



Architecture

Virtual Desktop Service

NetApp
January 03, 2023

This PDF was generated from https://docs.netapp.com/fr-fr/virtual-desktop-service/Architectural.change_data_layer.Azure_Files.html on January 03, 2023. Always check docs.netapp.com for the latest.

Table des matières

- Architecture 1
 - Redirection de la plateforme de stockage 1
 - Considérations relatives à la migration des données. 6
 - Processus de renouvellement de certificat SSL générique 8
 - Guide de démontage AVD 15

Architecture

Redirection de la plateforme de stockage

Présentation

Les technologies de déploiement des services de postes de travail virtuels offrent de nombreuses options de stockage en fonction de l'infrastructure sous-jacente. Ce guide explique comment procéder à des modifications après le déploiement.

La performance des postes de travail virtuels dépend de diverses ressources clés, la performance du stockage est l'une des principales variables. Or, à mesure que les exigences évoluent et que les charges de travail évoluent, l'infrastructure de stockage doit être modifiée. Dans la plupart des cas, cela implique de migrer d'une plateforme de serveur de fichiers vers une technologie de stockage NetApp (comme Azure NetApp Files, NetApp Cloud Volumes Service dans Google ou NetApp Cloud Volumes ONTAP dans AWS), car ces technologies offrent généralement le profil de performances le plus adapté aux environnements d'end-user computing.

Création de la nouvelle couche de stockage

Compte tenu de la grande variété de services de stockage potentiels couvrant une large gamme de fournisseurs de solutions d'infrastructure cloud et HCI, ce guide suppose qu'un nouveau service de stockage a déjà été mis en place et que les chemins d'accès SMB connaissent bien.

Créer des dossiers de stockage

1. Dans le nouveau service de stockage, créez trois dossiers :

- /Données
- /Accueil
- /Pro

[]

2. Définir les autorisations de dossier

a. Dans Propriétés du dossier, sélectionnez *Security*, > *Avancé* > *Désactiver l'héritage*

[]

b. Ajustez les paramètres restants selon les paramètres de la couche de stockage d'origine créés par l'automatisation du déploiement.

Déplacement des données

Les répertoires, données, fichiers et paramètres de sécurité peuvent être déplacés de différentes façons. La syntaxe robocopy suivante permet d'effectuer les modifications nécessaires. Les chemins doivent être modifiés selon votre environnement.

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

Redirection du chemin SMB au moment de la mise en service

Au moment de la mise en service, quelques modifications rediriger toutes les fonctionnalités de stockage dans l'environnement VDS.

Mettre à jour les stratégies de groupe

1. La stratégie de groupe des utilisateurs (nommée *<code de société>-utilisateurs*) doit être mise à jour avec le nouveau chemin de partage. Sélectionnez *Configuration utilisateur > Paramètres Windows > Préférences > cartes de lecteur*

[]

2. Cliquez avec le bouton droit de la souris sur *H:*, sélectionnez *Propriétés > Modifier > action : remplacer* et entrez le nouveau chemin

[]

3. Avec AD classique ou hybride, mettez à jour le partage défini dans ADUC dans l'UO de l'entreprise. Ceci est reflété dans la gestion des dossiers VDS.

[]

Mettre à jour les chemins de profil FSLogix

1. Ouvrez Regedit sur le serveur de fichiers d'origine et sur tout autre hôte de session provisionné.



Ceci peut également être défini via une stratégie GPO si vous le souhaitez.

2. Modifiez la valeur *VHDlocations* avec la nouvelle valeur. Ce devrait être le nouveau chemin SMB plus *pro/profilisecondes* comme indiqué dans la capture d'écran ci-dessous.

[]

Mettez à jour les paramètres de redirection de dossier pour les répertoires d'accueil

1. Open Group Policy Management, Select Users GPO liés à DC=domain, DC=mobi/Cloud Workspace/Cloud Workspace Companies/<code entreprise><code entreprise> utilisateurs de postes de travail.
2. Modifier les chemins de redirection de dossier sous *Configuration utilisateur> stratégies> Paramètres Windows> Redirection de dossiers*.
3. Seuls les postes de travail et les documents doivent être mis à jour et les chemins doivent correspondre au nouveau point de montage du chemin SMB pour le volume domestique

[]

Mettre à jour la base de données SQL VDS avec le Centre de commande

CWMGR1 contient un utilitaire d'aide appelé Command Center qui peut mettre à jour la base de données VDS en bloc.

Pour effectuer les mises à jour finales de la base de données :

1. Connectez-vous à CWMGR1, naviguez et exécutez CommandCenter.exe

[]

2. Accédez à l'onglet *Operations*, cliquez sur *Load Data* pour remplir le menu déroulant Company Code (Code de société), sélectionnez le code de société et entrez les nouveaux chemins de stockage pour la couche de stockage, puis cliquez sur *Execute Command*.

[]

Redirection de la plateforme de stockage vers Azure Files

Présentation

Les technologies de déploiement des services de postes de travail virtuels offrent de nombreuses options de stockage en fonction de l'infrastructure sous-jacente. Ce guide explique comment modifier l'utilisation d'Azure Files après le déploiement.

