked), and 'Notification email' (set to 'toby.vanroojen@netapp.com').

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

The screenshot shows the 'Provisioning' step of the NetApp VDS wizard. On the left, a sidebar shows the user profile (Toby vanRoojen) and navigation options: Demo, Provisioning (selected), IaaS and Platform, VMs and Network, Review, Status, and Help/Support. The main area is titled 'Provisioning' and 'VMs and Network Configuration'. It includes fields for 'Platform VM configuration' (Single virtual machine selected), 'Time zone' (America/Los Angeles, Vancouver (UTC-07:00)), 'Virtual network scope' (10.0.0.0/20), and 'Network subnet groups' (listing Tenant, Services, Platform, and Directory subnets). A 'Validate' button shows a success message: 'Validation of network scope succeeded'. At the bottom are 'Save' and 'Next →' buttons.

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.

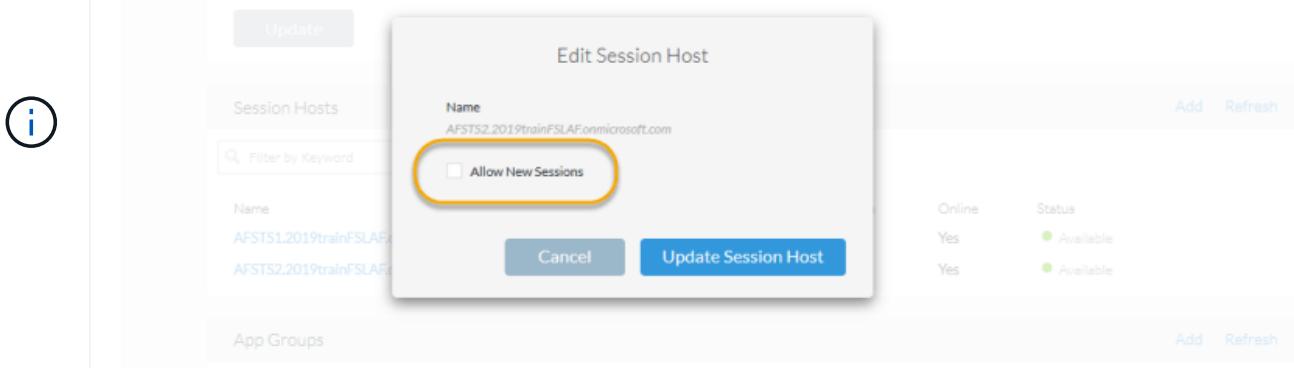
The screenshot shows the 'WVD Host Pools' section within the 'TrainWWD2's Workspace (rs6a)' page. The left sidebar has 'Workspaces' selected. The main area shows a table with one row named 'hostpool1'. The 'Add' button is highlighted with a large black arrow pointing to it.

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

- Click on the Users and Groups tab

The screenshot shows the Cloud Workspace interface. The left sidebar has a 'Workspaces' section with several items: Dashboard, Organizations, Deployments, Workspaces (which is selected and highlighted in blue), App Services, Service Board, Scripted Events, Admins, and Reports. The main content area is titled 'TrainWVD2's Workspace (rs6a)' and shows the 'Users & Groups' tab selected. On the left, there's a 'Groups' section with a search bar and a table for managing groups. On the right, there's a 'Users' section with a search bar, a warning message about pending approvals, and a table listing users. The user 'Toby vanRoojen' is listed with a status of 'Pending (Pending Cloud Workspace)' and an 'Offline' connection status. The 'Add' button is visible at the top right of the users section.

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

This screenshot is similar to the previous one, showing the 'Users & Groups' tab selected. However, the 'Enable Cloud Workspace' button for the user 'Toby vanRoojen' is now highlighted with a blue box and a black arrow points to it. The user's status has changed to 'Available' with an 'Online' connection status. The rest of the interface remains the same, with the 'Groups' and 'Users' sections visible.

- 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 'CJCS 5.3 WVD'. The left sidebar has a 'Workspaces' menu item selected. The main area shows 'WVD Details' with a Tenant ID and an 'HTML5 URL' pointing to <https://rdweb.wvd.microsoft.com/webclient/index.html>. Below this is the 'WVD Host Pools' section, which contains a table with one row. The row has columns for Name ('apps'), Description ('apps'), Tenant ('z58b'), Type ('Shared'), and Session Hosts (values 1 and 4). A yellow arrow points to the 'Desktop Users' link in the 'Name' column. At the bottom of the table, there is a 'Filter by Keyword' input field and a 'Add' button.

Name	Description	Tenant	Type	Session Hosts
apps Desktop Users	apps Hostpool for Desktop Users	z58b	Shared	1 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 modal titled 'Edit Session Host' with fields for 'Name' (Z58BTS1) and 'Allow New Sessions' (checked). A yellow arrow points from this modal to the 'Session Hosts' table below. The table lists four hosts: Z58BTS1, Z58BTS2, Z58BTS3, and Z58BTS4, all with 'Allow New Session' set to 'Yes' and 'Sessions' at 0. A yellow box highlights the first host, Z58BTS1.

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' (Name: hostpool1, Description: First Host Pool, Host Pool Type: Shared, Load Balancer Type: BreadthFirst, Max Session Limit Per Server: 999999) and 'Session Hosts' (two hosts listed). Below these is the 'App Groups' section, which contains a single entry: 'Desktop Application Group' (Name: Desktop Application Group, Description: Desktop Application Group, Resource: Desktop, Users: 1, Remote Apps: 1). A black arrow points to the 'Users' link under the 'Desktop Application Group' entry.

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

The screenshot shows the Cloud Workspace interface with the 'Host Pool Details' page for 'WVD Host Pool hostpool1'. A modal window titled 'Edit App Group' is displayed, containing fields for 'Description' (set to 'Desktop Application Group') and a 'Users' section which shows '1 users added'. Below the modal, the main host pool details are visible, including the host pool name, description ('First Host Pool'), and type ('Shared'). The 'App Groups' section shows one group named 'Desktop Application Group' with one user assigned. The 'Active Users' section indicates no active users found.

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:

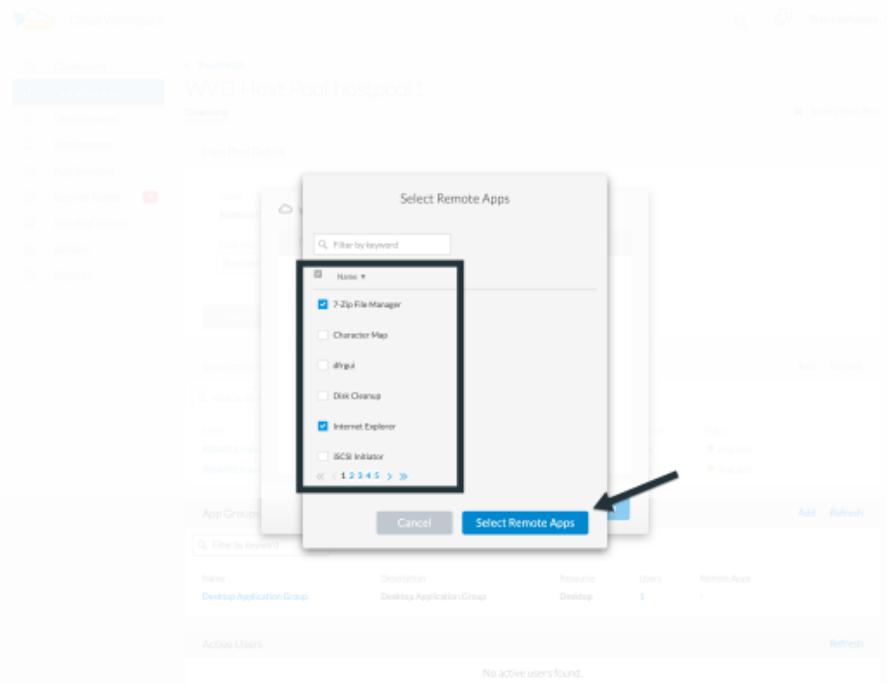
1. Click the Add button in the app groups section header

The screenshot shows the Cloud Workspace interface for managing a WVD Host Pool named 'hostpool1'. In the 'Host Pool Details' section, the host pool is described as a 'First Host Pool' of type 'Shared'. The 'Session Hosts' section lists two hosts: 'RS6AT51.trainwvd.com' and 'RS6AT52.trainwvd.com', both marked as 'Available'. The 'App Groups' section shows a single group named 'Desktop Application Group' associated with a 'Desktop' resource and one user. An arrow points to the 'Add' button in the 'App Groups' section.

