



Dokumentation Des Virtual Desktop Service

Virtual Desktop Service

NetApp
November 18, 2022

Inhaltsverzeichnis

Dokumentation Des Virtual Desktop Service	1
Überblick	1
Support Erhalten	1
Weitere Ressourcen	2
Implementierung mit VDS	3
Azure	3
Google	49
Architektur	64
Umleitung Der Storage-Plattform	64
Überlegungen Zur Datenmigration	69
Verlängerung des Platzhalter-SSL-Zertifikats	71
AVD-Rückführung	73
Vereinfachtes	77
Implementierungen	77
Applikationen Unterstützt	92
Skriptbasierte Ereignisse	105
Command Center	113
Ressourcenoptimierung	119
Anwenderadministration	123
Systemadministration	133
Fehlerbehebung	147
Fehlerbehebung bei fehlgeschlagenen VDS-Aktionen	147
Fehlerbehebung In Bezug Auf Die Qualität Der Internetverbindung	150
Desktop-Hintergrund für Benutzersitzungen aktivieren	151
Fehlerbehebung Beim Drucken Von Problemen	152
Azure vCPU Kernquote	153
Entsperren Von Benutzerkonten	153
Fehlerbehebung Bei Der Leistung Von Virtuellen Maschinen	154
DNS leitet für Azure FÜGT & SSO über O365-Identität weiter	156
Fehlerbehebung Bei Applikationsproblemen	157
Referenz	159
Versionshinweise	159
Anforderungen Von Endbenutzern	239
VDS-Umgebungen ändern	245
Dokumentation Der Skriptbibliothek	246
Erweitert	264
NetApp VDS v5.4-Videos	266
VDS-Inhalte auf NetApp TV	266
Implementieren Sie AVD oder RDS in Azure mit NetApp VDS v5.4	266
Erstellen Sie mit NetApp VDS v5.4 einen AVD Host-Pool	266
AVD-Benutzer und App-Gruppen in Azure mit NetApp VDS v5.4 hinzufügen und managen	267
Optimieren Sie den Azure Ressourcenverbrauch in VDS 5.4	268
Tägliche Administration von RDS und AVD mit NetApp VDS v5.4	268

Aktualisieren des AVD-Hostpools von v1 (Herbst 2019) auf v2 (Frühjahr 2020)	268
---	-----

Dokumentation Des Virtual Desktop Service

Überblick

NetApp Virtual Desktop Service (VDS) bewältigt die Komplexität bei der Implementierung und dem Management von virtuellen Desktops in der Public Cloud. Diese werden sowohl als flexibler Software-Service zum Management Ihrer Virtual Desktop Infrastructure (VDI) als auch als vollständig gemanagte VDI-as-a-Service-Plattform bereitgestellt. Durch den Virtual Desktop Service entfällt die Komplexität bei der Implementierung von Desktops in der Cloud. Hunderte von Aufgaben, die 2-3 Tage gedauert haben, wurden in nur wenigen Stunden erledigt.

Vorteile Von Virtual Desktop Service:

- **Senkung Der Infrastrukturkosten**

Mit unserem anpassbaren Ressourcenplanungssystem optimieren wir die Infrastrukturkosten um bis zu 50 %.

- **Risiko Reduzieren**

Implementieren Sie Desktops in logische Workflows gemäß Best Practices für die Cloud, z. B. Microsoft Best Practice-Standards für Azure Virtual Desktop (AVD).

- **Custom Automation**

Event-basierte Automatisierungs- und Orchestrierungs-Engine mit Ihrer aktuellen Skripte macht das Management so einfach, dass allgemeine IT-Administratoren Ihre Cloud-Desktops managen können.

- * Multi-Cloud*

Steuerung mehrerer Mandanten über AWS, Azure und Google über eine einzige grafische Benutzeroberfläche

- **Flexible Steuerung**

Maximieren Sie Ihre geschäftliche Flexibilität mit einem einzigen Portal zur Steuerung aller Schichten Ihres Technologie-Stacks.

Weitere Informationen: <https://cloud.netapp.com/virtual-desktop-service>

Support Erhalten

E-Mail-Support: support@spotpc.netapp.com

Telefon-Support: 844.645.6789

["VDS-Support-Portal"](#)

Normaler Support während der Geschäftszeiten: Montag bis Freitag, 7:7 Uhr bis 22:00 Uhr Central Time.

- Support nach Geschäftsschluss (On-Call) ist nur per Telefon verfügbar.

Weitere Ressourcen

Kostenrechner

Azure

- <https://manage.vds.netapp.com/azure-cost-estimator>

Google Cloud

- <https://manage.vds.netapp.com/google-cost-estimator>

Downloads

Remote Desktop Services-Clients (RDS)

- "VDS RDS-Client für Windows"
- "VDS Web Client"
- "Microsoft RD-Client"

Azure Virtual Desktop (AVD)-Clients

- "Microsoft AVD für Windows-Client"
- "Microsoft AVD Web-Client"
- "Microsoft AVD für Android-Client"
- "Microsoft AVD für macOS Client"
- "Microsoft AVD für iOS-Client"

Weitere Downloads

- "RemoteScan-Client"
- "VDS RDS Windows Client-Designer"

Implementierung mit VDS

Azure

Azure Virtual Desktop

AVD-Bereitstellungsleitfaden

Überblick

Dieser Leitfaden enthält eine Schritt-für-Schritt-Anleitung zum Erstellen einer Azure Virtual Desktop-Implementierung (AVD) unter Verwendung von NetApp Virtual Desktop Service (VDS) in Azure.

Der Leitfaden beginnt bei: <https://cwasetup.cloudworkspace.com/>

Dieser Proof of Concept (POC)-Leitfaden soll Ihnen dabei helfen, AVD schnell in Ihrem eigenen Azure-Test zu implementieren und zu konfigurieren. In diesem Leitfaden wird von einer Bereitstellung vor Ort im grünen Bereich in einen sauberen, nicht produktiven Azure Active Directory-Mandanten ausgegangen.

Produktionsimplementierungen, insbesondere in bestehenden AD- oder Azure AD-Umgebungen, sind häufig jedoch nicht in diesem POC-Leitfaden berücksichtigt. Komplexe Machbarkeitsstudien und Implementierungen in der Produktion sollten mit den NetApp VDS Sales-/Services-Teams initiiert werden und jedoch nicht als Self-Service-Lösung eingesetzt werden.

Dieses POC-Dokument führt Sie durch die gesamte AVD-Implementierung und bietet eine kurze Übersicht über die wichtigsten Bereiche der Konfiguration nach der Implementierung, die in der VDS-Plattform verfügbar ist. Nach der Fertigstellung verfügen Sie über eine voll implementierte und funktionale AVD-Umgebung, komplett mit Host-Pools, App-Gruppen und Benutzern. Optional haben Sie die Möglichkeit, automatisierte Anwendungsbereitstellung, Sicherheitsgruppen, Dateifreigabeberechtigungen, Azure Cloud Backup, intelligente Kostenoptimierung zu konfigurieren. VDS setzt eine Reihe von Best-Practice-Einstellungen über GPO ein. Anweisungen zum optionalen Deaktivieren dieser Steuerelemente sind ebenfalls enthalten, falls Ihr POC keine Sicherheitskontrollen benötigt, ähnlich wie eine nicht verwaltete lokale Geräteumgebung.

AVD-Grundlagen

Azure Virtual Desktop ist ein umfassender Service zur Desktop- und Applikationsvirtualisierung, der in der Cloud ausgeführt wird. Hier ist eine kurze Liste von einigen der wichtigsten Funktionen:

- Plattform-Services wie Gateways, Vermittlung, Lizenzierung und Anmeldung sowie als Service von Microsoft. Dies minimierte Infrastruktur-Bedarf für Hosting und Management.
- Azure Active Directory kann als Identitäts-Provider genutzt werden, sodass es die Schichten zusätzlicher Azure Sicherheitsservices wie z. B. bedingten Zugriff gibt.
- Benutzer erhalten Single Sign-on-Erfahrung für Microsoft-Dienste.
- Benutzersitzungen verbinden sich über eine proprietäre Reverse-Connect-Technologie mit dem Session-Host. Das bedeutet, dass keine eingehenden Ports geöffnet werden müssen, stattdessen erstellt ein Agent eine ausgehende Verbindung zur AVD-Verwaltungsebene, die wiederum mit dem Endgerät verbunden wird.
- Die Rückwärtsverbindung ermöglicht sogar die Ausführung von Virtual Machines, ohne im öffentlichen Internet verfügbar zu sein, wodurch isolierte Workloads auch während der Remote-Konnektivität möglich sind.

- AVD bietet Zugriff auf Windows 10 Multi Session, sodass Sie Windows 10 Enterprise-Erfahrungen mit der Effizienz von User Sessions mit hoher Dichte durchführen können.
- FSLogix-Profil-Containerisierungstechnologie verbessert die Performance von Benutzersitzungen, Storage-Effizienz und verbessert das Office-Erlebnis in nicht-persistenten Umgebungen.
- AVD unterstützt den Vollzugriff auf Desktops und RemoteApp. Sowohl persistente als auch nicht persistente Erfahrungen und dedizierte und Multi-Session-Erfahrungen.
- Unternehmen können Windows-Lizenzen sparen, weil AVD „Windows 10 Enterprise E3 pro Benutzer“ nutzen kann. Dadurch werden RDS-CALs ersetzt und die Kosten pro Stunde für Host-VMs in Azure deutlich reduziert.

Umfang des Leitfadens

In diesem Leitfaden erfahren Sie, wie AVD mithilfe von NetApp VDS-Technologie implementiert wird, und zwar aus Sicht eines Azure- und VDS-Administrators. Ohne Vorkonfiguration bringen Sie den Azure-Mandanten und das Abonnement mit sich und in diesem Leitfaden können Sie das AVD-End-to-End-System einrichten

Dieser Leitfaden umfasst die folgenden Schritte:

1. Prerequisites,Bestätigen Sie die Voraussetzungen für den Azure-Mandanten, das Azure-Abonnement und die Berechtigungen des Azure-Administratorkontos
2. Discovery Details,Sammelt die erforderlichen Details zur Bestandsaufnahme
3. Setup Sections,Erstellen Sie die Azure-Umgebung mit dem speziell entwickelten VDS für Azure Setup-Assistenten
4. AVD Host Pool,Erstellen Sie den ersten Host-Pool mit einem standardmäßigen Windows 10-EVD-Image
5. VDS desktops to users,Zuweisen von virtuellen Desktops zu Azure AD-Benutzern
6. app group,Fügen Sie Benutzer zur Standard-App-Gruppe hinzu, um Benutzern die Desktop-Umgebung bereitzustellen. Optional Additional AVD App Group(s),Erstellen Sie zusätzliche Host-Pools für die Bereitstellung von RemoteApp-Services
7. User AVD Access,Verbinden Sie sich als Endbenutzer über Client-Software und/oder Web-Client
8. connection options,Stellen Sie eine Verbindung zu den Plattform- und Client-Services als lokaler und Domain-Administrator her
9. Authentication (MFA),Optional können Sie die VDS-Multi-Faktor-Authentifizierung für VDS-Administratoren AVD-Endbenutzer aktivieren
10. Entitlement Workflow,Gehen Sie optional den gesamten Workflow für Anwendungsberechtigungen durch, einschließlich Befüllen der App-Bibliothek, Automatisierung von ApplikationInstallationen, Maskierung durch Benutzer und Sicherheitsgruppen
11. AD Security Groups,Optional können Sie Active Directory-Sicherheitsgruppen, Ordnerberechtigungen und Anwendungsberechtigungen nach Gruppe erstellen und verwalten.
12. Cost Optimization Options,Optional können Sie Technologien zur Kostenoptimierung wie Workload Scheduling und Live-Skalierung konfigurieren
13. and Manage VM Images,Optional können Sie ein Virtual-Machine-Image für zukünftige Bereitstellungen erstellen, aktualisieren und Sysprep erstellen
14. Azure Cloud Backup Service,Optionale Konfiguration von Azure Cloud Backup
15. App Management/Policy Mode,Deaktivieren Sie optional die Standardrichtlinien für Sicherheitskontrollgruppen

Voraussetzungen für Azure

VDS verwendet zur Bereitstellung der AVD-Instanz den nativen Azure-Sicherheitskontext. Bevor Sie den VDS Setup-Assistenten starten, müssen einige Azure-Voraussetzungen geschaffen werden.

Während der Implementierung werden Servicekonten und Berechtigungen über die Authentifizierung eines vorhandenen Administratorkontos aus dem Azure-Mandanten gewährt.

Checkliste für die Schnellvoraussetzungen

- Azure Tenant mit Azure AD-Instanz (kann eine Microsoft 365-Instanz sein)
- Azure Abonnement
- Verfügbare Azure Quote für virtuelle Azure-Maschinen
- Azure-Administratorkonto mit globalen Administratorrollen und Abonnementberechtigungen



Detaillierte Voraussetzungen werden auf dokumentiert "[Dieses PDF-Dokument](#)"

Azure-Administrator in Azure AD

Der vorhandene Azure Administrator muss ein Azure AD-Konto im Zielmandant sein. Windows Server AD-Konten können mit dem VDS Setup implementiert werden. Es sind jedoch zusätzliche Schritte erforderlich, um eine Synchronisierung mit Azure AD einzurichten (nicht im Umfang dieses Leitfadens enthalten)

Sie können dies bestätigen, indem Sie das Benutzerkonto im Azure Management Portal unter Benutzer > Alle Benutzer suchen.[]

Globale Administratorrolle

Der Azure-Administrator muss der globalen Administratorrolle im Azure-Mandanten zugewiesen werden.

So überprüfen Sie Ihre Rolle in Azure AD:

1. Melden Sie sich unter beim Azure Portal an <https://portal.azure.com/>
2. Suchen Sie nach Azure Active Directory, und wählen Sie ihn aus
3. Klicken Sie im nächsten Fensterbereich rechts auf die Option Benutzer im Abschnitt Verwalten
4. Klicken Sie auf den Namen des Administratorbenutzers, den Sie überprüfen
5. Klicken Sie auf die Verzeichnisrolle. Im rechten Bereich sollte die globale Administratorrolle aufgelistet werden[]

Wenn dieser Benutzer nicht über die globale Administratorrolle verfügt, können Sie die folgenden Schritte durchführen, um sie hinzuzufügen (beachten Sie, dass das angemeldete Konto ein globaler Administrator sein muss, um diese Schritte auszuführen):

1. Klicken Sie oben auf der Detailseite des Benutzerverzeichnisses in Schritt 5 oben auf der Detailseite auf die Schaltfläche Zuordnung hinzufügen.
2. Klicken Sie in der Liste der Rollen auf Global Administrator. Klicken Sie auf die Schaltfläche Hinzufügen.[]

Azure-Abonnement

Der Azure Administrator muss auch im Abonnement Eigentümer sein, der die Implementierung enthält.

So überprüfen Sie, ob der Administrator ein Subscription Owner ist:

1. Melden Sie sich unter beim Azure Portal an <https://portal.azure.com/>
2. Suchen Sie nach, und wählen Sie Abonnements aus
3. Klicken Sie im nächsten Fensterbereich rechts auf den Namen des Abonnements, um die Abonnementdetails anzuzeigen
4. Klicken Sie im zweiten Fensterbereich von links auf den Menüpunkt Access Control (IAM)
5. Klicken Sie auf die Registerkarte Rollenzuweisungen. Der Azure Administrator sollte im Abschnitt „Eigentümer“ aufgeführt sein.[]

Wenn der Azure Administrator nicht aufgeführt ist, können Sie das Konto als Abbonementeigentümer hinzufügen, indem Sie die folgenden Schritte durchführen:

1. Klicken Sie oben auf der Seite auf die Schaltfläche Hinzufügen und wählen Sie die Option Rollenzuweisung hinzufügen
2. Rechts wird ein Dialog angezeigt. Wählen Sie in der Dropdown-Liste Rolle „Eigentümer“, und geben Sie dann im Feld Auswählen den Benutzernamen des Administrators ein. Wenn der vollständige Name des Administrators angezeigt wird, wählen Sie ihn aus
3. Klicken Sie unten im Dialogfeld auf die Schaltfläche Speichern[]

Azure Computing-Kernkontingent

Der CWA Setup-Assistent und das VDS-Portal erstellen neue virtuelle Maschinen und das Azure-Abonnement muss über eine Quote verfügen, um erfolgreich ausgeführt zu werden.

Gehen Sie wie folgt vor, um das Kontingent zu überprüfen:

1. Navigieren Sie zum Modul Abonnements und klicken Sie auf „Nutzung + Quoten“.
2. Wählen Sie im Drop-Down-Menü „Provider“ alle Anbieter aus, wählen Sie „Microsoft.Compute“ im Drop-Down-Menü „Provider“ aus
3. Wählen Sie den Zielbereich in der Dropdown-Liste „Standorte“ aus
4. Es sollte eine Liste der verfügbaren Quoten nach der Produktfamilie virtueller Maschinen angezeigt werden[]Wenn Sie die Quote erhöhen müssen, klicken Sie auf Anfrage steigern und befolgen Sie die Anweisungen, um zusätzliche Kapazität hinzuzufügen. Für die Erstabfertigung fordern Sie speziell ein erhöhtes Angebot für die „Standard DSv3-vCPUs“ an.

Erfassen von Details zur Bestandsaufnahme

Nachdem Sie den CWA Setup-Assistenten durchlaufen haben, müssen Sie mehrere Fragen beantworten. NetApp VDS bietet eine verknüpfte PDF-Datei, die vor der Implementierung zur Aufzeichnung dieser Auswahl verwendet werden kann. Folgende Elemente sind enthalten:

Element	Beschreibung
VDS Admin-Berechtigungen	Sammeln Sie die vorhandenen VDS-Administratoranmeldeinformationen, wenn Sie sie bereits besitzen. Anderenfalls wird während der Implementierung ein neues Administratorkonto erstellt.
Azure Region	Legen Sie die Zielregion für Azure fest, die auf der Performance und Verfügbarkeit von Services basiert. Das " Microsoft Tool " Kann den Endbenutzer anhand der Region einschätzen.

Element	Beschreibung
Typ Active Directory	Die VMs müssen einer Domäne beitreten, können aber nicht direkt mit Azure AD beitreten. Mit der VDS-Implementierung kann eine neue Virtual Machine erstellt oder ein vorhandener Domain Controller verwendet werden.
File Management	Die Performance hängt in hohem Maße von der Geschwindigkeit der Festplatte ab, insbesondere im Zusammenhang mit Storage für Benutzerprofile. Der VDS-Einrichtungsassistent kann einen einfachen Dateiserver bereitstellen oder Azure NetApp Files (ANF) konfigurieren. Für nahezu jede Produktionsumgebung wird ANF jedoch für einen POC empfohlen, da die File-Server-Option eine ausreichende Performance bietet. Storage-Optionen können nach der Implementierung überarbeitet werden, einschließlich vorhandener Storage-Ressourcen in Azure. Details finden Sie in den ANF-Preisen: https://azure.microsoft.com/en-us/pricing/details/netapp/
Umfang Des Virtuellen Netzwerks	Für die Bereitstellung ist ein routingbarer /20-Netzwerkbereich erforderlich. Mit dem VDS-Setup-Assistenten können Sie diesen Bereich definieren. Es ist wichtig, dass sich dieser Bereich nicht mit vorhandenen vNets in Azure oder On-Premises überschneidet (falls die beiden Netzwerke über einen VPN oder ExpressRoute verbunden werden).

VDS-Setup-Abschnitte

Melden Sie sich bei an <https://cwasetup.cloudworkspace.com/> Mit den Azure Admin-Berechtigungen finden Sie im Abschnitt „Voraussetzungen“.

IaaS und Plattform

[]

Azure AD-Domain-Name

Der Azure AD-Domänenname wird vom ausgewählten Mandanten übernommen.

Standort

Wählen Sie eine entsprechende Region **Azure** aus. Das "[Microsoft Tool](#)" Kann den Endbenutzer anhand der Region einschätzen.

Typ Active Directory

VDS kann mit einer **neuen virtuellen Maschine** für die Domain Controller-Funktion oder zur Nutzung eines vorhandenen Domain Controllers bereitgestellt werden. In diesem Handbuch wählen wir New Windows Server Active Directory aus, das eine oder zwei VMs (basierend auf den während dieses Prozesses getroffenen Entscheidungen) im Abonnement erstellt.

Ein detaillierter Artikel zu einer vorhandenen AD-Implementierung finden Sie "[Hier](#)".

Active Directory-Domänenname

Geben Sie einen **Domänennamen** ein. Es wird empfohlen, den Azure AD-Domänennamen von oben zu spiegeln.

Dateimanagement

VDS kann eine einfache Virtual Machine des Dateiservers bereitstellen oder Azure NetApp Files einrichten und konfigurieren. In der Produktion empfiehlt Microsoft, 30 gb pro Benutzer zuzuweisen, und wir haben festgestellt, dass für eine optimale Performance 5-15 IOPS pro Benutzer erforderlich sind.

In einer POC-Umgebung (außerhalb der Produktionsumgebung) ist der File-Server eine kostengünstige und einfache Implementierungsoption, in der die verfügbare Performance von Azure Managed Disks vom IOPS-Verbrauch selbst einer kleinen Produktionsimplementierung überfordert werden kann.

Beispielsweise unterstützt ein SSD-Standardlaufwerk mit 4 TB in Azure bis zu 500 IOPS, wodurch insgesamt maximal 100 Benutzer mit 5 IOPS pro Benutzer unterstützt werden können. Bei ANF Premium würde das Storage Setup derselben Größe 16,000 IOPS unterstützen und 32x mehr IOPS buchen.

Für die Produktion AVD-Bereitstellungen, **Azure NetApp Files ist Microsofts Empfehlung.**



Azure NetApp Files muss für das Abonnement verfügbar sein, auf dem Sie bereitgestellt werden möchten. Wenden Sie sich bitte an Ihren NetApp Ansprechpartner oder nutzen Sie den folgenden Link: <https://aka.ms/azurenetafiles>

Zudem müssen Sie NetApp als Provider für Ihr Abonnement registrieren. Dies können Sie wie folgt erreichen:

- Navigieren Sie im Azure-Portal zu Abonnements
 - Klicken Sie Auf Ressourcenanbieter
 - Filter für NetApp
 - Wählen Sie den Anbieter aus, und klicken Sie auf Registrieren

RDS-Lizenznummer

Mit NetApp VDS können RDS- und/oder AVD-Umgebungen implementiert werden. Bei der Bereitstellung von AVD kann dieses Feld **leer bleiben**.

Thinprint

Mit NetApp VDS können RDS- und/oder AVD-Umgebungen implementiert werden. Bei der Bereitstellung von AVD kann dieser Schalter **aus** bleiben (ein-/Ausschalter links).

Benachrichtigungs-E-Mail

VDS sendet Benachrichtigungen zur Bereitstellung und laufende Gesundheitsberichte an die **E-Mail**. Dies kann später geändert werden.

VMs und Netzwerk

Es gibt eine Vielzahl von Services, die ausgeführt werden müssen, um eine VDS-Umgebung zu unterstützen – diese werden gemeinsam als „VDS-Plattform“ bezeichnet. Je nach Konfiguration können diese CWMGR, ein oder zwei RDS Gateways, ein oder zwei HTML5 Gateways, einen FTPS Server und ein oder zwei Active Directory VMs umfassen.

Bei den meisten AVD-Bereitstellungen kommt die Option Single Virtual Machine zum Einsatz, da Microsoft die AVD-Gateways als PaaS-Service verwaltet.

Für kleinere und einfachere Umgebungen, in denen RDS-Anwendungsfälle enthalten sind, können alle diese

Services zur Senkung der VM-Kosten (bei eingeschränkter Skalierbarkeit) zu einer Option mit einzelnen Virtual Machines zusammengefasst werden. Für RDS-Anwendungsfälle mit mehr als 100 Benutzern wird die Option mehrere virtuelle Maschinen empfohlen, um die Skalierbarkeit von RDS und/oder HTML5-Gateway zu vereinfachen[]

Konfiguration der Plattform-VM

Mit NetApp VDS können RDS- und/oder AVD-Umgebungen implementiert werden. Bei der Bereitstellung von AVD wird die Auswahl einer einzelnen virtuellen Maschine empfohlen. Bei RDS-Implementierungen müssen Sie zusätzliche Komponenten wie Brokers und Gateways implementieren und managen. In der Produktion sollten diese Services auf dedizierten und redundanten Virtual Machines ausgeführt werden. Für AVD werden alle diese Dienste von Azure als inkludiert bereitgestellt und somit wird die **Single Virtual Machine** Konfiguration empfohlen.

Nur eine Virtual Machine

Dies ist die empfohlene Auswahl für Bereitstellungen, die ausschließlich AVD verwenden (und nicht RDS oder eine Kombination der beiden). In der Implementierung einer einzelnen Virtual Machine werden alle folgenden Rollen auf einer einzelnen VM in Azure gehostet:

- CW-Manager
- HTML5-Gateway
- RDS-Gateway
- Remote-App
- FTPS-Server (optional)
- Domänencontroller-Rolle

Die maximal empfohlene Benutzeranzahl für RDS-Anwendungsfälle in dieser Konfiguration beträgt 100 Benutzer. In dieser Konfiguration bieten ausgewogene RDS/HTML5-Gateways keine Option, was die Redundanz und Optionen für zukünftige Skalierungen einschränkt. Auch dieses Limit gilt nicht für AVD-Bereitstellungen, da Microsoft die Gateways als PaaS-Service verwaltet.



Wenn diese Umgebung für die Mandantenfähigkeit entwickelt wurde, wird eine Konfiguration einer einzelnen Virtual Machine nicht unterstützt – weder AVD noch AD Connect.

Mehrere Virtual Machines

Beim Aufteilen der VDS-Plattform in mehrere virtuelle Maschinen werden die folgenden Rollen auf dedizierten VMs in Azure gehostet:

- Remote-Desktop-Gateway

VDS Setup kann zur Bereitstellung und Konfiguration von einem oder zwei RDS Gateways verwendet werden. Diese Gateways leiten die RDS-Benutzersitzung vom offenen Internet an die in der Implementierung verwendeten Session-Host-VMs weiter. RDS Gateways verfügen über eine wichtige Funktion, um RDS vor direkten Angriffen aus dem offenen Internet zu schützen und den gesamten RDS-Datenverkehr in der Umgebung zu verschlüsseln. Bei Auswahl von zwei Remote Desktop Gateways implementiert das VDS Setup zwei VMs und konfiguriert sie so, dass ein Lastausgleich der eingehenden RDS-Benutzersitzungen möglich wird.

- HTML5-Gateway

VDS Setup kann zur Bereitstellung und Konfiguration von einem oder zwei HTML5 Gateways verwendet werden. Diese Gateways hosten die HTML5-Dienste, die von der Funktion *Connect to Server* in VDS und dem webbasierten VDS-Client (H5 Portal) verwendet werden. Wenn zwei HTML5-Portale ausgewählt wurden, implementiert das VDS Setup zwei VMs und konfiguriert sie so, dass ein Lastausgleich der eingehenden HTML5-Benutzersitzungen möglich ist.



Bei der Verwendung mehrerer Serveroption (auch wenn Benutzer nur über den installierten VDS Client eine Verbindung herstellen) wird mindestens ein HTML5-Gateway dringend empfohlen, um die *Connect to Server*-Funktionalität von VDS zu aktivieren.

- Hinweise Zur Gateway-Skalierbarkeit

In RDS-Anwendungsfällen lässt sich die maximale Größe der Umgebung mit zusätzlichen Gateway VMs horizontal skalieren, wobei jeder RDS oder HTML5 Gateway ca. 500 Benutzer unterstützen kann. Weitere Gateways können zu einem späteren Zeitpunkt mit minimaler Unterstützung von NetApp Professional Services hinzugefügt werden

Wenn diese Umgebung für die Mandantenfähigkeit entwickelt wurde, ist die Auswahl mehrerer Virtual Machines erforderlich.

Zeitzone

Während die Erfahrungen der Endbenutzer ihre lokale Zeitzone widerspiegeln, muss eine Standardzeitzone ausgewählt werden. Wählen Sie die Zeitzone aus, in der die **primäre Verabreichung** der Umgebung ausgeführt werden soll.

Umfang virtueller Netzwerke

Eine Best Practice besteht darin, VMs je nach Verwendungszweck in unterschiedlichen Subnetzen zu isolieren. Definieren Sie zunächst den Netzwerkumfang und fügen Sie einen Bereich /20 hinzu.

VDS Setup erkennt und schlägt einen Bereich vor, der sich als erfolgreich erweisen sollte. Gemäß den Best Practices müssen die Subnetz-IP-Adressen in einen privaten IP-Adressbereich fallen.

Diese Bereiche sind:

- 192.168.0.0 bis 192.168.255.255
- 172.16.0.0 bis 172.31.255.255
- 10.0.0.0 bis 10.255.255.255

Überprüfen und Anpassen Sie bei Bedarf, und klicken Sie dann auf Validieren, um Subnetze für die folgenden Bereiche zu identifizieren:

- Mandant: In diesem Bereich befinden sich Session-Host-Server und Datenbankserver
- Services: In diesem Bereich befinden sich PaaS-Dienste wie Azure NetApp Files
- Plattform: Dies ist der Bereich, in dem sich die Plattform-Server befinden
- Verzeichnis: Dies ist der Bereich, in dem sich AD-Server befinden

Prüfen

Auf der letzten Seite können Sie Ihre Auswahl überprüfen. Wenn Sie die Überprüfung abgeschlossen haben, klicken Sie auf die Schaltfläche „Validieren“. VDS Setup prüft alle Einträge und stellt sicher, dass die

Bereitstellung mit den bereitgestellten Informationen fortfahren kann. Diese Validierung kann 2-10 Minuten in Anspruch nehmen. Um den Fortschritt zu verfolgen, können Sie auf das Logologo (oben rechts) klicken, um die Validierungsaktivität anzuzeigen.

Nach Abschluss der Validierung wird die grüne Schaltfläche für die Bereitstellung anstelle der Schaltfläche „Validieren“ angezeigt. Klicken Sie auf die Bereitstellung, um den Bereitstellungsprozess für Ihre Implementierung zu starten.

Status

Der Bereitstellungsprozess dauert je nach Azure Workload und Ihren getroffenen Entscheidungen zwischen 2-4 Stunden. Sie können den Fortschritt im Protokoll verfolgen, indem Sie auf die Statusseite klicken oder auf die E-Mail warten, die Ihnen den Abschluss des Bereitstellungsprozesses mitteilen wird. Die Implementierung erstellt die Virtual Machines und Azure Komponenten, die zur Unterstützung von VDS und Remote Desktop oder einer AVD-Implementierung erforderlich sind. Dies umfasst eine einzelne Virtual Machine, die sowohl als Remote-Desktop-Session-Host als auch als File Server fungieren kann. In einer AVD-Implementierung fungiert diese virtuelle Maschine nur als Dateiserver.

Installieren und konfigurieren Sie AD Connect

Unmittelbar nach erfolgreicher Installation muss AD Connect auf dem Domain Controller installiert und konfiguriert werden. In einer singe Plattform VM Setup ist die CWMGR1 Maschine das DC. Die Benutzer in AD müssen die Synchronisierung zwischen Azure AD und der lokalen Domäne durchführen.

Gehen Sie wie folgt vor, um AD Connect zu installieren und zu konfigurieren:

1. Stellen Sie eine Verbindung mit dem Domänencontroller als Domänenadministrator her.
 - a. Anmeldedaten aus Azure Key Vault erhalten (siehe ["Anweisungen zu Key Vault finden Sie hier"](#))
2. Installieren Sie AD Connect, melden Sie sich mit dem Domänenadministrator (mit Rollenberechtigungen für Enterprise Admin) und der globalen Administrator von Azure AD an

AVD-Dienste aktivieren

Sobald die Bereitstellung abgeschlossen ist, wird die AVD-Funktion im nächsten Schritt aktiviert. Für den AVD-Prozess muss der Azure Administrator mehrere Schritte durchführen, um seine Azure AD-Domäne zu registrieren und das Abonnement für den Zugriff über die Azure AVD-Services durchzuführen. Ähnlich benötigt Microsoft VDS, um dieselben Berechtigungen für unsere Automatisierungssaplikation in Azure anzufordern. Die nachstehenden Schritte führen Sie durch diesen Prozess.

Erstellen Sie den AVD-Hostpool

Der Endbenutzer-Zugriff auf virtuelle AVD-Maschinen wird durch Hostpools verwaltet, die virtuelle Maschinen und Anwendungsgruppen enthalten, die wiederum die Benutzer und die Art des Benutzerzugriffs enthalten.

Um Ihren ersten Host-Pool zu erstellen

1. Klicken Sie auf die Schaltfläche Hinzufügen auf der rechten Seite der Kopfzeile des AVD-Hostpools.[]
2. Geben Sie einen Namen und eine Beschreibung für Ihren Host-Pool ein.
3. Wählen Sie einen Host-Pool-Typ aus
 - a. **Pool** bedeutet, dass mehrere Benutzer mit denselben Anwendungen auf denselben Pool virtueller Maschinen zugreifen.
 - b. **Personal** erstellt einen Host-Pool, in dem Benutzern eine eigene Session-Host-VM zugewiesen wird.
4. Wählen Sie den Typ Load Balancer aus

- a. **Tiefe zuerst** füllt die erste gemeinsam genutzte virtuelle Maschine auf die maximale Anzahl der Benutzer, bevor sie auf der zweiten virtuellen Maschine im Pool beginnt
 - b. **Breite First** verteilt Benutzer auf alle virtuellen Maschinen im Pool in runder Robin-Weise
5. Wählen Sie eine Azure Virtual Machines-Vorlage zum Erstellen der virtuellen Maschinen in diesem Pool aus. Während VDS alle Vorlagen enthält, die im Abonnement verfügbar sind, empfehlen wir die Auswahl des neuesten Windows 10 Multiuser Builds für die beste Erfahrung. Der aktuelle Build ist Windows-10-20h1-evd. (Optional können Sie mithilfe der Provisioning Collection-Funktion ein Gold-Image erstellen, um Hosts von einem individuellen Image der Virtual Machine zu erstellen.)
6. Wählen Sie die Azure Maschinengröße aus. Zu Evaluierungszwecken empfiehlt NetApp die D-Series (Standard-Maschinentyp für mehrere Benutzer) bzw. die E-Series (Erweiterte Speicherkonfiguration für Szenarien mit mehreren Benutzern und höheren Anforderungen). Die Maschinengrößen können später im VDS geändert werden, wenn Sie mit unterschiedlichen Serien und Größen experimentieren möchten
7. Wählen Sie in der Dropdown-Liste einen kompatiblen Speichertyp für die Managed Disk-Instanzen der virtuellen Maschinen aus
8. Wählen Sie die Anzahl der virtuellen Maschinen aus, die im Rahmen des Hostpool-Erstellungsprozesses erstellt werden sollen. Sie können später dem Pool virtuelle Maschinen hinzufügen. VDS erstellt jedoch die Anzahl der von Ihnen anfragenden virtuellen Maschinen und fügt diese nach der Erstellung dem Host-Pool hinzu
9. Klicken Sie auf die Schaltfläche Hostpool hinzufügen, um den Erstellungsvorgang zu starten. Sie können den Fortschritt auf der AVD-Seite verfolgen oder die Details des Prozessprotokolls auf der Seite Name der Bereitstellungen/Bereitstellung im Abschnitt Aufgaben anzeigen
10. Sobald der Host-Pool erstellt wurde, wird er in der Liste Host-Pool auf der AVD-Seite angezeigt. Klicken Sie auf den Namen des Host-Pools, um seine Detailseite zu sehen, die eine Liste seiner virtuellen Maschinen, App-Gruppen und aktiven Benutzer enthält



AVD-Hosts werden in VDS mit einer Einstellung erstellt, die die Verbindung von Benutzersitzungen nicht zulässt. Dies ist durch das Design, um Anpassungen zu ermöglichen, bevor Benutzerverbindungen akzeptiert werden. Diese Einstellung kann durch Bearbeiten der Einstellungen des Sitzungshosts geändert werden. []

Aktivieren Sie VDS-Desktops für Benutzer

Wie bereits erwähnt, erstellt VDS alle Elemente, die zur Unterstützung der Endbenutzer-Workspaces während der Implementierung erforderlich sind. Sobald die Bereitstellung abgeschlossen ist, müssen Sie den Workspace-Zugriff für jeden Benutzer aktivieren, der in die AVD-Umgebung eingeführt werden soll. In diesem Schritt werden die Profilkonfiguration und der Zugriff auf die Endbenutzerdatenebene erstellt, was der Standard für einen virtuellen Desktop ist. VDS verwendet diese Konfiguration, um die Azure AD-Endbenutzer mit den AVD-App-Pools zu verbinden.

Gehen Sie wie folgt vor, um Arbeitsbereiche für Endbenutzer zu aktivieren:

1. Melden Sie sich bei VDS an <https://manage.cloudworkspace.com> Verwenden des primären VDS-Administratorkontos, das Sie während der Bereitstellung erstellt haben. Falls Sie Ihre Kontoinformationen nicht speichern, wenden Sie sich bitte an NetApp VDS, um Hilfe beim Abrufen des Kontos zu erhalten
2. Klicken Sie auf das Menüelement Arbeitsräume und dann auf den Namen des Arbeitsbereichs, der während der Bereitstellung automatisch erstellt wurde
3. Klicken Sie auf die Registerkarte Benutzer und Gruppen[]
4. Scrollen Sie für jeden Benutzer, den Sie aktivieren möchten, über den Benutzernamen und klicken Sie dann auf das Zahnrad-Symbol

5. Wählen Sie die Option „Cloud Workspace aktivieren“[]
6. Die Aktivierung dauert etwa 30-90 Sekunden. Beachten Sie, dass sich der Benutzerstatus von „Ausstehend“ in „verfügbar“ ändert



Durch die Aktivierung von Azure AD-Domänendiensten wird eine gemanagte Domäne in Azure erstellt, und jede neu erstellte AVD-Virtual Machine wird zu dieser Domäne verbunden. Damit die herkömmliche Anmeldung bei den Virtual Machines funktioniert, muss der Passwort-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.

Aktivieren von Benutzersitzungen

Standardmäßig können Session-Hosts keine Benutzerverbindungen akzeptieren. Diese Einstellung wird häufig als „Drain-Modus“ bezeichnet, da sie in der Produktion verwendet werden kann, um neue Benutzersitzungen zu verhindern, so dass der Host schließlich alle Benutzersitzungen entfernen kann. Wenn neue Benutzersitzungen auf einem Host erlaubt sind, wird diese Aktion allgemein als Platzierung des Session-Hosts „in Rotation“ bezeichnet.

In der Produktion ist es sinnvoll, neue Hosts im Drain-Modus zu starten, da es normalerweise Konfigurationsaufgaben gibt, die abgeschlossen werden müssen, bevor der Host für Produktions-Workloads bereit ist.

Beim Testen und Auswerten können Sie die Hosts sofort aus dem Ablassmodus nehmen, um die Benutzerverbindung zu ermöglichen und die Funktionalität zu bestätigen. Um Benutzersitzungen auf dem/den Sitzungshost(s) zu aktivieren, führen Sie folgende Schritte aus:

1. Navigieren Sie auf der Workspace-Seite zum AVD-Abschnitt.
2. Klicken Sie auf den Namen des Host Pools unter „AVD Host Pools“.[[]]
3. Klicken Sie auf den Namen des/der Sitzungshosts und aktivieren Sie das Kontrollkästchen „Neue Sitzungen zulassen“, klicken Sie auf „Sitzungshost aktualisieren“. Wiederholen Sie dies für alle Hosts, die in Rotation versetzt werden müssen.[[]]
4. Die aktuellen Statistiken von „Neue Sitzung zulassen“ werden auch auf der Haupt-AVD-Seite für jeden Host-Posten angezeigt.

Standard-App-Gruppe

Beachten Sie, dass die Desktop Application Group standardmäßig im Rahmen des Hostpool-Erstellungsprozesses erstellt wird. Diese Gruppe bietet interaktiven Desktop-Zugriff für alle Gruppenmitglieder. Zum Hinzufügen von Mitgliedern zur Gruppe:

1. Klicken Sie auf den Namen der App-Gruppe[[]]
2. Klicken Sie auf den Link, der die Anzahl der hinzugefügten Benutzer anzeigt[[]]
3. Wählen Sie die Benutzer aus, die Sie der App-Gruppe hinzufügen möchten, indem Sie das Kästchen neben ihrem Namen aktivieren
4. Klicken Sie auf die Schaltfläche Benutzer auswählen
5. Klicken Sie auf die Schaltfläche App-Gruppe aktualisieren

Zusätzliche AVD-App-Gruppen erstellen

Dem Host-Pool können weitere Applikationsgruppen hinzugefügt werden. Diese App-Gruppen veröffentlichen bestimmte Anwendungen aus den virtuellen Hostpool-Maschinen an die Benutzer der App-Gruppe, die RemoteApp verwenden.



AVD ermöglicht nur die Zuweisung von Endbenutzern zum Typ der Desktop App-Gruppe oder der RemoteApp-App-Gruppe, aber nicht beide im selben Host-Pool. Stellen Sie also sicher, dass Sie Ihre Benutzer entsprechend trennen. Wenn Benutzer auf einen Desktop und Streaming-Applikationen zugreifen müssen, ist ein zweiter Host-Pool erforderlich, um die Applikationen zu hosten.

So erstellen Sie eine neue Anwendungsgruppe:

1. Klicken Sie in der Kopfzeile des Bereichs „Anwendungsgruppen“ auf die Schaltfläche Hinzufügen[]
2. Geben Sie einen Namen und eine Beschreibung für die App-Gruppe ein
3. Wählen Sie Benutzer aus, die der Gruppe hinzugefügt werden sollen, indem Sie auf den Link Benutzer hinzufügen klicken. Wählen Sie jeden Benutzer aus, indem Sie auf das Kontrollkästchen neben seinem Namen klicken und dann auf die Schaltfläche Benutzer auswählen klicken[]
4. Klicken Sie auf den Link RemoteApps hinzufügen, um dieser Anwendungsgruppe Anwendungen hinzuzufügen. AVD generiert automatisch die Liste möglicher Anwendungen durch Scannen der Liste der auf der virtuellen Maschine installierten Anwendungen. Wählen Sie die Anwendung aus, indem Sie auf das Kontrollkästchen neben dem Anwendungsnamen klicken und dann auf die Schaltfläche RemoteApps auswählen klicken.[]
5. Klicken Sie auf die Schaltfläche App-Gruppe hinzufügen, um die App-Gruppe zu erstellen

AVD-Zugriff für Endbenutzer

Endbenutzer können über den Web Client oder einen installierten Client auf verschiedenen Plattformen auf AVD-Umgebungen zugreifen

- Web-Client: <https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-web>
- Web-Client-Anmelde-URL: <http://aka.ms/AVDweb>
- Windows-Client: <https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-windows-7-and-10>
- Android-Client: <https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-android>
- MacOS-Client: <https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-macos>
- IOS-Client: <https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-ios>
- IGEL Thin Client: <https://www.igel.com/igel-solution-family/windows-virtual-desktop/>

Melden Sie sich mit dem Benutzernamen und Kennwort des Endbenutzers an. Beachten Sie, dass Remote-App- und Desktop-Verbindungen (RADC), Remote Desktop Connection (mstsc) und die CloudWorksapce Client for Windows-Anwendung derzeit nicht die Möglichkeit zur Anmeldung bei AVD-Instanzen unterstützen.

Überwachen von Benutzeranmeldungen

Auf der Detailseite des Host-Pools wird auch eine Liste aktiver Benutzer angezeigt, wenn sie sich bei einer AVD-Sitzung anmelden.

Admin-Verbindungsoptionen

VDS-Administratoren können auf unterschiedliche Weise eine Verbindung zu virtuellen Maschinen in der Umgebung herstellen.

Verbindung zum Server herstellen

Im gesamten Portal finden VDS-Administratoren die Option „mit Server verbinden“. Standardmäßig verbindet diese Funktion den Admin mit der virtuellen Maschine, indem sie dynamisch lokale Admin-Anmeldeinformationen generiert und in eine Web-Client-Verbindung eingibt. Der Administrator muss keine Anmeldedaten kennen (und wird nie mit), um eine Verbindung herzustellen.

Dieses Standardverhalten kann wie im nächsten Abschnitt beschrieben pro Administrator deaktiviert werden.

.Tech/Level 3 Administratorkonten

Im CWA Setup wird ein „Level III“-Administratorkonto erstellt. Der Benutzername ist als [username.tech@domain.xyz](#) formatiert

Diese Konten, allgemein als ".Tech"-Konto, werden als Domain-Level-Administrator-Konten. VDS-Administratoren können ihr .Tech-Konto bei der Verbindung zu einem CWMGR1-Server (Plattform) und optional bei der Verbindung mit allen anderen virtuellen Maschinen in der Umgebung verwenden.

Um die automatische Anmeldefunktion für den lokalen Administrator zu deaktivieren und die Verwendung des Level III-Kontos zu erzwingen, ändern Sie diese Einstellung. Navigieren Sie zu VDS > Admins > Administratorname > Aktivieren Sie „Tech Account Enabled“. Wenn dieses Kontrollkästchen aktiviert ist, wird der VDS-Administrator nicht automatisch als lokaler Administrator bei virtuellen Maschinen angemeldet und stattdessen aufgefordert, seine .Tech-Anmeldedaten einzugeben.

Diese Zugangsdaten und andere relevante Zugangsdaten werden automatisch in *Azure Key Vault* gespeichert und sind über das Azure Management Portal unter zugänglich <https://portal.azure.com/>.

Optionale Aktionen nach der Implementierung

Multi-Faktor-Authentifizierung (MFA)

NetApp VDS beinhaltet kostenlos SMS/E-Mail MFA. Diese Funktion kann zur Sicherung von VDS-Administratorkonten und/oder Endbenutzerkonten verwendet werden. "[MFA-Artikel](#)"

Workflow für Anwendungsberechtigungen

VDS bietet einen Mechanismus, um Endbenutzern Zugriff auf Anwendungen aus einer vordefinierten Liste von Anwendungen, die als Anwendungskatalog bezeichnet werden, zuzuweisen. Der Applikationskatalog umfasst alle gemanagten Implementierungen.



Der automatisch bereitgestellte TSD1-Server muss unverändert bleiben, um Anwendungsberechtigungen zu unterstützen. Führen Sie die Funktion „in Daten konvertieren“ nicht gegen diese virtuelle Maschine aus.

Application Management wird in diesem Artikel ausführlich beschrieben: ""

Azure AD-Sicherheitsgruppen

VDS verfügt über Funktionen zum Erstellen, Befüllen und Löschen von Benutzergruppen, die durch Azure AD-Sicherheitsgruppen unterstützt werden. Diese Gruppen können wie jede andere Sicherheitsgruppe auch

außerhalb von VDS verwendet werden. In VDS können diese Gruppen verwendet werden, um Ordnerberechtigungen und Anwendungsberechtigungen zuzuweisen.

Erstellen von Benutzergruppen

Das Erstellen von Benutzergruppen erfolgt auf der Registerkarte Benutzer und Gruppen innerhalb eines Arbeitsbereichs.

Ordnerberechtigungen nach Gruppe zuweisen

Berechtigungen zum Anzeigen und Bearbeiten von Ordnern in der Firmenfreigabe können Benutzern oder Gruppen zugewiesen werden.

""

Anwendungen nach Gruppe zuweisen

Zusätzlich zur individuellen Zuweisung von Applikationen zu Benutzern können Applikationen Gruppen bereitgestellt werden.

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.[]

Optionen zur Kostenoptimierung konfigurieren

Das Workspace-Management erweitert auch die Verwaltung der Azure-Ressourcen, die die AVD-Implementierung unterstützen. VDS ermöglicht Ihnen die Konfiguration von Workload-Zeitplänen sowie der Live-Skalierung, um Azure Virtual Machines entsprechend der Endbenutzeraktivitäten ein- und auszuschalten. Diese Funktionen führen dazu, dass Azure Ressourcenauslastung und Ausgaben mit dem tatsächlichen Nutzungsmuster der Endbenutzer übereinstimmen. Wenn Sie darüber hinaus eine AVD-Proof-of-Concept-Implementierung konfiguriert haben, können Sie die gesamte Implementierung über die VDS-Schnittstelle drehen.

Workload-Planung

Workload Scheduling ist eine Funktion, mit der der Administrator einen festgelegten Zeitplan erstellen kann, damit die virtuellen Arbeitsumgebungen aktiviert sind, um Endbenutzersitzungen zu unterstützen. Wenn das Ende des geplanten Zeitraums für einen bestimmten Tag der Woche erreicht wird, stoppt/delokalisiert VDS die virtuellen Maschinen in Azure, so dass die Stundengebühren aufhören.

So aktivieren Sie das Workload-Scheduling:

1. Melden Sie sich bei VDS an <https://manage.cloudworkspace.com> Verwenden Ihrer VDS-Anmeldedaten.
2. Klicken Sie auf den Menüpunkt Arbeitsbereich und dann auf den Namen des Arbeitsbereichs in der Liste. []
3. Klicken Sie auf die Registerkarte Arbeitszeitplan. []
4. Klicken Sie in der Kopfzeile des Workload-Zeitplans auf den Link Verwalten. []
5. Wählen Sie im Dropdown-Menü Status einen Standardstatus aus: Immer ein (Standard), immer aus oder geplant.
6. Wenn Sie „terminiert“ auswählen, stehen Ihnen die Optionen für die Zeitplanung zur Verfügung:
 - a. Führen Sie jeden Tag im zugewiesenen Intervall aus. Mit dieser Option wird für alle sieben Tage der Woche die gleiche Startzeit und Endzeit festgelegt. []

- b. Führen Sie die Ausführung im zugewiesenen Intervall für die angegebenen Tage durch. Mit dieser Option wird der Zeitplan nur für ausgewählte Wochentage auf dieselbe Start- und Endzeit festgelegt. Nicht ausgewählte Wochentage führen dazu, dass VDS die virtuellen Maschinen für diese Tage nicht einschalten wird. []
- c. Lauf in variablen Zeitintervallen und Tagen. Mit dieser Option wird der Zeitplan für jeden ausgewählten Tag auf unterschiedliche Start- und Endzeiten festgelegt. []
- d. Klicken Sie auf die Schaltfläche Zeitplan aktualisieren, wenn Sie den Zeitplan festgelegt haben. []

Live-Skalierung

Durch die Live-Skalierung werden Virtual Machines in einem gemeinsam genutzten Host-Pool automatisch ein- und ausgeschaltet, je nach simultaner Auslastung. Wenn sich jeder Server füllt, wird ein zusätzlicher Server eingeschaltet, sodass er bereit ist, wenn der Host Pool Load Balancer Benutzersitzungsanforderungen sendet. Für eine effektive Nutzung der Live-Skalierung wählen Sie „Tiefe zuerst“ als Lastausgleichstyp.

So aktivieren Sie die Live-Skalierung:

1. Melden Sie sich bei VDS an <https://manage.cloudworkspace.com> Verwenden Ihrer VDS-Anmeldedaten.
2. Klicken Sie auf den Menüpunkt Arbeitsbereich und dann auf den Namen des Arbeitsbereichs in der Liste. []
3. Klicken Sie auf die Registerkarte Arbeitszeitplan. []
4. Klicken Sie im Abschnitt Live-Skalierung auf das Optionsfeld aktiviert. []
5. Klicken Sie auf die maximale Anzahl der Benutzer pro Server und geben Sie die maximale Anzahl ein. Je nach Größe der Virtual Machines liegt diese Zahl in der Regel zwischen 4 und 20. []
6. OPTIONAL: Klicken Sie auf die Option Extra Powered auf Servern aktiviert, und geben Sie eine Reihe von zusätzlichen Servern ein, die Sie für den Host-Pool verwenden möchten. Diese Einstellung aktiviert neben dem aktiv füllenden Server die angegebene Anzahl von Servern als Puffer für große Gruppen von Benutzern, die sich im selben Zeitfenster anmelden. []



Live-Skalierung gilt derzeit für alle gemeinsam genutzten Ressourcenpools. In naher Zukunft wird jeder Pool über unabhängige Live-Skalierung-Optionen verfügen.

Schalten Sie die gesamte Implementierung ab

Wenn Sie Ihre Evaluierungsimplementierung nur für sporadisch und nicht für die Produktion verwenden möchten, können Sie alle Virtual Machines der Bereitstellung deaktivieren, wenn Sie diese nicht nutzen.

Um die Implementierung ein- oder auszuschalten (d. h. die virtuellen Maschinen in der Implementierung auszuschalten), gehen Sie folgendermaßen vor:

1. Melden Sie sich bei VDS an <https://manage.cloudworkspace.com> Verwenden Ihrer VDS-Anmeldedaten.
2. Klicken Sie auf den Menüpunkt Bereitstellungen. [] Scrollen Sie mit dem Cursor über die Zeile für die Zielbereitstellung, um das Symbol für die Konfigurationsausrüstung anzuzeigen. []
3. Klicken Sie auf das Zahnrad, und wählen Sie dann Stopp. []
4. Um neu zu starten oder zu starten, befolgen Sie die Schritte 1-3, und wählen Sie dann Start. []



Es kann einige Minuten dauern, bis alle Virtual Machines der Implementierung angehalten oder gestartet werden.

Erstellen und Managen von VM Images

VDS enthält Funktionen zum Erstellen und Managen von Virtual-Machine-Images für zukünftige Bereitstellungen. Um diese Funktion zu erreichen, navigieren Sie zu: VDS > Bereitstellungen > Bereitstellungsname > Provisioning-Sammlungen. Die Funktionen der „VDI Image Collection“ sind hier dokumentiert: ""

Konfigurieren Sie Azure Cloud Backup Service

VDS kann Azure Cloud Backup, einen Azure PaaS-Service für das Backup von virtuellen Maschinen, nativ konfigurieren und managen. Backup-Richtlinien können einzelnen Maschinen oder Gruppen von Maschinen nach Typ oder Host-Pool zugewiesen werden. Details finden Sie hier: ""

Wählen Sie App-Management/Richtlinienmodus aus

Standardmäßig implementiert VDS eine Anzahl von Gruppenrichtlinienobjekten (GPO), die den Arbeitsbereich des Endbenutzers sperren. Diese Richtlinien verhindern den Zugriff auf die Standorte der zentralen Datenebene (z. B. c:\) und die Möglichkeit, Anwendungsininstallationen als Endbenutzer durchzuführen.

Diese Evaluierung soll die Funktionen von Windows Virtual Desktop demonstrieren, sodass Sie die Option haben, die Gruppenrichtlinienobjekte zu entfernen, sodass Sie einen „grundlegenden Arbeitsbereich“ implementieren können, der die gleiche Funktionalität und den gleichen Zugriff wie ein physischer Arbeitsbereich bietet. Führen Sie dazu die Schritte in der Option „Basic Workspace“ aus.

Sie können auch wählen, um den vollen virtuellen Desktop-Management-Funktionssatz zu verwenden, um einen „kontrollierten Arbeitsbereich“ zu implementieren. Diese Schritte umfassen die Erstellung und Verwaltung eines Anwendungskatalogs für Berechtigungen der Endbenutzeranwendung und die Verwendung von Administratorberechtigungen zum Verwalten des Zugriffs auf Anwendungen und Datenordner. Befolgen Sie die Schritte im Abschnitt „Controlled Workspace“, um diesen Workspace in Ihren AVD-Hostpools zu implementieren.

Gesteuerter AVD-Arbeitsbereich (Standardrichtlinien)

Die Verwendung eines kontrollierten Arbeitsbereichs ist der Standardmodus für VDS-Bereitstellungen. Die Richtlinien werden automatisch angewendet. In diesem Modus müssen VDS-Administratoren Anwendungen installieren, und den Endbenutzern wird dann über eine Verknüpfung auf dem Session-Desktop Zugriff auf die Anwendung gewährt. Auf ähnliche Weise wird dem Endbenutzer der Zugriff auf die Datenordner zugewiesen, indem zugewiesene freigegebene Ordner erstellt und Berechtigungen eingerichtet werden, um nur die zugeordneten Laufwerksbuchstaben anstelle der Standard-Boot- und/oder Datenlaufwerke zu sehen. Um diese Umgebung zu verwalten, befolgen Sie die nachstehenden Schritte, um Anwendungen zu installieren und Endbenutzern Zugang zu gewähren.

Zurücksetzen auf den AVD-Arbeitsbereich

Zum Erstellen eines grundlegenden Arbeitsbereichs müssen die standardmäßig erstellten Gruppenrichtlinienrichtlinien deaktiviert werden.

Gehen Sie dazu wie folgt vor:

1. Melden Sie sich bei VDS an <https://manage.cloudworkspace.com> Verwendung der primären Anmeldedaten des Administrators
2. Klicken Sie links auf den Menüpunkt Bereitstellungen. []
3. Klicken Sie auf den Namen Ihrer Bereitstellung. []
4. Scrollen Sie im Abschnitt Platform Servers (Mid page on right) nach rechts in die Zeile für CWMGR1, bis

das Getriebe angezeigt wird. []

5. Klicken Sie auf das Zahnrad und wählen Sie Verbinden. []
6. Geben Sie die „Tech“-Anmeldeinformationen ein, die Sie während der Bereitstellung erstellt haben, um sich mit HTML5-Zugriff auf den CWMGR1-Server anzumelden. []
7. Klicken Sie auf das Menü Start (Windows) und wählen Sie Windows Administrative Tools. []
8. Klicken Sie auf das Symbol Gruppenrichtlinienverwaltung. []
9. Klicken Sie auf das Element AADDC-Benutzer in der Liste im linken Bereich. []
10. Klicken Sie mit der rechten Maustaste auf die „Cloud Workspace Users“-Richtlinie in der Liste im rechten Fensterbereich, und deaktivieren Sie dann die Option „Link Enabled“. Klicken Sie auf OK, um diese Aktion zu bestätigen. [] []
11. Wählen Sie im Menü Aktion, Gruppenrichtlinienaktualisierung, und bestätigen Sie, dass Sie eine Richtlinienaktualisierung auf diesen Computern erzwingen möchten. []
12. Wiederholen Sie die Schritte 9 und 10, wählen Sie aber „AADDC-Benutzer“ und „Cloud Workspace-Unternehmen“ als Richtlinie, um den Link zu deaktivieren. Nach diesem Schritt müssen Sie keine Aktualisierung der Gruppenrichtlinien erzwingen. [] []
13. Schließen Sie den Editor Gruppenrichtlinienverwaltung und die Fenster Verwaltung und dann Abmelden. [] Diese Schritte stellen eine grundlegende Arbeitsumgebung für Endbenutzer dar. Um zu bestätigen, melden Sie sich als eines Ihrer Endbenutzerkonten an. Die Sitzungsumgebung sollte keine der Einschränkungen des kontrollierten Arbeitsbereichs aufweisen, wie z. B. das versteckte Startmenü, den gesperrten Zugriff auf das Laufwerk C:\ und das verborgene Bedienfeld.



Das während der Implementierung erstellte .tech-Konto hat vollständigen Zugriff auf die Installation von Anwendungen und die Änderung der Sicherheit von Ordnern unabhängig von VDS. Wenn Sie jedoch möchten, dass Endbenutzer aus der Azure AD-Domäne einen ähnlichen vollständigen Zugriff haben, sollten Sie diese der Gruppe der lokalen Administratoren auf jeder virtuellen Maschine hinzufügen.

AVD Deployment Guide – vorhandener AD-Zusatzhandbuch

Überblick

VDS Setup hat die Möglichkeit, eine neue Bereitstellung mit einer vorhandenen AD-Struktur zu verbinden. Diese Anweisung deckt diese Option im Detail ab. Dieser Artikel ist nicht eigenständiger, sondern eine detaillierte Erklärung einer Alternative zur neuen AD-Option, die in der beschrieben wird "[AVD-Bereitstellungsleitfaden](#)"

Typ Active Directory

Im nächsten Abschnitt wird der Bereitstellungstyp Active Directory für die VDS-Bereitstellung definiert. In diesem Handbuch werden wir vorhandenes Windows Server Active Directory auswählen, das eine bereits vorhandene AD-Struktur nutzt.

Vorhandenes AD-Netzwerk

VDS Setup zeigt eine Liste von vNets an, die die Verbindung zwischen der bestehenden AD-Struktur und Azure AD darstellen könnten. In der ausgewählten vnet-Version sollte ein von Azure gehostetes DC eingerichtet sein, das Sie in Azure konfiguriert haben. Zusätzlich verfügt vnet über benutzerdefinierte DNS-Einstellungen, auf die das von Azure gehostete DC verwiesen wird.

[]

Vorhandener Active Directory-Domänenname

Geben Sie den vorhandenen Domänennamen ein, der verwendet werden soll. Hinweis: Sie möchten die Domäne, die im Azure Portal unter dem Active Directory Modul zu finden ist, nicht verwenden, da sie zu DNS-Problemen führen kann. Das primäre Beispiel hierfür ist, dass Benutzer nicht über ihren Desktop auf diese Website (<yourdomain>.com, zum Beispiel) zugreifen können.

Vorhandener AD-Benutzername und Kennwort

Es gibt drei Möglichkeiten, die erforderlichen Zugangsdaten bereitzustellen, um die Implementierung mit einer vorhandenen AD-Struktur zu vereinfachen.

1. Geben Sie den Benutzernamen und das Kennwort für den Active Directory-Domänenadministrator an

Dies ist die einfachste Methode – Bereitstellung von Anmeldeinformationen für den Domänenadministrator, die zur Vereinfachung der Bereitstellung verwendet werden.



Dieses Konto kann für einen einmaligen Zweck erstellt und nach Abschluss des Implementierungsprozesses gelöscht werden.

2. Erstellen Sie Die Erforderlichen Berechtigungen Für Kontoabgleich

Bei dieser Methode müssen die Administratoren des Kunden hier manuell die Berechtigungsstruktur erstellen, dann hier die Anmeldedaten für das CloudWorkSpaceSVC-Konto eingeben und fortfahren.

3. Manueller Implementierungsprozess

Wenden Sie sich an den NetApp VDS Support, um Unterstützung bei der Konfiguration von AD-Zugriff mit den geringsten Berechtigungen bei Account-Principals zu erhalten.

Nächste Schritte

Dieser Artikel behandelt die einzigartigen Schritte zur Implementierung in einer vorhandenen AD Umgebung. Wenn Sie diese Schritte abgeschlossen haben, können Sie zurück zum Standard-Implementierungsleitfaden zurückkehren "[Hier](#)".

VDS-Komponenten und Berechtigungen

AVD- und VDS-Sicherheitseinheiten und -Dienste

Azure Virtual Desktop (AVD) erfordert für die Durchführung automatisierter Aktionen Sicherheitskonten und Komponenten sowohl in Azure AD als auch im lokalen Active Directory. Der NetApp Virtual Desktop Service (VDS) erstellt während des Implementierungsprozesses Komponenten und Sicherheitseinstellungen, mit denen Administratoren die AVD-Umgebung steuern können. In diesem Dokument werden die relevanten VDS-Konten, -Komponenten und -Sicherheitseinstellungen in beiden Umgebungen beschrieben.

Die Komponenten und Berechtigungen des Implementierungsprozesses unterscheiden sich hauptsächlich von den Komponenten der endgültigen implementierten Umgebung. Daher besteht dieser Artikel in zwei Hauptabschnitten, im Abschnitt zur Implementierungsautomatisierung und im Abschnitt zur implementierten Umgebung.

[Breite = 75 %]

Komponenten und Berechtigungen für die Automatisierung der AVD-Bereitstellung

BEI DER VDS-Implementierung werden mehrere Azure und NetApp Komponenten und Sicherheitsberechtigungen verwendet, um sowohl Implementierungen als auch Arbeitsumgebungen zu implementieren.

VDS Deployment Services

Enterprise-Applikationen

VDS nutzt Enterprise Applications und App-Registrierungen in der Azure AD-Domain eines Mandanten. Enterprise-Applikationen sind das Bindeglied für die Anrufe mit dem Azure Resource Manager, Azure Graph und (bei Verwendung der AVD Fall Release) AVD-API-Endpunkte aus dem Sicherheitskontext der Azure AD-Instanz. Dabei werden die delegierten Rollen und Berechtigungen verwendet, die dem zugeordneten Service Principal gewährt werden. App-Registrierungen können je nach Initialisierungsstatus der AVD-Dienste für den Mandanten über VDS erstellt werden.

Damit diese VMs erstellt und gemanagt werden können, erstellt VDS mehrere unterstützende Komponenten im Azure-Abonnement:

Cloud Workspace

Dies ist der erste Administrator von Enterprise-Anwendungen, der die Zustimmung erteilt und während des Bereitstellungsvorgangs des VDS-Setup-Assistenten verwendet wird.

