Deploying with VDS

Virtual Desktop Service

NetApp
December 18, 2020

Table of Contents

Deploying with VDS

Azure

Windows Virtual Desktop

WVD Deployment Guide

Overview

This guide will provide the step by step instructions to create a Windows Virtual Desktop (WVD) 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 WVD 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 WVD 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 WVD 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.

WVD basics

Windows 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 WVD 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.
- WVD 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.

- WVD 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 WVD 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 WVD 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 WVD 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 & WVD 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 WVD 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

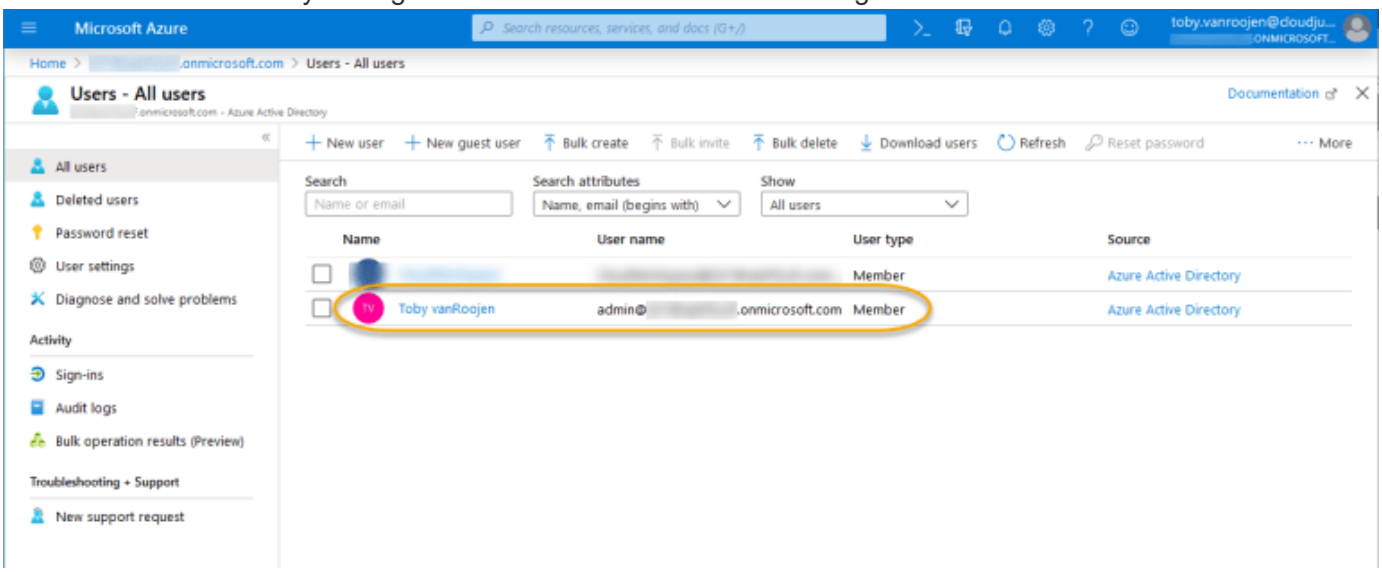
☑ Azure Admin Account with Global Admin and Subscription Ownership Roles

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.

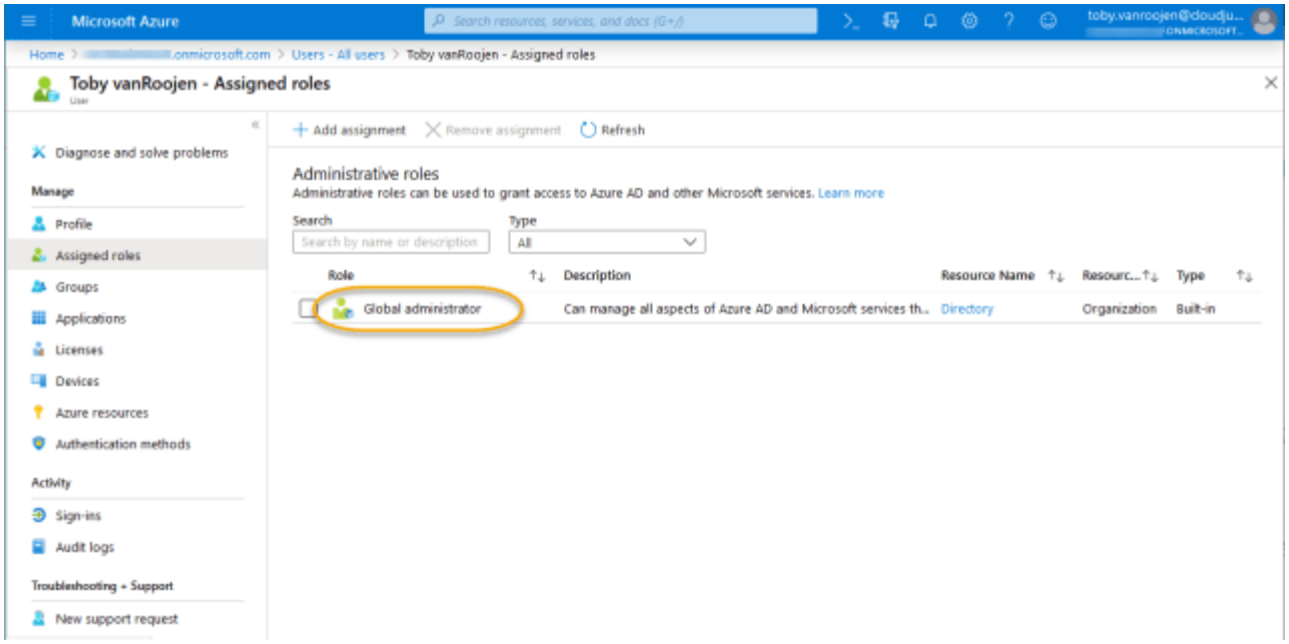


Global administrator role

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

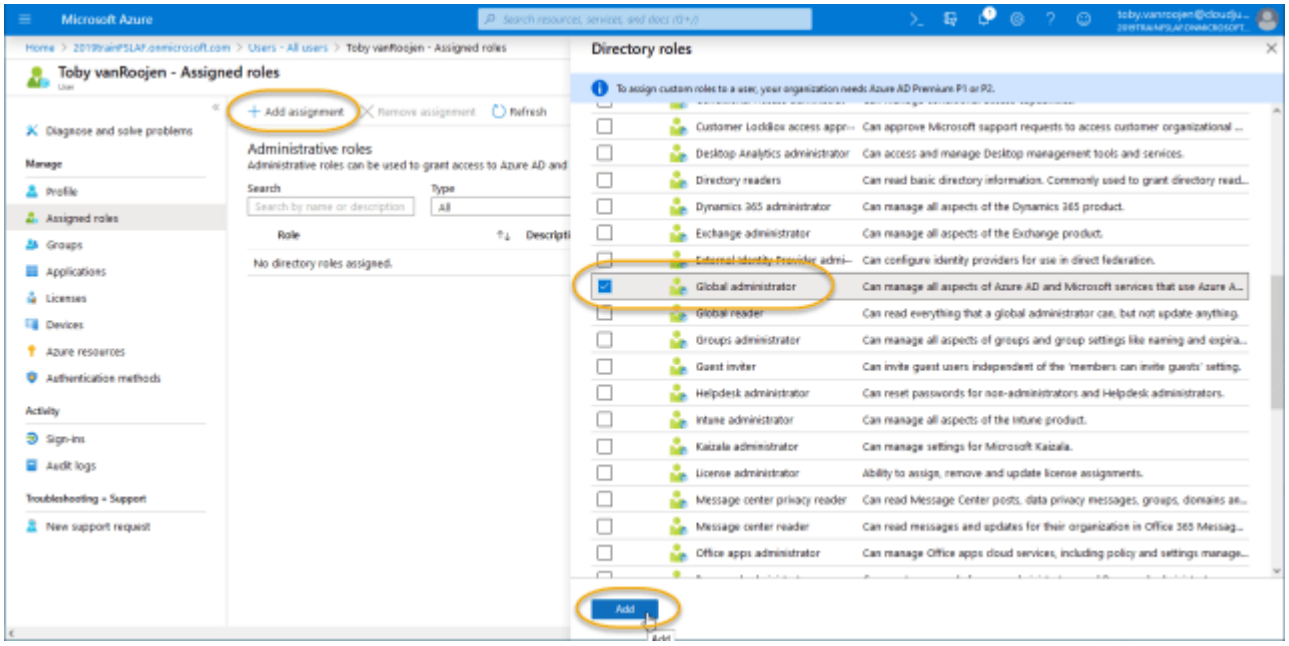
To check your role in Azure AD, follow these steps:

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



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.



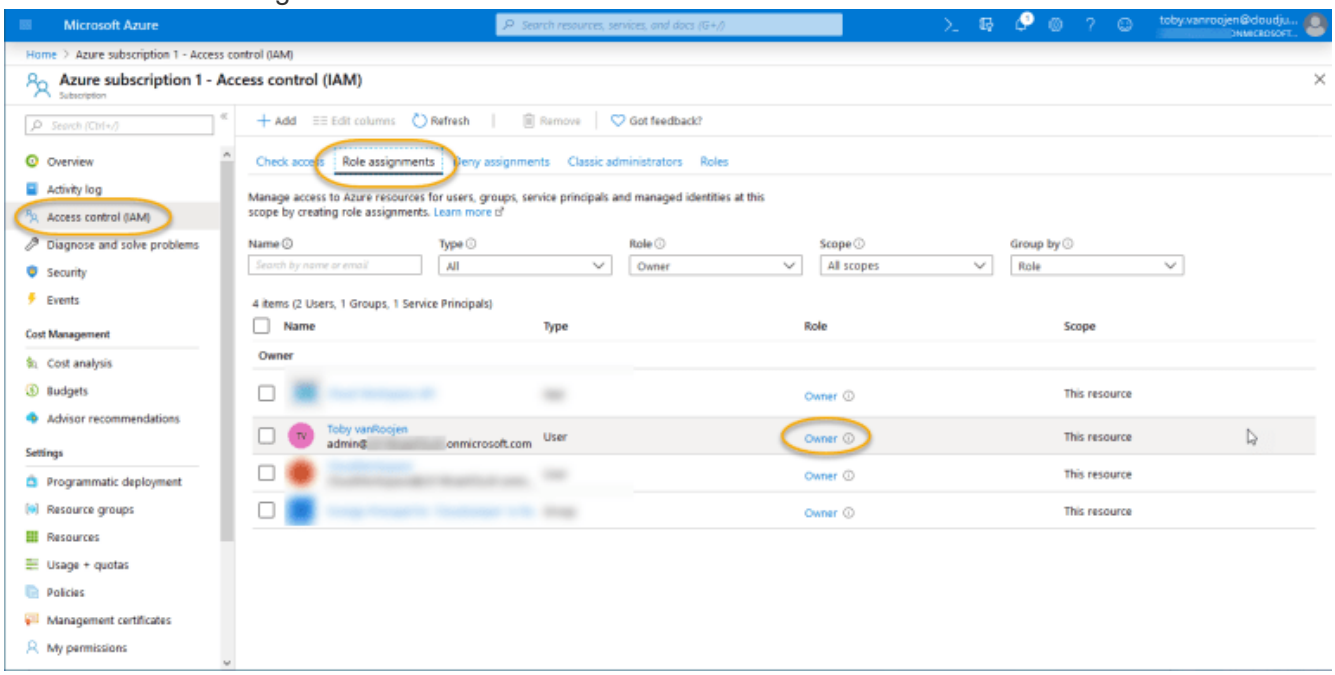
Azure subscription ownership

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:

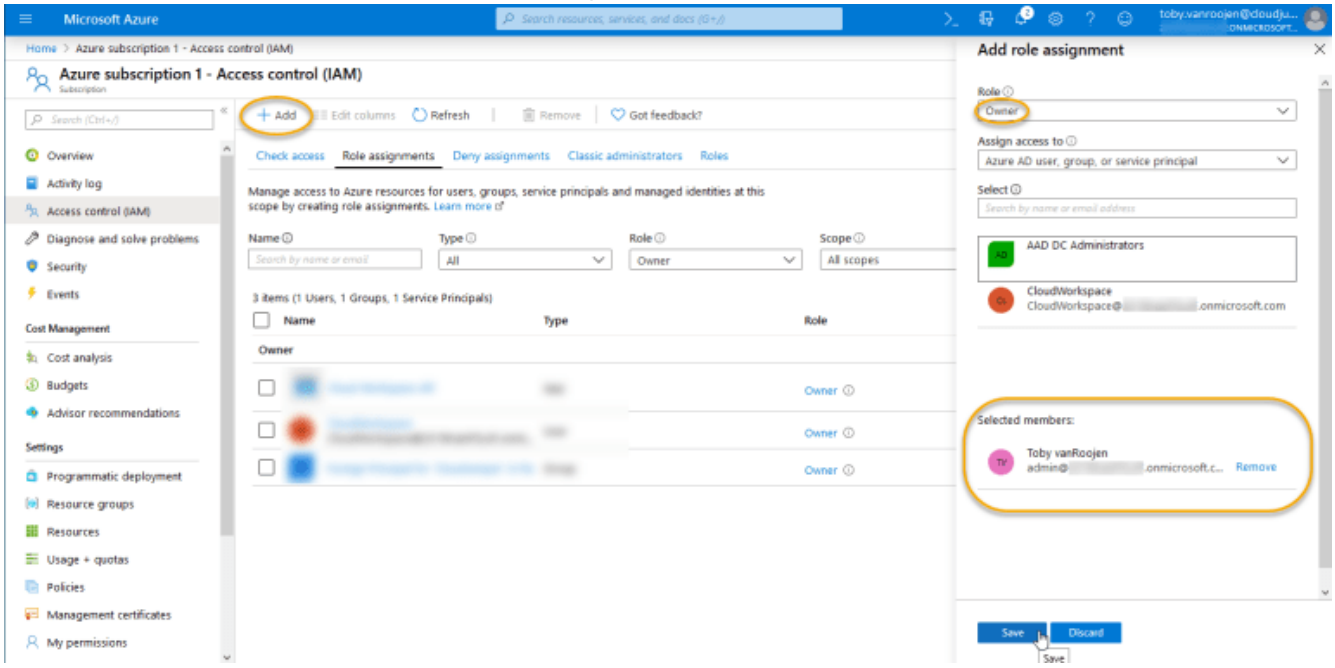
1. Log in to the Azure Portal at https://portal.azure.com/
2. Search for, and select Subscriptions

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.



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

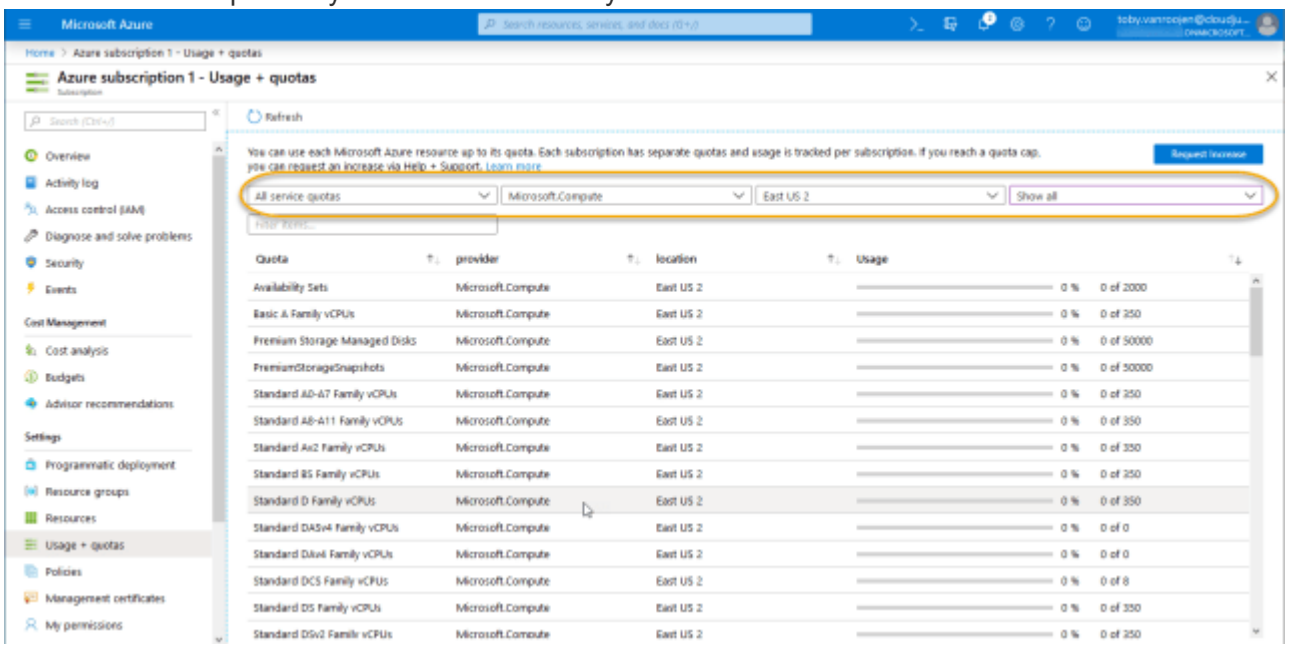


Azure compute core quota

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

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



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:

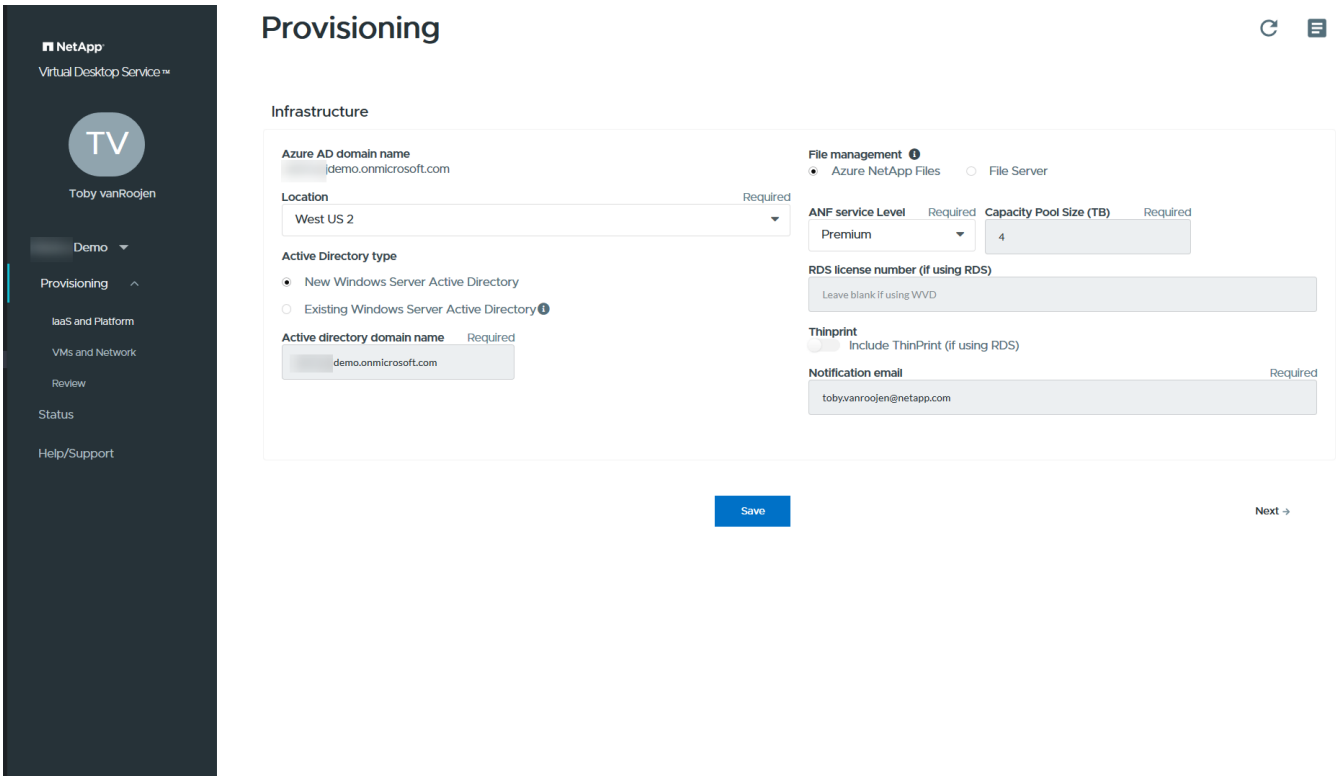
Item	Description
VDS admin credentials	Collect the existing VDS admin credentials if you already have them. Otherwise a new admin account will be created during deployment.
Azure Region	Determine the target Azure Region based on performance and availability of services. This Microsoft Tool can estimate 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 WVD 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 link: https://aka.ms/azurenetappfiles

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 WVD environments. When deploying WVD, this field can **remain empty**.

Thinprint

NetApp VDS can be used to deploy RDS and/or WVD environments. When deploying WVD, 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

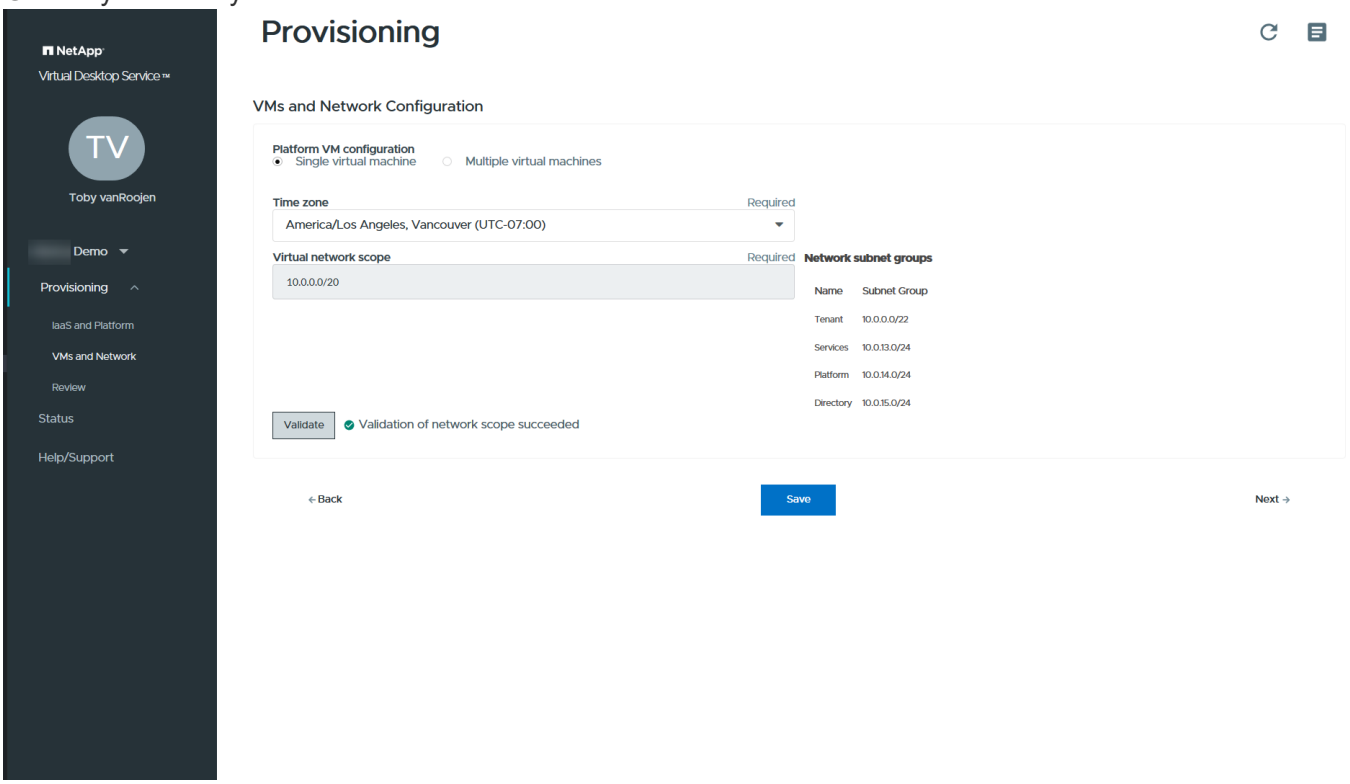
changed later.

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 WVD deployments leverage the Single virtual machine option, as Microsoft manages the WVD 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 WVD environments. When deploying WVD 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 WVD, 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 WVD (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 WVD 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 WVD 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 HTML 5 Gateways. These gateways serve up an HTML 5 VDS access client (e.g. https://login.cloudworkspace.com) based on the RemoteSpark technology. Licensing for this component is typically included in the cost of VDS licensing. When two HTM5 CW Portals are selected, VDS Setup deploys 2 VMs and configures them to load balance incoming HTML5 user sessions.
  Note that when using Multiple virtual machine option - even if you are only intend to support RDP connections for your RDS workloads - at least 1 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 WVD implementation. This includes a single virtual machine that can act as both a Remote Desktop session host and a file server. In a WVD 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 WVD services

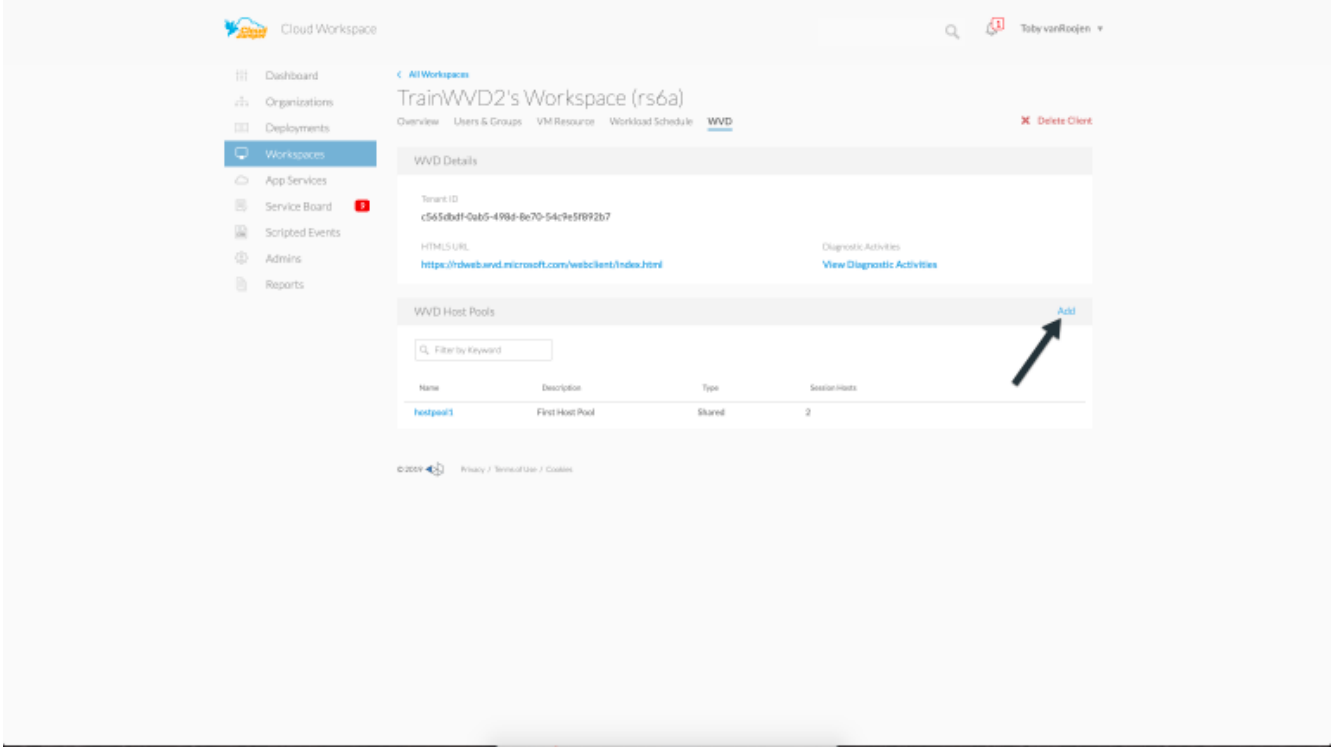
Once the deployment is complete, the next step is to enable the WVD functionality. The WVD enablement process requires the Azure Administrator to perform several steps to register their Azure AD domain and subscription for access using the Azure WVD services. Similarly, Microsoft requires VDS to request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

Create WVD host pool

End User access to WVD 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

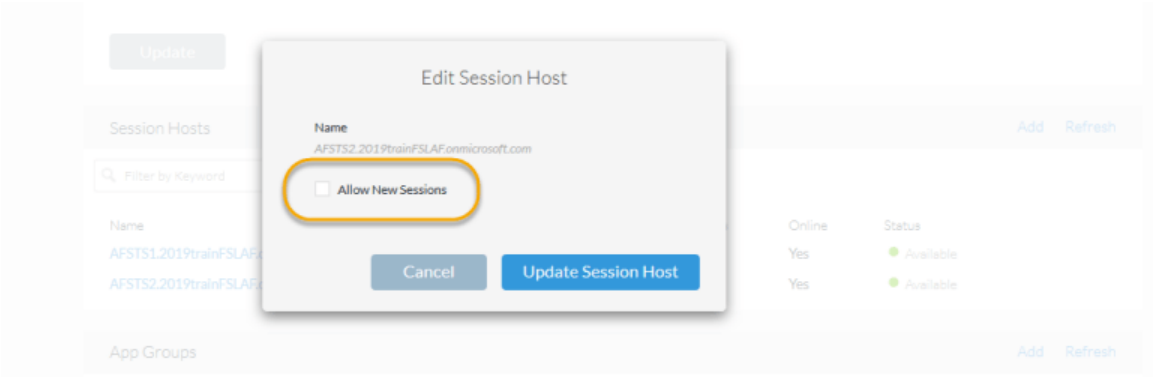
1. Click the Add button in the right hand side of the WVD host pools section header.



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 WVD 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 WVD 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

WVD 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.

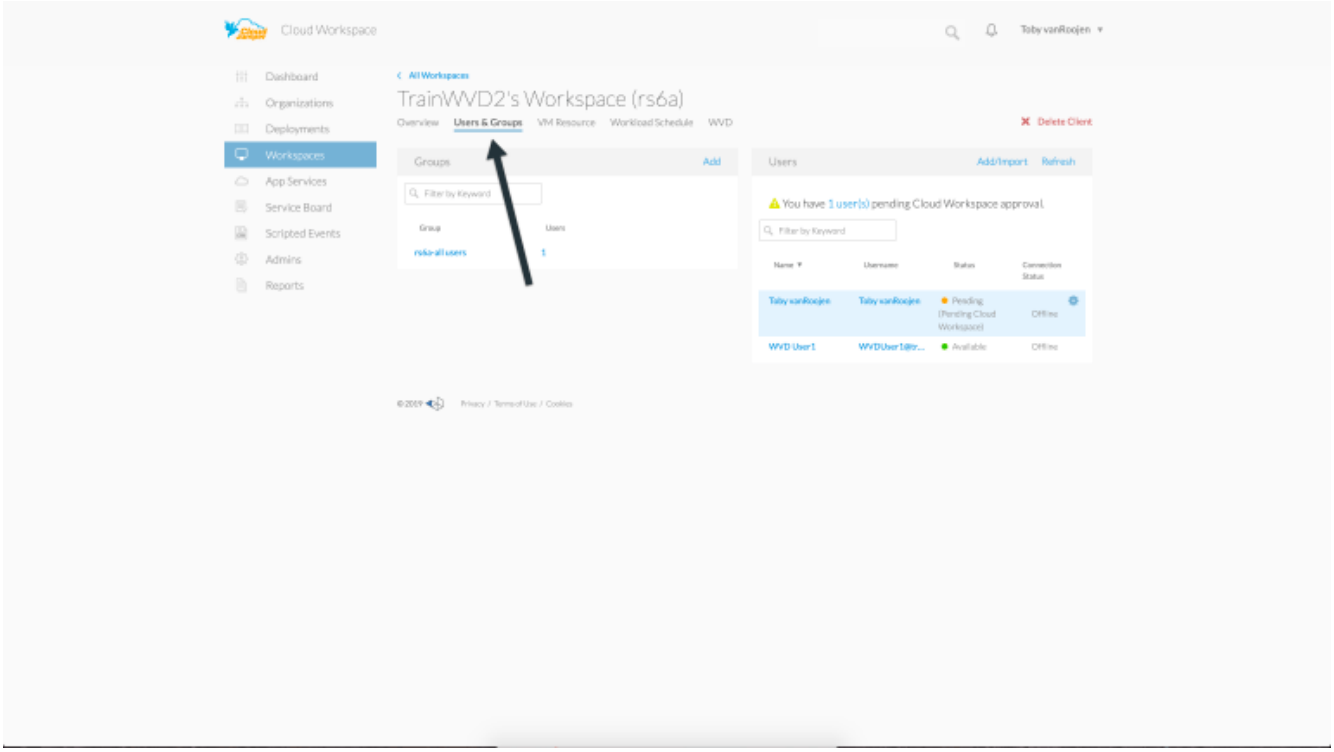


Enable VDS desktops for users

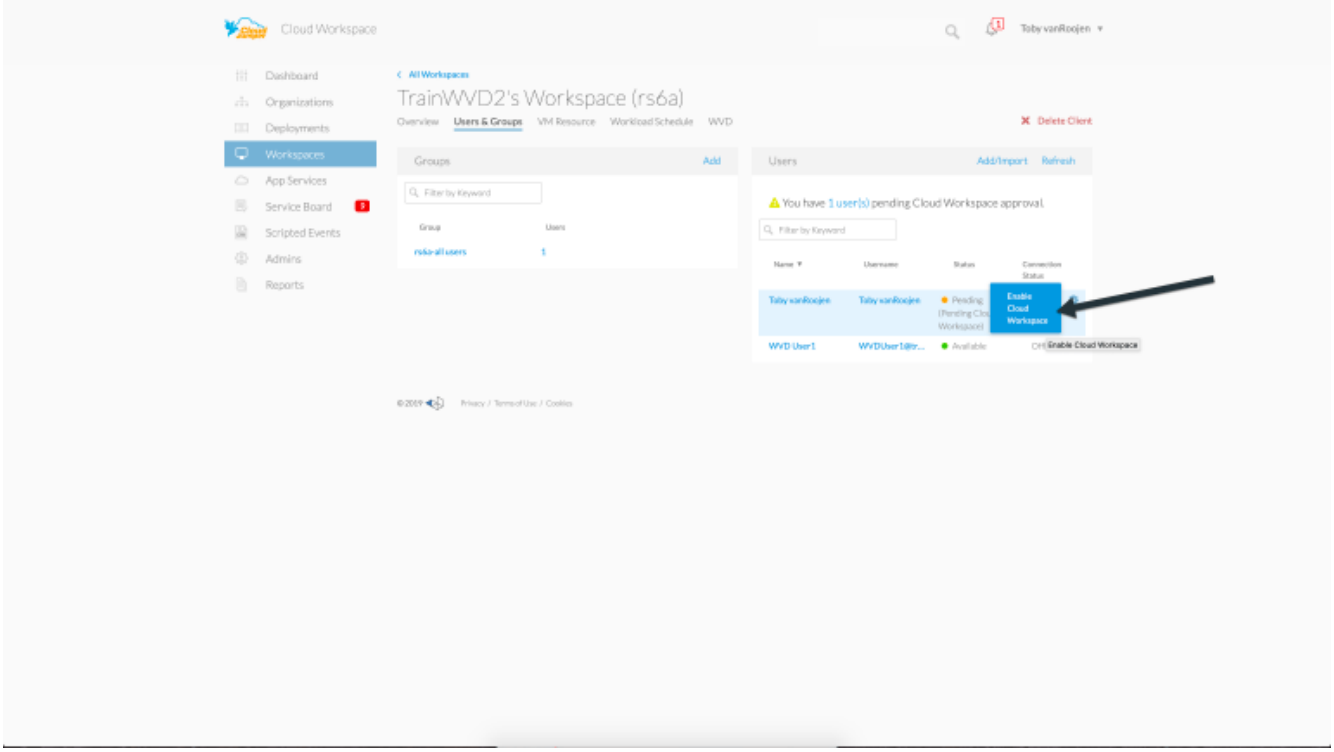
As noted above, VDS creates all the elements required to support end user workspaces during deployment. Once the deployment has completed, the next step is to enable workspace access for each user you want introduced to the WVD environment. This step creates the profile configuration and end user data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



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



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 WVD 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.

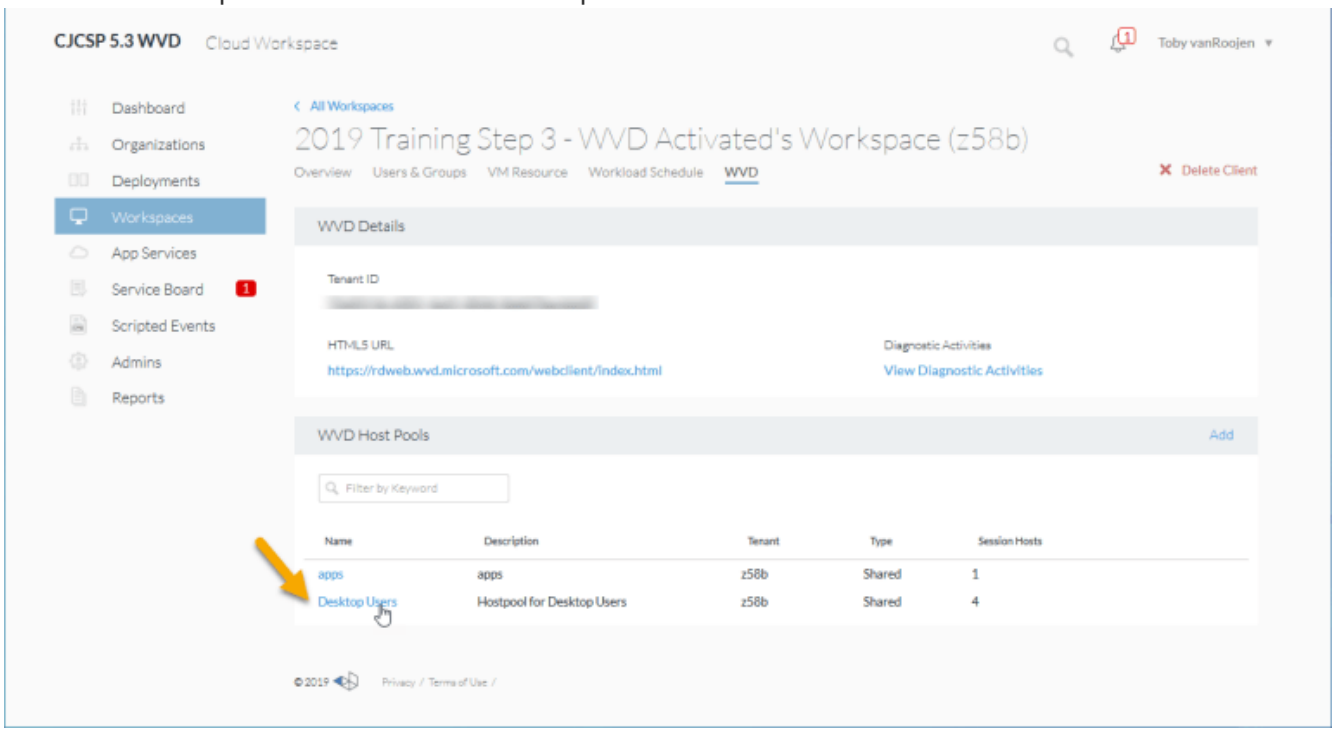
Enable user sessions

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.”