Conditions préalables

- AD Connect installé et configuré
- Compte d'administrateur global Azure
- Module PowerShell AZFilesHybrid <https://github.com/Azure-Samples/azure-files-samples/releases>
- Module AZ PowerShell
- Module PowerShell ActiveDirectory

Créer la nouvelle couche de stockage

1. Connectez-vous à Azure avec le compte d'administrateur global
2. Créez un nouveau compte de stockage dans le même emplacement et le même groupe de ressources que l'espace de travail

[]

3. Créez les partages de fichiers de données, d'accueil et professionnels sous le compte de stockage

[]

Configurer Active Directory

1. Créez une nouvelle unité organisationnelle nommée « compte de stockage » sous Cloud Workspace > Cloud Worksapce Service Accounts ou

[]

2. Activer l'authentification AD DS (obligatoire à l'aide de PowerShell) <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-enable>
 - a. DomainAccountType doit être de "ServiceLogonAccount"
 - b. OraganationalUnitDistinguishedName est le nom distinctif de l'UO créée à l'étape précédente (c'est-à-dire "OU=Storage Account,OU=Cloud Workspace Service Accounts,OU=Cloud Workspace,DC=TrainingKrisG,DC=onmicrosoft,DC=com")

Définissez les rôles des partages

1. Sur le portail Azure, donnez au technicien CloudWorkspaceSVC et Level3 le rôle « en partage de données SMB de stockage »

[]

2. Donnez le rôle « Storage File Data SMB Share Contributor » au “<company code>-all users`groupe ”

[]

Créez les répertoires

1. Créer un répertoire dans chaque partage (données, domicile, pro) en utilisant le code de société comme nom (dans cet exemple, le code de société est « kift »)

[]

2. Dans le répertoire <code entreprise> du partage pro, créez un répertoire "profileContainers"

[]

Définissez les autorisations NTFS

1. Connectez-vous aux partages

- a. Accédez au partage sous le compte de stockage sur le portail Azure, cliquez sur les trois points, puis cliquez sur connecter

[]

- b. Choisissez la méthode d'authentification Active Directory et cliquez sur l'icône Copier dans le presse-papiers dans le coin inférieur droit du code

[]

- c. Connectez-vous au serveur CWMGR1 avec un compte membre du groupe de techniciens Level3

- d. Exécutez le code copié dans PowerShell pour mapper le lecteur

- e. Faites de même pour chaque partage en choisissant une lettre de lecteur différente pour chaque partage

2. Désactivez l'héritage sur les répertoires <code entreprise>

3. System et AD Group ClientDHPAccess doivent disposer d'un contrôle total des répertoires <Company code>

4. Les ordinateurs de domaine doivent disposer d'un contrôle total du répertoire <code entreprise> dans le partage professionnel ainsi que du répertoire ProfileContainers dans




5. Le groupe AD de <code de l'entreprise>-tous les utilisateurs doivent avoir des données de lecture/dossier de liste permissions vers les répertoires de <code de l'entreprise> dans les partages home et pro

6. Le groupe AD <Company code>-All Users doit disposer des autorisations spéciales ci-dessous pour le répertoire dans le partage de données


[]

7. Le groupe AD <code société>-tous les utilisateurs doit disposer de l'autorisation Modifier dans le répertoire ProfileContainers


Mettre à jour les objets de stratégie de groupe

1. Mettre à jour cette stratégie <code entreprise> utilisateurs situés sous Cloud Workspace > Cloud Workspace Entreprises > <code entreprise> <code entreprise>-utilisateurs de postes de travail
 - a. Modifiez le mappage du lecteur de base pour pointer le nouveau partage de base

 - b. Modifiez la redirection de dossiers pour pointer le partage d'accueil pour le bureau et les documents

- 


Mettez à jour le partage dans les utilisateurs et les ordinateurs Active Directory

1. Avec AD classique ou hybride, le partage dans l'UO de code de l'entreprise doit être mis à jour vers le nouvel emplacement


Mettre à jour les chemins Data/Home/Pro dans VDS

1. Connectez-vous à CWMGR1 avec un compte du groupe de techniciens Level3 et lancez Command Center
2. Dans la liste déroulante commande, sélectionnez Modifier les données/Accueil/dossiers Pro
3. Cliquez sur le bouton Charger les données, puis assurez-vous que le code de société approprié est sélectionné dans le menu déroulant
4. Saisissez le nouveau path pour les emplacements de données, de domicile et de pro
5. Décochez la case est Windows Server
6. Cliquez sur le bouton Exécuter la commande


Mettre à jour les chemins de profil FSLogix

1. Ouvrez le registre edtory sur les hôtes de session
2. Modifiez l'entrée VHDLocations dans HKLM\SOFTWARE\FSLogix\Profiles pour qu'elle soit le chemin UNC vers le nouveau répertoire ProfileContainers


Configurez les sauvegardes

1. Il est recommandé d'installer et de configurer une stratégie de sauvegarde pour les nouveaux partages
2. Créez un nouveau coffre-fort de services de récupération dans le même groupe de ressources
3. Naviguez jusqu'au coffre-fort et sélectionnez sauvegarde sous mise en route

4. Choisissez Azure où la charge de travail s'exécute et le partage de fichiers Azure pour ce que vous voulez sauvegarder, puis cliquez sur Backup
5. Sélectionnez le compte de stockage utilisé pour créer les partages
6. Ajoutez les partages à sauvegarder
7. Modifiez et créez une stratégie de sauvegarde qui répond à vos besoins

Considérations relatives à la migration des données

Présentation

La migration des données est une exigence quasi universelle lors de la migration vers une solution cloud de tout type. Les administrateurs sont responsables de la migration des données vers leurs postes de travail virtuels, mais l'expérience de NetApp est disponible et elle s'avère extrêmement précieuse pour d'innombrables migrations client. L'environnement de postes de travail virtuels est tout simplement un environnement Windows hébergé, et toute méthode souhaitée peut probablement être prise en charge.