Die Cloud Workspace Enterprise Application fordert während des VDS-Setup-Prozesses einen bestimmten Satz von Berechtigungen an. Diese Berechtigungen sind:

- Zugriffsverzeichnis als registrierter Benutzer (Delegierter)
- Lesen und Schreiben von Verzeichnisdaten (delegiert)
- Benutzerprofil anmelden und lesen (delegiert)
- Benutzer anmelden (delegiert)
- Grundlegendes Profil Der Benutzer Anzeigen (Delegiert)
- Zugriff auf Azure Service Management als Benutzer der Organisation (delegiert)

Cloud Workspace-API

Bewältigt allgemeine Managementaufforderungen für Azure PaaS-Funktionen. Beispiele für Azure PaaS-Funktionen sind Azure Compute, Azure Backup, Azure Files usw. dieser Service Principal benötigt während der ersten Implementierung Eigentümer-Rechte für das Azure-Zielabonnement und Mitwirkende Rechte für das fortlaufende Management (Hinweis: Für die Nutzung von Azure Files sind Abonnementrechte für Eigentümer erforderlich, um die Berechtigungen pro Benutzer für Azure File Objects festzulegen.)

Die Cloud Workspace API Enterprise Application fordert während des VDS-Einrichtungsvorgangs einen bestimmten Satz von Berechtigungen an. Diese Berechtigungen sind:

- Anbieter des Abonnements (oder Abbonementeigentümer, falls Azure Files verwendet wird)
- Azure AD Diagramm
 - Lesen und Schreiben aller Applikationen (Anwendung)
 - Managen von Apps, die von dieser Applikation erstellt oder Eigentümer sind (Applikation)
 - Lese- und Schreibgeräte (Anwendung)

- Zugriff auf das Verzeichnis wie der angemeldete Benutzer (Delegierter)
- Verzeichnisdaten Lesen (Anwendung)
- Verzeichnisdaten Lesen (Delegiert)
- Lesen und Schreiben von Verzeichnisdaten (Anwendung)
- Lesen und Schreiben von Verzeichnisdaten (delegiert)
- Lese- und Schreib-Domains (Anwendung)
- Alle Gruppen Lesen (Delegiert)
- Alle Gruppen lesen und schreiben (delegiert)
- Alle Verborgenen Mitgliedschaften Lesen (Anwendung)
- Versteckte Mitgliedschaften Lesen (Delegiert)
- Benutzerprofil anmelden und lesen (delegiert)
- Alle Profile Aller Benutzer Lesen (Delegiert)
- Grundlegende Profile Aller Benutzer Lesen (Delegiert)
- Azure Service-Management
 - Zugriff auf Azure Service Management als Benutzer der Organisation (delegiert)

NetApp VDS

NetApp VDS Komponenten werden über die VDS-Kontrollebene verwendet, um die Implementierung und Konfiguration von AVD-Rollen, Services und Ressourcen zu automatisieren.

Benutzerdefinierte Rolle

Die Rolle „Automation Contributor“ wurde entwickelt, um Bereitstellungen mithilfe von geringst privilegierten Methoden zu vereinfachen. Durch diese Rolle kann die VM CWMGR1 auf das Azure Automatisierungskonto zugreifen.

Konto „Automatisierung“

Während der Implementierung wird ein Konto zur Automatisierung erstellt und ist eine erforderliche Komponente während des Bereitstellungsprozesses. Das Konto „Automatisierung“ enthält Variablen, Zugangsdaten, Module und Konfigurationen für den gewünschten Zustand und verweist auf den Key Vault.

Konfiguration des gewünschten Status

Dies ist die Methode, mit der die Konfiguration von CWMGR1 erstellt wird. Die Konfigurationsdatei wird auf die VM heruntergeladen und über den lokalen Configuration Manager auf der VM angewendet. Beispiele für Konfigurationselemente:

- Windows-Funktionen werden installiert
- Software wird installiert
- Software-Konfigurationen werden angewendet
- Sicherstellen, dass die richtigen Berechtigungssätze angewendet werden
- Anwenden des Let's-Verschlüsseln-Zertifikats
- Sicherstellen, dass DNS-Einträge korrekt sind

- Stellen Sie sicher, dass CWMGR1 mit der Domäne verbunden ist

Module:

- ActiveDirectoryDSC: Gewünschter Status Konfiguration Ressource für die Bereitstellung und Konfiguration von Active Directory. Mit diesen Ressourcen können Sie neue Domänen, untergeordnete Domänen und hochverfügbarkeits-Domänencontroller konfigurieren, domänenübergreifende Trusts einrichten und Benutzer, Gruppen und OUs verwalten.
- AZ.Accounts: Ein von Microsoft bereitgeordnetes Modul für das Management von Anmeldedaten und allgemeinen Konfigurationselementen für Azure Module
- AZ.Automation: Ein von Microsoft bereitgeordnetes Modul für Azure Automation Kommandlets
- Az.Compute: A das von Microsoft bereitgestellte Modul für Azure Compute Commandlets
- AZ.KeyVault: Ein von Microsoft bereitgeordnetes Modul für Azure Key Vault Kommandlets
- AZ.Resources: Ein von Microsoft bereitgeordnetes Modul für Azure Resource Manager Befehle
- CChoco: Konfigurationsressource für den gewünschten Zustand zum Herunterladen und Installieren von Paketen mit Chocolatey
- CjAz: Dieses von NetApp erstellte Modul stellt dem Azure Automatisierungsmodul Automatisierungs-Tools zur Verfügung
- CjAzACS: Dieses von NetApp erstellte Modul enthält Funktionen zur Umgebungsautomatisierung und PowerShell Prozesse, die aus dem Benutzerkontext heraus ausgeführt werden.
- CjAzBuild: Dieses von NetApp erstellte Modul enthält Build- und Wartungsautomatisierung sowie PowerShell Prozesse, die im Systemkontext ausgeführt werden.
- CNtfsAccessControl: Konfigurationsressource für den gewünschten Zustand für die Verwaltung der NTFS-Zugriffskontrolle
- ComputerManagementDsc: Konfigurationsressource für den gewünschten Zustand, die Computerverwaltungsaufgaben wie das Verbinden einer Domäne und das Planen von Aufgaben sowie das Konfigurieren von Elementen wie virtuellem Speicher, Ereignisprotokollen, Zeitzonen und Energieeinstellungen ermöglichen.
- CUserRightsAssignment: Konfigurationsressource mit gewünschtem Status, die die Verwaltung von Benutzerrechten wie Login-Rechten und -Berechtigungen ermöglicht
- NetworkingDSC: t gewünschter Status Konfigurationsressource für das Netzwerk
- XCertificate: Konfigurationsressource für den gewünschten Zustand, um die Verwaltung von Zertifikaten auf Windows Server zu vereinfachen.
- XDnsServer: Konfigurationsressource für den gewünschten Zustand zur Konfiguration und Verwaltung von Windows Server DNS Server
- XNetworking: Konfigurationsressource für den gewünschten Status im Zusammenhang mit dem Netzwerk.
- "XRemoteDesktopAdmin": Dieses Modul verwendet ein Repository, das die gewünschten Zustandskonfigurationsressourcen enthält, um Remote-Desktop-Einstellungen und Windows-Firewall auf einem lokalen oder entfernten Rechner zu konfigurieren.
- XRemoteDesktopSessionHost: Konfigurationsressource für den gewünschten Zustand (xRDSessionDeployment, xRDSessionCollection, xRDSessionCollectionConfiguration und xRDRemoteApp) ermöglicht die Erstellung und Konfiguration einer RDSH-Instanz (Remote Desktop Session Host)
- XSmbShare: Konfigurationsressource für den gewünschten Status für die Konfiguration und das Management einer SMB-Freigabe

- XSystemSecurity: Konfigurationsressource für den gewünschten Zustand zur Verwaltung von UAC und IE Esc



Azure Virtual Desktop installiert auch Azure Komponenten, darunter Enterprise Applications und App-Registrierungen für Azure Virtual Desktop und Azure Virtual Desktop Client, der AVD-Mandant, AVD Host Pools, AVD App Groups und AVD Registered Virtual Machines. Während VDS Automation Components diese Komponenten verwalten, steuert AVD die Standardkonfiguration und den Attributsatz. Weitere Informationen finden Sie in der AVD-Dokumentation.

Hybrid-AD-Komponenten

Um die Integration in vorhandenes AD vor Ort oder in der Public Cloud zu erleichtern, sind zusätzliche Komponenten und Berechtigungen in der vorhandenen AD-Umgebung erforderlich.

Domain Controller

Der vorhandene Domänen-Controller kann über AD Connect und/oder einem Site-to-Site-VPN (oder Azure ExpressRoute) in eine AVD-Implementierung integriert werden.

AD-Connect

Um eine erfolgreiche Benutzerauthentifizierung über die AVD-PaaS-Dienste zu erleichtern, kann AD Connect verwendet werden, um den Domänencontroller mit Azure AD zu synchronisieren.

Sicherheitsgruppe

VDS verwendet eine Active Directory-Sicherheitsgruppe CW-Infrastruktur, um die erforderlichen Berechtigungen für die Automatisierung der Active Directory-abhängigen Aufgaben wie Domain-Beitritt und GPO-Richtlinienanhang zu enthalten.

Service-Konto

VDS verwendet ein Active Directory-Dienstkonto namens CloudWorkspaceSVC, das als Identität für die VDS-Windows-Dienste und den IIS-Anwendungsdienst verwendet wird. Dieses Konto ist nicht interaktiv (erlaubt keine RDP-Anmeldung) und ist das primäre Mitglied des CW-Infrastruktur-Kontos

VPN oder ExpressRoute

Ein Site-to-Site-VPN oder Azure ExpressRoute kann verwendet werden, um Azure VMs direkt mit der vorhandenen Domäne zu verbinden. Dies ist eine optionale Konfiguration, die verfügbar ist, wenn die Projektanforderungen dies vorschreiben.

Lokale AD-Berechtigungsdelegation

NetApp stellt ein optionales Tool zur Optimierung des Hybrid AD-Prozesses bereit. Bei Verwendung des optionalen NetApp Tools müssen folgende Aufgaben ausgeführt werden:

- Führen Sie die Ausführung auf einem Server-Betriebssystem statt auf einem Workstation-Betriebssystem aus
- Führen Sie einen Server aus, der mit der Domäne verbunden ist oder ein Domänencontroller ist
- Setzen Sie PowerShell 5.0 oder höher auf dem Server, auf dem das Tool ausgeführt wird (falls nicht auf dem Domain Controller ausgeführt wird) und dem Domain Controller ein

- Sie können von einem Benutzer mit Domänenadministratorrechten ausgeführt WERDEN ODER von einem Benutzer mit lokalen Administratorberechtigungen ausgeführt werden und eine Domänenadministratorberechtigung (zur Verwendung mit RunAs) bereitstellen.

Ob manuell erstellt oder durch das Tool von NetApp angewendet wird, sind die erforderlichen Berechtigungen:

- CW-Infrastrukturgruppe
 - Die Sicherheitsgruppe Cloud Workspace-Infrastruktur (**CW-Infrastruktur**) erhält volle Kontrolle auf der OU-Ebene des Cloud Workspace und allen abwärts befindlichen Objekten
 - <Bereitstellungscode>.cloudWorkspace.App DNS Zone – CW-Infrastrukturgruppe gewährt CreateChild, DeleteChild, ListChildren, ReadProperty, DeleteTree, ExtendedRight, Delete, GenericWrite
 - DNS-Server – CW-Infrastrukturgruppe gewährt ReadProperty, GenericExecute
 - Lokaler Administratorzugriff für erstellte VMs (CWMGR1, AVD-Session-VMs) (erfolgt nach Gruppenrichtlinie auf den gemanagten AVD-Systemen)
- CW-CWMGRAccess Group Diese Gruppe bietet lokale Administratorrechte für CWMGR1 auf allen Vorlagen, der einzelne Server, die neue native Active Directory-Vorlage verwendet die integrierten Gruppen Server-Operatoren Remote Desktop-Benutzer und Netzwerk-Konfigurationsoperatoren.

AVD-Umgebungskomponenten und -Berechtigungen

Sobald der Automatisierungsprozess für die Bereitstellung abgeschlossen ist, sind die fortlaufende Nutzung und Verwaltung von Bereitstellungen und Workspaces eine Reihe von Komponenten und Berechtigungen erforderlich, wie unten definiert. Viele der Komponenten und Berechtigungen von oben bleiben relevant, aber dieser Abschnitt konzentriert sich auf die Definition der Struktur eines implementierten.

Die Komponenten von VDS-Implementierungen und Workspaces lassen sich in verschiedene logische Kategorien einteilen:

- Endbenutzer-Clients
- VDS-Komponenten der Steuerebene
- Komponenten von Microsoft Azure AVD-PaaS
- KOMPONENTEN DER VDS-Plattform
- VDS Workspace-Komponenten in Azure Tenant
- Hybrid-AD-Komponenten

Endbenutzer-Clients

Benutzer können eine Verbindung zu ihrem AVD-Desktop und/oder über verschiedene Endpunkttypen herstellen. Microsoft hat Client-Anwendungen für Windows, macOS, Android und iOS veröffentlicht. Darüber hinaus steht ein Web-Client für Client-freien Zugriff zur Verfügung.

Es gibt einige Linux-Thin-Client-Anbieter, die Endpunktclient für AVD veröffentlicht haben. Diese sind unter aufgeführt <https://docs.microsoft.com/en-us/azure/virtual-desktop/linux-overview>

VDS-Komponenten der Steuerebene

VDS REST-API

VDS ist auf vollständig dokumentierten REST-APIs aufgebaut, so dass alle Aktionen in der Web-App sind auch

über die API verfügbar. Dokumentation für die API ist hier:
<https://api.cloudworkspace.com/5.4/swagger/ui/index#>

VDS Web-App

VDS-Administratoren können die ADS-Anwendung über die VDS-Web-App interagieren. Dieses Web-Portal befindet sich unter: <https://manage.cloudworkspace.com>

Datenbank der Kontrollebene

VDS-Daten und -Einstellungen werden in der SQL-Datenbank der Kontrollebene gespeichert, die von NetApp gehostet und gemanagt wird.

VDS-Kommunikation

Komponenten der Azure-Mandanten

DIE AUTOMATISIERUNG DER VDS-Implementierung erstellt eine einzelne Azure-Ressourcengruppe, die die anderen AVD-Komponenten einschließlich VMs, Netzwerknetzen, Netzwerksicherheitsgruppen und entweder Azure Files-Container oder Azure NetApp Files-Kapazitätspools enthält. Hinweis – standardmäßig ist eine einzelne Ressourcengruppe, aber VDS bietet Tools, um Ressourcen in weiteren Ressourcengruppen zu erstellen, falls gewünscht.

Komponenten von Microsoft Azure AVD-PaaS

AVD REST-API

Microsoft AVD kann über API verwaltet werden. VDS nutzt diese APIs ausführlich zur Automatisierung und zum Management von AVD-Umgebungen. Die Dokumentation befindet sich unter: <https://docs.microsoft.com/en-us/rest/api/desktopvirtualization/>

Session-Broker

Der Broker bestimmt die für den Benutzer autorisierten Ressourcen und orchestriert die Verbindung des Benutzers zum Gateway.

Azure Diagnose

Azure Diagnostics wurde speziell zur Unterstützung von AVD-Implementierungen entwickelt.

AVD-Webclient

Microsoft hat einen Web-Client bereitgestellt, über den Benutzer eine Verbindung zu ihren AVD-Ressourcen ohne lokal installierten Client herstellen können.

Session-Gateway

Der lokal installierte RD-Client stellt eine Verbindung zum Gateway her, um sicher mit der AVD-Umgebung zu kommunizieren.

KOMPONENTEN DER VDS-Plattform

CKWMGR1

CMWGR1 ist die VDS-Kontroll-VM für jede Implementierung. Standardmäßig wird es als Windows 2019 Server VM im Azure-Zielabonnement erstellt. Im Abschnitt Lokale Bereitstellung finden Sie eine Liste der auf CWMGR1 installierten VDS- und Drittanbieterkomponenten.

Für AVD müssen die AVD-VMs einer Active Directory-Domäne hinzugefügt werden. Um diesen Prozess zu vereinfachen und Automatisierungstools für das Management der VDS-Umgebung bereitzustellen, werden mehrere Komponenten auf der oben beschriebenen CWMGR1-VM installiert und der AD-Instanz mehrere Komponenten hinzugefügt. Zu den Komponenten gehören:

- **Windows Services** - VDS verwendet Windows-Dienste zur Durchführung von Automatisierungs- und Management-Aktionen innerhalb einer Bereitstellung:
 - **CW Automation Service** ist ein Windows-Dienst, der auf CWMGR1 in jeder AVD-Bereitstellung bereitgestellt wird und viele der benutzerbezogenen Automatisierungsaufgaben in der Umgebung ausführt. Dieser Dienst wird unter dem Konto **CloudWorkspaceSVC** AD ausgeführt.
 - **CW VM Automation Service** ist ein Windows-Dienst, der auf CWMGR1 in jeder AVD-Bereitstellung bereitgestellt wird und die Verwaltungsfunktionen der virtuellen Maschine ausführt. Dieser Dienst wird unter dem Konto **CloudWorkspaceSVC** AD ausgeführt.
 - **CW Agent Service** ist ein Windows-Dienst, der auf jeder virtuellen Maschine unter VDS-Verwaltung bereitgestellt wird, einschließlich CWMGR1. Dieser Dienst läuft unter dem **LocalSystem** Kontext auf der virtuellen Maschine.
 - **CWManagerX API** ist ein IIS-App-Pool-basierter Listener, der in jeder AVD-Bereitstellung auf CWMGR1 installiert ist. Damit werden eingehende Anfragen von der globalen Kontrollebene verarbeitet und unter dem Konto **CloudWorkspaceSVC** AD ausgeführt.
- **SQL Server 2017 Express** – VDS erstellt eine SQL Server Express-Instanz auf der CWMGR1 VM zur Verwaltung der Metadaten, die von den Automatisierungskomponenten generiert werden.
- **Internet Information Services (IIS)** – IIS ist auf CWMGR1 aktiviert, um die IIS-Anwendung CWManagerX und CWApps zu hosten (nur wenn die RDS RemoteApp-Funktionalität aktiviert ist). VDS erfordert IIS Version 7.5 oder höher.
- **HTML5 Portal (optional)** – VDS installiert den Spark Gateway-Dienst, um HTML5-Zugriff auf die VMs in der Bereitstellung und von der VDS-Webanwendung zu ermöglichen. Dies ist eine Java-basierte Anwendung und kann deaktiviert und entfernt werden, wenn diese Zugriffsmethode nicht gewünscht ist.
- **RD Gateway (optional)** – VDS ermöglicht es der RD Gateway-Rolle auf CWMGR1, RDP-Zugriff auf RDS Collection-basierte Ressourcen-Pools zu bieten. Diese Rolle kann deaktiviert/deinstalliert werden, wenn nur AVD Reverse Connect-Zugriff gewünscht wird.
- **RD Web (optional)** – VDS aktiviert die RD-Webrolle und erstellt die CWApps IIS-Webanwendung. Diese Rolle kann deaktiviert werden, wenn nur AVD-Zugriff gewünscht wird.
- **DC Config** – eine Windows-Anwendung, die zur Durchführung von Deployment- und VDS-Site-spezifischen Konfigurationsaufgaben und erweiterten Konfigurationsaufgaben verwendet wird.
- **Test VDC Tools** – eine Windows-Anwendung, die die direkte Aufgabenausführung für Konfigurationsänderungen auf Virtual Machine- und Client-Ebene unterstützt, die in seltenen Fällen verwendet werden, in denen API- oder Web-Anwendungen für Fehlerbehebungs Zwecke geändert werden müssen.
- **Let's Verschlüsselte Wildcard-Zertifikat (optional)** – erstellt und verwaltet durch VDS – alle VMs, die HTTPS-Datenverkehr über TLS erfordern, werden mit dem Zertifikat nachts aktualisiert. Die Erneuerung erfolgt ebenfalls automatisch (die Zertifikate sind 90 Tage lang so dass die Erneuerung kurz zuvor beginnt). Auf Wunsch kann der Kunde ein eigenes Wildcard-Zertifikat vorlegen. VDS benötigt außerdem mehrere Active Directory-Komponenten zur Unterstützung der Automatisierungsaufgaben. Ziel des Designs ist es,

eine Mindestanzahl von AD-Komponenten und Berechtigungen zu verwenden und gleichzeitig die Umgebung für automatisiertes Management zu unterstützen. Beispielsweise:

- **Cloud Workspace Organisationseinheit (OU)** – Diese Organisationseinheit fungiert als primärer AD-Container für die erforderlichen untergeordneten Komponenten. Berechtigungen für die CW-Infrastruktur- und Client-DHP-Zugriffsgruppen werden auf dieser Ebene und ihren untergeordneten Komponenten festgelegt. In Anhang A finden Sie Untereinheiten, die in dieser Organisationseinheit erstellt wurden.
- **Cloud Workspace Infrastructure Group (CW-Infrastruktur)** ist eine im lokalen AD erstellte Sicherheitsgruppe, die die Zuweisung der erforderlichen delegierten Berechtigungen zum VDS-Dienstkonto (**CloudWorkspaceSVC**) ermöglicht.
- **Client DHP Access Group (ClientDHPAccess)** ist eine Sicherheitsgruppe, die im lokalen AD erstellt wurde, um VDS zu ermöglichen, den Speicherort zu bestimmen, an dem sich die gemeinsam genutzten Unternehmens-, Benutzer- und Profildaten befinden.
- **CloudWorkspaceSVC**-Servicekonto (Mitglied der Cloud Workspace Infrastructure Group)
- **DNS-Zone für <Bereitstellungscode>.cloudWorkspace.App-Domäne** (diese Domäne verwaltet die automatisch erstellten DNS-Namen für Session-Host-VMs) – erstellt durch Bereitstellungsconfiguration.
- *NetApp spezifische Gruppenrichtlinienobjekte, die mit verschiedenen untergeordneten Organisationseinheiten des Cloud Workspace verbunden sind. Die Gruppenrichtlinienobjekte:
 - **Cloud Workspace GPO (verknüpft mit Cloud Workspace OU)** – definiert Zugriffsprotokolle und -Methoden für Mitglieder der CW-Infrastruktur Group. Fügt die Gruppe auch der lokalen Administratorgruppe auf AVD-Sitzungshosts hinzu.
 - **Cloud Workspace Firewall GPO** (verknüpft mit dedizierten Kunden-Servern, Remote Desktop und Staging OUs) - erstellt eine Richtlinie, die Verbindungen zu Sitzungshosts von Plattform-Servern sicherstellt und isoliert.
 - **Cloud Workspace RDS** (dedizierte Kunden Server, Remote Desktop und Staging OUs) - Policy Set Limits für Sitzungsqualität, Zuverlässigkeit, Timeout-Limits. Für RDS-Sitzungen wird der Wert des TS Licensing-Servers definiert.
 - **Cloud Workspace Companies** (NICHT standardmäßig VERKNÜPFT) – optionales GPO zur „Sperrung“ einer Benutzersitzung/-Arbeitsumgebung durch Verhinderung des Zugriffs auf administrative Tools und Bereiche. Kann verknüpft/aktiviert werden, um einen Arbeitsbereich mit eingeschränkten Aktivitäten bereitzustellen.



Die Standardkonfigurationen für die Gruppenrichtlinieneinstellung können auf Anfrage bereitgestellt werden.

VDS Workspace-Komponenten

Datenebene

Azure NetApp Dateien

Ein Azure NetApp Files-Kapazitätspool und zugehörige Volumes werden erstellt, wenn Sie Azure NetApp Files im VDS-Setup die Option „Datenebene“ als Option „Datenebene“ auswählen. Das Volume hostet den gemeinsam genutzten, abgestellten Speicher für Benutzerprofile (über FSLogix Container), Benutzerpersönliche Ordner und den Ordner für die gemeinsame Nutzung von Unternehmensdaten.

Azure Files

Wenn Sie im CWS-Setup Azure Files als Data Layer-Option auswählen, wird eine Azure-Dateifreigabe und das zugehörige Azure-Speicherkonto erstellt. Der Azure File Share hostet den gemeinsam genutzten, abgestellten

Speicher für Benutzerprofile (über FSLogix Container), persönliche Anwenderordner und den Ordner für die gemeinsame Nutzung von Unternehmensdaten.

File Server mit Managed Disk

Eine Windows Server-VM wird mit einer verwalteten Festplatte erstellt, wenn Sie im VDS-Setup den Datei-Server als Datenebene-Option wählen. Der File Server hostet den gemeinsam genutzten, abgestellten Speicher für Benutzerprofile (über FSLogix Container), Benutzerpersönliche Ordner und den Ordner für die gemeinsame Nutzung von Unternehmensdaten.

Azure Networking

Virtuelles Azure Netzwerk

VDS erstellt ein Azure Virtual Network und unterstützt Subnetze. VDS erfordert ein separates Subnetz für CWMGR1, AVD Host Machines und Azure Domain Controller und Peering zwischen den Subnetzen. Beachten Sie, dass das AD-Controller-Subnetz normalerweise bereits vorhanden ist, sodass die implementierten VDS-Subnetze mit dem vorhandenen Subnetz Peering erforderlich sind.

Netzwerksicherheitsgruppen

Eine Netzwerksicherheitsgruppe wird erstellt, um den Zugriff auf die CWMGR1-VM zu steuern.

- Mandant: Enthält IP-Adressen, die nach Session-Host und Daten-VMs verwendet werden können
- Services: Enthält IP-Adressen zur Nutzung durch PaaS-Dienste (z. B. Azure NetApp Files)
- Plattform: Enthält IP-Adressen zur Verwendung als NetApp Plattform-VMs (CWMGR1 und alle Gateway-Server)
- Verzeichnis: Enthält IP-Adressen zur Verwendung als Active Directory-VMs

Azure AD

Mit der VDS-Automatisierung und -Orchestrierung werden Virtual Machines in eine Zielinstanz Active Directory implementiert und anschließend die Maschinen dem zugewiesenen Host-Pool hinzugefügt. AVD Virtual Machines werden auf Computerebene sowohl durch die AD-Struktur (Organisationseinheiten, Gruppenrichtlinien, lokale Computeradministratorberechtigungen usw.) als auch durch die Mitgliedschaft in der AVD-Struktur (Hostpools, Mitgliedschaft in Workspace-App-Gruppen) gesteuert, die von Azure AD-Einheiten und -Berechtigungen gesteuert werden. VDS verarbeitet diese „Dual-Control“-Umgebung mit der VDS Enterprise-Anwendung/Azure Service Principal für AVD-Aktionen und dem lokalen AD-Servicekonto (CloudWorkspaceSVC) für lokale AD- und lokale Computeraktionen.

Die spezifischen Schritte zum Erstellen einer virtuellen AVD-Maschine und zum Hinzufügen eines AVD-Hostpools umfassen:

- Erstellen einer Virtual Machine aus Azure-Vorlage, die für das mit AVD verknüpfte Azure-Abonnement sichtbar ist (nutzt Azure Service Principal Berechtigungen)
- Die DNS-Adresse für neue Virtual Machine prüfen/konfigurieren, indem das während der VDS-Bereitstellung festgelegte Azure vnet verwendet wird (erfordert lokale AD-Berechtigungen (alle Aufgaben sind oben an CW-Infrastruktur delegiert), legt den Namen der Virtual Machine mithilfe des Standard-VDS-Benennungsschemas **{companycode}TS{Sequenznummer}** fest. Beispiel: XYZTS3. (Erfordert lokale AD-Berechtigungen (platziert in der Organisationsstruktur, die wir On-Prem erstellt haben (Remote-Desktop/unternehmenscode/shared) (gleiche Berechtigung/Gruppenbeschreibung wie oben)
- Platziert virtuelle Maschine in einer festgelegten Active Directory-Organisationseinheit (AD) (erfordert die

delegierten Berechtigungen an die Organisationsstruktur der Organisationseinheit (festgelegt während des manuellen Prozesses oben)

- Internes AD-DNS-Verzeichnis mit dem neuen Gerätenamen/-IP-Adresse aktualisieren (erfordert lokale AD-Berechtigungen)
- Werden Sie einer neuen Virtual Machine mit der lokalen AD-Domäne beitreten (erfordert lokale AD-Berechtigungen)
- Lokale VDS-Datenbank mit neuen Serverinformationen aktualisieren (keine zusätzlichen Berechtigungen erforderlich)
- Verbinden Sie die VM mit dem designierten AVD Host Pool (AVD Service Principal Berechtigungen erforderlich)
- Installieren von chocolatey-Komponenten auf der neuen virtuellen Maschine (erfordert lokales Administratorrecht für den Computer für das Konto **CloudWorkspaceSVC**)
- Installieren von FSLogix-Komponenten für die AVD-Instanz (erfordert lokale Computer-Administratorberechtigungen auf der AVD-OU im lokalen AD)
- Aktualisieren Sie das Gruppenrichtlinienobjekt der AD Windows Firewall, um den Datenverkehr zur neuen VM zu ermöglichen (erfordert die Erstellung/Änderung von AD-Gruppenrichtlinienobjekt für Richtlinien der AVD-Organisationseinheit und der zugehörigen Virtual Machines. Erfordert die Erstellung/Änderung der AD-Gruppenrichtlinienrichtlinie auf der AVD-Organisationseinheit im lokalen AD. Kann nach der Installation deaktiviert werden, wenn keine VMs über VDS verwaltet werden.)
- Flag „Neue Verbindungen zulassen“ auf der neuen virtuellen Maschine setzen (erfordert Azure Service Principal Berechtigungen)

Verbindung von VMs mit Azure AD

Virtual Machines im Azure-Mandanten müssen der Domäne hinzugefügt werden, allerdings können keine VMs direkt mit Azure AD verbunden werden. Daher implementiert VDS die Domänen-Controller-Rolle in der VDS-Plattform. Anschließend synchronisieren wir dieses DC mit Azure AD mithilfe von AD Connect. Zu den alternativen Konfigurationsoptionen gehören z. B. Azure AD Domain Services (AADDS), die Synchronisierung mit einem hybriden DC (eine lokale oder andere VM) über AD Connect oder das direkte Verbinden der VMs mit einem hybriden Datacenter über ein Site-to-Site-VPN oder Azure ExpressRoute.

AVD-Host-Pools

Host-Pools sind eine Sammlung aus einer oder mehreren identischen Virtual Machines (VMs) in Azure Virtual Desktop-Umgebungen. Jeder Host-Pool kann eine Applikationsgruppe enthalten, mit der Benutzer wie auf einem physischen Desktop interagieren können.

Session-Hosts

Innerhalb eines Host-Pools finden sich eine oder mehrere identische Virtual Machines. Diese Benutzersitzungen, die mit diesem Hostpool verbunden sind, werden durch den AVD-Load-Balancer-Service ausgeglichen.

Applikationsgruppen

Standardmäßig wird die App-Gruppe *Desktop Users* bei der Bereitstellung erstellt. Alle Benutzer innerhalb dieser App-Gruppe werden mit einem vollständigen Windows-Desktop-Erlebnis präsentiert. Außerdem können Applikationsgruppen erstellt werden, um Streaming-App-Services zu bedienen.

Arbeitsbereich Protokollanalyse

Ein Arbeitsbereich Log Analytics wird erstellt, um Protokolle aus den Bereitstellungs- und DSC-Prozessen sowie anderen Services zu speichern. Dies kann nach der Bereitstellung gelöscht werden, aber dies wird nicht empfohlen, da es andere Funktionalität ermöglicht. Protokolle werden standardmäßig 30 Tage aufbewahrt und für die Aufbewahrung fallen keine Kosten an.

Verfügbarkeitsgruppen

Ein Verfügbarkeitsset wird als Teil des Implementierungsprozesses eingerichtet, um gemeinsam genutzte VMs (gemeinsam genutzte AVD-Host-Pools, RDS-Ressourcen-Pools) über Fehlerdomänen hinweg zu trennen. Dies kann nach der Implementierung gelöscht werden, allerdings deaktiviert diese Option, um eine zusätzliche Fehlertoleranz für gemeinsam genutzte VMs bereitzustellen.

Azure Recovery Vault

Während der Implementierung wird von VDS Automation ein Recovery Service Vault erstellt. Dies ist derzeit standardmäßig aktiviert, da Azure Backup während des Bereitstellungsprozesses auf CWMGR1 angewendet wird. Dieser kann bei Bedarf deaktiviert und entfernt werden, wird aber bei aktiviertem Azure Backup in der Umgebung neu erstellt.

Azure Schlüsselspeicher

Während des Implementierungsprozesses wird ein Azure Key Vault erstellt und zur Speicherung von Zertifikaten, API-Schlüsseln und Anmeldeinformationen verwendet, die von Azure Automation Accounts bei der Implementierung verwendet werden.

Anhang A – Standardstruktur der Organisationseinheit des Cloud Workspace

- Cloud Workspace
 - Cloud Workspace-Unternehmen
 - Cloud Workspace Server
 - Dedizierte Kundenserver
 - Infrastruktur
- CWMGR Server
- Gateway Server
- FTP-Server
- VM-Vorlage
 - Remote Desktop
 - Staging
 - Cloud Workspace Servicekonten
 - Client-Servicekonten
 - Infrastructure Service Accounts
 - Tech-Benutzer Von Cloud Workspace
 - Gruppen
 - Techniker Von Tech 3

Voraussetzungen für AVD und VDS v5.4

AVD- und VDS-Anforderungen und Hinweise

In diesem Dokument werden die erforderlichen Elemente zur Implementierung von Azure Virtual Desktop (AVD) mithilfe von NetApp Virtual Desktop Service (VDS) beschrieben. Die „Quick Checklist“ enthält eine kurze Liste der erforderlichen Komponenten und Schritte zur Vorabbereitstellung, um eine effiziente Bereitstellung zu gewährleisten. Der restliche Leitfaden bietet je nach getroffenen Konfigurationsauswahl detailliertere Informationen für jedes Element.

Schnelle Checkliste

Azure-Anforderungen

- Azure AD-Mandant
- Microsoft 365-Lizenzierung zur Unterstützung von AVD
- Azure Abonnement
- Verfügbare Azure Quote für virtuelle Azure-Maschinen
- Azure-Administratorkonto mit globalen Administratorrollen und Abonnementberechtigungen
- Domänenadministratorkonto mit der Rolle „Enterprise Admin“ für AD Connect Setup

Informationen vor der Implementierung

- Bestimmen Sie die Gesamtzahl der Benutzer
- Azure Region Bestimmen
- Bestimmen Sie Den Active Directory-Typ
- Storage-Typ Ermitteln
- Host-VM-Image oder -Anforderungen ermitteln
- Bewerten vorhandener Azure und On-Premises-Netzwerkconfiguration

VDS-Bereitstellung – Detaillierte Anforderungen

Verbindungsanforderungen für Endbenutzer

Die folgenden Remote Desktop-Clients unterstützen Azure Virtual Desktop:

- Windows Desktop
- Web
- MacOS
- IOS
- IGEL Think Client (Linux)
- Android (Vorschau)



Azure Virtual Desktop unterstützt den Remote App und Desktop Connections-Client (RADC) oder den MSTSC-Client (Remote Desktop Connection) nicht.



Azure Virtual Desktop unterstützt derzeit den Remote Desktop-Client aus dem Windows Store nicht. Unterstützung für diesen Client wird in einem zukünftigen Release hinzugefügt.

Die Remote Desktop Clients müssen Zugriff auf die folgenden URLs haben:

Adresse	Ausgehender TCP-Port	Zweck	Client(e)
*.AVD.microsoft.com	443	Dienstverkehr	Alle
*.servicebus.windows.net 443 Fehlerbehebungsdaten	Alle	go.microsoft.com	443
Microsoft FWLinks	Alle	Aka.ms	443
Microsoft URL-Shortener	Alle	docs.microsoft.com	443
Dokumentation	Alle	privacy.microsoft.com	443
Datenschutzerklärung	Alle	query.prod.cms.rt.microsoft.com	443



Das Öffnen dieser URLs ist für ein zuverlässiges Client-Erlebnis unerlässlich. Das Blockieren des Zugriffs auf diese URLs wird nicht unterstützt und wirkt sich auf die Servicefunktionalität aus. Diese URLs entsprechen nur den Client-Sites und -Ressourcen und enthalten keine URLs für andere Dienste wie Azure Active Directory.

Startpunkt DES VDS-Setup-Assistenten

Der VDS-Setup-Assistent kann einen Großteil der erforderlichen Voraussetzungen für eine erfolgreiche AVD-Bereitstellung verarbeiten. Der Setup-Assistent ("") Erzeugt oder verwendet die folgenden Komponenten.

Azure-Mandant

Erforderlich: ein Azure-Mandant und Azure Active Directory

Die AVD-Aktivierung in Azure ist eine mandantenfähige Einstellung. VDS unterstützt die Ausführung einer AVD-Instanz pro Mandant.

Azure-Abonnement

Erforderlich: ein Azure Abonnement (beachten Sie die Abonnement-ID, die Sie verwenden möchten)

Alle bereitgestellten Azure Ressourcen sollten in einem dedizierten Abonnement eingerichtet werden. Das erleichtert die Kostenverfolgung für AVD und vereinfacht den Bereitstellungsprozess. HINWEIS: Kostenlose Azure-Testversionen werden nicht unterstützt, da sie nicht über ausreichende Gutschriften für die Bereitstellung einer funktionsfähigen AVD-Implementierung verfügen.

Azure Kernkontingent

Genügend Quote für die VM-Familien, die Sie verwenden werden - insbesondere mindestens 10 Kerne der D v3-Familie für die anfängliche Plattform-Bereitstellung (so wenige wie 2 Kerne verwendet werden können, aber 10 deckt jede erste Möglichkeit der Bereitstellung).

Azure-Administratorkonto

Erforderlich: ein globales Azure-Administratorkonto.

Der VDS-Einrichtungsassistent fordert den Azure Admin an, dem VDS-Dienstprincipal delegierte Berechtigungen zu erteilen und die VDS Azure Enterprise-Applikation zu installieren. Der Administrator muss die folgenden Azure-Rollen zugewiesen haben:

- Globaler Administrator auf dem Mandanten
- Besitzerrolle im Abonnement

VM Image

Erforderlich: ein Azure-Image, das Multi-Session Windows 10 unterstützt.

Im Azure Marketplace finden Sie die aktuellsten Versionen ihres Basis-Images unter Windows 10. Alle Azure-Abonnements können automatisch auf diese zugreifen. Wenn Sie ein anderes Bild oder ein benutzerdefiniertes Image verwenden möchten, soll das VDS-Team Ratschläge zum Erstellen oder Ändern anderer Bilder geben oder allgemeine Fragen zu Azure-Bildern mit uns teilen und wir können ein Gespräch vereinbaren.

Active Directory

Für AVD muss die Benutzeridentität ein Bestandteil von Azure AD sein und die VMs zu einer Active Directory-Domäne gehören, die mit derselben Azure AD-Instanz synchronisiert wird. VMs können nicht direkt mit der Azure AD-Instanz verbunden werden, daher muss ein Domänen-Controller mit Azure AD konfiguriert und synchronisiert werden.

Folgende unterstützte Optionen werden unterstützt:

- Der automatisierte Aufbau einer Active Directory-Instanz innerhalb des Abonnements. Die AD-Instanz wird typischerweise durch VDS auf der VDS Control VM (CWMGR1) für Azure Virtual Desktop-Implementierungen erstellt, die diese Option verwenden. AD Connect muss im Rahmen der Einrichtung für die Synchronisierung mit Azure AD konfiguriert sein.

□

- Integration in eine vorhandene Active Directory-Domäne, auf die über das Azure-Abonnement (normalerweise über Azure VPN oder Express Route) zugegriffen werden kann, und hat ihre Benutzerliste mit Azure AD über AD Connect oder ein Produkt eines Drittanbieters synchronisiert.

□

Storage-Ebene

Bei AVD ist die Storage-Strategie so ausgelegt, dass sich keine persistenten Benutzer-/Unternehmensdaten auf den AVD-Session-VMs befinden. Persistente Daten für Benutzerprofile, Benutzerdateien und Ordner sowie Unternehmens-/Applikationsdaten werden auf einem oder mehreren Daten-Volumes gehostet, die auf einer unabhängigen Datenebene gehostet werden.

FSLogix ist eine Technologie für Containerbildung und löst zahlreiche Probleme bei der Benutzerprofil (wie Datenwildwuchs und langsame Anmeldungen), indem ein User Profile Container (VHD oder VHDX Format) beim Initialisieren der Session-Hosts eingebunden wird.

Aufgrund dieser Architektur ist eine Datenspeicherfunktion erforderlich. Diese Funktion muss in der Lage sein, den Datentransfer jeden Morgen/Nachmittag zu verarbeiten, wenn ein großer Teil der Benutzer sich

gleichzeitig anmeldet/abmeldet. Selbst Umgebungen mittlerer Größe können erhebliche Anforderungen an den Datentransfer stellen. Die Festplatten-Performance der Daten-Storage-Ebene ist eine der primären Performance-Variablen für den Endbenutzer. Dabei muss besonders darauf Wert gelegt werden, die Performance dieses Storage angemessen zu dimensionieren, nicht nur die Storage-Menge. Im Allgemeinen sollte die Storage-Ebene so dimensioniert sein, dass sie 5-15 IOPS pro Benutzer unterstützt.

Der VDS Setup-Assistent unterstützt die folgenden Konfigurationen:

- Einrichtung und Konfiguration von Azure NetApp Files (ANF) (empfohlen). *ANF Standard Service Level unterstützt bis zu 150 Benutzer, Umgebungen mit 150-500 Benutzern ANF Premium wird empfohlen. Für 500+ Benutzer wird ANF Ultra empfohlen.*

□

- Einrichtung und Konfiguration einer File Server VM

□

Netzwerkbetrieb

Erforderlich: Inventarisierung aller vorhandenen Netzwerknetze einschließlich der Subnetze, die über eine Azure Express Route oder VPN zum Azure Abonnement sichtbar sind. Die Implementierung muss sich überschneidende Subnetze vermeiden.

Mit dem VDS-Setup-Assistenten können Sie den Netzwerkbereich definieren, falls im Rahmen der geplanten Integration in vorhandene Netzwerke ein Bereich erforderlich oder vermieden werden muss.

Bestimmen Sie während der Bereitstellung einen IP-Bereich für den Benutzer. Gemäß Azure Best Practices werden nur IP-Adressen in einem privaten Bereich unterstützt.

Zu den unterstützten Optionen gehören die folgenden Optionen, jedoch standardmäßig ein Bereich von /20:

- 192.168.0.0 bis 192.168.255.255
- 172.16.0.0 bis 172.31.255.255
- 10.0.0.0 bis 10.255.255.255

CKWMGR1

Einige der einzigartigen Funktionen von VDS, wie zum Beispiel die kostensparende Funktion für Workload Scheduling und Live Scaling, erfordern eine administrative Präsenz im Mandanten und im Abonnement. Daher wird eine administrative VM namens CWMGR1 im Rahmen der Automatisierung des VDS-Einrichtungsassistenten bereitgestellt. Neben VDS-Automatisierungsaufgaben enthält diese VM auch VDS-Konfigurationen in einer SQL Express-Datenbank, lokale Protokolldateien und ein erweitertes Konfigurationsprogramm mit dem Namen DCConfig.

Je nach Auswahl im VDS-Einrichtungsassistenten kann diese VM weitere Funktionen hosten, darunter:

- Ein RDS-Gateway (wird nur in RDS-Implementierungen verwendet)
- Ein HTML 5-Gateway (nur in RDS-Implementierungen verwendet)
- Ein RDS-Lizenzserver (wird nur in RDS-Implementierungen verwendet)
- Ein Domain-Controller (falls ausgewählt)

Entscheidungsbaum im Bereitstellungsassistenten

Im Rahmen der ersten Implementierung werden eine Reihe von Fragen beantwortet, um die Einstellungen für die neue Umgebung anzupassen. Im Folgenden finden Sie einen Überblick über die wichtigsten Entscheidungen, die getroffen werden sollen.

Azure Region

Legen Sie fest, welche Region oder Regionen Azure Ihre AVD Virtual Machines hosten wird. Beachten Sie, dass für Azure NetApp Files und bestimmte VM-Familien (z. B. VMs mit GPU-Unterstützung) eine definierte Support-Liste für Azure-Regionen vorhanden ist, während AVD in den meisten Regionen verfügbar ist.

- Dieser Link kann zur Identifizierung verwendet werden "[Produktverfügbarkeit von Azure nach Region](#)"

Typ Active Directory

Legen Sie fest, welchen Active Directory-Typ Sie verwenden möchten:

- Active Directory vor Ort vorhanden
- Siehe "[AVD VDS-Komponenten und -Berechtigungen](#)" Dokument, um die erforderlichen Berechtigungen und Komponenten in Azure und der lokalen Active Directory-Umgebung zu erläutern
- Neue auf Azure Abonnementbasis basierende Active Directory Instanz
- Azure Active Directory Domain Services

Datenspeicher

Legen Sie fest, wo die Daten für Benutzerprofile, einzelne Dateien und Unternehmensfreigaben platziert werden. Zur Auswahl stehen:

- Azure NetApp Dateien
- Azure Files
- Herkömmlicher Dateiserver (Azure VM mit Managed Disk)

NetApp VDS Implementierungsanforderungen für vorhandene Komponenten

NetApp VDS-Implementierung mit vorhandenen Active Directory Domain Controllern

Dieser Konfigurationstyp erweitert eine vorhandene Active Directory-Domäne, um die AVD-Instanz zu unterstützen. In diesem Fall implementiert VDS eine begrenzte Anzahl von Komponenten in der Domäne, um automatisierte Bereitstellungs- und Verwaltungsaufgaben für die AVD-Komponenten zu unterstützen.

Diese Konfiguration erfordert:

- Ein vorhandener Active Directory-Domänencontroller, auf den VMs auf dem Azure vnet zugreifen können, normalerweise über Azure VPN oder Express Route ODER über einen in Azure erstellten Domänen-Controller.
- Erweiterung der VDS-Komponenten und -Berechtigungen, die für das VDS-Management von AVD-Hostpools und Daten-Volumes erforderlich sind, wenn sie der Domäne hinzugefügt werden. Im AVD VDS-Handbuch für Komponenten und Berechtigungen werden die erforderlichen Komponenten und Berechtigungen definiert, und für den Bereitstellungsvorgang ist ein Domänenbenutzer mit Domänenberechtigungen erforderlich, um das Skript auszuführen, mit dem die erforderlichen Elemente erstellt werden.

- Beachten Sie, dass durch die VDS-Implementierung standardmäßig bei von VDS erstellten VMs ein vnet erstellt wird. Die vnet kann entweder mit vorhandenen Azure-Netzwerk-VNets Peered werden oder die CWMGR1-VM kann mit den erforderlichen vordefinierten Subnetzen in ein vorhandenes vnet verschoben werden.

Identifikationsdaten und Werkzeug zur Vorbereitung der Domäne

Administratoren müssen an einem bestimmten Punkt des Bereitstellungsprozesses eine Domänenadministratorberechtigung bereitstellen. Eine temporäre Domänenadministratorberechtigung kann später erstellt, verwendet und gelöscht werden (sobald der Bereitstellungsprozess abgeschlossen ist). Alternativ können Kunden, die Unterstützung beim Aufbau der Voraussetzungen benötigen, das Domain Preparation Tool nutzen.

NetApp VDS-Implementierung mit vorhandenem Filesystem

VDS erstellt Windows-Freigaben, mit denen über AVD-Session-VMs auf Benutzerprofile, persönliche Ordner und Unternehmensdaten zugegriffen werden kann. VDS implementiert standardmäßig entweder die File-Server- oder Azure NetApp File-Optionen, aber wenn Sie eine vorhandene Dateispeicherkomponente besitzen, kann VDS die Freigaben auf diese Komponente verweisen, sobald die VDS-Bereitstellung abgeschlossen ist.

Die Anforderungen für die Nutzung der vorhandenen Storage-Komponente und:

- Die Komponente muss SMB v3 unterstützen
- Die Komponente muss mit derselben Active Directory-Domäne wie die AVD-Sitzungshosts verbunden sein
- Die Komponente muss in der Lage sein, einen UNC-Pfad zur Verwendung in der VDS-Konfiguration zur Verfügung zu stellen – ein Pfad kann für alle drei Freigaben verwendet werden, oder es können separate Pfade für jedes dieser Freigaben festgelegt werden. Beachten Sie, dass VDS Berechtigungen auf Benutzerebene für diese Freigaben festlegen wird. Beachten Sie daher das VDS AVD Components and Permissions Dokument, um sicherzustellen, dass die entsprechenden Berechtigungen für die VDS Automation Services erteilt wurden.

NetApp VDS-Implementierung mit vorhandenen Azure AD Domain Services

Für diese Konfiguration ist ein Prozess erforderlich, um die Attribute der vorhandenen Azure Active Directory Domain Services-Instanz zu identifizieren. Wenden Sie sich an Ihren Account Manager, um eine Bereitstellung dieses Typs anzufordern. NetApp VDS-Implementierung mit vorhandener AVD-Implementierung bei diesem Konfigurationstyp wird vorausgesetzt, dass die erforderlichen Azure vnet-, Active Directory- und AVD-Komponenten bereits vorhanden sind. Die VDS-Implementierung erfolgt auf dieselbe Weise wie die Konfiguration „NetApp VDS Deployment with Existing AD“, fügt jedoch die folgenden Anforderungen hinzu:

- Rd-Eigentümerrolle für den AVD-Mandanten muss den VDS Enterprise Applications in Azure gewährt werden
- AVD Host Pool und AVD Host Pool VMs müssen über die VDS Import Funktion in der VDS Web App in VDS importiert werden Dieser Prozess sammelt die Metadaten der AVD-Host-Pools und der VM-Session und speichert sie in VDS, sodass diese Elemente vom VDS gemanagt werden können
- AVD-Benutzerdaten müssen mithilfe des CRA-Tools in den VDS-Benutzerabschnitt importiert werden. Dieser Prozess fügt Metadaten zu jedem Benutzer in die VDS-Steuerebene ein, sodass die AVD App Group-Mitgliedschaft und die Sitzungsinformationen über VDS verwaltet werden können

ANHANG A: VDS-Steuerebenen-URLs und IP-Adressen

VDS-Komponenten im Azure-Abonnement kommunizieren mit den globalen VDS-Komponenten der

Kontrollebene, wie der VDS-Webanwendung und den VDS-API-Endpunkten. Für den Zugriff müssen die folgenden Basis-URI-Adressen für den bidirektionalen Zugriff auf Port 443 sicher gestellt werden:

"" "" "" "" ""

Wenn Ihr Zutrittskontrollgerät nur eine sichere Liste nach IP-Adresse erstellen kann, sollte die folgende Liste der IP-Adressen geschützt werden. Beachten Sie, dass VDS den Azure Traffic Manager Service verwendet. Diese Liste kann sich daher im Laufe der Zeit ändern:

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.227 23.99.136.91
40.122.119.157 40.78.132.166 40.78.129.17 40.122.52.167 40.70.147.2 40.86.99.202 13.68.19.178
13.68.114.184 137.116.69.208 13.68.18.80 13.68.114.115 13.68.114.136 40.70.63.81 52.171.218.239
52.171.223.92 52.171.217.31 52.171.216.93 52.171.220.134 92.242.140.21

ANHANG B: Microsoft AVD-Anforderungen

Dieser Abschnitt zu den Microsoft AVD-Anforderungen enthält eine Zusammenfassung der AVD-Anforderungen von Microsoft. Vollständige und aktuelle AVD-Anforderungen finden Sie hier:

<https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements>

Host-Lizenzierung für Azure Virtual Desktop-Session

Azure Virtual Desktop unterstützt die folgenden Betriebssysteme. Stellen Sie also sicher, dass Sie über die entsprechenden Lizenzen für Ihre Benutzer verfügen, die auf dem Desktop und den Apps basieren, die Sie implementieren möchten:

BETRIEBSSYSTEM	Erforderliche Lizenz
Windows 10 Enterprise Multi-Session oder Windows 10 Enterprise	MICROSOFT 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5
Windows 7 Enterprise	MICROSOFT 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5
Windows Server 2012 R2, 2016, 2019	RDS Client Access License (CAL) mit Software Assurance

URL-Zugriff für AVD-Maschinen

Die virtuellen Azure-Maschinen, die Sie für Azure Virtual Desktop erstellen, müssen Zugriff auf die folgenden URLs haben:

Adresse	Ausgehender TCP-Port	Zweck	Service-Tag
*.AVD.microsoft.com	443	Dienstverkehr	Windows VirtualDesktop
mrsglobalsteus2prod.blob.core.windows.net	443	Agent- und SXS-Stack-Updates	AzureCloud
*.core.windows.net	443	Agent-Traffic	AzureCloud
*.servicebus.windows.net	443	Agent-Traffic	AzureCloud
prod.warmpath.msftcloudes.com	443	Agent-Traffic	AzureCloud

Adresse	Ausgehender TCP-Port	Zweck	Service-Tag
catalogartifact.azureedge.net	443	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Windows-Aktivierung	Internet
AVDportalstorageblob.blob.core.windows.net	443	Support im Azure-Portal	AzureCloud

In der folgenden Tabelle sind optionale URLs aufgeführt, auf die Ihre virtuellen Azure-Maschinen Zugriff haben:

Adresse	Ausgehender TCP-Port	Zweck	Service-Tag
*.microsoftonline.com	443	Authentifizierung bei MS Online Services	Keine
*.events.data.microsoft.com	443	Telemetrie-Service	Keine
www.msftconnecttest.com	443	Erkennt, ob das Betriebssystem mit dem Internet verbunden ist	Keine
*.prod.do.dsp.mp.microsoft.com	443	Windows Update	Keine
login.windows.net	443	Melden Sie sich bei MS Online Services, Office 365 an	Keine
*.sfx.ms	443	Updates für die OneDrive Client-Software	Keine
*.digicert.com	443	Überprüfung des Zertifikatsannulfs	Keine

Optimale Performance-Faktoren

Stellen Sie sicher, dass Ihr Netzwerk die folgenden Anforderungen erfüllt, um eine optimale Leistung zu erzielen:

- Die RTT-Latenz (Round Trip) vom Netzwerk des Clients in die Azure-Region, in der Host-Pools eingesetzt wurden, sollte weniger als 150 ms betragen.
- Der Netzwerkverkehr kann außerhalb der Grenzen von Ländern/Regionen fließen, wenn VMs, auf denen Desktops und Applikationen gehostet werden, eine Verbindung zum Management-Service herstellen.
- Um die Netzwerk-Performance zu optimieren, empfehlen wir, dass die VMs des Session-Hosts in derselben Azure-Region wie der Management-Service zusammenliegen.

Unterstützte BS-Images für Virtual Machines

Azure Virtual Desktop unterstützt die folgenden x64-Betriebssystem-Images:

- Windows 10 Enterprise Multi-Session, Version 1809 oder höher
- Windows 10 Enterprise, Version 1809 oder höher

- Windows 7 Enterprise
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure Virtual Desktop unterstützt keine Images des Betriebssystems x86 (32 Bit), Windows 10 Enterprise N oder Windows 10 Enterprise KN. Aufgrund der Sektorgröße unterstützt Windows 7 zudem keine VHD- oder VHDX-basierten Profillösungen, die auf Managed Azure Storage gehostet werden.

Die verfügbaren Automatisierungs- und Implementierungsoptionen hängen davon ab, welches Betriebssystem und welche Version Sie wählen. Die in der folgenden Tabelle aufgeführten Angaben werden gezeigt:

Betriebssystem	Azure Image-Galerie	Manuelle VM-Implementierung	INTEGRATION VON ARM-Vorlagen	Bereitstellen von Host-Pools auf Azure Marketplace
Windows 10 Multisession, Version 1903	Ja.	Ja.	Ja.	Ja.
Windows 10 Multisession, Version 1809	Ja.	Ja.	Nein	Nein
Windows 10 Enterprise, Version 1903	Ja.	Ja.	Ja.	Ja.
Windows 10 Enterprise, Version 1809	Ja.	Ja.	Nein	Nein
Windows 7 Enterprise	Ja.	Ja.	Nein	Nein
Windows Server 2019	Ja.	Ja.	Nein	Nein
Windows Server 2016	Ja.	Ja.	Ja.	Ja.
Windows Server 2012 R2	Ja.	Ja.	Nein	Nein

Voraussetzungen für AVD und VDS v6.0

AVD- und VDS-Anforderungen und Hinweise

In diesem Dokument werden die erforderlichen Elemente zur Implementierung von Azure Virtual Desktop (AVD) mithilfe von NetApp Virtual Desktop Service (VDS) beschrieben. Die „Quick Checklist“ enthält eine kurze Liste der erforderlichen Komponenten und Schritte zur Vorabbereitstellung, um eine effiziente Bereitstellung zu gewährleisten. Der restliche Leitfaden bietet je nach getroffenen Konfigurationsauswahl detailliertere Informationen für jedes Element.

Schnelle Checkliste

Azure-Anforderungen

- Azure AD-Mandant
- Microsoft 365-Lizenzierung zur Unterstützung von AVD
- Azure Abonnement
- Verfügbare Azure Quote für virtuelle Azure-Maschinen
- Azure-Administratorkonto mit globalen Administratorrollen und Abonnementberechtigungen

- Domänenadministratorkonto mit der Rolle „Enterprise Admin“ für AD Connect Setup

Informationen vor der Implementierung

- Bestimmen Sie die Gesamtzahl der Benutzer
- Azure Region Bestimmen
- Bestimmen Sie Den Active Directory-Typ
- Storage-Typ Ermitteln
- Host-VM-Image oder -Anforderungen ermitteln
- Bewerten vorhandener Azure und On-Premises-Netzwerkconfiguration

VDS-Bereitstellung – Detaillierte Anforderungen

Verbindungsanforderungen für Endbenutzer

Die folgenden Remote Desktop-Clients unterstützen Azure Virtual Desktop:

- Windows Desktop
- Web
- MacOS
- IOS
- IGEL Think Client (Linux)
- Android (Vorschau)



Azure Virtual Desktop unterstützt den Remote App und Desktop Connections-Client (RADC) oder den MSTSC-Client (Remote Desktop Connection) nicht.



Azure Virtual Desktop unterstützt derzeit den Remote Desktop-Client aus dem Windows Store nicht. Unterstützung für diesen Client wird in einem zukünftigen Release hinzugefügt.

Die Remote Desktop Clients müssen Zugriff auf die folgenden URLs haben:

Adresse	Ausgehender TCP-Port	Zweck	Client(e)
*.wvd.microsoft.com	443	Dienstverkehr	Alle
*.servicebus.windows.net	443	Fehlerbehebungsdaten	Alle
go.microsoft.com	443	Microsoft FWLinks	Alle
Aka.ms	443	Microsoft URL-Shortener	Alle
docs.microsoft.com	443	Dokumentation	Alle
privacy.microsoft.com	443	Datenschutzerklärung	Alle
query.prod.cms.rt.microsoft.com	443	Client-Updates	Windows Desktop



Das Öffnen dieser URLs ist für ein zuverlässiges Client-Erlebnis unerlässlich. Das Blockieren des Zugriffs auf diese URLs wird nicht unterstützt und wirkt sich auf die Servicefunktionalität aus. Diese URLs entsprechen nur den Client-Sites und -Ressourcen und enthalten keine URLs für andere Dienste wie Azure Active Directory.

Startpunkt DES VDS-Setup-Assistenten

Der VDS-Setup-Assistent kann einen Großteil der erforderlichen Voraussetzungen für eine erfolgreiche AVD-Bereitstellung verarbeiten. Der Setup-Assistent ("") Erzeugt oder verwendet die folgenden Komponenten.

Azure-Mandant

Erforderlich: ein Azure-Mandant und Azure Active Directory

Die AVD-Aktivierung in Azure ist eine mandantenfähige Einstellung. VDS unterstützt die Ausführung einer AVD-Instanz pro Mandant.

Azure-Abonnement

Erforderlich: ein Azure Abonnement (beachten Sie die Abonnement-ID, die Sie verwenden möchten)

Alle bereitgestellten Azure Ressourcen sollten in einem dedizierten Abonnement eingerichtet werden. Das erleichtert die Kostenverfolgung für AVD und vereinfacht den Bereitstellungsprozess. HINWEIS: Kostenlose Azure-Testversionen werden nicht unterstützt, da sie nicht über ausreichende Gutschriften für die Bereitstellung einer funktionsfähigen AVD-Implementierung verfügen.

Azure Kernkontingent

Genügend Quote für die VM-Familien, die Sie verwenden werden - insbesondere mindestens 10 Kerne der D v3-Familie für die anfängliche Plattform-Bereitstellung (so wenige wie 2 Kerne verwendet werden können, aber 10 deckt jede erste Möglichkeit der Bereitstellung).

Azure-Administratorkonto

Erforderlich: ein globales Azure-Administratorkonto.

Der VDS-Einrichtungsassistent fordert den Azure Admin an, dem VDS-Dienstprincipal delegierte Berechtigungen zu erteilen und die VDS Azure Enterprise-Applikation zu installieren. Der Administrator muss die folgenden Azure-Rollen zugewiesen haben:

- Globaler Administrator auf dem Mandanten
- Besitzerrolle im Abonnement

VM Image

Erforderlich: ein Azure-Image, das Multi-Session Windows 10 unterstützt.

Im Azure Marketplace finden Sie die aktuellsten Versionen ihres Basis-Images unter Windows 10. Alle Azure-Abonnements können automatisch auf diese zugreifen. Wenn Sie ein anderes Bild oder ein benutzerdefiniertes Image verwenden möchten, soll das VDS-Team Ratschläge zum Erstellen oder Ändern anderer Bilder geben oder allgemeine Fragen zu Azure-Bildern mit uns teilen und wir können ein Gespräch vereinbaren.

Active Directory

Für AVD muss die Benutzeridentität ein Bestandteil von Azure AD sein und die VMs zu einer Active Directory-Domäne gehören, die mit derselben Azure AD-Instanz synchronisiert wird. VMs können nicht direkt mit der Azure AD-Instanz verbunden werden, daher muss ein Domänen-Controller mit Azure AD konfiguriert und synchronisiert werden.

Folgende unterstützte Optionen werden unterstützt:

- Der automatisierte Aufbau einer Active Directory-Instanz innerhalb des Abonnements. Die AD-Instanz wird typischerweise durch VDS auf der VDS Control VM (CWMGR1) für Azure Virtual Desktop-Implementierungen erstellt, die diese Option verwenden. AD Connect muss im Rahmen der Einrichtung für die Synchronisierung mit Azure AD konfiguriert sein.

[]

- Integration in eine vorhandene Active Directory-Domäne, auf die über das Azure-Abonnement (normalerweise über Azure VPN oder Express Route) zugegriffen werden kann, und hat ihre Benutzerliste mit Azure AD über AD Connect oder ein Produkt eines Drittanbieters synchronisiert.

[]

Storage-Ebene

Bei AVD ist die Storage-Strategie so ausgelegt, dass sich keine persistenten Benutzer-/Unternehmensdaten auf den AVD-Session-VMs befinden. Persistente Daten für Benutzerprofile, Benutzerdateien und Ordner sowie Unternehmens-/Applikationsdaten werden auf einem oder mehreren Daten-Volumes gehostet, die auf einer unabhängigen Datenebene gehostet werden.

FSLogix ist eine Technologie für Containerbildung und löst zahlreiche Probleme bei der Benutzerprofil (wie Datenwildwuchs und langsame Anmeldungen), indem ein User Profile Container (VHD oder VHDX Format) beim Initialisieren der Session-Hosts eingebunden wird.

Aufgrund dieser Architektur ist eine Datenspeicherfunktion erforderlich. Diese Funktion muss in der Lage sein, den Datentransfer jeden Morgen/Nachmittag zu verarbeiten, wenn ein großer Teil der Benutzer sich gleichzeitig anmeldet/abmeldet. Selbst Umgebungen mittlerer Größe können erhebliche Anforderungen an den Datentransfer stellen. Die Festplatten-Performance der Daten-Storage-Ebene ist eine der primären Performance-Variablen für den Endbenutzer. Dabei muss besonders darauf Wert gelegt werden, die Performance dieses Storage angemessen zu dimensionieren, nicht nur die Storage-Menge. Im Allgemeinen sollte die Storage-Ebene so dimensioniert sein, dass sie 5-15 IOPS pro Benutzer unterstützt.

Der VDS Setup-Assistent unterstützt die folgenden Konfigurationen:

- Einrichtung und Konfiguration von Azure NetApp Files (ANF) (empfohlen). *ANF Standard Service Level unterstützt bis zu 150 Benutzer, Umgebungen mit 150-500 Benutzern ANF Premium wird empfohlen. Für 500+ Benutzer wird ANF Ultra empfohlen.*

[]

- Einrichtung und Konfiguration einer File Server VM

[]

Netzwerkbetrieb

Erforderlich: Inventarisierung aller vorhandenen Netzwerknetze einschließlich der Subnetze, die über eine Azure Express Route oder VPN zum Azure Abonnement sichtbar sind. Die Implementierung muss sich überschneidende Subnetze vermeiden.