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

The screenshot shows the 'Select Remote Apps' dialog box overlaid on the Cloud Workspace interface. The dialog lists various applications installed on the virtual machine, including 7-Zip File Manager, Character Map, Disk Cleanup, Internet Explorer, and SCSI Initiator. Two applications are selected: '7-Zip File Manager' and 'Internet Explorer'. An arrow points to the 'Select Remote Apps' button at the bottom right of the dialog.

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.



- 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 for 'TrainWVD2's Workspace (rs6a)'. The left sidebar has a 'Workspaces' menu item highlighted with a blue box. Three arrows point to the 'Groups' tab, the 'Add' button, and the 'Users' table. The 'Users & Groups' tab is selected. The 'Groups' section shows 1 total user and 2 users. The 'Users' section shows two users: 'Toby vanRooijen' and 'WVD User1'. Both users are listed as available and offline.

Name	Username	Status	Connection Status
Toby vanRooijen	admin@trainwv...	Available	Offline
WVD User1	WvDUser1@r...	Available	Offline

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

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

choose users

assign applications

Update Group

rs6a-all users

Users

Name	Username
<input checked="" type="checkbox"/> WVD User1	WVDUser1@trainwvd2.onmicrosoft.com
<input checked="" type="checkbox"/> Toby vanRoejen	admin@trainwvd2.onmicrosoft.com

Cancel **Update Group**

TrainWVD2

rs6a-all users's Applications

Applications

Name
<input checked="" type="checkbox"/> Todo - Current Version (v. Latest)
<input type="checkbox"/> Calculator

Cancel **Update**

Configure cost optimization options

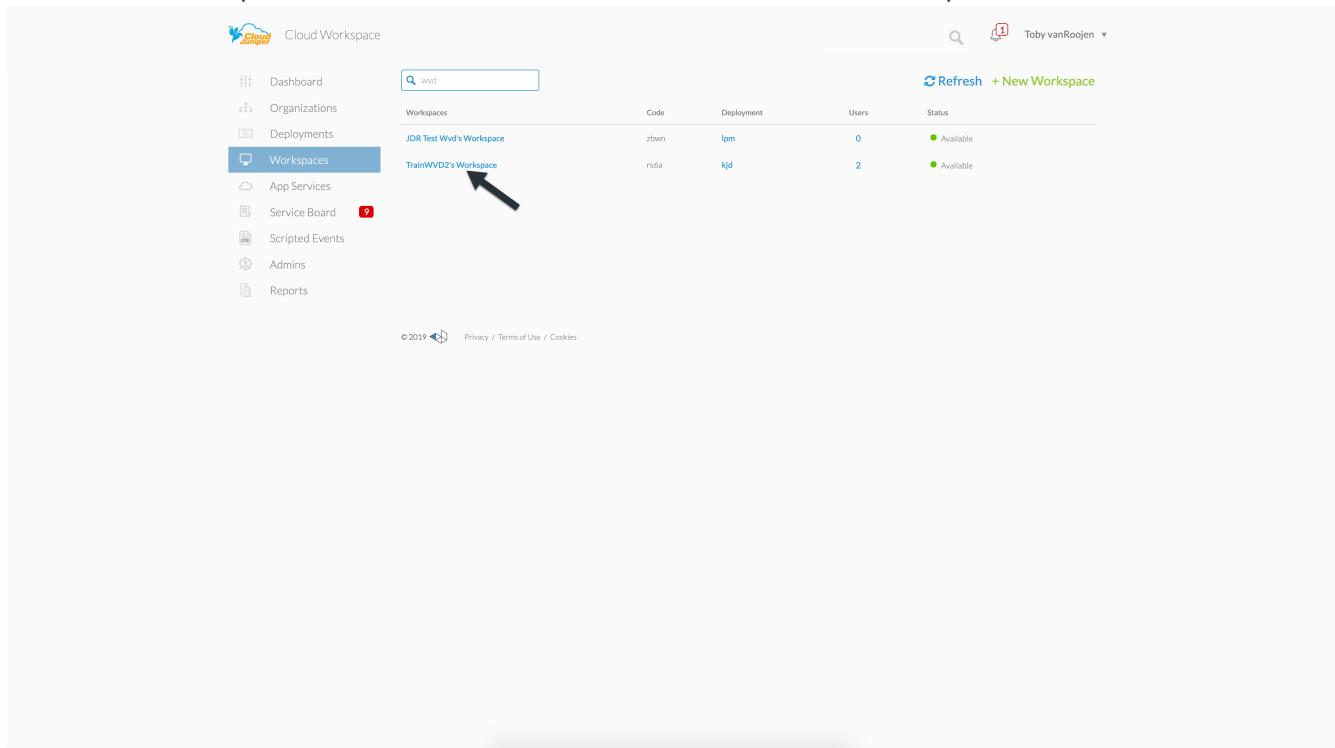
Workspace management also extends to managing the Azure resources that support the AVD implementation. VDS allows you to configure both Workload Schedules and Live Scaling to turn Azure virtual machines on and off based on end user activities. These features result in matching Azure resource utilization 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.



The screenshot shows the Cloud Workspace web interface. On the left, there is a sidebar with various menu items: Dashboard, Organizations, Deployments, Workspaces (which is selected and highlighted in blue), App Services, Service Board (with a red notification badge), Scripted Events, Admins, and Reports. In the center, there is a search bar with the text 'wvd'. Below it is a table titled 'Workspaces' with the following data:

Workspace	Code	Deployment	Users	Status
JDR Test Wvd's Workspace	zbnw	lpm	0	● Available
TrainWVD2's Workspace	rs6a	kjd	2	● Available

At the bottom of the page, there is a footer with links for 'Privacy / Terms of Use / Cookies' and copyright information: '© 2019'. There is also a 'Refresh' button and a '+ New Workspace' link in the top right corner.

3. Click on the Workload Schedule tab.

Cloud Workspace

TrainWVD2's Workspace (rs6a)

Overview Users & Groups VM Resource Workload Schedule WVD

Active Users

Resource Consumption

Deployment

trainwvd2.onmicrosoft.com (kjd) Azure Available

No App Services.

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

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

Cloud Workspace

TrainWVD2's Workspace (rs6a)