Données généralement migrées :

- Profils utilisateur (Bureau, documents, Favoris, etc.)
- Partages de serveur de fichiers
- Partages de données (données d'application, bases de données, caches de sauvegarde)

L'environnement de postes de travail virtuels comporte deux emplacements principaux où les données sont stockées et organisées :

- Le lecteur utilisateur (généralement H:\) : il s'agit du lecteur mappé visible pour chaque utilisateur.
 - Ceci est mappé sur le chemin <LECTEUR>:\home\CustomerCode\user.name\
 - Chaque utilisateur dispose de son propre lecteur H:\ et ne peut pas voir un autre utilisateur
- Lecteur partagé (généralement i:\) : il s'agit du lecteur mappé partagé visible pour tous les utilisateurs
 - Ceci est renvoyé au chemin <LECTEUR>:\data\CustomerCode\
 - Tous les utilisateurs peuvent accéder à ce lecteur. Leur niveau d'accès aux dossiers/fichiers contenus est géré dans la section dossiers de VDS.

Processus de migration générique

1. Réplication des données dans l'environnement cloud
2. Déplacez les données vers le chemin approprié pour les lecteurs H:\ et i:\
3. Attribuez les autorisations appropriées dans l'environnement de bureau virtuel

Transferts FTPS et considérations

Migration avec FTPS

1. Si le rôle de serveur FTPS a été activé pendant le processus de déploiement CWA, rassemblez les informations d'identification FTPS en vous connectant à VDS, en accédant aux rapports et en exécutant le rapport client principal de votre organisation
2. Charger les données
3. Déplacez les données vers le chemin approprié pour les lecteurs H:\ et i:\

4. Attribuez les autorisations appropriées dans l'environnement Virtual Desktop via le module dossiers



Lors du transfert de données via FTPS, toute interruption empêche le transfert des données comme prévu. Étant donné que les serveurs gérés par Virtual Desktop Services sont redémarrés chaque nuit, la stratégie standard de transmission de nuit sera probablement interrompue. Pour contourner ce problème, les administrateurs peuvent activer le mode migration pour empêcher le redémarrage des ordinateurs virtuels pendant une semaine.

L'activation du mode migration est simple : accédez à l'organisation, faites défiler vers le bas jusqu'à la section Paramètres du bureau virtuel et cochez la case mode migration, puis cliquez sur mettre à jour.



NetApp recommande aux administrateurs d'activer un paramètre de conformité qui aide les entreprises à respecter les contrôles PCI, HIPAA et NIST via le renforcement des passerelles du déploiement, etc. Il n'autorise pas non plus le rôle de serveur FTP par défaut, si activé, d'accepter les transmissions non chiffrées par défaut via le port 21. FileZilla n'autorise pas SFTP, ce qui signifie que les connexions doivent être effectuées à l'aide de FTPS sur le port 990.

Pour activer ce paramètre, connectez-vous à CWMGR1 et accédez au programme CwVmAutomationService, puis activez la conformité PCI v3.

Outils de synchronisation et considérations

La synchronisation et le partage de fichiers d'entreprise, souvent appelés outils EFSS ou de synchronisation, peuvent s'avérer extrêmement utiles pour la migration des données. En effet, l'outil permet d'enregistrer les modifications de chaque côté jusqu'à la mise en service. Des outils comme OneDrive, fourni avec Office 365, peuvent vous aider à synchroniser les données des serveurs de fichiers. Elle s'avère également utile pour les déploiements d'utilisateurs VDI, où il existe une relation 1:1 entre l'utilisateur et la machine virtuelle, tant que l'utilisateur n'essaie pas de synchroniser du contenu partagé sur son serveur VDI lorsque des données partagées peuvent être déployées une fois sur le serveur partagé (en général, l:\) les besoins de l'ensemble de l'entreprise. Migration de SQL et de données similaires (fichiers ouverts)

Les solutions courantes de synchronisation et/ou de migration ne transfèrent pas de fichiers ouverts, ce qui comprend les types de fichiers suivants :

- Fichiers de boîte aux lettres (.ost)
- Fichiers QuickBooks
- Fichiers Microsoft Access
- Les bases de données SQL

Cela signifie que si un seul élément de l'ensemble du fichier (1 nouvel e-mail apparaît, par exemple) ou de la base de données (1 nouvel enregistrement est entré dans le système d'une application), l'ensemble du fichier est différent et les outils de synchronisation standard (Dropbox, par exemple) je pense qu'il s'agit d'un fichier entièrement nouveau et qu'il doit être redéplacé. Au besoin, des outils spécialisés peuvent être achetés auprès de fournisseurs tiers.

L'accès à un VAR tiers est souvent rationalisé et destiné à importer/exporter des bases de données.

