



Google

Virtual Desktop Service

NetApp
December 10, 2020

This PDF was generated from https://docs.netapp.com/us-en/virtual-desktop-service/Deploying.GCP.RDS.deploying_rds_in_gcp.html on December 10, 2020. Always check docs.netapp.com for the latest.



Table of Contents

Google	1
RDS Deployment Guide for Google Cloud (GCP)	1
Google Compute Platform (GCP) and VDS Prerequisites	28

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:

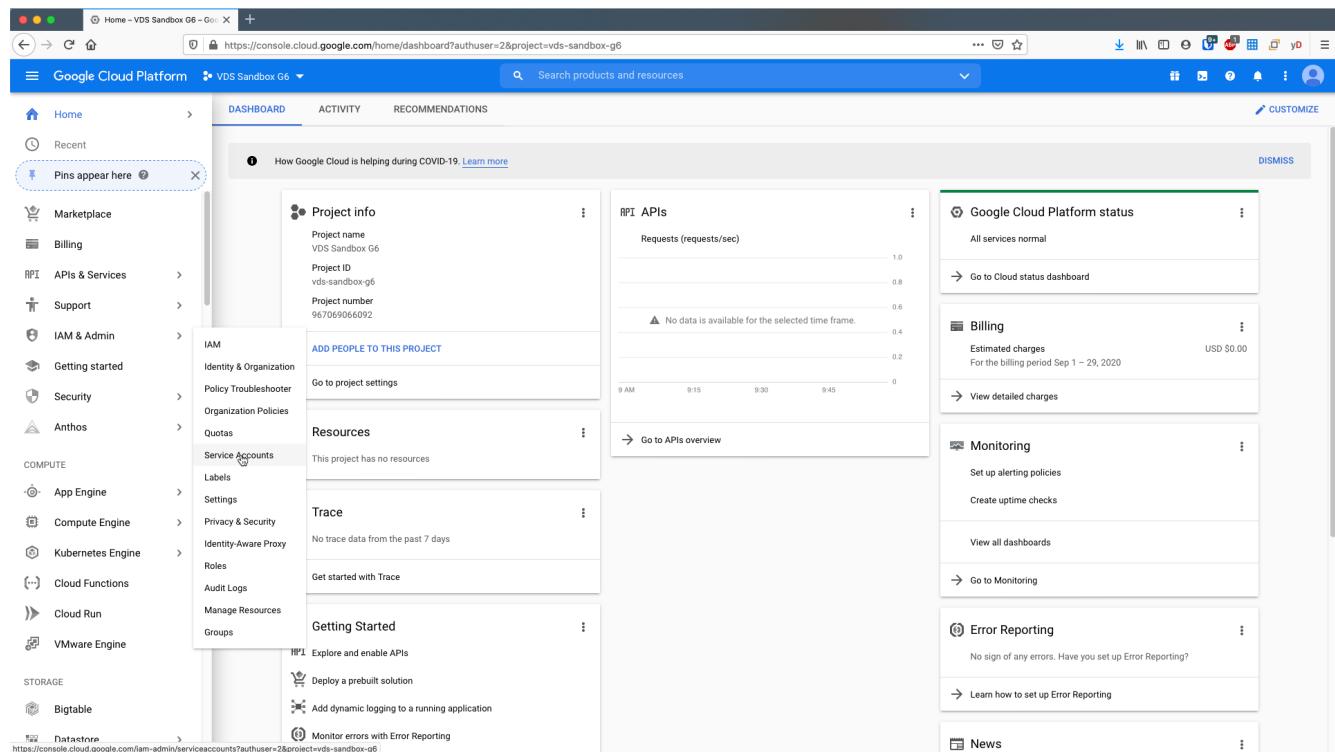
- RDS gateway server(s)
- Web client access server(s)
- Domain controller server(s)
- RDS licensing service
- ThinPrint licensing service
- Filezilla FTPS server service

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

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

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

Create service account

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

Service account details

Service account name
novelocity

Display name for this service account

Service account ID
novelocity @vds-sandbox-g6.iam.gserviceaccount.com

Service account description
VDS deploy for Toby

Describe what this service account will do

CREATE CANCEL

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

The screenshot shows the 'Create service account - IAM' page in the Google Cloud Platform. The left sidebar is titled 'IAM & Admin' and includes options like IAM, Identity & Organization, Policy Troubleshooter, Organization Policies, Quotas, Service Accounts (which is selected), Labels, Settings, Privacy & Security, Identity-Aware Proxy, Roles, Audit Logs, and Groups. The main area has three steps: 'Service account details' (checked), 'Grant this service account access to project (optional)', and 'Grant users access to this service account (optional)'. A sub-modal window titled 'Service account permissions (optional)' is open, showing a list of roles under 'Select a role'. The 'Owner' role is selected and highlighted in grey. Other roles listed include BigQuery Data Owner, Cloud Datastore Owner, Chat Bots Owner, and a 'Condition' section. At the bottom of the modal is a 'MANAGE ROLES' link.

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

The screenshot shows the 'Grant users access to this service account (optional)' page. The left sidebar is identical to the previous screen. The main area has three steps: 'Service account details' (checked), 'Grant this service account access to project (optional)' (checked), and 'Grant users access to this service account (optional)'. Under 'Grant users access to this service account (optional)', there are two sections: 'Service account users role' (selected) and 'Service account admins role'. On the right side, there is an 'INFO PANEL' titled 'Permissions' with a 'Show inherited permissions' toggle switch (which is turned on). Below it is a tree view of roles and members, showing 'Owner (2)' under 'Role / Member ↑ Inheritance'. At the bottom of the main area are 'DONE' and 'CANCEL' buttons, with 'DONE' being highlighted by a mouse cursor.

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

Service accounts for project "VDS Sandbox G6"

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

7. Select P12, click CREATE

Create private key for "novelocity"

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

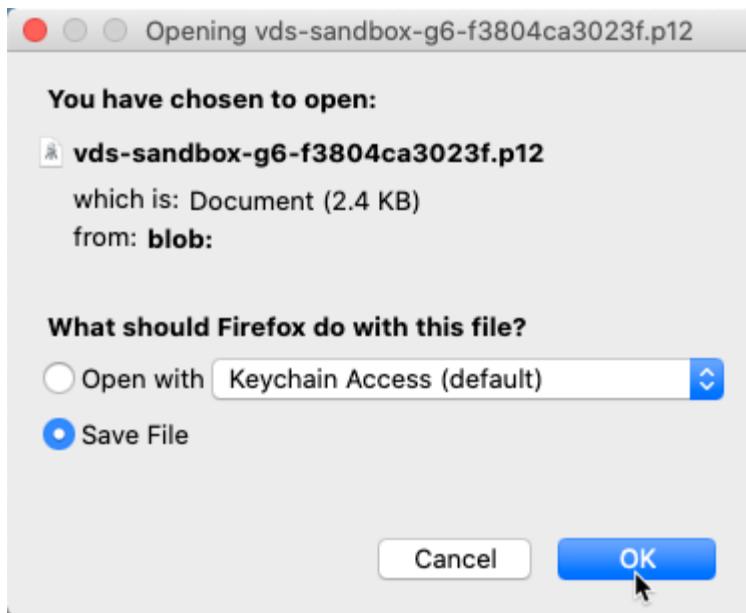
Key type

JSON
Recommended

P12
For backward compatibility with code using the P12 format

CANCEL CREATE

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



A screenshot of the Google Cloud Platform IAM & Admin service accounts page. The URL is https://console.cloud.google.com/iam-admin/serviceaccounts?authuser=2&project=vds-sandbox-g6. The left sidebar shows "Service Accounts" is selected. The main table lists a single service account: "novavelocity@vds-sandbox-g6.iam.gserviceaccount.com" with status "Enabled", name "novavelocity", description "VDS deploy for Toby", key ID "f3804ca3023f5bf048ec7c006ffdb818c9a0fed", and creation date "Sep 29, 2020". A modal dialog box is overlaid on the page, titled "Private key saved to your computer". It contains a warning message: "vds-sandbox-g6-f3804ca3023f.p12 allows access to your cloud resources, so store it securely." Below this is a note: "This is the private key's password. It will not be shown again. You must present this password to use the private key." A text input field contains the password "notasecret". At the bottom right of the modal is a "CLOSE" button.