Overview Users & Groups VM Resource **Workload Schedule** WVD

Live Scaling

Enabled Disabled

Extra Powered On Servers Enabled

Shared Users Per Server Enabled

Number of Shared Users Per Server
2

Max Shared Users Per Server Enabled

Update

Workload Schedule

Description
Workload is running 24/7

Custom Scheduling
Off

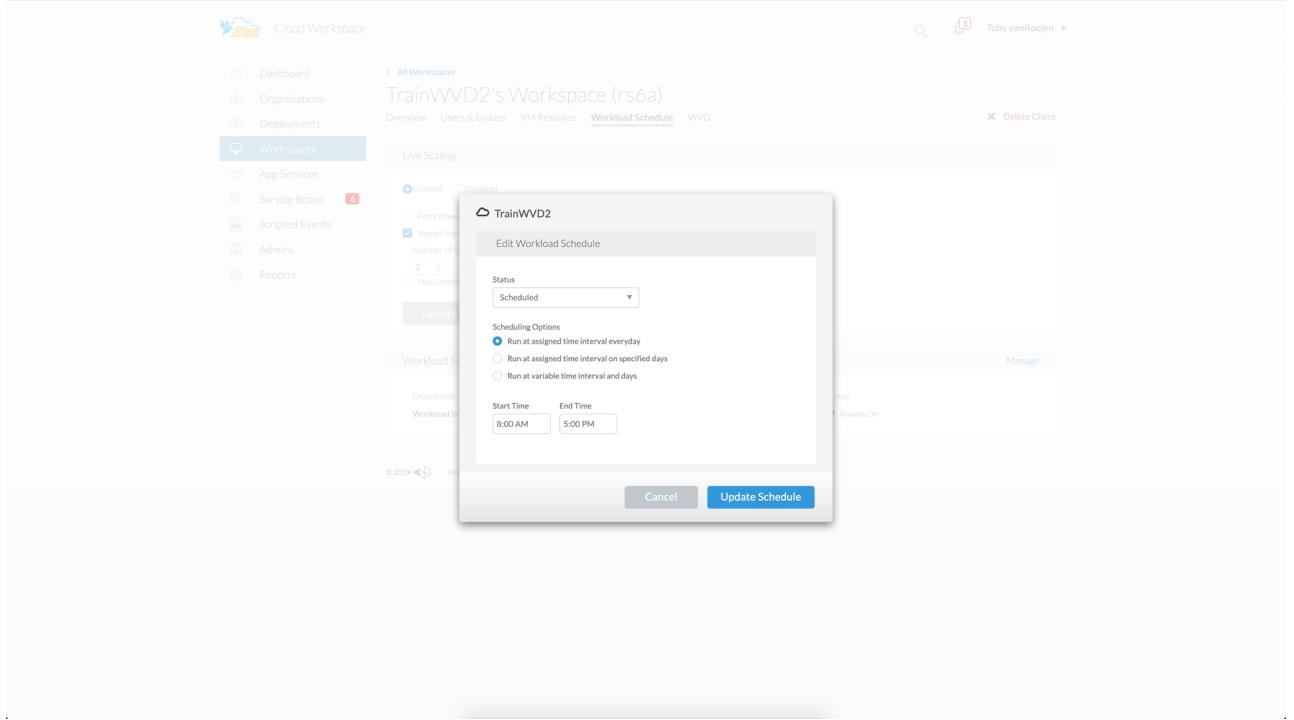
Status
Always On

Manage

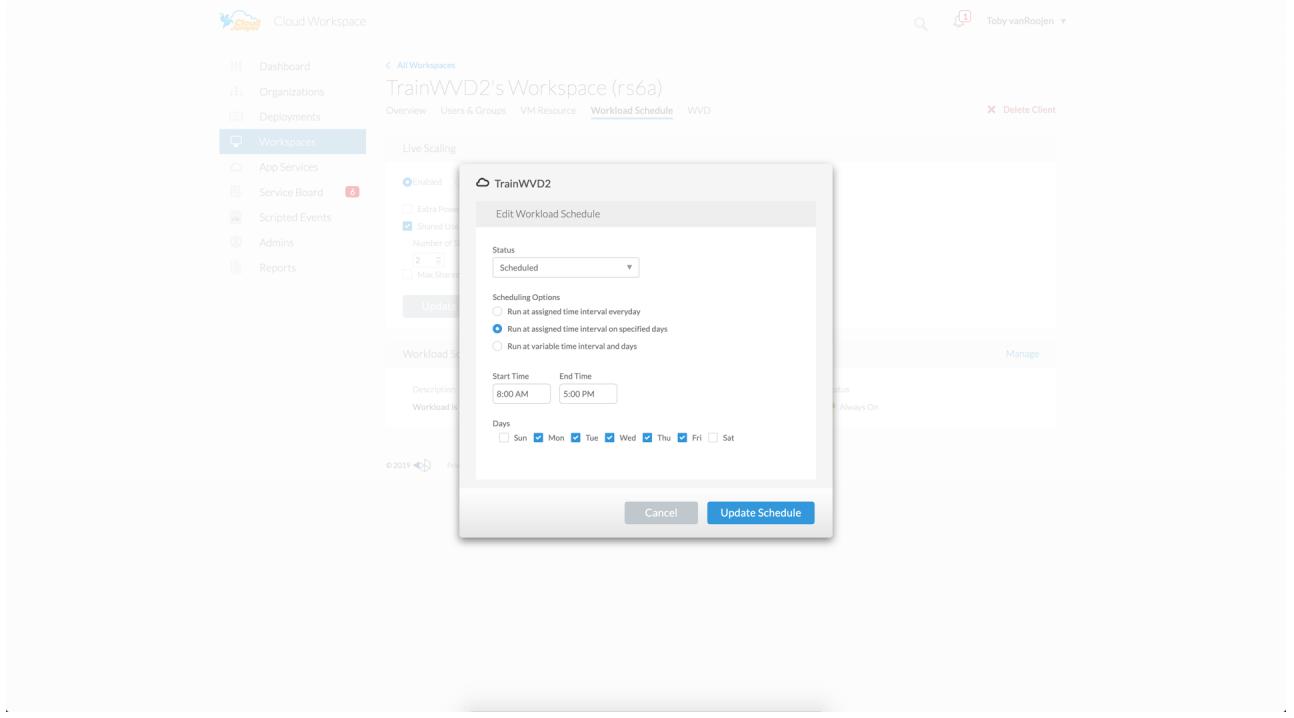
5. Choose a default state from the Status drop down: Always On (default), Always Off, or Scheduled.

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.



- b. 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.

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 it's 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. On the left, there is a sidebar with various menu items: Dashboard, Organizations, Deployments, Workspaces (which is selected and highlighted in blue), App Services, Service Board (with a red notification badge), Scripted Events, Admins, and Reports. In the center, there is a search bar with the text 'wvd'. Below the search bar is a table titled 'Workspaces' with two rows. The first row is for 'JDR Test Wvd's Workspace' and the second row is for 'TrainWVD2's Workspace'. The 'TrainWVD2's Workspace' row has a black arrow pointing to it from the left. The table columns include 'Code' (zbnw, rs6a), 'Deployment' (lpm, kjd), 'Users' (0, 2), and 'Status' (Available, Available). At the top right, there is a 'Refresh' button and a '+ New Workspace' link. The bottom of the page includes copyright information and links for Privacy, Terms of Use, and Cookies.

3. Click on the Workload Schedule tab.

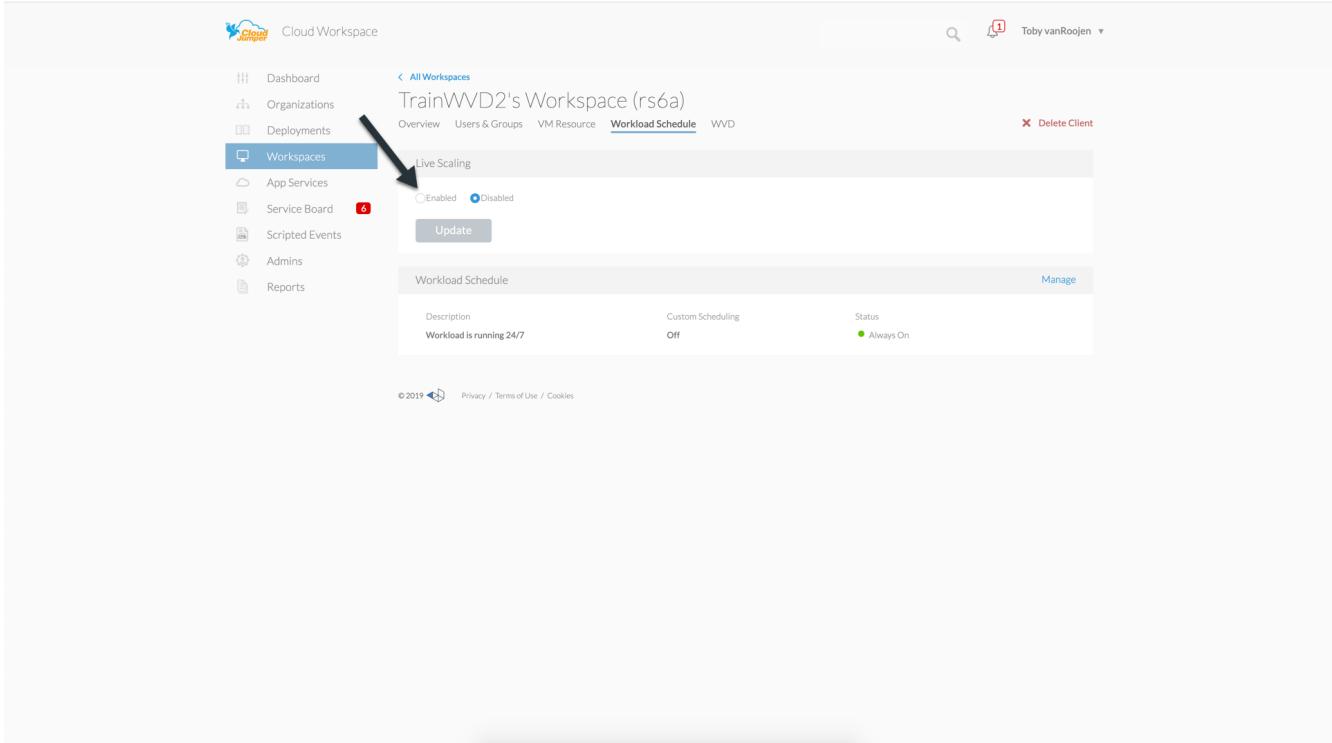
The screenshot shows the 'TrainWVD2's Workspace (rs6a)' page. The top navigation bar includes 'All Workspaces', 'Overview', 'Users & Groups', 'VM Resource', 'Workload Schedule' (which is selected and highlighted in blue), and 'VWD'. Below the navigation bar are two line charts: 'Active Users' and 'Resource Consumption'. The 'Active Users' chart shows a single orange line with data points at approximately 0.8, 0.8, 0.8, 0.8, 0.8, 0.8, 0.8, 0.8, 0.8, 1.5, and 2.0. The 'Resource Consumption' chart shows two lines: 'Total CPU' (blue) and 'Total RAM (GB)' (green). The 'Total CPU' line remains flat at 2.0 until August 19, then rises to 4.0. The 'Total RAM (GB)' line starts at 8.0, drops to 4.0, stays flat until August 19, then rises to 10.0. A legend indicates 'Last 7 Days' for the resource consumption data. Below the charts, there are sections for 'Deployment' (trainwvd2.onmicrosoft.com (kj)) and 'App Services' (No App Services). At the bottom, there are two tables: 'Company Details' and 'Contact Details'.