Disques d'expédition

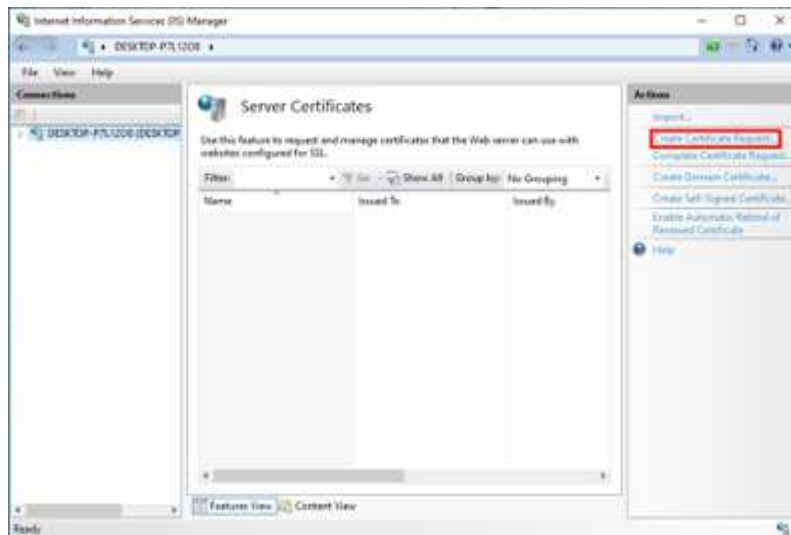
De nombreux fournisseurs de data centers n'ont plus de disques durs à expédier, c'est-à-dire, ou ils exigent que vous respectiez leurs règles et procédures spécifiques.

Microsoft Azure permet aux entreprises d'utiliser Azure Data Box, dont les administrateurs peuvent bénéficier en assurant la coordination avec leurs représentants Microsoft.

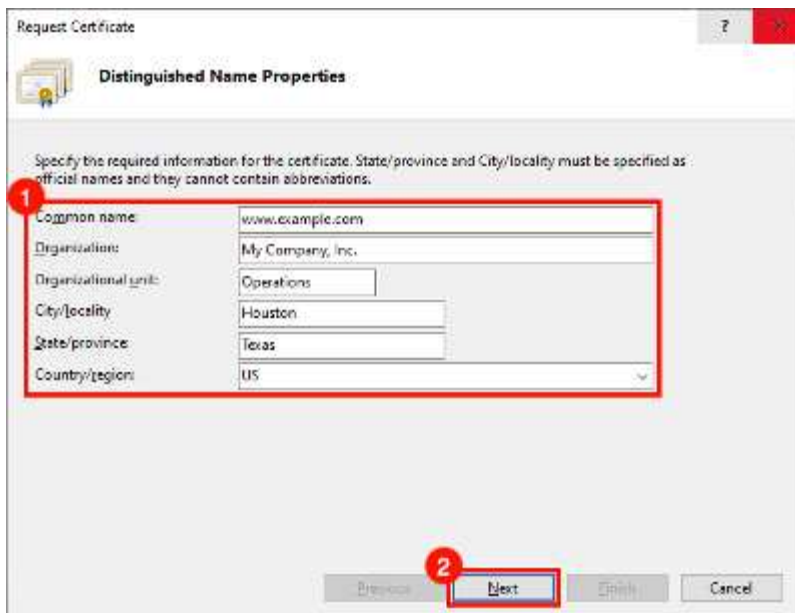
Processus de renouvellement de certificat SSL générique

Créer une demande de signature de certificat (CSR) :

1. Connectez-vous au CWMGR1
2. Ouvrez IIS Manager à partir des outils d'administration
3. Sélectionnez CWMGR1 et ouvrez les certificats de serveur
4. Cliquez sur Créer une demande de certificat dans le volet actions



5. Remplissez les propriétés du nom unique dans l'Assistant demande de certificat et cliquez sur Suivant :
 - a. Nom commun : FQDN du caractère générique - *.domain.com
 - b. Organisation : nom légalement enregistré de votre entreprise
 - c. Unité organisationnelle: «ELLE» fonctionne bien
 - d. Ville : ville où se trouve la société
 - e. State : emplacement de la société
 - f. Pays : pays dans lequel se trouve la société



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.

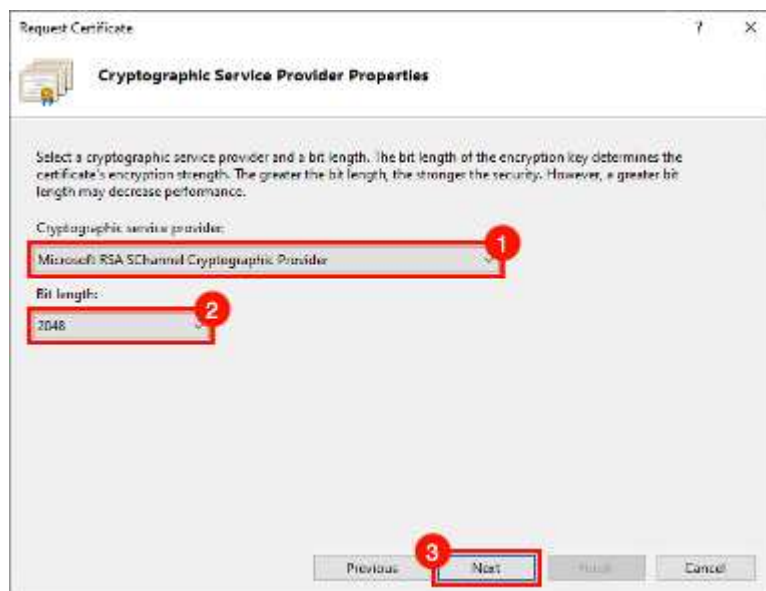
1

| | |
|----------------------|------------------|
| 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. Sur la page Propriétés du fournisseur de services cryptographiques, vérifiez que les éléments ci-dessous apparaissent et cliquez sur Suivant :



