Systemadministration

Virtual Desktop Service

NetApp
December 15, 2022

Inhaltsverzeichnis

Systemadministration

Erstellen Sie ein Domain Admin-Konto („Level 3“)

Überblick

Gelegentlich benötigen VDS-Administratoren Anmeldeinformationen auf Domänenebene für das Management der Umgebung. In VDS werden diese als „Level 3“- oder „.Tech“-Konto bezeichnet.

Diese Anweisungen zeigen, wie diese Konten mit den entsprechenden Berechtigungen erstellt werden können.

Windows Server Domain Controller

Wenn ein intern gehosteter Domänencontroller (oder ein lokales DC, das über eine VPN/Express Route mit Azure verbunden ist) ausgeführt wird, können .Tech-Konten direkt in Active Directory Manager verwaltet werden.

1. Stellen Sie eine Verbindung zum Domänencontroller (CWMGR1, DC01 oder zur vorhandenen VM) mit einem Domain Admin (.Tech)-Konto her.
2. Erstellen Sie einen neuen Benutzer (falls erforderlich).
3. Fügen Sie den Benutzer der Sicherheitsgruppe „Level3 Technicians“ hinzu

   [Management.System Administration.Domain-Admin-Konto erstellen 9ee17] |

Management.System_Administration.create_domain_admin_account-9ee17.png

a. Wenn die Sicherheitsgruppe „Level3 Technicians“ fehlt, erstellen Sie bitte die Gruppe und machen Sie sie zu einem Mitglied der Sicherheitsgruppe „CW-Infrastructure“.

   [Management.System Administration.Create Domain Admin Konto 0fc27] |

Management.System_Administration.create_domain_admin_account-0fc27.png

Das Hinzufügen von „.tech“ am Ende des Benutzernamens ist eine empfohlene Best Practice, um Administratorkonten von den Endkundenkonten zu beschreiben.

Azure AD Domain Services

Bei Ausführung in Azure AD-Domänendiensten oder Benutzerverwaltung in Azure AD können diese Konten (d. h. Kennwortänderung) im Azure Management Portal als normaler Azure AD-Benutzer gemanagt werden.

Neue Konten können erstellt werden, indem sie zu diesen Rollen hinzugefügt werden, sollten ihnen die erforderlichen Berechtigungen geben:

1. AAD DC-Administratoren
2. ClientDHPAccess
3. Globaler Administrator im Verzeichnis.

Das Hinzufügen von „.tech“ am Ende des Benutzernamens ist eine empfohlene Best Practice, um Administratorkonten von den Endkundenkonten zu beschreiben.

[]

Bereitstellen von zeitweiligen Zugangs zu Dritten

Überblick

Der Zugang zu Dritten ist eine gängige Praxis bei der Migration zu einer beliebigen Cloud-Lösung.

VDS-Administratoren entscheiden sich oft dafür, diesen Dritten nicht das gleiche Zugriffsniveau wie sie zu geben, um eine „am wenigsten erforderliche“ Sicherheitszugangsrichtlinie zu befolgen.

Um Administratorzugriff für Dritte einzurichten, melden Sie sich beim VDS an und navigieren Sie zum Organisationsmodul, klicken Sie in die Organisation und klicken Sie auf Benutzer und Gruppen.

Erstellen Sie dann ein neues Benutzerkonto für den Dritten, und blättern Sie nach unten, bis Sie den Abschnitt „Administratorzugriff“ sehen und das Kontrollkästchen aktivieren, um Administratorrechte zu aktivieren.

[]

Der VDS Admin wird dann mit dem Bildschirm Admin Access Setup angezeigt. Es ist nicht erforderlich, den Benutzernamen, die Anmeldung oder das Passwort zu ändern. Fügen Sie einfach Telefonnummer und/oder E-Mail hinzu, wenn Sie die Multi-Faktor-Authentifizierung erzwingen möchten, und wählen Sie die Zugriffsstufe für die Erteilung aus.