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

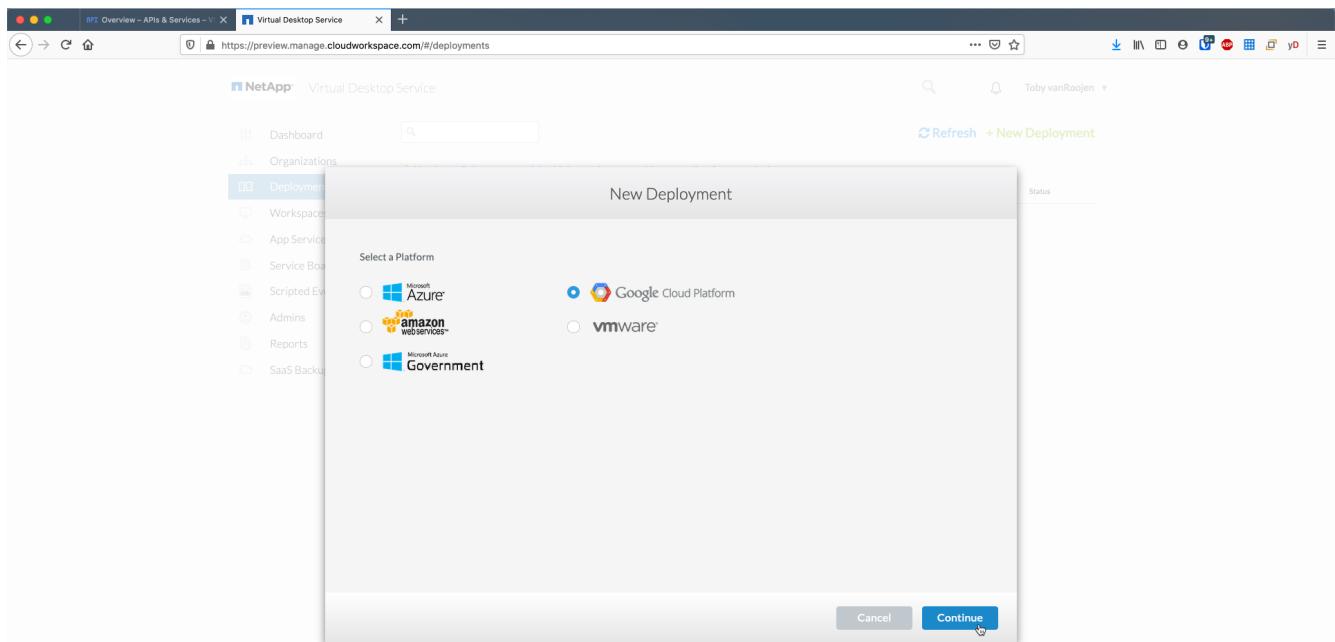
1. In VDS, navigate to *Deployments* and click *+ New Deployment*

The screenshot shows the NetApp Virtual Desktop Service interface. The left sidebar has a 'Deployments' section selected. The main area displays a message: '⚠ You have 5 deployment(s) which require manual intervention for completion'. Below this are tabs for Deployment, Code, Version, Infrastructure Platform, Clients, Connection, and Status. A search bar and a refresh button are at the top right. The bottom left shows a copyright notice for 2020.

2. Enter a name for the deployment

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

3. Select *Google Cloud Platform*

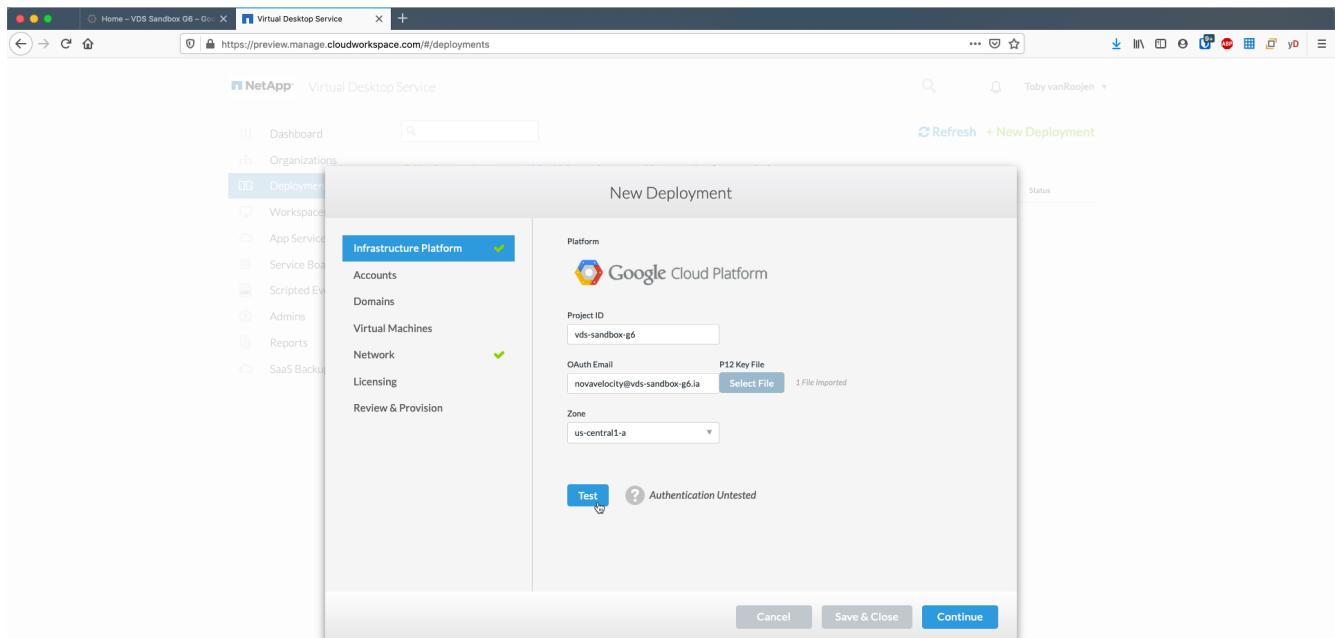


Infrastructure platform

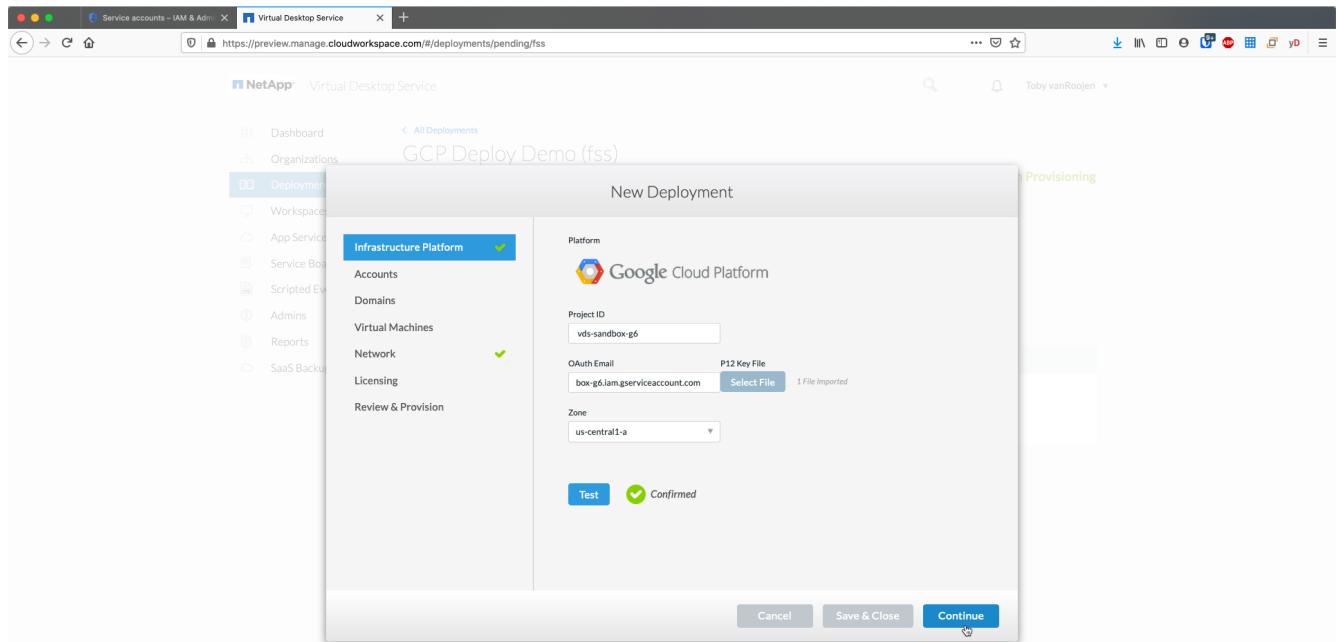
1. Enter the *Project ID* and OAuth Email address. Upload the .P12 file from earlier in this guide and select the appropriate zone for this deployment. Click *Test* to confirm the entries are correct and the appropriate permissions have been set.



