



Dokumentation Des Virtual Desktop Managed Services

Virtual Desktop Managed Service

NetApp
December 15, 2022

This PDF was generated from <https://docs.netapp.com/de-de/virtual-desktop-managed-service/index.html> on December 15, 2022. Always check docs.netapp.com for the latest.

Inhaltsverzeichnis

Dokumentation Des Virtual Desktop Managed Services	1
Überblick	1
Unterstützung erhalten	1
Windows Virtual Desktop (WVD)-Clients	1
Servicekomponenten	1
Erste Schritte	4
Voraussetzungen für Virtual Desktop Managed Service (VDMS)	4
Zusammenfassung des Virtual Desktop Managed Service (VDMS)	5
Lernprogramme	8
Installieren von Anwendungen auf der virtuellen Maschine(en) des Sitzungshosts	8
Aktualisieren und Implementieren von VM Images	10
Zuweisen von Benutzern zu Anwendungsgruppen	12
Generieren Sie die Anmeldeinformationen für Domänenadministratoranmeldeinformationen in VDMS. . . .	13
Benutzerzugriff Wird Hinzugefügt	15
Benutzerzugriff Wird Entfernt	20
Hinzufügen und Entfernen von Administratoren in VDMS	22
Häufig gestellte FRAGEN ZU VDMS	24
VDS-Administratorberechtigungen	24

Dokumentation Des Virtual Desktop Managed Services

Überblick

Die Virtual Desktop Managed Service (VDMS) von NetApp löst die Komplexität bei der Bereitstellung und dem Management von Virtual Desktops in der Public Cloud, die als Managed VDI as a Service-Plattform bereitgestellt werden.

Unterstützung erhalten

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

Telefon-Support: 844.645.6789

["VDMS Support-Portal"](#)

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

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

Windows Virtual Desktop (WVD)-Clients

- ["Microsoft WVD für Windows-Client"](#)
- ["Microsoft WVD Web-Client"](#)
- ["Microsoft WVD für Android-Client"](#)
- ["Microsoft WVD für macOS-Client"](#)
- ["Microsoft WVD für iOS-Client"](#)

Servicekomponenten

VDMS sind ein Co-Managed-Services-Angebot, das mehrere Technologien von NetApp und Microsoft vereint und Best Practices aus mehr als 20 Jahren auf dem EUC-Markt anwendet. Unter einer ausgewählten Komponentenliste werden die Komponenten aufgeführt. Aufgrund unterschiedlicher Kundenanforderungen werden in allen Implementierungen nicht alle Komponenten verwendet.

NetApp

- ["Azure NetApp Dateien \(ANF\)"](#)
 - Die Daten-Storage-Ebene für Implementierungen mit mehr als 49 Anwendern basiert auf ANF.
 - Bei Implementierungen mit <250 Benutzern wird die Standard-Performance-Tier verwendet.
 - Für Implementierungen mit >249 Benutzern wird die Premium Performance Tier verwendet.
- ["NetApp Cloud Backup"](#)
 - NetApp Cloud Backup dient zum Backup von ANF Storage Volumes.
- ["NetApp Cloud Sync"](#)

- Mit NetApp Cloud Sync können Daten zu VDMS migriert werden, wenn ANF die Storage-Layer-Technologie ist.
- **"NetApp Cloud Insights"**
 - NetApp Cloud Insights wird von unserem Support- und Service-Team für das Performance-Monitoring verwendet.
- **"Unterstützung VON NetApp VDMS"**
 - VDMS umfassen Support bei 24/7-Vorfällen und Onboarding-Services eines spezialisierten Support-Teams von NetApp

Microsoft

- **"Azure Files (AF)"**
 - Die Daten-Storage-Ebene für Implementierungen mit weniger als 50 Anwendern basiert auf AF-Technologie. Wir konfigurieren die „transaktionsoptimierte“ Tier in einem GPV2-Speicherkonto.
 - Für Bereitstellungen mit >49 Benutzern wird ANF verwendet.
- **"Azure Cloud Backup"**
 - Azure Cloud Backup dient zur Sicherung von AF Storage Volumes und Virtual Machines.
- **"Azure File Sync"**
 - Mit Azure File Sync können Daten zu VDMS migriert werden, wenn AF die Technologie auf Storage-Ebene ist.
- **"Azure Defender"**
 - VDMS aktivieren (und beinhalten Lizenzierung) Azure Defender, einen erweiterten Sicherheitsdienst auf allen virtuellen Maschinen in der Umgebung. Das Management und die Administration erfolgen über das Azure Security Center durch den Kunden und/oder seinen IT-Service-Provider. Das Verwalten von Azure Security Center ist kein Service in VDMS.
- **"Azure Virtual Machines"**
 - VDMS basieren stark auf Windows-basierten Azure Virtual Machines zum Hosten von Benutzersitzungen und Kundenapplikationen.
- **"Azure Virtual Network Peering"**
 - VDMS können das virtuelle Netzwerk-Peering von Azure nutzen, um sich in den vorhandenen Active Directory Domain Controller (AD DC) des Kunden zu integrieren.
- **"Azure VPN"**
 - VDMS können Azure Site-to-Site VPN nutzen, um sich in den vorhandenen Active Directory Domain Controller (AD DC) des Kunden zu integrieren.
- **"Windows Virtual Desktop (WVD)"**
 - VDMS nutzen die native WVD-Funktionalität zur Unterstützung der Vermittlung von Benutzersitzungen, Authentifizierung, Windows-Lizenzierung und mehr.
- **"Azure AD Connect"**
 - Für WVD müssen die lokale Domäne (AD DC) und Azure AD über die Azure AD Connect Applikation synchron sein.
- **"Microsoft 365 (M365)"**
 - WVD-Benutzersitzungen und Windows 10 Enterprise für die Sitzungshosts werden über bestimmte M365-Lizenztypen dem Benutzer lizenziert. Die Zuweisung der entsprechenden M365-Lizenzierung für

alle VDMS ist eine WVD- und VDMS-Anforderung. Diese Lizenzierung ist nicht in VDMS enthalten. Es liegt in der Verantwortung des Kunden und/oder seines IT-Serviceanbieters, die M365-Lizenzen zu verwalten.

Erste Schritte

Voraussetzungen für Virtual Desktop Managed Service (VDMS)

M365-Lizenzierung

VDMS werden mit Microsoft Windows Virtual Desktop (WVD)-Technologie erstellt. Gemäß den WVD-Voraussetzungen müssen den Endbenutzern spezifische Microsoft 365 (M365)-Lizenzen zugewiesen werden. Diese Lizenzierung ist nicht im VDMS-Abonnement enthalten. NetApp verkauft diese Lizenz nicht oder bietet sie anderweitig an.

Die Verantwortung für die Einhaltung der M365-/WVD-Lizenzierung bleibt bei dem Kundenunternehmen, Partnerunternehmen und/oder dem jeweiligen M365-Anbieter.

Es gibt eine Vielzahl von M365-Plänen, die die WVD-Lizenzierung für VDMS unterstützen. Details können sein "[Gefunden hier](#)".

M365/Azure AD-Mandant

Der Kunde muss über einen vorhandenen Azure AD Mandanten verfügen. Microsoft 365 basiert auf derselben Azure AD-Mandantenstruktur, daher erfüllt die M365-Lizenzierungsanforderungen (oben) auch diese Anforderung.

