



Google

Virtual Desktop Service

NetApp

January 03, 2023

This PDF was generated from https://docs.netapp.com/de-de/virtual-desktop-service/Deploying.GCP.RDS.deploying_rds_in_gcp.html on January 03, 2023. Always check docs.netapp.com for the latest.

Inhaltsverzeichnis

- Google 1
 - RDS – Implementierungsleitfaden für Google Cloud (GCP) 1
 - Voraussetzungen für die Google Compute Platform (GCP) und VDS 11

RDS – Implementierungsleitfaden für Google Cloud (GCP)

Überblick

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

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

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

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

Implementierungsarchitektur

[Breite = 75 %]

RDS – Grundlagen

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

- RDS Gateway Server(en)
- Web-Client-Zugriffsserver
- Domänen-Controller-Server
- RDS-Lizenzservice
- ThinPrint Lizenzdienst
- FileZilla FTPS Server Service

Umfang des Leitfadens

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

Erstellen eines Servicekontos

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



2. KLIKEN SIE AUF + *SERVICEKONTO ERSTELLEN*



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



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



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



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



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



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



Google Compute-API aktivieren

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



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



Neue VDS-Implementierung erstellen

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

[]

2. Geben Sie einen Namen für die Bereitstellung ein

[]

3. Wählen Sie *Google Cloud Platform*

[]

Infrastrukturplattformen

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



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

[]

2. Klicken Sie nach der Bestätigung auf *Continue*

[]

Konten

Lokale VM-Konten

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



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

SMTP-Konto

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

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

[]

Level-3-Techniker

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

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



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



Domänen

Active Directory damit füllt

Geben Sie den gewünschten AD-Domänennamen ein.

Öffentliche Domäne

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



Virtual Machines

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

Konfiguration der Plattform-VM

Nur eine Virtual Machine

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

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

- Domain Controller

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



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

Mehrere Server

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

- Remote-Desktop-Gateway

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

- HTML5-Gateway

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



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

- Hinweise Zur Gateway-Skalierbarkeit

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

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

Servicrollen

- Cwmgr1

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

werden diese Services zu verschiedenen VMs verschoben.

- CWPortal1(2)

Das erste HTML5-Gateway heißt *CWPortal1*, die zweite ist *CWPortal2*. Ein oder zwei können bei der Implementierung erstellt werden. Zusätzliche Server können nach der Implementierung hinzugefügt werden, um die Kapazität zu steigern (~500 Verbindungen pro Server).

- CWRDSGateway1(2)

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

- Remote-App

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

- Domänen-Controller

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

□

Betriebssystem

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

Zeitzone

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

Zusätzliche Services

FTP

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

□

Netzwerk

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

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

VDS Setup erkennt und schlägt einen Bereich vor, der sich als erfolgreich erweisen sollte. Gemäß den Best

Practices müssen die Subnetz-IP-Adressen in einen privaten IP-Adressbereich fallen.

Diese Bereiche sind:

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

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

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

[]

Lizenzierung

SPLA

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

SPLA-Produkte

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

ThinPrint

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

[]

Prüfung und Bereitstellung

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

Nächste Schritte

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

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

von 1-2 Stunden abgeschlossen ist.

Erstellen Sie eine neue Bereitstellungsammlung

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

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

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



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



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

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



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



5. Wählen Sie optional die Anwendungen aus, die auf diesem Image installiert werden sollen.

- a. Die Liste der verfügbaren Anwendungen wird in der App-Bibliothek ausgefüllt, auf die Sie zugreifen können, indem Sie oben rechts auf der Seite „*Settings > App Catalog*“ auf das Menü „admin Name“ klicken.



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

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

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



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



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



[]

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

[]5

Neuen Arbeitsbereich erstellen

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

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

Client und Einstellungen

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

[]

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

[]

- a. Geben Sie die Firmendetails ein, und wählen Sie die Bereitstellung aus, in die dieser Arbeitsbereich bereitgestellt werden soll.
- b. **Datenlaufwerk:** Definieren Sie den Laufwerkbuchstaben, der für das Laufwerk verwendet werden soll.
- c. **User Home Drive:** Definieren Sie den Laufwerkbuchstaben, der für das zugeordnete Laufwerk des Einzelnen verwendet werden soll.
- d. **Zusätzliche Einstellungen**

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

- i. *Remote-App aktivieren:* die Remote-App stellt Anwendungen als Streaming-Anwendungen statt (oder zusätzlich zu), die eine vollständige Remote-Desktop-Sitzung präsentieren.
- ii. *App locker aktivieren:* VDS enthält die Anwendungsbereitstellung und die Berechtigungsfunktion. Standardmäßig werden die Anwendungen den Endbenutzern angezeigt bzw. ausgeblendet. Durch das Aktivieren von App locker wird der Zugriff auf Anwendungen über eine GPO-Safelliste durchgesetzt.
- iii. *Workspace Benutzerdatenspeicherung aktivieren:* Bestimmen Sie, ob Endbenutzer auf ihrem virtuellen Desktop auf den Storage zugreifen müssen. Bei RDS-Implementierungen sollte diese Einstellung immer aktiviert werden, um den Datenzugriff für Benutzerprofile zu ermöglichen.