Mit dem VDS-Setup-Assistenten können Sie den Netzwerkbereich definieren, falls im Rahmen der geplanten Integration in vorhandene Netzwerke ein Bereich erforderlich oder vermieden werden muss.

Bestimmen Sie während der Bereitstellung einen IP-Bereich für den Benutzer. Gemäß Azure Best Practices werden nur IP-Adressen in einem privaten Bereich unterstützt.

Zu den unterstützten Optionen gehören die folgenden Optionen, jedoch standardmäßig ein Bereich von /20:

- 192.168.0.0 bis 192.168.255.255
- 172.16.0.0 bis 172.31.255.255
- 10.0.0.0 bis 10.255.255.255

CKWMGR1

Einige der einzigartigen Funktionen von VDS, wie zum Beispiel die kostensparende Funktion für Workload Scheduling und Live Scaling, erfordern eine administrative Präsenz im Mandanten und im Abonnement. Daher wird eine administrative VM namens CWMGR1 im Rahmen der Automatisierung des VDS-Einrichtungsassistenten bereitgestellt. Neben VDS-Automatisierungsaufgaben enthält diese VM auch VDS-Konfigurationen in einer SQL Express-Datenbank, lokale Protokolldateien und ein erweitertes Konfigurationsprogramm mit dem Namen DCConfig.

Je nach Auswahl im VDS-Einrichtungsassistenten kann diese VM weitere Funktionen hosten, darunter:

- Ein RDS-Gateway (wird nur in RDS-Implementierungen verwendet)
- Ein HTML 5-Gateway (nur in RDS-Implementierungen verwendet)
- Ein RDS-Lizenzserver (wird nur in RDS-Implementierungen verwendet)
- Ein Domain-Controller (falls ausgewählt)

Entscheidungsbaum im Bereitstellungsassistenten

Im Rahmen der ersten Implementierung werden eine Reihe von Fragen beantwortet, um die Einstellungen für die neue Umgebung anzupassen. Im Folgenden finden Sie einen Überblick über die wichtigsten Entscheidungen, die getroffen werden sollen.

Azure Region

Legen Sie fest, welche Region oder Regionen Azure Ihre AVD Virtual Machines hosten wird. Beachten Sie, dass für Azure NetApp Files und bestimmte VM-Familien (z. B. VMs mit GPU-Unterstützung) eine definierte Support-Liste für Azure-Regionen vorhanden ist, während AVD in den meisten Regionen verfügbar ist.

- Dieser Link kann zur Identifizierung verwendet werden ["Produktverfügbarkeit von Azure nach Region"](#)

Typ Active Directory

Legen Sie fest, welchen Active Directory-Typ Sie verwenden möchten:

- Active Directory vor Ort vorhanden

- Siehe "[AVD VDS-Komponenten und -Berechtigungen](#)" Dokument, um die erforderlichen Berechtigungen und Komponenten in Azure und der lokalen Active Directory-Umgebung zu erläutern
- Neue auf Azure Abonnementbasis basierende Active Directory Instanz
- Azure Active Directory Domain Services

Datenspeicher

Legen Sie fest, wo die Daten für Benutzerprofile, einzelne Dateien und Unternehmensfreigaben platziert werden. Zur Auswahl stehen:

- Azure NetApp Dateien
- Azure Files
- Herkömmlicher Dateiserver (Azure VM mit Managed Disk)

NetApp VDS Implementierungsanforderungen für vorhandene Komponenten

NetApp VDS-Implementierung mit vorhandenen Active Directory Domain Controllern

Dieser Konfigurationstyp erweitert eine vorhandene Active Directory-Domäne, um die AVD-Instanz zu unterstützen. In diesem Fall implementiert VDS eine begrenzte Anzahl von Komponenten in der Domäne, um automatisierte Bereitstellungs- und Verwaltungsaufgaben für die AVD-Komponenten zu unterstützen.

Diese Konfiguration erfordert:

- Ein vorhandener Active Directory-Domänencontroller, auf den VMs auf dem Azure vnet zugreifen können, normalerweise über Azure VPN oder Express Route ODER über einen in Azure erstellten Domänen-Controller.
- Erweiterung der VDS-Komponenten und -Berechtigungen, die für das VDS-Management von AVD-Hostpools und Daten-Volumes erforderlich sind, wenn sie der Domäne hinzugefügt werden. Im AVD VDS-Handbuch für Komponenten und Berechtigungen werden die erforderlichen Komponenten und Berechtigungen definiert, und für den Bereitstellungsvorgang ist ein Domänenbenutzer mit Domänenberechtigungen erforderlich, um das Skript auszuführen, mit dem die erforderlichen Elemente erstellt werden.
- Beachten Sie, dass durch die VDS-Implementierung standardmäßig bei von VDS erstellten VMs ein vnet erstellt wird. Die vnet kann entweder mit vorhandenen Azure-Netzwerk-VNets Peered werden oder die CWMGR1-VM kann mit den erforderlichen vordefinierten Subnetzen in ein vorhandenes vnet verschoben werden.

Identifikationsdaten und Werkzeug zur Vorbereitung der Domäne

Administratoren müssen an einem bestimmten Punkt des Bereitstellungsprozesses eine Domänenadministratorberechtigung bereitstellen. Eine temporäre Domänenadministratorberechtigung kann später erstellt, verwendet und gelöscht werden (sobald der Bereitstellungsprozess abgeschlossen ist). Alternativ können Kunden, die Unterstützung beim Aufbau der Voraussetzungen benötigen, das Domain Preparation Tool nutzen.

NetApp VDS-Implementierung mit vorhandenem Filesystem

VDS erstellt Windows-Freigaben, mit denen über AVD-Session-VMs auf Benutzerprofile, persönliche Ordner und Unternehmensdaten zugegriffen werden kann. VDS implementiert standardmäßig entweder die File-Server- oder Azure NetApp File-Optionen, aber wenn Sie eine vorhandene Dateispeicherkomponente besitzen, kann VDS die Freigaben auf diese Komponente verweisen, sobald die VDS-Bereitstellung

abgeschlossen ist.

Die Anforderungen für die Nutzung der vorhandenen Storage-Komponente und:

- Die Komponente muss SMB v3 unterstützen
- Die Komponente muss mit derselben Active Directory-Domäne wie die AVD-Sitzungshosts verbunden sein
- Die Komponente muss in der Lage sein, einen UNC-Pfad zur Verwendung in der VDS-Konfiguration zur Verfügung zu stellen – ein Pfad kann für alle drei Freigaben verwendet werden, oder es können separate Pfade für jedes dieser Freigaben festgelegt werden. Beachten Sie, dass VDS Berechtigungen auf Benutzerebene für diese Freigaben festlegen wird. Beachten Sie daher das VDS AVD Components and Permissions Dokument, um sicherzustellen, dass die entsprechenden Berechtigungen für die VDS Automation Services erteilt wurden.

NetApp VDS-Implementierung mit vorhandenen Azure AD Domain Services

Für diese Konfiguration ist ein Prozess erforderlich, um die Attribute der vorhandenen Azure Active Directory Domain Services-Instanz zu identifizieren. Wenden Sie sich an Ihren Account Manager, um eine Bereitstellung dieses Typs anzufordern. NetApp VDS-Implementierung mit vorhandener AVD-Implementierung bei diesem Konfigurationstyp wird vorausgesetzt, dass die erforderlichen Azure vnet-, Active Directory- und AVD-Komponenten bereits vorhanden sind. Die VDS-Implementierung erfolgt auf dieselbe Weise wie die Konfiguration „NetApp VDS Deployment with Existing AD“, fügt jedoch die folgenden Anforderungen hinzu:

- Rd-Eigentümerrolle für den AVD-Mandanten muss den VDS Enterprise Applications in Azure gewährt werden
- AVD Host Pool und AVD Host Pool VMs müssen über die VDS Import Funktion in der VDS Web App in VDS importiert werden Dieser Prozess sammelt die Metadaten der AVD-Host-Pools und der VM-Session und speichert sie in VDS, sodass diese Elemente vom VDS gemanagt werden können
- AVD-Benutzerdaten müssen mithilfe des CRA-Tools in den VDS-Benutzerabschnitt importiert werden. Dieser Prozess fügt Metadaten zu jedem Benutzer in die VDS-Steuerebene ein, sodass die AVD App Group-Mitgliedschaft und die Sitzungsinformationen über VDS verwaltet werden können

ANHANG A: VDS-Steuerebenen-URLs und IP-Adressen

VDS-Komponenten im Azure-Abonnement kommunizieren mit den globalen VDS-Komponenten der Kontrollebene, wie der VDS-Webanwendung und den VDS-API-Endpunkten. Für den Zugriff müssen die folgenden Basis-URI-Adressen für den bidirektionalen Zugriff auf Port 443 sicher gestellt werden:

... ..

Wenn Ihr Zutrittskontrollgerät nur eine sichere Liste nach IP-Adresse erstellen kann, sollte die folgende Liste der IP-Adressen geschützt werden. Beachten Sie, dass VDS den Azure Traffic Manager Service verwendet. Diese Liste kann sich daher im Laufe der Zeit ändern:

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.227 23.99.136.91
40.122.119.157 40.78.132.166 40.78.129.17 40.122.52.167 40.70.147.2 40.86.99.202 13.68.19.178
13.68.114.184 137.116.69.208 13.68.18.80 13.68.114.115 13.68.114.136 40.70.63.81 52.171.218.239
52.171.223.92 52.171.217.31 52.171.216.93 52.171.220.134 92.242.140.21

ANHANG B: Microsoft AVD-Anforderungen

Dieser Abschnitt zu den Microsoft AVD-Anforderungen enthält eine Zusammenfassung der AVD-Anforderungen von Microsoft. Vollständige und aktuelle AVD-Anforderungen finden Sie hier:

<https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements>

Host-Lizenzierung für Azure Virtual Desktop-Session

Azure Virtual Desktop unterstützt die folgenden Betriebssysteme. Stellen Sie also sicher, dass Sie über die entsprechenden Lizenzen für Ihre Benutzer verfügen, die auf dem Desktop und den Apps basieren, die Sie implementieren möchten:

BETRIEBSSYSTEM	Erforderliche Lizenz
Windows 10 Enterprise Multi-Session oder Windows 10 Enterprise	MICROSOFT 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5
Windows 7 Enterprise	MICROSOFT 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5
Windows Server 2012 R2, 2016, 2019	RDS Client Access License (CAL) mit Software Assurance

URL-Zugriff für AVD-Maschinen

Die virtuellen Azure-Maschinen, die Sie für Azure Virtual Desktop erstellen, müssen Zugriff auf die folgenden URLs haben:

Adresse	Ausgehender TCP-Port	Zweck	Service-Tag
*.AVD.microsoft.com	443	Dienstverkehr	Windows VirtualDesktop
mrsglobalsteus2prod.blob.core.windows.net	443	Agent- und SXS-Stack-Updates	AzureCloud
*.core.windows.net	443	Agent-Traffic	AzureCloud
*.servicebus.windows.net	443	Agent-Traffic	AzureCloud
prod.warmpath.msftcloudes.com	443	Agent-Traffic	AzureCloud
catalogartifact.azureedge.net	443	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Windows-Aktivierung	Internet
AVDportalstorageblob.blob.core.windows.net	443	Support im Azure-Portal	AzureCloud

In der folgenden Tabelle sind optionale URLs aufgeführt, auf die Ihre virtuellen Azure-Maschinen Zugriff haben:

Adresse	Ausgehender TCP-Port	Zweck	Service-Tag
*.microsoftonline.com	443	Authentifizierung bei MS Online Services	Keine
*.events.data.microsoft.com	443	Telemetrie-Service	Keine
www.msftconnecttest.com	443	Erkennt, ob das Betriebssystem mit dem Internet verbunden ist	Keine

Adresse	Ausgehender TCP-Port	Zweck	Service-Tag
*.prod.do.dsp.mp.microsoft.com	443	Windows Update	Keine
login.windows.net	443	Melden Sie sich bei MS Online Services, Office 365 an	Keine
*.sfx.ms	443	Updates für die OneDrive Client-Software	Keine
*.digicert.com	443	Überprüfung des Zertifikatsannulfs	Keine

Optimale Performance-Faktoren

Stellen Sie sicher, dass Ihr Netzwerk die folgenden Anforderungen erfüllt, um eine optimale Leistung zu erzielen:

- Die RTT-Latenz (Round Trip) vom Netzwerk des Clients in die Azure-Region, in der Host-Pools eingesetzt wurden, sollte weniger als 150 ms betragen.
- Der Netzwerkverkehr kann außerhalb der Grenzen von Ländern/Regionen fließen, wenn VMs, auf denen Desktops und Applikationen gehostet werden, eine Verbindung zum Management-Service herstellen.
- Um die Netzwerk-Performance zu optimieren, empfehlen wir, dass die VMs des Session-Hosts in derselben Azure-Region wie der Management-Service zusammenliegen.

Unterstützte BS-Images für Virtual Machines

Azure Virtual Desktop unterstützt die folgenden x64-Betriebssystem-Images:

- Windows 10 Enterprise Multi-Session, Version 1809 oder höher
- Windows 10 Enterprise, Version 1809 oder höher
- Windows 7 Enterprise
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure Virtual Desktop unterstützt keine Images des Betriebssystems x86 (32 Bit), Windows 10 Enterprise N oder Windows 10 Enterprise KN. Aufgrund der Sektorgröße unterstützt Windows 7 zudem keine VHD- oder VHDX-basierten Profillösungen, die auf Managed Azure Storage gehostet werden.

Die verfügbaren Automatisierungs- und Implementierungsoptionen hängen davon ab, welches Betriebssystem und welche Version Sie wählen. Die in der folgenden Tabelle aufgeführten Angaben werden gezeigt:

Betriebssystem	Azure Image-Galerie	Manuelle VM-Implementierung	INTEGRATION VON ARM-Vorlagen	Bereitstellen von Host-Pools auf Azure Marketplace
Windows 10 Multisession, Version 1903	Ja.	Ja.	Ja.	Ja.

Betriebssystem	Azure Image-Galerie	Manuelle VM-Implementierung	INTEGRATION VON ARM-Vorlagen	Bereitstellen von Host-Pools auf Azure Marketplace
Windows 10 Multisession, Version 1809	Ja.	Ja.	Nein	Nein
Windows 10 Enterprise, Version 1903	Ja.	Ja.	Ja.	Ja.
Windows 10 Enterprise, Version 1809	Ja.	Ja.	Nein	Nein
Windows 7 Enterprise	Ja.	Ja.	Nein	Nein
Windows Server 2019	Ja.	Ja.	Nein	Nein
Windows Server 2016	Ja.	Ja.	Ja.	Ja.
Windows Server 2012 R2	Ja.	Ja.	Nein	Nein

Google

RDS – Implementierungsleitfaden für Google Cloud (GCP)

Überblick

Dieser Leitfaden enthält Schritt-für-Schritt-Anleitungen zum Erstellen einer RDS-Implementierung (Remote Desktop Service) unter Verwendung von NetApp Virtual Desktop Service (VDS) in Google Cloud.

Dieser Proof of Concept (POC) Leitfaden soll Ihnen dabei helfen, RDS schnell in Ihrem eigenen GCP-Test-Projekt zu implementieren und zu konfigurieren.

Produktionsimplementierungen, insbesondere in bestehenden AD-Umgebungen, sind zwar häufig in diesem POC-Leitfaden jedoch nicht berücksichtigt. Komplexe Machbarkeitsstudien und Implementierungen in der Produktion sollten mit den NetApp VDS Sales-/Services-Teams initiiert werden und jedoch nicht als Self-Service-Lösung eingesetzt werden.

Dieses POC-Dokument erläutert die gesamte RDS-Implementierung und bietet eine kurze Tour zu den wichtigsten Bereichen der Konfiguration nach der Implementierung, die in der VDS-Plattform verfügbar ist. Nach der Fertigstellung verfügen Sie über eine voll implementierte und funktionale RDS-Umgebung, die mit Sitzungshosts, Anwendungen und Benutzern abgeschlossen ist. Optional haben Sie die Möglichkeit, automatisierte Anwendungsbereitstellung, Sicherheitsgruppen, Dateifreigabeberechtigungen, Cloud Backup, intelligente Kostenoptimierung zu konfigurieren. VDS setzt eine Reihe von Best-Practice-Einstellungen über GPO ein. Anweisungen zum optionalen Deaktivieren dieser Steuerelemente sind ebenfalls enthalten, falls Ihr POC keine Sicherheitskontrollen benötigt, ähnlich wie eine nicht verwaltete lokale Geräteumgebung.

Implementierungsarchitektur

[Breite = 75 %]

RDS – Grundlagen

VDS implementiert eine voll funktionsfähige RDS-Umgebung und dabei alle erforderlichen Services von Grund auf. Diese Funktion kann Folgendes umfassen:

- RDS Gateway Server(en)

- Web-Client-Zugriffsserver
- Domänen-Controller-Server
- RDS-Lizenzservice
- ThinPrint Lizenzdienst
- FileZilla FTPS Server Service

Umfang des Leitfadens

In diesem Leitfaden erfahren Sie, wie RDS mithilfe von NetApp VDS-Technologie implementiert wird, und zwar aus der Perspektive eines GCP- und VDS-Administrators. Um das GCP-Projekt ohne Vorkonfiguration einzurichten, unterstützt Sie in diesem Leitfaden die komplette RDS-Einrichtung

Erstellen eines Servicekontos

1. Navigieren Sie in GCP zu (oder suchen Sie nach) *IAM & Admin > Service Accounts*



2. KLICKEN SIE AUF + *SERVICEKONTO ERSTELLEN*



3. Geben Sie einen eindeutigen Dienstkontonamen ein, und klicken Sie auf „*CREATE*“. Notieren Sie sich die E-Mail-Adresse des Service-Kontos, die in einem späteren Schritt verwendet wird.



4. Wählen Sie die Rolle „*Owner*“ für das Servicekonto aus, und klicken Sie auf „*CONTINUE*“



5. Auf der nächsten Seite (*Grant Users Access to this Service Account(fakultativ)*) sind keine Änderungen erforderlich, klicken Sie auf *FERTIG*



6. Klicken Sie auf der Seite *Servicekonten* auf das Aktionsmenü und wählen Sie die Option *Taste erstellen*



7. Wählen Sie *P12*, klicken Sie auf *CREATE*



8. Laden Sie die P12-Datei herunter, und speichern Sie sie auf Ihrem Computer. Das *Private Key-Passwort* wurde nicht geändert.



Google Compute-API aktivieren

1. Navigieren Sie in GCP zu (oder suchen Sie nach) *APIs & Services > Library*



2. Navigieren Sie in der GCP API Library zu (oder suchen Sie nach) *Compute Engine API*, klicken Sie auf **AKTIVIEREN**



Neue VDS-Implementierung erstellen

1. Navigieren Sie im VDS zu *Deployments* und klicken Sie auf **+ New Deployment**



2. Geben Sie einen Namen für die Bereitstellung ein



3. Wählen Sie *Google Cloud Platform*



Infrastrukturplattformen

1. Geben Sie die *Projekt-ID* und die OAuth-E-Mail-Adresse ein. Laden Sie die .P12-Datei von einer früheren Version in diesem Handbuch hoch, und wählen Sie die entsprechende Zone für diese Bereitstellung aus. Klicken Sie auf *Test*, um zu bestätigen, dass die Einträge korrekt sind und die entsprechenden Berechtigungen festgelegt wurden.



Die OAuth-E-Mail ist die Adresse des Service-Kontos, das zuvor in diesem Handbuch erstellt wurde.



2. Klicken Sie nach der Bestätigung auf *Continue*



Konten

Lokale VM-Konten

1. Geben Sie ein Kennwort für das lokale Administratorkonto ein. Dieses Passwort zur späteren Verwendung dokumentieren.
2. Geben Sie ein Kennwort für das SQL SA-Konto ein. Dieses Passwort zur späteren Verwendung dokumentieren.



Die Passwortkomplexität erfordert ein Minimum von 8 Zeichen mit 3 der 4 folgenden Zeichentypen: Groß-/Kleinbuchstaben, Zahl, Sonderzeichen

SMTP-Konto

VDS kann E-Mail-Benachrichtigungen über benutzerdefinierte SMTP-Einstellungen senden, oder der integrierte SMTP-Dienst kann durch Auswahl von *Automatic* verwendet werden.

1. Geben Sie eine E-Mail-Adresse ein, die als *von*-Adresse verwendet werden soll, wenn die E-Mail-Benachrichtigung vom VDS gesendet wird. *No-reply@<your-Domain>.com* ist ein gängiges Format.
2. Geben Sie eine E-Mail-Adresse ein, an die Erfolgsberichte weitergeleitet werden sollen.
3. Geben Sie eine E-Mail-Adresse ein, an die Fehlerberichte weitergeleitet werden sollen.



Level-3-Techniker

Level-3-Technikerkonten (auch bekannt als *Tech-Konten*) sind Konten auf Domänenebene, die VDS-Administratoren bei der Durchführung administrativer Aufgaben auf den VMs in der VDS-Umgebung verwenden können. Mit diesem Schritt und/oder später können weitere Konten erstellt werden.

1. Geben Sie den Benutzernamen und das Kennwort für das/die Administratorkonto der Stufe 3 ein. „.Tech“ wird dem Benutzernamen angehängt, den Sie eingeben, um Kunden bei der Differenzierung zwischen Endbenutzer und technischen Accounts zu unterstützen. Dokumentieren Sie diese Anmeldeinformationen zur späteren Verwendung.



Als Best Practice empfiehlt es sich, benannte Konten für alle VDS-Administratoren zu definieren, die über Anmeldeinformationen auf Domänenebene in der Umgebung verfügen sollten. VDS-Administratoren ohne diese Art von Konto können immer noch über die in VDS integrierte *Connect to Server*-Funktion auf VM-Ebene-Administratorzugriff haben.



Domänen

Active Directory damit füllt

Geben Sie den gewünschten AD-Domännennamen ein.

Öffentliche Domäne

Der externe Zugriff ist über ein SSL-Zertifikat gesichert. Dies kann mit Ihrer eigenen Domain und einem selbst verwalteten SSL-Zertifikat angepasst werden. Wenn Sie *Automatic* auswählen, kann VDS das SSL-Zertifikat verwalten, einschließlich einer automatischen 90-tägigen Aktualisierung des Zertifikats. Bei der automatischen Verwendung verwendet jede Bereitstellung eine eindeutige Subdomäne von *cloudWorkspace.App*.



Virtual Machines

Für RDS-Implementierungen müssen die erforderlichen Komponenten wie Domänen-Controller, RDS-Broker und RDS-Gateways auf dem/den Plattform-Server installiert werden. In der Produktion sollten diese Services auf dedizierten und redundanten Virtual Machines ausgeführt werden. Für Proof of Concept-Implementierungen kann eine einzelne VM zum Hosten all dieser Services verwendet werden.

Konfiguration der Plattform-VM

Nur eine Virtual Machine

Dies ist die empfohlene Auswahl für POC-Implementierungen. In einer Implementierung einer einzelnen Virtual Machine werden alle folgenden Rollen auf einer einzelnen VM gehostet:

- CW-Manager
- HTML5-Gateway
- RDS-Gateway
- Remote-App
- FTPS-Server (optional)
- Domain Controller

Die maximal empfohlene Benutzeranzahl für RDS-Anwendungsfälle in dieser Konfiguration beträgt 100 Benutzer. In dieser Konfiguration bieten ausgewogene RDS/HTML5-Gateways keine Option, was die Redundanz und Optionen für zukünftige Skalierungen einschränkt.



Wenn diese Umgebung für Mandantenfähigkeit entwickelt wurde, wird eine Konfiguration einer einzelnen Virtual Machine nicht unterstützt.

Mehrere Server

Wenn Sie die VDS-Plattform in mehrere virtuelle Maschinen aufteilen, werden die folgenden Rollen auf dedizierten VMs gehostet:

- Remote-Desktop-Gateway

VDS Setup kann zur Bereitstellung und Konfiguration von einem oder zwei RDS Gateways verwendet werden. Diese Gateways leiten die RDS-Benutzersitzung vom offenen Internet an die in der Implementierung verwendeten Session-Host-VMs weiter. RDS Gateways verfügen über eine wichtige Funktion, um RDS vor direkten Angriffen aus dem offenen Internet zu schützen und den gesamten RDS-Datenverkehr in der Umgebung zu verschlüsseln. Bei Auswahl von zwei Remote Desktop Gateways implementiert das VDS Setup zwei VMs und konfiguriert sie so, dass ein Lastausgleich der eingehenden RDS-Benutzersitzungen möglich wird.

- HTML5-Gateway

VDS Setup kann zur Bereitstellung und Konfiguration von einem oder zwei HTML5 Gateways verwendet werden. Diese Gateways hosten die HTML5-Dienste, die von der Funktion *Connect to Server* in VDS und dem webbasierten VDS-Client (H5 Portal) verwendet werden. Wenn zwei HTML5-Portale ausgewählt wurden, implementiert das VDS Setup zwei VMs und konfiguriert sie so, dass ein Lastausgleich der eingehenden HTML5-Benutzersitzungen möglich ist.



Bei der Verwendung mehrerer Serveroption (auch wenn Benutzer nur über den installierten VDS Client eine Verbindung herstellen) wird mindestens ein HTML5-Gateway dringend empfohlen, um die *Connect to Server*-Funktionalität von VDS zu aktivieren.

- Hinweise Zur Gateway-Skalierbarkeit

In RDS-Anwendungsfällen lässt sich die maximale Größe der Umgebung mit zusätzlichen Gateway VMs horizontal skalieren, wobei jeder RDS oder HTML5 Gateway ca. 500 Benutzer unterstützen kann. Weitere

Gateways können zu einem späteren Zeitpunkt mit minimaler Unterstützung von NetApp Professional Services hinzugefügt werden

Wenn diese Umgebung für die Mandantenfähigkeit entwickelt wird, ist die Auswahl „multiple Servers“ erforderlich.

Servicrollen

- Cwmgr1

Diese VM ist die administrative VM des NetApp VDS. Es führt die SQL Express-Datenbank, Hilfsprogramme und andere administrative Dienste aus. In einer Implementierung mit einem *einzelnen Server* kann diese VM auch die anderen Services hosten, aber in einer *mehreren Server* Konfiguration werden diese Services zu verschiedenen VMs verschoben.

- CWPPortal1(2)

Das erste HTML5-Gateway heißt *CWPPortal1*, die zweite ist *CWPPortal2*. Ein oder zwei können bei der Implementierung erstellt werden. Zusätzliche Server können nach der Implementierung hinzugefügt werden, um die Kapazität zu steigern (~500 Verbindungen pro Server).

- CWRDSGateway1(2)

Der erste RDS-Gateway heißt *CWRDSGateway1*, der zweite lautet *CWRDSGateway2*. Ein oder zwei können bei der Implementierung erstellt werden. Zusätzliche Server können nach der Implementierung hinzugefügt werden, um die Kapazität zu steigern (~500 Verbindungen pro Server).

- Remote-App

App Service ist eine spezielle Sammlung für das Hosting von RemotApp-Anwendungen, verwendet aber die RDS-Gateways und ihre RDWeb-Rollen, um Benutzersitzungsanfragen zu leiten und die RDWeb-Abonnementliste zu hosten. Für diese Service-Rolle ist keine dedizierte VM implementiert.

- Domänen-Controller

Bei der Implementierung können ein oder zwei Domänen-Controller automatisch erstellt und für den Einsatz mit VDS konfiguriert werden.

[]

Betriebssystem

Wählen Sie das gewünschte Serverbetriebssystem aus, das für die Plattformserver bereitgestellt werden soll.

Zeitzone

Wählen Sie die gewünschte Zeitzone aus. Die Plattformserver werden zu diesem Zeitpunkt konfiguriert, und Protokolldateien entsprechen dieser Zeitzone. Die Endbenutzersitzung spiegelt unabhängig von dieser Einstellung weiterhin ihre eigene Zeitzone wider.

Zusätzliche Services

FTP

VDS kann Filezilla optional installieren und so konfigurieren, dass ein FTPS-Server zum Verschieben von Daten in die Umgebung und aus der Umgebung ausgeführt wird. Diese Technologie ist älter und moderne Datenübertragungsmethoden (wie Google Drive) werden empfohlen.



Netzwerk

Eine Best Practice besteht darin, VMs je nach Verwendungszweck in unterschiedlichen Subnetzen zu isolieren.

Definieren Sie den Umfang des Netzwerks, und fügen Sie einen Bereich von /20 hinzu.

VDS Setup erkennt und schlägt einen Bereich vor, der sich als erfolgreich erweisen sollte. Gemäß den Best Practices müssen die Subnetz-IP-Adressen in einen privaten IP-Adressbereich fallen.

Diese Bereiche sind:

- 192.168.0.0 bis 192.168.255.255
- 172.16.0.0 bis 172.31.255.255
- 10.0.0.0 bis 10.255.255.255

Überprüfen und Anpassen Sie bei Bedarf, und klicken Sie dann auf Validieren, um Subnetze für die folgenden Bereiche zu identifizieren:

- Mandant: Dies ist der Bereich, in dem sich Session-Host-Server und Datenbankserver befinden
- Services: Das ist der Bereich, in dem PaaS-Dienste wie Cloud Volumes Service residieren
- Plattform: Dies ist der Bereich, in dem Platform-Server residieren
- Verzeichnis: Dies ist der Bereich, in dem sich AD-Server befinden



Lizenzierung

SPLA

Geben Sie Ihre SPLA-Nummer ein, damit VDS den RDS-Lizenzierungsservice für eine einfachere SPLA-RDS-CAL-Berichterstellung konfigurieren kann. Für eine POC-Bereitstellung kann eine temporäre Nummer (z. B. 12345) eingegeben werden, aber nach einem Testzeitraum (~120 Tage) wird die Verbindung der RDS-Sitzungen unterbrochen.

SPLA-Produkte

Geben Sie die MAK-Lizenzcodes für alle über SPLA lizenzierten Office-Produkte ein, um eine vereinfachte SPLA-Berichterstattung über VDS-Berichte zu ermöglichen.

ThinPrint

Wählen Sie die Installation des im Lieferumfang enthaltenen ThinPrint Lizenzservers und der Lizenz, um die Umleitung des Endnutzers zu vereinfachen.



Prüfung und Bereitstellung

Sobald alle Schritte abgeschlossen sind, überprüfen Sie die Auswahl und validieren Sie die Umgebung und stellen Sie sie bereit.[]

Nächste Schritte

Der Implementierungsprozess implementiert nun eine neue RDS-Umgebung mit den im Implementierungsassistenten ausgewählten Optionen.

Sie erhalten mehrere E-Mails, sobald die Bereitstellung abgeschlossen ist. Nach der Fertigstellung steht Ihnen eine Umgebung für Ihren ersten Arbeitsbereich zur Verfügung. Ein Arbeitsbereich enthält die Sitzungshosts und Datenserver, die zur Unterstützung der Endbenutzer benötigt werden. Kommen Sie zurück zu diesem Leitfaden, um die nächsten Schritte zu befolgen, sobald die Automatisierung der Implementierung innerhalb von 1-2 Stunden abgeschlossen ist.

Erstellen Sie eine neue Bereitstellungsammlung

Bereitstellungssammlungen sind Funktionen in VDS, die die Erstellung, Anpassung und Sysprep von VM-Images ermöglichen. Sobald wir die Implementierung am Arbeitsplatz abgeschlossen haben, benötigen wir ein Image, das bereitgestellt werden muss. Die folgenden Schritte führen Sie bei der Erstellung eines VM-Images durch.

Führen Sie diese Schritte aus, um ein Basis-Image für die Implementierung zu erstellen:

1. Navigieren Sie zu *Bereitstellungen > Provisioning Collections*, klicken Sie auf *Add*



2. Geben Sie einen Namen und eine Beschreibung ein. Wählen Sie *Typ: Shared*.



Sie können „Shared“ oder „VDI“ auswählen. Shared unterstützt einen Session-Server sowie (optional) einen Business-Server für Anwendungen wie eine Datenbank. VDI ist ein einzelnes VM-Image für VMs, das individuellen Benutzern zugewiesen wird.

3. Klicken Sie auf *Hinzufügen*, um den Typ des zu errichtenden Serverabbildes festzulegen.



4. Wählen Sie TSData als *Server-Rolle*, das entsprechende VM-Image (in diesem Fall Server 2016) und den gewünschten Speichertyp aus. Klicken Sie Auf *Server Hinzufügen*



5. Wählen Sie optional die Anwendungen aus, die auf diesem Image installiert werden sollen.
 - a. Die Liste der verfügbaren Anwendungen wird in der App-Bibliothek ausgefüllt, auf die Sie zugreifen können, indem Sie oben rechts auf der Seite „*Settings > App Catalog*“ auf das Menü „admin Name“ klicken.



6. Klicken Sie auf *Sammlung hinzufügen* und warten Sie, bis die VM erstellt wurde. VDS erstellt eine VM, auf die zugegriffen und angepasst werden kann.

7. Sobald die VM-Erstellung abgeschlossen ist, stellen Sie eine Verbindung mit dem Server her und nehmen Sie die gewünschten Änderungen vor.

a. Wenn der Status „*Collection Validation*“ angezeigt wird, klicken Sie auf den Sammlungsnamen.

□

b. Klicken Sie dann auf den Namen der *_Server-Vorlage_*

□

c. Klicken Sie schließlich auf die Schaltfläche *Connect to Server*, um eine Verbindung zu herstellen zu können, und melden Sie sich automatisch mit den lokalen Admin-Zugangsdaten bei der VM an.

□

□

8. Wenn alle Anpassungen abgeschlossen sind, klicken Sie auf *Sammlung validieren*, sodass VDS Sysprep erstellen und das Bild fertigstellen kann. Nach Abschluss wird die VM gelöscht und das Image ist für die Bereitstellung innerhalb von VDS-Implementierungsassistenten verfügbar.

□5

Neuen Arbeitsbereich erstellen

Ein Arbeitsbereich ist eine Sammlung von Session-Hosts und Datenservern, die eine Gruppe von Benutzern unterstützen. Eine Implementierung kann einen einzelnen Arbeitsbereich (Einzelmandant) oder mehrere Arbeitsbereiche (mandantenfähig) enthalten.

Arbeitsbereiche definieren die RDS-Serversammlung für eine bestimmte Gruppe. In diesem Beispiel werden wir eine einzelne Sammlung implementieren, um die Fähigkeit der virtuellen Desktops zu demonstrieren. Das Modell kann jedoch auf mehrere Workspaces/RDS-Sammlungen erweitert werden, um verschiedene Gruppen und Standorte im selben Active Directory-Domänenbereich zu unterstützen. Optional können Administratoren den Zugriff auf Arbeitsbereiche/Sammlungen einschränken, um Anwendungsfälle zu unterstützen, für die nur ein eingeschränkter Zugriff auf Applikationen und Daten erforderlich ist.

Client und Einstellungen

1. Navigieren Sie im NetApp VDS zu *Workspaces* und klicken Sie auf + *New Workspace*

□

2. Klicken Sie auf *Hinzufügen*, um einen neuen Client zu erstellen. Die Kundendetails stellen in der Regel entweder die Unternehmensinformationen oder die Informationen für einen bestimmten Standort/eine bestimmte Abteilung dar.

□

a. Geben Sie die Firmendetails ein, und wählen Sie die Bereitstellung aus, in die dieser Arbeitsbereich bereitgestellt werden soll.

b. **Datenlaufwerk:** Definieren Sie den Laufwerkbuchstaben, der für das Laufwerk verwendet werden soll.

c. **User Home Drive:** Definieren Sie den Laufwerkbuchstaben, der für das zugeordnete Laufwerk des Einzelnen verwendet werden soll.

d. Zusätzliche Einstellungen

Die folgenden Einstellungen können bei der Bereitstellung und/oder bei der Auswahl nach der Bereitstellung definiert werden.

- i. *Remote-App aktivieren*: die Remote-App stellt Anwendungen als Streaming-Anwendungen statt (oder zusätzlich zu), die eine vollständige Remote-Desktop-Sitzung präsentieren.
- ii. *App locker aktivieren*: VDS enthält die Anwendungsbereitstellung und die Berechtigungsfunktion. Standardmäßig werden die Anwendungen den Endbenutzern angezeigt bzw. ausgeblendet. Durch das Aktivieren von App locker wird der Zugriff auf Anwendungen über eine GPO-Safelliste durchgesetzt.
- iii. *Workspace Benutzerdatenspeicherung aktivieren*: Bestimmen Sie, ob Endbenutzer auf ihrem virtuellen Desktop auf den Storage zugreifen müssen. Bei RDS-Implementierungen sollte diese Einstellung immer aktiviert werden, um den Datenzugriff für Benutzerprofile zu ermöglichen.
- iv. *Druckerzugriff deaktivieren*: VDS kann den Zugriff auf lokale Drucker blockieren.
- v. *Zugriff auf Task Manager zulassen*: VDS kann den Endbenutzer-Zugriff auf den Task-Manager in Windows aktivieren/deaktivieren.
- vi. *Komplexes Benutzerpasswort benötigen*: komplexe Passwörter erfordern ermöglicht die systemeigenen Regeln für das Kennwort des Windows Servers. Außerdem wird die automatische zeitverzögerte Entsperrung gesperrter Benutzerkonten deaktiviert. Wenn diese Option aktiviert ist, ist ein Eingreifen des Administrators erforderlich, wenn Endbenutzer ihre Konten mit mehreren fehlgeschlagenen Kennwortversuchen sperren.
- vii. *MFA für alle Benutzer aktivieren*: VDS enthält einen kostenlosen E-Mail-/SMS-MFA-Dienst, der zum Schutz des Benutzerzugriffs und/oder des VDS-Administratorkontos verwendet werden kann. Wenn Sie diese Option aktivieren, müssen sich alle Endbenutzer in diesem Workspace mit MFA authentifizieren, um auf ihren Desktop und/oder ihre Anwendungen zuzugreifen.

Anwendungen auswählen

Wählen Sie die Windows-Betriebssystemversion und die Provisioning-Sammlung aus, die zuvor in diesem Handbuch erstellt wurden.

Zu diesem Zeitpunkt können weitere Applikationen hinzugefügt werden. Bei diesem POC behandeln wir jedoch die Berechtigungen für Applikationen nach der Implementierung.

□

Benutzer Hinzufügen

Benutzer können hinzugefügt werden, indem Sie eine vorhandene AD Sicherheitsgruppe oder einzelne Benutzer auswählen. In diesem POC-Leitfaden werden Benutzer nach der Implementierung hinzugefügt.

□

Prüfung und Bereitstellung

Überprüfen Sie auf der letzten Seite die ausgewählten Optionen und klicken Sie auf *Provisioning*, um den automatisierten Aufbau der RDS-Ressourcen zu starten.

□



Während des Bereitstellungsprozesses werden Protokolle erstellt und können unter „*Task History*“ am Ende der Seite „Deployment Details“ aufgerufen werden. Aufrufen, indem Sie zu *VDS > Bereitstellungen > Bereitstellungsname* navigieren

Nächste Schritte

Durch den Automatisierungsprozess am Arbeitsplatz werden nun neue RDS-Ressourcen mit den Optionen bereitgestellt, die Sie im Implementierungsassistenten ausgewählt haben.

Nach dem Abschluss stehen Ihnen verschiedene Workflows zur Anpassung der typischen RDS-Implementierung zur Verfügung.

- ["Benutzer Hinzufügen"](#)
- ["Endbenutzerzugriff"](#)
- ["Applikationsberechtigung"](#)
- ["Kostenoptimierung"](#)

Voraussetzungen für die Google Compute Platform (GCP) und VDS

GCP- und VDS-Anforderungen und -Hinweise

In diesem Dokument werden die erforderlichen Elemente zur Implementierung von Remote Desktop Services (RDS) mithilfe von NetApp Virtual Desktop Service (VDS) beschrieben. Die „Quick Checklist“ enthält eine kurze Liste der erforderlichen Komponenten und Schritte zur Vorabbereitung, um eine effiziente Bereitstellung zu gewährleisten. Der restliche Leitfaden bietet je nach getroffenen Konfigurationsauswahl detailliertere Informationen für jedes Element.

[Breite = 75 %]

Schnelle Checkliste

GCP-Anforderungen

- GCP-Mandant
- GCP-Projekt
- Servicekonto mit der Rolle des Eigentümers zugewiesen

Informationen vor der Implementierung

- Bestimmen Sie die Gesamtzahl der Benutzer
- GCP-Region und -Zone festlegen
- Bestimmen Sie den Typ des aktiven Verzeichnisses
- Ermitteln Sie den Storage-Typ
- Host-VM-Image oder -Anforderungen ermitteln
- Bewertung vorhandener GCP- und On-Premises-Netzwerkconfiguration

VDS-Bereitstellung – Detaillierte Anforderungen

Verbindungsanforderungen für Endbenutzer

Die folgenden Remote Desktop-Clients unterstützen RDS in GCP:

- "NetApp VDS Client für Windows"
 - NetApp VDS Client für Windows: URL-Safelisting-Anforderungen für ausgehende urls
 - `api.cloudworkspace.com`
 - `VdsClient.App`
 - `api.vdsclient.App`
 - `Bin.vdsclient.App`
 - Erweiterte Funktionen:
 - VDS Wake on demand
 - ThinPrint Client und Läuse nsen
 - Self-Service-Kennwort zurücksetzen
 - Automatische Aushandlung von Server- und Gateway-Adressen
 - Umfassende Unterstützung von Desktop- und Streaming-Applikationen
 - Verfügbares benutzerdefiniertes Branding
 - Installer-Switches für die automatische Bereitstellung und Konfiguration
 - Integrierte Tools zur Fehlerbehebung
- "NetApp VDS Web-Client"
- "Microsoft RD-Client"
 - Windows
 - MacOS
 - ISO
 - Android
- Software von Drittanbietern und/oder Thin Clients
 - Anforderung: Unterstützen Sie die Konfiguration des RD-Gateways

Storage-Ebene

Bei VDS implementierte RDS-Lösung wurde die Storage-Strategie so entwickelt, dass sich keine persistenten Benutzer-/Unternehmensdaten auf den AVD-Session-VMs befinden. Persistente Daten für Benutzerprofile, Benutzerdateien und Ordner sowie Unternehmens-/Applikationsdaten werden auf einem oder mehreren Daten-Volumes gehostet, die auf einer unabhängigen Datenebene gehostet werden.

FSLogix ist eine Technologie für Containerbildung und löst zahlreiche Probleme bei der Benutzerprofil (wie Datenwildwuchs und langsame Anmeldungen), indem ein User Profile Container (VHD oder VHDX Format) beim Initialisieren der Session-Hosts eingebunden wird.

Aufgrund dieser Architektur ist eine Datenspeicherfunktion erforderlich. Diese Funktion muss in der Lage sein, den Datentransfer jeden Morgen/Nachmittag zu verarbeiten, wenn ein großer Teil der Benutzer sich gleichzeitig anmeldet/abmeldet. Selbst Umgebungen mittlerer Größe können erhebliche Anforderungen an den Datentransfer stellen. Die Festplatten-Performance der Daten-Storage-Ebene ist eine der primären Performance-Variablen für den Endbenutzer. Dabei muss besonders darauf Wert legen, die Performance dieses Storage angemessen zu dimensionieren, nicht nur die Storage-Menge. Im Allgemeinen sollte die

Storage-Ebene so dimensioniert sein, dass sie 5-15 IOPS pro Benutzer unterstützt.

Netzwerkbetrieb

Erforderlich: Inventarisierung aller vorhandenen Netzwerknetze einschließlich aller Subnetze, die über ein VPN für das GCP-Projekt sichtbar sind. Die Implementierung muss sich überschneidende Subnetze vermeiden.

Mit dem VDS-Setup-Assistenten können Sie den Netzwerkbereich definieren, falls im Rahmen der geplanten Integration in vorhandene Netzwerke ein Bereich erforderlich oder vermieden werden muss.

Bestimmen Sie während der Bereitstellung einen IP-Bereich für den Benutzer. Gemäß Best Practices werden nur IP-Adressen in einem privaten Bereich unterstützt.

Zu den unterstützten Optionen gehören die folgenden Optionen, jedoch standardmäßig ein Bereich von /20:

- 192.168.0.0 bis 192.168.255.255
- 172.16.0.0 bis 172.31.255.255
- 10.0.0.0 bis 10.255.255.255

CKWMGR1

Einige der einzigartigen Funktionen von VDS, wie zum Beispiel die kostensparende Funktion für Workload Scheduling und Live Scaling, erfordern einen administrativen Präsenz innerhalb des Unternehmens und des Projekts. Daher wird eine administrative VM namens CWMGR1 im Rahmen der Automatisierung des VDS-Einrichtungsassistenten bereitgestellt. Neben VDS-Automatisierungsaufgaben enthält diese VM auch VDS-Konfigurationen in einer SQL Express-Datenbank, lokale Protokolldateien und ein erweitertes Konfigurationsprogramm mit dem Namen DCConfig.

Je nach Auswahl im VDS-Einrichtungsassistenten kann diese VM weitere Funktionen hosten, darunter:

- Ein RDS-Gateway
- Ein HTML 5-Gateway
- Einen RDS-Lizenzserver
- Ein Domänencontroller

Entscheidungsbaum im Bereitstellungsassistenten

Im Rahmen der ersten Implementierung werden eine Reihe von Fragen beantwortet, um die Einstellungen für die neue Umgebung anzupassen. Im Folgenden finden Sie einen Überblick über die wichtigsten Entscheidungen, die getroffen werden sollen.

GCP-Region

Legen Sie fest, welche GCP-Region oder -Regionen Ihre VDS-Virtual Machines hosten. Beachten Sie, dass die Region basierend auf der Nähe zu den Endbenutzern und den verfügbaren Services ausgewählt werden sollte.

Datenspeicher

Legen Sie fest, wo die Daten für Benutzerprofile, einzelne Dateien und Unternehmensfreigaben platziert werden. Zur Auswahl stehen:

- Cloud Volumes Service für GCP

- Herkömmlicher File Server

NetApp VDS Implementierungsanforderungen für vorhandene Komponenten

NetApp VDS-Implementierung mit vorhandenen Active Directory Domain Controllern

Dieser Konfigurationstyp erweitert eine vorhandene Active Directory-Domäne, um die RDS-Instanz zu unterstützen. In diesem Fall implementiert VDS eine begrenzte Anzahl an Komponenten in der Domäne, um automatisierte Bereitstellungs- und Managementaufgaben für die RDS-Komponenten zu unterstützen.

Diese Konfiguration erfordert:

- Ein vorhandener Active Directory-Domänen-Controller, auf den VMs im GCP-VPC-Netzwerk zugegriffen werden kann, normalerweise über einen VPN oder einen in GCP erstellten Domänen-Controller.
- Zusätzliche VDS-Komponenten und -Berechtigungen, die für das VDS-Management von RDS-Hosts und Daten-Volumes erforderlich sind, sobald diese in der Domäne zusammengeführt werden. Für den Bereitstellungsprozess ist ein Domänenbenutzer mit Domänenberechtigungen erforderlich, um das Skript auszuführen, mit dem die erforderlichen Elemente erstellt werden.
- Die VDS-Implementierung erstellt standardmäßig ein VPC-Netzwerk für von VDS erstellte VMs. Das VPC-Netzwerk kann entweder über vorhandene VPC-Netzwerke Peering durchgeführt werden oder die CWMGR1-VM kann zu einem vorhandenen VPC-Netzwerk mit den erforderlichen vorab definierten Subnetzen verschoben werden.

Identifikationsdaten und Werkzeug zur Vorbereitung der Domäne

Administratoren müssen an einem bestimmten Punkt des Bereitstellungsprozesses eine Domänenadministratorberechtigung bereitstellen. Eine temporäre Domänenadministratorberechtigung kann später erstellt, verwendet und gelöscht werden (sobald der Bereitstellungsprozess abgeschlossen ist). Alternativ können Kunden, die Unterstützung beim Aufbau der Voraussetzungen benötigen, das Domain Preparation Tool nutzen.

NetApp VDS-Implementierung mit vorhandenem Filesystem

VDS erstellt Windows-Freigaben, mit denen über RDS-Session-Hosts auf Benutzerprofile, persönliche Ordner und Unternehmensdaten zugegriffen werden kann. VDS stellt standardmäßig entweder den Dateiserver bereit. Wenn Sie jedoch bereits über eine Dateispeicherkomponente verfügen, kann VDS die Freigaben auf diese Komponente verweisen, sobald die VDS-Bereitstellung abgeschlossen ist.

Die Anforderungen für die Nutzung der vorhandenen Storage-Komponente und:

- Die Komponente muss SMB v3 unterstützen
- Die Komponente muss mit derselben Active Directory-Domäne verbunden sein wie der/die RDS-Sitzungshost(s).
- Die Komponente muss in der Lage sein, einen UNC-Pfad zur Verwendung in der VDS-Konfiguration zur Verfügung zu stellen – ein Pfad kann für alle drei Freigaben verwendet werden, oder es können separate Pfade für jedes dieser Freigaben festgelegt werden. Beachten Sie, dass VDS Berechtigungen auf Benutzerebene für diese Freigaben setzt. Stellen Sie sicher, dass die entsprechenden Berechtigungen für VDS Automation Services erteilt wurden.

ANHANG A: VDS-Steuerebenen-URLs und IP-Adressen

VDS-Komponenten im GCP-Projekt kommunizieren mit den globalen VDS-Komponenten der Kontrollebene, die in Azure gehostet werden, einschließlich der VDS-Webanwendung und der VDS-API-Endpunkte. Für den Zugriff müssen die folgenden Basis-URI-Adressen für den bidirektionalen Zugriff auf Port 443 sicher gestellt

werden:

|||||

Wenn Ihr Zutrittskontrollgerät nur eine sichere Liste nach IP-Adresse erstellen kann, sollte die folgende Liste der IP-Adressen geschützt werden. Beachten Sie, dass VDS einen Load Balancer mit redundanten öffentlichen IP-Adressen verwendet. Diese Liste kann sich mit der Zeit ändern:

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.227 23.99.136.91
40.122.119.157 40.78.132.166 40.78.129.17 40.122.52.167 40.70.147.2 40.86.99.202 13.68.19.178
13.68.114.184 137.116.69.208 13.68.18.80 13.68.114.115 13.68.114.136 40.70.63.81 52.171.218.239
52.171.223.92 52.171.217.31 52.171.216.93 52.171.220.134 92.242.140.21

Optimale Performance-Faktoren

Stellen Sie sicher, dass Ihr Netzwerk die folgenden Anforderungen erfüllt, um eine optimale Leistung zu erzielen:

- Die RTT-Latenz (Round-Trip) vom Netzwerk des Clients in die GCP-Region, in der die Session-Hosts implementiert wurden, sollte weniger als 150 ms betragen.
- Der Netzwerkverkehr kann außerhalb der Grenzen von Ländern/Regionen fließen, wenn VMs, auf denen Desktops und Applikationen gehostet werden, eine Verbindung zum Management-Service herstellen.
- Um die Netzwerk-Performance zu optimieren, sollten die VMs des Session-Hosts in derselben Region wie der Management-Service untergebracht werden.

Unterstützte BS-Images für Virtual Machines

RDS-Session-Hots, implementiert von VDS, unterstützen die folgenden x64-Betriebssystem-Images:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Architektur

Umleitung Der Storage-Plattform

Überblick

Bereitstellungstechnologien für Virtual Desktop Services ermöglichen unterschiedliche Storage-Optionen je nach zugrunde liegender Infrastruktur und dieser Leitfaden beschreibt, wie eine Änderung nach der Implementierung vorgenommen werden kann.

Die Performance virtueller Desktops hängt von verschiedenen wichtigen Ressourcen ab. Die Storage-Performance ist eine der primären Variablen. Wenn sich Anforderungen ändern und Workloads steigen, ist es häufig erforderlich, die Storage-Infrastruktur zu ändern. In fast allen Fällen umfasst dies die Migration von einer File-Server-Plattform zu NetApp Storage-Technologie (z. B. Azure NetApp Files, NetApp Cloud Volumes Service in Google oder NetApp Cloud Volumes ONTAP in AWS), da diese Technologien typischerweise das beste Performance-Profil für Endbenutzer-Computing-Umgebungen bieten.

Erstellen der neuen Speicherebene

Aufgrund der Vielzahl potenzieller Storage-Services in zahlreichen Cloud- und HCI-Infrastrukturanbietern wird in diesem Leitfaden davon ausgegangen, dass bereits ein neuer Storage-Service etabliert wurde und der bekannte SMB-Pfad(e) enthält.

Erstellen von Speicherordnern

1. Erstellen Sie im neuen Speicherdienst drei Ordner:

- /Daten
- /Home
- /Pro

[]

2. Legen Sie Die Ordnerberechtigungen Fest

a. Wählen Sie unter Ordneigenschaften die Option *Sicherheit*, >Erweitert > Vererbung deaktivieren

[]

b. Sie können die verbleibenden Einstellungen an die Einstellungen der ursprünglichen Storage-Ebene anpassen, die ursprünglich durch die Automatisierung der Implementierung erstellt wurden.

Verschieben von Daten




Verzeichnisse, Daten, Dateien und Sicherheitseinstellungen können auf verschiedene Arten verschoben werden. Die folgende robocopy-Syntax führt zu den erforderlichen Änderungen. Die Pfade müssen an Ihre Umgebung angepasst werden.

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


Umleitung des SMB-Pfads bei der Umstellung

Wenn der Zeitpunkt der Umstellung zu verkürzen ist, werden einige Änderungen alle Storage-Funktionen in der VDS-Umgebung umleiten.

Gruppenrichtlinienobjekte aktualisieren

1. Das Gruppenrichtlinienobjekt Benutzer (mit dem Namen *<company-Code>-Users*) muss mit dem neuen Freigabepfad aktualisiert werden. Wählen Sie *Benutzerkonfiguration > Windows-Einstellungen > Einstellungen > Laufwerkskarten*

2. Klicken Sie mit der rechten Maustaste auf *H:*, wählen Sie *Eigenschaften > Bearbeiten > Aktion: Ersetzen_*, und geben Sie den neuen Pfad ein

3. Mit Classic- oder Hybrid-AD-Update wird die Freigabe in ADUC in der Firma OU definiert. Dies spiegelt sich in der VDS-Ordnerverwaltung wieder.


Aktualisieren der FSLogix-Profilpfade

1. Öffnen Sie Regedit auf dem ursprünglichen Dateiserver und allen anderen bereitgestellten Sitzungshosts.
 Dies kann bei Bedarf auch über eine GPO-Richtlinie festgelegt werden.
2. Bearbeiten Sie den Wert *VHDLocations* mit dem neuen Wert. Dies sollte der neue SMB Pfad plus *pro/profilecontainers* sein, wie in der Abbildung unten gezeigt.



Aktualisieren Sie die Ordnerumleitungseinstellungen für die Home-Verzeichnisse

1. Open Group Policy Management, wählen Sie das Gruppenrichtlinienobjekt Benutzer aus, das mit DC=Domain,DC=mobi/Cloud Workspace/Cloud Workspace Companies/<company-Code>/<company-Code>-Desktop-Benutzer verknüpft ist.
2. Ordnerumleitungspfade bearbeiten unter Benutzerkonfiguration>Richtlinien>Windows-Einstellungen>Ordnerumleitung.
3. Nur Desktop und Dokumente müssen aktualisiert werden. Die Pfade sollten mit dem neuen SMB-Pfad-Bereitstellungspunkt für Home Volume übereinstimmen



Aktualisieren Sie die VDS SQL-Datenbank mit Command Center

CWMGR1 enthält eine Hilfsprogramm-Anwendungen namens Command Center, die Bulk-Update der VDS-Datenbank kann.

So stellen Sie die endgültige Datenbank-Aktualisierung vor:

1. Stellen Sie eine Verbindung zu CWMGR1 her, navigieren Sie und führen Sie CommandCenter.exe aus

[]

2. Navigieren Sie zur Registerkarte *Operations*, klicken Sie auf *Daten laden*, um das Dropdown-Menü Company Code auszufüllen, wählen Sie den Unternehmenscode aus, und geben Sie die neuen Speicherpfade für die Speicherebene ein, und klicken Sie dann auf *Execute Command*.

[]

Umleitung der Storage-Plattform auf Azure Files

Überblick

Mithilfe von Bereitstellungstechnologien für Virtual Desktop Services können verschiedene Storage-Optionen genutzt werden, abhängig von der zugrunde liegenden Infrastruktur. In diesem Leitfaden wird beschrieben, wie Sie die Nutzung von Azure Files nach der Implementierung ändern.

Voraussetzungen

- AD Connect installiert und eingerichtet
- Globales Azure-Administratorkonto
- AZFilesHybrid PowerShell-Modul <https://github.com/Azure-Samples/azure-files-samples/releases>
- AZ PowerShell-Modul
- ActiveDirectory PowerShell-Modul

Erstellen Sie die neue Speicherebene

1. Melden Sie sich mit dem globalen Administratorkonto bei Azure an
2. Erstellen Sie ein neues Speicherkonto an demselben Speicherort und in derselben Ressourcengruppe wie der Arbeitsbereich

[]

3. Erstellen Sie die Daten-, Home- und Pro-File Shares unter dem Storage-Konto

[]

Einrichten Von Active Directory

1. Erstellen Sie unter Cloud Workspace > Cloud Worksapce Service Accounts OU eine neue Organisationseinheit mit dem Namen „Storage Account“

[]

2. Aktivieren der AD DS-Authentifizierung (muss mit PowerShell durchgeführt werden) <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-enable>
 - a. DomänenAccountType sollte sein "ServiceLogonAccount,"
 - b. OraganisierungsUnitDistinguishedName ist der im vorherigen Schritt erstellte Name der OU (d.h. "OU=Storage Account,OU=Cloud Workspace Service Accounts,OU=Cloud

Workspace,DC=TrainingKrisG,DC=onmicrosoft,DC=com,,)

Legen Sie die Rollen für die Freigaben fest

1. Geben Sie im Azure-Portal „Storage File Data SMB Share Elevated Contributor“ die Rolle von CloudWorkspaceSVC und Level3-Technikern

[]

2. Dem wird die Rolle „Storage File Data SMB Share Contributor“ zugewiesen „<company code>-all users“-Gruppe“

[]

Erstellen Sie die Verzeichnisse

1. Erstellen Sie in jeder Freigabe ein Verzeichnis (Daten, Zuhause, pro), indem Sie den Unternehmenscode als Namen verwenden (in diesem Beispiel lautet der Unternehmenscode „kift“).

[]

2. Erstellen Sie im Verzeichnis <company Code> des Proshare ein Verzeichnis „ProfilContainers“

[]

Legen Sie die NTFS-Berechtigungen fest

1. Stellen Sie eine Verbindung zu den Freigaben her
 - a. Navigieren Sie im Azure-Portal zu der Freigabe unter dem Storage-Konto, klicken Sie auf die drei Punkte und klicken Sie anschließend auf Verbinden

[]

 - b. Wählen Sie die Methode Active Directory for Authentication aus, und klicken Sie in der rechten unteren Ecke des Codes auf das Symbol in die Zwischenablage kopieren

[]

 - c. Melden Sie sich am CWMGR1-Server mit einem Konto an, das Mitglied der Level3-Technikerguppe ist
 - d. Führen Sie den kopierten Code in PowerShell aus, um das Laufwerk zuzuordnen
 - e. Führen Sie für jede Freigabe das gleiche aus, während Sie einen anderen Laufwerksbuchstaben für jeden auswählen
2. Deaktivieren Sie die Vererbung in den Verzeichnissen <company Code>
3. System und AD Group Client DHPAccess sollten die Verzeichnisse <company Code> vollständig steuern
4. Domain Computers sollten die volle Kontrolle über das Verzeichnis <company Code> im Pro-Share sowie das Verzeichnis ProfilContainers in haben
5. Die <company Code>-all Users AD Group sollte Listen Ordner/read Data permissions in den Verzeichnissen <company Code> im Home und pro Shares haben
6. Die AD-Gruppe <company Code>-all Users sollte die unten aufgeführten Sonderberechtigungen für das Verzeichnis in der Datenfreigabe besitzen

[]

7. Die AD-Gruppe <company Code>-all Users sollte über die Berechtigung Ändern im ProfilContainers-Verzeichnis verfügen

Gruppenrichtlinienobjekte Aktualisieren

1. Aktualisieren Sie das Gruppenrichtlinienobjekt <Unternehmenscode> Benutzer unter Cloud Workspace > Cloud Workspace Companies > <Company Code> <Company Code>-Desktop-Benutzer
 - a. Ändern Sie die Zuordnung des Home-Laufwerks, um die neue Home-Freigabe zu zeigen
- b. Ändern Sie die Ordnerumleitung, um die Home-Freigabe für Desktop und Dokumente zu zeigen

[]

[]

[]

Aktualisieren Sie die Freigabe in Active Directory-Benutzern und -Computern

1. Bei klassischer oder hybrider AD muss der Anteil im Unternehmenscode OU auf den neuen Standort aktualisiert werden

[]

Aktualisieren von Daten-/Home-/Pro-Pfaden im VDS

1. Melden Sie sich bei CWMGR1 mit einem Konto in der Level3 Technicians Group an und starten Sie Command Center
2. Wählen Sie in der Dropdown-Liste Befehl die Option Daten/Home/Pro Ordner ändern aus
3. Klicken Sie auf die Schaltfläche Daten laden, und stellen Sie sicher, dass der richtige Unternehmenscode aus der Dropdown-Liste ausgewählt ist
4. Geben Sie die neue Patsh für die Daten-, Home- und pro-Standorte ein
5. Deaktivieren Sie das Kontrollkästchen IS Windows Server
6. Klicken Sie auf die Schaltfläche Befehl ausführen

[]

Aktualisieren der FSLogix-Profilpfade

1. Öffnen Sie den Registrierungseditiv auf den Session-Hosts
2. Bearbeiten Sie den Eintrag VHDLocations unter HKLM\SOFTWARE\FSLogix\Profiles, um den UNC-Pfad zum neuen ProfilContainers-Verzeichnis zu erhalten

[]

Backups Konfigurieren

1. Es wird empfohlen, eine Backup-Richtlinie für die neuen Freigaben einzurichten und zu konfigurieren
2. Erstellen Sie einen neuen Recovery Services Vault in derselben Ressourcengruppe
3. Navigieren Sie zum Tresor, und wählen Sie unter erste Schritte Sicherung aus
4. Wählen Sie Azure für den aktiven Workload und die Azure-Dateifreigabe für das, was Sie sichern möchten, und klicken Sie dann auf Backup
5. Wählen Sie das Speicherkonto aus, das zum Erstellen der Freigaben verwendet wird
6. Fügen Sie die Shares hinzu, die gesichert werden sollen
7. Bearbeiten und Erstellen einer Backup-Richtlinie, die Ihren Anforderungen entspricht

Überlegungen Zur Datenmigration

Überblick

Das Migrieren von Daten ist eine nahezu universelle Anforderung für die Migration zu einer beliebigen Cloud-Lösung. Während Administratoren für die Migration von Daten in ihre Virtual Desktops verantwortlich sind, steht NetApp aufgrund seiner Erfahrung für unzählige Kundenmigrationen im Einsatz. Bei der Virtual Desktop-Umgebung handelt es sich lediglich um eine gehostete Windows-Umgebung, sodass wahrscheinlich alle gewünschten Methoden unterstützt werden können.

Üblicherweise migrierte Daten:

- Benutzerprofile (Desktop, Dokumente, Favoriten usw....)
- File Server-Freigaben
- Datenfreigaben (App-Daten, Datenbanken, Backup-Caches)

In der Virtual Desktop-Umgebung gibt es zwei primäre Orte, an denen Daten gespeichert und organisiert sind:

- Das Laufwerk Benutzer (normalerweise H:): Dies ist das zugeordnete Laufwerk, das für jeden Benutzer sichtbar ist.
 - Dies wird wieder dem Pfad <DRIVE>:\Home\CustomerCode\user.name\ zugeordnet
 - Jeder Benutzer hat sein eigenes Laufwerk H:\ und kann keinen anderen Benutzer sehen
- Das freigegebene (typischerweise I:) Laufwerk: Dies ist das freigegebene zugeordnete Laufwerk, das für alle Benutzer sichtbar ist
 - Dies wird dem Pfad <DRIVE>:\Data\CustomerCode\ zugeordnet
 - Alle Benutzer können auf dieses Laufwerk zugreifen. Ihre Zugriffsebene auf enthaltene Ordner/Dateien wird im Bereich Ordner von VDS verwaltet.