CSP-Reseller-Beziehung

NetApp implementiert VDMS über unsere CSP-Partnerschaft mit Microsoft in einem dedizierten Azure-Abonnement. Um dieses Abonnement zu implementieren, muss NetApp eine Reseller-Beziehung mit dem Azure AD-Mandanten des Kunden einrichten. Ein globaler Administrator für den Azure AD Mandanten des Kunden kann diese Beziehung hier akzeptieren:

<https://admin.microsoft.com/Adminportal/Home?invType=ResellerRelationship&partnerId=47c1f6d2-b112-48e0-915f-4304efffb3e8&msspId=0&DAP=true#/BillingAccounts/partner-invitation>

Multi-Partner-Funktionen nicht:

- Ändern Sie die vorhandenen Abonnements des Kunden
- Die bestehenden Abonnements oder Kontoeigentümer des Kunden wechseln
- Ändern Sie die Bedingungen oder die Verpflichtungen des Kunden für eine der bestehenden Abonnements
- Ändern Sie den Partner des Datensatzes für ein Abonnement
- Weitere Einzelheiten dazu: <https://docs.microsoft.com/en-us/partner-center/multipartner>

Delegierte Administratorrechte

Der Link „Einladung“ (oben) beinhaltet eine Anfrage für delegierte Administratorberechtigungen. Mit der Akzeptanz werden die Rollen des NetApp Global Admin und Helpdesk Administrators im Azure AD-Mandanten des Kunden zugewiesen.

Umfang Des Virtuellen Netzwerks

VDMS werden in einem virtuellen Netzwerk in Azure bereitgestellt. Der für dieses Netzwerk verwendete /20-IP-Bereich kann sich nicht mit anderen Netzwerken in ihrer Umgebung überschneiden.

In jedem Szenario, in dem eine Netzwerkverbindung zwischen dem virtuellen VDMS-Netzwerk und anderen Kundennetzwerken hinzugefügt wird, wird die Überschneidung mit einem anderen Netzwerk-IP-Bereich VDMS unterbrochen. Daher ist es wichtig, dass VDMS einen völlig unbenutzten /20-Bereich verwenden.

Der Umfang des /20-Netzwerks muss in einem dieser IP-Bereiche landen:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

VDMS-Arbeitsblatt bereitstellen

Der Kunde/Partner muss das Arbeitsblatt zum Bereitstellen VON VDMS unter folgender Adresse ausfüllen: <https://www.deployvdms.com/>

Vorhandene AD-Integration

Die Integration VON VDMS in einen vorhandenen Active Directory Domain Controller (AD DC) erfordert mehrere zusätzliche Voraussetzungen:

Anmeldeinformationen Für Lokale Domänenadministration

Ein lokales Domain-Administratorkonto mit Domainjoin-Rechten, auf der bestehenden Domain ist erforderlich, um die Integration zu etablieren.

Azure AD Connect

WVD erfordert, dass Azure AD mithilfe von AD Connect mit dem AD DC synchronisiert wird. Wenn dies nicht bereits eingerichtet ist, wird dies angezeigt "Utility" Muss auf Ihrem AD DC installiert und konfiguriert sein.

/===== Network Contributor Role for vnet Peering /===== Local Gateway Device Admin Rights to Setup VPN
/===== DNS Zones (Need more Tech info) /===== no multi-Domain forrest, users must be in the Domain we are Deploying to

Zusammenfassung des Virtual Desktop Managed Service (VDMS)

Zuweisung Von Benutzerressourcen



Dieser Artikel soll die technischen Details des VDMS genau beschreiben. Service-Details können sich ändern. Dieser Artikel stellt keine Änderung oder Änderung vorhandener Vereinbarungen, Verträge oder anderer Vereinbarungen zwischen NetApp und Kunden oder Partnern dar.

Freigegebene Benutzer (SKU: VDMS-SUBS-SHARED-USER)

Gemeinsame Benutzersitzungen werden auf einer virtuellen Session-Host-Maschine (SHVM) mit bis zu 10 Benutzersitzungen ausgeführt. Die Gesamtzahl der zugewiesenen gemeinsam genutzten SHVMs garantiert mindestens einen gemeinsam genutzten SHVM für alle 10 freigegebenen Benutzer in der Umgebung.

Ressourcen, die pro freigegebenen Benutzer zugewiesen sind:

- 8/10ths eines vCPU-Kerns
- 6.4 gib RAM
- 25 gib Storage

Shared SHVM Technische Daten:

- In der Regel aus dem "Esv3", "Eav4" Und "Easyv4" Familien von Azure Virtual Machines
- 128 gib Standard-SSD-BS-Festplatte
- Windows 10 Enterprise für Virtual Desktop
- FSLogix-Benutzerprofil für angehängte Container
- Attached Storage für Unternehmensanteil

VDI-BENUTZER (SKU: VDMS-SUBS-VDI-USER)

Die Session eines VDI-Benutzers wird auf einer dedizierten Session Host Virtual Machine (SHVM) ausgeführt, die keine anderen Benutzersitzungen hostet. Die Gesamtzahl an VDI SHVMs entspricht der Gesamtzahl an VDI-Nutzern in der Umgebung.

Zugewiesene Ressourcen pro VDI-Benutzer:

- 2 vCPU-Kerne
- 8 gib RAM
- 25 gib Storage

VDI SHVM Technische Details:

- In der Regel aus dem "Dsv3", "Davor 4" Und "Dasv4" Familien von Azure Virtual Machines
- 128 gib Standard-HDD-BS-Festplatte
- Windows 10 Enterprise für Virtual Desktop
- FSLogix-Benutzerprofil für angehängte Container
- Attached Storage für Unternehmensanteil

GPU-BENUTZER (SKU: VDMS-SUBS-GPU-USER)

Die Session eines GPU-Benutzers wird auf einer dedizierten Session-Host Virtual Machine (SHVM) ausgeführt, die keine anderen Benutzersitzungen hostet. Die Gesamtzahl der GPU-SHVMs entspricht der Gesamtzahl der GPU-Benutzer in der Umgebung.

Zugewiesene Ressourcen pro GPU-Benutzer:

- 8 gib GPU-RAM

- 25 gib Storage

GPU SHVM Technische Details:

- In der Regel aus dem "NVv3" Und "NVv4" Familien von Azure Virtual Machines
- 128 gib Standard-HDD-BS-Festplatte
- Windows 10 Enterprise für Virtual Desktop
- FSLogix-Benutzerprofil für angehängte Container
- Attached Storage für Unternehmensanteil

Andere VDMS SKUs

Business Server (SKU: VDMS-AZURE-BUSINESS-VM)

Der Business Server kann einer Umgebung hinzugefügt werden, um Anwendungen und Services zu unterstützen.

Jeder Business Server VM wird mindestens zugewiesen:

- 8 vCPUs
- 64 gib RAM
- 128 gib Standard-SSD-BS-Festplatte
- Windows Server 2012R2/2016/2019
- In der Regel aus dem "Esv3", "Eav4" Und "Easyv4" Familien von Azure Virtual Machines

Zusätzlicher Storage (SKU: VDMS-1 TB-STORAGE-HPRSCLR)

Datenspeicherebene ist der primäre Storage-Mechanismus für die VDMS-Umgebung und läuft entweder auf Azure Dateien oder Azure NetApp Files (ANF). Die verwendete Speichertechnologie wird von den insgesamt gekauften VDMS bestimmt. Zusätzliche Kapazität kann in Schritten von 1 tib hinzugefügt werden.

Benutzerprofile, Benutzerdaten, Unternehmensfreigaben, Applikationsdaten und Datenbanken sollten von diesem Storage Service ausgeführt werden. Es empfiehlt sich, möglichst keine Daten auf VM-Festplatten zu speichern.

Die Kapazität entspricht der Summe der Benutzerzuweisung (25 gib/Benutzer) und des erworbenen zusätzlichen TIBs Storage.

