



Architetturale

Virtual Desktop Service

NetApp
May 24, 2023

This PDF was generated from https://docs.netapp.com/it-it/virtual-desktop-service/Architetturale.change_data_layer.Azure_Files.html on May 24, 2023. Always check docs.netapp.com for the latest.

Sommario

- Architetturale 1
 - Reindirizzamento della piattaforma di storage 1
 - Considerazioni sulla migrazione dei dati 6
 - Processo di rinnovo del certificato SSL con caratteri jolly 8
 - Guida all'apprendimento di AVD 15

Architetturale

Reindirizzamento della piattaforma di storage

Panoramica

Le tecnologie di implementazione di Virtual Desktop Service consentono una vasta gamma di opzioni di storage, a seconda dell'infrastruttura sottostante, in questa guida vengono fornite informazioni su come apportare modifiche dopo l'implementazione.

Le performance dei desktop virtuali dipendono da una varietà di risorse chiave, mentre le performance dello storage sono una delle variabili principali. Man mano che i requisiti cambiano e i carichi di lavoro si evolvono, la necessità di cambiare l'infrastruttura storage è un compito comune. In quasi tutti i casi, ciò comporta la migrazione da una piattaforma di file server alla tecnologia di storage NetApp (come Azure NetApp Files, NetApp Cloud Volumes Service in Google o NetApp Cloud Volumes ONTAP in AWS), poiché queste tecnologie offrono in genere il miglior profilo di performance per gli ambienti di calcolo degli utenti finali.

Creazione del nuovo layer di storage

A causa dell'ampia varietà di potenziali servizi di storage in una vasta gamma di provider di infrastrutture cloud e HCI, questa guida presuppone che sia già stato stabilito un nuovo servizio di storage e che i percorsi SMB siano noti.

Creare cartelle di storage

1. Nel nuovo servizio di storage, creare tre cartelle:

- /Dati
- /Home
- /Pro

[]

2. Impostare le autorizzazioni per le cartelle

- a. In Folder Properties (Proprietà cartella), selezionare *Security (sicurezza)*, >*Advanced (Avanzate)* > *Disable ereditarietà*

[]

- b. Regolare le restanti impostazioni in modo che corrispondano alle impostazioni del layer di storage originale create in origine dall'automazione dell'implementazione.

Spostamento dei dati




Le directory, i dati, i file e le impostazioni di sicurezza possono essere spostati in diversi modi. La seguente sintassi di robocopy consentirà di apportare le modifiche necessarie. I percorsi devono essere modificati in base all'ambiente in uso.

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



Reindirizzamento del percorso SMB al cutover

Quando arriverà il momento del cutover, alcune modifiche reindirizzeranno tutte le funzionalità dello storage nell'ambiente VDS.


Aggiornare gli oggetti Criteri di gruppo

1. L'oggetto Criteri di gruppo utenti (denominato *<company-code>-users*) deve essere aggiornato con il nuovo percorso di condivisione. Selezionare *Configurazione utente > Impostazioni di Windows > Preferenze > Mappe unità*

2. Fare clic con il pulsante destro del mouse su *H:*, selezionare *Proprietà > Modifica > azione: Sostituire_ e immettere il nuovo percorso*

3. Con Classic o Hybrid ad, aggiornare la condivisione definita in ADUC nell'unità organizzativa aziendale. Ciò si riflette nella gestione delle cartelle VDS.


Aggiorna i percorsi del profilo FSLogix

1. Aprire Regedit sul file server originale e su qualsiasi altro host di sessione con provisioning.
 Se lo si desidera, è possibile impostare questa opzione anche tramite un criterio GPO.
2. Modificare il valore *VHDLocations* con il nuovo valore. Questo dovrebbe essere il nuovo percorso SMB più *pro/profilecontainers*, come mostrato nella schermata seguente.


Aggiornare le impostazioni di reindirizzamento delle cartelle per le home directory

1. Aprire Gestione criteri di gruppo, selezionare l'oggetto Criteri di gruppo utenti collegato a *DC=dominio,DC=mobi/Area di lavoro cloud/Società area di lavoro cloud/utenti <company-code>/<company-code>-desktop*.
2. Modificare i percorsi di reindirizzamento delle cartelle in *Configurazione utente > Criteri > Impostazioni Windows > Reindirizzamento cartelle*.
3. Solo Desktop e documenti devono essere aggiornati e i percorsi devono corrispondere al nuovo punto di montaggio del percorso SMB per il volume Home


Aggiornare il database SQL VDS con Command Center

CWMGR1 contiene un'utilità di supporto chiamata Command Center che può aggiornare in blocco il database VDS.

Per eseguire gli aggiornamenti finali del database:

1. Connettersi a CWMGR1, navigare ed eseguire CommandCenter.exe

[]

2. Accedere alla scheda *Operations*, fare clic su *Load Data* per compilare il menu a discesa Company Code (Codice società), selezionare il codice della società e immettere i nuovi percorsi di storage per il layer di storage, quindi fare clic su *Execute Command*.