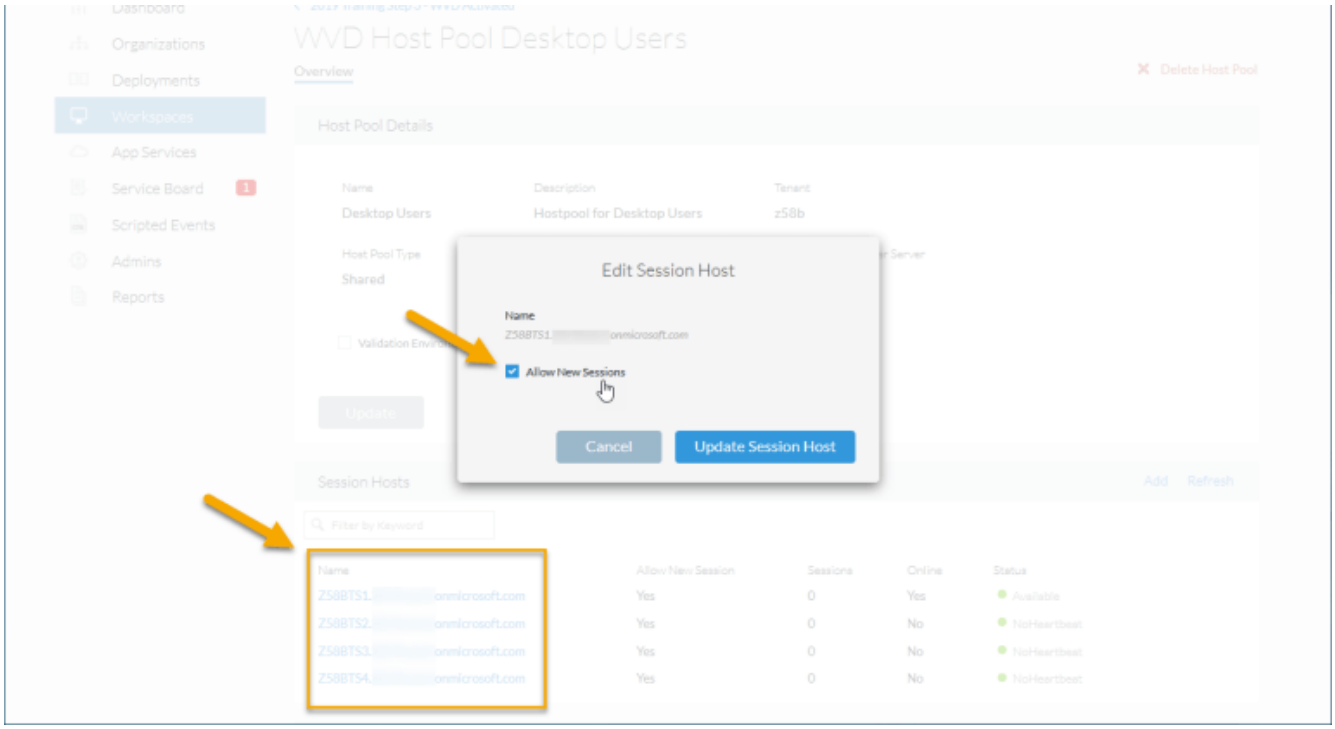
In production it makes sense to start new hosts in drain mode because there are typically configuration tasks that need to be completed before the host is ready for production workloads.

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 WVD Section of the workspace page.
2. Click on the host pool name under “WVD host pools”.



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.

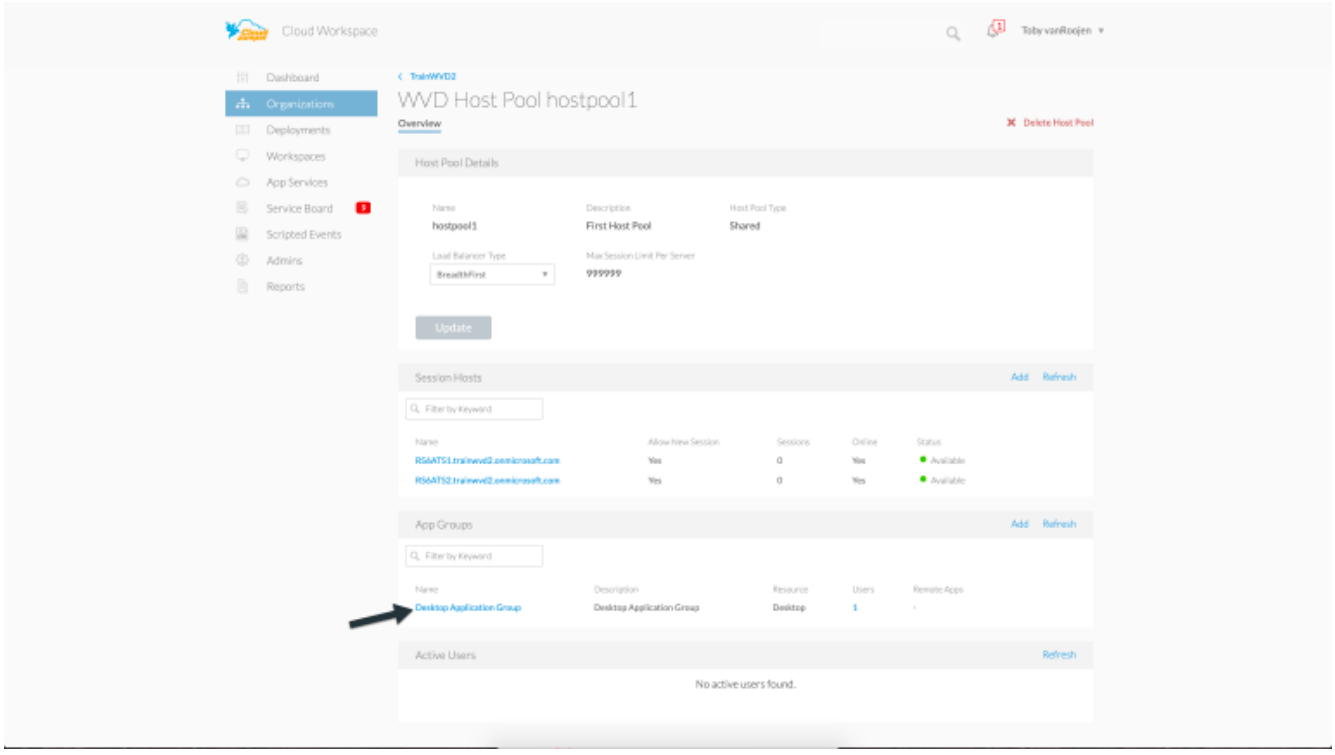


4. The current stats of “Allow New Session” is also displayed on the main WVD page for each host line item.

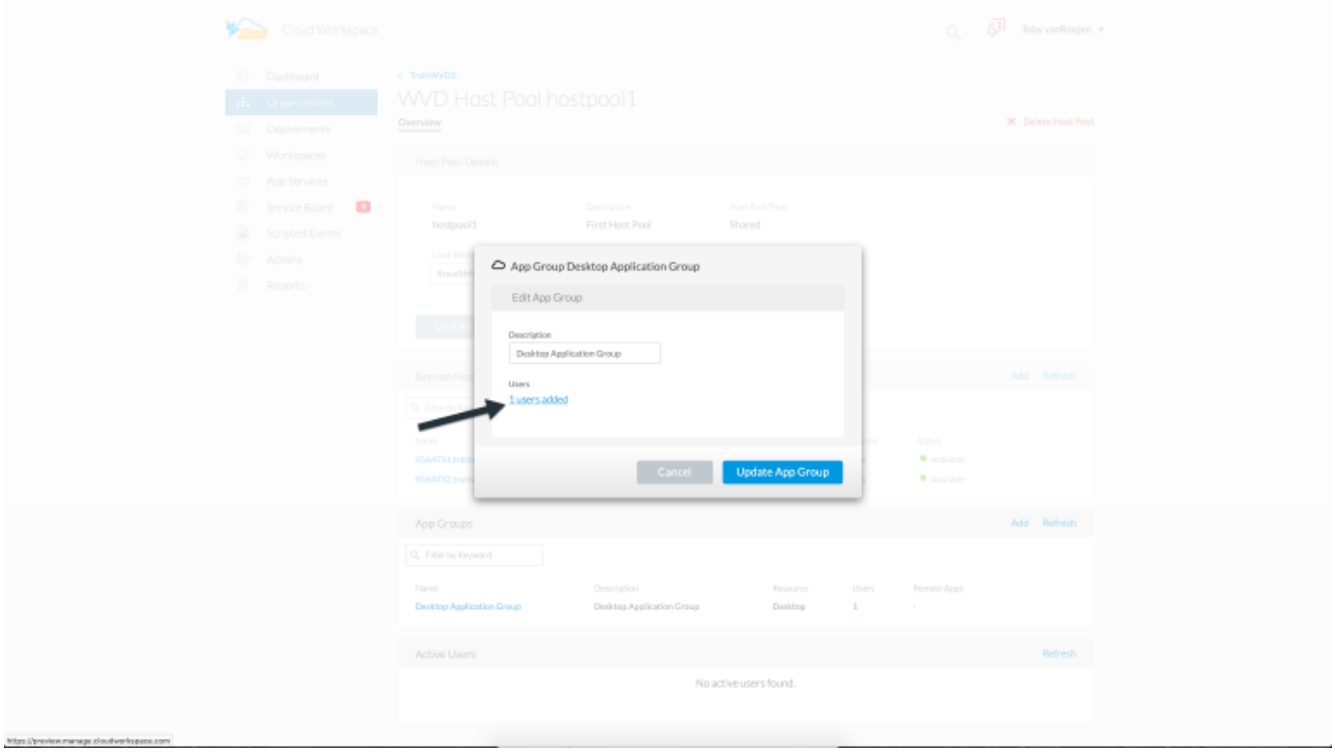
Default app group

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



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

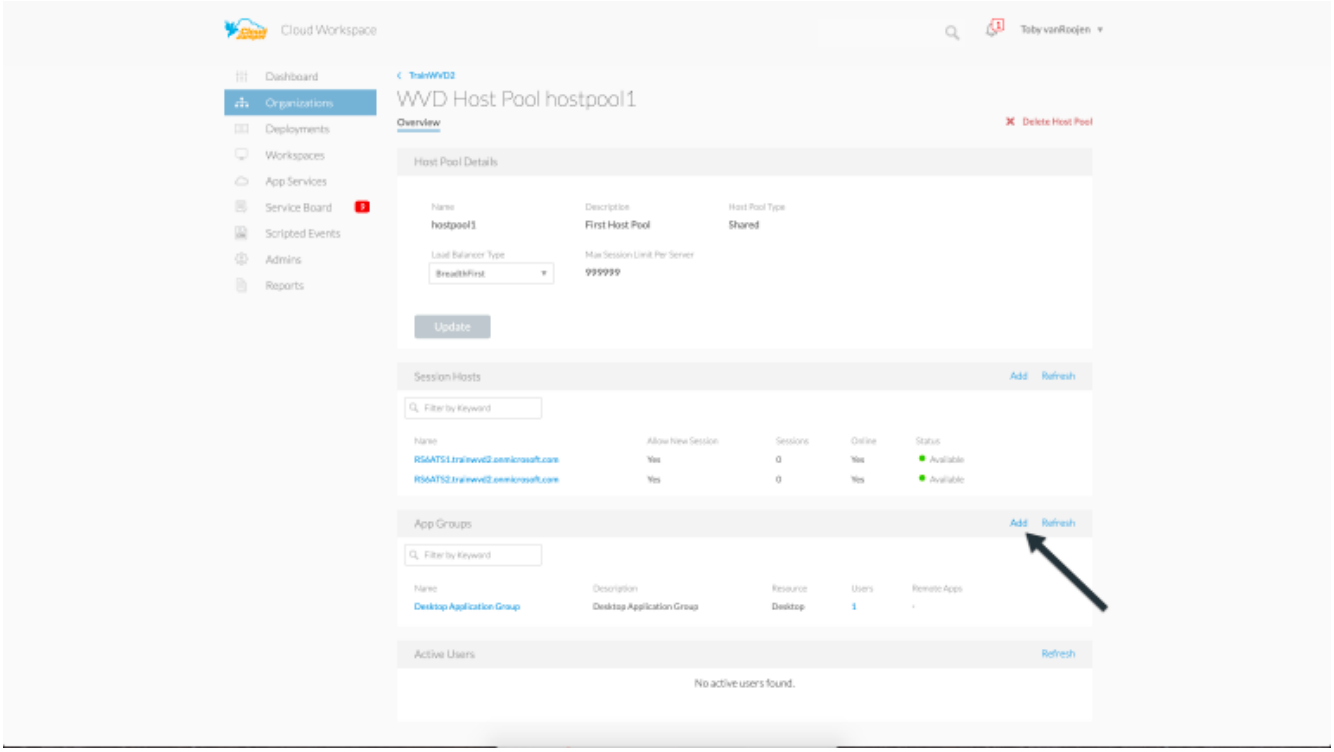
Create additional WVD app group(s)

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.

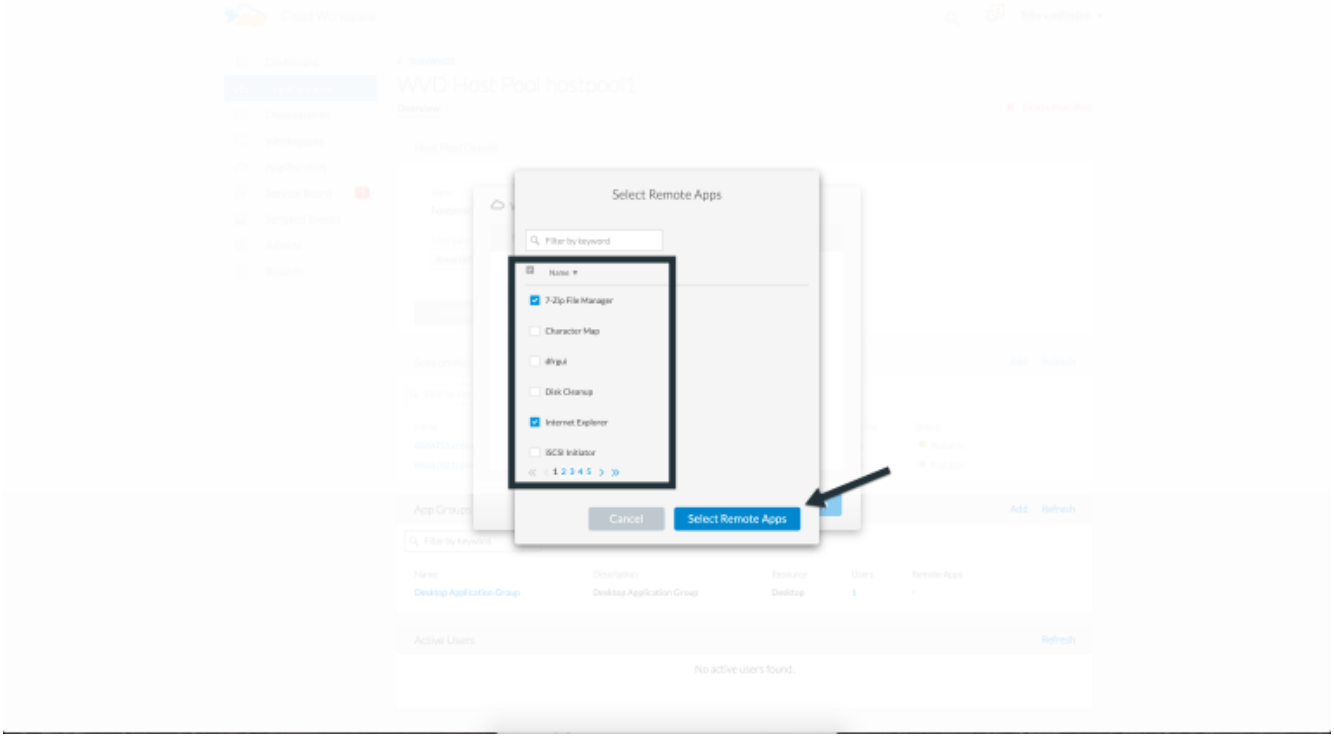
WVD only allows end users to be assigned to the Desktop App Group type or RemoteApp App Group type but not both in the same host pool, so make sure you segregate your users accordingly. If users need access to a desktop and streaming apps, a 2nd host pool is required to host the app(s).

To create a new App Group:

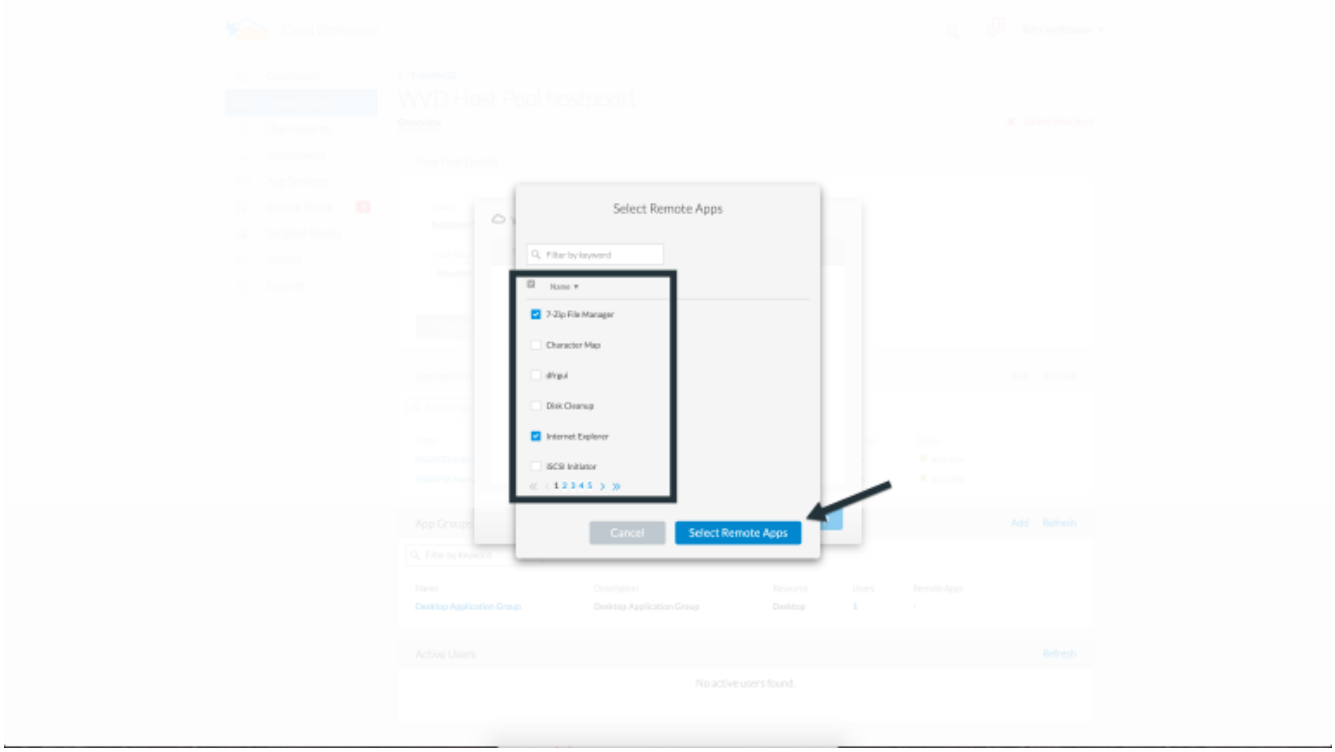
1. Click the Add button in the app groups section header



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



4. Click the Add RemoteApps link to add applications to this App Group. WVD 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 WVD access

End users can access WVD 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/wvdweb
- 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 WVD instances.

Monitor user logins

The host pool detail page will also display a list of active users when they log in to a WVD 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: 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

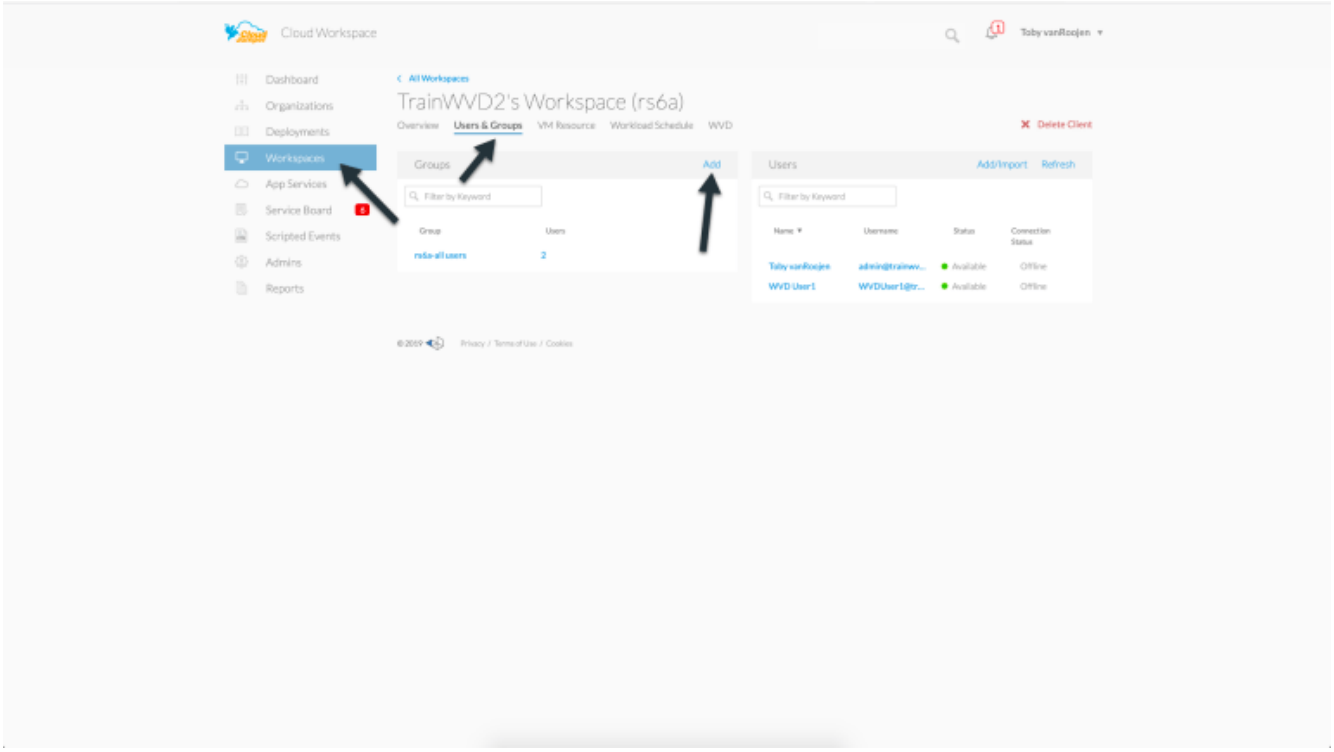
Permissions to view and edit folders in the company share can be assigned to users or groups.

Management.User_Administration.manage_folders_and_permissions.html

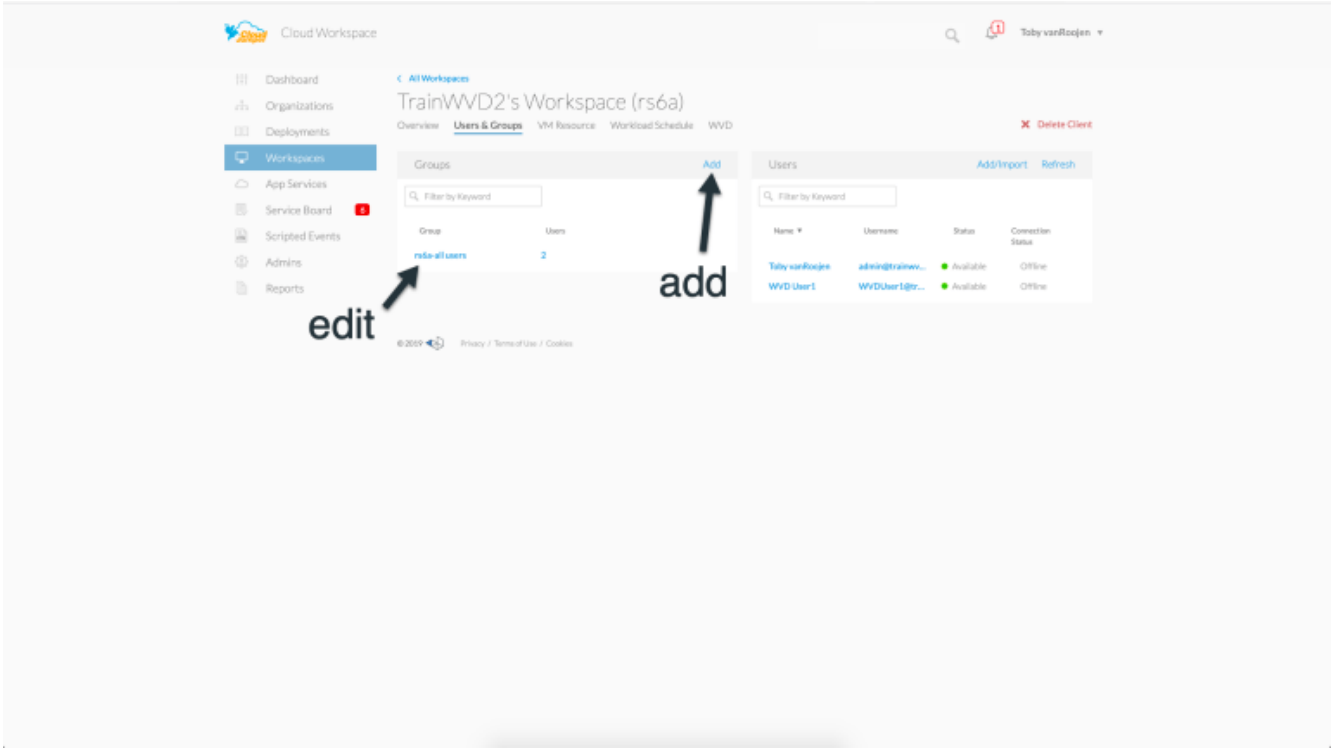
Assign applications by group

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

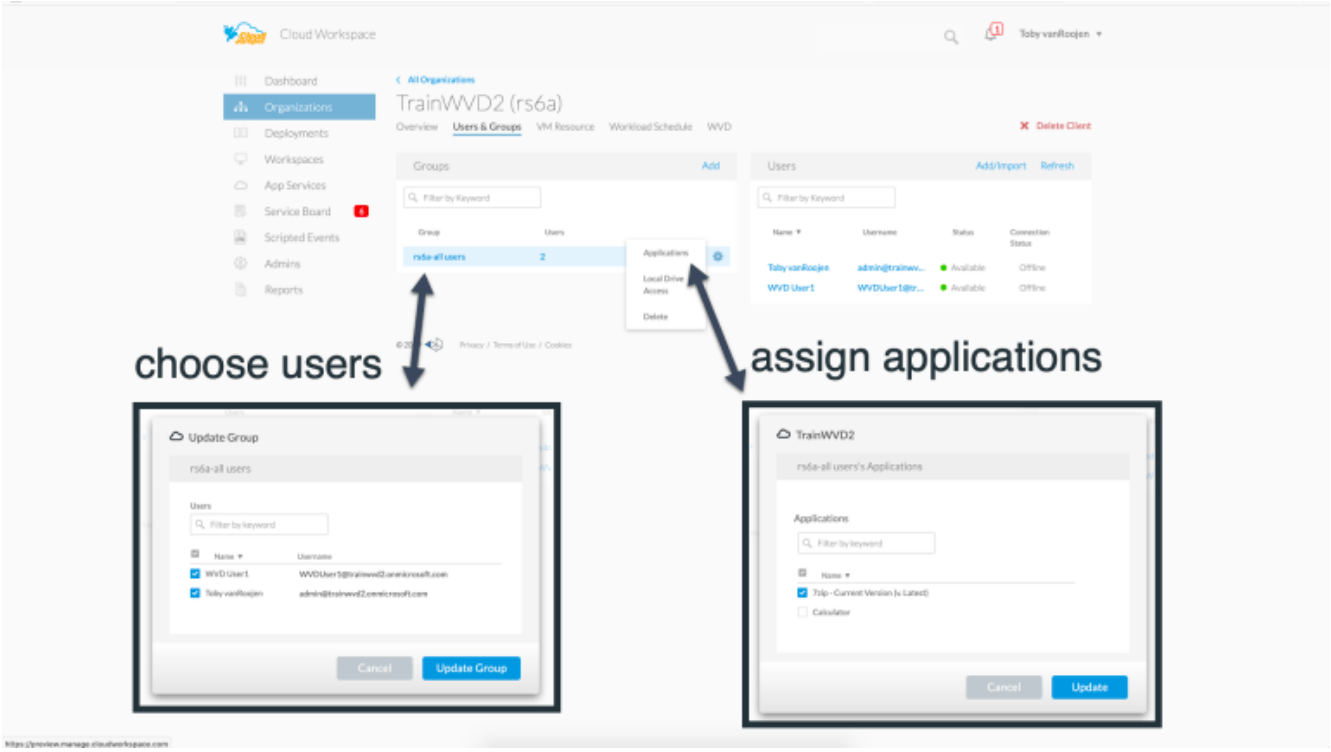
1. Navigate to the Users and Groups Detail.



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



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



Configure cost optimization options

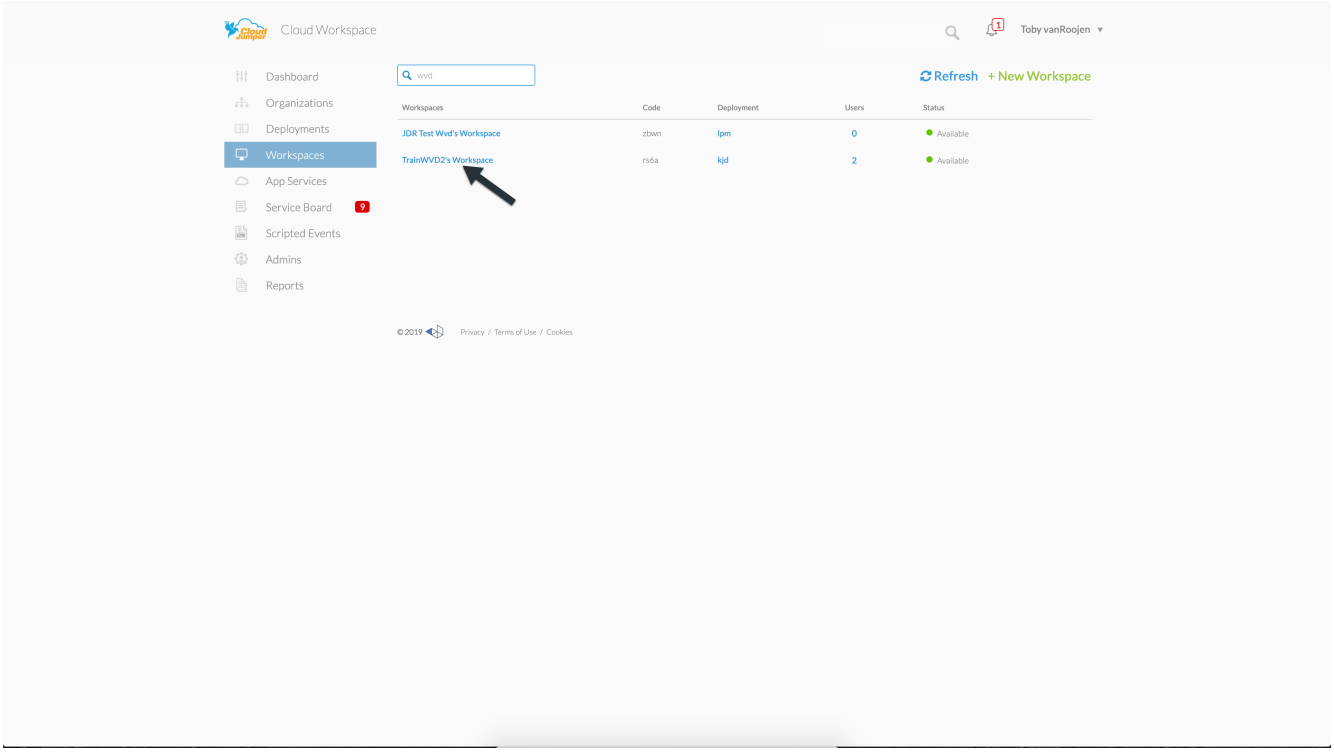
Workspace management also extends to managing the Azure resources that support the WVD implementation. VDS allows you to configure both Workload Schedules and Live Scaling to turn Azure virtual machines on and off based on end user activities. These features result in matching Azure resource utilization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

Workload scheduling

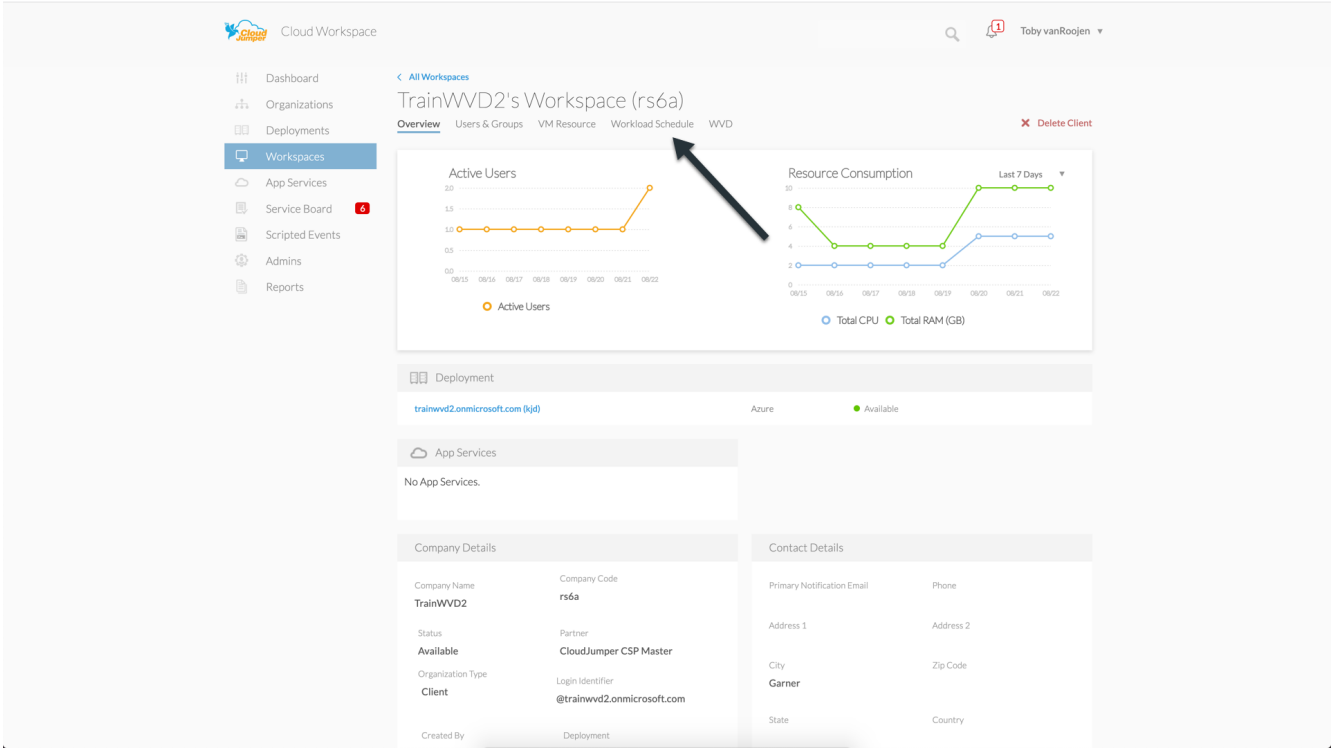
Workload Scheduling is a feature that allows the Administrator to create a set schedule for the Workspace virtual machines to be on to support end user sessions. When the end of the scheduled time period is reached for a specific day of the week, VDS Stops/Deallocates the virtual machines in Azure so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

To enable Workload Scheduling:

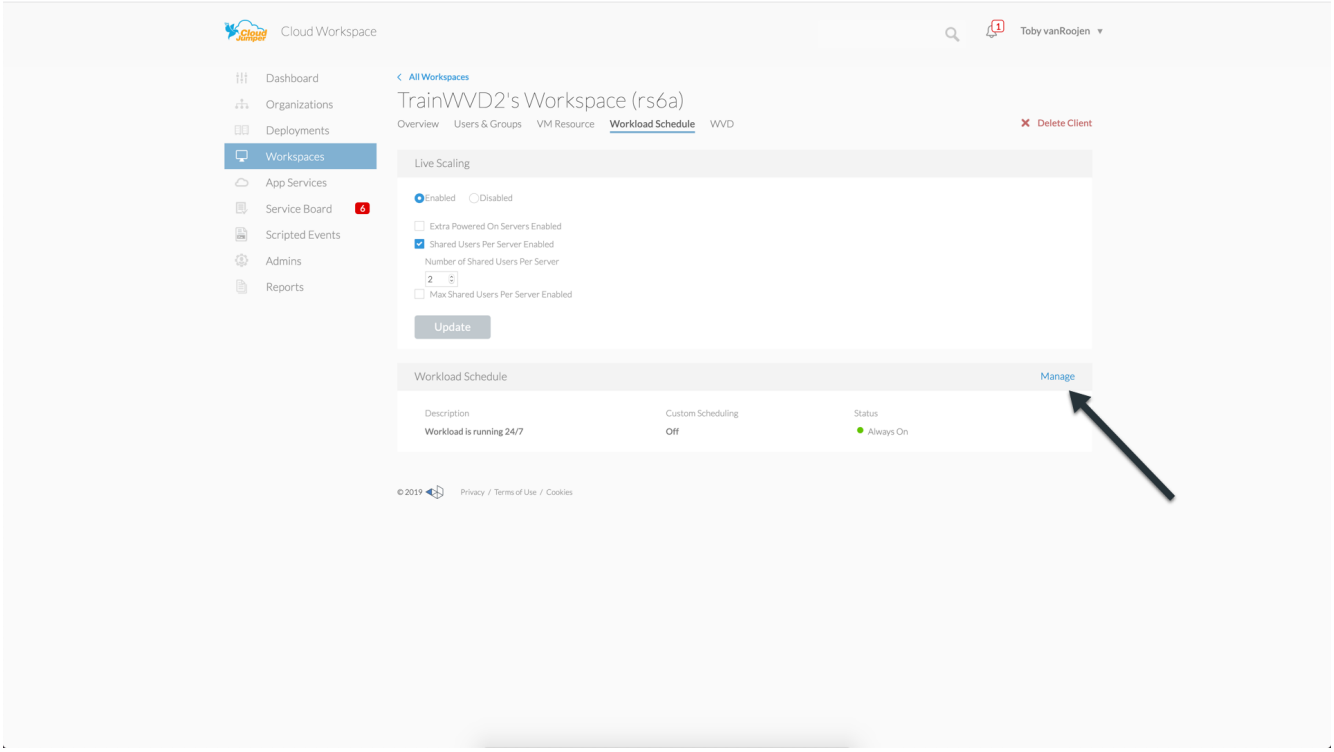
1. Log in to VDS at https://manage.cloudworkspace.com using your VDS credentials.
2. Click on the Workspace menu item and then click on the name of the Workspace in the list.