Generischer Migrationsprozess

1. Replizieren von Daten in die Cloud-Umgebung
2. Verschieben Sie die Daten auf den entsprechenden Pfad für die Laufwerke H:\ und I:\
3. Weisen Sie in der Virtual Desktop-Umgebung entsprechende Berechtigungen zu

FTPS-Transfers und -Überlegungen

Migration mit FTPS

1. Wenn die FTPS-Serverrolle während des CWA-Bereitstellungsprozesses aktiviert wurde, sammeln Sie FTPS-Anmeldeinformationen, indem Sie sich beim VDS anmelden, zu Berichten navigieren und den Master Client-Bericht für Ihr Unternehmen ausführen
2. Daten hochladen
3. Verschieben Sie die Daten auf den entsprechenden Pfad für die Laufwerke H:\ und I:\
4. Weisen Sie in der virtuellen Desktop-Umgebung über das Ordnermodul entsprechende Berechtigungen zu



Bei der Übertragung von Daten über FTPS verhindert jede Unterbrechung, dass die Daten wie vorgesehen übertragen werden. Da die von Virtual Desktop Services gemanagten Server nachts neu gestartet werden, wird die standardmäßige Übertragungsstrategie über Nacht wahrscheinlich unterbrochen. Administratoren können den Migrationsmodus aktivieren, sodass die VMs nicht mehr für eine Woche neu gestartet werden können.

Die Aktivierung des Migrationsmodus ist einfach: Navigieren Sie zur Organisation, scrollen Sie dann zum Abschnitt Virtual Desktop Settings und aktivieren Sie das Kontrollkästchen für den Migrationsmodus, und klicken Sie dann auf Update.



NetApp empfiehlt Administratoren die Aktivierung einer Compliance-Einstellung, die Unternehmen bei der Einhaltung von PCI-, HIPAA- und NIST-Kontrollen unterstützt, indem sie Gateways der Bereitstellung usw. härten. Dadurch wird auch die standardmäßige FTP-Server-Rolle, sofern aktiviert, von der Annahme unverschlüsselter Standardübertragungen über Port 21 deaktiviert. FileZilla erlaubt SFTP nicht, was bedeutet, dass Verbindungen mit FTPS über Port 990 hergestellt werden sollten.

Um diese Einstellung zu aktivieren, stellen Sie eine Verbindung zu CWMGR1 her, navigieren Sie zum Programm CwVmAutomationService und aktivieren Sie dann die PCI v3-Konformität.

Synchronisierung von Tools und Überlegungen

Enterprise File Sync and Share, das häufig als EFSS- oder Sync-Tools bezeichnet wird, kann besonders bei der Datenmigration von Nutzen sein, da das Tool Änderungen auf beiden Seiten bis zur Umstellung erfasst. Tools wie OneDrive, das mit Office 365 kommt, können Ihnen helfen, Dateiserver-Daten zu synchronisieren. Es ist auch nützlich für VDI-Benutzer-Bereitstellungen als auch, wo es eine 1:1-Beziehung zwischen dem Benutzer und der VM, solange der Benutzer nicht versucht, gemeinsam genutzte Inhalte auf ihren VDI-Server zu synchronisieren, wenn gemeinsam genutzte Daten einmal auf die Shared bereitgestellt werden (typischerweise I:\) Antrieb für das gesamte Unternehmen. Migration von SQL und ähnlichen Daten (Open Files)

Offene Dateien werden von gängigen Sync- und/oder Migrationslösungen nicht übertragen, darunter folgende Dateitypen:

- Mailbox-Dateien (.ost)
- QuickBooks-Dateien
- Microsoft Access-Dateien
- SQL Datenbanken

Das heißt, wenn ein einzelnes Element der gesamten Datei (z.B. 1 neue E-Mail) oder Datenbank (1 neuer

Datensatz wird in das System einer App eingegeben) erscheint, dann ist die gesamte Datei anders und Standard-Sync-Tools (z.B. Dropbox) Werden annehmen, dass es eine völlig neue Datei ist und erneut verschoben werden muss. Auf Wunsch stehen spezielle Tools für den Kauf bei Drittanbietern zur Verfügung.

Eine weitere häufige Vorgehensweise bei diesen Migrationen ist der Zugriff auf VAR-Mitarbeiter von Drittanbietern, die häufig den Import/Export von Datenbanken optimiert haben.

Frachtfestplatten

Viele Datacenter Provider senden keine Festplatten mehr an – entweder diese oder Sie müssen ihre spezifischen Richtlinien und Verfahren befolgen.

Microsoft Azure ermöglicht Unternehmen die Nutzung von Azure Data Box, zu denen Administratoren von der Koordinierung mit ihren Microsoft Vertretern profitieren können.

Verlängerung des Platzhalter-SSL-Zertifikats

Zertifikatsignierungsanforderung (CSR) erstellen:

1. Stellen Sie eine Verbindung zu CWMGR1 her
2. Öffnen Sie IIS Manager über Administrator-Tools
3. Wählen Sie CWMGR1 und öffnen Sie Server Certificates
4. Klicken Sie im Bereich Aktionen auf Zertifikatanforderung erstellen

[]

5. Geben Sie die Distinguished Name Properties im Assistenten für das Anforderungszertifikat ein, und klicken Sie auf Weiter:
 - a. Allgemeiner Name: FQDN des Platzhalters - *.domain.com
 - b. Organisation: Der gesetzlich registrierte Name Ihrer Firma
 - c. Organisationseinheit: 'Funktioniert gut
 - d. Stadt: Stadt, in der die Firma liegt
 - e. Staat: Geben Sie an, wo die Firma ansässig ist
 - f. Land: Land, in dem die Firma ansässig ist

[]

6. Überprüfen Sie auf der Seite Eigenschaften von Cryptographic Service Provider, ob das folgende angezeigt wird, und klicken Sie auf Weiter:

[]

7. Geben Sie einen Dateinamen an, und suchen Sie nach einem Speicherort, an dem Sie den CSR speichern möchten. Wenn Sie keinen Speicherort angeben, befindet sich der CSR in C:\Windows\System32:

[]

8. Klicken Sie auf Fertig stellen. Sie verwenden diese Textdatei, um Ihre Bestellung an die Zertifikatregistrierung zu senden

9. Wenden Sie sich an den Registrar-Support, um einen neuen Wildcard SSL für Ihr Zertifikat zu kaufen:
*.domain.com
10. Speichern Sie nach dem Erhalt Ihres SSL-Zertifikats die SSL-Zertifikat .cer-Datei an einem Speicherort auf CWMGR1 und folgen Sie den folgenden Schritten.

Installieren und Konfigurieren von CSR:

1. Stellen Sie eine Verbindung zu CWMGR1 her
2. Öffnen Sie IIS Manager über Administrator-Tools
3. Wählen Sie CWMGR1 und öffnen Sie 'SServer Certificates'
4. Klicken Sie im Bereich Aktionen auf Zertifikatanforderung abschließen

[]

5. Füllen Sie die folgenden Felder in der vollständigen Zertifikatanforderung aus, und klicken Sie auf OK:

[]

- a. Dateiname: Wählen Sie die zuvor gespeicherte .cer-Datei aus
- b. Anzeigename: *.domain.com
- c. Zertifikatspeicher: Wählen Sie entweder Webhosting oder Personal

SSL-Zertifikat wird zugewiesen:

1. Vergewissern Sie sich, dass der Migrationsmodus nicht aktiviert ist. Diese finden Sie auf der Seite Arbeitsbereichsübersicht unter Sicherheitseinstellungen in VDS.

[]

2. Stellen Sie eine Verbindung zu CWMGR1 her
3. Öffnen Sie IIS Manager über Administrator-Tools
4. Wählen Sie CWMGR1 und öffnen Sie 'SServer Certificates'
5. Klicken Sie im Aktionsbereich auf Exportieren
6. Exportieren Sie das Zertifikat im .pfx-Format
7. Erstellen Sie ein Passwort. Speichern Sie das Kennwort so, wie es benötigt wird, um die .pfx-Datei in Zukunft zu importieren oder erneut zu verwenden
8. Speichern Sie die .pfx-Datei im Verzeichnis C:\installiert\RDPcert
9. Klicken Sie auf OK, und schließen Sie IIS Manager

[]

10. Öffnen Sie DCConfig
11. Aktualisieren Sie unter Platzhalterzertifikat den Zertifikatspfad in die neue .pfx-Datei
12. Geben Sie bei der entsprechenden Aufforderung das .pfx-Passwort ein
13. Klicken Sie Auf Speichern

[]

14. Wenn das Zertifikat 30 Tage länger gültig ist, kann die Automatisierung das neue Zertifikat während der morgendlichen täglichen Aktionen während der Woche anwenden
15. Überprüfen Sie regelmäßig die Plattformserver, um zu überprüfen, ob das neue Zertifikat sich verbreitet hat. Benutzerbindung validieren und testen, um zu bestätigen
 - a. Wechseln Sie auf dem Server zu Admin Tools
 - b. Wählen Sie Remote Desktop Services > Remote Desktop Gateway Manager
 - c. Klicken Sie mit der rechten Maustaste auf den Namen des Gateway-Servers, und wählen Sie Eigenschaften. Klicken Sie auf die Registerkarte SSL-Zertifikat, um das Ablaufdatum zu überprüfen

□
16. Überprüfen Sie regelmäßig die Client-VMs, auf denen die Connection Broker-Rolle ausgeführt wird
 - a. Wechseln Sie zu Server Manager > Remote Desktop Services
 - b. Wählen Sie unter Bereitstellungsübersicht die Dropdown-Liste Aufgaben aus, und wählen Sie die Option Bereitstellungseigenschaften bearbeiten

□

 - c. Klicken Sie auf Zertifikate, wählen Sie Zertifikat aus und klicken Sie auf Details anzeigen. Das Ablaufdatum wird aufgelistet.

□

□
17. Wenn Sie weniger als 30 Tage oder lieber das neue Zertifikat sofort ausdrucken möchten, erzwingen Sie das Update mit TestVdcTools. Dies sollte während eines Wartungsfensters erfolgen, da die Verbindung für alle angemeldeten Benutzer unterbrochen wird und Ihre Verbindung zu CWMGR1 verloren geht.
 - a. Gehen Sie zu C:\Programme\CloudWorkspace\TestVdcTools, klicken Sie auf die Registerkarte Operationen und wählen Sie den Befehl Platzhalter Cert-Install aus
 - b. Lassen Sie das Serverfeld leer
 - c. Aktivieren Sie das Kontrollkästchen Kraft
 - d. Klicken Sie Auf Befehl Ausführen
 - e. Überprüfen Sie, ob Zertifikatpropagiert mit den oben aufgeführten Schritten ausgeführt wird

□

AVD-Rückführung

Überblick

In diesem Artikel werden das Entfernen von VDS und der NetApp Steuerung unter Beibehaltung des AVD-Benutzerzugriffs behandelt. Und in Zukunft wäre das Management mit nativen Azure/Windows-Administrationstools. Nach Abschluss dieses Vorgangs wird empfohlen, sich an support@spotpc.netapp.com zu wenden, damit NetApp unsere Back-End- und Billing-Systeme bereinigen kann.

Ausgangszustand

- AVD-Bereitstellung
- TDS1 ist FS Logix FileShare
- TS1 ist Session-Host
- Benutzer ist angemeldet und FS Logix-Datenträger wurde erstellt in:

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

CW Agent-Dienst löschen

Der CW-Agent wird auf allen Maschinen in der Umgebung ausgeführt. Der Dienst, der diesen Prozess startet, sollte mit dem folgenden Befehl für jede VM in der Umgebung deinstalliert werden. CWMGR1 kann übersprungen werden, da die VM heruntergefahren und schließlich in den meisten Fällen gelöscht wird. Im Idealfall würde diese Aktion über skriptbasierte Automatisierung ausgeführt. Das Video unten zeigt, dass es manuell gemacht wurde.

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

Löschen Sie das Video zum CW Agent-Dienst

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

Löschen Sie das CW-Agentenverzeichnis

Bei der vorherigen Deinstallation wurde der Dienst entfernt, der CW Agent startet, die Dateien aber verbleiben. Löschen Sie das Verzeichnis:

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

CW Agent-Verzeichnisvideo löschen

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

Entfernen Sie Startverknüpfungen

Das Verzeichnis der Startelemente enthält zwei Verknüpfungen zu Dateien, die im vorherigen Schritt gelöscht wurden. Um Fehlermeldungen für Endbenutzer zu vermeiden, sollten diese Dateien gelöscht werden.

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

Entfernen Sie Startverknüpfungen Video

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

Link 'Benutzer' und 'Unternehmen' GPOs aufheben

VDS implementiert drei Gruppenrichtlinienobjekte. Wir empfehlen die Verknüpfung von zwei von ihnen und die Überprüfung des Inhalts der dritten.

Link Aufheben:

- ADDC-Benutzer > Cloud Workspace-Unternehmen
- ADDC-Benutzer > Cloud Workspace-Benutzer

Durchsehen:

- ADDC-Computer > Cloud Workspace-Computer

Link 'Benutzer' und 'Unternehmen' GPOs-Video aufheben

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

Schalten Sie den CWMGR1 aus

Mit den vorgenommenen Änderungen am Gruppenrichtlinienobjekt können wir die CWMGR1 VM jetzt herunterfahren. Sobald die fortgesetzte AVD-Funktion bestätigt wurde, kann diese VM dauerhaft gelöscht werden.

In extrem seltenen Fällen muss diese VM gewartet werden, wenn eine andere Serverrolle läuft (z.B. DC, FTP-Server...). In diesem Fall können drei Dienste deaktiviert werden, um die VDS-Funktion auf CWMGR1 zu deaktivieren:

- CW-Agent (siehe oben)
- CW Automation Service
- CW VM Automation

CWMGR1-Video herunterfahren

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

Löschen von NetApp VDS-Servicekonten

Die von VDS verwendeten Azure AD-Servicekonten können entfernt werden. Melden Sie sich im Azure Management-Portal an und löschen Sie die Benutzer:

- CloudWorkSpaceSVC
- CloudWorkSpaceCASVC

Andere Benutzerkonten können beibehalten werden:

- Endanwender
- Azure-Administrator

- .Tech Domain-Administratoren

Video zum Löschen von VDS-Servicekonten für NetApp

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

App-Registrierungen löschen

Bei der Bereitstellung von VDS werden zwei App-Registrierungen durchgeführt. Diese können gelöscht werden:

- Cloud Workspace-API
- Cloud Workspace AVD

Video zum Löschen von App-Registrierungen

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

Unternehmensanwendungen löschen

Bei der Implementierung von VDS werden zwei Enterprise-Applikationen implementiert. Diese können gelöscht werden:

- Cloud Workspace
- Cloud Workspace Management-API

Video zu Unternehmensanwendungen löschen

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

Bestätigen Sie, dass CWMGR1 angehalten wurde

Bevor Sie testen, ob die Endbenutzer noch eine Verbindung herstellen können, bestätigen Sie, dass der CWMGR1 für einen realistischen Test angehalten wurde.

Bestätigen Sie, dass das Video „CWMGR1 wurde angehalten“ wurde

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

Anmeldung und Endbenutzer

Um den Erfolg zu bestätigen, melden Sie sich als Endbenutzer an und bestätigen Sie, dass die Funktionalität erhalten bleibt.

Anmeldung und Endbenutzervideo

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

Vereinfachtes

Implementierungen

Provisioning Collections

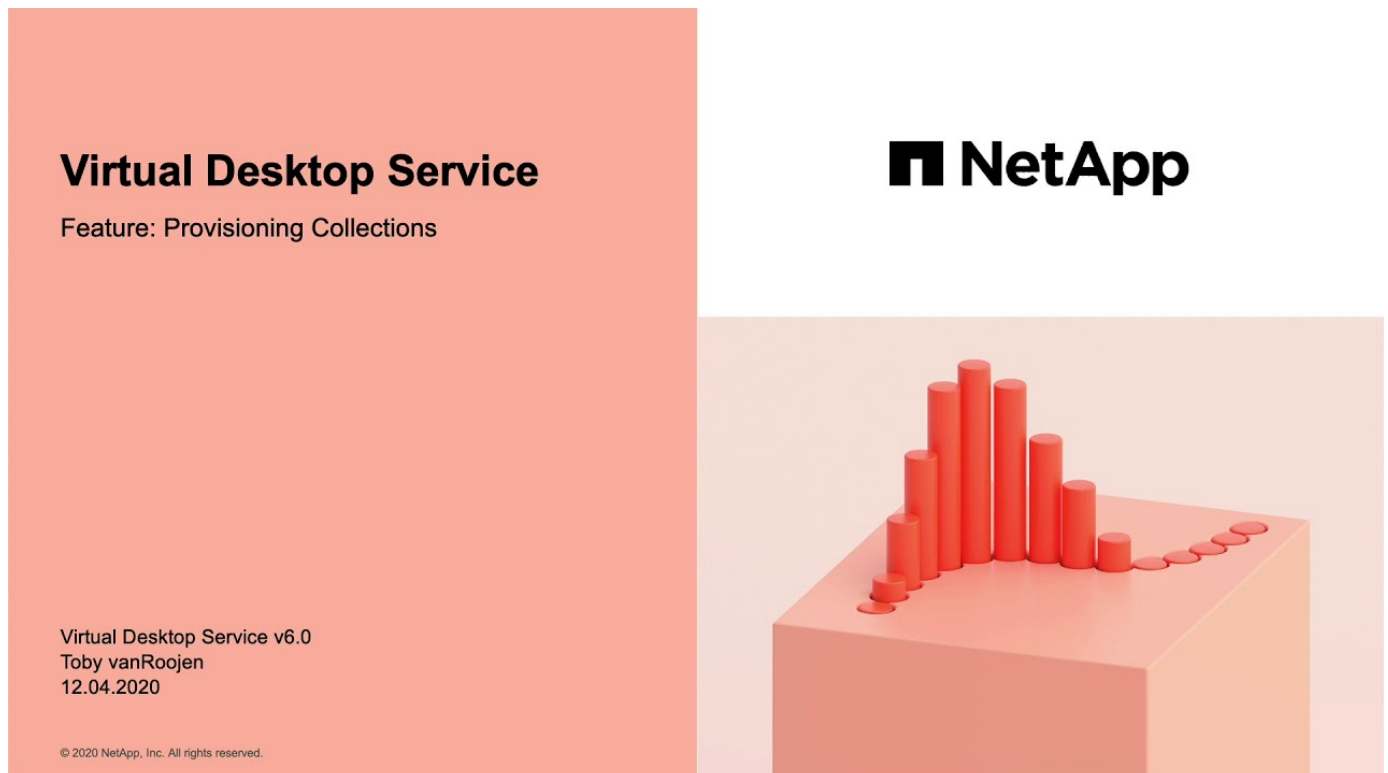
Überblick

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 Laufwerksbuchstaben, 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. **TSDaten** - Diese VM ist sowohl der Session-Host als auch der Speicher-Host (maximal: Ein TSDaten 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] |

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] |

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] |

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] |



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] |

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] |

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] |

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] |

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] |

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] |

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] |

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] |

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 komplizierteres 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] |

2. Klicken Sie in der App-Gruppe auf Bearbeiten

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

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] |

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] |

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] |

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] |

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] |

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 werden von jedem VDS-Administrator mit entsprechenden Administratorberechtigungen zum Abschnitt „skriptbasierte Ereignisse“ gelöscht und bearbeitet.

Globaler Filter

NetApp veröffentlicht zudem eine Bibliothek mit globalen Skripten, 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] |

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@loginIdentifizier 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] |

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] |

Aktivität Hinzufügen

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

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

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] |

- **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 Galerieübersicht kopieren

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

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] |

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] |



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] |

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 entschärft 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 Gerätespeicher 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 for Individual Users, MFA für einzelne Benutzer aktivieren
2. MFA for All Users, MFA für alle Benutzer erforderlich
3. MFA for Individual Administrators ,MFA für einzelne Administratoren aktivieren
4. User Initial Setup,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] |



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.

◦ TSDData

- 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
 TSDData: 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 'Sie 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.[]

Fehlerbehebung

Fehlerbehebung bei fehlgeschlagenen VDS-Aktionen

Überblick

Ein Großteil der Protokollierung, die in VDS stattfindet, ist in der Web-UI aufgrund des schieren Volumens nicht zugänglich. Detailliertere Protokolle finden Sie am Endpunkt. Diese Protokolle werden im Folgenden beschrieben.

In VDS v5.4+ werden die Protokolle im folgenden Ordnerpfad gefunden:

```
C:\programdata\cloudworkspace
```

In früheren VDS-Versionen können sie sich in den folgenden Pfaden befinden:

```
C:\Program Files\CloudWorkspace\  
C:\Program Files\CloudJumper\  
C:\Program Files\IndependenceIT\
```



Der Dateityp variiert auch nach VDS-Version. Protokolldateien sind entweder .txt- oder .log-Dateien, die in Unterordnern des oben beschriebenen Pfads gefunden werden.

Automatisierungsprotokolle

CW VM Automation Service-Protokoll

```
CwVmAutomationService.log
```

Der CW VM Automation Service ist ein Windows-Dienst, der für das Management aller virtuellen Maschinen in der Bereitstellung verantwortlich ist. Als Windows-Dienst wird er immer in einer Bereitstellung ausgeführt, hat aber zwei Hauptbetriebsarten: Den geplanten Task-Modus und den Ereignismodus.

Der geplante Task-Modus besteht aus Aktivitäten, die im Rahmen eines Zeitplans auf den VMs ausgeführt werden, einschließlich Erfassung von Sizing- und Performance-Daten, Neubooten von VMs, Einchecking-Status (ein oder aus) im Vergleich zu Regelsätzen, die durch die Funktionen „Workload Schedule“ und „Live Scaling“ generiert werden. Die Protokolle bezeichnen diese Aktionstypen in der 5. Spalte mit Namen wie „tägliche Aktionen“, „wöchentliche Aktionen“ und „tägliche Wartung“. Wenn Sie Fragen wie „Warum hat Server X Neustart letzte Nacht um 2:00 am“ oder „Warum ist dieser Server an, wenn ich denke, es sollte aus“ beheben, dann sind die geplanten Aufgaben für diese spezifischen VMs in der Regel der beste Ort, um zu schauen.

Der Ereignismodus wird aktiviert, wenn ein Benutzer oder ein anderer VDS-Dienst, wie z. B. der CW Automation Service, zur Fertigstellung einer Aufgabe auffordert. Beispiele für diese Art von Aktivität sind eine

Benutzeranfrage zum Erstellen eines neuen Servers oder CW Automation, in der die Größe und der Zustand der zu prüfenden Server angefordert werden, weil dem Arbeitsbereich weitere Benutzer hinzugefügt wurden. Diese Ereignisse haben in der Regel Protokolleinträge mit dem Ereignisnamen „Create Server“ und dem tatsächlichen Namen der VM direkt daneben (z. B. Server NXTS2 erstellen). Bei der Fehlerbehebung dieser Art von Ereignissen ist es normalerweise am besten, zum unteren Rand des Protokolls zu blättern und dann zur aufwärts Suche nach dem VM-Namen. Sie können dann weitere Zeilen nach oben scrollen, um zu sehen, wo der Prozess gestartet wurde.

CW Automation Service-Protokoll

`CWAutomationService.log`

Das CW Automation Service-Protokoll ist der primäre Windows-Service zur Verwaltung der Komponenten einer Workspace-Bereitstellung. Er führt die Aufgaben aus, die für das Management von Benutzern, Applikationen, Datengeräten und Richtlinien erforderlich sind. Darüber hinaus kann die IT Aufgaben für den CW VM Automation Service erstellen, wenn die Größe, Anzahl oder der Zustand der VMs in der Bereitstellung geändert werden müssen.

Wie der CW VM Automation Service führt der CW Automation-Service sowohl geplante Aufgaben als auch ereignisgesteuerte Aufgaben aus, wobei letzterer der häufigere Typ ist. Das Protokoll für den CW Automation Service beginnt jede Zeile mit der Einheit und Aktion, die bearbeitet wird (z. B. Start Server NXTS1). Die Suche nach dem Entity-Namen am unteren Rand der Datei ist der schnellste Weg, um die spezifischen Protokollzeilen zu finden, die für die Aufgabe gelten.

CW Agent Service-Protokoll

`CwAgent.log`

Der CW Agent Service führt alle Aufgaben aus, die lokal für eine bestimmte VM liegen, einschließlich der Prüfung der Ressourcenebenen und der Auslastung der VM, der Prüfung, ob die VM über ein gültiges Zertifikat für den TLS-Datenverkehr verfügt, und prüft, ob der obligatorische Neustart-Zeitraum erreicht ist. Neben der Überprüfung detaillierter Informationen zu diesen Aufgaben kann dieses Protokoll auch verwendet werden, um auf unerwartete VM-Neustarts oder unerwartete Netzwerk- oder Ressourcenaktivitäten zu prüfen.

CWManagerX-Protokoll

CWManagerX.log

CWManagerX ist ein Webservice, der die Kommunikationsverbindung zwischen der lokalen Bereitstellung und der globalen VDS-Kontrollebene bereitstellt. Aufgaben und Datenanfragen, die aus der VDS-Webanwendung oder der VDS-API stammen, werden über diesen Webdienst an die lokale Bereitstellung übermittelt. Von dort aus werden die Aufgaben und Anforderungen an den entsprechenden Webservice (oben beschrieben) oder in seltenen Fällen direkt an Active Directory weitergeleitet. Da es sich dabei meist um eine Kommunikationsverbindung handelt, gibt es bei normaler Kommunikation nicht viel Protokollierung, aber dieses Protokoll enthält Fehler, wenn die Kommunikationsverbindung unterbrochen oder falsch ausgeführt wird.

DC-Konfigurationsprotokoll

DCConfig.log

Bei DC Config handelt es sich um eine Windows-Anwendung, die bestimmte Konfigurationsparameter bereitstellt, die nicht in der VDS-Webanwendungsoberfläche verfügbar sind. Im Protokoll DC Config werden die Aktivitäten aufgeführt, die ausgeführt werden, wenn Konfigurationsänderungen in DC Config vorgenommen werden.

CAVDCDeployment-Protokoll

CAVDCDeployment.log

CW VDC Deployment ist eine Windows-Anwendung, die die für die Erstellung einer Implementierung in Azure erforderlichen Aufgaben ausführt. Das Protokoll verfolgt die Konfiguration der Windows-Services des Cloud Workspace, der Standard-GPOs sowie Routing- und Ressourcenregeln.

Verschiedene Protokolle

CwVmAutomationService-Installing.log

CwAgent-Installing.log

Die verbleibenden Protokolle verfolgen die Installation der oben beschriebenen Windows-Dienste und -Anwendung. Da VDS-Dienste automatisch aktualisieren, wenn eine neue Version für diese spezifische Bereitstellung bestimmt ist, verfolgen diese Protokolle den Upgrade-Prozess, da der Service oder die Anwendung während des Upgrades normalerweise deaktiviert werden müssen. Wenn Sie feststellen, dass die Dienste ständig gestoppt werden, können diese Protokolle helfen festzustellen, ob ein Upgrade auf einen bestimmten Service die Ursache ist. In diesen Fällen würde es erwarten, dass ein Fehler in diesen Protokollen angezeigt wird, in denen erläutert wird, warum das Upgrade fehlgeschlagen ist.

Zugriff auf Protokolle und Überprüfung von Informationen

+[]

1. VDS speichert ausführliche Protokolle und stellt einige von ihnen im Abschnitt „Aufgabenverlauf“ der Seite „Bereitstellungen“ im VDS bereit. Klicken Sie auf Ansicht, um Details zu den aufgeführten Aufgaben anzuzeigen.

[]

2. Manchmal enthält der Aufgabenverlauf nicht genügend Details, um die wahre Ursache zu identifizieren. Um den Bereich Task History nutzbar zu halten und nicht von allen protokollierten Ereignissen überfordert zu werden, wird hier nur eine Teilmenge an Aufgabebereitstellungen dargestellt. Für einen tieferen Einblick in die oben genannten Text-Log-Dateien können weitere Details bereitgestellt werden.

- a. Um auf dieses Protokoll zuzugreifen, navigieren Sie zum Abschnitt Bereitstellungen und klicken Sie auf das Zahnradsymbol neben der CWMGR1-VM, und klicken Sie dann auf Verbinden (oder stellen Sie im Fall des CwAgent-Protokolls eine Verbindung zur entsprechenden VM her).

[]

3. Bei der Verbindung zu einem Platform Sever (wie dem CWMGR1) werden Sie nicht automatisch beim Server angemeldet (im Gegensatz zur Verbindung mit einem Server im Mandanten). Sie müssen sich mit einem Level3 .tech-Konto anmelden.

[]

4. Navigieren Sie dann wie oben gezeigt zum Pfad und öffnen Sie die Protokolldatei.

[]

5. Diese Textdatei enthält ein Protokoll aller Ereignisse, das älteste der neuesten Ereignisse ist:

[]

6. Beim Öffnen eines Support-Cases mit NetApp VDS wird die Möglichkeit, die hier gefundenen Fehler bereitzustellen, DIE Beschleunigung der Problemlösung DEUTLICH beschleunigen.

Fehlerbehebung In Bezug Auf Die Qualität Der Internetverbindung

Symptome

Wenn Benutzerverbindungen getrennt werden müssen, muss eine Verbindung wiederhergestellt werden. Laggy Interface Antwort, allgemeine Performance-Probleme, die nicht scheinen, mit Ressource (RAM/CPU) Lasten zusammenhängen.

Ursache

Wenn Benutzer Performance-Probleme melden, Benutzerverbindungen fallen gelassen oder eine laggy Schnittstelle, die häufigste Ursache sind nicht Ressourcen überhaupt, sondern die Netzwerkverbindungen zwischen dem Kunden und dem Rechenzentrum. Diese Verbindungen laufen über ihren ISP, verschiedene Internet-Backbone-Betreiber und schließlich in das Rechenzentrum. Dabei werden die Daten durch mehrere Zwischenstopps geleitet. Jeder dieser Hops kann zu Netzwerklatenz, verlorenen Paketen und Jitter führen, die

alle zur wahrgenommenen Performance der Desktop Computing-Umgebung auf dem virtuellen Desktop beitragen können.

Tier 1-Triage und Fehlerbehebung enthalten grundlegende Schritte wie die Bestätigung von Ressourcen (RAM, CPU und HDD-Platz) ausreichend sind. Sobald der Vorgang abgeschlossen ist, ist das Testen der Netzwerkkonnektivität ein großer nächster Schritt bei der Fehlerbehebung. Auflösung

Primäre Option: Der NetApp VDS Windows-Client verfügt über integrierte Diagnosetools

Der Diagnosetest kann innerhalb des Virtual Desktop Client ausgeführt und an Ihre E-Mail gesendet werden.

1. Klicken Sie auf das Voreinstellung-Symbol (vier horizontale Linien in der oberen Menüleiste).
2. Klicken Sie Auf Hilfe
3. Klicken Sie Auf Netzwerk-Test
4. Geben Sie den Benutzernamen ein, bei dem die Probleme auftreten, und klicken Sie auf Ausführen
5. Geben Sie nach Abschluss Ihre E-Mail-Adresse ein, um einen E-Mail-Bericht zu erhalten
6. Lesen Sie den Bericht, um mögliche Verbindungsprobleme zu beheben

[]

[]

Sekundäre Option: Manuelle Analyse mit PingPlotter

Um zu bestätigen, dass die Netzwerkverbindung des Clients die Ursache ist, können Sie das kostenlose Dienstprogramm PingPlotter ausführen. Dieses Dienstprogramm sendet alle paar Sekunden einen Ping und berichtet über die Geschwindigkeit (Latenz) der Umrundung dieses Ping. Es notiert auch den Paketverlust (PL) Prozentsatz an jedem Hop entlang der Route. Wenn eine hohe Latenz und/oder ein hoher Paketverlust beobachtet wird, ist es ein guter Hinweis darauf, dass die Leistungsprobleme durch die Qualität der Internetverbindung am Hop verursacht werden, die diese Probleme zeigt.

1. Herunterladen und installieren "[Ping-Plotter](#)" (Verfügbar für MacOS, Windows und iOS).
2. Geben Sie das Gateway des Datacenters ein, in dem der Mandant bereitgestellt wird.
3. Lassen Sie es mehrere Minuten laufen. Idealerweise, während Performance-Probleme oder Distimmigungen auftreten.
4. Erfassen Sie die Daten mit „Bild speichern...“ Über das Menü Datei, wenn es für eine zusätzliche Fehlerbehebung benötigt wird.

Desktop-Hintergrund für Benutzersitzungen aktivieren

Überblick

Bei Remote-Sitzungen ist die Hintergrundanzeige standardmäßig deaktiviert, um die Leistung zu verbessern. Das Ergebnis ist ein schwarzes Hintergrundbild, das Benutzer oft anpassen möchten. Diese Einstellung kann mit einer einfachen GPO-Bearbeitung geändert werden

Wichtig:

1. Melden Sie sich bei einem Plattform-Server an (z. B. CWMGR1) Verwendung von Level3 .tech-Konto

2. Öffnen Sie Die Group Policy Management Console
3. Suchen Sie das GPO rdsh (gekennzeichnet als „Unternehmenscode“ rdsh (z. B. „Xyz1 rdsh“)) Klicken Sie mit der rechten Maustaste auf das GPO „xyz1 rdsh“, wählen Sie „Bearbeiten“
 - a. In Azure AD-Domänendiensten wird das GPO „ADDC“ genannt „Computer > Cloud Workspace-Computer“.
4. Ändern Sie die Richtlinie: Computerkonfiguration > Richtlinien > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remote Desktop Session Host > Remote Session Environment > Remote Desktop Wallpaper entfernen. Setzen Sie diese Einstellung auf deaktiviert

□ □ □

Fehlerbehebung Beim Drucken Von Problemen

Fehler

Das Drucken auf dem lokalen Drucker über den Cloud-Desktop funktioniert nicht.

Remote Desktop Services mit ThinPrint

VDS umfasst optional ThinPrint für RDS-Implementierungen (Remote Desktop Services). Die Software und die Lizenzierung werden bei der ersten Implementierung automatisch konfiguriert. Wenn ThinPrint in Gebrauch ist, können die folgenden Abschnitte die Fehlerbehebung bei Problemen mit dem Drucken erleichtern.

Ursache

Es gibt verschiedene Methoden zur Verbindung mit dem Cloud-Desktop. Diese Methode unterscheidet sich in der Ausführung von Druckfunktionen und damit in der Gewissheit, welche Art von Zugriff für die Fehlersuche benötigt wird:

1. Verwenden des Access-Client von CloudJumper auf einem Windows-Gerät
 - a. ThinPrint wird auf dem lokalen Gerät ausgeführt und leitet die Kommunikation zwischen dem Drucker und dem Cloud-Desktop weiter
2. Verwenden des HTML5-Browsers auf jedem Gerät
 - a. Der Browser zeigt das gedruckte Dokument als PDF an, um lokal herunterzuladen und zu drucken
3. Verwenden eines manuell konfigurierten RDP-Clients (normalerweise) auf einem Mac oder Linux-Computer
 - a. Lokale Drucker werden mit dem Cloud-Desktop freigegeben, indem sie „Lokale Ressourcen“ im RDP-Client manuell konfigurieren.

Auflösung

1. Versuchen Sie, ein Dokument vom lokalen Gerät zu drucken, um zu bestätigen, dass das lokale Gerät erfolgreich eine Verbindung zum Drucker herstellt.
2. Deinstallieren Sie ThinPrint, und installieren Sie es erneut, wenn Sie den Access Client auf einem Windows-Gerät verwenden. <https://www.thinprint.com/en/resources-support/software/clientsandtools/>
3. Notieren Sie sich den Zugriffstyp und die Ergebnisse der ersten beiden Schritte in einem neuen Fall mit CloudJumper Support.

Azure Virtual Desktop

VDS implementiert keine Drucklösung oder spezielle Druckkonfiguration für AVD-Umgebungen. Fragen zum Drucken sollten an Microsoft oder (wenn eine implementiert wurde) an den Hersteller der Drucktechnologie gerichtet werden.

Azure vCPU Kernquote

Aktuelle Quote Anzeigen

1. Melden Sie sich bei der Azure Konsole an, navigieren Sie zum Modul „Abonnements“ und klicken Sie auf „Quoten“. Wählen Sie dann im Dropdown-Menü Provider alle Provider aus, wählen Sie im Dropdown-Menü „Alle anzeigen“ aus und wählen Sie die Azure-Region aus, in der Ihr Cloud Workspace bereitgestellt wird.

□

2. Dann werden Sie sehen, wie viel Sie verbrauchen gegen Wie viel Kontingent haben Sie verfügbar. In der nachstehenden Abbildung verbraucht CloudJumper 42 CPUs von den 350 CPUs, die für die BS-Produktfamilie von VMs verfügbar sind. Steigende Kontingente

□

3. Wenn Sie Ihre Quote erhöhen möchten, klicken Sie auf Anfrage steigern und sagen Sie es, was Sie erhöhen möchten (99% der Zeit wird dies Compute/CPUs sein).

□

4. Wählen Sie die Region aus, in der Ihr Cloud Workspace bereitgestellt wird, und die VM-Familie, für die Sie die Quote erhöhen möchten.

□

5. Geben Sie Ihre Kontaktinformationen ein und klicken Sie auf Erstellen, um die Anfrage an Microsoft zu übermitteln. In der Regel erhöhen sie das sehr schnell.

Entsperren Von Benutzerkonten

Überblick

Das Entsperren eines gesperrten Kontos für einen Endbenutzer ist ein einfacher Prozess, der ein mittelmäßig häufiges Problem behebt, das Endbenutzer berichten.

Nach vier fehlgeschlagenen Anmeldeversuchen wird der Benutzer gesperrt. Die Dauer beträgt 30 Minuten, es sei denn, das Konto hat die Passwortkomplexität aktiviert, in diesem Fall kann die Sperrung nur manuell durchgeführt werden.

Das Benutzerkonto kann in der Liste der Benutzer auf der Seite Benutzer und Gruppen in den Arbeitsbereichen oder auf der Seite Benutzerdetails entsperrt werden.

Seite „Benutzer Und Gruppen“

□ □



Fehlerbehebung Bei Der Leistung Von Virtuellen Maschinen

NetApp bietet Kunden Einblick in die Fehlerbehebung bei der Server-Performance für Benutzer/Applikationen. Alle Unternehmen nutzen Ressourcen anders, je nachdem, wie viele Endanwender sich gleichzeitig angemeldet haben: Nutzung von Applikationen, falls SQL Standard installiert ist oder nicht SQL Express usw. Es ist also wichtig, die Vorgänge zu überprüfen, wenn ein Benutzer Performance-Probleme meldet.

Überblick

Jede App ist anders, und selbst die gleiche Software, die von der gleichen Anzahl von Benutzern ausgeführt wird, kann verschiedene Ressourcenverbrauchsmuster haben. Aus diesem Grund hilft es, die Anwendungen zu verstehen, die Ihre Benutzer verwenden und was wirklich die Macht der App. Handelt es sich um CPU, RAM oder Storage? Diese Überlegungen helfen Ihnen bei der Fehlerbehebung.

Nach unserer Erfahrung haben sich diese als allgemein wahrhaftige Aussagen erwiesen, die Ihnen helfen, zu beginnen:

CPU: this is usually the culprit/limiting factor if the app in question is home-grown and/or an Excel issue
RAM: this is usually the culprit/limiting factor if SQL Standard is used
Storage: this is usually a contributing factor if disk consumption is greater than 90%.



Wenn SQL Express verwendet wird, ist es wahrscheinlich ein einschränkender Faktor – es begrenzt den RAM-Verbrauch auf 1 GB, die unter den erforderlichen Spezifikationen des Software-Anbieters sein kann.

In nächtlichen Ressourcenberichten

VDS sendet nächtliche Berichte mit Informationen über jede VM. Dieser Bericht enthält viele nützliche Informationen, darunter Empfehlungen, ob Ressourcen erhöht oder verringert werden sollen. Hier einige Auszüge:

Dieses Bild zeigt, ob Sie CPU/RAM auf VMs für einen bestimmten Arbeitsbereich erhöhen oder verringern sollten.[]

In der Abbildung unten sehen wir, dass es eine Spalte gibt, die zeigt, wie lange der Server seit dem Neustart des Servers vergangen ist.[]

In diesem Image sehen wir einen Vergleich zwischen Storage Provisioning und Verbraucht – Dies wird zu einem guten Thema, um kurz zu untersuchen auf den ersten oder sobald Sie bestätigt haben, dass CPU/RAM nicht das Problem sind.[]

Anzeige des CPU-/RAM-Ressourcenverbrauchs in Echtzeit

1. Melden Sie sich beim VDS an, klicken Sie dann auf das Organisationsmodul und wählen Sie die

gewünschte Organisation aus.

[]

2. Sie können den Server finden, an dem der Benutzer angemeldet ist, indem Sie ihn im Abschnitt Benutzer suchen.

[]

3. Blättern Sie dann nach unten, bis Sie den Abschnitt „Server“ sehen. Suchen Sie den Server, auf dem der Benutzer, der das Problem meldet, angemeldet ist, und klicken Sie auf das Einstellrad, und stellen Sie dann eine Verbindung her.

[]

4. Wenn Sie eine Verbindung zum Server hergestellt haben, klicken Sie auf die Schaltfläche Start. Klicken Sie dann auf Task-Manager.

[]

5. Der Task-Manager gibt Ihnen einen umfassenden Einblick in das Geschehen, genau in diesem Moment. Dies ist der absolut beste Weg, um zu sehen, was Ihre Benutzer im Moment beeinflussen sie ein Problem an Sie melden.
6. Sie können die auf dem Server ausgeführten Prozesse überprüfen, ermitteln, welche Ursache das Problem hat und entweder mit dem Kunden kommunizieren oder die Prozesse vor Ort beenden.

[]

7. Sie können auch die Registerkarte Performance anzeigen, um zu zeigen, was passiert, live. Dies ist ein gewaltiger Schritt zur Fehlerbehebung: Die Endbenutzer müssen die Schritte wiederholen, die sie unternommen haben, um ein Performance-Problem zu verursachen, und dann sehen, was passiert. Ähnlich, wenn sie folgen allgemeinen Rat (schließen Sie überschüssigen Chrome-Browser-Tabs, wie Google Chrome Tabs sind eine gemeinsame Ressource Verbraucher) können Sie sehen Ressourcenverbrauch Rückgang.

[]

8. Auf der Registerkarte „Benutzer“ können Sie anzeigen, welcher Benutzer – falls überhaupt – die Ressourcen verbraucht, was zu einer Spitzenauslastung führt.

[]

9. Sie können jeden Endbenutzer erweitern, um zu sehen, welche spezifischen Prozesse sie laufen und wie viel jeder verbraucht.

[]

10. Eine weitere Option ist die Anzeige, welche Dienste ausgeführt werden.

[]

11. Kunden können den Ressourcenmonitor auch öffnen, um weitere Einzelheiten zu erfahren.

[]

Erwägen Storage-PerformAkne

Einer der häufigsten Ursachen für Performance-Probleme mit vms ist die unzureichende Performance von Festplatten. Standard- (und sogar SSD-Festplatten) sind nicht für die hohe I/O-Last ausgelegt, die für VDS Workloads erforderlich ist. Benutzer-Logins erfolgen in der Regel in Bündel und jeder erfordert erhebliche I/O, da Profile und Einstellungen geladen werden. Die hochperformanten Storage-Technologien von NetApp wie Azure NetApp Files, CVO und CVS eignen sich besonders gut für diesen Workload und sollten als Standardoption für VDS-Workloads angesehen werden.

Berücksichtigung des Storage-Verbrauchs

Microsoft gilt seit langem als Best Practice, beim Festplattenverbrauch jedes Laufwerks mindestens 90 % zu zulässt. Dies führt in ihren Augen zu einem Performance-Einbußen und kann zu weiteren Herausforderungen führen. Beispielsweise fehlt es an genügend Storage für Backups, sodass Benutzer nicht mehr arbeiten können.

RMM-Tools können Speicher-Monitoring-Services anbieten, einschließlich der Möglichkeit, Schwellenwerte und Warnmeldungen festzulegen. Wenn der Speicher zu einer Herausforderung für Sie wird, empfiehlt es sich, diese Art von Warnmeldungen mit Ihrem RMM-Anbieter zu aktivieren.

Zur tieferen Untersuchung installieren Sie Software, um den Laufwerkverbrauch zu überprüfen.

Aus Gesprächen mit Kunden haben sich WinDirStat oder TreeSize als bevorzugte Anwendungen für die Kontrolle des Antriebsverbrauchs erwiesen.

WinDirStat kann eine vollständige Festplatte über das Netzwerk untersuchen, wenn nicht genügend Speicherplatz vorhanden ist, um eine App lokal zu installieren/auszuführen oder die Anmeldung blockiert ist:

+[]

DNS leitet für Azure FÜGT & SSO über O365-Identität weiter

Überblick

Benutzer können nicht auf Firmen-Websites auf primären E-Mail-Domain zugreifen.

Zum Beispiel können NetApp Mitarbeiter in VDS-Arbeitsbereichen nicht auf netapp.com zugreifen, wenn ihr SSO-Konto user@netapp.com ist

Dedizierte VDS-Implementierungen nutzen die interne Domäne des Azure-Mandanten.

Auflösung

Um dies zu lösen, muss das Team des Unternehmens, das DNS verwaltet, eine DNS-Suchzone für Ihre interne Domäne erstellen, damit sie die richtige externe IP-Adresse auflösen kann (um NetApp zu diesem Zweck NetApp Mitarbeiter innerhalb ihres virtuellen Desktops auf netapp.com durchsuchen zu können).

Schritt für Schritt

1. Installieren Sie die DNS-Server-Tools auf CWMGR1 – damit können Sie DNS verwalten.

[]

[]
[]
[]
[]

2. Nach der Installation können Sie zu Systemsteuerung → System und Sicherheit → Verwaltung Tools gehen und DNS öffnen.

[]

3. Wenn Sie nach dem DNS-Server gefragt werden, auf dem DNS ausgeführt wird, möchten Sie Ihren Domainnamen eingeben (in dem Beispiel, das wir verwendet haben, wäre dies *netapp.com*).

Fehlerbehebung Bei Applikationsproblemen

Überblick

Fehlerbehebung bei einem Anwendungsfehler ist eine gängige administrative Praxis, die nicht VDS selbst beinhaltet, aber wird stark unterstützt durch VDS und die Kontrolle, die es Administratoren bietet. Da NetApp VDS keine Fehlerbehebung für diese Probleme bei den Kunden übernimmt, können wir anhand unserer Erfahrungen Administratoren Ratschläge geben, nachdem wir einige grundlegende Informationen wie die folgenden ermittelt haben, um sich ausführlicher mit den Endbenutzern und/oder Drittanbietern zu beschäftigen.

- Name des Benutzers, der das Problem auftritt
- Name der Anwendung, mit der der Benutzer arbeitete
- Der Server, auf dem die Benutzersitzung war
- Schritte zur Reproduktion des Problems

Überprüfen Ihrer Tools

Monitoring

Nachdem Sie den Server identifiziert haben, den der Benutzer verwendet hat, überprüfen Sie Ihre Überwachungslösung, um zu überprüfen, ob der Ressourcenverbrauch (CPU und RAM) im normalen Bereich liegt. Sie können auch validieren, dass anwendungsspezifische Anforderungen (ein besonderer Service, der Probleme verursachen wird, wenn es nicht läuft) sind funktionsfähig. In solchen Situationen können erweiterte Einstellungen wie die Überwachung der oben/unten genannten Dienste ausgelöst worden sein.

Virenschutz

Als Administrator mit Zugriff auf die Server und auf Azure Active Directory können Sie die erkannten Daten und die festgelegten Richtlinien überprüfen. Sollte ein unvorhergesehener Vorfall vorhanden sein, kann es zu Auswirkungen auf Ihre Applikation kommen.

Weitere Tools

Einige Anwendungen erfordern zusätzliche Komponenten, wie z. B. ein Servicekonto, das unbestimmte Zeit angemeldet bleibt, oder ein VPN an eine physische Ausrüstung (z. B. eine Netzwerk-Appliance vor Ort oder

ein Gerät der Fertigungsausrüstung oder Diagnoseprogramm). In diesen Fällen können anwendungsspezifische Fehler durch eine andere Ursache als die Installation der Anwendung oder die Konfiguration der Einstellungen verursacht werden.

Erweiterung des Zugriffs auf Dritte

Anwendungen und/oder deren Datenbanken werden häufig von dem Softwareanbieter (ISV) selbst oder einem Drittanbieter installiert, konfiguriert und unterstützt. In diesen Situationen möchten Sie den temporären Administratorzugriff auf folgende Schritte ausweiten: ["Bereitstellen von zeitweiligen Zugangs zu Dritten"](#)

Als Best Practice empfiehlt es sich, diese Konten von Dritten nach Abschluss des Upgrades oder Updates oder nach Behebung des Problems herunterzufahren.

In vielen Fällen erfordert ein Software-Wartungsvertrag mit dem ISV, um eine solche Fehlerbehebung durchzuführen. Falls dies nicht der Fall ist, kann Ihnen der ISV dieses Problem möglicherweise erst unterstützen, wenn er vorhanden ist.



Möglicherweise besteht auch darin, dass das Problem der Fehlerbehebung auf die Hardware (Desktops, Laptops, Thin Clients usw.) zurückzuführen ist, mit der die Endbenutzer arbeiten. Ein Beispiel könnte sein, dass ein Upgrade des Laptops eines Benutzers könnte die Maschine in den Augen einer dünnen Client-Konfigurationsdatei sperren, was bedeutet, dass die Endbenutzer nicht auf die Tools zugreifen können, die ihnen erlauben, sich an ihrem virtuellen Desktop anzumelden. In diesem Fall kann ein Wartungsvertrag für Hardware erforderlich sein, bevor der Hersteller Ihnen behilflich sein wird.

Referenz

Versionshinweise

Virtual Desktop Service – v6.0 Versionshinweise

VDS v6 Veröffentlichung: Donnerstag 17. November 2020 um 23 Uhr Ost

Auswirkung: Benutzer werden das VDS Client für Windows Update beim nächsten Start sehen

Verbesserungen

- Korrigieren Sie bei der Erstellung von Client-Verbindungsdateien ein Syntaxproblem mit dem Parameter 'Umleitungsservername verwenden'. Für VDS-Client verwendetes Aktualisierungs-Code-Signierungszertifikat

VDS v6-Veröffentlichung: Donnerstag, Oktober 6, 2022

Komponenten: Virtual Desktop Service v6 *Wann:* 10pm - 11pm Eastern *Auswirkungen:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Jährliche Schlüsselrotation der Performance-Datenautomatisierung
- In diesem Release-Zyklus wurden die jährlichen Rotationen von automatisierten Access Tokens für den VDS-Performance-Datenservice von Cloud Insights verwendet. Diese Änderung hatte keine wesentlichen Auswirkungen auf den Endbenutzer oder den Administratorzugriff in der VDS-Webanwendung.
- FsLogix Verkürzung der Container-Aktion aus täglichen Aktionen entfernt
- Die FsLogix Verkürzung Container-Aktion läuft jetzt nur wöchentlich, normalerweise Sonntag 12:01 Uhr Ortszeit
- Fehler behoben – Duplizieren von Namensreferenzen in der VDS-Servertabelle hat zu Fehlern bei täglichen Aktionen geführt
- DIE VDS-Automatisierung verarbeitet jetzt tägliche Aktionen einmal für den Servernamen korrekt und verhindert so den Fehler, der die Verarbeitung nicht mehr abhält.
- VDS Web Application (Versionen vor v6) – Entfernen Data Center Option Löschen für nicht autorisierte Admin-Konten
- Diese Änderung erfordert Bearbeitungsberechtigung auf Datacenter-Ebene und entfernt die Löschoption für alle anderen Admin-Benutzerkonten.
- UI Enhancement: Bestätigungsdialogfeld hinzufügen beim Löschen von AVD-Hostpool-Objekten
- Fehler behoben: Fehler beim Hochladen von Protokolldaten aus Bereitstellungen in einigen Szenarien
- Funktion: Unterstützung der lokalen Kontrollebene für vCloud Director REST API v35

VDS v6 Release: Donnerstag, September 22, 2022

Komponenten: Virtual Desktop Service v6 *Wann:* 10pm - 11pm Eastern *Auswirkungen:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Fehler behoben – Beheben von Kantenfällen beim Verkleinern von FSLogix-Profilcontainern
- VDS verkleinert jetzt mithilfe von Azure Files Storage die Profilcontainer in Workspaces richtig

VDS v6 Release: Fr., Sept. 9, 2022

Komponenten: Virtual Desktop Service v6 *Wann:* 10pm - 11pm Eastern *Auswirkungen:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Fehler behoben: FSLogix-Profilshrumpfbild funktioniert nicht in Randfällen
- In bestimmten seltenen Workspace-/Verzeichniskonfigurationen konnte die FSLogix-Profilcontainer die Schrumpfautomatisierung im VDS nicht ordnungsgemäß ausführen
- Funktion: Automatische Konfiguration neuer CI-Mandanten für Implementierungen
- VDS implementiert nun automatisch neue/aktualisierte Cloud Insights-Kontoinformationen für Mandantenressourcen und macht manuelle Konfigurationsschritte überflüssig

VDS v6 Veröffentlichung: Donnerstag, August 25, 2022

Komponenten: Virtual Desktop Service v6 *Wann:* 10pm - 11pm Eastern *Auswirkungen:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Fehler behoben: Option zum Deaktivieren des Administratorzugriffs für einen Workspace-Benutzer fehlt
- VDS zeigt jetzt eine Option zum Deaktivieren des Administratorzugriffs für einen Workspace-Benutzer an, der zuvor Zugriff auf die Verwaltung des Arbeitsbereichs erhalten hat
- Fehler behoben – App-Gruppe kann nicht zum AVD-Hostpool hinzugefügt werden
- VDS ist jetzt in der richtigen Handhabung von Randfällen, bei denen ein AVD-Host-Pool und ein Arbeitsbereich nicht richtig aufeinander abgestimmt sind

VDS v6 Veröffentlichung: Donnerstag, August 11, 2022

Komponenten: Virtual Desktop Service v6 *Wann:* 10pm - 11pm Eastern *Auswirkungen:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Keine Updates

VDS v6 Veröffentlichung: Donnerstag, Juli 28, 2022

Komponenten: Virtual Desktop Service v6 *Wann:* 10pm - 11pm Eastern *Auswirkungen:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Entfernen Sie den Link 'reRegistrierung für Sandbox' von der VDS-Anmeldeseite

VDS v6 Veröffentlichung: Donnerstag, Juli 14, 2022

Komponenten: Virtual Desktop Service v6 *Wann:* 10pm - 11pm Eastern *Auswirkungen:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Funktion - Neue optionale Einstellung zum Konfigurieren von Aufbewahrungszeitraum für die Anmelde-Tracker-Tabelle für Benutzeraktivitäten
- VDS ermöglicht jetzt die Konfiguration in lokalen Steuerebenen-Komponenten, um die Aufbewahrungsdauer der Benutzeraktivitätsprotokollierung unabhängig von anderen Protokollen zu steuern
- Feature: Stellen Sie AVD-Sitzungshosts so ein, dass die Hybrid-Lizenzeinstellung standardmäßig verwendet wird
- VDS erstellt jetzt neue AVD-Session-Hosts mit der 'Hybrid Licensing'-Einstellung standardmäßig

VDS v6 Release: Donnerstag, Jun. 23, 2022

Komponenten: Virtual Desktop Service v6 *Wann:* 10pm - 11pm Eastern *Auswirkungen:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Fehler behoben: Fehler in VDS Web App beim Ändern eines skriptbasierten Ereignisses
- VDS behandelt nun bei der Bearbeitung von skriptbasierten Ereignisobjekten ein Problem mit der Groß- und Kleinschreibung korrekt

VDS v6 Release: Donnerstag, Jun. 9, 2022

Komponenten: Virtual Desktop Service v6 *Wann:* 10pm - 11pm Eastern *Auswirkungen:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Keine Updates

VDS v6-Veröffentlichung: Donnerstag, 26. Mai 2022

Komponenten: Virtual Desktop Service v6 *Wann:* 10pm - 11pm Eastern *Auswirkungen:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Keine Updates

VDS v6-Veröffentlichung: Donnerstag, 12. Mai 2022

Komponenten: Virtual Desktop Service v6 *Wann:* 10pm - 11pm Eastern *Auswirkungen:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Keine Updates

VDS v6 Release: Mon., 2. Mai 2022

Komponenten: Virtual Desktop Service v6 *Wann:* 10pm - 11pm Eastern *Auswirkungen:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Keine Updates

VDS v6 Release: Donnerstag, April 28, 2022

Components: Virtual Desktop Service v6 *Wann:* Donnerstag, der 28. April 2022 um 22:00 Uhr bis 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Verschiedene proaktive Verbesserungen und Fehlerbehebungen

VDS v6 Release: Donnerstag, April 14, 2022

Components: Virtual Desktop Service v6 *Wann:* Donnerstag, der 14. April 2022 um 22:00 - 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Verschiedene proaktive Verbesserungen und Fehlerbehebungen

VDS v6 Release: Donnerstag, März 31, 2022

Components: Virtual Desktop Service v6 *When:* Donnerstag, 31. März 2022 um 22 Uhr - 23 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Verschiedene proaktive Verbesserungen und Fehlerbehebungen

VDS v6 Release: Donnerstag, März 17, 2022

Components: Virtual Desktop Service v6 *Wann:* Donnerstag, der 17. März 2022 um 22:00 Uhr bis 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Verschiedene proaktive Verbesserungen und Fehlerbehebungen

VDS v6 Release: Donnerstag, März 3, 2022

Components: Virtual Desktop Service v6 *Wann:* Donnerstag, der 3. März 2022 um 22:00 Uhr bis 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Verbesserte Erfahrung beim Trennen von einem Server nach Verwendung der Verbindung mit dem Server-Funktion
- Verschiedene proaktive Verbesserungen und Fehlerbehebungen

VDS v6 Veröffentlichung: Donnerstag, 17. Februar 2022

Components: Virtual Desktop Service v6 *Wann:* Donnerstag, der 17. Februar 2022 um 22:00 - 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Einführung von Anwendungsinstanzen, die ein verbessertes Management verschiedener Versionen und Editionen derselben Software ermöglichen
- Verschiedene proaktive Verbesserungen und Fehlerbehebungen

VDS v6-Veröffentlichung: Donnerstag, 3. Februar 2022

Components: Virtual Desktop Service v6 *Wann:* Donnerstag, der 3. Februar 2022 von 10.00 bis 23 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Verbesserung der Profilroaming-Suche für VDMS
- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen

VDS v6 Veröffentlichung: Donnerstag, der 20. Januar 2022

Components: Virtual Desktop Service v6 *Wann:* Donnerstag, 20. Januar 2022 von 22 bis 23 Uhr Eastern *Impact:* der Zugriff auf Desktops und Anwendungsservices für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Fehlerbehebung für ein Problem mit der Link-Weiterleitung mit dem Azure Cost Estimator (ACE)
- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen

VDS v6 Veröffentlichung: Donnerstag, 6. Januar 2022

Components: Virtual Desktop Service v6 *When:* Donnerstag, 6. Januar 2022 von 22 bis 23 Uhr Eastern

Impact: der Zugriff auf Desktops und Anwendungsservices für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Bericht Self-Service Password Reset sowohl für Partner als auch für Unterpublisher vorstellen
- Bug Fix für ein eindeutiges Problem mit Azure-Autorisierung zu Beginn des Implementierungsprozesses.

VDS v6 Veröffentlichung: Donnerstag, der 16. Dezember 2021

Components: Virtual Desktop Service v6 *Wann:* Donnerstag, der 16. Dezember 2021 von 22 bis 23 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Verbesserungen bei sekundären SMS-Nachrichtenübertragungen für MFA, falls der primäre SMS-Anbieter nicht verfügbar ist
- Aktualisieren Sie das für den VDS-Client für Windows verwendete Zertifikat

VDS v6 Veröffentlichung: Donnerstag, der 2. Dezember 2021 - Keine Änderungen geplant

Components: Virtual Desktop Service v6 *Wann:* Donnerstag, 2. Dezember 2021 von 22 bis 23 Uhr Eastern *Impact:* Keine

VDS v6 Hotfix: Donnerstag, 18. November 2021

Components: Virtual Desktop Service v6 *Wann:* Donnerstag, der 18. November 2021 von 22 bis 23 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Bug fix für ein PAM-Problem, bei dem AAD auf AADDS basiert

VDS v6 Hotfix: Montag, der 8. November 2021

Components: Virtual Desktop Service v6 *Wann:* Montag, der 8. November 2021 von 22 bis 23 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Aktivieren Sie die Chat-Box in der VDS-Benutzeroberfläche für alle Benutzer
- Bug Fix für eine eindeutige Kombination aus Implementierungsauswahl

VDS v6 Veröffentlichung: Sonntag, 7. November 2021

Components: Virtual Desktop Service v6 *Wann:* Sonntag, 7. November 2021 um 22 Uhr bis 23 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Führen Sie eine Command Center-Option ein, um das automatische Verkleinern von FSLogix-Profilen zu deaktivieren
- Bug Fix für PAM, wenn die Implementierung Azure Active Directory Domain Services (ADDS) nutzt
- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen

Kostenplaner Für Azure

- Aktualisierte Services in verschiedenen Regionen verfügbar

VDS v6-Veröffentlichung: Donnerstag, 21. Oktober 2021

Components: Virtual Desktop Service v6 *When:* Donnerstag, 21. Oktober 2021 um 22 Uhr – 23 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Führen Sie eine Command Center-Option ein, um das automatische Verkleinern von FSLogix-Profilen zu deaktivieren
- Verbesserungen an einem nächtlichen Bericht, der zeigt, wo FSLogix-Profile montiert werden
- Die für die Plattform-VM verwendete Standard-VM-Serie/-Größe in der Azure US South Central-Region auf D2S v4 aktualisieren

VDS v6 Veröffentlichung: Donnerstag, der 7. Oktober 2021

Components: Virtual Desktop Service v6 *When:* Donnerstag, 7. Oktober 2021 um 22 Uhr – 23 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Bug fix für ein Szenario, in dem eine spezifische Provisioning Sammlung Konfiguration nicht richtig gespeichert

VDS v6 Veröffentlichung: Donnerstag, der 23. September 2021

Components: Virtual Desktop Service v6 *Wann:* Donnerstag, 23. September 2021 um 22 Uhr – 23 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Aktualisierung in PAM zur Integration in AADDS-basierte Bereitstellungen
- Zeigt RemoteApp-URLs im Workspace-Modul für nicht-AVD-Bereitstellungen an
- Bug Fix für ein Szenario, in dem ein Endbenutzer zu einem Administrator in einer bestimmten lokalen Active Directory-Konfiguration wird

VDS v6 Veröffentlichung: Donnerstag, 9. September 2021

Components: Virtual Desktop Service v6 *Wann:* Donnerstag, 9. September 2021 um 22 Uhr – 23 Uhr Eastern

Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen

VDS v6 Veröffentlichung: Donnerstag, 26. August 2021

Components: Virtual Desktop Service v6 *When:* Donnerstag, 26. August 2021 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Aktualisieren Sie die URL auf dem Desktop eines Benutzers, wenn ihnen Zugriff auf die VDS-Management-UI gewährt wird

VDS v6 Veröffentlichung: Donnerstag, 12. August 2021

Components: Virtual Desktop Service v6 *When:* Donnerstag, 12. August 2021 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Verbesserung der Funktionalität und des Kontexts von Cloud Insights
- Verbesserte Handhabung von Häufigkeiten beim Backup-Zeitplan
- Bug Fix - Beheben eines Problems für CwVmAutomation Service Überprüfung der config beim Service-Neustart
- Fehlerbehebung - Beheben eines Problems für DCConfig, das das Speichern von Konfigurationen in bestimmten Szenarien nicht zulässt
- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen

VDS v6 Hotfix: Dienstag, 30. Juli 2021

Components: Virtual Desktop Service v6 *Wann:* Freitag, der 30. Juli 2021 um 19:00 – 20:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Anwendungsservices für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Update der Implementierungsvorlage zur Vereinfachung der Automatisierungsverbesserungen

VDS v6 Veröffentlichung: Donnerstag, 29. Juli 2021

Components: Virtual Desktop Service v6 *Wann:* Donnerstag, der 29. Juli 2021 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Bug Fix - Beheben eines Problems für VMware-Bereitstellungen, bei denen CWAgent nicht wie

vorgesehen installiert wurde

- Bug Fix - Beheben eines Problems für VMware-Bereitstellungen, bei dem die Erstellung eines Servers mit der Data-Rolle nicht wie vorgesehen funktioniert

VDS v6 Hotfix: Dienstag, der 20. Juli 2021

Components: Virtual Desktop Service v6 *Wann:* Dienstag, der 20. Juli 2021 um 22 Uhr – 23 Uhr Eastern

Impact: der Zugriff auf Desktops und Anwendungsservices für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Beheben Sie ein Problem, das zu einer ungewöhnlich großen Menge an API-Traffic in einer bestimmten Konfiguration führt

VDS 6.0 Veröffentlichung: Donnerstag, 15. Juli 2021

Components: 6.0 Virtual Desktop Service *When:* Donnerstag, der 15. Juli 2021 um 22 Uhr – 23 Uhr Eastern

Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Erweiterung der Cloud Insights-Integration: Erfassung von Performance-Metriken pro Benutzer und Anzeige im Benutzerkontext
- Verbesserungen bei der ANF Provisioning-Automatisierung – verbesserte automatisierte Registrierung von NetApp als Anbieter im Azure-Mandanten des Kunden
- Einstellung beim Erstellen eines neuen AVD-Arbeitsbereichs formulieren
- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen

VDS 6.0 Veröffentlichung: Donnerstag, 24. Juni 2021

Components: 6.0 Virtual Desktop Service *Wann:* Donnerstag, der 4. Juni 2021 um 22 Uhr – 23 Uhr Eastern

Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.



