NetApp für GCP/GCVE

NetApp Solutions

NetApp
May 07, 2024

Inhalt

NetApp Hybrid-Multi-Cloud mit VMware Lösungen

Schutz von Workloads in GCP/GCVE

Applikationskonsistente Disaster Recovery mit NetApp SnapCenter und Veeam Replizierung

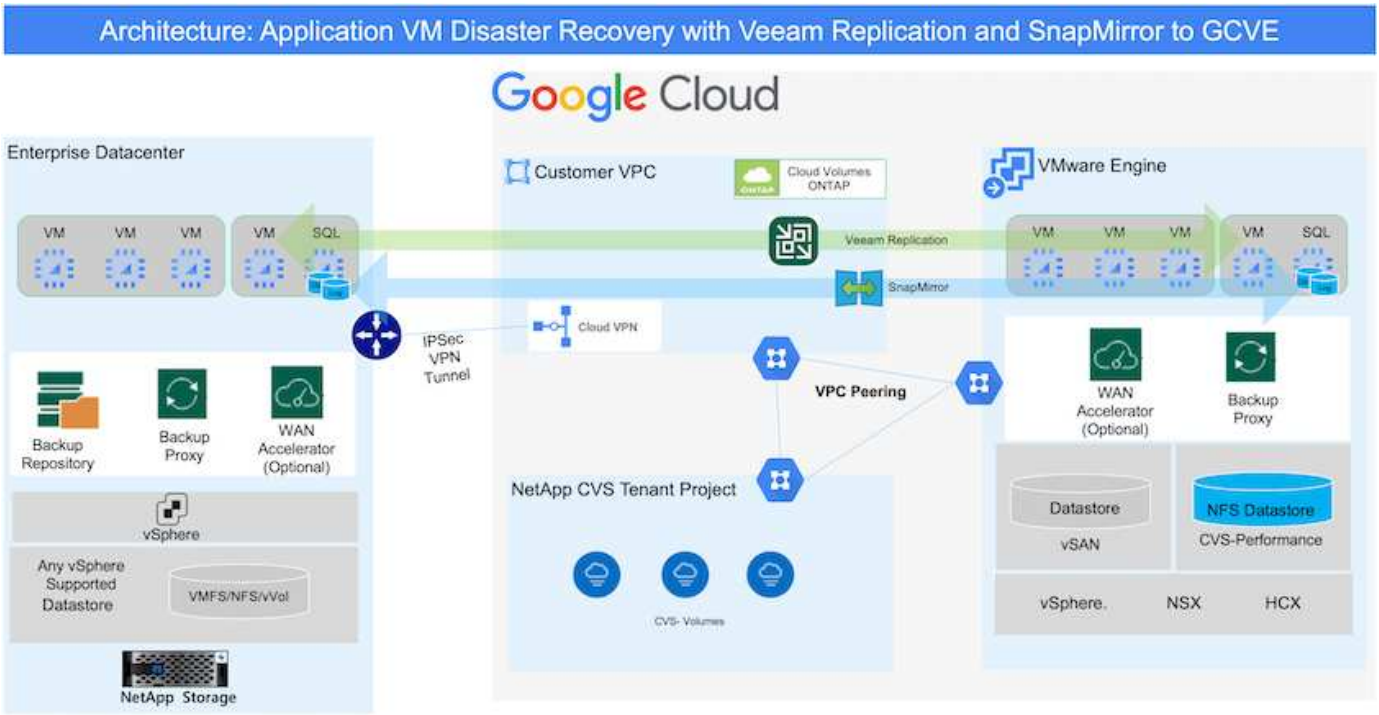
Autoren: Suresh ThopPay, NetApp

Überblick

Viele Kunden suchen nach einer effektiven Disaster Recovery-Lösung für ihre Applikations-VMs, die auf VMware vSphere gehostet werden. Viele von ihnen nutzen ihre bestehende Backup-Lösung, um im Diaster Recovery durchzuführen.
Oft erhöht diese Lösung die RTO und entspricht nicht ihren Erwartungen. Um RPO und RTO zu reduzieren, kann die Veeam VM-Replizierung sogar von On-Premises zu GCVE genutzt werden, sofern Netzwerkverbindungen und Umgebung mit entsprechenden Berechtigungen verfügbar sind.
HINWEIS: Veeam VM Replication schützt keine über VM-Gastsysteme verbundenen Storage-Geräte wie iSCSI- oder NFS-Mounts innerhalb der Gast-VM. Sie müssen sie separat schützen.

Für eine applikationskonsistente Replizierung für SQL VM und zur Reduzierung des RTO wurde SnapCenter zum Orchestrieren von snapmirror Vorgängen von SQL Datenbank- und Protokoll-Volumes eingesetzt.

Dieses Dokument bietet eine Schritt-für-Schritt-Methode zum Einrichten und Durchführen von Disaster-Recovery mit NetApp SnapMirror, Veeam und der Google Cloud VMware Engine (GCVE).



Voraussetzungen

Dieses Dokument konzentriert sich auf den Gast-Storage für Applikationsdaten (auch als Gastsystem bekannt) und wir gehen davon aus, dass die On-Premises-Umgebung SnapCenter für applikationskonsistente Backups verwendet.

> Dieses Dokument bezieht sich auf jede Backup- oder Recovery-Lösung eines Drittanbieters. Je nach der in der Umgebung verwendeten Lösung befolgen Sie Best Practices, um Backup-Richtlinien zu erstellen, die die SLAs des Unternehmens erfüllen.

Für die Verbindung zwischen der lokalen Umgebung und dem Google Cloud-Netzwerk können Sie die Konnektivitätsoptionen wie dediziertes Interconnect oder Cloud VPN verwenden. Segmente sollten basierend auf dem lokalen VLAN-Design erstellt werden.

> Es gibt mehrere Optionen, um On-Premises-Datacenter mit Google Cloud zu verbinden, was uns daran hindert, einen bestimmten Workflow in diesem Dokument zu beschreiben. Die entsprechende On-Premises-zu-Google-Verbindungsmethode finden Sie in der Google Cloud-Dokumentation.

Implementieren der DR-Lösung

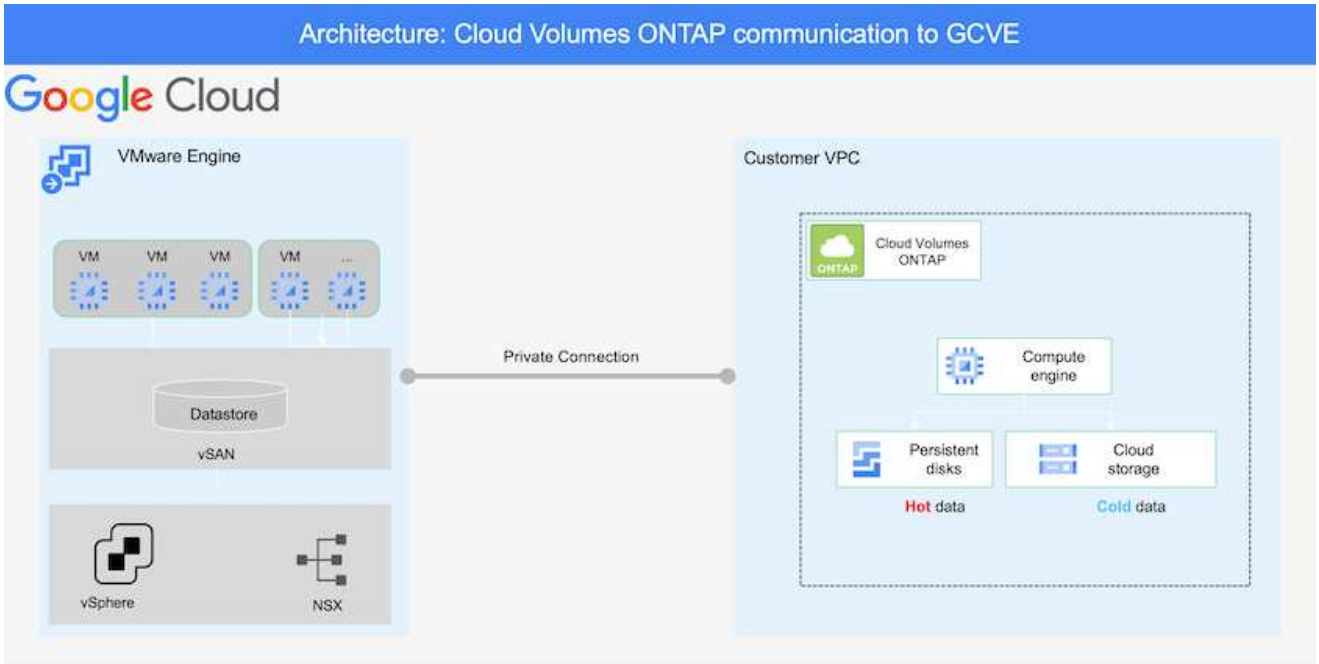
Übersicht Zur Lösungsimplementierung

1. Stellen Sie sicher, dass die Applikationsdaten mit SnapCenter zusammen mit den erforderlichen RPO-Anforderungen gesichert werden.
2. Stellen Sie mit BlueXP innerhalb des entsprechenden Abonnements und virtuellen Netzwerks Cloud Volumes ONTAP mit der korrekten Instanzgröße bereit.
   a. Konfiguration von SnapMirror für die entsprechenden Applikations-Volumes
   b. Aktualisieren Sie die Backup-Richtlinien in SnapCenter, um SnapMirror Updates nach den geplanten Aufgaben auszulösen.
3. Installieren Sie die Veeam Software und beginnen Sie mit der Replizierung von Virtual Machines zu Google Cloud VMware Engine Instanz.
4. Brechen Sie während eines Ausfalls die SnapMirror Beziehung mit BlueXP auf und lösen Sie Failover von Virtual Machines mit Veeam aus.
   a. Schließen Sie die ISCSI-LUNs und NFS-Mounts für die Applikations-VMs wieder an.
   b. Anwendungen online schalten.
5. Rufen Sie Failback auf den geschützten Standort auf, indem Sie SnapMirror nach der Wiederherstellung des primären Standorts erneut resynchronisieren.

Einzelheiten Zur Bereitstellung

Konfiguration von CVO auf Google Cloud und Replizierung von Volumes zu CVO

Als ersten Schritt müssen Sie Cloud Volumes ONTAP auf Google Cloud konfigurieren ("cvo") Und replizieren Sie die gewünschten Volumen zu Cloud Volumes ONTAP mit den gewünschten Frequenzen und Snapshot-Aufbewahrung.



Eine Schritt-für-Schritt-Anleitung zum Einrichten von SnapCenter und Replizieren der Daten finden Sie unter "Einrichtung der Replikation mit SnapCenter"

Überprüfen Sie den SQL VM-Schutz mit SnapCenter

Konfigurieren Sie GCVE-Hosts und CVO-Datenzugriff

Zwei wichtige Faktoren, die bei der Implementierung des SDDC berücksichtigt werden müssen, sind die Größe des SDDC-Clusters in der GCVE-Lösung und die Dauer, bis das SDDC den Betrieb aufrecht erhalten hat. Diese beiden wichtigen Überlegungen für eine Disaster-Recovery-Lösung tragen zur Senkung der Gesamtbetriebskosten bei. Das SDDC kann mit nur drei Hosts eingerichtet sein und bis hin zu einem Cluster mit mehreren Hosts in einer umfassenden Implementierung.

Der NetApp Cloud Volume Service für NFS-Datastore und die Cloud Volumes ONTAP für SQL-Datenbanken und das Protokoll können in jede VPC implementiert werden. GCVE sollte über eine private Verbindung zu dieser VPC verfügen, um den NFS-Datastore zu mounten und die VM mit den iSCSI-LUNs zu verbinden.

Informationen zum Konfigurieren von GCVE SDDC finden Sie unter "Implementieren und Konfigurieren der Virtualisierungsumgebung auf der Google Cloud Platform (GCP)". Überprüfen Sie als Voraussetzung, ob die Gast-VMs auf den GCVE-Hosts Daten aus dem Cloud Volumes ONTAP nutzen können, nachdem eine Verbindung hergestellt wurde.

Nachdem Cloud Volumes ONTAP und GCVE ordnungsgemäß konfiguriert wurden, beginnen Sie mit der Konfiguration von Veeam, um die Wiederherstellung lokaler Workloads auf GCVE (VMs mit Applikations-VMDKs und VMs mit in-Guest-Storage) zu automatisieren. Dazu nutzen Sie die Veeam Replication-Funktion und können SnapMirror für Applikations-Volumes-Kopien in Cloud Volumes ONTAP nutzen.

Veeam Komponenten Installieren

Der Veeam Backup-Server, Backup-Repository und Backup-Proxy, der bereitgestellt werden muss, basieren auf einem Implementierungsszenario. In diesem Anwendungsfall müssen kein Objektspeicher für Veeam implementiert und auch kein Scale-out-Repository erforderlich sein.
"Das Installationsverfahren finden Sie in der Veeam-Dokumentation"
Weitere Informationen finden Sie unter "Migration mit Veeam Replication"

VM Replication mit Veeam einrichten

VCenter vor Ort und GCVE vCenter müssen bei Veeam registriert werden. "VSphere VM Replication Job einrichten" Wählen Sie im Assistenten zur Gastverarbeitung die Option Anwendungsverarbeitung deaktivieren, da wir SnapCenter für applikationsgerechtes Backup und Recovery verwenden werden.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

Failover von Microsoft SQL Server VM

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

Vorteile dieser Lösung

- Nutzt die effiziente und ausfallsichere Replizierung von SnapMirror
- Wiederherstellung zu beliebigen verfügbaren Zeitpunkten mit ONTAP Snapshot Aufbewahrung

- Eine vollständige Automatisierung steht für alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs zur Verfügung – von den Schritten für Storage, Computing, Netzwerk und Applikationen.
- SnapCenter nutzt Klonmechanismen, die das replizierte Volume nicht ändern.
  - So wird das Risiko einer Beschädigung von Daten von Volumes und Snapshots vermieden.
  - Keine Replizierungsunterbrechungen während der DR-Test-Workflows
  - Nutzung der DR-Daten für Workflows über DR hinaus, wie Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests und Korrekturtests
- Veeam Replication ermöglicht das Ändern der VM-IP-Adressen am DR-Standort.

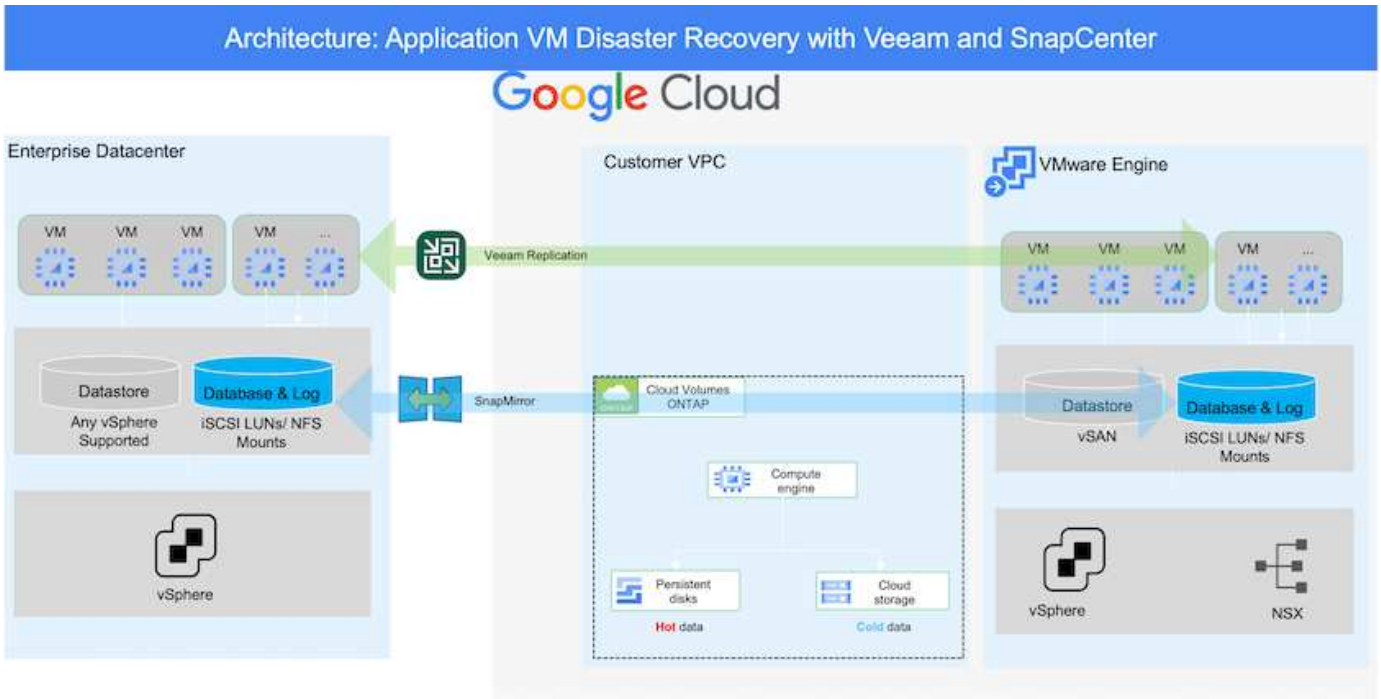
Disaster Recovery für Applikationen mit SnapCenter, Cloud Volumes ONTAP und Veeam Replication

Autoren: Suresh ThopPay, NetApp

Überblick

Disaster Recovery in die Cloud ist eine stabile und kostengünstige Möglichkeit zum Schutz von Workloads vor Standortausfällen und Datenbeschädigungen wie Ransomware. Mit NetApp SnapMirror können lokale VMware Workloads, die Storage mit Anbindung des Gastspeichers verwenden, auf NetApp Cloud Volumes ONTAP repliziert werden, die in Google Cloud ausgeführt werden. Dies bezieht sich auf Applikationsdaten, doch was ist mit den eigentlichen VMs selbst. Disaster Recovery sollte alle abhängigen Komponenten, einschließlich Virtual Machines, VMDKs, Applikationsdaten und mehr, abdecken. Dazu kann SnapMirror zusammen mit Veeam verwendet werden, um Workloads, die von On-Premises zu Cloud Volumes ONTAP repliziert wurden, nahtlos wiederherzustellen und gleichzeitig mit vSAN Storage für VM-VMDKs zu verwenden.

Dieses Dokument bietet eine Schritt-für-Schritt-Methode zum Einrichten und Durchführen von Disaster-Recovery mit NetApp SnapMirror, Veeam und der Google Cloud VMware Engine (GCVE).



Voraussetzungen

Dieses Dokument konzentriert sich auf den Gast-Storage für Applikationsdaten (auch als Gastsystem bekannt) und wir gehen davon aus, dass die On-Premises-Umgebung SnapCenter für applikationskonsistente Backups verwendet.

> Dieses Dokument bezieht sich auf jede Backup- oder Recovery-Lösung eines Drittanbieters. Je nach der in der Umgebung verwendeten Lösung befolgen Sie Best Practices, um Backup-Richtlinien zu erstellen, die die SLAs des Unternehmens erfüllen.

Für die Verbindung zwischen der lokalen Umgebung und dem Google Cloud-Netzwerk können Sie die Konnektivitätsoptionen wie dediziertes Interconnect oder Cloud VPN verwenden. Segmente sollten basierend auf dem lokalen VLAN-Design erstellt werden.

> Es gibt mehrere Optionen, um On-Premises-Datacenter mit Google Cloud zu verbinden, was uns daran hindert, einen bestimmten Workflow in diesem Dokument zu beschreiben. Die entsprechende On-Premises-zu-Google-Verbindungsmethode finden Sie in der Google Cloud-Dokumentation.

Implementieren der DR-Lösung

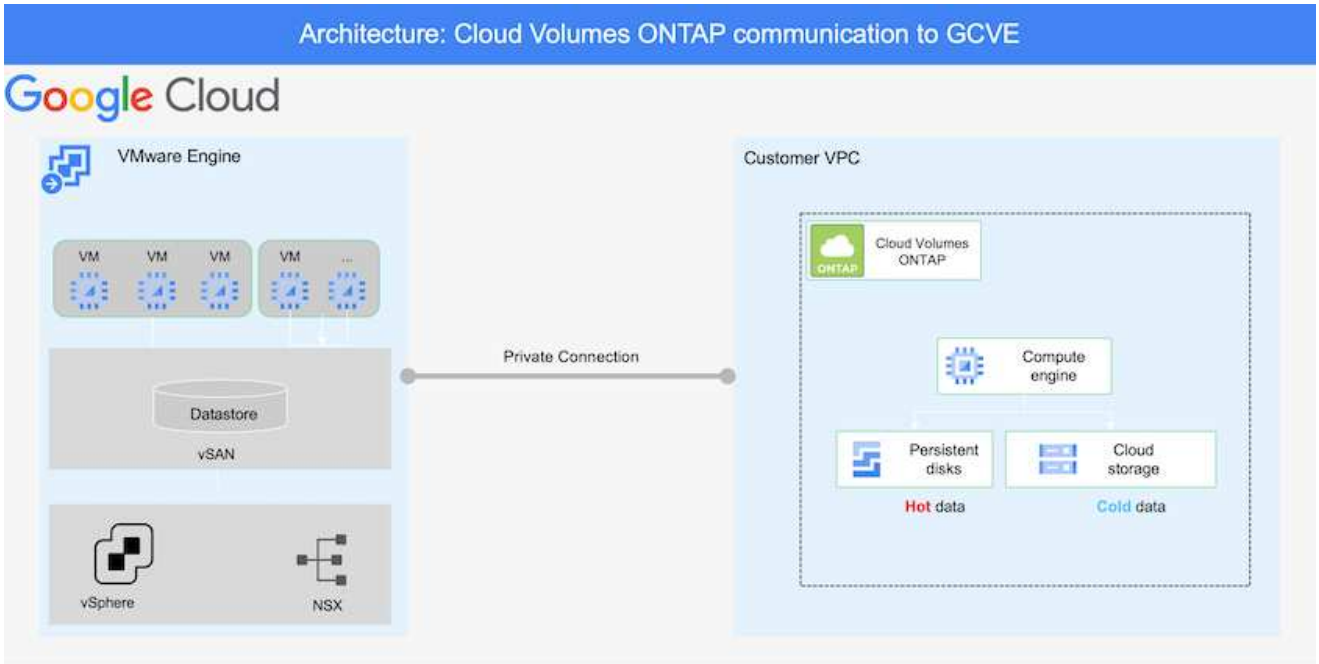
Übersicht Zur Lösungsimplementierung

1. Stellen Sie sicher, dass die Applikationsdaten mit SnapCenter zusammen mit den erforderlichen RPO-Anforderungen gesichert werden.
2. Stellen Sie mithilfe von Cloud Manager Cloud Volumes ONTAP mit der richtigen Instanzgröße innerhalb des entsprechenden Abonnements und des virtuellen Netzwerks bereit.
   a. Konfiguration von SnapMirror für die entsprechenden Applikations-Volumes
   b. Aktualisieren Sie die Backup-Richtlinien in SnapCenter, um SnapMirror Updates nach den geplanten Aufgaben auszulösen.
3. Installieren Sie die Veeam Software und beginnen Sie mit der Replizierung von Virtual Machines zu Google Cloud VMware Engine Instanz.
4. Brechen Sie während eines Notfallereignisses die SnapMirror Beziehung mithilfe von Cloud Manager auf und lösen Sie das Failover von Virtual Machines mit Veeam aus.
   a. Schließen Sie die ISCSI-LUNs und NFS-Mounts für die Applikations-VMs wieder an.
   b. Anwendungen online schalten.
5. Rufen Sie Failback auf den geschützten Standort auf, indem Sie SnapMirror nach der Wiederherstellung des primären Standorts erneut resynchronisieren.

Einzelheiten Zur Bereitstellung

Konfiguration von CVO auf Google Cloud und Replizierung von Volumes zu CVO

Als ersten Schritt müssen Sie Cloud Volumes ONTAP auf Google Cloud konfigurieren ("cvo") Und replizieren Sie die gewünschten Volumen zu Cloud Volumes ONTAP mit den gewünschten Frequenzen und Snapshot-Aufbewahrung.



Eine Schritt-für-Schritt-Anleitung zum Einrichten von SnapCenter und zum Replizieren der Daten finden Sie unter "Einrichtung der Replikation mit SnapCenter"

Einrichtung der Replikation mit SnapCenter

Konfigurieren Sie GCVE-Hosts und CVO-Datenzugriff

Zwei wichtige Faktoren, die bei der Implementierung des SDDC berücksichtigt werden müssen, sind die Größe des SDDC-Clusters in der GCVE-Lösung und die Dauer, bis das SDDC den Betrieb aufrecht erhalten hat. Diese beiden wichtigen Überlegungen für eine Disaster-Recovery-Lösung tragen zur Senkung der Gesamtbetriebskosten bei. Das SDDC kann mit nur drei Hosts eingerichtet sein und bis hin zu einem Cluster mit mehreren Hosts in einer umfassenden Implementierung.

Cloud Volumes ONTAP kann in jede VPC implementiert werden und GCVE sollte über eine private Verbindung zu dieser VPC verfügen, damit VM-Verbindung mit iSCSI-LUNs hergestellt werden kann.

Informationen zum Konfigurieren von GCVE SDDC finden Sie unter "Implementieren und Konfigurieren der Virtualisierungsumgebung auf der Google Cloud Platform (GCP)". Überprüfen Sie als Voraussetzung, ob die Gast-VMs auf den GCVE-Hosts Daten aus dem Cloud Volumes ONTAP nutzen können, nachdem eine Verbindung hergestellt wurde.

Nachdem Cloud Volumes ONTAP und GCVE ordnungsgemäß konfiguriert wurden, beginnen Sie mit der Konfiguration von Veeam, um die Wiederherstellung lokaler Workloads auf GCVE (VMs mit Applikations-VMDKs und VMs mit in-Guest-Storage) zu automatisieren. Dazu nutzen Sie die Veeam Replication-Funktion und können SnapMirror für Applikations-Volumes-Kopien in Cloud Volumes ONTAP nutzen.

Veeam Komponenten Installieren

Der Veeam Backup-Server, Backup-Repository und Backup-Proxy, der bereitgestellt werden muss, basieren auf einem Implementierungsszenario. In diesem Anwendungsfall müssen kein Objektspeicher für Veeam implementiert und auch kein Scale-out-Repository erforderlich sein.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Das Installationsverfahren finden Sie in der Veeam-Dokumentation"]

VM Replication mit Veeam einrichten

VCenter vor Ort und GCVE vCenter müssen bei Veeam registriert werden. "VSphere VM Replication Job einrichten" Wählen Sie im Assistenten zur Gastverarbeitung die Option Anwendungsverarbeitung deaktivieren, da wir SnapCenter für applikationsgerechtes Backup und Recovery verwenden werden.

VSphere VM Replication Job einrichten

Failover von Microsoft SQL Server VM

Failover von Microsoft SQL Server VM

Vorteile dieser Lösung

- Nutzt die effiziente und ausfallsichere Replizierung von SnapMirror
- Wiederherstellung zu beliebigen verfügbaren Zeitpunkten mit ONTAP Snapshot Aufbewahrung
- Eine vollständige Automatisierung steht für alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs zur Verfügung – von den Schritten für Storage, Computing, Netzwerk und Applikationen.
- SnapCenter nutzt Klonmechanismen, die das replizierte Volume nicht ändern.
  - So wird das Risiko einer Beschädigung von Daten von Volumes und Snapshots vermieden.
  - Keine Replizierungsunterbrechungen während der DR-Test-Workflows
  - Nutzung der DR-Daten für Workflows über DR hinaus, wie Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests und Korrekturtests
- Veeam Replication ermöglicht das Ändern der VM-IP-Adressen am DR-Standort.

Migration von Workloads auf GCP/GCVE

Workloads mit VMware HCX - QuickStart Guide auf den NetApp Cloud Volume Service Datastore auf der Google Cloud VMware Engine migrieren

Autor(en): NetApp Solutions Engineering

Übersicht: Migration von Virtual Machines mit VMware HCX, NetApp Cloud Volume Service Datastores und Google Cloud VMware Engine (GCVE)

Eine der gängigsten Anwendungsfälle für die Google Cloud VMware Engine und einen Cloud Volume Service-Datastore ist die Migration von VMware Workloads. VMware HCX ist eine bevorzugte Option und bietet verschiedene Migrationsmechanismen zum Verschieben von On-Premises-Virtual Machines (VMs) und deren

Daten in NFS-Datastores des Cloud Volume Service.

VMware HCX ist primär eine Migrationsplattform, die entwickelt wurde, um die Migration von Applikationen, die Ausbalancierung von Workloads und sogar Business Continuity Cloud-übergreifend zu vereinfachen. Dies ist Teil von Google Cloud VMware Engine Private Cloud und bietet zahlreiche Möglichkeiten zur Migration von Workloads und kann für Disaster-Recovery-Vorgänge (DR) genutzt werden.

Dieses Dokument enthält eine Schritt-für-Schritt-Anleitung für die Bereitstellung von Cloud Volume Service Datastore. Anschließend werden alle wichtigen Komponenten von VMware HCX heruntergeladen, implementiert und konfiguriert, einschließlich aller wichtigen Komponenten vor Ort und der Google Cloud VMware Engine Seite mit Interconnect, Netzwerkerweiterung und WAN-Optimierung für die Aktivierung verschiedener VM-Migrationsmechanismen.

> VMware HCX arbeitet mit jedem Datenspeichertyp zusammen, da die Migration auf VM-Ebene erfolgt. Daher eignet sich dieses Dokument für bestehende NetApp Kunden und andere Kunden, die den Cloud Volume Service mit der Google Cloud VMware Engine als kostengünstige VMware Cloud-Implementierung planen.

Allgemeine Schritte

Diese Liste enthält die grundlegenden Schritte, die zum Pairing und Migrieren der VMs zu HCX Cloud Manager auf der Google Cloud VMware Engine Seite von HCX Connector vor Ort erforderlich sind:

1. Bereiten Sie HCX über das Google VMware Engine Portal vor.
2. Laden Sie das Installationsprogramm für die HCX Connector Open Virtualization Appliance (OVA) im lokalen VMware vCenter Server herunter und implementieren Sie es.
3. HCX mit dem Lizenzschlüssel aktivieren.
4. Verbinden Sie den lokalen VMware HCX Connector mit der Google Cloud VMware Engine HCX Cloud Manager.
5. Sie konfigurieren das Netzwerkprofil, das Computing-Profil und das Service-Mesh.
6. (Optional) Sie können eine Netzwerkerweiterung vornehmen, um bei Migrationen eine erneute IP-Adresse zu vermeiden.
7. Validieren des Appliance-Status und Sicherstellen der Möglichkeit der Migration
8. Migration der VM-Workloads

Voraussetzungen

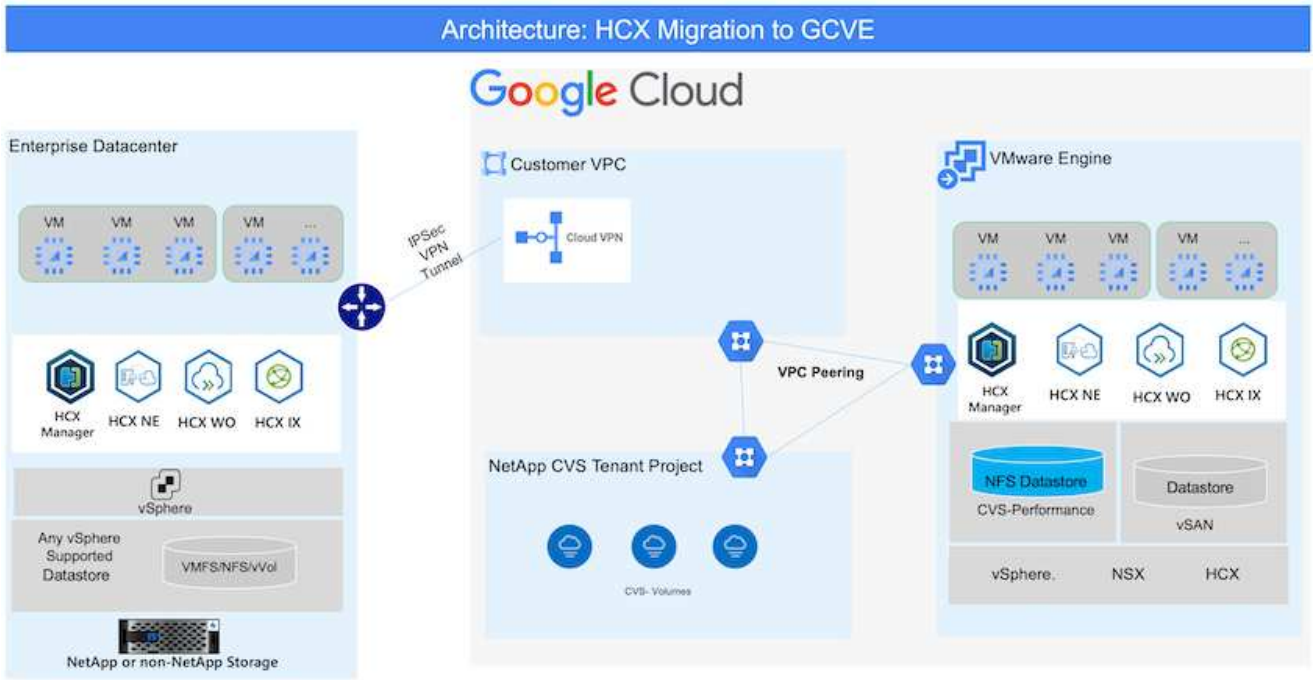
Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind. Weitere Informationen finden Sie unter "Verlinken". Nachdem die Voraussetzungen, einschließlich Konnektivität, vorhanden sind, laden Sie den HCX-Lizenzschlüssel aus dem Google Cloud VMware Engine-Portal herunter. Nach dem Herunterladen des OVA-Installationsprogramms gehen Sie wie unten beschrieben mit der Installation vor.

> HCX Advanced ist die Standardoption und die VMware HCX Enterprise Edition ist auch über ein Support-Ticket erhältlich und wird ohne zusätzliche Kosten unterstützt. Siehe "Dieser Link"

- Verwenden Sie ein vorhandenes softwaredefiniertes Google Cloud VMware Engine Datacenter (SDDC) oder erstellen Sie mithilfe dieses Modells eine Private Cloud "Link von NetApp" Oder hier "Google-Link".
- Die Migration von VMs und zugehörigen Daten vom lokalen Datacenter mit VMware vSphere erfordert Netzwerkkonnektivität vom Datacenter zur SDDC-Umgebung. Vor der Migration von Workloads "Einrichten eines Cloud-VPN oder einer Cloud Interconnect-Verbindung" Zwischen der lokalen Umgebung und der jeweiligen Private Cloud verschieben.
- Der Netzwerkpfad von der lokalen VMware vCenter Server Umgebung zur privaten Cloud der Google Cloud VMware Engine muss die Migration von VMs mithilfe von vMotion unterstützen.
- Stellen Sie sicher, dass die erforderlichen "Firewall-Regeln und -Ports" Sind für vMotion Traffic zwischen dem lokalen vCenter Server und SDDC vCenter zulässig.
- Cloud Volume Service NFS-Volume sollte als Datastore in der Google Cloud VMware Engine gemountet werden. Befolgen Sie die in diesem Schritt beschriebenen Schritte "Verlinken" Cloud Volume Service-Datenspeicher an Google Cloud VMware Engines Hosts anhängen.

Übergeordnete Architektur

Die Lab-Umgebung vor Ort für diese Validierung wurde zu Testzwecken über ein Cloud-VPN verbunden, das On-Premises-Konnektivität mit Google Cloud VPC ermöglicht.



Nähere Informationen zu HCX finden Sie unter "Link zu VMware"

Lösungsimplementierung

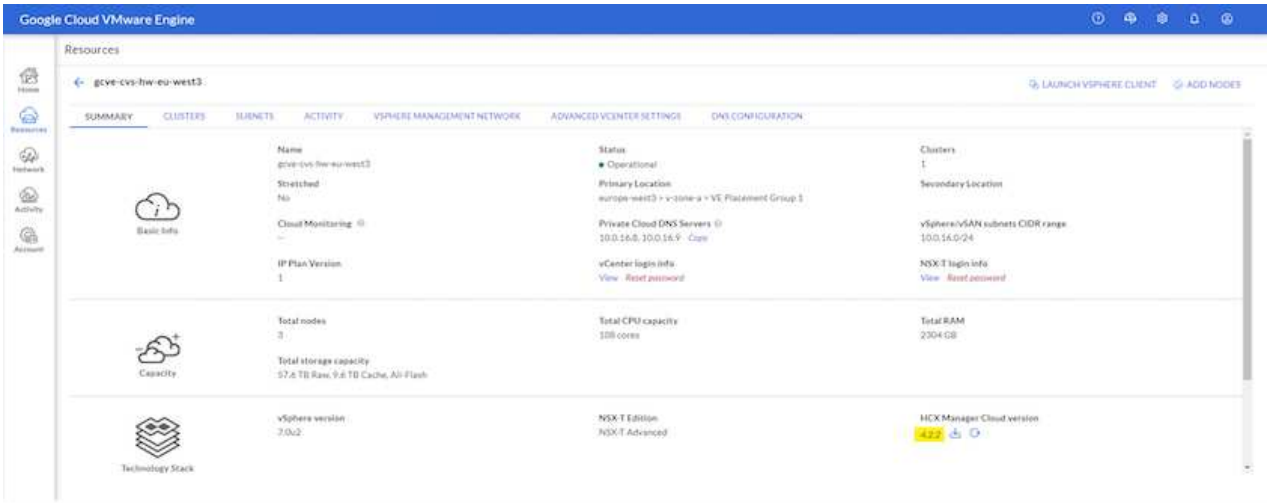
Führen Sie die folgenden Schritte aus, um die Implementierung dieser Lösung abzuschließen:

Schritt 1: HCX über das Google VMware Engine Portal vorbereiten

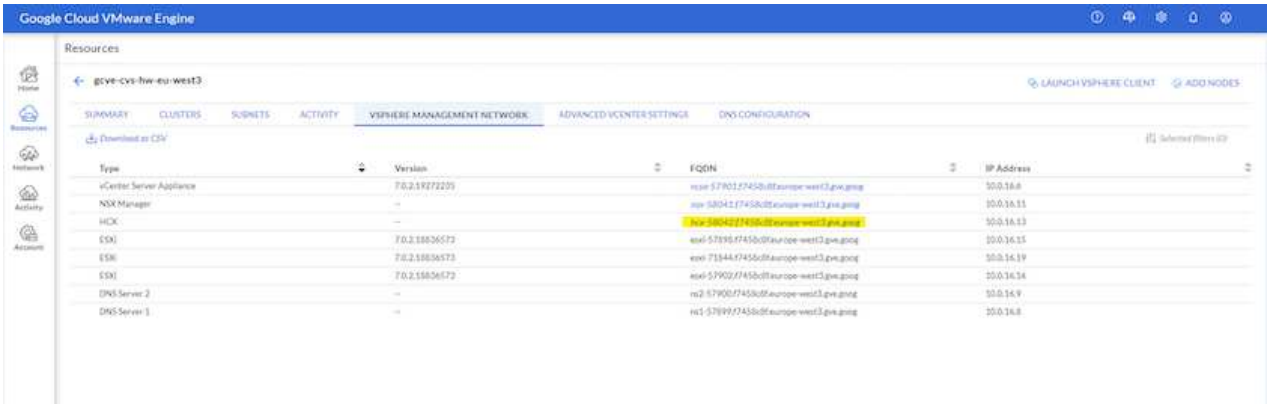
HCX Cloud Manager wird automatisch installiert, wenn Sie eine Private Cloud mit VMware Engine bereitstellen. Gehen Sie wie folgt vor, um die Standortpaarung vorzubereiten:

1. Melden Sie sich beim Google VMware Engine Portal an und melden Sie sich beim HCX Cloud Manager an.

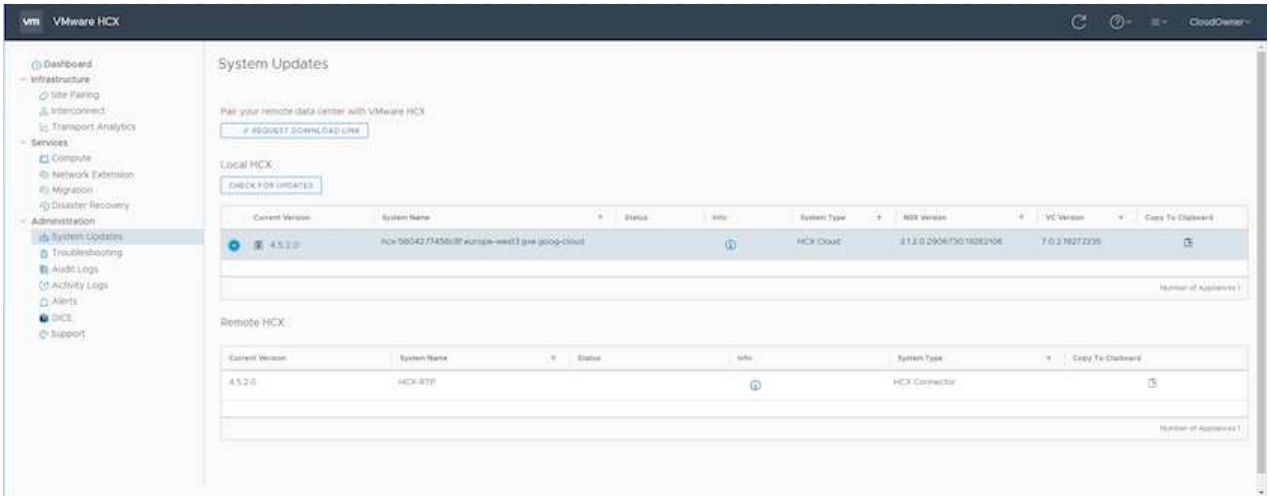
   Sie können sich bei der HCX Console anmelden, indem Sie auf den Link zur HCX-Version klicken

   Oder klicken Sie unter der Registerkarte vSphere Management Network auf HCX FQDN.

