



Architectural

Virtual Desktop Service

NetApp

December 10, 2020

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



Table of Contents

- Architectural 1
 - Redirecting Storage Platform 1
 - Data Migration Considerations 8
 - Wildcard SSL Certificate Renewal Process 10
 - WVD Teardown Guide 17

Architectural

Redirecting Storage Platform

Overview

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

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

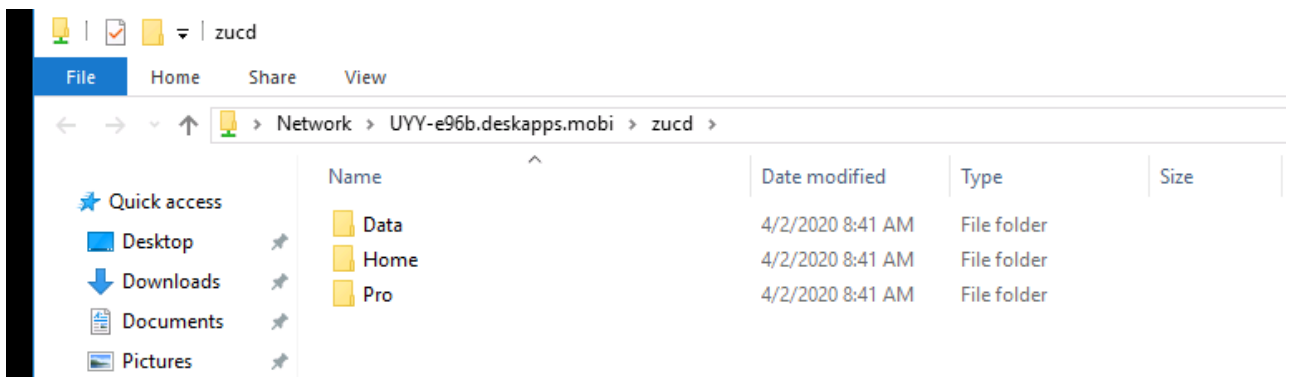
Creating the new storage layer

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

Create storage folders

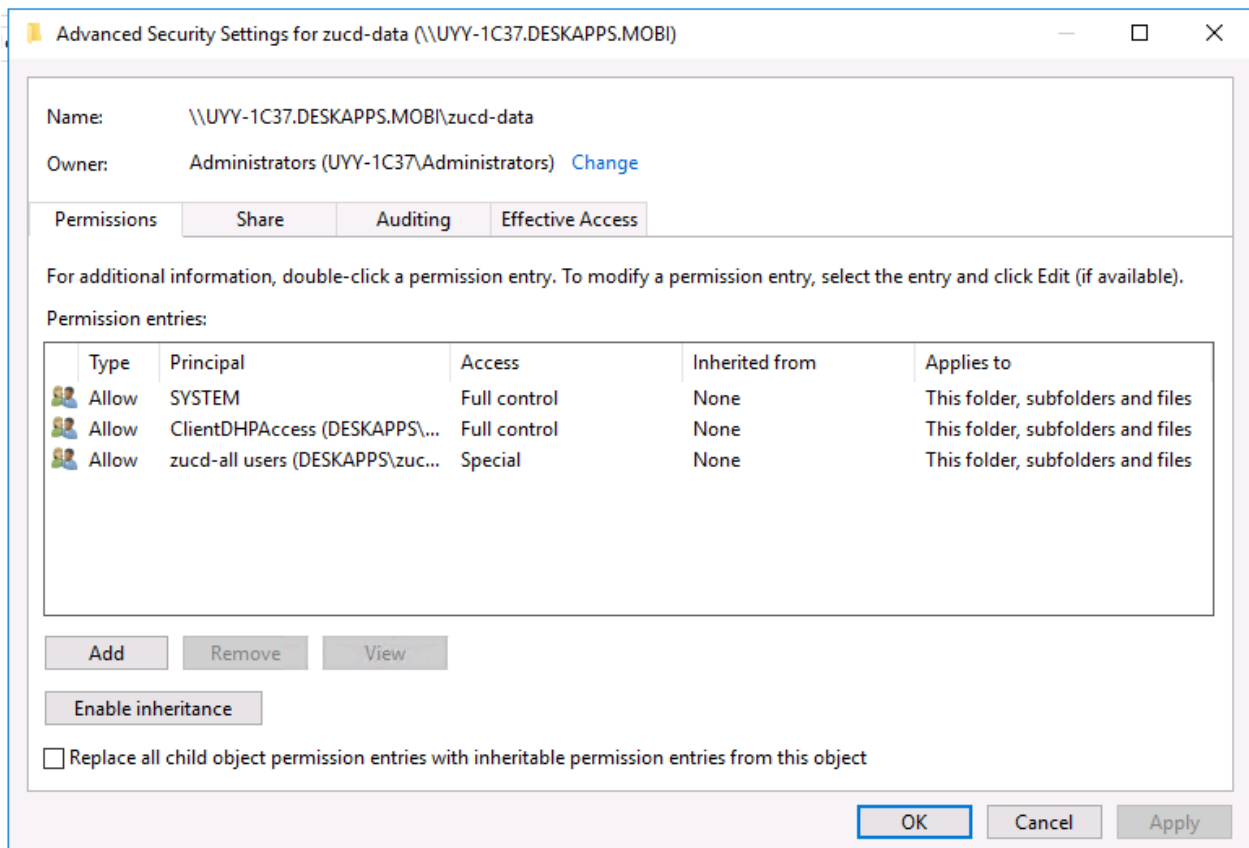
1. In the new storage service, create three folders:

- /Data
- /Home
- /Pro



2. Set Folder Permissions

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



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

Moving data

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

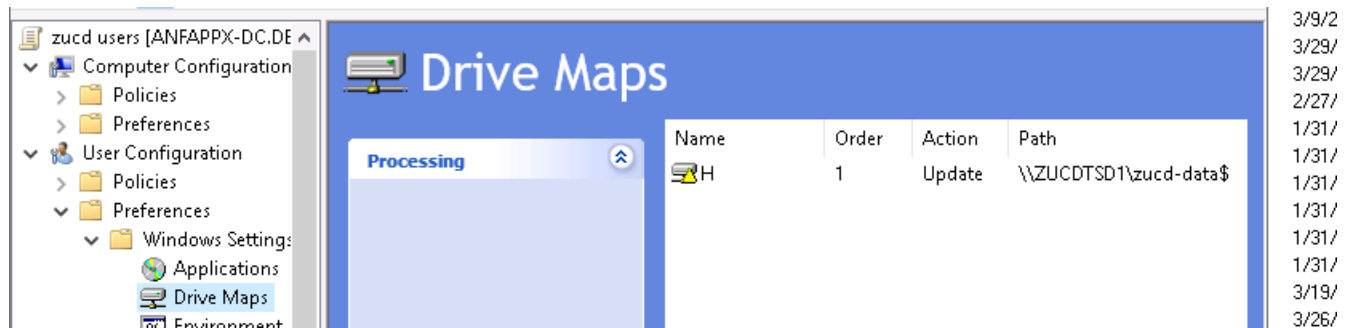
```
robocopy c:\data\zucd \\uyv-1c37.deskapps.mobi\zucd-data /xd ~snapshot /MIR /CopyAll /R:1 /W:1 /tee /log:C:\temp\roboitD.txt
```

Redirecting the SMB path at cutover

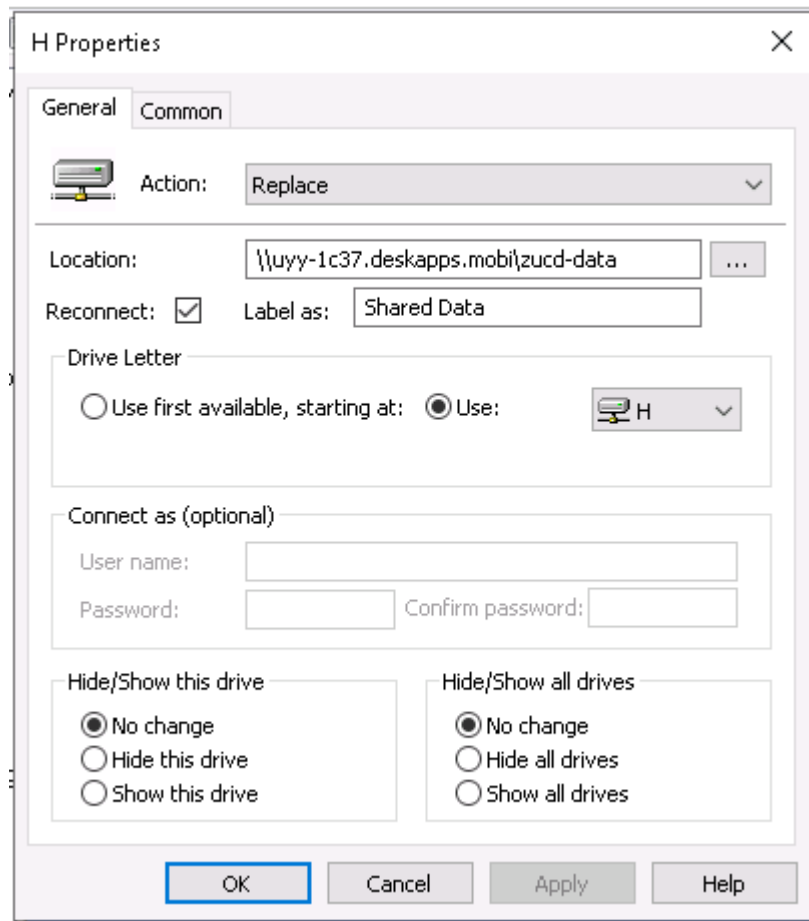
When the time for cutover comes, a few changes will redirect all the storage functionality across the VDS environment.

