Architektur

Virtual Desktop Service

NetApp
February 20, 2023

Inhaltsverzeichnis

Architektur

Umleitung Der Storage-Plattform

Überblick

Bereitstellungstechnologien für Virtual Desktop Services ermöglichen unterschiedliche Storage-Optionen je nach zugrunde liegender Infrastruktur und dieser Leitfaden beschreibt, wie eine Änderung nach der Implementierung vorgenommen werden kann.

Die Performance virtueller Desktops hängt von verschiedenen wichtigen Ressourcen ab. Die Storage-Performance ist eine der primären Variablen. Wenn sich Anforderungen ändern und Workloads steigen, ist es häufig erforderlich, die Storage-Infrastruktur zu ändern. In fast allen Fällen umfasst dies die Migration von einer File-Server-Plattform zu NetApp Storage-Technologie (z. B. Azure NetApp Files, NetApp Cloud Volumes Service in Google oder NetApp Cloud Volumes ONTAP in AWS), da diese Technologien typischerweise das beste Performance-Profil für Endbenutzer-Computing-Umgebungen bieten.

Erstellen der neuen Speicherebene

Aufgrund der Vielzahl potenzieller Storage-Services in zahlreichen Cloud- und HCI-Infrastrukturanbietern wird in diesem Leitfaden davon ausgegangen, dass bereits ein neuer Storage-Service etabliert wurde und der bekannte SMB-Pfad(e) enthält.

Erstellen von Speicherordnern

1. Erstellen Sie im neuen Speicherdienst drei Ordner:
   - /Daten
   - /Home
   - /Pro

     []

2. Legen Sie Die Ordnerberechtigungen Fest
   a. Wählen Sie unter Ordnereigenschaften die Option *Sicherheit, >Erweitert > Vererbung deaktivieren*

      []

   b. Sie können die verbleibenden Einstellungen an die Einstellungen der ursprünglichen Storage-Ebene anpassen, die ursprünglich durch die Automatisierung der Implementierung erstellt wurden.

Verschieben von Daten

Verzeichnisse, Daten, Dateien und Sicherheitseinstellungen können auf verschiedene Arten verschoben werden. Die folgende robocopy-Syntax führt zu den erforderlichen Änderungen. Die Pfade müssen an Ihre Umgebung angepasst werden.

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

Umleitung des SMB-Pfads bei der Umstellung

Wenn der Zeitpunkt der Umstellung zu verkürzen ist, werden einige Änderungen alle Storage-Funktionen in der VDS-Umgebung umleiten.

Gruppenrichtlinienobjekte aktualisieren

1. Das Gruppenrichtlinienobjekt Benutzer (mit dem Namen *<company-Code>-Users*) muss mit dem neuen Freigabepfad aktualisiert werden. Wählen Sie *Benutzerkonfiguration* > *Windows-Einstellungen* > *Einstellungen* > *Laufwerkskarten*

   []

2. Klicken Sie mit der rechten Maustaste auf *H:*, wählen Sie Eigenschaften > Bearbeiten > Aktion: Ersetzen_, und geben Sie den neuen Pfad ein

   []

3. Mit Classic- oder Hybrid-AD-Update wird die Freigabe in ADUC in der Firma OU definiert. Dies spiegelt sich in der VDS-Ordnerverwaltung wieder.

   []

Aktualisieren der FSLogix-Profilpfade

1. Öffnen Sie Regedit auf dem ursprünglichen Dateiserver und allen anderen bereitgestellten Sitzungshosts.

   Dies kann bei Bedarf auch über eine GPO-Richtlinie festgelegt werden.

2. Bearbeiten Sie den Wert *VHDLocations* mit dem neuen Wert. Dies sollte der neue SMB Pfad plus *pro/profilecontainers* sein, wie in der Abbildung unten gezeigt.

   []

Aktualisieren Sie die Ordnerumleitungseinstellungen für die Home-Verzeichnisse

1. Open Group Policy Management, wählen Sie das Gruppenrichtlinienobjekt Benutzer aus, das mit DC=Domain,DC=mobi/Cloud Workspace/Cloud Workspace Companies/<company-Code>/<company-Code>-Desktop-Benutzer verknüpft ist.
2. Ordnerumleitungspfade bearbeiten unter Benutzerkonfiguration>Richtlinien>Windows-Einstellungen>Ordnerumleitung.
3. Nur Desktop und Dokumente müssen aktualisiert werden. Die Pfade sollten mit dem neuen SMB-Pfad-Bereitstellungspunkt für Home Volume übereinstimmen

   []

Aktualisieren Sie die VDS SQL-Datenbank mit Command Center

CWMGR1 enthält eine Hilfsprogramm-Anwendungen namens Command Center, die Bulk-Update der VDS-Datenbank kann.

So stellen Sie die endgültige Datenbank-Aktualisierung vor:

1. Stellen Sie eine Verbindung zu CWMGR1 her, navigieren Sie und führen Sie CommandCenter.exe aus

   []

2. Navigieren Sie zur Registerkarte *Operations*, klicken Sie auf *Daten laden*, um das Dropdown-Menü Company Code auszufüllen, wählen Sie den Unternehmenscode aus, und geben Sie die neuen Speicherpfade für die Speicherebene ein, und klicken Sie dann auf *Execute Command*.

   []

Umleitung der Storage-Plattform auf Azure Files

Überblick

Mithilfe von Bereitstellungstechnologien für Virtual Desktop Services können verschiedene Storage-Optionen genutzt werden, abhängig von der zugrunde liegenden Infrastruktur. In diesem Leitfaden wird beschrieben, wie Sie die Nutzung von Azure Files nach der Implementierung ändern.