Metrisch	"Azure Files GPV2"	"ANF Standard"	"ANF Premium"
Benutzeranzahl	10-49	50-249	250 und höher
Mindestgröße	250 gib	4 tib	4 tib
IOPS	Bis zu 1,000	Bis zu 250 tib	Bis zu 1,000 tib

Lernprogramme

Installieren von Anwendungen auf der virtuellen Maschine(en) des Sitzungshosts

Methodik Der Applikationsbereitstellung

Benutzer können auf alle Anwendungen zugreifen, die auf der virtuellen Session-Host-Maschine (SHVM) installiert sind, auf der ihre Benutzersitzung ausgeführt wird.

Benutzer werden einem Pool von SHVMs („Host Pool“) basierend auf ihrer Mitgliedschaft in einer Benutzergruppe zugewiesen. Jeder SHVM in diesem Host-Pool basiert auf dem gleichen VM Image, hat dieselben Anwendungen und läuft auf den gleichen VM-Ressourcen. Bei jeder Verbindung eines Benutzers werden sie dem SHVM in seinem Host-Pool mit den wenigsten aktuellen Benutzersitzungen zugewiesen.

Durch Hinzufügen oder Entfernen von Anwendungen aus jedem SHVM im Hostpool kann der VDMS-Administrator kontrollieren, auf welche Anwendungen VDMS Benutzer zugreifen können.

Das Hinzufügen (oder Entfernen) von Anwendungen aus jedem SHVM kann direkt auf jedem SHVM-Image oder zu einem einzelnen VM-Image durchgeführt werden, das wiederum auf allen SHVMs im Host-Pool eingesetzt werden kann.

Dieser Artikel behandelt die direkte Installation von Anwendungen auf den SHVMs. VM-Image-Management ist in abgedeckt ["Diesen Artikel"](#).

Manueller Zugriff

Das VDMS-Managementportal ermöglicht den direkten Zugriff auf jede VM über ein lokales „Just-in-Time“-Administratorkonto für alle SHVMs und Business Server. Über diesen Zugriff kann eine manuelle Verbindung zu jeder VM hergestellt werden, um Applikationen manuell zu installieren und andere Konfigurationsänderungen vorzunehmen.

Diese Funktion finden Sie unter Workspace > Server > Aktionen > Verbinden

Virtual Desktop Service
Version: 6.0
Environment: production

- Home
- Organizations
- Deployments
- Workspaces
- Service Board
- Scripted Events
- Admins
- Reports
- Applications
- Cost Estimator
- SaaS Backup

Customer

[Home](#) > [Workspaces](#) > [NetApp VDMS](#) > [Servers](#)

NetApp VDMS

Workspace

[Overview](#)
[Users & Groups](#)
[Workload Schedule](#)
[WVD](#)
[Servers](#)

[Refresh](#)
[Edit](#)

Servers

Filter By

[Export](#)
[Refresh](#)

Name	Type	Machine Size	RAM	CPU	Online	Status	Actions
JZSXTSD1	TSDData	Standard_B2s	4 RAM	2 CPU	Online	Available	⋮
JZSXTS1	TS	Standard_D2s_v4	8 RAM	2 CPU	Online	Available	Backup Reboot Connect Stop
JZSXTS2	TS	Standard_D2s_v4	8 RAM	2 CPU	Online	Available	

[Previous](#)
Page 1 of 1
[Next](#)

Wenn Anmeldedaten für den Domänenadministrator erforderlich sind, werden mit DER PAM-Funktion (Privileged Access Management) VDMS Anmeldedaten für den Domänenadministrator generiert. Angaben können sein "Gefunden hier".

VDMS Automation

Im VDMS-Portal enthält der Abschnitt „skriptbasierte Ereignisse“ Funktionen zur Remote-Ausführung von Code.

Die Registerkarte „Repository“ enthält unter „skriptbasierte Ereignisse“ globale Skripte, die von NetApp veröffentlicht werden. Benutzerdefinierte Skripts können über die Schaltfläche „+ Skript hinzufügen“ hinzugefügt werden.

Auf der Registerkarte „Vorgänge“ finden Sie unter „skriptbasierte Ereignisse“ den Auslöser, der dazu führt, dass ein Skript für eine Reihe von VMs ausgeführt wird. FÜR VDMS sollten die Ereignistypen „manuell“ und „geplant“ am besten ein Skript über die entsprechenden virtuellen Maschinen übertragen werden.



Für Aktivitäten gibt es viele Trigger, die als „Ereignistypen“ bezeichnet werden. Für VDMS gelten die Typen „Application Install“ und „Application Uninstall“ nicht. Dies sind RDS-spezifische Auslöser und sollten für VDMS nicht verwendet werden, da VDMS ein WVD-basierter Service ist und der Designarchitektur von RDS entsprechen.

Weitere Automatisierungstools

Virtuelle Maschinen in VDMS können mit Management Tools von Drittanbietern verwaltet werden. Applikationsänderungen und andere VM-Konfigurationsänderungen können über alle kompatiblen Tools umgesetzt werden.

Aktualisieren und Implementieren von VM Images

Methodik Der Applikationsbereitstellung

Benutzer können auf alle Anwendungen zugreifen, die auf der virtuellen Session-Host-Maschine (SHVM) installiert sind, auf der ihre Benutzersitzung ausgeführt wird.

Benutzer werden einem Pool von SHVMs („Host Pool“) basierend auf ihrer Mitgliedschaft in einer Benutzergruppe zugewiesen. Jeder SHVM in diesem Host-Pool basiert auf dem gleichen VM Image, hat dieselben Anwendungen und läuft auf den gleichen VM-Ressourcen. Bei jeder Verbindung eines Benutzers werden sie dem SHVM in seinem Host-Pool mit den wenigsten aktuellen Benutzersitzungen zugewiesen.

Durch Hinzufügen oder Entfernen von Anwendungen aus jedem SHVM im Hostpool kann der VDMS-Administrator kontrollieren, auf welche Anwendungen VDMS Benutzer zugreifen können.

Das Hinzufügen (oder Entfernen) von Anwendungen aus jedem SHVM kann direkt auf jedem SHVM-Image oder zu einem einzelnen VM-Image durchgeführt werden, das wiederum auf allen SHVMs im Host-Pool eingesetzt werden kann.

Dieser Artikel befasst sich mit VM Image Management. Die direkte Installation von Anwendungen auf den SHVMs wird in abgedeckt ["Diesen Artikel"](#).

Das VM-Image wird aktualisiert

Die empfohlene Methode zum Hinzufügen (oder Entfernen) von Anwendungen zu SHVM(s) ist, indem das VM-Image bearbeitet wird, das dem Host-Pool zugewiesen ist. Sobald das VM-Image angepasst und validiert wurde, kann das VDMS Support-Team es auf Anfrage für alle SHVMs im Host Pool bereitstellen.

So bearbeiten Sie das VM Image

1. Navigieren Sie in der Bereitstellung im VDS-Portal zu „Provisioning Collections“
2. Klicken Sie auf die Provisioning-Sammlung, die dem Host-Pool zugeordnet ist, den Sie aktualisieren möchten.

Name	Type	Operating System	Servers	Apps	Min. Cache	Current Cache	Status	Actions
Shared users	VDI		1	0	0	0	Available	
VDI Users	VDI		1	0	0	0	Pending	

- a. Notieren Sie sich den Namen der VM-Vorlage im Abschnitt „Server“.

Servers				
Filter By <input type="text" value="Keyword"/>				
Name	Role	VM Template	Storage Type	Actions
	TS	sharedusers4044ver3	Standard_LRS	⋮

Servers

Template	Storage Type	Actions
sharedusers4044ver3	Standard_LRS	⋮
		<div>  Edit </div> <div>  Delete </div>
Previous Page 1 of 1 Next		

3. Bearbeiten Sie die Server-Vorlage und stellen Sie sicher, dass es sich bei der Quellvorlage um die in Schritt 2.a angegebenen VM-Vorlage handelt. Oben. Klicken Sie Auf „Weiter“.