Company Name	Company Code	Primary Notification Email	Phone
TrainWVD2	rs6a		

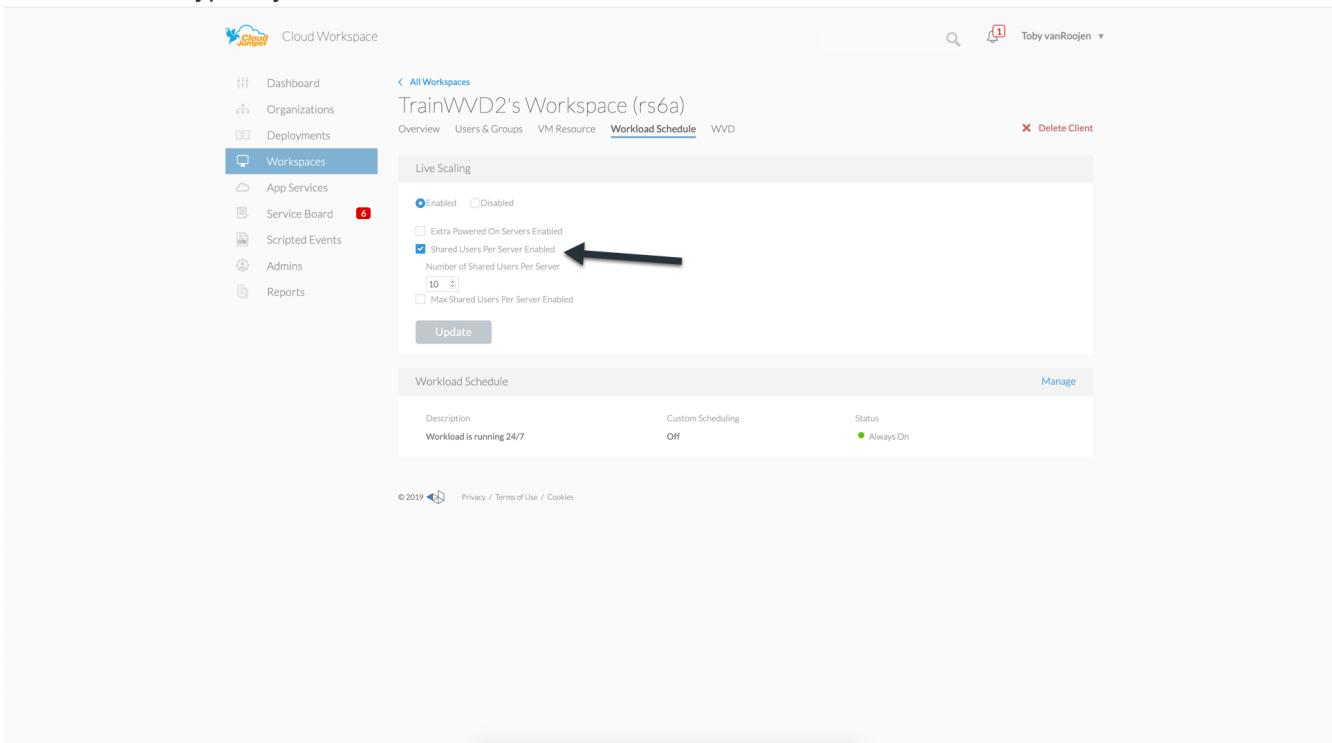
Status	Partner	Address 1	Address 2
Available	CloudJumper CSP Master		

Organization Type	Login Identifier	City	Zip Code
Client	@trainwvd2.onmicrosoft.com	Garner	

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



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.



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 Cloud Workspace interface with the 'Workspaces' menu selected. A modal dialog is open for 'TrainWVD2's Workspace (rs6a)'. Inside the dialog, under the 'Workload Schedule' tab, there are several configuration options:

- Enabled
- Disabled
- Extra Powered On Servers Enabled
- Shared Users Per Server Enabled
- Number of Shared Users Per Server: 10
- Max Shared Users Per Server Enabled

At the bottom left of the dialog is a 'Update' button.

i 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.

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

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

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	0	● Offline	● Available

3. Click on the gear, then choose Stop.

The screenshot shows the Cloud Workspace interface with the 'Deployments' tab selected. A search bar at the top contains the text 'wvd'. A warning message indicates there are 16 deployments requiring manual intervention. The main table lists two deployments: 'trainwvd2.onmicrosoft.com' (Code: kjd, Version: 5.3, Infrastructure Platform: Azure, Clients: 1, Connection: Online, Status: Available) and 'wvdgpu.onmicrosoft.com' (Code: ceb, Version: 5.2, Infrastructure Platform: Azure, Clients: -, Connection: Offline, Status: Available). A context menu is open over the 'Status' column for the first deployment, with the 'Stop' option highlighted by a black arrow.

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

The screenshot shows the Cloud Workspace interface with the 'Deployments' tab selected. A search bar at the top contains the text 'wvd'. A warning message indicates there are 16 deployments requiring manual intervention. The main table lists two deployments: 'trainwvd2.onmicrosoft.com' (Code: kjd, Version: 5.3, Infrastructure Platform: Azure, Clients: 1, Connection: Online, Status: Available) and 'wvdgpu.onmicrosoft.com' (Code: ceb, Version: 5.2, Infrastructure Platform: Azure, Clients: -, Connection: Offline, Status: Available). A context menu is open over the 'Status' column for the first deployment, with the 'Start' option highlighted by a black arrow.



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)

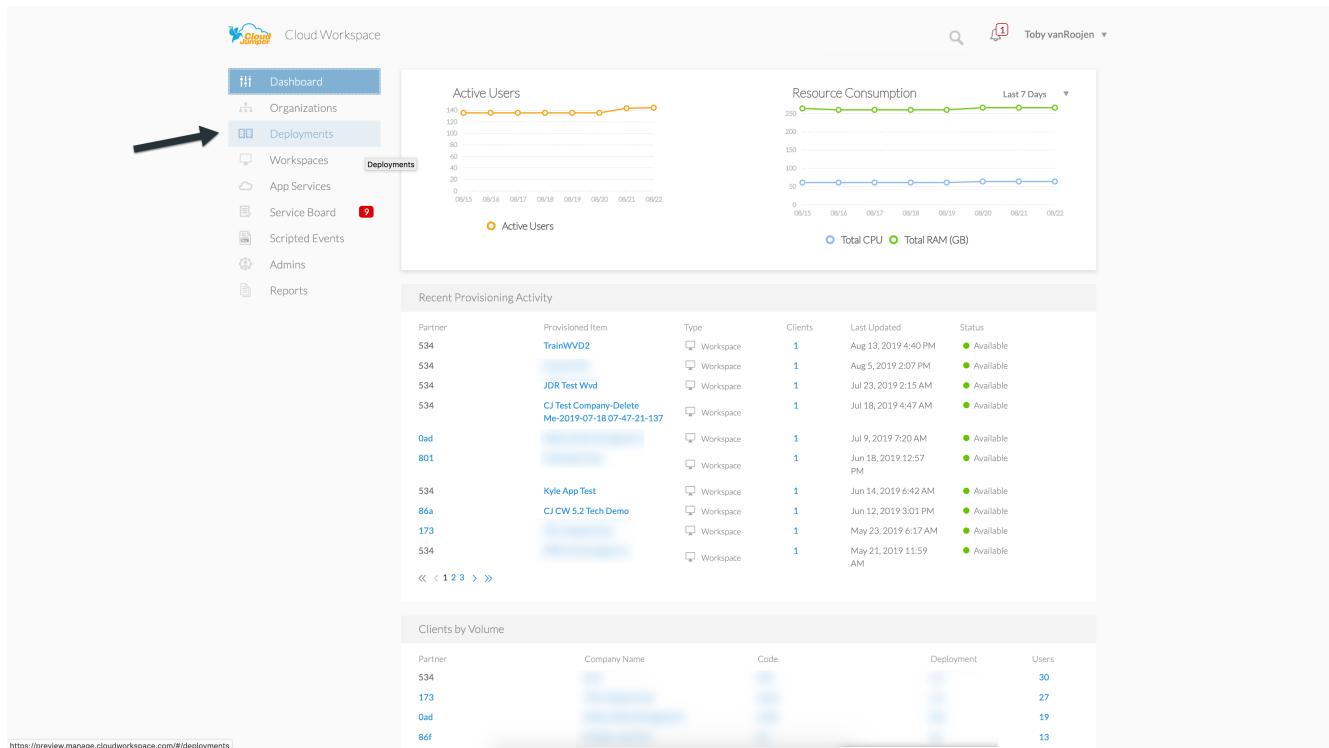
Using a controlled workspace is the default mode for VDS deployments. The polices are applied automatically. This mode requires VDS Administrators to install applications and then end users are granted access to the application via a shortcut on the session desktop. In a similar fashion, access to the 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