Voraussetzungen

- AD Connect installiert und eingerichtet
- Globales Azure-Administratorkonto
- AZFilesHybrid PowerShell-Modul https://github.com/Azure-Samples/azure-files-samples/releases
- AZ PowerShell-Modul
- ActiveDirectory PowerShell-Modul

Erstellen Sie die neue Speicherebene

1. Melden Sie sich mit dem globalen Administratorkonto bei Azure an
2. Erstellen Sie ein neues Speicherkonto an demselben Speicherort und in derselben Ressourcengruppe wie der Arbeitsbereich

   []

3. Erstellen Sie die Daten-, Home- und Pro-File Shares unter dem Storage-Konto

   []

Einrichten Von Active Directory

1. Erstellen Sie unter Cloud Workspace > Cloud Worksapce Service Accounts OU eine neue Organisationseinheit mit dem Namen „`Storage Account`“

   []

2. Aktivieren der AD DS-Authentifizierung (muss mit PowerShell durchgeführt werden) https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-enable
   a. DomänenAccountType sollte sein “`ServiceLogonAccount`„
   b. OraganisierungalUnitDistinguishedName ist der im vorherigen Schritt erstellte Name der OU (d.h. “`OU=Storage Account,OU=Cloud Workspace Service Accounts,OU=Cloud`

`Workspace,DC=TrainingKrisG,DC=onmicrosoft,DC=com„`)

Legen Sie die Rollen für die Freigaben fest

1. Geben Sie im Azure-Portal „`Storage File Data SMB Share Elevated Contributor`“ die Rolle von CloudWorkspaceSVC und Level3-Technikern

   []

2. Dem wird die Rolle „Storage File Data SMB Share Contributor“ zugewiesen “`<company code>-all users`„-Gruppe“

   []

Erstellen Sie die Verzeichnisse

1. Erstellen Sie in jeder Freigabe ein Verzeichnis (Daten, Zuhause, pro), indem Sie den Unternehmenscode als Namen verwenden (in diesem Beispiel lautet der Unternehmenscode „`kift`“).

   []

2. Erstellen Sie im Verzeichnis <company Code> des Proshare ein Verzeichnis „`ProfilContainers`“

   []

Legen Sie die NTFS-Berechtigungen fest

1. Stellen Sie eine Verbindung zu den Freigaben her
   a. Navigieren Sie im Azure-Portal zu der Freigabe unter dem Storage-Konto, klicken Sie auf die drei Punkte und klicken Sie anschließend auf Verbinden

      []

   b. Wählen Sie die Methode Active Directory for Authentication aus, und klicken Sie in der rechten unteren Ecke des Codes auf das Symbol in die Zwischenablage kopieren

      []

   c. Melden Sie sich am CWMGR1-Server mit einem Konto an, das Mitglied der Level3-Technikergruppe ist
   d. Führen Sie den kopierten Code in PowerShell aus, um das Laufwerk zuzuordnen
   e. Führen Sie für jede Freigabe das gleiche aus, während Sie einen anderen Laufwerksbuchstaben für jeden auswählen
2. Deaktivieren Sie die Vererbung in den Verzeichnissen <company Code>
3. System und AD Group Client DHPAccess sollten die Verzeichnisse <company Code> vollständig steuern
4. Domain Computers sollten die volle Kontrolle über das Verzeichnis <company Code> im Pro-Share sowie das Verzeichnis ProfilContainers in haben
5. Die <company Code>-all Users AD Group sollte Listen Ordner/read Data permissons in den Verzeichnissen <company Code> im Home und pro Shares haben
6. Die AD-Gruppe <company Code>-all Users sollte die unten aufgeführten Sonderberechtigungen für das Verzeichnis in der Datenfreigabe besitzen

[]

7. Die AD-Gruppe <company Code>-all Users sollte über die Berechtigung Ändern im ProfilContainers-Verzeichnis verfügen

Gruppenrichtlinienobjekte Aktualisieren

1. Aktualisieren Sie das Gruppenrichtlinienobjekt <Unternehmenscode> Benutzer unter Cloud Workspace > Cloud Workspace Companies > <Company Code> <Company Code>-Desktop-Benutzer

   a. Ändern Sie die Zuordnung des Home-Laufwerks, um die neue Home-Freigabe zu zeigen

      []

   b. Ändern Sie die Ordnerumleitung, um die Home-Freigabe für Desktop und Dokumente zu zeigen

      []

   []

Aktualisieren Sie die Freigabe in Active Directory-Benutzern und -Computern

1. Bei klassischer oder hybrider AD muss der Anteil im Unternehmenscode OU auf den neuen Standort aktualisiert werden

   []

Aktualisieren von Daten-/Home-/Pro-Pfaden im VDS

1. Melden Sie sich bei CWMGR1 mit einem Konto in der Level3 Technicians Group an und starten Sie Command Center
2. Wählen Sie in der Dropdown-Liste Befehl die Option Daten/Home/Pro Ordner ändern aus
3. Klicken Sie auf die Schaltfläche Daten laden, und stellen Sie sicher, dass der richtige Unternehmenscode aus der Dropdown-Liste ausgewählt ist
4. Geben Sie die neue Patsh für die Daten-, Home- und pro-Standorte ein
5. Deaktivieren Sie das Kontrollkästchen IS Windows Server
6. Klicken Sie auf die Schaltfläche Befehl ausführen

   []

Aktualisieren der FSLogix-Profilpfade

1. Öffnen Sie den Registrierungseditiv auf den Session-Hosts
2. Bearbeiten Sie den Eintrag VHDLockations unter HKLM\SOFTWARE\FSLogix\Profiles, um den UNC-Pfad zum neuen ProfilContainers-Verzeichnis zu erhalten

   []

