Vereinfachtes

Virtual Desktop Service

NetApp
February 20, 2023

Inhaltsverzeichnis

Vereinfachtes

Implementierungen

Provisioning Collections

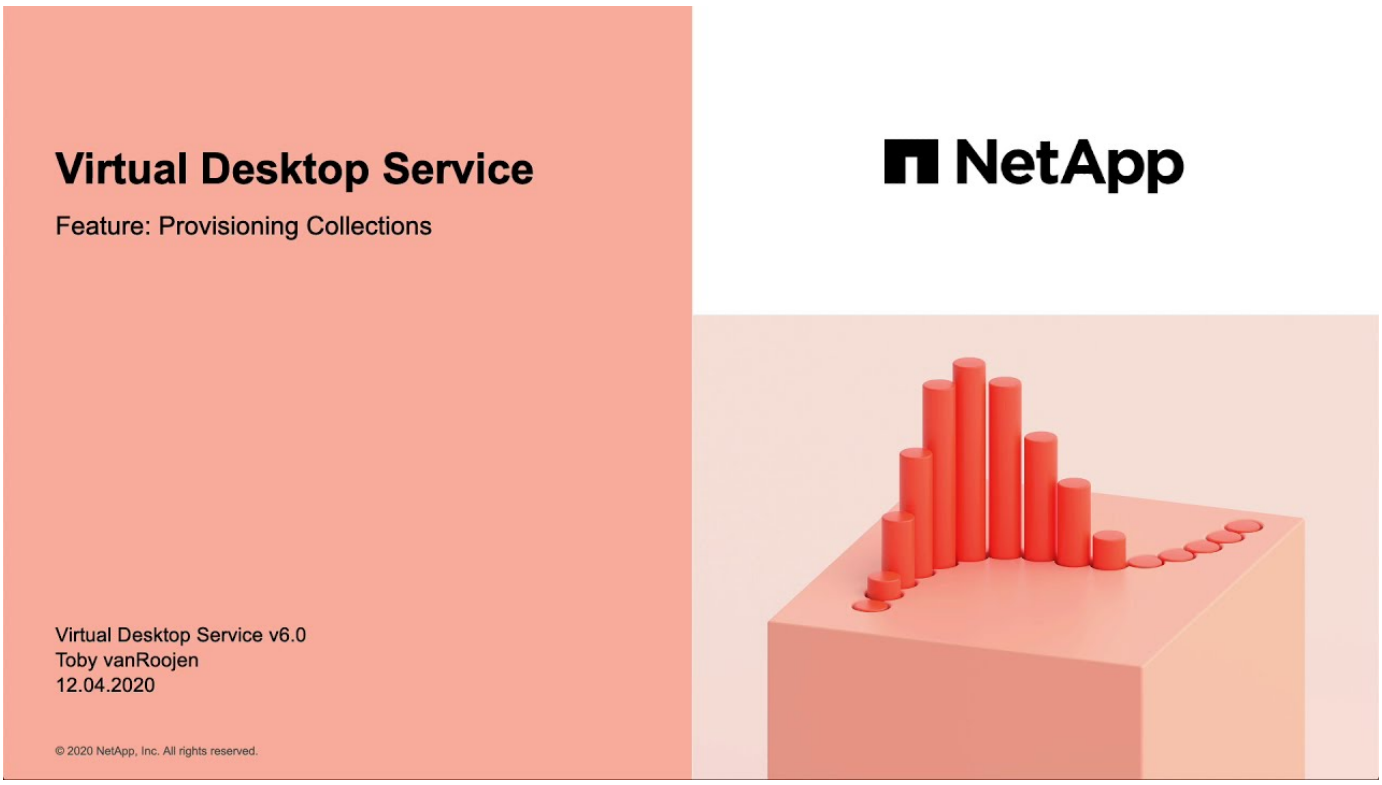
Überblick

Provisioning Collections ist eine Funktion von VDS, die sich mit der Erstellung und Verwaltung von VM-Images bezieht.

Im allgemeinen lautet der Workflow für die Provisioning Collection wie folgt:

1. Eine temporäre VM (z.B. „CWT1“) basiert auf einem vorhandenen Bild (entweder einem Lagerbild oder einer zuvor gespeicherten Provisioning Collection).
2. Der VDS-Administrator passt die temporäre VM an, um sie mit an ihre Anforderungen anzupassen "Skriptbasierte Ereignisse", "Verbindung zum Server herstellen" Und/oder Management Tools von Drittanbietern.
3. Sobald der VDS-Administrator angepasst ist, klicken Sie auf **Validieren** und lösen einen Validierungsprozess aus, der das Abschließen des Images automatisiert, wobei Sysprep ausgeführt wird, die temporäre VM gelöscht wird und das Image für die Bereitstellung im gesamten VDS verfügbar wird.

Video Demo - Verwalten von VM-Images für VDI-Session-Hosts



Provisioning-Erfassungstypen

Es gibt zwei unterschiedliche Arten von Sammlungen mit speziellen Anwendungsbeispielen, ***Shared*** und ***VDI***.

Freigegeben

Der Typ ***Shared*** ist eine Sammlung von VM Images(s), die entwickelt wurden, um eine gesamte Umgebung mit mehreren unterschiedlichen VM-Images und VM-Rollen bereitzustellen.

VDI

Der Typ ***VDI*** ist ein einzelnes VM-Image, das zur Nutzung und Wiederverwendung für die Bereitstellung mehrerer identischer VMs entwickelt wurde, die normalerweise zum Hosten von Benutzersitzungen verwendet werden. Bei allen Typen von AVD-Session-Hosts sollte der Typ *VDI* ausgewählt werden, auch bei Hosts, auf denen mehrere Sitzungen pro VM ausgeführt werden.

Erstellen einer neuen Provisioning Collection

Provisioning Collections finden Sie in der VDS-Schnittstelle in jeder Bereitstellung unter der Unterregisterkarte ***Provisioning Collections***.

[Breite = 75 %]

Um eine neue Sammlung zu erstellen

1. Klicken Sie auf die Schaltfläche **+ *Sammlung hinzufügen***.
2. Füllen Sie die folgenden Felder aus:
    a. **Name**
    b. **Beschreibung**(Optional)
    c. **Typ** - Shared oder VDI
    d. **Betriebssystem**
    e. **Share Drive** - Wenn diese VM verwendet wird, um Benutzer Profile oder Firmendaten zu hosten, wählen Sie den Laufwerkbuchstaben, auf dem gehostet wird. Falls nicht, mit „C“ belassen
    f. **Minimum Cache** - WENN Sie und VDS VMs erstellen, die für eine sofortige Bereitstellung bereitgehalten werden sollen, geben Sie die minimale Anzahl zwischengespeicherter VMs an, die beibehalten werden sollen. Wenn die Implementierung neuer VMs so lange warten kann, wie der Hypervisor zur Erstellung einer VM benötigt, kann dieser Wert auf „0“ gesetzt werden, um Kosten zu sparen.
    g. **Server Hinzufügen**
        i. **Rolle** (wenn der Typ „gemeinsam genutzt“ ausgewählt ist)
            A. **TS** - Diese VM funktioniert nur als Session-Host
            B. **Daten** - Diese VM wird keine Benutzersitzungen hosten
            C. **TSData** - Diese VM ist sowohl der Session-Host als auch der Speicher-Host (maximal: Ein TSData pro Workspace)
        ii. **VM Template** - Wählen Sie aus der Liste verfügbar sind sowohl Stock-Hypervisor-Images als auch zuvor gespeicherte Provisioning-Sammlungen zur Auswahl verfügbar.
            A. HINWEIS: Für Windows 7-Bilder aus dem Azure Marketplace ist PowerShell-Remoting nicht aktiviert. Um ein Windows 7-Image zu verwenden, müssen Sie in Ihrer gemeinsamen Bildergalerie ein benutzerdefiniertes Image mit aktiviertem PowerShell-Remoting bereitstellen.
            B. HINWEIS: Mit einer vorhandenen Provisioning Collection können Sie vorhandene Images im Rahmen eines geplanten Image-Upgrades aktualisieren und neu bereitstellen.
        iii. **Speichertyp** - Wählen Sie die Geschwindigkeit der OS-Festplatte unter Berücksichtigung der

Kosten und Leistung

iv. **Datenlaufwerk** - optional aktivieren Sie eine zweite Festplatte, die an dieses Bild angeschlossen ist, in der Regel für die oben in 2.e. referenzierte Speicherebene

   A. **Datenlaufwerk** - Wählen Sie die Geschwindigkeit der 2. (Daten) Festplatte unter Berücksichtigung von Kosten und Leistung

   B. **Datenlaufwerk-Größe (GB)** - Definieren Sie die Größe der 2. (Daten-)Festplatte unter Berücksichtigung von Kapazität, Kosten und Leistung

h. **Anwendungen hinzufügen** - Wählen Sie eine Anwendung aus der Anwendungsbibliothek aus, die (1) auf diesem Image installiert wird und (2) von VDS-Anwendungsberechtigungen verwaltet wird. (Dies gilt nur für RDS-Implementierungen. Für AVD-Arbeitsbereiche sollte es leer bleiben)

Anpassen der temporären VM

VDS enthält Funktionen, die das Entfernen des VM-Zugriffs von der VDS-Webschnittstelle ermöglichen. Standardmäßig wird ein lokales Windows-Administratorkonto mit einem rotierenden Passwort erstellt und an die VM weitergeleitet, sodass der lokale VDS-Admin-Zugriff hat, ohne dass die lokalen Anmeldedaten des lokalen Administrators bekannt sein müssen.

> ⓘ Die Funktion „mit Server verbinden“ verfügt über eine alternative Einstellung, bei der der VDS-Administrator bei jeder Verbindung zur Eingabe von Anmeldeinformationen aufgefordert wird. Diese Einstellung kann aktiviert/deaktiviert werden, indem das VDS-Administratorkonto im Abschnitt „Admin“ von VDS bearbeitet wird. Die Funktion heißt *Tech Account* und wenn Sie das Kontrollkästchen aktivieren, müssen bei der Verwendung von Connect to Server Anmeldedaten eingegeben werden. Wenn Sie dieses Kontrollkästchen deaktivieren, wird die automatische Injektion lokaler Windows-Admin-Anmeldeinformationen bei jeder Verbindung aktiviert.

Der VDS-Administrator muss lediglich eine Verbindung zur temporären VM über Connect to Server oder einen anderen Prozess herstellen und die Änderungen entsprechend vornehmen.

Überprüfung der Sammlung

Sobald die Anpassung abgeschlossen ist, kann der VDS-Administrator das Bild schließen und Sysprep durch Klicken auf **Validieren** aus dem Aktionen-Symbol.

[Management.Deployments.provisioning Sammlungen eda7e] |

Management.Deployments.provisioning_collections-ed97e.png

Verwenden der Sammlung

Nach Abschluss der Validierung ändert sich der Status der Provisioning Collection in **verfügbar**. Aus der Provisioning Collection kann der VDS-Administrator den **VM Template**-Namen identifizieren, der zur Identifizierung dieser Provisioning-Sammlung im gesamten VDS verwendet wird.

[Management.Deployments.provisioning Kollektionen f5a49] |

Management.Deployments.provisioning_collections-f5a49.png

Neuer Server

Auf der Seite Workspace > Servers kann ein neuer Server erstellt werden, und das Dialogfeld fordert die VM-Vorlage auf. Der Vorlagenname von oben ist in dieser Liste zu finden:

[Breite = 75 %]

VDS bietet eine einfache Möglichkeit, Sitzungshosts in einer RDS-Umgebung mithilfe von Provisioning Collections und der **Add Server**-Funktionalität zu aktualisieren. Dieser Vorgang kann ohne Beeinträchtigung der Endbenutzer durchgeführt und mit nachfolgenden Image-Aktualisierungen wiederholt werden, basierend auf vorherigen Bildwiederholungen. Weitere Informationen zu diesem Prozess finden Sie im **"RDS Session Host Update Prozess"** Abschnitt unten.