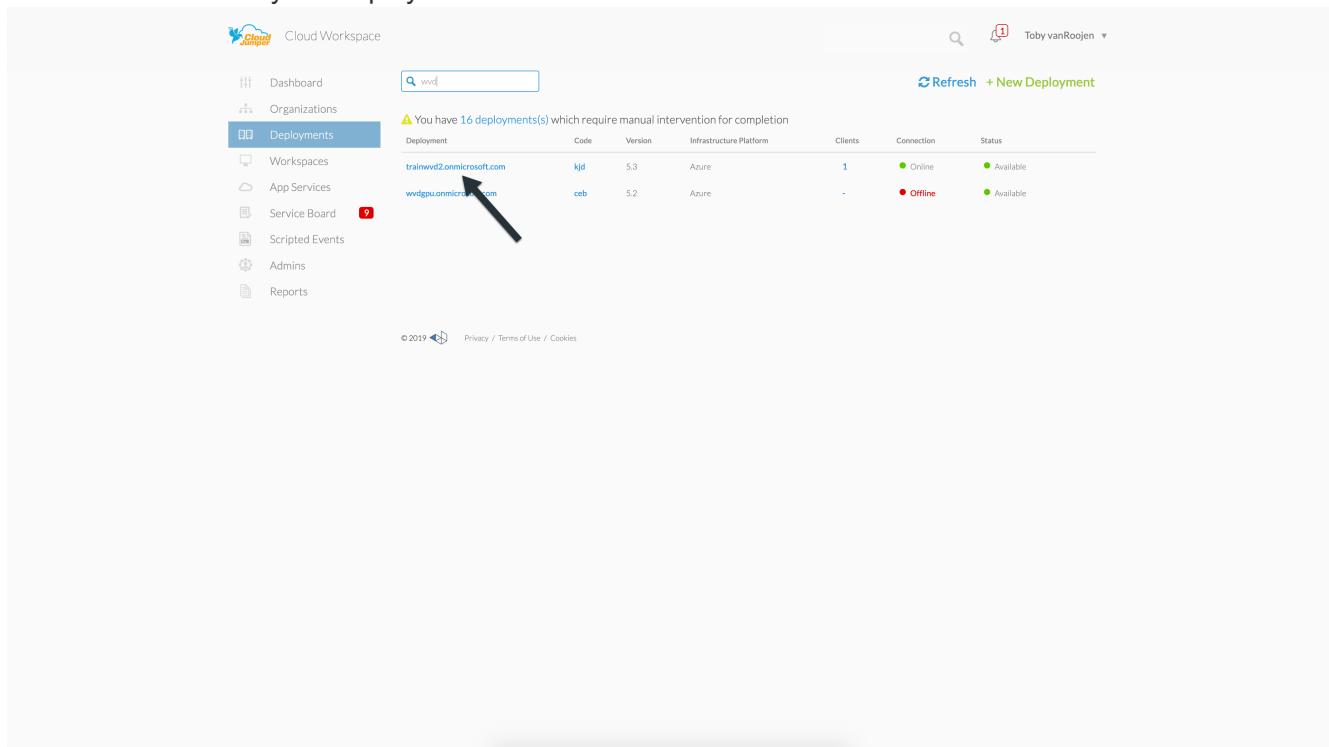
Creating a basic workspace requires disabling the default GPO policies that are created by default.

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.