Update GPOs

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



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



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



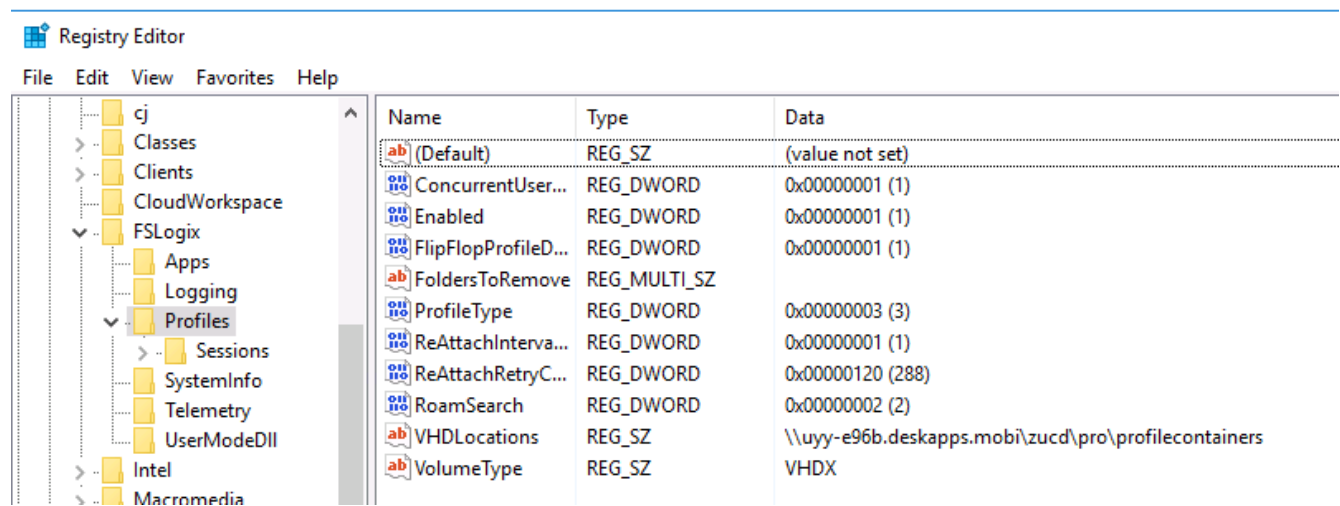
Update FSLogix profile paths

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



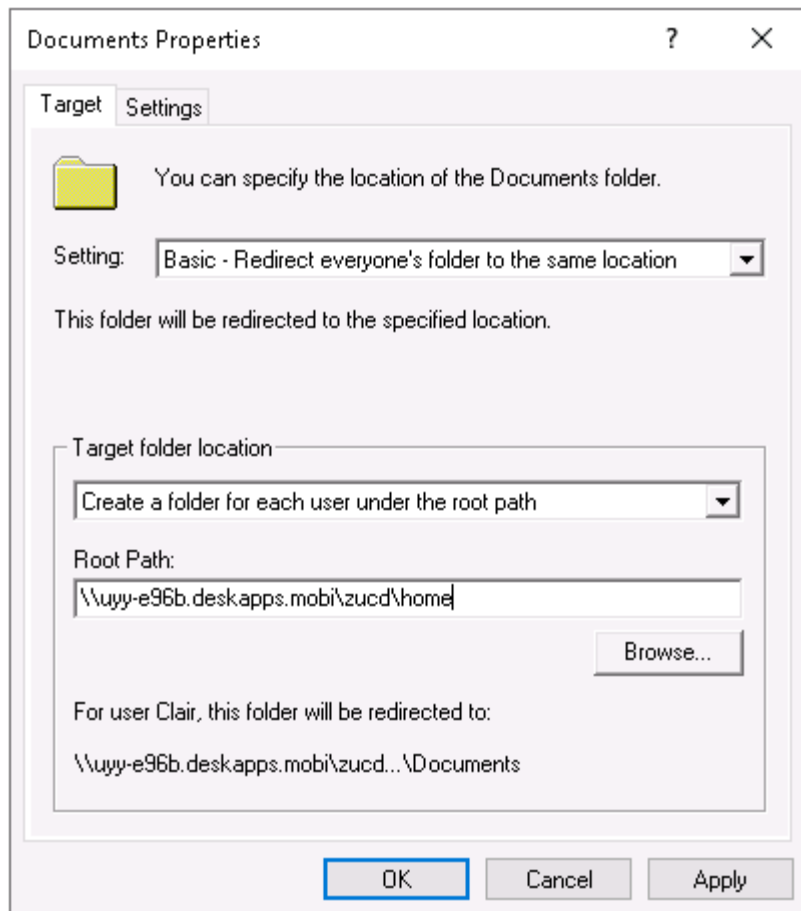
This can also be set via a GPO policy if desired.