Die nächste VDS-Version wird am Donnerstag, den 7. Juli 15, geplant sein.

Virtual Desktop Service

- Updates zur Berechnung, dass Windows Virtual Desktop (WVD) jetzt Azure Virtual Desktop (AVD) ist
- Fehler bei der Formatierung des Benutzernamens in Excel-Exporten
- Verbesserte Konfigurationen für benutzerdefinierte HTML5-Anmeldeseiten
- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen

Kostenplaner

- Updates zur Berechnung, dass Windows Virtual Desktop (WVD) jetzt Azure Virtual Desktop (AVD) ist
- Aktualisierungen zum reflektieren mehr Services/GPU-VMs sind in neuen Regionen verfügbar

VDS 6.0 Veröffentlichung: Donnerstag, 10. Juni 2021

Components: 6.0 Virtual Desktop Service *When:* Donnerstag, der 10. Juni 2021 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Einführung eines zusätzlichen browserbasierten HTML5-Gateways/Zugriffspunkts für VMs
- Verbessertes Benutzerrouting nach dem Löschen eines Host-Pools
- Fehlerbehebung für ein Szenario, in dem der Import eines nicht verwalteten Hostpools nicht wie erwartet funktioniert
- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen

VDS 6.0 Veröffentlichung: Donnerstag, 10. Juni 2021

Components: 6.0 Virtual Desktop Service *When:* Donnerstag, der 10. Juni 2021 um 22:00 Uhr Eastern
Auswirkungen: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Technische Verbesserungen:

- Aktualisieren Sie die auf jeder VM installierte Version des .NET-Frameworks von v4.7.2 bis v4.8.0
- Zusätzliche Back-End-Durchsetzung der Verwendung von https:// und TLS 1.2 oder höher zwischen dem Local Control Plane Team und einer anderen Einheit
- Fehlerbehebung für den Vorgang Sicherung löschen im Command Center – dieser verweist nun korrekt auf die Zeitzone von CWMGR1
- Benennen Sie die Aktion Command Center aus der Azure-Dateifreigabe in die Azure-Files-Freigabe um
- Updates der Namenskonvention in Azure Shared Image Gallery
- Verbesserte Erfassung der gleichzeitigen Benutzeranmeldeanzahl
- Aktualisierung auf ausgehenden Datenverkehr von CWMGR1 zulässig, wenn der Datenverkehr von der CWMGR1-VM begrenzt wird
- Wenn Sie den ausgehenden Datenverkehr von CWMGR1 nicht einschränken, müssen Sie hier keine Aktualisierungen vornehmen
- Wenn Sie den ausgehenden Datenverkehr von CWMGR1 einschränken, lassen Sie den Zugriff auf `vdctoolsapiprimary.azurewebsites.net` zu. Hinweis: Sie müssen den Zugriff auf `vdctoolsapi.trafficmanager.net` nicht mehr zulassen.

Verbesserungen der Implementierung:

- Legen Sie die Grundlage für die künftige Unterstützung von benutzerdefinierten Präfixen bei Servernamen
- Verbesserte Prozessautomatisierung und Redundanzen bei Azure Implementierungen
- Zahlreiche Erweiterungen zur Automatisierung der Implementierung von Google Cloud Platform
- Unterstützung von Windows Server 2019 in Google Cloud Platform Implementierungen
- Fehlerbehebung für eine Auswahl von Szenarien, in denen das Windows 10 20H2 EVD-Image angezeigt wird

Verbesserungen bei der Servicebereitstellung:

- Einführung der Cloud Insights-Integration für Streaming-Performance-Daten für Benutzerfreundlichkeit, VM- und Storage-Ebenen
- Enthält eine Funktion, mit der Sie schnell zu einer kürzlich besuchten VDS-Seite navigieren können
- Deutlich verbesserte Liste (Benutzer, Gruppen, Server, Applikationen, etc.) Ladezeiten für Azure Bereitstellungen
- Ermöglicht den einfachen Export von Benutzerlisten, Gruppen, Servern, Administratoren, Berichten usw.
- Bietet die Möglichkeit, zu kontrollieren, welche VDS MFA-Methoden für Kunden verfügbar sind (Kunde bevorzugt E-Mail oder beispielsweise SMS)
- Führt anpassbare „From“-Felder für VDS-E-Mails zum Zurücksetzen des Kennworts ein
- Gibt die Option an, dass VDS-Self-Service-Kennwort-Reset-E-Mails nur für bestimmte Domänen zulassen kann (im Besitz des Unternehmens vs Persönlich, zum Beispiel)
- Führt ein Update ein, das den Benutzer dazu auffordert, seine E-Mail zu seinem Konto hinzuzufügen, damit er es verwenden kann oder MFA/Self-Service-Kennwort zurücksetzen kann
- Starten Sie auch alle VMs innerhalb der Implementierung, wenn Sie eine aufgestoppte Implementierung starten
- Performance-Verbesserung beim ermitteln der IP-Adresse, die neu erstellten Azure VMs zugewiesen werden soll

VDS 6.0 Veröffentlichung: Donnerstag, 27. Mai 2021

Components: 6.0 Virtual Desktop Service *When:* Donnerstag, der 27. Mai 2021 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Einführung von Start On Connect für gebündelte Sitzungshosts in AVD-Hostpools
- Einführung von Performance-Kennzahlen für Benutzer mithilfe der Cloud Insights Integration
- Zeigen Sie die Registerkarte Server im Workspaces-Modul stärker an
- Lassen Sie die Wiederherstellung einer VM über Azure Backup zu, wenn die VM aus VDS gelöscht wurde
- Verbesserte Handhabung der Connect to Server-Funktionalität
- Verbesserte Handhabung von Variablen bei der automatischen Erstellung und Aktualisierung von Zertifikaten
- Fehlerbehebung für ein Problem, bei dem das Klicken auf ein X in einem Dropdown-Menü die Auswahl nicht wie erwartet gelöscht
- Verbesserte Zuverlässigkeit und automatische Fehlerbehandlung bei SMS-Nachrichtenaufforderungen
- Aktualisieren der Benutzerunterstützrolle – dies kann nun Prozesse für einen angemeldeten Benutzer beenden
- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen

VDS 6.0 Veröffentlichung: Donnerstag, 13. Mai 2021

Components: 6.0 Virtual Desktop Service *When:* Donnerstag, der 13. Mai 2021 um 22 Uhr – 23 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff

auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Einführung von zusätzlichen AVD-Host-Pool-Eigenschaften
- Zusätzliche Automatisierungsoptionen in Azure Implementierungen bei Back-End-Serviceproblemen
- Fügen Sie den Servernamen in die Registerkarte „Neuer Browser“ ein, wenn Sie die Funktion „mit Server verbinden“ verwenden
- Zeigen Sie die Anzahl der Benutzer in jeder Gruppe an
- Erhöhte Ausfallsicherheit für die Funktion „Connect to Server“ in allen Implementierungen
- Zusätzliche Verbesserungen beim Einrichten von MFA-Optionen für Unternehmen und Endbenutzer
 - Wenn SMS als einzige verfügbare MFA-Option eingestellt ist, benötigen Sie eine Telefonnummer, aber keine E-Mail-Adresse
 - Wenn E-Mail als einzige verfügbare MFA-Option eingestellt ist, benötigen Sie eine E-Mail-Adresse, jedoch keine Telefonnummer
 - Wenn sowohl SMS als auch E-Mail als Optionen für MFA eingestellt sind, benötigen Sie sowohl eine E-Mail-Adresse als auch eine Telefonnummer
- Clarity Improvement - Entfernen Sie die Größe eines Azure Backup Snapshot, da Azure nicht die Größe des Snapshots zurück
- Hinzufügen der Möglichkeit zum Löschen eines Snapshots in Umgebungen außerhalb von Azure
- Fehlerbehebung für die Erstellung von AVD-Host-Pools bei Verwendung von Sonderzeichen
- Bug Fix für das Workload-Scheduling für den Host Pool über die Registerkarte „Ressourcen“
- Fehlerbehebung für eine Fehlermeldung, die beim Abbrechen eines Benutzerimports für Massenvorgänge angezeigt wird
- Fehlerbehebung für ein mögliches Szenario mit den Einstellungen der Anwendung, die zu einer Provisioning Collection hinzugefügt wurden
- Aktualisierung der E-Mail-Adresse, an die Benachrichtigungen/Nachrichten gesendet werden – Nachrichten werden nun von noreply@vds.netapp.com gesendet
 - Kunden, die eingehende E-Mail-Adressen sicher stellen, sollten diese E-Mail-Adresse hinzufügen

VDS 6.0 Veröffentlichung: Donnerstag, 29. April 2021

Components: 6.0 Virtual Desktop Service *Wann:* Donnerstag, der 29. April 2021 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Einführung der Start-on-Connect-Funktion für Personal AVD-Hostpools
- Speicherkontext im Workspace-Modul einführen
- Einführung der Überwachung von Storage (Azure NetApp Files) über Cloud Insights Integration
 - IOPS-Monitoring
 - Latenzüberwachung
 - Kapazitätsüberwachung

- Verbesserte Protokollierung für VM-Klonaktionen
- Fehlerbehebung für ein bestimmtes Workload-Planungsszenario
- Bug fix für nicht anzeigen einer VM-Zeitzone in einem bestimmten Szenario
- Fehlerbehebung für das Nichtabmelden eines AVD-Benutzers in einem bestimmten Szenario
- Updates zu automatisch generierten E-Mails, die mit dem NetApp Branding übereinstimmen

VDS 6.0 Hotfix: Freitag, der 16. April 2021

Components: 6.0 Virtual Desktop Service *Wann:* Freitag, der 16. April 2021 um 22:00 – 23:00 Uhr Eastern

Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Lösen Sie ein Problem mit automatisierten Zertifikaterzeugung, die nach dem Update der letzten Nacht entstanden, die automatisierte Zertifikatverwaltung verbessert

VDS 6.0 Veröffentlichung: Donnerstag, 15. April 2021

Components: 6.0 Virtual Desktop Service *When:* Donnerstag, der 15. April 2021 um 22:00 – 23:00 Uhr Eastern

Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Verbesserungen bei der Cloud Insights-Integration:
 - Übersprungene Frames – Unzureichende Netzwerkressourcen
 - Übersprungene Frames – Unzureichende Client-Ressourcen
 - Frame Übersprungen – Unzureichende Server-Ressourcen
 - Betriebssystemfestplatte – Byte-Lesen
 - Betriebssystemfestplatte – Bytes schreiben
 - Betriebssystemfestplatte – Byte/Sekunde wird gelesen
 - BS-Festplatte: Byte/Sekunde schreiben
- Aktualisierung auf Aufgabenverlauf im Modul Bereitstellungen – verbesserte Handhabung des Aufgabenverlaufs
- Bug-fix für ein Problem, wo ein Azure Backup konnte nicht wiederhergestellt werden, um CWMGR1 von einer Festplatte in einer Untermenge von Szenarien
- Bug fix für ein Problem, bei dem Zertifikate nicht automatisch aktualisiert und erstellt wurden
- Bug fix für ein Problem, wo eine gestoppt Bereitstellung nicht schnell genug gestartet
- Aktualisieren Sie in die Dropdown-Liste Status beim Erstellen eines Arbeitsbereichs – entfernen Sie den Eintrag „National“ aus der Liste
- Weitere Updates mit dem NetApp Branding

VDS 6.0: Mittwoch, der 7. April 2021

Components: 6.0 Virtual Desktop Service *When:* Mittwoch, der 7. April 2021 um 22:00 – 23:00 Uhr Eastern

Impact: der Zugriff auf Desktops und Anwendungsservices für Endbenutzer bleibt ununterbrochen. Der Zugriff

auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Aufgrund der immer variabler Reaktionszeiten aus Azure wird die Wartezeit auf eine Antwort bei der Eingabe der Azure Zugangsdaten während des Implementierungsassistenten erhöht.

VDS 6.0 Veröffentlichung: Donnerstag, 1. April 2021

Components: 6.0 Virtual Desktop Service *When:* Donnerstag, 1. April 2021 um 22:00 – 23:00 Uhr Eastern

Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Updates zur Integration von NetApp Cloud Insights – neue Streaming-Datenpunkte:
 - NVIDIA-GPU-Performance-Daten
 - Round Trip Time
 - Verzögerung Der Benutzereingabe
- Aktualisierung der Funktion „Verbinden mit Server“, um Administratorverbindungen zu VMs zu ermöglichen, selbst wenn VMs so eingestellt sind, dass die Verbindungen von Endbenutzern entzulässt
- API-Verbesserungen für aktivierte Theming & Branding in einer späteren Version
- Verbesserte Sichtbarkeit des Aktionsmenüs in HTML5-Verbindungen über Connect to Server oder RDS-Benutzersitzungen über HTML5
- Erhöhen Sie die MENGE der Zeichen, die im Namen eines Vorgangs „skriptbasierte Ereignisse“ unterstützt werden
- Betriebssystemoptionen für Provisioning Collections nach Typ aktualisiert
 - Verwenden Sie für AVD und Windows 10 den VDI-Erfassungstyp, um sicherzustellen, dass das Windows 10-Betriebssystem vorhanden ist
 - Verwenden Sie für ein Windows-Server-Betriebssystem den Sammeltyp „gemeinsam genutzt“
- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen

Virtual Desktop Service – v5.4 Versionshinweise

VDS 5.4 Veröffentlichung: Donnerstag, 12. August 2021

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 12. August 2021 um 22:00 – 23:00 Uhr Eastern

Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Aktualisierte AVD-Host-Pool-Links

VDS 5.4 Veröffentlichung: Donnerstag, 13. Mai 2021

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 13. Mai 2021 um 22 Uhr – 23 Uhr Eastern

Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Fehlerbehebung für die Erstellung von AVD-Host-Pools bei Verwendung von Sonderzeichen
- Erweiterungen der Automatisierung für lange Domain-Namen im Bereitstellungsassistenten von CWA Setup
- Bug Fix für das Klonen von Servern in einem Teil der Szenarien in GCP-Implementierungen
- Bug fix für ein Szenario, in dem das Löschen eines Snapshots nicht wie vorgesehen funktioniert
- Aktualisierung der E-Mail-Adresse, an die Benachrichtigungen/Nachrichten gesendet werden – Nachrichten werden nun von noreply@vds.netapp.com gesendet
 - Kunden, die eingehende E-Mail-Adressen sicher stellen, sollten diese E-Mail-Adresse hinzufügen

VDS 5.4 Veröffentlichung: Donnerstag, 29. April 2021

Components: 5.4 Virtual Desktop Service *Wann:* Donnerstag, der 29. April 2021 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

(Keine Updates für diese Version)

VDS 5.4 Hotfix: Freitag, 16. April 2021

Components: 5.4 Virtual Desktop Service *Wann:* Freitag, der 16. April 2021 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Lösen Sie ein Problem mit automatisierten Zertifikaterzeugung, die nach dem Update der letzten Nacht entstanden, die automatisierte Zertifikatverwaltung verbessert

VDS 5.4 Veröffentlichung: Donnerstag, 15. April 2021

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 15. April 2021 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Kontinuierliche Updates zur Verbesserung der Konnektivität und Kommunikation mit dem vSphere/vCloud Hypervisor
- Fehlerbehebung für ein einzelnes Szenario, in dem ein Benutzer keinen AVD-Sitzungshost klonen konnte

VDS 5.4 Hotfix: Dienstag, 23. März 2021

Components: 5.4 Virtual Desktop Service *Wann:* Dienstag, der 23. März 2021 um 22 Uhr bis 23 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Update zu den Anzeigepools: Lösen Sie ein Problem in einer Teilmenge von Szenarien, in denen neu erstellte Hostpools erfolgreich abgeschlossen wurden, aber nicht unmittelbar in der VDS-UI vorhanden

sind

VDS 5.4 Veröffentlichung: Donnerstag 18. März 2021

Components: 5.4 Virtual Desktop Service *Wann:* Donnerstag, der 18. März 2021 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

- Virtual Desktop Service
- Lassen Sie die Verbindung zum Server zulassen, wenn Endbenutzerverbindungen mit einer VM nicht zulässig sind
- Einstellung der PAM-Nachrichten, die Benutzer erhalten, per SMS ausformulieren
- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen

VDS 5.4 Hotfix: Dienstag, 9. März 2021

Components: 5.4 Virtual Desktop Service *Wann:* Dienstag, der 9. März 2021 um 5:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Wenden Sie ein Update an, um ein Problem mit dem Server verbinden in einem Teil der Szenarien zu lösen

VDS 5.4 Release: Donnerstag, März 4, 2021

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 4. März 2021 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Einführung des DSC-gestützten Implementierungsmodells für die Google Cloud Platform-Implementierung
- Skriptbasierte Ereignisse werden aktualisiert, um zu verhindern, dass ein Skript gelöscht wird, während es aktiv ausgeführt wird
- Verbesserungen der Automatisierung bei der Handhabung von NetBIOS für bestehende Active Directory-Umgebungen durch den Bereitstellungsassistenten
- Unterstützung bei der Anwendung verschiedener Backup-Zeitpläne für einzelne Plattform-Server
- Unterstützen Sie das Ändern des Kennworts eines Benutzers, damit er bei der nächsten Anmeldung im selben Befehl sein Passwort zurücksetzen muss
- Fehlerbehebung: Festlegen des Migrationsmodus für einzelne VMs, um Einstellungen des Implementierungsmodus außer Kraft zu setzen
- Bug Fix für vSphere Szenario, bei dem das Senden zu viele API-Befehle gleichzeitig zu einer Verzögerung beim Starten von VMs führte
- Aktualisierung neuer Bereitstellungen zur Unterstützung von .NET 4.8.0
- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen

VDS 5.4 Veröffentlichung: Donnerstag, Februar 18, 2021

Components: 5.4 Virtual Desktop Service *Wann:* Donnerstag, der 18. Februar 2021 um 22:00 - 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Aktualisiert die Standardinstallationsmethode für FSLogix gemäß den Best Practices von Microsoft
- Proaktive Upgrades auf Plattformkomponenten zur Unterstützung einer höheren Benutzeraktivität
- Verbesserte Automatisierung beim Umgang mit Variablen für das Zertifikatmanagement
- Unterstützen Sie bei der nächsten Anmeldung, wenn Sie Ihr Passwort ändern, das Zurücksetzen der MFA-Einstellungen eines Benutzers erzwingen
- Entfernen Sie die VDS-Admin-Gruppe aus der Verwaltung im Gruppen-Modul VDS in AADDs-Bereitstellungen

Kostenplaner

- Updates, die sicherstellen, dass bestimmte VMs nicht mehr über Promo-Preispunkte verfügen

VDS 5.4 Veröffentlichung: Donnerstag, Februar 4, 2021

Components: 5.4 Virtual Desktop Service *Wann:* Donnerstag, der 4. Februar 2021 um 22:00 - 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Verbesserte variable Handhabung bei der Verwendung von Connect to Server-Funktionalität
- API – Nebenfunktion für Reboot und Multi-Select-Reboot-Funktion
- Verbesserungen bei der Bereitstellungsautomatisierung in Google Cloud Platform
- Verbesserte Handhabung von ausgeschalteten Bereitstellungen der Google Cloud Platform

VDS 5.4: Donnerstag, 21. Januar 2021

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 21. Januar 2021 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Entfernung von TSD1-VMs aus Implementierungen, bei der PaaS-Services für das Datenmanagement ausgewählt werden
- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen
- Prozessoptimierung für Implementierungskonfigurationen mit mehreren Servern
- Bug Fix für eine bestimmte Konfiguration für eine GCP-Implementierung
- Bug fix für das Erstellen von Azure Files Shares über das Command Center
- Update zur Bereitstellung von Server 2019 als Betriebssystem in GCP

Kostenplaner

- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen

VDS 5.4 Hotfix: Mon. Januar 18, 2021

Components: 5.4 Virtual Desktop Service *Wann:* Montag, der 18. Januar 2021 um 22 Uhr – 23 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- VDS wird ein Update auf Bereitstellungen mit SendGrid für SMTP-Relais anwenden
- SendGrid stellt am Mittwoch 1/20 eine bahnbrechende Veränderung vor
- Das VDS-Team hatte bereits Upgrades auf SendGrid untersucht
- Wir waren uns dieser bevorstehenden Änderung bewusst und haben eine Alternative (Postmark) getestet und validiert.
- Das VDS-Team hat nicht nur eine bahnbrechende Änderung verringert, sondern auch die Zuverlässigkeit und Performance bei Implementierungen verbessert, die Postmark statt SendGrid nutzen

VDS 5.4 Hotfix: Fr. Januar 8, 2021

Components: 5.4 Virtual Desktop Service *When:* Mittwoch, der 8. Januar 2021 um 12 Uhr – 19:05 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Kurze, nachfolgende Aktualisierung, um sicherzustellen, dass VDCTools in allen Bereitstellungen aktuell ist
 - Durch das Design werden Updates auf VDCTools intelligent angewendet – das Update wartet, bis keine Aktionen ausgeführt werden. Anschließend werden alle während des kurzen Aktualisierungszeitraums ergriffenen Maßnahmen automatisch abgeschlossen

VDS 5.4: Donnerstag, 7. Januar 2021

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 7. Januar 2021 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Anwendungsservices für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen
- Textaktualisierung: Ändern Sie die Aktion Command Center von Azure File Share erstellen auf Azure Files Share erstellen
- Prozessverbesserungen für die Verwendung von Command Center zur Aktualisierung von Daten-/Home-/Pro-Ordern

Kostenplaner

- Verschiedene proaktive Sicherheits- und Leistungsverbesserungen

VDS 5.4: Donnerstag, 17. Dezember 2020

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 17. Dezember 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.



Die nächste Veröffentlichung findet am Donnerstag, der 7. Januar 2021 statt Silvester 2020 statt.

Virtual Desktop Service

- Verbesserte Automatisierung der Implementierung bei Verwendung von Azure NetApp Files
- Verbesserung der Provisioning-Sammlungen mit aktualisierten Windows 10-Bildern
- Aktualisierung auf VCC, um Variablen in Konfigurationen mit mehreren Standorten besser zu unterstützen
- Kleinere proaktive Verbesserung der Funktionalität von Standorten
- API-Verbesserungen zu Peak Live-Skalierbarkeit innerhalb von Live-Skalierung
- Allgemeine Nutzbarkeit und Verbesserung der Textklarheit in DC Config
- Verschiedene Bugfixes und Sicherheitsverbesserungen hinter den Kulissen

VDS 5.4: Donnerstag, 3. Dezember 2020

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 3. Dezember 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Aktualisierung auf die Installationsmethode FSLogix
- Fortlaufende proaktive Sicherheitsmaßnahmen

VDS-Einrichtung

- Update auf Azure NetApp Files-Bereitstellungsautomatisierung – Unterstützung beim Erstellen:
- Kapazitäts-Pool/Volume mit mindestens 4 TB
- 500 TB Kapazitäts-Pool/100 TB Volume bei maximal
- Verbessertes variables Handling für erweiterte Implementierungsoptionen

Kostenplaner

- Entfernen von Disk-Operationen aus dem Google Cost Estimator
- Aktualisierungen, die neue Services widerspiegeln, die nach Region im Azure Cost Estimator verfügbar sind

VDS 5.4: Donnerstag, 19. November 2020

Components: 5.4 Virtual Desktop Service *Wann:* Donnerstag, der 19. November 2020 um 22 Uhr bis 23 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

VDS

- Die E-Mails des Privileged Account Management (PAM) enthalten jetzt auch Einzelheiten zum Bereitstellungscode
- Optimierung von Berechtigungen für Azure Active Directory Domain Services (AADDS)-Bereitstellungen
- Bessere Übersichtlichkeit für Administratoren, die Admin-Aufgaben in einer komplett heruntergealteten Bereitstellung ausführen möchten
- Fehlerbehebung für eine Fehlermeldung, die angezeigt wird, wenn ein VDS-Administrator Details zur RemoteApp-App-Gruppe für einen Host-Pool ansieht, der heruntergefahren wurde
- Aktualisierung von API-Benutzern wird so formuliert, dass sie VDS-API-Benutzer sind
- Schnellere Ergebnisse für die Rückgabe des Datacenter-Statusberichts
- Verbesserte Handhabung von Variablen für tägliche Aktionen (z. B. nächtliche Neustarts) für VMs
- Fehlerbehebung für ein Szenario, in dem die in DC Config eingegebenen IP-Adressen nicht korrekt gespeichert wurden
- Fehlerbehebung für ein Szenario, in dem das Entsperren eines Administratorkontos nicht wie vorgesehen funktioniert

VDS-Einrichtung

- Aktualisierung des Formfaktors – Auflösen eines Szenarios, in dem die Aktionsschaltflächen im VDS-Einrichtungsassistenten abgeschnitten wurden

VDS 5.4: Donnerstag, 5. November 2020

Components: 5.4 Virtual Desktop Service *Wann:* Donnerstag, der 5. November 2020 um 22:00 - 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

VDS

- Einführung des Scale-out-Mechanismus für Standorte im Command Center – Verwenden Sie ein weiteres Azure-Abonnement mit derselben Mandanten-ID und Client-ID
- Die Erstellung von VMs, deren Data-Rolle jetzt als in der VDS-UI ausgewählte VM implementiert wird, erfolgt jedoch wieder auf die für die Implementierung festgelegte Standardeinstellung, wenn die ausgewählte VM nicht verfügbar ist
- Allgemeine Verbesserungen bei Workload Scheduling und Live Scaling
- Bug fix for Apply All Checkbox for admin permissions
- Fehlerbehebung für ein Anzeigeproblem, wenn in einer RemoteApp App App-Gruppe ausgewählte Apps angezeigt werden
- Fehlerbehebung für eine Fehlermeldung eine Untergruppe von Benutzern wird beim Zugriff auf das Command Center angezeigt
- Automatisierte Prozessverbesserungen für manuelle Zertifikatinstallationen auf HTML5 Gateway VMs
- Fortlaufende proaktive Sicherheitsmaßnahmen

VDS-Einrichtung

- Verbesserte Azure NetApp Files Orchestrierung

- Fortlaufende Verbesserungen für den reibungslosen Umgang mit Azure Implementierungsvariablen
- Bei neuen Active Directory-Bereitstellungen ist die Active Directory-Funktion für den Papierkorb automatisch aktiviert
- Verbesserte Koordinierung der Implementierung für Google Cloud Platform

VDS 5.4 Hotfix: Mi. 28. Oktober 2020

Components: 5.4 Virtual Desktop Service *When:* Mittwoch, der 28. Oktober 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

VDS-Einrichtung

- Fehlerbehebung für ein Szenario, in dem Netzwerkdetails nicht ordnungsgemäß in den Bereitstellungsassistenten eingegeben werden konnten

VDS 5.4: Donnerstag, 22. Oktober 2020

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 22. Oktober 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

VDS

- Wenn ein VDS-Administrator einen AVD-Hostpool löscht, wird die Zuweisung von Benutzern aus diesem Hostpool automatisch aufgehoben
- Einführung eines verbesserten, umbenannten Automatisierungstreibers – Command Center – in CWMGR1
- Fehlerbehebung für das Verhalten von Workload Scheduling in einem Bug Fix zum Aktualisieren der Standortdetails, wenn dieser sich in AWS befindet
- Bug fix für Wake-On-Demand-Aktivierung mit spezifischen Live-Scaling-Einstellungen angewendet
- Fehler beim Erstellen eines zweiten Standorts, wenn falsche Einstellungen am ursprünglichen Standort vorhanden waren
- Benutzerfreundliche Verbesserungen für statische IP-Details in DC-Konfig
- Aktualisierung der Konventionen auf Administratorberechtigungen benennen – Aktualisierung der Rechenzentrumsberechtigungen auf Bereitstellungsberechtigungen
- Aktualisierung, um zu reflektieren, dass weniger Datenbankeinträge in einzelnen Server-BereitstellungsBuilds erforderlich sind
- Aktualisierung auf manuelle Aktualisierung des AADDs-Bereitstellungsprozesses zur Optimierung von Berechtigungen
- Fehlerbehebung für die Berichterstattung in VDS bei Änderung der Daten, die der Bericht zurückgeben soll
- Fehlerbehebung beim Erstellen einer Windows Server 2012 R2-Vorlage über Provisioning Collections
- Verschiedene Leistungsverbesserungen

VDS-Einrichtung

- Verbesserungen bei der Automatisierung des primären Domänencontrollers und der DNS-Komponenten einer Implementierung
- Verschiedene Aktualisierungen zur Unterstützung der Auswahl aus einer Liste verfügbarer Netzwerke in

einer zukünftigen Version

Kostenplaner

- Verbesserte Handhabung des Hinzufügens von SQL zu VMs

REST API

- Neuer API-Aufruf zur Ermittlung der gültigen und für ein Abonnement verfügbaren Azure-Regionen
- Neuer API-Aufruf, um zu ermitteln, ob ein Kunde Cloud Insights-Zugriff hat
- Neuer API-Aufruf, um zu ermitteln, ob ein Kunde Cloud Insights für seine Cloud Workspace-Umgebung aktiviert hat

VDS 5.4 Hotfix: Mi., 13. Oktober 2020

Components: 5.4 Virtual Desktop Service *When:* Mittwoch, der 13. Oktober 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Kostenplaner

- Fehlerbehebung bei einem Problem, bei dem ein Szenario im Azure Cost Estimator verwendet wird, bei dem RDS-VMs die Preise für das Betriebssystem falsch aufwendeten
- Bug Fix für ein Szenario, in dem die Auswahl von Storage-PaaS-Diensten im Azure Cost Estimator und Google Cost Estimator zu einem überhöhten Preis pro VDI-Benutzer führte

VDS 5.4: Donnerstag, 8. Oktober 2020

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 8. Oktober 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

VDS

- Die Stabilitätsverbesserungen bei der Erstellung einer VM während Stunden, in denen Workload Scheduling angewendet wird
- Fehlerbehebung für ein Anzeigeproblem beim Erstellen neuer App-Dienste
- Dynamische Bestätigung der Vorzeiten von .NET und ThinPrint für nicht-Azure-Implementierungen
- Fehlerbehebung für ein Anzeigeproblem bei der Überprüfung des Bereitstellungsstatus eines Arbeitsbereichs
- Bug Fix für die Erstellung einer VM in vSphere mit einer spezifischen Kombination von Einstellungen
- Fehlerbehebung für einen Checkbox-Fehler unter einer Reihe von Berechtigungen
- Fehlerbehebung für ein Anzeigeproblem, bei dem doppelte Gateways in DCConfig angezeigt wurden
- Branding-Updates

Kostenplaner

- Aktualisieren Sie auf die Anzeige der Details zur CPU-Skalierung pro Workload-Typ

VDS 5.4 Hotfix: Mi., 30. September 2020

Components: 5.4 Virtual Desktop Service *When:* Mittwoch, der 30. September 2020 um 21:00 – 22:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

VDS

- Fehlerbehebung für ein Problem, bei dem eine Untergruppe von App Services-VMs nicht ordnungsgemäß als Cache-VMs gekennzeichnet wurde
- Aktualisieren Sie auf die zugrunde liegende SMTP-Konfiguration, um Probleme bei der Konfiguration des E-Mail-Relay-Kontos zu vermeiden
 - Hinweis: Da es sich nun um einen Service für Kontrollebene handelt, ist die Bereitstellung schlanker und die Anzahl der Berechtigungen/Komponenten eines Kunden geringer
- Fehlerbehebung, um zu verhindern, dass ein Administrator mit DCConfig das Kennwort eines Servicekontos zurücksetzen kann

VDS-Einrichtung

- Verbesserte Handhabung von Umgebungsvariablen für Azure NetApp Files Implementierungen
- Verbesserte Automatisierung der Implementierung: Verbesserte Handhabung von Umgebungsvariablen zur Sicherstellung der erforderlichen PowerShell Komponenten

REST API

- Einführung von API-Unterstützung für Azure Implementierungen zur Nutzung einer vorhandenen Ressourcengruppe
- Einführung der API-Unterstützung für vorhandene AD-Implementierungen mit unterschiedlichen Domain-/NetBIOS-Namen

VDS 5.4: Donnerstag, 24. September 2020

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 24. September 2020 um 22:00 - 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

VDS

- Performance-Verbesserung: Die Liste der Benutzer, für die Cloud Workspaces aktiviert werden können, wird jetzt schneller aufgefüllt
- Fehlerbehebung für standortspezifische AVD-Session-Hostserver-Importe
- Verbesserung der Bereitstellungsautomatisierung - Einführung einer optionalen Einstellung zur Weiterleitung von AD-Anfragen an CWMGR1
- Verbesserte Handhabung von Variablen beim Import von Servern, um sicherzustellen, dass CWAgent ordnungsgemäß installiert ist
- Zusätzliche RBAC-Kontrollen über TestVDCTools einführen – für den Zugriff ist eine Mitgliedschaft in der CW-Infrastructure-Gruppe erforderlich
- Feinabstimmung der Berechtigungen – Erteile Administratoren in der CW-CWMGRAccess-Gruppe Zugriff auf Registrierungseinträge für VDS-Einstellungen
- Aktualisierung für Wake-on-Demand für persönliche AVD-Hostpools, um Updates für die Frühjahrsversion

abzubilden – schalten Sie nur die dem Benutzer zugewiesene VM ein

- Aktualisieren von Namenskonventionen für Unternehmenscodes in Azure Implementierungen – verhindert, dass Azure Backup die Wiederherstellung einer VM, die mit einer Zahl beginnt, nicht ausführen kann
- Ersetzen Sie die Verwendung von SendGrid für SMTP-Übertragung durch eine globale Kontrollebene, um ein Problem mit dem Backend von SendGrid zu lösen. Dadurch ist die Bereitstellungsdauer bei geringeren Berechtigungen/Komponenten geringer

VDS-Einrichtung

- Aktualisierungen der VM-Mengenauswahl, die in Bereitstellungen mit mehreren Servern verfügbar ist

REST API

- Fügen Sie Windows 2019 hinzu, um die Methode /DataCenterProvisioning/OperatingSystems ZU ERHALTEN
- Automatisches Befüllen von vor- und Nachnamen des VDS-Administrators bei der Erstellung von Administratoren über die API-Methode

Kostenschätzer

- Einführung von Google Cost Estimator und eine Eingabeaufforderung für den Hyperscaler, den Sie für Ihre Schätzung verwenden möchten – Azure oder GCP
- Einführung reservierter Instanzen in den Azure Cost Estimator
- Aktualisierte Liste der verfügbaren Services pro aktualisierten Azure-Produkte, die nach Region erhältlich sind

VDS 5.4: Donnerstag, 10. September 2020

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 10. September 2020 um 22:00 Uhr bis 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Verbesserte Durchsetzungsmechanismus zur Bestätigung der Installation von FSLogix
- Unterstützung für Konfigurationen mit mehreren Servern für vorhandene AD Implementierungen
- Verringern Sie die Anzahl der API-Aufrufe, die zur Rückgabe einer Liste von Azure-Vorlagen verwendet werden
- Verbesserte Verwaltung der Benutzer in den Host-Pools AVD Spring Release / v2
- Referentielle Link-Aktualisierung im nächtlichen Bericht der Serverressource
- Korrektur für das Ändern von Administratorpasswörtern zur Unterstützung verbesserter, schlankerer Berechtigungssätze in AD
- Bug fix für das Erstellen von VMs aus einer Vorlage über Tools auf CWMGR1
- Suchvorgänge in VDS zeigen nun auf Inhalte unter docs.netapp.com
- Verbesserungen bei der Reaktionszeit für Endbenutzer, die auf die VDS-Administratorschnittstelle zugreifen, wobei MFA aktiviert ist

VDS-Einrichtung

- Der Link nach der Bereitstellung verweist nun auf Anweisungen hier
- Aktualisierte Optionen zur Plattformkonfiguration für vorhandene AD-Implementierungen
- Verbesserte automatisierte Prozesse für die Implementierung von Google Cloud Platform

VDS 5.4 Hotfix: Dienstag, 1. September 2020

Components: 5.4 Virtual Desktop Service *Wann:* Dienstag, 1. September 2020 um 22:10 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

VDS-Einrichtung

- Fehlerbehebung für einen referenziellen Link auf der Registerkarte AVD

VDS 5.4: Donnerstag, 27. August 2020

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 27. August 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Einführung der Möglichkeit, die VDS-Schnittstelle zur automatischen Aktualisierung von AVD-Hostpools von der Herbst-Version bis zur Frühjahrsversion zu verwenden
- Optimierte Automatisierung zur Berücksichtigung aktueller Updates, was zu einem schlankeren Berechtigungsset erforderlich
- Verbesserungen bei der Implementierungsautomatisierung für GCP-, AWS- und vSphere-Implementierungen
- Fehlerbehebung für ein Skript-Ereignisszenario, bei dem Datum und Uhrzeit als aktuelles Datum und Uhrzeit angezeigt wurden
- Bug Fix für die gleichzeitige Bereitstellung großer Mengen von AVD-Session-Host-VMs
- Unterstützung für mehr Azure VM-Typen
- Unterstützung für mehr GCP-VM-Typen
- Verbesserte Handhabung von Variablen während der Implementierung
- Bug Fix für vSphere Implementierungsautomatisierung
- Bei der Fehlerbehebung für ein Szenario beim Deaktivieren eines Cloud Workspace für einen Benutzer wurde ein unerwartetes Ergebnis ausgegeben
- Fehlerbehebung für Anwendungen von Drittanbietern und RemoteApp-Anwendung mit MFA aktiviert
- Höhere Leistung des Service Board, wenn eine Bereitstellung offline ist
- Aktualisierungen zum NetApp Logo/zur Formulierung

VDS-Einrichtung

- Einführung einer Implementierungsoption für mehrere Server für native/Greenfield Active Directory-Implementierungen
- Weitere Verbesserungen bei der Automatisierung der Implementierung

Kostenplaner Für Azure

- Hybrid-Benefits-Funktionalität von Azure herausgeben
- Fehlerbehebung für ein Anzeigeproblem, wenn Sie benutzerdefinierte Namensinformationen in die VM-Details eingeben
- Fehlerbehebung zur Anpassung von Speicherdetails in einer bestimmten Reihenfolge

VDS 5.4 Hotfix: Mi., 19. August 2020

Components: 5.4 Virtual Desktop Service *Wann:* Mittwoch, der 19. August 2020 um 5:20 – 5:25 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

VDS-Einrichtung

- Bug Fix für variables Handling um flexible Automatisierung zu ermöglichen
- Bug Fix für DNS-Handling in einem einzelnen Implementierungsszenario
- Reduzierte Mitgliedsanforderungen der CW-Infrastructure Gruppe

VDS 5.4 Hotfix: Dienstag, 18. August 2020

Components: 5.4 Virtual Desktop Service *Wann:* Dienstag, der 18. August 2020 um 10 Uhr – 15:15 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Kostenplaner Für Azure

- Bug Fix für das Hinzufügen weiterer Laufwerke bei bestimmten VM-Typen

VDS 5.4: Donnerstag, 13. August 2020

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 13. August 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Fügen Sie die Option „Verbinden mit Server“ für AVD-Sitzungshosts vom AVD-Modul hinzu
- Bug Fix für einen Teil der Szenarien, in denen keine zusätzlichen Admin-Konten erstellt werden können
- Namenskonvention für Ressourcen aktualisieren – Ändern Sie Power User zu VDI User

VDS-Einrichtung

- Automatische Validierung vorab genehmigter Netzwerkeinstellungen und weitere Optimierung der Bereitstellungs-Workflows
- Reduzierte Berechtigungsanforderungen für vorhandene AD-Implementierungen
- Domännennamen zulassen, die länger als 15 Zeichen sind
- Text Layout fix für eine eindeutige Kombination von Auswahlen
- Fortsetzen von Azure-Bereitstellungen zulassen, wenn die SendGrid-Komponente einen temporären Fehler zeigt

VDS-Tools und -Services

- Proaktive Sicherheitsverbesserungen hinter den Kulissen
- Zusätzliche Performance-Verbesserungen bei der Live-Skalierung
- Verbesserte Unterstützung von Hyperscaler-Implementierungen mit Hunderten von Standorten
- Bug Fix für ein Szenario, in dem die Implementierung mehrerer VMs in einem einzigen Befehl nur teilweise erfolgreich war
- Verbesserte Eingabeaufforderungen beim Zuweisen von ungültigen Pfaden als Ziel für Daten-, Home- und Profildatenorte
- Bug fix für ein Szenario, in dem das Erstellen von VMs via Azure Backup nicht wie vorgesehen funktioniert
- Weitere Schritte zur Validierung der Implementierung wurden in den GCP- und AWS-Implementierungsprozess hinzugefügt
- Zusätzliche Optionen zur Verwaltung externer DNS-Einträge
- Unterstützung separater Ressourcengruppen für VMs, VNETs, Services wie Azure NetApp Files, Log Analytics Workspaces
- Kleine Back-End-Verbesserungen beim Erstellungsprozess für Provisioning, Erfassungs-/Bilderstellung

Kostenplaner Für Azure

- Fügen Sie die Unterstützung der Festplatte für kurzlebige Betriebssysteme hinzu
- Verbesserte Tooltips für die Speicherauswahl
- Ein Szenario, in dem ein Benutzer negative Benutzerzahlen eingeben konnte, wird nicht zugelassen
- Zeigen Sie den Dateiserver an, wenn Sie die AVD- und File Server-Auswahl verwenden

VDS 5.4 Hotfix: Montag, 3. August 2020

Components: 5.4 Virtual Desktop Service *When:* Montag, der 3. August 2020 um 11 Uhr – 19:05 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

VDS-Tools und -Services

- Verbesserte Handhabung von Variablen bei der Automatisierung der Implementierung

VDS 5.4: Donnerstag, 30. Juli 2020

Components: 5.4 Virtual Desktop Service *Wann:* Donnerstag, der 30. Juli 2020 um 22 Uhr – 23 Uhr Eastern
Impact: der Zugriff auf Desktops und Anwendungsservices für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Proaktive Sicherheitsverbesserungen hinter den Kulissen
- Verbesserte Performance-Überwachung hinter den Kulissen
- Bug Fix für ein Szenario, in dem das Erstellen eines neuen VDS-Administrators eine falsche positive Warnung enthält

VDS-Einrichtung

- Reduzierte Berechtigungseinstellungen für administrative Konten während des Implementierungsprozesses in Azure
- Fehlerbehebung für eine Teilmenge von Anmeldungen für das Testkonto

VDS-Tools und -Services

- Verbesserte Handhabung des FSLogix Installationsprozesses
- Proaktive Sicherheitsverbesserungen hinter den Kulissen
- Verbesserte Erfassung von Datenpunkten zur gleichzeitigen Nutzung
- Verbesserte Handhabung von Zertifikaten für HTML5-Verbindungen
- Anpassung an das DNS-Abschnittslayout für verbesserte Klarheit
- Anpassung an den Solarwinds-Überwachungsworkflow
- Aktualisierte Verarbeitung statischer IP-Adressen

Kostenplaner Für Azure

- Fragen Sie, ob die Daten des Kunden Hochverfügbarkeit sein müssen, und falls ja, stellen Sie fest, ob Kosten- und Arbeitseinsparungen durch Nutzung eines PaaS-Dienstes wie Azure NetApp Files verfügbar sind
- Aktualisieren und standardisieren Sie den Standard-Storage-Typ für AVD- und RDS-Workloads auf Premium-SSD
- Hinter den Kulissen Leistungsverbesserungen * == VDS 5.4 Hotfix: Thurs, 23. Juli 2020

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 23. Juli 2020 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

VDS-Einrichtung

- Verbesserungen der Automatisierung für DNS-Einstellungen in Azure Implementierungen
- Allgemeine Überprüfungen und Verbesserungen bei der Automatisierung der Implementierung

VDS 5.4: Donnerstag, 16. Juli 2020

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 16. Juli 2020 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Proaktive Sicherheitsverbesserungen hinter den Kulissen
- Optimierung des Bereitstellungsprozesses der AVD-Anwendungsgruppe durch automatische Auswahl des AVD-Arbeitsbereichs, wenn nur ein AVD-Arbeitsbereich vorhanden ist
- Leistungsverbesserungen im Workspace-Modul über Paginieren von Gruppen unter der Registerkarte Benutzer und Gruppen
- Wenn VDS-Administratoren auf der Registerkarte Bereitstellungen Azure auswählen, weisen Sie den Benutzer stattdessen zur Anmeldung bei VDS-Setup auf

VDS-Einrichtung

- Proaktive Sicherheitsverbesserungen hinter den Kulissen
- Verbessertes Layout für einen optimierten Implementierungs-Workflow
- Erweiterte Beschreibungen für Bereitstellungen mit einer vorhandenen Active Directory-Struktur
- Allgemeine Verbesserungen und Bug Fixes zur Automatisierung der Implementierung

VDS-Tools und -Services

- Bug fix für die TestVDCTools-Leistung in Einzelservers-Bereitstellungen

REST API

- Verbesserung der Benutzerfreundlichkeit bei der API-Nutzung für Azure-Bereitstellungen – erfasste Benutzernamen, auch wenn die Vornamen nicht für den Benutzer in Azure AD definiert wurden

HTML5-Anmeldeerlebnis

- Fehlerbehebung für Wake-on-Demand-Service für Session-Hosts, die die AVD Spring Release (AVD v2) nutzen
- Aktualisierungen zum NetApp Branding/Phrasieren

Kostenplaner Für Azure

- Preisanzeige dynamisch nach Region
- Zeigen Sie an, ob relevante Services in der Region verfügbar sind, um sicherzustellen, dass der Benutzer versteht, ob die gewünschte Funktionalität in dieser Region verfügbar ist. Diese Services sind:
 - Azure NetApp Dateien
 - Azure Active Directory Domain Services
 - NV und NV v4 (GPU aktiviert) virtuelle Maschinen

VDS 5.4 Release: Fr., 26. Juni 2020

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, 26. Juni 2020 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

Ab Freitag, dem 17. Juli 2020 wird das Release von v5.4 als Produktionsversion unterstützt.

VDS Client für Windows - Versionsinformationen

Datum: Donnerstag, 29. Juli 2020 um 23 Uhr Ost

Auswirkung: Benutzer werden das VDS Client für Windows Update beim nächsten Start sehen

Verbesserungen

- Rationalisierung des Installationsprozesses – neue Endbenutzer müssen bei der Installation des VDS-Clients für Windows keine Allgemeinen Geschäftsbedingungen mehr akzeptieren

- Fügen Sie während des Installationsprozesses eine Bestätigung hinzu, um zu bestätigen, dass das Gerät des Endbenutzers Zugriff auf den Ort hat, an dem automatische Updates entstehen

Datum: Donnerstag, 27. Mai 2020 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Fehlerbehebungen

- Verbesserte Übersichtlichkeit der angezeigten Fehlermeldung, wenn das angegebene Passwort nicht lang genug ist

Datum: Donnerstag, 13. Mai 2020 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- Zusätzliche Automatisierung, um die Verfügbarkeit der Ressourcen für die Endbenutzer sicherzustellen

Aktualisierungen

- Die URL, die für den Zugriff auf automatische Updates erforderlich ist, ändert sich. Wenn Sie nicht aktiv den eingehenden Verkehr sicher sind, müssen Sie keine Änderungen vornehmen.
 - Alle Endbenutzer können weiterhin auf ihre Desktops zugreifen, auch wenn keine Änderungen vorgenommen werden
 - Organisationen, die den eingehenden Datenverkehr aktiv sichern, müssen sicherstellen, dass Endbenutzer-Geräte Zugriff auf die neuen URLs oben haben, um den Zugriff auf automatische Updates zu gewährleisten
 - Die aktuellen Quellen für Updates sind:
 - Primär: cwc.cloudworkspace.com
 - Sekundär: cloudjumper.com
 - Die neuen Quellen für Aktualisierungen sind:
 - Primär: Bin.vdsclient.App
 - Sekundär: cwc.cloudworkspace.com
 - Neue Benutzer, die den Cloud Workspace Client für Windows installieren, benötigen weiterhin Zugriff auf die aufgeführten URLs "[Hier](#)"

Datum: Donnerstag, 29. April 2020 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Clientupdate beim nächsten Start sehen

(Keine Updates für diese Version)

Datum: Donnerstag, 15. April 2020 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Fehlerbehebungen

- Lösen Sie ein Problem, bei dem die Ergebnisse von Netzwerktests nicht wie vorgesehen gesendet werden

Datum: Donnerstag 1. April 2020 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- Update zu RemoteApp-Anwendungen – beim Starten einzelner Apps werden keine Anmeldeinformationen mehr angezeigt
- Aktualisieren, damit Endbenutzer zwischen der Verwendung von ThinPrint und der Windows-Druckerumleitung zum Drucken wechseln können
- Aktualisieren, damit der VDS-Client für Windows Designer-Benutzer die Druckumleitungsdienste ausschließen kann

VDS 5.4: Donnerstag, 21. Januar 2021

Components: 5.4 Virtual Desktop Service *Wann:* Donnerstag, der 21. Januar 2021 um 22 Uhr - 23 Uhr Eastern

Impact: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- Verbesserte Benutzerfreundlichkeit für Endbenutzer – bessere Handhabung von Benutzern, die aus externen Domänen importiert wurden

Datum: Donnerstag, 11. Juni 2020 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- Aktualisieren Sie den aktuellen AVD RDP-Client, der für die Installation verfügbar ist

Datum: Donnerstag, 28. Mai 2020 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- Aktualisierungen zum NetApp Branding/Phrasieren Hinweis: Dieses neue Branding wird angewendet für:
 - Neue VDS Client-Downloads
 - Vorhandener, nicht bearbeiteter VDS-Client für Windows-Installationen
 - Bestehende benutzerdefinierte Clients erhalten nur dann ein neues Banner-Image, wenn es noch nie angepasst wurde. Wenn das Bannerbild angepasst wurde, bleibt es unverändert. Alle anderen Farben und Ausformulierungen bleiben gleich.

Datum: Donnerstag, 14. Mai 2020 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

- Keine Aktualisierungen dieses Release-Zyklus.

Datum: Donnerstag, 30. April 2020 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Fehlerbehebungen

- Bug Fix für eine Untermenge von Szenarien, in denen kein Self-Service-Passwort zurückgesetzt wurde

Datum: Donnerstag, 16. April 2020 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

- Keine Aktualisierungen dieses Release-Zyklus.

Datum: Donnerstag 2. April 2020 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

- Keine Aktualisierungen dieses Release-Zyklus.

Datum: Donnerstag, 19. März 2020 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

- Keine Aktualisierungen dieses Release-Zyklus.

Datum: Donnerstag, 5. März 2020 um 22 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- Die anmutige Handhabung eines Fransen-Fehlers mit dem RDP-Protokoll, bei dem ältere Anmeldeinformationstypen mit den aktuellen Patches auf einem RDS-Gateway gemischt werden, kann zu einer Verbindung zu Session-Hosts nicht führen
 - Wenn die Workstation des Endbenutzers (ob durch einen externen Administrator, einen internen Administrator oder über die Standardeinstellungen der Arbeitsstation) für die Verwendung älterer Anmeldungstypen eingerichtet ist, besteht die geringe Möglichkeit, dass diese Benutzer vor dieser Version beeinträchtigt haben könnten
- Zeigen Sie im Cloud Workspace Client Designer auf die Schaltfläche Info eine aktualisierte Dokumentationsquelle
- Der automatische Aktualisierungsvorgang für den Cloud Workspace Client Designer wurde verbessert

Datum: Donnerstag, 20. Februar 2020 um 22 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- Proaktive Verbesserung von Sicherheit, Stabilität und Skalierbarkeit

Überlegungen

- Der Cloud Workspace-Client für Windows wird weiterhin automatisch aktualisiert, solange er vor 4 gestartet wird. Wenn ein Benutzer den Cloud Workspace Client für Windows vor 4/2 nicht startet, funktioniert seine Verbindung zum Desktop weiterhin, muss er aber den Cloud Workspace Client für Windows deinstallieren und neu installieren, um die automatische Update-Funktion fortzusetzen.
- Wenn Ihr Unternehmen Webfilterung verwendet, bitte safelist Zugriff auf cwc.cloudworkspace.com und cwc-cloud.cloudworkspace.com, so dass Auto-Update-Funktion bleibt an Ort und Stelle

Datum: Donnerstag, 9. Januar 2020 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

- Keine Aktualisierungen dieses Release-Zyklus.

Datum: Donnerstag, 19. Dezember 2019 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

- Keine Aktualisierungen dieses Release-Zyklus.

Datum: Montag 2. Dezember 2019 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

- Keine Aktualisierungen dieses Release-Zyklus.

Datum: Donnerstag, 14. November 2019 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- Verbesserte Klarheit aus dem Grund, ein Benutzer würde sehen, 'Ihre Dienste sind derzeit offline' Nachricht. Mögliche Ursachen für eine Meldung sind:
 - Der Host-Server der Sitzung ist so geplant, dass er offline ist, und der Benutzer verfügt nicht über die Berechtigungen zum Aktivieren nach Bedarf.
 - Wenn der Benutzer den Cloud Workspace Client verwendet hat, wird angezeigt: „Ihre Dienste sind derzeit offline, wenden Sie sich bitte an den Administrator, wenn Sie Zugriff benötigen.“
 - Wenn der Benutzer das HTML5-Login-Portal verwendet, würden sie sehen: "Ihre Dienste sind derzeit geplant, offline zu sein. Bitte wenden Sie sich an Ihren Administrator, wenn Sie Zugriff benötigen.“
 - Der Host-Server für die Sitzung ist so geplant, dass er online ist, und der Benutzer verfügt nicht über die Berechtigung „Wake-On-Demand“.
 - Wenn der Benutzer den Cloud Workspace Client verwendet hat, wird angezeigt: „Ihre Dienste sind derzeit offline, wenden Sie sich bitte an den Administrator, wenn Sie Zugriff benötigen.“
 - Wenn der Benutzer das HTML5-Login-Portal verwendet, würden sie sehen: "Ihre Dienste sind derzeit offline. Bitte wenden Sie sich an Ihren Administrator, wenn Sie Zugriff benötigen.“
 - Der Host-Server der Sitzung ist so geplant, dass er offline ist, und der Benutzer verfügt über Berechtigungen zum Aktivieren nach Bedarf.
 - Wenn der Benutzer den Cloud Workspace Client verwendet hat, wird angezeigt: „Ihre Dienste sind

derzeit offline, wenden Sie sich bitte an den Administrator, wenn Sie Zugriff benötigen.“

- Wenn der Benutzer das HTML5-Login-Portal verwendet, würden sie sehen: „Ihre Dienste sind derzeit geplant, offline zu sein. Klicken SIE AUF START, um sie online zu bringen und zu verbinden.“
- Der Host-Server für die Sitzung ist online, und der Benutzer verfügt über die Berechtigung „Wake-On-Demand“.
- Wenn der Benutzer den Cloud Workspace Client verwendet hat, würde er sehen: „Bitte lassen Sie 2-5 Minuten, damit Ihr Workspace gestartet wird.“
- Wenn der Benutzer das HTML5-Login-Portal verwendet, würden sie sehen: „Ihre Dienste sind derzeit offline. Klicken SIE AUF START, um sie online zu bringen und zu verbinden.“

Datum: Donnerstag, 31. Oktober 2019 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

- Keine Aktualisierungen dieses Release-Zyklus.

Datum: Donnerstag, 17. November 2019 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- AVD-Elemente hinzufügen:

Datum: Donnerstag, 3. Oktober 2019 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- Verbesserte Handhabung von Code-Signing-Zertifikaten

Fehlerbehebungen

- Beheben Sie ein Problem, bei dem Benutzer, die RemoteApp aufrufen, die keine ihnen zugewiesenen Apps hatten, einen Fehler sahen
- Lösen Sie ein Problem, bei dem ein Benutzer seine Internetverbindung verliert, während er sich beim virtuellen Desktop anmeldet

Datum: Donnerstag, 19. September 2019 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- AVD-Elemente hinzufügen:
 - Wenn der Endbenutzer Zugriff auf AVD-Ressourcen hat, zeigen Sie eine AVD-Registerkarte an
 - Auf der Registerkarte AVD stehen folgende Optionen zur Verfügung:
 - Installieren Sie den AVD RD-Client, falls er nicht bereits installiert ist
 - Wenn der AVD RD-Client installiert ist, starten Sie den RD-Client

- Starten Sie Web Client, um den Benutzer zur AVD HTML5-Anmeldeseite zu bringen
- Klicken Sie auf Fertig, um zur vorherigen Seite zurückzukehren

Datum: Donnerstag, 5. September 2019 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

- Keine Aktualisierungen dieses Release-Zyklus.

Datum: Donnerstag, 22. August 2019 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

- Keine Aktualisierungen dieses Release-Zyklus.

Datum: Donnerstag, 8. August 2019 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

- Keine Aktualisierungen dieses Release-Zyklus.

Datum: Donnerstag, 25. Juli 2019 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

- Keine Aktualisierungen dieses Release-Zyklus.

Datum: Donnerstag, 11. Juli 2019 um 23 Uhr Ost

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

- Keine Aktualisierungen dieses Release-Zyklus.

Datum: Freitag, 21. Juni 2019 um 4 Uhr Eastern

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

- Keine Aktualisierungen dieses Release-Zyklus.

Datum: Freitag, 7. Juni 2019 um 4 Uhr Eastern

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- Aktivieren Sie Cloud Workspace Client, um RDP-Verbindungen automatisch zu starten, unabhängig davon, auf welche Dateart die Zuordnung für rdp-Dateien eingestellt ist

Datum: Freitag, 24. Mai 2019 um 4 Uhr Eastern

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- Verbesserte Leistung während der Anmeldung
- Kürzere Ladezeit bei der Einführung

Datum: Freitag, 10. Mai 2019 um 4 Uhr Eastern

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- Verbesserte Leistung während der Anmeldung
- Kürzere Ladezeit bei der Einführung

Datum: Freitag, 12. April 2019 um 4 Uhr Eastern

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- Verbesserte Anmeldegeschwindigkeit für Wake-on-Demand
- Nach dem erfolgreichen Start des Cloud Workspace Clients für Windows werden wir die Feedback-Schaltfläche entfernen, um Speicherplatz in der Benutzeroberfläche freizugeben

Fehlerbehebungen

- Beheben Sie ein Problem, bei dem die Schaltfläche Anmelden nicht reagiert, nachdem eine Aktion „Wake On Demand“ nicht erfolgreich ausgeführt wurde

Datum: Freitag, 15. März 2019 um 4 Uhr Eastern

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- Administratoren, die den Cloud Workspace-Client für Windows verwenden, zulassen, dass sie eine Support-E-Mail-Adresse ODER eine Telefonnummer angeben, die nicht beides erfordert
- Stellen Sie sicher, dass die HTML5-URL, die im Cloud Workspace Client bereitgestellt wird, eine gültige URL ist – andernfalls ist dies standardmäßig auf <https://login.cloudjumper.com> gesetzt
- Optimierung der Anwendung von Updates für Endbenutzer

Datum: Freitag, 29. Februar 2019 um 4 Uhr Eastern

Auswirkung: Benutzer werden das RDP-Client-Update beim nächsten Start sehen

Verbesserungen

- Der AppData-Ordner wurde aus Gründen der Klarheit von `c:\Users\<username>\appdata\local\RDPClient` in `c:\Users\<username>\appdata\local\Cloud Workspace` verschoben
- Implementierung eines Mechanismus zur Optimierung von Upgrade-Pfaden, wenn ein Benutzer seinen Client nicht in mehreren Versionen aktualisiert hat
- Für Benutzer, die mit der Beta-Version des Clients arbeiten, wurden erweiterte Protokolldetails aktiviert

Fehlerbehebungen

- Während der Aktualisierung werden nicht mehr mehrere Zeilen angezeigt

Datum: Freitag, 15. Februar 2019 um 4 Uhr Eastern

Auswirkung: Benutzer werden das RDP-Client-Update sehen, wenn sie es starten

Verbesserungen

- Aktivieren Sie Optionen für die Installation von Silent/Quiet für Remote-Installationen
 - Die Markierungen für die Installation lauten wie folgt:
 - /S oder /stumm oder /q oder /quiet
 - Diese Flags installieren den Client im Hintergrund – der Client wird nach Abschluss der Installation nicht gestartet
 - /P oder /passiv
 - In beiden Fällen wird der Installationsprozess angezeigt, es sind jedoch keine Eingaben erforderlich, und der Client wird nach Abschluss der Installation gestartet
 - /Nothinprint
 - Schließt ThinPrint aus dem Installationsprozess aus
- Registry-Einträge wurden zu HKLM\Software\CloudJumper\Cloud Workspace Client\Branding hinzugefügt:
 - ClipboardSharingEnabled: True/False – ermöglicht oder disallowed Clipboard-Umleitung
 - RemoteAppEnabled: True/False – ermöglicht oder lässt den Zugriff auf die RemoteApp-Funktionalität zu
 - ShowUnternehmenNameInTitle: True/False – gibt an, ob der Firmenname angezeigt wird oder nicht
- Folgende Dateien können zu c:\Programme (x86)\Cloud Workspace hinzugefügt werden:
 - banner.jpg, Banner.png, banner.gif oder banner.bmp und dies wird im Kundenfenster angezeigt.
 - Diese Bilder sollten im Verhältnis 21:9 liegen

Fehlerbehebungen

- Das registrierte Symbol wurde angepasst
- Leere Telefon- und E-Mail-Einträge auf der Hilfeseite wurden behoben

Frühere Versionen

Virtual Desktop Service – Version 5.3



Für V5.3 von VDS gibt es keine weiteren wiederkehrenden Versionen – alle Versionen werden als Hotfixes betrachtet.

VDS 5.3: Donnerstag, 17. Dezember 2020

Components: 5.3 Virtual Desktop Service *When:* Donnerstag, der 17. Dezember 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.



Der nächste Release-Zyklus wird am Donnerstag, der 7. Januar 2021 statt Silvester 2020.