Für Datenbankadministratoren wie VAR oder ISV ist *Servers* in der Regel das einzige erforderliche Zugriffsmodul.

[]

Nach dem Speichern erhält der Endbenutzer Zugriff auf Self-Management-Funktionen, indem er sich mit seinen standardmäßigen Benutzeranmeldeinformationen für Virtual Desktop beim VDS anmeldet.

Wenn sich der neu erstellte Benutzer anmeldet, werden nur die Module angezeigt, die Sie ihm zugewiesen haben. Sie können die Organisation auswählen, nach unten zum Abschnitt Server blättern und sich mit dem Servernamen verbinden, den Sie ihnen mitteilen (z. B. <XYZ>D1, wobei XYZ Ihr Unternehmenscode ist und D1 bestimmt, dass der Server ein Datenserver ist. Im folgenden Beispiel möchten wir ihnen mitteilen, sich mit dem TSD1-Server zu verbinden, um ihre Aufgaben auszuführen.

[]

Backup-Zeitplan Konfigurieren

Überblick

VDS kann native Backup-Services bei einigen Infrastrukturanbietern, einschließlich Azure, konfigurieren und managen.

Azure

In Azure kann VDS Backups automatisch mithilfe von nativen konfigurieren "Azure Cloud Backup" Durch lokal redundanten Storage (LRS). Geografisch redundanter Storage (GRS) kann bei Bedarf im Azure Management Portal konfiguriert werden.

- Für jeden Servertyp können individuelle Backup-Richtlinien definiert werden (mit Standardempfehlungen). Darüber hinaus können einzelnen Maschinen innerhalb der VDS-Benutzeroberfläche einen Zeitplan unabhängig (von ihrem Servertyp) zugewiesen werden. Diese Einstellung kann durch Klicken auf den Servernamen auf der Workspace-Seite in der Server-Detailansicht angewendet werden (siehe Video unten: Einstellen einzelner Backup-Richtlinien).
  - Daten
    - Backup mit 7 täglichen, 5 wöchentlichen & 2 monatlichen Backups. Verlängern Sie Aufbewahrungsfristen basierend auf geschäftlichen Anforderungen.
    - Dies gilt sowohl für einen dedizierten Data Server als auch für Add-on VPS VMs für Applikationen und Datenbanken.
  - Infrastruktur
    - CWMGR1 – Backup täglich und halten 7 täglich, 5 wöchentlich, 2 monatlich.
    - RDS Gateway – wöchentlich sichern und wöchentlich 4 behalten.
    - HTML5 Gateway – wöchentlich sichern und 4 wöchentlich aufbewahren.
  - Power-User (auch VDI-Benutzer)
    - Sichern Sie die VM nicht, da die Daten auf einem D1- oder TSD1-Server gespeichert werden sollen.
    - Beachten Sie, dass einige Applikationen Daten lokal speichern. In diesem Fall sollten besondere Überlegungen angestellt werden.
    - Sollte eine VM ausfällt, kann die neue VM per Klonen eine andere erstellt werden. Sollte nur eine VDI VM (oder eine eindeutige VM-Erstellung) vorhanden sein, sollte ein Backup durchgeführt werden, damit keine vollständige Wiederherstellung der VM erforderlich ist.
    - Anstatt alle VDI-Server zu sichern, können die Kosten minimiert werden, indem eine einzelne VM manuell für ein Backup direkt im Azure-Managementportal konfiguriert wird.
  - TS
    - Sichern Sie die VM nicht, da die Daten auf einem D1- oder TSD1-Server gespeichert werden

sollen.

- Beachten Sie, dass einige Applikationen Daten lokal speichern. In diesem Fall sollten besondere Überlegungen angestellt werden.
- Sollte eine VM ausfällt, kann die neue VM per Klonen eine andere erstellt werden. Falls nur eine TS-VM vorhanden ist, empfiehlt es sich, sie zu sichern, damit keine vollständige Wiederherstellung der VM erforderlich ist.
- Anstatt alle TS-Server zu sichern, können die Kosten minimiert werden, indem eine einzelne VM manuell für ein Backup direkt im Azure-Managementportal konfiguriert wird.