Backups Konfigurieren

1. Es wird empfohlen, eine Backup-Richtlinie für die neuen Freigaben einzurichten und zu konfigurieren
2. Erstellen Sie einen neuen Recovery Services Vault in derselben Ressourcengruppe
3. Navigieren Sie zum Tresor, und wählen Sie unter erste Schritte Sicherung aus
4. Wählen Sie Azure für den aktiven Workload und die Azure-Dateifreigabe für das, was Sie sichern möchten, und klicken Sie dann auf Backup
5. Wählen Sie das Speicherkonto aus, das zum Erstellen der Freigaben verwendet wird
6. Fügen Sie die Shares hinzu, die gesichert werden sollen
7. Bearbeiten und Erstellen einer Backup-Richtlinie, die Ihren Anforderungen entspricht

Überlegungen Zur Datenmigration

Überblick

Das Migrieren von Daten ist eine nahezu universelle Anforderung für die Migration zu einer beliebigen Cloud-Lösung. Während Administratoren für die Migration von Daten in ihre Virtual Desktops verantwortlich sind, steht NetApp aufgrund seiner Erfahrung für unzählige Kundenmigrationen im Einsatz. Bei der Virtual Desktop-Umgebung handelt es sich lediglich um eine gehostete Windows-Umgebung, sodass wahrscheinlich alle gewünschten Methoden unterstützt werden können.

Üblicherweise migrierte Daten:

- Benutzerprofile (Desktop, Dokumente, Favoriten usw.…)
- File Server-Freigaben
- Datenfreigaben (App-Daten, Datenbanken, Backup-Caches)

In der Virtual Desktop-Umgebung gibt es zwei primäre Orte, an denen Daten gespeichert und organisiert sind:

- Das Laufwerk Benutzer (normalerweise H:\): Dies ist das zugeordnete Laufwerk, das für jeden Benutzer sichtbar ist.
  - Dies wird wieder dem Pfad <DRIVE>:\Home\CustomerCode\user.name\ zugeordnet
  - Jeder Benutzer hat sein eigenes Laufwerk H:\ und kann keinen anderen Benutzer sehen
- Das freigegebene (typischerweise i:\) Laufwerk: Dies ist das freigegebene zugeordnete Laufwerk, das für alle Benutzer sichtbar ist
  - Dies wird dem Pfad <DRIVE>:\Data\CustomerCode\ zugeordnet
  - Alle Benutzer können auf dieses Laufwerk zugreifen. Ihre Zugriffsebene auf enthaltene Ordner/Dateien wird im Bereich Ordner von VDS verwaltet.

Generischer Migrationsprozess

1. Replizieren von Daten in die Cloud-Umgebung
2. Verschieben Sie die Daten auf den entsprechenden Pfad für die Laufwerke H:\ und I:\
3. Weisen Sie in der Virtual Desktop-Umgebung entsprechende Berechtigungen zu

FTPS-Transfers und -Überlegungen

Migration mit FTPS

1. Wenn die FTPS-Serverrolle während des CWA-Bereitstellungsprozesses aktiviert wurde, sammeln Sie FTPS-Anmeldeinformationen, indem Sie sich beim VDS anmelden, zu Berichten navigieren und den Master Client-Bericht für Ihr Unternehmen ausführen
2. Daten hochladen
3. Verschieben Sie die Daten auf den entsprechenden Pfad für die Laufwerke H:\ und I:\
4. Weisen Sie in der virtuellen Desktop-Umgebung über das Ordnermodul entsprechende Berechtigungen zu

> Bei der Übertragung von Daten über FTPS verhindert jede Unterbrechung, dass die Daten wie vorgesehen übertragen werden. Da die von Virtual Desktop Services gemanagten Server nachts neu gestartet werden, wird die standardmäßige Übertragungsstrategie über Nacht wahrscheinlich unterbrochen. Administratoren können den Migrationsmodus aktivieren, sodass die VMs nicht mehr für eine Woche neu gestartet werden können.

Die Aktivierung des Migrationsmodus ist einfach: Navigieren Sie zur Organisation, scrollen Sie dann zum Abschnitt Virtual Desktop Settings und aktivieren Sie das Kontrollkästchen für den Migrationsmodus, und klicken Sie dann auf Update.

> NetApp empfiehlt Administratoren die Aktivierung einer Compliance-Einstellung, die Unternehmen bei der Einhaltung von PCI-, HIPAA- und NIST-Kontrollen unterstützt, indem sie Gateways der Bereitstellung usw. härten. Dadurch wird auch die standardmäßige FTP-Server-Rolle, sofern aktiviert, von der Annahme unverschlüsselter Standardübertragungen über Port 21 deaktiviert. FileZilla erlaubt SFTP nicht, was bedeutet, dass Verbindungen mit FTPS über Port 990 hergestellt werden sollten.

Um diese Einstellung zu aktivieren, stellen Sie eine Verbindung zu CWMGR1 her, navigieren Sie zum Programm CwVmAutomationService und aktivieren Sie dann die PCI v3-Konformität.

Synchronisierung von Tools und Überlegungen

Enterprise File Sync and Share, das häufig als EFSS- oder Sync-Tools bezeichnet wird, kann besonders bei der Datenmigration von Nutzen sein, da das Tool Änderungen auf beiden Seiten bis zur Umstellung erfasst. Tools wie OneDrive, das mit Office 365 kommt, können Ihnen helfen, Dateiserver-Daten zu synchronisieren. Es ist auch nützlich für VDI-Benutzer-Bereitstellungen als auch, wo es eine 1:1-Beziehung zwischen dem Benutzer und der VM, solange der Benutzer nicht versucht, gemeinsam genutzte Inhalte auf ihren VDI-Server zu synchronisieren, wenn gemeinsam genutzte Daten einmal auf die Shared bereitgestellt werden (typischerweise I:\) Antrieb für das gesamte Unternehmen. Migration von SQL und ähnlichen Daten (Open Files)

Offene Dateien werden von gängigen Sync- und/oder Migrationslösungen nicht übertragen, darunter folgende Dateitypen:

- Mailbox-Dateien (.ost)
- QuickBooks-Dateien
- Microsoft Access-Dateien
- SQL Datenbanken

Das heißt, wenn ein einzelnes Element der gesamten Datei (z.B. 1 neue E-Mail) oder Datenbank (1 neuer

Datensatz wird in das System einer App eingegeben) erscheint, dann ist die gesamte Datei anders und Standard-Sync-Tools (z.B. Dropbox) Werden annehmen, dass es eine völlig neue Datei ist und erneut verschoben werden muss. Auf Wunsch stehen spezielle Tools für den Kauf bei Drittanbietern zur Verfügung.