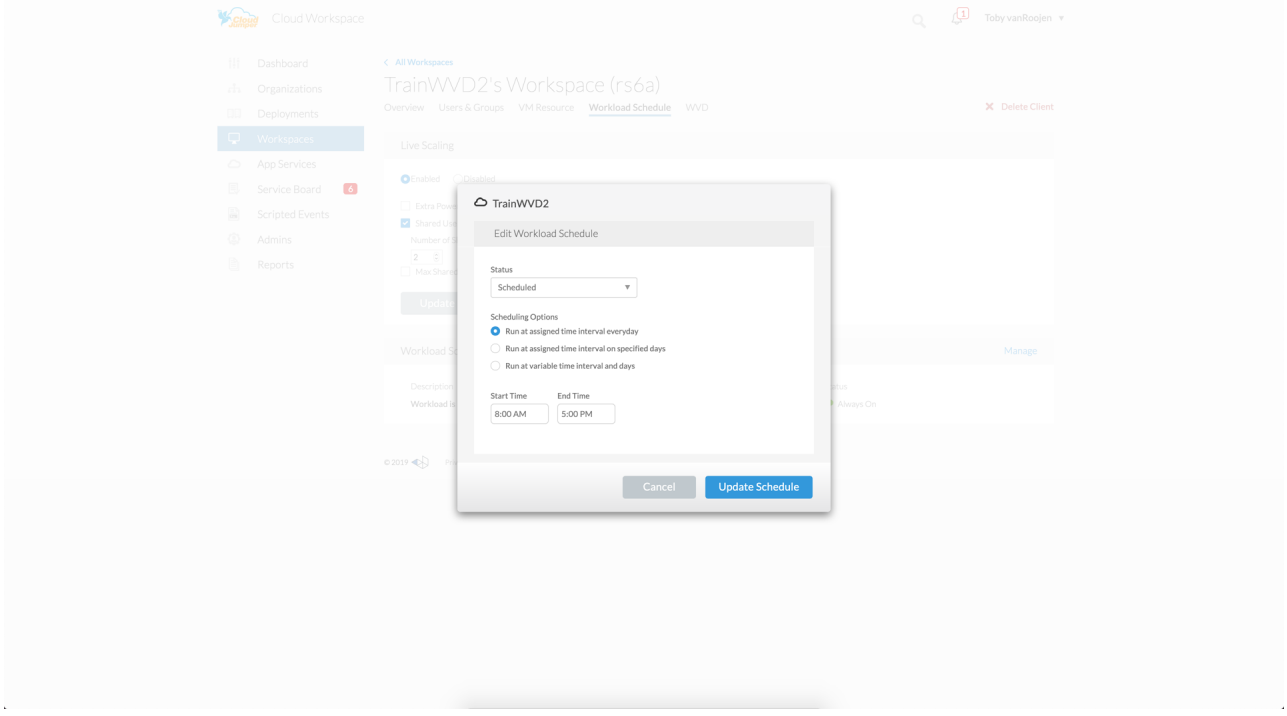
3. Click on the Workload Schedule tab.



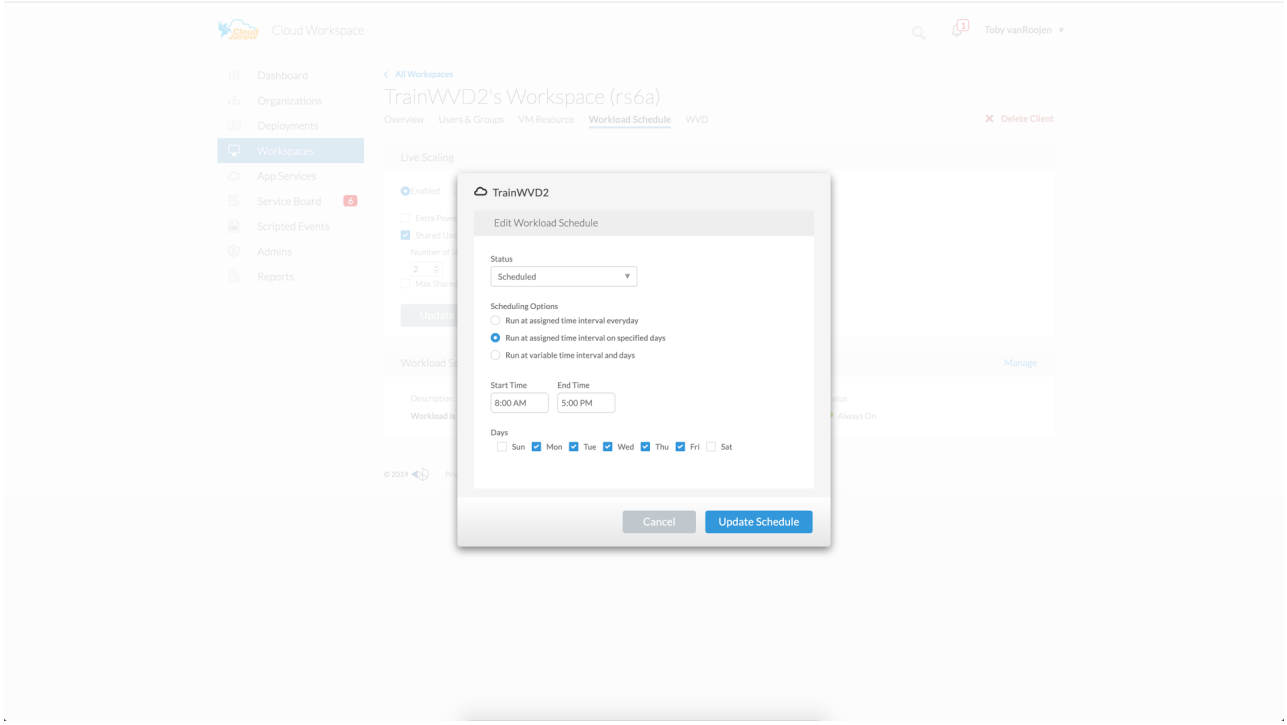
4. Click the Manage link in the Workload Schedule header.



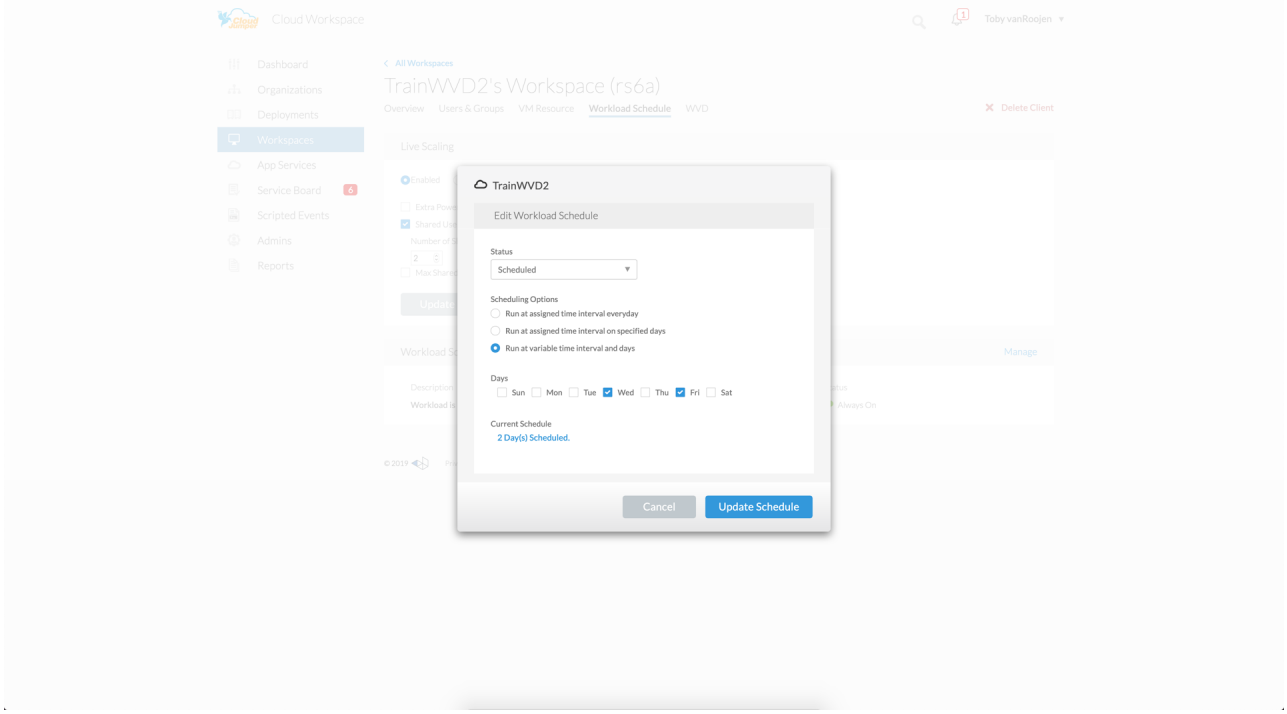
5. Choose a default state from the Status drop down: Always On (default), Always Off, or Scheduled.
6. If you choose Scheduled, the Scheduling options include:
   a. Run at Assigned Interval every day. This option sets the schedule to be the same Start Time and End Time for all seven days of the week.



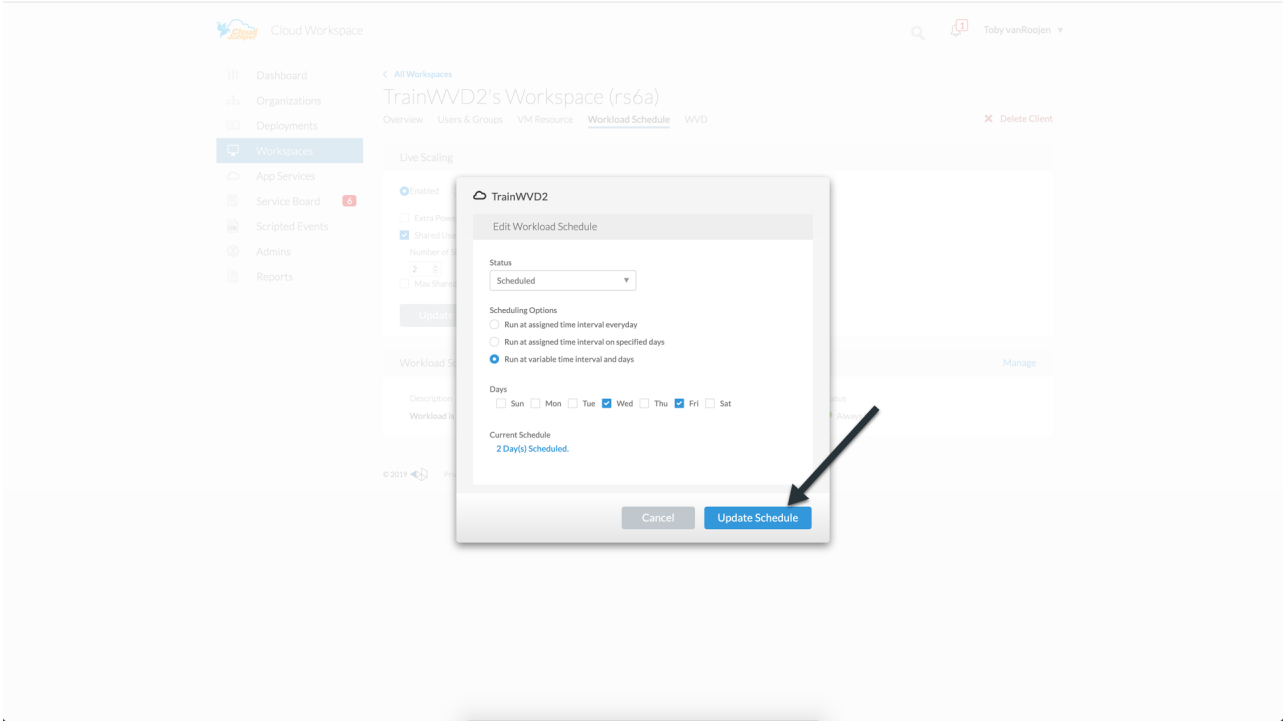
   b. Run at Assigned Interval for Specified Days. This option sets the schedule to the same Start Tie and End Time only for selected days of the week. Non-selected days of the week will cause VDS to not turn the virtual machines on for those days.



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.

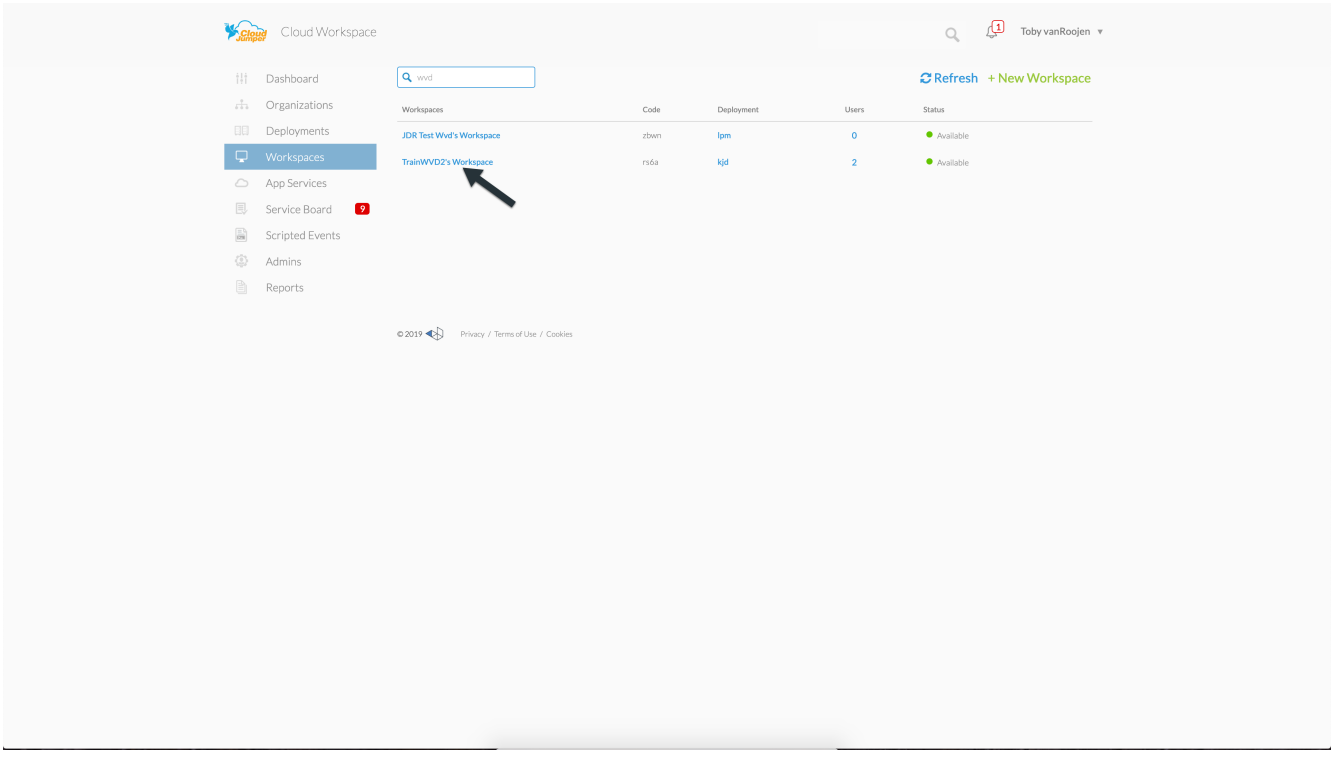


Live Scaling

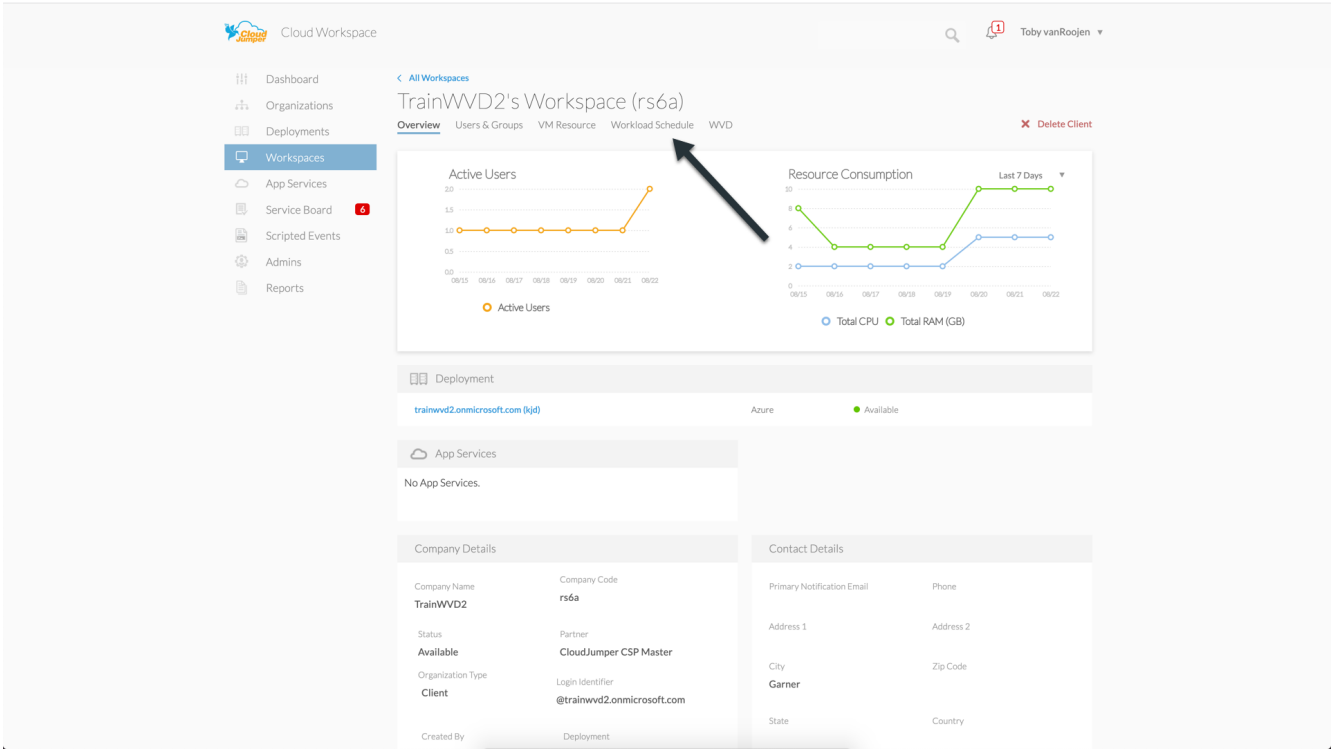
Live Scaling automatically turns virtual machines in a shared host pool on and off depending on concurrent user load. As each server fills up, an additional server is turned on so that its ready when the host pool load balancer sends user session requests. For effective use of Live Scaling, choose “Depth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

To enable Live Scaling:

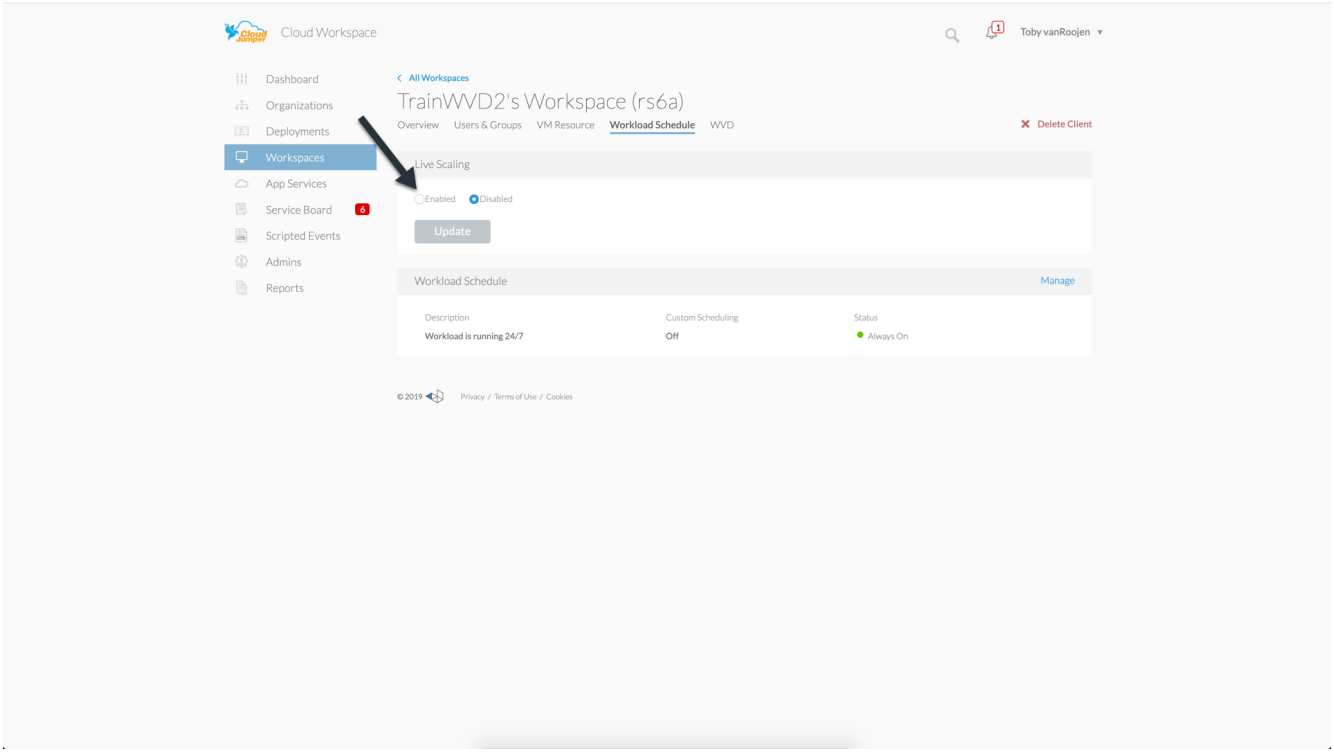
1. Log in to VDS at https://manage.cloudworkspace.com using your VDS credentials.
2. Click on the Workspace menu item and then click on the name of the Workspace in the list.



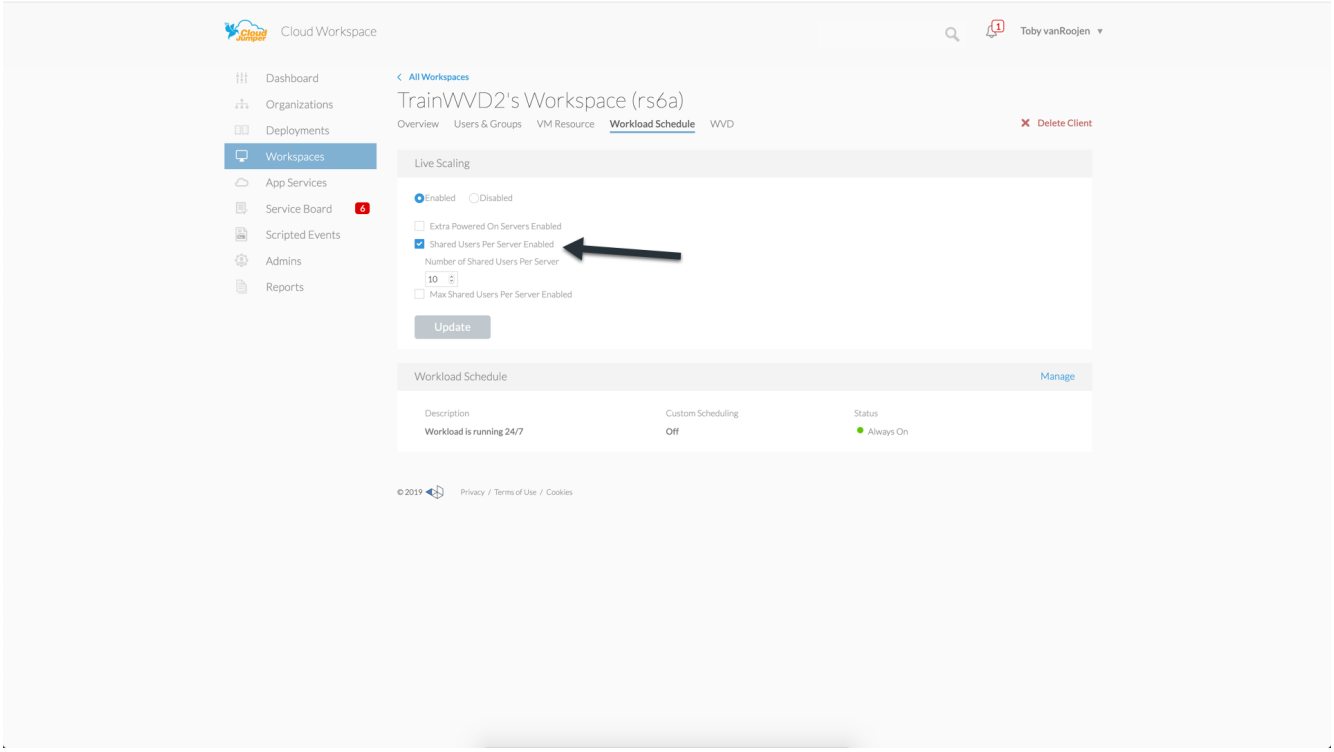
3. Click on the Workload Schedule tab.



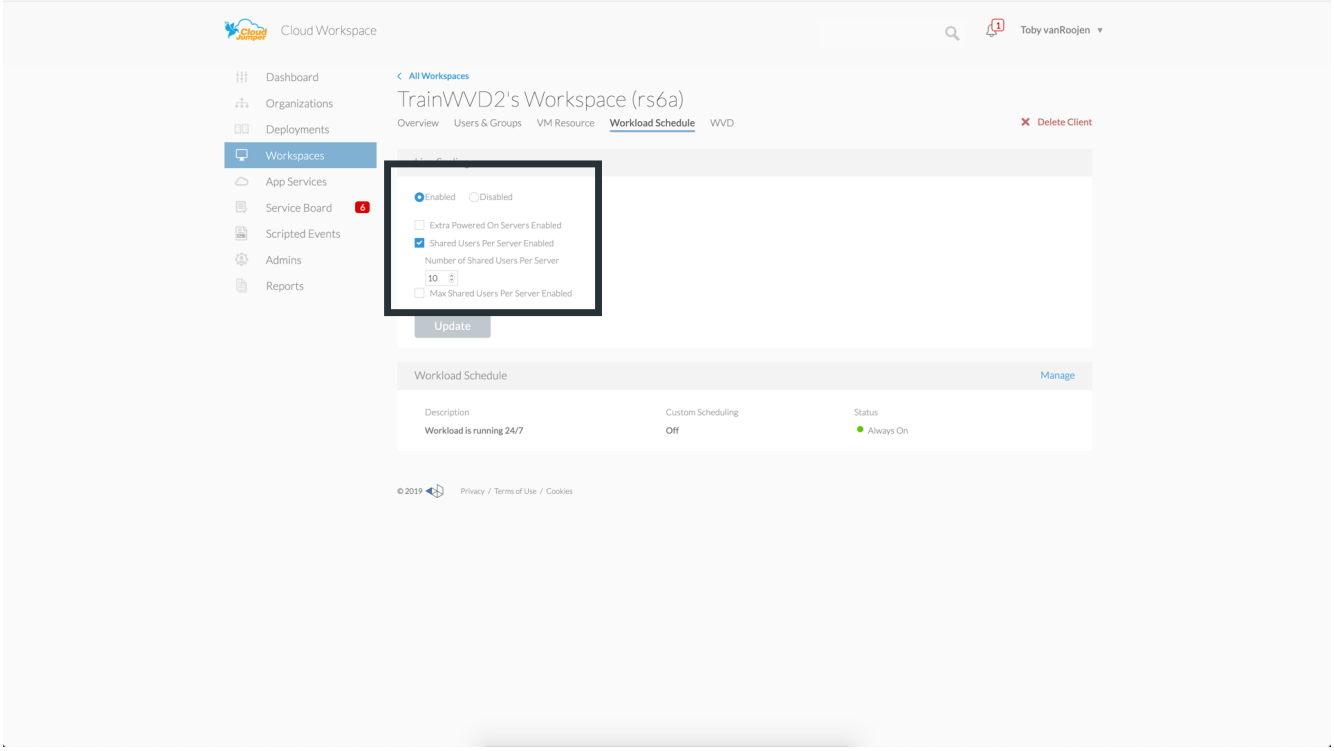
4. Click the Enabled radio button in the Live Scaling section.



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.



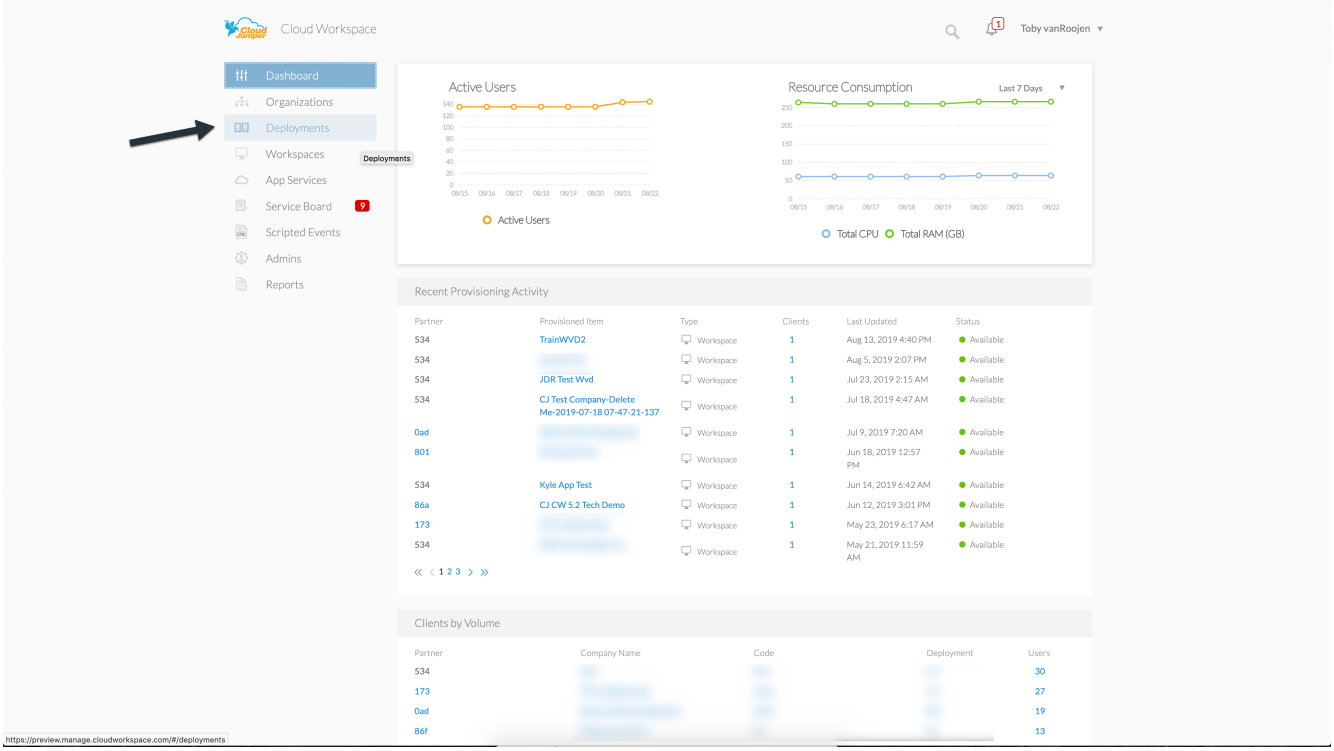
Live Scaling currently applies to all Shared resource pools. In the near future each pool will have independent Live Scaling options.

Power down the entire deployment

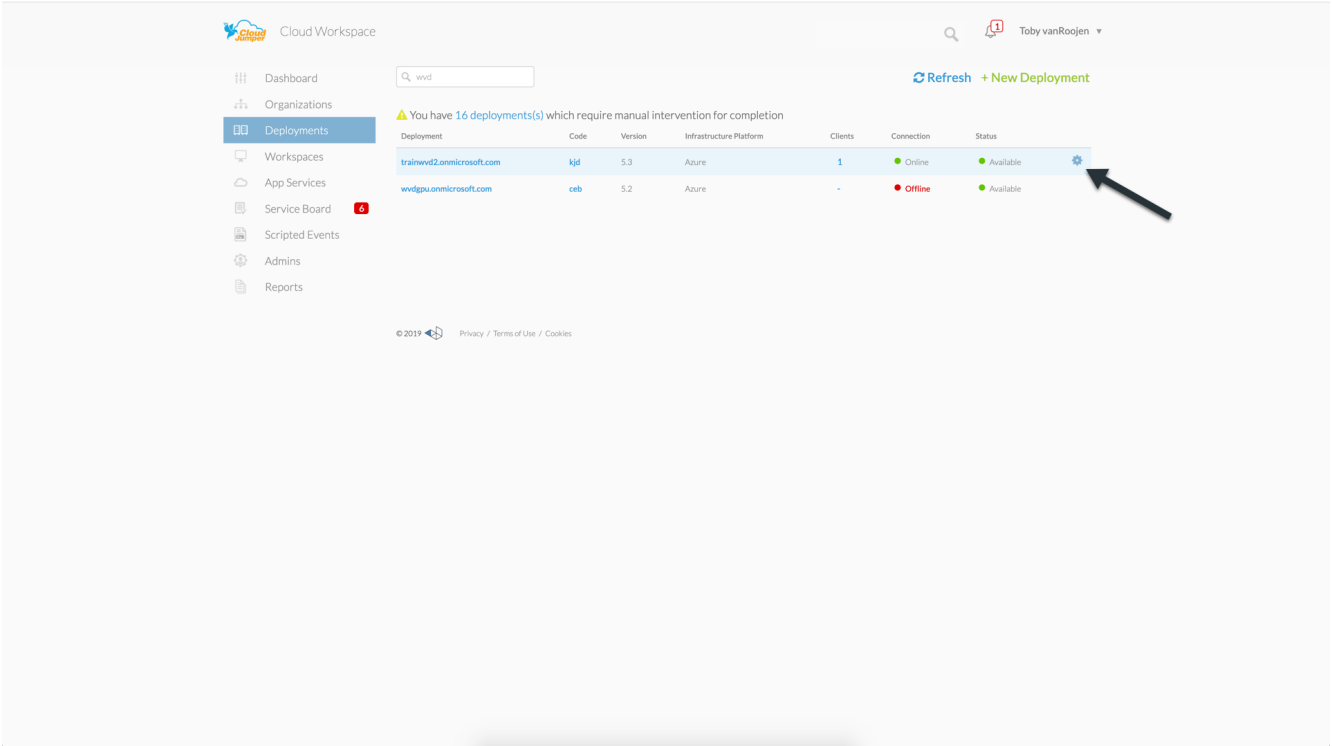
If you plan to only use your evaluation deployment on a sporadic, non-production basis you can turn off all the virtual machines in the deployment when you are not using them.