Neuer AVD-Hostpool

Auf der Seite Workspace > AVD > Host Pools können Sie einen neuen AVD Host Pool erstellen, indem Sie auf **+ Host Pool hinzufügen** klicken. Das Dialogfeld wird zur VM-Vorlage aufgefordert. Der Vorlagenname von oben ist in dieser Liste zu finden:

[Management.Deployments.provisioning Kollektionen ba2f5] |

Management.Deployments.provisioning_collections-ba2f5.png

Neue AVD-Sitzungshost(s)

Auf der Seite Workspace > AVD > Host Pool > Sitzungshosts können neue AVD-Sitzungshost(s) erstellt werden, indem Sie auf **+ Sitzungshost hinzufügen** klicken. Das Dialogfeld wird zur VM-Vorlage aufgefordert. Der Vorlagenname von oben ist in dieser Liste zu finden:

[Management.Deployments.provisioning Kollektionen ba5e9] |

Management.Deployments.provisioning_collections-ba5e9.png

VDS bietet eine einfache Möglichkeit, Sitzungshosts in einem AVD-Hostpool mithilfe von Provisioning Collections und der **Session-Host hinzufügen**-Funktion zu aktualisieren. Dieser Vorgang kann ohne Beeinträchtigung der Endbenutzer durchgeführt und mit nachfolgenden Image-Aktualisierungen wiederholt werden, basierend auf vorherigen Bildwiederholungen. Weitere Informationen zu diesem Prozess finden Sie im **"Aktualisierungsprozess für AVD-Sitzungshost"** Abschnitt unten.

Neuer Arbeitsbereich

Auf der Seite Workspaces kann ein neuer Arbeitsbereich erstellt werden, indem Sie auf **+ New Workspace** klicken. Das Dialogfeld wird zur Provisioning Collection aufgefordert. Der Name der Sammlung für freigegebene Provisioning wird in dieser Liste gefunden.

[Management.Deployments.provisioning Kollektionen 5c941] |

Management.Deployments.provisioning_collections-5c941.png

Neue Provisioning Collection –

Auf der Seite „Deployment > Provisioning Collection“ können Sie eine neue Provisioning Collection erstellen, indem Sie auf **+ Add Collection** klicken. Beim Hinzufügen von Servern zu dieser Sammlung wird das Dialogfeld zur VM-Vorlage aufgefordert. Der Vorlagenname von oben ist in dieser Liste zu finden:

[Management.Deployments.provisioning Kollektionen 9eac4] |

Management.Deployments.provisioning_collections-9eac4.png

Ergänzung 1 – RDS-Sitzungshosts

RDS Session Host Update-Prozess

VDS bietet eine einfache Möglichkeit, Sitzungshosts in einer RDS-Umgebung mithilfe von Provisioning Collections und der **Add Server**-Funktionalität zu aktualisieren. Dieser Vorgang kann ohne Beeinträchtigung der Endbenutzer durchgeführt und mit nachfolgenden Image-Aktualisierungen wiederholt werden, basierend auf vorherigen Bildwiederholungen.

Die Aktualisierung des RDS Session-Hosts erfolgt wie folgt:

1. Erstellen Sie eine neue VDI Provisioning Collection, passen Sie die Sammlung gemäß den obigen Anweisungen an und validieren Sie sie.
   a. Im Allgemeinen wird diese Provisioning-Sammlung auf der vorherigen VM-Vorlage aufgebaut und einen Prozess „Öffnen, Speichern unter“ emuliert.
2. Wenn die Provisioning Collection validiert wurde, navigieren Sie zur Seite *Workspace* > *Servers*, klicken Sie auf **+ Add Server**

   [Management.Deployments.provisioning collections.rds-Sitzung hostet e8204] |

Management.Deployments.provisioning_collections.rds_session_hosts-e8204.png

3. Wählen Sie **TS** als **Server-Rolle** aus
4. Wählen Sie die neueste **VM Template** aus. Wählen Sie je nach Ihren Anforderungen die passende Auswahl für **Maschinengröße** und **Speichertyp** aus. Lassen Sie **Datenlaufwerk** deaktiviert.
5. Wiederholen Sie diesen Vorgang für die Gesamtanzahl der für die Umgebung erforderlichen Session-Hosts.
6. Klicken Sie auf **Server hinzufügen**. Die Sitzungshosts bauen auf der Grundlage der ausgewählten VM-Vorlage auf und starten in nur 10-15 Minuten (je nach Hypervisor) online.
   a. Beachten Sie, dass die Sitzungshosts, die sich derzeit in der Umgebung befinden, letztendlich deaktiviert werden, nachdem dieser neue Host online geschaltet wurde. Die Erstellung von ausreichend neuen Hosts ist geplant, um den gesamten Workload in dieser Umgebung zu unterstützen.
7. Wenn ein neuer Host online geschaltet wird, bleibt die Standardeinstellung in **Neue Sitzungen deaktivieren**. Für jeden Sitzungshost kann der Schalter **Neue Sitzungen zulassen** verwendet werden, um zu verwalten, welche Hosts neue Benutzersitzungen empfangen können. Auf diese Einstellung können Sie zugreifen, indem Sie die Einstellungen jedes einzelnen Host-Servers bearbeiten. Sobald ausreichend neue Hosts aufgebaut und die Funktionalität bestätigt wurde, kann diese Einstellung sowohl auf den neuen als auch auf den alten Hosts verwaltet werden, um alle neuen Sitzungen an die neuen Hosts weiterzuleiten. Die alten Hosts, mit **Neue Sitzungen zulassen** auf **deaktiviert** eingestellt, können weiterhin bestehende Benutzersitzungen ausführen und hosten.

   [Management.Deployments.provisioning Collections.rds-Sitzung hostet 726d1] |

Management.Deployments.provisioning_collections.rds_session_hosts-726d1.png

8. Da sich Benutzer vom alten Host(s) abmelden und keine neuen Benutzersitzungen den alten Host(s) anschließen, können die alten Host(s), bei denen **Sessions = 0** gelöscht werden kann, durch Anklicken des Symbols **Aktionen** und Auswählen von **delete** gelöscht werden.

   [Management.Deployments.provisioning collections.rds Session hostet 45d32] |

Management.Deployments.provisioning_collections.rds_session_hosts-45d32.png

Ergänzung 2: AVD-Sitzungshosts

AVD-Host-Update-Prozess

VDS bietet eine einfache Möglichkeit, Sitzungshosts in einem AVD-Hostpool mithilfe von Provisioning Collections und der **Session-Host hinzufügen**-Funktion zu aktualisieren. Dieser Vorgang kann ohne Beeinträchtigung der Endbenutzer durchgeführt und mit nachfolgenden Image-Aktualisierungen wiederholt werden, basierend auf vorherigen Bildwiederholungen.

Die Aktualisierung des AVD Session-Hosts erfolgt wie folgt:

1. Erstellen Sie eine neue VDI Provisioning Collection, passen Sie die Sammlung gemäß den obigen Anweisungen an und validieren Sie sie.
    a. Im Allgemeinen wird diese Provisioning-Sammlung auf der vorherigen VM-Vorlage aufgebaut und einen Prozess „Öffnen, Speichern unter“ emuliert.
2. Sobald die Provisioning Collection validiert wurde, navigieren Sie zur Seite *Workspace* > *AVD* > *Host Pools*, und klicken Sie auf den Namen des Host-Pools
3. Klicken Sie auf der Seite *Host Pool* > *Session Hosts* auf **+ Session Host hinzufügen**

    [Management.Deployments.provisioning Sammlungen 9ed95] |

Management.Deployments.provisioning_collections-9ed95.png

4. Wählen Sie die neueste **VM Template** aus. Wählen Sie je nach Ihren Anforderungen die passende Auswahl für **Maschinengröße** und **Speichertyp** aus.
5. Geben Sie die **Anzahl der Instanzen** ein, die der Gesamtanzahl der erforderlichen Sitzungshosts entspricht. Normalerweise wird dies die gleiche Nummer sein wie derzeit im Host-Pool, aber es kann eine beliebige Zahl sein.
   a. Beachten Sie, dass die Sitzungshosts, die sich derzeit im Host-Pool befinden, letztendlich deaktiviert werden, nachdem dieser neue Host online geschaltet wurde. Planen Sie, dass die * Anzahl der eingegebenen Instanzen* ausreichend ist, um den gesamten Workload in diesem Host-Pool zu unterstützen.
6. Klicken Sie auf **Speichern**, die Session-Hosts bauen auf der ausgewählten VM-Vorlage auf und starten in nur 10-15 Minuten (je nach Hypervisor) online.
7. Wenn ein neuer Host online geschaltet wird, bleibt die Standardeinstellung in **Neue Sitzungen deaktivieren**. Für jeden Sitzungshost kann der Schalter **Neue Sitzungen zulassen** verwendet werden, um zu verwalten, welche Hosts neue Benutzersitzungen empfangen können. Sobald ausreichend neue Hosts aufgebaut und die Funktionalität bestätigt wurde, kann diese Einstellung sowohl auf den neuen als auch auf den alten Hosts verwaltet werden, um alle neuen Sitzungen an die neuen Hosts weiterzuleiten. Die alten Hosts, mit **Neue Sitzungen zulassen** auf **deaktiviert** eingestellt, können weiterhin bestehende Benutzersitzungen ausführen und hosten.

   [Management.Deployments.provisioning Kollektionen be47e] |

Management.Deployments.provisioning_collections-be47e.png

8. Da sich Benutzer vom alten Host(s) abmelden und keine neuen Benutzersitzungen den alten Host(s) anschließen, können die alten Host(s), bei denen **Sessions = 0** gelöscht werden kann, durch Anklicken des Symbols **Aktionen** und Auswählen von **delete** gelöscht werden.

   [Management.Deployments.provisioning Kollektionen cefb9] |

Management.Deployments.provisioning_collections-cefb9.png

VDS logische Hierarchie - Übersicht

Überblick

VDS organisiert Konzepte in verschiedene Schichten einer logischen Hierarchie. In diesem Artikel wird erläutert, wie sie zu einem gemeinsamen System passen.

VDS-Organisationsschema

Das VDS-Verwaltungsportal finden Sie unter https://manage.vds.netapp.com. Diese Webschnittstelle ist eine zentrale Konsole zum Verwalten aller VDS-bezogenen Objekte. Innerhalb der VDS-Weboberfläche sind die folgenden Komponenten- und logischen Container-Hierarchie vorhanden.

VDS-Bereitstellung

Bei *Deployment* handelt es sich um ein VDS-Konzept, das *VDS Workspace(s)* organisiert und enthält. In bestimmten Implementierungsarchitekturen kann eine Implementierung mehrere VDS-Arbeitsbereiche enthalten.

> Das Ausführen mehrerer VDS-Workspaces innerhalb einer einzelnen Implementierung heißt „Mandantenfähigkeit“ – dies ist nur eine Option bei RDS-Implementierungen. AVD-Implementierungen unterstützen diesen Ansatz nicht.

Eine Bereitstellung wird durch ihre Active Directory Domäne definiert, und es gibt eine 1:1-Beziehung zwischen der AD-Domäne und einer Bereitstellung.

Bestimmte VM-Ressourcen werden zur Unterstützung einer Implementierung implementiert, die bei der Implementierung für alle VDS-Arbeitsbereiche gemeinsam genutzt wird. Z. B. jede Implementierung enthält eine VM mit dem Namen „CWMGR1“, ein Server, auf dem VDS-Applikationen ausgeführt werden, eine SQL Express-Datenbank und vereinfacht das Management der VDS Workspace(s) (und der enthaltenen Ressourcen) in der Implementierung.

VDS-Arbeitsbereich

> Es besteht ein Unterschied zwischen einem „**VDS** Workspace“ und einem „**AVD** Workspace“.

Ein VDS Workspace ist ein logischer Container in der Implementierung für die Client-Ressourcen (Endbenutzer). Zu diesen Ressourcen zählen Virtual Machines (für Session-Hosts, Applikations-Server, Datenbank-Server, File Server usw.), virtuelles Netzwerk, Storage und andere Hypervisor-Infrastruktur.

Der VDS Workspace verfügt außerdem über Managementfunktionen zum Managen von Benutzern, Sicherheitsgruppen, Workload Scheduling, Applikationen, Automatisierung, VMs und AVD-Konfiguration.

In der Regel wird ein VDS Workspace mit einem einzelnen Unternehmen oder (in Unternehmensimplementierungen) einer Geschäftseinheit ausgerichtet.

VDS-Standorte

Innerhalb einer Implementierung können mehrere Standorte für unterschiedliche Infrastrukturanbieter erstellt werden, die alle innerhalb einer einzigen Bereitstellung gemanagt werden.

Dies ist hilfreich, wenn ein einzelnes Unternehmen oder eine Geschäftseinheit Benutzer und Applikationen über mehrere physische Standorte (z. B. Nordamerika und EMEA), Hypervisor-Abonnements (zur Ausrichtung der Kosten an Geschäftseinheiten) und sogar Hypervisoren (z. B. Benutzer in Azure, Google Compute und On-Premises HCI auf vSphere) hosten muss.

