



Datenebene Ändern

Virtual Desktop Service

NetApp

December 15, 2022

This PDF was generated from https://docs.netapp.com/de-de/virtual-desktop-service/Architectural.change_data_layer.Azure_Files.html on December 15, 2022. Always check docs.netapp.com for the latest.

Inhaltsverzeichnis

- Umleitung Der Storage-Plattform 1
 - Überblick 1
 - Umleitung der Storage-Plattform auf Azure Files..... 3

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 Ordneigenschaften 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 permissions 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 Registrierungseditor auf den Session-Hosts
2. Bearbeiten Sie den Eintrag VHDLocations 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

Copyright-Informationen

Copyright © 2022 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.