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

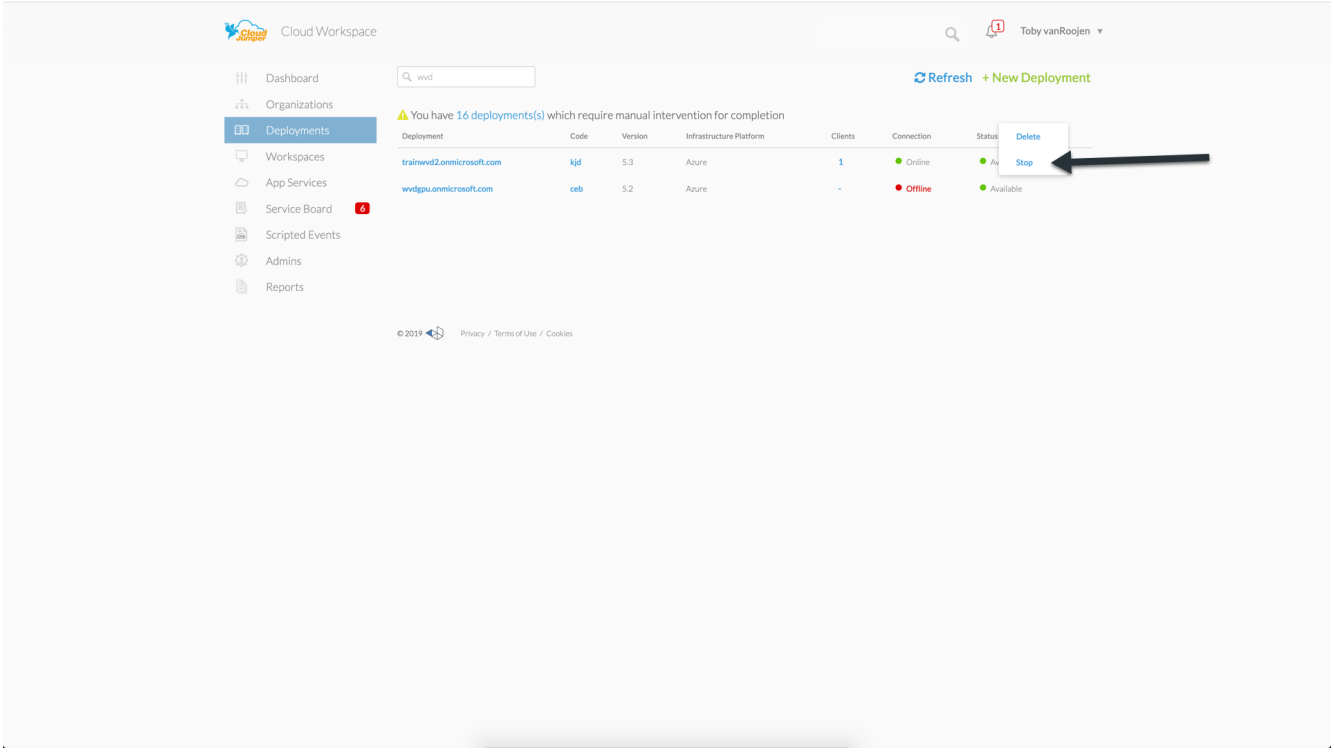
1. Log in to VDS at https://manage.cloudworkspace.com using your VDS credentials.
2. Click on the Deployments menu item.



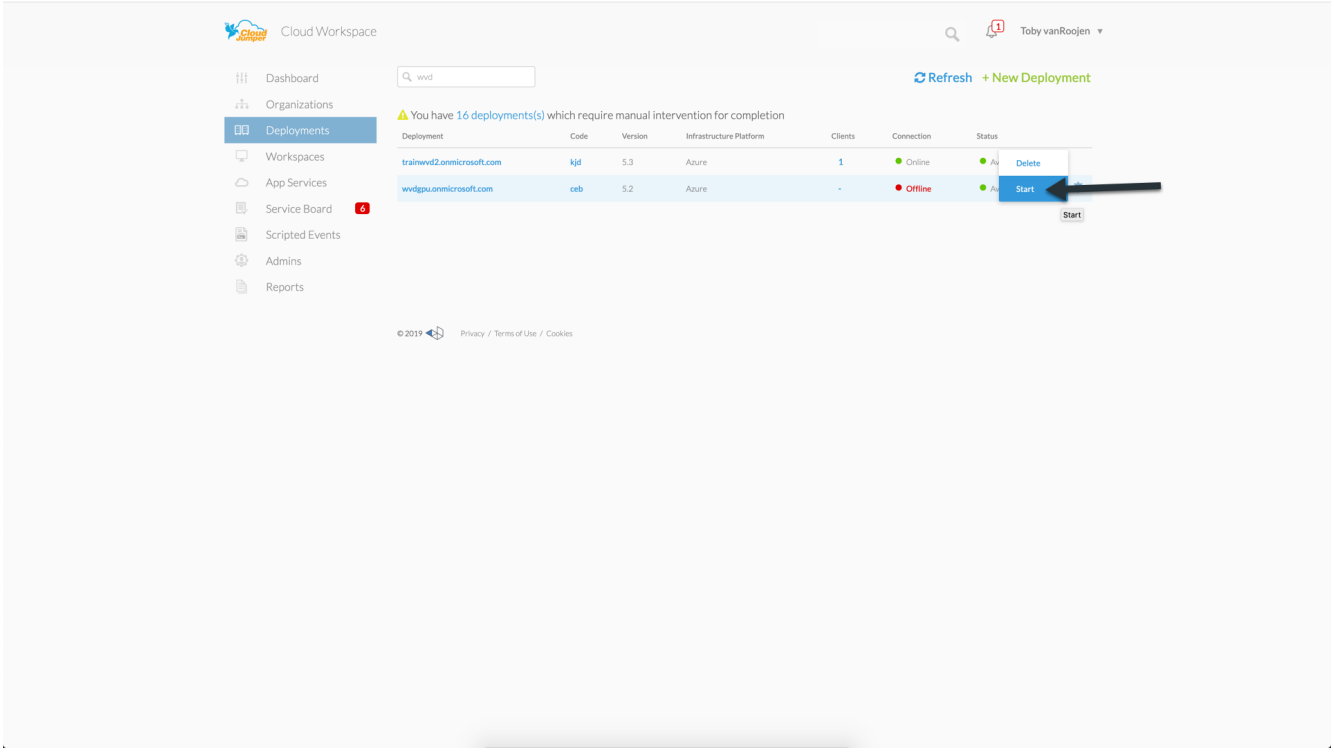
Scroll your cursor over the line for the target Deployment to display the Configuration gear icon.



3. Click on the gear, then choose Stop.



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



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://flightschool.cloudjumper.com/cwms/provisioning-collections/

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: 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 WVD host pools.

Controlled WVD workspace (default policies)

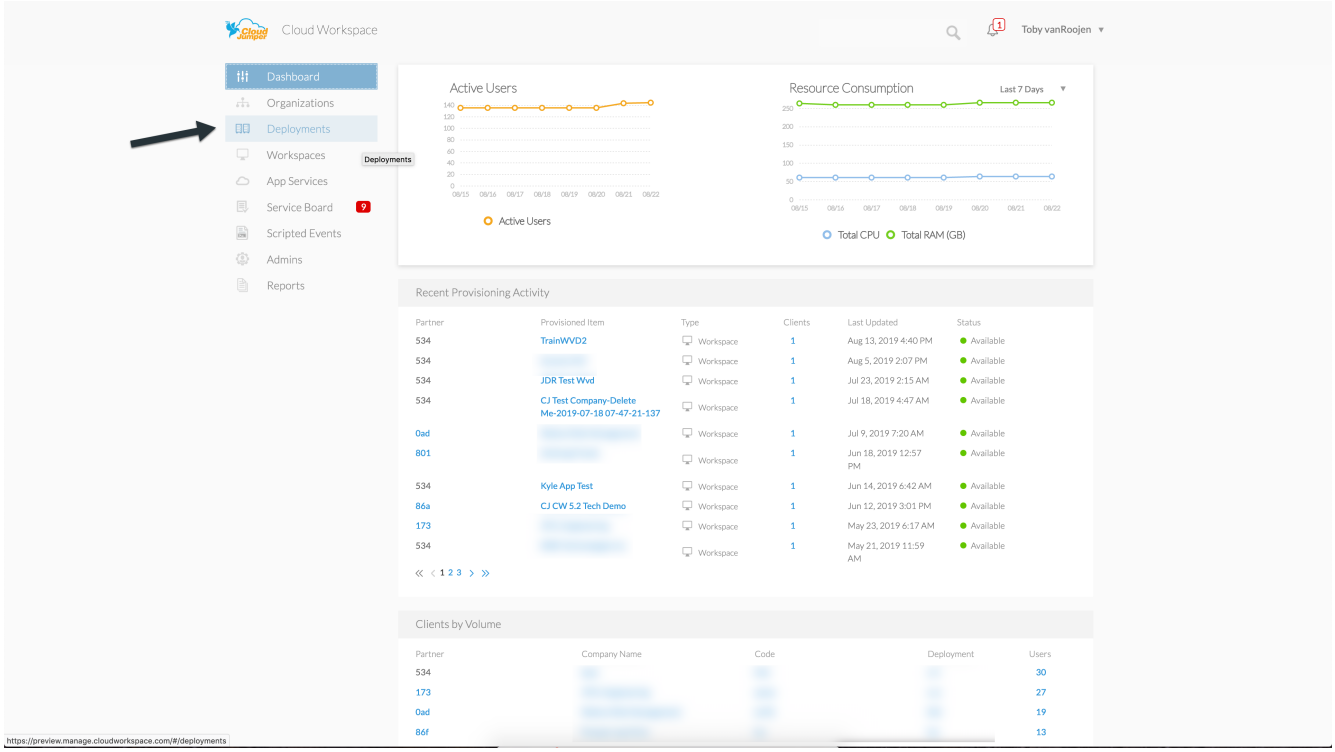
Using a controlled workspace is the default mode for VDS deployments. The polices are applied automatically. This mode requires VDS Administrators to install applications and then end users are granted access to the application via a shortcut on the session desktop. In a similar fashion, access to the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

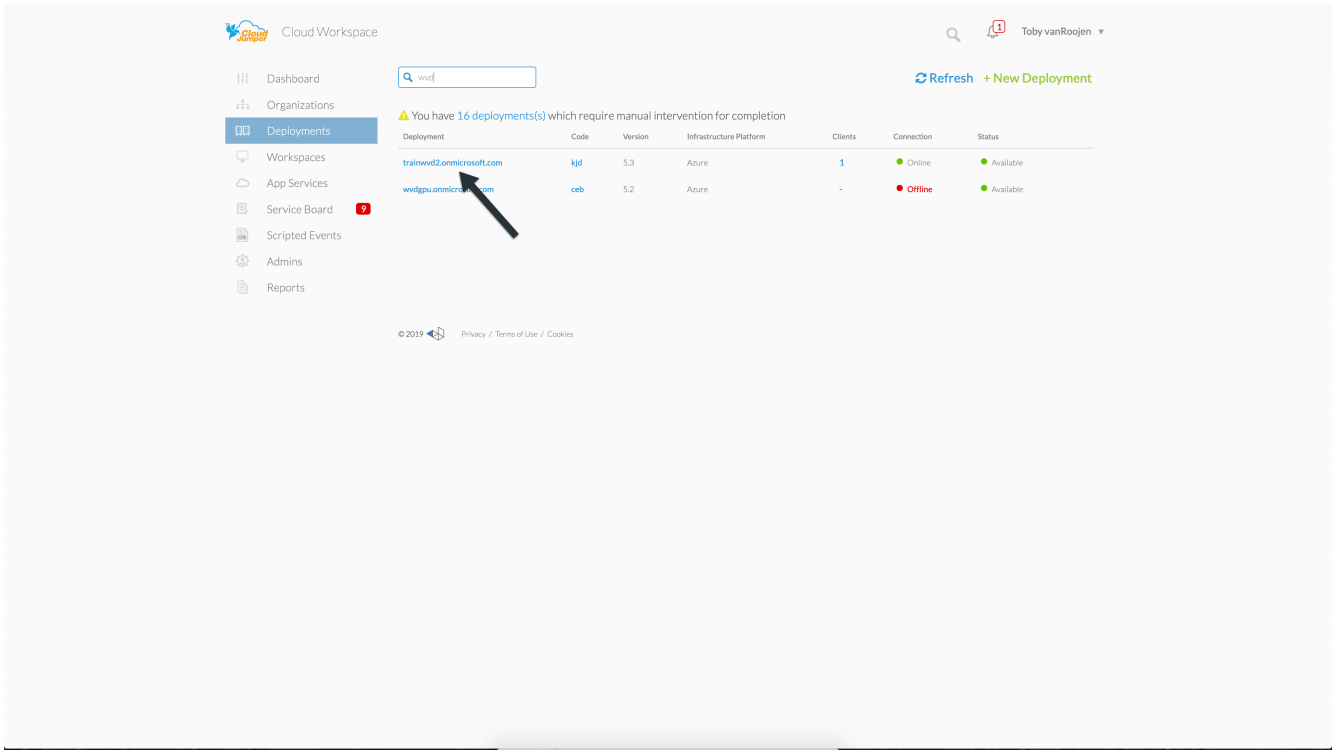
Creating a basic workspace requires disabling the default GPO policies that are created by default.

To do this, follow this one-time process:

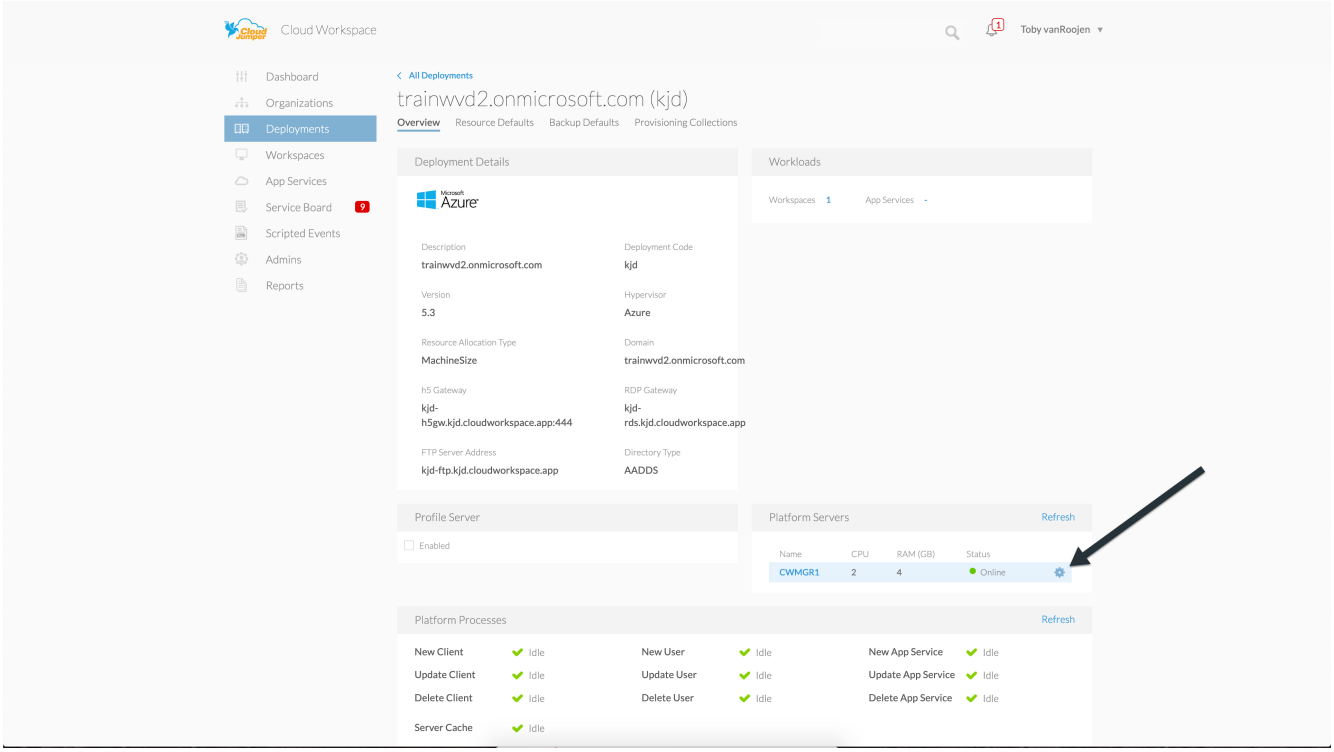
1. Log in to VDS at https://manage.cloudworkspace.com using your primary admin credentials.
2. Click on the Deployments menu item on the left.



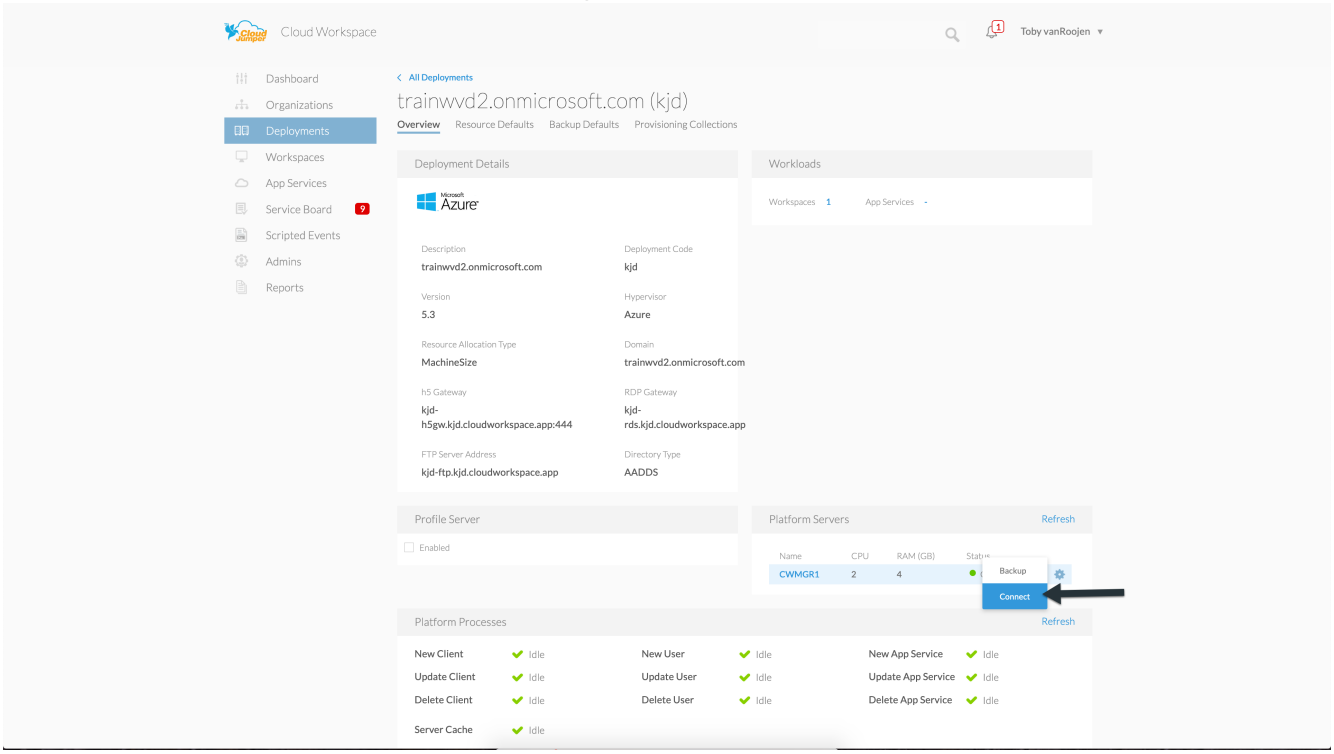
3. Click on the name of your Deployment.



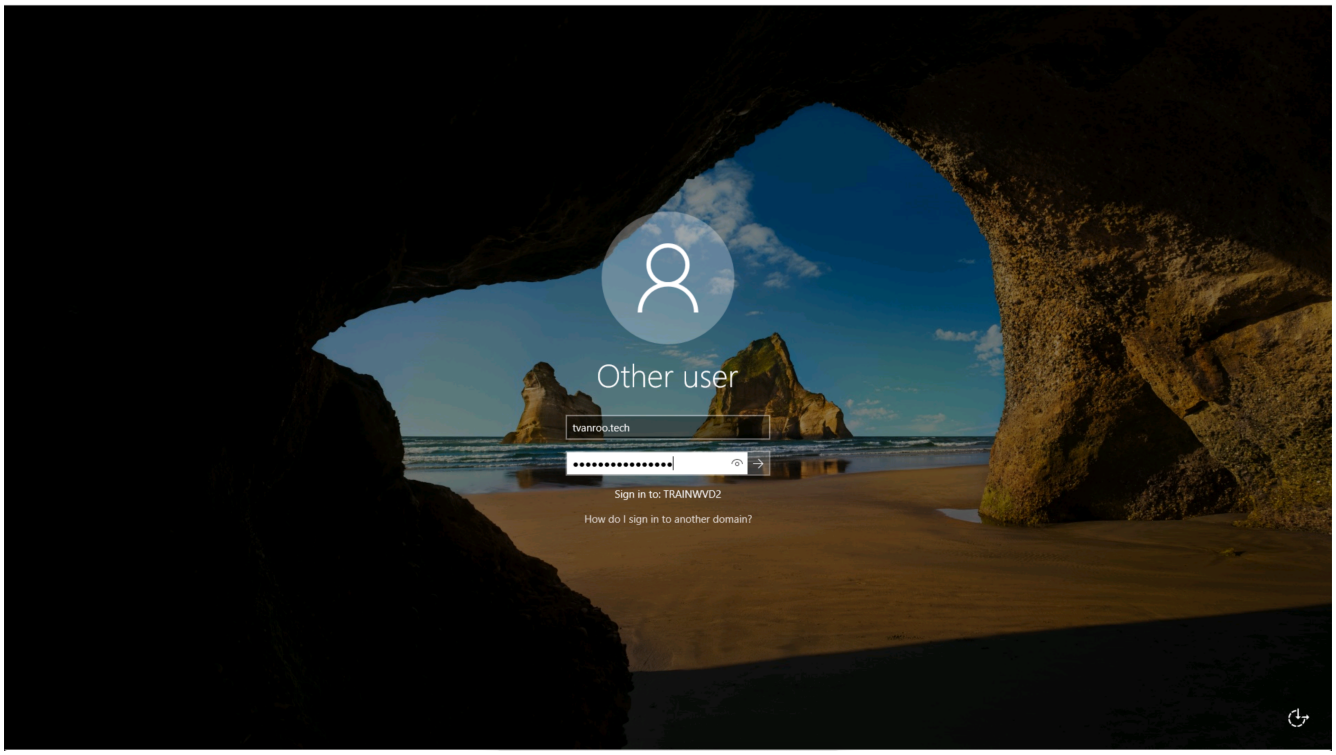
4. Under the Platform Servers section (mid page on right), scroll to the right of the line for CWMGR1 until the gear appears.



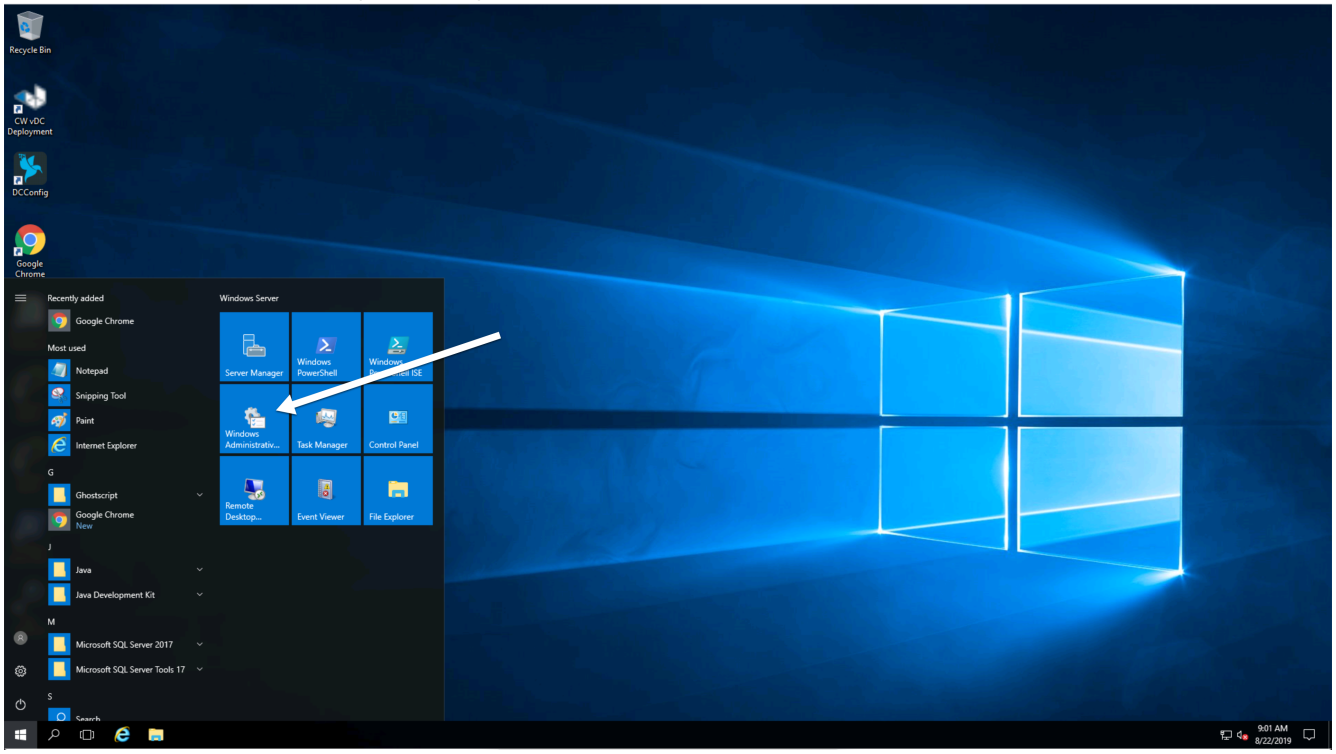
5. Click on the gear and choose Connect.



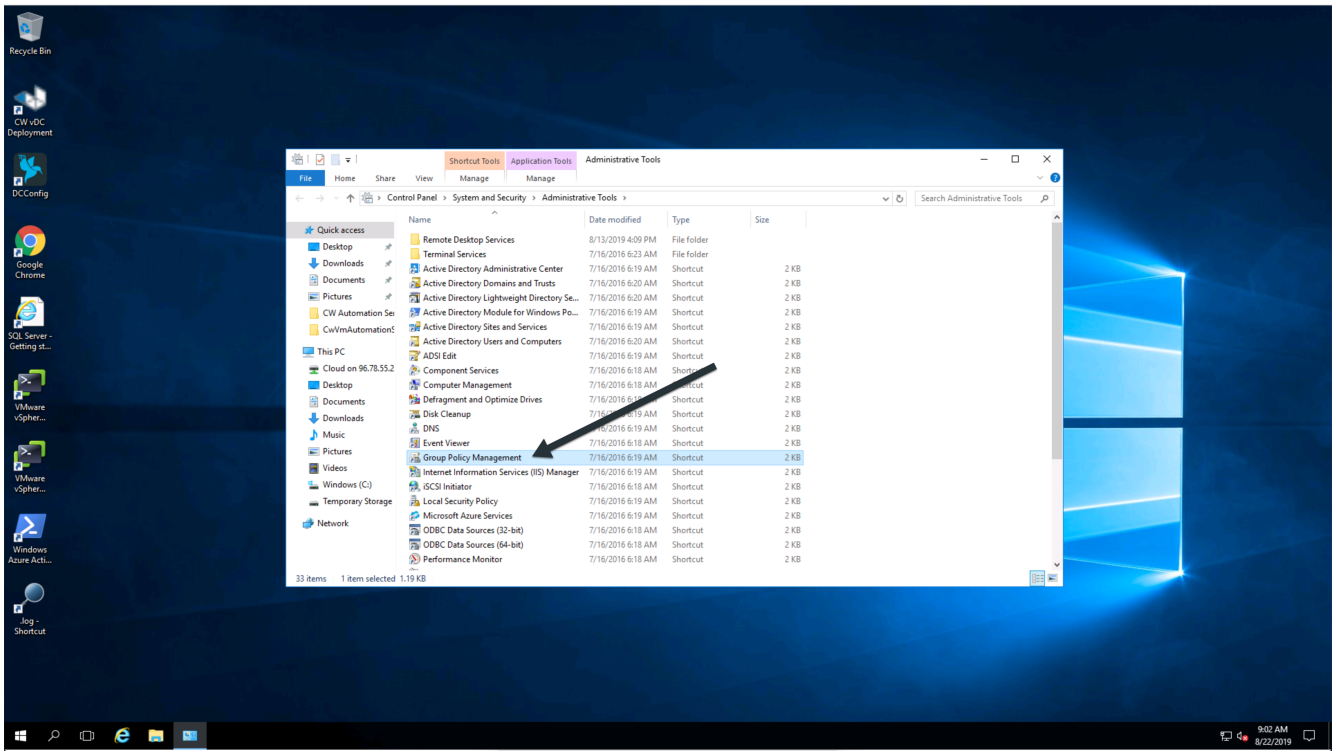
6. Enter the “Tech” credentials you created during provisioning to log on to the CWMGR1 server using HTML5 access.



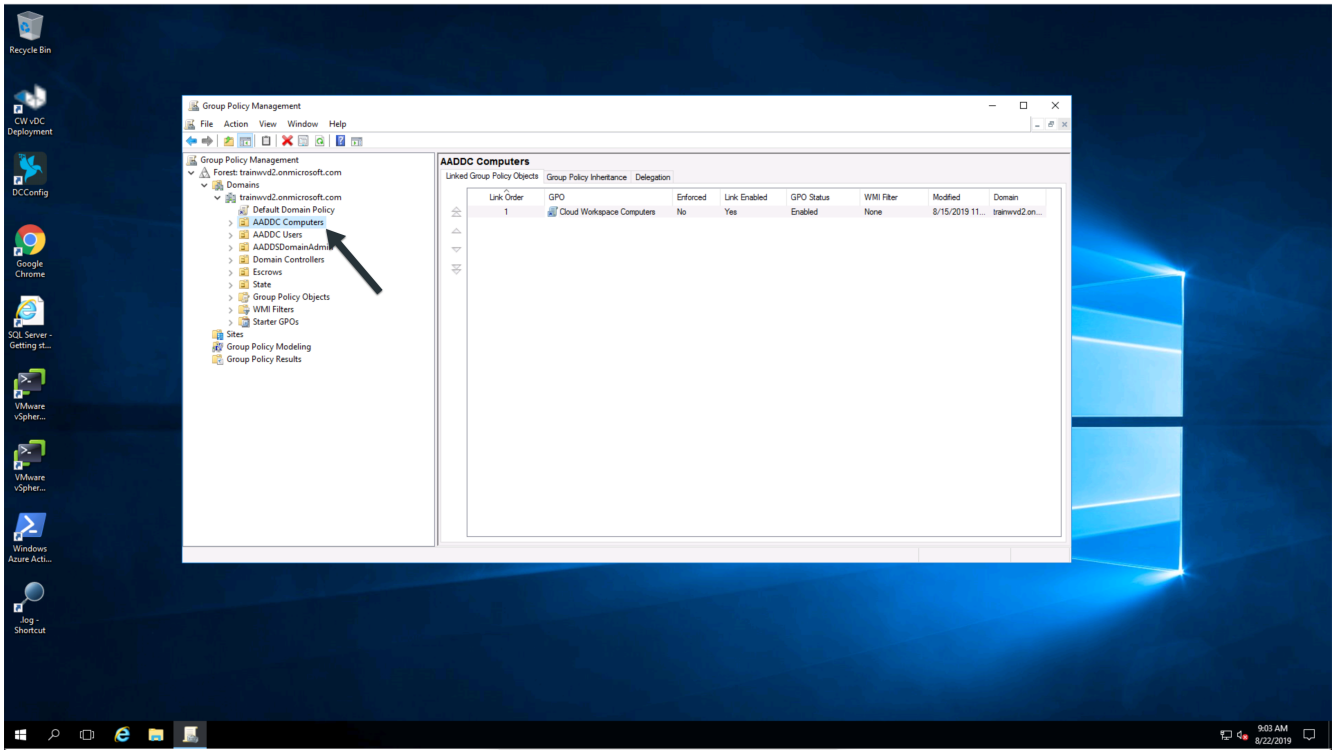
7. Click the Start (Windows) menu, choose Windows Administrative Tools.



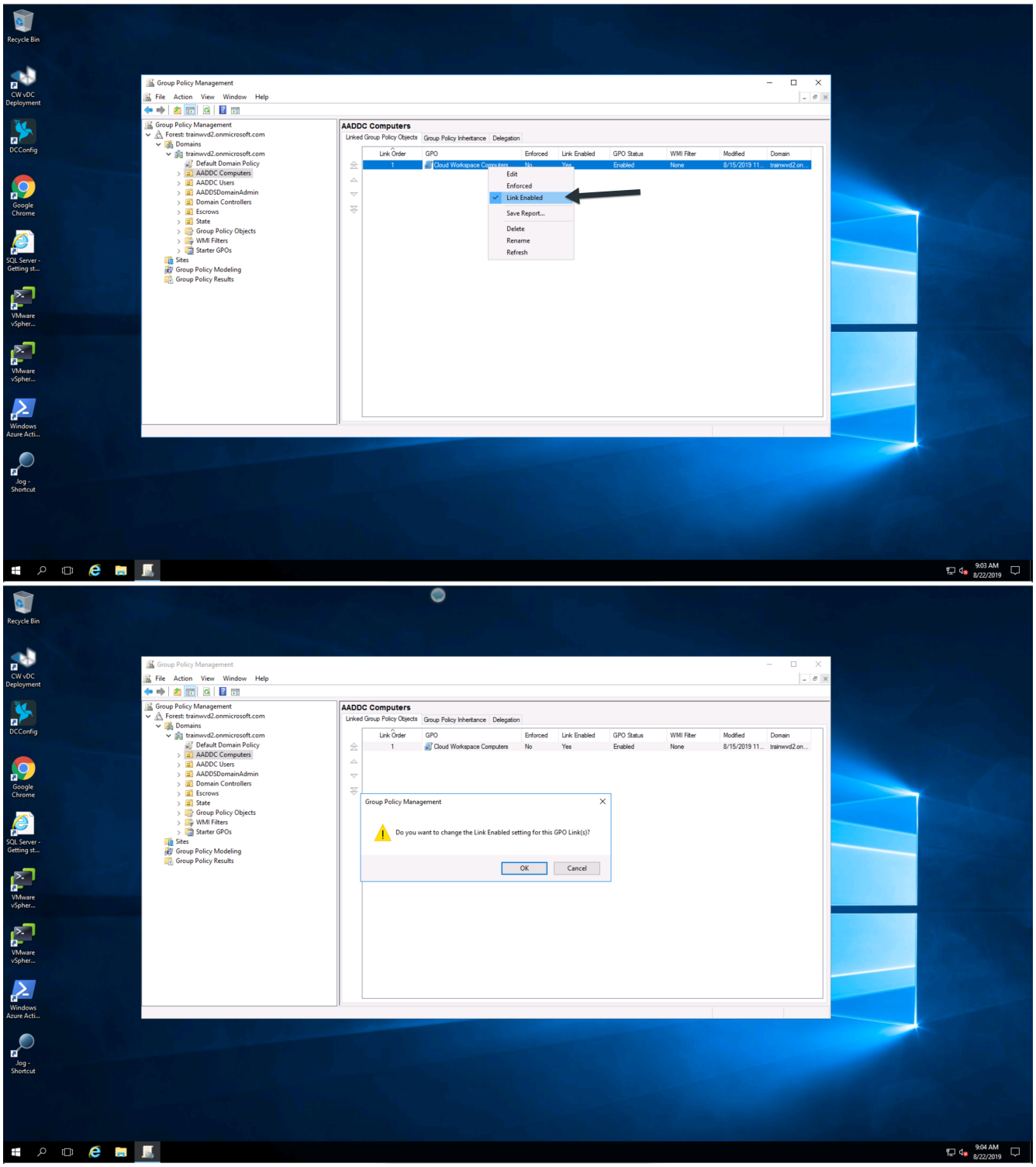
8. Click the Group Policy Management icon.



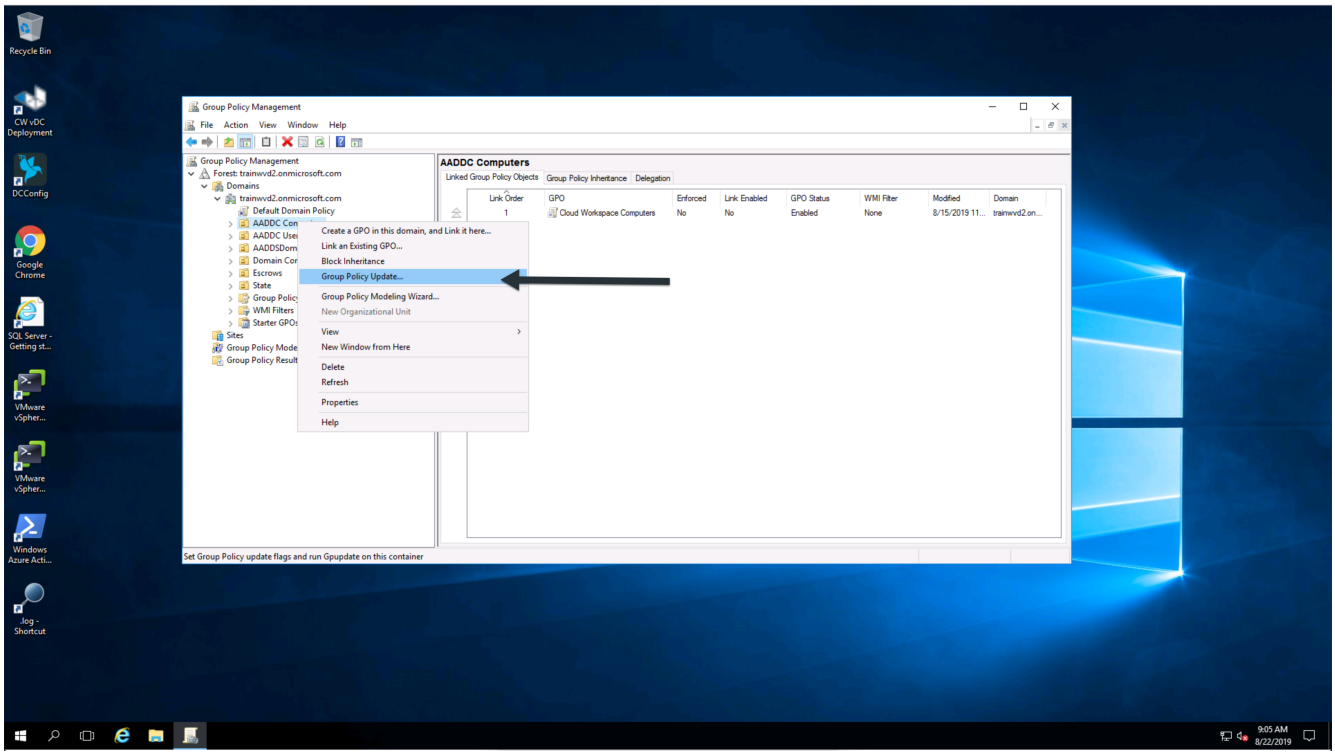
9. Click on the AADDC Users item in the list in the left pane.