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



Update the folder redirection settings for the home directories

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

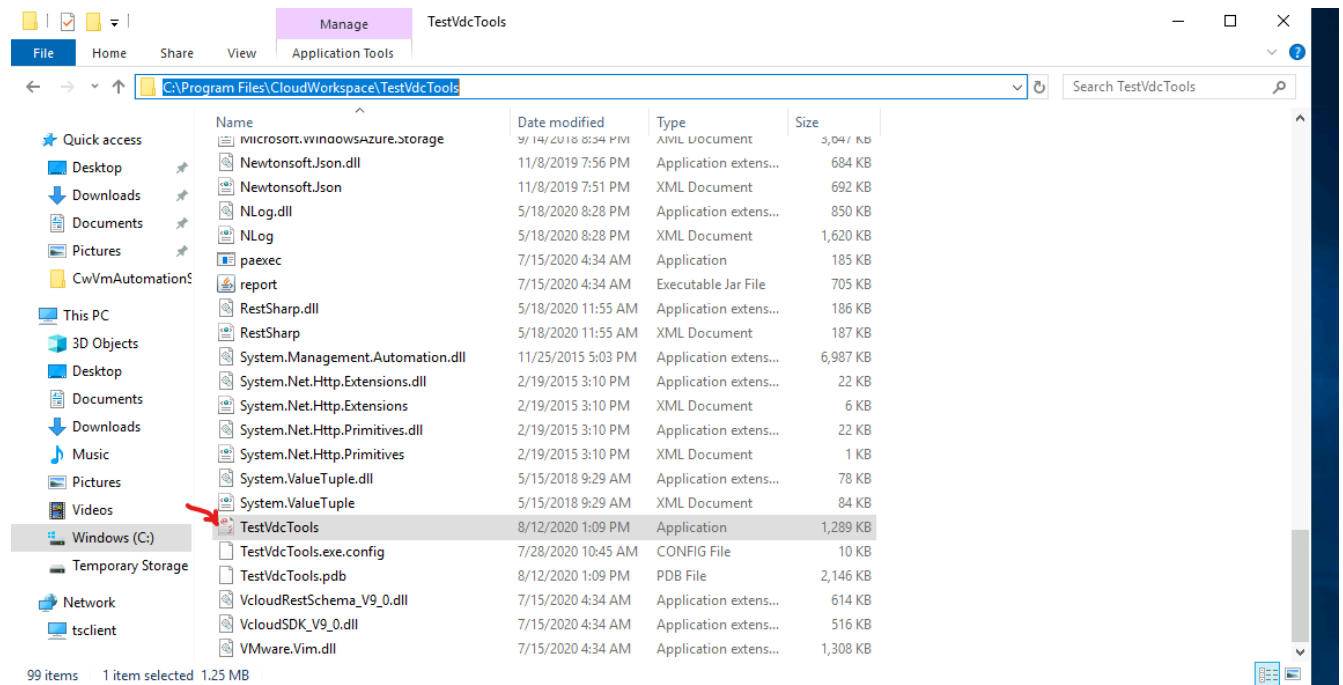


Update the VDS SQL database with TestVDC Tools

CWMGR1 contains a helper utility applications called TestVDC Tools which can bulk update the VDS database.

To make the final database updates:

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



2. Navigate to the *Operations* tab and enter the new storage paths(s) for the storage layer then click *Execute Command*.

Tests Operations Advanced Hypervisor

Command

Change Data/Home/Pro Folders



Load Data

Company Code



Data

☐ Is Windows Server

Home

☐ Is Windows Server

Pro

☐ Is Windows Server

Execute Command

View All Logs

Clear Log



Data Migration Considerations

Overview

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

Data that is typically migrated:

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

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

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

Generic migration process

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

FTPS transfers & considerations

Migration with FTPS

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



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

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



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

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

Sync tools and considerations

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

Migrating SQL and Similar Data (Open Files)

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

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

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

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

Shipping drives

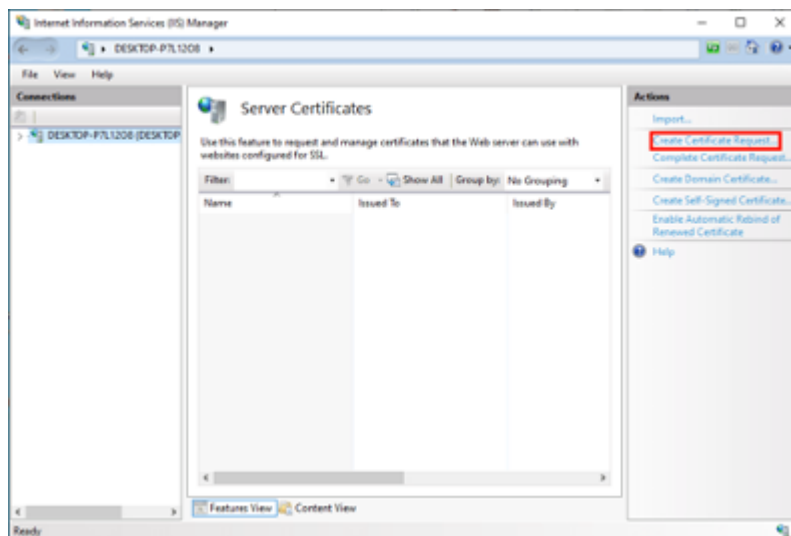
Many data center providers no longer ship hard drives – either that, or they require you to follow their specific policies and procedures.

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

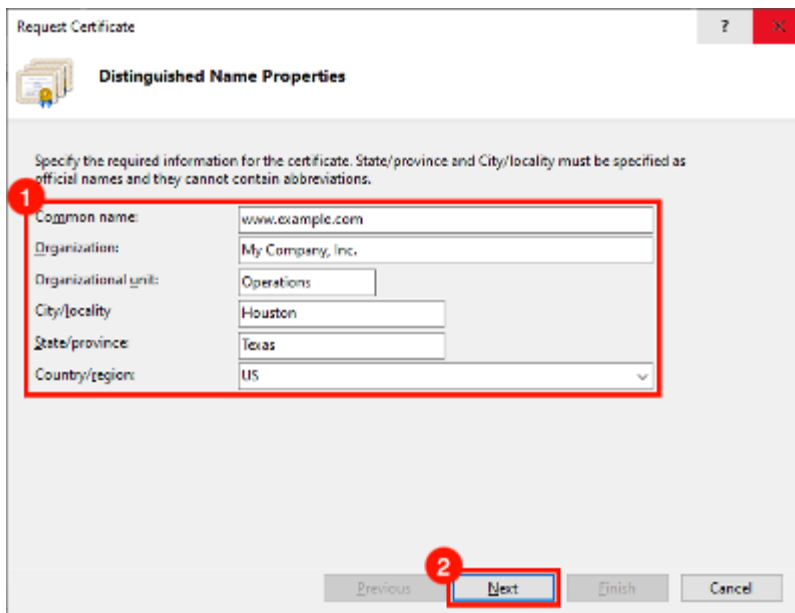
Wildcard SSL Certificate Renewal Process

Create a certificate signing request (CSR):

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



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



The dialog box is titled "Request Certificate" and "Distinguished Name Properties". It contains a text box for "Common name" with the value "www.example.com", a text box for "Organization" with the value "My Company, Inc.", a text box for "Organizational unit" with the value "Operations", a text box for "City/locality" with the value "Houston", a text box for "State/province" with the value "Texas", and a dropdown menu for "Country/region" with the value "US". A red box highlights the entire form area, and a red circle with the number "1" is next to the "Common name" field. At the bottom, there are buttons for "Previous", "Next", "Finish", and "Cancel". A red box highlights the "Next" button, and a red circle with the number "2" is next to it.

Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

1

Common name: www.example.com

Organization: My Company, Inc.

Organizational unit: Operations

City/locality: Houston

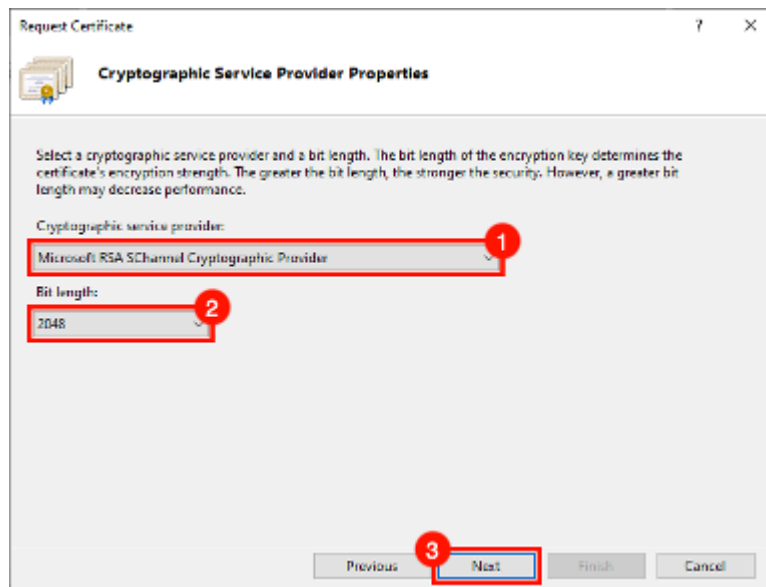
State/province: Texas

Country/region: US

2

Previous Next Finish Cancel

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



The dialog box is titled "Request Certificate" and "Cryptographic Service Provider Properties". It contains a text box for "Cryptographic service provider" with the value "Microsoft RSA SChannel Cryptographic Provider", and a dropdown menu for "Bit length" with the value "2048". A red box highlights the "Cryptographic service provider" field, and a red circle with the number "1" is next to it. Another red box highlights the "Bit length" dropdown, and a red circle with the number "2" is next to it. At the bottom, there are buttons for "Previous", "Next", "Finish", and "Cancel". A red box highlights the "Next" button, and a red circle with the number "3" is next to it.

Request Certificate

Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

1

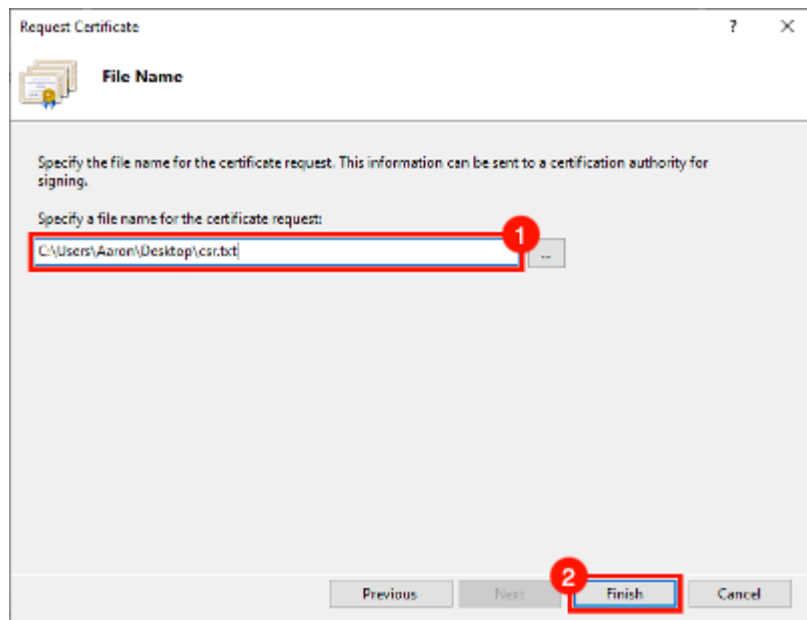
Bit length: 2048

2

3

Previous Next Finish Cancel

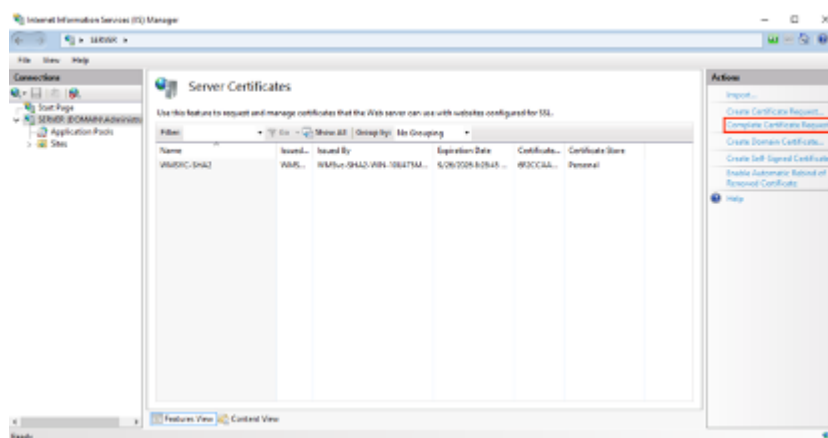
7. Specify a file name and browse to a location where you want to save the CSR. If you do not specify a location, the CSR will be in C:\Windows\System32:



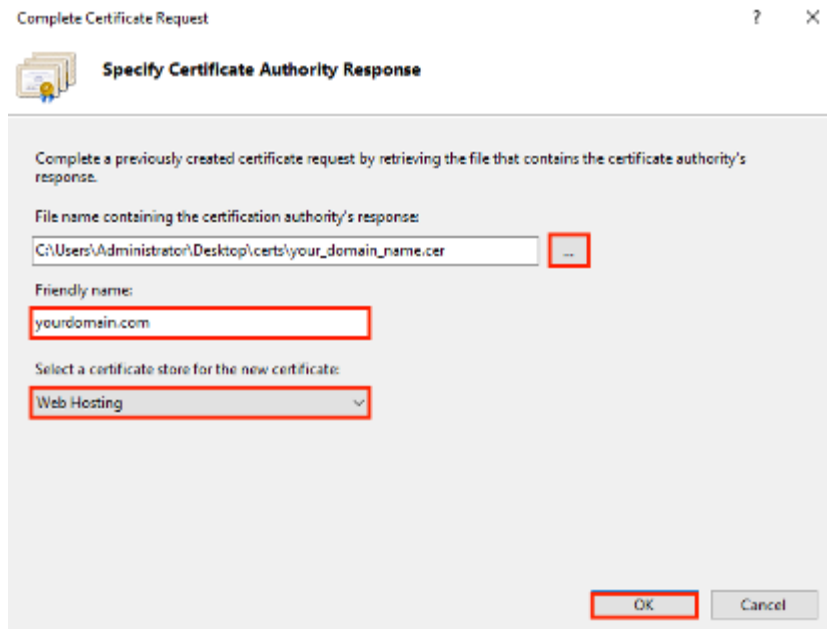
8. Click Finish when completed. You will use this text file to submit your order to certificate registrar
9. Reach out to registrar support to purchase a new Wildcard SSL for your certificate: *.domain.com
10. After receiving your SSL certificate, save the SSL certificate .cer file in a location on CWMGR1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

Installing and configuring CSR:

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



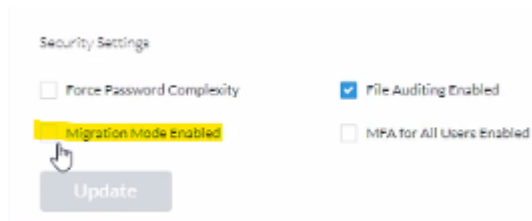
5. Complete the below fields in the Complete Certificate Request and click OK:



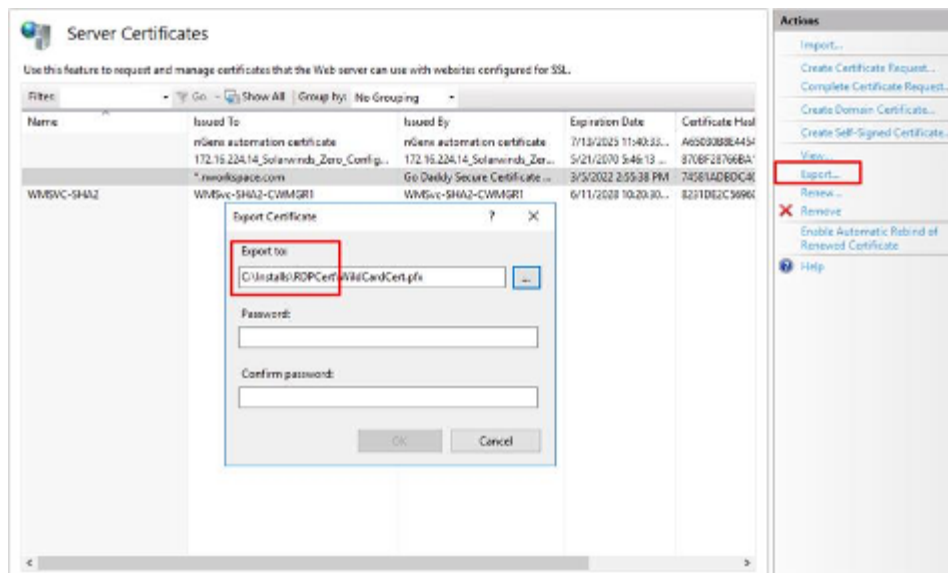
- a. File Name: Select .cer file that was saved previously
- b. Friendly name: *.domain.com
- c. Certificate store: Select either Web Hosting or Personal

Assigning SSL certificate:

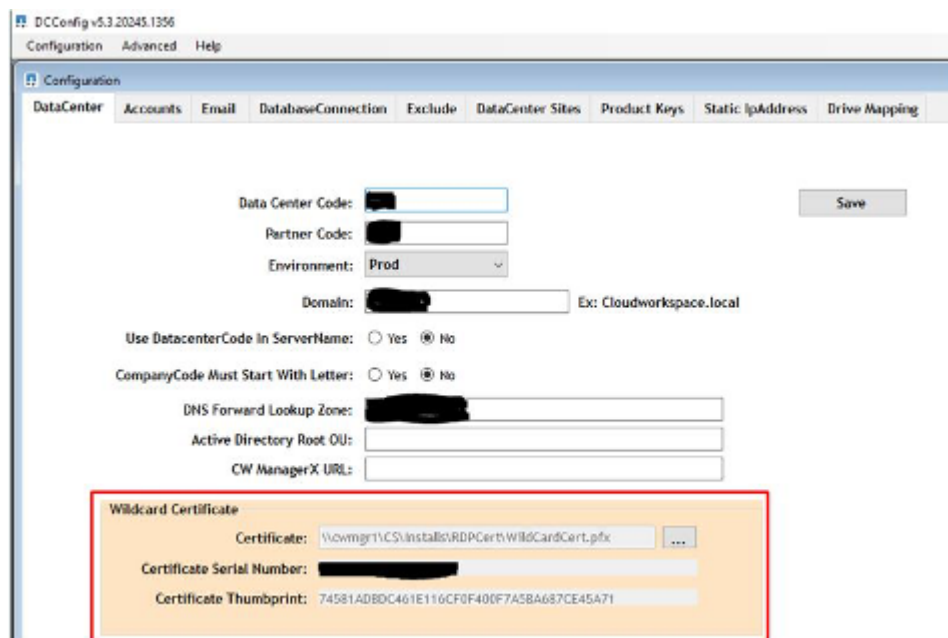
1. Verify that Migration Mode is not enabled. This can be found on the Workspace Overview page under Security Settings in VDS.