Edit Server

VM Template Required

Storage Type Required

☐ Data Drive

Cancel

Continue



Diese Einstellungen können nicht bearbeitet werden: 1. Typ = VDI 2. Share Drive = leer 3. Mindestcache = 0 4. Datenlaufwerk = Deaktiviert 5. Speichertyp = Standard_LRS

1. Die VDMS-Automatisierung baut jetzt eine temporäre VM in Azure auf, der Maschinenname lautet CWT#. Eine Erstellung dieser VM kann 25 Minuten dauern. Nach Abschluss des Vorgangs ändert sich der Status

in „Ausstehend“.

- a. Beachten Sie: Diese VM wird bis zum Abschluss des Anpassungsprozesses ausgeführt. Daher ist es wichtig, die VM innerhalb eines oder zwei Tages zu erstellen, anzupassen und zu validieren.
2. Sobald die temporäre VM bereit ist, können Sie sich bei der VM anmelden, indem Sie die Bereitstellungssammlung bearbeiten und dann auf dem Server auf „Verbinden“ klicken.
 - a. Wenn Sie zur Eingabe der Zugangsdaten aufgefordert werden, können die Anmeldeinformationen für den Domänenadministrator von jedem VDMS-Administrator mit „PAM Approver“-Rechten generiert werden.

So stellen Sie ein aktualisiertes VM-Image bereit

1. Wenn das VM-Image validiert wurde, wenden Sie sich an das VDMS-Support-Team, um eine Image-Aktualisierung zu planen.
2. Das Team wird neue Sitzungshosts basierend auf dem neuen Image erstellen.
 - a. Falls erforderlich, koordinieren Sie bitte die Zeit zum Testen der neuen Hosts, bevor wir neue Benutzer zu den neuen Hosts weiterleiten.
3. Sobald das Support-Team fertig ist, werden alle neuen Benutzersitzungen zu den neuen Hosts weitergeleitet. Wir schalten die alten Hosts aus, sobald keine Benutzer verbunden sind. Diese alten VMs befinden sich im Status „dezugewiesen“ für ein „warmes Failover“, doch werden diese VMs nach 7 Tagen automatisch gelöscht.

Ändern der SHVM(s) direkt

Änderungen können direkt auf den SHVM(s) manuell oder über alle verfügbaren Automatisierungstools vorgenommen werden. Weitere Informationen dazu finden Sie in ["Diesen Artikel"](#).

Wenn Sie Änderungen direkt an den SHVMs in einem Host-Pool vornehmen, ist es wichtig, dass jeder SHVM auf die gleiche Weise konfiguriert bleibt, oder dass die Benutzer bei der Verbindung mit verschiedenen SHVMs inkonsistente Erfahrungen haben.



Standardmäßig werden einzelne SHVMs nicht gesichert, da sie in der Regel keine eindeutigen Daten haben und auf einem standardisierten VM Image basieren. Wenn Sie Änderungen direkt an den SHVMs vornehmen, wenden Sie sich an den Support, um eine Backup-Richtlinie auf eine der SHVMs im Host-Pool anzuwenden.

Sysprep-Fehlerbehebung

Die FUNKTION „Validieren“ DES VDMS-Images verwendet das Dienstprogramm Sysprep von Microsoft. Wenn die Validierung fehlschlägt, ist die häufigste Ursache ein Sysprep-Fehler. Um Fehler zu beheben, starten Sie in der Sysprep-Protokolldatei auf der CWT# VM im Pfad: C:\Windows\system32\Sysprep\Panther\setupact.log

Zuweisen von Benutzern zu Anwendungsgruppen

Methode Der Benutzerzuweisung

Benutzer werden über AD-Sicherheitsgruppen einer virtuellen Session-Host-Maschine (SHVM) zugewiesen.

Für jeden Host-Pool gibt es eine verknüpfte Benutzergruppe auf der Registerkarte „Benutzer & Gruppen“ im Arbeitsbereich.

Benutzergruppen werden mit der Workspace-ID (ein eindeutiger 3-4-stelliger Code für jeden Arbeitsbereich)

benannt, gefolgt vom Namen des Host-Pools.

Zum Beispiel ist die Gruppe „jzxx freigegebene Benutzer“ mit dem Host-Pool für freigegebene Benutzer in VDMS verknüpft. Alle Benutzer, die „jzxx freigegebene Benutzer“ hinzugefügt wurden, werden den Sitzungshosts im Host-Pool „freigegebene Benutzer“ Zugriff zugewiesen.

Um einen Benutzer seinem Host-Pool zuzuweisen

1. Navigieren Sie im Arbeitsbereich zu „Benutzer & Gruppen“
2. Benutzer können der Gruppe hinzugefügt werden, indem Sie die Benutzerliste innerhalb der Gruppe bearbeiten.
3. Die Automatisierung synchronisiert automatisch die Mitglieder der Benutzergruppe, so dass dem Benutzer der Zugriff auf den entsprechenden Host-Pool, die App-Gruppe und die Anwendungen gewährt wird.



Benutzer sollten nur einer (und nur einer) App-Gruppe zugewiesen werden. Der Typ des Host-Pools (Shared, VDI oder GPU) muss mit den lizenzierten SKUs übereinstimmen, die für VDMS erworben wurden. Eine falsche Ausrichtung von Benutzern und/oder eine Zuweisung zu mehreren Applikationsgruppen kann zu Ressourcenkonflikten führen und deren Kollegen in der Umgebung möglicherweise beeinträchtigen.

Generieren Sie die Anmeldeinformationen für Domänenadministratoranmeldeinformationen in VDMS

Management Von Privilegierten Zugriffsberechtigungen

VDMS Administratoren können die Funktion „PAM Approver“ erhalten, mit der der Administrator PAM-Anfragen erteilen kann.

PAM-Anfragen generieren ein Administratorkonto auf Domänenebene, das zur Authentifizierung in VDMS VMs verwendet wird, wenn die Just-in-Time-Anmeldedaten der lokalen Administratoren nicht ausreichen.

Jeder VDMS-Administrator kann eine PAM-Anfrage einreichen, aber nur Administratoren mit der Rolle „PAM Approver“ können die Anforderungen genehmigen. Ein PAM Approver kann seinen eigenen Antrag anfordern und genehmigen.

Senden Sie eine PAM-Anfrage

Um eine PAM-Anfrage einzureichen

1. Navigieren Sie oben rechts zu Ihrem Admin-Benutzernamen und klicken Sie auf „Einstellungen“.
2. Wählen Sie die Registerkarte „PAM Requests“ aus
3. Klicken Sie Auf „+ Hinzufügen“.
 - a. Wählen Sie eine Dauer aus, nach der diese Anmeldedaten verfallen
 - b. Wählen Sie die Implementierung aus
 - c. Geben Sie eine E-Mail-Adresse ein, die die Anmeldeinformationen eingegeben werden können. Dies kann eine beliebige E-Mail-Adresse sein, die es Dritten (z. B. einem Anbieter) ermöglicht, Domänenberechtigungen zu erhalten.
 - d. Geben Sie eine Telefonnummer ein, die SMS empfangen kann
 - e. Geben Sie alle Hinweise für die Protokolle und die Überprüfung durch den PAM Approver ein.