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:

1

Microsoft RSA Schannel Cryptographic Provider

Bit length:

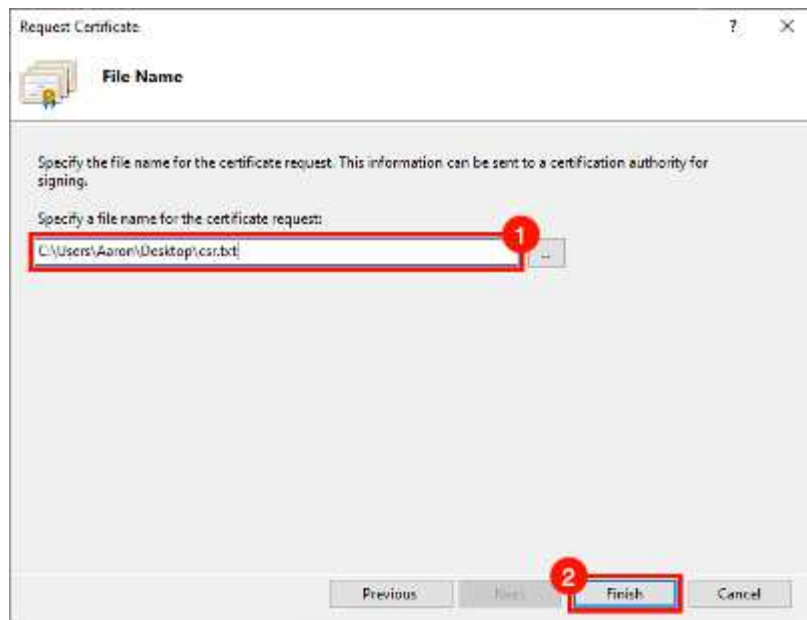
2

2048

3

Previous Next Finish Cancel

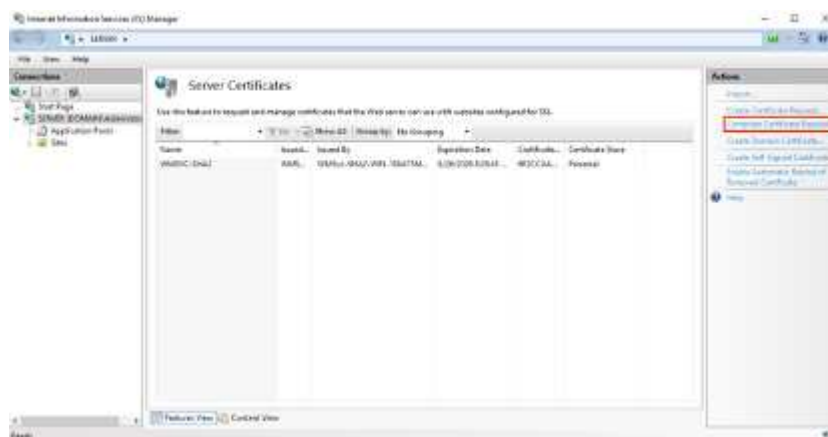
7. Spécifiez un nom de fichier et naviguez jusqu'à l'emplacement où vous souhaitez enregistrer la RSC. Si vous ne spécifiez pas d'emplacement, la RSC se trouve dans C:\Windows\System32 :



8. Lorsque vous avez terminé, cliquez sur Terminer. Vous utiliserez ce fichier texte pour soumettre votre commande au bureau d'enregistrement des certificats
9. Contacter le service d'enregistrement pour acheter un nouveau SSL générique pour votre certificat : *.domain.com
10. Après avoir reçu votre certificat SSL, enregistrez le fichier .cer du certificat SSL dans un emplacement sur CWMGR1 et suivez les étapes ci-dessous.

Installation et configuration de CSR :

1. Connectez-vous au CWMGR1
2. Ouvrez IIS Manager à partir des outils d'administration
3. Sélectionnez CWMGR1 et ouvrez "certificats serveur"
4. Cliquez sur remplir la demande de certificat dans le volet actions



5. Renseignez les champs ci-dessous dans la demande de certificat complète et cliquez sur OK :



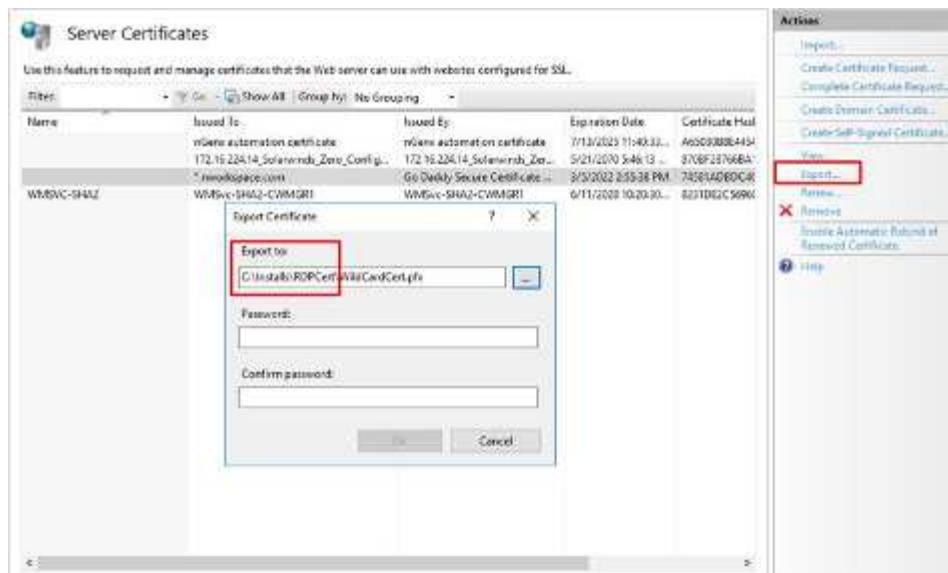
- a. Nom du fichier : sélectionnez le fichier .cer qui a été enregistré précédemment
- b. Nom convivial : *.domain.com
- c. Stockage de certificats : sélectionnez hébergement Web ou personnel