2. Gehen Sie in HCX Cloud Manager zu **Administration > System Updates**.
3. Klicken Sie auf **Download-Link anfordern** und laden Sie die OVA-Datei herunter.



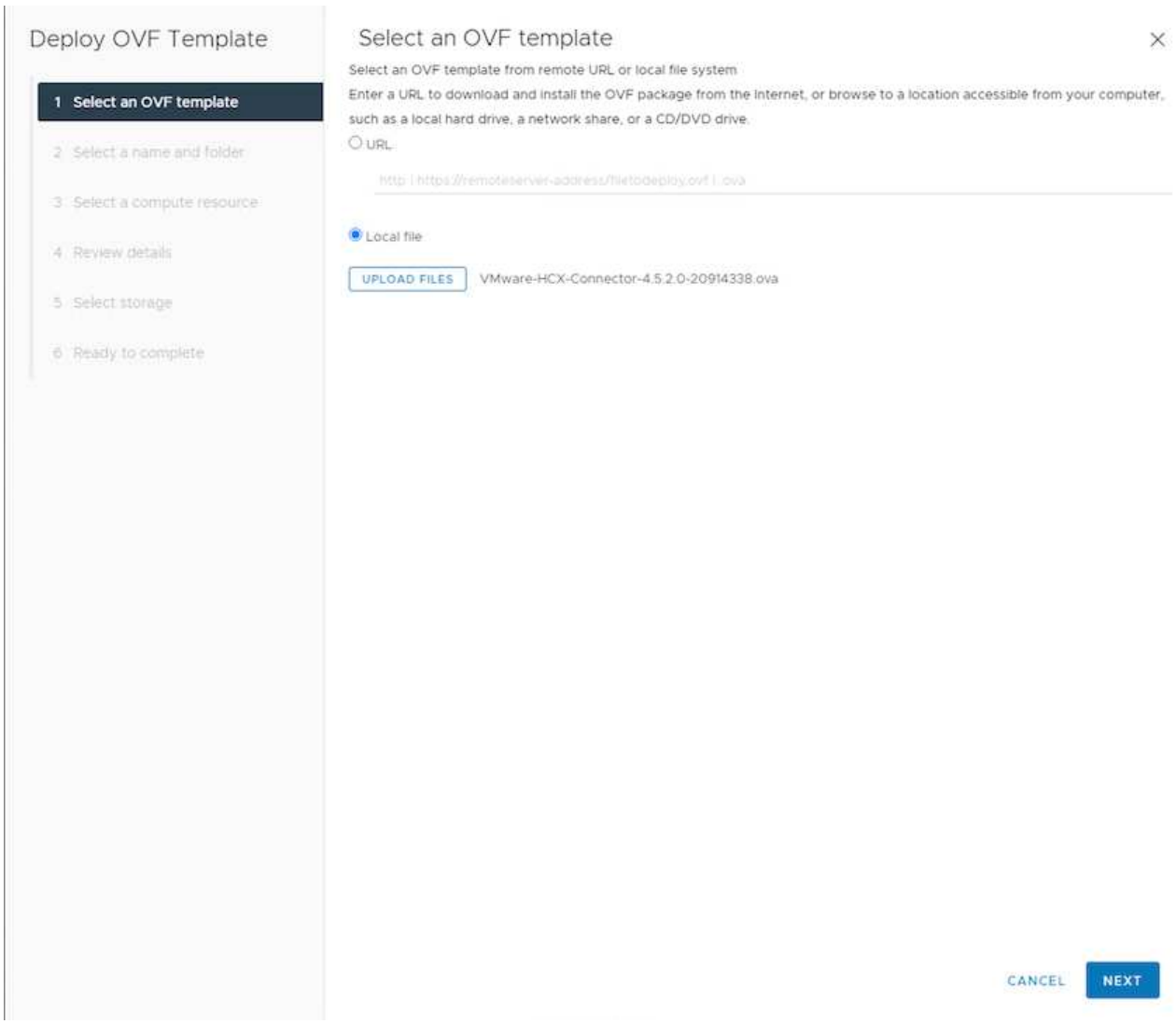
4. Aktualisieren Sie HCX Cloud Manager auf die neueste Version, die über die Benutzeroberfläche von HCX Cloud Manager verfügbar ist.

Schritt 2: Stellen Sie das Installationsprogramm OVA im lokalen vCenter Server bereit

Damit der On-Premises Connector eine Verbindung zum HCX Manager in der Google Cloud VMware Engine herstellen kann, müssen die entsprechenden Firewall-Ports in der On-Premises-Umgebung geöffnet sein.

So laden Sie den HCX Connector auf dem lokalen vCenter Server herunter und installieren ihn:

1. Laden Sie die ova von der HCX-Konsole auf Google Cloud VMware Engine wie im vorherigen Schritt angegeben herunter.
2. Nachdem die OVA heruntergeladen wurde, stellen Sie sie in der lokalen VMware vSphere Umgebung mithilfe der Option **Deploy OVF Template** bereit.



3. Geben Sie alle erforderlichen Informationen für die OVA-Bereitstellung ein, klicken Sie auf **Weiter** und klicken Sie dann auf **Fertig stellen**, um die OVA des VMware HCX-Connectors bereitzustellen.

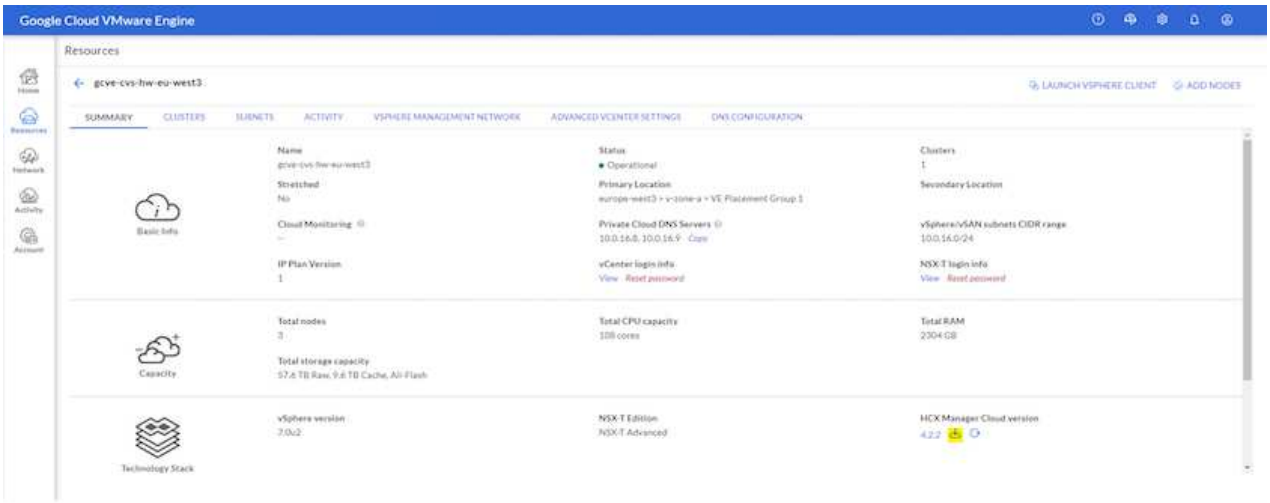
   Schalten Sie die virtuelle Appliance manuell ein.

Eine Schritt-für-Schritt-Anleitung finden Sie im "VMware HCX-Benutzerhandbuch".

Schritt 3: HCX Connector mit dem Lizenzschlüssel aktivieren

Nachdem Sie den VMware HCX Connector OVA vor Ort bereitgestellt und das Gerät gestartet haben, führen Sie die folgenden Schritte aus, um den HCX Connector zu aktivieren. Generieren Sie den Lizenzschlüssel aus dem Google Cloud VMware Engine Portal und aktivieren Sie ihn im VMware HCX Manager.

1. Klicken Sie im VMware Engine-Portal auf Ressourcen, wählen Sie die Private Cloud und **Klicken Sie auf das Download-Symbol unter HCX Manager Cloud Version**
   .



   Öffnen Sie die heruntergeladene Datei und kopieren Sie die Zeichenfolge für den Lizenzschlüssel.

2. Melden Sie sich beim lokalen VMware HCX Manager unter an "https://hcxmanagerIP:9443" Administratordaten werden verwendet.

   > Verwenden Sie die hcxmanagerIP und das Passwort, das während der OVA-Bereitstellung definiert wurde.

3. Geben Sie in der Lizenzierung den aus Schritt 3 kopierten Schlüssel ein und klicken Sie auf **Aktivieren**.

   > Der HCX-Connector sollte über einen Internetzugang verfügen.

4. Geben Sie unter **Datacenter Location** den nächstgelegenen Standort für die Installation des VMware HCX Managers vor Ort an. Klicken Sie Auf **Weiter**.
5. Aktualisieren Sie unter **Systemname** den Namen und klicken Sie auf **Weiter**.
6. Klicken Sie Auf **Ja, Weiter**.
7. Geben Sie unter **Connect Your vCenter** den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des vCenter Servers und die entsprechenden Anmeldeinformationen an und klicken Sie auf **Continue**.

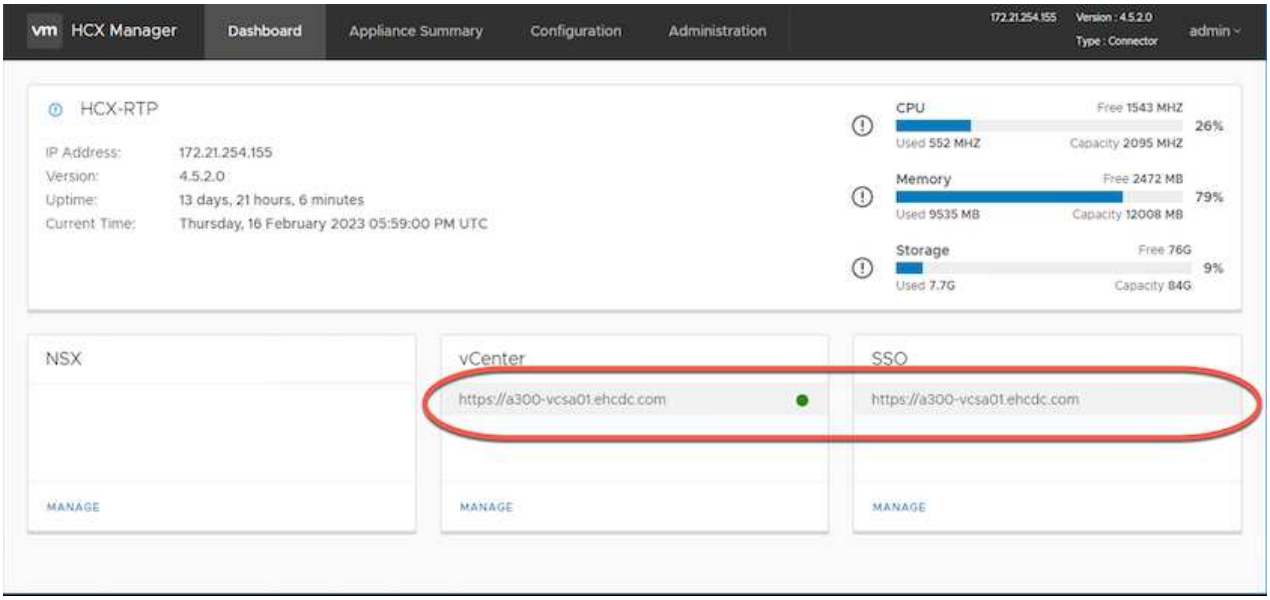
   > Verwenden Sie den FQDN, um Verbindungsprobleme später zu vermeiden.

8. Geben Sie unter **SSO/PSC** konfigurieren den (PSC) FQDN oder die IP-Adresse des Plattform-Services-Controllers an und klicken Sie auf **Weiter**.

Geben Sie für Embedded PSC den VMware vCenter Server FQDN oder die IP-Adresse ein.

9. Überprüfen Sie, ob die eingegebenen Informationen korrekt sind, und klicken Sie auf **Neustart**.
10. Nach dem Neustart der Dienste wird vCenter Server auf der angezeigten Seite grün angezeigt. Sowohl vCenter Server als auch SSO müssen über die entsprechenden Konfigurationsparameter verfügen, die mit der vorherigen Seite übereinstimmen sollten.

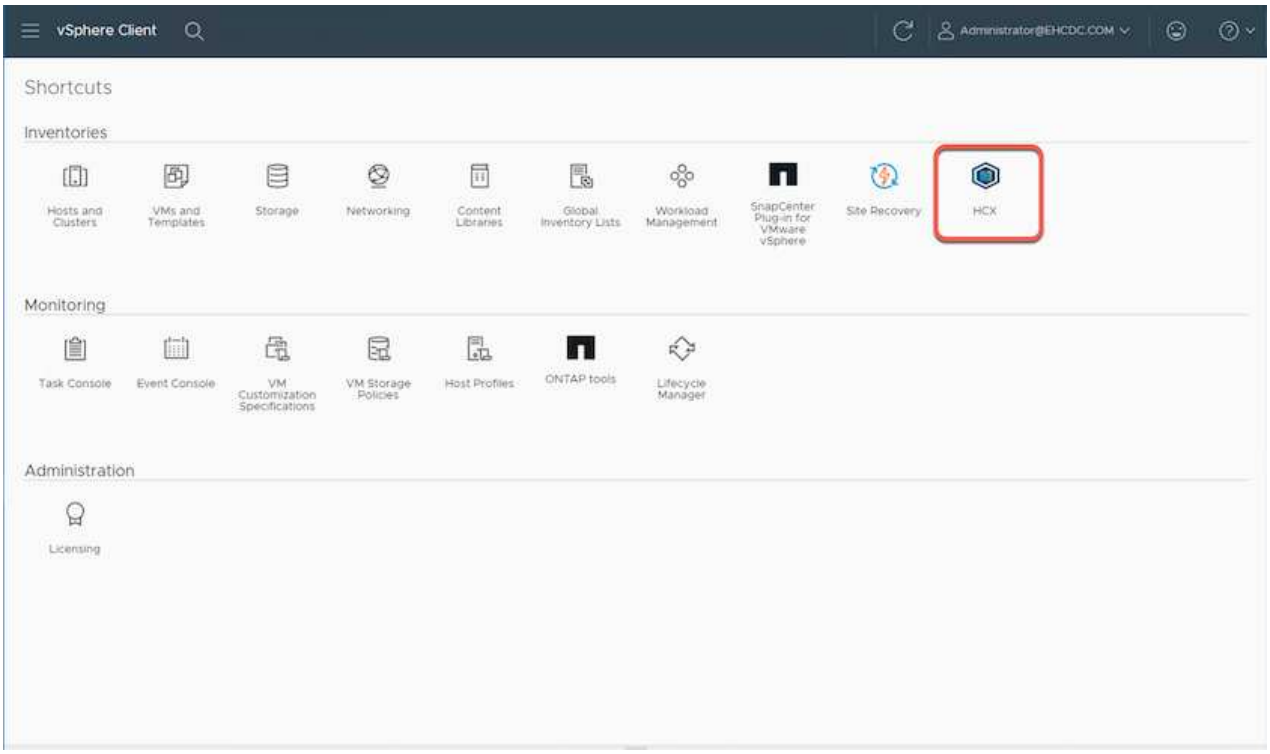
Dieser Vorgang dauert etwa 10 bis 20 Minuten, und das Plug-in wird dem vCenter Server hinzugefügt.



Schritt 4: Verbinden Sie den VMware HCX Connector vor Ort mit der Google Cloud VMware Engine HCX Cloud Manager

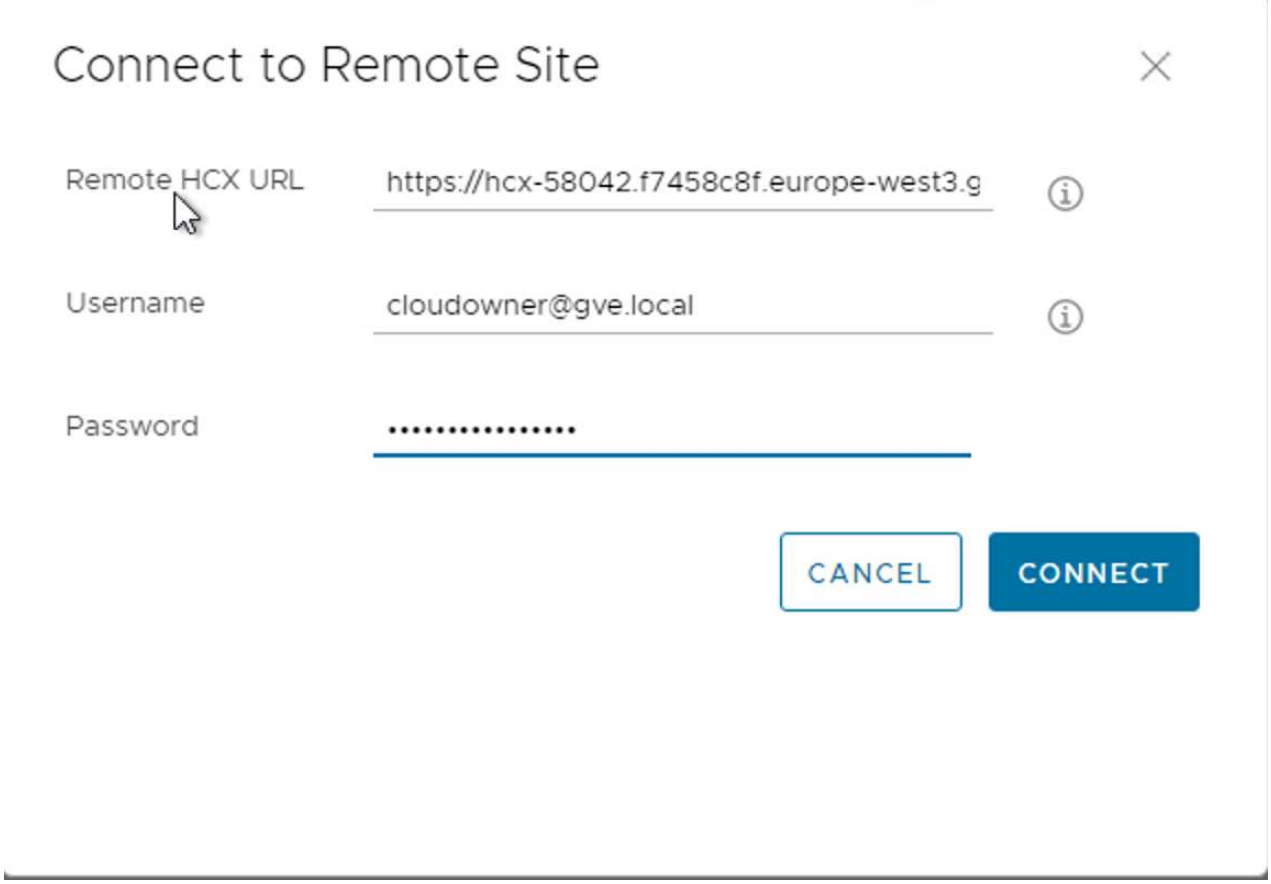
Nachdem HCX Connector im lokalen vCenter bereitgestellt und konfiguriert wurde, stellen Sie eine Verbindung zum Cloud Manager her, indem Sie die Paarung hinzufügen. Gehen Sie wie folgt vor, um die Standortpaarung zu konfigurieren:

1. Um ein Standortpaar zwischen der lokalen vCenter Umgebung und der Google Cloud VMware Engine SDDC zu erstellen, melden Sie sich beim lokalen vCenter Server an und greifen Sie auf das neue HCX vSphere Web Client Plug-in zu.



2. Klicken Sie unter Infrastruktur auf **Site Pairing hinzufügen**.

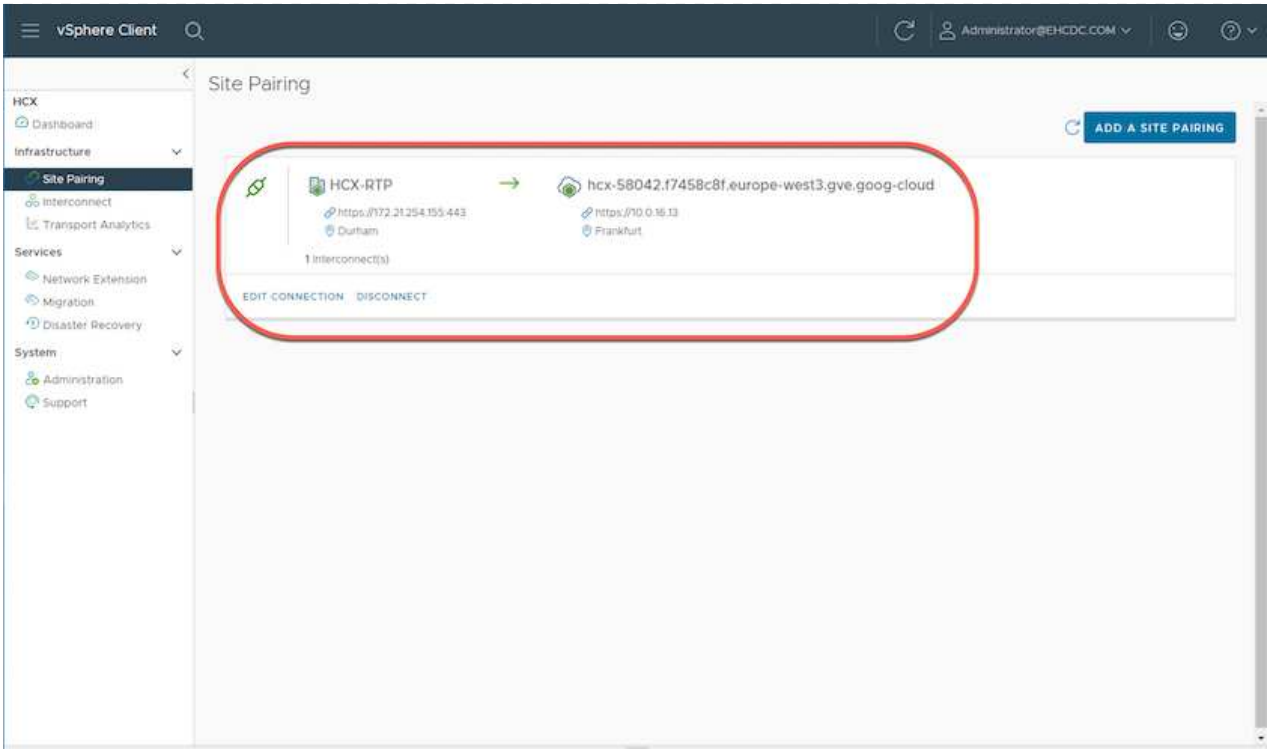
> Geben Sie die URL oder IP-Adresse des Google Cloud VMware Engine HCX Cloud Manager und die Anmeldedaten für Benutzer mit Cloud-Owner-Rollenberechtigungen für den Zugriff auf die private Cloud ein.



3. Klicken Sie Auf **Verbinden**.

> VMware HCX Connector muss über Port 443 zu HCX Cloud Manager IP weiterleiten können.

4. Nach der Erstellung der Kopplung steht die neu konfigurierte Standortpairing auf dem HCX Dashboard zur Verfügung.

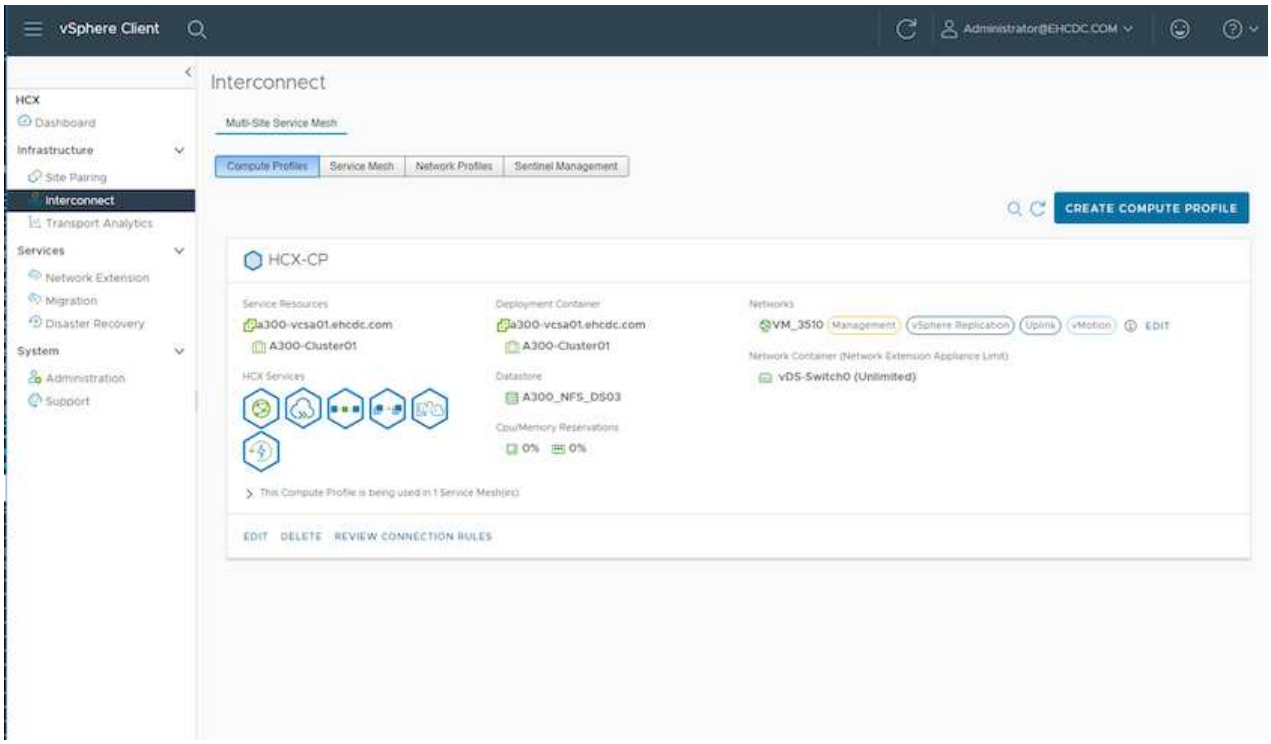

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
1 Interconnect(s)
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud
https://10.0.16.13
Frankfurt
EDIT CONNECTION
DISCONNECT

Schritt 5: Netzwerkprofil, Computing-Profil und Service-Mesh konfigurieren

Die VMware HCX Interconnect Service Appliance bietet Replizierungs- und vMotion-basierte Migrationsfunktionen über das Internet und private Verbindungen zum Zielstandort. Das Interconnect bietet Verschlüsselung, Traffic Engineering und VM-Mobilität. Um eine Interconnect Service Appliance zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie unter Infrastruktur die Option **Interconnect > Multi-Site Service Mesh > Compute Profiles > Create Compute Profile** aus.

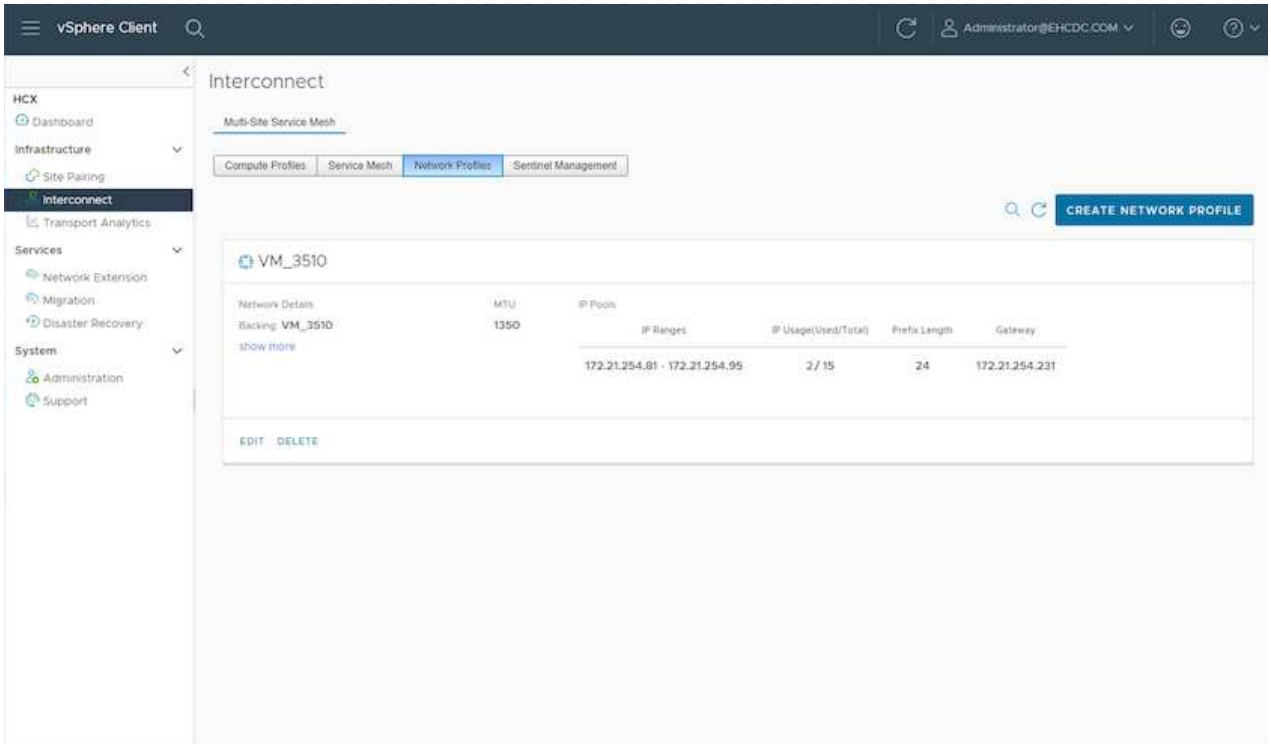
   Die Computing-Profile definieren die Implementierungsparameter einschließlich der Appliances, die bereitgestellt werden und welche Teile des VMware Datacenters für den HCX-Service verfügbar sind.



2. Erstellen Sie nach dem Erstellen des Rechenprofils die Netzwerkprofile, indem Sie **Multi-Site Service Mesh > Netzwerkprofile > Netzwerkprofil erstellen** auswählen.

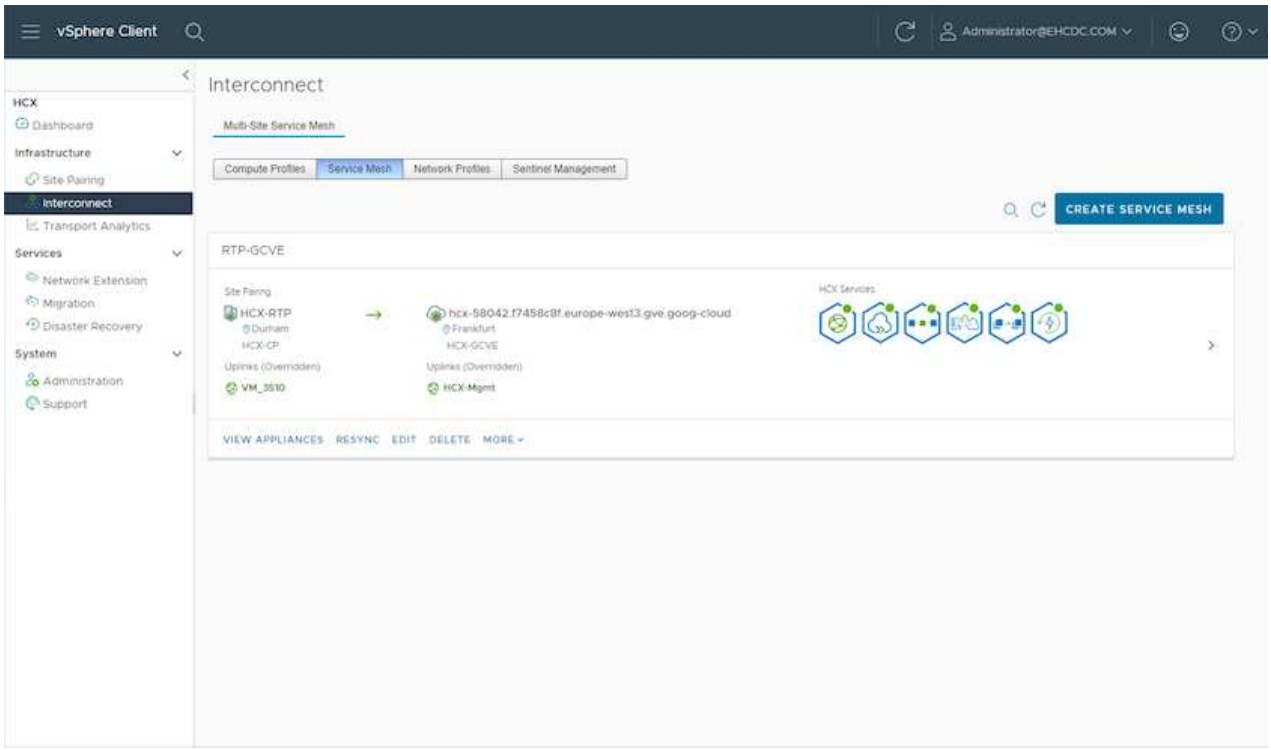
   Das Netzwerkprofil definiert einen Bereich von IP-Adressen und Netzwerken, die von HCX für seine virtuellen Appliances verwendet werden.

   Für diesen Schritt werden mindestens zwei IP-Adressen benötigt. Diese IP-Adressen werden den Interconnect Appliances vom Managementnetzwerk zugewiesen.

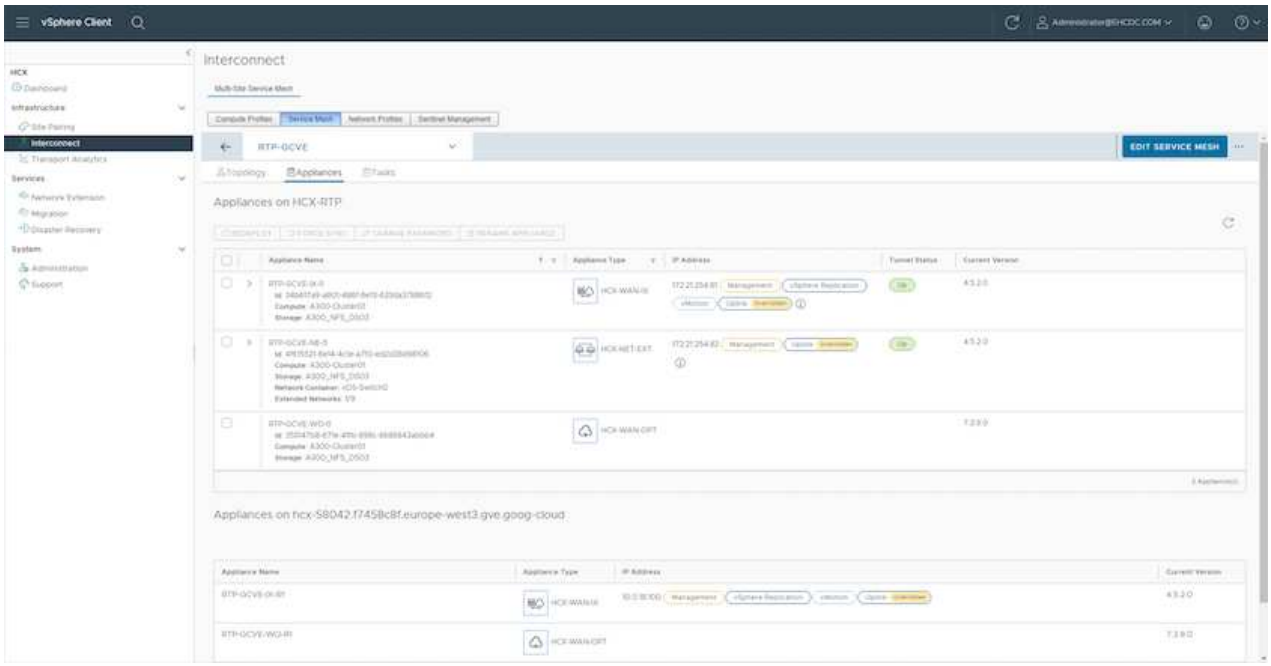


3. Derzeit wurden die Computing- und Netzwerkprofile erfolgreich erstellt.
4. Erstellen Sie das Service Mesh, indem Sie in der Option **Interconnect** die Registerkarte **Service Mesh** auswählen und die On-Premises- und GCVE SDDC-Sites auswählen.
5. Das Service Mesh gibt ein lokales und entferntes Compute- und Netzwerkprofilpaar an.

> Im Rahmen dieses Prozesses werden die HCX-Appliances sowohl an den Quell- als auch an den Zielstandorten bereitgestellt und automatisch konfiguriert, um eine sichere Transportstruktur zu erstellen.



6. Dies ist der letzte Konfigurationsschritt. Die Implementierung sollte also fast 30 Minuten dauern. Nach der Konfiguration des Service-Mesh ist die Umgebung bereit, wobei die IPsec-Tunnel erfolgreich erstellt wurden, um die Workload-VMs zu migrieren.



Schritt 6: Migration von Workloads

Workloads können mithilfe verschiedener VMware HCX Migrationstechnologien bidirektional zwischen lokalen und GCVE SDDCs migriert werden. VMs können mithilfe von mehreren Migrationstechnologien wie HCX Bulk Migration, HCX vMotion, HCX Cold Migration, HCX Replication Assisted vMotion (erhältlich mit HCX Enterprise Edition) und HCX OS Assisted Migration (erhältlich mit der HCX Enterprise Edition) in und von VMware HCX Enterprise Edition verschoben werden.

Weitere Informationen zu verschiedenen HCX-Migrationsmechanismen finden Sie unter "Migrationstypen von VMware HCX".

Die HCX-IX Appliance verwendet den Mobility Agent Service, um vMotion-, Cold- und Replication Assisted vMotion-Migrationen (RAV) durchzuführen.

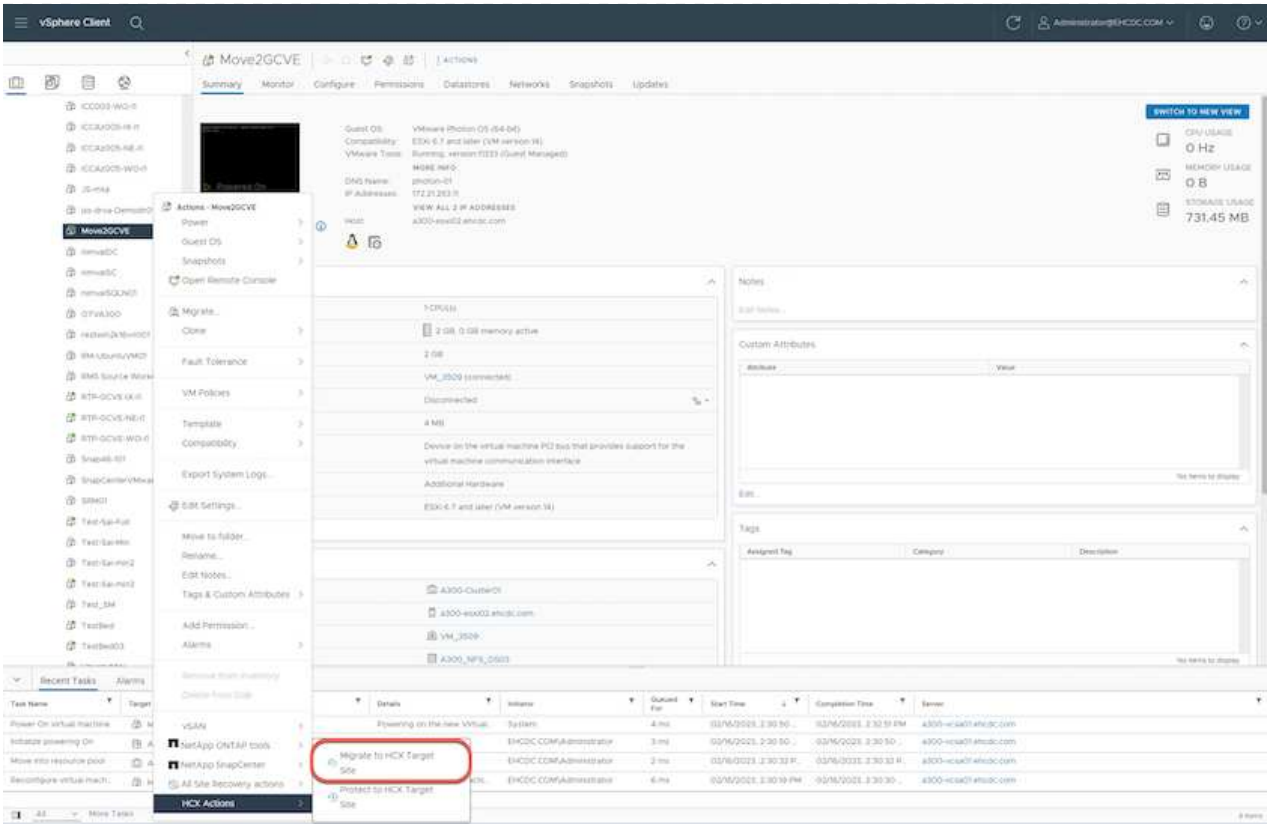
> Die HCX-IX Appliance fügt den Mobility Agent-Service als Hostobjekt im vCenter Server hinzu. Der auf diesem Objekt angezeigte Prozessor, Arbeitsspeicher, Speicher und Netzwerkressourcen stellen nicht den tatsächlichen Verbrauch des physischen Hypervisors dar, der die IX-Appliance hostet.