◦ TSData

- Backup mit 7 täglichen, 5 wöchentlichen & 2 monatlichen Backups. Verlängern Sie Aufbewahrungsfristen basierend auf geschäftlichen Anforderungen.

- Die Richtlinien können so festgelegt werden, dass Backups täglich oder wöchentlich durchgeführt werden. Azure unterstützt keine häufigeren Zeitpläne.
- Geben Sie für tägliche Zeitpläne die bevorzugte Zeit für das Backup ein. Geben Sie bei wöchentlichen Schichtplänen den bevorzugten Tag und die gewünschte Zeit ein, um das Backup zu erstellen. Hinweis: Die Einstellung auf exakt 12:00 Uhr kann Probleme in Azure Backup verursachen, daher wird 12:01 am empfohlen.
- Legen Sie fest, wie viele tägliche, wöchentliche, monatliche und jährliche Backups aufbewahrt werden sollen.

Legen Sie die Standardeinstellungen für die Bereitstellung fest

[]

Gehen Sie wie folgt vor, um Azure Backup für die gesamte Implementierung einzurichten:

1. Navigieren Sie zur Detailseite Bereitstellungen, und wählen Sie Standardeinstellungen sichern
2. Wählen Sie einen Servertyp aus dem Dropdown-Menü aus. Folgende Servertypen sind verfügbar:

```
Data: these are for LOB/database server types
Infrastructure: these are platform servers
Power User: these are for Users with a TS server dedicated solely to
them
TS: these are terminal servers that Users launch sessions on
TSData: these are servers doubling as terminal and data servers.
```

◦ Auf diese Weise werden die übergeordneten Backup-Einstellungen für die gesamte Implementierung definiert. Diese können, falls gewünscht, später auf einer Server-spezifischen Ebene außer Kraft gesetzt werden.

3. Klicken Sie auf das Einstellrad und dann auf das daraufhin angezeigte Popup-Fenster „Bearbeiten“.
4. Wählen Sie die folgenden Sicherungseinstellungen aus:

```
On or off
Daily or weekly
What time of day backups take place
How long each backup type (daily, weekly, etc.) should be retained
```

5. Klicken Sie schließlich auf Zeitplan erstellen (oder bearbeiten), um diese Einstellungen zu übernehmen.

Festlegung einzelner Backup-Richtlinien

Um serverspezifische integrierte Backup-Einstellungen anzuwenden, navigieren Sie zu einer Detailseite des Arbeitsbereichs.

1. Blättern Sie nach unten zum Abschnitt Server, und klicken Sie auf den Servernamen
2. Klicken Sie Auf Zeitplan Hinzufügen
3. Übernehmen Sie die Backup-Einstellungen wie gewünscht, und klicken Sie auf Zeitplan erstellen

Wiederherstellung aus Backup

Um Backups einer bestimmten VM wiederherzustellen, navigieren Sie zu dieser Detailseite des Arbeitsbereichs.

1. Blättern Sie nach unten zum Abschnitt Server, und klicken Sie auf den Servernamen
2. Blättern Sie nach unten zum Abschnitt Backups, und klicken Sie auf das Rad, um Ihre Optionen zu erweitern, und wählen Sie dann entweder aus
3. Wiederherstellen auf Server oder Wiederherstellen auf Festplatte (Verbinden Sie ein Laufwerk aus dem Backup, damit Sie Daten aus dem Backup auf die vorhandene Version der VM kopieren können).
4. Fahren Sie wie bei jedem anderen Restore-Szenario mit Ihrer Wiederherstellung fort.