Attribution d'un certificat SSL :

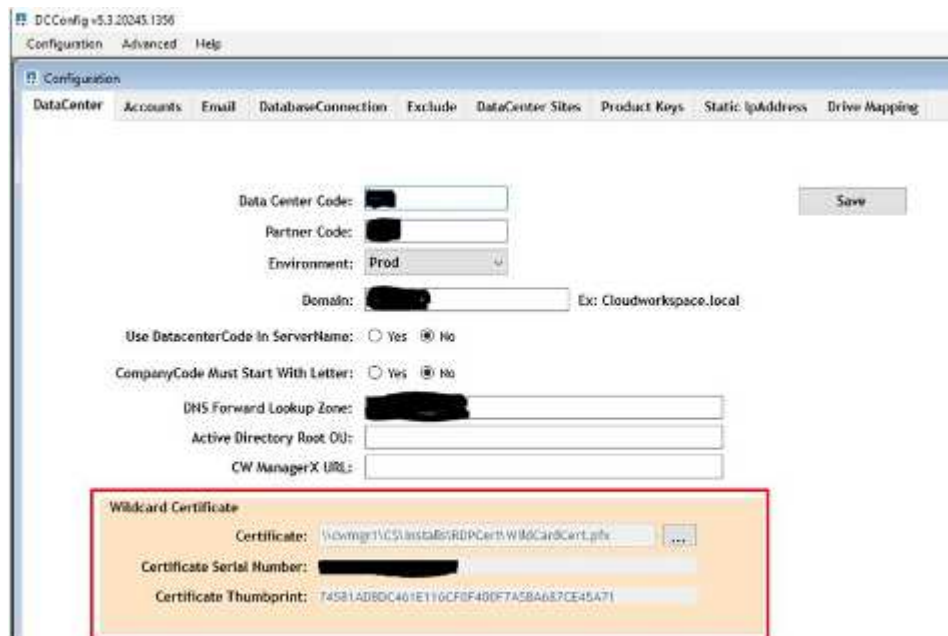
1. Vérifiez que le mode migration n'est pas activé. Ceci se trouve sur la page vue d'ensemble de l'espace de travail sous Paramètres de sécurité dans VDS.



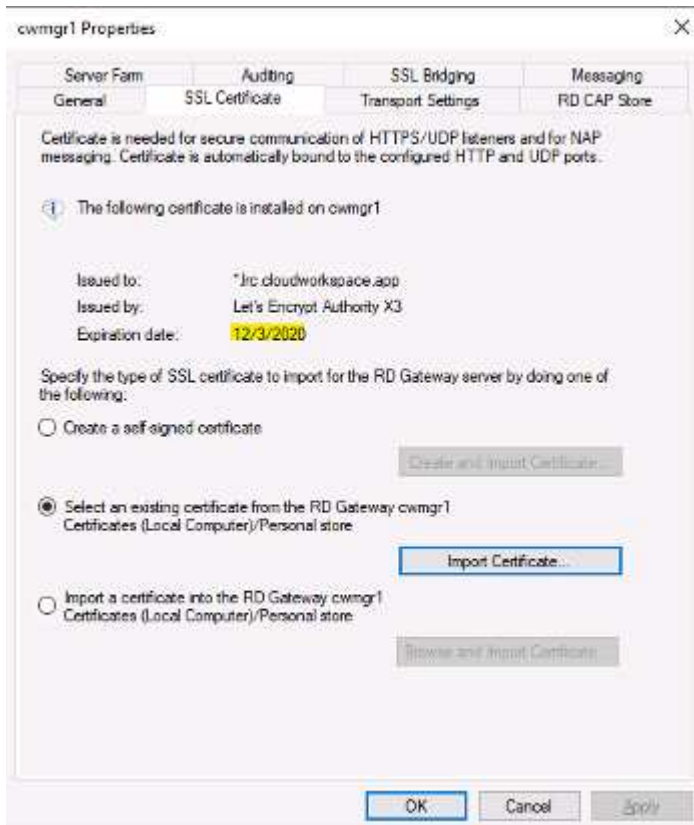
2. Connectez-vous au CWMGR1
3. Ouvrez IIS Manager à partir des outils d'administration
4. Sélectionnez CWMGR1 et ouvrez "certificats serveur"
5. Cliquez sur Exporter dans le volet actions
6. Exportez le certificat au format .pfx
7. Créez un mot de passe. Enregistrez le mot de passe car il sera nécessaire d'importer ou de réutiliser le fichier .pfx à l'avenir
8. Enregistrez le fichier .pfx dans le répertoire C:\installs\RDPcert
9. Cliquez sur OK et fermez IIS Manager