[]

Reindirizzamento della piattaforma di storage ai file Azure

Panoramica

Le tecnologie di implementazione di Virtual Desktop Service consentono una vasta gamma di opzioni di storage a seconda dell'infrastruttura sottostante. Questa guida spiega come apportare una modifica all'utilizzo dei file Azure dopo la distribuzione.

Prerequisiti

- AD Connect installato e configurato
- Account amministratore globale Azure
- AZFilesModule PowerShell ibrido <https://github.com/Azure-Samples/azure-files-samples/releases>
- Modulo AZ PowerShell
- Modulo ActiveDirectory PowerShell

Creare il nuovo layer di storage

1. Accedere ad Azure con l'account amministratore globale
2. Creare un nuovo account di storage nella stessa posizione e nello stesso gruppo di risorse dell'area di lavoro

[]

3. Creare le condivisioni di dati, home e file pro sotto l'account storage

[]

Configurare Active Directory

1. Creare una nuova unità organizzativa denominata "Storage account" in Cloud Workspace > Cloud Worksapce Service Accounts OU

[]

2. Abilitare l'autenticazione ad DS (deve essere eseguita utilizzando PowerShell) <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-enable>
 - a. DomainAccountType deve essere "ServiceLogonAccount"
 - b. OrganizationalUnitDistinguishedName è il nome distinto dell'unità organizzativa creata nel passaggio precedente (ad es "OU=Storage Account,OU=Cloud Worksapce Service Accounts,OU=Cloud Workspace,DC=TrainingKrisG,DC=onmicrosoft,DC=com")

Impostare i ruoli per le condivisioni

1. Nel portale Azure, assegnare il ruolo di "Storage file Data SMB Share Elevated Contributor" ai tecnici di CloudWorkspaceSVC e Level3

[]

2. Assegnare il ruolo di "Storage file Data SMB Share Contributor" a "<company code>-all users" gruppo

[]

Creare le directory

1. Creare una directory in ogni condivisione (dati, home, pro) utilizzando il codice della società come nome (in questo esempio, il codice della società è "kift")

[]

2. Nella directory <company code> della condivisione professionale, creare una directory "ProfileContainers"

[]

Impostare le autorizzazioni NTFS

1. Connettersi alle condivisioni

- a. Accedere alla condivisione sotto l'account di storage nel portale Azure, fare clic sui tre punti, quindi fare clic su Connect (Connetti)

[]

- b. Scegliere Active Directory for Authentication Method (Active Directory per metodo di autenticazione) e fare clic sull'icona Copy to Appunti (Copia negli Appunti) nell'angolo inferiore destro del codice

[]

- c. Accedere al server CWMGR1 con un account membro del gruppo Level3 Technicians

- d. Eseguire il codice copiato in PowerShell per mappare l'unità

- e. Fare lo stesso per ciascuna condivisione scegliendo una lettera di unità diversa per ciascuna

2. Disattivare l'ereditarietà nelle directory <company code>

3. System e il ClientDHPAccess del gruppo ad devono avere il controllo completo delle directory <company code>

4. I computer di dominio devono avere il controllo completo della directory <company code> nella condivisione pro e della directory ProfileContainers all'interno di

5. Il gruppo ad di utenti <company code>-all deve disporre dei dati di lettura/cartella elenco nelle directory <company code> delle condivisioni home e pro

6. Il gruppo ad <company code>-All Users deve disporre delle autorizzazioni speciali riportate di seguito per la directory nella condivisione dei dati

[]

7. Il gruppo ad di utenti <company code>-all deve disporre dell'autorizzazione Modifica per la directory

Aggiorna oggetti Criteri di gruppo

1. Aggiornare gli utenti di GPO <company code> in Area di lavoro cloud > Aziende area di lavoro cloud > <company code> > utenti <company code>-desktop

- a. Modificare la mappatura dell'unità Home per puntare la nuova condivisione domestica

[]

- b. Modificare il reindirizzamento cartelle per puntare la home share per Desktop e documenti

[]

[]

Aggiornare la condivisione in utenti e computer di Active Directory

1. Con l'ad classico o ibrido, la condivisione nell'unità organizzativa del codice aziendale deve essere aggiornata nella nuova posizione

[]

Aggiornare i percorsi Data/Home/Pro in VDS

1. Accedi a CWMGR1 con un account nel gruppo Level3 Technicians e avvia Command Center
2. Nell'elenco a discesa dei comandi, selezionare Change Data/Home/Pro Folders (Modifica dati/Home/cartelle Pro)
3. Fare clic sul pulsante Load Data (carica dati), quindi assicurarsi di aver selezionato il codice società corretto dall'elenco a discesa
4. Immettere il nuovo patsh per le posizioni dei dati, della casa e dei professionisti
5. Deselezionare la casella is Windows Server (è Windows Server)
6. Fare clic sul pulsante Execute Command (Esegui comando)

[]