Eine weitere häufige Vorgehensweise bei diesen Migrationen ist der Zugriff auf VAR-Mitarbeiter von Drittanbietern, die häufig den Import/Export von Datenbanken optimiert haben.

Frachtfestplatten

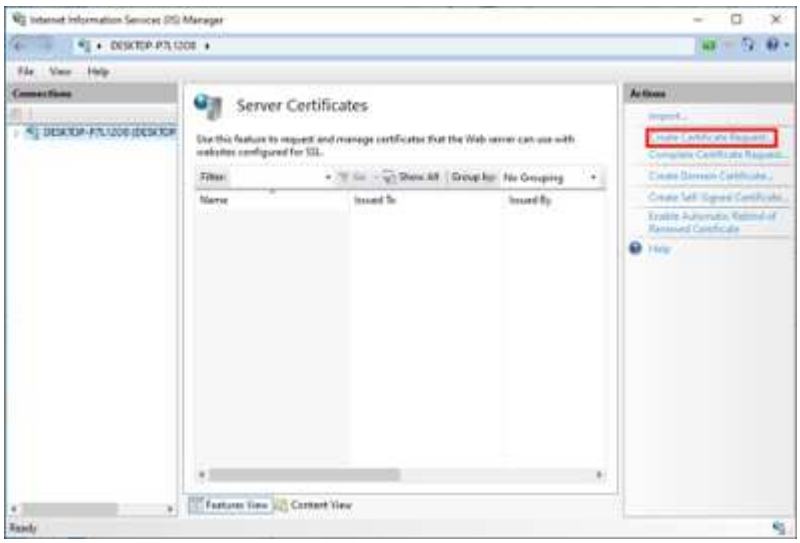
Viele Datacenter Provider senden keine Festplatten mehr an – entweder diese oder Sie müssen ihre spezifischen Richtlinien und Verfahren befolgen.

Microsoft Azure ermöglicht Unternehmen die Nutzung von Azure Data Box, zu denen Administratoren von der Koordinierung mit ihren Microsoft Vertretern profitieren können.

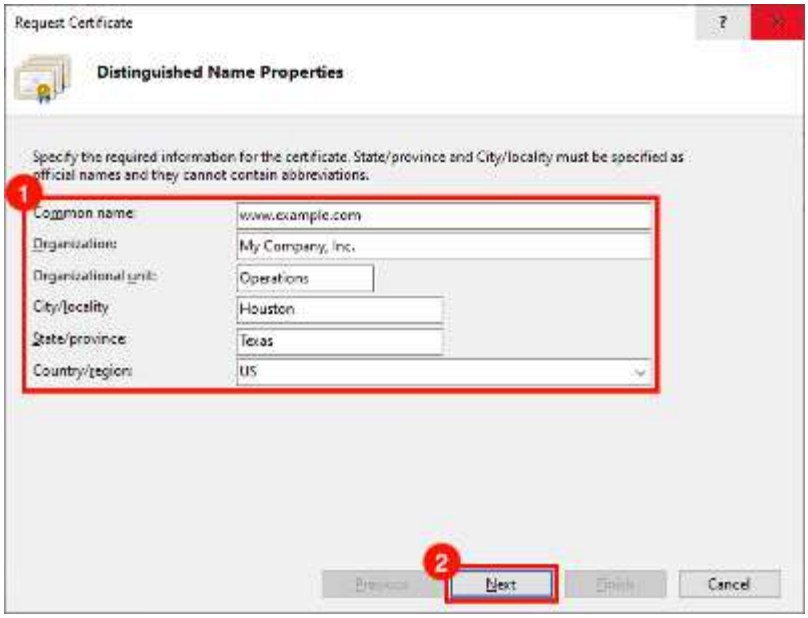
Verlängerung des Platzhalter-SSL-Zertifikats

Zertifikatsignierungsanforderung (CSR) erstellen:

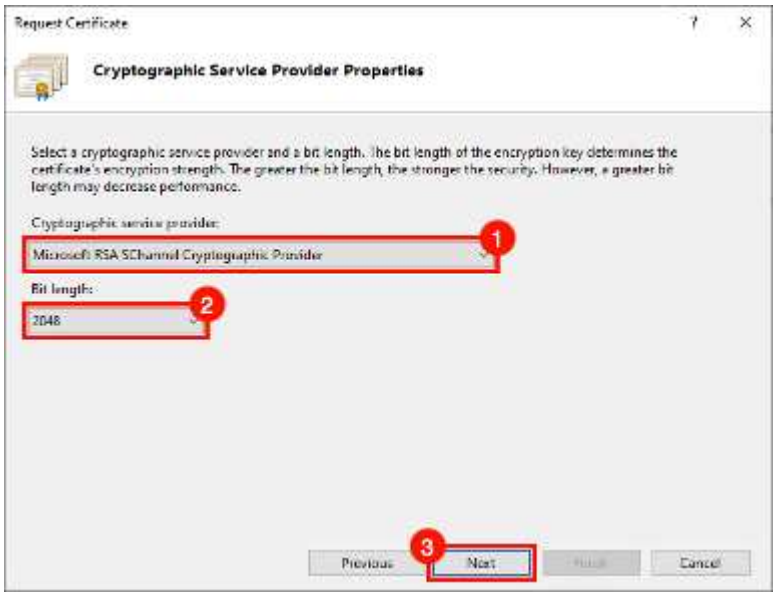
1. Stellen Sie eine Verbindung zu CWMGR1 her
2. Öffnen Sie IIS Manager über Administrator-Tools
3. Wählen Sie CWMGR1 und öffnen Sie Server Certificates
4. Klicken Sie im Bereich Aktionen auf Zertifikatanforderung erstellen