HCX vMotion

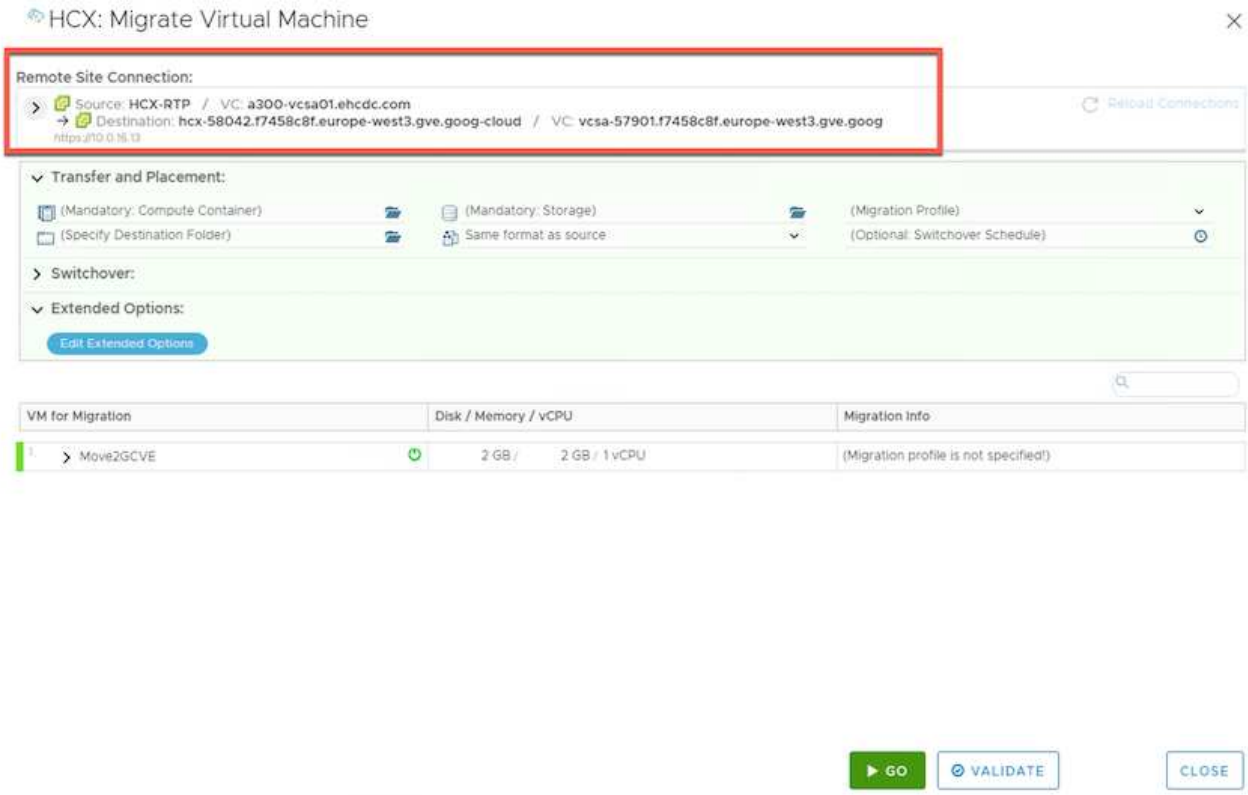
In diesem Abschnitt wird der HCX vMotion-Mechanismus beschrieben. Diese Migrationstechnologie verwendet das VMware vMotion Protokoll für die Migration einer VM zu GCVE. Die vMotion Migrationsoption wird verwendet, um den VM-Status einer einzelnen VM gleichzeitig zu migrieren. Während dieser Migrationsmethode kommt es zu keiner Serviceunterbrechung.

> Eine Netzwerkerweiterung sollte vorhanden sein (für die Portgruppe, an der die VM angeschlossen ist), um die VM zu migrieren, ohne dass eine IP-Adressänderung notwendig ist.

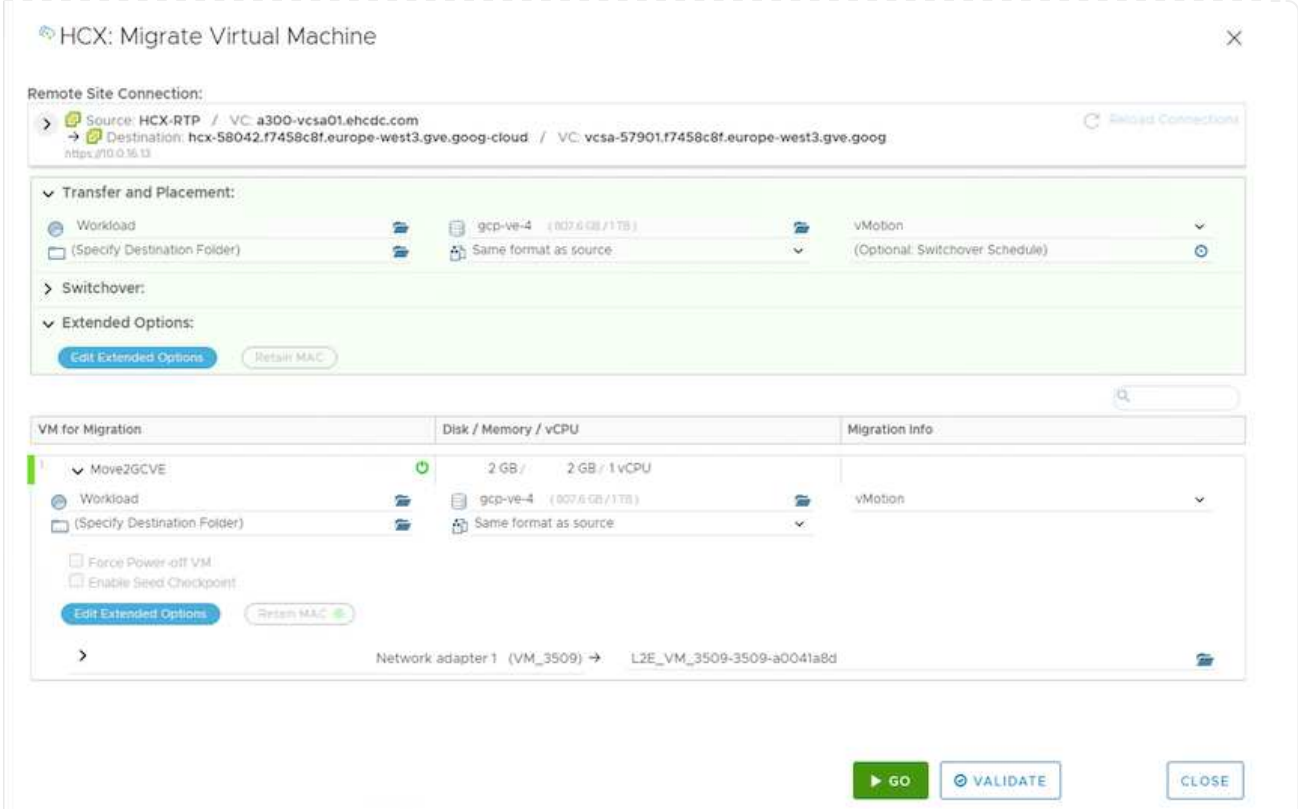
1. Wechseln Sie vom lokalen vSphere-Client zum Inventory, klicken Sie mit der rechten Maustaste auf die zu migrierende VM und wählen Sie HCX Actions > Migrate to HCX Target Site aus.



2. Wählen Sie im Assistenten zum Migrieren von Virtual Machine die Remote-Standortverbindung (Ziel-GCVE) aus.



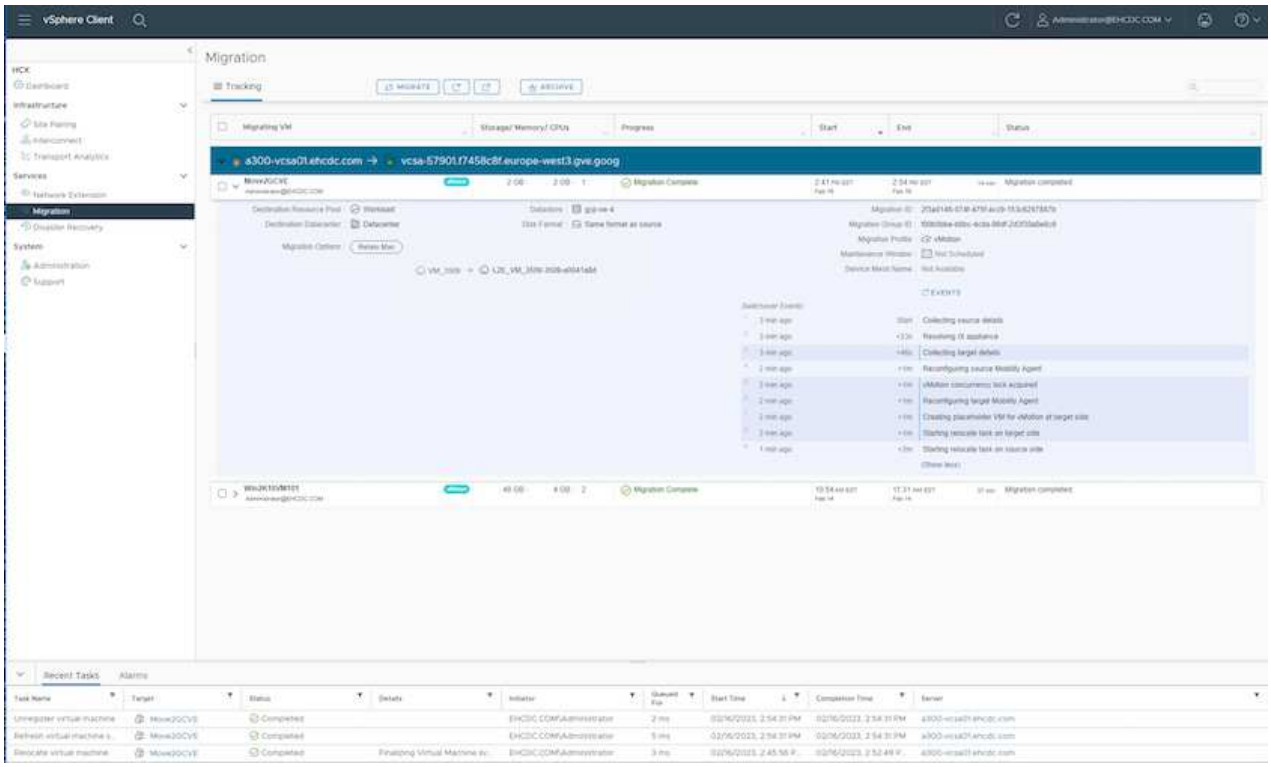
3. Aktualisieren Sie die Pflichtfelder (Cluster, Speicher und Zielnetzwerk), und klicken Sie auf Validieren.



4. Klicken Sie nach Abschluss der Validierungsprüfungen auf Los, um die Migration zu starten.

> Der vMotion Transfer erfasst den aktiven VM-Speicher, seinen Ausführungszustand, seine IP-Adresse und seine MAC-Adresse. Weitere Informationen zu den Anforderungen und Einschränkungen von HCX vMotion finden Sie unter "VMware HCX vMotion und „Cold Migration“ verstehen".

5. Über das Dashboard HCX > Migration können Sie den Fortschritt und den Abschluss von vMotion überwachen.



Der CVS Ziel-NFS-Datastore sollte über ausreichend Speicherplatz für die Migration verfügen.

Schlussfolgerung

Egal, ob Sie auf All-Cloud- oder Hybrid-Cloud-Umgebungen oder Daten auf Storage eines beliebigen Typs oder Anbieters vor Ort abzielen – Cloud Volume Service und HCX bieten hervorragende Optionen für die Implementierung und Migration der Applikations-Workloads und senken gleichzeitig die TCO, indem die Datenanforderungen nahtlos auf die Applikationsebene reduziert werden. Wie auch immer der Anwendungsfall aussieht: Die Google Cloud VMware Engine und Cloud Volume Service sorgen für die schnelle Realisierung der Cloud-Vorteile, eine konsistente Infrastruktur und Abläufe vor Ort und in mehreren Clouds, bidirektionale Workload-Portabilität und Kapazität und Performance der Enterprise-Klasse. Es handelt sich dabei um denselben bekannten Prozess und dieselben Verfahren, die zum Verbinden des Storage und zur Migration von VMs mithilfe von VMware vSphere Replication, VMware vMotion oder sogar NFS (Network File Copy) verwendet werden.

Erkenntnisse Aus

Zu den wichtigsten Punkten dieses Dokuments gehören:

- Sie können Cloud Volume Service jetzt als Datastore auf dem Google Cloud VMware Engine SDDC nutzen.
- Daten lassen sich problemlos von On-Premises- zu Cloud Volume Service-Datastores migrieren.
- Erweitern und verkleinern Sie den Cloud Volume Service-Datastore einfach, um die Kapazitäts- und Performance-Anforderungen während der Migration zu erfüllen.

Videos von Google und VMware als Referenz

Von Google

- "HCX Connector mit GCVE bereitstellen"
- "Konfigurieren Sie HCX ServiceMesh mit GCVE"
- "VM mit HCX auf GCVE migrieren"

Von VMware

- "HCX Connector-Bereitstellung für GCVE"
- "HCX ServiceMesh-Konfiguration für GCVE"
- "HCX-Workload-Migration zu GCVE"

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie unter den folgenden Links:

- Dokumentation der Google Cloud VMware Engine

  "https://cloud.google.com/vmware-engine/docs/overview"

- Dokumentation des Cloud Volume Service

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes"

- VMware HCX-Benutzerhandbuch

  "https://docs.vmware.com/en/VMware-HCX/index.html"

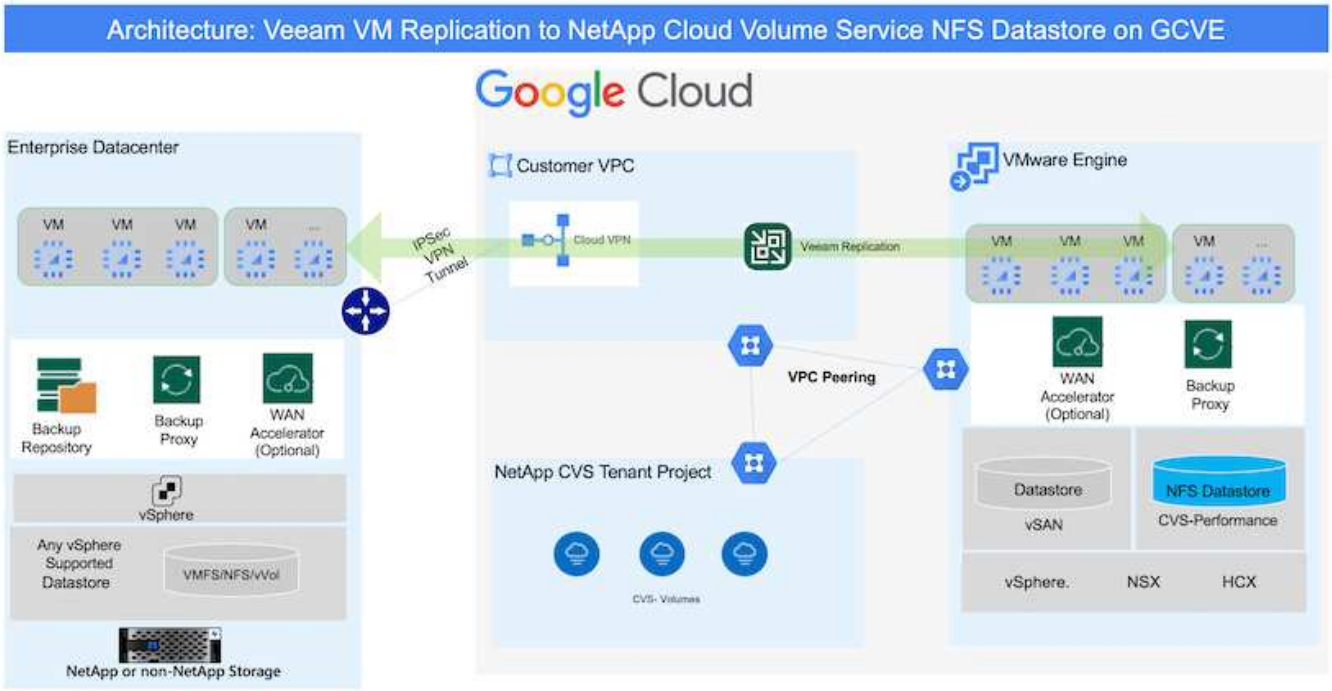
VM-Migration zu NetApp Cloud Volume Service NFS-Datastore auf Google Cloud VMware Engine mithilfe der Veeam Replizierungsfunktion

Überblick

Autoren: Suresh ThopPay, NetApp

VM-Workloads, die auf VMware vSphere ausgeführt werden, können mithilfe der Veeam Replication-Funktion in die Google Cloud VMware Engine (GCVE) migriert werden.

Dieses Dokument bietet einen Schritt-für-Schritt-Ansatz für die Einrichtung und Durchführung der VM-Migration mit NetApp Cloud Volume Service, Veeam und der Google Cloud VMware Engine (GCVE).



Voraussetzungen

In diesem Dokument wird vorausgesetzt, dass Sie entweder Google Cloud VPN oder Cloud Interconnect oder eine andere Netzwerkoption einsetzen, um die Netzwerkverbindung von bestehenden vSphere Servern zur Google Cloud VMware Engine herzustellen.

> Es gibt mehrere Optionen, um On-Premises-Datacenter mit Google Cloud zu verbinden, was uns daran hindert, einen bestimmten Workflow in diesem Dokument zu beschreiben. Siehe "Google Cloud-Dokumentation" Für die geeignete On-Premises-zu-Google-Verbindungsmethode.

Bereitstellen der Migrationslösung

Übersicht Zur Lösungsimplementierung

1. Stellen Sie sicher, dass der NFS-Datastore aus dem NetApp-Cloud-Volume-Service in GCVE vCenter gemountet ist.
2. Sicherstellen, dass Veeam Backup Recovery in vorhandener VMware vSphere-Umgebung implementiert wird
3. Erstellen Sie einen Replikationsjob, um die Replikation virtueller Maschinen auf die Instanz der Google Cloud VMware Engine zu starten.
4. Führen Sie ein Failover des Veeam Replication Job durch.
5. Führen Sie ein Permanent Failover auf Veeam durch.

Einzelheiten Zur Bereitstellung

Stellen Sie sicher, dass der NFS-Datastore aus dem NetApp-Cloud-Volume-Service in GCVE vCenter gemountet ist

Melden Sie sich bei GCVE vCenter an, und stellen Sie sicher, dass ein NFS-Datastore mit ausreichend

Speicherplatz verfügbar ist.
Falls nicht, wenden Sie sich bitte an "Mounten Sie NetApp CVS als NFS-Datastore in GCVE"

Sicherstellen, dass Veeam Backup Recovery in vorhandener VMware vSphere-Umgebung implementiert wird

Weitere Informationen finden Sie unter "Veeam Replizierungskomponenten" Dokumentation zur Installation der erforderlichen Komponenten.

Erstellen Sie einen Replikationsjob, um die Replikation virtueller Maschinen auf die Instanz der Google Cloud VMware Engine zu starten.

VCenter vor Ort und GCVE vCenter müssen bei Veeam registriert werden. "VSphere VM Replication Job einrichten"
Hier ist ein Video, in dem erklärt wird, wie
"Konfigurieren Sie Den Replikationsjob".

> Die ReplikatVM kann eine andere IP-Adresse als die Quell-VM haben und kann auch mit einer anderen Portgruppe verbunden werden. Weitere Informationen finden Sie im Video oben.

Führen Sie ein Failover des Veeam Replication Job durch

Führen Sie zum Migrieren von VMs aus "Führen Sie Ein Failover Durch"

Führen Sie ein Permanent Failover auf Veeam durch.

Um GCVE als Ihre neue Quellumgebung zu behandeln, führen Sie aus "Permanenter Failover"

Vorteile dieser Lösung

- Die vorhandene Veeam Backup-Infrastruktur kann für die Migration genutzt werden.
- Veeam Replication ermöglicht das Ändern von VM-IP-Adressen am Zielstandort.
- Vorhandene Daten, die außerhalb von Veeam repliziert wurden (wie replizierte Daten von BlueXP), können neu zugeordnet werden.
- Kann unterschiedliche Netzwerk-Portgruppen am Zielstandort angeben.
- Kann die Reihenfolge der VMs angeben, die eingeschaltet werden sollen.
- Verwendet VMware Change Block Tracking, um die Datenmenge zu minimieren, die über WAN gesendet werden soll.
- Möglichkeit zum Ausführen von Pre- und Post-Skripten für die Replizierung.
- Möglichkeit zur Ausführung von Pre-und Post-Skripten für Snapshots.

Regionale Verfügbarkeit – ergänzender NFS-Datastore für Google Cloud Platform (GCP)

Zusätzlicher NFS-Datastore für GCVE wird von NetApp Cloud Volume Service unterstützt.

Für den GCVE NFS Datastore können nur CVS-Performance Volumes verwendet werden. Informationen zum verfügbaren Speicherort finden Sie unter "Globale Regionalkarte"

Google Cloud VMware Engine ist an folgenden Standorten verfügbar

asia-northeast1 > v-zone-a > VE Placement Group 1
asia-northeast1 > v-zone-a > VE Placement Group 2
asia-south1 > v-zone-a > VE Placement Group 2
asia-south1 > v-zone-a > VE Placement Group 1
asia-southeast1 > v-zone-a > VE Placement Group 1
asia-southeast1 > v-zone-a > VE Placement Group 2
australia-southeast1 > v-zone-b > VE Placement Group 1
australia-southeast1 > v-zone-a > VE Placement Group 1
australia-southeast1 > v-zone-b > VE Placement Group 2
australia-southeast1 > v-zone-a > VE Placement Group 2
europe-west2 > v-zone-a > VE Placement Group 2
europe-west2 > v-zone-a > VE Placement Group 1
europe-west3 > v-zone-b > VE Placement Group 2
europe-west3 > v-zone-a > VE Placement Group 3
europe-west3 > v-zone-a > VE Placement Group 4
europe-west3 > v-zone-b > VE Placement Group 1
europe-west3 > v-zone-a > VE Placement Group 2
europe-west3 > v-zone-a > VE Placement Group 1
europe-west4 > v-zone-a > VE Placement Group 2
europe-west4 > v-zone-a > VE Placement Group 1
europe-west6 > v-zone-a > VE Placement Group 1
europe-west8 > v-zone-a > VE Placement Group 1
northamerica-northeast1 > v-zone-a > VE Placement Group 1
northamerica-northeast1 > v-zone-a > VE Placement Group 2
northamerica-northeast2 > v-zone-a > VE Placement Group 2
northamerica-northeast2 > v-zone-a > VE Placement Group 1
southamerica-east1 > v-zone-a > VE Placement Group 1
southamerica-east1 > v-zone-a > VE Placement Group 2
us-central1 > v-zone-a > VE Placement Group 2
us-central1 > v-zone-a > VE Placement Group 5
us-central1 > v-zone-a > VE Placement Group 1
us-central1 > v-zone-a > VE Placement Group 3
us-east4 > v-zone-a > VE Placement Group 5
us-east4 > v-zone-a > VE Placement Group 10
us-east4 > v-zone-a > VE Placement Group 6
us-east4 > v-zone-a > VE Placement Group 3
us-east4 > v-zone-b > VE Placement Group 5
us-east4 > v-zone-a > VE Placement Group 1
us-east4 > v-zone-b > VE Placement Group 1
us-east4 > v-zone-a > VE Placement Group 4
us-east4 > v-zone-b > VE Placement Group 6
us-east4 > v-zone-a > VE Placement Group 2
us-west2 > v-zone-a > VE Placement Group 3
us-west2 > v-zone-a > VE Placement Group 4
us-west2 > v-zone-a > VE Placement Group 5
us-west2 > v-zone-a > VE Placement Group 2
us-west2 > v-zone-a > VE Placement Group 1
us-west2 > v-zone-a > VE Placement Group 6

Um die Latenz zu minimieren, sollten sich NetApp CVS Volume und GCVE, wo Sie das Volume mounten möchten, in derselben Verfügbarkeitszone befinden.
Arbeiten Sie mit Google und NetApp Solution Architects zusammen, um Verfügbarkeit und TCO-Optimierung zu optimieren.

Sicherheitsüberblick – NetApp Cloud Volumes Service (CVS) in Google Cloud

TR-4918: Sicherheitsübersicht - NetApp Cloud Volumes Service in Google Cloud

Oliver Krause, Justin Parisi, NetApp

Dokumentumfang

Die Sicherheit – insbesondere in der Cloud, wo die Infrastruktur außerhalb der Kontrolle der Storage-Administratoren liegt – ist entscheidend, wenn es um die Übergabe der Daten an die von Cloud-Providern angebotenen Service-Angebote geht. Dieses Dokument bietet einen Überblick über die Sicherheitsangebote von NetApp "Cloud Volumes Service bietet in Google Cloud".

Zielgruppe

Die Zielgruppe dieses Dokuments umfasst die folgenden Rollen:

- Cloud Provider
- Storage-Administratoren
- Storage-Architekten
- Feldressourcen
- Geschäftliche Entscheidungsträger

Wenn Sie Fragen zum Inhalt dieses technischen Berichts haben, finden Sie im Abschnitt "„Kontaktieren Sie uns.“"

Abkürzung	Definition
CVS-SW	Cloud Volumes Service, Diensttyp CVS
CVS-Performance	Cloud Volume Service, Servicetyp CVS-Performance
PSA	

Wie Cloud Volumes Service in Google Cloud Ihre Daten sichert

Cloud Volumes Service in Google Cloud bietet zahlreiche Möglichkeiten zur nativen Sicherung Ihrer Daten.

Sichere Architektur und Mandantenmodell

Cloud Volumes Service bietet eine sichere Architektur in Google Cloud, indem das Service-Management (Kontrollebene) und der Datenzugriff (Datenebene) über verschiedene Endpunkte segmentiert werden, sodass keine Auswirkung auf den anderen Endpunkte besteht (siehe Abschnitt "„Cloud Volumes Service Architecture“"). Sie verwendet Googles "Zugang zu privaten Services" (PSA) Framework zur Bereitstellung des

Service. In diesem Rahmen wird zwischen dem von NetApp bereitgestellten und betriebenen Service-Produzenten unterschieden. Dabei handelt es sich um eine Virtual Private Cloud (VPC) in einem Kundenprojekt, in dem die Clients gehostet werden, die auf Cloud Volumes Service-Dateifreigaben zugreifen möchten.

In dieser Architektur finden Mandanten (siehe Abschnitt "„Tenancy model“") Sind als Google Cloud-Projekte definiert, die vollständig voneinander getrennt sind, es sei denn, der Benutzer hat ausdrücklich eine Verbindung. Mandanten ermöglichen durch die Cloud Volumes Service Volume-Plattform die vollständige Isolierung von Daten-Volumes, externen Name Services und anderen wichtigen Lösungselementen von anderen Mandanten. Da die Cloud Volumes Service Plattform über VPC Peering verbunden ist, gilt diese Isolierung auch für die IT. Sie können die Freigabe von Cloud Volumes Service Volumes zwischen mehreren Projekten mithilfe einer gemeinsam genutzten VPC aktivieren (siehe Abschnitt "„Gemeinsame VPCs“"). Zugriffssteuerung kann auf SMB-Freigaben und NFS-Exporte angewendet werden, um zu beschränken, wer bzw. welche Datensätze angezeigt oder geändert werden können.

Starkes Identitätsmanagement für die Kontrollebene

In der Kontrollebene, auf der die Cloud Volumes Service-Konfiguration stattfindet, wird das Identitätsmanagement mit verwaltet "Identitäts-Zugriffsmanagement (Identity Access Management, IAM)". IAM ist ein Standardservice, mit dem die Authentifizierung (Logins) und Autorisierung (Berechtigungen) für Google Cloud-Projektinstanzen gesteuert werden kann. Die gesamte Konfiguration erfolgt über Cloud Volumes Service APIs über einen sicheren HTTPS-Transport mithilfe der TLS 1.2-Verschlüsselung. Die Authentifizierung erfolgt über JWT-Token für zusätzliche Sicherheit. Die Google-Konsole-Benutzeroberfläche für Cloud Volumes Service übersetzt Benutzereingaben in Cloud Volumes Service-API-Aufrufe.

Sicherheitshärtung – Begrenzung von Angriffsflächen

Ein Teil der effektiven Sicherheit ist die Begrenzung der Anzahl der Angriffsflächen, die in einem Service verfügbar sind. Angriffsflächen können eine Vielzahl von Dingen umfassen, beispielsweise Daten im Ruhezustand, Übertragungs- und Logins während der Übertragung und die Datensätze selbst.

Ein Managed Service entfernt einige Angriffsflächen inhärent in seinem Design. Infrastruktur-Management, wie im Abschnitt beschrieben "„Service-Betrieb“," Wird von einem dedizierten Team durchgeführt und verringert automatisch die Anzahl der Male, die ein Mensch tatsächlich bei Konfigurationen berührt, wodurch die Anzahl vorsätzlicher und unbeabsichtigter Fehler reduziert wird. Die Netzwerkumgebung ist abgezäunt, sodass nur erforderliche Services aufeinander zugreifen können. Die Verschlüsselung wird in den Datenspeicher integriert. Cloud Volumes Service Administratoren benötigen lediglich die Datenebene Sicherheitsaspekte. Wenn Sie den Großteil der Verwaltung hinter einer API-Schnittstelle verbergen, wird die Sicherheit durch Begrenzung der Angriffsflächen erreicht.

Zero-Trust-Modell

In der Vergangenheit BESTAND DIE IT-Sicherheitsphilosophie darin, Vertrauen zu geben, zu verifizieren und zu manifestieren, dass sie sich ausschließlich auf externe Mechanismen (wie Firewalls und Intrusion Detection Systems) zur Minderung von Bedrohungen verlassen. Angriffe und Verstöße wurden jedoch entwickelt, um die Verifizierung in Umgebungen durch Phishing, Social Engineering, Bedrohungen von innen und andere Methoden zu umgehen, die die Verifizierung in Netzwerke und Verwüstung ermöglichen.

Zero Trust hat sich zu einer neuen Sicherheitsmethode entwickelt, wobei das aktuelle Mantra „Vertrauen Sie nichts, während Sie noch alles überprüfen“ ist. Daher ist standardmäßig kein Zugriff zulässig. Dieses Mantra wird auf verschiedene Arten durchgesetzt, darunter Standard-Firewalls und Intrusion Detection-Systeme (IDS) sowie folgende Methoden:

- Starke Authentifizierungsmethoden (z. B. AES-verschlüsselte Kerberos- oder JWT-Token)

- Einzelne, starke Identifikationsquellen (z. B. Windows Active Directory, Lightweight Directory Access Protocol (LDAP) und Google IAM)
- Netzwerksegmentierung und sichere Mandantenfähigkeit (standardmäßig sind nur Mandanten Zugriff erlaubt)
- Granulare Zugriffssteuerung mit den geringsten Zugriffsrichtlinien
- Kleine exklusive Listen von engagierten, vertrauenswürdigen Administratoren mit digitalen Audit- und Papiertrails

Cloud Volumes Service läuft in Google Cloud hält sich an das Zero-Trust-Modell durch die Umsetzung der "Vertrauen nichts, alles überprüfen" Haltung.

Verschlüsselung

Verschlüsselung von Daten im Ruhezustand (siehe Abschnitt "„Datenverschlüsselung im Ruhezustand“") Mit XTS-AES-256-Chiffren mit NetApp Volume Encryption (NVE) und im Flight mit "„SMB-Verschlüsselung“" Oder NFS Kerberos 5p-Support. Gut zu wissen, dass regionsübergreifende Replikationstransfers durch TLS 1.2-Verschlüsselung geschützt sind (siehe Abschnitt "„Regionenübergreifende Replikation“"). Darüber hinaus bietet Google Networking auch verschlüsselte Kommunikation (siehe Abschnitt "„Datenverschlüsselung während der Übertragung“") Für eine zusätzliche Schutzschicht gegen Angriffe. Weitere Informationen zur Transportverschlüsselung finden Sie im Abschnitt "„Google Cloud-Netzwerk“".

Datensicherung und Backups

Bei der Sicherheit geht es nicht nur um die Verhinderung von Angriffen. Es geht auch darum, wie wir nach Angriffen eine Wiederherstellung durchführen, wenn sie auftreten. Diese Strategie umfasst Datenschutz und -Backups. Cloud Volumes Service bietet Methoden zur Replizierung in andere Regionen bei Ausfällen (siehe Abschnitt "„Regionenübergreifende Replikation“") Oder wenn ein Datensatz von einem Ransomware-Angriff betroffen ist. Sie kann auch asynchrone Daten-Backups von Standorten außerhalb der Cloud Volumes Service Instanz mithilfe von durchführen "Cloud Volumes Service-Backup". Mit regelmäßigen Backups kann das Abmildern von Sicherheitsereignissen Zeit in Anspruch nehmen, Geld und Aufwand für Administratoren einsparen.

Schnelle Abwehr von Ransomware mit branchenführenden Snapshot Kopien

Zusätzlich zu Datensicherung und Backups unterstützt Cloud Volumes Service auch unveränderliche Snapshot Kopien (siehe Abschnitt "„Unveränderliche Snapshot Kopien“") Von Volumes, die eine Wiederherstellung nach Ransomware-Angriffen ermöglichen (siehe Abschnitt "„Service-Betrieb“"Innerhalb von Sekunden nach der Entdeckung des Problems und mit minimaler Unterbrechung. Die Recovery-Zeit und -Auswirkungen hängen vom Snapshot Zeitplan ab. Allerdings können Snapshot-Kopien erstellt werden, die bei Ransomware-Angriffen nur eine Stunde Deltawerte liefern. Snapshot Kopien haben nahezu unmerkliche Auswirkungen auf die Performance und Kapazitätsauslastung und stellen einen Ansatz mit niedrigem Risiko und hoher Rendite zum Schutz Ihrer Datensätze dar.

Sicherheitsüberlegungen und Angriffsflächen

Der erste Schritt zum Verständnis der Datensicherung besteht darin, die Risiken und potenziellen Angriffsflächen zu identifizieren.

Dazu gehören (aber nicht beschränkt auf) die folgenden:

- Administration und Anmeldung
- Daten im Ruhezustand

- Genutzte Daten
- Netzwerk und Firewalls
- Ransomware, Malware und Viren

Das Verständnis von Angriffsflächen kann Ihnen helfen, Ihre Umgebungen besser zu schützen. Cloud Volumes Service in Google Cloud berücksichtigt bereits viele dieser Themen und implementiert Sicherheitsfunktionen standardmäßig ohne administrative Eingriffe.

Sichere Anmeldungen sicherstellen

Bei der Sicherung Ihrer kritischen Infrastrukturkomponenten ist es von größter Wichtigkeit, sicherzustellen, dass nur genehmigte Benutzer sich einloggen und Ihre Umgebungen managen können. Wenn fehlerhafte Akteure die Anmeldedaten in Ihrem System verletzen, haben sie die Schlüssel zum Schloss und können alles tun, was sie wollen: Konfigurationen ändern, Volumes und Backups löschen, Backdoors erstellen oder Snapshot-Zeitpläne deaktivieren.

Cloud Volumes Service für Google Cloud bietet Schutz vor unautorisierten administrativen Anmeldungen durch den Ausfall von Storage als Service (StaaS). Cloud Volumes Service wird vom Cloud-Provider komplett gewartet, ohne dass eine externe Anmeldung verfügbar ist. Alle Setup- und Konfigurationsvorgänge sind vollautomatisiert, sodass ein Administrator in seltenen Fällen nie mit den Systemen interagieren muss.

Wenn Anmeldung erforderlich ist, sichert Cloud Volumes Service in Google Cloud Anmeldungen, indem eine sehr kurze Liste vertrauenswürdiger Administratoren geführt wird, die Zugriff haben, um sich bei den Systemen anzumelden. Diese Gatekeeping hilft, die Anzahl potenzieller schlechter Akteure mit Zugriff zu reduzieren. Darüber hinaus verbirgt das Google Cloud-Netzwerk die Systeme hinter Schichten der Netzwerksicherheit und legt nur das, was für die Außenwelt benötigt wird, offen. Weitere Informationen zur Google Cloud- und Cloud Volumes Service-Architektur finden Sie im Abschnitt "„Cloud Volumes Service Architecture“."

Cluster-Administration und Upgrades

Zu den zwei Bereichen mit potenziellen Sicherheitsrisiken zählen die Clusterverwaltung (was passiert, wenn ein schlechter Akteur Administratorzugriff hat) und Upgrades (was passiert, wenn ein Software-Image beeinträchtigt wird).

Sicherung der Storage-Administration

Der als Service bereitgestellte Storage beseitigt das zusätzliche Risiko, dass Administratoren diesem Zugriff nicht mehr an Anwender außerhalb des Cloud-Datacenters ausgesetzt sind. Stattdessen gilt die einzige Konfiguration für die Datenzugriffsebene durch Kunden. Jeder Mandant managt seine eigenen Volumes, und ein Mandant kann andere Cloud Volumes Service Instanzen nicht erreichen. Der Service wird durch Automatisierung gemanagt, wobei in einer sehr kleinen Liste vertrauenswürdiger Administratoren über die im Abschnitt behandelten Prozesse Zugriff auf die Systeme gewährt wird "„Service-Betrieb“."

Der Servicetyp CVS-Performance bietet regionenübergreifende Replizierung als Option zur Sicherung von Daten für eine andere Region bei Ausfall. In diesen Fällen kann ein Failover der Cloud Volumes Service in die nicht betroffene Region durchgeführt werden, um den Datenzugriff zu gewährleisten.

Service-Upgrades

Updates helfen, gefährdete Systeme zu schützen. Jedes Update bietet Verbesserungen der Sicherheit und Fehlerbehebungen zur Minimierung von Angriffsflächen. Software-Updates werden aus zentralen Repositorys heruntergeladen und validiert, bevor die Updates überprüft werden, ob offizielle Bilder verwendet werden und dass die Upgrades nicht durch fehlerhafte Akteure beeinträchtigt werden.

Mit Cloud Volumes Service werden Updates von den Cloud-Provider-Teams durchgeführt, die Risiken für Administratoren abschaffen, indem Experten versiert in Konfiguration und Upgrades sind, die den Prozess automatisiert und vollständig getestet haben. Upgrades werden unterbrechungsfrei durchgeführt und Cloud Volumes Service behält die neuesten Updates bei, um optimale Ergebnisse zu erzielen.

Informationen über das Administrator-Team, das diese Service-Upgrades durchführt, finden Sie im Abschnitt "„Service-Betrieb“."

Sicherheit von Daten im Ruhezustand

Die Verschlüsselung ruhender Daten ist wichtig, um sensible Daten bei Diebstahl, Rückgabe oder neuer Verwendung einer Festplatte zu schützen. Daten in Cloud Volumes Service werden mithilfe von softwarebasierter Verschlüsselung im Ruhezustand gesichert.

- Google-generierte Schlüssel werden für CVS-SW verwendet.
- Für die CVS-Performance werden die Schlüssel pro Volume in einem in Cloud Volumes Service integrierten Schlüsselmanager gespeichert, der mit NetApp ONTAP CryptoMod die AES-256-Verschlüsselung generiert. CryptoMod ist in der nach FIPS 140-2 validierten CMVP-Modulliste aufgeführt. Siehe "FIPS 140-2 Zertifikat #4144".

Im November 2021 wurde eine Vorschau auf die Funktionalität Customer-Managed Encryption (CMEK) für CVS-Performance bereitgestellt. Diese Funktionalität ermöglicht Ihnen die Verschlüsselung der Schlüssel pro Volume mit Master-Schlüsseln für einzelne Projekte und Regionen, die im Google Key Management Service (KMS) gehostet werden. KMS ermöglicht es Ihnen, externe Schlüsselmanager anzubinden.

Details zur Konfiguration von KMS für CVS-Performance finden Sie unter "Weitere Informationen finden Sie in der Cloud Volumes Service-Dokumentation".

Weitere Informationen zur Architektur finden Sie im Abschnitt "„Cloud Volumes Service Architecture“."

Sicherheit der aktiven Daten

Sie müssen nicht nur Daten im Ruhezustand sichern, sondern auch bei laufender Übertragung zwischen der Cloud Volumes Service Instanz und einem Client oder Replizierungsziel sichern können. Cloud Volumes Service bietet Verschlüsselung von Daten auf der Übertragungsstrecke über NAS-Protokolle. Dabei kommen Verschlüsselungsmethoden wie SMB-Verschlüsselung mit Kerberos, das Signing/Sealing von Paketen und NFS Kerberos 5p für die End-to-End-Verschlüsselung von Datentransfers zum Einsatz.

Die Replizierung von Cloud Volumes Service Volumes verwendet TLS 1.2, die von AES-GCM-Verschlüsselungsmethoden profitiert.

Die unsicheres in-Flight-Protokolle wie Telnet, NDMP usw. sind standardmäßig deaktiviert. DNS ist jedoch nicht durch Cloud Volumes Service verschlüsselt (keine DNS-sec-Unterstützung) und sollte, wenn möglich, mit externer Netzwerkverschlüsselung verschlüsselt werden. Siehe Abschnitt "„Datenverschlüsselung während der Übertragung“" Finden Sie weitere Informationen über die Sicherung Ihrer aktiven Daten.

Informationen zur Verschlüsselung von NAS-Protokollen finden Sie im Abschnitt "„NAS-Protokolle“."

Benutzer und Gruppen für NAS-Berechtigungen

Bei der Sicherung Ihrer Daten in der Cloud ist eine ordnungsgemäße Benutzer- und Gruppenauthentifizierung erforderlich, wobei die Benutzer, die auf die Daten zugreifen, als echte Benutzer in der Umgebung überprüft werden und die Gruppen gültige Benutzer enthalten. Diese Benutzer und Gruppen bieten ersten Zugriff auf Freigabe und Export sowie Berechtigungsvalidierung für Dateien und Ordner im Speichersystem.

Cloud Volumes Service verwendet die standardmäßige, auf Active Directory basierende Windows-Benutzer- und Gruppenauthentifizierung für SMB-Freigaben und Windows-artige Berechtigungen. Der Service kann auch UNIX Identitätsanbieter wie LDAP für UNIX Benutzer und Gruppen für NFS-Exporte, NFSv4 ID-Validierung, Kerberos-Authentifizierung und NFSv4 ACLs nutzen.

> Derzeit wird mit Cloud Volumes Service nur Active Directory LDAP zur LDAP-Funktionalität unterstützt.