10. Ouvrez DCConfig
11. Sous certificat générique, mettez à jour le chemin d'accès de certificat vers le nouveau fichier .pfx
12. Entrez le mot de passe .pfx lorsque vous y êtes invité
13. Cliquez sur Save



14. Si le certificat est valide pendant 30 jours de plus, laissez l'automatisation appliquer le nouveau certificat pendant la tâche actions quotidiennes du matin pendant toute la semaine
15. Vérifiez régulièrement les serveurs de plate-forme pour vérifier que le nouveau certificat a été propagé. Valider et tester la connectivité des utilisateurs pour confirmer
 - a. Sur le serveur, accédez à Outils d'administration
 - b. Sélectionnez Remote Desktop Services > Remote Desktop Gateway Manager
 - c. Cliquez avec le bouton droit de la souris sur le nom du serveur de passerelle, puis sélectionnez Propriétés. Cliquez sur l'onglet certificat SSL pour vérifier la date d'expiration

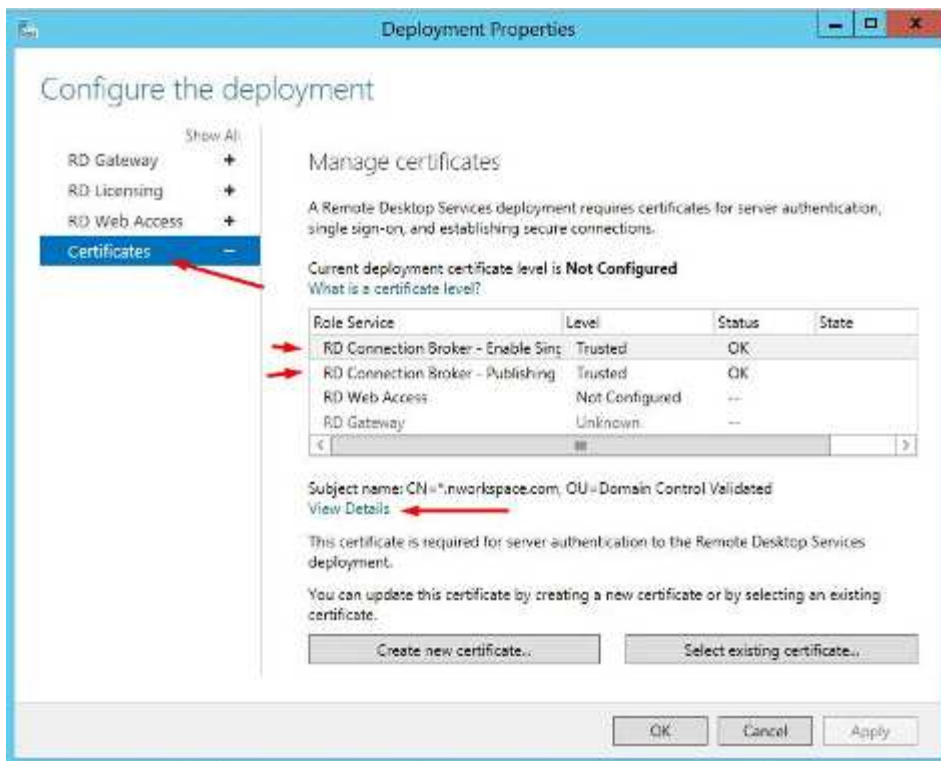


16. Vérifier régulièrement les VM clients qui exécutent le rôle Connection Broker

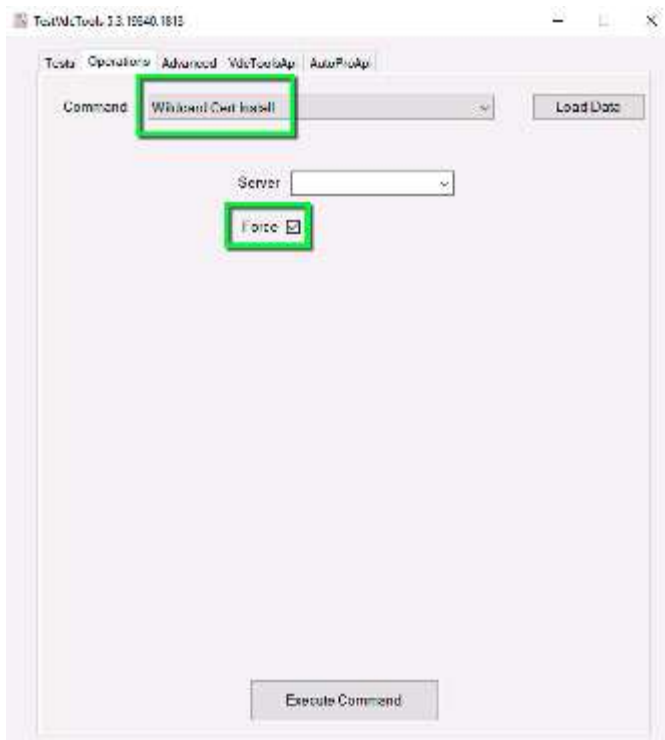
- a. Accédez à Server Manager > Remote Desktop Services
- b. Sous vue d'ensemble du déploiement, sélectionnez la liste déroulante tâches et choisissez Modifier les propriétés du déploiement



- c. Cliquez sur certificats, sélectionnez certificat et cliquez sur Afficher les détails. La date d'expiration sera indiquée.