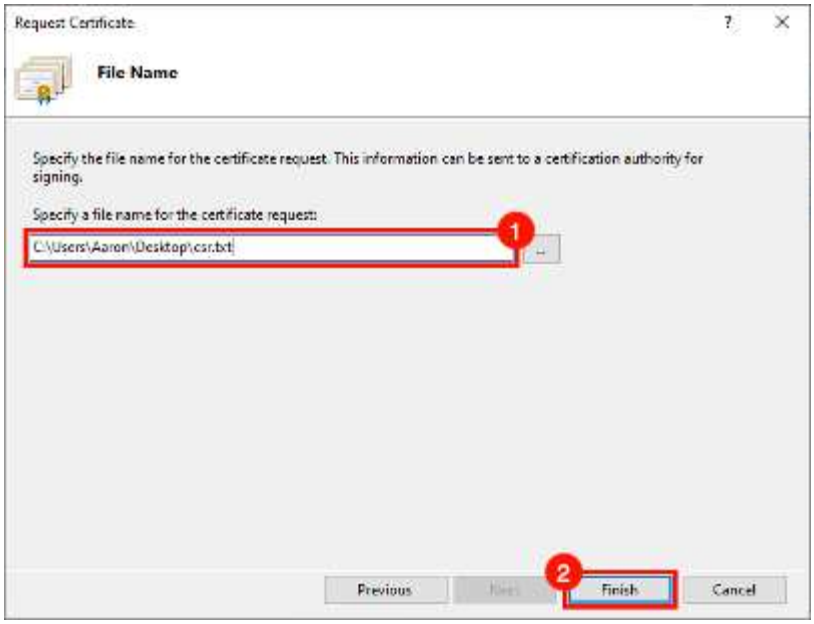
5. Geben Sie die Distinguished Name Properties im Assistenten für das Anforderungszertifikat ein, und klicken Sie auf Weiter:
   a. Allgemeiner Name: FQDN des Platzhalters - *.domain.com
   b. Organisation: Der gesetzlich registrierte Name Ihrer Firma
   c. Organisationseinheit: ‘Funktioniert gut
   d. Stadt: Stadt, in der die Firma liegt
   e. Staat: Geben Sie an, wo die Firma ansässig ist
   f. Land: Land, in dem die Firma ansässig ist



6. Überprüfen Sie auf der Seite Eigenschaften von Cryptographic Service Provider, ob das folgende angezeigt wird, und klicken Sie auf Weiter:



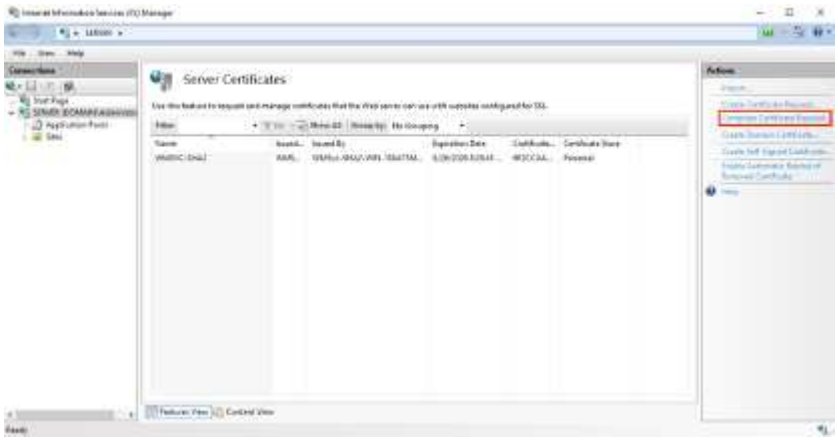
7. Geben Sie einen Dateinamen an, und suchen Sie nach einem Speicherort, an dem Sie den CSR speichern möchten. Wenn Sie keinen Speicherort angeben, befindet sich der CSR in C:\Windows\System32:



8. Klicken Sie auf Fertig stellen. Sie verwenden diese Textdatei, um Ihre Bestellung an die Zertifikatregistrierung zu senden
9. Wenden Sie sich an den Registrar-Support, um einen neuen Wildcard SSL für Ihr Zertifikat zu kaufen: *.domain.com
10. Speichern Sie nach dem Erhalt Ihres SSL-Zertifikats die SSL-Zertifikat .cer-Datei an einem Speicherort auf CWMGR1 und folgen Sie den folgenden Schritten.

