Azure Virtual Desktop

Virtual Desktop Service

NetApp
February 20, 2023

Inhaltsverzeichnis

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-Containerierungstechnologie 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. Bestätigen Sie die Voraussetzungen für den Azure-Mandanten, das Azure-Abonnement und die Berechtigungen des Azure-Administratorkontos
2. Sammelt die erforderlichen Details zur Bestandsaufnahme
3. Erstellen Sie die Azure-Umgebung mit dem speziell entwickelten VDS für Azure Setup-Assistenten
4. Erstellen Sie den ersten Host-Pool mit einem standardmäßigen Windows 10-EVD-Image
5. Zuweisen von virtuellen Desktops zu Azure AD-Benutzern
6. Fügen Sie Benutzer zur Standard-App-Gruppe hinzu, um Benutzern die Desktop-Umgebung bereitzustellen. Optional Erstellen Sie zusätzliche Host-Pools für die Bereitstellung von RemoteApp-Services
7. Verbinden Sie sich als Endbenutzer über Client-Software und/oder Web-Client
8. Stellen Sie eine Verbindung zu den Plattform- und Client-Services als lokaler und Domain-Administrator her
9. <<Multi-Faktor-Authentifizierung (MFA),Optional können Sie die VDS-Multi-Faktor-Authentifizierung für VDS-Administratoren AVD-Endbenutzer aktivieren
10. Gehen Sie optional den gesamten Workflow für Anwendungsberechtigungen durch, einschließlich Befüllen der App-Bibliothek, Automatisierung von ApplikationInstallationen, Maskierung durch Benutzer und Sicherheitsgruppen
11. Optional können Sie Active Directory-Sicherheitsgruppen, Ordnerberechtigungen und Anwendungsberechtigungen nach Gruppe erstellen und verwalten.
12. Optional können Sie Technologien zur Kostenoptimierung wie Workload Scheduling und Live-Skalierung konfigurieren
13. Optional können Sie ein Virtual-Machine-Image für zukünftige Bereitstellungen erstellen, aktualisieren und Sysprep erstellen
14. Optionale Konfiguration von Azure Cloud Backup
15. 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 Abonnementeigentümer 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 Erstbereitstellung 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.
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.

Element	Beschreibung
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/azurenetappfiles

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 Automatisierungsapplikation 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, Anwendungsinstallationen 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 Abonnementeigentümer, 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-CWMGRAcess 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 nutzte 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 Fehlerbehebungszwecke 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-Infrastructure)** 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 Bereitstellungskonfiguration.
- *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-Infrastructure 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{Sequenzenumber}*** fest. Beispiel: XYZTS3. (Erfordert lokale AD-Berechtigungen (platziert in der Organisationsstruktur, die wir On-Prem erstellt haben (Remote-Desktop/unternehmencode/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-Netzwerkkonfiguration

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 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.

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 einen administrativen 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

Adresse	Ausgehender TCP-Port	Zweck	Service-Tag
*.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-Netzwerkkonfiguration

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 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.

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 einen administrativen 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
*.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