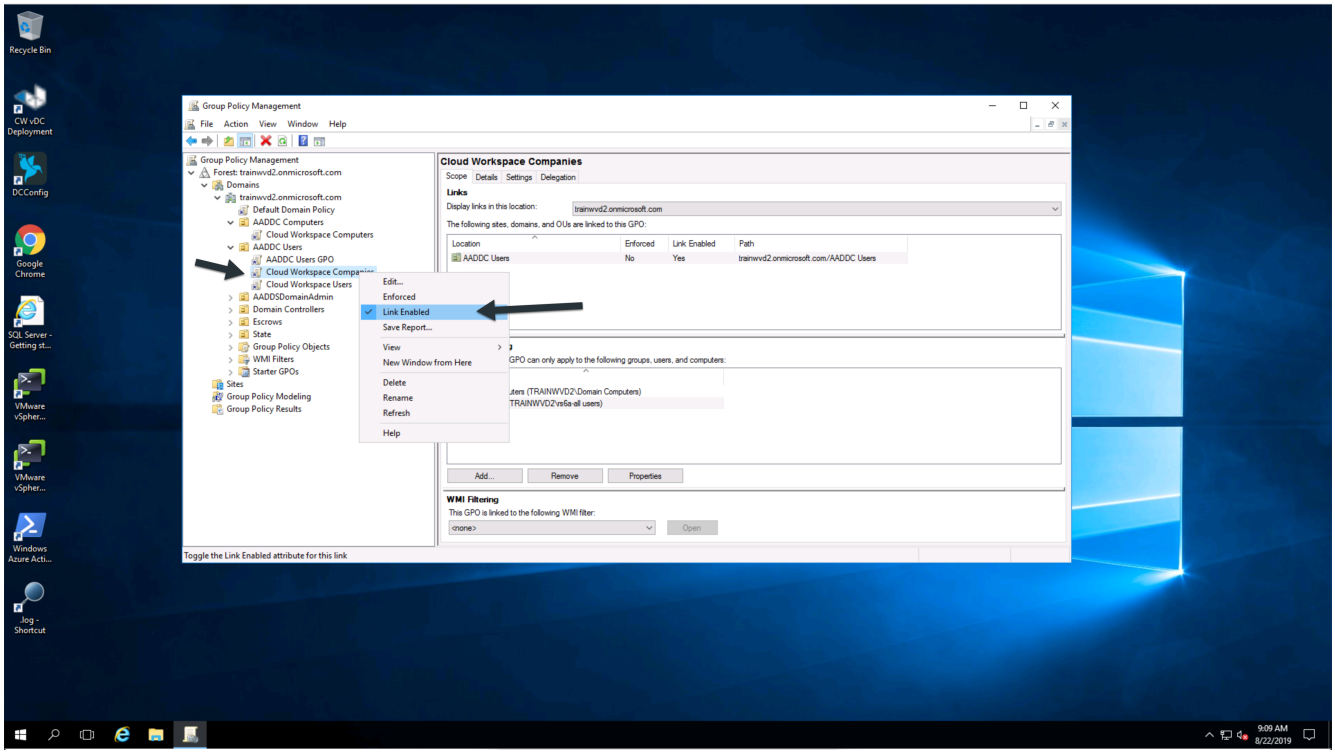
10. Right click on the “Cloud Workspace Users” policy in the list on the right pane, then deselect the “Link Enabled” option. Click OK to confirm this action.

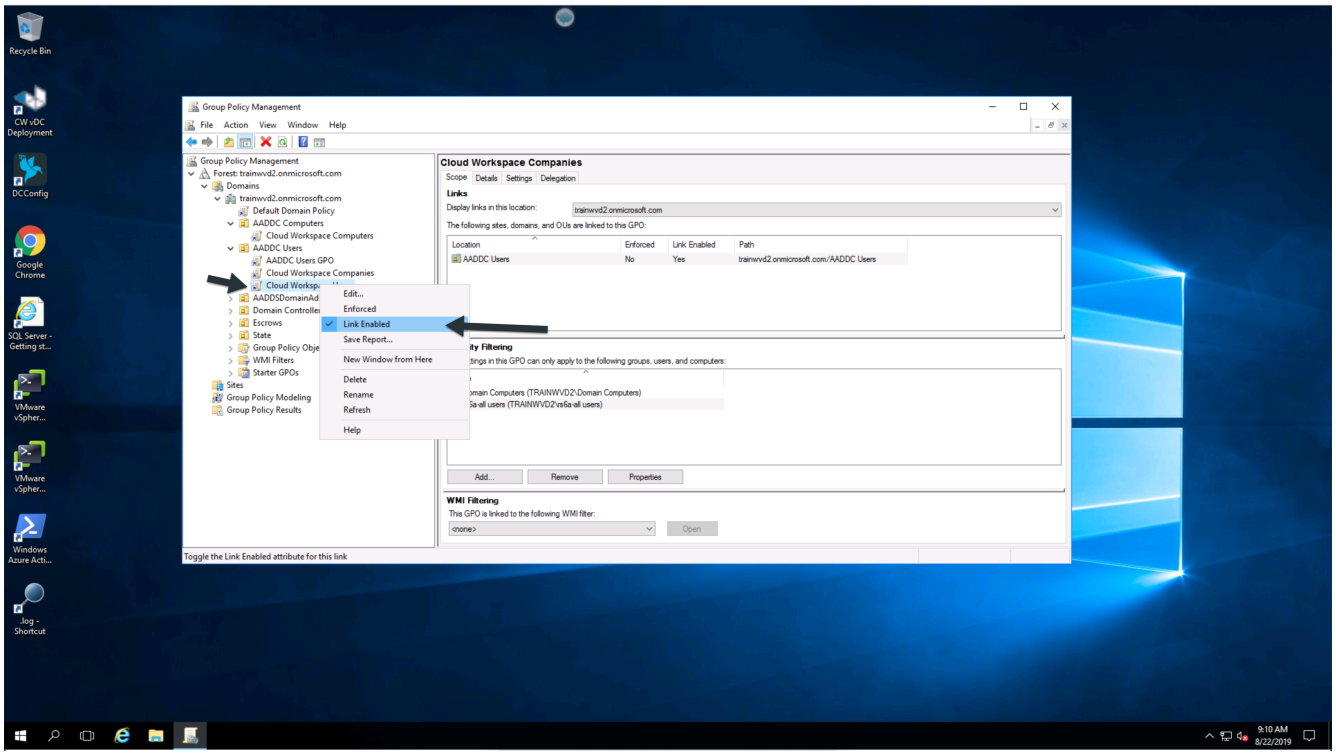


11. Select Action, Group Policy Update from the menu, then confirm that you want to force a policy update on those computers.

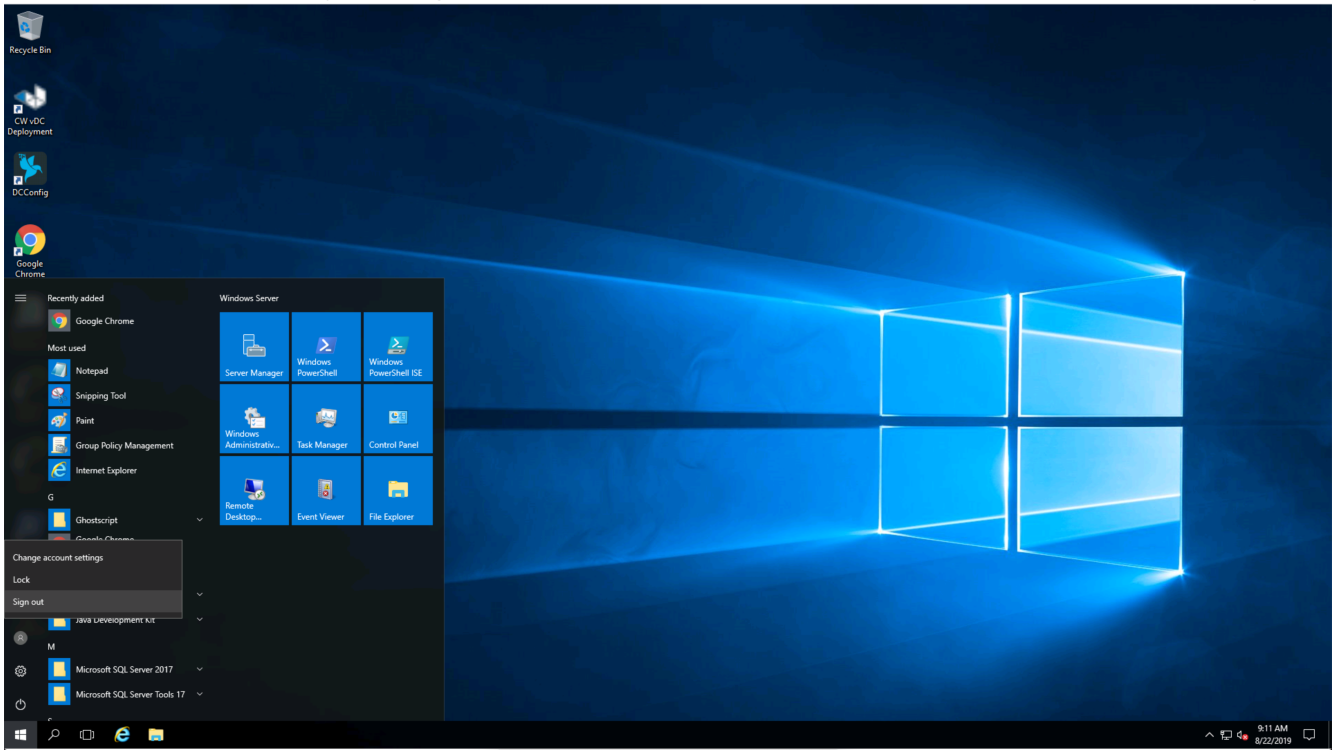


12. Repeat steps 9 and 10 but select “AADDC Users” and “Cloud Workspace Companies” as the policy to disable the Link. You do not need to force a Group Policy update after this step.





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.

WVD Deployment Guide - Existing AD Supplemental

Overview

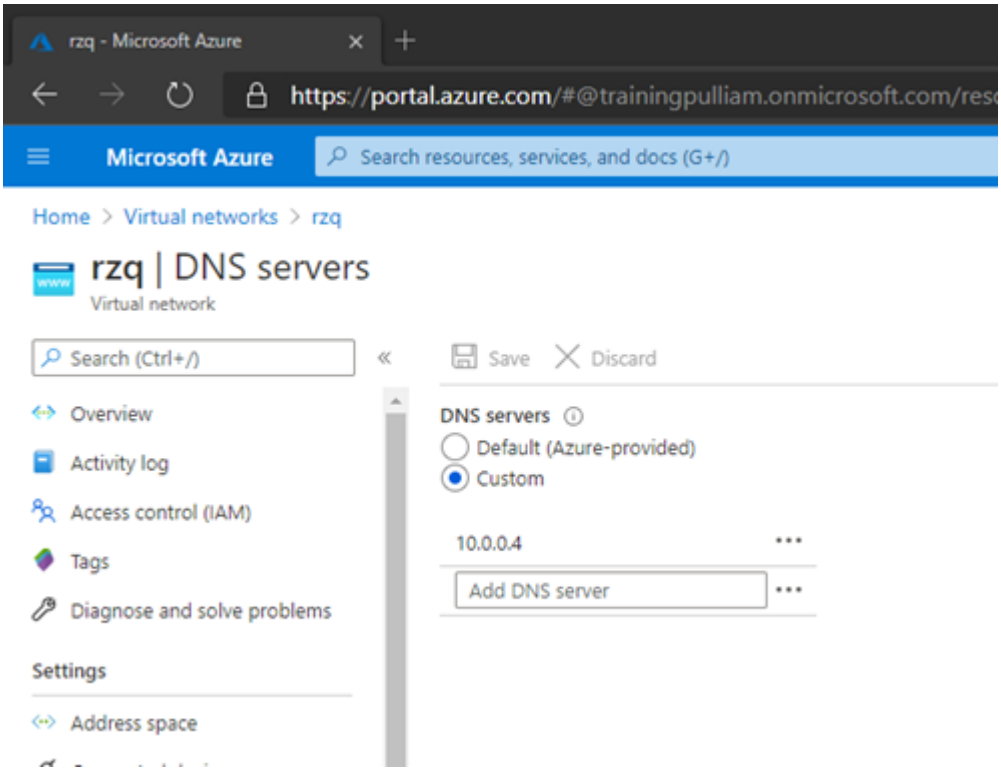
VDS Setup has the ability to connect a new deployment to an existing AD structure. These instruction cover that option in detail.
This article does not stand-alone, rather it is a detailed explanation of an alternative to the New AD option covered in the WVD Deployment Guide

Active Directory type

The next section defines to make is 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.



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.
Provide Active Directory Domain Admin Username and Password

This is the easiest method – providing domain admin credential that are used to facilitate the deployment.
Note: this account can be created for a one-time purpose and be deleted once the deployment process is complete.
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.
Manual Deployment Process
This option involves running the NetApp VDS Domain Preparation Tool, to build these permissions out automatically.

NetApp VDS deployment preparation tool

Access method

PowerShell commands

Requirements

1. Run on a server OS as opposed to a Workstation OS
2. Run on a server that is joined to the domain or is a domain controller
3. 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
4. Be executed by a user with Domain Admin privileges OR be executed by a user with local administrator permissions and ability to supply a Domain Administrator credential (for use with RunAs)
   Steps Overview:
5. Log into VDS Setup and extend permissions, then select the subscription you wish to deploy into
6. Once VDS Setup has loaded, click Review in the navigation bar on the left and note the deployment code for later
7. Log into any local domain joined machine (preferably Domain Controller, but any local domain joined machine will work) and run 3 actions with NetApp VDS Deployment Preparation Tool.
   Detailed Steps:
   Launch PowerShell, as ADMINISTRATOR, from the Domain Controller (or any local domain joined machine will work)
8. Run the following commands, individually, to launch NetApp VDS Deployment Preparation Tool:

```
[System.Net.ServicePointManager]::SecurityProtocol
=[System.Net.SecurityProtocolType]::'Ssl3','Tls','Tls11','Tls12';'
```

```
iex (new-object
system.net.webclient).donwloadstring('https://cjbootstrap3.cjautomate.ne
t/cjboostrapmenu.ps1')
```

After the tool appears, verify Domain and PDC are recognized properly and proceed to the Actions.

1. Select Action ‘Download this tool and click ‘Go’.
2. Select Action ‘Install Prerequisites’:
   a. If logged in as a user that is not a Domain Administrator, select RunAs and enter Domain Administrator

credentials.

b. Click ‘Go’.

3. Select Action ‘Prepare the domain’:

   a. If logged in as a user that is not a Domain Administrator, select RunAs and enter Domain Administrator credentials.

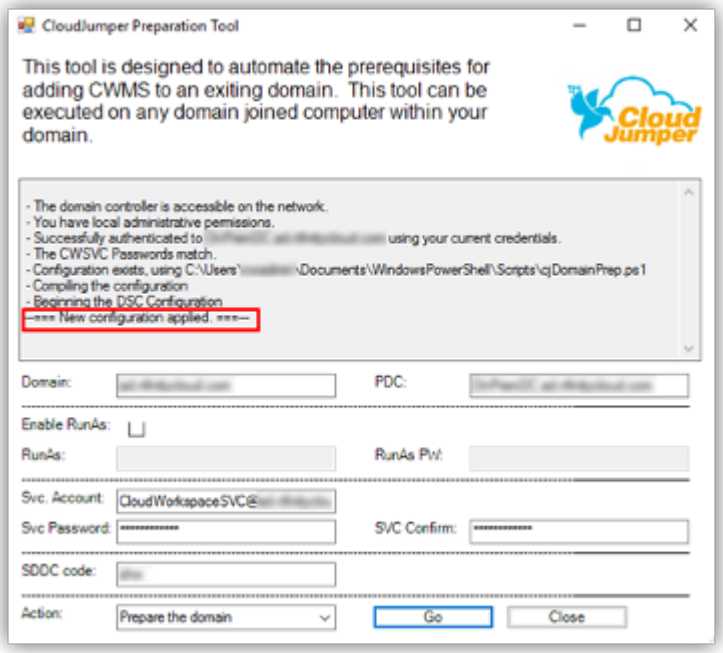
   b. Set the Svc account password.

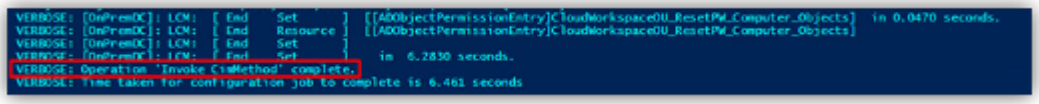
   c. Enter the SDDC code displayed in VDS Setup provisioning.

> This SDDC code is displayed in the VDS Setup WEB GUI window

4. Click ‘Go’.

5. Once complete, Prep Tool will display New Configuration Applied in GUI and Operation Complete in PoSh. Click Close:





Typing A and hitting Enter

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

WVD and VDS security entities and services

Windows Virtual Desktop (WVD) requires security accounts and components in both Azure AD and the local Active Directory to perform automated actions. NetApp's Virtual Desktop Service (VDS) creates components and security settings during the deployment process that allow administrators to control the WVD 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.

WVD 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 WVD Fall Release) WVD 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 WVD 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 WVD 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 execute from within the user context.
- cjAzBuild: this NetApp-created module contains build and maintenance automation and PowerShell processes that execute 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

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

Hybrid AD components

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

Domain Controller

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

AD Connect

To facilitate successful user authentication through the WVD 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 executed by a user with Domain Admin privileges OR be executed by a user with local administrator permissions and ability to supply a Domain Administrator credential (for use with RunAs)

Whether created manually or applied by 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, WVD session VMs) (done by group policy on the managed WVD 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.

WVD 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 WVD-PaaS components
- VDS platform components
- VDS workspace components in Azure Tenant
- Hybrid AD Components

End user clients

Users can connect to their WVD 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 think-client vendors who have published endpoint client for WVD. These are listed at https://docs.microsoft.com/en-us/azure/virtual-desktop/linux-overview

VDS control plane components

VDS REST API

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

VDS web app

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

Control plane database

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

VDS Comms

Azure tenant components

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

Microsoft Azure WVD-PaaS components

WVD REST API

Microsoft WVD can be managed via API. VDS leveraged these APIs extensively to automate and managed WVD 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 WVD deployments.

WVD web client

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

Session gateway

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

VDS platform components

CWMGR1

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

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

- **Windows Services** - VDS uses Windows services to perform automation and management actions from within a deployment:
  - **CW Automation Service** is a Windows Service deployed on CWMGR1 in each WVD deployment that performs many of the user-facing automation tasks in the environment. This service runs under the **CloudWorkspaceSVC** AD account.
  - **CW VM Automation Service** is a Windows Service deployed on CWMGR1 in each WVD deployment that performs the virtual machine management functions. This service runs under the **CloudWorkspaceSVC** AD account.
  - **CW Agent Service** is a Windows Service deployed to each virtual machine under VDS management, including CWMGR1. This service runs under the **LocalSystem** context on the virtual machine.
  - **CWManagerX API** is an IIS app pool-based listener installed on CWMGR1 in each WVD deployment. This handles inbound requests from the global control plane and is run under the **CloudWorkspaceSVC** AD account.
- **SQL Server 2017 Express** – VDS creates a SQL Server Express instance on the CWMGR1 VM to manage the metadata generated by the automation components.
- **Internet Information Services (IIS)** – IIS is enabled on CWMGR1 to host the CWManagerX and CWApps IIS application (only if RDS RemoteApp functionality is enabled). VDS requires IIS version 7.5 or greater.
- **HTML5 Portal (Optional)** – VDS installs the Spark Gateway service to provide HTML5 access to the VMs in the Deployment and from the VDS web application. This is a Java based application and can be disabled and removed if this method of access is not desired.
- **RD Gateway (Optional)** – VDS enables the RD Gateway role on CWMGR1 to provide RDP access to RDS Collection based Resource Pools. This role can be disabled/uninstalled if only WVD Reverse Connect access is desired.
- **RD Web (Optional)** – VDS enables the RD Web role and creates the CWApps IIS web application. This role can be disabled if only WVD access is desired.
- **DC Config** – a Windows application used to perform Deployment and VDS Site specific configuration and advanced configuration tasks.
- **Test VDC Tools** – a Windows application that supports direct task execution for Virtual Machine and client level configuration changes used in the rare case where API or Web Application tasks need to be modified for troubleshooting purposes.
- **Let's Encrypt Wildcard Certificate (Optional)** – created and managed by VDS – all VMs that require HTTPS traffic over TLS are updated with the certificate nightly. Renewal is also handled by automated task (certificates are 90 day so renewal starts shortly before). Customer can provide their own wildcard certificate 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 WVD session hosts.
  - **Cloud Workspace Firewall GPO** (linked to Dedicated Customers Servers, Remote Desktop and Staging OUs) - creates a policy that ensures and isolates connections to sessions hosts from Platform server(s).
  - **Cloud Workspace RDS** (Dedicated Customers Servers, Remote Desktop and Staging OUs) - policy set limits for session quality, reliability, disconnect timeout limits. For RDS sessions the TS licensing Server Value is defined.
  - **Cloud Workspace Companies** (NOT LINKED by default) – optional GPO to “lock down” a user session/ workspace by preventing access to administrative tools and areas. Can be linked/enabled to provide a restricted activity workspace.

Default Group Policy setting configurations can be provided on request.

VDS workspace components

Data layer

Azure NetApp Files

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

Azure Files

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

File server with Managed Disk

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

Azure networking

Azure virtual network

VDS creates an Azure Virtual Network and supporting subnets. VDS requires a separate subnet for CWMGR1, WVD host machines, and Azure domain controllers and peering between the subnets. Note that the AD controller subnet typically already exists so the VDS deployed subnets will need to be peered with the existing subnet.

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. WVD virtual machines are governed at a computer level by both the AD structure (organizational units, group policy, local computer administrator permissions etc.) and membership in the WVD structure (host pools, 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 WVD actions and the local AD service account (CloudWorkspaceSVC) for local AD and local computer actions.

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

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

Joining VMs to Azure AD

Virtual machines in the Azure tenant need to be joined to the domain however VMs cannot joining directly to Azure AD. Therefore, VDS deploys the domain controller role in the VDS platform and then we sync that DC with Azure AD using AD Connect. Alternative configuration options include using Azure AD Domain Services

(AADDS), syncing to a hybrid DC (a VM on-premises or elsewhere) using AD Connect, or directly joining the VMs to a hybrid DC through a site-to-site VPN or Azure ExpressRoute.

WVD Host pools

Host pools are a collection of one or more identical virtual machines (VMs) within Windows 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 WVD 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 WVD 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

WVD and VDS Prerequisites

WVD and VDS requirements and notes

This document describes the required elements for deploying Windows Virtual Desktop (WVD) 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 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
- 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 Windows Virtual Desktop:

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

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

Windows 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)
*.wvd.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 WVD 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

WVD activation in Azure is a tenant-wide setting. VDS supports running one WVD 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 WVD 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 WVD 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.

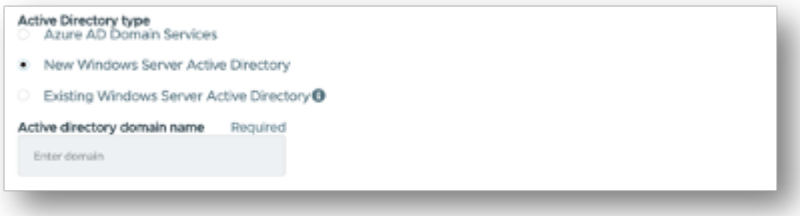
The Azure Marketplace provides the most recent versions of their base Windows 10 image and all Azure subscriptions have access to those automatically. If you want to use a different image or a custom image, want the VDS team to provide advice about creating or modifying other images or have general questions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

Active Directory

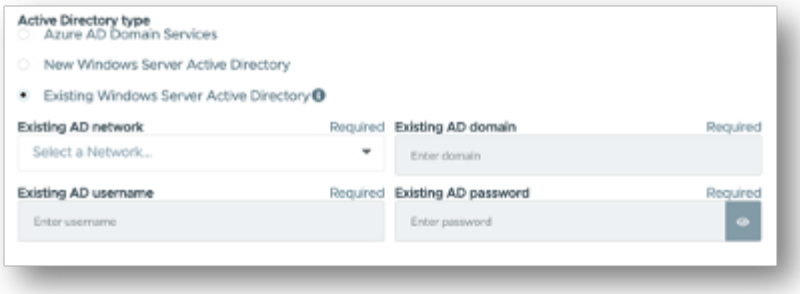
WVD requires that the user identity be a part of Azure AD and that the VMs are joined to an Active Directory domain that is synced with that same Azure AD instance. VMs cannot be attached directly to the Azure AD instance so a domain controller needs to be configured and in-sync with Azure AD.

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 Windows 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

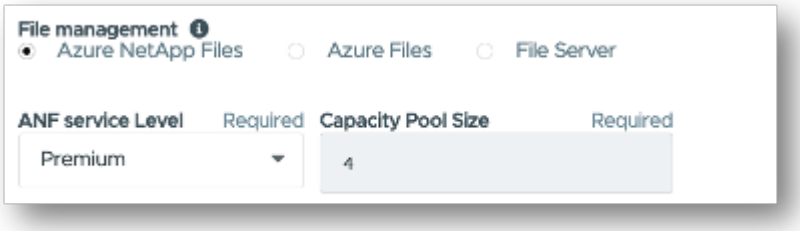
In WVD the storage strategy is designed so that no persistent user/company data resides on the WVD session VMs. Persistent data for user profiles, user files and folders, and corporate/application data are hosted on one or more data volume(s) hosted on an independent data layer.

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

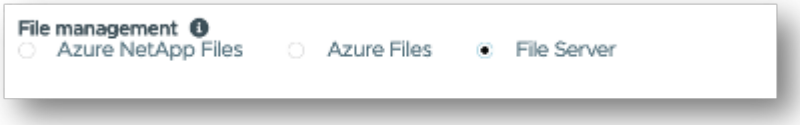
Due to this architecture a data storage function is required. This function must be able to handle the data transfer required each morning/afternoon when a significant portion of the users login/logoff at the same time. Even moderately sized environments can have significant data transfer requirements.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

The VDS Setup wizard supports the following configurations:

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



- Setup and configuration of a File Server VM



Networking

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

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

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

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

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

CWMGR1

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

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

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

Decision tree in the Deployment Wizard

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

Azure region

Decide which Azure region or regions will host your WVD Virtual Machines. Note that Azure NetApp Files and certain VM families (GPU enabled VMs, for example) have a defined Azure region support list while WVD 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 WVD 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 WVD instance. In this case VDS deploys a limited set of components into the domain to support automated provisioning and management tasks for the WVD 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 WVD host pools and data volumes as they are joined to the domain. The WVD VDS Components and Permissions guide defines the required components and permissions and the deployment process requires a Domain user with domain privileges to execute 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 WVD 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 WVD 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 WVD 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 WVD deployment
This configuration type assumes that the necessary Azure VNet, Active Directory, and WVD 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 WVD Tenant needs to be granted to the VDS Enterprise Applications in the Azure
- WVD Host Pool and WVD Host Pool VMs need to be imported into VDS using the VDS Import function in the VDS Web App. This process collects the WVD host pool and session VM metadata and stores in it VDS so that these elements can be managed by VDS
- WVD 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 WVD App Group membership and session information can be managed by VDS

APPENDIX A: VDS control plane URLs and IP addresses

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

api.cloudworkspace.com
autoprodb.database.windows.net
vdctoolsapi.trafficmanager.net
cjbootstrap3.cjautomate.net

If your access control device can only white list by IP address, the following list of IP addresses should be whitelisted. 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 WVD requirements

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

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

Windows Virtual Desktop session host licensing

Windows 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 WVD machines

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

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

Windows 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

Windows 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:

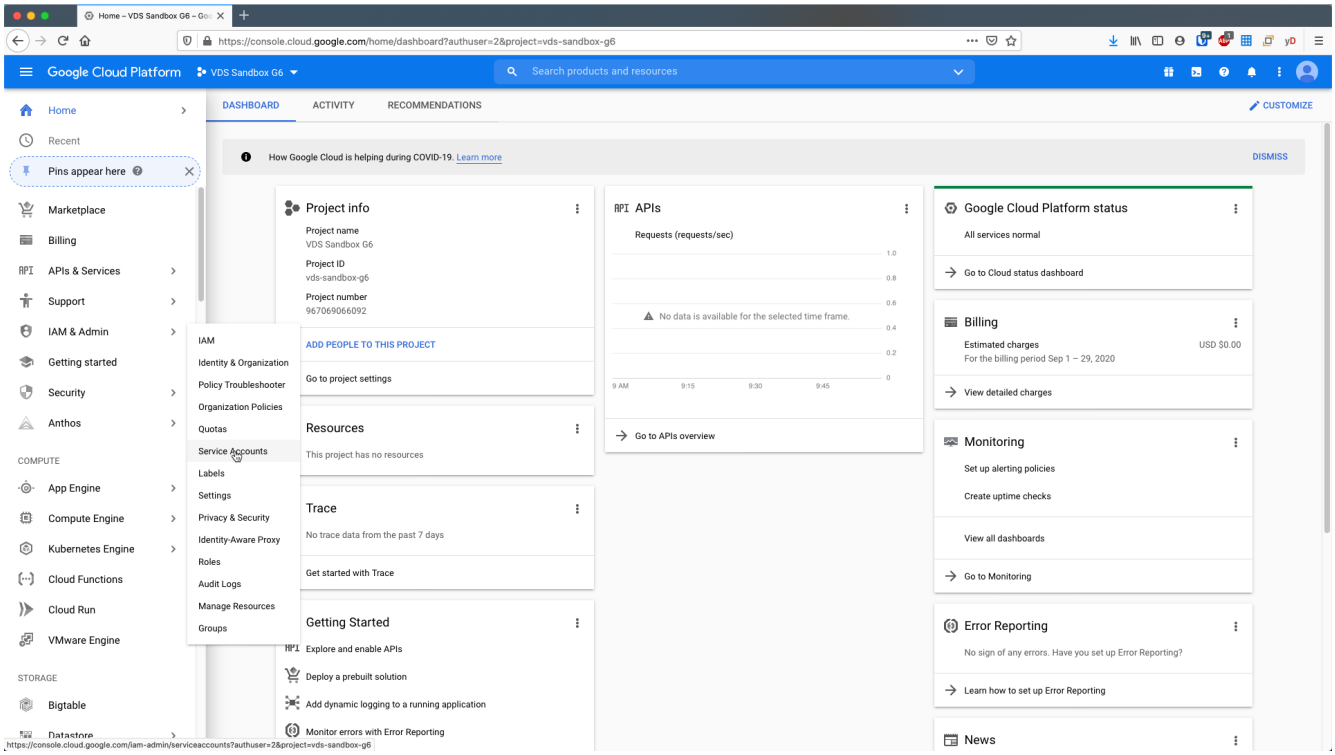
- RDS gateway server(s)
- Web client access server(s)
- Domain controller server(s)
- RDS licensing service
- ThinPrint licensing service
- Filezilla FTPS server service

Guide scope

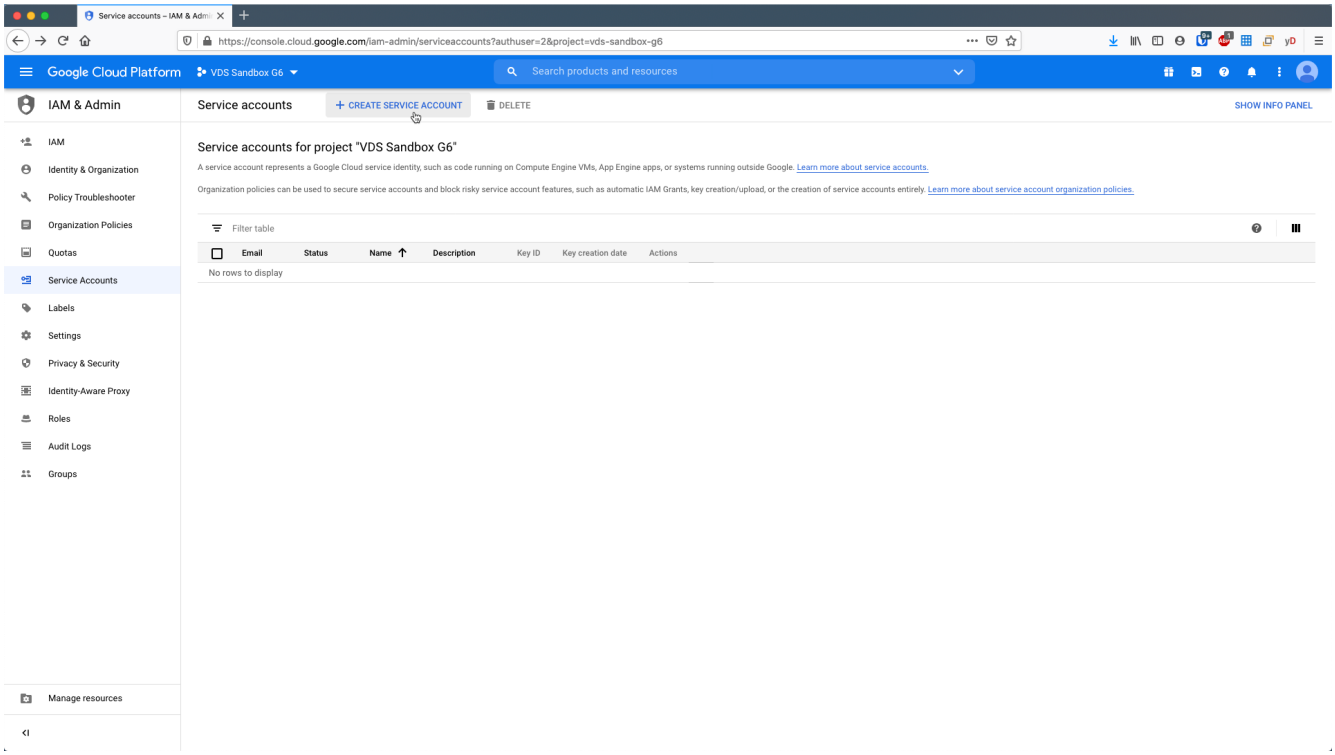
This guide walks you through the deployment of RDS using NetApp VDS technology from the perspective of a GCP and VDS administrator. You bring the GCP project with zero pre-configuration and this guide helps you setup RDS end-to-end.