Aggiorna i percorsi del profilo FSLogix

1. Aprire l'editorio del Registro di sistema sugli host di sessione
2. Modificare la voce VHDLocations in HKLM/SOFTWARE/FSLogix/Profiles in modo che sia il percorso UNC alla nuova directory ProfileContainers

[]

Configurare i backup

1. Si consiglia di impostare e configurare un criterio di backup per le nuove condivisioni
2. Creare un nuovo vault dei servizi di ripristino nello stesso gruppo di risorse
3. Accedere al vault e selezionare Backup in Getting Started (Guida introduttiva)

4. Scegliere Azure per il carico di lavoro in esecuzione e Azure file share per il backup, quindi fare clic su Backup
5. Selezionare l'account di storage utilizzato per creare le condivisioni
6. Aggiungere le condivisioni di cui eseguire il backup
7. Modifica e crea una policy di backup che si adatti alle tue esigenze

Considerazioni sulla migrazione dei dati

Panoramica

La migrazione dei dati è un requisito quasi universale quando si esegue la migrazione a una soluzione cloud di qualsiasi tipo. Mentre gli amministratori sono responsabili della migrazione dei dati nei propri desktop virtuali, l'esperienza di NetApp è disponibile e si è dimostrata inestimabile per innumerevoli migrazioni dei clienti. L'ambiente Virtual Desktop è semplicemente un ambiente Windows ospitato, pertanto è possibile utilizzare qualsiasi metodo.

Dati di solito migrati:

- Profili utente (Desktop, documenti, Preferiti, ecc....)
- Condivisioni file server
- Condivisioni di dati (dati delle applicazioni, database, cache di backup)

Nell'ambiente Virtual Desktop, i dati vengono memorizzati e organizzati in due posizioni principali:

- L'unità utente (in genere H:): È l'unità mappata visibile per ciascun utente.
 - Questo viene mappato di nuovo al percorso <DRIVE>: user.name
 - Ogni utente dispone di un proprio disco H: E non può vedere un altro utente
- L'unità condivisa (in genere i:): Si tratta dell'unità condivisa mappata visibile a tutti gli utenti
 - Questo viene mappato di nuovo al percorso <DRIVE>: Dati/Codice cliente
 - Tutti gli utenti possono accedere a questo disco. Il loro livello di accesso alle cartelle/file contenuti viene gestito nella sezione cartelle di VDS.

Processo di migrazione generico

1. Replica dei dati nell'ambiente cloud
2. Spostare i dati nel percorso appropriato per i dischi H: E i:
3. Assegnare le autorizzazioni appropriate nell'ambiente Virtual Desktop

Trasferimenti FTPS e considerazioni

Migrazione con FTPS

1. Se il ruolo del server FTPS è stato attivato durante il processo di implementazione di CWA, raccogliere le credenziali FTPS accedendo a VDS, accedendo ai report ed eseguendo il report del client master per l'organizzazione
2. Caricare i dati
3. Spostare i dati nel percorso appropriato per i dischi H: E i:

4. Assegnare le autorizzazioni appropriate nell'ambiente Virtual Desktop tramite il modulo cartelle



Durante il trasferimento dei dati tramite FTPS, qualsiasi interruzione impedirà il trasferimento dei dati come previsto. Poiché i server gestiti da Virtual Desktop Services vengono riavviati ogni notte, la strategia di trasmissione standard durante la notte potrebbe essere interrotta. Per ovviare a questo problema, gli amministratori possono attivare la modalità di migrazione per impedire il riavvio delle macchine virtuali per 1 settimana.

Abilitare la modalità di migrazione è semplice: Accedere all'organizzazione, quindi scorrere fino alla sezione Impostazioni desktop virtuale e selezionare la casella modalità di migrazione, quindi fare clic su Aggiorna.



NetApp consiglia agli amministratori di abilitare un'impostazione di conformità che consenta alle organizzazioni di soddisfare i controlli PCI, HIPAA e NIST tramite la protezione avanzata dei gateway di implementazione, ecc. In questo modo, il ruolo del server FTP predefinito, se attivato, non accetta trasmissioni predefinite non crittografate tramite la porta 21. FileZilla non supporta SFTP, il che significa che le connessioni devono essere effettuate utilizzando FTPS sulla porta 990.

Per attivare questa impostazione, connettersi a CWMGR1 e accedere al programma CwVmAutomationService, quindi attivare la conformità PCI v3.