AVD-Arbeitsbereiche

Es besteht ein Unterschied zwischen einem „**VDS** Workspace“ und einem „**AVD** Workspace“.

Ein AVD Workspace ist ein logischer Container, der sich in einem VDS Workspace und einer VDS-Site befindet. Sie kann auf ähnliche Weise wie eine VDS-Site zum segmentieren von Management- und Betriebsrichtlinien in derselben Implementierung verwendet werden.

AVD-Host-Pools

AVD-Hostpools sind logische Container, die sich in einem AVD-Arbeitsbereich befinden und die Sitzungshosts und Anwendungsgruppen-Benutzer zum Server der Benutzersitzungen und zum Steuern des Zugriffs auf einzelne Ressourcen halten.

AVD-Anwendungsgruppen

Jeder AVD-Host-Pool beginnt mit einer einzigen „Desktop“-App-Gruppe. Benutzer und/oder Gruppen können dieser (oder einer anderen) App-Gruppe zugewiesen werden, um den zugewiesenen Benutzern den Zugriff auf die Ressourcen in der App-Gruppe zu ermöglichen.

In einem Host-Pool in VDS können weitere App-Gruppen erstellt werden. Alle zusätzlichen App-Gruppen sind „RemoteApp“-Anwendungsgruppen und dienen RemoteApp-Ressourcen, anstatt eine vollständige Windows-Desktop-Erfahrung zu ermöglichen.

Applikationen Unterstützt

Applikationsberechtigung

Überblick

VDS verfügt über eine robuste integrierte Anwendungsautomatisierung und Berechtigungsfunktionalität. Mit dieser Funktion können Benutzer auf verschiedene Anwendungen zugreifen, während eine Verbindung zu demselben Sitzungshost(s) hergestellt wird. Dies wird durch einige benutzerdefinierte GPOs, die Verknüpfungen ausblenden zusammen mit der Automatisierung selektiv platziert Verknüpfungen auf den Desktops der Benutzer.

Dieser Workflow gilt nur für RDS-Implementierungen. Informationen zu AVD-Anwendungsberechtigungen finden Sie unter "Anwendungsberechtigungsworkflow für AVD"

Anwendungen können Benutzern direkt oder über in VDS gemanagte Sicherheitsgruppen zugewiesen werden.

Im allgemeinen folgt der Bereitstellungsprozess von Applikationen diesen Schritten.

1. App(s) zum App-Katalog hinzufügen
2. Fügen Sie dem Arbeitsbereich App(s) hinzu
3. Installieren Sie die Anwendung auf allen Sitzungshosts
4. Wählen Sie den Verknüpfungspfad aus

5. Weisen Sie Benutzern und/oder Gruppen Apps zu

Die Schritte 3 und 4 können wie unten dargestellt vollständig automatisiert werden

Video-Präsentation

Fügen Sie Anwendungen zum App-Katalog hinzu

VDS-Anwendungsberechtigung beginnt mit dem App-Katalog. Dies ist eine Liste aller Anwendungen, die für die Bereitstellung in Endbenutzerumgebungen zur Verfügung stehen.

Führen Sie die folgenden Schritte aus, um dem Katalog Anwendungen hinzuzufügen

1. Melden Sie sich bei VDS an https://manage.cloudworkspace.com Verwendung der primären Anmeldedaten des Administrators
2. Klicken Sie oben rechts auf das Pfeilsymbol neben Ihrem Benutzernamen und wählen Sie Einstellungen aus.
3. Klicken Sie auf die Registerkarte App Catalog.
4. Klicken Sie in der Titelleiste des Anwendungskatalogs auf die Option App hinzufügen.
5. Um eine Gruppe von Anwendungen hinzuzufügen, wählen Sie die Option Apps importieren.
   a. Es wird ein Dialogfeld angezeigt, in dem eine Excel-Vorlage zum Herunterladen angezeigt wird, die das richtige Format für die Anwendungsliste erzeugt.
   b. Für diese Bewertung hat NetApp VDS eine Beispiel-Applikationsliste für den Import erstellt. Diese finden Sie hier.
   c. Klicken Sie auf den Bereich Hochladen und wählen Sie die Datei mit der Anwendungsvorlage aus. Klicken Sie auf die Schaltfläche Importieren.
6. Wenn Sie einzelne Anwendungen hinzufügen möchten, wählen Sie die Schaltfläche App hinzufügen, und es wird ein Dialogfeld angezeigt.

a. Geben Sie den Namen der Anwendung ein.

b. Mit einer externen ID kann eine interne Tracking-ID eingegeben werden, z. B. eine Produkt-SKU oder ein Abrechnungsverfolgungscode (optional).

c. Aktivieren Sie das Kontrollkästchen Abonnement, wenn Sie über die Anwendungen als Abonnementprodukt berichten möchten (optional).

d. Wenn das Produkt nicht nach Version installiert wird (z. B. Chrome), aktivieren Sie das Kontrollkästchen Version nicht erforderlich. So können Produkte mit kontinuierlicher Aktualisierung installiert werden, ohne ihre Versionen nachzuverfolgen.

e. Wenn ein Produkt mehrere benannte Versionen unterstützt (z. B. QuickBooks), müssen Sie dieses Kontrollkästchen aktivieren, damit Sie mehrere Versionen installieren und jede verfügbare Version in der Liste der Anwendungen, die für und Endbenutzer berechtigt sein können, VDS-spezifisch besitzen können.

f. Aktivieren Sie „kein Benutzer-Desktop-Symbol“, wenn VDS kein Desktop-Symbol für dieses Produkt bereitstellen soll. Dies wird für „Backend“-Produkte wie SQL Server verwendet, da Endbenutzer keine Anwendung haben, auf die sie zugreifen können.

g. „App muss zugeordnet sein“ setzt die Notwendigkeit, eine zugehörige App zu installieren. Für eine Client-Server-Anwendung kann es z. B. erforderlich sein, dass auch SQL Server oder MySQL installiert werden muss.

h. Wenn Sie das Feld Lizenz erforderlich aktivieren, wird angezeigt, dass VDS eine Lizenzdatei für eine Installation dieser Anwendung anfordern sollte, bevor der Anwendungsstatus auf aktiv gesetzt wird. Dieser Schritt wird auf der Seite Anwendungsdetails von VDS durchgeführt.

i. Sichtbar für Alle – Anwendungsberechtigungen können auf bestimmte Teilpartner in einer Mehrkanalhierarchie beschränkt werden. Klicken Sie zu Evaluierungszwecken auf das Kontrollkästchen, damit alle Benutzer es in ihrer Liste der verfügbaren Anwendungen sehen können.

Fügen Sie die Anwendung dem Arbeitsbereich hinzu

Um den Bereitstellungsprozess zu starten, fügen Sie die App zum Arbeitsbereich hinzu.

Führen Sie dazu die folgenden Schritte aus

1. Klicken Sie Auf Arbeitsbereiche
2. Blättern Sie nach unten zu „Apps“
3. Klicken Sie Auf Hinzufügen
4. Aktivieren Sie die Anwendung(en), geben Sie die erforderlichen Informationen ein, klicken Sie auf Anwendung hinzufügen und klicken Sie auf Apps hinzufügen.

Installieren Sie die Anwendung manuell

Sobald die Anwendung dem Arbeitsbereich hinzugefügt wurde, müssen Sie diese Anwendung auf allen Sitzungshosts installieren. Dies kann manuell und/oder automatisiert werden.

Führen Sie die folgenden Schritte aus, um Anwendungen manuell auf Sitzungshosts zu installieren

1. Navigieren Sie zu Service Board.
2. Klicken Sie auf die Aufgabe des Service Board.
3. Klicken Sie auf die Servernamen, um eine Verbindung als lokaler Administrator herzustellen.
4. Installieren Sie die App(s), bestätigen Sie, dass die Verknüpfung zu dieser Anwendung im Startmenü-Pfad gefunden wird.

a. Für Server 2016 und Windows 10: C:\ProgramData\Microsoft\Windows\Startmenü\Programme.

5. Gehen Sie zurück zur Aufgabe des Service-Mainboards, klicken Sie auf Durchsuchen und wählen Sie entweder die Verknüpfung oder einen Ordner mit Verknüpfungen aus.
6. Je nachdem, welche Option Sie auswählen, wird auf dem Desktop des Endbenutzers angezeigt, wenn die App zugewiesen wurde.
7. Ordner sind großartig, wenn eine Anwendung tatsächlich mehrere Anwendungen ist. Z. B. „Microsoft Office“ ist einfacher als Ordner mit jeder App als Verknüpfung im Ordner bereitzustellen.
8. Klicken Sie Auf Installation Abschließen.
9. Öffnen Sie bei Bedarf das erstellte Symbol Serviceboard Task hinzufügen, und bestätigen Sie, dass das Symbol hinzugefügt wurde.

Anwendungen zu Benutzern zuweisen

Die Anwendungsberechtigungen werden von VDS verwaltet, und die Anwendung kann Benutzern auf drei Arten zugewiesen werden

Anwendungen zu Benutzern zuweisen

1. Navigieren Sie zur Seite „Benutzerdetails“.
2. Navigieren Sie zum Abschnitt Anwendungen.
3. Aktivieren Sie das Kontrollkästchen neben allen für diesen Benutzer erforderlichen Anwendungen.

Weisen Sie einer Anwendung Benutzer zu

1. Navigieren Sie auf der Seite Arbeitsbereichdetails zum Abschnitt Anwendungen.
2. Klicken Sie auf den Namen der Anwendung.
3. Aktivieren Sie das Kontrollkästchen neben den Benutzern, die die Anwendung verwenden.

Anwendungen und Benutzer zu Benutzergruppen zuweisen

1. Navigieren Sie zu den Benutzern und Gruppen-Details.
2. Fügen Sie eine neue Gruppe hinzu oder bearbeiten Sie eine vorhandene Gruppe.
3. Weisen Sie der Gruppe Benutzer und Anwendungen zu.

Anwendungsberechtigungsworkflow für AVD

Überblick

In einer Azure Virtual Desktop-Umgebung (AVD) wird der Applikationszugriff durch Mitgliedschaft in der Applikationsgruppe gemanagt.

Dieser Workflow gilt nur für AVD-Bereitstellungen. Dokumentation der RDS-Anwendungsberechtigungen finden Sie unter "Workflow für Applikationsberechtigung für RDS"

AVD ist ein gut dokumentierter Service und es gibt viele "Öffentliche Ressourcen zur Information". VDS überschneidet nicht die Standardart, wie AVD funktioniert. Dieser Artikel soll vielmehr veranschaulichen, wie VDS das Standardkonzept in allen AVD-Bereitstellungen annähert.

Überprüfen der "VDS logische Hierarchie - Übersicht" Artikel kann vor oder während der Überarbeitung dieses Artikels nützlich sein.

Die Ansicht Für Endbenutzer

In Azure Virtual Desktop erhält jeder Endbenutzer von seinem AVD-Administrator Zugriff auf RemoteApp(s) und/oder Desktops. Dies erfolgt über die Zuweisung der App-Gruppe in VDS.

RemoteApp bezieht sich auf eine Anwendung, die Remote auf dem Session-Host ausgeführt wird, aber auf dem lokalen Gerät ohne den Desktop-Kontext dargestellt wird. Diese Applikation wird allgemein als „Streaming-Applikation“ bezeichnet und sieht auf dem lokalen Gerät wie eine lokale Applikation aus, läuft jedoch im Sicherheitskontext und in der Storage- und Computing-Schicht des Session-Hosts.

Desktop bezieht sich auf die volle Windows-Erfahrung, die auf dem Session-Host ausgeführt wird und auf dem lokalen Gerät dargestellt wird, normalerweise in einem Vollbildfenster. Dieser Desktop selbst wird allgemein als „Remote-Desktop“ bezeichnet und enthält alle Anwendungen, die auf diesem Sitzungshost installiert sind und vom Benutzer über das Fenster der Desktop-Sitzung gestartet werden können.

Bei der Anmeldung erhält der Endbenutzer die ihm vom Administrator zugewiesenen Ressourcen. Nachfolgend sehen Sie ein Beispiel für die Ansicht, die ein Endbenutzer beim Anmelden mit seinem AVD-Client sehen kann. Dies ist ein komplizierteren Beispiel, oftmals hat ein Endbenutzer nur einen dingle Desktop oder eine RemoteApp zugewiesen. Endbenutzer können auf eine dieser Ressourcen doppelklicken, um die Applikation bzw. den Desktop zu starten.