Create service account

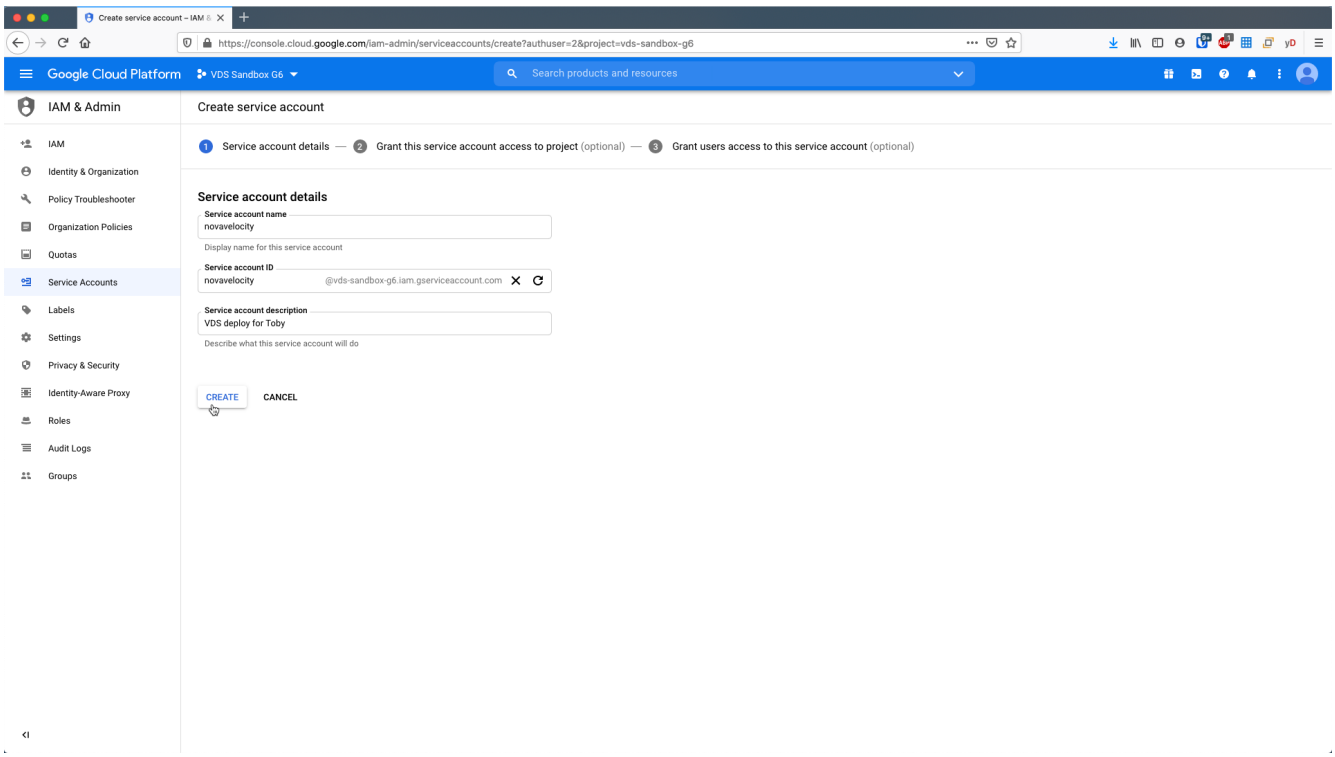
1. In GCP, navigate to (or search for) *IAM & Admin* > *Service Accounts*



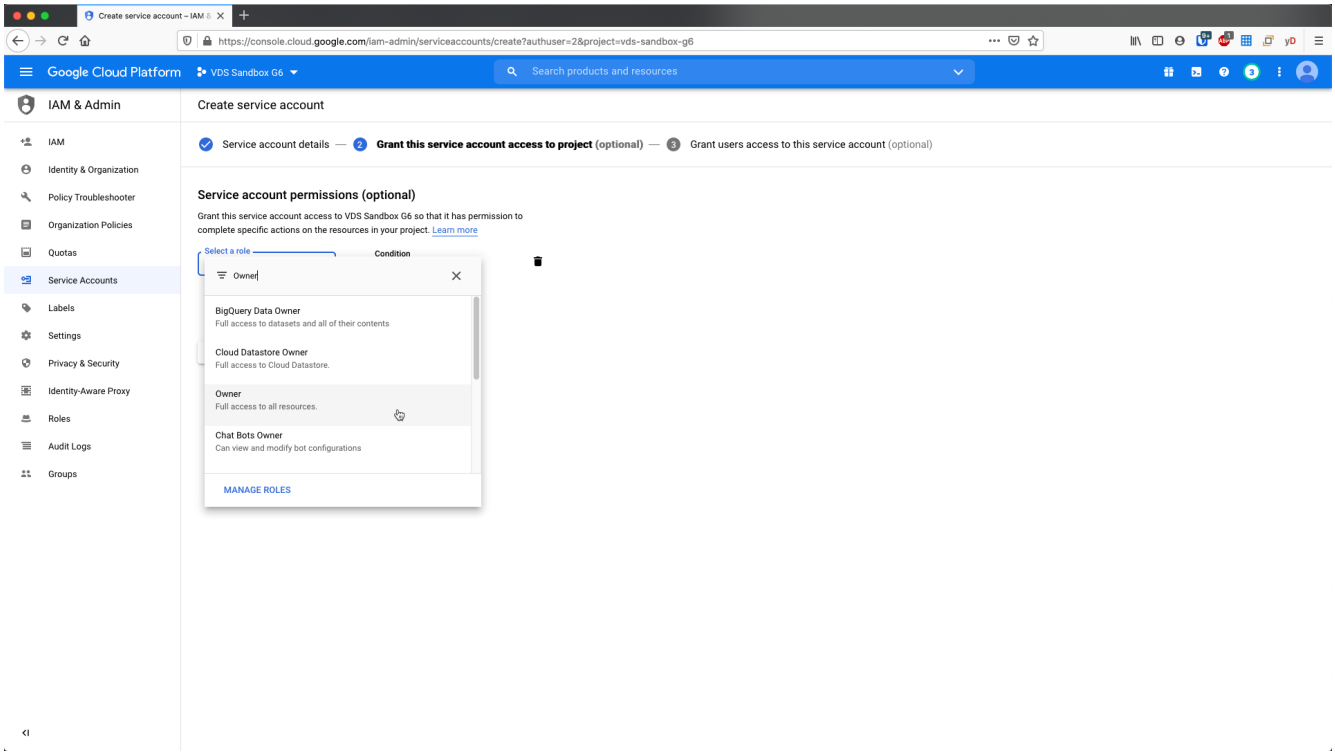
2. Click + *CREATE SERVICE ACCOUNT*



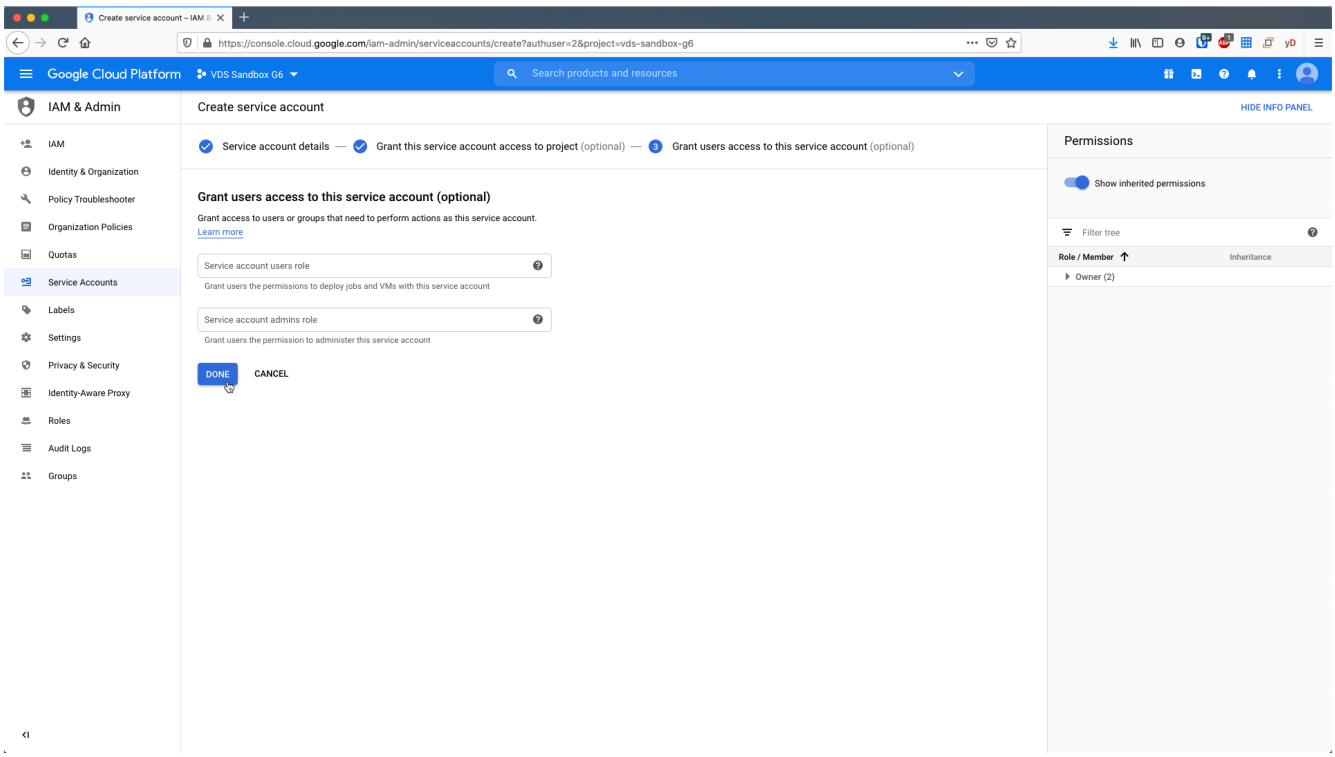
3. Enter a unique service account name, click *CREATE*. Make a note of the service account's email address which will be used in a later step.



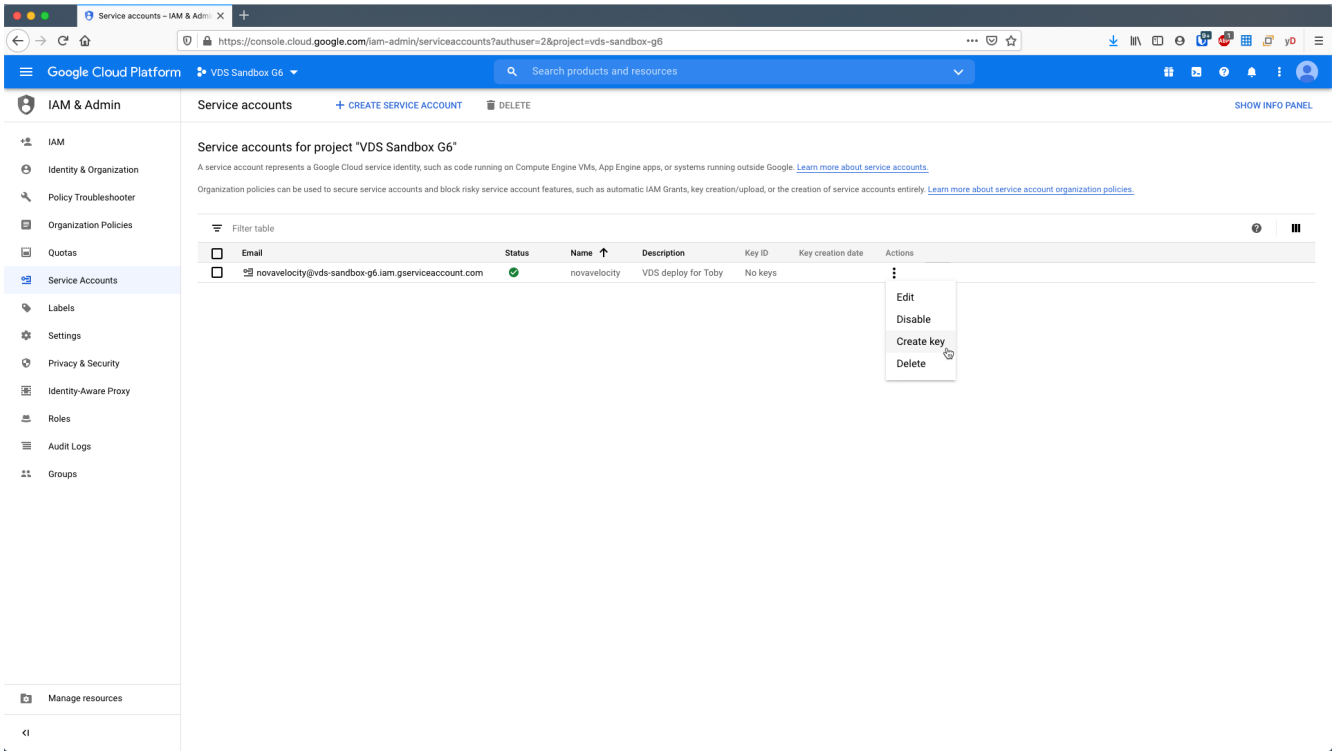
4. Select the *Owner* role for the service account, click *CONTINUE*



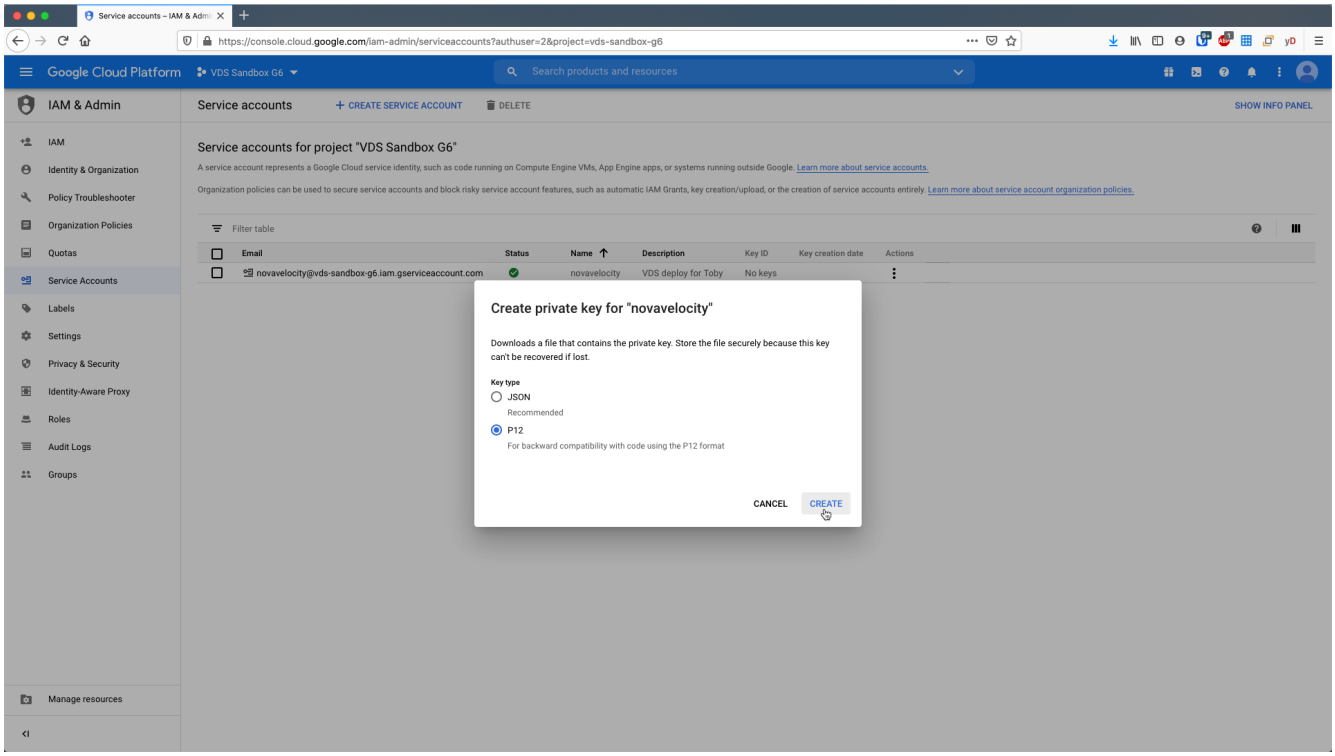
5. No changes are necessary on the next page (*Grant users access to this service account(optional)*), click *DONE*



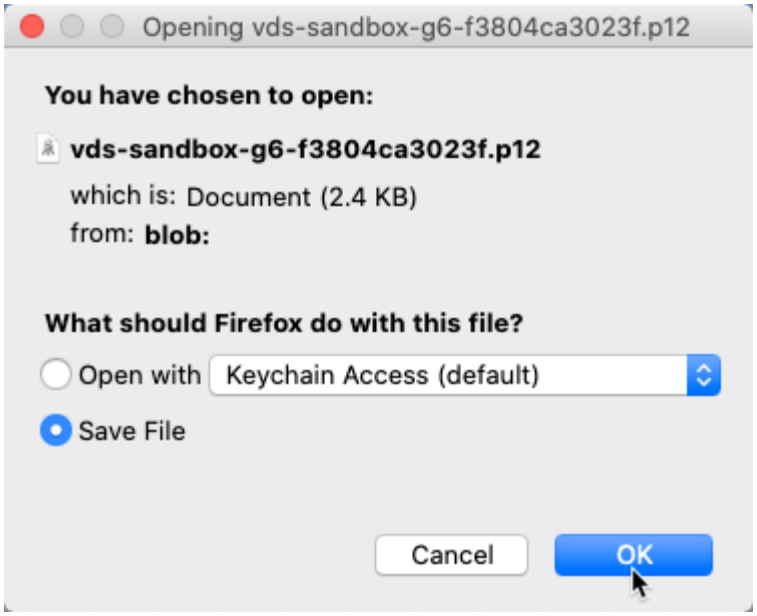
6. From the *Service accounts* page, click the action menu and select *Create key*

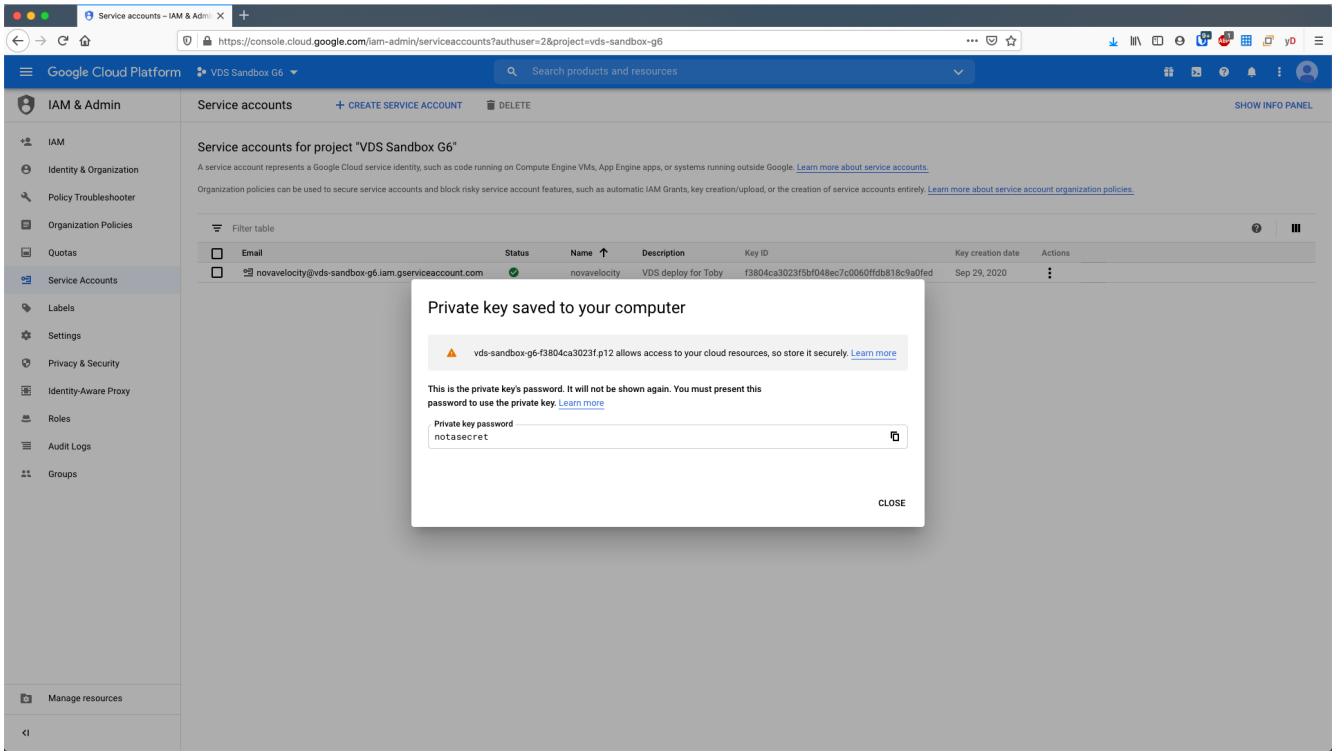


7. Select *P12*, click *CREATE*



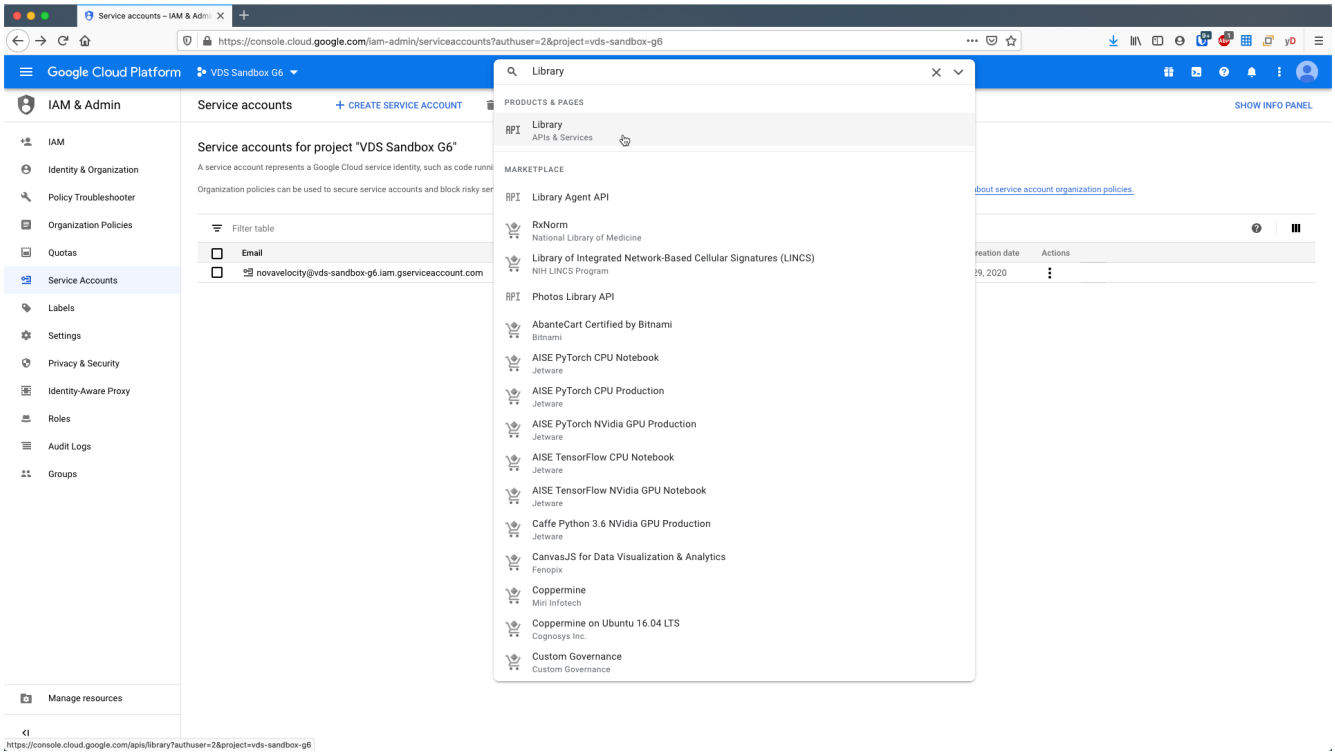
8. Download the .P12 file and save it to your computer. Leaved the *Private key password* unchanged.



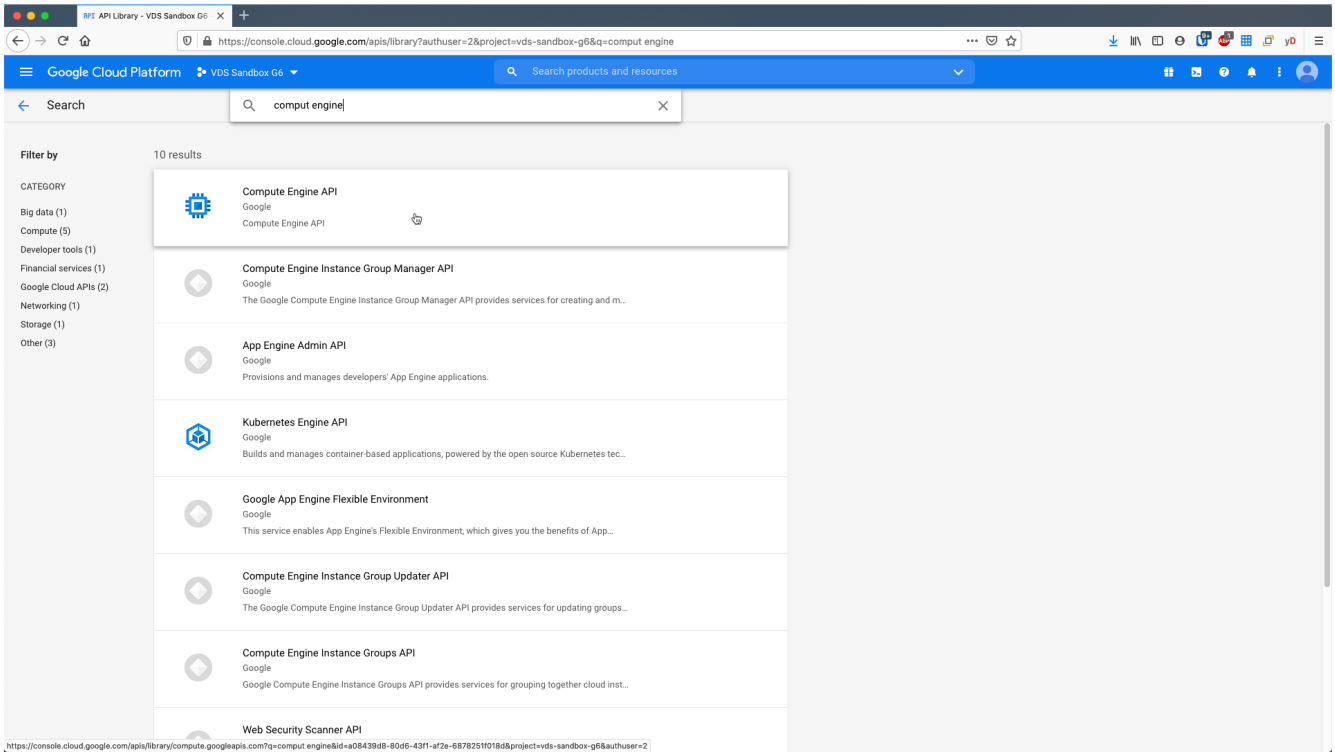


Enable Google compute API

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

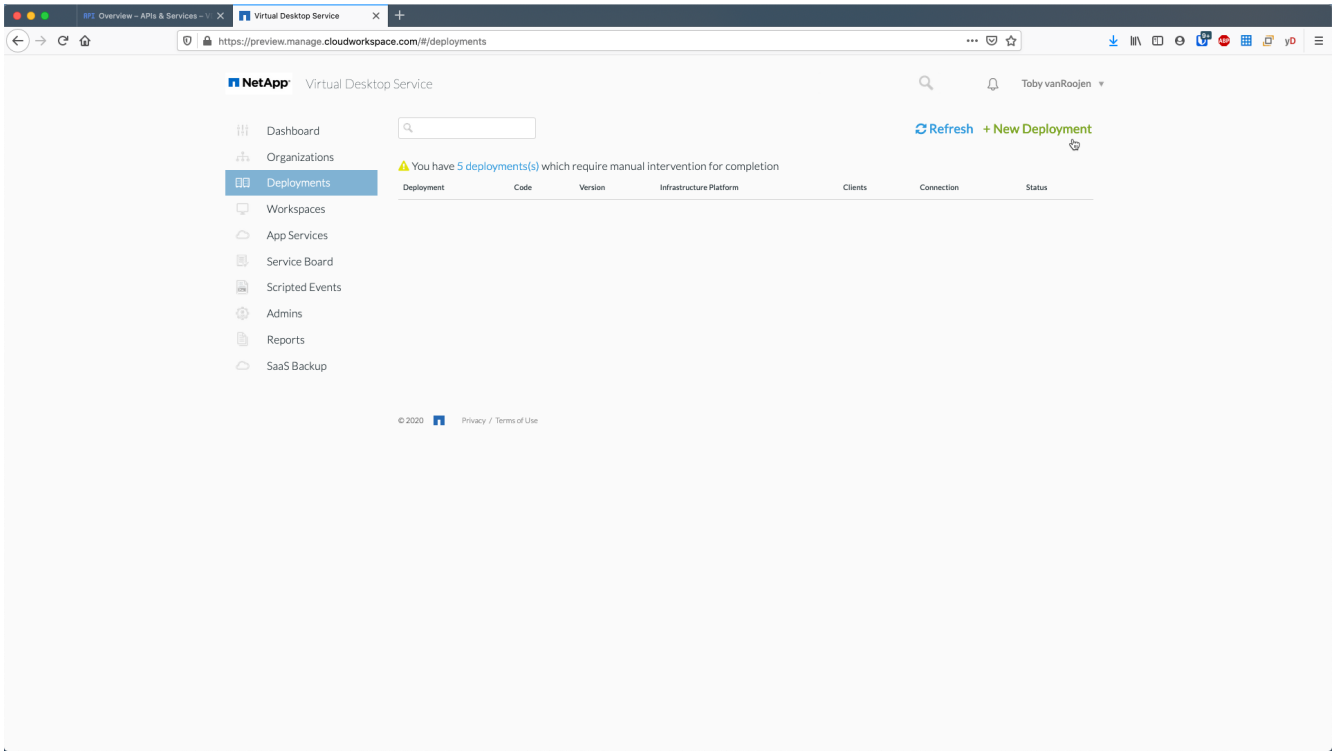


2. In the GCP API Library, navigate to (or search for) *Compute Engine API*, Click *ENABLE*

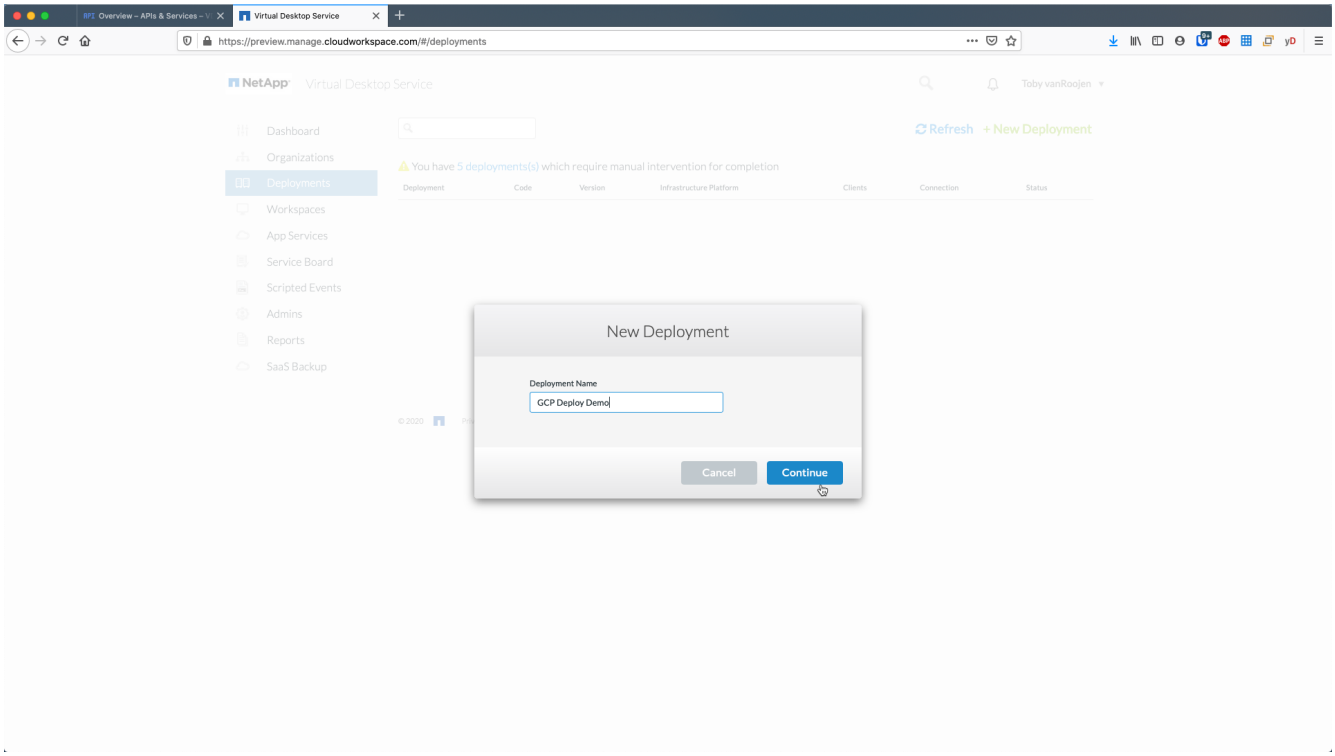


Create new VDS deployment

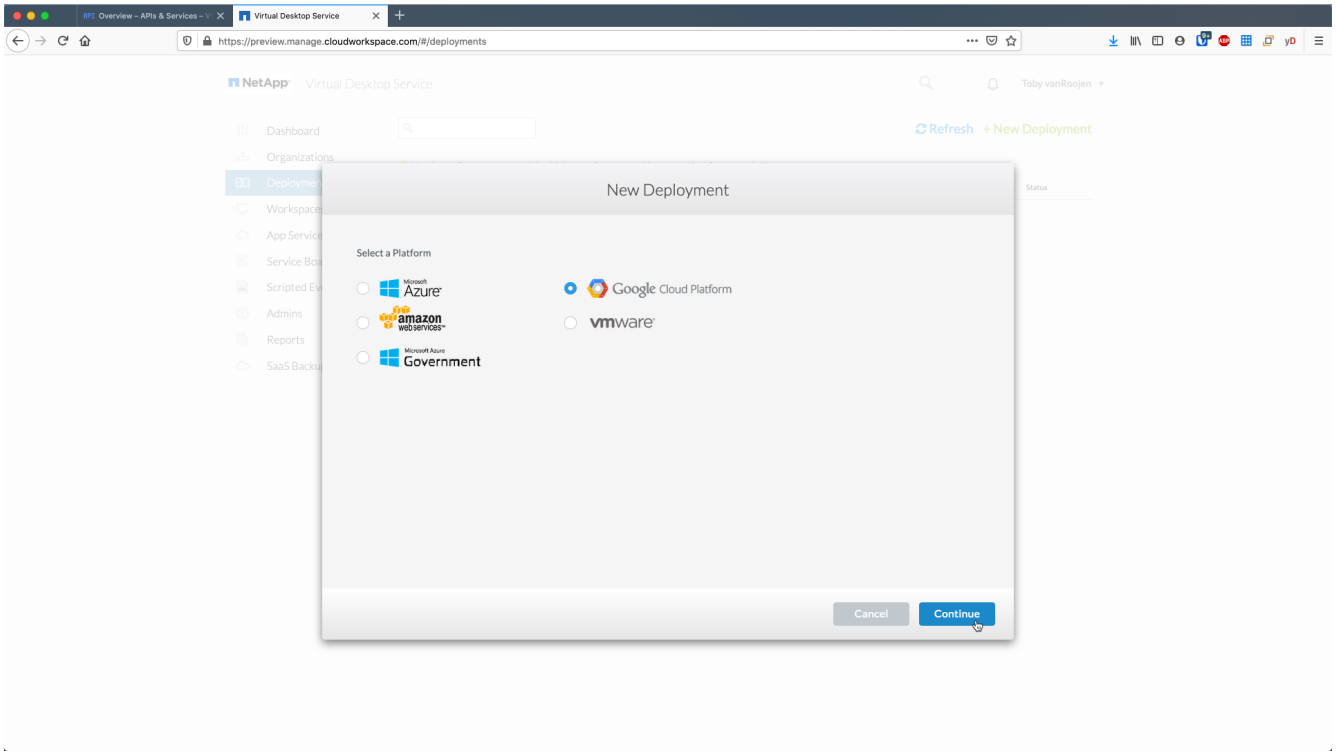
1. In VDS, navigate to *Deployments* and click *+ New Deployment*