Considerazioni e strumenti di sincronizzazione

Enterprise file Sync and Share, spesso definito EFSS o strumenti di sincronizzazione, può essere estremamente utile nella migrazione dei dati, in quanto lo strumento acquisirà le modifiche da ogni lato fino al cutover. Strumenti come OneDrive, fornito con Office 365, possono aiutarti a sincronizzare i dati del file server. È utile anche per le implementazioni degli utenti VDI, in cui esiste una relazione 1:1 tra l'utente e la macchina virtuale, a condizione che l'utente non tenti di sincronizzare il contenuto condiviso sul server VDI quando i dati condivisi possono essere implementati una volta su Shared (in genere i:) per l'intera organizzazione. Migrazione di SQL e dati simili (file aperti)

Le comuni soluzioni di sincronizzazione e/o migrazione non trasferiscono file aperti, che includono tipi di file come:

- File mailbox (.OST)
- File QuickBooks
- File Microsoft Access
- Database SQL

Ciò significa che se viene visualizzato un singolo elemento dell'intero file (ad esempio, 1 nuovo messaggio e-mail) o del database (viene inserito 1 nuovo record nel sistema di un'applicazione), l'intero file è diverso e gli strumenti di sincronizzazione standard (ad esempio Dropbox) ritieni che si tratti di un file completamente nuovo e che deve essere spostato di nuovo. Se lo si desidera, sono disponibili strumenti specializzati per l'acquisto presso fornitori di terze parti.

Un altro modo comune per gestire queste migrazioni è quello di fornire l'accesso a un VAR di terze parti, che spesso ha semplificato l'importazione/esportazione di database.

Spedizione delle unità

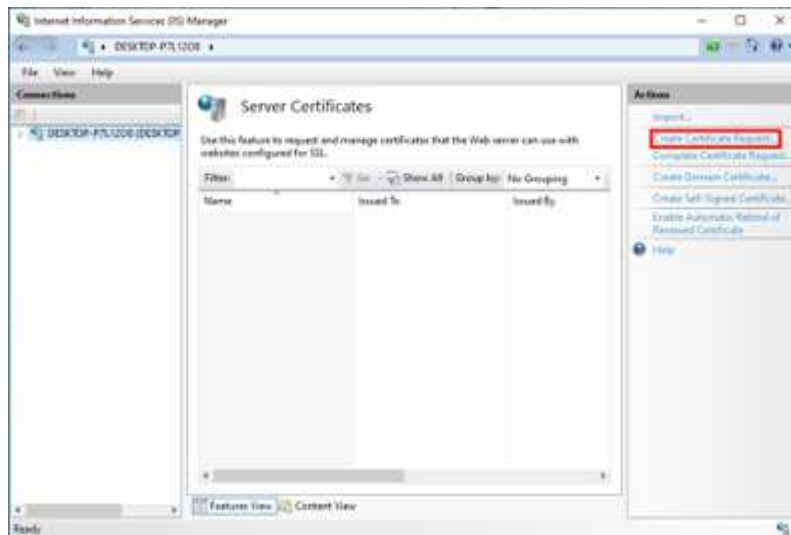
Molti data center provider non spediscono più dischi rigidi, o richiedono di seguire le proprie policy e procedure specifiche.

Microsoft Azure consente alle organizzazioni di utilizzare Azure Data Box, di cui gli amministratori possono usufruire coordinandosi con i propri rappresentanti Microsoft.

Processo di rinnovo del certificato SSL con caratteri jolly

Creare una richiesta di firma del certificato (CSR):

1. Connettersi a CWMGR1
2. Aprire Gestione IIS da Strumenti di amministrazione
3. Selezionare CWMGR1 e aprire certificati server
4. Fare clic su Create Certificate Request (Crea richiesta certificato) nel riquadro Actions (azioni)



5. Compilare le Proprietà nome distinto nella procedura guidata richiesta certificato e fare clic su Avanti:
 - a. Nome comune: FQDN del carattere jolly - *.domain.com
 - b. Organizzazione: Il nome legale della tua azienda
 - c. Unità organizzativa: 'FUNZIONA bene
 - d. Città: Città in cui si trova l'azienda
 - e. Stato: Stato in cui si trova l'azienda
 - f. Paese: Paese in cui si trova l'azienda

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. Nella pagina Cryptographic Service Provider Properties (Proprietà provider di servizi di crittografia), verificare che venga visualizzato quanto segue e fare clic su Next (Avanti):

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:

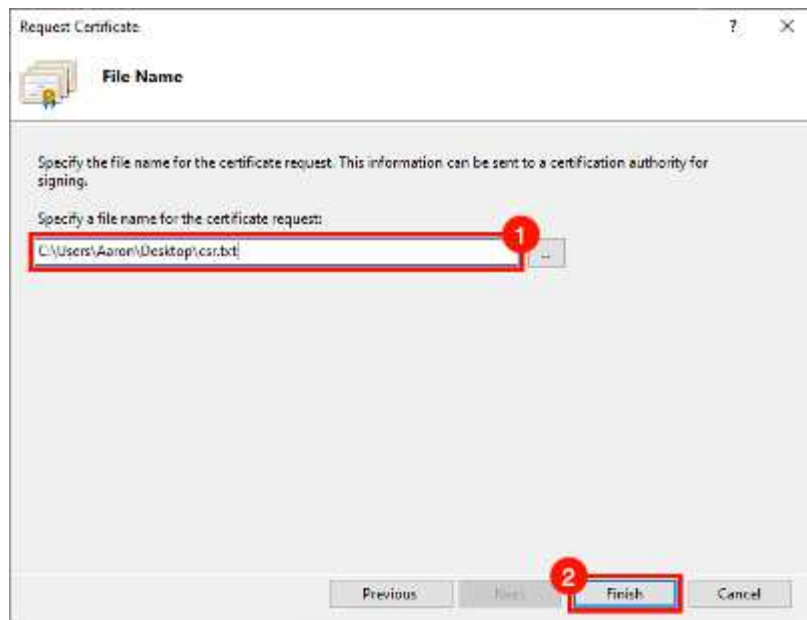
2

2048

3

Previous Next Finish Cancel

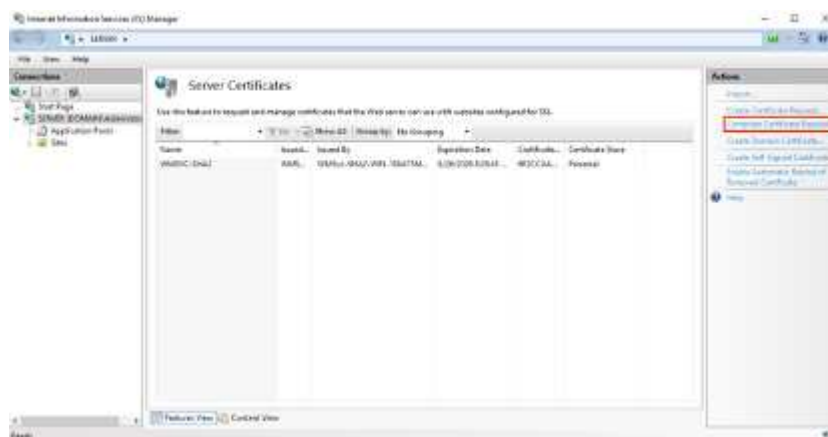
7. Specificare un nome di file e individuare la posizione in cui si desidera salvare la CSR. Se non si specifica una posizione, la CSR sarà in C:



8. Al termine, fare clic su Finish (fine) Questo file di testo verrà utilizzato per inviare l'ordine al registrar del certificato
9. Contatta il supporto del registrar per acquistare un nuovo SSL con caratteri jolly per il tuo certificato:
*.domain.com
10. Dopo aver ricevuto il certificato SSL, salvare il file .cer del certificato SSL in una posizione su CWMGR1 e seguire la procedura riportata di seguito.

Installazione e configurazione della CSR:

1. Connettersi a CWMGR1
2. Aprire Gestione IIS da Strumenti di amministrazione
3. Selezionare CWMGR1 e aprire 'Scertificati server'
4. Fare clic su complete Certificate Request (completa richiesta certificato) nel riquadro Actions (azioni)



5. Completare i campi riportati di seguito nella richiesta di certificato completa e fare clic su OK:



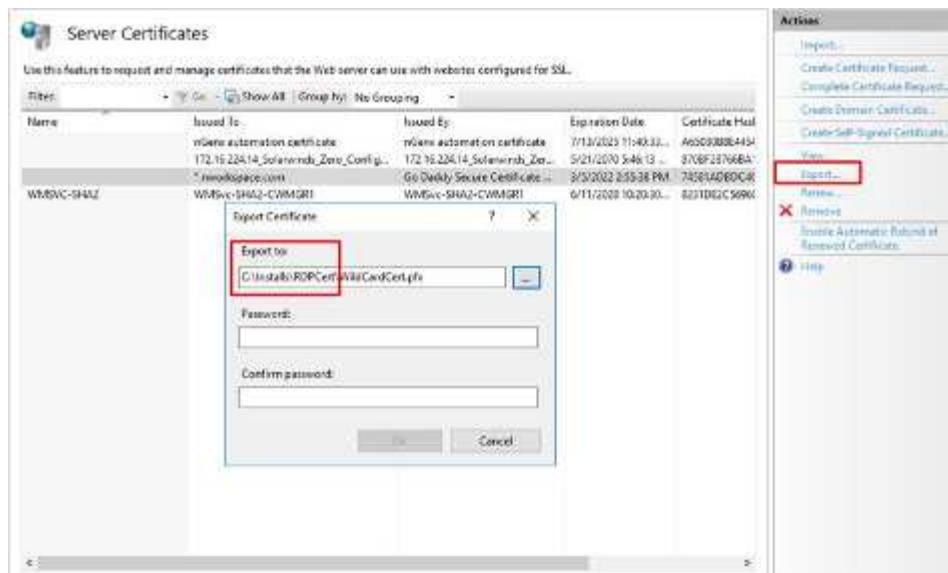
- a. File Name (Nome file): Selezionare il file .cer salvato in precedenza
- b. Nome descrittivo: *.domain.com
- c. Archivio certificati: Selezionare Web Hosting o Personal

Assegnazione del certificato SSL:

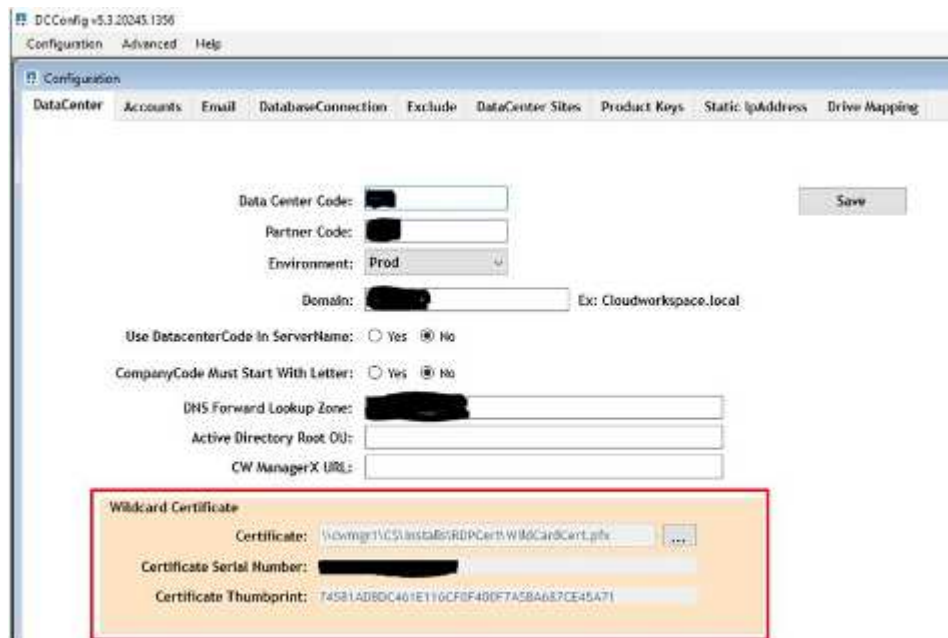
1. Verificare che la modalità di migrazione non sia attivata. Questa opzione è disponibile nella pagina Panoramica dell'area di lavoro in Impostazioni di protezione in VDS.



2. Connettersi a CWMGR1
3. Aprire Gestione IIS da Strumenti di amministrazione
4. Selezionare CWMGR1 e aprire 'Scertificati server'
5. Fare clic su Export (Esporta) nel riquadro Actions (azioni)
6. Esportare il certificato in formato .pfx
7. Creare una password. Memorizzare la password come sarà necessaria per importare o riutilizzare il file .pfx in futuro
8. Salvare il file .pfx nella directory C:/installs/RDPcert
9. Fare clic su OK e chiudere Gestione IIS

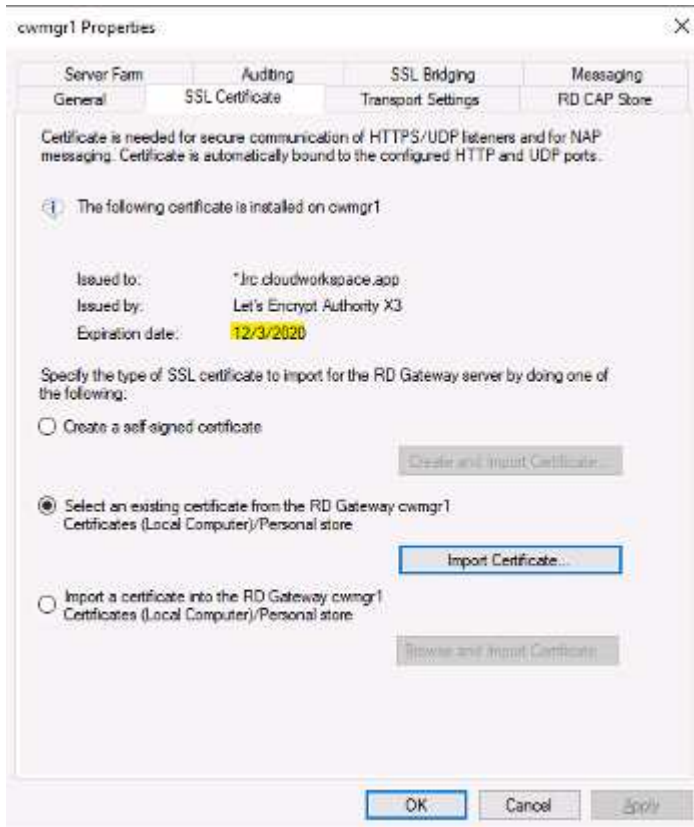


10. Aprire DCConfig
11. In certificato con caratteri jolly, aggiornare il percorso del certificato al nuovo file .pfx
12. Inserire la password .pfx quando richiesto
13. Fare clic su Salva