3. Click on the name of your Deployment.



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

Refresh

CWMGR1 2 4 Online

Connect

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

Refresh

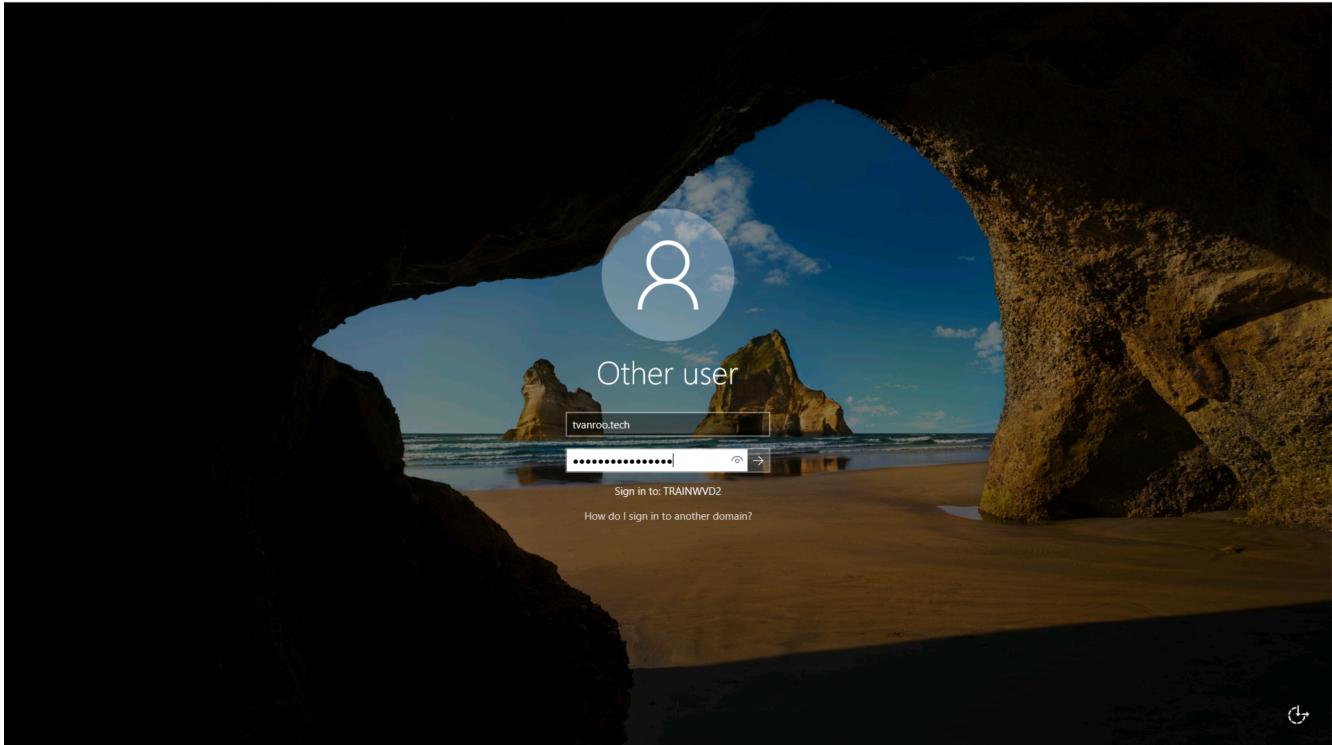
CWMGR1 2 4 Online

Backup

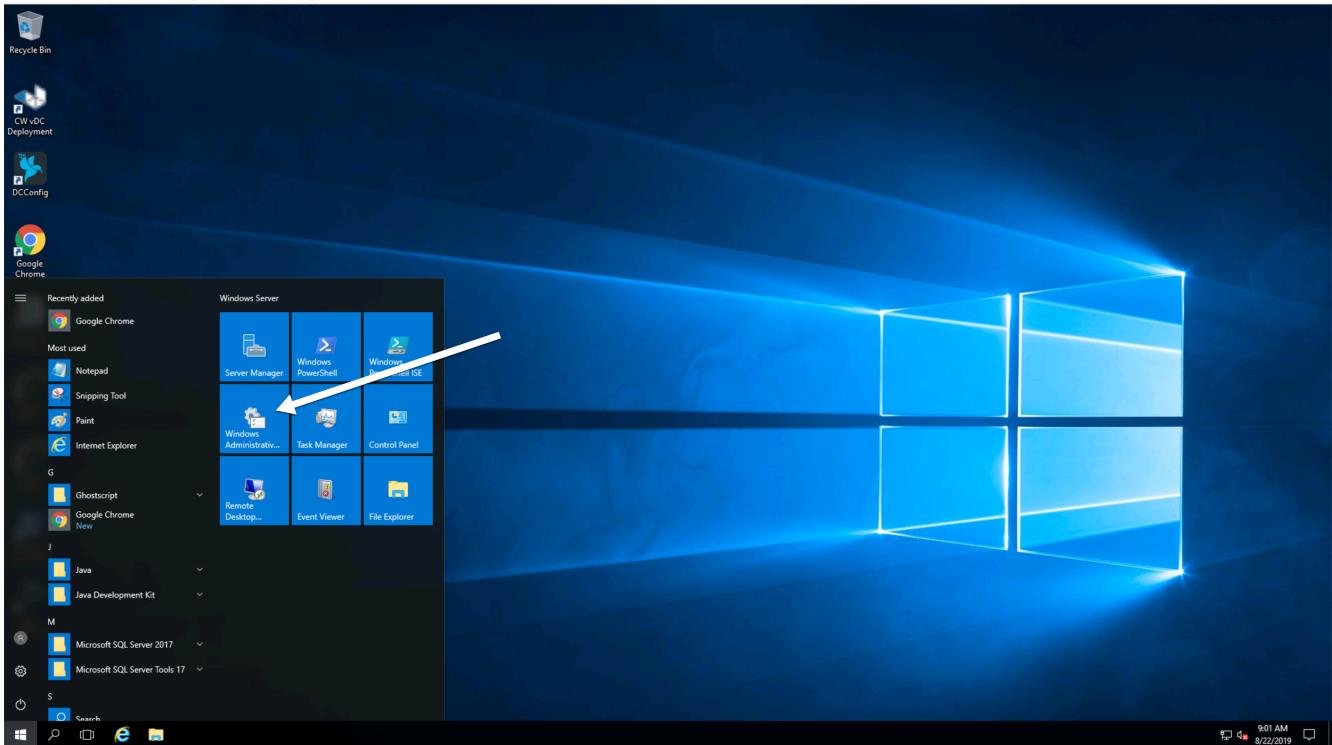
Connect

Connect

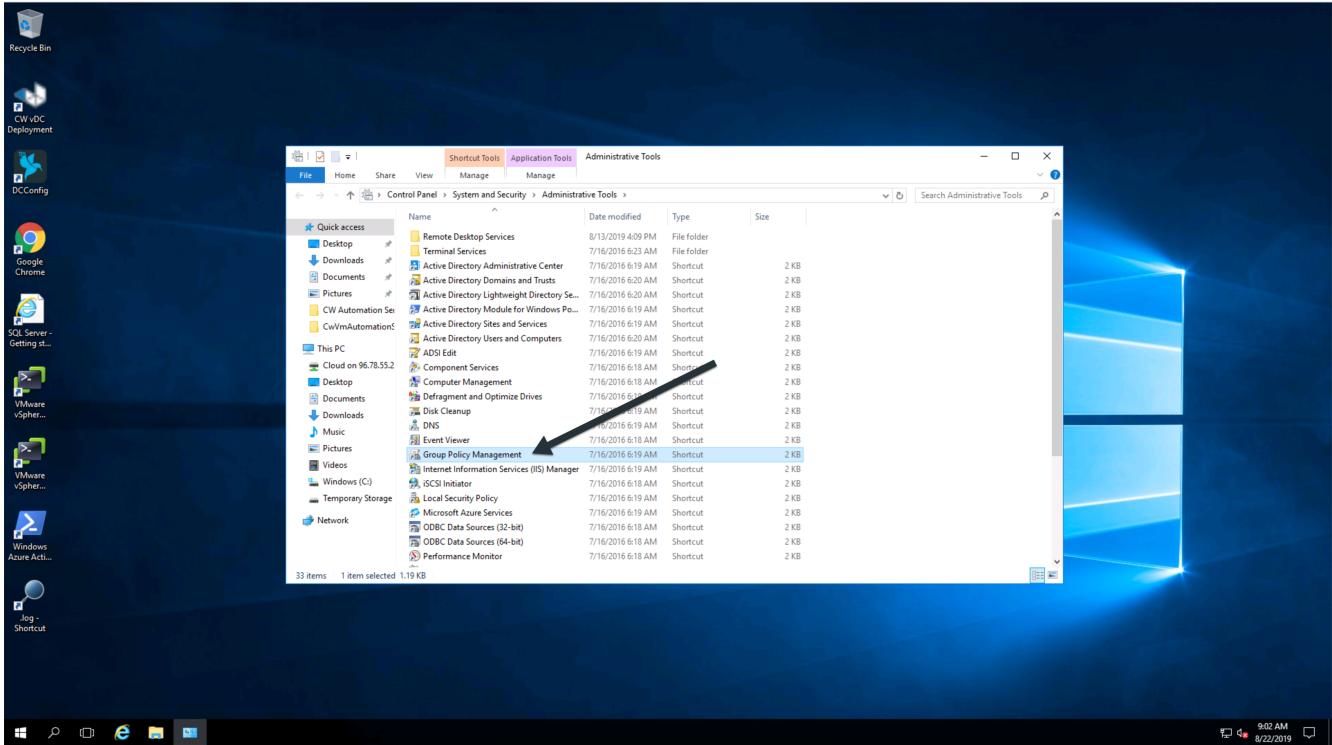
6. Enter the “Tech” credentials you created during provisioning to log on to the CWMGR1 server using HTML5 access.



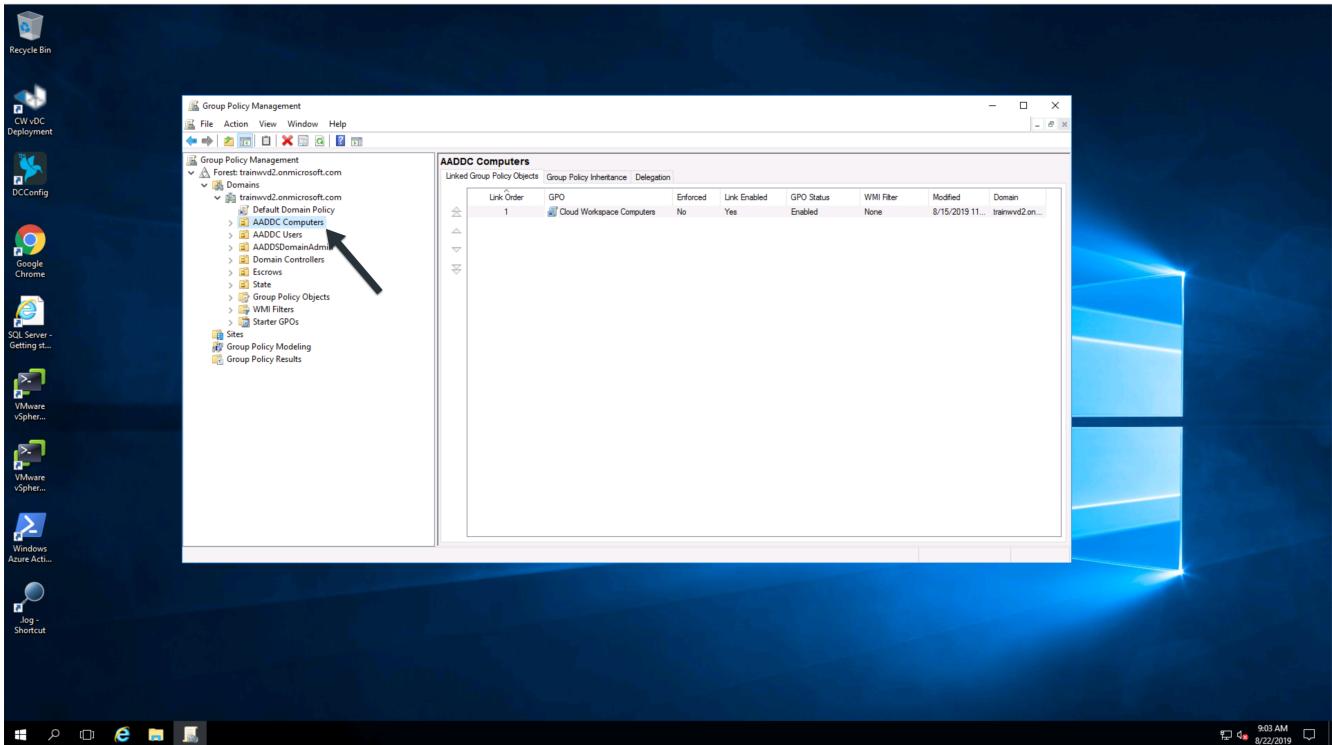
7. Click the Start (Windows) menu, choose Windows Administrative Tools.