> ⓘ Die Kosten hängen davon ab, welchen Zeitplan Sie beibehalten möchten, und werden vollständig von den Azure Backup-Kosten gesteuert. Die Backup-Preise für VMs finden Sie im Azure Kostenrechner: https://azure.microsoft.com/en-us/pricing/calculator/

Klonen Von Virtual Machines

Überblick

Mit dem Virtual Desktop Service (VDS) kann eine vorhandene Virtual Machine (VM) geklont werden. Diese Funktionalität soll die Verfügbarkeit der Servereinheit automatisch erhöhen, wenn die festgelegte Anzahl der Benutzer wächst ODER zusätzliche Server für verfügbare Ressourcenpools bereitgestellt werden.

Administratoren verwenden das Klonen in VDS auf zweierlei Weise:

1. Bei Bedarf automatische Erstellung eines neuen Servers von einem vorhandenen Client-Server aus
2. Proaktive, automatisierte Erstellung neuer Client-Server(s) zur automatischen Skalierung von Ressourcen basierend auf Regeln, die von Partnern definiert und gesteuert werden

Klonen zum Hinzufügen weiterer gemeinsam genutzter Server

Ein Klon ist eine Kopie einer vorhandenen Virtual Machine. Klonfunktionen sparen Zeit und unterstützen

Administratoren bei der Skalierung, da die Installation eines Gastbetriebssystems und von Applikationen sehr zeitaufwendig sein kann. Mit Klonen können Sie aus einer einzigen Installation und Konfiguration zahlreiche Kopien einer Virtual Machine erstellen. Dies sieht in der Regel wie folgt aus:

1. Installieren Sie alle gewünschten Anwendungen und Einstellungen auf einem TS- oder TSD-Server
2. Navigieren Sie zu Workspaces > Server-Abschnitt > Zahnrad-Symbol für den Quellserver > Klicken Sie auf Klonen
3. Ausführung des Klonprozesses (normalerweise 45-90 Minuten)
4. Im letzten Schritt wird der geklonte Server aktiviert und in den RDS-Pool gestellt, um neue Verbindungen zu akzeptieren. Geklonte Server erfordern möglicherweise eine individuelle Konfiguration nach dem Klonen, daher wartet VDS darauf, dass der Administrator den Server manuell rotieren muss.

Wiederholen Sie dies so oft wie nötig.[]

Um die Kapazität für Benutzer in einer gemeinsamen Host-Umgebung zu erhöhen, ist das Klonen eines Session-Hosts ein einfacher Prozess, der nur wenige Schritte in Anspruch nimmt.

1. Wählen Sie einen Sitzungshost zum Klonen aus. Vergewissern Sie sich, dass derzeit keine Benutzer am Computer angemeldet sind.
2. Navigieren Sie in VDS zum Arbeitsbereich des Ziel-Clients. Blättern Sie zum Abschnitt Server, klicken Sie auf das Zahnrad-Symbol, und wählen Sie Klonen. Dieser Prozess dauert viel Zeit und nimmt die Quellmaschine offline. Rechnen Sie mit einer Fertigstellung von mehr als 30 Minuten.

   [] []

3. Der Prozess wird den Server herunterfahren, den Server auf ein anderes Image klonen und Sysprep das Image auf das nächste TS# für den Kunden erstellen. Der Server zeigt in der Liste Server als *Type=Staged* und *Status=Aktivierung erforderlich* an.

   []

4. Melden Sie sich beim Server an und stellen Sie sicher, dass der Server bereit für die Produktion ist.

   []

5. Klicken Sie anschließend auf Aktivieren, um den Server zum Sitzungs-Host-Pool hinzuzufügen, um mit der Annahme von Benutzerverbindungen zu beginnen.

   []

VDS-Klonprozess Definition

Der Schritt-für-Schritt-Prozess wird unter VDS > Deployment > Task History unter jeder Clone Server-Operation beschrieben. Der Prozess umfasst 20+ Schritte, die mit dem Zugriff auf den Hypervisor beginnen, um den Klonprozess zu starten, und endet mit der Aktivierung des geklonten Servers. Der Klonprozess umfasst wichtige Schritte, darunter:

- DNS konfigurieren und Servername festlegen
- StaticIP zuweisen
- Zur Domäne hinzufügen
- Active Directory Aktualisieren

- VDS-DB aktualisieren (SQL-Instanz auf CWMGR1)
- Erstellen Sie Firewall-Regeln für den Klon

Neben dem Aufgabenverlauf können die Detailschritte für jeden Klonprozess im CwVmAutomationService-Log auf CWMGR1 im Virtual Desktop Deployment jedes Partners angezeigt werden. Die Überprüfung dieser Protokolldateien ist dokumentiert "Hier".