Erkennung, Verhinderung und Minimierung von Ransomware, Malware und Viren

Ransomware, Malware und Viren sind für Administratoren eine persistente Bedrohung. Die Erkennung, das Vorbeugen und die Minimierung dieser Bedrohungen steht für Unternehmen immer im Mittelpunkt. Ein einzelnes Ransomware-Ereignis auf einem kritischen Datensatz kann potenziell Millionen US-Dollar kosten. Daher ist es vorteilhaft, alles zu tun, um das Risiko zu minimieren.

Obwohl Cloud Volumes Service derzeit nicht schließt native Detection oder Prävention Maßnahmen, wie Virenschutz oder "Automatische Ransomware-Erkennung", Es gibt Möglichkeiten, nach einem Ransomware-Ereignis schnell wiederherzustellen, indem es regelmäßige Snapshot-Zeitpläne ermöglicht. Snapshot-Kopien sind unveränderliche und schreibgeschützte Verweise auf geänderte Blöcke im Filesystem, werden praktisch sofort erzeugt, haben minimale Auswirkungen auf die Performance und verbrauchen nur Speicherplatz, wenn Daten geändert oder gelöscht werden. Sie können Zeitpläne für Snapshot Kopien einrichten, die auf Ihre gewünschte akzeptable Recovery Point Objective (RPO)/Recovery Time Objective (RTO) abgestimmt sind und bis zu 1,024 Snapshot Kopien pro Volume aufbewahren.

Snapshot Support ist ohne zusätzliche Kosten enthalten (Storage-Kosten für veränderte Blöcke/Daten, die von Snapshot Kopien aufbewahrt Cloud Volumes Service werden) und kann bei einem Ransomware-Angriff genutzt werden, um ein Rollback auf eine Snapshot Kopie vor dem Angriff durchzuführen. Snapshot Wiederherstellungen dauern nur wenige Sekunden und Daten können wieder wie gewohnt bereit sein. Weitere Informationen finden Sie unter "NetApp Lösung gegen Ransomware".

Die Auswirkungen von Ransomware auf Ihr Unternehmen zu verhindern, ist ein mehrschichtiger Ansatz erforderlich, der einen oder mehrere der folgenden Elemente umfasst:

- Endpoint-Schutz
- Schutz vor externen Bedrohungen durch Netzwerk-Firewalls
- Erkennung von Datenanomalien
- Mehrere Backups (vor Ort und extern) kritischer Datensätze
- Regelmäßige Restore-Tests von Backups
- Unveränderliche schreibgeschützte NetApp Snapshot Kopien
- Multi-Faktor-Authentifizierung für kritische Infrastrukturen
- Sicherheitsprüfungen von Systemanmeldungen

Diese Liste ist bei weitem nicht erschöpfend, aber ist eine gute Blaupause, wenn man mit dem Potential der Ransomware-Angriffe zu folgen. Cloud Volumes Service in Google Cloud bietet verschiedene Möglichkeiten zum Schutz vor Ransomware-Ereignissen und zur Reduzierung der Auswirkungen.

Unveränderliche Snapshot Kopien

Cloud Volumes Service bietet native unveränderliche, schreibgeschützte Snapshot Kopien, die in einem anpassbaren Zeitplan erstellt werden, um schnelle zeitpunktgenaue Recovery beim Löschen von Daten zu ermöglichen oder wenn ein gesamtes Volume durch einen Ransomware-Angriff zu Opfer gebracht wurde.

Snapshots können zu vorherigen guten Snapshot Kopien schnell wiederhergestellt werden und minimieren Datenverluste aufgrund der Aufbewahrungsdauer Ihrer Snapshot-Zeitpläne und RTO/RPO. Der Performance-Effekt mit der Snapshot Technologie ist zu vernachlässigen.

Da Snapshot Kopien in Cloud Volumes Service schreibgeschützt sind, können diese nicht durch Ransomware infiziert werden, wenn die Ransomware nicht in den Datensatz „unbemerkt“ und Snapshot-Kopien der von Ransomware infizierten Daten erstellt wurde. Deshalb ist es notwendig, auf der Basis von Datenanomalien auch Ransomware-Erkennung in Betracht zu ziehen. Cloud Volumes Service bietet derzeit keine native Erkennung, Sie können jedoch externe Überwachungssoftware verwenden.

Backups und Restores

Cloud Volumes Service bietet standardmäßige NAS-Client-Backup-Funktionen (z. B. Backups über NFS oder SMB).

- CVS-Performance bietet regionenübergreifende Volume-Replizierung zu anderen CVS-Performance Volumes. Weitere Informationen finden Sie unter "Volume-Replizierung" In der Cloud Volumes Service-Dokumentation.
- CVS-SW bietet Service-native Backup-/Restore-Funktionen für Volumes. Weitere Informationen finden Sie unter "Cloud-Backup" In der Cloud Volumes Service-Dokumentation.

Die Volume-Replizierung liefert eine exakte Kopie des Quell-Volumes für schnelles Failover im Falle eines Ausfalls, einschließlich Ransomware-Ereignissen.

Regionsübergreifende Replizierung

CVS-Performance ermöglicht die sichere Replizierung von Volumes über Google Cloud Regionen hinweg zur Datensicherung und Archivierung von Anwendungsfällen. Dazu wird mit TLS1.2 AES 256 GCM-Verschlüsselung auf einem von NetApp gesteuerten Backend-Service-Netzwerk über spezifische Schnittstellen verwendet, die für die Replizierung im Google-Netzwerk verwendet werden. Ein primäres Volume (Quell-Volume) enthält die aktiven Produktionsdaten und repliziert auf ein sekundäres Volume (Ziel-Volume), um ein exaktes Replikat des primären Datensatzes zu erstellen.

Bei der anfänglichen Replizierung werden alle Blöcke übertragen, jedoch werden nur die geänderten Blöcke in einem primären Volume übertragen. Wird beispielsweise eine Datenbank mit 1 TB auf einem primären Volume auf das sekundäre Volume repliziert, so werden bei der ersten Replizierung 1 TB Speicherplatz übertragen. Wenn diese Datenbank einige hundert Zeilen (hypothetisch einige MB) hat, die zwischen der Initialisierung und dem nächsten Update wechseln, werden nur die Blöcke mit den geänderten Zeilen auf das sekundäre (wenige MB) repliziert. So wird sichergestellt, dass die Übertragungszeiten niedrig bleiben und die Replizierungskosten sinken.

Alle Berechtigungen für Dateien und Ordner werden auf das sekundäre Volume repliziert, aber die Zugriffsberechtigungen für die Freigabe (wie Exportrichtlinien und Regeln oder SMB-Freigaben und ACLs für die Freigabe) müssen separat gehandhabt werden. Bei einem Site-Failover sollte der Zielstandort dieselben Namensdienste und Active Directory-Domänenverbindungen nutzen, um eine konsistente Handhabung von Benutzer- und Gruppenidentitäten und -Berechtigungen zu ermöglichen. Sie können ein sekundäres Volume im Notfall als Failover-Ziel verwenden, indem Sie die Replizierungsbeziehung unterbrechen, die das sekundäre Volume in Lese- und Schreibvorgänge konvertiert.

Volume-Replikate sind schreibgeschützt, d. h. eine unveränderliche Kopie der Daten an einem externen Standort zur schnellen Recovery von Daten in Instanzen, in denen ein Virus infizierte Daten hat oder Ransomware den primären Datensatz verschlüsselt hat. Nur-Lese-Daten werden nicht verschlüsselt, aber, wenn das primäre Volume betroffen ist und Replikation auftritt, die infizierten Blöcke replizieren auch. Zur Wiederherstellung können Sie ältere, nicht betroffene Snapshot Kopien verwenden. Je nachdem, wie schnell ein Angriff erkannt wird, fallen jedoch unter Umständen die versprochenen RTO/RPO-Vorgaben aus.

Darüber hinaus können Sie mit dem Management der regionsübergreifenden Replizierung (CRR) in Google Cloud böswillige Administratoraktionen, wie z. B. Volume-Löschungen, Snapshot-Löschungen oder Änderungen bei Snapshot-Planungen, verhindern. Dazu werden benutzerdefinierte Rollen erstellt, die Volume-Administratoren trennen, die Quell-Volumes löschen, aber keine Spiegelungen unterbrechen und daher keine Ziel-Volumes von CRR-Administratoren löschen können, die keine Volume-Vorgänge ausführen können. Siehe "Überlegungen Zur Sicherheit" In der Cloud Volumes Service-Dokumentation finden Sie Berechtigungen, die von den einzelnen Administratorgruppen zulässig sind.

Cloud Volumes Service-Backup

Cloud Volumes Service bietet zwar eine hohe Datenaufbewahrung, externe Ereignisse können jedoch zu Datenverlusten führen. Falls es zu Sicherheitsereignisse wie Viren oder Ransomware kommt, werden Backups und Restores so wichtig, dass der Datenzugriff rechtzeitig wiederaufgenommen werden kann. Ein Administrator kann ein Cloud Volumes Service Volume versehentlich löschen. Oder Benutzer möchten einfach noch viele Monate Backup-Versionen ihrer Daten aufbewahren und den zusätzlichen Speicherplatz für Snapshot-Kopien innerhalb des Volumes zu einer Kostenanforderung machen. Snapshot-Kopien sollten die bevorzugte Methode sein, Backup-Versionen für die letzten Wochen zu behalten, um verlorene Daten von ihnen wiederherzustellen, sie befinden sich jedoch im Volume und gehen verloren, wenn das Volume entfernt wird.

Aus allen diesen Gründen bietet NetApp Cloud Volumes Service Backup-Services über an "Cloud Volumes Service-Backup".

Cloud Volumes Service Backup erzeugt eine Kopie des Volumes auf Google Cloud Storage (GCS). Es sichert nur die tatsächlichen Daten, die innerhalb des Volume gespeichert sind, nicht den freien Speicherplatz. Es funktioniert wie immer inkrementell, d. h., es überträgt den Volume-Inhalt einmal und von dort auf wird nur geänderte Daten gesichert. Im Vergleich zu klassischen Backup-Konzepten mit mehreren vollständigen Backups spart das Unternehmen viel Storage und senkt dadurch die Kosten. Da der monatliche Preis von Backup-Speicherplatz im Vergleich zu einem Volume niedriger ist, ist es der ideale Ort, um Backup-Versionen länger zu halten.

Benutzer können ein Cloud Volumes Service Backup verwenden, um jede Backup-Version auf demselben oder einem anderen Volume innerhalb derselben Region wiederherzustellen. Wenn das Quell-Volume gelöscht wird, werden die Backup-Daten aufbewahrt und müssen unabhängig gemanagt werden (beispielsweise gelöscht).

Cloud Volumes Service Backup ist optional in Cloud Volumes Service integriert. Benutzer legen fest, welche Volumes gesichert werden sollen, indem Cloud Volumes Service Backup für einzelne Volumes aktiviert wird. Siehe "Cloud Volumes Service Backup-Dokumentation" Weitere Informationen zu Backups finden Sie im "Anzahl der maximal unterstützten Backup-Versionen", Planung, und "Preisgestaltung".

Alle Backup-Daten eines Projekts werden innerhalb eines GCS-Buckets gespeichert, der durch den Service gemanagt wird und für den Benutzer nicht sichtbar ist. Jedes Projekt verwendet einen anderen Bucket. Derzeit befinden sich die Buckets im gleichen Bereich wie die Cloud Volumes Service Volumes, es werden jedoch noch weitere Optionen erläutert. In der Dokumentation finden Sie den aktuellen Status.

Der Datentransport von einem Cloud Volumes Service-Bucket zu GCS nutzt Service-interne Google-Netzwerke mit HTTPS und TLS1.2. Die Daten werden im Ruhezustand mit von Google gemanagten Schlüsseln verschlüsselt.

Um Cloud Volumes Service-Backups zu managen (Backups erstellen, löschen und wiederherstellen), muss ein Benutzer über die verfügen "Rollen/netappCloudVolumes.admin" Rolle:

Der Netapp Architektur Sind

Überblick

Als Teil des Vertrauens einer Cloud-Lösung müssen Sie die Architektur und die Art und Weise der Sicherheit kennen. In diesem Abschnitt werden verschiedene Aspekte der Cloud Volumes Service-Architektur in Google erläutert, um mögliche Bedenken hinsichtlich der Datensicherheit zu zerstreuen und Bereiche herauszurufen, in denen zusätzliche Konfigurationsschritte erforderlich sind, um die sichere Implementierung zu erhalten.

Die allgemeine Architektur von Cloud Volumes Service kann in zwei Hauptkomponenten aufgeteilt werden: Die Kontrollebene und die Datenebene.

Kontrollebene

Die Kontrollebene in Cloud Volumes Service ist die von Cloud Volumes Service-Administratoren und der nativen Automatisierungssoftware von NetApp gemanagte Back-End-Infrastruktur. Diese Ebene ist für Endbenutzer vollständig transparent und beinhaltet Netzwerk, Storage-Hardware, Software-Updates usw., um einen Mehrwert für eine Cloud-residente Lösung wie Cloud Volumes Service bereitzustellen.

Datenebene

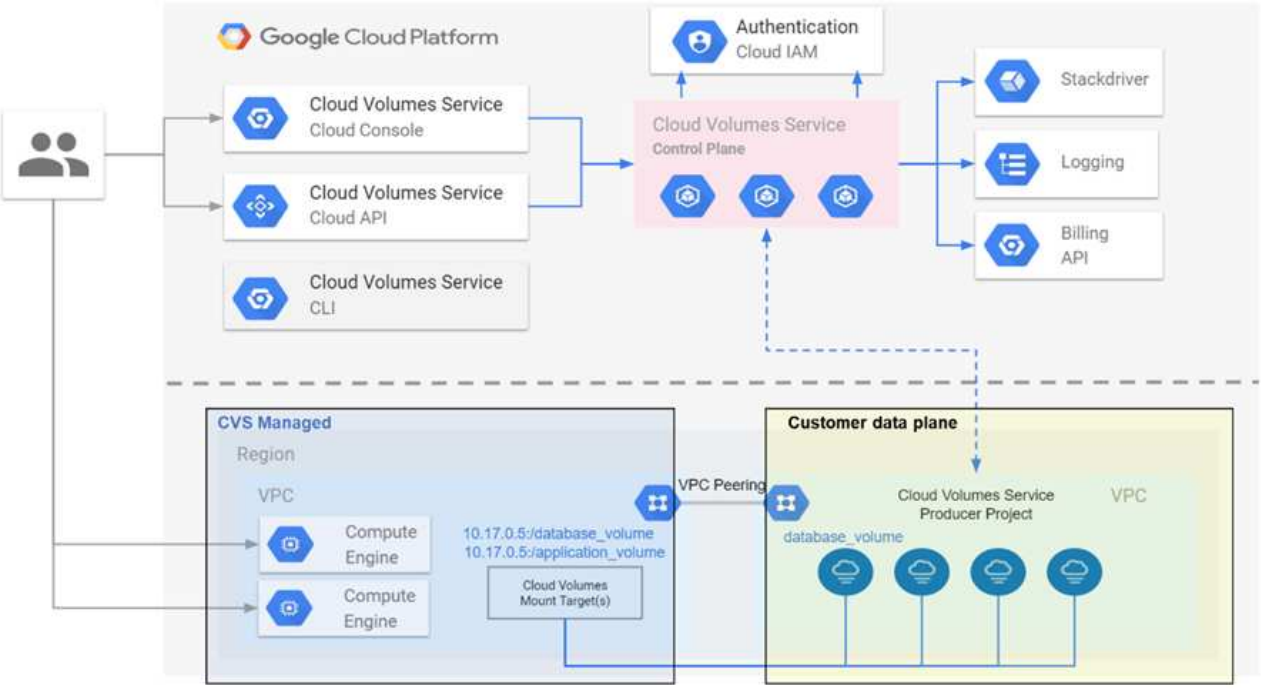
Die Datenebene in Cloud Volumes Service umfasst die tatsächlichen Daten-Volumes und die gesamte Cloud Volumes Service-Konfiguration (wie Zugriffssteuerung, Kerberos Authentifizierung usw.). Die Datenebene unterliegt vollständig der Kontrolle von Endbenutzern und Nutzern der Cloud Volumes Service Plattform.

Es gibt unterschiedliche Arten, wie jede Ebene gesichert und verwaltet wird. In den folgenden Abschnitten werden diese Unterschiede näher beschrieben. Zunächst wird die Cloud Volumes Service Architektur im Überblick angezeigt.

Architektur von Cloud Volumes Service

Cloud Volumes Service verwendet in ähnlicher Weise wie andere Cloud-native Dienste von Google wie CloudSQL, Google Cloud VMware Engine (GCVE) und FileStore "Google PSA" Für die Bereitstellung des Service. In PSA werden Dienste innerhalb eines Service-Producer-Projekts aufgebaut, das verwendet wird "VPC-Netzwerk-Peering" So stellen Sie eine Verbindung zum Serviceverbraucher her. Der Hersteller des Service wird von NetApp bereitgestellt und betrieben. Der Serviceverbraucher ist eine VPC in einem Kundenprojekt und hostet die Clients, die auf Cloud Volumes Service Dateifreigaben zugreifen möchten.

Die folgende Abbildung, auf die im Bezug genommen wird "Abschnitt zur Architektur" In der Cloud Volumes Service-Dokumentation wird eine allgemeine Ansicht angezeigt.



Der Teil über der gepunkteten Linie zeigt die Kontrollebene des Services an, der den Volumenlebenszyklus steuert. Der Teil unterhalb der gepunkteten Linie zeigt die Datenebene. Das linke blaue Feld zeigt die Benutzer-VPC (Service-Verbraucher), das rechte blaue Feld ist der von NetApp bereitgestellte Service-Hersteller. Beide sind über VPC-Peering verbunden.

Tenancy-Modell

In Cloud Volumes Service gelten einzelne Projekte als eigenständige Mandanten. Das bedeutet, dass Manipulationen von Volumes, Snapshot Kopien usw. pro Projekt durchgeführt werden. Das heißt, alle Volumes sind im Besitz des Projekts, in dem sie erstellt wurden. Nur das Projekt kann standardmäßig die darin enthaltenen Daten managen und darauf zugreifen. Dies wird als Ansicht der Kontrollebene des Services betrachtet.

Gemeinsam genutzte VPCs

In der Ansicht „Datenebene“ kann Cloud Volumes Service eine Verbindung zu einer gemeinsamen VPC herstellen. Sie können Volumes im Hosting-Projekt oder in einem der Service-Projekte erstellen, die mit der gemeinsam genutzten VPC verbunden sind. Alle mit dieser gemeinsamen VPC verbundenen Projekte (Host oder Service) sind in der Lage, die Volumes auf der Netzwerkebene (TCP/IP) zu erreichen. Da alle Clients mit Netzwerkkonnektivität auf der gemeinsam genutzten VPC potenziell über NAS-Protokolle auf die Daten zugreifen können, muss die Zugriffssteuerung für das individuelle Volume (z. B. User-/Group-Zugriffssteuerungslisten (ACLs) und Hostnamen/IP-Adressen für NFS-Exporte) verwendet werden, um zu kontrollieren, wer auf die Daten zugreifen kann.

Sie können Cloud Volumes Service mit bis zu fünf VPCs pro Kundenprojekt verbinden. In der Kontrollebene können Sie mit dem Projekt alle erstellten Volumes managen – unabhängig von der VPC, mit der sie verbunden sind. Auf der Datenebene sind VPCs voneinander isoliert, wobei jedes Volume nur mit einer VPC verbunden werden kann.

Der Zugriff auf einzelne Volumes wird über protokollspezifische Zugriffskontrollmechanismen (NFS/SMB) gesteuert.

Das bedeutet, dass auf der Netzwerkebene alle mit der gemeinsam genutzten VPC verbundenen Projekte in der Lage sind, das Volume zu sehen, während auf der Managementseite nur die Kontrollebene es dem Owner-Projekt erlaubt, das Volume zu sehen.

VPC-Service-Kontrollen

VPC-Service-Kontrollen einrichten eine Zugriffskontrollumgebung um Google Cloud Services herum, die mit dem Internet verbunden sind und weltweit zugänglich sind. Diese Dienste bieten Zugriffskontrolle über Benutzeridentitäten, können aber nicht einschränken, aus welchen Netzwerkstandortanforderungen stammen. Die VPC-Service-Kontrollen schließen diese Lücke, indem sie Funktionen zur Einschränkung des Zugriffs auf definierte Netzwerke einführen.

Die Cloud Volumes Service-Datenebene ist nicht mit dem externen Internet verbunden, sondern mit privaten VPCs mit klar definierten Netzwerkgrenzen (Perimeter). Innerhalb dieses Netzwerks verwendet jedes Volume eine protokollspezifische Zugriffssteuerung. Jegliche externe Netzwerkverbindung wird explizit von Google Cloud-Projektadministratoren erstellt. Die Kontrollebene bietet jedoch nicht denselben Schutz wie die Datenebene und kann von jedem beliebigen Ort mit gültigen Zugangsdaten aufgerufen werden ("JWT-Token").

Kurz gesagt, die Cloud Volumes Service Datenebene bietet die Möglichkeit der Netzwerk-Zugriffssteuerung, ohne dass die VPC-Service-Kontrollen unterstützt werden müssen. Außerdem werden nicht explizit VPC-Service-Controls verwendet.

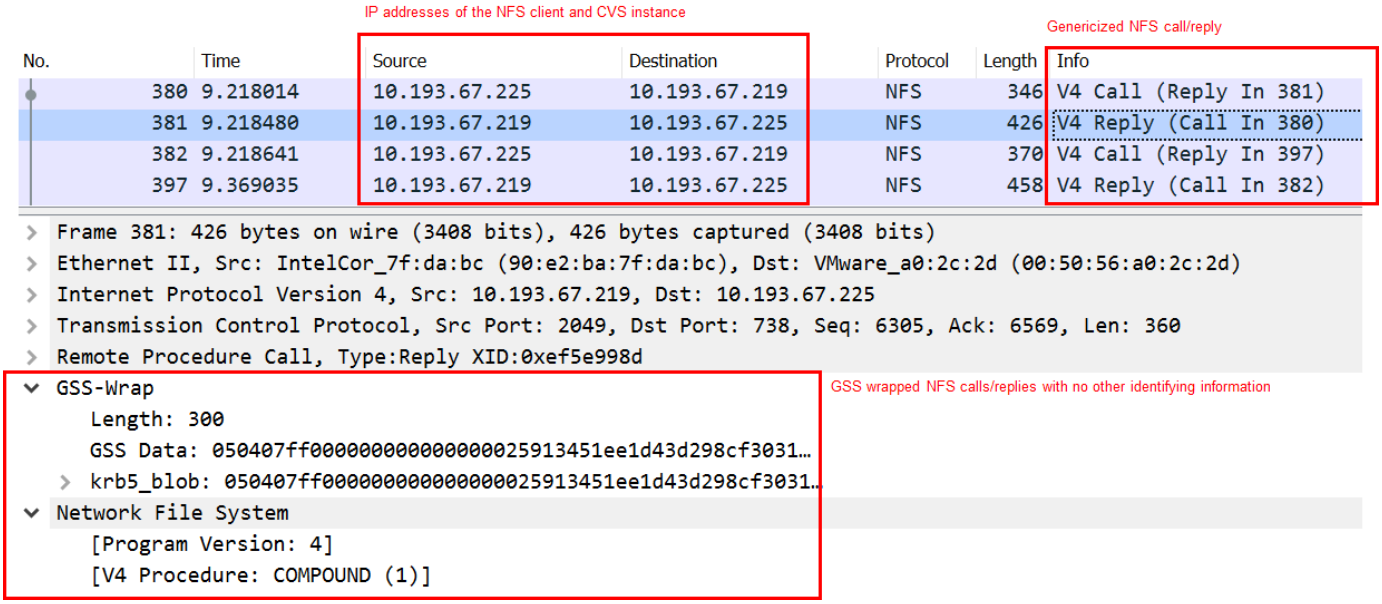
Überlegungen zu Packet Sniffing/Trace

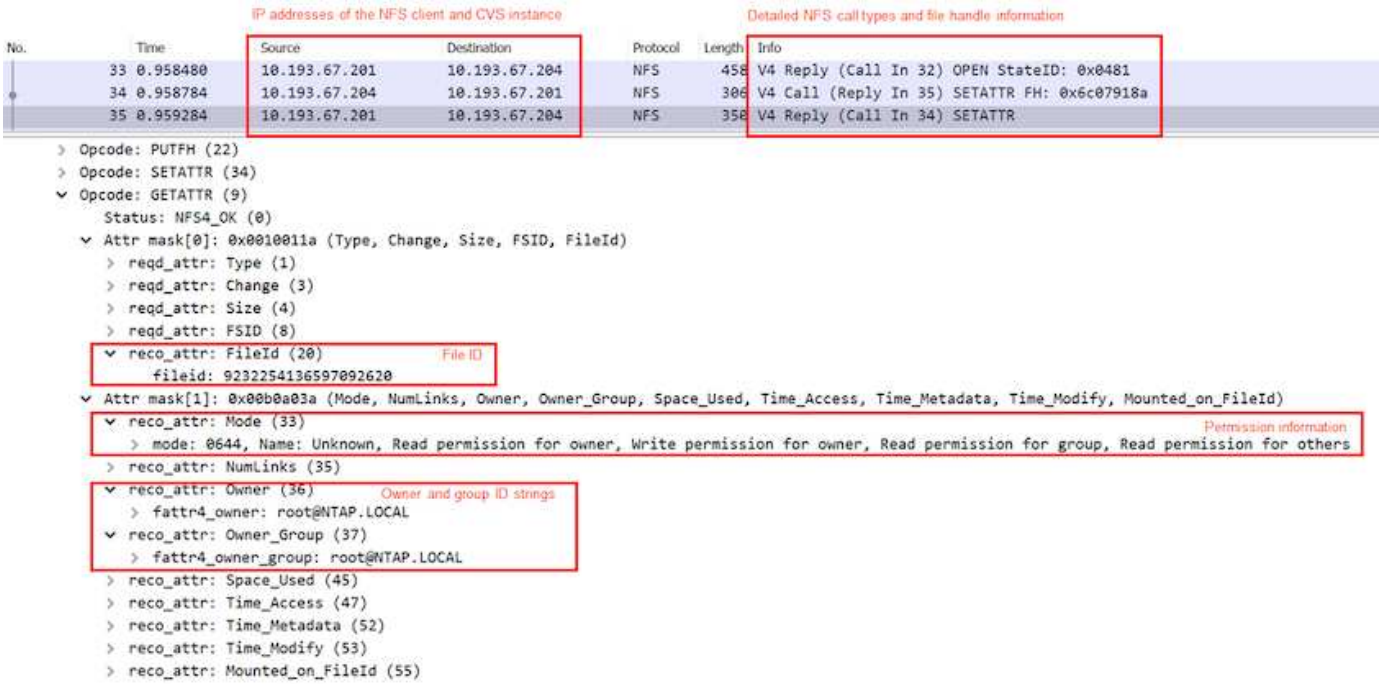
Paketerfassungen können für die Behebung von Netzwerkproblemen oder anderen Problemen (z. B. NAS-Berechtigungen, LDAP-Konnektivität usw.) nützlich sein, können aber auch missverständlich verwendet werden, um Informationen über Netzwerk-IP-Adressen, MAC-Adressen, Benutzer- und Gruppennamen und die Sicherheitsstufe für Endpunkte zu erhalten. Aufgrund der Art und Weise, wie Google Cloud-Netzwerke, VPCs und Firewall-Regeln konfiguriert werden, sollte ein unerwünschter Zugriff auf Netzwerkpakete ohne Benutzeranmeldung oder nur schwer zu erhalten sein "JWT-Token" In Cloud-Instanzen integriert. Paketerfassungen sind nur auf Endpunkten (z. B. Virtual Machines (VMs) möglich und nur in Endpunkten innerhalb der VPC möglich, es sei denn, ein Shared VPC und/oder ein externer Netzwerktunnel/IP-Weiterleitung wird verwendet, um explizit externen Traffic zu Endpunkten zu erlauben. Es gibt keine Möglichkeit, den Verkehr außerhalb der Kunden zu schnuppern.

Bei gemeinsamen VPCs wird die Verschlüsselung auf der Übertragungsstrecke mit NFS Kerberos und/oder genutzt "SMB-Verschlüsselung" Kann einen Großteil der Informationen aus Spuren verbergen. Allerdings wird noch etwas Verkehr in Klartext gesendet, wie "DNS" Und "LDAP-Abfragen". Die folgende Abbildung zeigt eine Paketerfassung aus einer Klartext-LDAP-Abfrage, die aus Cloud Volumes Service stammt, und die potenziellen identifizierenden Informationen, die freigelegt wurden. LDAP-Abfragen in Cloud Volumes Service unterstützen derzeit keine Verschlüsselung oder LDAP über SSL. CVS-Performance unterstützt LDAP-Signatur, falls durch Active Directory angefordert. CVS-SW unterstützt LDAP-Signatur nicht.

UnixUserPassword wird von LDAP abgefragt und nicht im Klartext, sondern in einem gesalzenem Hash gesendet. Standardmäßig füllt Windows LDAP die Felder unixUserPassword nicht aus. Dieses Feld ist nur erforderlich, wenn Sie Windows LDAP für interaktive Anmeldungen über LDAP für Clients verwenden müssen. Cloud Volumes Service unterstützt keine interaktiven LDAP-Anmeldungen bei den Instanzen.

Die folgende Abbildung zeigt eine Paketerfassung aus einem NFS-Kerberos-Gespräch neben einer NFS-Erfassung über AUTH_SYS. Beachten Sie, wie sich die Informationen in einer Kurve zwischen den beiden unterscheiden und wie die Aktivierung der Verschlüsselung während der Übertragung eine größere Gesamtsicherheit für den NAS-Datenverkehr bietet.





VM-Netzwerkschnittstellen

Angreifer können versuchen, eine neue Netzwerkschnittstellenkarte (NIC) zu einer VM in hinzuzufügen "Promiskuous Modus" (Port-Spiegelung) oder aktivieren Sie den Promiskuus-Modus auf einer vorhandenen NIC, um den gesamten Datenverkehr zu entschnüffeln. Beim Hinzufügen einer neuen NIC muss in Google Cloud eine VM vollständig heruntergefahren werden, was zu Warnmeldungen führt. So können Angreifer nicht unbemerkt das tun.

Darüber hinaus können NICs überhaupt nicht auf den promiskuitiven Modus eingestellt werden und erzeugen in Google Cloud Warnmeldungen.

Kontrollebene Architektur

Alle Management-Aktionen an Cloud Volumes Service werden über die API ausgeführt. Das in die GCP Cloud Console integrierte Cloud Volumes Service-Management verwendet auch die Cloud Volumes Service-API.

Identitäts- und Zugriffsmanagement

Identitäts- und Zugriffsmanagement ("IAM") Ist ein Standardservice, mit dem Sie Authentifizierung (Logins) und Berechtigungen (Berechtigungen) für Google Cloud-Projektinstanzen steuern können. Google IAM bietet ein vollständiges Audit-Protokoll über Berechtigungen zum Berechtigungs- und Entfernen. Derzeit bietet Cloud Volumes Service keine Prüfung auf Kontrollebenen.

Autorisierungs-/Berechtigungs-Übersicht

IAM bietet integrierte, granulare Berechtigungen für Cloud Volumes Service. Hier finden Sie ein "Vollständige Liste mit granularen Berechtigungen hier".

IAM bietet außerdem zwei vordefinierte Rollen, die als Namen bezeichnet werden `netappcloudvolumes.admin` Und `netappcloudvolumes.viewer`. Diese Rollen können bestimmten Benutzern oder Servicekonten zugewiesen werden.

Weisen Sie geeignete Rollen und Berechtigungen zu, um IAM-Benutzern das Management von Cloud Volumes Service zu ermöglichen.

Beispiele für die Verwendung granularer Berechtigungen sind:

- Erstellen Sie eine benutzerdefinierte Rolle nur mit Berechtigungen zum Abrufen/Auflisten/Erstellen/Aktualisieren, damit Benutzer Volumes nicht löschen können.
- Verwenden Sie eine benutzerdefinierte Rolle nur mit `snapshot.*` Berechtigungen zum Erstellen eines Servicekontos, das zum Aufbau einer applikationskonsistenten Snapshot Integration verwendet wird.
- Erstellen Sie eine benutzerdefinierte Rolle zum Delegieren `volumereplication.*` An bestimmte Benutzer.

Servicekonten

Um Cloud Volumes Service-API-Aufrufe über Skripte oder durchzuführen "Terraform", Sie müssen ein Dienstkonto mit dem erstellen `roles/netappcloudvolumes.admin` Rolle: Sie können dieses Dienstkonto verwenden, um die JWT-Token zu generieren, die zur Authentifizierung von Cloud Volumes Service-API-Anforderungen erforderlich sind:

- Generieren Sie einen JSON-Schlüssel und verwenden Sie Google APIs, um daraus ein JWT-Token abzuleiten. Dies ist der einfachste Ansatz, aber es beinhaltet manuelle Geheimnisse (den JSON-Schlüssel) Management.
- Nutzung "Imitation von Servicekonten" Mit `roles/iam.serviceAccountTokenCreator`. Der Code (Skript, Terraform usw.) läuft mit "Standardanmeldedaten Für Anwendungen" Und personifiziert das Servicekonto, um seine Berechtigungen zu erhalten. Dieser Ansatz spiegelt die Best Practices für die Sicherheit von Google wider.

Siehe "Erstellen Ihres Servicekontos und privaten Schlüssels" In der Google Cloud Dokumentation finden Sie weitere Informationen.

Cloud Volumes Service API

Die Cloud Volumes Service API verwendet eine REST-basierte API mithilfe von HTTPS (TLSv1.2) als zugrunde liegenden Netzwerktransport. Hier finden Sie die neueste API-Definition "Hier" Und Informationen zur Verwendung der API unter "Cloud Volumes APIs in der Google Cloud-Dokumentation".

Der API-Endpunkt wird durch NetApp mit Standard-HTTPS-Funktionalität (TLSv1.2) betrieben und gesichert.

JWT-Token

Die Authentifizierung an der API erfolgt mit JWT-Inhabertoken ("RFC-7519"). Gültige JWT-Token müssen über die Google Cloud IAM-Authentifizierung abgerufen werden. Dazu muss ein Token vom IAM abgerufen werden, indem ein JSON-Schlüssel für ein Servicekonto bereitgestellt wird.

Audit-Protokollierung

Derzeit sind keine vom Benutzer zugänglichen Prüfprotokolle für Kontrollebenen verfügbar.

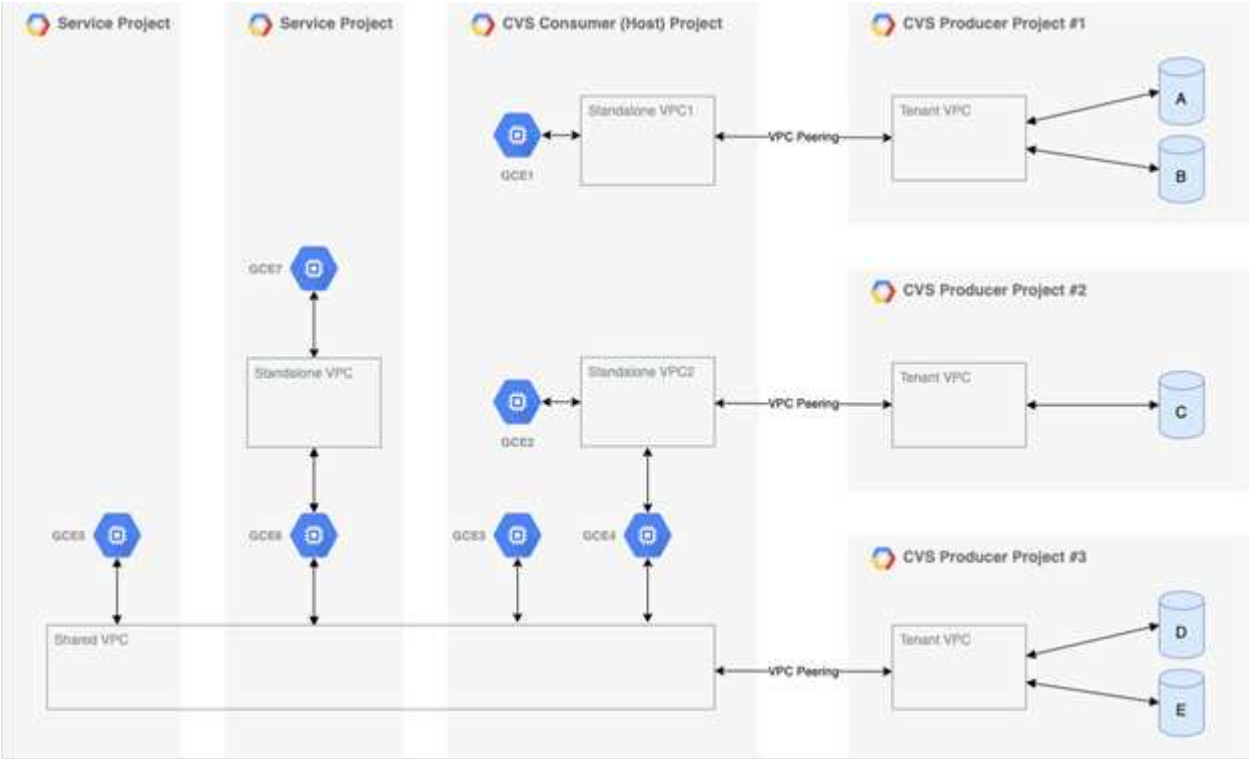
Datenplanarchitektur

Cloud Volumes Service für Google Cloud nutzt die Google Cloud "Zugang zu privaten Services" Framework: In diesem Framework können sich Benutzer mit dem Cloud Volumes Service verbinden. Dieses Framework verwendet Service Networking und VPC

Peering so wie andere Google Cloud-Services, dass die vollständige Isolierung zwischen Mandanten gewährleistet ist.

Eine Übersicht über die Architektur von Cloud Volumes Service für Google Cloud finden Sie unter "Architektur für Cloud Volumes Service".

Benutzer-VPCs (Standalone oder Shared) werden an VPCs innerhalb von Cloud Volumes Service gemanagten Mandantenprojekten weitergegeben, die die Volumes hostet.



Die obige Abbildung zeigt ein Projekt (das CVS Verbraucherprojekt in der Mitte) mit drei VPC-Netzwerken, die mit Cloud Volumes Service verbunden sind, und mehreren Compute Engine VMs (GCE1-7), die Volumes gemeinsam nutzen:

- VPC1 ermöglicht GCE1 auf Volumes A und B. zuzugreifen
- VPC2 ermöglicht GCE2 und GCE4 den Zugriff auf Lautstärke C.
- Das dritte VPC-Netzwerk ist eine gemeinsame VPC, von der zwei Service-Projekte gemeinsam genutzt werden. GCE3, GCE4, GCE5 und GCE6 können auf Volumes D und E. zugreifen Shared VPC-Netzwerke werden nur für Volumes des Servicetyps „CVS-Performance“ unterstützt.

GCE7 kann auf keine Volumes zugreifen.

Die Daten können sowohl bei der Übertragung (mit Kerberos- und/oder SMB-Verschlüsselung) als auch im Ruhezustand in Cloud Volumes Service verschlüsselt werden.

Datenverschlüsselung während der Übertragung

Die übertragenen Daten können auf der NAS-Protokollebene verschlüsselt und das Google Cloud-Netzwerk selbst verschlüsselt werden, wie in den folgenden Abschnitten beschrieben.

Google Cloud Network

Google Cloud verschlüsselt den Datenverkehr auf Netzwerkebene wie in beschrieben "Verschlüsselung während der Übertragung" In der Google-Dokumentation. Wie im Abschnitt „Cloud Volumes Services Architecture“ erwähnt, wird Cloud Volumes Service aus einem von NetApp gesteuerten PSA Producer-Projekt bereitgestellt.

Im Fall von CVS-SW führt der Producer-Mandant Google VMs aus, um den Service bereitzustellen. Der Datenverkehr zwischen Benutzer-VMs und Cloud Volumes Service-VMs wird automatisch durch Google verschlüsselt.

Obwohl der Datenpfad für CVS-Performance nicht vollständig auf der Netzwerkebene verschlüsselt ist, verwenden NetApp und Google eine Kombination "Der IEEE 802.1AE Verschlüsselung (MACsec)", "Kapselung" (Datenverschlüsselung) und Netzwerke mit physischen Einschränkungen zum Schutz der Daten bei der Übertragung zwischen dem Cloud Volumes Service CVS-Performance Servicetyp und Google Cloud

NAS-Protokolle

Die NAS-Protokolle NFS und SMB bieten optionale Transportverschlüsselung auf Protokollebene.

SMB-Verschlüsselung

"SMB-Verschlüsselung" Bietet End-to-End-Verschlüsselung von SMB-Daten und schützt Daten vor abfallenden Ereignissen in nicht vertrauenswürdigen Netzwerken. Sie können die Verschlüsselung sowohl für die Client-/Server-Datenverbindung (nur für SMB3.x-fähige Clients verfügbar) als auch für die Server/Domain-Controller-Authentifizierung aktivieren.

Wenn die SMB-Verschlüsselung aktiviert ist, können Clients, die keine Verschlüsselung unterstützen, nicht auf die Freigabe zugreifen.

Cloud Volumes Service unterstützt RC4-HMAC, AES-128-CTS-HMAC-SHA1 und AES-256-CTS-HMAC-SHA1-Sicherheitschiffren für SMB-Verschlüsselung. SMB verhandelt den vom Server am häufigsten unterstützten Verschlüsselungstyp.

Kerberos: NFSv4.1

Für NFSv4.1 bietet CVS-Performance Kerberos-Authentifizierung wie in beschrieben "RFC7530". Sie können Kerberos auf Volume-Basis aktivieren.

Der derzeit stärkste verfügbare Verschlüsselungstyp für Kerberos ist AES-256-CTS-HMAC-SHA1. NetApp Cloud Volumes Service unterstützt AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3 und DES für NFS. Es unterstützt auch ARCFOUR-HMAC (RC4) für CIFS/SMB-Datenverkehr, jedoch nicht für NFS.

Kerberos bietet drei verschiedene Sicherheitsstufen für NFS-Mounts, die Möglichkeiten bieten, wie stark die Kerberos-Sicherheit sein sollte.