[Management.Deployments.vds-Standorte 0e49c] | *Management.Deployments.vds_sites-0e49c.png*

In diesem komplexeren Beispiel hat dieser Benutzer Zugriff auf zwei verschiedene Desktop-Sitzungen und 4 verschiedene Streaming-Applikationen:

- * Verfügbare Desktops*
  - NVIDIA GPU-Desktop
  - Gemeinsamer AVD Pool Desktop
  - Betrieb 2 Pool Desktop
- * Verfügbare RemoteApps*
  - AutoCAD 2021
  - Revit 2021
  - Microsoft Edge
  - Notizblock

Hinter den Kulissen werden diese Applikationen und Desktops auf verschiedenen Session-Hosts, AVD-Workspaces gehostet und können sogar in verschiedenen Azure Regionen gehostet werden.

Die folgende Grafik veranschaulicht den Hosting-Bereich und die Zuweisung dieser Ressourcen für den Endbenutzer.

[Management.Deployments.vds-Standorte 0e880] | *Management.Deployments.vds_sites-0e880.png*

Wie oben dargestellt, werden die verschiedenen für diesen Endbenutzer verfügbaren Ressourcen auf verschiedenen Session-Hosts in verschiedenen Host-Pools gehostet und von verschiedenen IT-Abteilungen in unterschiedlichen AVD-Arbeitsbereichen gemanagt. Diese Ressourcen könnten in diesem Beispiel nicht angezeigt werden, aber mithilfe der Funktion VDS-Sites auch in verschiedenen Azure Regionen und/oder

Abonnements gehostet werden.

Desktop-Zugriff Wird Bereitgestellt

Standardmäßig beginnt jeder Host-Pool mit einer einzelnen Applikationsgruppe, die verwendet wird, um Zugriff auf die Windows-Desktop-Erfahrung zu zuweisen. Alle auf diesen Session-Hosts installierten Anwendungen können den Endbenutzern, die dieser App-Gruppe zugewiesen sind, zugänglich gemacht werden.

So aktivieren Sie die Desktop-Ressource für Benutzer in VDS:

1. Navigieren Sie zur Seite Arbeitsbereiche > AVD > Host Pool > App Groups, und klicken Sie auf die App-Gruppe für die „Desktop“-Ressource.

   [Management.Applications.avd-Anwendungsberechtigungen-Workflow 349fe] |

Management.Applications.avd_application_entitlement_workflow-349fe.png

2. Klicken Sie in der App-Gruppe auf Bearbeiten

   [Management.Applications.avd-Anwendungsberechtigungen-Workflow 3bcfc] |

Management.Applications.avd_application_entitlement_workflow-3bcfc.png

3. Im Dialogfeld „Bearbeiten“ können Sie dieser App-Gruppe Benutzer nach Benutzer und/oder nach Gruppen hinzufügen oder diese entfernen.

   [Management.Applications.avd-Anwendungsberechtigungen-Workflow 07ff0] |

Management.Applications.avd_application_entitlement_workflow-07ff0.png

RemoteApp Access wird bereitgestellt

Um den Zugriff auf RemoteApps bereitzustellen, muss innerhalb des Host-Pools eine neue App-Gruppe erstellt werden. Nach dem Erstellen müssen die entsprechenden Apps dieser App-Gruppe zugewiesen werden.

> Alle Anwendungen auf diesen Sitzungshosts stehen bereits allen Benutzern zur Verfügung, die der „Desktop“ AppGroup dieses Hostpools zugewiesen sind. Es ist nicht notwendig, auch Zugriff über eine RemoteApp App App-Gruppe bereitzustellen, nur um den Zugriff auf Apps zu ermöglichen. Eine RemoteApp-App-Gruppe ist nur erforderlich, um den Zugriff auf Apps zu ermöglichen, die auf dem lokalen Gerät als Streaming-App ausgeführt werden.

Erstellen Sie eine neue App-Gruppe

1. Navigieren Sie zur Seite Arbeitsbereiche > AVD > Host Pool > App Groups, und klicken Sie auf die Schaltfläche *+ App Group* hinzufügen

   [Management.Applications.avd-Anwendungsberechtigungen-Workflow d33da] |

Management.Applications.avd_application_entitlement_workflow-d33da.png

2. Geben Sie den Namen, den Arbeitsbereich und den Anzeigenamen für diese App-Gruppe ein. Wählen Sie die Benutzer und/oder Gruppen aus, die zugewiesen werden sollen, und klicken Sie auf „*Save*“

   [Management.Applications.avd-Anwendungsberechtigungen-Workflow 242eb] |

Management.Applications.avd_application_entitlement_workflow-242eb.png

Anwendungen zur App-Gruppe hinzufügen

1. Navigieren Sie zur Seite Arbeitsbereiche > AVD > Host Pool > App Groups, und klicken Sie auf die App-Gruppe für die RemoteApp-Ressource.

   [Management.Applications.avd-Anwendungsberechtigungen-Workflow 3dcde] |

Management.Applications.avd_application_entitlement_workflow-3dcde.png

2. Klicken Sie in der App-Gruppe auf Bearbeiten

   [Management.Applications.avd-Anwendungsberechtigungen-Workflow 27a41] |

Management.Applications.avd_application_entitlement_workflow-27a41.png

3. Scrollen Sie nach unten zum Abschnitt „Remote Apps“. Dieser Abschnitt kann einen Moment dauern, bis VDS die Sitzungshosts abfragt, um verfügbare Apps für das Streaming anzuzeigen.

   [Management.Applications.avd-Anwendungsberechtigungen-Workflow 1e9f2] |

Management.Applications.avd_application_entitlement_workflow-1e9f2.png

4. Suchen Sie alle Apps, auf die die Benutzer in diesen Applikationsgruppen als RemoteApp-Ressource zugreifen sollen, und wählen Sie diese aus.

Skriptbasierte Ereignisse

Skriptbasierte Ereignisse

Überblick

Mithilfe von skriptbasierten Ereignissen kann der erweiterte Administrator mithilfe eines Mechanismus individuelle Automatisierungsfunktionen für Systemwartung, Benutzerwarnungen, Gruppenrichtlinienmanagement oder andere Ereignisse erstellen. Skripte können als ausführbarer Prozess mit Argumenten bezeichnet werden oder als Argumente für ein anderes ausführbares Programm verwendet werden. Mit dieser Funktionalität können Skripts kombiniert und verschachtelt werden, um komplexe Anpassungs- und Integrationsanforderungen zu unterstützen.

Ein detailliertes Beispiel für skriptbasierte Ereignisse in Aktion finden Sie im "Leitfaden Zur Anwendungsberechtigung".

Zudem ermöglicht das Skript-Ereignis die Erstellung von Automatisierungen, die kein Skript zur Verarbeitung benötigen, sondern der Automatisierungsfluss wird durch einen Systemauslöser gestartet und führt ein bestehendes Programm oder Systemdienstprogramm mit optionalen Argumenten aus.

Skripte Ereignisse enthalten sowohl ein **Repository** von Skripten als auch **Aktivitäten**. Skripte enthalten die Anweisungen auf **Was** zu tun, während Aktivitäten die Skripte mit dem entsprechenden Trigger und Ziel (**wann und wo**) für das Skript verknüpfen.

Repository

Auf der Registerkarte „Repository“ wird eine Liste aller Skripts angezeigt, die über Ihr VDS-Konto bereitgestellt werden können. Dies ist ein benutzerdefiniertes Repository, das von allen Administratoren in Ihrer VDS-Instanz gemeinsam genutzt wird. Der Zugriff auf skriptbasierte Ereignisse kann über die Seite „_VDS > Administratoren > Berechtigungen “ gemanagt werden.

[Sub.Management.skriptbasierte Ereignisse.skriptbasierte Ereignisse 1ce76] |

sub.Management.Scripted_Events.scripted_events-1ce76.png

Kundenfilter

Jede VDS-Administratororganisation verfügt über eine private Bibliothek mit Skripten, die von ihrem Unternehmen erstellt und/oder angepasst wurden. Diese Skripte sind als Skripttyp „Kunde“ definiert. Kundenskripte ein werden von jedem VDS-Administrator mit entsprechenden Administratorberechtigungen zum Abschnitt „skriptbasierte Ereignisse“ gelöscht und bearbeitet.

Globaler Filter

NetApp veröffentlicht zudem eine Bibliothek mit globalen Skripts, die in allen VDS-Administratororganisationen identisch sind. Diese Skripte sind als Skripttyp „Global“ definiert. Globale Skripts können von keinem VDS-Administrator bearbeitet oder gelöscht werden. Vielmehr können globale Skripte „geklont“ werden und das resultierende Skript ist ein „Kunde“-Skript, das bearbeitet und verwendet werden kann.

Skript Herunterladen

Durch die Möglichkeit, die mit einem Skript-Ereignis verknüpfte Skriptdatei herunterzuladen, kann der VDS-Administrator die zugrunde liegende Skriptdatei vor der Bereitstellung überprüfen und bearbeiten. Das Ausführen eines Skripts, das du nicht vollständig verstehst, ist niemals ratsam.

[Sub.Management.skriptbasierte Ereignisse.skriptbasierte Ereignisse 02a9b] |

sub.Management.Scripted_Events.scripted_events-02a9b.png

Skript Hinzufügen

Durch Klicken auf die Schaltfläche + *Skript hinzufügen* wird eine neue Seite zum Erstellen eines Skripts und Speichern im Repository geöffnet.

[Management.skriptbasierte Ereignisse.skriptbasierte Ereignisse a53fa] |

Management.Scripted_Events.scripted_events-a53fa.png

Die folgenden Felder müssen ausgefüllt werden, um ein neues Skript zu erstellen:

- **Name**
- **Skriptdatei Einschließen**
  - Ja - ermöglicht das Hochladen und Ausführen einer Skriptdatei (z. B. einer .ps1-Datei) durch die ausführbare Datei „Ausführen mit“.
  - Nein - entfernt das Feld „Script File“ (unten) und führt einfach den Befehl „Execute with“ und „Arguments“ aus
- **Skriptdatei**
  - Wenn *Skript-Datei einschließen = ja* dieses Feld sichtbar ist und das Hochladen einer Skriptdatei ermöglicht.
- **Mit** Ausführen
  - Definiert den Pfad der ausführbaren Datei, die zum Ausführen der Skriptdatei oder des Befehls verwendet wird, der ausgeführt wird.
  - Wenn Sie zum Beispiel PowerShell verwenden möchten, würde der Wert „Ausführen mit“ *C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe* sein
- **Argumente**
  - Definiert alle zusätzlichen Argumente, die gegen den Befehl „mit ausführen“ ausgeführt werden.
  - VDS bietet einige kontextbezogene Variablen, die verwendet werden können, darunter:
    - %companycode% - Unternehmenscode zur Laufzeit
    - %Servername% - VM-Name zur Laufzeit
    - %samaccountname% - <username>.<companycode>
    - %applicationname% - angeforderter Anwendungsname zur Laufzeit
    - %Scriptname% - Skriptname zur Laufzeit
    - %Username% - Benutzername@loginIdentifier zur Laufzeit
- **Dokumentation URL**
  - In diesem Feld kann der Autor des Skripts mit der außerhalb von VDS gefundenen Dokumentation verknüpfen, z. B. mit einem vom VDS-Administrator verwendeten Knowledge Base-System.

Skript Bearbeiten

Wenn Sie auf den Namen eines Skripts im Repository klicken, wird eine neue Seite mit Details zum Skript und einer Aktionsschaltfläche geöffnet, um **edit** zu öffnen.

Beim Bearbeiten eines Skripts können dieselben Felder wie oben im dokumentiert bearbeitet werden "Skript Hinzufügen" Abschnitt.

Auf dieser Skript-Detailseite können Sie auch **das Skript löschen und *download** alle hochgeladenen Skriptdateien.

[Management.skriptbasierte Ereignisse.skriptbasierte Ereignisse 3e756] |

Management.Scripted_Events.scripted_events-3e756.png

Aktivitäten

Aktivitäten verknüpfen ein Skript aus dem Repository mit einer Implementierung, einer Untermenge von VMs und einem auslösenden Ereignis.

[Management.skriptbasierte Ereignisse.skriptbasierte Ereignisse f971c] |

Management.Scripted_Events.scripted_events-f971c.png

Aktivität Hinzufügen

Durch Klicken auf die Schaltfläche + *Add Activity* wird eine neue Seite zum Erstellen einer Aktivität geöffnet.