- iv. *Druckerzugriff deaktivieren*: VDS kann den Zugriff auf lokale Drucker blockieren.
- v. *Zugriff auf Task Manager zulassen*: VDS kann den Endbenutzer-Zugriff auf den Task-Manager in Windows aktivieren/deaktivieren.
- vi. *Komplexes Benutzerpasswort benötigen*: komplexe Passwörter erfordern ermöglicht die systemeigenen Regeln für das Kennwort des Windows Servers. Außerdem wird die automatische zeitverzögerte Entsperrung gesperrter Benutzerkonten deaktiviert. Wenn diese Option aktiviert ist, ist ein Eingreifen des Administrators erforderlich, wenn Endbenutzer ihre Konten mit mehreren fehlgeschlagenen Kennwortversuchen sperren.
- vii. *MFA für alle Benutzer aktivieren*: VDS enthält einen kostenlosen E-Mail-/SMS-MFA-Dienst, der zum Schutz des Benutzerzugriffs und/oder des VDS-Administratorkontos verwendet werden kann. Wenn Sie diese Option aktivieren, müssen sich alle Endbenutzer in diesem Workspace mit MFA authentifizieren, um auf ihren Desktop und/oder ihre Anwendungen zuzugreifen.

Anwendungen auswählen

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

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

□

Benutzer Hinzufügen

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

□

Prüfung und Bereitstellung

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

□



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

Nächste Schritte

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

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

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

- ["Kostenoptimierung"](#)

Voraussetzungen für die Google Compute Platform (GCP) und VDS

GCP- und VDS-Anforderungen und -Hinweise

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

[Breite = 75 %]

Schnelle Checkliste

GCP-Anforderungen

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

Informationen vor der Implementierung

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

VDS-Bereitstellung – Detaillierte Anforderungen

Verbindungsanforderungen für Endbenutzer

Die folgenden Remote Desktop-Clients unterstützen RDS in GCP:

- ["NetApp VDS Client für Windows"](#)
 - NetApp VDS Client für Windows: URL-Safelisting-Anforderungen für ausgehende urls
 - `api.cloudworkspace.com`
 - `VdsClient.App`
 - `api.vdsclient.App`
 - `Bin.vdsclient.App`
 - Erweiterte Funktionen:
 - VDS Wake on demand

- ThinPrint Client und Läuse nsen
- Self-Service-Kennwort zurücksetzen
- Automatische Aushandlung von Server- und Gateway-Adressen
- Umfassende Unterstützung von Desktop- und Streaming-Applikationen
- Verfügbares benutzerdefiniertes Branding
- Installer-Switches für die automatische Bereitstellung und Konfiguration
- Integrierte Tools zur Fehlerbehebung
- "NetApp VDS Web-Client"
- "Microsoft RD-Client"
 - Windows
 - MacOS
 - ISO
 - Android
- Software von Drittanbietern und/oder Thin Clients
 - Anforderung: Unterstützen Sie die Konfiguration des RD-Gateways

Storage-Ebene

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

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

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

Netzwerkbetrieb

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

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

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

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

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

CKWMGR1

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

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

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

Entscheidungsbaum im Bereitstellungsassistenten

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

GCP-Region

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

Datenspeicher

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

- Cloud Volumes Service für GCP
- Herkömmlicher File Server

NetApp VDS Implementierungsanforderungen für vorhandene Komponenten

NetApp VDS-Implementierung mit vorhandenen Active Directory Domain Controllern

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

Diese Konfiguration erfordert:

- Ein vorhandener Active Directory-Domänen-Controller, auf den VMs im GCP-VPC-Netzwerk zugegriffen werden kann, normalerweise über einen VPN oder einen in GCP erstellten Domänen-Controller.

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

Identifikationsdaten und Werkzeug zur Vorbereitung der Domäne

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

NetApp VDS-Implementierung mit vorhandenem Filesystem

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

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

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

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

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

||| ||| ||| |||

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

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

Optimale Performance-Faktoren

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

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

Unterstützte BS-Images für Virtual Machines

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

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

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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