As per RedHat "Allgemeine Mount-Optionen" Dokumentation:

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

Je mehr der Kerberos-Sicherheitslevel zu tun hat, desto schlechter ist die Performance, da Client und Server Zeit damit verbringen, NFS-Vorgänge für jedes gesendete Paket zu verschlüsseln und zu entschlüsseln. Viele Clients und NFS Server unterstützen AES-NI-Entlastung der CPUs, um insgesamt eine bessere Benutzererfahrung zu erzielen. Die Auswirkungen von Kerberos 5p (vollständige End-to-End-Verschlüsselung) sind jedoch deutlich höher als die Auswirkungen von Kerberos 5 (Benutzerauthentifizierung).

Die folgende Tabelle zeigt Unterschiede in den einzelnen Ebenen in Bezug auf Sicherheit und Performance.

Sicherheitsstufe	Sicherheit	Leistung
NFSv3 – sys	• Am wenigsten sicher; Klartext mit numerischen Benutzer-IDs/Gruppen-IDs • Kann UID, GID, Client-IP-Adressen, Exportpfade, Dateinamen, Berechtigungen in Paketaufnahmen	• Das Beste für die meisten Fälle
NFSv4.x – sys	• Sicherer als NFSv3 (Client-IDs, Namenszeichenfolge/Domänen zeichenfolge-Übereinstimmung), aber immer noch Klartext • Kann UID, GID, Client-IP-Adressen, Namensstrings, Domänen-IDs, anzeigen Pfade, Dateinamen und Berechtigungen in Paketaufnahmen exportieren	• Gut für sequenzielle Workloads (z. B. VMs, Datenbanken, große Dateien) • Schlecht mit hoher Dateianzahl/hohen Metadaten (30-50% schlechter)

Sicherheitsstufe	Sicherheit	Leistung
NFS – krb5	• Kerberos-Verschlüsselung für Anmeldeinformationen in jedem NFS-Paket – schließt UID/GID von Benutzern/Gruppen in RPC-Aufrufen in GSS-Wrapper • Benutzer, die Zugriff auf das Mount anfordern, benötigen ein gültiges Kerberos-Ticket (entweder über den Benutzernamen/das Passwort oder den Austausch des manuellen Schlüssels); das Ticket läuft nach einem bestimmten Zeitraum ab und der Benutzer muss sich erneut authentifizieren, um Zugriff zu erhalten • Keine Verschlüsselung für NFS-Vorgänge oder Zusatz-Protokolle wie Mount/Portmapper/nlm (kann Exportpfade, IP-Adressen, Dateihandles, Berechtigungen, Dateinamen, Uhrzeit/Mtime in Paketaufnahmen)	• Am besten in den meisten Fällen für Kerberos; schlechter als AUTH_SYS

Sicherheitsstufe	Sicherheit	Leistung
NFS – krb5i	• Kerberos-Verschlüsselung für Anmeldeinformationen in jedem NFS-Paket – schließt UID/GID von Benutzern/Gruppen in RPC-Aufrufen in GSS-Wrapper • Benutzer, die Zugriff auf das Mount anfordern, benötigen ein gültiges Kerberos-Ticket (entweder über Benutzernamen/Passwort oder den Austausch des manuellen Schlüssels); das Ticket läuft nach einem bestimmten Zeitraum ab und der Benutzer muss sich erneut authentifizieren, um Zugriff zu erhalten • Keine Verschlüsselung für NFS-Vorgänge oder Zusatz-Protokolle wie Mount/Portmapper/nlm (kann Exportpfade, IP-Adressen, Dateihandles, Berechtigungen, Dateinamen, Uhrzeit/Mtime in Paketaufnahmen) • Kerberos GSS-Prüfsumme wird zu jedem Paket hinzugefügt, damit die Pakete nicht abgefangen werden. Wenn Prüfsummen übereinstimmen, ist das Gespräch zulässig.	• Besser als krb5p, da die NFS-Nutzlast nicht verschlüsselt ist; nur der zusätzliche Overhead im Vergleich zu krb5 ist die Integritäts-Prüfsumme. Die Leistung von krb5i wird nicht viel schlechter sein als krb5, aber wird einige Verschlechterung zu sehen.

Sicherheitsstufe	Sicherheit	Leistung
NFS – krb5p	• Kerberos-Verschlüsselung für Anmeldeinformationen in jedem NFS-Paket – schließt UID/GID von Benutzern/Gruppen in RPC-Aufrufen in GSS-Wrapper • Benutzer, die Zugriff auf das Mount anfordern, benötigen ein gültiges Kerberos-Ticket (entweder über Benutzernamen/Passwort oder den manuellen Schlüsseltab-Austausch); das Ticket läuft nach einem festgelegten Zeitraum ab und der Benutzer muss sich erneut authentifizieren, um Zugriff zu erhalten • Alle Payloads des NFS-Pakets sind mit dem GSS-Wrapper verschlüsselt (Dateihandles, Berechtigungen, Dateinamen, atime/mtime in Paketaufnahmen können nicht angezeigt werden). • Umfasst die Integritätsprüfung. • Der NFS Operationstyp ist sichtbar (FSINFO, ACCESS, GETATTR usw.). • Zusatzprotokolle (Mount, Portmap, nlm usw.) sind nicht verschlüsselt - (kann Exportpfade, IP-Adressen sehen)	• Schlechteste Leistung der Sicherheitsstufen; krb5p muss mehr verschlüsseln/entschlüsseln. • Bessere Performance als krb5p mit NFSv4.x für Workloads mit hoher Dateianzahl.

In Cloud Volumes Service wird ein konfigurierter Active Directory-Server als Kerberos-Server und LDAP-Server verwendet (um Benutzeridentitäten aus einem RFC2307-kompatiblen Schema zu suchen). Es werden keine anderen Kerberos oder LDAP-Server unterstützt. NetApp empfiehlt besonders, LDAP für das Identitätsmanagement in Cloud Volumes Service zu verwenden. Informationen darüber, wie NFS Kerberos in Paketaufnahmen angezeigt wird, finden Sie im Abschnitt "„Packet Sniffing/Trace Betrachtungen.“"

Verschlüsselung von Daten im Ruhezustand

Alle Volumes in Cloud Volumes Service werden im Ruhezustand mit AES-256-Verschlüsselung verschlüsselt, d. h. alle auf das Medium geschriebenen Benutzerdaten werden verschlüsselt und können nur mit einem Schlüssel pro Volume entschlüsselt werden.

- Für CVS-SW werden von Google generierte Schlüssel verwendet.

- Die Schlüssel für CVS-Performance werden in einem im Cloud Volumes Service integrierten Schlüsselmanager gespeichert, der die Schlüssel pro Volume enthält.

Ab November 2021 wurde eine Vorschau auf die Funktionalität der vom Kunden gemanagten Verschlüsselungsschlüssel (CMEK) bereitgestellt. So können Sie die Schlüssel pro Volume mit einem in einzelnen Projekten und Regionen gehosteten Master-Schlüssel verschlüsseln "Google Key Management Service (KMS):" KMS ermöglicht es Ihnen, externe Schlüsselmanager anzubinden.

Informationen zur Konfiguration von KMS für CVS-Performance finden Sie unter "Einrichten von vom Kunden gemanagten Verschlüsselungsschlüsseln".

Firewall

Cloud Volumes Service legt mehrere TCP Ports für NFS- und SMB-Freigaben bereit:

- "Für NFS-Zugriff erforderliche Ports"
- "Für SMB-Zugriff erforderliche Ports"

Außerdem erfordern SMB, NFS mit LDAP, einschließlich Kerberos und Dual-Protokoll-Konfigurationen den Zugriff auf eine Windows Active Directory Domain. Active Directory-Verbindungen müssen sein "Konfiguriert" Pro Region. Active Directory-Domänencontroller (DC) werden mithilfe identifiziert "DNS-basierte DC-Erkennung" Verwenden der angegebenen DNS-Server. Alle zurückgegebenen Datacenter werden genutzt. Die Liste der geeigneten DCs kann durch Angabe einer Active Directory-Site beschränkt werden.

Cloud Volumes Service erreicht mit IP-Adressen aus dem CIDR-Bereich, der dem zugewiesen ist `gcloud compute address` Befehl während "On-Boarding the Cloud Volumes Service". Sie können dieses CIDR als Quelladressen verwenden, um eingehende Firewalls für Ihre Active Directory-Domänencontroller zu konfigurieren.

Active Directory-Domänencontroller müssen "Legen Sie wie hier erwähnt Ports den Cloud Volumes Service-CIDRs offen".

NAS-Protokolle

Übersicht über NAS-Protokolle

Die NAS-Protokolle umfassen NFS (v3 und v4.1) und SMB/CIFS (2.x und 3.x). Mit diesen Protokollen ermöglicht CVS gemeinsamen Zugriff auf Daten über mehrere NAS Clients hinweg. Darüber hinaus ermöglicht Cloud Volumes Service den gleichzeitigen Zugriff auf NFS- und SMB/CIFS-Clients (Dual-Protokoll), während sämtliche Identitäts- und Berechtigungseinstellungen auf Dateien und Ordnern in den NAS-Freigaben berücksichtigt werden. Cloud Volumes Service unterstützt die Protokollverschlüsselung im laufenden Betrieb mit SMB-Verschlüsselung und NFS Kerberos 5p, um die höchstmögliche Sicherheit bei Datentransfers zu gewährleisten.

> Das Dual-Protokoll ist nur mit CVS-Performance verfügbar.

Grundlagen der NAS-Protokolle

NAS-Protokolle sind Möglichkeiten für mehrere Clients im Netzwerk, um auf dieselben Daten in einem Storage-System zuzugreifen, beispielsweise auf Cloud Volumes Service

in GCP. NFS und SMB sind die definierten NAS-Protokolle und werden auf Client-/Server-Basis ausgeführt, wobei Cloud Volumes Service als Server fungiert. Clients senden Zugriffs-, Lese- und Schreibanfragen an den Server, und der Server ist für die Koordinierung der Sperrmechanismen für Dateien, die Speicherung von Berechtigungen und die Bearbeitung von Identitäts- und Authentifizierungsanforderungen zuständig.

Der folgende allgemeine Prozess wird beispielsweise verfolgt, wenn ein NAS-Client eine neue Datei in einem Ordner erstellen möchte.

1. Der Client fragt den Server nach Informationen zum Verzeichnis (Berechtigungen, Eigentümer, Gruppe, Datei-ID, verfügbarer Speicherplatz, Und so weiter); der Server antwortet mit den Informationen, wenn der anfragende Client und der Benutzer die erforderlichen Berechtigungen für den übergeordneten Ordner haben.
2. Wenn die Berechtigungen im Verzeichnis den Zugriff zulassen, fragt der Client den Server, ob der erstellte Dateiname bereits im Dateisystem vorhanden ist. Wenn der Dateiname bereits verwendet wird, schlägt die Erstellung fehl. Wenn der Dateiname nicht vorhanden ist, lässt der Server dem Client wissen, dass er fortgesetzt werden kann.
3. Der Client ruft den Server aus, um die Datei mit dem Verzeichnis-Handle und dem Dateinamen zu erstellen, und legt die Zugriffszeiten und die geänderten Zeiten fest. Der Server gibt eine eindeutige Datei-ID für die Datei aus, um sicherzustellen, dass keine anderen Dateien mit derselben Datei-ID erstellt werden.
4. Der Client sendet einen Anruf, um Dateiattribute vor DEM SCHREIBVORGANG zu überprüfen. Falls dies durch Berechtigungen möglich ist, schreibt der Client die neue Datei. Falls das Protokoll oder die Applikation gesperrt wird, fordert der Client den Server zur Sperrung auf, um zu verhindern, dass andere Clients auf die Datei zugreifen können, während diese gesperrt ist, um Datenbeschädigungen zu verhindern.

NFS

NFS ist ein Distributed File System-Protokoll. Es handelt sich um einen offenen IETF-Standard, der in Request for Comments (RFC) definiert ist und unter dem jeder dieses Protokoll implementieren kann.

Volumes in Cloud Volumes Service werden für NFS-Clients freigegeben, indem ein Pfad exportiert wird, der für einen Client oder eine Gruppe von Clients zugänglich ist. Die Berechtigungen zum Mounten dieser Exporte werden durch Richtlinien und Regeln für den Export definiert, die von Cloud Volumes Service-Administratoren konfiguriert werden können.

Die NetApp NFS-Implementierung gilt als Gold-Standard für das Protokoll und wird in unzähligen Enterprise-NAS-Umgebungen eingesetzt. In den folgenden Abschnitten werden NFS, spezifische Sicherheitsfunktionen in Cloud Volumes Service sowie deren Implementierung behandelt.

Lokale UNIX-Standardbenutzer und -Gruppen

Cloud Volumes Service enthält mehrere UNIX Standard-Benutzer und -Gruppen für verschiedene grundlegende Funktionen. Diese Benutzer und Gruppen können derzeit nicht geändert oder gelöscht werden. Neue lokale Benutzer und Gruppen können derzeit nicht zu Cloud Volumes Service hinzugefügt werden. UNIX-Benutzer und -Gruppen außerhalb der Standardbenutzer und -Gruppen müssen von einem externen LDAP-Namensdienst bereitgestellt werden.

Die folgende Tabelle zeigt die Standardbenutzer und -Gruppen sowie die zugehörigen numerischen IDs. NetApp empfiehlt, keine neuen Benutzer oder Gruppen in LDAP oder auf den lokalen Clients zu erstellen, die

diese numerischen IDs erneut verwenden.

Standardbenutzer: Numerische IDs	Standardgruppen: Numerische IDs
• Stammverzeichnis:0 • Pcuser:65534 • Niemand:65535	• Stammverzeichnis:0 • Daemon: 1 • Pcuser:65534 • Niemand:65535

Bei der Verwendung von NFSv4.1 wird der Root-Benutzer möglicherweise als niemand angezeigt, wenn er Verzeichnislisting-Befehle auf NFS-Clients ausführt. Dies liegt an der Konfiguration der ID-Domänenzuordnung des Clients. Siehe Abschnitt genannt NFSv4.1 und der niemand-Benutzer/Gruppe Finden Sie weitere Informationen zu diesem Problem und wie Sie es lösen können.

Der Root-Benutzer

In Linux hat das Root-Konto Zugriff auf alle Befehle, Dateien und Ordner in einem Linux-basierten Dateisystem. Aufgrund der Leistungsfähigkeit dieses Kontos müssen Benutzer häufig aufgrund von Best Practices für die Sicherheit deaktiviert oder auf irgendeine Weise eingeschränkt werden. Bei NFS-Exporten kann die Leistung, die ein Root-Benutzer über die Dateien und Ordner hat, im Cloud Volumes Service über Exportrichtlinien und -Regeln gesteuert werden. Auch das Konzept wird als Root Squash bezeichnet.

Root-Squashing sorgt dafür, dass der Root-Benutzer, der auf eine NFS-Bereitstellung zugreift, auf den anonymen numerischen Benutzer 65534 (siehe Abschnitt „Der anonyme Benutzer“) und ist derzeit nur verfügbar, wenn CVS-Performance verwendet wird, indem Sie bei der Erstellung von Regeln für Exportrichtlinien aus für Root-Zugriff auswählen. Wenn der Root-Benutzer auf den anonymen Benutzer zerquetscht wird, hat er keinen Zugriff mehr auf das Ausführen von Chown oder "Setuid/setgid-Befehle (das klebrige Bit)" In Dateien oder Ordnern im NFS-Mount und Dateien oder Ordnern, die vom Root-Benutzer erstellt wurden, zeigen die Anon-UID als Eigentümer/Gruppe an. Darüber hinaus können NFSv4 ACLs nicht vom Root-Benutzer geändert werden. Der Root-Benutzer hat jedoch weiterhin Zugriff auf chmod und gelöschte Dateien, für die er keine expliziten Berechtigungen besitzt. Wenn Sie den Zugriff auf die Datei- und Ordnerberechtigungen eines Root-Benutzers beschränken möchten, ziehen Sie in Betracht, ein Volume mit NTFS ACLs zu verwenden und einen Windows-Benutzer mit dem Namen zu erstellen `root`, Und die gewünschten Berechtigungen auf die Dateien oder Ordner anwenden.

Der anonyme Benutzer

Die anonyme (anon) Benutzer-ID gibt eine UNIX-Benutzer-ID oder einen UNIX-Benutzernamen an, der Client-Anforderungen ohne gültige NFS-Anmeldeinformationen zugeordnet ist. Dies kann den Root-Benutzer einschließen, wenn Root-Squashing verwendet wird. Der anon-Benutzer in Cloud Volumes Service ist 65534.

Diese UID ist normalerweise dem Benutzernamen zugeordnet `nobody` Oder `nfsnobody` In Linux Umgebungen zu managen. Cloud Volumes Service verwendet auch 65534 als den lokalen UNIX-Benutzer` pcuser` (siehe Abschnitt “Lokale UNIX-Standardbenutzer und -Gruppen“), der auch der Standard-Fallback-Benutzer für Windows auf UNIX-Namenszuordnungen ist, wenn kein gültiger übereinstimmender UNIX-Benutzer in LDAP gefunden werden kann.

Aufgrund der Unterschiede bei Benutzernamen in Linux und Cloud Volumes Service für UID 65534, konnte die Namenszeichenfolge für Benutzer, die 65534 zugeordnet sind, bei der Verwendung von NFSv4.1 nicht übereinstimmen. Dies könnte zu sehen sein `nobody` Als Benutzer auf einigen Dateien und Ordnern. Siehe Abschnitt „NFSv4.1 und der niemand-Benutzer/Gruppe“ Für Informationen zu diesem Problem und zur Lösung

dieses Problems.

Zugriffssteuerung/Exporte

Der erste Export-/Freigabzugriff für NFS-Mounts wird über hostbasierte Exportrichtlinien gesteuert, die in einer Exportrichtlinie enthalten sind. Eine Host-IP, ein Hostname, ein Subnetz, eine Netzwerkgruppe oder eine Domäne sind definiert, um den Zugriff auf die Bereitstellung der NFS-Freigabe und die Zugriffsebene zu ermöglichen, die dem Host erlaubt ist. Die Konfigurationsoptionen für die Exportrichtlinie hängen von der Cloud Volumes Service-Ebene ab.

Für CVS-SW stehen die folgenden Optionen für die Konfiguration von Exportrichtlinien zur Verfügung:

- **Client-Match.** kommagetrennte Liste von IP-Adressen, kommagetrennte Liste von Hostnamen, Subnetzen, Netzgruppen, Domain-Namen.
- **RO/RW-Zugriffsregeln.** Wählen Sie Lese-/Schreibschutz oder Schreibschutz, um den Zugriff auf den Export zu steuern.CVS-Performance bietet die folgenden Optionen:
- **Client-Match.** kommagetrennte Liste von IP-Adressen, kommagetrennte Liste von Hostnamen, Subnetzen, Netzgruppen, Domain-Namen.
- **RO/RW-Zugriffsregeln.** Wählen Sie Lese-/Schreibschutz oder Schreibschutz, um den Zugriff auf den Export zu steuern.
- **Root-Zugriff (ein/aus).** konfiguriert Root Squash (siehe Abschnitt „Der Root-Benutzer„ Weitere Informationen).
- **Protokolltyp.** Dies beschränkt den Zugriff auf die NFS-Bereitstellung auf eine bestimmte Protokollversion. Wenn Sie sowohl NFSv3 als auch NFSv4.1 für das Volume angeben, lassen Sie entweder beide Felder leer oder aktivieren Sie beide Kontrollkästchen.
- **Kerberos-Sicherheitsstufe (wenn Kerberos aktivieren ausgewählt ist).** bietet die Optionen von krb5, krb5i und/oder krb5p für schreibgeschützten oder schreibgeschützten Zugriff.

Eigentümerschaft (chown) und Change Group (chgrp) ändern

NFS auf Cloud Volumes Service ermöglicht es dem Root-Benutzer nur chown/chgrp auf Dateien und Ordnern auszuführen. Andere Benutzer sehen ein `Operation not permitted` Fehler – auch bei den eigenen Dateien. Wenn Sie Root Squash verwenden (wie im Abschnitt “ beschriebenDer Root-Benutzer“), wird die Root zu einem nicht-Root-Benutzer gequetscht und darf keinen Zugriff auf Chown und chgrp haben. Derzeit gibt es in Cloud Volumes Service keine Problemumgehungen, um chown und chgrp für nicht-Root-Benutzer zu ermöglichen. Wenn Eigentumsänderungen erforderlich sind, ziehen Sie die Verwendung von doppelten Protokoll-Volumes in Erwägung und legen Sie den Sicherheitsstil auf NTFS fest, um die Berechtigungen von Windows-Seite aus zu steuern.

Berechtigungsmanagement

Cloud Volumes Service unterstützt beide Mode-Bits (z. B. 644, 777 usw. für rwx) und NFSv4.1 ACLs, um die Berechtigungen auf NFS-Clients für Volumes zu steuern, die den UNIX-Sicherheitsstil nutzen. Hierfür wird das standardmäßige Berechtigungsmanagement verwendet (z. B. chmod, chown oder nfs4_setfacl) und arbeitet mit jedem Linux-Client zusammen, der diese unterstützt.

Wenn Sie außerdem Dual-Protokoll-Volumes auf NTFS setzen, können NFS-Clients die Cloud Volumes Service-Namenszuweisung für Windows-Benutzer nutzen, die dann zur Behebung der NTFS-Berechtigungen verwendet werden. Dazu ist eine LDAP-Verbindung zu Cloud Volumes Service erforderlich, um numerische ID-zu-Benutzernamen-Übersetzungen bereitzustellen, da Cloud Volumes Service einen gültigen UNIX-Benutzernamen benötigt, um einen Windows-Benutzernamen korrekt zuzuordnen.

Bereitstellung granularer ACLs für NFSv3

Mode-Bit-Berechtigungen decken nur Besitzer, Gruppe und alle anderen in der Semantik ab. Dies bedeutet, dass für Basic NFSv3 keine granularen Benutzerzugriffskontrollen vorhanden sind. Cloud Volumes Service unterstützt weder POSIX ACLs noch erweiterte Attribute (wie z. B. Chattr), sodass granulare ACLs nur in den folgenden Szenarien mit NFSv3 möglich sind:

- NTFS Security Style Volumes (CIFS Server erforderlich) mit gültigen Zuordnungen von UNIX zu Windows-Benutzern.
- NFSv4.1 ACLs werden mithilfe eines Administrator-Clients unter Verwendung von NFSv4.1 angewendet.

Beide Methoden erfordern eine LDAP-Verbindung für das UNIX-Identitätsmanagement und eine gültige UNIX-Benutzer- und Gruppeninformationen (siehe Abschnitt "„LDAP“") Und sind nur mit CVS-Performance Instanzen verfügbar. Um Volumes im NTFS-Sicherheitsstil mit NFS zu verwenden, müssen Sie Dual-Protokoll (SMB und NFSv3) oder Dual-Protokoll (SMB und NFSv4.1) verwenden, auch wenn keine SMB-Verbindungen hergestellt werden. Um NFSv4.1 ACLs für NFSv3-Mounts zu verwenden, müssen Sie auswählen `Both (NFSv3/NFSv4.1)` Als Protokolltyp.

Normale UNIX Modus Bits bieten nicht die gleiche Granularitätsebene in Berechtigungen, die NTFS oder NFSv4.x ACLs bieten. In der folgenden Tabelle wird die Berechtigungsgranularität zwischen NFSv3-Modus-Bits und NFSv4.1 ACLs verglichen. Informationen zu NFSv4.1 ACLs finden Sie unter "nfs4_acl – NFSv4 Access Control-Listen".

Bits im NFSv3 Modus	NFSv4.1 ACLs
• Legen Sie bei der Ausführung die Benutzer-ID fest • Legen Sie bei der Ausführung die Gruppen-ID fest • Getauschtes Text speichern (nicht in POSIX definiert) • Leseberechtigung für Eigentümer • Schreibberechtigung für Eigentümer • Berechtigung für Eigentümer einer Datei ausführen oder die Berechtigung für Eigentümer im Verzeichnis suchen (suchen) • Berechtigung für Gruppe lesen • Schreibberechtigung für Gruppe • Berechtigung für eine Gruppe in einer Datei ausführen oder die Berechtigung für die Gruppe im Verzeichnis suchen (suchen) • Lesen Sie die Erlaubnis für andere • Schreibberechtigung für andere • Berechtigung für andere in einer Datei ausführen oder die Berechtigung für andere Personen im Verzeichnis suchen (suchen)	ACE-Typen (Access Control Entry) (allow/Deny/Audit) * Vererbung-Flags * Verzeichnis-Erben * Datei-Erben * No-propate-Erben * Erben-only Berechtigungen * Read-Data (Files) / list-Directory (Verzeichnisse) * Write-Data (Files) / create-file (Directories) * append-Data (files) / create-Unterverzeichnis (Directories) * execute (files) / change-Directory (Directories) * delete * delete-child * read-attributes * write-named-aCLL * write-awned-attributes * read-ACL Synchronize-awner

Schließlich ist die NFS-Gruppenmitgliedschaft (sowohl in NFSv3 als AUCH NFSV4.x) auf ein Standardlimit von 16 für AUTH_SYS begrenzt, gemäß den RPC-Paketlimits. NFS Kerberos bietet bis zu 32 Gruppen und NFSv4

ACLs entfernen die Beschränkung durch granulare Benutzer- und Gruppen-ACLs (bis zu 1024 Einträge pro ACE).

Darüber hinaus bietet Cloud Volumes Service erweiterte Gruppen-Support, um die maximal unterstützten Gruppen auf 32 zu erweitern. Dazu ist eine LDAP-Verbindung zu einem LDAP-Server erforderlich, der gültige UNIX-Benutzer- und Gruppenidentitäten enthält. Weitere Informationen zur Konfiguration finden Sie unter "Erstellen und Managen von NFS-Volumes" In der Google-Dokumentation.

NFSv3-Benutzer- und Gruppen-IDs

NFSv3-Benutzer- und Gruppen-IDs kommen über das Netzwerk als numerische IDs und nicht als Namen. Cloud Volumes Service bietet keine Nutzername-Auflösung für diese numerischen IDs mit NFSv3, mit UNIX-Sicherheitsstil-Volumes mit Just-Mode-Bits. Wenn NFSv4.1 ACLs vorhanden sind, ist eine numerische ID-Suche und/oder Suche nach Namespace erforderlich, um die ACL ordnungsgemäß zu lösen – sogar bei Verwendung von NFSv3. Bei NTFS-Volumes im Sicherheitsstil muss Cloud Volumes Service eine numerische ID einem gültigen UNIX-Benutzer auflösen und dann einem gültigen Windows-Benutzer zuordnen, um Zugriffsrechte auszuhandeln.

Sicherheitseinschränkungen von NFSv3 Benutzer- und Gruppen-IDs

Bei NFSv3 müssen Client und Server niemals bestätigen, dass der Benutzer, der einen Lese- oder Schreibversuch mit einer numerischen ID versucht, ein gültiger Benutzer ist; er ist einfach implizit vertrauenswürdig. Das öffnet das Dateisystem bis zu potenziellen Verstößen, indem es einfach eine numerische ID vortäuscht. Um Sicherheitslücken wie diese zu verhindern, gibt es einige Optionen für Cloud Volumes Service.

- Die Implementierung von Kerberos für NFS zwingt Benutzer, sich mit einem Benutzernamen und einem Kennwort oder einer Keytab-Datei zu authentifizieren, um ein Kerberos-Ticket für den Zugriff in einem Mount zu erhalten. Kerberos ist mit CVS-Performance-Instanzen und nur mit NFSv4.1 verfügbar.
- Die Einschränkung der Liste der Hosts in Ihren Exportrichtlinien beschränkt die Grenzen, die NFSv3-Clients auf das Cloud Volumes Service-Volume zugreifen können.
- Durch die Verwendung von Dual-Protokoll-Volumes und die Anwendung von NTFS-ACLs auf das Volume sind NFSv3-Clients gezwungen, numerische IDs auf gültige UNIX-Benutzernamen zu lösen, um sich für den ordnungsgemäßen Zugriff auf Mounts zu authentifizieren. Dazu muss LDAP aktiviert und UNIX-Benutzer- und Gruppenidentitäten konfiguriert werden.
- Das Squashing des Root-Benutzers begrenzt den Schaden, den ein Root-Benutzer auf einen NFS-Mount tun kann, aber das Risiko wird nicht vollständig beseitigt. Weitere Informationen finden Sie im Abschnitt „Der Root-Benutzer.“

Letztendlich ist die NFS-Sicherheit auf das beschränkt, was die Protokollversion verwendet, die Sie Angebote verwenden. NFSv3, obwohl mehr Performance im Allgemeinen als NFSv4.1, nicht dasselbe Maß an Sicherheit bietet.

NFSv4.1

NFSv4.1 bietet im Vergleich zu NFSv3 eine höhere Sicherheit und Zuverlässigkeit. Dies hat folgende Gründe:

- Integrierte Sperrung über einen Leasingbasierten Mechanismus
- Statusorientierte Sessions
- Alle NFS-Funktionen über einen einzelnen Port (2049)
- Nur TCP

- ID-Domain-Zuordnung
- Kerberos Integration (NFSv3 kann Kerberos verwenden, aber nur für NFS, nicht für zusätzliche Protokolle wie NLM)

NFSv4.1-Abhängigkeiten

Aufgrund der zusätzlichen Sicherheitsfunktionen in NFSv4.1 sind einige externe Abhängigkeiten beteiligt, die nicht für die Verwendung von NFSv3 benötigt wurden (ähnlich wie SMB Abhängigkeiten wie Active Directory erfordert).

NFSv4.1 ACLs

Cloud Volumes Service bietet Unterstützung für NFSv4.x ACLs, die bestimmte Vorteile gegenüber normalen POSIX-Berechtigungen bieten, wie z. B.:

- Granulare Steuerung des Benutzerzugriffs auf Dateien und Verzeichnisse
- Bessere NFS-Sicherheit
- Bessere Interoperabilität mit CIFS/SMB
- Entfernung der NFS-Beschränkung von 16 Gruppen pro Benutzer mit AUTH_SYS-Sicherheit
- ACLs umgehen die Notwendigkeit einer Gruppen-ID-Lösung (GID), die effektiv das GID limitNFSv4.1 ACLs werden von NFS-Clients gesteuert, nicht von Cloud Volumes Service. Um NFSv4.1 ACLs zu verwenden, stellen Sie sicher, dass die Softwareversion Ihres Clients sie unterstützt und die richtigen NFS-Dienstprogramme installiert sind.

Kompatibilität zwischen NFSv4.1 ACLs und SMB-Clients

NFSv4 ACLs unterscheiden sich von Windows ACLs auf Dateiebene (NTFS ACLs), haben aber ähnliche Funktionen. In NAS-Umgebungen mit mehreren Protokollen, wenn NFSv4.1 ACLs vorhanden sind und Sie Dual-Protokoll-Zugriff verwenden (NFS und SMB auf den gleichen Datensätzen), werden Clients mit SMB2.0 und später nicht in der Lage sein, ACLs von Windows-Sicherheitregisterkarten anzuzeigen oder zu verwalten.

Funktionsweise von NFSv4.1 ACLs

Als Referenz sind folgende Begriffe definiert:

- **Access control list (ACL).** eine Liste der Berechtigungs Einträge.
- **Zugangskontrolleintrag (ACE).** Ein Berechtigungseintrag in der Liste.

Wenn ein Client während einer SETATTR-Operation eine NFSv4.1-ACL für eine Datei setzt, setzt Cloud Volumes Service diese ACL für das Objekt und ersetzt eine vorhandene ACL. Wenn es keine ACL für eine Datei gibt, werden die Modus-Berechtigungen für die Datei von EIGENTÜMER@, GROUP@ und EVERYONE@ berechnet. Wenn SUID/SGID/STICKY Bits in der Datei vorhanden sind, sind diese nicht betroffen.

Wenn ein Client während einer GETATTR Operation eine NFSv4.1 ACL für eine Datei erhält, liest Cloud Volumes Service die mit dem Objekt verknüpfte NFSv4.1 ACL, erstellt eine Liste von Aces und gibt die Liste an den Client zurück. Wenn die Datei über eine NT ACL oder Mode Bits verfügt, wird eine ACL aus Modus-Bits erstellt und an den Client zurückgegeben.

Der Zugriff wird verweigert, wenn in der ACL ein ACE VERWEIGERN vorhanden ist; der Zugriff wird gewährt, wenn ACE ZULASSEN vorhanden ist. Der Zugang wird jedoch auch verweigert, wenn keines der Asse in der ACL vorhanden ist.

Ein Sicherheitsdeskriptor besteht aus einer Sicherheits-ACL (SACL) und einer Ermessensdatei (Discretionary ACL, DACL). Bei der Ausführung von NFSv4.1 mit CIFS/SMB ist die DACL 1-to-One-Zuordnung mit NFSv4 und CIFS. Die DACL besteht aus DEM ERLAUBEN und DEN LEUGNEN Assen.

Wenn ein einfaches `chmod` Wird auf einer Datei oder einem Ordner mit NFSv4.1 ACLs gesetzt ausgeführt, bestehende Benutzer- und Gruppen-ACLs bleiben erhalten, aber der STANDARDEIGENTÜMER@, GROUP@, EVERYONE@ ACLs werden geändert.

Ein Client, der NFSv4.1 ACLs verwendet, kann ACLs für Dateien und Verzeichnisse auf dem System festlegen und anzeigen. Wenn eine neue Datei oder ein Unterverzeichnis in einem Verzeichnis erstellt wird, das über eine ACL verfügt, erbt dieses Objekt alle Asse in der ACL, die mit dem entsprechenden gekennzeichnet wurden "Ervererbungsflaggen".

Wenn eine Datei oder ein Verzeichnis über eine NFSv4.1-ACL verfügt, wird diese ACL verwendet, um den Zugriff zu steuern, unabhängig davon, welches Protokoll für den Zugriff auf die Datei oder das Verzeichnis verwendet wird.

Dateien und Verzeichnisse erben Asse von NFSv4 ACLs auf übergeordneten Verzeichnissen (möglicherweise mit entsprechenden Änderungen), solange die Asse mit den korrekten Vererbung-Flags markiert wurden.

Wenn eine Datei oder ein Verzeichnis als Ergebnis einer NFSv4-Anforderung erstellt wird, hängt die ACL für die resultierende Datei oder das Verzeichnis davon ab, ob die Dateierstellungsanforderung eine ACL oder nur standardmäßige UNIX-Dateizugriffsberechtigungen enthält. Die ACL hängt auch davon ab, ob das übergeordnete Verzeichnis über eine ACL verfügt.

- Wenn die Anforderung eine ACL enthält, wird diese ACL verwendet.
- Wenn die Anforderung nur standardmäßige UNIX-Dateizugriffsberechtigungen enthält und das übergeordnete Verzeichnis keine ACL besitzt, wird der Client-Dateimodus verwendet, um standardmäßige UNIX-Dateizugriffsberechtigungen festzulegen.
- Wenn die Anforderung nur Standardberechtigungen für den Zugriff auf UNIX-Dateien enthält und das übergeordnete Verzeichnis über eine nicht vererbbare ACL verfügt, wird eine Standard-ACL auf Basis der Mode-Bits, die an die Anforderung übergeben wurden, auf dem neuen Objekt festgelegt.
- Wenn die Anforderung nur Standardzugriffsberechtigungen für UNIX-Dateien enthält, aber das übergeordnete Verzeichnis über eine ACL verfügt, werden die Asse in der ACL des übergeordneten Verzeichnisses von der neuen Datei oder dem neuen Verzeichnis geerbt, solange die Aces mit den entsprechenden Vererbung-Flags gekennzeichnet wurden.

ACE-Berechtigungen

Die Berechtigungen für NFSv4.1 ACLs verwenden eine Reihe von Groß- und Kleinbuchstaben (z. B. `rxtncy`) Um den Zugriff zu steuern. Weitere Informationen zu diesen Buchstabenwerten finden Sie unter "WIE: Verwenden Sie NFSv4 ACL".

NFSv4.1 ACL-Verhalten mit Umask und ACL-Vererbung

"NFSv4 ACLs bieten die Möglichkeit, eine ACL-Vererbung anzubieten". ACL-Vererbung bedeutet, dass Dateien oder Ordner, die unter Objekten mit NFSv4.1 ACLs-Satz erstellt wurden, die ACLs basierend auf der Konfiguration des erben können "ACL-Vererbungskennzeichnung".

"Umfragen" Wird verwendet, um die Berechtigungsstufe zu steuern, auf der Dateien und Ordner in einem Verzeichnis ohne Administratorinteraktion erstellt werden. Standardmäßig können mit Cloud Volumes Service übernommene ACLs überschrieben werden. Dies ist ein erwartetes Verhalten wie per "RFC 5661".

ACL-Formatierung

NFSv4.1 ACLs haben bestimmte Formatierung. Das folgende Beispiel ist ein ACE-Satz für eine Datei:

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

Das vorangegangene Beispiel folgt den Richtlinien im ACL-Format von:

```
type:flags:principal:permissions
```

Einen Typ von `A` Bedeutet „Zulassen“. Die Erben-Flags werden in diesem Fall nicht festgelegt, da der Principal keine Gruppe ist und keine Vererbung beinhaltet. Da es sich bei ACE nicht um EINEN AUDIT-Eintrag handelt, müssen die Audit-Flags nicht festgelegt werden. Weitere Informationen zu NFSv4.1 ACLs finden Sie unter "http://linux.die.net/man/5/nfs4_acl".

Wenn die NFSv4.1 ACL nicht richtig eingestellt ist (oder eine Namenszeichenfolge nicht vom Client und Server aufgelöst werden kann), verhält sich die ACL möglicherweise nicht wie erwartet. Andernfalls kann die ACL-Änderung nicht angewendet werden und einen Fehler verursacht.

Beispielfehler sind:

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

Explizites ABLEHNEN

Die Berechtigungen in NFSv4.1 können explizite DENY-Attribute für EIGENTÜMER, GRUPPE und ALLE enthalten. Das liegt daran, dass NFSv4.1 ACLs Standard-Deny sind. Dies bedeutet, dass, wenn eine ACL nicht ausdrücklich von einem ACE gewährt wird, sie verweigert wird. Explizite DENY-Attribute überschreiben alle ZUGRIFFSOPTIONEN, explizit oder nicht.

DENY Aces werden mit einem Attribut-Tag von festgelegt `D`.

Im folgenden Beispiel ist DER GRUPPE@ alle Lese- und Ausführungsberechtigungen erlaubt, aber der gesamte Schreibzugriff wird verweigert.

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

DENY Aces sollten möglichst vermieden werden, da sie verwirrend und kompliziert sein können; ACLS, die

nicht explizit definiert sind, WERDEN implizit verweigert. Wenn Asse VERWEIGERN festgelegt sind, wird Benutzern möglicherweise der Zugriff verweigert, wenn sie erwarten, dass ihnen Zugriff gewährt wird.

Der vorhergehende Satz von Assen entspricht 755 im Modus Bits, was bedeutet:

- Der Eigentümer hat volle Rechte.
- Gruppen haben schreibgeschützt.
- Andere haben nur gelesen.

Selbst wenn die Berechtigungen auf das Äquivalent von 775 angepasst werden, kann der Zugriff aufgrund der expliziten DENY-Einstellung für ALLE verweigert werden.

Abhängigkeiten für die Zuordnung der NFSv4.1 ID-Domäne

NFSv4.1 nutzt die ID-Domain-Mapping-Logik als Sicherheitsschicht, um zu überprüfen, ob ein Benutzer, der auf einen NFSv4.1-Mount zugreifen möchte, tatsächlich derjenige ist, der behauptet. In diesen Fällen hängt der vom NFSv4.1-Client stammende Benutzername und Gruppenname eine Namenszeichenfolge an und sendet sie an die Cloud Volumes Service-Instanz. Wenn diese Kombination aus Benutzername/Gruppenname und ID-Zeichenfolge nicht übereinstimmt, dann wird der Benutzer und/oder die Gruppe auf den Standard-niemand-Benutzer gesetzt, der im angegeben wurde `/etc/idmapd.conf` Datei auf dem Client.

Diese ID-Zeichenfolge ist eine Voraussetzung für die ordnungsgemäße Einhaltung von Berechtigungen, insbesondere wenn NFSv4.1 ACLs und/oder Kerberos verwendet werden. Daher sind Serverabhängigkeiten des Nameservice wie LDAP-Server erforderlich, um die Konsistenz zwischen Clients und Cloud Volumes Service für eine ordnungsgemäße Identitätsauflösung von Benutzer und Gruppennamen zu gewährleisten.

Cloud Volumes Service verwendet einen statischen Standard-ID-Domänennamen von `defaultv4iddomain.com`. NFS-Clients verwenden standardmäßig den DNS-Domain-Namen für seine ID-Domain-Namen-Einstellungen. Sie können den ID-Domain-Namen in jedoch manuell anpassen `/etc/idmapd.conf`.

Wenn LDAP in Cloud Volumes Service aktiviert ist, dann Cloud Volumes Service automatisiert die NFS ID Domain zu ändern, was für die Suche Domain in DNS konfiguriert ist und Clients nicht geändert werden müssen, es sei denn sie verwenden unterschiedliche DNS Domain Suchnamen.

Wenn Cloud Volumes Service einen Benutzernamen oder Gruppennamen in lokalen Dateien oder LDAP auflösen kann, wird die Domänenzeichenfolge verwendet und nicht übereinstimmende Domänen-IDs Squash an niemand. Wenn Cloud Volumes Service einen Benutzernamen oder Gruppennamen nicht in lokalen Dateien oder LDAP finden kann, wird der numerische ID-Wert verwendet, und der NFS-Client löst den Namen richtig aus (dies entspricht dem NFSv3-Verhalten).

Ohne die NFSv4.1 ID-Domäne des Clients zu ändern, um mit dem zu übereinstimmen, was der Cloud Volumes Service-Datenträger verwendet, sehen Sie folgendes Verhalten:

- UNIX-Benutzer und -Gruppen mit lokalen Einträgen in Cloud Volumes Service (wie root, wie in lokalen UNIX-Benutzern und -Gruppen definiert) werden auf den nobody-Wert gequetscht.
- UNIX-Benutzer und -Gruppen mit Einträgen in LDAP (wenn Cloud Volumes Service so konfiguriert ist, dass sie LDAP verwenden), nehmen keine Wimpern auf, wenn sich DNS-Domänen zwischen NFS-Clients und Cloud Volumes Service unterscheiden.
- UNIX-Benutzer und -Gruppen ohne lokale Einträge oder LDAP-Einträge verwenden den numerischen ID-Wert und lösen den auf dem NFS-Client angegebenen Namen. Wenn auf dem Client kein Name vorhanden ist, wird nur die numerische ID angezeigt.