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



2. Once confirmed, click *Continue*



Accounts

Local VM accounts

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

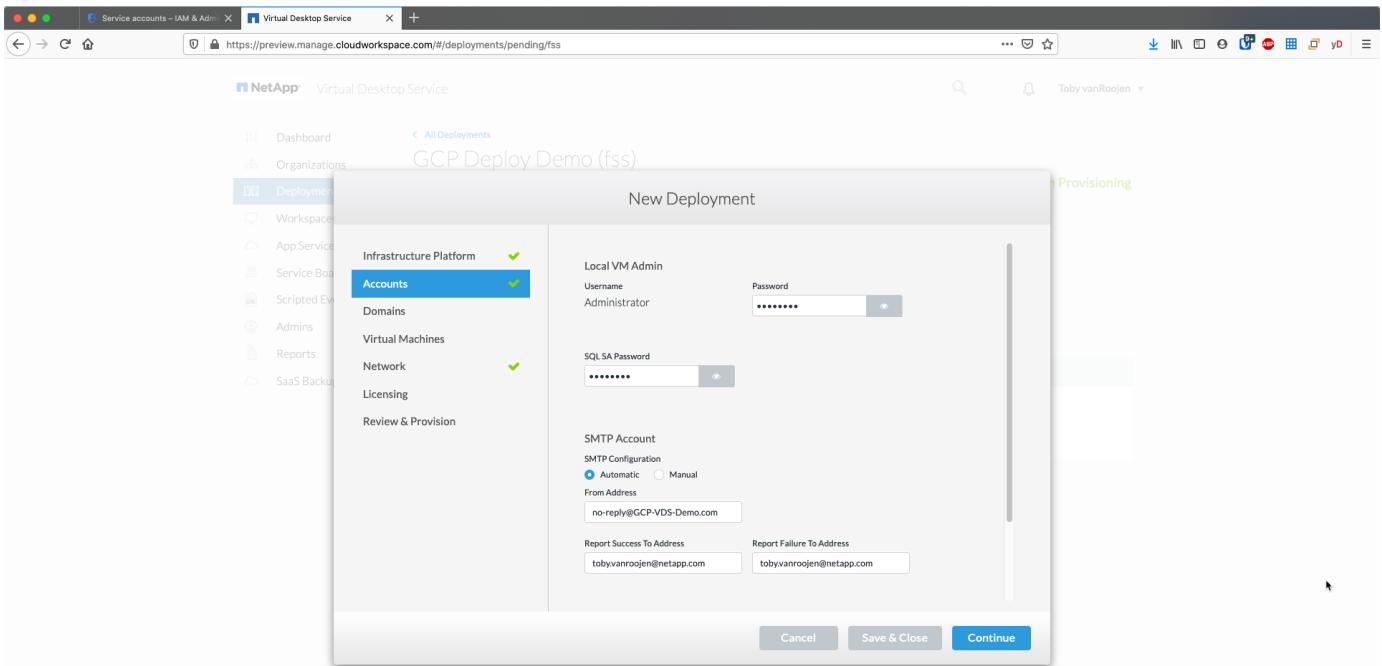


Password complexity requires an 8 character minimum with 3 of the 4 following character types: uppercase, lowercase, number, special character