14. Se il certificato è valido per altri 30 giorni, consentire all'automazione di applicare il nuovo certificato durante l'attività Morning Daily Actions per tutta la settimana
15. Controllare periodicamente i server della piattaforma per verificare che il nuovo certificato sia stato propagato. Convalidare e verificare la connettività dell'utente per confermarla.
 - a. Sul server, accedere a Admin Tools (Strumenti di amministrazione)
 - b. Selezionare Remote Desktop Services (servizi desktop remoto) > Remote Desktop Gateway Manager (Gestione gateway desktop remoto)
 - c. Fare clic con il pulsante destro del mouse sul nome del server gateway e selezionare Proprietà. Fare

clic sulla scheda SSL Certificate (certificato SSL) per visualizzare la data di scadenza

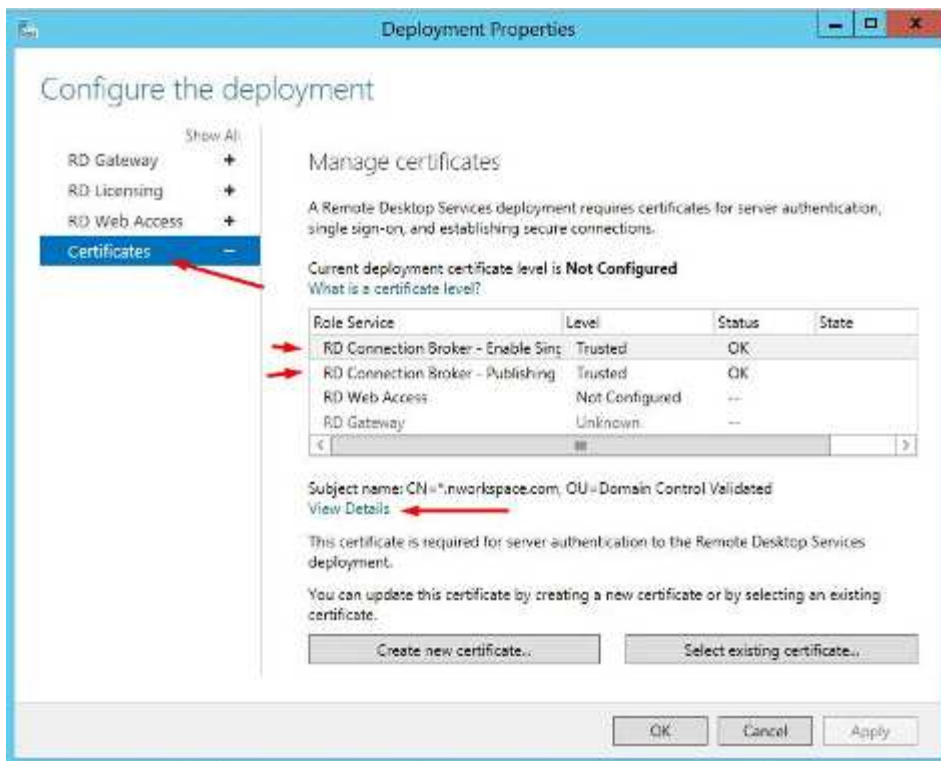


16. Controllare periodicamente le macchine virtuali client che eseguono il ruolo di Connection Broker

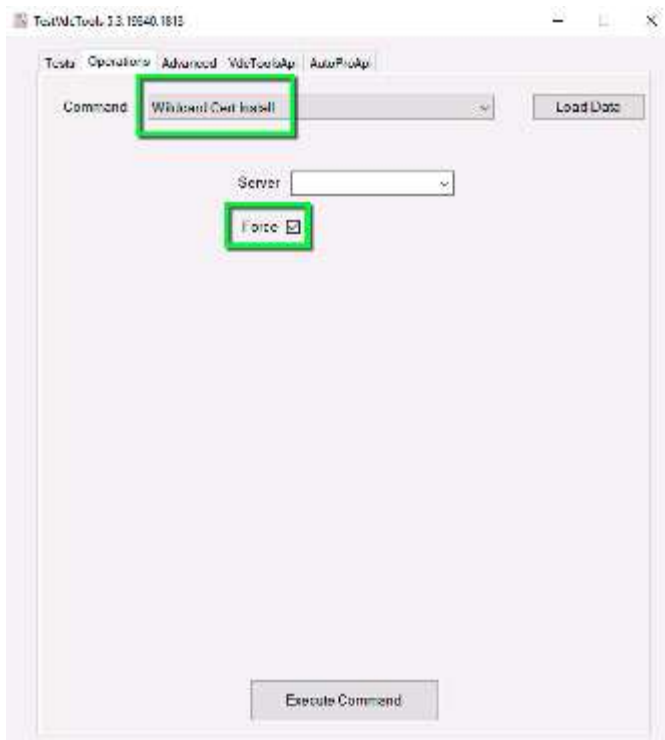
- a. Accedere a Server Manager > Remote Desktop Services (Gestione server > servizi desktop remoto)
- b. In Panoramica della distribuzione, selezionare il menu a discesa attività e scegliere Modifica proprietà di distribuzione



- c. Fare clic su certificati, selezionare certificato e fare clic su Visualizza dettagli. La data di scadenza verrà elencata.