Die Ergebnisse des vorhergehenden Szenarios:

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

Wenn die Client- und Server-ID-Domänen übereinstimmen, wird die gleiche Dateiliste angezeigt:

```
# ls -la
total 8
drwxr-xr-x 2 root   root         4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root         4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835         9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

Weitere Informationen zu diesem Thema und wie man es löst, finden Sie im Abschnitt „NFSv4.1 und der niemand-Benutzer/Gruppe.“

Kerberos Abhängigkeiten

Wenn Sie Kerberos mit NFS verwenden möchten, müssen Sie für Cloud Volumes Service Folgendes haben:

- Active Directory-Domäne für Kerberos-Verteilzentrum-Dienste (KDC)
- Active Directory-Domäne mit Benutzer- und Gruppenattributen, die mit UNIX-Informationen für LDAP-Funktionalität gefüllt sind (NFS-Kerberos im Cloud Volumes Service benötigt für die ordnungsgemäße Funktion einen Benutzer-SPN für UNIX-Benutzerzuordnung).
- LDAP auf der Cloud Volumes Service-Instanz aktiviert
- Active Directory-Domäne für DNS-Services

NFSv4.1 und der niemand-Benutzer/Gruppe

Eines der häufigsten Probleme bei einer NFSv4.1-Konfiguration ist, wenn eine Datei oder ein Ordner in einer Auflistung mit angezeigt wird `ls` Als im Besitz des `user:group` Kombination von `nobody:nobody`.

Beispiel:

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

Und die numerische ID lautet `99`.

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

In manchen Fällen wird die Datei möglicherweise den korrekten Eigentümer, aber angezeigt `nobody` Als Gruppe.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

Wer ist niemand?

Der `nobody` Benutzer in NFSv4.1 unterscheidet sich von dem `nfsnobody` Benutzer: Sie können anzeigen, wie ein NFS Client jeden Benutzer sieht, indem Sie die ausführen `id` Befehl:

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

Mit NFSv4.1, das `nobody` Der von definierte Standardbenutzer ist der Benutzer `idmapd.conf` Datei und kann als jeder Benutzer definiert werden, den Sie verwenden möchten.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

Warum passiert das?

Da Sicherheit durch Namenszeichenzuordnung ein Schlüsseltenet von NFSv4.1-Operationen ist, ist das Standardverhalten, wenn eine Namenszeichenfolge nicht richtig übereinstimmt, dass der Benutzer zu einem Squash, der normalerweise keinen Zugriff auf Dateien und Ordner hat, die Benutzer und Gruppen gehören.

Wenn Sie sehen `nobody` Für den Benutzer und/oder die Gruppe in Dateilisten bedeutet dies im Allgemeinen, dass etwas in NFSv4.1 falsch konfiguriert ist. Hier kann die Empfindlichkeit des Falles ins Spiel kommen.

Wenn z. B. user1@CVSDEMO.LOCAL (uid 1234, gid 1234) auf einen Export zugreift, muss Cloud Volumes Service user1@CVSDEMO.LOCAL (uid 1234, gid 1234) finden können. Wenn der Benutzer in Cloud Volumes Service ist USER1@CVSDEMO.LOCAL, dann wird es nicht übereinstimmen (GROSSUSER1 vs. Kleinbuchstaben user1). In vielen Fällen können Sie Folgendes in der Meldungsdatei auf dem Client sehen:

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

Der Client und Server müssen beide zustimmen, dass ein Benutzer tatsächlich der Meinung ist, dass er sein soll. Sie müssen daher Folgendes überprüfen, um sicherzustellen, dass der Benutzer, der den Client sieht, dieselben Informationen hat wie der Benutzer, den Cloud Volumes Service sieht.

- **NFSv4.x ID Domain.** Client: `idmapd.conf` Datei; Cloud Volumes Service verwendet `defaultv4iddomain.com` Und kann nicht manuell geändert werden. Bei Verwendung von LDAP mit NFSv4.1 ändert Cloud Volumes Service die ID-Domäne in das, was die DNS-Suchdomäne verwendet, was mit der AD-Domäne identisch ist.
- **Benutzername und numerische IDs.** Dies legt fest, wo der Client nach Benutzernamen sucht und die Namensdienstschalter-Konfiguration nutzt – Client: `nsswitch.conf` Und/oder lokale Passwd- und Gruppendateien; Cloud Volumes Service erlaubt keine Änderungen, sondern fügt der Konfiguration automatisch LDAP hinzu, wenn sie aktiviert ist.
- **Gruppenname und numerische IDs.** Dies legt fest, wo der Client nach Gruppennamen sucht und nutzt die Namensdienst-Switch-Konfiguration – Client: `nsswitch.conf` Und/oder lokale Passwd- und Gruppendateien; Cloud Volumes Service erlaubt keine Änderungen, sondern fügt der Konfiguration automatisch LDAP hinzu, wenn sie aktiviert ist.

In fast allen Fällen, wenn Sie sehen `nobody` Bei Benutzer- und Gruppenlisten von Clients handelt es sich um das Problem der Übersetzung von Benutzer- oder Gruppennamen-Domänen-ID zwischen Cloud Volumes Service und dem NFS-Client. Um dieses Szenario zu vermeiden, verwenden Sie LDAP, um Benutzer- und Gruppeninformationen zwischen Clients und Cloud Volumes Service aufzulösen.

Anzeigen von Name-ID-Strings für NFSv4.1 auf Clients

Wenn Sie NFSv4.1 verwenden, gibt es ein Name-String-Mapping, das während NFS-Vorgängen stattfindet, wie zuvor beschrieben.

Zusätzlich zu verwenden `/var/log/messages` Um ein Problem mit NFSv4-IDs zu finden, können Sie das verwenden "Nfsidmap -l" Befehl auf dem NFS Client, um anzuzeigen, welche Benutzernamen der NFSv4-Domäne ordnungsgemäß zugeordnet haben.

Dies wird beispielsweise nach einem Benutzer ausgegeben, der vom Client gefunden werden kann und Cloud Volumes Service auf einen NFSv4.x Mount zugreift:

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

Wenn ein Benutzer, der der NFSv4.1 ID-Domäne nicht ordnungsgemäß zugeordnet ist (in diesem Fall `netapp-user`) Versucht, auf denselben Mount zuzugreifen und berührt eine Datei, sie sind zugewiesen

`nobody:nobody`, Wie erwartet.

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

Der `nfsidmap -l` Ausgabe zeigt den Benutzer an `pcuser` Im Display, aber nicht `netapp-user`; Dies ist der anonyme Benutzer in unserer Export-Policy Regel (`65534`).

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

SMB

"SMB" Das von Microsoft entwickelte Netzwerk-File-Sharing-Protokoll bietet zentralisierte Benutzer-/Gruppenauthentifizierung, Berechtigungen, Sperren und Dateifreigabe für mehrere SMB-Clients über ein Ethernet-Netzwerk. Dateien und Ordner werden Clients über Freigaben angezeigt, die mit einer Vielzahl von Freigabeeigenschaften konfiguriert werden können und die Zugriffskontrolle über Berechtigungen auf Share-Ebene bietet. SMB kann jedem Client angezeigt werden, der Protokolle unterstützt, einschließlich Windows-, Apple- und Linux-Clients.

Cloud Volumes Service unterstützt die Protokollversionen SMB 2.1 und 3.x.

Zugriffssteuerung/SMB-Freigaben

- Wenn ein Windows-Benutzername Zugriff auf das Cloud Volumes Service-Volume anfordert, sucht Cloud Volumes Service nach einem UNIX-Benutzernamen mit den von Cloud Volumes Service-Administratoren konfigurierten Methoden.

- Wenn ein externer UNIX Identity Provider (LDAP) konfiguriert ist und Windows/UNIX Nutzernamen identisch sind, werden Windows-Benutzernamen ohne zusätzliche Konfiguration 1:1 zu UNIX Benutzernamen mappen. Wenn LDAP aktiviert ist, wird Active Directory verwendet, um die UNIX-Attribute für Benutzer- und Gruppenobjekte zu hosten.
- Wenn Windows-Namen und UNIX-Namen nicht identisch sind, muss LDAP konfiguriert werden, damit Cloud Volumes Service die LDAP-Namenszuordnungskonfiguration verwenden kann (siehe Abschnitt "„LDAP für asymmetrisches Namenszuordnungen verwenden“").
- Wenn LDAP nicht verwendet wird, werden Windows SMB-Benutzer einem lokalen UNIX-Standardbenutzer zugeordnet `pcuser` Im Cloud Volumes Service. Das bedeutet Dateien, die von Benutzern in Windows geschrieben wurden, die dem zugeordnet sind `pcuser` Zeigen Sie die UNIX-Eigentümerschaft als `pcuser` In NAS-Umgebungen mit mehreren Protokollen. `pcuser` Hier ist effektiv das `nobody` Benutzer in Linux-Umgebungen (UID 65534).

Bei Implementierungen nur mit SMB gilt das `pcuser` Mapping tritt immer noch auf, aber es wird keine Rolle spielen, weil Windows-Benutzer und Gruppen-Eigentum korrekt angezeigt wird und NFS-Zugriff auf das SMB-only Volumen ist nicht erlaubt. Außerdem unterstützen SMB-only Volumes nach der Erstellung keine Konvertierung in NFS- oder Dual-Protokoll-Volumes.

Windows nutzt Kerberos für die Benutzerauthentifizierung mit den Active Directory-Domänencontrollern, die einen Austausch von Benutzername/Passwort mit den AD-DCs erfordern, die sich außerhalb der Cloud Volumes Service-Instanz befinden. Kerberos-Authentifizierung wird verwendet, wenn das verwendet wird `\\SERVERNAME` UNC-Pfad wird von den SMB-Clients verwendet, und folgende lautet „true“:

- DNS A/AAAA-Eintrag für SERVERNAME vorhanden
- Für SERVERNAME ist ein gültiger SPN für SMB/CIFS-Zugriff vorhanden

Wenn ein Cloud Volumes Service SMB Volume erstellt wird, wird der Name des Maschinenkontos wie in Abschnitt definiert erstellt "„Wie Cloud Volumes Service in Active Directory erscheint.“" Der Name des Computerkontos wird auch zum SMB-Freigabepfad, da Cloud Volumes Service dynamische DNS (DDNS) verwendet, um die erforderlichen A/AAAA- und PTR-Einträge im DNS und die erforderlichen SPN-Einträge auf dem Computerkonto-Principal zu erstellen.

> Damit PTR-Einträge erstellt werden können, muss auf dem DNS-Server die Reverse-Lookup-Zone für die IP-Adresse der Cloud Volumes Service-Instanz vorhanden sein.

Beispielsweise verwendet dieses Cloud Volumes Service Volume den folgenden UNC-Freigabepfad: `\\cvs-east- 433d.cvsdemo.local`.

Im Active Directory sind dies die von Cloud Volumes Service generierten SPN-Einträge:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

Dies ist das Ergebnis des DNS-Vorwärts-/Reverse-Lookups:

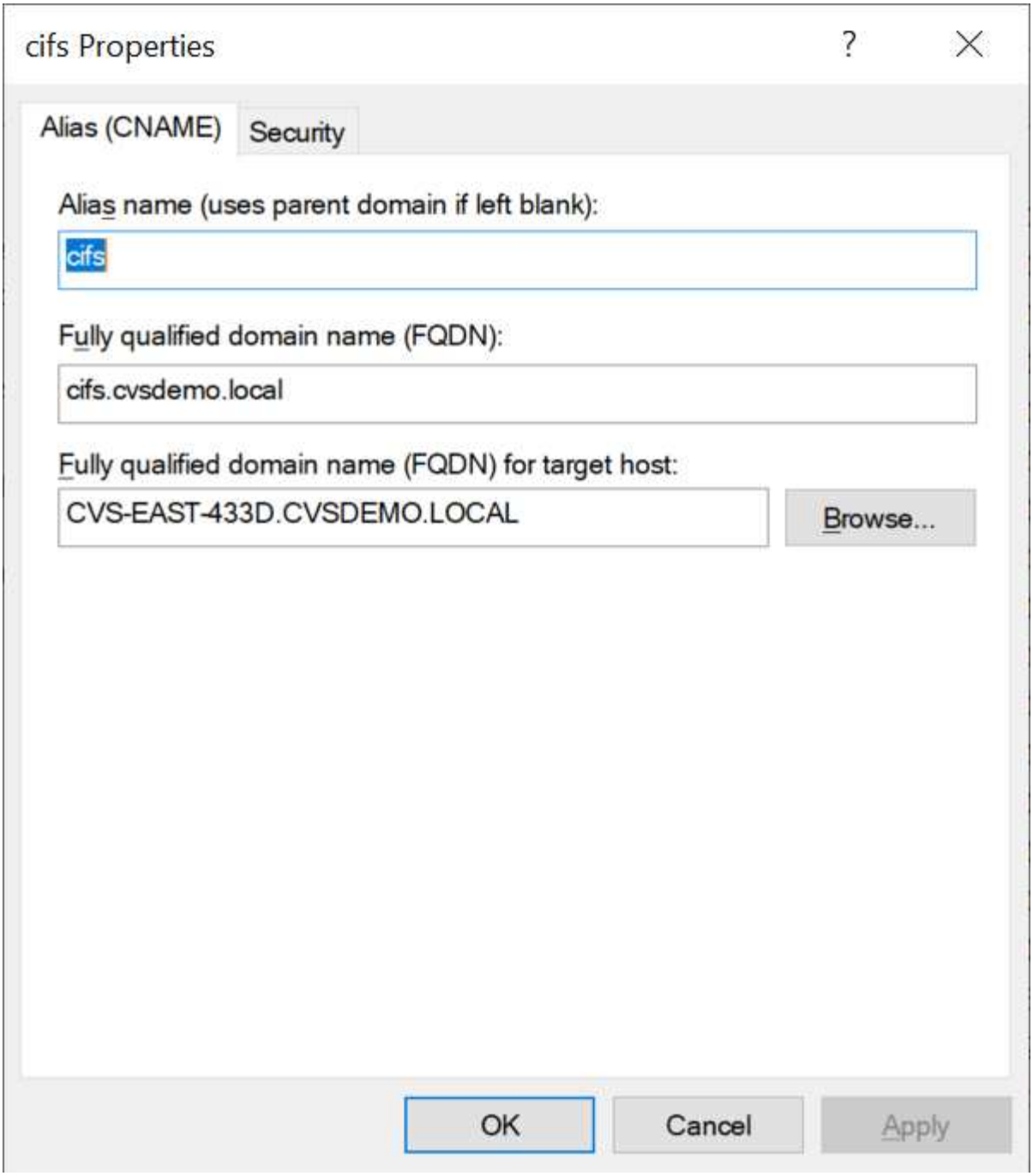
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

Optional kann eine bessere Zugriffssteuerung durch Aktivieren/Aktivieren der SMB-Verschlüsselung für SMB-Freigaben in Cloud Volumes Service angewendet werden. Wenn die SMB-Verschlüsselung von einem der Endpunkte nicht unterstützt wird, ist der Zugriff nicht zulässig.

Verwenden von SMB-Namenaliasen

In einigen Fällen kann es ein Sicherheitsbedenken für Endbenutzer sein, den Namen des für Cloud Volumes Service verwendeten Computerkontos zu kennen. In anderen Fällen möchten Sie Ihren Endbenutzern möglicherweise lediglich einen einfacheren Zugriffspfad bieten. In diesen Fällen können Sie SMB-Aliase erstellen.

Wenn Sie Aliase für den SMB-Freigabepfad erstellen möchten, können Sie den Namen CNAME-Datensatz in DNS verwenden. Beispiel: Wenn Sie den Namen verwenden möchten `\\CIFS` Auf Freigaben statt auf `\\cvs-east- 433d.cvsdemo.local`, Aber Sie möchten immer noch Kerberos-Authentifizierung verwenden, ein CNAME in DNS, der auf den vorhandenen A/AAAA-Datensatz verweist, und ein zusätzlicher SPN, der dem bestehenden Computerkonto hinzugefügt wurde, bietet Kerberos-Zugriff.



Dies ist das resultierende DNS-Weitersuchergebnis nach dem Hinzufügen eines CNAME:

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

Dies ist die resultierende SPN-Abfrage nach dem Hinzufügen neuer SPNs:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

In einer Paketerfassung können wir die Session-Setup-Anforderung mit dem SPN sehen, der an den CNAME gebunden ist.

```
431 4.156722    SMB2    308 Negotiate Protocol Response
432 4.156785    SMB2    232 Negotiate Protocol Request
434 4.158108    SMB2    374 Negotiate Protocol Response
435 4.160977    SMB2   1978 Session Setup Request
437 4.166224    SMB2    322 Session Setup Response
438 4.166891    SMB2    152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063    SMB2    138 Tree Connect Response

    realm: CVSDEMO.LOCAL
  ⌄ sname
      name-type: kRB5-NT-SRV-INST (2)
    ⌄ sname-string: 2 items
        SNameString: cifs
        SNameString: cifs
  ⌄ enc-part
      etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

SMB-Authentifizierungsdialekte

Cloud Volumes Service unterstützt Folgendes "Dialekte" Für SMB-Authentifizierung:

- LM
- NTLM
- NTLMv2
- Kerberos

Kerberos-Authentifizierung für SMB-Freigabe-Zugriff ist die sicherste Authentifizierungsstufe, die Sie verwenden können. Mit AES- und SMB-Verschlüsselung wird die Sicherheit weiter erhöht.

Cloud Volumes Service unterstützt außerdem die Rückwärtskompatibilität für die LM- und NTLM-Authentifizierung. Wenn Kerberos falsch konfiguriert ist (z. B. beim Erstellen von SMB-Aliasen), geht der Zugriff auf Shares auf schwächere Authentifizierungsmethoden zurück (z. B. NTLMv2). Da diese Mechanismen weniger sicher sind, sind sie in einigen Active Directory-Umgebungen deaktiviert. Wenn schwächere Authentifizierungsmethoden deaktiviert sind und Kerberos nicht richtig konfiguriert ist, schlägt der Zugriff auf die Freigabe fehl, da keine gültige Authentifizierungsmethode vorhanden ist, auf die Sie zurückgreifen können.

Informationen zum Konfigurieren/Anzeigen der unterstützten Authentifizierungsstufen in Active Directory finden Sie unter "Netzwerksicherheit: Authentifizierungsebene des LAN Managers".

Berechtigungsmodelle

NTFS/Dateiberechtigungen

NTFS-Berechtigungen sind die Berechtigungen, die auf Dateien und Ordner in Dateisystemen angewendet werden, die der NTFS-Logik entsprechen. Sie können NTFS-Berechtigungen in anwenden `Basic` Oder `Advanced` Und kann auf festgelegt werden `Allow` Oder `Deny` Für die Zugriffssteuerung.

Grundlegende Berechtigungen beinhalten Folgendes:

- Volle Kontrolle
- Ändern
- Lesen Und Ausführen
- Lesen
- Schreiben

Wenn Sie Berechtigungen für einen Benutzer oder eine Gruppe festlegen, die als ACE bezeichnet wird, befindet sie sich in einer ACL. NTFS-Berechtigungen verwenden die gleichen Grundlagen zum Lesen/Schreiben/Ausführen wie UNIX-Mode-Bits, können aber auch auf granularere und erweiterte Zugriffskontrollen (auch bekannt als Spezialberechtigungen), wie zum Beispiel Besitzrechte übernehmen, Ordner erstellen/Daten anhängen, Attribute schreiben usw. erweitern.

Bits des Standard-UNIX-Modus bieten nicht dieselbe Granularität wie NTFS-Berechtigungen (beispielsweise die Möglichkeit, Berechtigungen für einzelne Benutzer und Gruppenobjekte in einer ACL festzulegen oder erweiterte Attribute festzulegen). NFSv4.1 ACLs bieten jedoch dieselben Funktionen wie NTFS ACLs.

NTFS-Berechtigungen sind spezifischer als Freigabeberechtigungen und können in Verbindung mit Freigabeberechtigungen verwendet werden. Bei NTFS-Berechtigungsstrukturen gilt die restriktivere Vorgehensweise. Als solche überschreibt explizite Denals für einen Benutzer oder eine Gruppe sogar die volle Kontrolle, wenn die Zugriffsrechte definiert werden.

NTFS-Berechtigungen werden von Windows SMB Clients gesteuert.

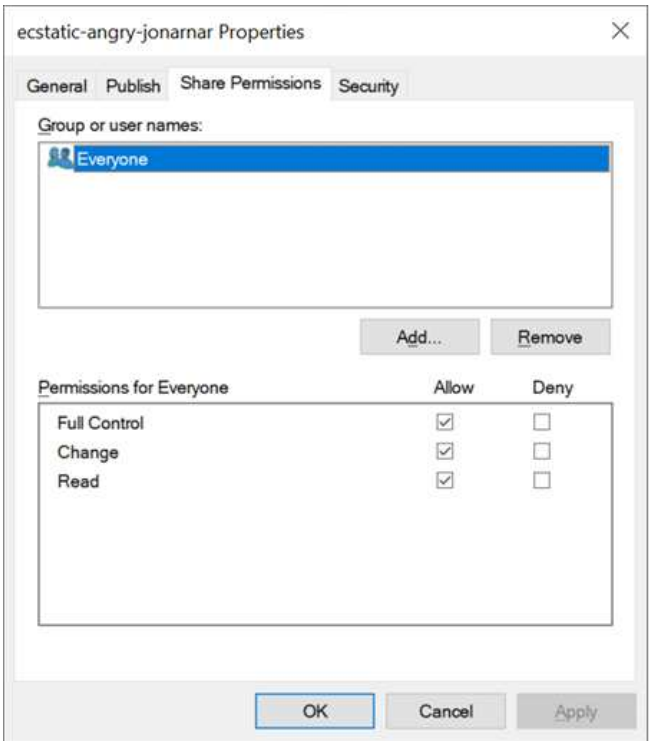
Freigabeberechtigungen

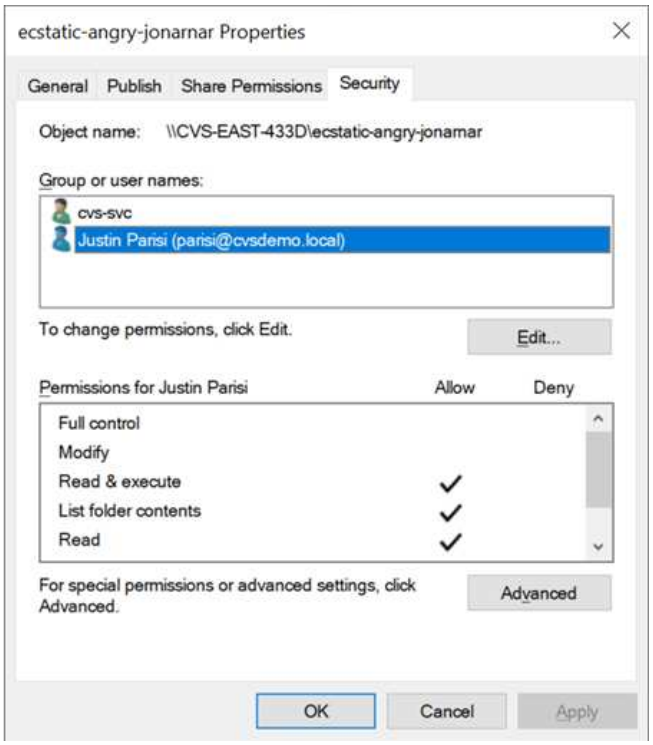
Freigabeberechtigungen sind allgemeiner als NTFS-Berechtigungen (nur Lesen/Ändern/Vollzugriff) und steuern den anfänglichen Eintrag in eine SMB-Freigabe – ähnlich wie die NFS-Exportrichtlinien funktionieren.

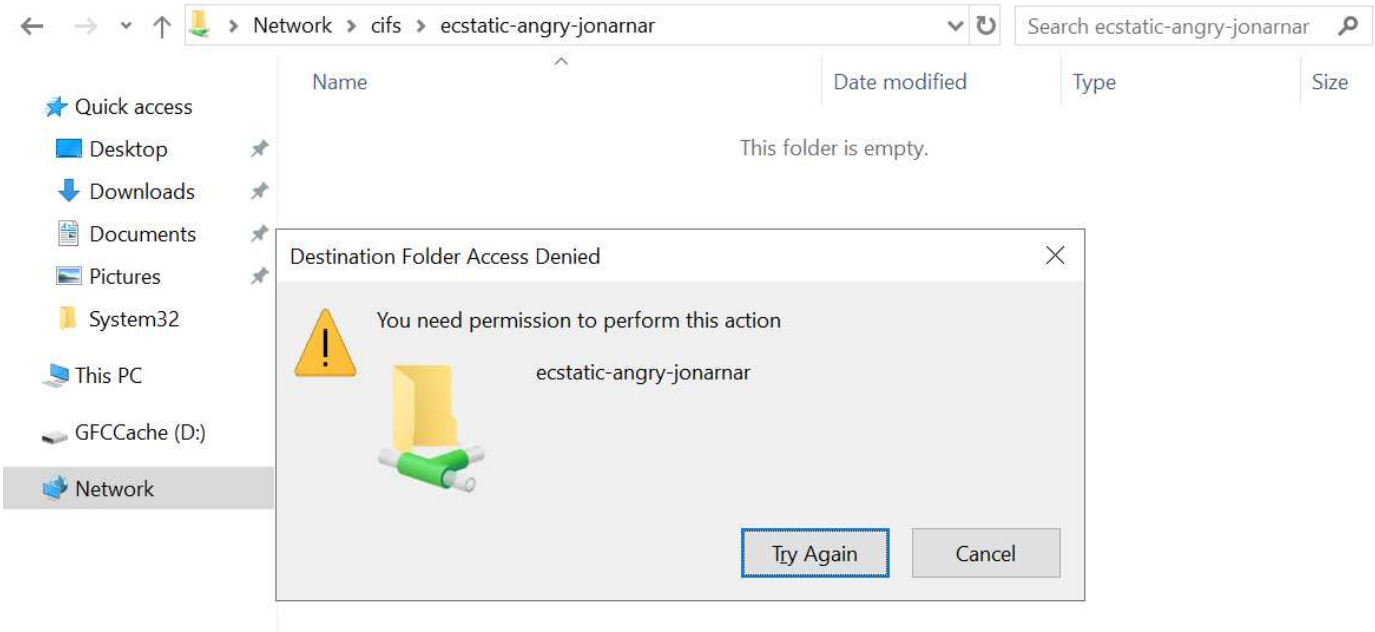
Obwohl die NFS-Exportrichtlinien den Zugriff über hostbasierte Informationen wie IP-Adressen oder Hostnamen steuern, können SMB-Freigabe-Berechtigungen den Zugriff über Benutzer- und Gruppennamen in einer Share-ACL steuern. Sie können die Share ACLs entweder über den Windows Client oder über die Cloud Volumes Service Management UI festlegen.

Standardmäßig enthalten alle ACLs und Initial Volume ACLs mit vollständiger Kontrolle. Die Datei ACLs sollten geändert werden, aber Freigabeberechtigungen werden durch die Dateiberechtigungen für Objekte in der Freigabe überbeherrscht.

Wenn ein Benutzer beispielsweise nur Lesezugriff auf die Cloud Volumes Service Volume-Datei-ACL hat, wird ihm der Zugriff auf die Erstellung von Dateien und Ordnern verweigert, obwohl die share ACL für alle mit Full Control eingestellt ist, wie in der folgenden Abbildung dargestellt.







Gehen Sie wie folgt vor, um die besten Sicherheitsergebnisse zu erzielen:

- Entfernen Sie alle aus den Freigabe- und Datei-ACLs und legen Sie stattdessen den Freigaberzugriff für Benutzer oder Gruppen fest.
- Verwenden Sie Gruppen zur Zugriffssteuerung anstelle einzelner Benutzer, um das Management zu vereinfachen und das Entfernen bzw. Hinzufügen von Benutzern zu beschleunigen, um ACLs über das Gruppenmanagement zu teilen.
- Weniger restriktiver, allgemeiner Zugriff auf die Asse auf den Freigabeberechtigungen und Sperrung des Zugriffs auf Benutzer und Gruppen mit Dateiberechtigungen für eine granularere Zugriffskontrolle.
- Die allgemeine Verwendung von expliziten Ablehnen von ACLs vermeiden, da sie ACLs außer Kraft setzen. Beschränken Sie die Verwendung expliziter Ablehnen von ACLs für Benutzer oder Gruppen, die

schnell vom Zugriff auf ein Dateisystem eingeschränkt werden müssen.

- Achten Sie darauf, dass Sie auf die achten "ACL-Vererbung" Einstellungen beim Ändern von Berechtigungen; das Festlegen des Vererbungsfahs auf der obersten Ebene eines Verzeichnisses oder Volumes mit hoher Dateianzahl bedeutet, dass jede Datei unter diesem Verzeichnis oder Volume über geerbte Berechtigungen verfügt, die ihr hinzugefügt wurden. Dies kann unerwünschte Verhaltensweisen wie unbeabsichtigten Zugriff/Denial-of-DoS und lange Abgänge von Berechtigungsänderungen verursachen, wenn jede Datei angepasst wird.

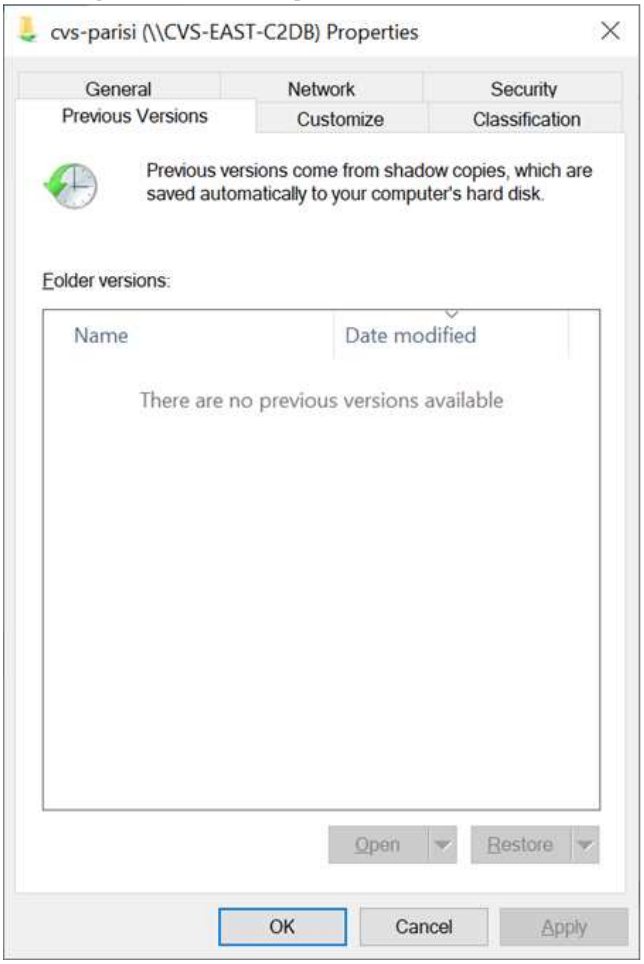
Sicherheitsfunktionen für die SMB-Freigabe

Wenn Sie zum ersten Mal ein Volume mit SMB-Zugriff in Cloud Volumes Service erstellen, erhalten Sie eine Reihe von Optionen zum Sichern des Volumes.

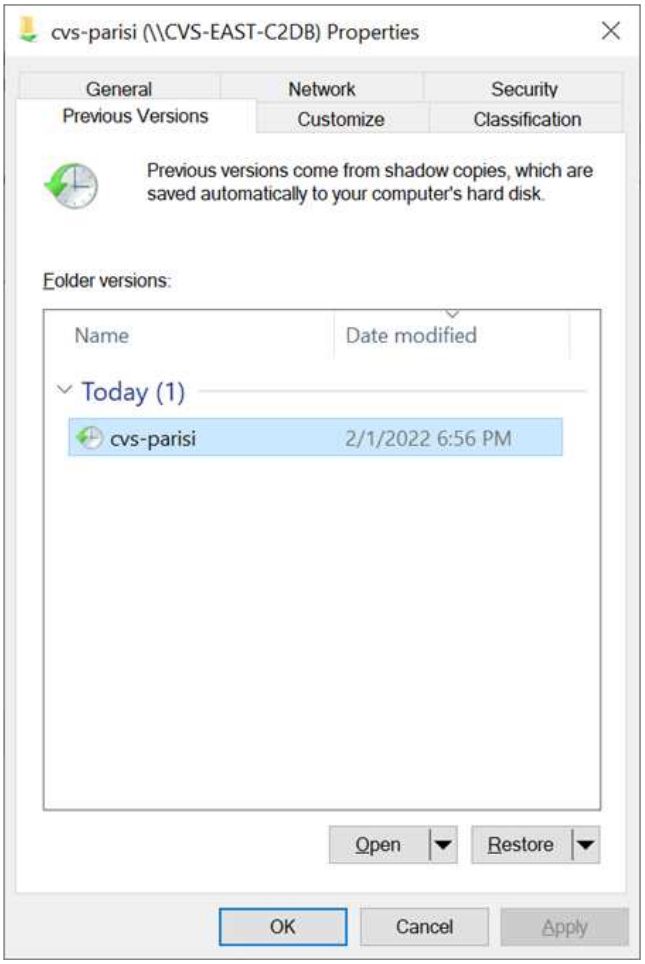
Einige dieser Optionen hängen von der Cloud Volumes Service-Ebene (Leistung oder Software) ab und stehen zur Auswahl:

- **Snapshot-Verzeichnis sichtbar machen (sowohl für CVS-Performance als auch für CVS-SW verfügbar).** mit dieser Option lässt sich kontrollieren, ob SMB-Clients in einem SMB-Share auf das Snapshot-Verzeichnis zugreifen können (`\\server\share\~snapshot` Und/oder Registerkarte frühere Versionen). Die Standardeinstellung ist nicht aktiviert, was bedeutet, dass das Volume standardmäßig den Zugriff auf das ausgeblendet und deaktiviert `~snapshot` Verzeichnis, und es werden keine Snapshot-Kopien auf der Registerkarte Vorherige Versionen des Volumes angezeigt.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



Das Ausblenden von Snapshot Kopien vor Endbenutzern kann aus Sicherheitsgründen oder aus Performance-

Gründen (Ausblenden dieser Ordner vor AV-Scans) oder unter Voreinstellung gewünscht werden. Cloud Volumes Service Snapshots sind schreibgeschützt, d. h. selbst wenn diese Snapshots sichtbar sind, können Endanwender Dateien im Snapshot Verzeichnis nicht löschen oder ändern. Dateiberechtigungen auf die Dateien oder Ordner beim Erstellen der Snapshot Kopie. Wenn sich die Berechtigungen einer Datei oder eines Ordners zwischen Snapshot Kopien ändern, gelten die Änderungen auch für die Dateien oder Ordner im Snapshot Verzeichnis. Benutzer und Gruppen können auf Basis von Berechtigungen auf diese Dateien oder Ordner zugreifen. Das Löschen oder Modifizierungen von Dateien im Snapshot Verzeichnis ist zwar nicht möglich, aber es ist möglich, Dateien oder Ordner aus dem Snapshot Verzeichnis zu kopieren.

- **SMB-Verschlüsselung aktivieren (sowohl für CVS-Performance als auch für CVS-SW verfügbar).** SMB-Verschlüsselung ist auf der SMB-Freigabe standardmäßig deaktiviert (deaktiviert). Wenn Sie das Kontrollkästchen aktiviert SMB-Verschlüsselung aktivieren, bedeutet dies, dass der Datenverkehr zwischen dem SMB-Client und dem -Server im laufenden Vorgang verschlüsselt wird, wobei die am höchsten unterstützten Verschlüsselungsstufen ausgehandelt werden. Cloud Volumes Service unterstützt bis zu AES-256-Verschlüsselung für SMB. Durch die Aktivierung der SMB-Verschlüsselung kommen Performance-Einbußen mit sich, die für Ihre SMB-Clients möglicherweise nicht spürbar sind – in etwa im Bereich von 10 bis 20 %. NetApp empfiehlt Tests nachdrücklich, um zu prüfen, ob diese Performance-Einbußen akzeptabel sind.
- **SMB-Share ausblenden (verfügbar sowohl für CVS-Performance als auch CVS-SW).** durch diese Option wird der SMB-Share-Pfad vom normalen Browsing ausgeblendet. Das bedeutet, dass Clients, die den Freigabepfad nicht kennen, die Freigaben beim Zugriff auf den Standard-UNC-Pfad nicht sehen können (z. B. `\\CVS-SMB`). Wenn das Kontrollkästchen aktiviert ist, können nur Clients darauf zugreifen, die den SMB-Freigabepfad explizit kennen oder über den von einem Gruppenrichtlinienobjekt definierten Freigabepfad verfügen (Sicherheit durch Obfuscation).
- **Access-Based Enumeration (ABE) aktivieren (nur CVS-SW).** Dies ähnelt dem Ausblenden der SMB-Freigabe, außer die Freigaben oder Dateien sind nur Benutzern oder Gruppen verborgen, die keine Berechtigung zum Zugriff auf die Objekte haben. Beispiel: Wenn Windows-Benutzer `joe` Ist mindestens nicht erlaubt Lese-Zugriff durch die Berechtigungen, dann der Windows-Benutzer `joe` SMB-Freigabe oder Dateien können überhaupt nicht angezeigt werden. Dies ist standardmäßig deaktiviert und Sie können sie durch Aktivieren des Kästchens aktivieren. Weitere Informationen zu ABE finden Sie im NetApp Knowledge Base-Artikel "Wie funktioniert Access Based Enumeration (ABE)?"
- **Kontinuierliche verfügbare (CA) Freigabesupport aktivieren (nur CVS-Performance).** "Kontinuierlich verfügbare SMB-Freigaben" Bietet eine Möglichkeit, Applikationsunterbrechungen bei Failover-Ereignissen zu minimieren, indem Sperrstatus über Nodes im Cloud Volumes Service-Back-End-System hinweg repliziert werden. Dies ist keine Sicherheitsfunktion, bietet aber insgesamt eine höhere Ausfallsicherheit. Derzeit werden nur SQL Server- und FSLogix-Anwendungen unterstützt.

Ausgeblendete Standardfreigaben

Wenn in Cloud Volumes Service ein SMB Server erstellt wird, gibt es diese "Versteckte administrative Freigaben" (Unter Verwendung der Namenskonvention für USD), die zusätzlich zum SMB-Share des Daten-Volumes erstellt werden. Dazu gehören C€ (Namespace Access) und IPC€ (gemeinsame Nutzung von benannten Rohren für die Kommunikation zwischen Programmen, wie z. B. die Remote Procedure Calls (RPC), die für den Zugriff auf die Microsoft Management Console (MMC) verwendet werden).

Die IPC-USD-Freigabe enthält keine Share-ACLs und kann nicht geändert werden – sie wird streng für RPC-Aufrufe und verwendet "Windows deaktiviert standardmäßig den anonymen Zugriff auf diese Freigaben".

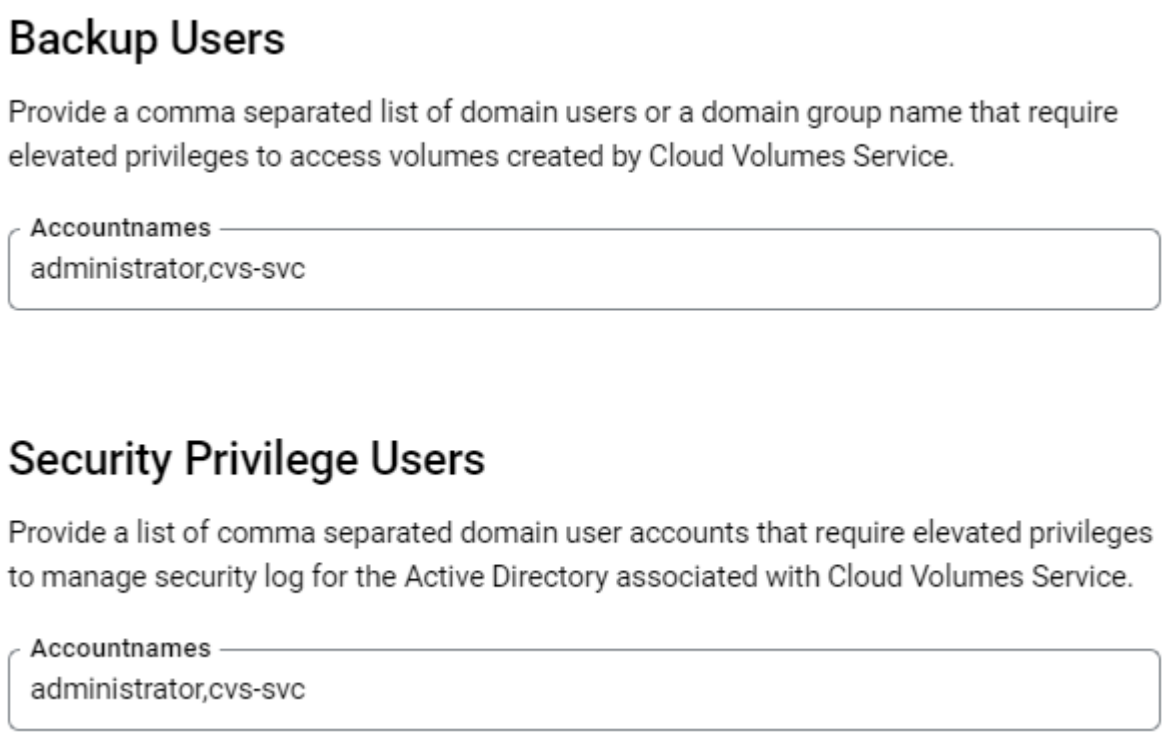
Der Wert-Anteil ermöglicht standardmäßig den Zugriff von BUILTIN/Administratoren, aber die Cloud Volumes Service-Automatisierung entfernt das Share-ACL und erlaubt keinen Zugriff auf jemanden, da der Zugriff auf die C€-Aktie eine Übersicht über alle gemounteten Volumes in den Cloud Volumes Service-Dateisystemen ermöglicht. Daher wird versucht, zu navigieren `\\SERVER\C$` Fehler.