Installieren und Konfigurieren von CSR:

1. Stellen Sie eine Verbindung zu CWMGR1 her
2. Öffnen Sie IIS Manager über Administrator-Tools
3. Wählen Sie CWMGR1 und öffnen Sie ‘SServer Certificates’
4. Klicken Sie im Bereich Aktionen auf Zertifikatanforderung abschließen



5. Füllen Sie die folgenden Felder in der vollständigen Zertifikatanforderung aus, und klicken Sie auf OK:

a. Dateiname: Wählen Sie die zuvor gespeicherte .cer-Datei aus

b. Anzeigename: *.domain.com

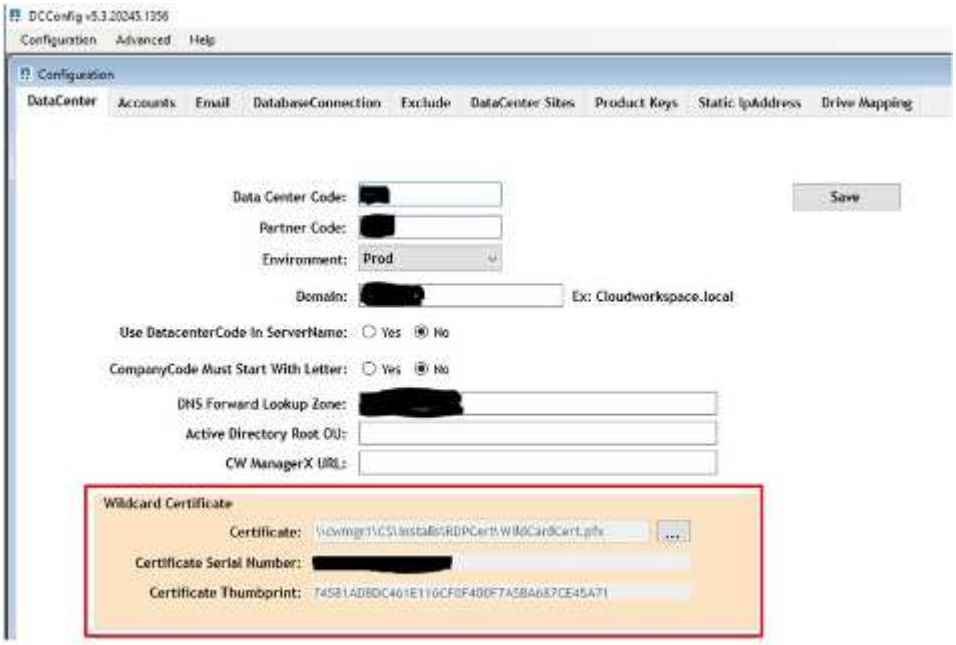
c. Zertifikatspeicher: Wählen Sie entweder Webhosting oder Personal

SSL-Zertifikat wird zugewiesen:

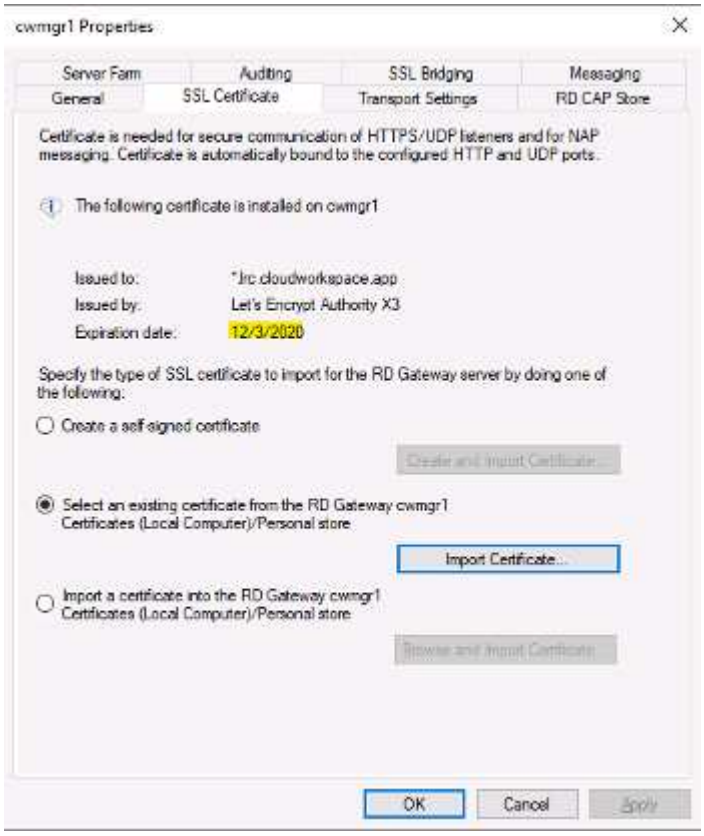
1. Vergewissern Sie sich, dass der Migrationsmodus nicht aktiviert ist. Diese finden Sie auf der Seite Arbeitsbereichsübersicht unter Sicherheitseinstellungen in VDS.

2. Stellen Sie eine Verbindung zu CWMGR1 her
3. Öffnen Sie IIS Manager über Administrator-Tools
4. Wählen Sie CWMGR1 und öffnen Sie ‘SServer Certificates’
5. Klicken Sie im Aktionsbereich auf Exportieren
6. Exportieren Sie das Zertifikat im .pfx-Format
7. Erstellen Sie ein Passwort. Speichern Sie das Kennwort so, wie es benötigt wird, um die .pfx-Datei in Zukunft zu importieren oder erneut zu verwenden
8. Speichern Sie die .pfx-Datei im Verzeichnis C:\installiert\RDPcert
9. Klicken Sie auf OK, und schließen Sie IIS Manager

10. Öffnen Sie DCConfig
11. Aktualisieren Sie unter Platzhalterzertifikat den Zertifikatspfad in die neue .pfx-Datei
12. Geben Sie bei der entsprechenden Aufforderung das .pfx-Passwort ein
13. Klicken Sie Auf Speichern