SMTP account

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

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



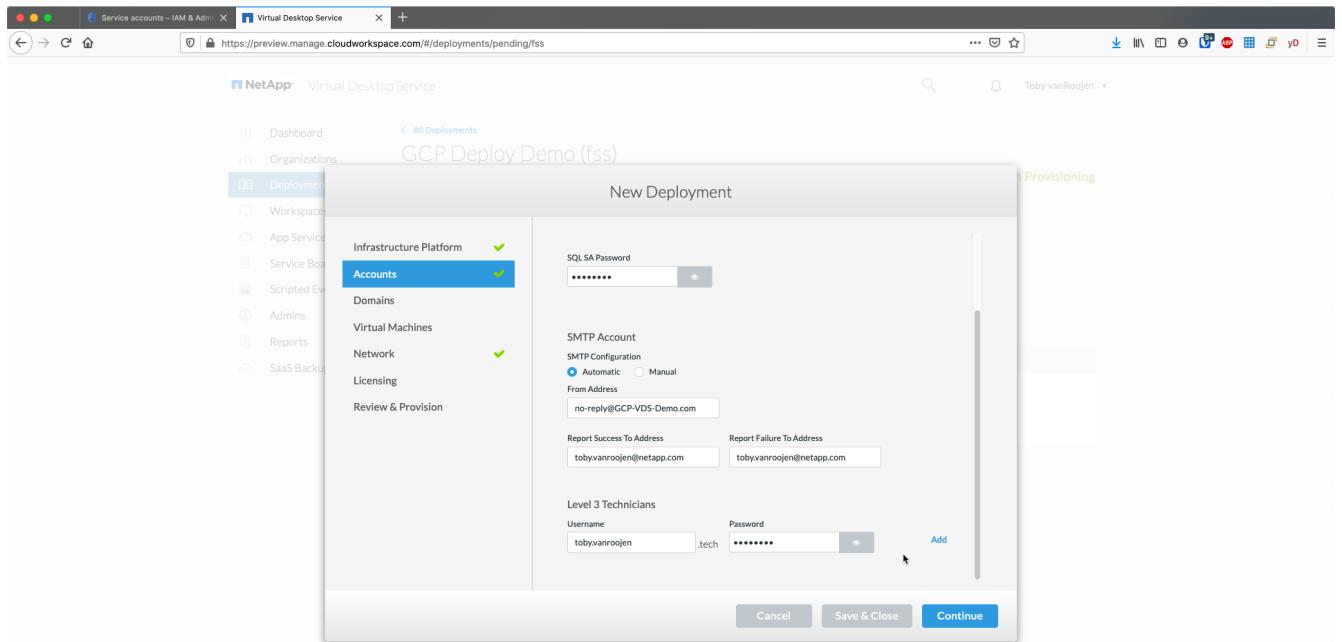
Level 3 technicians

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

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



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



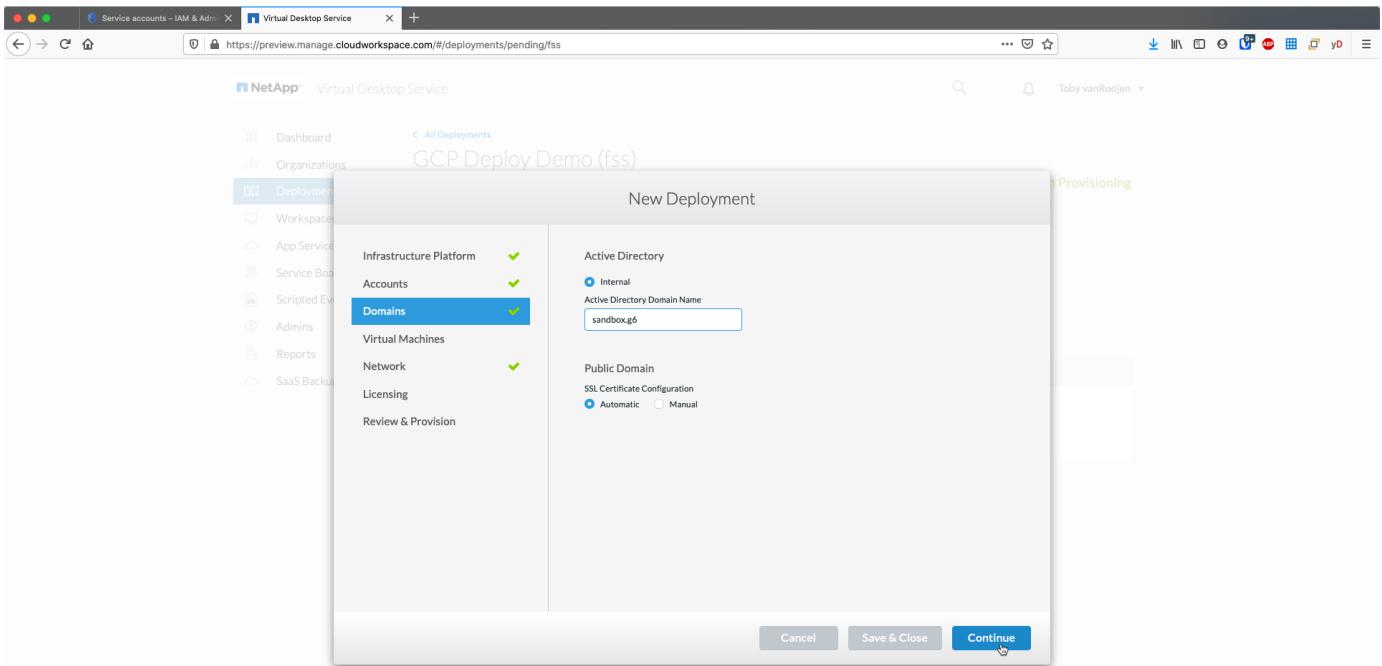
Domains

Active directory

Enter the desired AD domain name.

Public domain

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



Virtual machines

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

Platform VM configuration

Single virtual machine

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

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

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



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

Multiple servers

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

- Remote Desktop Gateway

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

- HTML5 Gateway

VDS Setup can be used to deploy and configure one or two 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.

New Deployment

Included services and VMs	
Service	# of VMs
Cwmgr1	1
CWPortal1(2)	2 ▾
CWRDSGateway1(2)	1 ▾
Remote App	1
Domain Controllers	1

of Domain Controllers
2 ▾

Cancel Save & Close Continue

Operating system

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

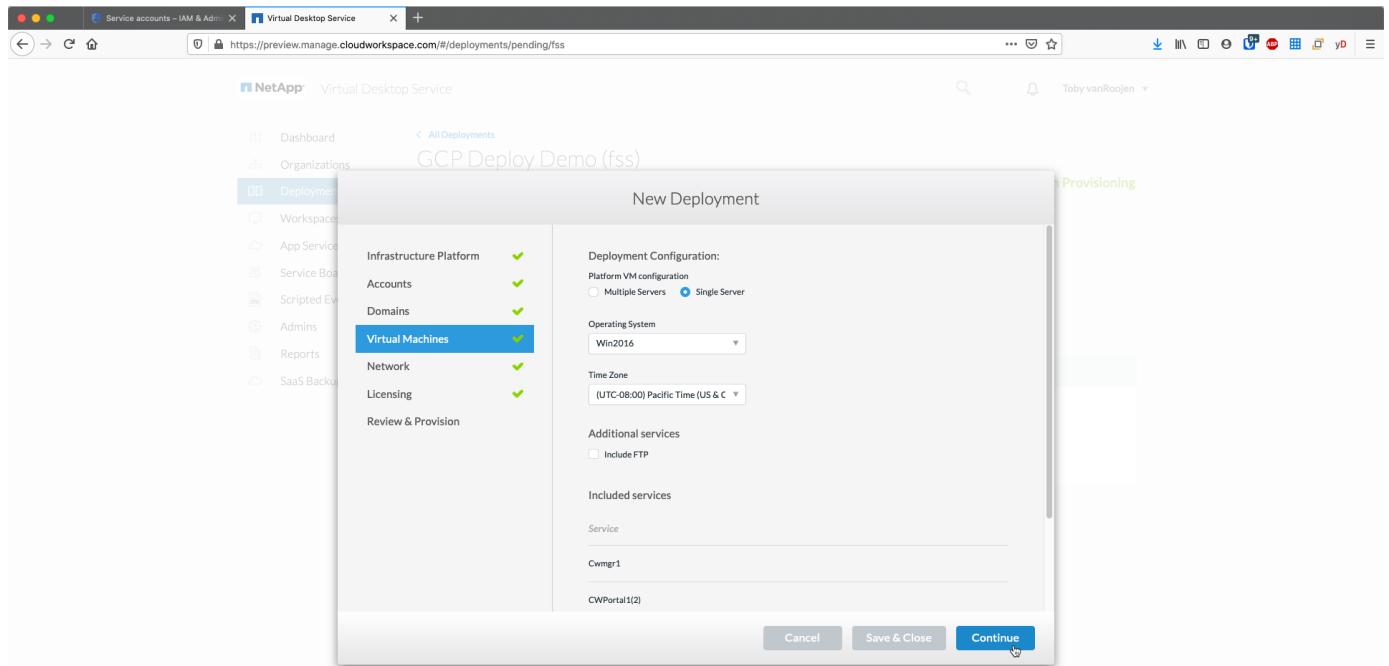
Time zone

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

Name	IP Range	Start IP	End IP
Global Network	10.0.0.0/20	10.0.0.0	10.0.15.255
Domain Controller/Platform Server Subnet Range (Subnet1)	10.0.0.28	10.0.0.0	10.0.0.15
Client Server Subnet Range (Subnet2)	10.0.2.0/23	10.0.2.0	10.0.3.255

Licensing

SPLA

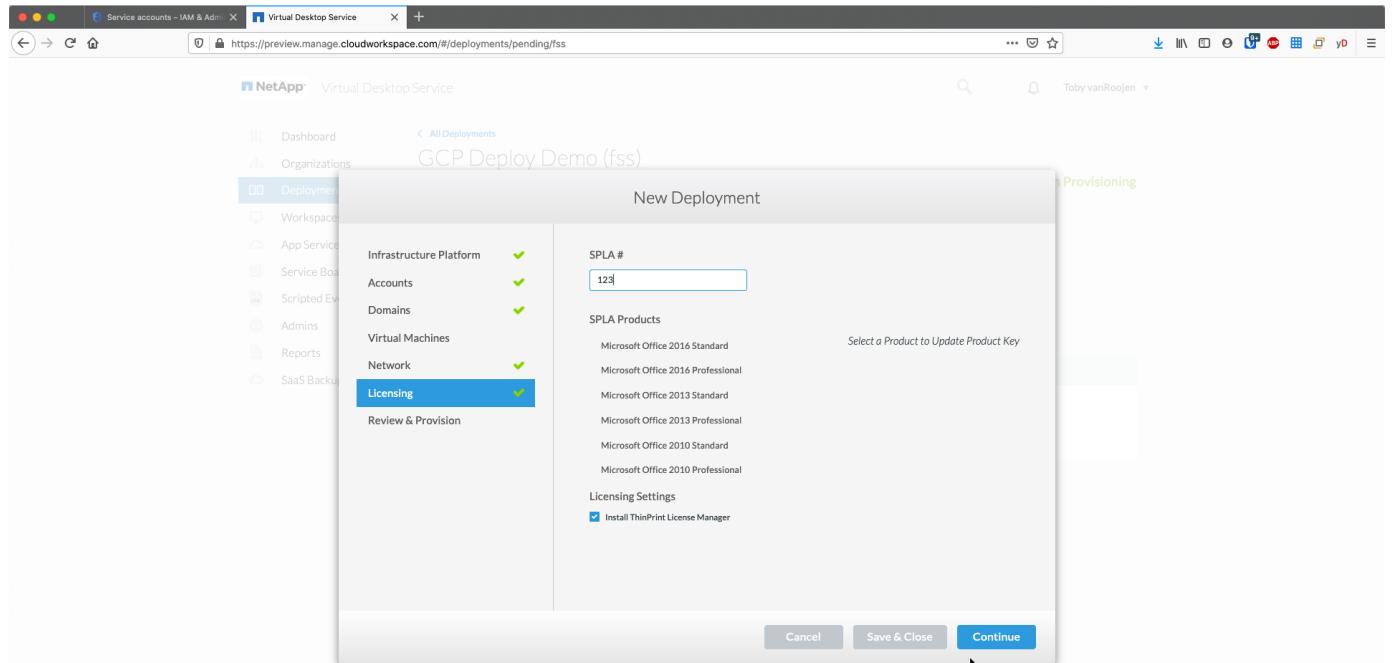
Enter your SPLA number so VDS can configure the RDS licensing service for easier SPLA RDS CAL reporting. A temporary number (such as 12345) can be entered for a POC deployment but after a trial period (~120 days) the RDS sessions will stop connecting.