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

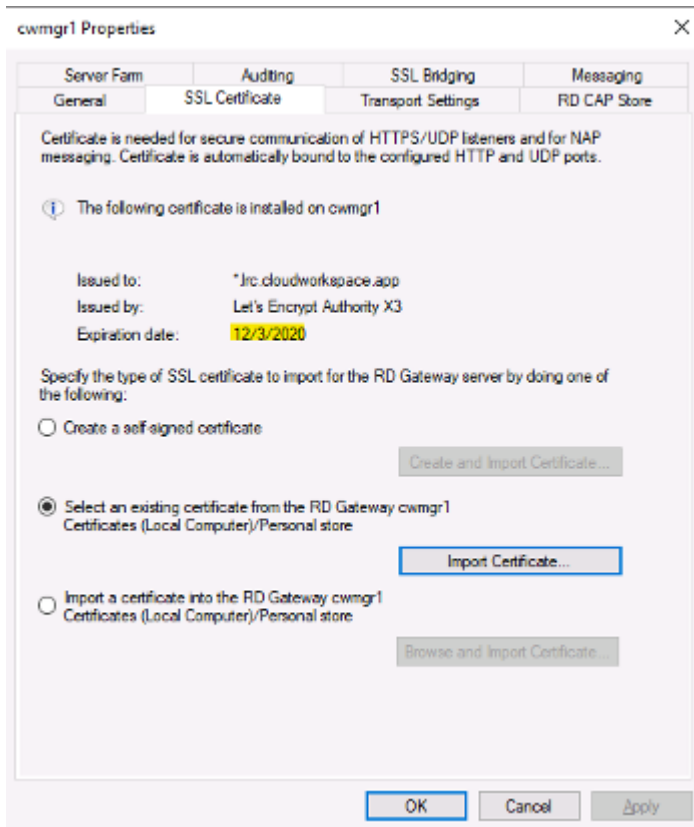


10. Open DCConfig
11. Under Wildcard Certificate, update the Certificate path to new .pfx file
12. Enter .pfx password when prompted
13. Click Save



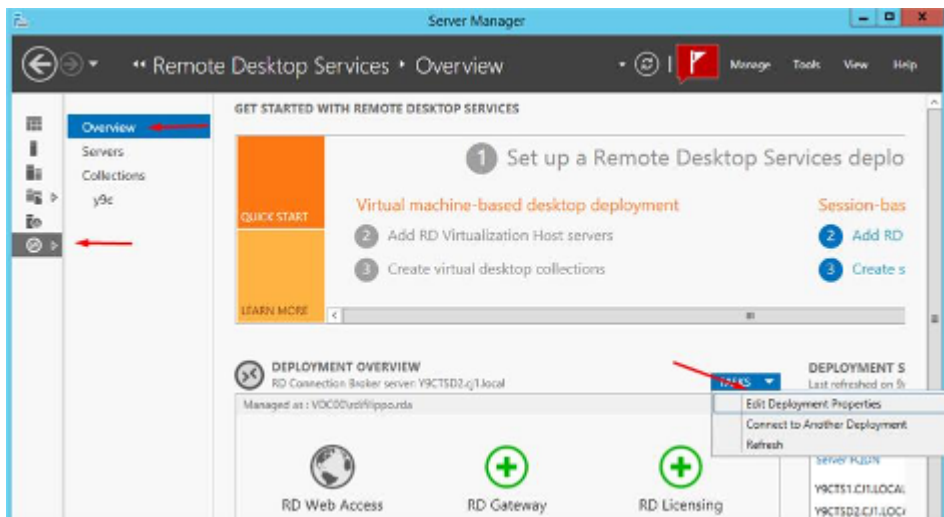
14. If the certificate is valid for 30 more days, allow automation to apply the new certificate during the morning Daily Actions task throughout the week
15. Periodically check the Platform servers to verify that the new certificate has propagated. Validate and test user connectivity to confirm.
 - a. On the server, go to Admin Tools
 - b. Select Remote Desktop Services > Remote Desktop Gateway Manager

- c. Right click on gateway server name, select Properties. Click on the SSL Certificate tab to review expiration date