14. Wenn das Zertifikat 30 Tage länger gültig ist, kann die Automatisierung das neue Zertifikat während der morgendlichen täglichen Aktionen während der Woche anwenden
15. Überprüfen Sie regelmäßig die Plattformserver, um zu überprüfen, ob das neue Zertifikat sich verbreitet hat. Benutzerverbindung validieren und testen, um zu bestätigen
    a. Wechseln Sie auf dem Server zu Admin Tools
    b. Wählen Sie Remote Desktop Services > Remote Desktop Gateway Manager
    c. Klicken Sie mit der rechten Maustaste auf den Namen des Gateway-Servers, und wählen Sie Eigenschaften. Klicken Sie auf die Registerkarte SSL-Zertifikat, um das Ablaufdatum zu überprüfen

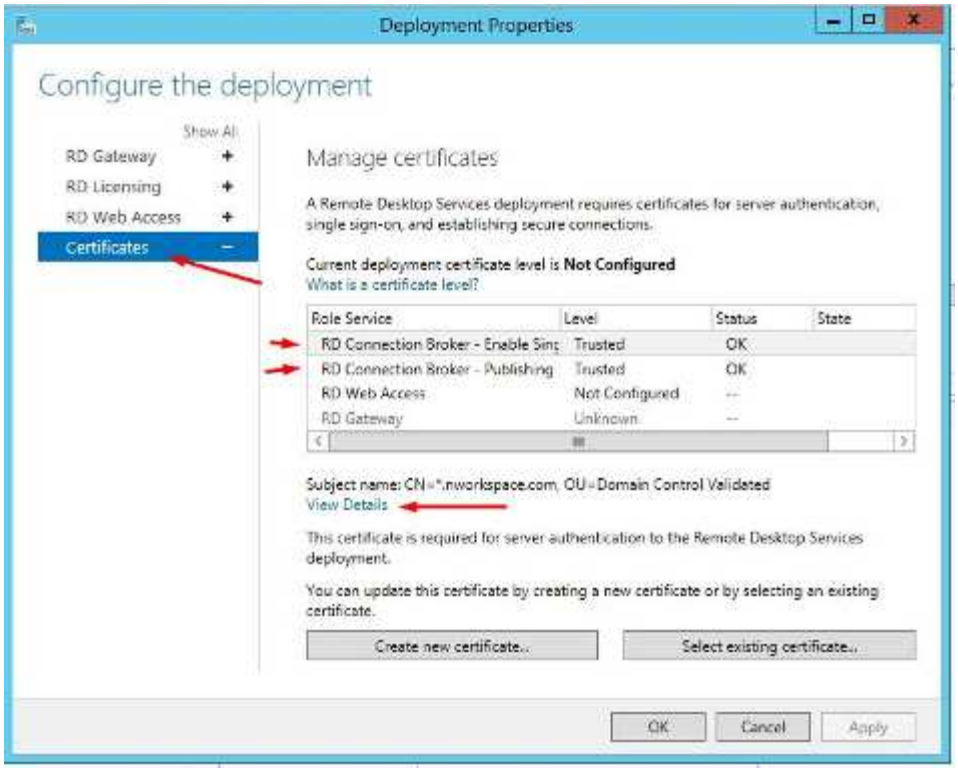


16. Überprüfen Sie regelmäßig die Client-VMs, auf denen die Connection Broker-Rolle ausgeführt wird

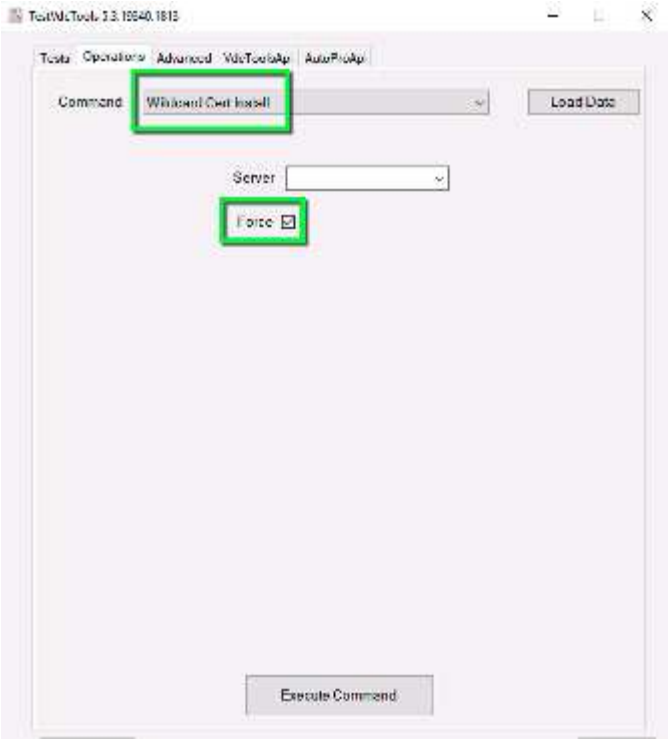
    a. Wechseln Sie zu Server Manager > Remote Desktop Services

    b. Wählen Sie unter Bereitstellungsübersicht die Dropdown-Liste Aufgaben aus, und wählen Sie die Option Bereitstellungseigenschaften bearbeiten

    c. Klicken Sie auf Zertifikate, wählen Sie Zertifikat aus und klicken Sie auf Details anzeigen. Das Ablaufdatum wird aufgelistet.



17. Wenn Sie weniger als 30 Tage oder lieber das neue Zertifikat sofort ausdrucken möchten, erzwingen Sie das Update mit TestVdcTools. Dies sollte während eines Wartungsfensters erfolgen, da die Verbindung für alle angemeldeten Benutzer unterbrochen wird und Ihre Verbindung zu CWMGR1 verloren geht.
    a. Gehen Sie zu C:\Programme\CloudWorkspace\TestVdcTools, klicken Sie auf die Registerkarte Operationen und wählen Sie den Befehl Platzhalter Cert-Install aus
    b. Lassen Sie das Serverfeld leer
    c. Aktivieren Sie das Kontrollkästchen Kraft
    d. Klicken Sie Auf Befehl Ausführen
    e. Überprüfen Sie, ob Zertifikatpropagiert mit den oben aufgeführten Schritten ausgeführt wird



AVD-Rückführung

Überblick

In diesem Artikel werden das Entfernen von VDS und der NetApp Steuerung unter Beibehaltung des AVD-Benutzerzugriffs behandelt. Und in Zukunft wäre das Management mit nativen Azure/Windows-Administrationstools. Nach Abschluss dieses Vorgangs wird empfohlen, sich an support@spotpc.netapp.com zu wenden, damit NetApp unsere Back-End- und Billing-Systeme bereinigen kann.