Virtual Desktop Service

- SMTP-Dienst aktualisieren, um Postmark zu nutzen

VDS 5.3: Donnerstag, 22. Oktober 2020

Components: 5.3 Virtual Desktop Service *When:* Donnerstag, der 22. Oktober 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

VDS

- Bug Fix für Szenarien, in denen sich der MFA-Agent in einem Ordner mit früheren IIT-Namenskonventionen befindet

VDS 5.3: Donnerstag, 8. Oktober 2020

Components: 5.4 Virtual Desktop Service *When:* Donnerstag, der 8. Oktober 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

VDS

- Fehlerbehebung für Provisioning Collections – Hypervisor-Vorlage nicht automatisch ausgewählt

VDS 5.3: Donnerstag, 10. September 2020

Components: 5.3 Virtual Desktop Service *When:* Donnerstag, der 10. September 2020 um 22:00 Uhr bis 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Verringern Sie die Anzahl der API-Aufrufe, die zur Rückgabe einer Liste von Azure-Vorlagen verwendet werden
- Referentielle Link-Aktualisierung im nächtlichen Bericht der Serverressource
- Korrektur für das Ändern von Administratorpasswörtern zur Unterstützung verbesserter, schlankerer Berechtigungssätze in AD

VDS 5.3: Donnerstag, 27. August 2020

Components: 5.3 Virtual Desktop Service *When:* Donnerstag, der 13. August 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Fehlerbehebung für ein Skript-Ereignisszenario, bei dem Datum und Uhrzeit als aktuelles Datum und Uhrzeit angezeigt wurden

Kostenplaner Für Azure

- Hybrid-Benefits-Funktionalität von Azure herausgeben
- Fehlerbehebung für ein Anzeigeproblem, wenn Sie benutzerdefinierte Namensinformationen in die VM-Details eingeben

VDS 5.3: Donnerstag, 13. August 2020

Components: 5.3 Virtual Desktop Service *When:* Donnerstag, der 13. August 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Kostenplaner Für Azure

- Fügen Sie die Unterstützung der Festplatte für kurzlebige Betriebssysteme hinzu
- Verbesserte Tooltips für die Speicherauswahl
- Ein Szenario, in dem ein Benutzer negative Benutzerzahlen eingeben konnte, wird nicht zugelassen
- Zeigen Sie den Dateiserver an, wenn Sie die AVD- und File Server-Auswahl verwenden

VDS 5.3: Donnerstag, 30. Juli 2020

Components: 5.3 Virtual Desktop Service *Wann:* Donnerstag, der 30. Juli 2020 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Desktops und Anwendungsservices für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Fehlerbehebung für eine Gruppe von Szenarien, in denen AVD Diagnostics nicht ordnungsgemäß angezeigt wurde

Kostenplaner Für Azure

- Fragen Sie, ob die Daten des Kunden Hochverfügbarkeit sein müssen, und falls ja, stellen Sie fest, ob Kosten- und Arbeitseinsparungen durch Nutzung eines PaaS-Dienstes wie Azure NetApp Files verfügbar sind
- Aktualisieren und standardisieren Sie den Standard-Storage-Typ für AVD- und RDS-Workloads auf Premium-SSD
- Performance-Verbesserungen hinter den Kulissen

VDS 5.3: Donnerstag, 16. Juli 2020

Components: 5.3 Virtual Desktop Service *When:* Donnerstag, 16. Juli 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Proaktive Sicherheitsverbesserungen hinter den Kulissen
- Leistungsverbesserungen im Workspace-Modul über Paginieren von Gruppen unter der Registerkarte Benutzer und Gruppen

VDS-Einrichtung

- Sobald neue Automatisierungsoptionen verfügbar sind, aktualisieren Sie bei Bereitstellungen mit der Auswahl von Azure Active Directory Domain Services (AADDs), um die Nutzung des Standard Service Tier sicherzustellen
- Aktualisieren, um eine Änderung an einem Microsoft ARM-API-Aufruf widerzuspiegeln

HTML5-Anmeldeerlebnis

- Aktualisierungen zum NetApp Branding/Phrasieren

Kostenplaner Für Azure

- Preisanzeige dynamisch nach Region
- Zeigen Sie an, ob relevante Services in der Region verfügbar sind, um sicherzustellen, dass der Benutzer versteht, ob die gewünschte Funktionalität in dieser Region verfügbar ist. Diese Services sind:
- Azure NetApp Dateien
- Azure Active Directory Domain Services
- NV und NV v4 (GPU aktiviert) virtuelle Maschinen

VDS 5.3: Donnerstag, 25. Juni 2020

Components: 5.3 Virtual Desktop Service *When:* Donnerstag, 25. Juni 2020 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Aktualisierungen zum NetApp Branding/Phrasieren
- Fehlerbehebung für ein isoliertes Szenario, in dem die Liste der Benutzer nicht wie erwartet bestückt war
- Bug Fix für ein Szenario, in dem manuelle Bereitstellungen eine GPO-Konfiguration erhielten, die nur teilweise korrekt war

VDS-Setup-Assistent

- Support für American Express
- Aktualisierungen zum NetApp Branding/Phrasieren

REST API

- Fortlaufende Verbesserungen, mit denen Listendaten schneller erfasst und angezeigt werden können

VDS 5.3: Donnerstag, 11. Juni 2020

Components: 5.3 Virtual Desktop Service *When:* Donnerstag, 11. Juni 2020 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Proaktive Verbesserungen bei der API-Verarbeitung

- Anhaltende proaktive Härtung von Plattformelementen

Cloud Workspace Tools und Services

- Fortwährende Verbesserungen bei Live-Skalierungs-Triggern
- Verbesserte automatische Korrektur von Problemen, die bei der Migration einer Bereitstellung von vCloud zu vSphere erkannt wurden

VDS 5.3 Hotfix: Donnerstag 7. Mai 2020

Components: 5.3 Virtual Desktop Service *Wann:* Mittwoch, der 3. Juni 2020 um 10:00 – 10:30 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Cloud Workspace Tools und Services

- Fehlerbehebung für ein automatisiertes Element der Automatisierung der Plattformbereitstellung Dies gilt nur für völlig neue Implementierungen – bestehende Implementierungen werden nicht beeinträchtigt.
- Bug Fix für Bereitstellungen in einer vorhandenen Active Directory-Struktur

VDS 5.3: Donnerstag, 28. Mai 2020

Components: 5.3 Virtual Desktop Service *When:* Donnerstag, 28. Mai 2020 um 22:00 – 23:00 Uhr Eastern
Impact: der Zugriff auf Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf den Virtual Desktop Service bleibt verfügbar.

Virtual Desktop Service

- Aktualisierungen zum NetApp Branding/Phrasieren
- Leistungsverbesserungen für das Workspace-Modul
- Proaktive Stabilitätsverbesserung VDS-Funktionen mit Unterstützung häufig verwendeter API-Aufrufe

Bereitstellung Von Virtual Desktop Services

- Weitere Optimierung des Platzbedarfs der VDS-Plattform in Azure Implementierungen
- Fehlerbehebung für ein optionales Szenario bei der Bereitstellung in einer vorhandenen Active Directory-Struktur

Virtual Desktop Service Tools und Services

- Laufende Verbesserungen der Anzahl der Benutzer, die bei einem Server angemeldet sind, werden für die Live-Skalierung identifiziert

Virtual Desktop Service Web Client

- Aktualisiertes Branding mit NetApp Branding/Formulierung
- Unterstützung für die Verkürzung von URLs, die als Favoriten gespeichert sind, die länger als die Standard-Web Client-Links zu den Standard-Web-Client-Links sind (z. B. cloudworkspace.com/login/ bis cloudworkspace.com)

Kostenplaner Für Azure

- SQL Server-Optionen für weitere VM-Serien/-Größen hinzufügen
- Aktualisierung auf die Art und Weise, wie IP-Adresspreise angezeigt werden – zeigen Sie die IP-Adresskosten nicht an, es sei denn, es werden zusätzliche IP-Adressen hinzugefügt

CWMS 5.3: Donnerstag, 14. Mai 2020

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 14. Mai 2020 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Kostenplaner Für Azure

- Aktualisierte Angaben zu NetApp Branding/Formulierung
- Aktualisierter Plattform-Server zur Berücksichtigung der Verwendung von D2S v3
- Aktualisierte Windows 10 Enterprise E3 Lizenzdetails und Preispunkt
- Ändern Sie die Standard-Storage-Auswahl zu Azure NetApp Files

CWMS 5.3 Hotfix: Donnerstag 7.Mai 2020

Components: 5.3 Cloud Workspace Management Suite *Wann:* Freitag, der 8. Mai 2020 um 10:15 Uhr – 10:30 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsservices für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Tools und Services

- Fehlerbehebung für die Methode, bei der DNS-Datensätze für eine bestimmte Kombination von Einstellungen während des Bereitstellungsprozesses eingestellt werden

CWMS 5.3: Donnerstag, 30. April 2020

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 30. April 2020 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Verbesserte Sitzungsnachverfolgung für ein zukünftiges Update – die Option zur Vorschau zukünftiger Funktionen
- Aktualisieren Sie auf skriptbasierte Ereignisse, um mehr Flexibilität bei Anwendungen und Aktivitäten zu ermöglichen
- Fehlerbehebung für eine bestimmte Kombination von Provisioning Collections-Konfigurationen

Cloud Workspace Tools und Services

- Ermöglicht das Festlegen von Workload Scheduling pro AVD-Hostpool
- Verbesserte Erstellung neuer Implementierungen in einer vorhandenen AD Struktur
- Aktivieren Sie die Möglichkeit, Datenpfade zu Daten, zu Hause oder Profil für Unternehmen zuzuweisen, die Azure Files verwenden

- Aktivieren Sie die Möglichkeit, Ressourcen-Pools zu managen
- Verbesserte Handhabung von Sonderzeichen im Bereitstellungsassistenten
- Anpassungen automatisierter HTML5-Komponenten im Rahmen der Implementierung für RDS-Workloads (nicht AVD)

REST API

- Aktualisierte Liste der verfügbaren Azure Regionen für die Implementierung
- Verbesserte Handhabung der Azure Backup Integration für Server mit der TSDData-Rolle
- Beheben Sie ein Problem in einer Teilmenge von Szenarien, in denen eine fehlgeschlagene Anmeldung zwei fehlgeschlagene Anmeldeversuche zur Protokollierung führt

CWA-Setup

- Stellen Sie gemäß den Best Practices von Azure fest, dass sich die Subnetz-IP-Details in einem Private IP-Adressbereich befinden. Folgende private IP-Bereiche werden akzeptiert:
 - 192.168.0.0 bis 192.168.255.255
 - 172.16.0.0 bis 172.31.255.255
 - 10.0.0.0 bis 10.255.255.255

HTML5-Anmeldeerlebnis

- Hosting-Verbesserungen hinter den Kulissen für <https://login.cloudworkspace.com> Und <https://login.cloudjumper.com>. Hinweis: Benutzerdefinierte HTML5-Login-Portale werden keine Auswirkungen haben.
- Bug Fix für eine Untermenge von Szenarien, in denen kein Self-Service-Passwort zurückgesetzt wurde

CWMS 5.3 Hotfix: Wedn. April 22, 2020

Components: 5.3 Cloud Workspace Management Suite *Wann:* Mittwoch, der 22. April 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Performance Upgrade für mehr Kundennutzung

CWMS 5.3: Donnerstag, 16. April 2020

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 16. April 2020 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Kontinuierliche Verbesserungen der Validierung der VM-Erstellung von AVD Host Pool (Berücksichtigung von Azure-Prozesszeiten aufgrund eines Anstiegs der Azure-Aktivitäten aufgrund von COVID-19)
- Verbesserung der AVD-Stabilität bei der Initialisierung von AVD – wenn der AVD-Mandantenname nicht global für AVD eindeutig ist, ersetzt CloudJumper ihn durch eine aktualisierte Zeichenfolge, die nur für die Bereitstellung/den Mandanten verwendet wird.

- Unterstützung für Sonderzeichen in E-Mail-Adressen in der CWMS-Funktion zum Zurücksetzen von Kennwörtern einschließen
- Fehlerbehebung für eine Untermenge von Szenarien beim Hinzufügen von Apps zu einer AVD RemoteApp-Gruppe nicht Apps aus dem Startmenü
- Fehlerbehebung für einen Teil des Benutzeraktivitätsberichts
- Entfernen der Anforderung für eine Beschreibung eines AVD-Host-Pools (bleibt als optionales Feld erhalten)
- Bug Fix für ein einzelnes Fransen-Szenario, in dem VMs in einem gemeinsamen Host-Pool als VDI VMs getaggt wurden

CWA-Setup

- Zusätzlicher Support für Bestellcodes für Distributor-Workflows

Cloud Workspace Tools und Services

- Verbesserungen bei der Verwaltung von VMs, die vom Tool Solarwinds Orion RMM verwaltet werden, um das Workload Scheduling zu unterstützen

CWMS 5.3: Donnerstag, 2. April 2020

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 2. April 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Aktivitätsverlauf Behebung eines Anzeigeproblems für regionale Bereitstellungen, bei denen die Datumslokalisierung verhindert hat, dass ein Aktivitätsverlauf in CWMS sichtbar ist
- Erweiterung der Provisioning-Sammlung für Bilder jeder Größe
- Bugfix für AADDs-Bereitstellungen in Azure-Mandanten mit mehreren Domänen – neu erstellte Benutzer würden zuvor die primäre Azure-Domain verwenden, anstatt die Login-ID des Workspace zu entsprechen
- Fehlerbehebung für den Aktivitätsverlauf bei der Aktualisierung eines Benutzernamens – die Funktion funktioniert wie erwartet, der vorherige Benutzername wurde jedoch nicht korrekt angezeigt

CWA-Setup

- Verbesserte Handhabung von MFA bei CWMS-Konten, die bei der Registrierung verwendet werden
- Während der Implementierung wurden reduzierte Berechtigungen angewendet

Cloud Workspace Tools und Services

- Geringere Berechtigungen für laufende Services/Automatisierung erforderlich
- Prozessverbesserungen zur Reduzierung des Ressourcenverbrauchs auf CWMGR1

REST API

- Fehlerbehebung für den Aktivitätsverlauf bei der Aktualisierung eines Benutzernamens

CWMS 5.3 Hotfix: Tues. 24. März 2020

Components: 5.3 Cloud Workspace Management Suite *Wann:* Dienstag, der 24. März 2020 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Kostenplaner Für Azure

- Aktualisierte Beschreibung der AVD-Benutzertypen und der Programme, die sie gemäß Microsoft-Dokumentation ausführen
- Erhöhte Klarheit bei der CWMS-Lizenzierung

CWMS 5.3: Donnerstag, 19. März 2020

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 19. März 2020 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Verbindung zur Serveroptimierung für Bereitstellungen an mehreren Standorten: Automatische Erkennung des Standorts, mit dem der CWMS-Administrator die Verbindung herstellt und verarbeitet
- Durch die Aktivierung des Migrationsmodus wird die Live-Skalierung deaktiviert
- Fehlerbehebung beim Aktivieren neuer Cloud Workspace Services für einen vorhandenen Client

CWA-Setup

- Verbesserungen am Implementierungsassistenten im Hintergrund

CWMS 5.3: Donnerstag, 5. März 2020

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 5. März 2020 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Leistungsverbesserung für den Master Client Report
- Entfernen Sie die Löschfunktion von einer VM, die nicht richtig erstellt wurde, da es nicht gelöscht werden kann, wenn es nie erstellt wurde

Cloud Workspace Tools und Services

- Fehlerbehebung bei der anmutig umkonfigurierten Implementierung von Bereitstellungen an mehreren Standorten, bei denen die DC-Konfigurationseinstellungen nicht ordnungsgemäß konfiguriert sind
- Bug Fix für Bereitstellungen an mehreren Standorten, bei denen vSphere Sites Ressourcen-Zuweisungstypen auf Fixed festgelegt haben

HTML 5-Portal

- Prozessverbesserungen für Benutzer, die sich mit AVD-Anmeldeinformationen anmelden

Kostenplaner Für Azure

- Verbesserung der Übersichtlichkeit bei Live-Skalierung
- Einstellungen so formulieren, dass sie mit Microsoft AVD-Messaging übereinstimmen
- Bug Fix für Details zur Einsparung von Workloads Scheduling und Live-Skalierung in stark angepassten Angeboten

CWMS 5.3: Donnerstag, 20. Februar 2020

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 20. Februar 2020 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Wechseln Sie im Workspaces-Modul auf die Registerkarte VM-Ressource zu Bereitstellung

CWA-Setup

- Optimierung der Anwendung von Richtlinien während der Implementierung
- Erhöhte Sicherheit bei neuen Implementierungen mithilfe von Azure Active Directory Domain Services
- Erhöhte Sicherheit für neue Implementierungen: Erfordert während der Implementierung eine definierte Subnetzisolierung (im Gegensatz zu flachen Subnetzen)
- Bug Fix für RDS-Implementierungen (nicht AVD) im Rahmen der ThinPrint-Lizenzierung
- Bug Fix zur ordnungsgemäßen Handhabung, ob ThinPrint in DC Config installiert ist
- Zusätzliche Überprüfungen und Validierungen für Unternehmen, die sich für die Nutzung der FTP-Funktionalität entscheiden

Cloud Workspace Tools und Services

- Fehlerbehebung für automatische Aktionen, wenn bei einer Implementierung mit mehreren Standorten ein falsch konfigurierter Standort vorliegt
- Bug-Fix für eine Instanz, in der das Löschen einer VM nicht richtig aus der VM hinter den Kulissen
- Funktionsverbesserungen und Fehlerbehebungen beim Testen der Hypervisor-Konnektivität in DC Config

REST API

- Leistungsverbesserungen beim Anzeigen der Benutzerliste für ein Unternehmen
- Leistungsverbesserungen beim Anzeigen der Anwendungsliste für eine Organisation
- Verbesserte Funktionalität beim Hinzufügen von Benutzern zu AVD-Anwendungsgruppen:
- Begrenzen Sie die Anzahl der importierten Benutzer auf 425
- Wenn Sie versuchen, mehr als 425 Benutzer zu importieren, fahren Sie mit dem Import der ersten 425 Benutzer fort und zeigen Sie an, dass AVD-Limit für Benutzerimporte 425 beträgt und dass sie mit zusätzlichen Importen in 5 Minuten fortfahren können
- Aktualisieren, um zu reflektieren, dass die Anzahl der Benutzer in einer Gruppe die Anzahl der Cloud Workspace-Benutzer in einer Gruppe ist, anstatt die Gesamtzahl der Benutzer in einer Gruppe (was bei der Bereitstellung in einer vorhandenen Active Directory-Struktur kleiner sein kann)

- Anwendungszuweisungen über Sicherheitsgruppe für benannte Benutzer aktivieren, die Mitglied der Gruppe sind (verschachtelte Gruppen erhalten die App-Zuweisung nicht)

Kostenplaner Für Azure

- Fügen Sie am Ende der Seite einen Link hinzu, damit Benutzer Hilfe anfordern können
- Standard-Azure NetApp Files auf die Premium-Stufe
- Fügen Sie der Auswahl für den Fileserver-Storage-Typ Premium-SSD hinzu
- Update-Text für Azure Active Directory-Domänendienste – Wechsel von AADDS zu Azure AD-Domänendiensten
- Update Text für Active Directory – Wechsel von Windows Active Directory-VMs zu Windows Server Active Directory

CWMS 5.3 Hotfix: Donnerstag, 13. Februar 2020

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 13. Februar 2020 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Kostenplaner Für Azure

- Fehlerbehebung bei Preisfehlern bei der Verwendung von VMs der E-Series in einem Teil der Szenarien

CWMS 5.3: Donnerstag, 6. Februar 2020

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 6. Februar 2020 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Verbesserte Details zum Bereitstellungsstatus bei der Erstellung von VMs
- Verbesserte Handhabung der Automatisierung von neu erstellten Host-VMs, die Teil eines AVD-Host-Pools sind
- Leistungsverbesserung im Benutzeraktivitätsbericht, wenn „nur Server-Benutzer“ eingeschlossen wird

Cloud Workspace Tools und Services

- Bug Fix für das Datenpfadmanagement, wenn Administratoren Benutzerkonten manuell im herkömmlichen (nicht Azure) Active Directory bearbeiten
- Verbesserte Workload-Planungsstabilität in differenzierten Szenarien

Kostenplaner Für Azure

- Beschreiben Sie die spezifischen Einsparungen, die durch Workload Scheduling und Live-Skalierung separat im Vergleich zu erzielen sind Kombiniert
- Zeigen Sie die S-Versionen von Servern an, um Premium (SSD) Storage zu unterstützen
- Verbessertes Layout für gedruckte Schätzungen
- Fehlerbehebung für ein Problem, bei dem die Preise für SQL Server nicht korrekt berechnet wurden

CWMS 5.3: Donnerstag, 23. Januar 2020

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 23. Januar 2020 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Leiten Sie die ältere um <https://iit.hostwindow.net> Die moderne Anlage <https://manage.cloudworkspace.com>
- Fehlerbehebung für einen Teil der CWMS-Administratoren, die sich über IE 11 anmelden
- Korrigieren Sie ein visuelles Problem, bei dem das Löschen eines API-Benutzers sie hinter den Kulissen korrekt gelöscht hat, aber in CWMS nicht als gelöscht angezeigt wurde
- Optimieren Sie den Vorgang des Löschvorgangs von Abonnements, damit Sie eine neue/Testumgebung neu bereitstellen können
- Erweiterung der Dienstplattine – nur auf Sitzungshostservern, die online sind, um Symbole für Anwendungsverknüpfungen zu platzieren

Cloud-Ressourcenapplikation

- Unterstützung beim Importieren von Benutzern aus einer OU- oder Active Directory-Sicherheitsgruppe über die Befehlszeile

Cloud Workspace Tools und Services

- Verbesserungen der Live-Skalierung im Hintergrund

CWA-Setup

- Verbesserte Handhabung von Szenarien, wenn das Konto während des CWA-Setup-Prozesses MFA angewendet hat

Kostenplaner Für Azure

- Update VM Dimensionierung standardmäßig zu spiegeln Microsoft-Empfehlungen

CWMS 5.3: Donnerstag, 9. Januar 2020

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 9. Januar 2020 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Aktualisieren von Formulierungen in der E-Mail erhalten Administratoren nach dem Erstellen eines neuen Arbeitsbereichs, um aktualisierte Links wiederzugeben
- Fehler beheben für ein Problem, bei dem Server nicht in der Liste Server angezeigt wurden, wenn eine Reihe von Fehlern in der Ordnerberechtigung vorhanden war
- In der Server-Liste wurde kein Bug Fix für Server angezeigt, wenn kein Ressourcen-Pool in der Tabelle „Ressourcenpools“ in CWMGR1 vorhanden war

Cloud-Ressourcenapplikation

- Unterstützung beim Importieren von Benutzern aus einer Active Directory-Sicherheitsgruppe.
- Verbesserte Validierung – Stellen Sie sicher, dass für Kommandozeilenparameter/Server der richtige Befehlszeilenparameter verwendet wird
- Verbesserte Validierung – beim Importieren aus der Befehlszeile auf doppelte Benutzer prüfen
- Verbesserte Validierung – Stellen Sie sicher, dass die importierten Server zu der Site gehören, die beim Importieren aus der Befehlszeile angegeben wurde

REST API

- Weitere Sicherheitserweiterungen im Hintergrund

Cloud Workspace Tools und Services

- Verbesserte Stabilität bei der Befehlsverarbeitung hinter den Kulissen
- Verbesserungen bei Workload Scheduling und Live Scaling hinter den Kulissen
- Zusätzliche Stabilität bei Workload Scheduling und Live-Skalierung im Hintergrund
- Updates und Verbesserungen an FSLogix in neuen Bereitstellungen – Weiterleiten von Downloads und Favoriten in den Profilcontainer, um die Best Practices zu berücksichtigen
- Zusätzliche Stabilitätsverbesserungen bei der Erstellung von Host-Pools für Virtual Machines
- Geben Sie die Möglichkeit an, das Gateway für neue Standorte anzugeben
- Verbesserte Automatisierungsvalidierung für VMs
- Verbessertes automatisiertes Datenbankmanagement
- Verbesserte Handhabung der Benutzererstellung, wenn die Aktion exakt zur gleichen Zeit ausgeführt wird, wenn VMs heruntergefahren werden
- Optimierte Handhabung von temporären Festplatten in Microsoft Azure Implementierungen
- Verbesserte Handhabung der Ressourcenzuweisung für GCP-Implementierungen
- Bug Fix für Laufwerkserweiterung in den Rechenzentren ProfiBricks
- Verbesserte Stabilität für die Client-Erstellung auf Basis von App Services
- Fehlerbehebung und Stabilitätsverbesserungen nach dem Konvertieren eines Servers von einer Rolle zur anderen

CWMS 5.3 Release: Fr., 20. Dezember 2019

Components: 5.3 Cloud Workspace Management Suite *Wann:* Freitag, 20. Dezember 2019 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Tools und Services

- Beheben Sie das Szenario, in dem die Benutzeraktivitätsprotokollierung keine Daten erfolgreich aufzeichnet

CWMS 5.3: Donnerstag, 19. Dezember 2019

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 19. Dezember 2019 um 22 Uhr –

23 Uhr Eastern *Impact*: der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Verbesserungen bei der CWMS-Verfügbarkeitsüberwachung
- Beheben Sie ein Problem mit dem Anwender der AVD-App-Gruppe Modal, bei dem der Benutzername nicht immer richtig ausgewählt wird, wenn er Großbuchstaben enthält
- Fix für Paginierung in der Benutzerliste für 'User Support only' Admin-Rollenmitglieder
- Korrektur zur Ausrichtung der Optionsfelder im MFA-Setup-Dialog
- Verbesserung der Seitenladung Dashboard/Übersicht durch Entfernen der Abhängigkeit der Serviceboard
- Beheben Sie das Problem, bei dem Admin-Benutzer ihre eigenen Passwörter nicht zurücksetzen können, wenn sie keine Administratorberechtigungen für die Bearbeitung besitzen
- Verbesserungen beim Sammeln der Debug-Protokollierung für zukünftige Fehlerbehebung

Cloud-Ressourcenapplikation

- Feature Enhancement: Import von Benutzern auf der Basis von AD-Gruppenmitgliedschaft zulassen.
- Feature Enhancement: Vorgabe der Standard-Anmelde-ID während des Imports zulassen

Kostenplaner Für Azure

- Verbesserung von Text und Tooltip zum Speicher unter VMs

CWA-Setup

- Verbesserungen beim Workflow für die Implementierung freigeben

Cloud Workspace Tools und Services

- Verbesserung Handling der Sperrung des Datenservers bei der Erstellung neuer Benutzer
- Behebung eines Szenarios, in dem ein Client während der Workload-Planung falsch als Cache-Unternehmen gekennzeichnet ist
- Beheben Sie, um die Unternehmenstabelle korrekt zu aktualisieren, wenn eine Organisation ohne Arbeitsbereich erstellt wird
- Korrektur für ungültige Zeichen, die dem AVD-Host-Pool-Namen in der lokalen Steuerplandatenbank angehängt sind
- Beheben Sie Probleme mit der Workload-Planung, wenn eine VM in der lokalen Kontrollebendatenbank, nicht aber im Hypervisor aufgeführt ist
- Das Problem beheben, dass einige VMs nicht automatisch im Azure Hypervisor erweitert werden
- Korrektur für Client Provisioning Fehler 'Supplied Data drive not valid'
- Beheben Sie in bestimmten Szenarien den Fehler bei der Installation von CWAgent
- Verbesserung für TestVDCTools, um die Zuweisung von RDS-Gateway-URL während der Erstellung einer neuen Site zu ermöglichen
- Fix für Workload-Scheduling-Fehler in einigen Szenarien, wo es auf 'disabled' gesetzt ist
- Beheben Sie Probleme beim Starten von Servern, wenn sich der Server noch im Cache befindet

- Einige VMs können nach der automatischen Laufwerkserweiterung nicht mehr eingeschaltet werden
- Beheben Sie Probleme beim Verwalten von Ordnern/Berechtigungen bei Verwendung von Azure Dateien oder Azure NetApp Files

CWMS 5.3 Version: Mo. Dezember 2019

Components: 5.3 Cloud Workspace Management Suite *Wann:* Montag, 2. Dezember 2019 um 22:00 – 23:00 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Verbesserungen bei automatisierten FSLogix-Installationen
- Updates und Korrekturen zu Live-Skalierung
- Fügen Sie AMD (nicht-GPU) VMs zur Dropdown-Liste in CWMS hinzu
- Unterstützung mehrerer Mandanten in derselben AVD-Implementierung

CWA-Setup

- Verbesserungen bei der Übersichtlichkeit im Abschnitt Hilfe/Support CWA Setup

Kostenplaner Für Azure

- Fehlerbehebung für ein Szenario, in dem die Auswahl, Microsoft-Lizenzierung nicht in die Schätzung einzubeziehen, weiterhin diese enthält

Cloud-Ressourcenapplikation

- Zusätzliche Validierung bei Verwendung der Befehlszeilenfunktion der Datacenter-Site
- Neues Befehlszeilenargument – /listserversinsite
- Konfigurationserweiterung – beim Importieren eines Unternehmens legen Sie nun die RDSH-Bereitstellung so fest, dass das für den Standort konfigurierte RDHS-Gateway verwendet wird

Cloud Workspace Tools und Services

- Aktualisierte vCloud Support-Elemente in DC Config
- Erweiterung zu TestVDCTools zur korrekten Erkennung des Servertyps in spezifischen Szenarien

Veröffentlichung des KWMS 5.3: Donnerstag, 14. November 2019

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 14. November 2019 um 22 – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Zusätzliche Redundanz/Hochverfügbarkeit, die hinter den Kulissen hinzugefügt wurde
- Dropdown-Menüs in CWMS werden durchsucht
- Leistungsverbesserungen bei Verwendung des Workspaces-Moduls
- Leistungsverbesserungen bei Verwendung des Abschnitts Server des Arbeitsbereichs

- Zeigt den Host-Pool-Namen im Abschnitt Server des Arbeitsbereichs an
- Der Abschnitt Server des Arbeitsbereichs wird nun mit jeweils 15 Servern paginiert
- Fehlerbehebung für ein Szenario, in dem eine Untergruppe von Administratoren, die einen neuen Host Pool erstellen, keine VM-Vorlagen sehen würde
- Fehlerbehebung für ein Szenario, in dem die Navigation zu einem Host-Pool durchgeführt wird, dann zeigt ein zweiter Host-Pool manchmal Informationen aus dem ersten Host-Pool an
- Fehlerbehebung, bei dem sich eine Untergruppe von Administratoren nicht bei einer älteren Version von CWMS anmelden konnte
- Fehler beheben, bei der die Navigation zu AVD Diagnostics und dann zurück zu Workspaces angezeigt wird 'page not found'
- Ändern Sie den freundlichen Namen des Desktop eines Benutzers (was im AVD RDP-Client und in der blauen Leiste oben auf der Benutzersitzung angezeigt wird), um den Namen des Host-Pools anzupassen
- Server müssen manuell dem Pool mit dem Kontrollkästchen „Neue Sitzungen zulassen“ hinzugefügt werden, das standardmäßig deaktiviert ist. Das Kontrollkästchen wurde bereits standardmäßig aktiviert.

CWA-Setup

- Bereitstellungen verwenden jetzt automatisch FSLogix
- Fügen Sie Azure Files als optionales Speicherziel für den Daten-, Home- und Profilspeicher hinzu, wenn die Bereitstellung Azure Active Directory-Domänendienste verwendet
- Implementieren Sie ein Paket, um die Bereitstellungsautomatisierung zu unterstützen, wenn Azure Mandanten die rollenbasierte Zugriffssteuerung aktiviert haben
- Installieren Sie mit jeder Implementierung die neueste Version der Java- und HTML5-Lizenzierung
- Fehlerbehebung, wenn ein Subnetz-Bereich falsch berechnet wurde, was vor der Bereitstellung einen Validierungsfehler verursacht

HTML5-Anmeldeerlebnis

- Aktualisieren Sie das Standard-Branding, um das Branding des Cloud Workspace Client für Windows wiederzugeben. Eine Vorschau finden Sie hier.
- Installieren Sie in-Place-Branding-Updates auf weiteren HTML5-Anmeldeseiten

Kostenplaner Für Azure

- Aktualisieren Sie den Standard-Speicher-Tier für D4s v3-VMs (der Standard-VM-Typ für AVD) auf Premium-SSD, um die Standardeinstellung von Microsoft zu entsprechen

Cloud-Ressourcenapplikation

- Hinzufügen der Möglichkeit, einen Unternehmenscode vorab für die Verwendung während des Imports zuzuweisen

CWMS 5.3: Donnerstag, 31. Oktober 2019

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 31. Oktober 2019 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Update für Benutzer, die sich bei iit.hostwindow.net anmelden (die URL für die älteren v5.2-Bereitstellungen, von denen es nur wenige gibt) wird eine Aufforderung angezeigt, sie zu manage.cloudworkspace.com zu navigieren (die URL für v5.3 und zukünftige Bereitstellungen)
- Benutzer können AVD-Hostpools über CWMS löschen
- Verbesserung, die zukünftige Branding-Verbesserungen in CWMS ermöglicht
- Fehlerbehebung bei der Validierung einer VDI Provisioning Collection

Automatisierung Von Bereitstellungen

- Verbesserungen bei der automatisierten Problembehebung und Prozessoptimierung hinter den Kulissen

HTML5-Anmeldeerlebnis

- Wir werden eine Reihe von Verbesserungen bezüglich der Benutzerfreundlichkeit vornehmen, wenn sich Endbenutzer von login.cloudjumper.com oder login.cloudworkspace.com bei ihren virtuellen Desktops anmelden:
- Benutzer können die AVD-Hostpools anzeigen, auf die der Benutzer Zugriff hat
- Aktivieren Sie die Funktion „Wake-On-Demand“ für Benutzer mit den entsprechenden Berechtigungen, damit sie sich anmelden und zu einer Zeit arbeiten können, in der eine AVD-Host-VM offline sein soll
- Aktivieren Sie Self Service Password Reset für Benutzer, die in ihrem Benutzerkonto in CWMS eine E-Mail oder Telefonnummer festgelegt haben

Kostenplaner Für Azure

- Benutzern ermöglichen, Windows Active Directory-VMs auszuwählen, nachdem sie Anwendungsbeispiele von AVD für AD Connect ausgewählt haben
- Aktualisieren Sie die Standardspeichermenge für alle VMs auf 128 GB, um den Standardwert von Microsoft zu entsprechen
- Aktualisieren Sie die Standardeinstellung für Betriebszeitstunden auf 220, um den Standardwert von Microsoft zu entsprechen
- Aktualisieren Sie die Namen der Workload-Typen, um den Namen zu entsprechen, in die Microsoft sie geändert hat

CWMS 5.3: Donnerstag, 17. Oktober 2019

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 17. Oktober 2019 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Unterstützung für Server 2019 als Betriebssystem für den Arbeitsbereich einer Organisation
- Aktualisierung zur Verbesserung der Anzeige aktiver Benutzer in einem AVD-Hostpool
- Zulassen für mehrere Organisationen/Arbeitsbereiche unter einer AVD-Bereitstellung
- Schaltfläche „Aktualisieren“ hinzufügen, um mehrere Felder zu bearbeiten, die einem Administrator zugeordnet sind

- Fügen Sie die Schaltfläche „Aktualisieren“ hinzu, um Firmendaten und Kontaktinformationen zu bearbeiten
- Suchfunktion aktualisiert, um Flight School zu nutzen
- Links unten im KWMS aktualisiert
- Verwendung eines Validierungspools in AVD-Bereitstellungen ermöglichen – dies ermöglicht einen früheren Zugriff auf AVD-Funktionen, bevor diese verfügbar sind (Produktionsversion).
- Beheben Sie die Fehlerbehebung in einer Eingabeaufforderung, die auf eine Aktion reagiert, die von einem Administrator bei einer AADDs-Bereitstellung ausgeführt wurde
- Fehlerbehebung für eine Eingabeaufforderung für einen Administrator, der keine Berechtigungen für App-Dienste besitzt

REST API

- Unterstützung für Server 2019 als Betriebssystem für den Arbeitsbereich einer Organisation
- Bug fix für ein Szenario, in dem Anruf würde die Dienste eines Kunden als offline zurück

Automatisierung Von Bereitstellungen

- Fehlerbehebung für die automatische Generierung des Namens der Datacenter-Site
- Protokolldateien zusammengefasst und verschoben in c:\Programme auf c:\ProgramData

Cloud Workspace Tools und Services

- Unterstützung für den Zugriff auf Vorlagen aus der Azure Shared Image Gallery
- Verbesserung der Sicherheit – reduzierte Verwendung von Administratorkonten durch Ändern des Speicherorts von Protokolldateien von c:\Programme in c:\ProgramData (auch eine aktualisierte Best Practice von Microsoft)
- Erweiterung zur Erstellung von Rechenzentren in VDCTools – Standorte können mit einem Leerzeichen im Namen erstellt werden
- Feature Add für die automatische Erstellung von Rechenzentren Site – nun kann der Adressbereich automatisch ausgewählt werden
- Feature Add: Fügen Sie die Konfigurationsoption hinzu, um nicht verwaltete VHD-Dateien als Vorlagen zu verwenden
- Unterstützung für das Zuweisen einer VM-Serie/-Größe in der Provisioning-Sammlung
- Fehlerbehebung für eine Reihe von Szenarien, in denen eine Einstellung des Lizenzservers nicht ordnungsgemäß angewendet wurde
- Fehlerbehebung – Löschen von temporären Ordnern nach der Bereitstellung wie vorgesehen
- Fehlerbehebung für ein Szenario beim Erstellen eines Servers in Azure, der dieselbe IP-Adresse hat wie eine bereits verwendete VM

Kostenplaner Für Azure

- Die Preise aktualisieren, um zu berücksichtigen, dass AVD-Kunden für Linux-OS-VMs statt für Windows-OS-VMs bezahlen
- Option zur Integration der entsprechenden Microsoft-Lizenzierung hinzugefügt
- Update auf Speicher-Standardereinstellungen verwendet gemäß Microsofts aktualisierten Rechner (flach vs Benutzeranzahl)

- SQL-Preis für D4s v3 VMs hinzufügen
- Fehlerbehebung für ein Anzeigeproblem bei der Bearbeitung von VMs

CWMS 5.3: Donnerstag, 3. Oktober 2019

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 3. Oktober 2019 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Workflow-Verbesserung, bei der das Klicken auf „Zurück“ die Benutzer auf die Registerkarte Workspace statt auf die Registerkarte Organisationen zurückgibt
- Bei der Bereitstellung von Cloud Workspaces in Azure über CWMS bestätigen Sie, dass AADDS während des Validierungsschritts erfolgreich validiert wurde
- Unterstützung für Benutzernamen bis zu 256 Zeichen

CWA-Setup

- Systemverbesserungen zur Erinnerung an verknüpfte Partnerkonten für den Fall, dass der Benutzer sein Konto mit CWMS verknüpft, die Bereitstellung der Bereitstellung jedoch zum ersten Mal nicht abgeschlossen hat
- Fehlerbehebung für einen javascript-Fehler bei der Auswahl eines Mandanten zur Bereitstellung einer Cloud Workspace-Implementierung während des CSP-Workflows

Kostenplaner Für Azure

- Fügen Sie eine Option hinzu, um die Microsoft-Lizenzierung im Azure Cost Estimator anzuzeigen oder nicht anzuzeigen
- Wenn Sie diese Option nicht aktivieren (Standardverhalten), wird davon ausgegangen, dass das Unternehmen bereits Eigentümer der Microsoft-Lizenzierung über seine EA oder die bestehende Microsoft/Office 365-Lizenzierung ist
- Aktivieren dieser Option wird die Lösung um umfassendere, TCO-Kenntnisse vermittelt
- Bug Fix, wo die Betriebszeit bei einem Umschalten der Benutzer um jeweils 15 Minuten lang nicht verfügbar war
- Bug Fix für ein Szenario, in dem Benutzer den Tag so einstellen, dass er nachmittags/abends beginnt (PM-Einstellung) und am Morgen endet (AM-Einstellung).

CWMS 5.3: Donnerstag, 19. September 2019

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 19. September 2019 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Standardmäßig ist der Typ der Ressourcenzuordnung einer Azure-Bereitstellung auf Fixed gesetzt; wobei die VM-Serie/Größe ausgewählt ist, die vom Administrator in CWMS definiert wird
- Fügen Sie die Suchfunktion für die Audit-Funktion für Benutzeraktivitäten hinzu
- Verbesserung der Erstellung von Großbenutzern – Aktivieren Sie beim Importieren von Benutzern die

Funktion „Kennwortänderung bei der nächsten Anmeldung erzwingen“

- Fehlerbehebung bei falscher Anzeige der Warnung zum Inaktivitätszeitlimit von Sitzungen nach 5 Minuten statt 55 Minuten
- Benutzerunterstützungsrollenfix – eine Untergruppe von Administratoren mit dieser Rolle konnte die Liste der Benutzer für ihr Unternehmen nicht sehen
- Korrektur der Benutzersortierung: Die Sortierung nach Nutzernamen funktioniert wie vorgesehen, anstatt nach Status zu sortieren
- Die Heartbeat-Funktion wurde dem Abschnitt Übersicht der Registerkarte Bereitstellungen hinzugefügt. Dies zeigt an, bei der letzten Abfrage der Bereitstellung angezeigt wurde, um zu sehen, ob sie online ist
- Workflow-Verbesserungen: Wenn Sie im AVD-Modul auf „Zurück“ klicken, werden Sie nun anstelle des Organisationsmoduls mit dem Workspaces-Modul ausgestattet
- Stellen Sie sicher, dass der Master Client-Bericht vorhanden ist; verbergen Sie den nicht anwendbaren SPLA-Bericht für nicht-Master-Softwarepartner

Cloud Workspace Tools und Services

- Entfernen Sie den ThinPrint Standard-Agent von den Azure Virtual Desktop (AVD) Servern in den Host-Pools, da dies nicht der unterstützte ThinPrint Agent für AVD ist. Stattdessen sollten Unternehmen ThinPrint über ihre ezeep Lösung kontaktieren.
- Verbesserte Kennwortverschlüsselung im Hintergrund
- Fehlerbehebung bei der Passwortumsetzungsbenachrichtigung (PEN), bei der die Funktion „Passwort bei der nächsten Anmeldung ändern“ nicht wie vorgesehen funktioniert, wenn ein Administrator in CWMGR1 das Ablaufdatum des Kennworts auf Null gesetzt hat

Cloud Workspace für Azure Setup-App

- Fix für internationale Administratoren – dieser auf länger erfordert einen Staat, wenn das Land nicht die Vereinigten Staaten ist.
- Wenden Sie CloudJumper über Partner Admin Link (PAL) an, um Azure-Bereitstellungen auf Abonnementebene vorzustellen und zu zukünftig zu nutzen

CWMS 5.3: Donnerstag, 5. September 2019

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 5. September 2019 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

- Aktualisierungen für die Rolle „nur Benutzer-Support“:
- Hinzufügen der Funktionalität Suchen nach/Filtern von Benutzern
- Spalte „Verbindungsstatus“ für Benutzer und deren Verbindungen einschließen
- Geben Sie Zugriff auf die Funktion Kennwortänderung bei der nächsten Anmeldung erzwingen
- Sichtbarkeit der Funktion Löschen des Clients entfernen
- Abmeldung von KWMS nach 1 Stunde Inaktivität erzwingen
- Beheben Sie ein Problem mit der Anzeige, bei dem VM-Serien/Größen falsch angezeigt wurden, wenn VM-Rollen angezeigt werden, deren Ressourcenzuordnungstyp auf „repariert“ eingestellt ist

- Beheben Sie ein Anzeigeproblem, bei dem in Umgebungen mit Einstellung Workload Scheduling auf „Always Off“ fehlerhafte Einstellungen in CWMS angezeigt wurden, obwohl die Einstellung „Always Off“ hinter den Kulissen korrekt eingestellt war
- Aktualisierung von Berechtigungen – Entfernen der Registerkarte Ressourcenplanung, wenn der CWMS-Administrator keinen Zugriff auf die Funktion Ressourcen in CWMS hat
- Entfernen Sie die Möglichkeit, mehr als eine VM-Instanz in einem VDI-Benutzer-Host-Pool hinzuzufügen
- Fehlerbehebung für max. Benutzer pro Session-Host in einem AVD-Hostpool anzeigen – diese Werte entsprechen jetzt den Werten, die im Abschnitt Live-Skalierung der Registerkarte Workload Scheduling festgelegt sind

Cloud-Ressourcenapplikation

- Aktualisierte Funktionen – Unterstützung für die Verwendung von Command Line

Cloud Workspace Tools und Services

- Unterstützung der vCloud Rest-Schnittstelle

Veröffentlichung des CWMS 5.3: 22. August 2019

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 22. August 2019 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.3 Cloud Workspace Management Suite

- Fügen Sie der Registerkarte AVD eine Nachricht hinzu, in der unter welchen Umständen AVD unterstützt wird
- Workflow-Verbesserungen bei der Rückkehr von der Registerkarte AVD zum Arbeitsbereich
- Textbearbeitung in den Anweisungen auf dem AVD-Modul

5.3 Cloud Workspace for Azure Setup

- Entfernen Sie die Anforderung zur Eingabe eines Status, wenn sich der Kunde außerhalb der USA registriert
- CWMGR1 wird nun als D-Series-VM zur ursprünglichen Implementierung implementiert und dann nach der anfänglichen Implementierung kostenmäßig auf B2ms verschoben

Cloud Workspace Tools und Services

- Bug Fix für das SSL-Zertifikatmanagement in Legacy (2008 R2)-Umgebungen
- Zusätzliche Zustandsprüfungen für die Durchsetzung von Zertifikaten und das Lifecycle Management

Veröffentlichung des CWMS 5.3: 8. August 2019

Components: 5.3 Cloud Workspace Management Suite *Wann:* Donnerstag, 8. August 2019 um 22 Uhr – 23 Uhr Eastern *Impact:* der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.3 Cloud Workspace Management Suite

- Fehlerbehebung für eine Untergruppe von Szenarien, in denen die Verbindung zu CWMGR1 von CWMS nicht wie erwartet funktioniert

Cloud Workspace Management Suite – Version 5.2



Es wird keine weiteren wiederkehrenden Versionen für v5.2 von CWMS geben – alle Versionen werden als Hotfixes betrachtet.

CWMS 5.2 Release: Mo., 2. Dezember 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Montag, 2. Dezember 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Keine Aktualisierungen dieses Release-Zyklus.

Veröffentlichung des KWMS 5.2: Donnerstag, 14. November 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 14. November 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Keine Aktualisierungen dieses Release-Zyklus.

CWMS 5.2: Donnerstag, 31. Oktober 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 31. Oktober 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Keine Aktualisierungen dieses Release-Zyklus.

CWMS 5.2: Donnerstag, 17. Oktober 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 17. Oktober 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Keine Aktualisierungen dieses Release-Zyklus.

CWMS 5.2: Donnerstag, 3. Oktober 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 3. Oktober 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Keine Aktualisierungen dieses Release-Zyklus.

CWMS 5.2: Donnerstag, 19. September 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 19. September 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

Der Ressourcen-Zuweisungstyp einer Azure-Bereitstellung wird standardmäßig auf „Fixed“ gesetzt; Wenn die VM-Serie/Größe ausgewählt ist, die vom Administrator in CWMS definiert wurde Add search functionality for User Activity Audit functionality Bug fix for infaltim dichintivity Warnung after 5 minutes instead of 55 minutes User Support Role fix – a Subset of Admins with this role Konnte die Liste der Benutzer für ihre Organisation nicht sehen Benutzersortierung – Sortierung nach Nutzernamen funktioniert wie vorgesehen anstatt nach Status sortiert Sicherstellen Sie, dass der Master Client Report vorhanden ist; verbergen Sie den nicht anwendbaren SPLA-Bericht für nicht-Master-Softwarepartner

Cloud Workspace Tools und Services

Verbesserte Kennwortverschlüsselung hinter den Kulissen Bug fix for Password Enforcement Notification (PEN), bei dem die Verwendung der Funktion „Passwort bei der nächsten Anmeldung ändern“ nicht wie vorgesehen funktioniert, wenn ein Administrator in CWMGR1 die Passwortablaufdaten auf Null gesetzt hat

Setup-App für Cloud Workspace für Azure

Fix für internationale Administratoren – dieser auf länger erfordert einen Staat, wenn das Land nicht die Vereinigten Staaten ist. Wenden Sie CloudJumper über Partner Admin Link (PAL) an, um Azure-Bereitstellungen auf Abonnementebene vorzustellen und zu zukünftig zu nutzen

CWMS 5.2: Donnerstag, 5. September 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 5. September 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

Aktualisierungen für die Rolle „nur Benutzer-Support“: * Hinzufügen der Funktionalität Suchen nach/Filtern von Benutzern * Spalte Verbindungsstatus für Benutzer und ihre Verbindungen einschließen * Zugriff auf die Funktion Kennwortänderung bei Nächster Anmeldung erzwingen * Sichtbarkeit der Funktion Löschen des Clients nach 1 Stunde Inaktivität abmelden Beheben eines Anzeigeproblems Wenn VM-Serien/Größen bei der Anzeige von VM-Rollen, deren Ressourcenzuordnungstyp auf Behobene Korrektur gesetzt ist, für ein Anzeigeproblem falsch angezeigt wurden, bei dem in CWMS fehlerhafte Einstellungen in Umgebungen mit Einstellung „Workload Scheduling“ auf „Always Off“ angezeigt wurden, Trotz der korrekten Einstellung „immer aus“ hinter den Kulissen Update Berechtigungen – entfernen Sie die Registerkarte Ressourcenplanung, wenn der CWMS-Administrator keinen Zugriff auf die Funktion „Ressourcen“ in CWMS hat

Cloud-Ressourcenapplikation

Aktualisierte Funktionen – Unterstützung für die Verwendung von Command Line

Cloud Workspace Tools und Services

Unterstützung der vCloud Rest-Schnittstelle

CWMS 5.2: Donnerstag, 22. August 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 22. August 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Cloud Workspace Management Suite

Beheben eines Anzeigeproblems im Benutzerprofil für einige Monitorgrößen Hinzufügen einer klärenden Nachricht für nicht dynamische App-Dienste Benachrichtigung von Administratoren, dass es einige Minuten dauern kann, bis Änderungen wirksam werden Neue Schaltfläche hinzufügen für nicht dynamische App-Dienste, um es einfacher zu sagen, ob neue Clients/Benutzer haben Wurde hinzugefügt

Einrichtung von Cloud Workspace für Azure

Unterstützung von MFA für den Registrierungsprozess hinzufügen, wenn eine Verknüpfung zu einer vorhandenen CWMS-Kontoverbesserung zu Anweisungen nach der Bereitstellung – Link zu neuen und verbesserten öffentlichen KB Verbesserung zu Anweisungen nach der Bereitstellung – Link wird in einer neuen Registerkarte geöffnet

Cloud Workspace Tools und Services

Bug Fix für SSL-Zertifikatmanagement in Legacy (2008 R2)-Umgebungen Weitere Zustandsprüfungen für die Durchsetzung von Zertifikaten und das Lifecycle Management

CWMS 5.2: Donnerstag, 8. August 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 8. August 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Keine Updates für diese Version.

CWMS 5.2: Donnerstag, 25. Juli 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 25. Juli 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 CWA-Einrichtung

Eine Nachricht nach der Bereitstellung anzeigen, die CWA Setup-Benutzer an die CloudJumper Public KB leitet, wo sie die nächsten Schritte überprüfen können und wie sie ihre Bereitstellung verfeinern verbesserte Handhabung von Ländern außerhalb der USA während des Registrierungsvorgangs hinzugefügt ein Feld, um das Passwort des neu erstellten CWMS zu bestätigen melden Sie sich während des CWA-Setup-Prozesses SPLA-Lizenzierung entfernen unter Umständen, in denen RDS-Lizenzen nicht erforderlich sind

5.2 Cloud Workspace Management Suite

Verbesserte HTML5-Verbindungsverwaltung für CWMS-Administratoren in Einzelserver-Bereitstellungen Fehlerfix für ein Szenario, in dem die Verarbeitung eines Benutzers neu gestartet wird (wenn es zuvor gescheitert war) Das Ergebnis war eine „Internal Server Error“-Meldung SPLA-Lizenzabschnitt entfernen unter Umständen, in denen RDS-Lizenzen nicht erforderlich sind, einschließlich der automatischen SSL-Zertifikatverwaltung und des automatischen SMTP zum Provising-Assistenten in CWMS

5.2 Cloud Workspace Tools und Services

Wenn ein VDI-Benutzer seine VM abmeldet, wenn sie ausgeschaltet ist, schalten Sie die Azure Backup Erweiterung für diese VM aus. Wenn Sie TSD1-Server als VM wiederherstellen, Wiederherstellung als TS-VM statt zusätzlicher TSD-VM Steamlinierte Vorbereitung von Azure VMs für Azure Backup Handling Back-End-Verarbeitungsgeschwindigkeit und Sicherheitsverbesserungen

5.2 REST API

Verbesserte Handhabung von Serverinformationen, was schnellere Ladezeiten von Wake-On-Demand Servern ermöglicht

CWMS 5.2: Donnerstag, 11. Juli 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 11. Juli 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Tools und Services

Fortlaufende Verbesserungen der Sicherheit im Hintergrund Verbesserungen der fortlaufenden Stabilität bei automatisch generierten Zertifikaten Verbesserung der privilegierten Methodik – Anpassung an ein Konto mit weniger Berechtigungen/weniger Beeinträchtigung durch allgemeine Sperrungen, um nächtliche Neustarts zu verbessern für integrierte Backups für Azure Bereitstellungen Verbesserungen für integrierte Backups für GCP-Bereitstellungen Bug fix auf Server müssen nicht mehr ununterbrochen neu gestartet werden, um Ressourcenanpassungen anzuwenden, wenn sie bereits die Prozesserweiterung angepasst haben, um eine manuelle Zertifikatverwaltung zu ermöglichen, falls gewünscht

CWMS 5.2: Donnerstag, 20. Juni 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 20. Juni 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Management Suite

Verbesserte Handhabung von Benutzern, die über den CRA-Prozess in CWMS importiert werden. Korrekte Speicheranzeigen im Server-Abschnitt des Workspace-Moduls für eine Untermenge von Szenarien Aktualisiert Jahr am Ende der CWMS-Webschnittstelle

5.2 Cloud Workspace Tools und Services

Verbesserte automatisierte Zertifikatautomatisierung

5.2 REST API

Anzeige Korrektur: Zeigen Sie die korrekten Werte an, die zuvor in der Funktion Live-Skalierung eingegeben wurden, wenn Sie die Funktion Live-Skalierung erneut öffnen, können Sie einen Standard-Backup-Zeitplan für die Power User-Rolle (VDI-Benutzer) erstellen.

CWMS 5.2: Donnerstag, 6. Juni 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 6. Juni 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Tools und Services

Verbesserte Handhabung von mehreren E-Mails für Plattformbenachrichtigungen Bug fix für eine Untergruppe von Szenarien, in denen Workload Scheduling nicht richtig ausgeschaltet war Bug fix für eine Untermenge von Szenarien, in denen die Wiederherstellung von Servern aus Azure Backup nicht wieder die richtige Speicherart vs Ein Standard-Speichertyp

5.2 CWA-Einrichtung

Weitere Sicherheitserweiterungen während des CWA-Setup-Prozesses verbesserte automatisierte Handhabung von Subnetz- und Gateway-Einstellungen verbesserte Prozesse für die Handhabung von Benutzerkonten während des Registrierungsvorgangs beinhaltet einen Prozess zur Aktualisierung von Token, falls ein Benutzer länger als 1 Stunde im CWA-Setup-Prozess bleibt

CWMS 5.2: Donnerstag, 23. Mai 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 23. Mai 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Management Suite

Verbesserter Link im AVD-Tab im Workspaces-Modul Bug fix für ein Szenario, bei dem Sie durch Klicken auf einen Link zu einem Workspace aus dem Data Center-Modul nicht zu diesem Workspace Bug fix für ein Szenario gelangen würden, in dem die Aktualisierung der Kontaktinformationen für einen primären Administrator ihre entfernen würde Bezeichnung als Hauptadministrator

CWMS 5.2: Donnerstag, 9. Mai 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 9. Mai 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Tools und Services

Verbesserte Skalierbarkeit für Implementierungen mit mehreren Hundert bis mehrtausend VMs

CWMS 5.2: Donnerstag, 25. April 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 25. April 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Management Suite

Verbesserung der Schnittstelle: Falls Backups nicht für einen Server in Azure oder GCP aktiviert sind, entfernen Sie die Spalte „Größe“ aus dem Abschnitt „Backup“ eines Servers

5.2 Cloud Workspace Tools und Services

Bug Fix für ein Szenario, in dem das Ändern von Ressourcen für RDP- und/oder HTML5-Gateway-Server sie nach Abschluss der Ressourcenänderung nicht wieder online bringen würde

5.2 REST API

Verbesserte Handhabung anfänglicher MFA-Konfigurationen, unabhängig vom Szenario

5.2 CWA-Einrichtung

Unterstützung für bestehende CWMS-Konten, wodurch indirekte CSPs korrekt bereitgestellt werden können und der Prozess für bestehende Partner vereinfacht wird zusätzliche Validierung für Azure Active Directory Domain Services – zeigt einen Fehler an, wenn Azure Active Directory Domain Services ausgewählt, aber

bereits vorhanden ist

CWMS 5.2: Donnerstag, 11. April 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 11. April 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Management Suite

Fehlerbehebung für Provisioning Collections – Speichern einer Provisioning Collection mit einer App, die nicht havea ein Desktop-Symbol zeigt keinen Fehler mehr in CWMS Bug fix – Beheben eines Problems, bei dem das Starten eines Stopped Platform Servers aus CWMS einen Fehler anzeigt, weil es keinen Partner gab Code angehängt

5.2 Cloud Workspace Tools und Services

Stabilitätssteigerung beim Löschen von Servern in vCloud-Bereitstellungen – für den Fall, dass mehrere FMS in einer vApps gefunden werden, Löschen Sie nur die VM, anstatt die vApp zu löschen Fügen Sie eine Option hinzu, um keine Platzhalterzertifikate auf Infrastrukturservern zu installieren Verbesserungen beim Klonen von TSD-Servern in AzureAD Verbesserungen für Server Resource Report – Umgang mit Servern mit mehreren IP-Adressen Bug fix für einen Teil von Szenarien, wenn eine Liste von Backups für einen Server wurden nicht zur Überprüfung in AzureRM Bug Fix geladen, wenn versucht wird, VMs mit einem Präfix in Azure Classic zu klonen (alle neuen und neuesten Bereitstellungen verwenden AzureRM) Bug Fix für DNS-Fehler, die nicht korrekt im Server Resource Report for Server 2008 R2 gemeldet werden, Bug Fix für das Senden des Company Resource Reports, falls eine VM aus dem Hypervisor gelöscht wird (aber nicht aus AD) CWMS kann Azure Backups nicht im Hypervisor selbst finden (nur in AzureRM-Implementierungen).