[Management.skriptbasierte Ereignisse.skriptbasierte Ereignisse 02ef8] |

Management.Scripted_Events.scripted_events-02ef8.png

Die folgenden Felder müssen ausgefüllt werden, um einen neuen Vorgang zu erstellen:

- **Name**
- **Beschreibung** (Optional)
- * Bereitstellung*
- **Skript**
- **Argumente**
- **Aktiviert** Kontrollkästchen
- **Ereigniseinstellungen**

Aktivitätsauslösern

[Sub.Management.skriptbasierte Ereignisse.skriptbasierte Ereignisse CDFCD] |

sub.Management.Scripted_Events.scripted_events-cdfcd.png

- **Anwendungsinstallation**
  - Dies wird ausgelöst, wenn der VDS-Administrator auf der Seite *Workspace* > *Applications* auf „+ Hinzufügen…“ klickt.
  - Mit dieser Auswahl können Sie eine Anwendung aus der Anwendungsbibliothek auswählen und die Verknüpfung der Anwendung vordefinieren.
  - Detaillierte Anweisungen für diesen Auslöser sind im hervorgehoben "*Adobe Reader DC* -Skript -Dokumentation installieren".
- **Anwendung Deinstallieren**
  - Dies wird ausgelöst, wenn der VDS-Administrator auf der Seite *Workspace* > *Applications* auf „Actions > Uninstall“ klickt.
  - Mit dieser Auswahl können Sie eine Anwendung aus der Anwendungsbibliothek auswählen und die Verknüpfung der Anwendung vordefinieren.
  - Detaillierte Anweisungen für diesen Auslöser sind im hervorgehoben "*Adobe Reader DC*-Skript -Dokumentation deinstallieren".
- **Clone Server**
  - Dies wird ausgelöst, wenn die Klonfunktion auf eine vorhandene VM durchgeführt wird
- **Create Cache**
  - Dies wird jedes Mal ausgelöst, wenn eine neue VM durch VDS erstellt wird, um einen Sammel-Cache für die Bereitstellung zu nutzen
- **Create Client**
  - Dieser Vorgang wird bei jedem Hinzufügen einer neuen Client-Organisation zu VDS ausgelöst
- **Server Erstellen**
  - Diese Funktion wird jedes Mal ausgelöst, wenn eine neue VM mithilfe von VDS erstellt wird
- **Benutzer Erstellen**
  - Dieser Vorgang wird bei jedem Hinzufügen eines neuen Benutzers über VDS ausgelöst
- **Benutzer Löschen**
  - Dies wird jedes Mal ausgelöst, wenn ein neuer Benutzer über VDS gelöscht wird
- **Manuell**
  - Dies wird von einem VDS-Administrator manuell über die Seite „skriptbasierte Ereignisse > Aktivitäten“ ausgelöst
- **Manuelles Anwendungs-Update**
- **Geplant**
  - Dieser wird ausgelöst, wenn das definierte Datum/die definierte Uhrzeit erreicht wird
- **Server Starten**
  - Dies wird bei jedem Booten einer VM ausgelöst

Durch Klicken auf den Eintrag *Name* wird ein Dialogfeld geöffnet, in dem die Aktivität bearbeitet werden kann.

Command Center

Command Center Command: Übersicht

Überblick

Das Command Center ist eine ausführbare Datei, die auf dem CWMGR1 Platform Server in der Bereitstellung ausgeführt wird. Der Zugriff erfolgt über eine Verbindung zur VM CWMGR1 und die lokale Ausführung auf dieser VM.

Diese Applikation wurde für Fehlerbehebung, Diagnose und erweiterte Managementfunktionen konzipiert. Diese Applikation wird hauptsächlich von den internen Entwicklungs- und Support-Teams von NetApp verwendet, allerdings werden einige Funktionen gelegentlich von Kunden-Administratoren verwendet. Diese Dokumentation wird zur Unterstützung der Verwendung von Auswahlfunktionen bereitgestellt. Verwenden Sie diese Befehle sorgfältig und in Zusammenarbeit mit dem NetApp Support Team.

Command Center Wird Ausgeführt

So führen Sie die Command Center-Anwendung aus:

1. Verbindung zum Server herstellen Klicken Sie auf der Seite *VDS* > *Bereitstellung* > *Plattformserver* auf das Symbol *Actions* und wählen Sie „Verbinden“ aus.

   [Management.command Übersicht Mitte 68087] | *Management.command_center_overview-68087.png*

2. Geben Sie bei Aufforderung zur Eingabe von Anmeldedaten die Anmeldedaten für den Domänenadministrator ein
   a. Der Benutzer muss Mitglied der Sicherheitsgruppe „CW-Infrastructure“ sein. Aus Konsistenzgründen empfehlen wir, diese Mitgliedschaft hinzuzufügen, indem wir den Benutzer zur Gruppe „Level 3 Technicians“ in *AD* > *Cloud Workspace* > *Cloud Workspace Tech Users* > *Groups* machen

      [Management.command Mittelübersicht 1c42d] | *Management.command_center_overview-1c42d.png*

3. Suchen Sie das Desktop-Symbol für *Command Center* und führen Sie es aus

   [Management.command Übersicht Mitte 3c860] | *Management.command_center_overview-3c860.png*

   a. Um die erweiterte Registerkarte zu aktivieren, starten Sie die Anwendung mit dem Schalter "-showadvancedtab".

Registerkarte „Vorgänge“

[Management.command Übersicht Zentrum b614e] | *Management.command_center_overview-b614e.png*

Im Menü **Befehl** können Sie aus einer Liste von Aktionen auswählen (siehe unten).

Sobald ein Befehl ausgewählt wurde, können die Daten mit Bereitstellungsdaten über die Schaltfläche **Daten laden** ausgefüllt werden. Die Schaltfläche Daten laden wird auch verwendet, um den Hypervisor nach Daten zu fragen, sobald eine frühere Auswahl getroffen wurde (z. B. Laden einer Liste der verfügbaren Backup-Daten nach Auswahl einer bestimmten VM aus einer Dropdown-Liste)

[Management.command Übersicht Mitte 85417] | *Management.command_center_overview-85417.png*

Nachdem Sie eine Auswahl auf einem Befehl getroffen haben, wird der ausgewählte Prozess durch Klicken auf **Befehl ausführen** ausgeführt.

Um Protokolle zu prüfen, klicken Sie auf die Schaltfläche **Alle Protokolle anzeigen**. Die RAW-Textdatei wird geöffnet, wobei die neuesten Einträge unten angezeigt werden.

Befehlsliste

- "Vorlage in Galerie kopieren"

Betrieb

Command Center Befehl: Vorlage in Galerie kopieren

Warnung Für Command Center

> Das Command Center ist eine Anwendung, die auf dem CWMGR1-Plattformserver in der Bereitstellung ausgeführt wird. Diese Applikation wurde für Fehlerbehebung, Diagnose und erweiterte Managementfunktionen konzipiert. Diese Applikation wird hauptsächlich von den internen Entwicklungs- und Support-Teams von NetApp verwendet, allerdings werden einige Funktionen gelegentlich von Kunden-Administratoren verwendet. Diese Dokumentation wird zur Unterstützung der Verwendung von Auswahlfunktionen bereitgestellt. Verwenden Sie diese Befehle sorgfältig und in Zusammenarbeit mit dem NetApp Support Team. Weitere Informationen finden Sie im "Command Center – Übersicht" Artikel:

Vorlage in Galerie kopieren Übersicht

[Management.command Center.Operations.Vorlage in Galerie 67ea4 kopieren] |

Management.command_center.operations.copy_template_to_gallery-67ea4.png

Wenn eine VDI Provisioning Collection fertiggestellt ist, wird das Image in Azure als Image gespeichert und kann auf derselben VDS-Site bereitgestellt werden. Um das Image für die Bereitstellung in einer anderen Azure-Region innerhalb desselben Abonnements verfügbar zu machen, wird die Funktion „Vorlage in Galerie kopieren“ verwendet. Durch diese Aktion wird das VM-Image in die Galerie „gemeinsam genutzt“ kopiert und in alle ausgewählten Regionen repliziert.

[Management.command Center.Operations.Vorlage in Galerie ed821 kopieren] |

Management.command_center.operations.copy_template_to_gallery-ed821.png

Dropdown-Liste VM Template Availability in VDS

Nach Abschluss der Replikation wird das Image in VDS in der Dropdown-Liste zur Auswahl von VM-Vorlagen bei der Bereitstellung neuer VMs angezeigt. Das gemeinsam genutzte Bild steht für die Bereitstellung in allen Regionen zur Verfügung, die beim Kopieren ausgewählt wurden.

[Management.command Center.Operations.Vorlage in Galerie 04bd8 kopieren] |

Management.command_center.operations.copy_template_to_gallery-04bd8.png

VM Images, die in der Shared Gallery gespeichert sind, werden mit ihrer Version in Form von "-x.x.x" angefügt, wobei die Version mit der Bildversion im Azure Portal übereinstimmt.

[Management.command Center.Operations.Vorlage in Galerie e598 kopieren] |

Management.command_center.operations.copy_template_to_gallery-ee598.png

Die Replikation des Bildes kann eine Weile dauern (je nach Größe des Bildes) und der Status kann durch Klicken auf die Version (z.B. 1.0.0) in der Spalte „Name“, wie in der Abbildung oben hervorgehoben.

Regionale Verfügbarkeit

Implementierungen können nur in den Bereichen durchgeführt werden, in denen das Image repliziert wurde. Diese Option kann im Azure-Portal durch Anklicken der 1.x.x und dann auf *Update Replication* wie hier dargestellt geprüft werden:

[Management.command Center.Operations.Vorlage in Galerie 9b63a kopieren] |

Management.command_center.operations.copy_template_to_gallery-9b63a.png

Ressourcenoptimierung

Workload-Planung

Workload Scheduling ist eine Funktion, die das Zeitfenster für den aktiven Betrieb der Umgebung einplanen kann.

Die Workload-Planung kann auf „Always On“, „Always Off“ oder „Scheduled“ eingestellt werden. Wenn auf „geplant“ gesetzt, können die ein- und Ausschaltzeiten so fein eingestellt werden wie ein anderes Zeitfenster für jeden Wochentag.

[]

Wenn ein geplantes Ausschalten geplant wird, entweder über „Always Off“ oder „Scheduled“, werden alle virtuellen Mandantenmaschinen heruntergefahren. Plattformserver (wie z.B. CWMGR1) bleiben aktiv, um Funktionen wie Wake-on-Demand zu ermöglichen.

Workload Schedule funktioniert in Verbindung mit anderen Funktionen zur Ressourcenoptimierung, einschließlich Live Scaling und Wake On Demand.

Wake-on-Demand

Wake On Demand (WOD) ist eine zum Patent angemeldete Technologie, mit der die entsprechenden VM-Ressourcen für einen Endbenutzer aktiviert werden können, um unbeaufsichtigten Zugriff auf 24/7 zu ermöglichen, selbst wenn Ressourcen für den Betrieb geplant sind.

WOD für Remote Desktop Services

In RDS verfügt der VDS Windows Client über eine integrierte Wake-On-Demand-Integration und kann die entsprechenden Ressourcen ohne zusätzliche Benutzeraktionen aktivieren. Der Kunde muss lediglich seine normale Anmeldung einleiten, und der Client benachrichtigt sie über eine kurze Verzögerung, die die VM(s) aktiviert sind. Dieser Client (und damit die automatisierte Weckfunktion) steht nur zur Verfügung, wenn eine Verbindung von einem Windows-Gerät zu einer RDS-Umgebung hergestellt wird.

Ähnliche Funktionen sind für RDS-Implementierungen in den VDS Web-Client integriert. Der VDS Web Client ist verfügbar unter: ""

Wake-on-Demand-Funktionen sind nicht in den Microsoft RD-Client (für Windows oder eine andere Plattform) und keine anderen RD-Clients von Drittanbietern integriert.

Wake-On-Demand für Azure Virtual Desktop

In AVD sind die einzigen Clients, die für die Verbindung verwendet werden können, Microsoft bereitgestellt und enthalten somit nicht die Wake-on-Demand-Funktionalität.

VDS verfügt über eine Self-Service Wake-on-Demand-Funktion für AVD über den VDS Web Client. Der Web-Client kann dazu genutzt werden, die entsprechenden Ressourcen zu aktivieren, dann kann die Verbindung über den Standard-AVD-Client initiiert werden.