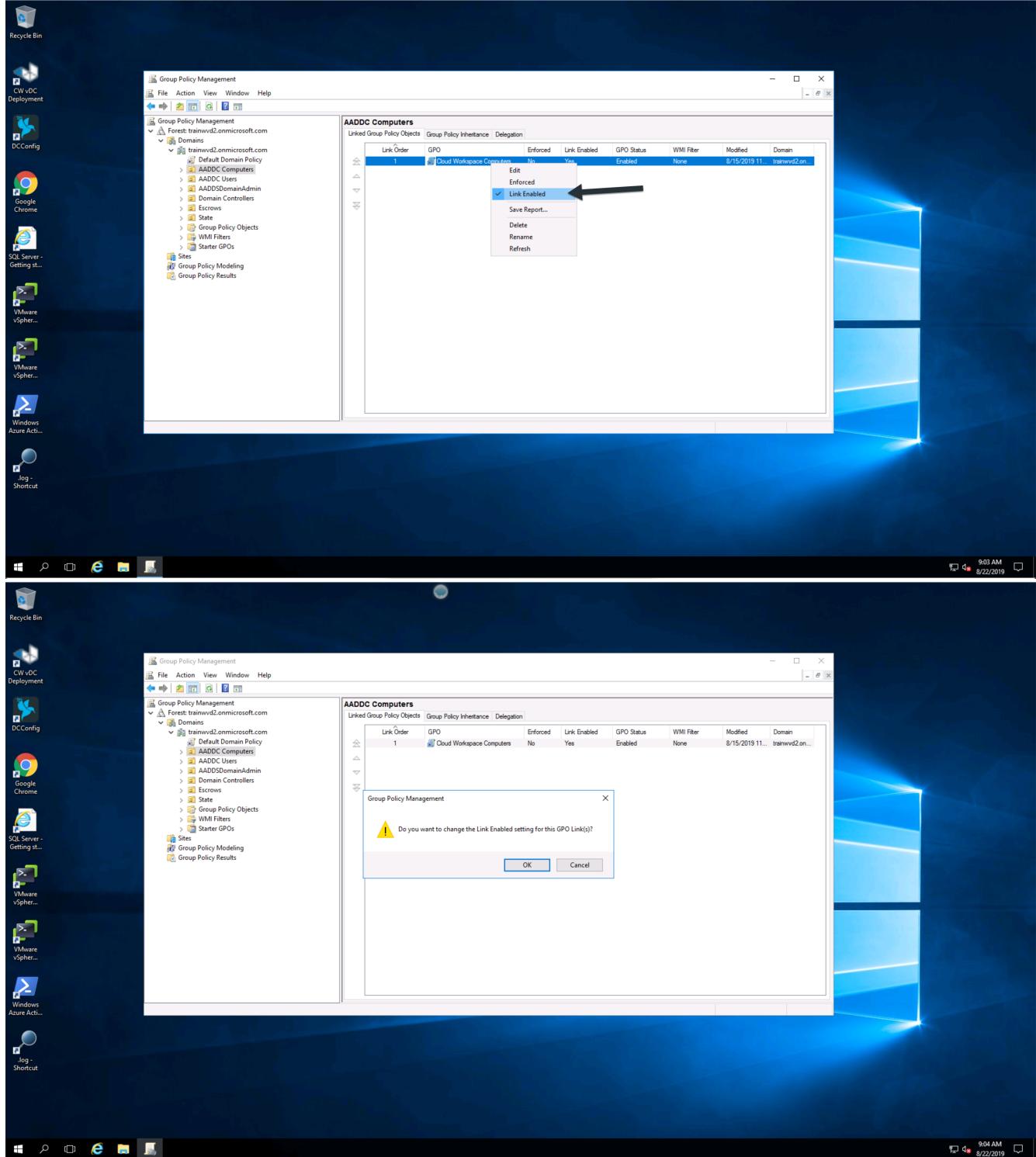
8. Click the Group Policy Management icon.



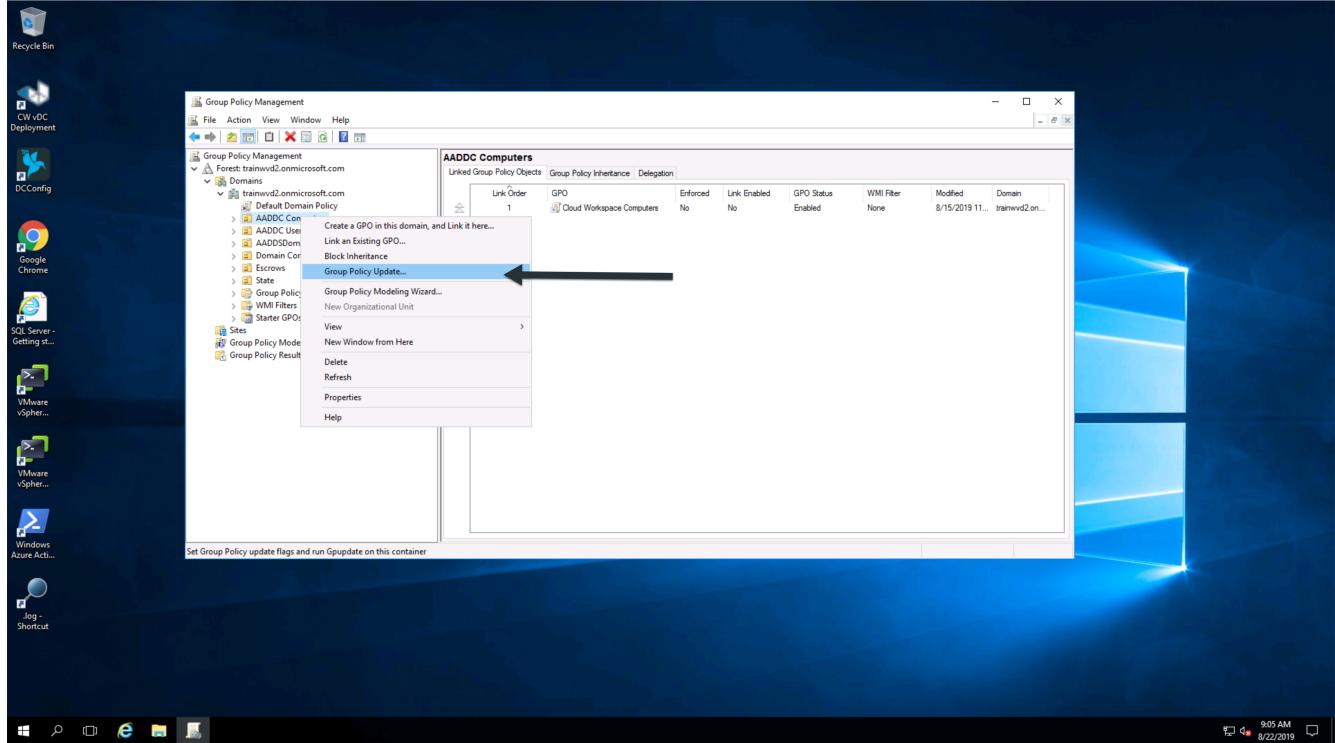
9. Click on the AADDC Users item in the list in the left pane.