Konten mit lokalen/BUILTIN-Administrator/Backup-Rechten

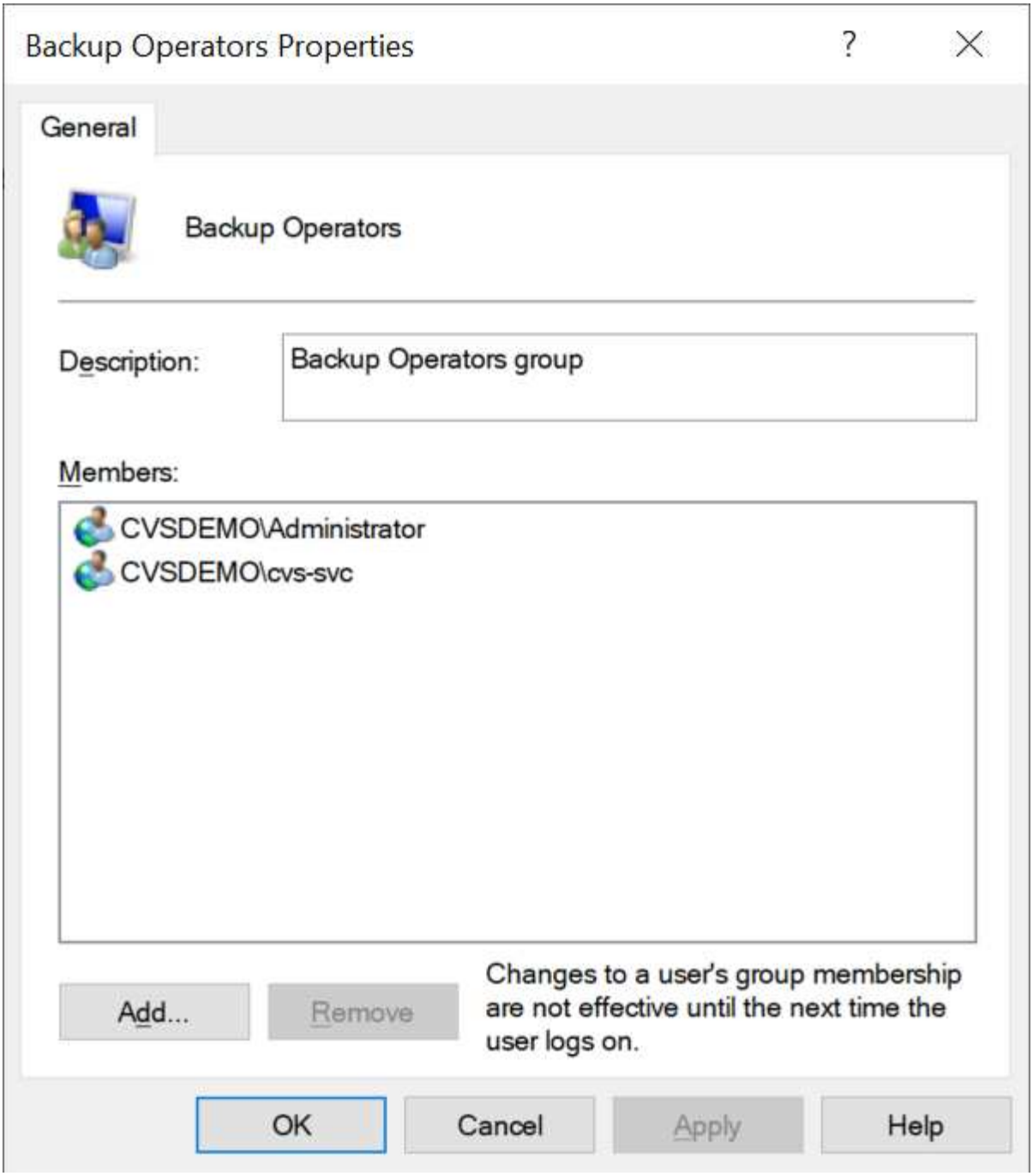
Cloud Volumes Service SMB-Server verfügen über ähnliche Funktionen wie normale Windows SMB-Server, da lokale Gruppen (z. B. BUILTIN\-Administratoren) Zugriffsrechte für ausgewählte Domänenbenutzer und -Gruppen anwenden.

Wenn Sie einen Benutzer angeben, der zu Backup-Benutzern hinzugefügt werden soll, wird der Benutzer der Gruppe BUILTIN\Backup Operators in der Cloud Volumes Service-Instanz hinzugefügt, die diese Active Directory-Verbindung verwendet, die dann den ruft "SeBackupPrivilege und SeRestorePrivilege".

Wenn Sie Benutzern von Sicherheitsberechtigungen einen Benutzer hinzufügen, erhält der Benutzer die SeSecurityPrivilege, die in einigen Anwendungsanwendungsfällen, wie z. B., nützlich ist "SQL Server auf SMB-Freigaben".



Sie können die Mitgliedschaften der lokalen Cloud Volumes Service-Gruppen über das MMC mit den entsprechenden Berechtigungen anzeigen. Die folgende Abbildung zeigt Benutzer, die mit der Cloud Volumes Service Konsole hinzugefügt wurden.

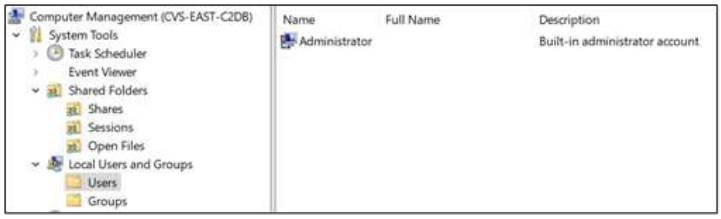


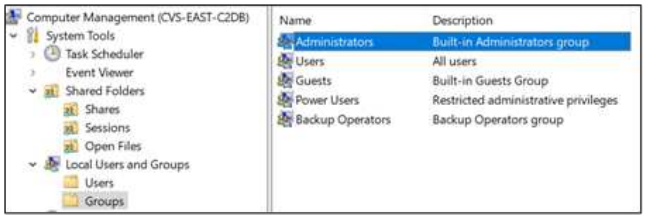
Die folgende Tabelle zeigt die Liste der Standard-BUILTIN-Gruppen und welche Benutzer/Gruppen standardmäßig hinzugefügt werden.

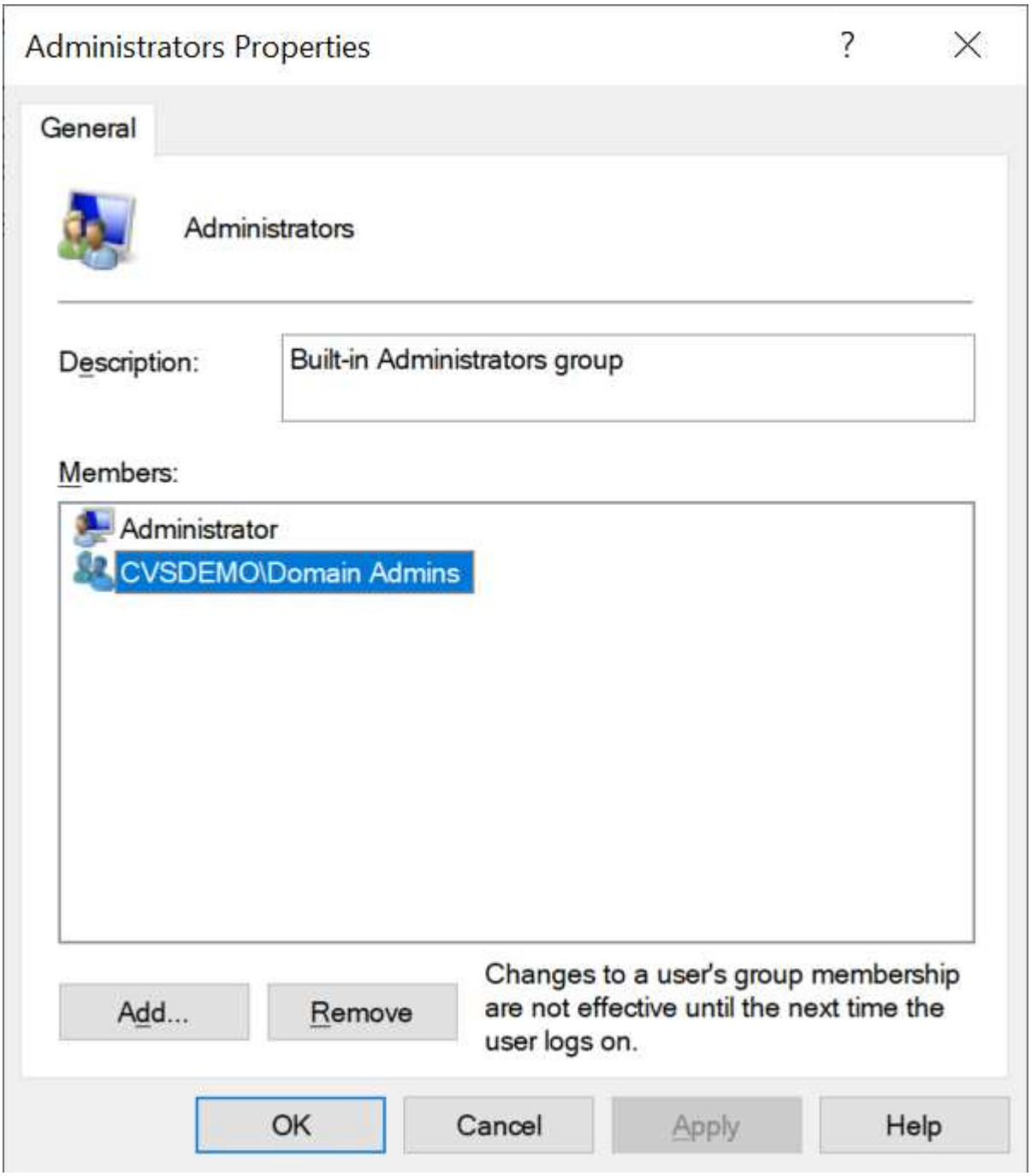
Lokale/BUILTIN-Gruppe	Standardmitglieder
BUILTIN\Administratoren*	DOMAIN\Domänen-Administratoren
BUILTIN\Backup Operators*	Keine
BAUEN Sie\Gäste	DOMAIN\Domain-Gäste
BUILTIN\Power-User	Keine
BUILTIN\Domain-Benutzer	DOMAIN\Domain-Benutzer

*Gruppenmitgliedschaft in Cloud Volumes Service Active Directory Verbindungskonfiguration gesteuert.

Sie können lokale Benutzer und Gruppen (und Gruppenmitglieder) im MMC-Fenster anzeigen, aber Sie können keine Objekte hinzufügen oder löschen oder Gruppenmitgliedschaften von dieser Konsole aus ändern. Standardmäßig werden nur die Gruppe Domänenadministratoren und der Administrator der BUILTIN\Administrators in Cloud Volumes Service hinzugefügt. Derzeit können Sie dies nicht ändern.







MMC-/Computermanagement-Zugriff

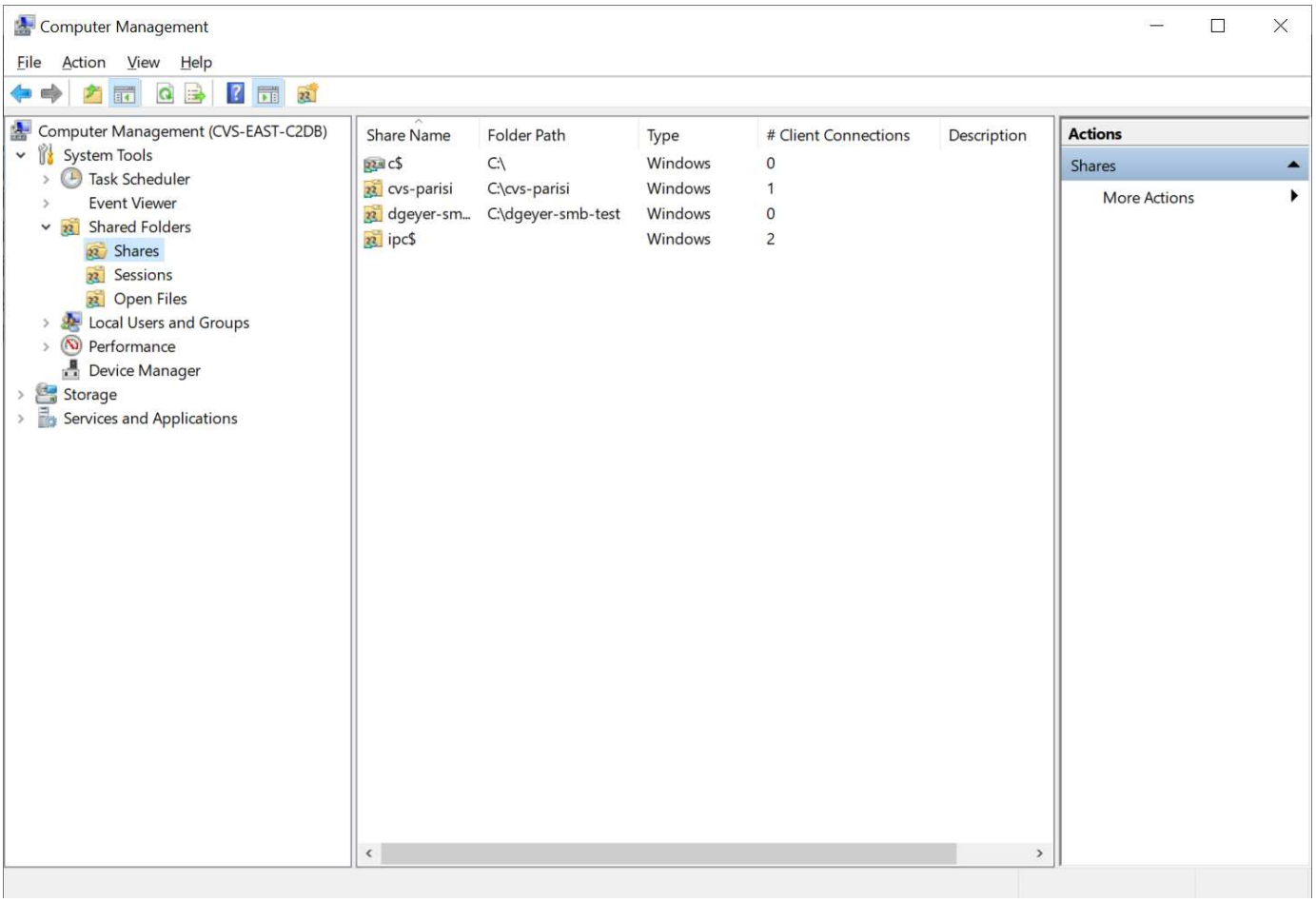
SMB-Zugriff in Cloud Volumes Service bietet Konnektivität zum Computer Management MMC, mit dem Sie Freigaben anzeigen, ACLs gemeinsam nutzen, SMB-Sessions anzeigen/managen und Dateien öffnen können.

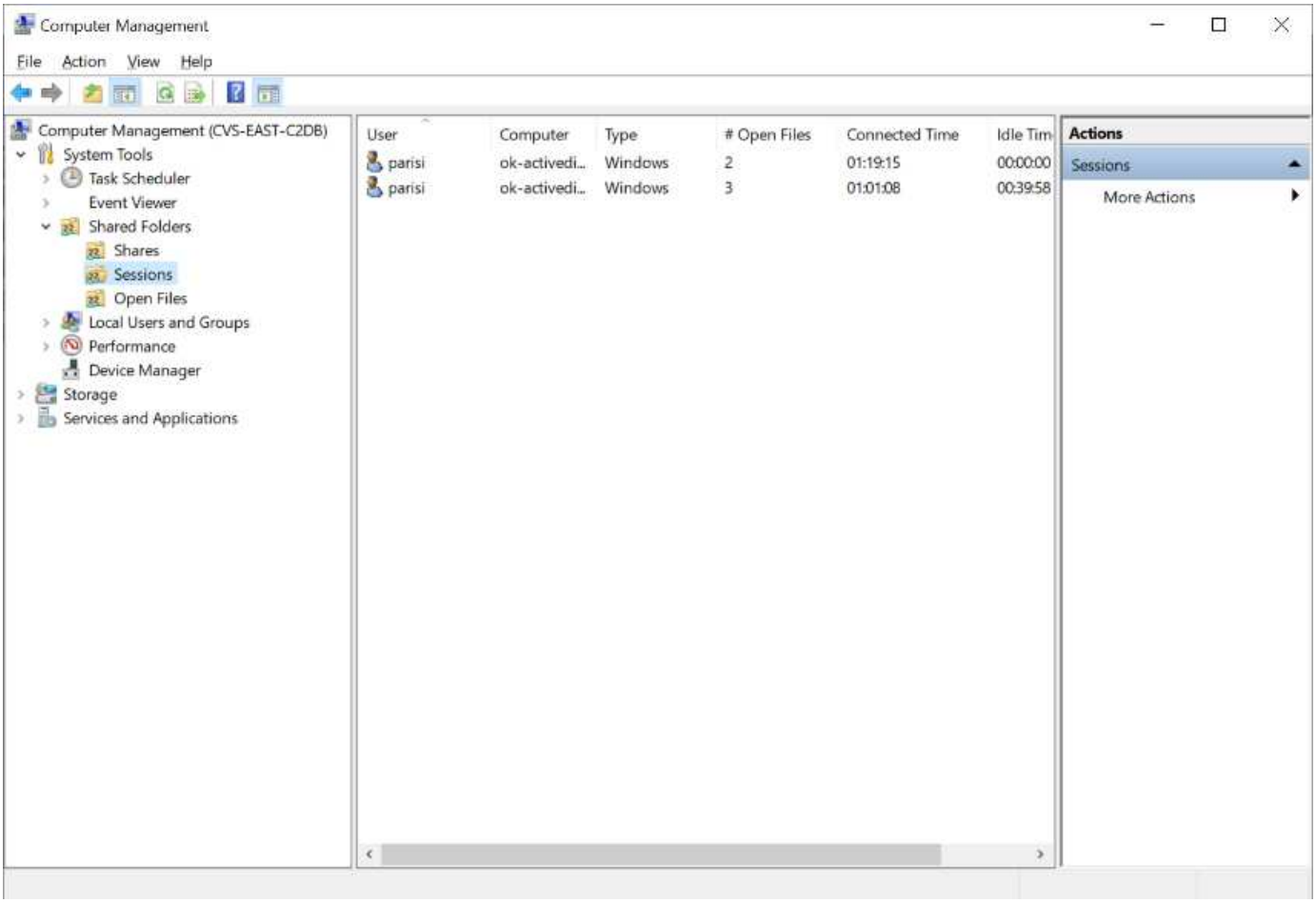
Damit Sie die MMC verwenden können, um SMB-Freigaben und -Sitzungen in Cloud Volumes Service anzuzeigen, muss der aktuell angemeldete Benutzer ein Domänenadministrator sein. Andere Benutzer haben Zugriff auf das Anzeigen oder Verwalten des SMB-Servers von MMC aus und erhalten ein Dialogfeld ohne Berechtigungen, wenn Sie versuchen, Freigaben oder Sitzungen in der Cloud Volumes Service SMB-Instanz anzuzeigen.

Um eine Verbindung zum SMB-Server herzustellen, öffnen Sie Computerverwaltung, klicken Sie mit der rechten Maustaste auf Computerverwaltung, und wählen Sie dann Verbindung zu einem anderen Computer herstellen. Daraufhin wird das Dialogfeld „Computer auswählen“ geöffnet, in dem Sie den SMB-Servernamen eingeben können (zu finden in den Cloud Volumes Service-Volume-Informationen).

Wenn Sie SMB-Freigaben mit den entsprechenden Berechtigungen anzeigen, sehen Sie alle verfügbaren Freigaben in der Cloud Volumes Service-Instanz, die die Active Directory-Verbindung nutzen. Um dieses Verhalten zu steuern, legen Sie die Option SMB-Freigaben ausblenden auf der Cloud Volumes Service-Volume-Instanz fest.

Denken Sie daran, dass pro Region nur eine Active Directory-Verbindung zulässig ist.





Die folgende Tabelle zeigt eine Liste der unterstützten/nicht unterstützten Funktionen für MMC.

Unterstützte Funktionen	Nicht unterstützte Funktionen
• Freigaben anzeigen • Anzeigen von aktiven SMB-Sitzungen • Öffnen Sie Dateien anzeigen • Zeigen Sie lokale Benutzer und Gruppen an • Zeigen Sie lokale Gruppenmitgliedschaften an • Listen Sie die Liste der Sitzungen, Dateien und Baumverbindungen im System auf • Schließen Sie offene Dateien im System • Offene Sitzungen schließen • Freigaben erstellen/managen	• Erstellen neuer lokaler Benutzer/Gruppen • Verwalten/Anzeigen vorhandener lokaler Benutzer/Gruppen • Zeigt Ereignisse oder Performance-Protokolle an • Storage-Management • Management von Services und Applikationen

Sicherheitsinformationen für SMB-Server

Der SMB-Server in Cloud Volumes Service verwendet eine Reihe von Optionen, die Sicherheitsrichtlinien für SMB-Verbindungen definieren, einschließlich Kerberos-Clock-Skew, Ticketalter, Verschlüsselung und mehr.

Die folgende Tabelle enthält eine Liste dieser Optionen, was sie tun, der Standardkonfigurationen und, ob sie mit Cloud Volumes Service geändert werden können. Einige Optionen gelten nicht für Cloud Volumes Service.

Sicherheitsoption	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
Maximale Kerberos-Uhr-Skew (Minuten)	Maximale Zeitabweichung zwischen Cloud Volumes Service und Domain Controllern Wenn die Zeitskew 5 Minuten überschreitet, schlägt die Kerberos-Authentifizierung fehl. Dieser Wert ist auf den Standardwert von Active Directory gesetzt.	5	Nein
Lebensdauer von Kerberos-Tickets (Stunden)	Maximale Zeit, bis ein Kerberos-Ticket gültig bleibt, bevor eine Erneuerung erforderlich ist. Wenn keine Verlängerung vor 10 Stunden erfolgt, müssen Sie ein neues Ticket einholen. Cloud Volumes Service führt diese Verlängerungen automatisch durch. 10 Stunden ist der Standardwert von Active Directory.	10	Nein
Maximale Kerberos-Ticketverlängerung (Tage)	Maximale Anzahl der Tage, an denen ein Kerberos-Ticket erneuert werden kann, bevor eine neue Autorisierungsanforderung erforderlich ist. Cloud Volumes Service verlängert automatisch die Tickets für SMB-Verbindungen. Sieben Tage ist der Standardwert von Active Directory.	7	Nein
Kerberos KDC-Verbindungszeitlimit (Sek.)	Die Anzahl der Sekunden, bevor eine KDC-Verbindung ausgeht.	3	Nein

Sicherheitsoption	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
Für eingehenden SMB-Datenverkehr müssen signiert werden	Für SMB-Datenverkehr muss eine Signatur erforderlich sein. Wenn auf „true“ gesetzt ist, unterstützen Clients, die keine Verbindung zum Signieren von Fehlschlagen unterstützen.	Falsch	
Komplexität des Kennworts für lokale Benutzerkonten erforderlich	Wird für Passwörter für lokale SMB-Benutzer verwendet. Cloud Volumes Service unterstützt die Erstellung lokaler Benutzer nicht, daher gilt diese Option nicht für Cloud Volumes Service.	Richtig	Nein
Verwenden Sie Start_tls für Active Directory-LDAP-Verbindungen	Wird zum Starten von TLS-Verbindungen für Active Directory LDAP verwendet. Cloud Volumes Service unterstützt derzeit die Aktivierung dieses Systems nicht.	Falsch	Nein
AES-128- und AES-256-Verschlüsselung für Kerberos aktiviert	Dies steuert, ob AES-Verschlüsselung für Active Directory-Verbindungen verwendet wird und wird über die Option AES-Verschlüsselung für Active Directory-Authentifizierung aktivieren bei der Erstellung/Änderung der Active Directory-Verbindung gesteuert.	Falsch	Ja.
LM-Kompatibilitätsstufe	Ebene der unterstützten Authentifizierungsdialekte für Active Directory-Verbindungen. Siehe Abschnitt „SMB-Authentifizierungsdialekte„ Weitere Informationen.	ntlmv2-krb	Nein

Sicherheitsoption	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
SMB-Verschlüsselung für eingehenden CIFS-Datenverkehr erforderlich	SMB-Verschlüsselung für alle Freigaben erforderlich Dies wird nicht von Cloud Volumes Service verwendet; stattdessen setzen Sie Verschlüsselung auf Volume-Basis (siehe Abschnitt „Sicherheitsfunktionen für die SMB-Freigabe„).	Falsch	Nein
Sicherheit Der Client-Sitzung	Legt das Signing und/oder Sealing für die LDAP-Kommunikation fest. Dies ist derzeit nicht in Cloud Volumes Service eingestellt, kann aber in zukünftigen Versionen zur Adresse benötigt werden. Die Behebung von Problemen mit der LDAP-Authentifizierung aufgrund des Windows-Patches wird im Abschnitt behandelt "„LDAP-Kanalbindung.“".	Keine	Nein
SMB2 aktivieren für Gleichstromverbindungen	Verwendet SMB2 für DC-Verbindungen. Standardmäßig aktiviert.	Systemstandard	Nein
LDAP Referral Chasing	Bei der Verwendung mehrerer LDAP-Server ermöglicht die Verweisungsjagd dem Client, auf andere LDAP-Server in der Liste zu verweisen, wenn ein Eintrag nicht im ersten Server gefunden wird. Dies wird derzeit nicht von Cloud Volumes Service unterstützt.	Falsch	Nein
Verwenden Sie LDAPS für sichere Active Directory-Verbindungen	Aktiviert die Verwendung von LDAP über SSL. Derzeit nicht unterstützt von Cloud Volumes Service.	Falsch	Nein

Sicherheitsoption	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
Für DC-Verbindung ist eine Verschlüsselung erforderlich	Verschlüsselung für erfolgreiche DC-Verbindungen erforderlich. In Cloud Volumes Service standardmäßig deaktiviert.	Falsch	Nein

Dual-Protokoll/Multiprotokoll

Cloud Volumes Service bietet die Möglichkeit, dieselben Datensätze sowohl für SMB- als auch für NFS-Clients zu nutzen, ohne dass die Zugriffsberechtigungen dafür unterbrochen werden ("Dual-Protokoll"). Dies geschieht durch die Koordinierung der Identitätszuordnung zwischen Protokollen und die Verwendung eines zentralen Backend-LDAP-Servers zur Bereitstellung der UNIX-Identitäten an Cloud Volumes Service. Sie können Windows Active Directory verwenden, um sowohl Windows- als auch UNIX-Benutzer zur Benutzerfreundlichkeit bereitzustellen.

Zugriffssteuerung

- **Zugriffskontrollen freigeben.** Bestimmen Sie, welche Clients und/oder Benutzer und Gruppen auf eine NAS-Freigabe zugreifen können. Für NFS kontrollieren Exportrichtlinien und Regeln den Client-Zugriff auf Exporte. NFS-Exporte werden von der Cloud Volumes Service Instanz gemanagt. SMB nutzt CIFS/SMB-Freigaben und ACLs für die Freigabe von ACLs und ermöglicht eine granularere Kontrolle auf Benutzer- und Gruppenebene. Sie können ACLs auf Share-Ebene nur über SMB-Clients konfigurieren "MMC/Computer-Management" Mit einem Konto, das über Administratorrechte auf der Cloud Volumes Service-Instanz verfügt (siehe Abschnitt "„Konten mit lokalen/BUILTIN-Administrator/Backup-Rechten.“").
- **Dateizugriffssteuerung.** Kontrollieren Sie Berechtigungen auf Datei- oder Ordnerebene und werden immer vom NAS-Client verwaltet. NFS Clients können die traditionellen Modus-Bits (rwx) oder NFSv4 ACLs nutzen. SMB-Clients nutzen NTFS-Berechtigungen.

Die Zugriffssteuerung für Volumes, die Daten sowohl für NFS als auch für SMB bereitstellen, hängt vom verwendeten Protokoll ab. Informationen zu Berechtigungen mit Dual-Protokoll finden Sie im Abschnitt „Berechtigungsmodell.“

Benutzerzuordnung

Wenn ein Client auf ein Volume zugreift, versucht Cloud Volumes Service, den eingehenden Benutzer in die entgegengesetzte Richtung einem gültigen Benutzer zuzuordnen. Dies ist notwendig, damit ein ordnungsgemäßer Zugriff über verschiedene Protokolle hinweg festgestellt werden kann und sicherzustellen ist, dass der Benutzer, der Zugriff beantragt, tatsächlich derjenige ist, der von ihm behauptet wird.

Beispiel: Wenn ein Windows-Benutzer mit dem Namen `joe` Versucht über SMB den Zugriff auf ein Volume mit UNIX-Berechtigungen, dann führt Cloud Volumes Service eine Suche durch, um einen entsprechenden UNIX-Benutzer zu finden `joe`. Ist eine vorhanden, so werden Dateien, die als Windows Benutzer in eine SMB-Freigabe geschrieben werden `joe` Wird als UNIX-Benutzer angezeigt `joe` Von NFS-Clients.

Alternativ können Sie auch festlegen, ob ein UNIX-Benutzer den Namen hat `joe` Versucht, auf ein Cloud Volumes Service-Volume mit Windows-Berechtigungen zuzugreifen, dann muss der UNIX-Benutzer in der Lage sein, einem gültigen Windows-Benutzer zuzuordnen. Andernfalls wird der Zugriff auf das Volume

verweigert.

Derzeit wird nur Active Directory für das externe UNIX-Identitätsmanagement mit LDAP unterstützt. Weitere Informationen zum Konfigurieren des Zugriffs auf diesen Dienst finden Sie unter "Erstellen einer AD-Verbindung".

Berechtigungsmodell

Bei der Verwendung von Dual-Protokoll-Setups verwendet Cloud Volumes Service Sicherheitsformate für Volumes, um den Typ der ACL zu bestimmen. Diese Sicherheitsstile werden basierend auf bestimmten NAS-Protokollen oder bei einem dualen Protokoll festgelegt. Sie sollten zur Zeit der Cloud Volumes Service Volume-Erstellung gewählt werden.

- Wenn Sie nur NFS verwenden, verwenden Cloud Volumes Service-Volumes UNIX-Berechtigungen.
- Wenn Sie nur SMB verwenden, verwenden Cloud Volumes Service Volumes NTFS-Berechtigungen.

Wenn Sie ein Dual-Protokoll-Volume erstellen, können Sie bei der Volume-Erstellung den ACL-Stil wählen. Diese Entscheidung sollte auf der Grundlage der gewünschten Berechtigungsverwaltung getroffen werden. Wenn Ihre Benutzer Berechtigungen von Windows-/SMB-Clients verwalten, wählen Sie NTFS. Wenn Ihre Benutzer NFS-Clients und chmod/chown verwenden möchten, verwenden Sie UNIX-Sicherheitsmethoden.

Überlegungen zum Erstellen von Active Directory-Verbindungen

Cloud Volumes Service bietet die Möglichkeit, Ihre Cloud Volumes Service Instanz mit einem externen Active Directory Server zu verbinden, um Identitäts-Management für SMB- und UNIX-Benutzer zu ermöglichen. Für die Verwendung von SMB in Cloud Volumes Service ist das Erstellen einer Active Directory-Verbindung erforderlich.

Bei der Konfiguration hierfür stehen verschiedene Optionen zur Verfügung, bei denen die Sicherheit berücksichtigt werden muss. Der externe Active Directory Server kann eine lokale oder Cloud-native Instanz sein. Wenn Sie einen lokalen Active Directory-Server verwenden, setzen Sie die Domäne nicht dem externen Netzwerk (z. B. mit einer DMZ oder einer externen IP-Adresse) aus. Verwenden Sie stattdessen sichere private Tunnel oder VPNs, One-Way-Forest-Trusts oder dedizierte Netzwerkverbindungen zu den On-Premises-Netzwerken mit "Privater Zugriff Auf Google". In der Google Cloud-Dokumentation finden Sie weitere Informationen zu "Best Practices Using Active Directory in Google Cloud".

> CVS-SW erfordert, dass sich Active Directory-Server in derselben Region befinden. Wenn eine DC-Verbindung in CVS-SW zu einer anderen Region versucht wird, schlägt der Versuch fehl. Wenn Sie CVS-SW verwenden, erstellen Sie Active Directory-Sites, die die Active Directory-Datacenter enthalten, und geben Sie dann Standorte in Cloud Volumes Service an, um regionale DC-Verbindungsversuche zu vermeiden.

Active Directory-Anmeldeinformationen

Wenn SMB oder LDAP für NFS aktiviert ist, interagiert Cloud Volumes Service mit den Active Directory Controllern, um ein Computerkonto-Objekt zu erstellen, das für die Authentifizierung verwendet werden soll. Dies unterscheidet sich nicht von der Verbindung eines Windows SMB-Clients zu einer Domäne und erfordert dieselben Zugriffsrechte für Organisationseinheiten (OUs) in Active Directory.

In vielen Fällen ist die Verwendung eines Windows-Administratorkontos auf externen Servern wie Cloud Volumes Service nicht gestattet. In einigen Fällen ist der Windows Administrator-Benutzer vollständig als bewährte Sicherheitsübung deaktiviert.

Zum Erstellen von SMB-Computerkonten erforderliche Berechtigungen

Um einem Active Directory Cloud Volumes Service-Maschinenobjekte hinzuzufügen, ein Konto, das entweder über Administratorrechte für die Domäne verfügt oder über "Delegierte Berechtigungen zum Erstellen und Ändern von Computerkontontobjekten" Für eine angegebene Organisationseinheit ist erforderlich. Dazu können Sie den Assistenten zur Delegierung von Computerobjekten in Active Directory verwenden, indem Sie eine benutzerdefinierte Aufgabe erstellen, die einem Benutzer den Zugriff auf das Erstellen/Löschen von Computerobjekten mit den folgenden Zugriffsberechtigungen bietet:

- Lese-/Schreibzugriff
- Alle Untergeordneten Objekte Erstellen/Löschen
- Lesen/Schreiben Aller Eigenschaften
- Passwort Ändern/Zurücksetzen

Dadurch wird der OU in Active Directory automatisch eine Sicherheits-ACL für den definierten Benutzer hinzugefügt und der Zugriff auf die Active Directory-Umgebung wird minimiert. Nachdem ein Benutzer delegiert wurde, können dieser Benutzername und dieses Passwort in diesem Fenster als Active Directory-Anmeldeinformationen angegeben werden.

> Der Benutzername und das Passwort, das an die Active Directory-Domäne übergeben wird, nutzen die Kerberos-Verschlüsselung während der Abfrage des Computerkontos und der Erstellung für zusätzliche Sicherheit.

Details zur Active Directory-Verbindung

Der "Active Directory-Verbindungsdetails" Bereitstellen von Feldern für Administratoren, um bestimmte Active Directory-Schemainformationen für die Platzierung von Computerkonten bereitzustellen, z. B.:

- **Active Directory-Verbindungstyp.** zur Angabe, ob die Active Directory-Verbindung in einer Region für Volumes von entweder Cloud Volumes Service oder CVS-Performance-Diensttypen verwendet wird. Wenn diese Funktion bei einer vorhandenen Verbindung falsch eingestellt ist, funktioniert sie möglicherweise nicht richtig, wenn sie verwendet oder bearbeitet wird.
- **Domain.** der Active Directory-Domänenname.
- **Site.** beschränkt Active Directory-Server auf einen bestimmten Standort für Sicherheit und Leistung "Überlegungen". Dies ist erforderlich, wenn mehrere Active Directory-Server Regionen umfassen, da Cloud Volumes Service derzeit keine Unterstützung bietet, um Active Directory-Authentifizierungsanforderungen an Active Directory-Server in einer anderen Region als der Cloud Volumes Service-Instanz zu erlauben. (Beispielsweise ist der Active Directory Domain Controller in einer Region, die nur CVS-Performance unterstützt, aber einen SMB-Share in einer CVS-SW-Instanz wünschen.)
- **DNS-Server.** DNS-Server zur Verwendung bei der Namensaufsuchen.
- **NetBIOS-Name (optional).** auf Wunsch der NetBIOS-Name für den Server. Dies wird verwendet, wenn neue Computerkonten mithilfe der Active Directory-Verbindung erstellt werden. Wenn beispielsweise der NetBIOS-Name auf CVS-EAST gesetzt ist, dann sind die Namen des Computerkontos CVS-EAST-{1234}. Siehe Abschnitt "Wie Cloud Volumes Service in Active Directory angezeigt wird" Finden Sie weitere Informationen.
- **Organisationseinheit (Organisationseinheit).** die spezifische Organisationseinheit, die das Computerkonto erstellt. Dies ist nützlich, wenn Sie die Kontrolle an einen Benutzer für Maschinenkonten an eine bestimmte OU delegieren.
- **AES-Verschlüsselung.** Sie können auch das Kontrollkästchen AES-Verschlüsselung für AD-Authentifizierung aktivieren oder deaktivieren. Das Aktivieren der AES-Verschlüsselung für die Active

Directory-Authentifizierung bietet zusätzliche Sicherheit für die Kommunikation zwischen Cloud Volumes Service und Active Directory bei Benutzer- und Gruppensuchen. Bevor Sie diese Option aktivieren, fragen Sie Ihren Domänenadministrator, ob die Active Directory-Domänencontroller die AES-Authentifizierung unterstützen.

> Standardmäßig deaktivieren die meisten Windows-Server schwächere Chiffren (wie DES oder RC4-HMAC) nicht, aber wenn Sie schwächere Chiffren deaktivieren möchten, bestätigen Sie, dass die Cloud Volumes Service Active Directory-Verbindung für die Aktivierung von AES konfiguriert wurde. Andernfalls treten Authentifizierungsfehler auf. Die Aktivierung der AES-Verschlüsselung deaktiviert nicht schwächere Chiffren, sondern fügt dem Cloud Volumes Service SMB-Maschinenkonto Unterstützung für AES-Chiffren hinzu.

Kerberos-Bereich – Details

Diese Option gilt nicht für SMB-Server. Es wird vielmehr verwendet, wenn NFS Kerberos für das Cloud Volumes Service System konfiguriert wird. Wenn diese Details ausgefüllt werden, wird der NFS-Kerberos-Bereich konfiguriert (ähnlich einer krb5.conf-Datei unter Linux) und wird verwendet, wenn NFS-Kerberos bei der Erstellung des Cloud Volumes Service-Volumes angegeben wird, da die Active Directory-Verbindung als NFS Kerberos-Verteilzentrum (KDC) fungiert.

> Nicht-Windows-Rechenzentren werden derzeit nicht für die Verwendung mit Cloud Volumes Service unterstützt.

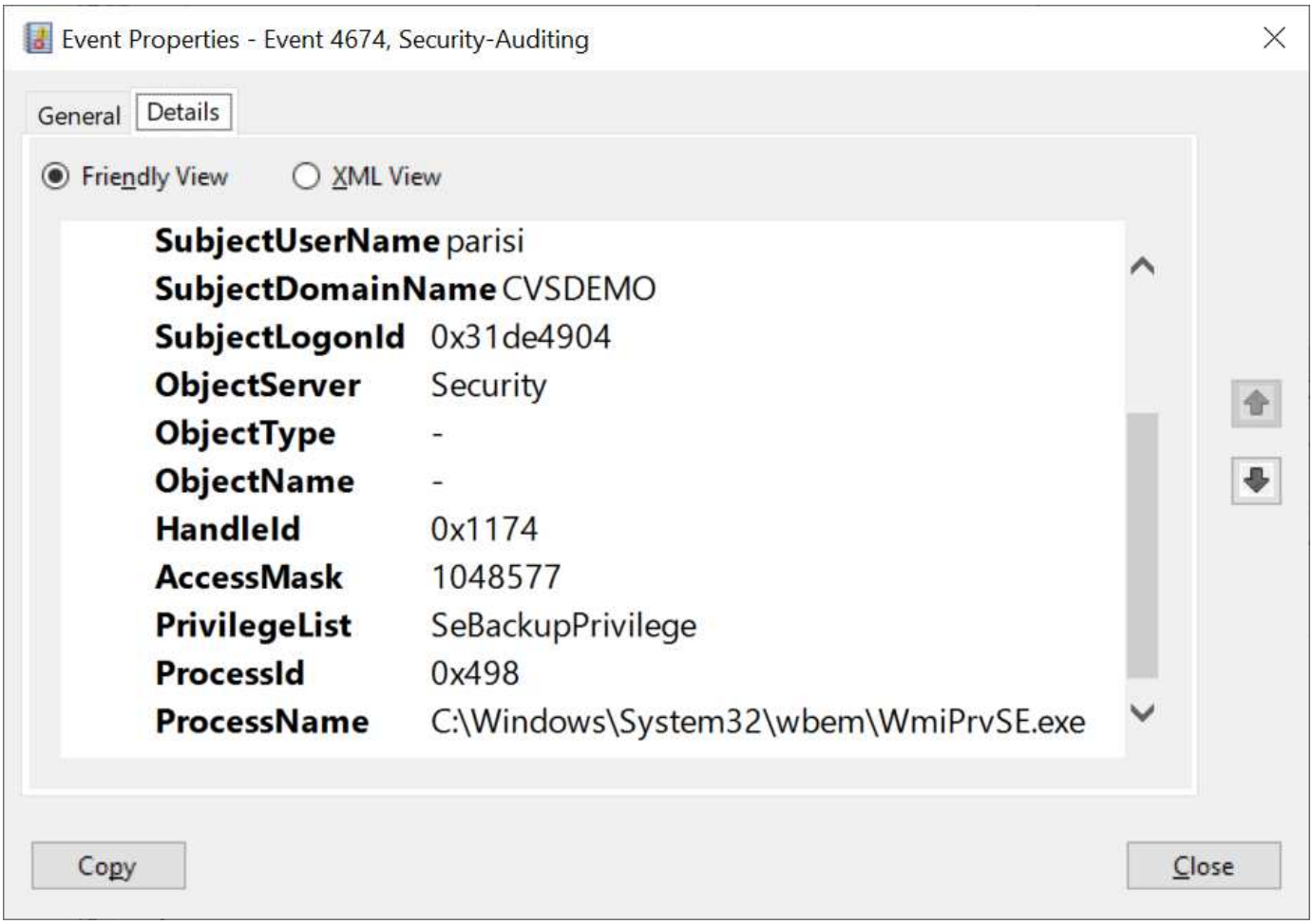
Region

In einer Region können Sie den Speicherort der Active Directory-Verbindung angeben. Diese Region muss dieselbe Region wie das Cloud Volumes Service-Volumen aufweisen.