SPLA products

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

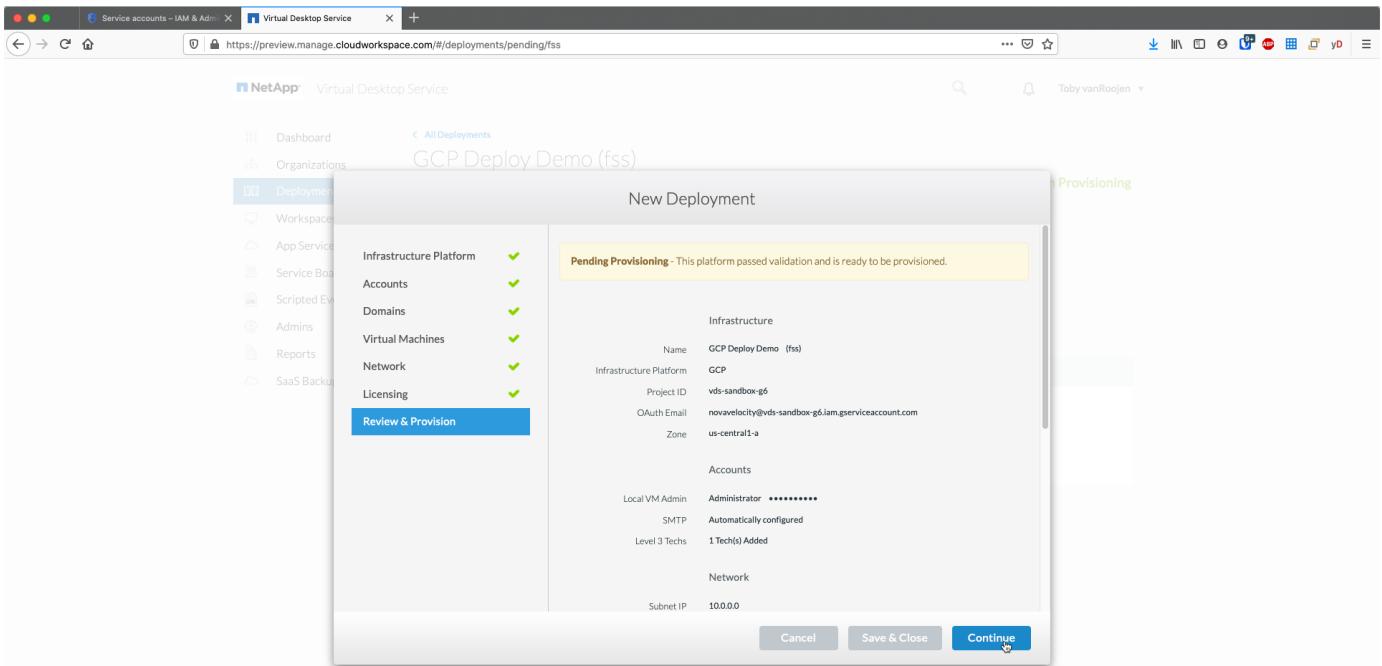
ThinPrint

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*

GCP Deploy Demo (fss)

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

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.

New Provisioning Collection

Provisioning Collection Settings

Name:

Description (Optional):

Type:

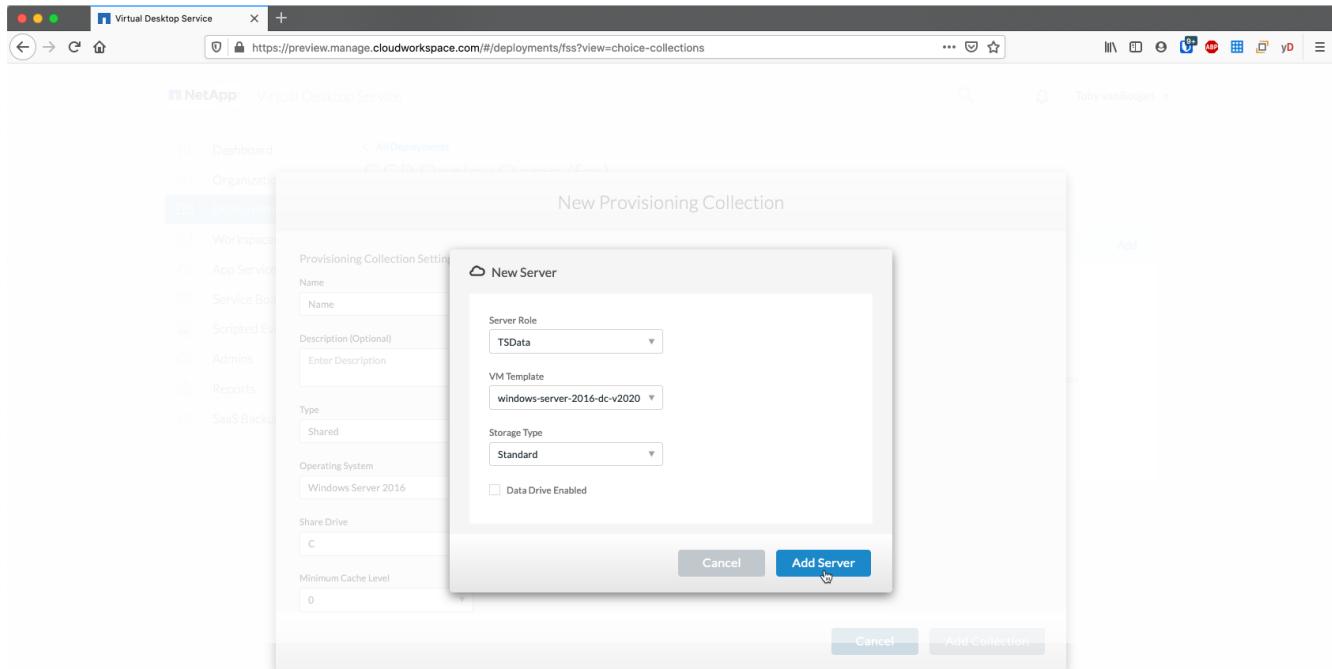
Servers: No Servers Added. A Server is required to continue.

Operating System:

Share Drive:

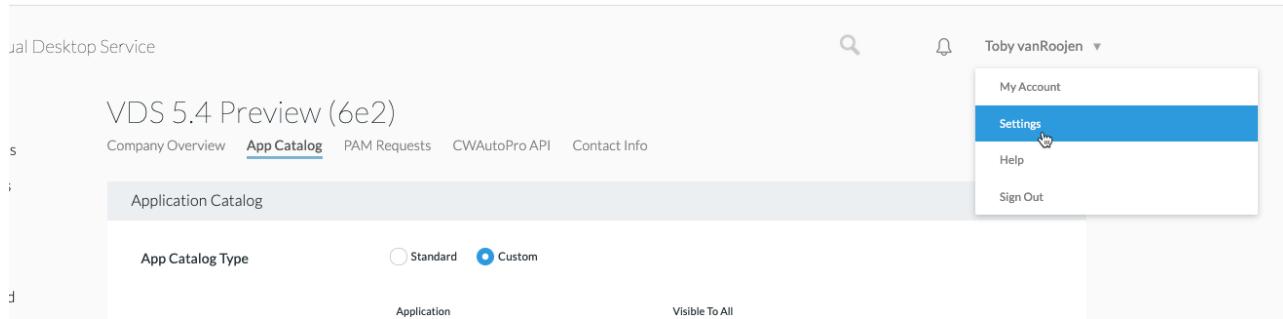
Minimum Cache Level:

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



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

- 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.



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

GCP Deploy Demo (fss)

Provisioning Collections

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

b. Then, click the *server template name*

This collection is ready to be validated. The collection will temporarily be locked while the hypervisor templates are created.