Automatisierte Erstellung neuer Server

Diese VDS-Funktion erhöht die Verfügbarkeit der Servereinheiten automatisch, da die definierte Benutzeranzahl zunimmt.

Der Partner definiert und verwaltet über VDS ("") > Client > Übersicht – VM-Ressourcen > Auto-Scaling. Mehrere Kontrollen werden ausgesetzt, um Partnern die automatische Skalierung zu aktivieren/deaktivieren sowie benutzerdefinierte Regeln für jeden Client zu erstellen, wie z. B. Anzahl/Benutzer/Server, zusätzlicher RAM pro Benutzer und Anzahl der Benutzer pro CPU.

Oben wird davon ausgegangen, dass das automatisierte Klonen für die gesamte Virtual Desktop-Implementierung aktiviert ist. Um beispielsweise das gesamte automatisierte Klonen zu beenden, deaktivieren Sie DCConfig im Fenster Erweitert die Option Servererstellung > automatisiertes Klonen aktiviert.

Wann wird der automatisierte Klonprozess ausgeführt?

Der automatisierte Klonprozess wird ausgeführt, wenn die tägliche Wartung konfiguriert wird. Der Standardwert ist Mitternacht, aber dieser kann bearbeitet werden. Ein Teil der täglichen Wartung ist es, den Thread „Ressourcen ändern“ für jeden Ressourcenpool auszuführen. Der Thread „Change Resources“ bestimmt die Anzahl der erforderlichen gemeinsamen Server, basierend auf der Anzahl der Benutzer, die die Poolkonfiguration benötigen (anpassbar; kann 10, 21, 30 usw. Benutzer pro Server sein).

„On Demand“ automatisiert die Erstellung eines neuen Servers

Diese VDS-Funktion ermöglicht das automatisierte „On Demand“-Klonen zusätzlicher Server zu verfügbaren Ressourcen-Pools.

Der VDS-Administrator meldet sich beim VDS an und findet unter Organisationen oder Arbeitsbereiche den spezifischen Client und öffnet die Registerkarte Übersicht. Die Server-Kachel führt alle Server (TSD1, TS1, D1 usw.) auf. Um einen einzelnen Server zu klonen, klicken Sie einfach auf das COG rechts neben dem Servernamen und wählen Sie Clone Option.

In der Regel dauert der Vorgang etwa eine Stunde. Die Dauer hängt jedoch von der Größe der VM und den verfügbaren Ressourcen des zugrunde liegenden Hypervisors ab. Bitte beachten Sie, dass der zu klonenden Server neu gestartet werden muss, damit Partner normalerweise nach mehreren Stunden oder während eines geplanten Wartungsfensters arbeiten.

Beim Klonen eines TSData-Servers wird einer der Schritte das Löschen der Ordner c:\Home, c:\Data und c:\Pro so sind sie keine doppelten Dateien. In diesem Fall konnte der Klonprozess Probleme beim Löschen dieser Dateien auftreten. Dieser Fehler ist unklar. Dies bedeutet in der Regel, dass das Klonereignis fehlgeschlagen ist, da eine offene Datei oder ein offener Prozess vorhanden war. Deaktivieren Sie als nächstes alle AV (da dies diesen Fehler erklären könnte).