4. Klicken Sie Auf „Anfrage Hinzufügen“.

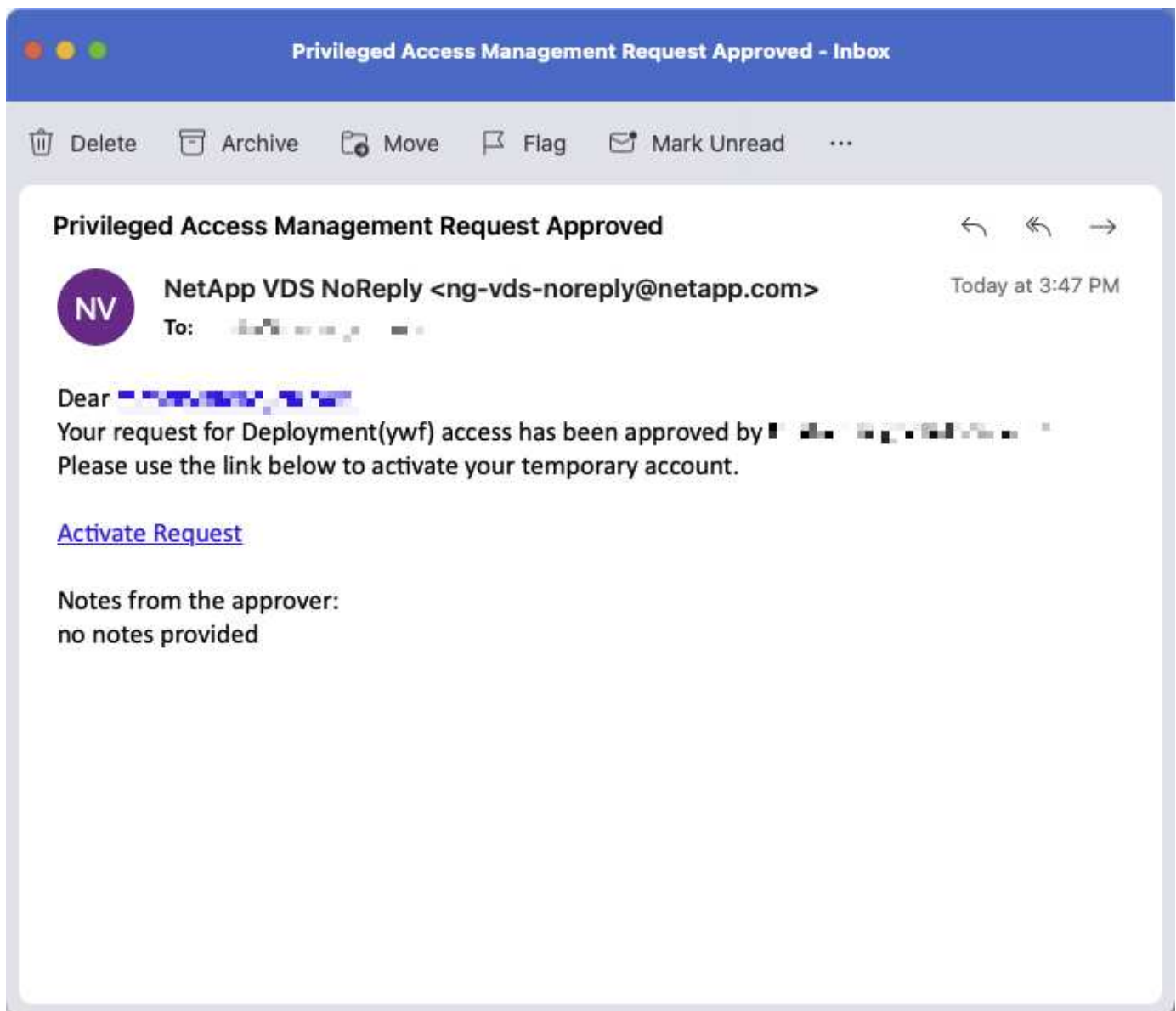
Genehmigen einer PAM-Anfrage

PAM-Anfragen prüfen und genehmigen/ablehnen

1. . Navigieren Sie oben rechts zu Ihrem Admin-Benutzernamen und klicken Sie auf „Einstellungen“.
2. Wählen Sie die Registerkarte „PAM Requests“ aus, und klicken Sie auf die Anfrage
3. Prüfen Sie die Anfrage und klicken Sie auf „Genehmigen“ oder „Ablehnen“.
4. Geben Sie alle für die Entscheidung über Genehmigung/Ablehnung relevanten Hinweise ein

Anhand von PAM generierten Zugangsdaten


Nach der Genehmigung wird die angegebene E-Mail-Adresse eine Bestätigungs-E-Mail geschickt, um ihre Anmeldedaten zu aktivieren:





Wenn Sie den Link „Anfrage aktivieren“ folgen, wird der Benutzer auf die folgende Seite gebracht und ihm per SMS einen Bestätigungscode zukommen lassen. Sie werden auch aufgefordert, ein sicheres Passwort

festzulegen.


Activate Your Account

 **Confirmation Code Sent**
We have sent a confirmation code to [redacted] - please enter the code below and set a password to activate your account.

Access Level Deployment	Confirmation Code Required
	<input type="text" value="[redacted]"/>
Password Required	Confirm Password Required
<input type="password" value="....."/> 	<input type="password" value="....."/> 

Nach erfolgreicher Überprüfung des Kontos erhält der Benutzer eine Bestätigung mit seinem Benutzernamen.

Activate Your Account

 **Successfully Activated Account**
Successfully activated account. Your account's username is [redacted]

Username
[redacted]

Benutzerzugriff Wird Hinzugefügt

Erstellung Eines Neuen Benutzers

Neue Active Directory-Bereitstellungen (für VDMS wurde eine neue Active Directory-Domäne erstellt)

1. Erstellen Sie den Benutzer in VDS
 - a. Navigieren Sie zum Arbeitsbereich, wählen Sie die Registerkarte „Benutzer & Gruppen“, klicken Sie auf „Hinzufügen“ und wählen Sie „Benutzer hinzufügen“.

CloudJumper Training PP
Virtual Desktop Service
Version 6.0
Enrollment production

Home > Workspaces > TrainingKrisG > Users & Groups

TrainingKrisG
Workspace

Overview **Users & Groups** Servers AVD More...

Users

Filter By
Q Keyword

Export Refresh **Add...** 3

Add User 4
Import from file

Username	Name	Connection	Status
Test1@TrainingKrisG.onmicrosoft.com	Tester 1	Not Connected	Available
test2@TrainingKrisG.onmicrosoft.com	Tester 2	Not Connected	Available

Previous Page 1 of 1 Next

Groups

Filter By
Q Keyword

Export **Add Group**

Name	Total Users	Actions
kift WVD Shared	2	
kift-all users	2	

Previous Page 1 of 1 Next

- b. Geben Sie die Benutzerinformationen ein, und klicken Sie dann auf „Benutzer hinzufügen“.

Add User

Username Required

Test3

First Name Required **Last Name** Required

Test User3

Email **Phone**

Test3@TrainingKrisG.onmicrosoft.com Phone...

☐ Multi-Factor Auth Enabled ☐ VDI User Enabled

☐ Wake On Demand Enabled ☒ Local Drive Access Enabled

☐ Force Password Reset at Next Login

Cancel
Add User

2. Benachrichtigen Sie NetApp über den zusätzlichen Benutzer mit einer der folgenden Methoden
 - a. E-Mail-Unterstützung: VDSsupport@netapp.com
 - b. Telefon-Support: 844.645.6789
 - c. "VDMS Support-Portal"
3. Weisen Sie den Benutzer seinem Host-Pool zu
 - a. Klicken Sie auf der Registerkarte Benutzer und Gruppen auf die Benutzergruppe, die mit dem Host-Pool verknüpft ist. Beispielsweise ist die Gruppe „kift WVD Shared“ mit dem WVD Shared Host Pool in VDMS verknüpft. Alle Benutzer, die „kift WVD Shared“ hinzugefügt wurden, werden Zugriff auf die Sitzungshosts im Host-Pool „WVD Shared“ erhalten.

CloudJumper Training PP
Virtual Desktop Service
Version 6.0
Environnement production

Home > Workspaces > TrainingKrisG > Users & Groups

TrainingKrisG Workspace

Refresh Edit Delete

Overview **Users & Groups** Servers AVD More...