So aktivieren Sie VM-Ressourcen in AVD:

1. Stellen Sie eine Verbindung zum VDS Web Client unter her ""

2. Melden Sie sich mit den AVD-Benutzeranmeldeinformationen an
    - Eine Warnmeldung gibt die Meldung _ „Sie haben die AVD-Dienste von Microsoft zur Verfügung. Klicken SIE HIER, um den Status anzuzeigen und Offline Host Pools zu starten.“_
3. Nach dem Klicken auf „*HERE*“ wird eine Liste der verfügbaren Host-Pools sowie der Link „Click to Start“ in der Status-Spalte angezeigt

    []

4. *Klicken Sie auf den Link Start* und warten Sie 1-5 Minuten, bis der Status in „Online“ geändert wird, und zeigen Sie ein grünes Statussymbol an
5. Stellen Sie eine Verbindung mit AVD über Ihren normalen Prozess her

Live-Skalierung

Live-Skalierung funktioniert in Verbindung mit Workload Scheduling, indem die Anzahl der Online-Sitzungshosts während der geplanten aktiven Zeit, wie in Workload Scheduling konfiguriert, verwaltet wird. Wenn es für den Offline-Modus geplant ist, wird die Verfügbarkeit des Host-Sitzungs durch Live Scaling nicht gesteuert. Die Live-Skalierung wirkt sich nur auf Shared-Benutzer und Shared-Server in RDS- und AVD-Umgebungen, VDI-Benutzer und VDI-VMs aus diesen Berechnungen aus. Alle anderen VM-Typen sind nicht betroffen.

> Die Einstellung AVD_Load Balancer type_ interagiert mit dieser Konfiguration, daher sollte bei der Auswahl dieser Einstellung ebenfalls darauf Wert genommen werden. Kosteneinsparungen werden durch eine „erste Tiefe“-Lösung maximiert, während die Leistung der Endbenutzer mit einem breiten First-Typ maximiert wird.

Wenn die Live-Skalierung ohne Optionen aktiviert ist, wählt die Automation Engine automatisch Werte für die Anzahl der Extra Powered auf Servern, für freigegebene Benutzer pro Server und für max. Freigegebene Benutzer pro Server aus.

- Die *Anzahl von Extra Powered auf Servern* ist standardmäßig auf 0 eingestellt, was bedeutet, dass 1 Server 24/7 ausführt.
- Die *Shared Users per Server* ist standardmäßig die Anzahl der Benutzer im Unternehmen geteilt durch die Anzahl der Server.
- Die Option „ *max Shared Users per Server*“ ist standardmäßig „skalierbar“.

Live Scaling schaltet die Server ein, wenn sich Benutzer anmelden und sie ausschalten, wenn sich Benutzer abmelden.

Die Stromversorgung eines zusätzlichen Servers wird automatisch ausgelöst, sobald die Gesamtzahl der aktiven Benutzer die Anzahl der freigegebenen Benutzer pro Server erreicht hat, multipliziert mit der Gesamtzahl der Powered on Servers.

```
 e.g. With 5 Shared Users per Server set (this is the default # we'll use
for all examples in this article) and 2 servers running, a 3rd server
won't be powered up until server 1 & 2 both have 5 or more active users.
Until that 3rd server is available, new connections will be load balanced
all available servers. In RDS and AVD Breadth mode, Load balancing sends
users to the server with the fewest active users (like water flowing to
the lowest point). In AVD Depth mode, Load balancing sends users to
servers in a sequential order, incrementing when the Max Shared Users
number is reached.
Durch die Live-Skalierung werden zudem die Server abgeschaltet, um Kosten
zu sparen. Wenn ein Server über 0 aktive Benutzer verfügt und ein anderer
Server über eine verfügbare Kapazität unter _freigegebene Benutzer pro
Server_ verfügt, wird der leere Server heruntergefahren.
```

Der Einschalten des nächsten Servers kann einige Minuten dauern. In bestimmten Situationen kann die Geschwindigkeit der Anmeldungen die Verfügbarkeit neuer Server überbieten. Wenn sich zum Beispiel 15 Personen in 5 Minuten anmelden, landen sie alle auf dem ersten Server (oder werden einer Sitzung verweigert), während ein 2. Und 3. In diesem Szenario kann die Überlastung eines einzelnen Servers durch zwei Strategien entschärfung werden:

1. Aktivieren Sie *Anzahl von Extra Powered auf Servern*, damit die zusätzlichen Server eingeschaltet und verfügbar sind, um Verbindungen zu akzeptieren und der Plattform Zeit zu geben, weitere Server zu erweitern.
    a. Bei Aktivierung wird die Zahl dem berechneten Bedarf hinzugefügt. Wenn Sie z. B. auf einen zusätzlichen Server (und 6 verbundene Benutzer) gesetzt haben, wären aufgrund der Anzahl der Benutzer zwei Server aktiv, plus einen dritten aufgrund der Einstellung „*Extra Powered on Servers*“.
2. Aktivieren Sie *max Shared Users pro Server*, um eine harte Grenze für die Anzahl der Benutzer pro Server zu setzen. Neue Verbindungen, die dieses Limit überschreiten würden, werden abgelehnt, der Endbenutzer erhält eine Fehlermeldung und muss es in ein paar Minuten erneut versuchen, sobald der zusätzliche Server verfügbar ist. Wenn eingestellt, definiert diese Zahl auch die Tiefe von AVD-freigegebenen Servern.
    a. Angenommen, das Delta zwischen *Shared Benutzern pro Server* und *max Shared Users pro Server* ist angemessen, sollten die neuen Server verfügbar sein, bevor das Maximum, jedoch in den extremsten Situationen (ungewöhnlich große Login-Anstürme) erreicht wird.

Skalierung der VM-Ressourcen

Die Skalierung der VM-Ressourcen ist eine optionale Funktion, mit der sich Größe und Anzahl der Host-VMs in einer Umgebung ändern lassen.

Bei Aktivierung berechnet VDS die entsprechende Größe und Menge der Host-VMs für Sitzungen basierend auf den von Ihnen ausgewählten Kriterien. Zu diesen Optionen gehören: Aktive Benutzer, benannte Benutzer, Serverlast und Behoben.

[]

Die Größe der VMs ist in der in der UI ausgewählten Familie von VMs enthalten, die durch Dropdown geändert werden kann. (Z. B. *DV3-Standardfamilie* in Azure)

[]

Skalierung je nach Anwender

Die unten stehende Funktion verhält sich gleichermaßen für „aktive Benutzer“ oder „Benutzeranzahl“. Bei der Benutzeranzahl handelt es sich um eine einfache Anzahl aller mit einem VDS-Desktop aktivierten Benutzer. Aktive Benutzer ist eine berechnete Variable, die auf den Daten der letzten 2 Wochen der Benutzersitzung basiert.

Bei der Berechnung auf Basis von Benutzern wird die Größe (und die Anzahl) der Session-Host-VMs auf Basis der definierten RAM- und CPU-Anforderungen berechnet. Der Administrator kann GB RAM, Anzahl der vCPU-Kerne pro Benutzer sowie zusätzliche nicht variable Ressourcen definieren.

In der Abbildung unten wird jedem Benutzer 2 GB RAM und 1/2 eines vCPU-Kerns zugewiesen. Zusätzlich beginnt der Server mit 2 vCPU Cores und 8 GB RAM.

[]

Außerdem kann der Administrator die Maximalgröße festlegen, auf die eine VM maximal erreichbar ist. Wenn die Umgebung erreicht ist, werden sie horizontal skaliert, indem zusätzliche VM-Session-Hosts hinzugefügt werden.

In dem Screenshot unten ist jede VM auf 32 GB RAM und 8 vCPU Kerne beschränkt.

[]

Wenn alle diese Variablen definiert sind, berechnet VDS die geeignete Größe und Menge der Host VMs für die Session. Dadurch wird die Zuweisung der entsprechenden Ressourcen auch beim Hinzufügen und Entfernen von Benutzern erheblich vereinfacht.

Skalierung je nach Serverlast

Bei der Berechnung auf Basis der Serverlast werden die Größe (und die Anzahl) der Host-VMs der Session basierend auf den durchschnittlichen CPU-/RAM-Auslastungsraten gemäß VDS im Zeitraum von zwei Wochen berechnet.

Wenn der maximale Schwellenwert überschritten wird, erhöht VDS die Größe oder erhöht die Menge, um die durchschnittliche Nutzung innerhalb des Bereichs wiederherzustellen.

Wie die benutzerbasierte Skalierung können auch die VM-Familie und die maximale VM-Größe definiert werden.

[]

Andere aktive Ressourcen

Workload Scheduling steuert die Plattformserver wie CWMGR1 nicht, da sie benötigt werden, um die Wake-On-Demand-Funktionalität auszulösen und andere Plattformaufgaben zu ermöglichen. Außerdem sollte 24/7 für den normalen Umgebungsbetrieb ausgeführt werden.

Zusätzliches Einsparpotenzial kann durch die Deaktivierung der gesamten Umgebung erreicht werden, wird aber nur für Umgebungen empfohlen, die nicht im produktiven Betrieb sind. Dies ist eine manuelle Aktion, die im Abschnitt Bereitstellungen von VDS ausgeführt werden kann. Um die Umgebung wieder in den normalen Status zu bringen, ist auf derselben Seite auch ein manueller Schritt erforderlich.

[] []

Anwenderadministration

Verwalten Von Benutzerkonten

Neuen Benutzer erstellen

Administratoren können Benutzer hinzufügen, indem sie auf Arbeitsbereiche > Benutzer und Gruppen > Hinzufügen/Importieren klicken

Benutzer können einzeln oder mit einem Massenimport hinzugefügt werden.

[Breite = 25 %]

Einschließlich genauer E-Mail und Handy # in dieser Phase verbessert den Prozess der Aktivierung MFA später erheblich.

Sobald Sie Benutzer erstellt haben, können Sie auf ihren Namen klicken, um Details zu sehen, wie wann sie erstellt wurden, ihren Verbindungsstatus (ob sie gerade angemeldet sind oder nicht) und was ihre spezifischen Einstellungen sind.

Aktivieren des Virtual Desktop für vorhandene AD-Benutzer

Wenn Benutzer bereits in AD vorhanden sind, können Sie den Virtual Desktop der Benutzer einfach aktivieren, indem Sie auf das System neben ihrem Namen klicken und dann ihren Desktop aktivieren.[Breite = 50 %]

Nur für den Azure AD-Domänendienst: Damit die Anmeldung funktioniert, muss der Password-Hash für Azure AD-Benutzer synchronisiert werden, um die NTLM- und Kerberos-Authentifizierung zu unterstützen. Am einfachsten ist es, das Benutzerpasswort in Office.com oder im Azure Portal zu ändern, sodass die Hash-Synchronisierung des Passworts erzwungen wird. Der Synchronisierungszyklus für Domain Service-Server kann bis zu 20 Minuten dauern, sodass Änderungen an Passwörtern in Azure AD in der Regel 20 Minuten in AADDS und damit in der VDS-Umgebung wieder aufnehmen können.

Benutzerkonto(e) löschen

Benutzerinformationen bearbeiten

Auf der Benutzerdetailseite können Änderungen an den Benutzerdetails wie Benutzername und Kontaktdaten vorgenommen werden. Die E-Mail- und Telefonwerte werden für den SSPR-Prozess (Self Service Password Reset) verwendet.

[]

Sicherheitseinstellungen für Benutzer bearbeiten

- VDI-Benutzer aktiviert – eine RDS-Einstellung, die, wenn sie aktiviert ist, einen dedizierten VM-Session-Host erstellt und diesem Benutzer als einzigen Benutzer zugewiesen wird, der eine Verbindung zu ihm herstellt. Im Rahmen der Aktivierung dieses Kontrollkästchens wird der CWMS-Administrator aufgefordert, VM-Image, -Größe und -Speichertyp auszuwählen.
    - AVD-VDI-Benutzer sollten auf der AVD-Seite als VDI-Hostpool verwaltet werden.

- Kontoablauf aktiviert – ermöglicht dem CWMS-Administrator, ein Ablaufdatum auf dem Endbenutzerkonto festzulegen.
- Passwort zurücksetzen bei der nächsten Anmeldung erzwingen – fordert den Endbenutzer auf, sein Passwort bei der nächsten Anmeldung zu ändern.
- Multi-Faktor Auth aktiviert – aktiviert MFA für den Endbenutzer und fordert ihn zur Einrichtung von MFA bei der nächsten Anmeldung auf.
- Mobile Drive Enabled – eine ältere Funktion, die in aktuellen RDS- oder AVD-Bereitstellungen nicht verwendet wird.
- Lokaler Laufwerkszugriff aktiviert – ermöglicht es dem Endbenutzer, von der Cloud-Umgebung aus auf den lokalen Gerätebsspeicher zuzugreifen, einschließlich Kopieren/Einfügen, USB-Massenspeicher und Systemlaufwerke.
- Wake-on-Demand aktiviert – für RDS-Benutzer, die sich über den CW-Client für Windows verbinden, erhalten sie dadurch die Berechtigung, ihre Umgebung zu nehmen, wenn sie außerhalb der normalen Arbeitszeiten gemäß Workload Schedule eine Verbindung herstellen.