2. Enter a name for the deployment



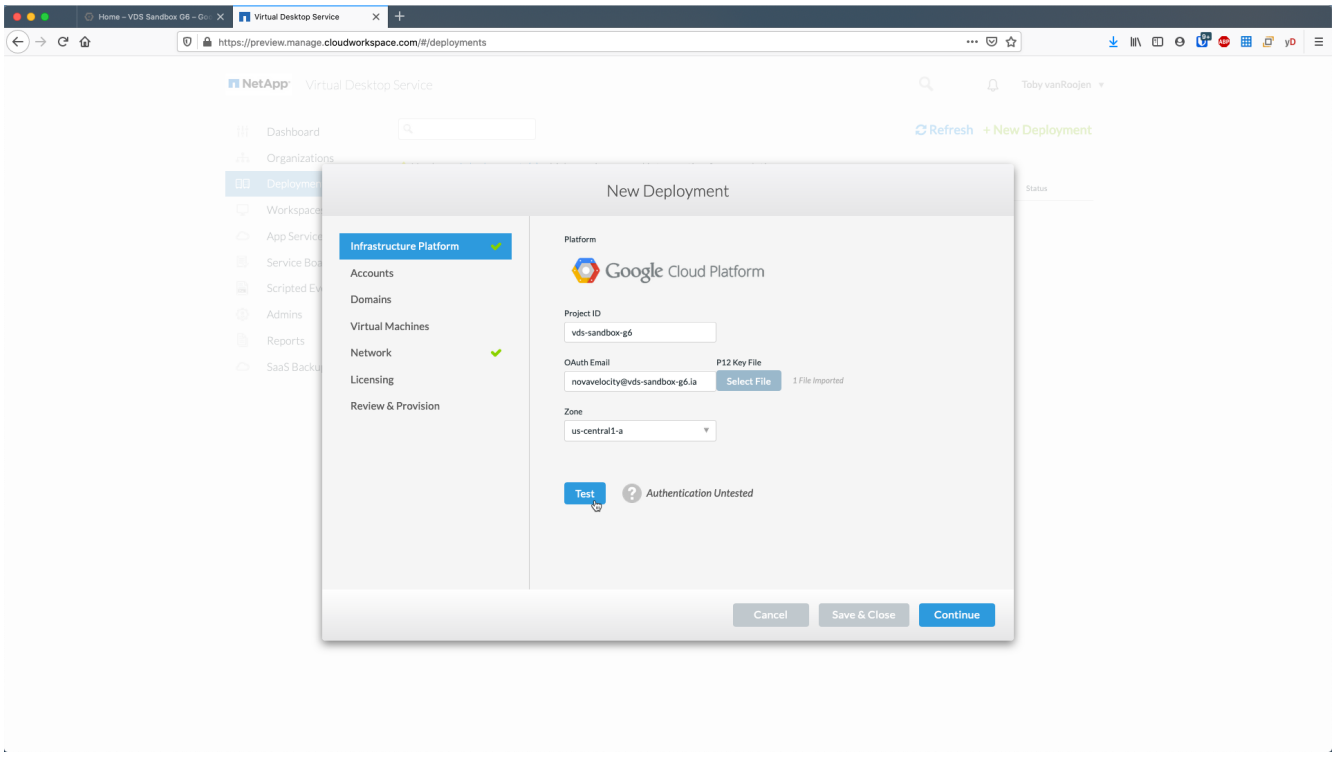
3. Select *Google Cloud Platform*



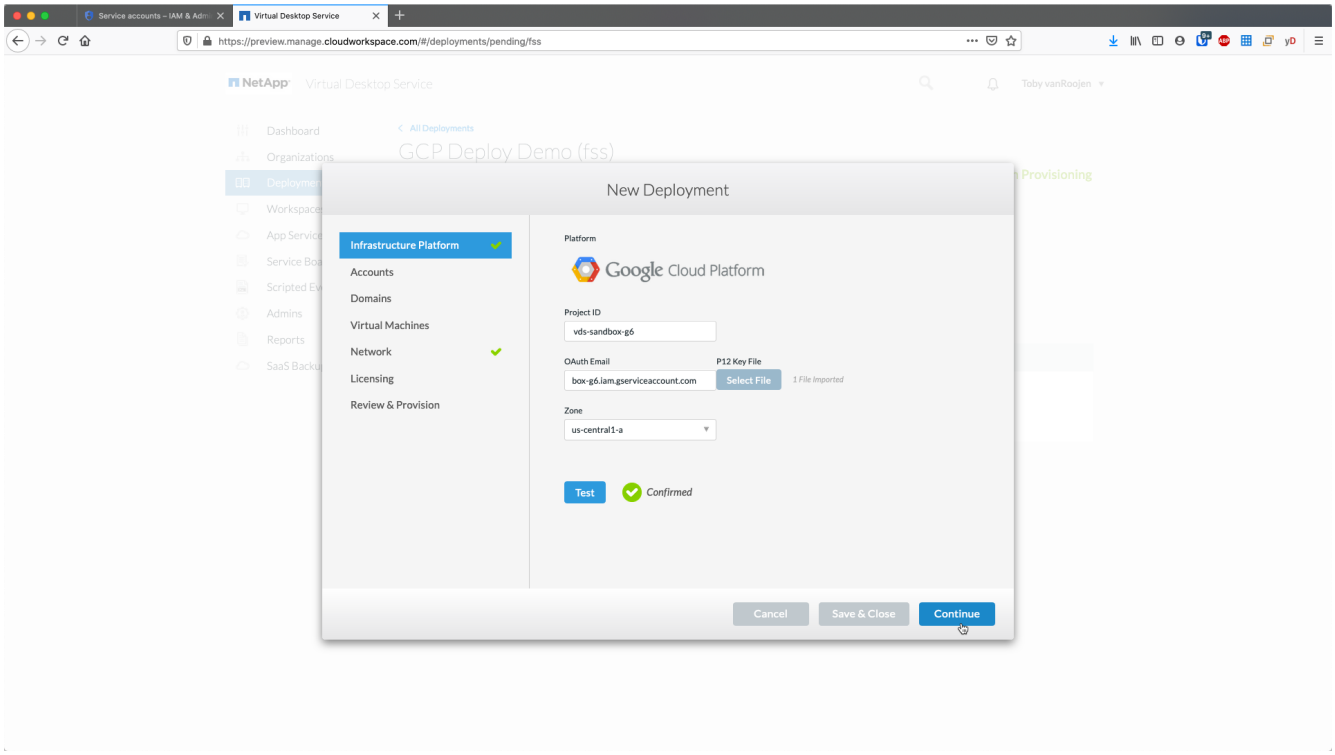
Infrastructure platform

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

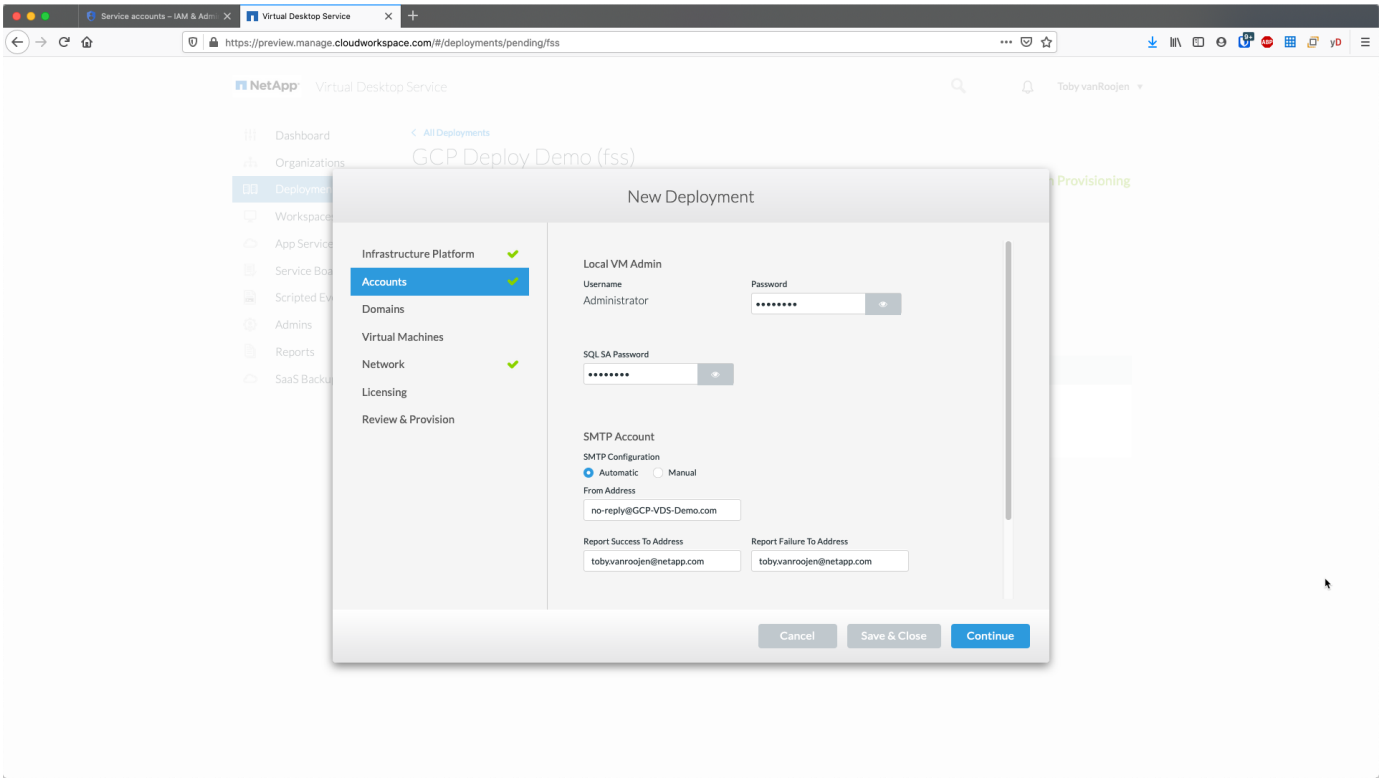
1. Provide a password for the local Administrator account. Document this password for later use.
2. Provide a password for the SQL SA account. Document this password for later use.

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.

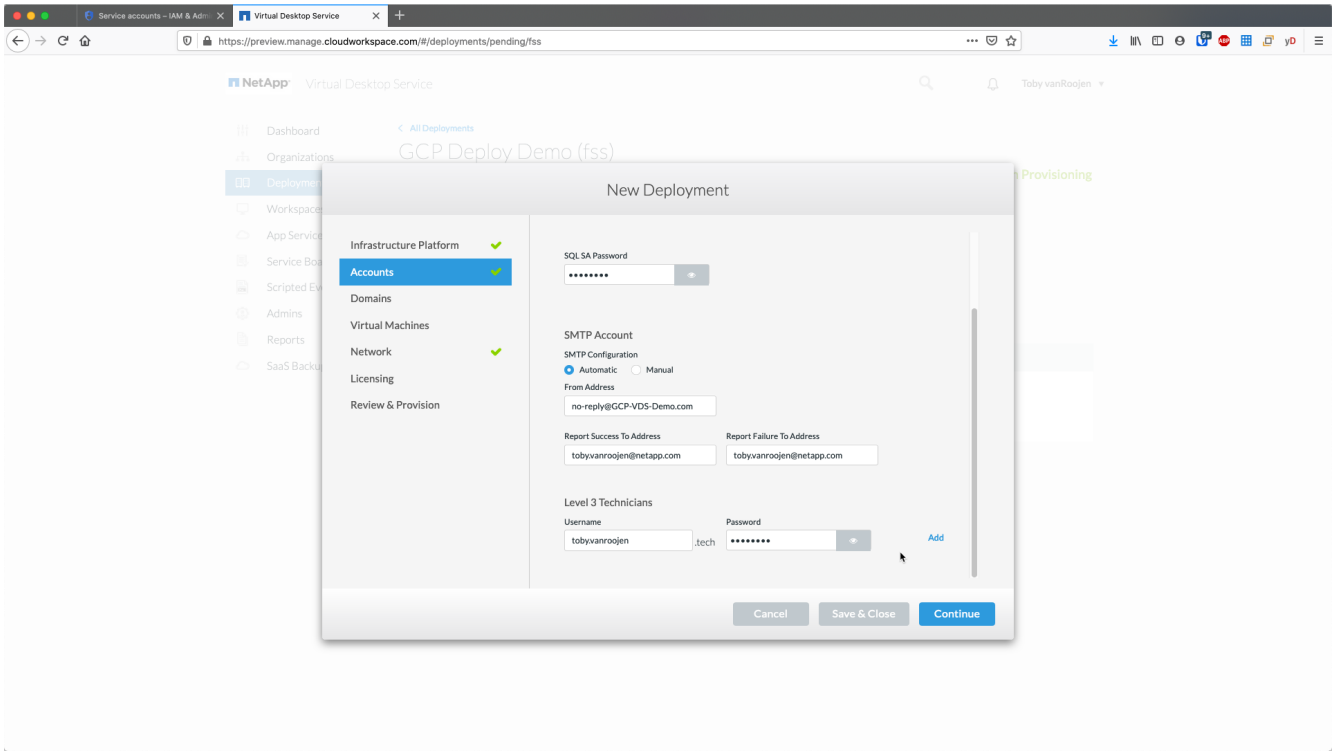


Level 3 technicians

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.



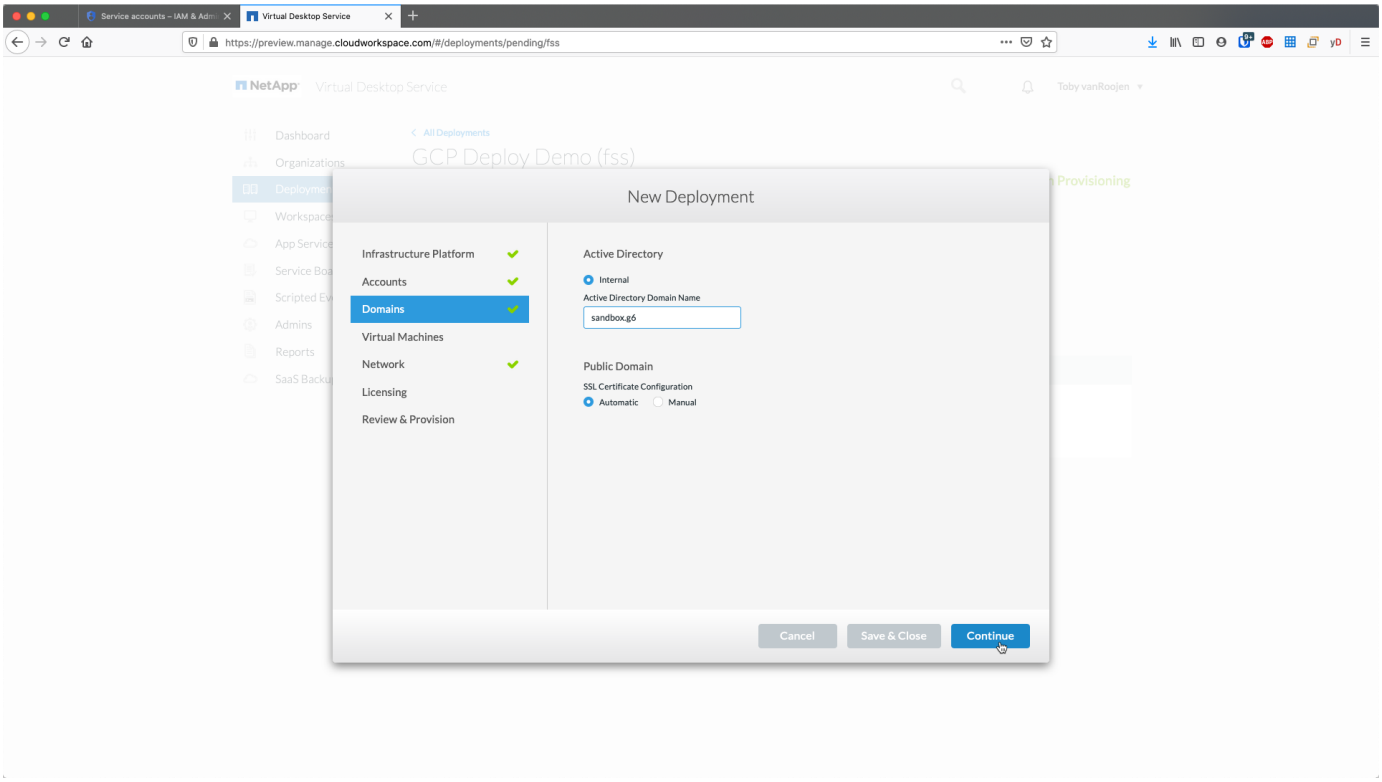
Domains

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 HTML 5 Gateways. These gateways serve up an HTML 5 VDS access client (e.g. https://login.cloudworkspace.com) based on the RemoteSpark technology. Licensing for this component is typically included in the cost of VDS licensing. When two HTM5 CW 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 RDS 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)

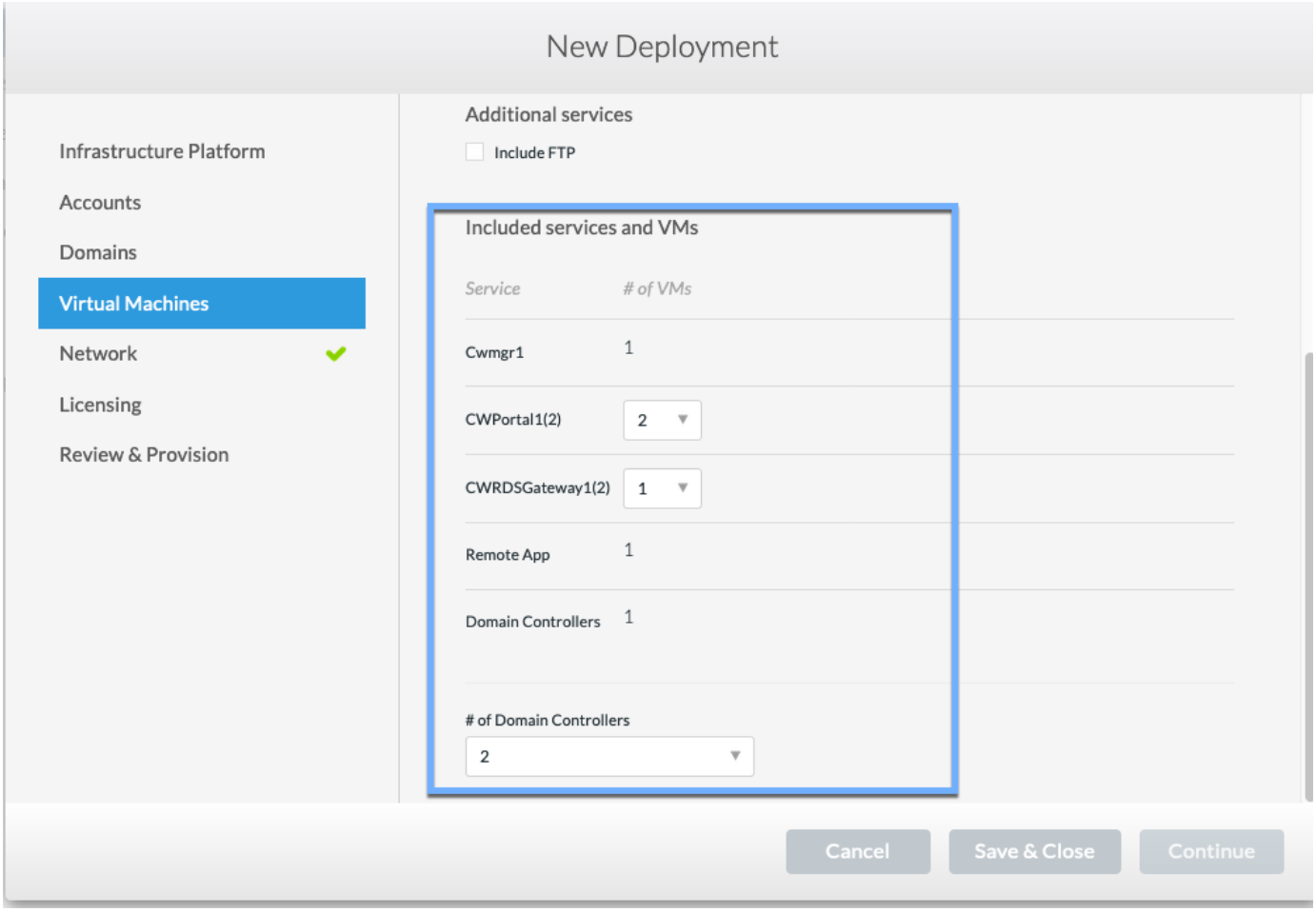
  The first RDS gateway is named *CWRDSGateway1*, the second is *CWRDSGateway2*. One or two can be created at deployment. Additional servers can be added post-deployment for increased capacity (~500 connections per server).

- 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.

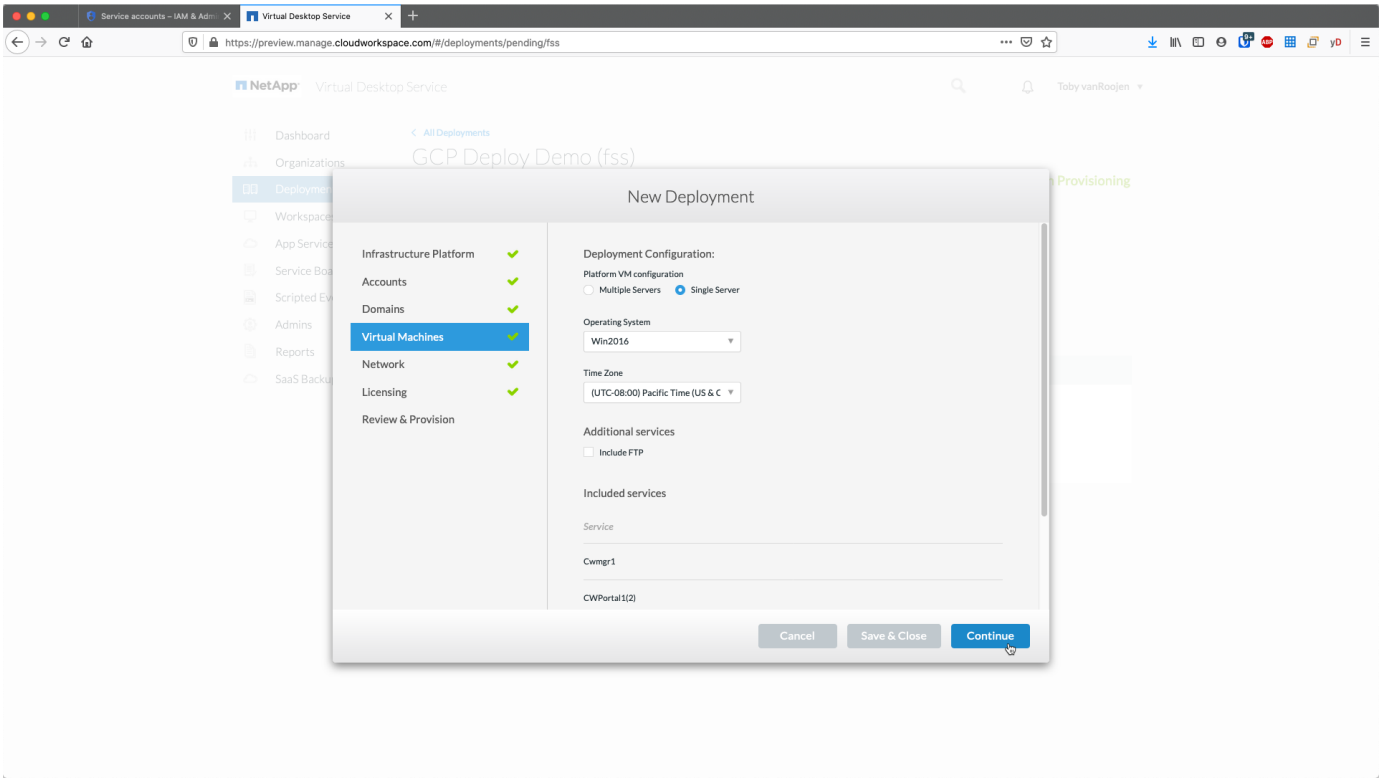
Time zone

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.

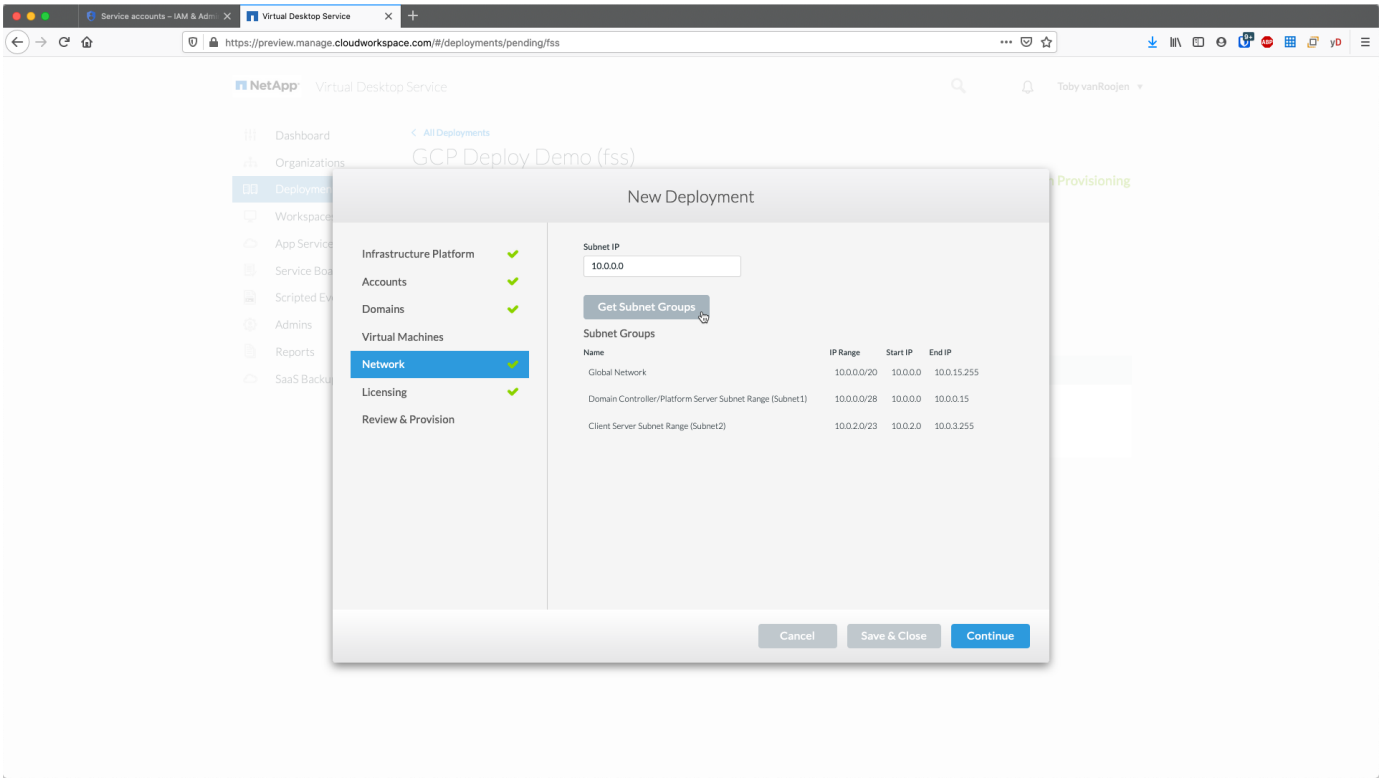
VDS Setup detects and suggests a range that should prove successful. Per best practices, the subnet IP addresses must fall into a private IP address range.

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

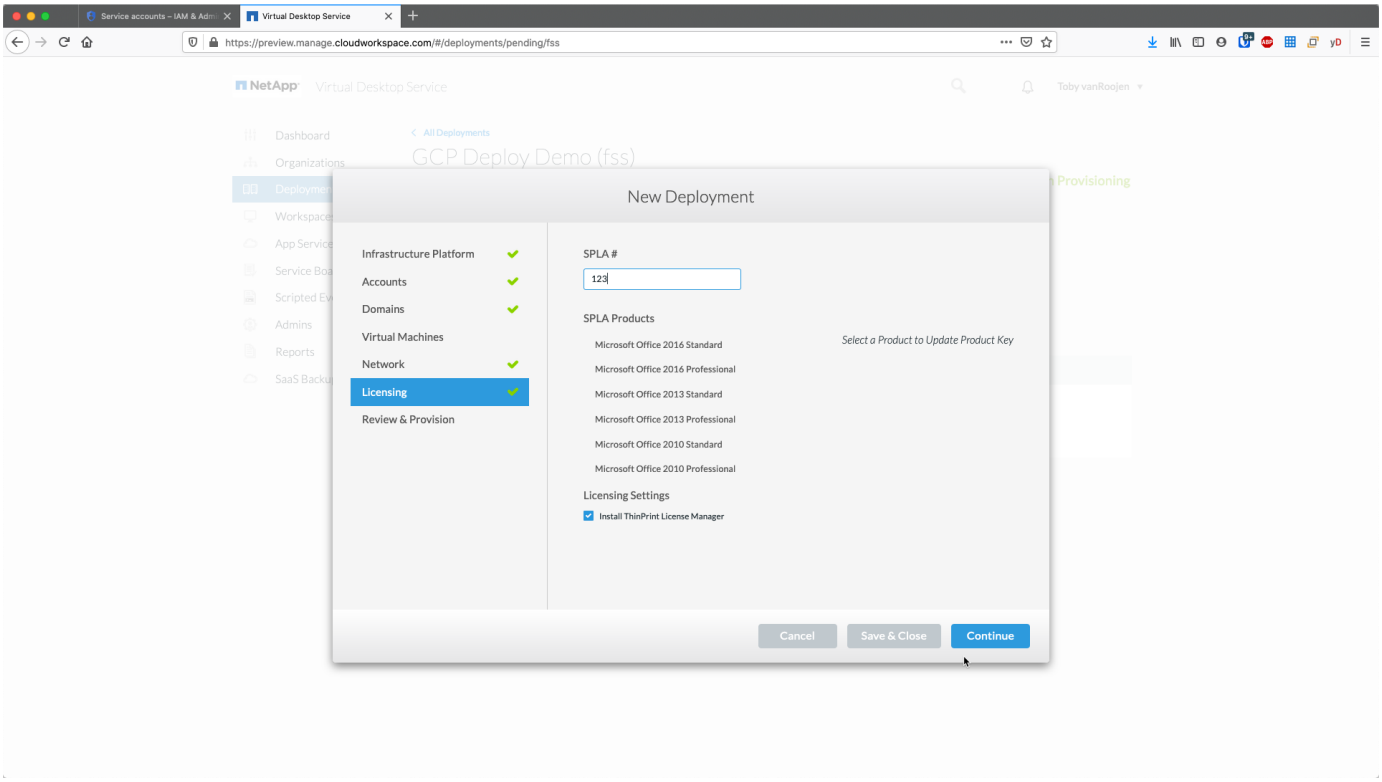
Enter your SPLA number so VDS can configure the RDS licensing service for easier SPLA RDS CAL reporting. A temporary number (such as 12345) can be entered for a POC deployment but after a trial period (~120 days) the RDS sessions will stop connecting.

SPLA products

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

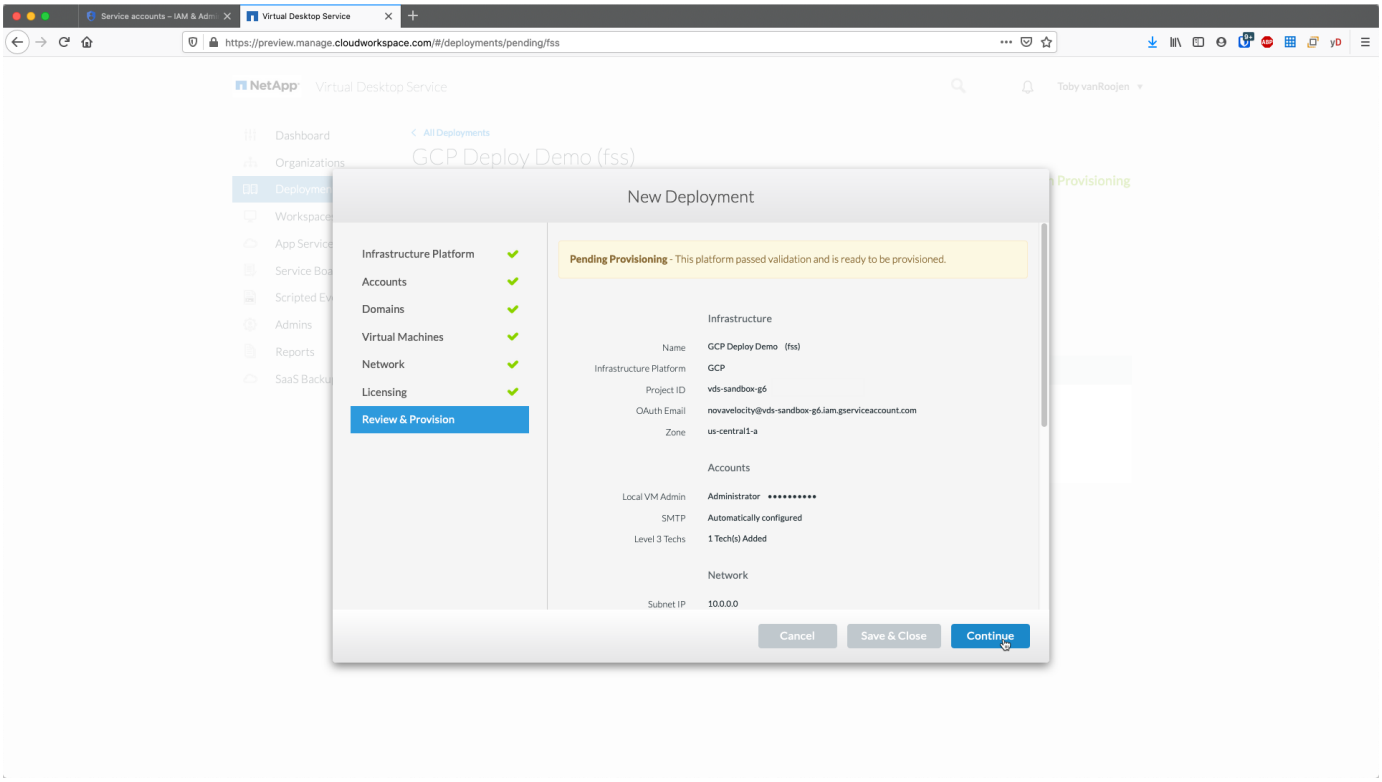
ThinPrint

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.

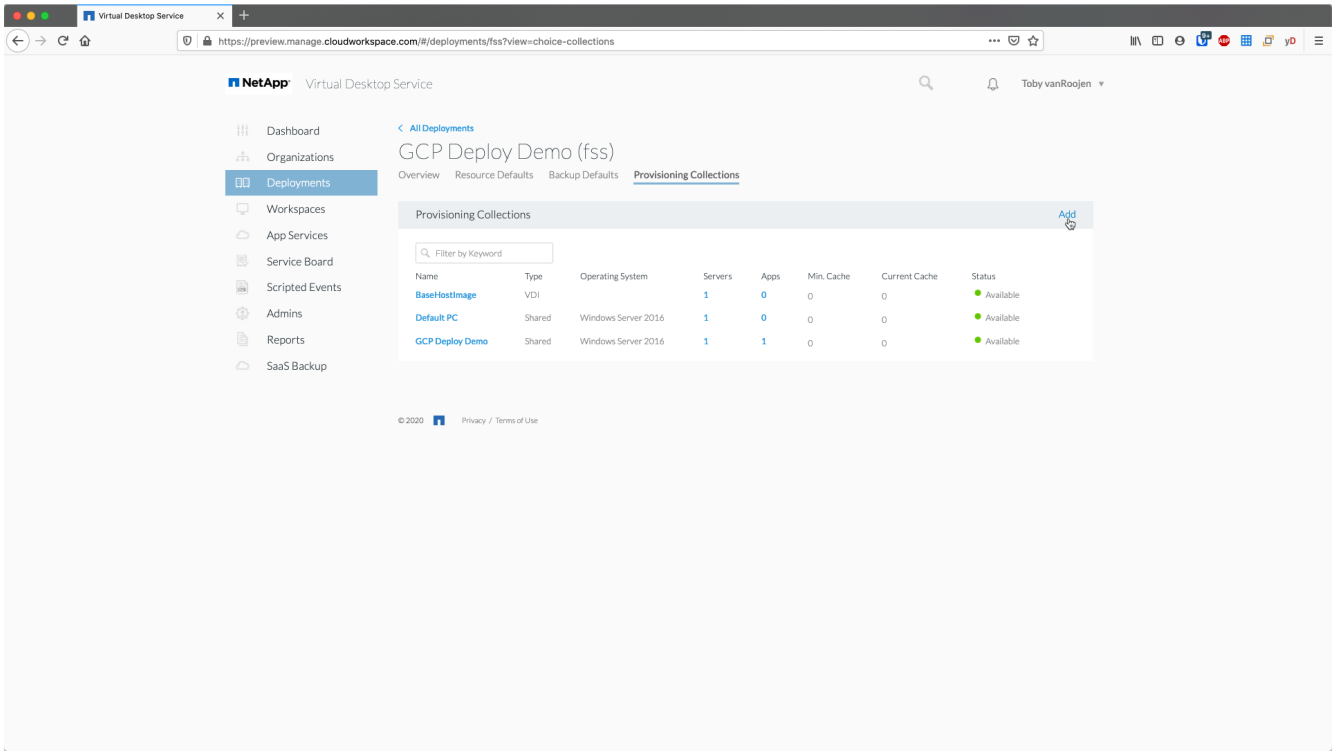
You'll receive multiple emails as the deployment completes. Once complete you'll have an environment ready for your first workspace. A workspace will contain the session hosts and data servers needed to support the end users. Come back to this guide to follow the next steps once the deployment automation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

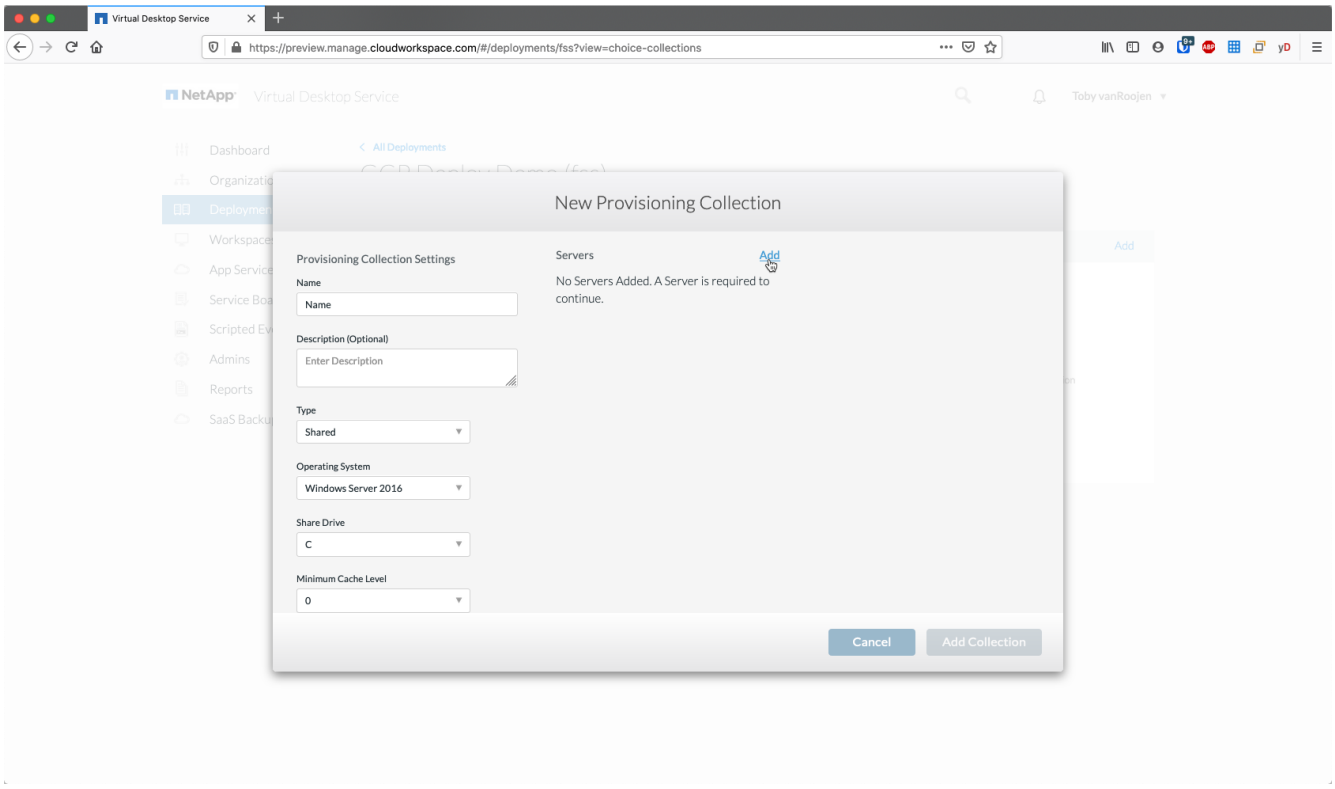
1. Navigate to *Deployments* > *Provisioning Collections*, click *Add*



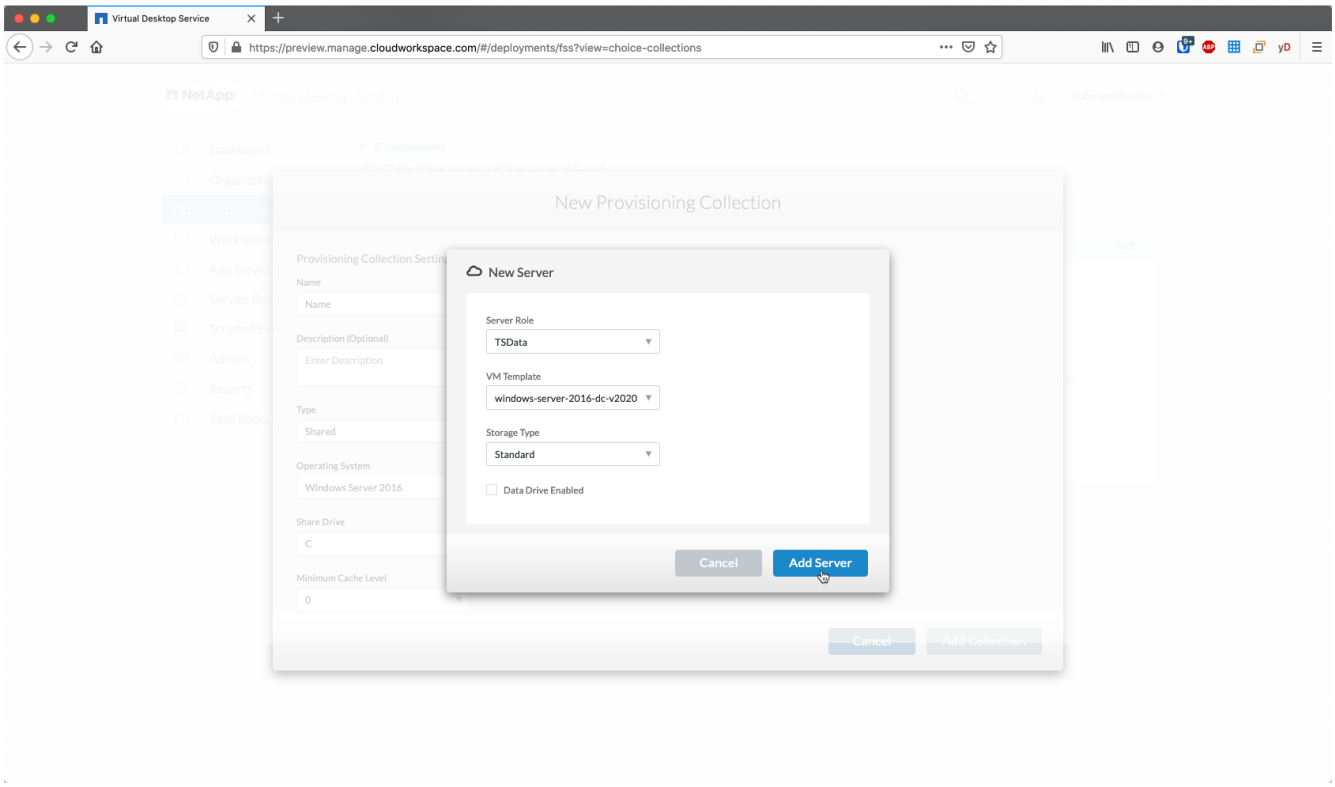
2. Enter a Name and Description. Choose *Type: Shared*.