Funktion zum automatischen Erhöhen des Festplattenspeicherplatz

Überblick

NetApp erkennt den Bedarf an Administratoren, eine einfache Möglichkeit zu geben, sicherzustellen, dass Benutzer immer über genügend Platz zum Abrufen und Speichern von Dokumenten verfügen. Dies gewährleistet auch, dass VMs über genügend freien Speicherplatz verfügen, um Backups erfolgreich durchzuführen und Administratoren sowie ihre Disaster Recovery- und Business Continuity-Pläne zu ermöglichen und zu unterstützen. Vor diesem Hintergrund haben wir eine Funktion entwickelt, die die verwendete verwaltete Festplatte automatisch auf die nächste Stufe erweitert, wenn nur wenig Speicherplatz vorhanden ist.

Dies ist eine Einstellung, die standardmäßig auf allen neuen VDS-Bereitstellungen in Azure angewendet wird, um sicherzustellen, dass alle Bereitstellungen Benutzer und Backups des Mandanten standardmäßig schützen.

Administratoren können dies überprüfen, indem sie zur Registerkarte Bereitstellungen navigieren, eine Implementierung auswählen und dann von dort aus eine Verbindung zu ihrem CWMGR1-Server herstellen. Öffnen Sie dann die DCConfig-Verknüpfung auf dem Desktop, und klicken Sie auf Erweitert, und scrollen Sie nach unten.

[]

Administratoren können den gewünschten freien Speicherplatz in GB oder in Prozent des Laufwerks ändern, der frei sein soll, bevor sie in dieselbe erweiterte Sektion von DCConfig auf die nächste Stufe der verwalteten Laufwerke wechseln.

[]

Einige praktische Anwendungsbeispiele:

- Wenn Sie sicherstellen möchten, dass auf Ihrem Laufwerk mindestens 50 GB verfügbar sind, setzen Sie MinFreeSpaceGB auf 50
- Wenn Sie sicherstellen möchten, dass mindestens 15 % Ihres Laufwerks frei sind, setzen Sie MinFreeSpacePercent von 10 auf 15.

Diese Aktion findet um Mitternacht in der Zeitzone des Servers statt.

Zugriff auf VDS-Anmeldedaten in Azure Key Vault

Überblick

CWASetup 5.4 ist eine Abkehr von früheren Azure-Bereitstellungsmethoden. Der Konfigurations- und Validierungsprozess optimiert den Bedarf an Informationen zur Beginn einer Implementierung. Viele dieser entfernten Eingabeaufforderungen gelten für Anmeldeinformationen oder Konten wie lokaler VM-Administrator, SMTP-Konto, Technischer Account, SQL SA usw. Diese Konten werden jetzt automatisch generiert und in Azure Key Vault gespeichert. Für den Zugriff auf diese automatisch generierten Konten ist standardmäßig ein weiterer Schritt erforderlich, wie unten beschrieben.

- Suchen Sie die „Key Vault“-Ressource und klicken Sie darauf:

[Breite = 75 %]

- Klicken Sie unter „Einstellungen“ auf „‘S‘Secrets“. Sie sehen eine Nachricht, die besagt, dass Sie nicht berechtigt sind, sich anzusehen:

  [Breite = 75 %]

- Fügen Sie eine ‘Zugriffsrichtlinie’ hinzu, um einem Azure AD-Konto (wie einem globalen Administrator oder Systemadministrator) Zugriff auf diese sensiblen Schlüssel zu gewähren:

  [Breite = 75 %]

- In diesem Beispiel wird ein globaler Administrator verwendet. Nach der Auswahl des Principal, klicken Sie ‘SAuswahl’, dann ‘Hinzufügen’:

  [Breite = 75 %]

- Klicken ‘SSie auf „Speichern“:

  [Breite = 75 %]

- Zugriffsrichtlinie wurde hinzugefügt:

  [Breite = 75 %]

- Überprüfen Sie die ‘Secrets’, ob das Konto nun Zugriff auf die Bereitstellungskonten hat:

  [Breite = 75 %]

- Wenn Sie z. B. die Domänenadministratorberechtigung zum Anmelden bei CWMGR1 und zum Aktualisieren der Gruppenrichtlinie benötigen, überprüfen Sie die Strings unter cjDomainAdministratorname und cjDomainAdministratorPassword, indem Sie auf jeden Eintrag klicken:

  [Breite = 75 %]

  [Breite = 75 %]

- Wert anzeigen oder kopieren:

  [Breite = 75 %]

Anwenden von Monitoring und Antivirus

Überblick

Virtual Desktop Service (VDS)-Administratoren sind für die Überwachung ihrer Plattforminfrastruktur (mindestens CWMGR1) und aller anderen Infrastrukturen und Virtual Machines (VMs) verantwortlich. In den meisten Fällen ordnen Administratoren das Monitoring der Infrastruktur (Hypervisor/SAN) direkt mit ihrem Datacenter-/IaaS-Provider zu. Die Administratoren sind für die Überwachung von Terminalservern und Datenservern verantwortlich, in der Regel durch die Bereitstellung ihrer bevorzugten RMM-Lösung (Remote Management and Monitoring).

Anti-Virus ist für den Administrator zuständig (für die Plattforminfrastruktur und Terminal/Datenserver VMs). Um diesen Prozess zu vereinfachen, wird auf VDS für Azure-Servern standardmäßig Windows Defender

angewendet.

> Achten Sie bei der Installation von Lösungen von Drittanbietern darauf, dass Firewalls und andere Komponenten, die die VDS-Automatisierung beeinträchtigen könnten, nicht berücksichtigt werden.

Genauer gesagt kann dies zu negativen Auswirkungen führen, wenn diese Anti-Virus-Agenten auf einem Server installiert werden, der von Virtual Desktop Service verwaltet wird.

Unsere allgemeine Anleitung ist, dass VDS-Plattformautomatisierung in der Regel nicht von Anti-Virus- oder Anti-Malware-Produkten beeinflusst wird, es eine bewährte Methode ist, Ausnahmen/Ausschlüsse für die folgenden Prozesse auf allen Plattformservern hinzuzufügen (CWMGR1, RDGateways, HTML5Gateways, FTP usw.):

```
*\paexec.exe
*\paexec_1_25.exe
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe
C:\Program Files\CloudWorkspace\CW Automation
Service\cw.automation.service.exe
C:\Program
Files\CloudWorkspace\CwVmAutomationService\CwVmAutomationService.exe
C:\Program Files (x86)\Myrtille\bin\Myrtille.Printer.exe
C:\Program Files (x86)\Myrtille\bin\Myrtille.Services.exe
```

Darüber hinaus empfehlen wir die sichere Auflistung der folgenden Prozesse auf Client-Servern:

```
C:\Program Files\CloudWorkspace\CwAgent\paexec.exe
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe
C:\Program Files\CloudWorkspace\CwRemoteApps\cwra.exe
C:\Program Files\CloudWorkspace\Pen\Pen.exe
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgent.exe
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgentMonitor.exe
```

Hinzufügen und Verschieben zugeordneter Laufwerke

Überblick

Standardmäßig sind drei freigegebene Ordner für Endbenutzersitzungen zugänglich. Diese Ordner befinden sich auf der definierten Speicherebene. Dies könnte auf dem File Server (TSD1 oder D1) oder einem Storage-Service wie Azure Files, Azure NetApp Files, NetApp CVO und NetApp CVS sein.

Um mit Klarheit zu helfen, wird dieser Artikel einen Beispielkunde mit dem Firmencode „NECA“ verwenden. In diesem Beispiel wird davon ausgegangen, dass ein einziger TDS1-Server mit dem Namen NECATSD1 bereitgestellt wurde. Wir werden durch den Prozess des Verschiebens eines Ordners auf eine andere VM (namens "NECAD1") arbeiten. Diese Strategie kann verwendet werden, um zwischen Partitionen auf demselben Rechner oder auf einen anderen Rechner zu verschieben, wie im folgenden Beispiel… dargestellt

Ordner Starting Location:

- Daten: NECATSD1\C:\Data\NECA\ (TSD1bedeutet, dass es der erste Terminalserver ist und auch als Datenserver funktioniert)
- FTP: NECATSD1\C:\FTP\NECA\
- Startseite: NECATSD1\C:\Home\NECA\