Gesperrtes Konto

Standardmäßig sperren fünf fehlgeschlagene Anmeldeversuche das Benutzerkonto. Das Benutzerkonto wird nach 30 Minuten entsperrt, es sei denn, *Enable Password Komplexitäts* ist aktiviert. Wenn die Passwortkomplexität aktiviert ist, wird das Konto nicht automatisch entsperrt. In beiden Fällen kann der VDS-Administrator das Benutzerkonto manuell von der Seite Benutzer/Gruppen im VDS entsperren.

Benutzerpasswort zurücksetzen

Setzt das Benutzerpasswort zurück.

Hinweis: Beim Zurücksetzen von Azure AD-Benutzerpasswörtern (oder beim Entsperren eines Kontos) kann es eine Verzögerung von bis zu 20 Minuten geben, wenn das Zurücksetzen über Azure AD propagiert.

Administratorzugriff

Wenn dies ermöglicht wird, erhält der Endbenutzer eingeschränkten Zugriff auf das Management-Portal für seinen Mandanten. Zu den üblichen Nutzungsmöglichkeiten gehört die Bereitstellung eines vor-Ort-Mitarbeiters, der auf das Zurücksetzen von Peers-Passwörtern, die Zuweisung von Anwendungen oder das Zulassen von manuellen Server-Wakeup-Zugriffen zugreifen kann. Berechtigungen, die steuern, welche Bereiche der Konsole angezeigt werden können, werden auch hier festgelegt.

Benutzer abmelden

Angemeldete Benutzer können vom VDS-Administrator von der Seite Benutzer/Gruppen im VDS abgemeldet werden.

Applikationen Unterstützt

Zeigt die in diesem Arbeitsbereich bereitgestellte Anwendung an. Das Kontrollkästchen stellt die Apps für diesen spezifischen Benutzer bereit. Vollständige Dokumentation zum Application Management finden Sie hier. Der Zugriff auf Anwendungen kann auch über die App-Schnittstelle oder auf Security Groups gewährt werden.

Benutzerprozesse anzeigen/beenden

Zeigt die Prozesse an, die derzeit in der Sitzung des Benutzers ausgeführt werden. Auch von dieser Schnittstelle können Prozesse beendet werden.

Managen Von Datenberechtigungen

Aus der Sicht des Endbenutzers

Endbenutzer von virtuellen Desktops können auf mehrere zugeordnete Laufwerke zugreifen. Zu diesen Laufwerken zählen eine auf FTA zugängliche Teamfreigabe, eine Company File Share und ihr Home Drive (für Dokumente, Desktop usw.…). . Alle diese zugeordneten Laufwerke verweisen auf eine zentrale Storage-Ebene entweder auf ein Storage-Service (z. B. Azure NetApp Files) oder auf einer File Server-VM.

Je nach Konfiguration des Benutzers kann der Benutzer nicht über die Laufwerke H: Oder F: Freigelegt haben, können sie nur ihren Desktop, Dokumente, etc… sehen Ordner. Darüber hinaus werden gelegentlich bei der Bereitstellung verschiedene Laufwerksbuchstaben vom VDS-Administrator festgelegt.[]

[]

Verwalten von Berechtigungen

MIT VDS können Administratoren Sicherheitsgruppen und Ordnerberechtigungen über das VDS-Portal bearbeiten.

Sicherheitsgruppen

Sicherheitsgruppen werden verwaltet, indem Sie im Abschnitt Gruppen auf Workspaces > Mandantenname > Benutzer & Gruppen > klicken

In diesem Abschnitt können Sie:

1. Erstellen Sie neue Sicherheitsgruppen
2. Benutzer zu den Gruppen hinzufügen/entfernen
3. Anwendungen Gruppen zuweisen
4. Aktivieren/Deaktivieren des Zugriffs auf lokale Laufwerke für Gruppen

[]

Ordnerberechtigungen

Ordnerberechtigungen werden verwaltet, indem Sie auf Workspaces > Mandantenname > Verwalten klicken (im Abschnitt Ordner).

In diesem Abschnitt können Sie:

1. Ordner Hinzufügen/Löschen
2. Weisen Sie Benutzern oder Gruppen Berechtigungen zu
3. Passen Sie die Berechtigungen an schreibgeschützt, vollständige Kontrolle und Keine an

[]

Applikationsberechtigung

Überblick

VDS verfügt über eine robuste integrierte Anwendungsautomatisierung und Berechtigungsfunktionalität. Mit dieser Funktion können Benutzer auf verschiedene Anwendungen zugreifen, während eine Verbindung zu demselben Sitzungshost(s) hergestellt wird. Dies wird durch einige benutzerdefinierte GPOs, die

Verknüpfungen ausblenden zusammen mit der Automatisierung selektiv platziert Verknüpfungen auf den Desktops der Benutzer.

Dieser Workflow gilt nur für RDS-Implementierungen. Informationen zu AVD-Anwendungsberechtigungen finden Sie unter "Anwendungsberechtigungsworkflow für AVD"

Anwendungen können Benutzern direkt oder über in VDS gemanagte Sicherheitsgruppen zugewiesen werden.

Im allgemeinen folgt der Bereitstellungsprozess von Applikationen diesen Schritten.

1. App(s) zum App-Katalog hinzufügen
2. Fügen Sie dem Arbeitsbereich App(s) hinzu
3. Installieren Sie die Anwendung auf allen Sitzungshosts
4. Wählen Sie den Verknüpfungspfad aus
5. Weisen Sie Benutzern und/oder Gruppen Apps zu

Die Schritte 3 und 4 können wie unten dargestellt vollständig automatisiert werden

Video-Präsentation

Fügen Sie Anwendungen zum App-Katalog hinzu

VDS-Anwendungsberechtigung beginnt mit dem App-Katalog. Dies ist eine Liste aller Anwendungen, die für die Bereitstellung in Endbenutzerumgebungen zur Verfügung stehen.

Führen Sie die folgenden Schritte aus, um dem Katalog Anwendungen hinzuzufügen

1. Melden Sie sich bei VDS an https://manage.cloudworkspace.com Verwendung der primären Anmeldedaten des Administrators
2. Klicken Sie oben rechts auf das Pfeilsymbol neben Ihrem Benutzernamen und wählen Sie Einstellungen

aus.

3. Klicken Sie auf die Registerkarte App Catalog.
4. Klicken Sie in der Titelleiste des Anwendungskatalogs auf die Option App hinzufügen.
5. Um eine Gruppe von Anwendungen hinzuzufügen, wählen Sie die Option Apps importieren.
   a. Es wird ein Dialogfeld angezeigt, in dem eine Excel-Vorlage zum Herunterladen angezeigt wird, die das richtige Format für die Anwendungsliste erzeugt.
   b. Für diese Bewertung hat NetApp VDS eine Beispiel-Applikationsliste für den Import erstellt. Diese finden Sie hier.
   c. Klicken Sie auf den Bereich Hochladen und wählen Sie die Datei mit der Anwendungsvorlage aus. Klicken Sie auf die Schaltfläche Importieren.
6. Wenn Sie einzelne Anwendungen hinzufügen möchten, wählen Sie die Schaltfläche App hinzufügen, und es wird ein Dialogfeld angezeigt.
   a. Geben Sie den Namen der Anwendung ein.
   b. Mit einer externen ID kann eine interne Tracking-ID eingegeben werden, z. B. eine Produkt-SKU oder ein Abrechnungsverfolgungscode (optional).
   c. Aktivieren Sie das Kontrollkästchen Abonnement, wenn Sie über die Anwendungen als Abonnementprodukt berichten möchten (optional).
   d. Wenn das Produkt nicht nach Version installiert wird (z. B. Chrome), aktivieren Sie das Kontrollkästchen Version nicht erforderlich. So können Produkte mit kontinuierlicher Aktualisierung installiert werden, ohne ihre Versionen nachzuverfolgen.
   e. Wenn ein Produkt mehrere benannte Versionen unterstützt (z. B. QuickBooks), müssen Sie dieses Kontrollkästchen aktivieren, damit Sie mehrere Versionen installieren und jede verfügbare Version in der Liste der Anwendungen, die für und Endbenutzer berechtigt sein können, VDS-spezifisch besitzen können.
   f. Aktivieren Sie „kein Benutzer-Desktop-Symbol“, wenn VDS kein Desktop-Symbol für dieses Produkt bereitstellen soll. Dies wird für „Backend“-Produkte wie SQL Server verwendet, da Endbenutzer keine Anwendung haben, auf die sie zugreifen können.
   g. „App muss zugeordnet sein“ setzt die Notwendigkeit, eine zugehörige App zu installieren. Für eine Client-Server-Anwendung kann es z. B. erforderlich sein, dass auch SQL Server oder MySQL installiert werden muss.
   h. Wenn Sie das Feld Lizenz erforderlich aktivieren, wird angezeigt, dass VDS eine Lizenzdatei für eine Installation dieser Anwendung anfordern sollte, bevor der Anwendungsstatus auf aktiv gesetzt wird. Dieser Schritt wird auf der Seite Anwendungsdetails von VDS durchgeführt.
   i. Sichtbar für Alle – Anwendungsberechtigungen können auf bestimmte Teilpartner in einer Mehrkanalhierarchie beschränkt werden. Klicken Sie zu Evaluierungszwecken auf das Kontrollkästchen, damit alle Benutzer es in ihrer Liste der verfügbaren Anwendungen sehen können.

Fügen Sie die Anwendung dem Arbeitsbereich hinzu

Um den Bereitstellungsprozess zu starten, fügen Sie die App zum Arbeitsbereich hinzu.

Führen Sie dazu die folgenden Schritte aus

1. Klicken Sie Auf Arbeitsbereiche
2. Blättern Sie nach unten zu „Apps“
3. Klicken Sie Auf Hinzufügen

4. Aktivieren Sie die Anwendung(en), geben Sie die erforderlichen Informationen ein, klicken Sie auf Anwendung hinzufügen und klicken Sie auf Apps hinzufügen.

Installieren Sie die Anwendung manuell

Sobald die Anwendung dem Arbeitsbereich hinzugefügt wurde, müssen Sie diese Anwendung auf allen Sitzungshosts installieren. Dies kann manuell und/oder automatisiert werden.

Führen Sie die folgenden Schritte aus, um Anwendungen manuell auf Sitzungshosts zu installieren

1. Navigieren Sie zu Service Board.
2. Klicken Sie auf die Aufgabe des Service Board.
3. Klicken Sie auf die Servernamen, um eine Verbindung als lokaler Administrator herzustellen.
4. Installieren Sie die App(s), bestätigen Sie, dass die Verknüpfung zu dieser Anwendung im Startmenü-Pfad gefunden wird.
    a. Für Server 2016 und Windows 10: C:\ProgramData\Microsoft\Windows\Startmenü\Programme.
5. Gehen Sie zurück zur Aufgabe des Service-Mainboards, klicken Sie auf Durchsuchen und wählen Sie entweder die Verknüpfung oder einen Ordner mit Verknüpfungen aus.
6. Je nachdem, welche Option Sie auswählen, wird auf dem Desktop des Endbenutzers angezeigt, wenn die App zugewiesen wurde.
7. Ordner sind großartig, wenn eine Anwendung tatsächlich mehrere Anwendungen ist. Z. B. „Microsoft Office“ ist einfacher als Ordner mit jeder App als Verknüpfung im Ordner bereitzustellen.
8. Klicken Sie Auf Installation Abschließen.
9. Öffnen Sie bei Bedarf das erstellte Symbol Serviceboard Task hinzufügen, und bestätigen Sie, dass das Symbol hinzugefügt wurde.

Anwendungen zu Benutzern zuweisen

Die Anwendungsberechtigungen werden von VDS verwaltet, und die Anwendung kann Benutzern auf drei Arten zugewiesen werden

Anwendungen zu Benutzern zuweisen

1. Navigieren Sie zur Seite „Benutzerdetails“.
2. Navigieren Sie zum Abschnitt Anwendungen.
3. Aktivieren Sie das Kontrollkästchen neben allen für diesen Benutzer erforderlichen Anwendungen.

Weisen Sie einer Anwendung Benutzer zu

1. Navigieren Sie auf der Seite Arbeitsbereichdetails zum Abschnitt Anwendungen.
2. Klicken Sie auf den Namen der Anwendung.
3. Aktivieren Sie das Kontrollkästchen neben den Benutzern, die die Anwendung verwenden.