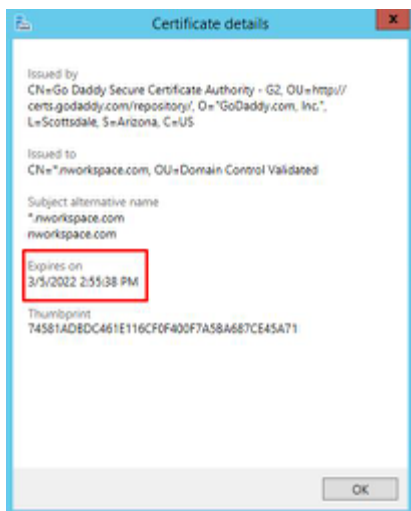
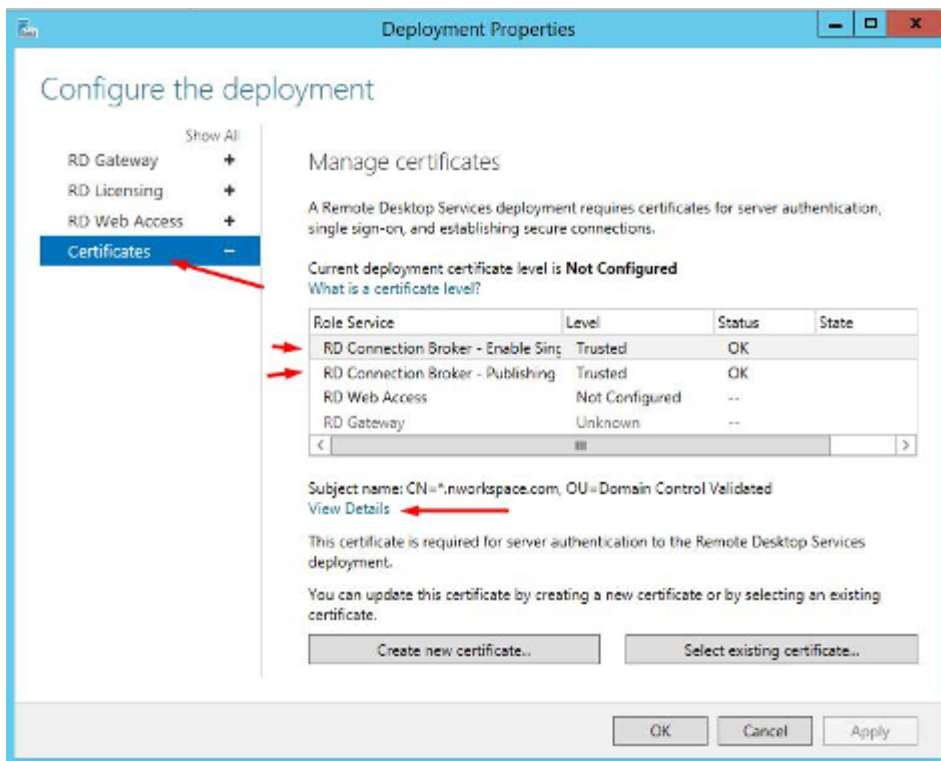


16. Periodically check the client VMs that are running the Connection Broker role

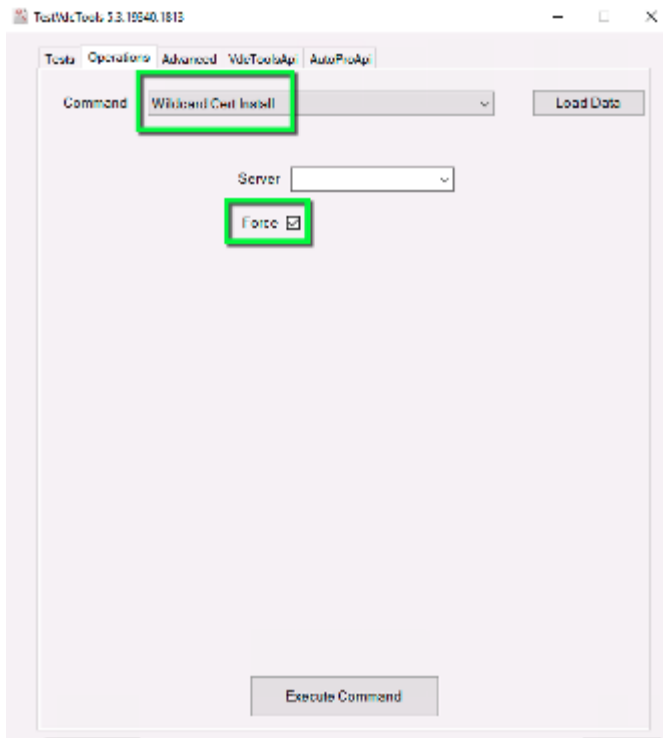
- a. Go to Server Manager > Remote Desktop Services
- b. Under Deployment Overview, select Tasks dropdown and choose Edit Deployment Properties



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



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



WVD Teardown Guide

Overview

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

Initial state

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

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

Delete CW Agent service

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

scripted automation. The video below shows it done manually.

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

Delete CW Agent service video


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

Delete CW agent directory

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

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

Delete CW Agent directory video

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

Remove startup shortcuts

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

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

Remove startup shortcuts video

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

Unlink 'Users' and 'Companies' GPOs

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


Unlink:

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

Review:

- AADDC Computers > Cloud Workspace Computers

Unlink 'Users' and 'Companies' GPOs video

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


Shutdown CWMGR1

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

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

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

Shutdown CWMGR1 video

 | https://img.youtube.com/vi/avk9HyIiC_s/maxresdefault.jpg

Delete NetApp VDS service accounts

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

- CloudWorkspaceSVC
- CloudWorkspaceCASVC

Other user accounts can be retained:

- End users
- Azure administrator
- .tech domain admins

Delete NetApp VDS service accounts video

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

Delete app registrations

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

- Cloud Workspace API
- Cloud Workspace WVD

Delete app registrations video


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

Delete enterprise applications

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

- Cloud Workspace
- Cloud Workspace Management API


Delete enterprise applications video

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

Confirm CWMGR1 is stopped

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

Confirm CWMGR1 is stopped video

 | <https://img.youtube.com/vi/Ux9nkDk5lU4/maxresdefault.jpg>

Login and end user

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

Login and end user video

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

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.