Ausgangszustand

- AVD-Bereitstellung
- TDS1 ist FS Logix FileShare
- TS1 ist Session-Host
- Benutzer ist angemeldet und FS Logix-Datenträger wurde erstellt in:

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

CW Agent-Dienst löschen

Der CW-Agent wird auf allen Maschinen in der Umgebung ausgeführt. Der Dienst, der diesen Prozess startet, sollte mit dem folgenden Befehl für jede VM in der Umgebung deinstalliert werden. CWMGR1 kann übersprungen werden, da die VM heruntergefahren und schließlich in den meisten Fällen gelöscht wird. Im Idealfall würde diese Aktion über skriptbasierte Automatisierung ausgeführt. Das Video unten zeigt, dass es manuell gemacht wurde.

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

Löschen Sie das Video zum CW Agent-Dienst

[] | *https://img.youtube.com/vi/l9ASmM5aap0/maxresdefault.jpg*

Löschen Sie das CW-Agentenverzeichnis

Bei der vorherigen Deinstallation wurde der Dienst entfernt, der CW Agent startet, die Dateien aber verbleiben. Löschen Sie das Verzeichnis:

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

CW Agent-Verzeichnisvideo löschen

[] | *https://img.youtube.com/vi/hMM_z4K2-il/maxresdefault.jpg*

Entfernen Sie Startverknüpfungen

Das Verzeichnis der Startelemente enthält zwei Verknüpfungen zu Dateien, die im vorherigen Schritt gelöscht wurden. Um Fehlermeldungen für Endbenutzer zu vermeiden, sollten diese Dateien gelöscht werden.

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

Entfernen Sie Startverknüpfungen Video

[] | *https://img.youtube.com/vi/U0YLZ3Qfu9w/maxresdefault.jpg*

Link ‘Benutzer’ und ‘Unternehmen’ GPOs aufheben

VDS implementiert drei Gruppenrichtlinienobjekte. Wir empfehlen die Verknüpfung von zwei von ihnen und die Überprüfung des Inhalts der dritten.

Link Aufheben:

- ADDC-Benutzer > Cloud Workspace-Unternehmen
- ADDC-Benutzer > Cloud Workspace-Benutzer

Durchsehen:

- ADDC-Computer > Cloud Workspace-Computer

Link ‘Benutzer’ und ‘Unternehmen’ GPOs-Video aufheben

[] | *https://img.youtube.com/vi/cb68ri3HKUw/maxresdefault.jpg*

Schalten Sie den CWMGR1 aus

Mit den vorgenommenen Änderungen am Gruppenrichtlinienobjekt können wir die CWMGR1 VM jetzt herunterfahren. Sobald die fortgesetzte AVD-Funktion bestätigt wurde, kann diese VM dauerhaft gelöscht werden.

In extrem seltenen Fällen muss diese VM gewartet werden, wenn eine andere Serverrolle läuft (z.B. DC, FTP-Server…). In diesem Fall können drei Dienste deaktiviert werden, um die VDS-Funktion auf CWMGR1 zu deaktivieren:

- CW-Agent (siehe oben)
- CW Automation Service
- CW VM Automation

CWMGR1-Video herunterfahren

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

Löschen von NetApp VDS-Servicekonten

Die von VDS verwendeten Azure AD-Servicekonten können entfernt werden. Melden Sie sich im Azure Management-Portal an und löschen Sie die Benutzer:

- CloudWorkSpaceSVC
- CloudWorkSpaceCASVC

Andere Benutzerkonten können beibehalten werden:

- Endanwender
- Azure-Administrator
- .Tech Domain-Administratoren

Video zum Löschen von VDS-Servicekonten für NetApp

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

App-Registrierungen löschen

Bei der Bereitstellung von VDS werden zwei App-Registrierungen durchgeführt. Diese können gelöscht werden:

- Cloud Workspace-API
- Cloud Workspace AVD

Video zum Löschen von App-Registrierungen

[] | *https://img.youtube.com/vi/iARz2nw1Oks/maxresdefault.jpg*

Unternehmensanwendungen löschen

Bei der Implementierung von VDS werden zwei Enterprise-Applikationen implementiert. Diese können gelöscht

werden:

- Cloud Workspace
- Cloud Workspace Management-API

Video zu Unternehmensanwendungen löschen

[] | *https://img.youtube.com/vi/3eQzTPdilWk/maxresdefault.jpg*

Bestätigen Sie, dass CWMGR1 angehalten wurde

Bevor Sie testen, ob die Endbenutzer noch eine Verbindung herstellen können, bestätigen Sie, dass der CWMGR1 für einen realistischen Test angehalten wurde.

Bestätigen Sie, dass das Video „CWMGR1 wurde angehalten“ wurde

[] | *https://img.youtube.com/vi/Ux9nkDk5IU4/maxresdefault.jpg*

Anmeldung und Endbenutzer

Um den Erfolg zu bestätigen, melden Sie sich als Endbenutzer an und bestätigen Sie, dass die Funktionalität erhalten bleibt.

Anmeldung und Endbenutzervideo

[] | *https://img.youtube.com/vi/SuS-OTHJz7Y/maxresdefault.jpg*