Ordner Endort:

- Daten: NECAD1\G:\Data\NECA\ (das D1bedeutet, dass es der erste Datenserver ist)
- FTP: Der gleiche Prozess gilt, es muss nicht dreimal beschrieben werden
- Home: Der gleiche Prozess gilt, es muss nicht 3x beschrieben werden

Fügen Sie eine Festplatte für G: Auf NECAD1 hinzu

1. Um den freigegebenen Ordner auf das Laufwerk E: Zu setzen, müssen wir einen über den Hypervisor hinzufügen (z.B. Azure Management Portal), initialisieren und formatieren Sie es

   []

2. Kopieren Sie den vorhandenen Ordner (auf NECATSD1, C:\)-Pfad zum neuen Speicherort (auf NECAD1, G:\)
3. Kopieren Sie die Ordner vom ursprünglichen Speicherort in den neuen Speicherort.

   []

Informationen aus der ursprünglichen Ordnerfreigabe erfassen (NECATSD1, C:\Data\NECA\)

1. Teilen Sie den neuen Ordner mit genau demselben Pfad wie den Ordner am ursprünglichen Speicherort.
2. Öffnen Sie den neuen Ordner NECAD1, G:\Data\ und in unserem Beispiel sehen Sie einen Ordner mit dem Firmencode „NECA“.

   []

3. Beachten Sie die Sicherheitsberechtigungen der ursprünglichen Ordnerfreigabe:

   []

4. Hier ist das typische Setup, aber es ist wichtig, die ursprünglichen Einstellungen zu kopieren, falls noch vorhandene Anpassungen vorhanden sind, die wir erhalten müssen. Alle anderen Benutzer-/Gruppenberechtigungen sollten aus der neuen Ordnerfreigabe entfernt werden
   - SYSTEM:Alle Berechtigungen zulässig
   - LocalClientDHPAccess (auf dem lokalen Computer):Alle Berechtigungen sind zulässig
   - ClientDHPAccess (in der Domäne): Alle Berechtigungen sind zulässig
   - NECA-all-Benutzer (auf der Domain): Alle Berechtigungen außer „Full Control“ erlaubt

Replizieren Sie den Freigabspfad und die Sicherheitsberechtigungen in den neuen freigegebenen Ordner

1. Gehen Sie zurück zum neuen Standort (NECAD1, G:\Data\NECA\ und teilen Sie den NECA-Ordner mit dem gleichen Netzwerkpfad (ohne die Maschine), in unserem Beispiel „neca-Data€“.

   []

2. Für die Benutzersicherheit fügen Sie alle Benutzer hinzu, legen Sie ihre Berechtigungen auf Übereinstimmung fest.

   []

3. Entfernen Sie alle anderen Benutzer-/Gruppenberechtigungen, die möglicherweise bereits vorhanden sind.

   []

Gruppenrichtlinie bearbeiten (nur wenn der Ordner auf eine neue Maschine verschoben wurde)

1. Als nächstes bearbeiten Sie die Drive Maps im Group Policy Management Editor. Für Azure AD-Domänendienste befindet sich die Zuordnung in:

   ```
   “Cloud Workspace Users > User Configuration > Preferences > Windows Settings> Drive Maps”
   ```

   []

2. Sobald die Gruppenrichtlinien aktualisiert werden, wird beim nächsten Verbindungszeitpunkt jedes Benutzers die zugeordneten Laufwerke angezeigt, die auf den neuen Speicherort verwiesen werden.
3. An diesem Punkt können Sie die ursprünglichen Ordner auf NECATSD1, C:\ löschen.

Fehlerbehebung

Wenn der Endbenutzer die zugeordneten Laufwerke mit einem roten X sieht, klicken Sie mit der rechten Maustaste auf das Laufwerk und wählen Sie trennen. Abmelden und wieder zurück im Laufwerk sind korrekt vorhanden.[]

Copyright-Informationen

Markeninformationen