5.2 CWA-Einrichtung

Hinzufügen einer Methode zur Validierung, dass für die Region, in der die Bereitstellung ausgewählt wurde, Azure Active Directory-Domänendienste verfügbar sind Hinzufügen weiterer Prüfungen zum Beheben von DNS-Timeout-Problemen in einer Untermenge von Szenarien B2s als Ziel für CMGR1-Bereitstellungen entfernen, da dies den Bereitstellungsprozess verlangsamt hat

CWMS 5.2: Donnerstag, 28. März 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 28. März 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsservices für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Management Suite

Hinzufügen des Abschnitts Azure Virtual Desktop zur CWMS-Schnittstelle ermöglicht es einem CWMS-Administrator, kein Firmenlogo unter Einstellungen → Logo-Anforderung für externe ID festzulegen, wenn eine App in einem benutzerdefinierten App-Katalog aktualisiert wird

5.2 Cloud Workspace Tools und Services

Weitere Optimierung und Verbesserung des Cloud Workspace für die Implementierung von Azure (CWA) Ein Premium-Storage-Konto ist nicht mehr erforderlich, um VMs mit Premium Storage in Azure RM-Implementierungen zu erstellen. Dieses Problem wird in einer Auswahl von Szenarien behoben, in denen Berichte zur Anwendungsnutzung keine Nutzungsdaten erfasst haben Ein Problem, bei dem das Aktualisieren von Zertifikaten auf HTML5-Portalservern zu einem Fehler führt, da die Lizenzierung von HTML5-Portalservern aktualisiert wurde. Fehlerbereinigter Speicherort für Passwortablaufbenachrichtigungen bei der Verwendung

von Azure Active Directory Domain Services, an den Password Expiration Notifications Protokolldateien schreibt, wird keine Passwörter aktualisiert

5.2 REST API

Bug Fix für Start/Stopp Platform Server (keine Customer-Server) im Data Center-Modul

5.2 CWA-Einrichtung

Verbesserungen für FTP-Rolleneinstellungen während der Bereitstellung verbesserter Mechanismus, um sicherzustellen, dass Administratoren jedes Mal das neueste Release sehen, wenn sie auf den CWA-Setup-Prozess zugreifen verbesserte Handhabung von Elementen, die sich während der Bereitstellung befinden Bug Fix für ein Szenario, in dem eine Bereitstellung falsch mit Azure AD gekennzeichnet wurde

CWMS 5.2 Minor Release: Donnerstag, 14. März 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 14. März 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsservices für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Management Suite

Ändern Sie den Namen der Funktion „Anwendungsüberwachung“ in „Anwendungsnutzungsverfolgung“. Verwenden Sie einen Fix, bei dem die Aktualisierung einer Suche nach skriptbasierten Ereignissen die ausgewählten Start-/Enddatum nicht erneut verwendet. Standarddatei-Audit startet mit dem Datumsfilter, der auf einen Tag vor dem aktuellen Datum eingestellt ist. Optimierung der zurückgegebenen Datenmenge Bug Fix für integrierte Backups für Azure, bei denen die Wiederherstellung von Backups auf einen Server nicht wie vorgesehen in einer Untergruppe von Szenarien funktioniert Behebung einer Anwendungsfehlermeldung beim Aktualisieren eines Clients, der zu einem App Service gehört

5.2 REST API

Azure Safeguard – Stellen Sie beim Hinzufügen eines Azure AD-Benutzers sicher, dass ihre E-Mail-Adresse nicht bereits dem Konto hinzugefügt wurde. Fehlerbehebung – Wenn Sie eine Anwendung für einen Client hinzufügen und gleichzeitig eine Gruppe erstellen, Fügen Sie die Benutzer der Gruppe wie vorgesehen hinzu Fügen Sie einen Validierungsschritt hinzu, wenn Sie den Zugriff auf RDSH-Server deaktivieren, um sicherzustellen, dass er nach dem Neustart eines Servers weiterhin angewendet wird Allgemeine Verbesserungen für die CWA-Workflow-Automatisierung Bug fix für einen Teil von Szenarien beim Hinzufügen einer App zu einer betroffenen Gruppe Andere Benutzer dieser Gruppe

5.2 CWA-Einrichtung

Fügen Sie eine Aktualisierungsoption für die Liste der Abonnements während des Bereitstellungsprozesses ein Auto-Set-Implementierungs-Flag für heruntergestuften, älteren MobileDrive-Service zu False Weitere Automatisierungsgarantien und Checks in Azure hinzu

CWMS 5.2 Minor Release: Donnerstag, 28. Februar 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 28. Februar 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Management Suite

Verbesserte Übersichtlichkeit und Bestätigungsnachricht für das, was passiert, wenn die Auswahl des "VDI-Benutzer"-Checkbox für Benutzer in der CWMS-Schnittstelle (löscht VDI-Benutzer-Server) und wie Sie fortfahren, wenn Sie nicht den Server löschen möchten Back-End Verbesserungen in der Zeitstempelhandling

5.2 Cloud Workspace Tools und Services

Aktualisierte Einstellungen für den Lizenzservernamen in Azure Domain Services Behind-the-Scenes Verbesserungen des Prozesses, durch den ein Benutzer sein eigenes Passwort ändern kann, nachdem er in seinem Cloud Workspace angemeldet wurde Native 2FA aktualisiert wurde, um CloudJumper Imagery anzuzeigen Bug fix for 2FA ist, wenn eine seltene Einstellung aktiviert ist

5.2 CWA-Einrichtung

Zusätzliche Hilfe/Support-Inhalte im CWA Setup-Assistenten Vertragsbedingungen und Preise zum CWA Setup-Assistenten hinzufügen verbesserter Mechanismus zur Erkennung von Quoten und Berechtigungen eines Abonnements Optimierung von Bereitstellungen auf Basis von Azure Active Directory Domain Services-basierten Bereitstellungen hinter den Kulissen Verbesserung des Speicherkontennamenformats Bug fix für FTP-Server Einstellungen in einem Teilsatz von Szenarien

CWMS 5.2 Minor Release: Donnerstag, 14. Februar 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 14. Februar 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Management Suite

Leistungssteigerung bei Benutzerverwaltungsaktionen zusätzliche Protokollierung aktiviert, um anzuzeigen, wer eine Änderung in einer Gruppe im Aufgabenverlauf des Rechenzentrums angefordert hat. Lösen Sie ein Problem im Standard-App-Katalog, in dem Anwendungen nicht in einer Untermenge von Szenarien angezeigt wurden, ein Problem in App Services mit Dynamic beheben Bereitstellung, wenn ein Fehler angezeigt wird, wenn zwei Anwendungen mit demselben Namen sind Entfernen Sie den SDDC Creation Wizard aus der CWMS 5.1 Schnittstelle * Wenn Sie ein SDDC ausführen, das auf 5.1 ist und ein neues SDDC bereitstellen möchten, Wenden Sie sich an support@cloudjumper.com, um ein Upgrade auf CWMS 5.2 zu planen. Korrigieren Sie einen Rechtschreibfehler im Bildschirm API-Benutzererstellung von CWMS

5.2 Cloud Workspace Tools und Services

In vCloud-basierten SDDCs, erneute Anmeldung an den Hypervisor in dem Fall, dass die Verbindung in vCloud-basierten SDDCs abläuft, erhöhen die Standard-Timeout beim Warten auf Server, um verbesserte Einschränkungen auf CloudJumper administrativen Zugriff zu starten

5.2 REST API

Bei der Bereitstellung eines neuen SDDC über die 5.1-Schnittstelle von CWMS wird die Meldung angezeigt, „Neue Rechenzentrumserstellung wird nur unterstützt, wenn v5.2 von CWMS verwendet wird.“

5.2 CWA-Einrichtung

Verbesserte automatische Fehlerbehandlung

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 31. Januar 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Management Suite

Verbindungsinformationen des Cloud Workspace-Client-Servers zum Abschnitt Übersicht des Cloud Workspace-Clients hinzufügen bearbeitbares Feld in den CWMS-Kontoeinstellungen hinzufügen, mit dem Sie Ihre Azure AD-Mandanten-ID eingeben können Verwenden Sie die modernste Version von Microsoft Standard Storage in neuen Azure-Bereitstellungen verbesserte Azure-Integration, Da integrierte Backups in Azure-Bereitstellungen für mindestens einen Tag aufbewahrt werden müssen verbesserte Handhabung in der Bereitstellung von Dynamic Provisioning für App Services Fügen Sie das Datum hinzu, an dem Serverspeicher in diesen Abschnitt des Servermoduls inventarisiert wird Anzeige, dass eine App einem Benutzer bereitgestellt wird, während der Der Status des Benutzers steht noch aus Cloud Workspace Wenn ein Benutzer ein VDI-Benutzer ist, zeigen Sie den VDI-Server auf der Seite Benutzer an Wenn ein Server für einen VDI-Benutzer ist, Benutzer auf der Server-Seite anzeigen Beheben eines Problems in bestimmten Szenarien, wenn ein Benutzer über eine offene Service-Board-Aufgabe verfügt, die mit seinem Benutzernamen verknüpft ist, schlägt der Remote-Zugriff auf die VM von CWMS fehl

5.2 Cloud Workspace Tools und Services

Verbesserte Handhabung von Live-Skalierung bei der Anmeldung von Benutzern über den Tag hinweg Hinzufügen von Automatisierungsvoraussetzungen für zukünftige Wake-On-Demand Verbesserungen Erweitern Automatisierungsvoraussetzungen für zukünftige Verbesserungen bei der Workload-Planung Beheben eines Problems, bei dem die Verwendung von Windows 10 für VDI-Server den Remote-Registrierungsdienst in Azure Active nicht richtig aktiviert hat Directory Domain Services-Bereitstellungen lösen ein Problem, bei dem die Verwendung von Windows 10 für VDI-Server die Sicherheitsgruppe für die lokale Remote Desktop-Benutzergruppe in Azure Active Directory-Domänendienstbereitstellungen nicht richtig eingestellt hat Ändern Sie die PCI-Compliance-Einstellung, um keine Aktion zu ergreifen, wenn sie nicht aktiviert ist, anstatt zu erzwingen Standardeinstellungen lösen ein Problem in Workload Scheduling, damit Benutzer mit aktiviertem Wake-on-Demand, die sich abmelden können Server herunterfahren, wenn sie für den Betrieb geplant sind. Einen Fehler beim Klonen eines Servers in der öffentlichen Cloud von ProfiBricks beheben Beheben eines Fehlers beim Klonen von Servern überprüft Server-Präfixe, dass Servernamen nicht in VDI-Benutzerszenarien dupliziert werden Fügen Sie ein Check in nächtlichen Berichten für zwischengespeicherte Kundencodes, die nicht mit einer gültigen Provisioning-Sammlung verbesserte Handhabung von Ausnahmen, wenn beide VM nicht im Hypervisor und CWAgent erfordert ein Update-Auflösen Problem Zurücksetzen von Passwörtern über die Benachrichtigung zum Ablauf von Kennwörtern zur korrekten Durchsetzung des Kennwortverlaufs

CWA-Setup

Option implementieren, um SMTP-Einstellungen automatisch zu konfigurieren Hinzufügen von Validierungsoptionen für die Standortliste, um zu überprüfen, ob das Abonnement über genügend Quota und genügend Berechtigungen verfügt, um VMs in der ausgewählten Azure Region zu erstellen Hinzugefügt Funktion, um nicht benötigte CloudWorkspace und andere Servicekonten mit Administratorberechtigungen am Ende von zu entfernen Der Bereitstellungsprozess in Azure Benachrichtigen Sie Benutzer, dass manuelle DNS-Zertifikat-Uploads überprüft wurden ein Problem gelöst, bei dem ThinPrint-Installationen nicht wie vorgesehen in bestimmten Szenarien installieren

CWMS 5.2 Minor Release: Donnerstag, 17. Januar 2019

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 17. Januar 2019 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für

Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Management Suite

Die Schnittstelle Workload Scheduling zeigt jetzt die Beschreibung als erste Spalte an und ändert den Namen von Scheduling in Custom Scheduling Fehlerfix für die Anzeige von Backups von Plattformservern in Azure-Bereitstellungen Bug Fix für Szenarien, in denen Endbenutzer-Selbstverwaltung für App-Services-Anwendungsfälle, in denen das Unternehmen nicht arbeitet Lassen Sie alle Cloud Workspace-Services einrichten

5.2 Cloud Workspace Tools und Services

Zusätzliche Unterstützung für PCI v3-Compliance Sicherheitsverbesserung: Neue CWMS-Bereitstellungen verwenden einen lokalen Administrator im Vergleich zu Ein Domänenadministrator zum Ausführen der CWAgent-Prozesse. Unterstützung für Windows Server 2019 in AzureRM-Bereitstellungen * Hinweis: Microsoft unterstützt Microsoft Office in dieser Version nicht und verbessert die Handhabung von Wake-On-Demand-Benutzern – wenn ihr Unternehmen die VMs herunterfahren soll, aber ein Benutzer mit Wake-on-Demand arbeitet weiterhin aktiv, Schalten Sie beim Klonen von VMs die Verbesserung der Stabilität des Unternehmens nicht aus – entfernen Sie Rollen wie Connection Broker von der neu erstellten VM, die von der geklonten VM kommt. Verbesserter Prozess für die Installation der ThinPrint Lizenz-Server-Rolle verbesserte AzureRM-Vorlage-Handling – gibt alle Vorlagen zurück, die für eine VM in Azure verfügbar sind, basierend auf der Hardware, auf der sie ausgeführt wird, Nicht nur Vorlagen in der Azure-Region des Mandanten bessere automatisierte Tests für vSphere-Bereitstellungen umfassen ein Check-in nächtliche E-Mail-Berichte, um zu sehen, ob ThinPrint-Lizenzserver installiert ist Bug Fix für Live-Skalierung in einer begrenzten Untermenge von Szenarien Bug Fix für das Klonen von Servern in bestimmten Szenarien in VCloud Deployments Bug fix for VM Name Prefixe in AzureRM-Bereitstellungen Bug Fix for Reporting error bei der Verwendung benutzerdefinierter Maschinengrößen in Google Cloud Platform Bug fix for Reporting Users with ThinPrint functionenVerclud Chinese Version of Windows from the list of Templates Available in AzureRM

CWA-Setup

Beheben Sie ein Szenario, in dem Passwörter, die die Mindestanzahl der erforderlichen Zeichen erfüllen, nicht akzeptiert wurden Ändern Sie die ID-Spalte in die Kundendomäne während des Mandantenauswahlprozesses für CSP Update auf den Anmeldevorgang, der die Kreditkarteneingabe optimiert

CWMS 5.2 Minor Release: Donnerstag, 20. Dezember 2018

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 20. Dezember 2018 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Einrichtung Von Cloud Workspace

Hinzufügen einer Funktion der FTP-DNS-Registrierung im Falle einer Single-Server-Bereitstellung und Automatic SSL wird während des Bereitstellungsprozesses ausgewählt automatisierter Prozess für die Beauftragung von Azure AD-Info. (TenantID, ClientID, Key) in Back-End-Tabellen der automatisierte Installationsprozess installiert nun den ThinPrint License Server 11 anstelle von 10

5.2 CWA-Einrichtung

Beheben Sie ein Problem, bei dem der Registrierungsvorgang Administratoren zu einer Anmeldeseite umgeleitet hat, wenn Sie fertig sind

CWMS 5.2 Minor Release: Donnerstag, 6. Dezember 2018

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 6. Dezember 2018 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Tools und Service

Unterstützung für die Erstellung von Servern mit Win10 OS verbesserte Geschwindigkeiten beim Laden einer VM aus dem Hypervisor Zurück korrekte Speichertypen verfügbar beim Erstellen von Servern in Azure Hinzufügen Protokollierung täglicher Berichte zum Back-End der Kontrollebene Vermeiden Sie ein Szenario, in dem sich Temp-Laufwerke automatisch in Azure erweitern könnten Legen Sie die Grundlage für eine zukünftige Änderung der Anzeige von Server OS bei der Auswahl einer Vorlage für die Bereitstellung Bug Fix für die nicht automatische Erweiterung eines Laufwerks in GCP Bug fix für die Bereitstellungsautomatisierung bei der Verwendung von Azure Active Directory Domain Services Wenn mehrere MGR-Server konfiguriert sind, Hinweis: Fehler im nächtlichen Bericht Bug Fix für automatisierte Tests für Public Cloud (Azure, GCP). Backups in VMware-Bereitstellungen Bug fix zur Ermittlung des Festplattenspeichers auf einer über HyperV-Bereitstellungen erstellten neuen VM Bug Fix für das Sammeln von Serverdaten bei AD-Root-OU ist keine Stabilitätsverbesserung beim Klonen von Servern auf Basis eines falsch konfigurierten Hypervisors

5.2 REST API

Unterstützung für Maschinenreihen in öffentlichen Trübgd-Bereitstellungen ermöglichen die Deaktivierung der Standard-Ressourcenzuordnung für einen SDDC Hinzugefügt DataCollectedDateUTC zu Speicherdetails für einen Server Hinzufügen der Fähigkeit zur Berechnung von Ressourcenwerten Neue Methode zum Abrufen detaillierter Verbindungsstatus von Benutzern Anzeige eines Fehlers in CWMS Beim Löschen eines Benutzers, der auch Administratorrechte hatte Behoben Probleme mit Laufwerkszuordnung für einen datenaktivierten App-Dienst wird nicht immer angezeigt Behobene Probleme beim Aktualisieren eines Clients und/oder Benutzers über CWMS, die über CWA importiert wurden Behobene Probleme bei der Erstellung eines neuen Benutzers und der Zuweisung von Anwendungen Der neue Benutzer erhält die Anwendungsverknüpfungen nicht in der Gruppe „Alle Benutzer“.

CWMS 5.2 Minor Release: Donnerstag, 1. November 2018

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 1. November 2018 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Management Suite

Fehlerbehebung für integrierte Backups Bug Fix für einen bestimmten Anwendungsfall in einer CRA-Bereitstellung

5.2 Cloud Workspace Tools und Services

Möglichkeit zur Rückgabe von verfügbaren Speichertypen in Azure ARM-Bereitstellungen bei Servererstellung Unterstützung für Active Directory-Topologie mit mehreren Standorten Beheben Sie ein Problem mit TestVDCTools bei der Verwendung von Azure Active Directory-Domänendienst Bug fix für nächtliche E-Mail-Berichte, wenn AD-Root OU leer ist

5.2 REST API

Unterstützung für das Entsperren von Benutzern, wenn Azure Active Directory Domain Services verwendet werden. Hinweis: Bitte beachten Sie, dass es aufgrund der Replikation zu einer Verzögerung von bis zu 20 Minuten kommen kann.

CWMS 5.2 Minor Release: Donnerstag, 18. Oktober 2018

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 18. Oktober 2018 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Management Suite

Im Datacenter-Assistenten Validierung von Wildcard-Zertifikaten aktivieren Allgemeine Verbesserungen hinter den Kulissen und Fehlerbehebungen eine Suchfunktion in der Anwendungstabelle hinzufügen verbesserte Sortierung in der Anwendungstabelle Details zum Abschließen der DNS-Registrierung im Data Center-Provisioning enthalten alle Unterpartner-Benutzer und -Gruppen in API-Call-Antworten für Dynamic App Services Fix ein Fehler, bei dem Migration-Modus nicht für einen Mieter in einem bestimmten Fall bleiben Add Extra Powered auf Servern, Gemeinsam genutzte Benutzer pro Server und Max Shared-Benutzer pro Server für Details zur Live-Skalierung Fügen Sie die DNS-Validierung zum Wildcard-Zertifikatstest hinzu, wenn Sie die Bereitstellung über den neuen Data Center-Assistenten durchführen

5.2 Cloud Workspace Tools und Service

Option aktivieren, um alle nach VM-Serie gruppierten VM-Größen zurückzugeben Alle verfügbaren VM-Größen vom Hypervisor auf Ressourcenzuordnung korrigieren bei der Berechnung von App Service-Benutzern aktivieren Option für automatisches Ressourcen-Update für CWMGR1 Wildcard-Zertifikatstatus einschließen DataCenterResources Report Aktivieren zukünftiger DNS-Erweiterungen Bug fix – Automatisches erweitern von Laufwerken in GCP-Bereitstellungen

5.2 REST API

Leistungsverbesserungen beim Auflisten von Clients/Benutzern Unterstützung für neue Live Scaling-Funktionen zulassen – Konfiguration von ExtraPoweredOnServers, SharedUsersPerServer und MaxSharedBenutzersdie PerServer API unterstützt jetzt die Möglichkeit, Wildcard-Zertifikatdomäne beim Erstellen neuer Plattform-Bereitstellungen zu validieren Neue API-Methode verfügbar, um Benutzeraktivitätsdaten für alle Partner-Clients zu erhalten

Bekanntes Problem: Wenn Sie eine dynamische Zuweisungsmethode „Active Users“ oder „User Count“ für Ressourcen-Pool-Größen innerhalb einer Azure ARM-Bereitstellung verwenden, zeigt die Zusammenfassung „Computed Resource per Server“ die Maschinengröße fälschlicherweise als Basic A-Serie an, anstatt den korrekten Typ der D-Serie zu verwenden.

CWMS 5.2 Minor Release: Donnerstag, 27. September 2018

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 27. September 2018 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungs-Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Management Suite

Vereinfachen Sie die Anzeige von Provisioning-Collection-VMs im Cache Fix eine Anzeige schrullig bei der Verwaltung von App-Services

5.2 Cloud Workspace Tools und Services

Bug Fix für einen obskuren Anwendungsfall für Endbenutzer-MFA-Update-API, um eine Schnittstelle mit den neuesten in Azure RM Update Testing für Azure RM zu verwenden, um die neueste API ersetzen Power User Terminologie mit VDI User Update E-Mail-Bericht, um zusätzliche CPU und RAM für einen Server Aktualisieren der Adressberichte stammen aus: Statt dnotifications@independenceit.com Nachrichten werden

dcnotifications@cloudjumper.com die Definition von Benutzern pro Server und zusätzliche VMs ermöglichen, über Verbesserungen der Performance der Live-Skalierung aktiv zu bleiben, wenn ein angestoppter SDDC/Deployment gestartet wird Sicherheitserweiterung – Partner mit mehreren SDDCs/Bereitstellungen können nicht von einer Verbindung zu Eine weitere Stabilitätsverbesserung – sollte die Automatisierung die Anzahl der Benutzer nicht zurückgeben, nehmen Sie keine Änderungen an der Ressourcenanzahl vor. Geringfügige kosmetische Verbesserungen

CWMS 5.2 Minor Release: Donnerstag, 6. September 2018

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 6. September 2018 um 22:00 – 23:00 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Management Suite

Hinzufügen der Möglichkeit zur Suche nach Unterpartnern im Benutzerdefinierten App-Katalog ein Fehler wurde behoben, bei dem die Aktualisierung des Bildschirms im Modul „Rechenzentren“ zu einer Fehlermeldung führt, die die Beschränkung auf die maximale Größe des Ordnernamens beseitigt und das Durchsuchen von Ordnern vereinfacht. Dadurch wird sichergestellt, dass die Ressourcen auf VMs zählen Nicht unter den angegebenen minimalen CPU- und RAM-Werten festlegen Rephrase Power User Terminologie to VDI User Behoben ein Fehler, bei dem ein generischer Fehler angezeigt wurde, obwohl der Back-End-Prozess erfolgreich abgeschlossen wurde verbesserte Anzeige des Servernamens im Assistenten für die Erstellung des Rechenzentrums Kontoablauf beheben, das nicht das gespeicherte Ablaufdatum anzeigt In CWMS

5.2 Cloud Workspace Tools und Services

Behoben einen Fehler mit MFA, wo Benutzer, die E-Mail manchmal nicht erhalten einen Code erlauben zusätzliche CPU und RAM eingegeben werden für Benutzer Anzahl Ressourcen Zuweisung Typ Fix einen Fehler, wo die Automation Engine nicht alle Maschinentypen auf Behoben ein Timing-Problem, das manchmal verursachen würde Klonen von Servern zum Löschen Automatisieren der zuvor manuellen Installation eines Wildcard-Zertifikats auf FTP-Server ein Prozess zum Löschen alter Zertifikate nach dem Aktualisieren von Platzhalterzertifikaten behebt ein Problem, bei dem bei der Verwendung von Data Enabled Application Services das Laufwerk X: Nicht immer einem Endbenutzer zugeordnet wird.

CWMS 5.2 Allgemeine Verfügbarkeit: Donnerstag, 10. August 2018

Komponenten: 5.2 Cloud Workspace Management Suite Wann: Donnerstag, 10. August 2018 um 22 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Application Services für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.2 Cloud Workspace Management Suite

Veröffentlichen Sie Komponenten der Webschnittstelle, um die Funktionen in der obigen Übersicht zu aktivieren

5.2 Cloud Workspace Tools und Services

Lassen Sie Back-End-Tools frei, um die Funktionen in der obigen Übersicht zu aktivieren

5.2 REST API

Release API to production to enable the features found in the overview above

Cloud Workspace Suite – Version 5.1



Es wird keine weiteren wiederkehrenden Versionen für v5.1 von CWMS geben – alle Versionen werden als Hotfixes betrachtet.

CWMS 5.1 Nebenveröffentlichung: Donnerstag, 18. Oktober 2018

Komponenten: 5.1 Cloud Workspace Management Suite Wann: Donnerstag, 18. Oktober 2018 @ 10.00 – 23 Uhr Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

Workspace Management Suite

- Fügen Sie eine Suchfunktion in der Anwendungstabelle hinzu
- Verbesserte Sortierung in der Anwendungstabelle

CWMS 5.1 Nebenversion: Donnerstag, 6. September 2018

Komponenten: 5.1 Cloud Workspace Management Suite Wann: Donnerstag, 6. September 2018 @ 10pm – 11pm Eastern Impact: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen. Der Zugriff auf die Cloud Workspace Management Suite bleibt verfügbar.

5.1 Cloud Workspace Management Suite

- Im Katalog „Benutzerdefinierte App“ wurde die Möglichkeit hinzugefügt, nach Unterpartnern zu suchen
- Es wurde ein Fehler behoben, bei dem die Aktualisierung des Bildschirms im Modul „Rechenzentren“ zu einer Fehlermeldung führt
- Entfernen der Beschränkung auf die maximale Ordernamengröße und erleichtern das Durchsuchen von Ordnern
- Stellen Sie sicher, dass die Ressourcenanzahl auf VMs niemals unter den festgelegten Mindestwerten für CPU und RAM liegen

5.1 Cloud Workspace Tools und Services

- Ein Fehler mit MFA behoben, wo Benutzer, die E-Mail gewählt haben, manchmal keinen Code erhalten
- Geben Sie für die Ressourcenzuordnungsart „Benutzeranzahl“ zusätzliche CPU und RAM ein
- Fehler bei der Ressourcenzuordnung für die Serverlastzuordnungsart behoben, bei der in einigen Fällen die Anzahl der benötigten Server ausgeschaltet war
- Sicherheit hinzufügen beim automatischen Neustart eines Servers – falls CwVmAutomationService belegt ist, versuchen Sie es in 20 Minuten erneut
- Verbesserte Handhabung von Platzhalterzertifikaten Installationen auf CWMGR1
- Fixdaten im Data Center Resource Report
- Verbesserte Handhabung von RAM-Ressourcen
- Verbesserte Berechnungen zu den verfügbaren Festplattenressourcen
- Einführung der Unterstützung von v4 der ProfiBricks API, ermöglicht die Einstellung der CPU-Familie
- Das Löschen alter temporärer Vorlagen in ProfiBricks wurde beim Erstellen einer Provisioning-Sammlung behoben

- Hat die Zeitüberschreitung beim Warten auf den Hypervisor von ProfitBricks erhöht, um eine VM zu erstellen
- Bei der Installation neuer Versionen von VdcTools, Update VdcToolsVersionRunningAtVdc sobald es in Bearbeitung ist, so dass die Automatisierung schneller läuft
- Es wurde ein Fehler behoben, der beim Installieren von Platzhalterzertifikaten auf RDP Gateway-Servern aufscheinen würde
- Automatisieren Sie die zuvor manuelle Installation eines Platzhalterzertifikats auf dem FTP-Server
- Ein Fehler wurde behoben, bei dem Benutzer aufgrund von Kennwortablaufhinweisen nicht gezwungen wurden, ihr Passwort zu aktualisieren
- Der Dateiaudit-Prozess wurde verbessert, um die Häufigkeit des Fehlers Unbekannter Benutzer zu verringern
- Es wurde ein Fehler behoben, bei dem der Datei-Audit-Bericht keine Ordner richtig ausschließt
- Es wurde eine Funktion hinzugefügt, um das Platzhalterzertifikat zu installieren, wenn das Zertifikat auf dem Verbindungs-Broker abgelaufen ist
- Es wurde ein Fehler behoben, bei dem die Hinweise zum Ablauf des Kennworts nicht angezeigt würden, wenn die Verknüpfung zur Benachrichtigung zum Ablauf des Kennworts aus dem Startordner entfernt wird (es wird neu installiert).
- Ein Fehler wurde behoben, bei dem das Platzhalterzertifikat ein Update auf HTML5-Portalservern nicht verzögert hat, wenn ein Benutzer angemeldet war
- Ein Fehler wurde behoben, bei dem Platzhalterzertifikat anzeigen würde, dass ein HTML5-Portalserver aktualisiert werden muss, wenn es bereits aktuell war
- Beim Installieren von Platzhalterzertifikaten auf Verbindungsbroker-Servern wurde ein Fehler behoben
- Ein Problem mit dem Klonen wurde behoben, wenn lokale VM-Konten entfernt wurden
- Das Problem beim Klonen von Servern wurde behoben, bei dem der Mandanten den Migrationsmodus aktiviert hat
- Es wurde ein Fehler beim Klonen von VMs in vCloud behoben, wobei der Hypervisor lange gedauert hat, bis die VM erstellt wurde
- Ein Fehler wurde behoben, bei dem das Löschen einer VM in AzureRM auch immer die zugehörigen verwalteten Laufwerke löschen würde
- Das Erstellen von VMs in AzureRM wurde durch ein seltenes Timing-Problem behoben, um zu verhindern, dass sich zwei Build-Vorgänge überschneiden
- Aktualisierte Liste der Maschinengrößen und -Typen in AzureRM
- Fehler bei der Konfiguration des Subnetzes im Hypervisor für GCP während der Bereitstellung behoben
- Fehler beim Speichern der Überwachungsdaten RE: Plattformzustand durch Entfernen einer Zeitüberschreitung, die dazu führte, dass Daten nicht geschrieben wurden, wenn ein Server beschäftigt ist
- Eine Funktion hinzugefügt, mit der jeder Server seine Zeitzone individuell einstellen kann oder nicht durch Plattformautomatisierung gesteuert wird
- Es wurde ein Fehler behoben, wenn VMs an einem sekundären Standort statische IP-Adressen vom primären Standort zurücksenden würden
- Fehler beim Erfassen des Usernamens für den Benutzeranmeldungsbericht behoben
- Es wurde ein Fehler behoben, bei dem die alten Überwachungsdaten nicht gelöscht wurden, indem der Anruf asynchron ausgeführt wurde, sodass keine Zeit für das Löschen erforderlich war
- Installieren Sie automatisch Platzhalterzertifikate auf allen Infrastrukturservern

CWMS 5.1 Nebenversion: Donnerstag, 12. Juli 2018

Komponenten: 5.1 CWMS Tools and Services Wann: Donnerstag, 12. Juli 2018 @ 10-10:30 Eastern Impact:
Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen.

5.1 CWMS Web-App

- Beheben Sie ein Problem bezüglich der Persistenz der Einstellungen des globalen App-Katalogs

CWMS 5.1 Nebenversion: Donnerstag, 17. Mai 2018

Komponenten: 5.1 CWMS Tools and Services Wann: Donnerstag, 17. Mai 2018 @ 10-11 Uhr EST
Auswirkungen: Der Zugriff auf Cloud Workspace Desktops und Anwendungsdienste für Endbenutzer bleibt ununterbrochen.

5.1 CWMS Web-App

- Beheben Sie ein Problem bezüglich der Zusammenfassungen von Benutzern für App-Services-Gruppen
- Beheben Sie ein Problem mit dem Data Center-Assistenten, der den Benutzernamen und das Kennwort vorgibt
- Fügen Sie im Data Center-Assistenten die Benutzervalidierung für lokale VM-Administratoren und Level 3-Techniker hinzu
- Verbesserte Sitzungsabwicklung, einschließlich automatischer Abmeldung von Benutzern nach einer Sitzungszeitüberschreitung
- Beheben Sie ein Problem beim Löschen von Administratoren, wenn ein primärer Administrator nicht erkannt werden konnte
- Platzhalter in Data Center ändern → Profilserver ändert sich von Profilnamen eingeben in Profil eingeben und Beschriftung von Profilname zu Servername ändern
- Das Aktivieren von AD-Admin funktioniert nicht für Benutzer außerhalb des Cloud Workspace
- Beheben Sie den JavaScript-Fehler, um das Hinzufügen neuer Benutzer/Gruppen für einen Kunden außerhalb des Cloud Workspace zu verhindern
- Zulassen, dass Master-Partner Active Directory-Benutzeradministratoren für Unterpartner erstellen
- Fehler beheben, der beim Zurücksetzen des Passworts eines Hauptadministratoradministratores eines Teilpartners zu einem Fehler führt

CWS 5.1 Nebenversion: Mi., Feb 21, 2018

Komponenten: 5.1 CW Werkzeuge und Dienstleistungen Wann: Mi., Feb 21, 2018 @ 10-11 Uhr EST
Auswirkungen: Der Zugriff auf Cloud Workspace Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen.

5.1 CW Web-App

- Problem beim Verwalten von Benutzerordnern über die Administratorrolle beheben

5.1 CW Tools und Dienstleistungen

- Stellen Sie sicher, dass der ausgefallene Server nicht automatisch gelöscht wird, wenn Sie einen „No Services“-Client mit einem Workspace aktualisieren
- GPO-Updates von W2016 verarbeiten, um zu verhindern, dass Popup-Meldungen für Benutzer, die bei

ihren RDS-Sitzungen auf W2016-VMs angemeldet sind, kurz sichtbar werden

5.1 REST API

- Fügen Sie neue Attribute hinzu (ändern Sie den SPLA-Bericht von CWS, um neue Attribute zu nutzen), um die Verwendung von auf Lizenzen basierenden Anwendungen (insbesondere SQL) zu optimieren.

CWS 5.1 Nebenversion: Mi., Feb 7, 2018

Komponenten: 5.1 CW Werkzeuge und Dienstleistungen Wann: Mi., Feb 7, 2018 @ 10-11 Uhr EST

Auswirkungen: Der Zugriff auf Cloud Workspace Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen.

5.1 CW Web-App

- Keine

5.1 CW Tools und Dienstleistungen

- Problem beheben Deaktivieren von App locker unter Windows 2016 (aufgrund neu entdeckter interner Probleme mit Windows 2016)
- Beheben Sie den Fehler, wenn die IP-Adresse aufgrund eines Fehlers falsch neu zugewiesen wird

5.1 REST API

- Beheben Sie das Speichern des Speichertyps, wenn Sie einen Server in einer Provisioning Collection ändern
- Beim Erstellen einer Provisioning Collection mit zwei Terminal Server (TS)-Servern sollte nur ein TS-Server zur Validierung der Sammlung erstellt werden

CWS 5.1 Nebenversion: Mi., Jan. 31, 2018

Komponenten: 5.1 CW Werkzeuge und Dienstleistungen Wann: Mi., Jan. 31, 2018 @ 10-11 Uhr EST

Auswirkungen: Der Zugriff auf Cloud Workspace Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen.

5.1 CW Web-App

- Erhöhen Sie die Anzahl der Zeilen pro Tabelle auf CWS-Modulen der obersten Ebene von 10 auf 20
- Beheben Sie nur Anwenderunterstützung Admin kann sich nicht in einen Client eintauchen

5.1 CW Tools und Dienstleistungen

- Fehler beheben, wenn die Vorlage nicht über .Net Framework v4.5.2 hat, schlägt die Server-Erstellung falsch fehl
- Behebung des Problems beim Klonen von VMs in Hyper-V

CWS 5.1 Nebenversion: Mi., Jan. 10, 2018

Komponenten: 5.1 CW Werkzeuge und Dienstleistungen Wann: Mi., Jan. 10, 2018 @ 10-11 Uhr EST

Auswirkungen: Der Zugriff auf Cloud Workspace Desktops und Applikations-Services für Endbenutzer bleibt ununterbrochen.

5.1 CW Tools und Dienstleistungen

CWS Version 5.1 Tools und Services (einschließlich CW Automation Service, VM Automation Service und CWAgent Service) werden aktualisiert, um alle Autorisierungsfehler zu beseitigen, die für bestimmte RemoteApp-Anwendungsszenarien auftreten. Insbesondere werden die Dienste geändert in:

- Ändern Sie die automatische Bereitstellung des SSL-Wildcard-Zertifikats für Sitzungsserver, damit es nur auf RemotedesktopverbindungBroker-Servern und Power User-Servern bereitgestellt wird. Server, die keine Broker-Sitzungen sind, verwenden das von Remote Desktop Services (RDS) generierte Standardzertifikat.
- Ändern Sie die externe DNS-Forward-Lookup-Zone in Active Directory am SDDC, um nur einen DNS-Datensatz für freigegebene Client-Sitzungsserver zu erstellen. Dieser Datensatz wird auf den RDS Broker Server (VM) des Clients verweisen, der wiederum den Lastenausgleich zwischen freigegebenen Sitzungsservern übernimmt. Power-User-Server werden weiterhin über separate DNS-Einträge verfügen.

Hinweis: Dieses Problem wurde nur von Endclient-Konfigurationen betroffen, bei denen mehrere freigegebene Sitzungsserver verwendet werden. Mithilfe dieser Konfiguration werden jedoch neue und geänderte Client-Konfigurationen implementiert.

CWS 5.1 Nebenversion: Mi., Jan. 3, 2018

Komponenten: 5.1 CW Web App Wann: Mi., Jan. 3, 2018 @ 10 - 10:30 EST Auswirkungen: Der Zugriff auf Cloud Workspace Desktops und Applikationsservices für Endanwender bleibt ununterbrochen.

5.1 CW Web-App

- Sortieren nach Unternehmenscode im Modul „Workspaces“ von CWS beheben
- Cloud Workspace-Benutzer beheben → Kennwortrücksetzung erzwingen, die keine Änderungen widerspiegelt (wenn Sie zu einem anderen Modul navigieren und dann zum Benutzer zurückkehren)
- SDDC Self-Deploy Wizard: Beim Prüfen der ThinPrint Installation (Abschnitt Lizenzierung) wird eine Bestätigungsmeldung modal hinzugefügt

CWS 5.1 Nebenversion: Tues., Dez. 5, 2017

Komponenten: 5.1 CW Web App Wann: Dienstag, Dezember 5, 2017 @ 10 - 10:30 EST Auswirkungen: Der Zugriff auf Cloud Workspace Desktops und Applikationsservices für Endanwender bleibt ununterbrochen.

5.1 CW Web-App

- Beheben Sie den CWS Admin MFA-Fehler im Internet Explorer (IE) 11
- Beheben Sie CWS-Gruppen → lokaler Laufwerkzugriff kehrt zurück 'nicht gefunden'
- Datacenter Self Deploy: Unterstützung für AzureRM (ARM) Azure Active Directory hinzufügen
- Anwendungskatalog: Sicherstellen, dass die Abonnementoption immer verfügbar ist/propagiert wird
- CWS-Skript-Ereignismodul > Skript-Aktivität → Anwendung hinzufügen: Falsche Anwendung korrigieren Icon-Pfad
- Verbesserung der Effizienz der Zugriffsanfrage für Administratoren zur Vermeidung von Fehlern beim Umleiten auf CWS v5.0
- Beheben Sie verschiedene Fehler beim Aktualisieren von AppService-Details und/oder Verwalten von Anwendungslizenzen für einen AppService
- CWS Workspace Module > Assistent zum Hinzufügen von Workspace → AppServices korrigieren falsches

Format, das an die globale Kontrollebene gesendet wird

- CWS Workspace Module > Assistent zum Hinzufügen von Workspace → Neuer Client → Schritt 3, Fix Updategruppe um JavaScript-Fehler zu beheben, um sicherzustellen, dass das Update verarbeitet wird

CWS 5.1 Nebenversion: Samstag, Nov. 11, 2017

Komponenten: 5.1 CW Web App Wann: Samstag, Nov. 11, 2017 @ 10 bis 23 Uhr EST Impact: Der Zugriff auf Cloud Workspace Desktops und Applikationsservices für Endbenutzer bleibt ununterbrochen.

5.1 CW Web-App

- Ab 10.00 Uhr EST am Nov. 11 müssen alle CWS 5.1-Partner verwenden <https://iit.hostwindow.net>. Diese URL wird zur Unterstützung von CWS 5.1 (sowie CWS 5.0) nachgerüstet. Partner sind dafür verantwortlich, dass ihre CWS-Administratoren und Endbenutzer mit CWS-Administratorzugriff diese Änderung kennen.

CWS 5.1 Nebenversion: Mon., Okt 30, 2017

Komponenten: 5.1 CW Web App und 5.1 CW Tools & Services Wann: Mon., Okt 30, 2017 @ 10 bis 23 Uhr EST Impact: Der Zugriff auf Cloud Workspace Desktops und Applikationsservices für Endbenutzer bleibt ununterbrochen

5.1 CW Web-App

- CWS Admin MFA: Drücken Sie Enter submit Code for MFA und beheben Sie Fehler, die das erneute Senden von MFA-Code verhindert
- SDDC Self Deploy Wizard: Für GCP haben den Administrator für den lokalen VM-Namen, anstatt nur deaktiviert zu sein
- SDDC Self Deploy Wizard: Mehr Breite des Dropdown-Menüs für Zeitzonen
- Skriptbasierte Ereignisse: Feld Argumente zur Skriptaktivität hinzufügen
- Skriptbasierte Ereignisse: Fügen Sie %applicationname% als Laufzeitvariable für skriptbasierte Ereignisskripte hinzu

5.1 CW Tools & Services

- E-Mail-Adresse des Endbenutzers: Problem beheben, bei dem E-Mail-Adressen nicht in die Datenbank für vorhandene Endbenutzer gespeichert werden
- Endbenutzer-Anmeldestatus: Problem beheben, UPN des Benutzers beim Anmelden zu erhalten
- Endbenutzer-Login-Status in AzureRM: Unterstützung von über Azure gemanagten Festplatten
- Vorlagen: Beheben Sie den Workflow, wenn Vorlagen nicht ordnungsgemäß gelöscht werden
- Ressourcen: Problem beheben Konvertieren von alten Ressourcen-Pools in neue Zuordnungstypen
- Datei-Audit-Bericht: Fehler beheben, die dazu führt, dass Benutzer unbekannt sind
- Windows 2016: Beheben, um sicherzustellen, dass GPO zum Entfernen von PowerShell-Symbolen aus Endbenutzer-Workspaces ordnungsgemäß angewendet wird
- Ressourcenzuordnungsbericht ändern: Fehler beheben, der falsch angezeigt wird
- Data Center Resources Report: Wenn der Hypervisor nicht konfiguriert ist, verfügbaren Festplattenspeicher oder VM Quote zurückzugeben, verhindern Sie, dass der Bericht Fehler anzeigt
- Infrastructure Server Monatliche Neustarts: Adressszenario, wenn Infrastruktur-Server nicht monatlich wie

geplant neu starten, weil sie nicht mit dem CWMGR1-Server kommunizieren konnten, da dieser Server beschäftigt ist, neu zu starten

5.1 Nebenveröffentlichung: Tues., Okt 3, 2017

Komponenten: 5.1 CW Web App und 5.1 CW Tools & Services Wann: Dienstag, Oktober 3, 2017 @ 10 bis 23 Uhr EST Impact: Der Zugriff auf Cloud Workspace Desktops und Applikationsservices für Endbenutzer bleibt ununterbrochen

5.1 CW Web-App

- AppServices: Problem beim Blockieren von Add-Lizenzen für AppService-Anwendungen beheben
- AppServices: Stellen Sie sicher, dass die Funktionalität „Neue Instanz hinzufügen“ für AppService-Anwendungen immer verfügbar ist
- Resource Pool Terminologie: Aktualisierung der Terminologie und gleichzeitige Anwendung der Ressourcen-Pool-Konfiguration auf Server auch dann, wenn keine Änderungen vorliegen – „Update“ auf „Apply to Servers“ geändert und „Edit“ wurde in „Manage“ geändert
- Arbeitslastplan: Sicherstellen, dass Bearbeiten Modal immer geöffnet wird
- Arbeitszeitplan: Stellen Sie sicher, dass Pfeile für die Auswahl der Zeit immer angezeigt werden
- Skriptbasierte Ereignisse: Erlauben Sie eine detaillierte Zeitauswahl
- CWS-Bericht 'Admin Access': Problem beheben, das IP-Spalte verursacht, mehrere IP-Adressen aufgeführt haben, anstatt nur die Client-IP

5.1 CW Tools & Services

- File Audit Service: Jetzt durchgängig deaktiviert
- Automation Service und neues SSL Wildcard Zertifikat (RDP-Verbindungen): Updatereihenfolge von Befehlen um sicherzustellen, dass das aktualisierte RDP-Zertifikat auf RDS Gateway immer aktualisiert wird (d. h. nicht im Cache gespeichert)

CWS® 5.1 erste Release-Übersicht

Cloud Workspace Suite 5.1 ist derzeit ab Q3 2017 in Public Beta verfügbar. Diese Version enthält ein Update sowohl der CWS-APIs als auch der Admin-Control-Schnittstelle. Die Version ist ein Update auf CWS 5.0 (veröffentlicht Q4 2016) und ist nicht „abwärtskompatibel“ zu Version 4.x Entities.

Nach der offiziellen Veröffentlichung im 4. Quartal 2017 gibt es keine Upgrade-Gebühr oder Implementierungskosten für den Umstieg auf CWS 5.1. Die Upgrades werden von CloudJumper in Abstimmung mit jedem Partner durchgeführt und unterbrechen nicht vorhandene Services. CWS 5.1 unterstützt weiterhin alle Funktionen der vorherigen Versionen und erweitert neue Funktionen, die sowohl die Administrator- als auch die Endbenutzererfahrung verbessern und die preisgekrönte Automatisierung und Orchestrierung, die mit früheren Versionen der Cloud Workspace Suite eingeführt wurde, weiter verbessern.

Das CWS 5.1-Upgrade ist die schnellste und einfachste noch durch die Erweiterung und Nutzung der aktualisierten Architektur- und REST-API-Plattform, die in CWS 5.0 eingeführt wurde. CWS 5.1 setzt das Engagement von CloudJumper für eine freundlichere Umgebung fort, damit externe Entwickler ihre Dienste und Produkte auf Cloud Workspace erweitern können.



CWS 4.x wird das offizielle Ende des Lebens am 12.31.2017 erreichen. Partner, die weiterhin auf der CWS 4.x-Plattform sind, erhalten keinen direkten Support mehr für 4.x-Bereitstellungen, und es werden keine weiteren 4.x-Updates oder Fehlerbehebungen bereitgestellt.

Highlights 5.1:

- Unterstützung für Windows 2016 Server
- Support für das Gesamtsystem für Microsoft Azure Resource Manager
- Unterstützung für Office 365 Einzelauthentifizierung
- MFA für CWS Portal-Administratoren
- Verbessertes Provisioning Collection Management
- Vom Administrator definierte Automatisierung und Scripting
- Schemata Zum Sizing Von Ressourcen

Unterstützung für Windows 2016 Server

- Unterstützt Windows Server 2016 Serverversionen für alle unterstützten Plattformen.
- Windows 2016 Server bietet das „Windows 10“-Desktop-Erlebnis für gemeinsame RDS-Sitzungsbenutzer und ermöglicht Konfigurationsoptionen wie GPU-Zuweisung für grafikintensive Anwendungen*.

Support für den gesamten Stack für Microsoft Azure Resource Manager

- Microsoft erfordert die Migration vom herkömmlichen Modell für Verschlüsselungsschlüssel/delegierte Benutzerberechtigungen für Konten zu dem Azure Resource Manager.
- Microsoft Azure Resource Manager ist ein Framework, mit dem Benutzer die Ressourcen in einer Lösung als Gruppe nutzen können.
- Die erforderlichen Authentifizierungsattribute werden einmal während der Implementierung des softwaredefinierten Datacenters (SDDC) erfasst und dann für andere Microsoft Azure-Aktivitäten verwendet, ohne dass ein erneute Eintrag oder eine erneute Authentifizierung erforderlich sind.

Unterstützung für Office 365-Einzelauthentifizierung

- Microsoft Office 365 verwendet ein Authentifizierungsmodell, bei dem Endbenutzer die Anmeldeinformationen jedes Mal eingeben müssen, wenn sie die Office Productivity Suite auf einem neuen Computer oder Gerät verwenden.
- CWS 5.1 verwaltet diese Anmeldeinformationen in der gesamten Serverfarm, so dass Endbenutzer nur bei der ersten Verwendung eines neuen Office 365-Abonnements eine Authentifizierung benötigen.

Verbessertes Provisioning-Erfassungsmanagement

- Das Konfigurieren und Managen von Hypervisor-Vorlagen für vordefinierte Workloads kann verwirrend sein, insbesondere wenn unterschiedliche Hypervisor-Plattformen eingesetzt werden.
- CWS 5.1 führt automatisierte Hypervisor-Verwaltungsfunktionen ein, die die Erstellung von Serverinstanzen auf der Grundlage einer vorhandenen Vorlage oder eines VM-Images des Cloud-Providers umfassen; direkte Verbindung/Anmeldung zum erstellten Server für die Installation von Anwendungen aus der CWS-Web-App; Automatische Vorlagenerstellung/Windows-Sysprep von der konfigurierten Serverinstanz sowie Validierung von Anwendungspfaden und Installation innerhalb von CWS, sodass kein direkter Zugriff auf das Hypervisor- oder Cloud-Service-Dashboard erforderlich ist.

MFA für CWS-Portaladministratoren

- CWS 5.1 enthält eine integrierte Multi-Faktor-Authentifizierungslösung (MFA), die nur für CWS-Administratoren geeignet ist

- Die Partner können ihre eigene MFA-Lösung für Endbenutzer implementieren. Beliebte Optionen sind Duo, Auth-Anvil und Azure MF. CloudJumper wird im 1. Quartal 2018 eigene integrierte MFA für Endbenutzer veröffentlichen

Vom Administrator definierte Automatisierung

- CWS bietet Service-Providern eine verbesserte Implementierungs-/Managementautomatisierung mit der vom Administrator definierten Automatisierung von Aufgaben/Skript-Ausführung.
- Mit dieser Verbesserung wird CWS 5.1 die Implementierung erheblich beschleunigen, das Management vereinfachen und die Overhead-Kosten reduzieren.
- CWS Administrator Defined Automation ermöglicht die Installation oder das Upgrade von Anwendungen auf Basis von Ereignissen, so dass Partner automatisierte Anwendungsinstallationen/Wartungsarbeiten mit dieser Methode auslösen können.

Management-Schemata zur Dimensionierung von Ressourcen

- Die Ressourcenfunktion CWS 5.1 verbessert die Fähigkeit, Ressourcen dynamisch zu skalieren, indem drei weitere Ressourcen-Schemata hinzugefügt werden
- Die vorhandenen Schemata Total Users werden jetzt um drei weitere Ressourcendimensionierungsschemata erweitert: Fixed, Active User & Activity-based
- Beispiel: Feste Methode unterstützt die genaue Spezifikation der CPU und des RAM.
- Alle Schemata zur Dimensionierung von Ressourcen ermöglichen weiterhin sofortige/erzwängliche Änderungen oder nächtliche automatische Prüfung/Änderung von Ressourcen.

CWS – v5.0 Versionshinweise



Für v5.0 von CWS gibt es keine weiteren wiederkehrenden Releases – alle Releases werden als Hotfixes betrachtet.

Überblick

CloudJumper hat die Cloud Workspace Suite 5.0 für die allgemeine Implementierung ab Q4 2016 veröffentlicht. Diese Version enthält ein Update sowohl der CWS-APIs als auch der Admin-Control-Schnittstelle. Das Release ist eine signifikante Änderung und ist nicht „abwärtskompatibel“ zu Version 4.x Einheiten.

Version 4.x wird weiterhin unterstützt, bis alle Partner Software Defined Data Centers (SDDCs) auf die Plattform 5.0 aktualisiert wurden. Upgrades werden von CloudJumper in Abstimmung mit jedem Partner abgeschlossen und bestehende Dienste nicht unterbrochen. Es entstehen keine Upgrade-Gebühren oder Implementierungskosten für den Wechsel. CWS 5 unterstützt weiterhin alle Funktionen der vorherigen Versionen und erweitert neue Funktionen, die sowohl die Administrator- als auch die Endbenutzererfahrung verbessern und die preisgekrönte Automatisierung und Orchestrierung, die mit früheren Versionen der Cloud Workspace Suite eingeführt wurde, weiter verbessern.

Mit CWS 5.0 hat CloudJumper alle Plattformen-APIs in DAS REST-API-Format umgeschrieben und die früheren SOAP-APIs vollständig ausgemustert. Diese aktualisierte Architektur wird die Weiterentwicklung von CloudJumper einfacher und schneller erleichtern und schafft eine noch freundlichere Umgebung für externe Entwickler, um ihre Services und Produkte auf der Basis von Cloud Workspace zu erweitern.

Highlights

- Vollständiges UI/UX Rewrite
- Azure AD-Integration
- Implementierung des Azure SDDC Self-Service
- App-Services
- Ressourcenplanung
- Live-Server-Skalierung – Plattformübergreifend
- Automatisiertes Klonen Von Servern – Plattformübergreifend
- Laufwerkfreigaben werden pro Client individuell angepasst

Wichtige Funktionen

Integration von Azure Active Directory (AD)

- Erstellen Sie SDDC als Private Cloud Active Directory, oder verwenden Sie Microsoft Azure-AD-als-Service
- Kombinieren Sie CWS mit Office365
- Unterstützung von SSO und MFA auf Basis von Azure

Implementierung des Azure SDDC Self-Service

- Vollständige Integration in Azure
- Schnelle Implementierung neuer SDDCs
- Implementieren Sie Private Enterprise Clouds innerhalb von Azure für jeden Workload, einschließlich Cloud Workspace Managed: WAAS, App Services, Private Web App und SharePoint

App-Services

- Implementieren Sie Applikationssilos zur Veröffentlichung von Applikationen als isolierte Service-Bausteine
- Apps, die von 'öffentlichen' App-Servern an viele benutzerdefinierte Einheiten geliefert werden
- Applikationen werden in dedizierten Server-Pools für einzelne Applikationen installiert
- Apps werden von den Anforderungen des Benutzerprofils und der Datenschicht entkoppelt
- Bauen Sie hochskalierbare App-Services auf
- Mehrere App-Services können zu Benutzersammlungen kombiniert werden
- CWS-Lizenzverfolgung und Nutzungsberichte

Live-Server-Skalierung – plattformübergreifend

- Intelligente, automatisierte Skalierung von Serverressourcen/aktiven Servern
- Managen Sie Server-Ressourcen optimal mit dynamischer Zunahme/Senkung bei Änderungen der Benutzerlast
- Automatische Skalierung von Serverressourcen, je nach Workload

Automatisiertes Serverklonen – plattformübergreifend

- Erhöhen Sie den Server automatisch, bis die Anzahl der verfügbaren Benutzer steigt
- Fügt den verfügbaren Ressourcen-Pools zusätzliche Server hinzu
- Kombinieren Sie die CWS Live Server Scaling-Funktion, um eine vollständig automatisierte Lösung zu schaffen

Ressourcenplanung

- Planen Sie die Servicezeiten auf Kundenbasis
- Kosteneindämmung für Public Clouds
- Schalten Sie die Systeme aus, wenn sie nicht verwendet werden, und aktivieren Sie sie nach einem vordefinierten Zeitplan erneut

Anforderungen Von Endbenutzern

Überblick

NetApp VDS verfolgt keine Endpunktgeräte verschiedener Benutzer und empfiehlt keine Empfehlung. Wir empfehlen einige Grundlagen, aber dadurch werden keine anderen möglichen Endpunktoptionen ausgeschlossen.

Remote-Desktop-Umgebungen können von verschiedenen Endgeräten aus darauf zugreifen. Kunden sind direkt bei Microsoft und Drittanbietern erhältlich. NetApp VDS bietet einen individuellen Verbindungs-Client für Windows Geräte (*NetApp VDS Client for Windows*) sowie einen Web-Client, der mit HTML 5 Browsern kompatibel ist.

Auf virtuelle Desktop-Umgebungen von Azure kann über verschiedene Endpunktgeräte zugegriffen werden. Im Gegensatz zu RDS können AVD-Umgebungen nur von nativen Microsoft-Clients genutzt werden. Microsoft hat Clients für Windows, MacOS, Android, iOS sowie einen Web-Client veröffentlicht. Darüber hinaus ist IGEL eine Partnerschaft eingegangen, um ein Linux-basiertes Thin-Client-Angebot anzubieten.

Verbindungsoptionen für Endbenutzer

Remote Desktop Services

NetApp VDS Client für Windows

Der NetApp VDS Client für Windows ist die beste Möglichkeit für Benutzer, eine Verbindung zu ihrer RDS-Umgebung herzustellen. Mit diesem einfachen Installationsprogramm können Benutzer nur mit ihrem Benutzernamen und Passwort eine Verbindung herstellen. Es ist keine Server- oder Gateway-Konfiguration erforderlich. Das Drucken und die Zuordnung lokaler Laufwerke werden automatisch aktiviert, und diese Methode hat die höchste Leistung.

VDS-Client-url-Sicherheit

Falls ausgehende Netzwerkverbindungen Controller sind und um sicherzustellen, dass sie weiterhin den NetApp VDS Client für Windows verwenden können, empfehlen wir Folgendes zur Safelist: *
`api.cloudworkspace.com * vdsclient.App * API.vdsclient.App * bin.vdsclient.App`

Auf Wunsch kann eine Markenversion dieser Bewerbung mit den Logos und Kontaktinformationen des Partners erstellt werden. Bitte wenden Sie sich an den Support, um dies anzufordern.

Der NetApp VDS Client kann hier heruntergeladen werden: <https://cwc.cloudworkspace.com/download/cwc-win-setup.exe>

Druck: bei der Verbindung mit dem NetApp VDS Client für Windows wird der Druck automatisch mithilfe von ThinPrint eingerichtet.

Lokaler Dateizugriff: standardmäßig teilt der NetApp VDS Client für Windows die lokalen Laufwerke (HDD, USB & Network) mit der Cloud-Benutzersitzung. Der Benutzer kann im Windows Explorer Daten von der „dieser PC“-Position aus durchsuchen und übertragen. Diese Funktion kann deaktiviert werden, indem der Arbeitsbereich oder der Benutzer im VDS bearbeitet wird.

VDS > Arbeitsbereiche > Benutzer und Gruppen > Sicherheitseinstellungen[]

NetApp VDS Web-Client

Der NetApp VDS Web-Client ist verfügbar unter <https://login.cloudworkspace.com/>

Endbenutzer können auch über eine Webseite auf ihren Desktop zugreifen, sofern ihr Browser HTML5 unterstützt. Browser-Kompatibilität für HTML5 kann unter geprüft werden <https://html5test.com/>

Für NetApp VDS Partner kann eine vollständig proprietäre Version dieser Seite erstellt werden. Der Partner muss ein SSL-Zertifikat bereitstellen und es gibt eine kleine Gebühr für die Implementierung von Professional Services. Wenden Sie sich an den Support, um mit dem Prozess zu beginnen.

Drucken: beim Herstellen einer Verbindung über HTML5 generiert der Druck vom Virtual Desktop eine PDF, die im Browser heruntergeladen wird und dann lokal gedruckt werden kann.

Lokaler Dateizugriff: bei der Verbindung über HTML5 kann der Benutzer Dateien auf das Cloud-Laufwerk hochladen. Dazu klicken Sie auf das Symbol der schwebenden Cloud, laden Sie die Datei hoch und navigieren Sie zu „This PC > Cloud on...“ Speicherort in Windows Explorer, um auf diese Datei in der Benutzersitzung des virtuellen Desktops zuzugreifen.

Manuell konfigurierter RDS-Client

Die zweite beste Verbindungsmethode ist die manuelle Konfiguration der Microsoft Remote Desktop-Anwendung. Das ist ideal für macOS, Linux, iOS, Android und ThinClients. Die einzige Voraussetzung ist, dass das Gerät/die Software über RDP eine Verbindung herstellen und ein RDS Gateway konfigurieren kann.

Die Informationen, die zum manuellen Konfigurieren eines RDP-Clients benötigt werden, sind (Links gehen Sie zu, wo diese Informationen gefunden werden können):

- Benutzername
- Passwort
- Server-Adresse (auch als PC-Name)
- Gateway-Adresse

Drucken: bei der Konfiguration eines lokalen RDP-Clients kann der Benutzer optional seinen Drucker in die Cloud-Umgebung zum Drucken weiterleiten.

Lokaler Dateizugriff: Wenn ein RDP-Client manuell konfiguriert wird, kann der Benutzer bestimmte Ordner für die virtuelle Desktop-Benutzersitzung freigeben.

Suchen der RDS-Gateway-Adresse

1. Navigieren Sie zu VDS (<https://manage.cloudworkspace.com>)
2. Klicken Sie Auf Bereitstellungen
3. Klicken Sie auf den Namen der Bereitstellung
4. Suchen Sie RDP Gateway unter Bereitstellungsdetails

[]

Suchen der Serveradresse für Benutzer auf einem freigegebenen Sitzungshost

Navigieren Sie zu VDS (<https://manage.cloudworkspace.com>)

1. Klicken Sie Auf Arbeitsbereiche
2. Klicken Sie auf den Namen des Arbeitsbereichs
3. Suchen Sie unter „Unternehmensinformationen“ die Serveradresse[]

Ermitteln der Server-Adresse für VDI-Benutzer

1. Navigieren Sie zu VDS (<https://manage.cloudworkspace.com>)
2. Klicken Sie Auf Arbeitsbereiche
3. Klicken Sie auf den Namen des Arbeitsbereichs
4. Suchen Sie unter „Unternehmensinformationen“ die Serveradresse[]
5. Klicken Sie auf die Registerkarte Benutzer und Gruppen
6. Klicken Sie auf den Benutzernamen
7. Suchen Sie die VDI Server-Adresse[]
8. Die Serveradresse für diesen vdi-Benutzer ist die Serveradresse: dvy.ada.cloudWorkspace.App, aber mit dem Firmencode (z.B. dvy) ersetzt durch den VDI Server-Wert (z.B. DVYTS1)...

e.g. DVYTS1.ada.cloudworkspace.app

RDS-Anforderungsmatrix

Typ	Betriebssystem	RDS-Zugriffsmethode(n) für Clients	RDS Web Client
Windows-PC	Windows 7 oder höher mit Microsoft RDP 8 App	NetApp VDS Clients konfigurieren den Client manuell	https://login.cloudworkspace.com/
MacOS	MacOS 10.10 oder höher und Microsoft Remote Desktop 8 App	Konfigurieren Sie Den Client Manuell	https://login.cloudworkspace.com/
IOS	IOS 8.0 oder höher und any "Remote Desktop App" Das RD-Gateways unterstützt	Konfigurieren Sie Den Client Manuell	https://login.cloudworkspace.com/

Typ	Betriebssystem	RDS-Zugriffsmethode(n) für Clients	RDS Web Client
Android	Android-Version, die ausgeführt werden kann "Microsoft Remote Desktop App"	Konfigurieren Sie Den Client Manuell	https://login.cloudworkspace.com/
Linux	Praktisch alle Versionen mit jeder RDS-Anwendung, die RD-Gateways unterstützt	Konfigurieren Sie Den Client Manuell	https://login.cloudworkspace.com/
Thin Client	Zahlreiche Thin Clients funktionieren, vorausgesetzt, sie unterstützen RD-Gateways. Wir empfehlen Windows-basierte Thin-Clients	Konfigurieren Sie Den Client Manuell	https://login.cloudworkspace.com/

Vergleichsmatrix

Elemente/Funktionen	HTML5-Browser	VDS Client für Windows	MacOS RDP-Client	RDP-Client auf mobilen Geräten	HTML5 Client auf mobilen Geräten
Zugriff Auf Lokale Laufwerke	Klicken Sie auf den Hintergrund und anschließend auf das Cloud-Symbol, das in der Mitte des oberen Bildschirmfensters angezeigt wird	Verfügbar in Windows Explorer	Klicken Sie mit der rechten Maustaste auf das RDP bearbeiten. Wechseln Sie zur Registerkarte Umleitung. Wählen Sie dann einen Ordner aus, den Sie zuordnen möchten. Melden Sie sich am Desktop an, und es wird als zugewiesenes Laufwerk angezeigt.	K. A.	K. A.

Elemente/Funktionen	HTML5-Browser	VDS Client für Windows	MacOS RDP-Client	RDP-Client auf mobilen Geräten	HTML5 Client auf mobilen Geräten
Bildschirmskalierung	Kann geändert werden, und ändert sich je nach Größe des Browser-Fensters. Dies kann nie größer als die Auflösung des Endpunkts (primär, Endpunkt-Monitor bei mehreren Monitoren)	Kann neu skaliert werden, entspricht aber immer der Bildschirmauflösung des Endpunkts (primärer Endpunkt-Monitor bei mehreren Monitoren)	Kann neu skaliert werden, entspricht aber immer der Bildschirmauflösung des Endpunkts (primärer Endpunkt-Monitor bei mehreren Monitoren)	K. A.	K. A.
Kopieren/Einfügen	Aktiviert durch Zwischenablage-Umleitung.	Aktiviert durch Zwischenablage-Umleitung.	Aktiviert durch Zwischenablage-Umleitung. Verwenden Sie in dem virtuellen Desktop Control + C oder V anstelle von Befehl + C oder V.	Aktiviert durch Zwischenablage-Umleitung.	Aktiviert durch Zwischenablage-Umleitung.
Druckerzuordnung	Drucken erfolgt über einen PDF-Druckertreiber, mit dem Browser lokale und Netzwerkdrucker erkennen	Alle lokalen und Netzwerkdrucker sind über das ThinPrint-Dienstprogramm abgebildet	Alle lokalen und Netzwerkdrucker sind über das ThinPrint-Dienstprogramm abgebildet	Alle lokalen und Netzwerkdrucker sind über das ThinPrint-Dienstprogramm abgebildet	Drucken erfolgt über einen PDF-Druckertreiber, mit dem Browser lokale und Netzwerkdrucker erkennen
Leistung	RemoteFX (Erweiterung von Audio und Video) nicht aktiviert	RemoteFX wurde über RDP aktiviert und verbessert die Audio-/Video-Leistung	RemoteFX wurde über RDP aktiviert und verbessert die Audio-/Video-Leistung	RemoteFX aktiviert, Verbesserung der Audio-/Video-Leistung	RemoteFX (Erweiterung von Audio/Video) nicht aktiviert
Verwendung der Maus auf dem Mobilgerät	K. A.	K. A.	K. A.	Tippen Sie auf den Bildschirm, um die Maus zu bewegen, und klicken Sie auf	Halten Sie den Bildschirm gedrückt und ziehen Sie, um die Maus zu bewegen, tippen Sie auf, um auf zu klicken

Peripheriegeräte

Drucken

- Der Virtual Desktop Client umfasst ThinPrint, das lokale Drucker nahtlos an den Cloud-Desktop weiterleitet.
- Die HTML5-Verbindungsmethode lädt ein PDF zum lokalen Drucken im Browser herunter.
- Mit der Microsoft Remote Desktop 8 App auf MacOS können Benutzer Drucker auf dem Cloud-Desktop freigeben

USB-Peripheriegeräte

Produkte wie Scanner, Kameras, Kartenleser, Audiogeräte haben Mischergebnisse. Eine Virtual Desktop-Bereitstellung ist nichts Besonderes, das dies verhindert, aber die beste Wahl ist, alle erforderlichen Geräte zu testen. Ihr Vertriebsmitarbeiter kann bei Bedarf die Einrichtung von Testkonten unterstützen.

Bandbreite

- NetApp empfiehlt eine Bandbreite von mindestens 150 kb pro Benutzer. Höhere Kapazität verbessert die Benutzerfreundlichkeit.
- Internetlatenz unter 100 ms und sehr geringer Jitter sind ebenso wichtig. KB-Artikel
- Zusätzliche Bandbreite wird durch die Verwendung VON VOIP, Video-Streaming, Audio-Streaming und allgemeinen Internet-Browsing eingeführt werden.
- Die vom Virtual Desktop selbst verbrauchte Bandbreite ist bei der Berechnung der Anforderungen an die Bandbreite des Benutzers eine der kleinsten Komponenten.

Empfehlungen zur Bandbreite von Microsoft

<https://docs.microsoft.com/en-us/azure/virtual-desktop/bandwidth-recommendations>

App-Empfehlungen

Workload	Beispielanwendungen	Empfohlene Bandbreite
Task Worker	Microsoft Word, Outlook, Excel, Adobe Reader	1.5 Mbit/S
Büroangestellte	Microsoft Word, Outlook, Excel, Adobe Reader, PowerPoint, Foto Viewer	3 Mbit/S
Knowledge Worker	Microsoft Word, Outlook, Excel, Adobe Reader, PowerPoint, Photo Viewer, Java	5 Mbit/S
Power Worker	Microsoft Word, Outlook, Excel, Adobe Reader, PowerPoint, Photo Viewer, Java, CAD/CAM, Illustration/Publishing	15 Mbit/S



Diese Empfehlungen gelten unabhängig davon, wie viele Benutzer sich in der Sitzung befinden.

Empfehlungen zur Anzeigeauflösung

Typische Bildschirmauflösungen bei 30 Bildern/s	Empfohlene Bandbreite
Etwa 1024 × 768 px	1.5 Mbit/S

Typische Bildschirmauflösungen bei 30 Bildern/s	Empfohlene Bandbreite
Etwa 1280 × 720 px	3 Mbit/S
Etwa 1920 × 1080 px	5 Mbit/S
Ca. 3840 × 2160 px (4K)	15 Mbit/S

Ressourcen für lokale Geräte

- Lokale Systemressourcen wie RAM, CPU, Netzwerkkarten und Grafikfunktionen verursachen Abweichungen in der Benutzererfahrung.
- Dies trifft AM MEISTEN auf Netzwerk- und Grafikfunktionen zu.
- 1 GB RAM und ein Low-Power-Prozessor auf einem kostengünstigen Windows-Gerät. 2-4 GB RAM wird als Minimum empfohlen.

Azure Virtual Desktop

AVD Windows-Client

Laden Sie den Windows 7/10-Client von herunter <https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-windows-7-10> Und melden Sie sich mit dem Benutzernamen und Kennwort des Endbenutzers an. Beachten Sie, dass Remote-App- und Desktop-Verbindungen (RADC), Remote Desktop Connection (mstsc) und der NetApp VDS Client für Windows-Applikation derzeit nicht die Möglichkeit zur Anmeldung bei AVD-Instanzen bieten.

AVD-Webclient

Navigieren Sie in einem Browser zur mit Azure Resource Manager integrierten Version des Web-Clients Azure Virtual Desktop unter <https://rdweb.AVD.microsoft.com/arm/webclient> Und melden Sie sich mit Ihrem Benutzerkonto an.



Wenn Sie Azure Virtual Desktop (klassisch) ohne Integration in Azure Resource Manager nutzen, stellen Sie eine Verbindung zu Ihren Ressourcen unter her <https://rdweb.AVD.microsoft.com/webclient> Stattdessen.

VDS-Umgebungen ändern

Überblick

Der Virtual Desktop Service von NetApp ermöglicht Unternehmen das Management von Implementierungen auf früheren Versionen, die Vorschau zukünftiger Versionen und das Management von Umgebungen, die eine Version vor (N-1-Methodik) ausführen.

URLs für den virtuellen Desktop-Dienst

Virtual Desktop Service ist die Managementkonsole, mit der Administratoren VDS-Implementierungen fortlaufend verwalten können.