Users

Filter By
Q Keyword Export Refresh + Add...

Username	Name	Connection	Status	Actions
Test3@TrainingKrisG.onmicrosoft.com	Test User3	Not Connected	Available	
Test1@TrainingKrisG.onmicrosoft.com	Tester 1	Not Connected	Available	
test2@TrainingKrisG.onmicrosoft.com	Tester 2	Not Connected	Available	

Previous Page 1 of 1 Next

Groups

Filter By
Q Keyword Export + Add Group

Name	Total Users	Actions
kift WVD Shared	2	
kift-all users	2	

Previous Page 1 of 1 Next

- b. Klicken Sie oben rechts im Feld Benutzer auf das Bearbeiten-Symbol und klicken Sie dann auf „Benutzer hinzufügen“.

CloudJumper Training PP
Virtual Desktop Service
Version 6.0
Environnement production

Home > Workspaces > TrainingKrisG > Users & Groups > kift WVD Shared

kift WVD Shared Group

Delete

Overview

Users

Filter By
Q Keyword Add Users

Name	Local Drive Access	Actions
Test1@TrainingKrisG.onmicrosoft.com	<input checked="" type="checkbox"/>	
test2@TrainingKrisG.onmicrosoft.com	<input checked="" type="checkbox"/>	

Previous Page 1 of 1 Next

Cancel Save

Applications

Filter By
Q Keyword

Name	Version	Enabled
Google Chrome	Latest	No

Previous Page 1 of 1 Next

- c. Aktivieren Sie das Kontrollkästchen neben den Benutzern, die hinzugefügt werden sollen, und klicken Sie dann auf „Weiter“.

Select Users

i 1 item(s) selected
 Show Clear

Filter By

<input type="checkbox"/>	Name	Username	Company Name	Company Code
<input type="checkbox"/>	Tester 1	Test1@TrainingKrisG.onmicrosoft.com	TrainingKrisG	kift
<input type="checkbox"/>	Tester 2	test2@TrainingKrisG.onmicrosoft.com	TrainingKrisG	kift
<input checked="" type="checkbox"/>	Test User3	Test3@TrainingKrisG.onmicrosoft.com	TrainingKrisG	kift

Previous
Page 1 of 1
Next

Cancel
Continue

d. Detailliertere Anweisungen finden Sie hier ["Hier"](#)

Vorhandene Active Directory-Bereitstellungen (VDMS stellen eine Verbindung zu einem vorhandenen Active Directory her)

1. Erstellen Sie den Benutzer wie gewohnt in Active Directory
2. Fügen Sie den Benutzer der Active Directory-Gruppe hinzu, die in der Bereitstellung aufgeführt ist

CloudJumper Training PP
Virtual Desktop Service
Version: 6.0
Environment: production

- Home
- Organizations
- Deployments
- Workspaces
- App Services
- Service Board
- Scripted Events
- Admins
- Reports
- Applications
- Cost Estimator
- SaaS Backup

Deployment Details

Name	TrainingKrisG.onmicrosoft.com	ID	vrg
Version	6.0	Hypervisor	Azure
Resource Allocation Type	MachineSize	Domain	TrainingKrisG.onmicrosoft.com
h5 Gateway	vrg-h5gw.vrg.cloudworkspace.app	RDP Gateway	vrg-rds.vrg.cloudworkspace.app
FTP Server Address	None	Directory Type	ActiveDirectory
Most Recent Heartbeat Jul 2, 2021, 3:51 PM			

PAM Approval Details

✗ Require Client Approval for PAM Access Requests

Processes

Client	User
New ✓ Idle	New ✓ Idle
Update ✓ Idle	Update ✓ Idle
Delete ✓ Idle	Delete ✓ Idle

App Service	Other
New ✓ Idle	Server Cache ✓ Idle
Update ✓ Idle	
Delete ✓ Idle	

Active Directory Group

Group Name
VDMS Access

3. Cloud Workspace aktivieren

4. Benachrichtigen Sie NetApp über den zusätzlichen Benutzer mit einer der folgenden Methoden

- a. E-Mail-Unterstützung: VDSsupport@netapp.com
- b. Telefon-Support: 844.645.6789
- c. ["VDMS Support-Portal"](#)

5. Weisen Sie den Benutzer seinem Host-Pool zu

- a. Klicken Sie auf der Registerkarte Benutzer und Gruppen auf die Benutzergruppe, die mit dem Host-Pool verknüpft ist. Beispielsweise ist die Gruppe „kift WVD Shared“ mit dem WVD Shared Host Pool in VDMS verknüpft. Alle Benutzer, die „kift WVD Shared“ hinzugefügt wurden, werden Zugriff auf die Sitzungshosts im Host-Pool „WVD Shared“ erhalten.

The screenshot shows the TrainingKrisG Workspace interface. On the left is a sidebar with navigation links: Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events, Admins, Reports, Applications, Cost Estimator, and SaaS Backup. The main content area has a top navigation bar with 'Home > Workspaces > TrainingKrisG > Users & Groups'. Below this is a 'TrainingKrisG Workspace' header with tabs for Overview, Users & Groups (selected), Servers, AVD, and More... On the right, there are buttons for Refresh, Edit, and Delete. The 'Users' section on the left has a 'Filter By' search bar, 'Export', 'Refresh', and 'Add...' buttons. It contains a table with columns: Username, Name, Connection, Status, and Actions. The table lists three users: Test3@TrainingKrisG.onmicrosoft.com (Test User3), Test1@TrainingKrisG.onmicrosoft.com (Tester 1), and test2@TrainingKrisG.onmicrosoft.com (Tester 2). All are 'Not Connected' and 'Available'. The 'Groups' section on the right has a 'Filter By' search bar, 'Export', and 'Add Group' buttons. It contains a table with columns: Name, Total Users, and Actions. It lists two groups: 'kift WVD Shared' (2 users) and 'kift-all users' (2 users). Both groups have a 'Previous', 'Page 1 of 1', and 'Next' pagination bar.

- b. Klicken Sie oben rechts im Feld Benutzer auf das Bearbeiten-Symbol und klicken Sie dann auf „Benutzer hinzufügen“.

The screenshot shows the TrainingKrisG Workspace interface for the 'kift WVD Shared' group. The top navigation bar shows 'Home > Workspaces > TrainingKrisG > Users & Groups > kift WVD Shared'. The 'kift WVD Shared Group' header has a 'Delete' button. Below this is an 'Overview' tab. The 'Users' section on the left has a 'Filter By' search bar, 'Add Users' button (with a red notification bubble), and a table with columns: Name, Local Drive Access, and Actions. The table lists two users: Test1@TrainingKrisG.onmicrosoft.com and test2@TrainingKrisG.onmicrosoft.com. Both have 'Local Drive Access' checked and a trash icon in the 'Actions' column. The 'Applications' section on the right has a 'Filter By' search bar and a table with columns: Name, Version, and Enabled. It lists one application: Google Chrome (Latest version, Enabled status). Both sections have a 'Previous', 'Page 1 of 1', and 'Next' pagination bar. At the bottom of the 'Users' section are 'Cancel' and 'Save' buttons.

- c. Aktivieren Sie das Kontrollkästchen neben den Benutzern, die hinzugefügt werden sollen, und klicken Sie dann auf „Weiter“.