Anwendungen und Benutzer zu Benutzergruppen zuweisen

1. Navigieren Sie zu den Benutzern und Gruppen-Details.
2. Fügen Sie eine neue Gruppe hinzu oder bearbeiten Sie eine vorhandene Gruppe.
3. Weisen Sie der Gruppe Benutzer und Anwendungen zu.

Benutzerpasswort Zurücksetzen

Schritte für das Benutzerpasswort zurücksetzen

1. Navigieren Sie zur Seite „verwendete Details“ im VDS

   []

2. Suchen Sie den Abschnitt Kennwort, geben Sie zweimal den neuen PW ein, und klicken Sie auf

   []

   []

Zeit, um wirksam zu werden

- Für Umgebungen, die ein „internes“ AD auf VMs in der Umgebung ausführen, sollte die Passwortänderung sofort wirksam werden.
- In Umgebungen, in denen Azure AD Domain Services (AADDS) ausgeführt wird, sollte die Passwortänderung ca. 20 Minuten in Anspruch nehmen.
- Der AD-Typ kann auf der Seite „Bereitstellungsdetails“ ermittelt werden:

  []

Self Service password Reset (SSRP)

Der NetApp VDS Windows-Client und der NetApp VDS Web-Client erhalten eine Eingabeaufforderung für Benutzer, die bei der Anmeldung bei einer Virtual Desktop-Implementierung mit v5.2 (oder höher) ein falsches Passwort eingeben. Falls der Benutzer sein Konto gesperrt hat, wird dieser Prozess auch das Konto eines Benutzers entsperren.

Hinweis: Benutzer müssen bereits eine Mobiltelefonnummer oder eine E-Mail-Adresse eingegeben haben, damit dieser Prozess funktioniert.

SSPR wird unterstützt durch:

- NetApp VDS Window Client
- NetApp VDS Web Client

In diesem Satz von Anweisungen werden Sie den Prozess der Verwendung von SSPR als einfache Mittel, um Benutzern zu ermöglichen, ihre Passwörter zurückzusetzen und ihre Konten zu entsperren.

NetApp VDS Windows-Client

1. Klicken Sie als Endbenutzer auf den Link Passwort vergessen, um fortzufahren.

   []

2. Wählen Sie aus, ob Sie Ihren Code über Ihr Mobiltelefon oder per E-Mail erhalten möchten.

   []

3. Wenn ein Endbenutzer nur eine dieser Kontaktmethoden bereitgestellt hat, wird dies die einzige Methode

angezeigt.

[]

4. Nach diesem Schritt wird den Benutzern ein Code-Feld angezeigt, in dem sie den Wert eingeben, der entweder auf ihrem Mobilgerät oder in ihrem Posteingang empfangen wurde (je nachdem, welcher Wert ausgewählt wurde). Geben Sie diesen Code gefolgt vom neuen Passwort ein und klicken Sie auf Zurücksetzen, um fortzufahren.

   []

5. Der Benutzer wird aufgefordert, ihn darüber zu informieren, dass das Zurücksetzen des Passworts erfolgreich abgeschlossen wurde. Klicken Sie auf „Fertig“, um den Anmeldevorgang abzuschließen.

   > Wenn Ihre Bereitstellung Azure Active Directory Domain Services verwendet, gibt es einen von Microsoft definierten Zeitraum zur Kennwortsynchronisation – alle 20 Minuten. Auch dies wird von Microsoft gesteuert und kann nicht geändert werden. In diesem Sinne zeigt VDS an, dass der Benutzer bis zu 20 Minuten warten sollte, bis sein neues Passwort wirksam wird. Wenn Ihre Bereitstellung Azure Active Directory Domain Services nicht verwendet, kann sich der Benutzer in Sekundenschnelle erneut anmelden.

   []

HTML5-Portal

1. Wenn der Benutzer beim Versuch, sich über den HTML5 anzumelden, das richtige Passwort nicht eingibt, wird ihm nun eine Option zum Zurücksetzen des Passworts angezeigt:

   []

2. Nachdem Sie auf die Option zum Zurücksetzen des Passworts geklickt haben, werden ihnen die Optionen zum Zurücksetzen angezeigt:

   []

3. Die Schaltfläche ‘Anfrage’ sendet einen generierten Code an die ausgewählte Option (in diesem Fall die E-Mail des Benutzers). Der Code ist 15 Minuten lang gültig.

   []

4. Das Kennwort wurde zurückgesetzt! Es ist wichtig zu beachten, dass Windows Active Directory häufig einen Moment benötigt, um die Änderung zu verbreiten. Wenn das neue Passwort also nicht sofort funktioniert, warten Sie einfach ein paar Minuten und versuchen Sie es erneut. Dies ist insbesondere für Benutzer mit Azure Active Directory Domain Services-Implementierung relevant, wobei das Zurücksetzen des Passworts bis zu 20 Minuten dauern kann.

   []

Aktivieren des Self-Service-Kennwortrücksetzens (SSPR) für Benutzer

Um Self Service Password Reset (SSPR) zu verwenden, müssen Administratoren zunächst eine Handynummer und/oder ein E-Mail-Konto für einen Endbenutzer eingeben. Es gibt zwei Möglichkeiten, wie unten beschrieben eine Handynummer und E-Mail-Adressen für einen virtuellen Desktop-Benutzer einzugeben.

In diesem Satz von Anweisungen werden Sie den Prozess der Konfiguration von SSPR als einfache Möglichkeit für Endbenutzer, ihre Passwörter zurückzusetzen, durchlaufen.

Massenimport von Benutzern über VDS

Navigieren Sie zunächst zum Workspaces-Modul, dann zu Benutzern & Gruppen und klicken Sie dann auf Hinzufügen/Importieren.

Sie können die folgenden Werte für Benutzer eingeben, wenn Sie sie einzeln erstellen:[]

Oder Sie können diese einschließen, wenn Benutzer im Massenimport die vorkonfigurierte Excel XLSX-Datei herunterladen und mit diesem Inhalt hochladen:[]

Bereitstellen der Daten über die VDS-API

NetApp VDS API – insbesondere dieser Aufruf https://api.cloudworkspace.com/5.4/swagger/ui/index#!/User/User_PutUser – Bietet die Möglichkeit, diese Informationen zu aktualisieren.

Das vorhandene Benutzertelefon wird aktualisiert

Aktualisieren Sie die Telefonnummer der Benutzer auf der Seite „Übersicht der Benutzerdetails“ im VDS.

[]

Verwenden anderer Konsolen

Hinweis: Es ist derzeit nicht möglich, eine Telefonnummer für einen Benutzer über die Azure Console, das Partner Center oder über die Office 365 Admin-Konsole bereitzustellen.

SSPR-Sendeadresse anpassen

NetApp VDS kann so konfiguriert werden, dass er die Bestätigungs-E-Mail *von* einer benutzerdefinierten Adresse sendet. Dies ist ein Service für unsere Service Provider-Partner, die ihre Endbenutzer möchten, dass sie die Reset-Passwort-E-Mail von ihrer eigenen angepassten E-Mail-Domäne erhalten.

Diese Anpassung erfordert einige weitere Schritte, um die Absendeadresse zu überprüfen. Um diesen Prozess zu starten, öffnen Sie einen Support-Fall mit VDS-Unterstützung und fordern eine benutzerdefinierte „Self Service Password Reset Source Address“ an. Bitte definieren Sie Folgendes:

- Ihr Partner-Code (dieser Code kann durch Klicken auf *settings* unter dem oberen rechten Pfeil nach unten Menü gefunden werden. Siehe Abbildung unten)

  []

- Gewünschte „von“-Adresse (gültig)
- Auf welche Clients die Einstellung angewendet werden soll (oder alle)

Die Eröffnung eines Support Cases kann per E-Mail an support@spotpc.netapp.com erfolgen

Sobald VDS-Unterstützung erhalten ist, wird die Adresse mit unserem SMTP-Dienst validiert und diese Einstellung aktiviert. Idealerweise haben Sie die Möglichkeit, öffentliche DNS-Datensätze in der Quelladdress Domain zu aktualisieren, um die Zustellung von E-Mails zu maximieren.

Komplexität von Passwörtern

VDS kann so konfiguriert werden, dass die Passwortkomplexität durchgesetzt wird. Die Einstellung hierzu finden Sie auf der Seite Arbeitsbereichdetails im Abschnitt Einstellungen des Cloud-Arbeitsbereichs.

[]

[]

Passwortkomplexität: Aus

Richtlinie	Richtlinie
Mindestkennwortlänge	8 Zeichen
Maximales Kennwortalter	110 Tage
Mindestalter Des Kennworts	0 Tage
Kennwortverlauf Erzwingen	24 Passwörter gespeichert
Passwort Sperren	Nach 5 falschen Einträgen erfolgt die automatische Sperrung
Sperrdauer	30 Minuten

Passwortkomplexität: Ein

Richtlinie	Richtlinie
Mindestkennwortlänge	8 Zeichen enthalten nicht den Kontonamen des Benutzers oder Teile des vollständigen Namens des Benutzers, die zwei aufeinanderfolgende Zeichen überschreiten, enthalten Zeichen aus drei der folgenden vier Kategorien: Englische Großbuchstaben (A bis Z) Englische Kleinbuchstaben (A bis z) Basis 10 Ziffern (0 bis 9) nicht-alphabetische Zeichen (z. B. !, €, #, %) Komplexitätsanforderungen werden durchgesetzt, wenn Passwörter geändert oder erstellt werden.
Maximales Kennwortalter	110 Tage
Mindestalter Des Kennworts	0 Tage
Kennwortverlauf Erzwingen	24 Passwörter gespeichert
Passwort Sperren	Nach 5 falschen Einträgen erfolgt die automatische Sperre
Sperrdauer	Bleibt gesperrt, bis der Administrator entsperrt wird

Multi-Faktor-Authentifizierung (MFA)

Überblick

NetApp Virtual Desktop Service (VDS) umfasst ohne Aufpreis einen SMS/E-Mail-basierten MFA Service. Dieser Service ist unabhängig von anderen Dienstleistungen (z.B. Azure Conditional Access) und kann zur Sicherung von Administratoranmeldungen auf VDS und Benutzeranmeldungen auf virtuellen Desktops verwendet werden.

MFA-Grundlagen

- VDS MFA kann Admin-Benutzern, einzelnen Endbenutzern oder für alle Endbenutzer angewendet werden
- VDS MFA kann SMS- oder E-Mail-Benachrichtigungen senden
- VDS MFA verfügt über eine Self-Service-Ersteinrichtung und Reset-Funktion

Umfang des Leitfadens

Dieses Handbuch erläutert die Einrichtung von MFA sowie die Darstellung der Benutzerfreundlichkeit

In diesem Leitfaden werden die folgenden Themen behandelt:

1. MFA für einzelne Benutzer aktivieren
2. MFA für alle Benutzer erforderlich
3. MFA für einzelne Administratoren aktivieren
4. Ersteinrichtung Des Endbenutzers

MFA für einzelne Benutzer aktivieren

MFA kann für einzelne Benutzer auf der Benutzer-Detailseite durch Klicken auf *Multi-Faktor Auth Enabled* aktiviert werden

Arbeitsbereiche > Workspace-Name > Benutzer & Gruppen > Benutzername > Multi-Faktor Auth aktiviert > Aktualisieren

MFA kann auch allen Benutzern zugewiesen werden. Wenn diese Einstellung aktiviert ist, wird das Kontrollkästchen aktiviert und _ (über Client-Einstellungen)_ wird an das Kontrollkästchen angehängt.

MFA für alle Benutzer erforderlich

MFA kann auf der Detailseite des Arbeitsbereichs für alle Benutzer aktiviert und durchgesetzt werden, indem Sie auf *MFA für Alle Benutzer aktiviert* klicken

Workspaces > Workspace-Name > MFA für alle Benutzer aktiviert >Update

Aktivierung von MFA für einzelne Administratoren

MFA ist auch für Administratorkonten verfügbar, die auf das VDS-Portal zugreifen. Dies kann pro Administrator auf der Seite „Administratordetails“ aktiviert werden. Administratoren > Admin-Name > Multi-Faktor-Auth Erforderlich > Aktualisieren

Ersteinrichtung

Bei der ersten Anmeldung nach der Aktivierung von MFA wird der Benutzer oder der Admin aufgefordert, eine E-Mail-Adresse oder Telefonnummer einzugeben. Sie erhalten einen Bestätigungscode, mit dem sie die erfolgreiche Anmeldung bestätigen können.

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.[]