Provisioning Collection Settings

Version 1

Name GCP

Description

Type VDI

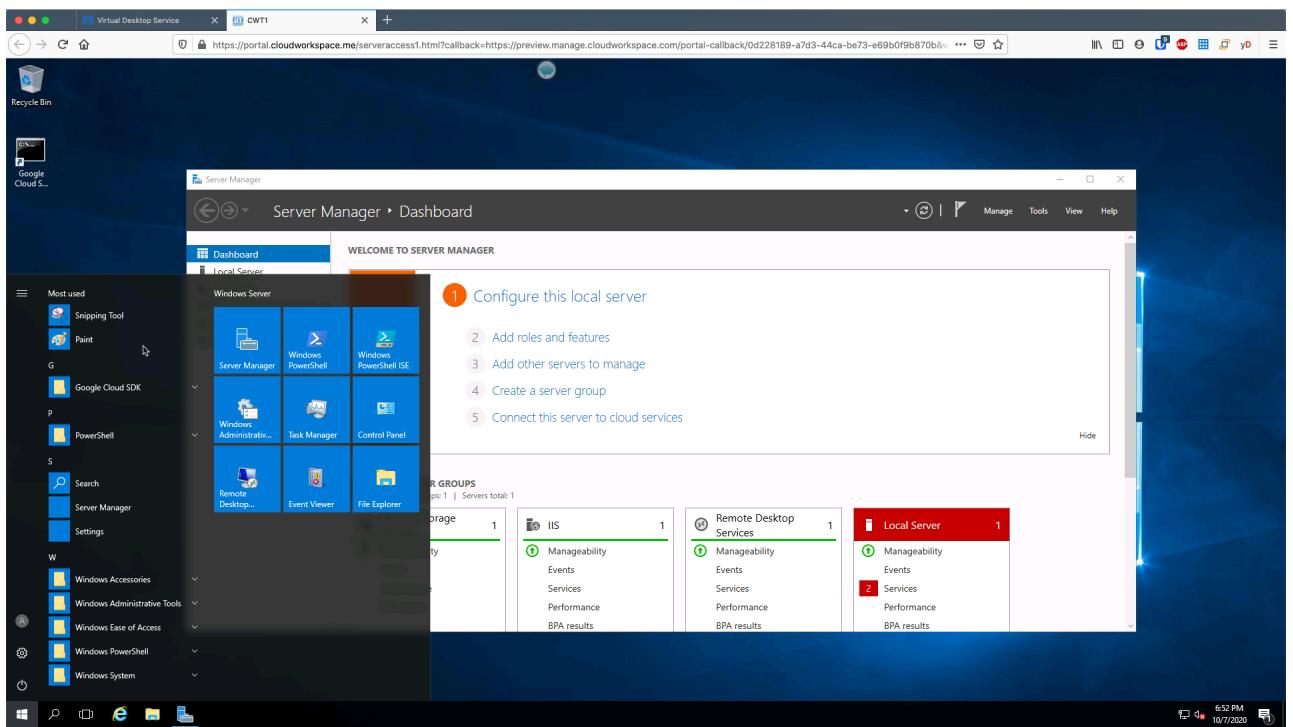
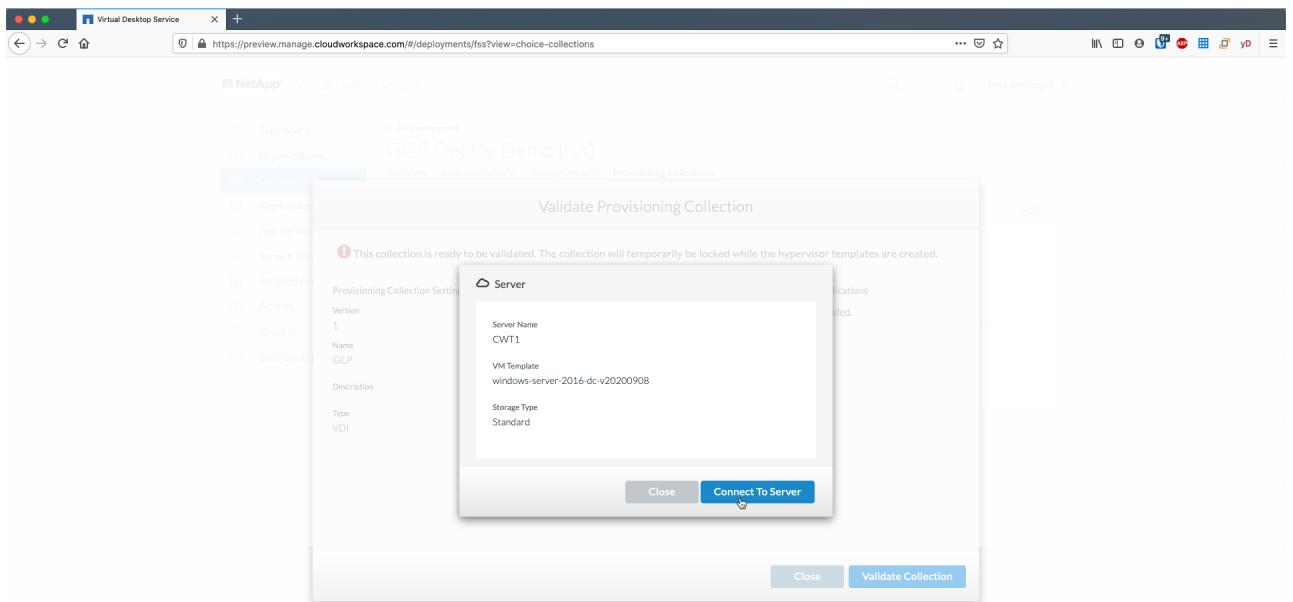
Servers

Included Applications

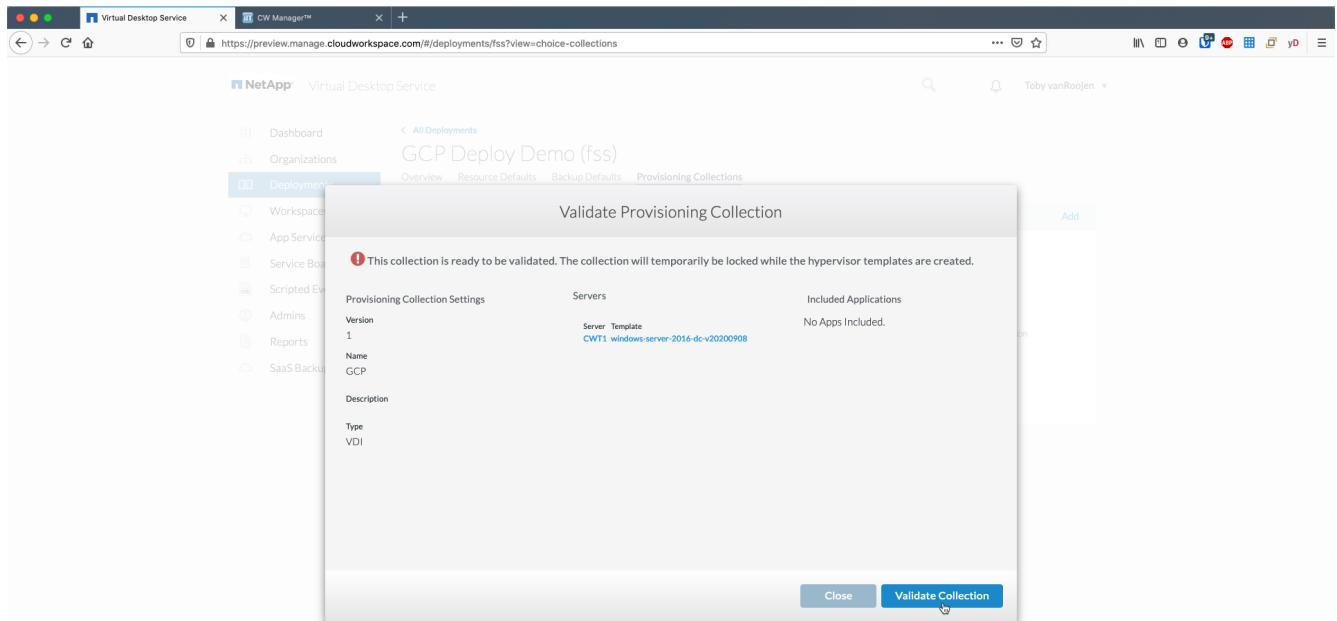
Server Template CWT1_windows-server-2016-dc-v20200908