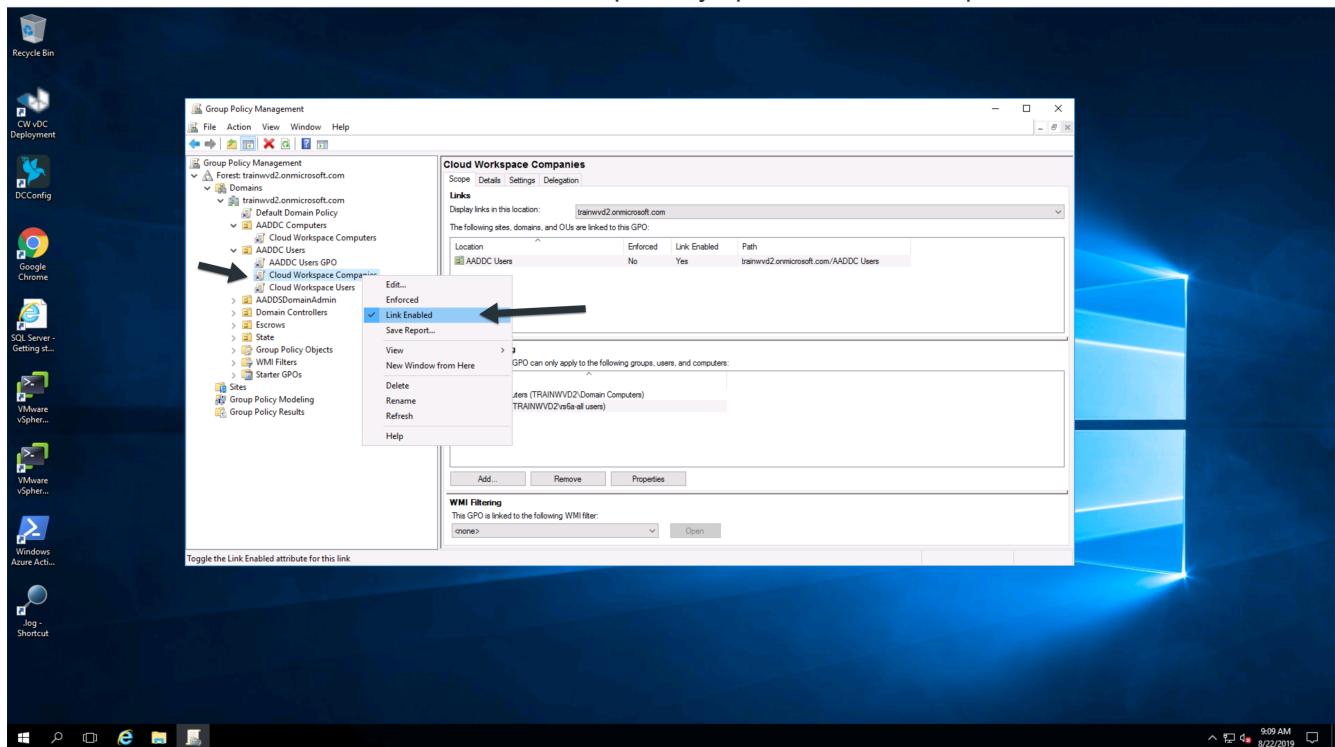
10. Right click on the "Cloud Workspace Users" policy in the list on the right pane, then deselect the "Link Enabled" option. Click OK to confirm this action.

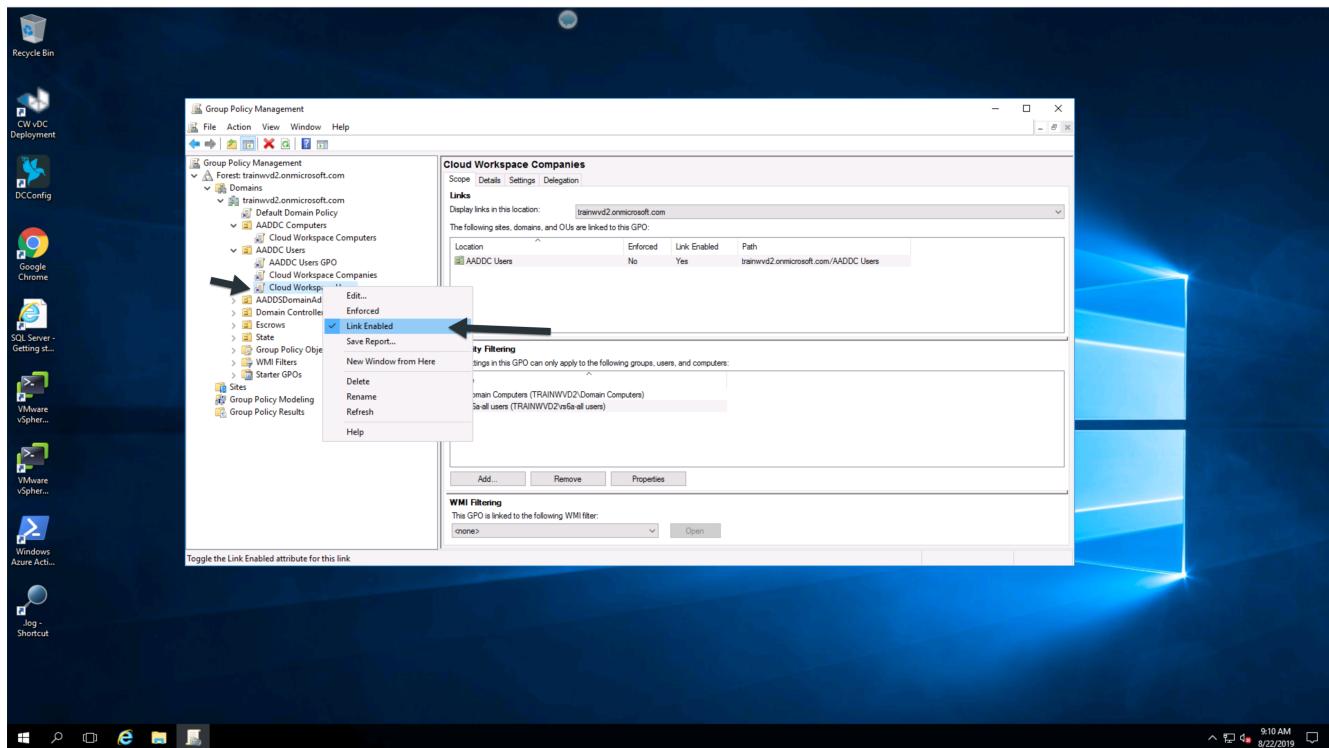


11. Select Action, Group Policy Update from the menu, then confirm that you want to force a policy update on those computers.

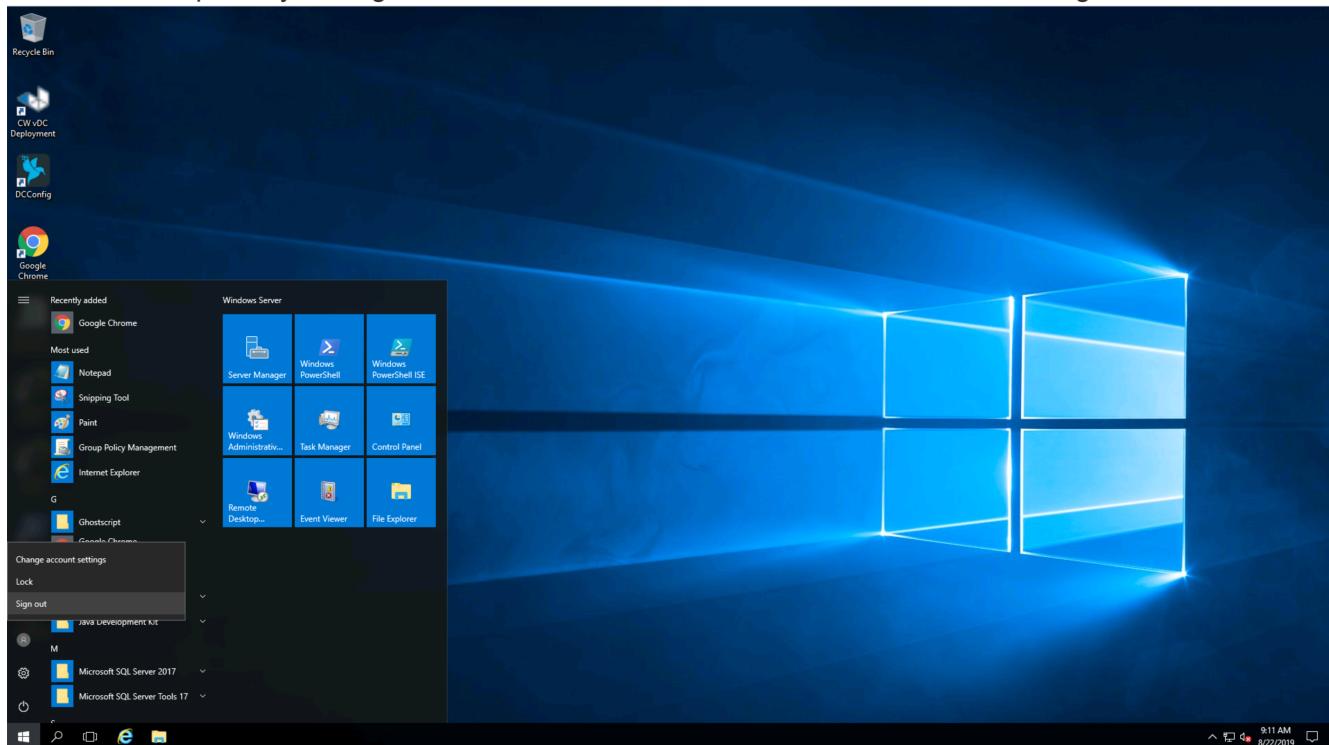


12. Repeat steps 9 and 10 but select “AADDC Users” and “Cloud Workspace Companies” as the policy to disable the Link. You do not need to force a Group Policy update after this step.





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.

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.