17. Si vous avez moins de 30 jours ou si vous préférez envoyer le nouveau certificat immédiatement, forcez la mise à jour avec TestVdcTools. Cela doit être fait pendant une fenêtre de maintenance car la connectivité de tous les utilisateurs connectés et votre connexion à CWMGR1 sera perdue.
 - a. Accédez à C:\Program Files\CloudWorkspace\TestVdcTools, cliquez sur l'onglet opérations et sélectionnez la commande générique Cert-Install
 - b. Laissez le champ serveur vide
 - c. Cochez la case Force
 - d. Cliquez sur Exécuter la commande
 - e. Vérifiez les propagations de certificat à l'aide des étapes indiquées ci-dessus



Guide de démontage AVD

Présentation

Cet article aborde le retrait des contrôles VDS et NetApp tout en conservant l'accès utilisateur final AVD. La gestion sera assurée par les outils d'administration Azure/Windows natifs. Une fois ce processus terminé, nous vous recommandons de contacter support@spotpc.netapp.com afin que NetApp puisse nettoyer nos systèmes de back-end et de facturation.

État initial

- Déploiement AVD
- TDS1 est un fichier de fichier FS Logix
- TS1 est l'hôte de session
- L'utilisateur s'est connecté et le disque FS Logix a été créé dans :

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

Supprimer le service Agent CW

L'agent CW s'exécute sur chaque machine de l'environnement. Le service qui démarre ce processus doit être désinstallé avec la commande suivante sur chaque machine virtuelle de l'environnement. CWMGR1 peut être ignoré car cette machine virtuelle sera arrêtée et éventuellement supprimée dans la plupart des cas. Dans l'idéal, cette action serait exécutée via une automatisation basée sur des scripts. La vidéo ci-dessous montre qu'elle a été réalisée manuellement.

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

Supprimer la vidéo du service CW Agent

 | <https://img.youtube.com/vi/I9ASmM5aap0/maxresdefault.jpg>

Supprimer le répertoire de l'agent CW

La désinstallation précédente a supprimé le service qui lance l'agent CW mais les fichiers restent. Supprimer le répertoire :

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

Permet de supprimer la vidéo du répertoire CW Agent

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

Supprimer les raccourcis de démarrage

Le répertoire des éléments de démarrage contient deux raccourcis vers les fichiers supprimés à l'étape précédente. Pour éviter les messages d'erreur de l'utilisateur final, ces fichiers doivent être supprimés.

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

Supprimer la vidéo des raccourcis de démarrage

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

Dissocier les GPO «utilisateurs» et «sociétés»

Trois GPO sont implémentés par VDS. Nous recommandons de délier deux d'entre eux et de revoir le contenu du troisième.

Dissocier :

- Utilisateurs ADDC > Cloud Workspace Companies
- Utilisateurs ADDC > utilisateurs Cloud Workspace

Révision :

- Ordinateurs AADDG > ordinateurs Cloud Workspace

Dissocier la vidéo des stratégies de groupe des «utilisateurs» et des «sociétés»

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

Arrêter CWMGR1

Avec les modifications GPO appliquées, nous pouvons maintenant arrêter la machine virtuelle CWMGR1. Une fois que la fonctionnalité AVD continue est confirmée, cette machine virtuelle peut être supprimée définitivement.

Dans les très rares cas, il est nécessaire de maintenir cette machine virtuelle si un autre rôle de serveur est en cours d'exécution (par exemple, DC, serveur FTP...). Dans ce cas, trois services peuvent être désactivés pour désactiver la fonctionnalité VDS sur CWMGR1 :

- Agent CW (voir ci-dessus)
- Service d'automatisation CW
- Automatisation des machines virtuelles CW

Arrêter la vidéo CWMGR1

 | https://img.youtube.com/vi/avk9HyliC_s/maxresdefault.jpg

Supprimez les comptes de service VDS NetApp

Les comptes de service Azure AD utilisés par VDS peuvent être supprimés. Connectez-vous au portail de gestion Azure et supprimez les utilisateurs :

- CloudWorkspaceSVC
- CloudWorkspaceCASVC

Les autres comptes utilisateur peuvent être conservés :

- Utilisateurs finaux
- Administrateur Azure
- administrateurs de domaine technique

Supprimez la vidéo des comptes de service VDS NetApp

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

Supprimer les enregistrements d'applications

Deux enregistrements d'applications sont effectués lors du déploiement de VDS. Vous pouvez les supprimer :

- API Cloud Workspace
- AVD de l'espace de travail cloud

Supprimer la vidéo d'enregistrement d'applications

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

Supprimer des applications d'entreprise

Deux applications d'entreprise sont déployées lors du déploiement de VDS. Vous pouvez les supprimer :

- Espace de travail cloud
- API de gestion de l'espace de travail cloud

Supprimer la vidéo des applications d'entreprise

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

Confirmez que le CWMGR1 est arrêté

Avant de tester que les utilisateurs finaux peuvent toujours se connecter, vérifiez que le CWMGR1 est arrêté pour un test réaliste.

Vérifiez que la vidéo CWMGR1 est arrêtée

 | <https://img.youtube.com/vi/Ux9nkDk5IU4/maxresdefault.jpg>

Connexion et utilisateur final

Pour confirmer votre réussite, connectez-vous en tant qu'utilisateur final et vérifiez que la fonctionnalité est conservée.

Vidéo de connexion et d'utilisateur final

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

Informations sur le copyright

Copyright © 2022 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.