Close Validate Collection

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



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



5

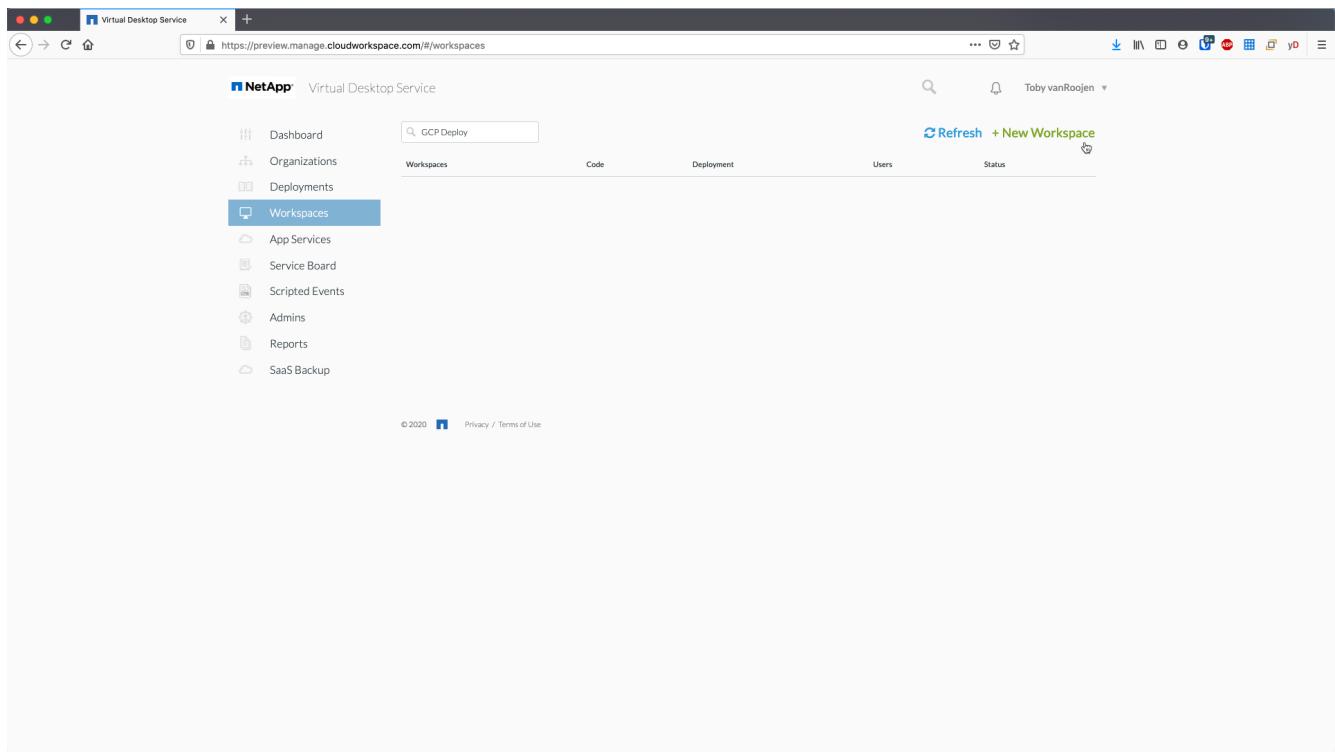
Create new workspace

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

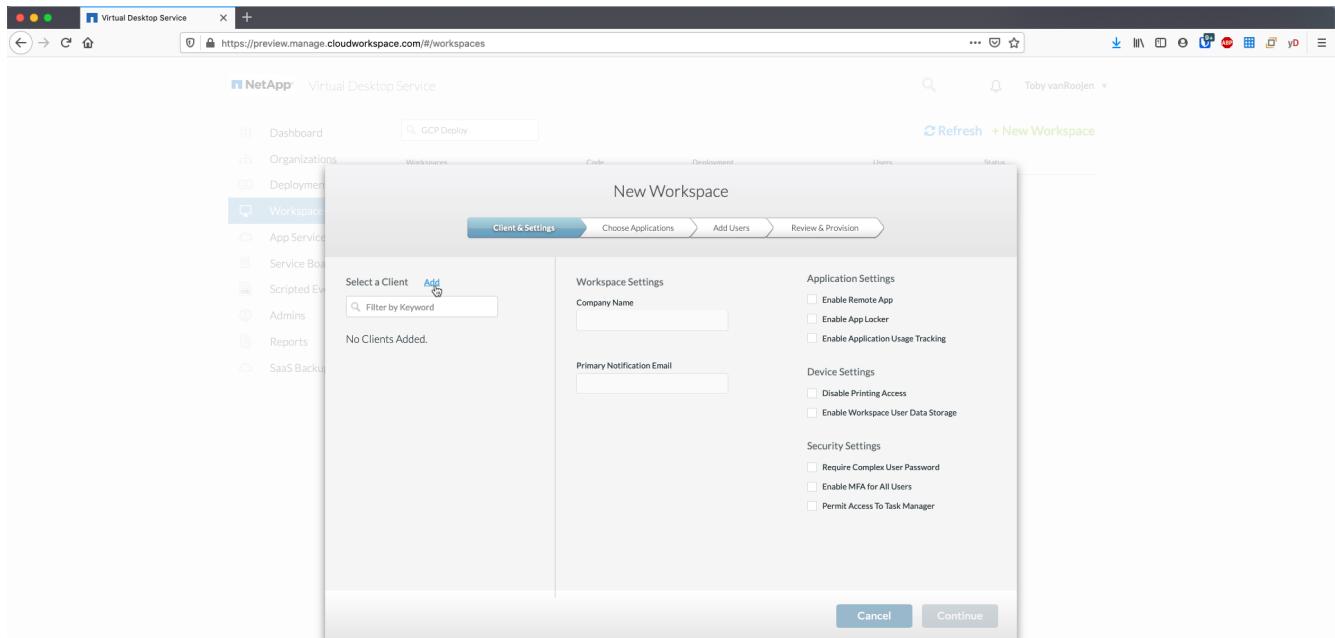
Workspaces define the RDS server collection for a specific group. In this example, we will deploy a single collection to demonstrate the virtual desktop capability. However, the model can be extended to multiple workspaces/ RDS collections to support different groups and different locations within the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

Client & settings

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



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



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

d. Additional Settings

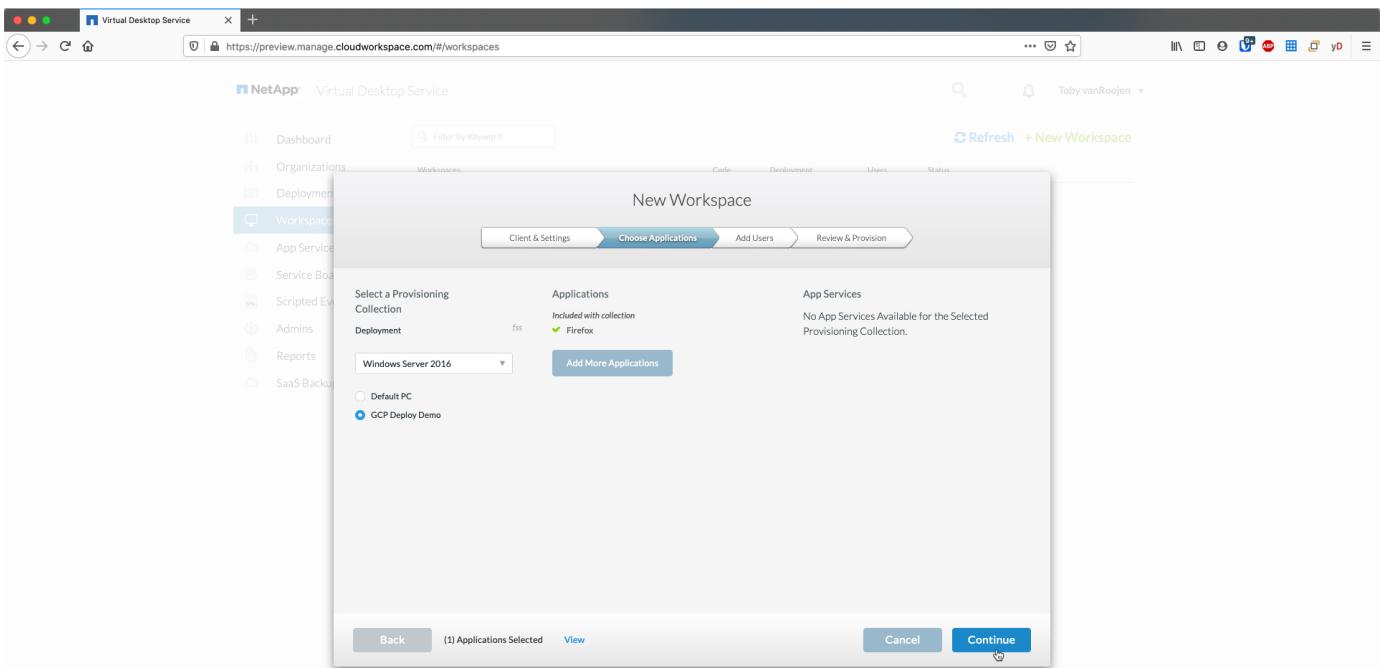
The following settings can be defined at deployment and/or selected post-deployment.