Select Users

i 1 item(s) selected
 Show Clear

Filter By

Keyword

<input type="checkbox"/>	Name	Username	Company Name	Company Code
<input type="checkbox"/>	Tester 1	Test1@TrainingKrisG.onmicrosoft.com	TrainingKrisG	kift
<input type="checkbox"/>	Tester 2	test2@TrainingKrisG.onmicrosoft.com	TrainingKrisG	kift
<input checked="" type="checkbox"/>	Test User3	Test3@TrainingKrisG.onmicrosoft.com	TrainingKrisG	kift

Previous
Page of 1
 Next

Cancel
Continue

d. Detailliertere Anweisungen finden Sie hier ["Hier"](#)

Benutzerzugriff Wird Entfernt

Entfernen eines Benutzers

Neue Active Directory-Bereitstellungen (für VDMS wurde eine neue Active Directory-Domäne erstellt)

1. Löschen Sie den Benutzer in VDMS

- Navigieren Sie zum Arbeitsbereich, wählen Sie die Registerkarte „Benutzer & Gruppen“, klicken Sie auf die Aktionspunkte neben dem zu löschenden Benutzer und klicken Sie dann auf „Löschen“.

CloudJumper Training PP
Virtual Desktop Service
Version 6.0
Enrollment production

Search

KG Kris

Home > Workspaces > TrainingKrisG > Users & Groups

TrainingKrisG
Workspace

Refresh Edit Delete

Overview **Users & Groups** Servers AVD More...

Users

Filter By

 Keyword
 Export Refresh + Add...

Username	Name	Connection	Status	Actions
Test3@TrainingKrisG.onmicrosoft.com	Test User3	Not Connected	Available	<div> Edit Delete Disable CloudWorkspace Reset Password </div>
Test1@TrainingKrisG.onmicrosoft.com	Tester 1	Not Connected	Available	
test2@TrainingKrisG.onmicrosoft.com	Tester 2	Not Connected	Available	

Previous
Page of 1
 Next

Groups

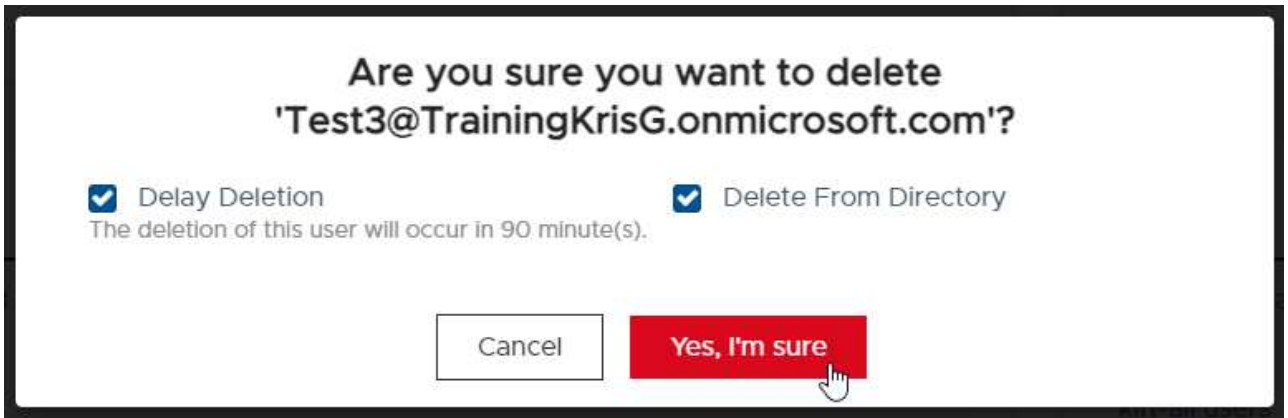
Filter By

 Keyword
 Export + Add Group

Name	Total Users	Actions
kift WVD Shared	2	⋮
kift-all users	3	⋮

Previous
Page of 1
 Next

- b. Es erscheint ein Popup-Fenster mit Optionen zum verzögern des Löschens und Löschen aus dem Verzeichnis



- i. Die Löschoption Delay wartet 90 Minuten vor dem Löschen des Benutzers, wodurch der Prozess abgebrochen werden kann. Aktivieren Sie dieses Kontrollkästchen.
- ii. Mit der Option aus Verzeichnis löschen wird das Active Directory-Benutzerkonto gelöscht. Dieses Kontrollkästchen sollte aktiviert sein.

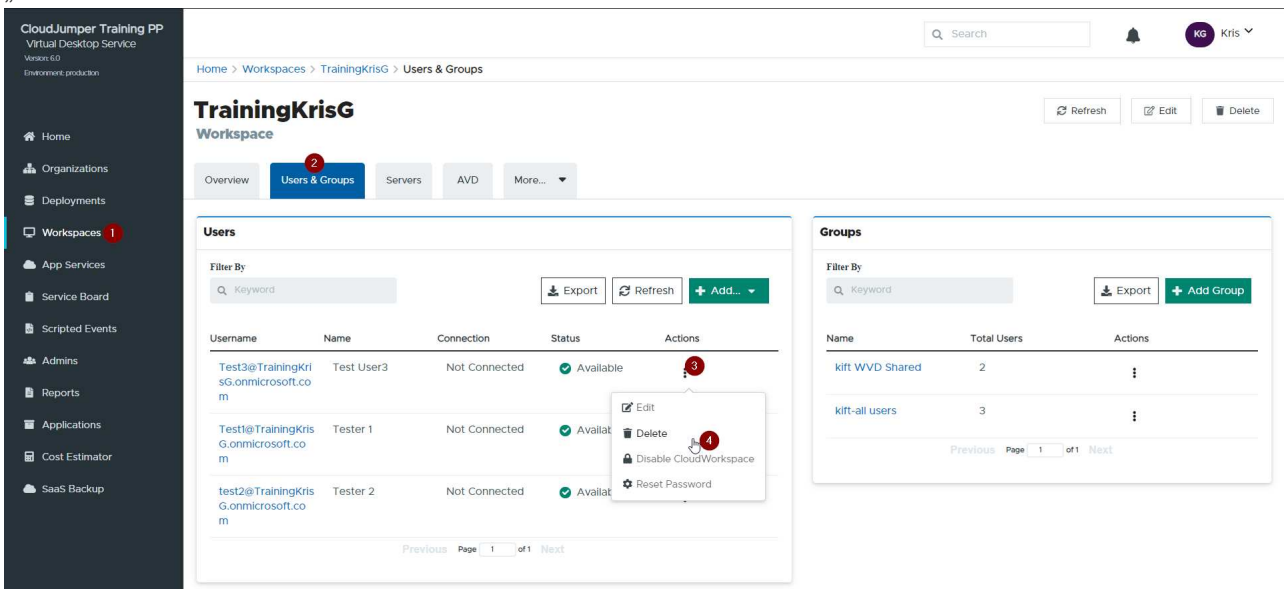
2. Benachrichtigen Sie NetApp über das Entfernen des Benutzers mit einer der folgenden Methoden

- a. E-Mail-Unterstützung: VDSsupport@netapp.com
- b. Telefon-Support: 844.645.6789
- c. ["VDMS Support-Portal"](#)

Vorhandene Active Directory-Bereitstellungen (VDMS stellen eine Verbindung zu einem vorhandenen Active Directory her)

1. Löschen Sie den Benutzer in VDMS

- a. Navigieren Sie zum Arbeitsbereich, wählen Sie die Registerkarte „Benutzer & Gruppen“, klicken Sie auf die Aktionspunkte neben dem zu löschenden Benutzer und klicken Sie dann auf „Löschen“.