17. Se si preferisce inviare il nuovo certificato immediatamente per meno di 30 giorni, forzare l'aggiornamento con TestVdcTools. Questa operazione deve essere eseguita durante una finestra di manutenzione, in quanto la connessione a CWMGR1 viene persa per tutti gli utenti connessi.
 - a. Accedere a C: Programmi, CloudWorkspace e TestVdcTools, fare clic sulla scheda operazioni e selezionare il comando con il carattere jolly Cert-Install
 - b. Lasciare vuoto il campo del server
 - c. Selezionare la casella forza
 - d. Fare clic su Esegui comando
 - e. Verificare la propagazione del certificato utilizzando i passaggi elencati in precedenza



Guida all'apprendimento di AVD

Panoramica

Questo articolo illustra la rimozione del controllo di VDS e NetApp mantenendo l'accesso dell'utente finale AVD. La gestione in futuro sarebbe basata su strumenti di amministrazione nativi di Azure/Windows. Una volta completato questo processo, si consiglia di contattare support@spotpc.netapp.com in modo che NetApp possa ripulire i sistemi di back-end e fatturazione.

Stato iniziale

- Implementazione AVD
- TDS1 è FS Logix FileShare
- TS1 è host di sessione
- L'utente ha effettuato l'accesso e il disco FS Logix è stato creato in:

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

Elimina servizio CW Agent

L'agente CW viene eseguito su ogni computer dell'ambiente. Il servizio che avvia questo processo deve essere disinstallato con il seguente comando su ogni macchina virtuale dell'ambiente. CWMGR1 può essere saltato, in quanto la macchina virtuale verrà arrestata ed eventualmente eliminata nella maggior parte dei casi. Idealmente, questa azione dovrebbe essere eseguita tramite l'automazione basata su script. Il video seguente mostra che è stato fatto manualmente.

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

Elimina il video del servizio CW Agent

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

Eliminare la directory degli agenti CW

La disinstallazione precedente ha rimosso il servizio che avvia CW Agent, ma i file rimangono. Eliminare la directory:

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

Elimina il video della directory di CW Agent

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

Rimuovere i collegamenti di avvio

La directory degli elementi di avvio contiene due collegamenti ai file cancellati nel passaggio precedente. Per evitare messaggi di errore dell'utente finale, questi file devono essere cancellati.

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

Rimuovere il video dei collegamenti di avvio

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

Scollegare gli oggetti Criteri di gruppo 'utenti' e 'aziende'

VDS ha implementato tre GPO. Si consiglia di scollegarne due e di rivedere il contenuto del terzo.

Scollega:

- Utenti AADDC > Aziende Cloud Workspace
- Utenti AADDC > utenti Cloud Workspace

Recensione:

- Computer AADDC > Cloud Workspace Computers

Scollegare il video degli oggetti Criteri di gruppo 'utenti' e 'aziende'

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

Arrestare CWMGR1

Con l'applicazione delle modifiche al GPO, è ora possibile arrestare la macchina virtuale CWMGR1. Una volta confermata la funzionalità AVD, questa macchina virtuale può essere eliminata in modo permanente.

In casi estremamente rari, è necessario mantenere questa macchina virtuale se è in esecuzione un altro ruolo di server (ad esempio, DC, FTP Server...). In tal caso, è possibile disattivare tre servizi per disattivare la funzionalità VDS su CWMGR1:

- Agente CW (vedere sopra)
- Servizio di automazione CW
- Automazione VM CW

Arrestare il video CWMGR1

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

Eliminare gli account dei servizi NetApp VDS

Gli account del servizio Azure ad utilizzati da VDS possono essere rimossi. Accedere al portale di gestione Azure ed eliminare gli utenti:

- CloudWorkspaceSVC
- CloudWorkspaceCASVC

È possibile conservare altri account utente:

- Utenti finali
- Amministratore di Azure
- amministratori di dominio .tech

Elimina il video degli account del servizio NetApp VDS

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

Eliminare le registrazioni delle applicazioni

Durante l'implementazione di VDS vengono effettuate due registrazioni di applicazioni. Questi possono essere cancellati:

- API Cloud Workspace
- Cloud Workspace AVD

Elimina il video di registrazione dell'applicazione

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

Eliminare le applicazioni aziendali

Durante l'implementazione di VDS vengono implementate due applicazioni aziendali. Questi possono essere cancellati:

- Cloud Workspace
- API Cloud Workspace Management

Elimina il video delle applicazioni aziendali

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

Verificare che CWMGR1 sia stato interrotto

Prima di verificare che gli utenti finali possano ancora connettersi, verificare che CWMGR1 sia stato arrestato per un test realistico.

Verificare che il video di CWMGR1 sia stato interrotto

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

Accesso e utente finale

Per confermare l'esito positivo, accedere come utente finale e verificare che la funzionalità sia mantenuta.

Login e video per l'utente finale

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

Informazioni sul copyright

Copyright © 2023 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.