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.

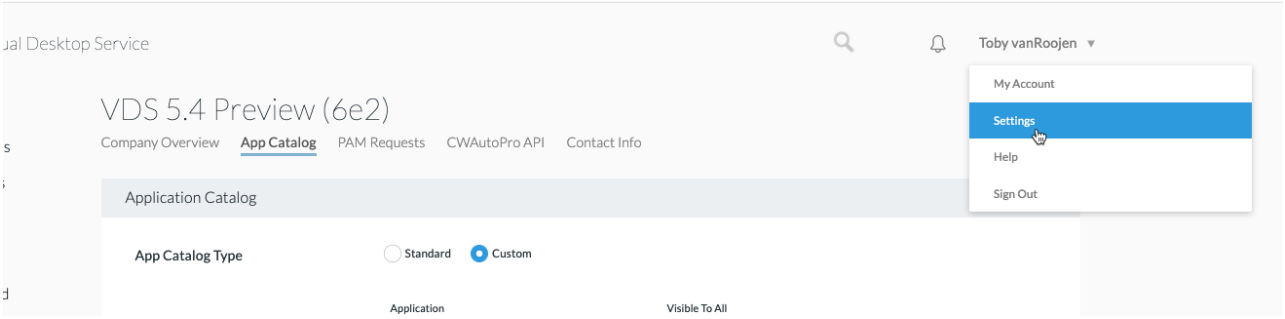
3. Click *Add* to define the type of server image to build.



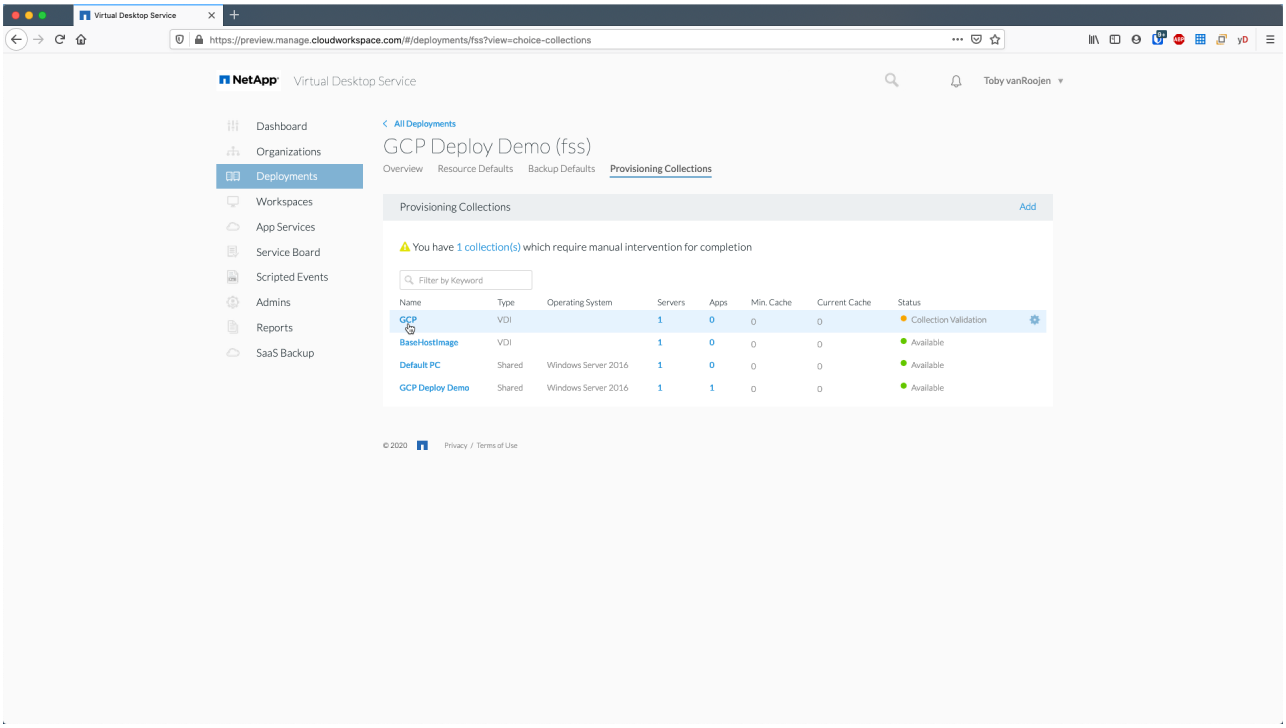
4. Select TSData as the *server role*, the appropriate VM image (Server 2016 in this case) and the desired storage type. Click *Add Server*



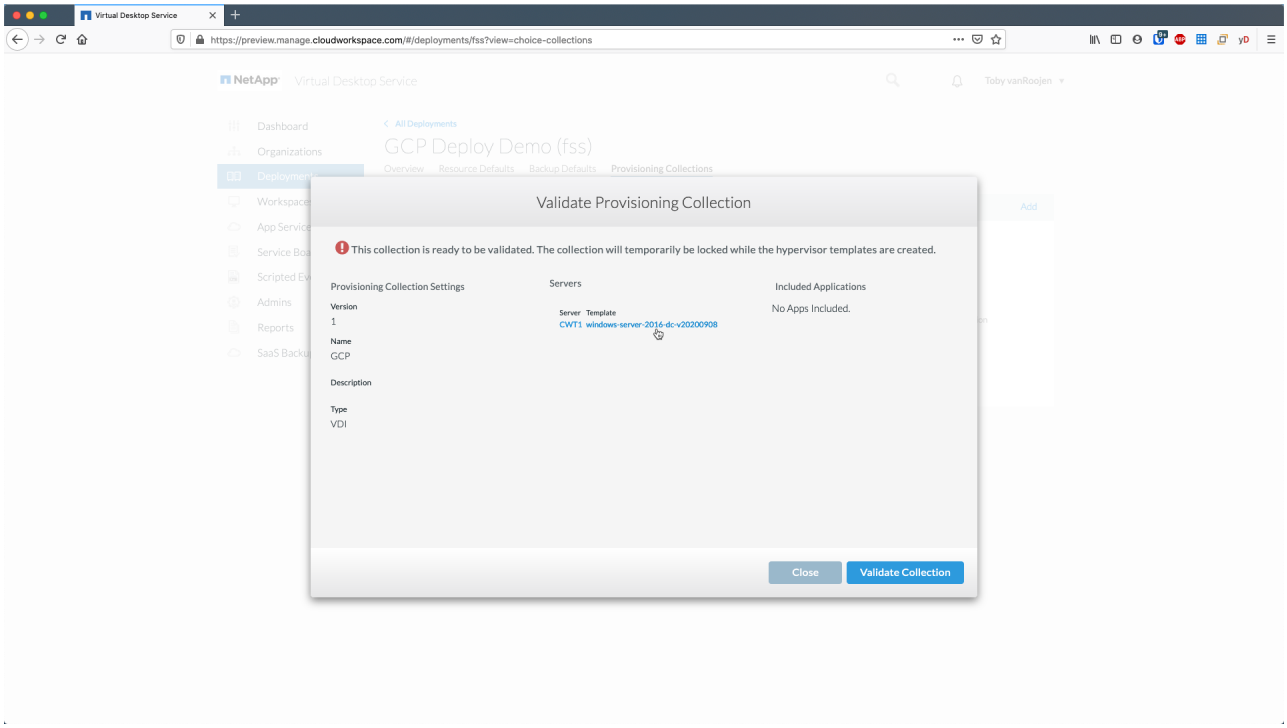
5. Optionally select the applications that will be installed on this image.
    a. The list of applications available is populated from the App Library that can be accessed by clicking the admin name menu in the upper right corner, under the *Settings* > *App Catalog* page.



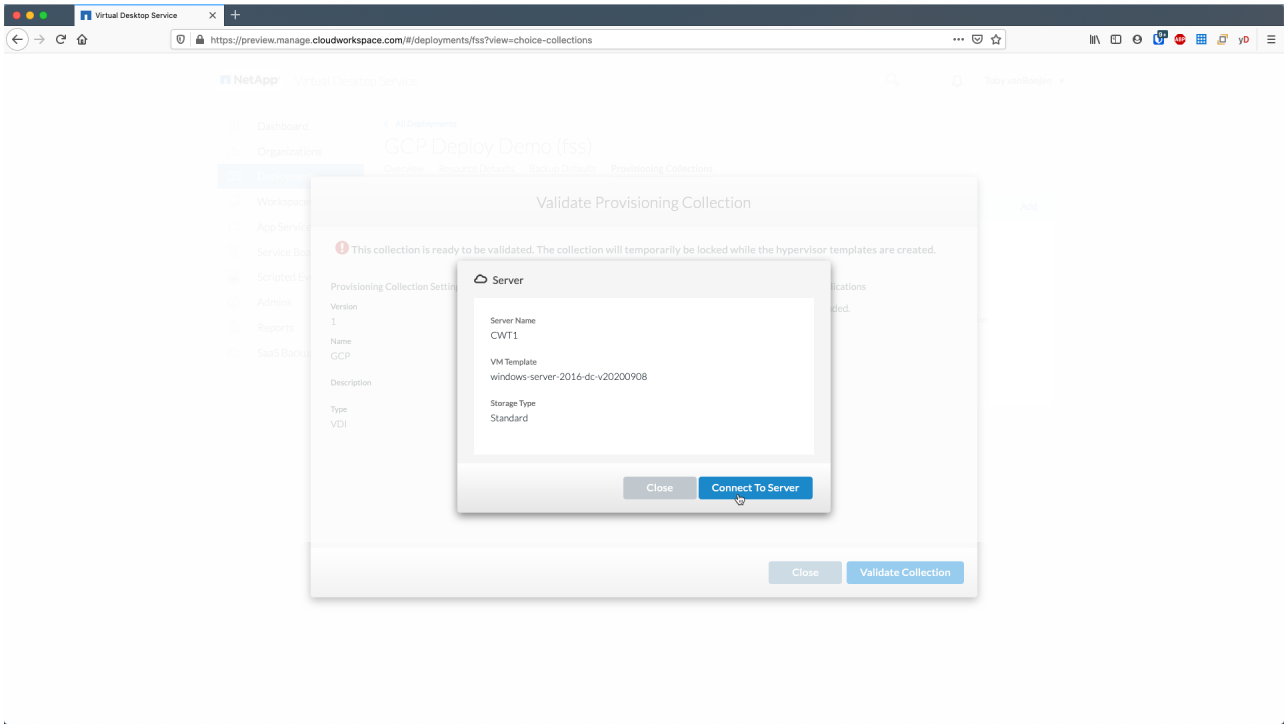
6. Click *Add Collection* and wait for the VM to be built. VDS will build a Vm that can be accessed and customized.
7. Once the VM build has completed, connect to the server and make the desired changes.
   a. Once the status shows *Collection Validation*, click the collection name.

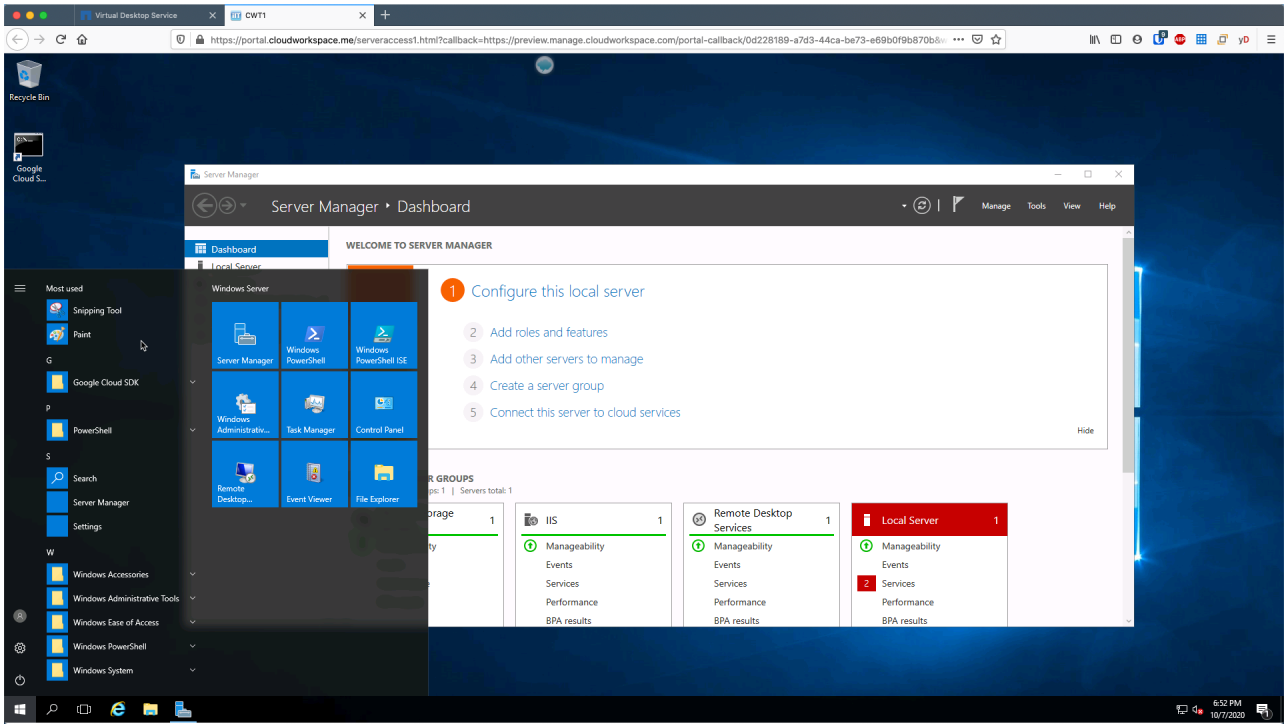


   b. Then, click the *server template name*

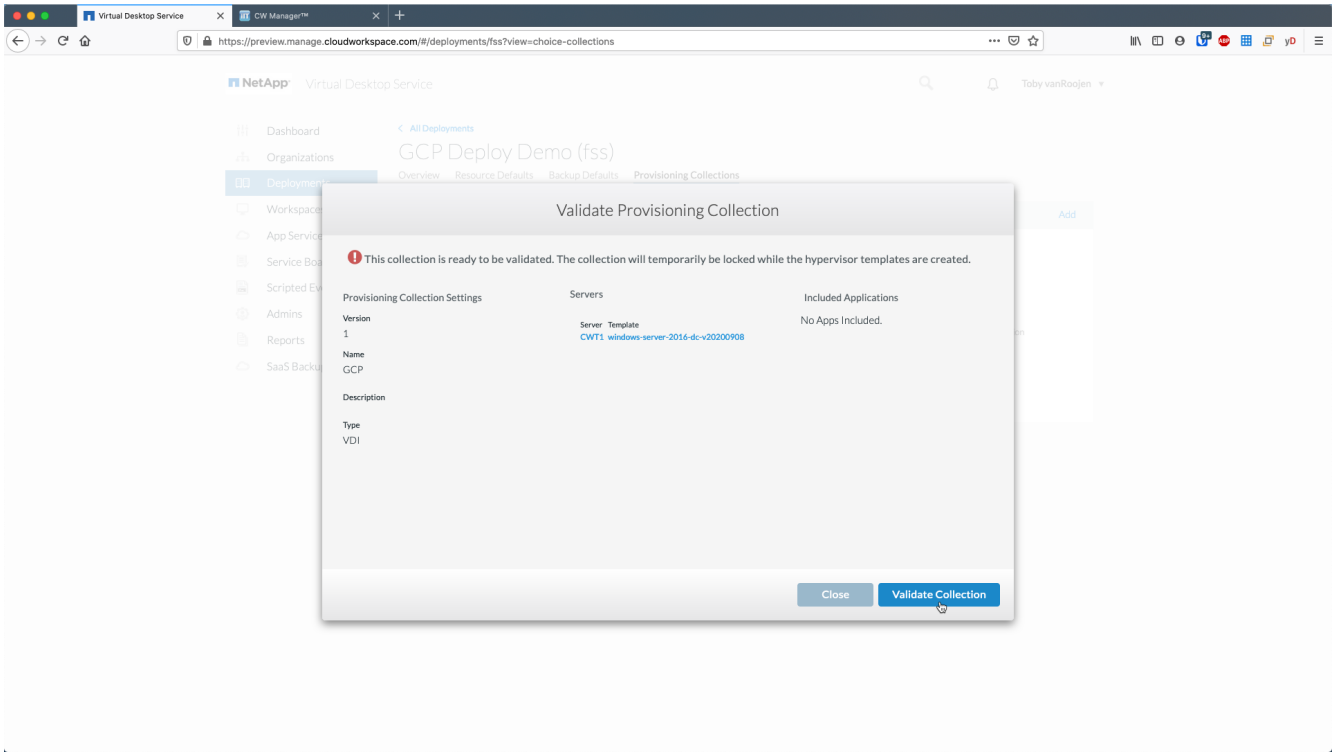


c. Finally, click the *Connect to Server* button to be connected and automatically logged into the VM with local admin credentials.





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 form within VDS deployment wizards.



5

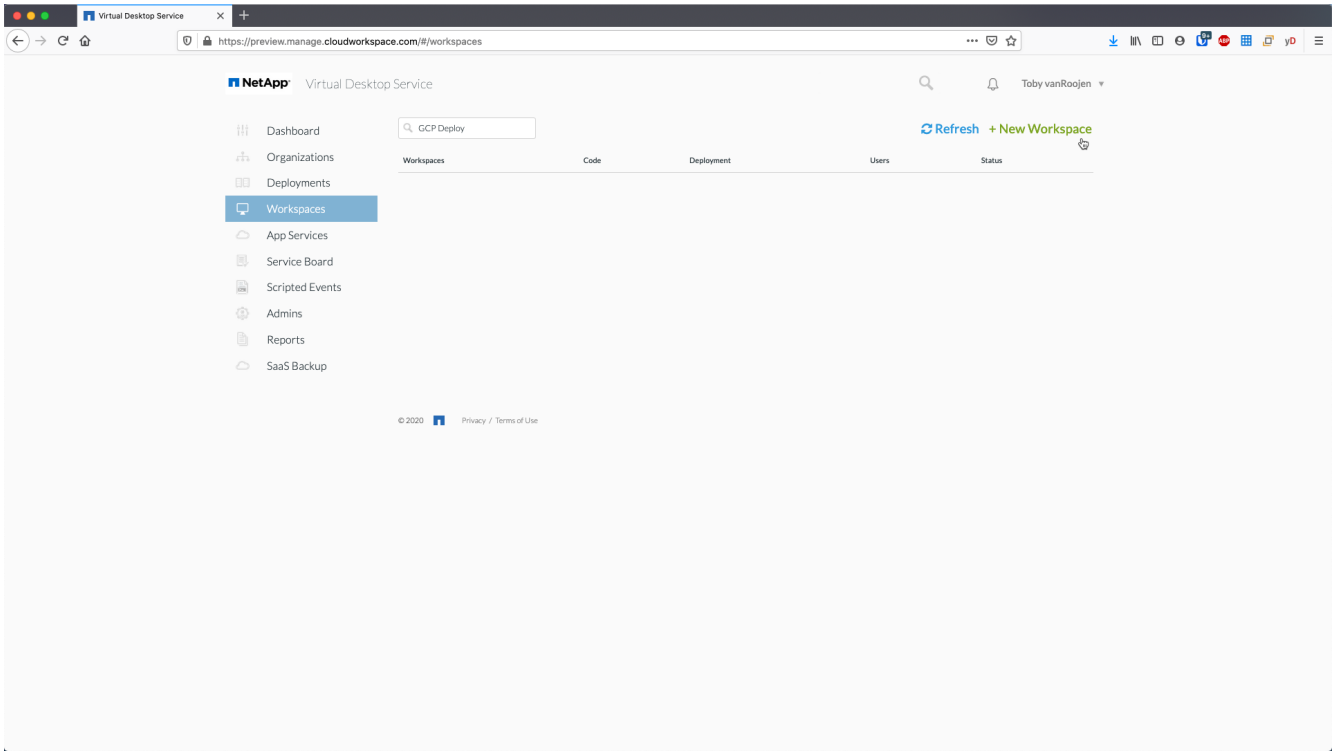
Create new workspace

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).

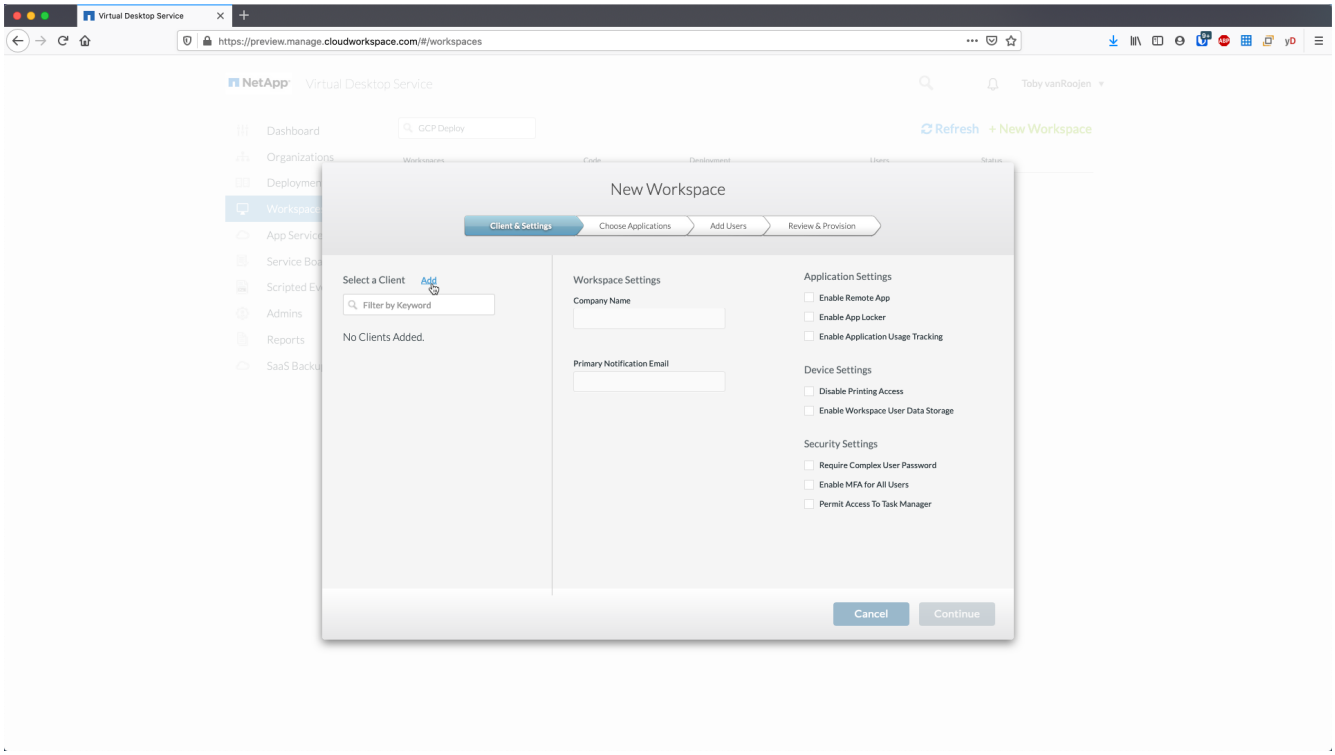
Workspaces define the RDS server collection for a specific group. In this example, we will deploy a single collection to demonstrate the virtual desktop capability. However, the model can be extended to multiple workspaces/ RDS collections to support different groups and different locations within the 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*



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.



a. Enter company details and select the deployment into which this workspace will be deployed.

b. **Data Drive:** Define the drive letter to be used for the company share mapped drive.

c. **User Home Drive:** Define the drive letter to be used for the individual's mapped drive.

d. **Additional Settings**

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

i. *Enable Remote App:* Remote app presents applications as streaming applications instead of (or in addition to) presenting a full remote desktop session.

ii. *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 whitelist.

iii. *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.

iv. *Disable Printer Access:* VDS can block access to local printers.

v. *Permit Access to Task Manager:* VDS can enable/disable end user access to the Task Manager in Windows.

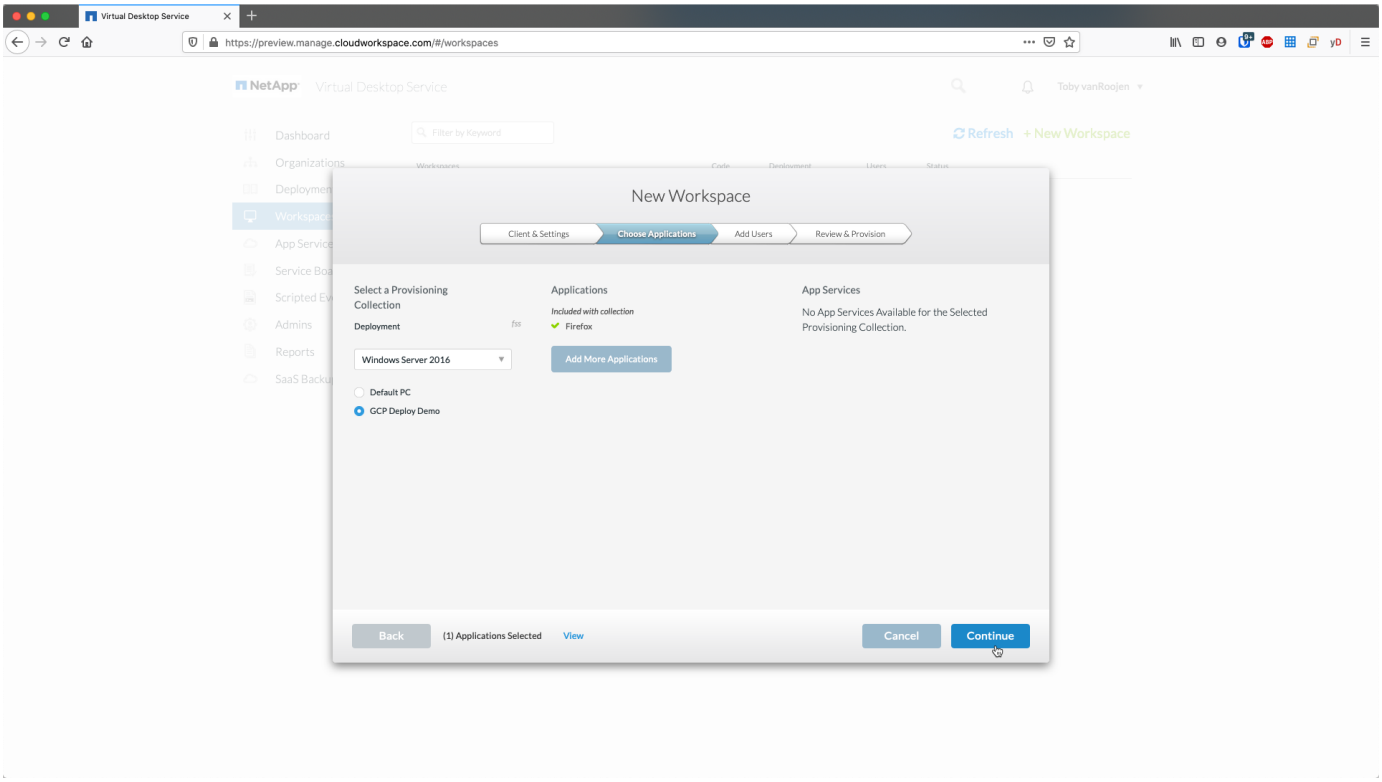
vi. *Require Complex User Password:* Requiring complex passwords enables the native Windows Server complex password rules. It also disables the time-delayed automatic unlock of locked user accounts. Thus, when enabled, admin intervention is required when end users lock their accounts with multiple failed password attempts.

vii. *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

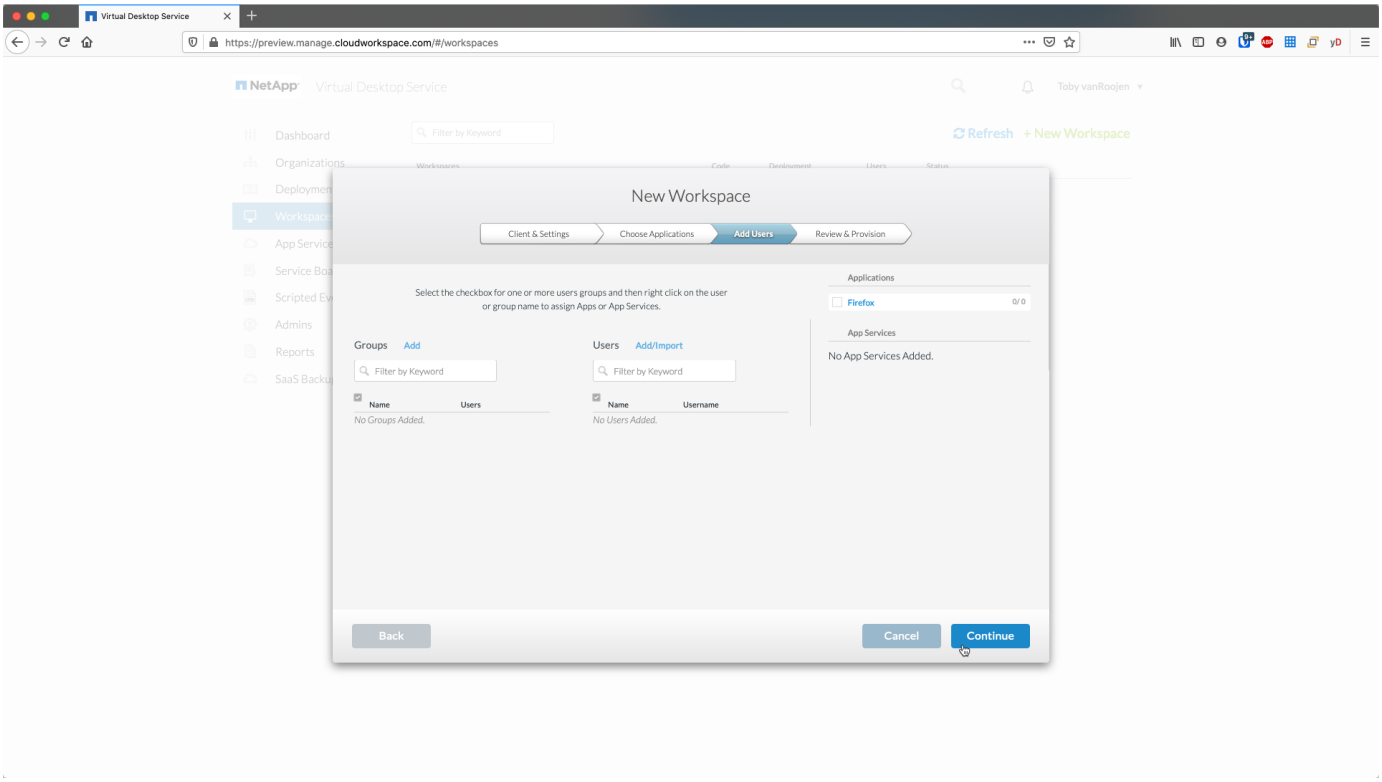
Select the Windows OS version and Provisioning collection created earlier in this guide.

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



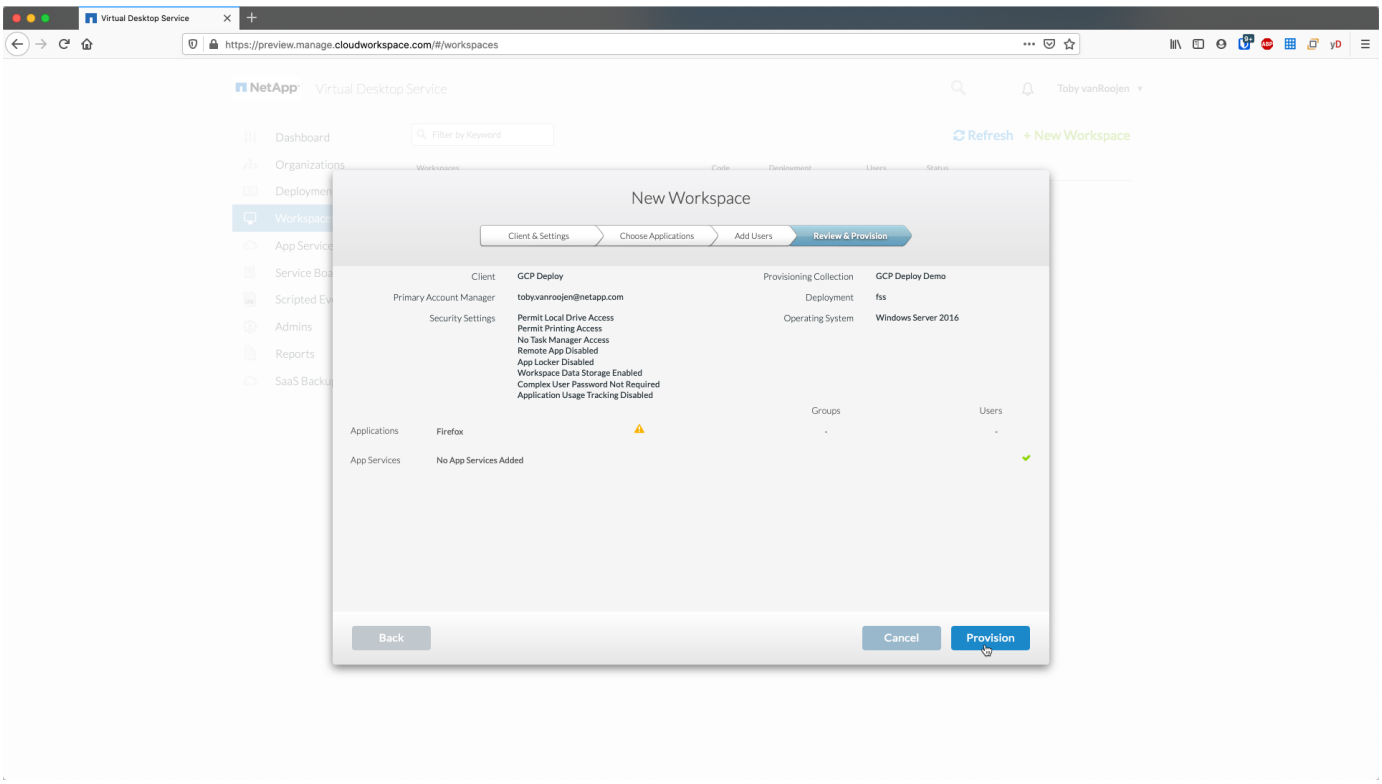
Add Users

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 whitelisting requirements
    - api.cloudworkspace.com
    - vdsclient.app
    - api.vdsclient.app
    - bin.vdsclient.app
    - vdsclient.blob.core.windows.net
  - Enhanced features:
    - VDS Wake on Demand
    - ThinPrint client and lice nsing
    - 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 WVD 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 execute 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 whitelisted for bi-directional access on port 443:

api.cloudworkspace.com
autoprodb.database.windows.net
vdctoolsapi.trafficmanager.net
cjbootstrap3.cjautomate.net

If your access control device can only white list by IP address, the following list of IP addresses should be whitelisted. 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 hsots, deployed by VDS, support the following x64 operating system images:

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