- 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

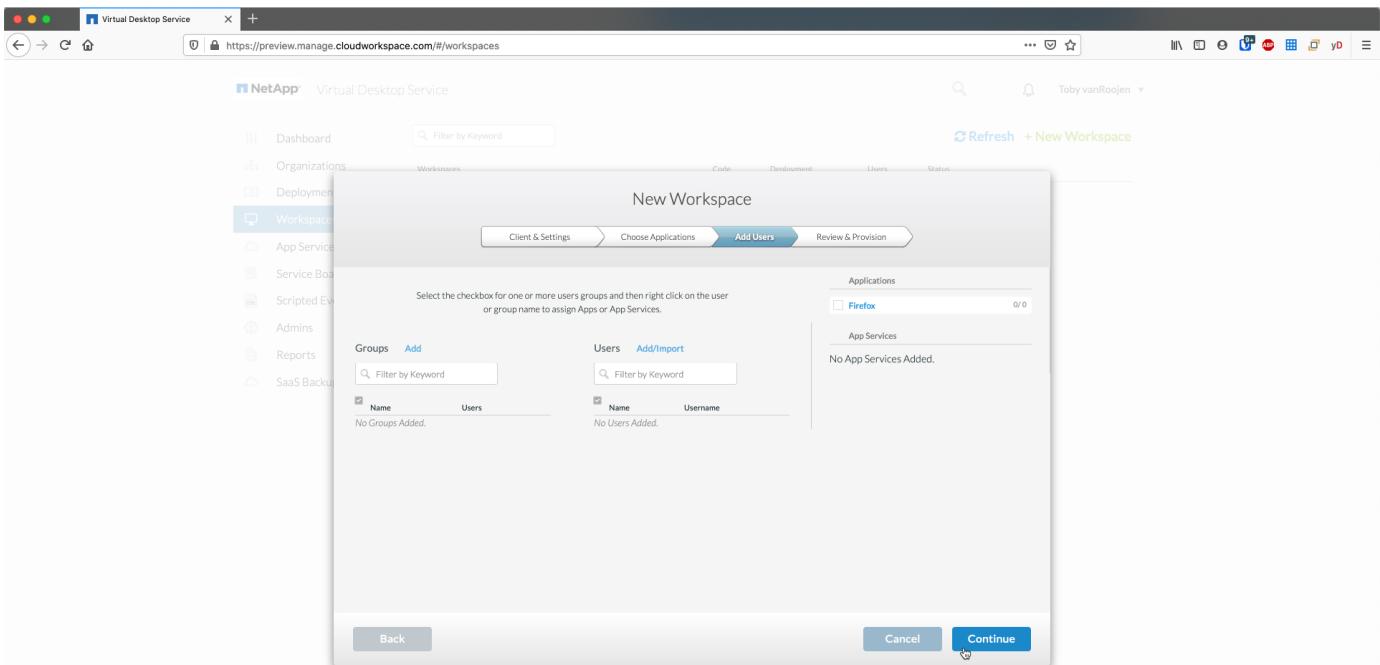
Select the Windows OS version and Provisioning collection created earlier in this guide.

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



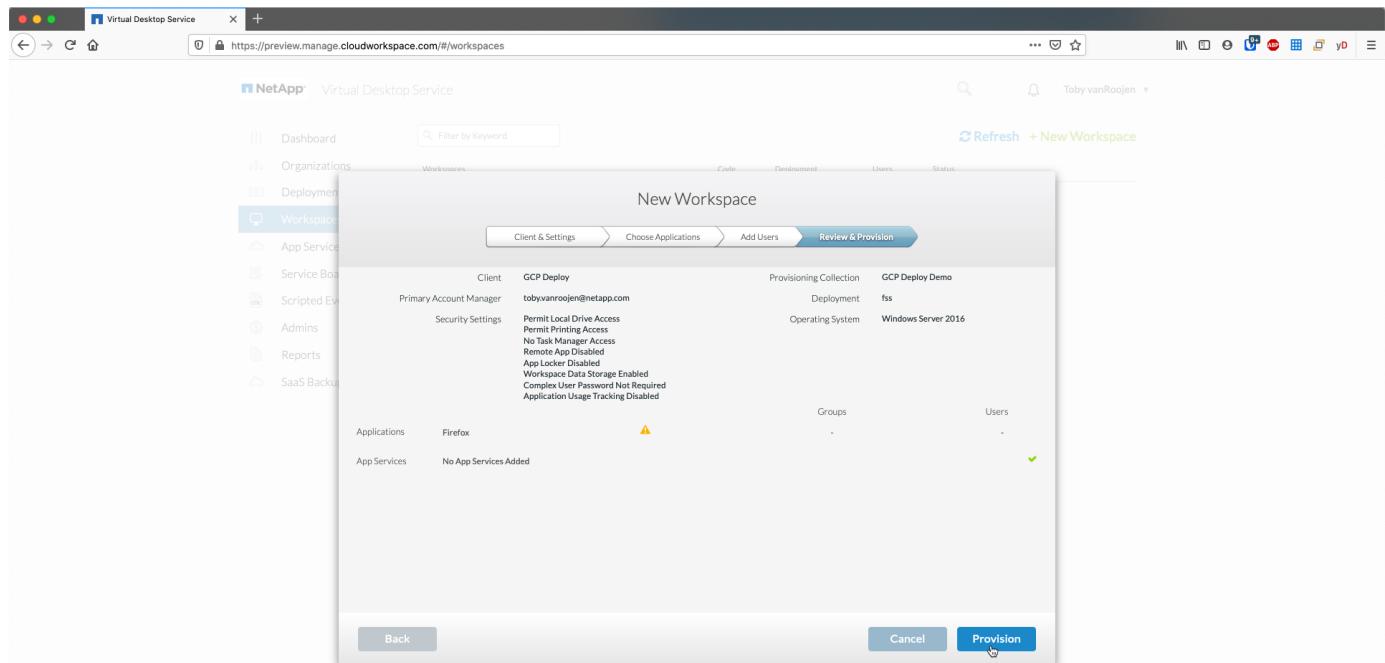
Add Users

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 licensing
- Self-service password reset
- Automatic server and gateway address negotiation
- Full desktop & streaming application support
- Available custom branding
- Installer switches for automated deployment and configuration
- Built-in troubleshooting tools
- [NetApp VDS web client](#)
- [Microsoft RD Client](#)
 - Windows
 - MacOS
 - iSO
 - Android
- 3rd party software and/or thin clients
 - Requirement: Support RD gateway configuration

Storage layer

In RDS deployed by VDS, the storage strategy is designed so that no persistent user/company data resides on the 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/logout 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 an 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 hosts, deployed by VDS, support the following x64 operating system images:

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

Copyright Information

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

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

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

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

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

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

Trademark Information

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