- b. Es erscheint ein Popup-Fenster mit Optionen zum verzögern des Löschens und Löschen aus dem Verzeichnis

**Are you sure you want to delete
'Test3@TrainingKrisG.onmicrosoft.com'?**

☒ Delay Deletion
The deletion of this user will occur in 90 minute(s).
☐ Delete From Directory

Cancel

Yes, I'm sure

- i. Die Löschoption Delay wartet 90 Minuten vor dem Löschen des Benutzers, wodurch der Prozess abgebrochen werden kann. Aktivieren Sie dieses Kontrollkästchen.
 - ii. Mit der Option aus Verzeichnis löschen wird das Active Directory-Benutzerkonto gelöscht. Es wird empfohlen, dass dieses Kontrollkästchen NICHT aktiviert ist, und der Löschvorgang Ihres Unternehmens-Benutzerkontos wird befolgt, um das Konto aus Active Directory zu löschen.
2. Benachrichtigen Sie NetApp über das Entfernen des Benutzers mit einer der folgenden Methoden
- a. E-Mail-Unterstützung: VDSsupport@netapp.com
 - b. Telefon-Support: 844.645.6789
 - c. ["VDMS Support-Portal"](#)

Hinzufügen und Entfernen von Administratoren in VDMS

Hinzufügen von Administratoren in VDMS

- Dieser Prozess wird von NetApp abgewickelt
- Wenden Sie sich mit einer der folgenden Methoden an die Unterstützung von NetApp VDMS:
 - a. E-Mail-Unterstützung: VDSsupport@netapp.com
 - b. Telefon-Support: 844.645.6789
 - c. ["VDMS Support-Portal"](#)
- Bitte geben Sie Folgendes für das neue Administratorkonto an:
 - a. Partnercode
 - b. Vor- und Nachname
 - c. E-Mail-Adresse
 - d. Wenn sich die Berechtigungen von den Standardvorgaben unterscheiden, die im beschrieben werden ["Administratorberechtigungen"](#)

Entfernen von Administratoren in VDMS

- Dieser Prozess wird von Partnern durchgeführt
 - a. Öffnen Sie die Registerkarte „Administratoren“
 - b. Klicken Sie rechts neben dem Admin auf die Aktionspunkte, die Sie entfernen möchten
 - c. Klicken Sie Auf „Löschen“.

d. Es wird ein Bestätigungsfeld angezeigt. Klicken Sie auf „Ja, ich bin mir sicher“.

CloudJumper Training PP
Virtual Desktop Service
Version: 6.0
Environment: production

Home > Admins

Admins

Filter By
Q. TestAdmin

Refresh Export + Add Admin

Username	Name	Primary	Active Directory	MFA	Actions
TestAdmin@Training	Test Admin	✗	✗	✗	<div>2 Edit Delete 3</div>

Previous Page 1 of 1

- Wenn Sie Fragen haben, wenden Sie sich über eine der folgenden Methoden an die NetApp VDMS:
 - a. E-Mail-Unterstützung: VDSsupport@netapp.com
 - b. Telefon-Support: 844.645.6789
 - c. ["VDMS Support-Portal"](#)

Häufig gestellte FRAGEN ZU VDMS

VDS-Administratorberechtigungen

Administratorberechtigungen – Übersicht

VDMS Administratoren haben beschränkten Zugriff auf das VDS-Verwaltungsportal. Da VDMS eine gemeinsam gemanagte Lösung sind, gibt es Berechtigungssätze, die für VDMS-Administratoren nicht aktiviert sind. Diese Aktionen sind für das NetApp Support-Team reserviert. Wenn Maßnahmen erforderlich sind, die aufgrund von Berechtigungsbeschränkungen nicht ausgeführt werden können, wenden Sie sich an den Support.

Einstellungen Für Den Kontotyp

Im VDMS-Administratorkonto sind die folgenden Einstellungen standardmäßig eingestellt.

Typ	Standardwert	Hinweise
Technischer Account	Falsch	Kann auf Anfrage an den NetApp Support geändert werden. Wenn diese Option aktiviert ist, wird Administrator bei der Verbindung zu einer beliebigen VM über das VDS-Portal aufgefordert. Wenn diese Option deaktiviert ist, wird der Administrator bei der Verbindung mit einer beliebigen Mandanten-VM über das VDS-Portal automatisch authentifiziert (mit automatisch generiertem lokalen Administratorkonto). Administratoren werden nach wie vor zur Eingabe von Anmeldeinformationen aufgefordert, wenn sie sich mit einer beliebigen Plattform-Server-VM verbinden.
"PAM Genehmiger"	Richtig	Kann auf Anfrage an den NetApp Support geändert werden. Allen Kunden muss mindestens ein Administratorkonto als PAM Approver aktiviert sein.
Benutzersupport	Falsch	Diese Funktion gilt nicht für VDMS.

Typ	Standardwert	Hinweise
Schattenbenutzer	Richtig	Kann auf Anfrage an den NetApp Support geändert werden. Wenn diese Option aktiviert ist, kann der Administrator eine Verbindung mit der Sitzung eines Endbenutzers herstellen und die für die Bereitstellung der Endbenutzerunterstützung erforderlichen Informationen anzeigen.
MFA aktiviert	Richtig	Erfordert, dass der Administratorzugriff auf DAS VDMS-Verwaltungsportal mithilfe integrierter MFA gesichert werden muss. SMS- und/oder E-Mail-Methoden werden unterstützt.

Administrator-Kontoberechtigungen

Im VDMS-Administratorkonto sind die folgenden Berechtigungen standardmäßig aktiviert.

Modul	Anzeigen	Bearbeiten	Löschen	Zusatz	Hinweise
Admin	Ein	Aus	Ein	Aus	Das Hinzufügen von Admin-Konten und/oder das Ändern von Admin-Berechtigungen wird vom NetApp Support bearbeitet.
App-Services	Aus	Aus	Aus	Aus	Die App-Services-Funktionen sind keine unterstützte Funktion in VDMS.

Modul	Anzeigen	Bearbeiten	Löschen	Zusatz	Hinweise
Applikationen Unterstützt	Aus	Aus	Aus	Aus	Die Anwendungsfunktionen in VDS sind RDS-spezifisch. VDMS sind ein WVD-basiertes Service- und Anwendungsmanagement wird mit dieser Funktion nicht behandelt. Siehe "Aktualisieren und Bereitstellen von Images" Weitere Informationen zur Anwendungsbereitstellung für VDMS.
Audits	Ein	Ein	Ein	Ein	
Clients	Ein	Ein	Aus	Aus	Die Erstellung/Entfernung des Clients erfolgt über den NetApp Support.
Implementierungen	Ein	Ein	Aus	Aus	Die Erstellung/Entfernung der Implementierung erfolgt über den NetApp Support.
Firewall-Regeln	Ein	Ein	Ein	Ein	
Ordner	Ein	Ein	Ein	Ein	
Gruppen	Ein	Ein	Aus	Ein	Das Löschen von Benutzergruppen wird vom NetApp Support bearbeitet. Bestimmte Benutzergruppen sind erforderlich

Modul	Anzeigen	Bearbeiten	Löschen	Zusatz	Hinweise
Partner	Ein	Aus	Aus	Aus	Die Funktionssatz für Partner ist keine unterstützte Funktion in VDMS. Zum Anzeigen von Mandantenlisten erforderliche Berechtigungen anzeigen.
Bereitstellungsvorlagen	Ein	Ein	Aus	Aus	Die Erstellung/Entfernung von Bildern erfolgt über den NetApp Support.
Berichte An	Ein	Ein	Ein	Ein	
Ressourcen	Ein	Aus	Aus	Aus	Ressourceneinstellungen werden durch NetApp Support übernommen.
Skriptbasierte Ereignisse	Ein	Ein	Ein	Ein	
Server	Ein	Ein	Aus	Aus	Einstellungen zur Servererstellung/-Entfernung werden vom NetApp Support übernommen.
Service Board	Ein	Ein	Ein	Ein	
Einstellungen	Ein	Ein	Ein	Ein	
Benutzer	Ein	Ein	Ein	Ein	
Arbeitsbereiche	Ein	Ein	Aus	Aus	Workspace-Erstellung/-Entfernung wird vom NetApp Support gehandhabt.

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.