Umgebung	Beschreibung	URL	Codebase	API-Dokumentation
Vorschau	Vorschaufenster der bevorstehenden Version	https://preview.manage.cloudworksace.com/	5.4	https://api.cloudworkspace.com/5.4/swagger/ui/index
Strom	Aktuelle Version	https://manage.vds.netapp.com/	6.0	https://api.cloudworkspace.com/6.0/swagger/ui/index
Zurück	Vorherige Version	https://manage.cloudworkspace.com/	5.4	https://api.cloudworkspace.com/5.4/swagger/ui/index

Bereitstellung Von Virtual Desktop Services

VDS bietet einen assistentengesteuerten Implementierungsprozess, mit dem Administratoren die Provisionierung einer AVD- und/oder virtuellen Desktop-Umgebung deutlich optimieren können.

Administratoren können keine Implementierungen in einer älteren Umgebung bereitstellen – nur in einer aktuellen oder Vorschauumgebung.

Umgebung	Beschreibung	URL	Codebase	Implementierungseinfaden
Strom	Aktuelle Version	https://manage.vds.netapp.com/deployments/add	5.4	"VDS v6.0 - Bereitstellungshandbuch"
Zurück	Vorherige Version	https://cwasetup.cloudworkspace.com	5.4	Wenden Sie Sich An Den Support

VDS Kostenplaner

Der VDS-Kostenplanator ist ein speziell entwickeltes Tool mit Mehrwert, mit dem Unternehmen die Kosten der Public Cloud entweder in Azure oder in Google Cloud abschätzen können. Das Tool bietet Möglichkeiten, die Budgets zu variieren und zu optimieren, um die Lösung bereitzustellen, die im Budget eines Unternehmens erforderlich ist.

Umgebung	Beschreibung	URL
Validierung	Vorschau für die kommende Version	https://val.manage.vds.netapp.com/cost-estimator
Strom	Aktuelle Version	https://manage.vds.netapp.com/cost-estimator

Dokumentation Der Skriptbibliothek

Scripted Event Documentation – Adobe Reader DC

Übersicht Über Globale Skripts

NetApp VDS umfasst eine Bibliothek mit vordefinierten skriptbasierten Ereignissen, die direkt in VDS-Umgebungen verwendet und/oder dupliziert und als Bausteine für individuelle skriptbasierte Ereignisse

verwendet werden können.

In diesem Artikel werden sowohl die Aktion Install/Enable als auch die Deinstallation/Deaktivierung behandelt.

Verwendung Von Globalen Skripten

Integrierte skriptbasierte Ereignisse wie diese sind bereits ausgefüllt. Wenn Sie das Kontrollkästchen „globaler“-Filter aktivieren, werden diese angezeigt.

Globale skriptbasierte Ereignisse wie diese sind schreibgeschützt. Sie können als ist verwendet werden oder über die Funktion „Klonen“ kann eine Kundenkopie für die Bearbeitung und Nutzung erstellt werden.

Die Schaltfläche Klonen befindet sich im Aktivitätsmenü auf der Seite „skriptbasierte Ereignisse“.

[Scriptbibliothek.Übersicht 2cb2] | [scriptlibrary.overview-2ccb2.png](#)

Adobe Reader DC-Übersicht

Dieses Skript-Paket installiert/deinstalliert *Adobe Reader DC* mithilfe des chocolatey-Paketmanagers (<https://chocolatey.org/>) Um die Bereitstellung zu erledigen. Chocolatey wird von VDS bereitgestellt, wenn VMs erstellt werden. Dieses Skript prüft aber auch Chocolatey und installiert es als Voraussetzung, wenn es fehlt.

Standardpfad für Verknüpfungen

Der standardmäßige Verknüpfungspfad wird unten eingegeben, für diese Anwendung ist die Verknüpfung:

\\shortcuts\Acrobat Reader DC.lnk

Screenshot des Dialogfensters „Aktivität hinzufügen“

[Scriptbibliothek.activity.InstallAdobeReader] | [scriptlibrary.activity.InstallAdobeReader.png](#)

Vorgang zur Installation/Deinstallation von Anwendungen hinzufügen

Damit ein Skript im Repository eine Aktion ausführen kann, muss ein Vorgang erstellt werden, um dieses Skript einem ausgewählten Trigger zuzuordnen. In diesem Beispiel wird diese Anwendung installiert/deinstalliert, wenn die App zum Arbeitsbereich hinzugefügt oder aus diesem entfernt wird (von der Seite *Workspace > Anwendungen* im VDS).

VDS skriptbasierte Ereignisse bieten viele andere Arten von Aktivitäts-Triggern wie *Create Server*, die als Alternative zum Ereignistyp *Application Install* (oder *Application Uninstall*) verwendet werden können. Mit *Create Server* würde diese App-Installation einfach auf alle neu erstellten VMs im VDS ausgeführt. *Create Server* und andere Trigger werden dokumentiert und können untersucht werden ["Hier"](#).



Diese Anwendung muss in der VDS-Anwendungsbibliothek vorhanden sein. Das ["Abschnitt"](#) Der Artikel über die Anwendungsberechtigung für RDS umfasst das Hinzufügen von Apps zur Bibliothek.

So erstellen Sie eine Aktivität und verknüpfen dieses Skript mit einer Aktion:

1. Navigieren Sie im VDS zum Abschnitt „*skriptbasierte Ereignisse*“
2. Klicken Sie unter „Aktivitäten“ auf + *Aktivität hinzufügen*
3. Geben Sie im geöffneten Dialogfeld die folgenden Informationen ein:
 - **Name:** Benennen Sie diese Aktivität

- **Beschreibung:** Geben Sie optional eine Beschreibung ein
- **Bereitstellung** Wählen Sie die gewünschte Bereitstellung aus der Dropdown-Liste aus
- **Skript:** Wählen Sie das Skript install (oder uninstall) aus dem Dropdown-Menü aus. Dies könnte das globale Skript oder Kundenskript sein, das Sie geklont und angepasst haben.
- **Argumente:** Legen Sie leer
- **Kontrollkästchen aktiviert:** Check Lieferumfang
- **Ereignistyp:** Wählen Sie Aus Application Install (Oder Application Uninstall) aus dem Dropdown-Menü
- **Anwendung:** Wählen Sie diese Anwendung aus der Dropdown-Liste aus
- **Verknüpfungspfad:** Geben Sie den Standard-Verknüpfungspfad für diese Anwendung ein (siehe oben)

Scripted Event Documentation - AMD Radeon Instinct Treiber

Übersicht Über Globale Skripts

NetApp VDS umfasst eine Bibliothek mit vordefinierten skriptbasierten Ereignissen, die direkt in VDS-Umgebungen verwendet und/oder dupliziert und als Bausteine für individuelle skriptbasierte Ereignisse verwendet werden können.

In diesem Artikel werden sowohl die Aktion Install/Enable als auch die Deinstallation/Deaktivierung behandelt.

Verwendung Von Globalen Skripten

Integrierte skriptbasierte Ereignisse wie diese sind bereits ausgefüllt. Wenn Sie das Kontrollkästchen „globaler“-Filter aktivieren, werden diese angezeigt.

Globale skriptbasierte Ereignisse wie diese sind schreibgeschützt. Sie können als ist verwendet werden oder über die Funktion „Klonen“ kann eine Kundenkopie für die Bearbeitung und Nutzung erstellt werden.

Die Schaltfläche Klonen befindet sich im Aktivitätsmenü auf der Seite „skriptbasierte Ereignisse“.

[Scriptbibliothek.Übersicht 2cb2] | [scriptlibrary.overview-2ccb2.png](#)

AMD Radeon Instinct Treiber – Übersicht

Dieses Skript-Paket installiert/deinstalliert *AMD Radeon Instinct Drivers* mithilfe des chocolatey-Paketmanagers (<https://chocolatey.org/>) Um die Bereitstellung zu erledigen. Chocolatey wird von VDS bereitgestellt, wenn VMs erstellt werden. Dieses Skript prüft aber auch Chocolatey und installiert es als Voraussetzung, wenn es fehlt.

Screenshot des Dialogfensters „Aktivität hinzufügen“

[Scriptbibliothek.activity.InstallAMDRadeonInstinctDrivers] |

Manuelle Aktivität hinzufügen

Damit ein Skript im Repository eine Aktion ausführen kann, muss ein Vorgang erstellt werden, um dieses Skript einem ausgewählten Trigger zuzuordnen. In diesem Beispiel wird die Aktivität ausgeführt, wenn der VDS Admin das Skript manuell auslöst.

VDS skriptbasierte Ereignisse bieten viele andere Arten von Aktivitäts-Triggern wie *Create Server*, die als Alternative zum Ereignistyp *Manual* verwendet werden können. Mit *Create Server* würde dieses Skript einfach auf allen neu erstellten VMs im VDS ausgeführt. *Create Server* und andere Trigger werden dokumentiert und können untersucht werden "[Hier](#)".

So erstellen Sie eine Aktivität und verknüpfen dieses Skript mit einer Aktion:

1. Navigieren Sie zum Abschnitt „skriptbasierte Ereignisse“ im VDS
2. Klicken Sie unter „Aktivitäten“ auf + *Aktivität hinzufügen*
3. Geben Sie im geöffneten Dialogfeld die folgenden Informationen ein:
 - **Name:** Benennen Sie diese Aktivität
 - **Beschreibung:** Geben Sie optional eine Beschreibung ein
 - **Bereitstellung** Wählen Sie die gewünschte Bereitstellung aus der Dropdown-Liste aus
 - **Skript:** Wählen Sie das Skript install (oder uninstall) aus dem Dropdown-Menü aus. Dies könnte das globale Skript oder Kundenscript sein, das Sie geklont und angepasst haben.
 - **Argumente:** Legen Sie leer
 - **Kontrollkästchen aktiviert:** Check Lieferumfang
 - **Ereignistyp:** Wählen Sie Aus Manual Aus der Dropdown-Liste
 - **Zieltyp:** Wählen Sie das aus Servers Optionsfeld
 - * **Verwaltete Server:*** Check Die Box für jede VM, die diese Deinstallation erhalten soll.

Scripted Event Documentation – Ezeep Print App

Übersicht Über Globale Skripts

NetApp VDS umfasst eine Bibliothek mit vordefinierten skriptbasierten Ereignissen, die direkt in VDS-Umgebungen verwendet und/oder dupliziert und als Bausteine für individuelle skriptbasierte Ereignisse verwendet werden können.

In diesem Artikel werden sowohl die Aktion Install/Enable als auch die Deinstallation/Deaktivierung behandelt.

Verwendung Von Globalen Skripten

Integrierte skriptbasierte Ereignisse wie diese sind bereits ausgefüllt. Wenn Sie das Kontrollkästchen „globaler“-Filter aktivieren, werden diese angezeigt.

Globale skriptbasierte Ereignisse wie diese sind schreibgeschützt. Sie können als ist verwendet werden oder über die Funktion „Klonen“ kann eine Kundenkopie für die Bearbeitung und Nutzung erstellt werden.

Die Schaltfläche Klonen befindet sich im Aktivitätsmenü auf der Seite „skriptbasierte Ereignisse“.

Übersicht über die Ezeep Print App

Dieses Skript-Paket installiert/deinstalliert *Ezeep Print App* mithilfe des chocolatey-Paketmanagers (<https://chocolatey.org/>) Um die Bereitstellung zu erledigen. Chocolatey wird von VDS bereitgestellt, wenn VMs erstellt werden. Dieses Skript prüft aber auch Chocolatey und installiert es als Voraussetzung, wenn es fehlt.

Standardpfad für Verknüpfungen

Der standardmäßige Verknüpfungspfad wird unten eingegeben, für diese Anwendung ist die Verknüpfung:

```
\\shortcuts\Printer Self Service.lnk
```

Screenshot des Dialogfensters „Aktivität hinzufügen“

[Scriptbibliothek.activity.InstallEzeepPrintApp] | *scriptlibrary.activity.InstallEzeepPrintApp.png*

Vorgang zur Installation/Deinstallation von Anwendungen hinzufügen

Damit ein Skript im Repository eine Aktion ausführen kann, muss ein Vorgang erstellt werden, um dieses Skript einem ausgewählten Trigger zuzuordnen. In diesem Beispiel wird diese Anwendung installiert/deinstalliert, wenn die App zum Arbeitsbereich hinzugefügt oder aus diesem entfernt wird (von der Seite *Workspace > Anwendungen* im VDS).

VDS skriptbasierte Ereignisse bieten viele andere Arten von Aktivitäts-Triggern wie *Create Server*, die als Alternative zum Ereignistyp *Application Install* (oder *Application Uninstall*) verwendet werden können. Mit *Create Server* würde diese App-Installation einfach auf alle neu erstellten VMs im VDS ausgeführt. *Create Server* und andere Trigger werden dokumentiert und können untersucht werden "[Hier](#)".



Diese Anwendung muss in der VDS-Anwendungsbibliothek vorhanden sein. Das "[Abschnitt](#)" Der Artikel über die Anwendungsberechtigung für RDS umfasst das Hinzufügen von Apps zur Bibliothek.

So erstellen Sie eine Aktivität und verknüpfen dieses Skript mit einer Aktion:

1. Navigieren Sie im VDS zum Abschnitt „*skriptbasierte Ereignisse*“
2. Klicken Sie unter „Aktivitäten“ auf + *Aktivität hinzufügen*
3. Geben Sie im geöffneten Dialogfeld die folgenden Informationen ein:
 - **Name:** Benennen Sie diese Aktivität
 - **Beschreibung:** Geben Sie optional eine Beschreibung ein
 - **Bereitstellung** Wählen Sie die gewünschte Bereitstellung aus der Dropdown-Liste aus
 - **Skript:** Wählen Sie das Skript *install* (oder *uninstall*) aus dem Dropdown-Menü aus. Dies könnte das globale Skript oder Kundenscript sein, das Sie geklont und angepasst haben.
 - **Argumente:** Legen Sie leer
 - **Kontrollkästchen aktiviert:** *Check* Lieferumfang
 - **Ereignistyp:** Wählen Sie Aus *Application Install* (Oder *Application Uninstall*) aus dem Dropdown-Menü
 - **Anwendung:** Wählen Sie diese Anwendung aus der Dropdown-Liste aus
 - **Verknüpfungspfad:** Geben Sie den Standard-Verknüpfungspfad für diese Anwendung ein (siehe oben)

Scripted Event Documentation - Google Chrome

Übersicht Über Globale Skripts

NetApp VDS umfasst eine Bibliothek mit vordefinierten skriptbasierten Ereignissen, die direkt in VDS-Umgebungen verwendet und/oder dupliziert und als Bausteine für individuelle skriptbasierte Ereignisse verwendet werden können.

In diesem Artikel werden sowohl die Aktion Install/Enable als auch die Deinstallation/Deaktivierung behandelt.

Verwendung Von Globalen Skripten

Integrierte skriptbasierte Ereignisse wie diese sind bereits ausgefüllt. Wenn Sie das Kontrollkästchen „globaler“-Filter aktivieren, werden diese angezeigt.

Globale skriptbasierte Ereignisse wie diese sind schreibgeschützt. Sie können als ist verwendet werden oder über die Funktion „Klonen“ kann eine Kundenkopie für die Bearbeitung und Nutzung erstellt werden.

Die Schaltfläche Klonen befindet sich im Aktivitätsmenü auf der Seite „skriptbasierte Ereignisse“.

[Scriptbibliothek.Übersicht 2cb2] | [scriptlibrary.overview-2ccb2.png](#)

Google Chrome Übersicht

Dieses Skript-Paket installiert/deinstalliert *Google Chrome* mit dem chocolatey Paketmanager (<https://chocolatey.org/>) Um die Bereitstellung zu erledigen. Chocolatey wird von VDS bereitgestellt, wenn VMs erstellt werden. Dieses Skript prüft aber auch Chocolatey und installiert es als Voraussetzung, wenn es fehlt.

Standardpfad für Verknüpfungen

Der standardmäßige Verknüpfungspfad wird unten eingegeben, für diese Anwendung ist die Verknüpfung:
\\shortcuts\Google Chrome.lnk

Screenshot des Dialogfensters „Aktivität hinzufügen“

[Scriptbibliothek.activity.InstallGoogleChrome] | [scriptlibrary.activity.InstallGoogleChrome.png](#)

Vorgang zur Installation/Deinstallation von Anwendungen hinzufügen

Damit ein Skript im Repository eine Aktion ausführen kann, muss ein Vorgang erstellt werden, um dieses Skript einem ausgewählten Trigger zuzuordnen. In diesem Beispiel wird diese Anwendung installiert/deinstalliert, wenn die App zum Arbeitsbereich hinzugefügt oder aus diesem entfernt wird (von der Seite *Workspace > Anwendungen* im VDS).

VDS skriptbasierte Ereignisse bieten viele andere Arten von Aktivitäts-Trigger wie *Create Server*, die als Alternative zum Ereignistyp *Application Install* (oder *Application Uninstall*) verwendet werden können. Mit *Create Server* würde diese App-Installation einfach auf alle neu erstellten VMs im VDS ausgeführt. *Create Server* und andere Trigger werden dokumentiert und können untersucht werden "[Hier](#)".



Diese Anwendung muss in der VDS-Anwendungsbibliothek vorhanden sein. Das "[Abschnitt](#)" Der Artikel über die Anwendungsberechtigung für RDS umfasst das Hinzufügen von Apps zur Bibliothek.

So erstellen Sie eine Aktivität und verknüpfen dieses Skript mit einer Aktion:

1. Navigieren Sie im VDS zum Abschnitt „*skriptbasierte Ereignisse*“
2. Klicken Sie unter „Aktivitäten“ auf + *Aktivität hinzufügen*
3. Geben Sie im geöffneten Dialogfeld die folgenden Informationen ein:
 - **Name:** Benennen Sie diese Aktivität
 - **Beschreibung:** Geben Sie optional eine Beschreibung ein
 - **Bereitstellung** Wählen Sie die gewünschte Bereitstellung aus der Dropdown-Liste aus
 - **Skript:** Wählen Sie das Skript install (oder uninstall) aus dem Dropdown-Menü aus. Dies könnte das globale Skript oder Kundenscript sein, das Sie geklont und angepasst haben.
 - **Argumente:** Legen Sie leer
 - **Kontrollkästchen aktiviert:** Check Lieferumfang
 - **Ereignistyp:** Wählen Sie Aus Application Install (Oder Application Uninstall) aus dem Dropdown-Menü
 - **Anwendung:** Wählen Sie diese Anwendung aus der Dropdown-Liste aus
 - **Verknüpfungspfad:** Geben Sie den Standard-Verknüpfungspfad für diese Anwendung ein (siehe oben)

Scripted Event Documentation – Microsoft Edge Chromium

Übersicht Über Globale Skripts

NetApp VDS umfasst eine Bibliothek mit vordefinierten skriptbasierten Ereignissen, die direkt in VDS-Umgebungen verwendet und/oder dupliziert und als Bausteine für individuelle skriptbasierte Ereignisse verwendet werden können.

In diesem Artikel werden sowohl die Aktion Install/Enable als auch die Deinstallation/Deaktivierung behandelt.

Verwendung Von Globalen Skripten

Integrierte skriptbasierte Ereignisse wie diese sind bereits ausgefüllt. Wenn Sie das Kontrollkästchen „globaler“-Filter aktivieren, werden diese angezeigt.

Globale skriptbasierte Ereignisse wie diese sind schreibgeschützt. Sie können als ist verwendet werden oder über die Funktion „Klonen“ kann eine Kundenkopie für die Bearbeitung und Nutzung erstellt werden.

Die Schaltfläche Klonen befindet sich im Aktivitätsmenü auf der Seite „skriptbasierte Ereignisse“.

[Scriptbibliothek.Übersicht 2cb2] | [scriptlibrary.overview-2ccb2.png](#)

Microsoft Edge Chromium-Übersicht

Dieses Skript-Paket installiert/deinstalliert *Microsoft Edge Chromium* mithilfe des chocolatey-Paketmanagers (<https://chocolatey.org/>) Um die Bereitstellung zu erledigen. Chocolatey wird von VDS bereitgestellt, wenn VMs erstellt werden. Dieses Skript prüft aber auch Chocolatey und installiert es als Voraussetzung, wenn es fehlt.

Standardpfad für Verknüpfungen

Der standardmäßige Verknüpfungspfad wird unten eingegeben, für diese Anwendung ist die Verknüpfung:
`\\shortcuts\Microsoft Edge.lnk`

Screenshot des Dialogfensters „Aktivität hinzufügen“

[Scriptbibliothek.activity.InstallMicrosoftEdgeChrom] | *scriptlibrary.activity.InstallMicrosoftEdgeChromium.png*

Vorgang zur Installation/Deinstallation von Anwendungen hinzufügen

Damit ein Skript im Repository eine Aktion ausführen kann, muss ein Vorgang erstellt werden, um dieses Skript einem ausgewählten Trigger zuzuordnen. In diesem Beispiel wird diese Anwendung installiert/deinstalliert, wenn die App zum Arbeitsbereich hinzugefügt oder aus diesem entfernt wird (von der Seite *Workspace > Anwendungen* im VDS).

VDS skriptbasierte Ereignisse bieten viele andere Arten von Aktivitäts-Triggern wie *Create Server*, die als Alternative zum Ereignistyp *Application Install* (oder *Application Uninstall*) verwendet werden können. Mit *Create Server* würde diese App-Installation einfach auf alle neu erstellten VMs im VDS ausgeführt. *Create Server* und andere Trigger werden dokumentiert und können untersucht werden ["Hier"](#).



Diese Anwendung muss in der VDS-Anwendungsbibliothek vorhanden sein. Das ["Abschnitt"](#) Der Artikel über die Anwendungsberechtigung für RDS umfasst das Hinzufügen von Apps zur Bibliothek.

So erstellen Sie eine Aktivität und verknüpfen dieses Skript mit einer Aktion:

1. Navigieren Sie im VDS zum Abschnitt „*skriptbasierte Ereignisse*“
2. Klicken Sie unter „Aktivitäten“ auf + *Aktivität hinzufügen*
3. Geben Sie im geöffneten Dialogfeld die folgenden Informationen ein:
 - **Name:** Benennen Sie diese Aktivität
 - **Beschreibung:** Geben Sie optional eine Beschreibung ein
 - **Bereitstellung** Wählen Sie die gewünschte Bereitstellung aus der Dropdown-Liste aus
 - **Skript:** Wählen Sie das Skript *install* (oder *uninstall*) aus dem Dropdown-Menü aus. Dies könnte das globale Skript oder Kundenscript sein, das Sie geklont und angepasst haben.
 - **Argumente:** Legen Sie leer
 - **Kontrollkästchen aktiviert:** *Check* Lieferumfang
 - **Ereignistyp:** Wählen Sie Aus *Application Install* (Oder *Application Uninstall*) aus dem Dropdown-Menü
 - **Anwendung:** Wählen Sie diese Anwendung aus der Dropdown-Liste aus
 - **Verknüpfungspfad:** Geben Sie den Standard-Verknüpfungspfad für diese Anwendung ein (siehe oben)

Skript-Ereignisdokumentation – Microsoft Office 365

Übersicht Über Globale Skripts

NetApp VDS umfasst eine Bibliothek mit vordefinierten skriptbasierten Ereignissen, die direkt in VDS-Umgebungen verwendet und/oder dupliziert und als Bausteine für individuelle skriptbasierte Ereignisse verwendet werden können.

In diesem Artikel werden sowohl die Aktion *Install/Enable* als auch die *Deinstallation/Deaktivierung* behandelt.

Verwendung Von Globalen Skripten

Integrierte skriptbasierte Ereignisse wie diese sind bereits ausgefüllt. Wenn Sie das Kontrollkästchen „globaler“-Filter aktivieren, werden diese angezeigt.

Globale skriptbasierte Ereignisse wie diese sind schreibgeschützt. Sie können als ist verwendet werden oder über die Funktion „Klonen“ kann eine Kundenkopie für die Bearbeitung und Nutzung erstellt werden.

Die Schaltfläche Klonen befindet sich im Aktivitätsmenü auf der Seite „skriptbasierte Ereignisse“.

[Scriptbibliothek.Übersicht 2cb2] | [scriptlibrary.overview-2ccb2.png](#)

Übersicht über Microsoft Office 365

Dieses Skript-Paket installiert/deinstalliert *Microsoft Office* mithilfe des chocolatey-Paketmanagers (<https://chocolatey.org/>) Um die Bereitstellung zu erledigen. Chocolatey wird von VDS bereitgestellt, wenn VMs erstellt werden. Dieses Skript prüft aber auch Chocolatey und installiert es als Voraussetzung, wenn es fehlt.



Dieses Installationsskript für Microsoft Office 365 enthält keine Microsoft Teams oder Microsoft One Drive. Diese werden als eigenständige automatisierte Skripte enthalten, die eine größere Flexibilität ermöglichen, da einige Implementierungen diese Applikationen nicht erfordern. Diese Bereitstellung kann kopiert und bearbeitet werden, um sie einzubeziehen (oder andere zu ändern "Office Deployment Tool" Einstellungen) durch Klonen des Skripts aus VDS und Bearbeiten des InstallMicrosoftOffice365.ps1, um unterschiedliche Werte in die XML-Konfigurationsdatei einzugeben.

Standardpfad für Verknüpfungen

Der standardmäßige Verknüpfungspfad wird unten eingegeben, für diese Anwendung ist die Verknüpfung:
\\folders\Microsoft Office

Screenshot des Dialogfensters „Aktivität hinzufügen“

[ScriptLibrary.activity.InstallMicrosoftOffice365] | [scriptlibrary.activity.InstallMicrosoftOffice365.png](#)

Vorgang zur Installation/Deinstallation von Anwendungen hinzufügen

Damit ein Skript im Repository eine Aktion ausführen kann, muss ein Vorgang erstellt werden, um dieses Skript einem ausgewählten Trigger zuzuordnen. In diesem Beispiel wird diese Anwendung installiert/deinstalliert, wenn die App zum Arbeitsbereich hinzugefügt oder aus diesem entfernt wird (von der Seite *Workspace > Anwendungen* im VDS).

VDS skriptbasierte Ereignisse bieten viele andere Arten von Aktivitäts-Triggern wie *Create Server*, die als Alternative zum Ereignistyp *Application Install* (oder *Application Uninstall*) verwendet werden können. Mit *Create Server* würde diese App-Installation einfach auf alle neu erstellten VMs im VDS ausgeführt. *Create Server* und andere Trigger werden dokumentiert und können untersucht werden "[Hier](#)".



Diese Anwendung muss in der VDS-Anwendungsbibliothek vorhanden sein. Das "[Abschnitt](#)" Der Artikel über die Anwendungsberechtigung für RDS umfasst das Hinzufügen von Apps zur Bibliothek.

So erstellen Sie eine Aktivität und verknüpfen dieses Skript mit einer Aktion:

1. Navigieren Sie im VDS zum Abschnitt „*skriptbasierte Ereignisse*“

2. Klicken Sie unter „Aktivitäten“ auf + *Aktivität hinzufügen*
3. Geben Sie im geöffneten Dialogfeld die folgenden Informationen ein:
 - **Name:** Benennen Sie diese Aktivität
 - **Beschreibung:** Geben Sie optional eine Beschreibung ein
 - **Bereitstellung** Wählen Sie die gewünschte Bereitstellung aus der Dropdown-Liste aus
 - **Skript:** Wählen Sie das Skript install (oder uninstall) aus dem Dropdown-Menü aus. Dies könnte das globale Skript oder Kundenskript sein, das Sie geklont und angepasst haben.
 - **Argumente:** Legen Sie leer
 - **Kontrollkästchen aktiviert:** Check Lieferumfang
 - **Ereignistyp:** Wählen Sie Aus Application Install (Oder Application Uninstall) aus dem Dropdown-Menü
 - **Anwendung:** Wählen Sie diese Anwendung aus der Dropdown-Liste aus
 - **Verknüpfungspfad:** Geben Sie den Standard-Verknüpfungspfad für diese Anwendung ein (siehe oben)

Scripted Event Documentation – Microsoft OneDrive

Übersicht Über Globale Skripts

NetApp VDS umfasst eine Bibliothek mit vordefinierten skriptbasierten Ereignissen, die direkt in VDS-Umgebungen verwendet und/oder dupliziert und als Bausteine für individuelle skriptbasierte Ereignisse verwendet werden können.

In diesem Artikel werden sowohl die Aktion Install/Enable als auch die Deinstallation/Deaktivierung behandelt.

Verwendung Von Globalen Skripten

Integrierte skriptbasierte Ereignisse wie diese sind bereits ausgefüllt. Wenn Sie das Kontrollkästchen „globaler“-Filter aktivieren, werden diese angezeigt.

Globale skriptbasierte Ereignisse wie diese sind schreibgeschützt. Sie können als ist verwendet werden oder über die Funktion „Klonen“ kann eine Kundenkopie für die Bearbeitung und Nutzung erstellt werden.

Die Schaltfläche Klonen befindet sich im Aktivitätsmenü auf der Seite „skriptbasierte Ereignisse“.

[Scriptbibliothek.Übersicht 2cb2] | [scriptlibrary.overview-2ccb2.png](#)

Microsoft OneDrive Übersicht

Dieses Skript-Paket installiert/deinstalliert *Microsoft OneDrive* mithilfe des chocolatey-Paketmanagers (<https://chocolatey.org/>) Um die Bereitstellung zu erledigen. Chocolatey wird von VDS bereitgestellt, wenn VMs erstellt werden. Dieses Skript prüft aber auch Chocolatey und installiert es als Voraussetzung, wenn es fehlt.

Standardpfad für Verknüpfungen

Der standardmäßige Verknüpfungspfad wird unten eingegeben, für diese Anwendung ist die Verknüpfung:
`\\shortcuts\OneDrive.lnk`

Screenshot des Dialogfensters „Aktivität hinzufügen“

[Scriptbibliothek.activity.InstallMicrosoftOneDrive] | *scriptlibrary.activity.InstallMicrosoftOneDrive.png*

Vorgang zur Installation/Deinstallation von Anwendungen hinzufügen

Damit ein Skript im Repository eine Aktion ausführen kann, muss ein Vorgang erstellt werden, um dieses Skript einem ausgewählten Trigger zuzuordnen. In diesem Beispiel wird diese Anwendung installiert/deinstalliert, wenn die App zum Arbeitsbereich hinzugefügt oder aus diesem entfernt wird (von der Seite *Workspace > Anwendungen* im VDS).

VDS skriptbasierte Ereignisse bieten viele andere Arten von Aktivitäts-Triggern wie *Create Server*, die als Alternative zum Ereignistyp *Application Install* (oder *Application Uninstall*) verwendet werden können. Mit *Create Server* würde diese App-Installation einfach auf alle neu erstellten VMs im VDS ausgeführt. *Create Server* und andere Trigger werden dokumentiert und können untersucht werden ["Hier"](#).



Diese Anwendung muss in der VDS-Anwendungsbibliothek vorhanden sein. Das ["Abschnitt"](#) Der Artikel über die Anwendungsberechtigung für RDS umfasst das Hinzufügen von Apps zur Bibliothek.

So erstellen Sie eine Aktivität und verknüpfen dieses Skript mit einer Aktion:

1. Navigieren Sie im VDS zum Abschnitt „*skriptbasierte Ereignisse*“
2. Klicken Sie unter „Aktivitäten“ auf **+ Aktivität hinzufügen**
3. Geben Sie im geöffneten Dialogfeld die folgenden Informationen ein:
 - **Name:** Benennen Sie diese Aktivität
 - **Beschreibung:** Geben Sie optional eine Beschreibung ein
 - **Bereitstellung** Wählen Sie die gewünschte Bereitstellung aus der Dropdown-Liste aus
 - **Skript:** Wählen Sie das Skript *install* (oder *uninstall*) aus dem Dropdown-Menü aus. Dies könnte das globale Skript oder Kundenscript sein, das Sie geklont und angepasst haben.
 - **Argumente:** Legen Sie leer
 - **Kontrollkästchen aktiviert:** *Check Lieferumfang*
 - **Ereignistyp:** Wählen Sie *Application Install* (Oder *Application Uninstall*) aus dem Dropdown-Menü
 - **Anwendung:** Wählen Sie diese Anwendung aus der Dropdown-Liste aus
 - **Verknüpfungspfad:** Geben Sie den Standard-Verknüpfungspfad für diese Anwendung ein (siehe oben)

Skriptbasierte Ereignisdokumentation – Microsoft-Teams

Übersicht Über Globale Skripts

NetApp VDS umfasst eine Bibliothek mit vordefinierten skriptbasierten Ereignissen, die direkt in VDS-Umgebungen verwendet und/oder dupliziert und als Bausteine für individuelle skriptbasierte Ereignisse verwendet werden können.

In diesem Artikel werden sowohl die Aktion *Install/Enable* als auch die *Deinstallation/Deaktivierung* behandelt.

Verwendung Von Globalen Skripten

Integrierte skriptbasierte Ereignisse wie diese sind bereits ausgefüllt. Wenn Sie das Kontrollkästchen „globaler“-Filter aktivieren, werden diese angezeigt.

Globale skriptbasierte Ereignisse wie diese sind schreibgeschützt. Sie können als ist verwendet werden oder über die Funktion „Klonen“ kann eine Kundenkopie für die Bearbeitung und Nutzung erstellt werden.

Die Schaltfläche Klonen befindet sich im Aktivitätsmenü auf der Seite „skriptbasierte Ereignisse“.

[Scriptbibliothek.Übersicht 2cb2] | [scriptlibrary.overview-2ccb2.png](#)

Microsoft Teams – Übersicht

Dieses Skript-Paket installiert/deinstalliert *Microsoft Teams* mit dem chocolatey-Paketmanager (<https://chocolatey.org/>) Um die Bereitstellung zu erledigen. Chocolatey wird von VDS bereitgestellt, wenn VMs erstellt werden. Dieses Skript prüft aber auch Chocolatey und installiert es als Voraussetzung, wenn es fehlt.



Diese Installation von Microsoft Teams wurde speziell für Implementierungen in einer RDS-Umgebung konfiguriert. "Ein anderes Skript für Microsoft-Teams" Wird für AVD-Bereitstellungen bereitgestellt.

Standardpfad für Verknüpfungen

Der standardmäßige Verknüpfungspfad wird unten eingegeben, für diese Anwendung ist die Verknüpfung:
\\shortcut\Microsoft Teams.lnk

Vorgang zur Installation/Deinstallation von Anwendungen hinzufügen

Damit ein Skript im Repository eine Aktion ausführen kann, muss ein Vorgang erstellt werden, um dieses Skript einem ausgewählten Trigger zuzuordnen. In diesem Beispiel wird diese Anwendung installiert/deinstalliert, wenn die App zum Arbeitsbereich hinzugefügt oder aus diesem entfernt wird (von der Seite *Workspace > Anwendungen* im VDS).

VDS skriptbasierte Ereignisse bieten viele andere Arten von Aktivitäts-Triggern wie *Create Server*, die als Alternative zum Ereignistyp *Application Install* (oder *Application Uninstall*) verwendet werden können. Mit *Create Server* würde diese App-Installation einfach auf alle neu erstellten VMs im VDS ausgeführt. *Create Server* und andere Trigger werden dokumentiert und können untersucht werden "[Hier](#)".



Diese Anwendung muss in der VDS-Anwendungsbibliothek vorhanden sein. Das "[Abschnitt](#)" Der Artikel über die Anwendungsberechtigung für RDS umfasst das Hinzufügen von Apps zur Bibliothek.

So erstellen Sie eine Aktivität und verknüpfen dieses Skript mit einer Aktion:

1. Navigieren Sie im VDS zum Abschnitt „*skriptbasierte Ereignisse*“
2. Klicken Sie unter „Aktivitäten“ auf + *Aktivität hinzufügen*
3. Geben Sie im geöffneten Dialogfeld die folgenden Informationen ein:
 - **Name:** Benennen Sie diese Aktivität
 - **Beschreibung:** Geben Sie optional eine Beschreibung ein
 - **Bereitstellung** Wählen Sie die gewünschte Bereitstellung aus der Dropdown-Liste aus
 - **Skript:** Wählen Sie das Skript install (oder uninstall) aus dem Dropdown-Menü aus. Dies könnte das

globale Skript oder Kundenskript sein, das Sie geklont und angepasst haben.

- **Argumente:** Legen Sie leer
- **Kontrollkästchen aktiviert:** Check Lieferumfang
- **Ereignistyp:** Wählen Sie Aus Application Install (Oder Application Uninstall) aus dem Dropdown-Menü
- **Anwendung:** Wählen Sie diese Anwendung aus der Dropdown-Liste aus
- **Verknüpfungspfad:** Geben Sie den Standard-Verknüpfungspfad für diese Anwendung ein (siehe oben)

Scripted Event Documentation – Microsoft-Teams für AVD

Übersicht Über Globale Skripts

NetApp VDS umfasst eine Bibliothek mit vordefinierten skriptbasierten Ereignissen, die direkt in VDS-Umgebungen verwendet und/oder dupliziert und als Bausteine für individuelle skriptbasierte Ereignisse verwendet werden können.

In diesem Artikel werden sowohl die Aktion Install/Enable als auch die Deinstallation/Deaktivierung behandelt.

Verwendung Von Globalen Skripten

Integrierte skriptbasierte Ereignisse wie diese sind bereits ausgefüllt. Wenn Sie das Kontrollkästchen „globaler“-Filter aktivieren, werden diese angezeigt.

Globale skriptbasierte Ereignisse wie diese sind schreibgeschützt. Sie können als ist verwendet werden oder über die Funktion „Klonen“ kann eine Kundenkopie für die Bearbeitung und Nutzung erstellt werden.

Die Schaltfläche Klonen befindet sich im Aktivitätsmenü auf der Seite „skriptbasierte Ereignisse“.

[Scriptbibliothek.Übersicht 2cb2] | [scriptlibrary.overview-2ccb2.png](#)

Microsoft-Teams für AVD-Übersicht

Dieses Skript-Paket installiert/deinstalliert *Microsoft Teams AVD* mit dem chocolatey-Paketmanager (<https://chocolatey.org/>) Um die Bereitstellung zu erledigen. Chocolatey wird von VDS bereitgestellt, wenn VMs erstellt werden. Dieses Skript prüft aber auch Chocolatey und installiert es als Voraussetzung, wenn es fehlt.



Diese Installation von Microsoft-Teams ist speziell für Implementierungen in einer AVD-Umgebung mit spezifischen Anpassungen und Komponenten für AVD in Azure konfiguriert. "[Ein anderes Skript für Microsoft-Teams](#)" Für RDS-Implementierungen verfügbar.

Standardpfad für Verknüpfungen

Der standardmäßige Verknüpfungspfad wird unten eingegeben, für diese Anwendung ist die Verknüpfung:
\\shortcut\Microsoft Teams AVD.lnk

Screenshot des Dialogfensters „Aktivität hinzufügen“

[Scriptbibliothek.script.InstallMicrosoftTeamsAVD] | [scriptlibrary.script.InstallMicrosoftTeamsAVD.png](#)

Vorgang zur Installation/Deinstallation von Anwendungen hinzufügen

Damit ein Skript im Repository eine Aktion ausführen kann, muss ein Vorgang erstellt werden, um dieses Skript einem ausgewählten Trigger zuzuordnen. In diesem Beispiel wird diese Anwendung installiert/deinstalliert, wenn die App zum Arbeitsbereich hinzugefügt oder aus diesem entfernt wird (von der Seite *Workspace > Anwendungen* im VDS).

VDS skriptbasierte Ereignisse bieten viele andere Arten von Aktivitäts-Triggern wie *Create Server*, die als Alternative zum Ereignistyp *Application Install* (oder *Application Uninstall*) verwendet werden können. Mit *Create Server* würde diese App-Installation einfach auf alle neu erstellten VMs im VDS ausgeführt. *Create Server* und andere Trigger werden dokumentiert und können untersucht werden "[Hier](#)".



Diese Anwendung muss in der VDS-Anwendungsbibliothek vorhanden sein. Das "[Abschnitt](#)" Der Artikel über die Anwendungsberechtigung für RDS umfasst das Hinzufügen von Apps zur Bibliothek.

So erstellen Sie eine Aktivität und verknüpfen dieses Skript mit einer Aktion:

1. Navigieren Sie im VDS zum Abschnitt „*skriptbasierte Ereignisse*“
2. Klicken Sie unter „Aktivitäten“ auf *+ Aktivität hinzufügen*
3. Geben Sie im geöffneten Dialogfeld die folgenden Informationen ein:
 - **Name:** Benennen Sie diese Aktivität
 - **Beschreibung:** Geben Sie optional eine Beschreibung ein
 - **Bereitstellung** Wählen Sie die gewünschte Bereitstellung aus der Dropdown-Liste aus
 - **Skript:** Wählen Sie das Skript *install* (oder *uninstall*) aus dem Dropdown-Menü aus. Dies könnte das globale Skript oder Kundenskript sein, das Sie geklont und angepasst haben.
 - **Argumente:** Legen Sie leer
 - **Kontrollkästchen aktiviert:** *Check Lieferumfang*
 - **Ereignistyp:** Wählen Sie *Aus Application Install* (Oder *Application Uninstall*) aus dem Dropdown-Menü
 - **Anwendung:** Wählen Sie diese Anwendung aus der Dropdown-Liste aus
 - **Verknüpfungspfad:** Geben Sie den Standard-Verknüpfungspfad für diese Anwendung ein (siehe oben)

Scripted Event Documentation - Nvidia Cuda Drivers

Übersicht Über Globale Skripts

NetApp VDS umfasst eine Bibliothek mit vordefinierten skriptbasierten Ereignissen, die direkt in VDS-Umgebungen verwendet und/oder dupliziert und als Bausteine für individuelle skriptbasierte Ereignisse verwendet werden können.

In diesem Artikel werden sowohl die Aktion *Install/Enable* als auch die *Deinstallation/Deaktivierung* behandelt.

Verwendung Von Globalen Skripten

Integrierte skriptbasierte Ereignisse wie diese sind bereits ausgefüllt. Wenn Sie das Kontrollkästchen „globaler“-Filter aktivieren, werden diese angezeigt.

Globale skriptbasierte Ereignisse wie diese sind schreibgeschützt. Sie können als ist verwendet werden oder

über die Funktion „Klonen“ kann eine Kundenkopie für die Bearbeitung und Nutzung erstellt werden.

Die Schaltfläche Klonen befindet sich im Aktivitätsmenü auf der Seite „skriptbasierte Ereignisse“.

[Scriptbibliothek.Übersicht 2cb2] | [scriptlibrary.overview-2ccb2.png](#)

NVIDIA-Cuda-Treiber – Übersicht

Dieses Skript-Paket installiert/deinstalliert *Nvidia Cuda Drivers* mit dem chocolatey-Paketmanager (<https://chocolatey.org/>) Um die Bereitstellung zu erledigen. Chocolatey wird von VDS bereitgestellt, wenn VMs erstellt werden. Dieses Skript prüft aber auch Chocolatey und installiert es als Voraussetzung, wenn es fehlt.

Screenshot des Dialogfensters „Aktivität hinzufügen“

[Scriptbibliothek.activity.InstallNvidiaCudaDrivers] | [scriptlibrary.activity.InstallNvidiaCudaDrivers.png](#)

Manuelle Aktivität hinzufügen

Damit ein Skript im Repository eine Aktion ausführen kann, muss ein Vorgang erstellt werden, um dieses Skript einem ausgewählten Trigger zuzuordnen. In diesem Beispiel wird die Aktivität ausgeführt, wenn der VDS Admin das Skript manuell auslöst.

VDS skriptbasierte Ereignisse bieten viele andere Arten von Aktivitäts-Triggern wie *Create Server*, die als Alternative zum Ereignistyp *Manual* verwendet werden können. Mit *Create Server* würde dieses Skript einfach auf allen neu erstellten VMs im VDS ausgeführt. *Create Server* und andere Trigger werden dokumentiert und können untersucht werden "[Hier](#)".

So erstellen Sie eine Aktivität und verknüpfen dieses Skript mit einer Aktion:

1. Navigieren Sie zum Abschnitt „skriptbasierte Ereignisse“ im VDS
2. Klicken Sie unter „Aktivitäten“ auf + *Aktivität hinzufügen*
3. Geben Sie im geöffneten Dialogfeld die folgenden Informationen ein:
 - **Name:** Benennen Sie diese Aktivität
 - **Beschreibung:** Geben Sie optional eine Beschreibung ein
 - **Bereitstellung** Wählen Sie die gewünschte Bereitstellung aus der Dropdown-Liste aus
 - **Skript:** Wählen Sie das Skript install (oder uninstall) aus dem Dropdown-Menü aus. Dies könnte das globale Skript oder Kundenskript sein, das Sie geklont und angepasst haben.
 - **Argumente:** Legen Sie leer
 - **Kontrollkästchen aktiviert:** Check Lieferumfang
 - **Ereignistyp:** Wählen Sie Aus *Manual* Aus der Dropdown-Liste
 - **Zieltyp:** Wählen Sie das aus *Servers* Optionsfeld
 - * **Verwaltete Server:** Check Die Box für jede VM, die diese Deinstallation erhalten soll.

Skriptbasierte Ereignisdokumentation – Nvidia-GRID-Treiber

Übersicht Über Globale Skripts

NetApp VDS umfasst eine Bibliothek mit vordefinierten skriptbasierten Ereignissen, die direkt in VDS-Umgebungen verwendet und/oder dupliziert und als Bausteine für individuelle skriptbasierte Ereignisse verwendet werden können.

In diesem Artikel werden sowohl die Aktion Install/Enable als auch die Deinstallation/Deaktivierung behandelt.

Verwendung Von Globalen Skripten

Integrierte skriptbasierte Ereignisse wie diese sind bereits ausgefüllt. Wenn Sie das Kontrollkästchen „globaler“-Filter aktivieren, werden diese angezeigt.

Globale skriptbasierte Ereignisse wie diese sind schreibgeschützt. Sie können als ist verwendet werden oder über die Funktion „Klonen“ kann eine Kundenkopie für die Bearbeitung und Nutzung erstellt werden.

Die Schaltfläche Klonen befindet sich im Aktivitätsmenü auf der Seite „skriptbasierte Ereignisse“.

[Scriptbibliothek.Übersicht 2cb2] | [scriptlibrary.overview-2ccb2.png](#)

Übersicht über NVIDIA GRID Treiber

Dieses Skript-Paket installiert/deinstalliert *Nvidia GRID Drivers* mithilfe des chocolatey-Paketmanagers (<https://chocolatey.org/>) Um die Bereitstellung zu erledigen. Chocolatey wird von VDS bereitgestellt, wenn VMs erstellt werden. Dieses Skript prüft aber auch Chocolatey und installiert es als Voraussetzung, wenn es fehlt.

Screenshot des Dialogfensters „Aktivität hinzufügen“

[Scriptbibliothek.activity.InstallNvidiaGridDrivers] | [scriptlibrary.activity.InstallNvidiaGridDrivers.png](#)

Manuelle Aktivität hinzufügen

Damit ein Skript im Repository eine Aktion ausführen kann, muss ein Vorgang erstellt werden, um dieses Skript einem ausgewählten Trigger zuzuordnen. In diesem Beispiel wird die Aktivität ausgeführt, wenn der VDS Admin das Skript manuell auslöst.

VDS skriptbasierte Ereignisse bieten viele andere Arten von Aktivitäts-Triggern wie *Create Server*, die als Alternative zum Ereignistyp *Manual* verwendet werden können. Mit *Create Server* würde dieses Skript einfach auf allen neu erstellten VMs im VDS ausgeführt. *Create Server* und andere Trigger werden dokumentiert und können untersucht werden "[Hier](#)".

So erstellen Sie eine Aktivität und verknüpfen dieses Skript mit einer Aktion:

1. Navigieren Sie zum Abschnitt „skriptbasierte Ereignisse“ im VDS
2. Klicken Sie unter „Aktivitäten“ auf + *Aktivität hinzufügen*
3. Geben Sie im geöffneten Dialogfeld die folgenden Informationen ein:
 - **Name:** Benennen Sie diese Aktivität
 - **Beschreibung:** Geben Sie optional eine Beschreibung ein
 - **Bereitstellung** Wählen Sie die gewünschte Bereitstellung aus der Dropdown-Liste aus
 - **Skript:** Wählen Sie das Skript install (oder uninstall) aus dem Dropdown-Menü aus. Dies könnte das globale Skript oder Kundenskript sein, das Sie geklont und angepasst haben.
 - **Argumente:** Legen Sie leer
 - **Kontrollkästchen aktiviert:** Check Lieferumfang
 - **Ereignistyp:** Wählen Sie Aus Manual Aus der Dropdown-Liste
 - **Zieltyp:** Wählen Sie das aus Servers Optionsfeld
 - * **Verwaltete Server:*** Check Die Box für jede VM, die diese Deinstallation erhalten soll.

Scripted Event Documentation – AVD-Bildschirmabscheider

Übersicht Über Globale Skripts

NetApp VDS umfasst eine Bibliothek mit vordefinierten skriptbasierten Ereignissen, die direkt in VDS-Umgebungen verwendet und/oder dupliziert und als Bausteine für individuelle skriptbasierte Ereignisse verwendet werden können.

In diesem Artikel werden sowohl die Aktion Install/Enable als auch die Deinstallation/Deaktivierung behandelt.

Verwendung Von Globalen Skripten

Integrierte skriptbasierte Ereignisse wie diese sind bereits ausgefüllt. Wenn Sie das Kontrollkästchen „globaler“-Filter aktivieren, werden diese angezeigt.

Globale skriptbasierte Ereignisse wie diese sind schreibgeschützt. Sie können als ist verwendet werden oder über die Funktion „Klonen“ kann eine Kundenkopie für die Bearbeitung und Nutzung erstellt werden.

Die Schaltfläche Klonen befindet sich im Aktivitätsmenü auf der Seite „skriptbasierte Ereignisse“.

[Scriptbibliothek.Übersicht 2cb2] | [scriptlibrary.overview-2ccb2.png](#)

AVD-Bildschirmenschutz – Übersicht

Dieses Skript-Paket aktiviert/deaktiviert die native AVD-Funktion *Screen Capture Protection*, indem Sie den (relevanten) Befehl mit PowerShell ausführen:

Aktivieren:

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v  
fEnableScreenCaptureProtection /t REG_DWORD /d 1
```

Deaktivieren:

```
reg delete "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v  
fEnableScreenCaptureProtection /f
```

Die Microsoft-Dokumentation zu dieser AVD-Funktion finden Sie hier:<https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide#session-host-security-best-practices>

Screenshot des Dialogfensters „Aktivität hinzufügen“

[Scriptbibliothek.AVDScreenCaptureProtection 216a6] | [scriptlibrary.AVDScreenCaptureProtection-216a6.png](#)

Manuelle Aktivität hinzufügen

Damit ein Skript im Repository eine Aktion ausführen kann, muss ein Vorgang erstellt werden, um dieses Skript einem ausgewählten Trigger zuzuordnen. In diesem Beispiel wird die Aktivität ausgeführt, wenn der VDS Admin das Skript manuell auslöst.

VDS skriptbasierte Ereignisse bieten viele andere Arten von Aktivitäts-Triggern wie *Create Server*, die als Alternative zum Ereignistyp *Manual* verwendet werden können. Mit *Create Server* würde dieses Skript einfach auf allen neu erstellten VMs im VDS ausgeführt. *Create Server* und andere Trigger werden dokumentiert und können untersucht werden "[Hier](#)".

So erstellen Sie eine Aktivität und verknüpfen dieses Skript mit einer Aktion:

1. Navigieren Sie zum Abschnitt „skriptbasierte Ereignisse“ im VDS
2. Klicken Sie unter „Aktivitäten“ auf **+ Aktivität hinzufügen**
3. Geben Sie im geöffneten Dialogfeld die folgenden Informationen ein:
 - **Name:** Benennen Sie diese Aktivität
 - **Beschreibung:** Geben Sie optional eine Beschreibung ein
 - **Bereitstellung** Wählen Sie die gewünschte Bereitstellung aus der Dropdown-Liste aus
 - **Skript:** Wählen Sie das Skript `install` (oder `uninstall`) aus dem Dropdown-Menü aus. Dies könnte das globale Skript oder Kundenscript sein, das Sie geklont und angepasst haben.
 - **Argumente:** Legen Sie leer
 - **Kontrollkästchen aktiviert:** `Check Lieferumfang`
 - **Ereignistyp:** Wählen Sie `Manual` aus der Dropdown-Liste
 - **Zieltyp:** Wählen Sie das aus `Servers` Optionsfeld
 - *** Verwaltete Server:** `Check` Die Box für jede VM, die diese Deinstallation erhalten soll.

Scripted Event Documentation - Zoom VDI AVD

Übersicht Über Globale Skripts

NetApp VDS umfasst eine Bibliothek mit vordefinierten skriptbasierten Ereignissen, die direkt in VDS-Umgebungen verwendet und/oder dupliziert und als Bausteine für individuelle skriptbasierte Ereignisse verwendet werden können.

In diesem Artikel werden sowohl die Aktion `Install/Enable` als auch die `Deinstallation/Deaktivierung` behandelt.

Verwendung Von Globalen Skripten

Integrierte skriptbasierte Ereignisse wie diese sind bereits ausgefüllt. Wenn Sie das Kontrollkästchen „globaler“-Filter aktivieren, werden diese angezeigt.

Globale skriptbasierte Ereignisse wie diese sind schreibgeschützt. Sie können als ist verwendet werden oder über die Funktion „Klonen“ kann eine Kundenkopie für die Bearbeitung und Nutzung erstellt werden.

Die Schaltfläche Klonen befindet sich im Aktivitätsmenü auf der Seite „skriptbasierte Ereignisse“.

[Scriptbibliothek.Übersicht 2cb2] | [scriptlibrary.overview-2ccb2.png](#)

Zoom für VDI/AVD-Übersicht

Dieses Skript-Paket installiert/deinstalliert *Zoom VDI-AVD* mit PowerShell für die Bereitstellung.



Die Zoomleistung wird verbessert, wenn die Audioumleitung auch für die VDI/AVD-Umgebung aktiviert ist.

Standardpfad für Verknüpfungen

Der standardmäßige Verknüpfungspfad wird unten eingegeben, für diese Anwendung ist die Verknüpfung:
`\\shortcuts\Zoom VDI.lnk`

Screenshot des Dialogfensters „Aktivität hinzufügen“

[Scriptbibliothek.activity.InstallZoomVDI AVD] | *scriptlibrary.activity.InstallZoomVDI-AVD.png*

Vorgang zur Installation/Deinstallation von Anwendungen hinzufügen

Damit ein Skript im Repository eine Aktion ausführen kann, muss ein Vorgang erstellt werden, um dieses Skript einem ausgewählten Trigger zuzuordnen. In diesem Beispiel wird diese Anwendung installiert/deinstalliert, wenn die App zum Arbeitsbereich hinzugefügt oder aus diesem entfernt wird (von der Seite *Workspace > Anwendungen* im VDS).

VDS skriptbasierte Ereignisse bieten viele andere Arten von Aktivitäts-Triggern wie *Create Server*, die als Alternative zum Ereignistyp *Application Install* (oder *Application Uninstall*) verwendet werden können. Mit *Create Server* würde diese App-Installation einfach auf alle neu erstellten VMs im VDS ausgeführt. *Create Server* und andere Trigger werden dokumentiert und können untersucht werden ["Hier"](#).



Diese Anwendung muss in der VDS-Anwendungsbibliothek vorhanden sein. Das ["Abschnitt"](#) Der Artikel über die Anwendungsberechtigung für RDS umfasst das Hinzufügen von Apps zur Bibliothek.

So erstellen Sie eine Aktivität und verknüpfen dieses Skript mit einer Aktion:

1. Navigieren Sie im VDS zum Abschnitt „*skriptbasierte Ereignisse*“
2. Klicken Sie unter „Aktivitäten“ auf **+ Aktivität hinzufügen**
3. Geben Sie im geöffneten Dialogfeld die folgenden Informationen ein:
 - **Name:** Benennen Sie diese Aktivität
 - **Beschreibung:** Geben Sie optional eine Beschreibung ein
 - **Bereitstellung** Wählen Sie die gewünschte Bereitstellung aus der Dropdown-Liste aus
 - **Skript:** Wählen Sie das Skript *install* (oder *uninstall*) aus dem Dropdown-Menü aus. Dies könnte das globale Skript oder Kundenscript sein, das Sie geklont und angepasst haben.
 - **Argumente:** Legen Sie leer
 - **Kontrollkästchen aktiviert:** *Check Lieferumfang*
 - **Ereignistyp:** Wählen Sie *Application Install* (Oder *Application Uninstall*) aus dem Dropdown-Menü
 - **Anwendung:** Wählen Sie diese Anwendung aus der Dropdown-Liste aus
 - **Verknüpfungspfad:** Geben Sie den Standard-Verknüpfungspfad für diese Anwendung ein (siehe oben)

Erweitert

FSLogix-Profil verkleinern

Überblick

VDS verfügt über einen integrierten Profilschrumpfbetrieb, der nachts läuft. Durch diese Automatisierung wird der FSLogix-Container eines Benutzerprofils automatisch verkleinert, wenn 5 GB oder mehr gespeichert werden können. Diese Automatisierung läuft nachts um 12:01 Uhr. Der 5-GB-Schwellenwert ist in DCConfig konfigurierbar, auf dem CWMGR1-Server gefunden.

NetApp VDS v5.4-Videos

VDS-Inhalte auf NetApp TV

VDS, GFC und ANF – die Lösung für weltweit eingesetzte Cloud-Desktops

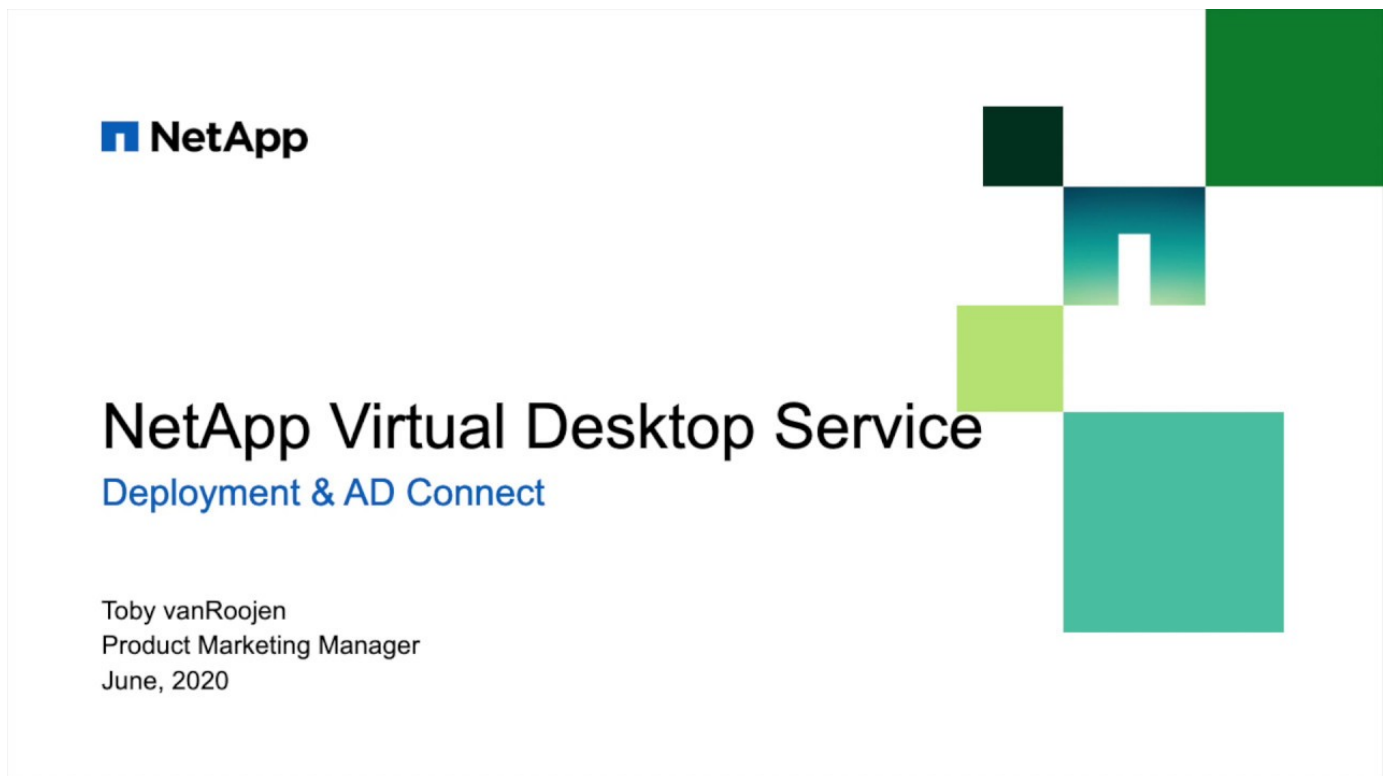
Azure NetApp Files hostet hochperformanten Storage, während Virtual Desktop Service und globaler Datei-Cache Sie Workspaces und Standortregionen über eine zentrale Konsole für Ihre global implementierten Cloud-Desktops managen.

[Link:<https://tv.netapp.com/detail/video/6182654694001>]

||||

Implementieren Sie AVD oder RDS in Azure mit NetApp VDS v5.4

Überblick



Erstellen Sie mit NetApp VDS v5.4 einen AVD Host-Pool

Überblick



NetApp Virtual Desktop Service

Creating WVD Host Pools

Toby vanRoojen
Product Marketing Manager
June, 2020

AVD-Benutzer und App-Gruppen in Azure mit NetApp VDS v5.4 hinzufügen und managen

Überblick



NetApp Virtual Desktop Service

Managing Users and App Groups

Toby vanRoojen
Product Marketing Manager
June, 2020

Optimieren Sie den Azure Ressourcenverbrauch in VDS 5.4

Überblick



NetApp Virtual Desktop Service

Cost Containment and Optimization

Toby vanRoojen
Product Marketing Manager
June, 2020

=

Tägliche Administration von RDS und AVD mit NetApp VDS v5.4

Überblick

 | <https://img.youtube.com/vi/uGEgA3hFdM4/maxresdefault.jpg>

Aktualisieren des AVD-Hostpools von v1 (Herbst 2019) auf v2 (Frühjahr 2020)

Überblick

In diesem Handbuch wird beschrieben, wie die VDS-Schnittstelle (Virtual Desktop Service) verwendet wird, um ein vorhandenes Upgrade eines vorhandenen AVD Fall Release (v1)-Hostpools durchzuführen, was zu einem AVD Spring Release (v2)-Hostpool führt. Ohne VDS sind für diese Umstellung geschulte Architekten erforderlich, um dies selbstständig zu ermitteln oder die Umgebung vollständig neu zu implementieren.

Voraussetzungen

In diesem Leitfaden wird vorausgesetzt, dass der Kunde folgende Leistungen hat:

- Mindestens ein Fall Release (v1) AVD-Host-Pool bereitgestellt

- V5.4 (oder höher) Bereitstellung von Virtual Desktop Services
- Alle VMs im Host-Pool müssen online sein und ausgeführt werden

Es ist erwähnenswert, dass der Virtual Desktop Service von NetApp vorhandene Host-Pools importieren kann, so dass Kunden VDS nutzen können, um Upgrades ohne VDS durchzuführen, auch wenn VDS nicht für die erste Bereitstellung des Host-Pools verwendet wurde.



Es empfiehlt sich, diese Aktion in einem festgelegten Wartungsfenster auszuführen, in dem Endbenutzer nicht aufgefordert werden, sich anzumelden (oder die VMs dürfen keine Benutzerverbindungen zulassen), da auf die Desktops des Endbenutzers während dieser Aktion nicht zugegriffen werden kann.

Prozessschritte

1. Navigieren Sie zum Workspaces-Modul und dann zur AVD-Registerkarte. Sie sehen dann den Abschnitt Host Pools, der jetzt eine Option zur Nutzung von VDS-Automatisierung zur Aktualisierung eines Host-Pools enthält.
2. Klicken Sie auf den Link Import V1 Host Pool, um den Host-Pool zu identifizieren, der auf V2 (AVD Spring Release) aktualisiert werden soll, um fortzufahren.



3. Wählen Sie dann im Dropdown-Menü den Host-Pool aus, zu dem Sie ein Upgrade durchführen möchten, und wählen Sie den Arbeitsbereich aus, dem Sie ihn zuweisen möchten. Klicken Sie dann auf die Schaltfläche Host-Pool importieren, um den automatischen Upgrade-Prozess zu starten. +[]
4. Wiederholen Sie diesen Vorgang für jeden Host-Pool, den Sie aktualisieren möchten. Nach Abschluss der Automatisierung sehen Sie den neu aktualisierten Spring Release (v2) Host-Pool auf der Registerkarte AVD von VDS.

Video-Demo



NetApp Virtual Desktop Service

Upgrading Spring (v1) WVD into Fall (v2)

Toby vanRoijen
Product Marketing Manager
September 2020



Bitte wenden Sie sich bei weiteren Fragen an Ihre Kundendienstmitarbeiter.

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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