- **Lokale NFS-Benutzer mit LDAP.** in diesem Abschnitt gibt es auch eine Option, lokale NFS-Benutzer mit LDAP zu erlauben. Diese Option muss nicht ausgewählt werden, wenn Sie Ihre UNIX-Benutzergruppenmitgliedschaft über die 16-Gruppen-Beschränkung von NFS hinaus erweitern möchten (erweiterte Gruppen). Die Verwendung erweiterter Gruppen erfordert jedoch einen konfigurierten LDAP-Server für UNIX-Identitäten. Wenn Sie keinen LDAP-Server haben, lassen Sie diese Option nicht ausgewählt. Wenn Sie über einen LDAP-Server verfügen und auch lokale UNIX-Benutzer verwenden möchten (z. B. Root), wählen Sie diese Option aus.

Backup-Benutzer

Mit dieser Option können Sie Windows-Benutzer angeben, die Sicherungsberechtigungen auf dem Cloud Volumes Service-Volume besitzen. Backup-Berechtigungen (SeBackupPrivilege) sind für einige Anwendungen erforderlich, um Daten in NAS-Volumes ordnungsgemäß zu sichern und wiederherzustellen. Dieser Benutzer hat einen hohen Zugriff auf die Daten des Volumes, daher sollten Sie es in Betracht ziehen "Aktivieren der Prüfung dieses Benutzerzugriffs". Nach Aktivierung werden Audit-Ereignisse in der Ereignisanzeige > Windows-Protokolle > Sicherheit angezeigt.



Benutzer mit Sicherheitsberechtigungen

Mit dieser Option können Sie Windows-Benutzer angeben, die über Sicherheitsberechtigungen für das Cloud Volumes Service-Volume verfügen. Für einige Anwendungen sind Sicherheitsberechtigungen (SeSecurityPrivilege) erforderlich ("Z. B. SQL Server") Die Berechtigungen während der Installation richtig einstellen. Diese Berechtigung ist zur Verwaltung des Sicherheitsprotokolls erforderlich. Obwohl dieses Privilege nicht so mächtig ist wie SeBackupPrivilege, empfiehlt NetApp Folgendes "Prüfung des Benutzerzugriffs von Benutzern" Bei Bedarf mit dieser Berechtigungsebene verfügbar.

Weitere Informationen finden Sie unter "Neue Anmeldung zugewiesene Sonderberechtigungen".

Wie Cloud Volumes Service in Active Directory angezeigt wird

Cloud Volumes Service wird in Active Directory als normales Konto-Objekt angezeigt. Die Namenskonventionen lauten wie folgt.

- CIFS/SMB und NFS Kerberos erstellen separate Computerkontoobjekte.
- NFS mit aktiviertem LDAP erstellt ein Maschinenkonto in Active Directory für Kerberos LDAP bindet.
- Duale Protokoll-Volumes mit LDAP nutzen das CIFS/SMB-Maschinenkonto für LDAP und SMB.
- CIFS/SMB-Maschinenkonten verwenden eine Namensgebungskonvention von NAME-1234 (zufällige vierstellige ID mit Bindestrich angefügt an <10 Zeichen Name) für das Maschinenkonto. SIE können DEN NAMEN durch die Einstellung des NetBIOS-Namens auf der Active Directory-Verbindung definieren (siehe Abschnitt „Details zur Active Directory-Verbindung„).
- NFS Kerberos verwendet NFS-NAME-1234 als Namenskonvention (bis zu 15 Zeichen). Wenn mehr als 15

Zeichen verwendet werden, lautet der Name NFS-CAM-NAME-1234.

- Nur NFS CVS-Performance-Instanzen mit aktiviertem LDAP erstellen ein SMB-Maschinenkonto, um es an den LDAP-Server zu binden, und zwar mit derselben Namenskonvention wie CIFS/SMB-Instanzen.
- Wenn ein SMB-Computerkonto erstellt wird, werden standardmäßig ausgeblendete Admin-Freigaben verwendet (siehe Abschnitt "„Standard versteckte Freigaben“") Werden auch erstellt (c€, Admin-Dollar, ipc-Dollar), aber diese Aktien haben keine ACLs zugewiesen und sind unzugänglich.
- Die Rechnungsobjekte werden standardmäßig in CN=Computer platziert, aber eine können Sie bei Bedarf eine andere OU festlegen. Siehe Abschnitt „Zum Erstellen von SMB-Computerkonten erforderliche Berechtigungen“ Informationen darüber, welche Zugriffsrechte zum Hinzufügen/Entfernen von Gerätekontonobjekten für Cloud Volumes Service erforderlich sind.

Wenn Cloud Volumes Service das SMB-Maschinenkonto zu Active Directory hinzufügt, werden die folgenden Felder ausgefüllt:

- cn (mit dem angegebenen SMB-Servernamen)
- DNSHostName (mit SMBserver.domain.com)
- MSDS-SupportedVerschlüsselungTypes (allows DES_CBC_MD5, RC4_HMAC_MD5, wenn die AES-Verschlüsselung nicht aktiviert ist; WENN die AES-Verschlüsselung aktiviert ist, SIND DES_CBC_MD5, RC4_HMAC_MD5, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96 für den Kerberos-Account zugelassen)
- Name (mit SMB-Servername)
- SAMAccountName (mit SMBserver-Kosten)
- ServicePrincipalName (mit Host/smbserver.domain.com und Host/smbserver-SPNs für Kerberos)

Wenn Sie schwächere Kerberos-Verschlüsselungstypen (Enctype) auf dem Maschinenkonto deaktivieren möchten, können Sie den Wert MSDS-SupportedVerschlüsselungTypes auf dem Maschinenkonto auf einen der Werte in der folgenden Tabelle ändern, um nur AES zu ermöglichen.

MSDS-SupportVerschlüsselungTypes Wert	Zuctype aktiviert
2	DES_CBC_MD5
4	RC4_HMAC
8	NUR AES128_CTS_HMAC_SHA1_96
16	NUR AES256_CTS_HMAC_SHA1_96
24	AES128_CTS_HMAC_SHA1_96 UND AES256_CTS_HMAC_SHA1_96
30	DES_CBC_MD5, RC4_HMAC, AES128_CTS_HMAC_SHA1_96 UND AES256_CTS_HMAC_SHA1_96

Um die AES-Verschlüsselung für SMB-Computerkonten zu aktivieren, klicken Sie beim Erstellen der Active Directory-Verbindung auf AES-Verschlüsselung für AD-Authentifizierung aktivieren.

Um die AES-Verschlüsselung für NFS-Kerberos zu aktivieren, "Weitere Informationen finden Sie in der Cloud Volumes Service-Dokumentation".

Andere NAS-Infrastruktur-Serviceabhängigkeiten (KDC, LDAP und DNS)

Bei der Verwendung von Cloud Volumes Service für NAS-Freigaben sind möglicherweise externe Abhängigkeiten erforderlich, um ordnungsgemäße Funktion sicherzustellen. Diese Abhängigkeiten spielen unter bestimmten Umständen eine Rolle. Die folgende Tabelle zeigt verschiedene Konfigurationsoptionen und ggf. erforderliche Abhängigkeiten.

Konfiguration	Erforderliche Abhängigkeiten
Nur NFSv3	Keine
Nur NFSv3 Kerberos	Windows Active Directory: * KDC * DNS * LDAP
Nur NFSv4.1	Konfiguration der Client-ID-Zuordnung (/etc/idmap.conf)
Nur Kerberos	• Konfiguration der Client-ID-Zuordnung (/etc/idmap.conf) • Windows Active Directory: KDC-DNS-LDAP
Nur SMB	Active Directory: * KDC * DNS
Multi-Protokoll-NAS (NFS und SMB)	• Konfiguration der Client-ID-Zuordnung (nur NFSv4.1; /etc/idmap.conf) • Windows Active Directory: KDC-DNS-LDAP

Kerberos Keytab-Rotation/Passwort-Reset für Computerkontoobjekte

Bei SMB-Computerkonten plant Cloud Volumes Service regelmäßige Passwortrücksetzungen für das SMB-Maschinenkonto. Diese Kennwortrücksetzung erfolgt mit Kerberos-Verschlüsselung und wird nach einem Zeitplan jeden vierten Sonntag zu einer zufälligen Zeit zwischen 23:00 und 1:00 UHR ausgeführt. Mit diesem Kennwort werden die Kerberos-Schlüsselversionen geändert, die Keytabs, die auf dem Cloud Volumes Service-System gespeichert sind, gedreht und die Sicherheit von SMB-Servern, die in Cloud Volumes Service ausgeführt werden, erhöht. Passwörter für Computerkonten sind randomisiert und Administratoren nicht bekannt.

Bei NFS-Kerberos-Computerkonten erfolgt ein Zurücksetzen des Passworts nur dann, wenn ein neuer Keytab mit dem KDC erstellt/ausgetauscht wird. Derzeit ist dies in Cloud Volumes Service nicht möglich.

Netzwerkports zur Verwendung mit LDAP und Kerberos

Wenn Sie LDAP und Kerberos verwenden, sollten Sie die von diesen Diensten verwendeten Netzwerkports ermitteln. Eine vollständige Liste der von Cloud Volumes Service verwendeten Ports finden Sie im "Cloud Volumes Service Dokumentation zu Sicherheitsüberlegungen".

LDAP

Cloud Volumes Service fungiert als LDAP-Client und verwendet Standard-LDAP-Suchanfragen für Benutzer- und Gruppensuchen nach UNIX-Identitäten. LDAP ist erforderlich, wenn Sie Benutzer und Gruppen außerhalb der von Cloud Volumes Service bereitgestellten Standardbenutzer verwenden möchten. LDAP ist auch erforderlich, wenn Sie die Verwendung von NFS Kerberos mit Benutzerprinzipals (z. B. user1@domain.com) planen. Derzeit wird nur LDAP unterstützt, die Microsoft Active Directory verwenden.

Wenn Sie Active Directory als UNIX LDAP-Server verwenden möchten, müssen Sie die erforderlichen UNIX-

Attribute für Benutzer und Gruppen ausfüllen, die Sie für UNIX-Identitäten verwenden möchten. Cloud Volumes Service verwendet eine Standard-LDAP-Schemavorlage, die Attribute basierend auf abfragt "RFC-2307-bis". Die folgende Tabelle zeigt die für Benutzer und Gruppen erforderlichen Mindestattribute für Active Directory und deren Verwendung für die einzelnen Attribute.

Weitere Informationen zum Festlegen von LDAP-Attributen in Active Directory finden Sie unter "Management des Dual-Protokoll-Zugriffs:"

Attribut	Das macht es
uid*	Gibt den UNIX-Benutzernamen an
UidNummer*	Gibt die numerische ID des UNIX-Benutzers an
GidNumber*	Gibt die numerische ID der primären Gruppe des UNIX-Benutzers an
ObjectClass*	Gibt an, welcher Objekttyp verwendet wird; Cloud Volumes Service erfordert, dass „Benutzer“ in die Liste der Objektklassen aufgenommen werden muss (ist standardmäßig in den meisten Active Directory-Bereitstellungen enthalten).
Name	Allgemeine Informationen zum Konto (echter Name, Telefonnummer usw.)
UnixUserpasswort	Kein Grund zur Festlegung; nicht in UNIX-Identitätssuchten für die NAS-Authentifizierung verwendet. Durch diese Einstellung wird der konfigurierte Wert unixUserPassword in Klartext gesetzt.
UnixHomeDirectory	Definiert den Pfad zu UNIX-Home-Verzeichnissen, wenn ein Benutzer sich von einem Linux-Client aus mit LDAP authentifiziert. Legen Sie diesen Wert fest, wenn Sie die Home-Directory-Funktion LDAP für UNIX verwenden möchten.
LoginShell	Definiert den Pfad zur Bash/Profile Shell für Linux-Clients, wenn ein Benutzer sich mit LDAP authentifiziert.

*Bezeichnet das Attribut, das für die ordnungsgemäße Funktion mit Cloud Volumes Service erforderlich ist. Die übrigen Attribute gelten nur für die Client-seitige Verwendung.

Attribut	Das macht es
kn*	Gibt den Namen der UNIX-Gruppe an. Bei der Verwendung von Active Directory für LDAP wird dieser Wert bei der ersten Erstellung des Objekts festgelegt, kann aber später geändert werden. Dieser Name darf nicht mit anderen Objekten identisch sein. Zum Beispiel, wenn Ihr UNIX-Benutzer namens user1 gehört zu einer Gruppe namens user1 auf Ihrem Linux-Client, Windows erlaubt nicht zwei Objekte mit dem gleichen cn-Attribut. Um dies zu umgehen, benennen Sie den Windows-Benutzer in einen eindeutigen Namen um (z. B. user1-UNIX); LDAP in Cloud Volumes Service verwendet das Attribut uid für UNIX-Benutzernamen.
GidNumber*	Gibt die numerische ID der UNIX-Gruppe an.
ObjectClass*	Gibt an, welcher Objekttyp verwendet wird; Cloud Volumes Service erfordert eine Gruppe, die in die Liste der Objektklassen aufgenommen werden soll (dieses Attribut ist standardmäßig in den meisten Active Directory-Bereitstellungen enthalten).
MitgliedschaftenUid	Gibt an, welche UNIX-Benutzer Mitglieder der UNIX-Gruppe sind. Bei Active Directory LDAP in Cloud Volumes Service ist dieses Feld nicht erforderlich. Das Cloud Volumes Service-LDAP-Schema verwendet das Mitgliedfeld für Gruppenmitgliedschaften.
Mitglied*	Erforderlich für Gruppenmitgliedschaften/sekundäre UNIX-Gruppen Dieses Feld wird ausgefüllt, indem Windows-Benutzer zu Windows-Gruppen hinzugefügt werden. Allerdings, wenn die Windows-Gruppen nicht über UNIX-Attribute gefüllt haben, sind sie nicht in der UNIX-Benutzer-Gruppenmitgliedliste enthalten. Alle Gruppen, die in NFS verfügbar sein müssen, müssen die in dieser Tabelle aufgeführten erforderlichen UNIX-Gruppenattribute ausfüllen.

*Bezeichnet das Attribut, das für die ordnungsgemäße Funktion mit Cloud Volumes Service erforderlich ist. Die übrigen Attribute gelten nur für die Client-seitige Verwendung.

LDAP-Bindeinformationen

Um Benutzer in LDAP abfragen zu können, muss Cloud Volumes Service den LDAP-Dienst binden (anmelden). Diese Anmeldung hat schreibgeschützte Berechtigungen und wird verwendet, um LDAP-UNIX-Attribute für Verzeichnissuchen abzufragen. Derzeit ist LDAP-Bindungen nur über die Verwendung eines SMB-Maschinenkontos möglich.

LDAP kann nur für aktiviert werden `CVS-Performance` Instanzen können für NFSv3, NFSv4.1 oder Dual-Protocol Volumes verwendet werden. Für die erfolgreiche Bereitstellung des LDAP-fähigen Volumes muss eine Active Directory-Verbindung in derselben Region wie das Cloud Volumes Service-Volume hergestellt werden.

Wenn LDAP aktiviert ist, tritt in bestimmten Szenarien Folgendes auf.

- Wenn nur NFSv3 oder NFSv4.1 für das Cloud Volumes Service-Projekt verwendet wird, wird im Active Directory-Domänencontroller ein neues Maschinenkonto erstellt, und der LDAP-Client in Cloud Volumes Service bindet sich mithilfe der Anmeldeinformationen für das Computerkonto an Active Directory. Für das NFS Volume und die verborgenen administrativen Standardfreigaben werden keine SMB-Freigaben erstellt (siehe Abschnitt "„Standard versteckte Freigaben“") Haben Freigabe-ACLs entfernt.
- Wenn Dual-Protokoll-Volumes für das Cloud Volumes Service-Projekt genutzt werden, wird nur das für SMB-Zugriff erstellte Maschinenkonto verwendet, um den LDAP-Client in Cloud Volumes Service an Active Directory zu binden. Es werden keine weiteren Computerkonten erstellt.
- Wenn dedizierte SMB-Volumes separat erstellt werden (entweder vor oder nach Aktivierung von NFS-Volumes mit LDAP), wird das Computerkonto für LDAP-Bindungen mit dem SMB-Computerkonto gemeinsam genutzt.
- Wenn NFS Kerberos ebenfalls aktiviert ist, werden zwei Computerkonten erstellt: Eins für SMB-Freigaben und/oder LDAP bindet und eins für die NFS-Kerberos-Authentifizierung.

LDAP-Abfragen

Obwohl LDAP-Bindungen verschlüsselt sind, werden LDAP-Abfragen über das Netzwerk im Klartext über den gemeinsamen LDAP-Port 389 übergeben. Dieser bekannte Port kann derzeit nicht in Cloud Volumes Service geändert werden. Infolgedessen kann ein Benutzer- und Gruppennamen, numerische IDs und Gruppenmitgliedschaften mit Zugriff auf Packet Sniffing im Netzwerk angezeigt werden.

Allerdings können Google Cloud VMs nicht schnuppern andere VM Unicast-Verkehr. Nur VMs, die aktiv am LDAP-Datenverkehr beteiligt sind (das heißt, binden zu können), können Datenverkehr vom LDAP-Server sehen. Weitere Informationen zum Packet Sniffing in Cloud Volumes Service finden Sie im Abschnitt "„Packet Sniffing/Trace Betrachtungen.“"

Standard für die LDAP-Client-Konfiguration

Wenn LDAP in einer Cloud Volumes Service-Instanz aktiviert ist, wird standardmäßig eine LDAP-Client-Konfiguration mit spezifischen Konfigurationsdetails erstellt. In einigen Fällen gelten Optionen entweder nicht für Cloud Volumes Service (nicht unterstützt) oder können nicht konfiguriert werden.

LDAP-Client-Option	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
LDAP-Serverliste	Legt LDAP-Servernamen oder IP-Adressen für Abfragen fest. Dies wird für Cloud Volumes Service nicht verwendet. Stattdessen wird Active Directory Domain zum Definieren von LDAP-Servern verwendet.	Nicht festgelegt	Nein
Active Directory-Domäne	Legt die Active Directory-Domäne für LDAP-Abfragen fest. Cloud Volumes Service nutzt SRV-Datensätze für LDAP in DNS, um LDAP-Server in der Domäne zu finden.	Legen Sie die Active Directory-Domäne fest, die in der Active Directory-Verbindung angegeben ist.	Nein

LDAP-Client-Option	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
Bevorzugte Active Directory-Server	Legt die bevorzugten Active Directory-Server fest, die für LDAP verwendet werden sollen. Nicht unterstützt durch Cloud Volumes Service. Verwenden Sie stattdessen Active Directory-Sites, um die LDAP-Serverauswahl zu steuern.	Nicht festgelegt.	Nein
Binden mit SMB Server Credentials	Bindet an LDAP über das SMB-Maschinenkonto. Derzeit ist die einzige unterstützte LDAP-Bindemethode in Cloud Volumes Service.	Richtig	Nein
Schemavorlage	Die Schemavorlage, die für LDAP-Abfragen verwendet wird.	MS-AD-BIS	Nein
LDAP-Serverport	Die für LDAP-Abfragen verwendete Portnummer. Cloud Volumes Service verwendet derzeit nur den Standard-LDAP-Port 389. LDAPS/Port 636 wird derzeit nicht unterstützt.	389	Nein
Ist LDAPS aktiviert	Steuert, ob LDAP over Secure Sockets Layer (SSL) für Abfragen und Bindungen verwendet wird. Derzeit nicht unterstützt von Cloud Volumes Service.	Falsch	Nein
Zeitüberschreitung bei Abfrage (Sek.)	Timeout für Abfragen. Wenn Abfragen länger als der angegebene Wert dauern, schlagen Abfragen fehl.	3	Nein

LDAP-Client-Option	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
Minimale Stufe Der Bind-Authentifizierung	Die minimal unterstützte Bindestufe. Da Cloud Volumes Service Computerkonten für LDAP-Bindungen verwendet und Active Directory standardmäßig keine anonymen Bindungen unterstützt, kommt diese Option aus Sicherheitsgründen nicht zum Spiel.	Anonym	Nein
DN binden	Der für Bindungen verwendete Benutzer/Distinguished Name (DN) wird verwendet, wenn einfache Bindung verwendet wird. Cloud Volumes Service verwendet Computerkonten für LDAP-Verbindungen und unterstützt derzeit keine einfache Bindeauthentifizierung.	Nicht festgelegt	Nein
Basis-DN	Der Basis-DN, der für LDAP-Suchen verwendet wird.	Die Windows-Domäne, die für die Active Directory-Verbindung im DN-Format verwendet wird (d. h. DC=Domain, DC=local).	Nein
Umfang der Basissuche	Der Suchbereich für Basis-DN-Suchvorgänge. Werte können Basis, Onelevel oder Unterbaum umfassen. Cloud Volumes Service unterstützt nur Unterbaumsuchen.	Unterbaum	Nein
Benutzer-DN	Definiert den DN, in dem der Benutzer nach LDAP-Abfragen startet. Derzeit wird Cloud Volumes Service nicht unterstützt, sodass alle Benutzersuchen am Basis-DN beginnen.	Nicht festgelegt	Nein

LDAP-Client-Option	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
Umfang der Benutzersuche	Der Suchbereich für Benutzer-DN sucht. Werte können Basis, Onelevel oder Unterbaum umfassen. Cloud Volumes Service unterstützt das Festlegen des Anwendungsbereichs für die Benutzersuche nicht.	Unterbaum	Nein
Gruppen-DN	Definiert den DN, in dem die Gruppensuche nach LDAP-Abfragen beginnen soll. Derzeit wird Cloud Volumes Service nicht unterstützt, daher beginnen alle Gruppensuchen am Basis-DN.	Nicht festgelegt	Nein
Bereich der Gruppensuche	Der Suchbereich für Gruppen-DN sucht. Werte können Basis, Onelevel oder Unterbaum umfassen. Cloud Volumes Service unterstützt das Festlegen des Umfangs der Gruppensuche nicht.	Unterbaum	Nein
Netzgruppe DN	Definiert den DN, in dem Netzgruppe nach LDAP-Abfragen startet. Derzeit wird Cloud Volumes Service nicht unterstützt, daher beginnen alle Netzgruppensuchvorgänge am Basis-DN.	Nicht festgelegt	Nein
Suchumfang für Netzgruppe	Der Suchbereich für Netzgruppe DN sucht. Werte können Basis, Onelevel oder Unterbaum umfassen. Cloud Volumes Service unterstützt nicht das Festlegen des Suchbereichs für Netzgruppen.	Unterbaum	Nein

LDAP-Client-Option	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
Verwenden Sie Start_tls über LDAP	Nutzt Start TLS für zertifikatbasierte LDAP-Verbindungen über Port 389. Derzeit nicht unterstützt von Cloud Volumes Service.	Falsch	Nein
Aktivieren Sie die Suche in netgroup-by-Host	Ermöglicht die Suche in einer Netzwerkgruppe nach Hostnamen und nicht die Erweiterung von Netgroups, um alle Mitglieder aufzulisten. Derzeit nicht unterstützt von Cloud Volumes Service.	Falsch	Nein
Netgroup-by-Host DN	Definiert den DN, in dem netgroup-by-Host nach LDAP-Abfragen startet. Netgroup-by-Host wird derzeit für Cloud Volumes Service nicht unterstützt.	Nicht festgelegt	Nein
Suchumfang für Netzgruppe nach Host	Der Suchbereich für netgroup-by-Host DN sucht. Werte können Basis, Onelevel oder Unterbaum enthalten. Netgroup-by-Host wird derzeit für Cloud Volumes Service nicht unterstützt.	Unterbaum	Nein
Sicherheit der Client-Session	Definiert, in welchem Maß die Sitzungssicherheit von LDAP verwendet wird (Zeichen, Siegel oder keine). Das LDAP-Signieren wird von CVS-Performance unterstützt, sofern dies von Active Directory angefordert wird. CVS-SW unterstützt LDAP-Signatur nicht. Für beide Servicetypen wird die Dichtung derzeit nicht unterstützt.	Keine	Nein

LDAP-Client-Option	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
LDAP-Verweisungsjagd	Bei der Verwendung mehrerer LDAP-Server ermöglicht die Verweisungsjagd dem Client, auf andere LDAP-Server in der Liste zu verweisen, wenn ein Eintrag nicht im ersten Server gefunden wird. Dies wird derzeit nicht von Cloud Volumes Service unterstützt.	Falsch	Nein
Filter für Gruppenmitgliedschaft	Bietet einen benutzerdefinierten LDAP-Suchfilter, der verwendet werden kann, wenn eine Gruppenmitgliedschaft von einem LDAP-Server aus gesucht wird. Derzeit nicht unterstützt mit Cloud Volumes Service.	Nicht festgelegt	Nein

LDAP für asymmetrische Namenszuweisung verwenden

Cloud Volumes Service ordnet Windows-Benutzern und UNIX-Benutzern standardmäßig ohne spezielle Konfiguration bidirektional identische Benutzernamen zu. Solange Cloud Volumes Service einen gültigen UNIX-Benutzer (mit LDAP) finden kann, erfolgt die 1:1-Namenszuweisung. Beispiel: Wenn Windows-Benutzer `johnsmith` Wird verwendet, dann, wenn Cloud Volumes Service einen UNIX-Benutzer namens finden kann `johnsmith` In LDAP ist die Namenszuordnung für diesen Benutzer erfolgreich, alle Dateien/Ordner, die von erstellt wurden `johnsmith` Zeigen Sie den korrekten Benutzerbesitz und alle ACLs an, die davon betroffen sind `johnsmith` Unabhängig vom verwendeten NAS-Protokoll honoriert werden. Dies wird als symmetrisches Namenszuordnungen bezeichnet.

Asymmetrisches Namenszuordnungen ist, wenn die Windows-Benutzer- und UNIX-Benutzeridentität nicht übereinstimmt. Beispiel: Wenn Windows-Benutzer `johnsmith` Hat eine UNIX-Identität von `jsmith`, Cloud Volumes Service braucht einen Weg, um über die Variation zu erzählen. Da Cloud Volumes Service derzeit nicht die Erstellung von statischen Name Mapping Regeln unterstützt, muss LDAP verwendet werden, um die Identität der Benutzer für Windows und UNIX Identitäten zu suchen, um die ordnungsgemäße Eigentum von Dateien und Ordnern und erwarteten Berechtigungen zu gewährleisten.

Standardmäßig enthält Cloud Volumes Service Folgendes `LDAP` Im ns-Switch der Instanz für die Name-Map-Datenbank, sodass Sie die Namenszuordnungsfunktion durch die Verwendung von LDAP für asymmetrische Namen bereitstellen können, müssen Sie nur einige der Benutzer-/Gruppenattribute ändern, um das zu reflektieren, was Cloud Volumes Service sucht.

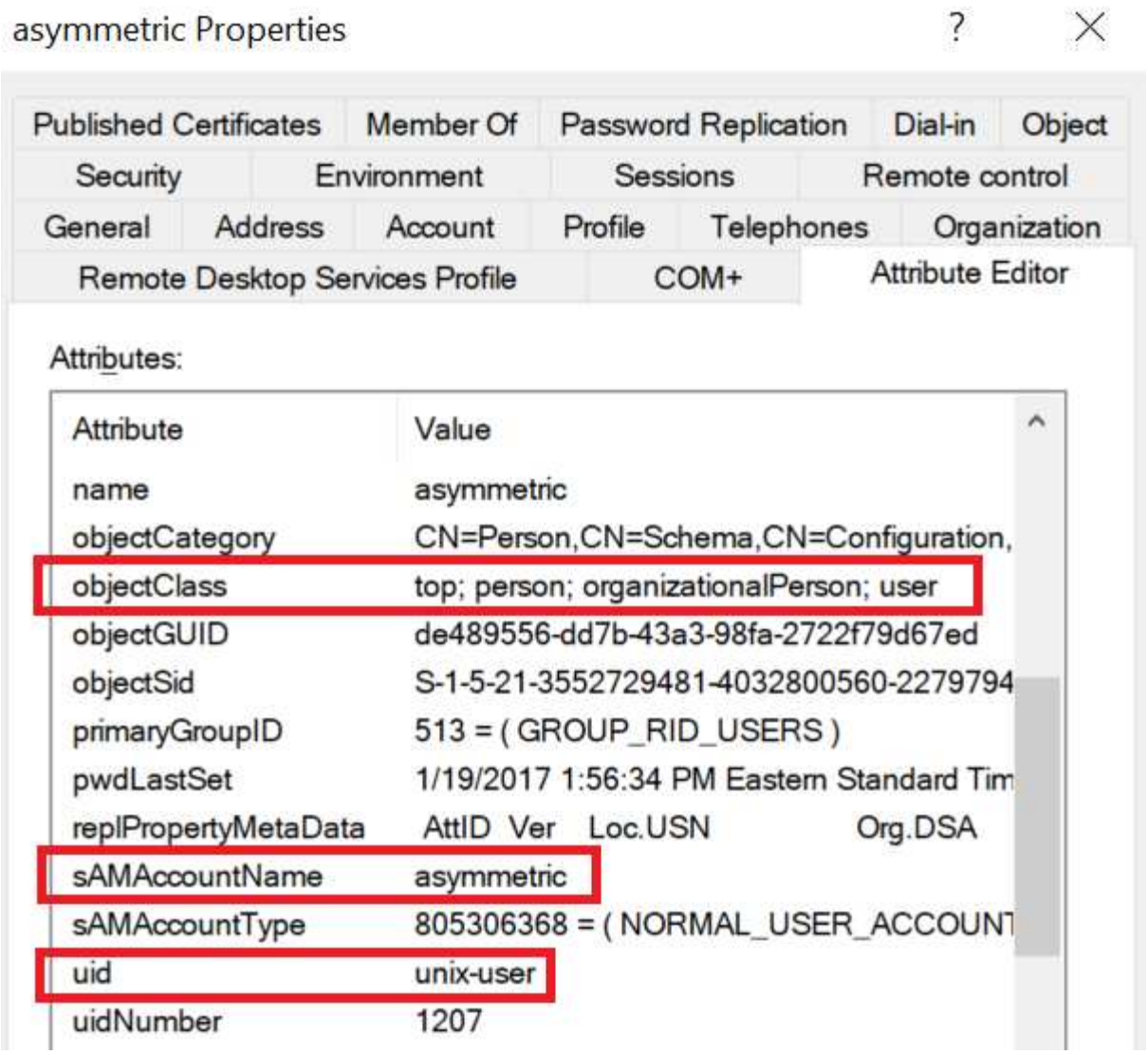
In der folgenden Tabelle wird gezeigt, welche Attribute für die asymmetrische Namenszuordnungsfunktion in LDAP ausgefüllt werden müssen. In den meisten Fällen ist Active Directory bereits dafür konfiguriert.

Cloud Volumes Service Attribut	Das macht es	Von Cloud Volumes Service für die Namenszuweisung verwendeter Wert
Windows auf UNIX objectClass	Gibt den Typ des verwendeten Objekts an. (D. h. Benutzer, Gruppe, PosixAccount usw.)	Muss Benutzer enthalten (kann mehrere andere Werte enthalten, falls gewünscht.)
Attribut Windows zu UNIX	Dies definiert den Windows-Benutzernamen bei der Erstellung. Cloud Volumes Service verwendet dies für Windows-to-UNIX-Lookups.	Hier ist keine Änderung erforderlich; sAMAccountName ist der gleiche wie der Windows-Anmeldename.
UID	Definiert den UNIX-Benutzernamen.	Gewünschter UNIX-Benutzername.

Cloud Volumes Service verwendet derzeit keine Domänenpräfixe in LDAP-Lookups, so dass mehrere Domänen-LDAP-Umgebungen nicht richtig funktionieren mit LDAP-Namemap-Lookups.

Im folgenden Beispiel wird ein Benutzer mit dem Windows-Namen angezeigt `asymmetric`, Der UNIX-Name `unix-user`, Und das Verhalten folgt es beim Schreiben von Dateien sowohl aus SMB und NFS.

Die folgende Abbildung zeigt, wie LDAP-Attribute vom Windows-Server aussehen.



Von einem NFS-Client aus können Sie den UNIX-Namen, nicht jedoch den Windows-Namen abfragen:

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

Wenn eine Datei aus NFS als geschrieben wird `unix-user`, Das folgende Ergebnis ist von dem NFS Client:

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

Von einem Windows-Client aus sehen Sie, dass der Eigentümer der Datei auf den richtigen Windows-Benutzer eingestellt ist:

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

Umgekehrt werden Dateien vom Windows-Benutzer erstellt `asymmetric` Von einem SMB-Client wird der richtige UNIX-Eigentümer angezeigt, wie im folgenden Text dargestellt.

SMB:

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

LDAP-Kanalbindung

Aufgrund einer Schwachstelle bei Windows Active Directory-Domänencontrollern "Microsoft Security Advisory ADV190023" Ändert die Art und Weise, wie DCs LDAP-Bindungen zulassen.

Die Auswirkungen von Cloud Volumes Service sind dieselben wie für alle LDAP-Clients. Cloud Volumes Service unterstützt derzeit keine Channel-Bindung. Da Cloud Volumes Service standardmäßig LDAP-Signatur durch Aushandlung unterstützt, sollte die LDAP-Channel-Bindung kein Problem darstellen. Wenn Sie Probleme mit der Bindung an LDAP bei aktivierter Kanalbindung haben, befolgen Sie die Schritte zur Problembehebung in ADV190023, damit LDAP-Bindungen von Cloud Volumes Service erfolgreich durchgeführt werden können.

DNS

Active Directory und Kerberos haben beide Abhängigkeiten von DNS für den Hostnamen zu IP/IP bis zur Auflösung des Hostnamens. DNS erfordert, dass Port 53 offen ist. Cloud Volumes Service nimmt keine Änderungen an DNS-Einträgen vor und unterstützt derzeit nicht die Verwendung von "Dynamisches DNS" An Netzwerkschnittstellen.

Sie können Active Directory DNS so konfigurieren, dass Sie festlegen können, welche Server DNS-Einträge aktualisieren können. Weitere Informationen finden Sie unter "Sicheres Windows DNS".

Beachten Sie, dass Ressourcen innerhalb eines Google-Projekts standardmäßig mit Google Cloud DNS, die nicht mit Active Directory DNS verbunden ist. Clients, die Cloud DNS verwenden, können keine UNC-Pfade auflösen, die von Cloud Volumes Service zurückgegeben werden. Windows-Clients, die mit der Active

Directory-Domäne verbunden sind, sind für die Verwendung von Active Directory DNS konfiguriert und können solche UNC-Pfade auflösen.

Um einem Client zu Active Directory beizutreten, müssen Sie seine DNS-Konfiguration so konfigurieren, dass Active Directory DNS verwendet wird. Optional können Sie Cloud DNS konfigurieren, um Anfragen an Active Directory DNS weiterzuleiten. Siehe "Warum kann mein Client den SMB NetBIOS-Namen nicht lösen?"Finden Sie weitere Informationen.

> Cloud Volumes Service unterstützt derzeit keine DNSSEC- und DNS-Abfragen werden im Klartext ausgeführt.

Prüfung von Dateizugriffen

Derzeit nicht unterstützt für Cloud Volumes Service.

Virenschutz

Sie müssen in Cloud Volumes Service am Client auf eine NAS-Freigabe Antivirenprüfungen durchführen. Derzeit ist keine native Virenschutz-Integration in Cloud Volumes Service möglich.

Service-Betrieb

Das Cloud Volumes Service-Team verwaltet die Backend-Services in Google Cloud und nutzt verschiedene Strategien, um die Plattform zu sichern und unerwünschte Zugriffe zu vermeiden.

Jeder Kunde erhält sein eigenes Subnetz, mit dem standardmäßig Zugriff von anderen Kunden isoliert ist. Jeder Mandant in Cloud Volumes Service erhält seinen eigenen Namespace und VLAN für eine vollständige Datenisolierung. Nachdem ein Benutzer authentifiziert wurde, kann die Service Delivery Engine (SDE) nur noch Konfigurationsdaten für diesen Mandanten lesen.

Physische Sicherheit

Mit entsprechender Vorabgenehmigung haben nur Techniker vor Ort und NetApp Außendiensttechniker (Field Support Engineers, FSEs) Zugriff auf den Käfig und die Racks für physische Arbeiten. Storage- und Netzwerk-Management ist nicht zulässig. Nur diese Ressourcen vor Ort sind in der Lage, Hardware-Wartungsarbeiten durchzuführen.

Für Techniker vor Ort wird ein Ticket für die Leistungsbeschreibung (Statement of Work, SOW) angehoben, das die Rack-ID und den Standort des Geräts (RU) enthält. Alle weiteren Details sind im Ticket enthalten. Bei NetApp FSEs muss ein Besuchsticket vor Ort mit COLO GELEGT werden, und das Ticket enthält die Daten, das Datum und die Zeit der Besucher zu Audit-Zwecken. Das SOW für den FSE wird intern an NetApp kommuniziert.

Operations Team

Das Betriebsteam für Cloud Volumes Service setzt sich aus Produktionstechnik und einem Site Reliability Engineer (SRE) für Cloud Volume Services sowie NetApp Field Support Engineers und Hardware-Partnern zusammen. Alle Mitglieder des Betriebsteams sind für die Arbeit in Google Cloud akkreditiert und für jedes angehobene Ticket werden detaillierte Arbeitsunterlagen aufbewahrt. Darüber hinaus gibt es einen strengen Änderungskontroll- und Genehmigungsprozess, um sicherzustellen, dass jede Entscheidung angemessen überprüft wird.

Das SRE-Team verwaltet die Kontrollebene und wie die Daten von UI-Anfragen an Back-End-Hardware und

-Software in Cloud Volumes Service weitergeleitet werden. Das SRE-Team verwaltet außerdem Systemressourcen, wie z. B. die maximale Anzahl von Volumes und Inode. SRES dürfen nicht mit Kundendaten interagieren oder Zugriff haben. Darüber hinaus koordiniert SRES mit Return Material Authorizations (RMAs), wie z. B. neue Festplatten- oder Speicherersatzanfragen für die Backend-Hardware.

Mitwirkungspflichten des Kunden

Kunden von Cloud Volumes Service verwalten das Active Directory und die Benutzerrollenverwaltung sowie die Menge und die Datenvorgänge ihrer Organisation. Kunden können über Administratorrollen verfügen und Berechtigungen an andere Endbenutzer innerhalb desselben Google Cloud-Projekts delegieren. Dabei werden die beiden vordefinierten Rollen verwendet, die NetApp und Google Cloud (Administrator und Viewer) bereitstellen.

Der Administrator kann eine beliebige VPC im Kundenprojekt an Cloud Volumes Service Peer, die der Kunde für angemessen entscheidet. Der Kunde ist selbst dafür verantwortlich, den Zugriff auf sein Google Cloud Marketplace Abonnement zu managen und die VPCs zu managen, die Zugriff auf die Datenebene haben.

Bösartiger SRE-Schutz

Ein Problem, das entstehen könnte, ist, wie schützt Cloud Volumes Service vor Szenarien, in denen es einen bösartigen SRE gibt oder wenn die SRE-Anmeldeinformationen kompromittiert wurden?

Der Zugang zur Produktionsumgebung ist nur mit einer begrenzten Anzahl von SRE-Einzelpersonen möglich. Darüber hinaus sind Administratorrechte auf eine Handvoll erfahrener Administratoren beschränkt. Alle Aktionen, die von jedem Mitarbeiter der Cloud Volumes Service Produktionsumgebung ausgeführt werden, werden protokolliert. Anomalien an der Basis- oder verdächtigen Aktivitäten werden durch unsere SIEM-Plattform (Security Information and Event Management) Threat Intelligence (Threat Intelligence Platform) erkannt. Dadurch können böswillige Aktionen nachverfolgt und abgemildert werden, bevor das Cloud Volumes Service-Backend zu einem zu großen Schaden angerichtet wird.

Volumenlebenszyklus

Cloud Volumes Service managt nur die Objekte innerhalb des Service, nicht die Daten innerhalb der Volumes. Nur Clients, die auf die Volumes zugreifen, können die Daten, ACLs, Dateieigentümer usw. managen. Die Daten in diesen Volumes sind im Ruhezustand verschlüsselt und der Zugriff ist auf Mandanten der Cloud Volumes Service Instanz beschränkt.

Der Lebenszyklus eines Volumes für Cloud Volumes Service ist create-Update-delete. Volumes behalten Snapshot Kopien von Volumes, bis die Volumes gelöscht werden. Nur validierte Cloud Volumes Service Administratoren können Volumes in Cloud Volumes Service löschen. Wenn ein Administrator eine Volume-Löschung angefordert hat, muss ein zusätzlicher Schritt zur Eingabe des Volume-Namens erforderlich sein, um die Löschung zu überprüfen. Nachdem ein Volume gelöscht wurde, ist das Volume verschwunden und kann nicht wiederhergestellt werden.

Falls ein Cloud Volumes Service-Vertrag beendet wird, kennzeichnet NetApp Volumes nach einem bestimmten Zeitraum zum Löschen. Bevor dieser Zeitraum abläuft, können Sie Volumes auf Kundenwunsch wiederherstellen.

Zertifizierungen

Cloud Volumes Services für Google Cloud sind derzeit nach den Standards ISO/IEC 27001:2013 und ISO/IEC 27018:2019 zertifiziert. Der Service erhielt kürzlich auch seinen SOC2 Type I Attestation Report. Weitere Informationen über die Verpflichtung von NetApp zur Datensicherheit und zum Datenschutz finden Sie unter "Compliance: Datensicherheit und Datenschutz".

DSGVO

Unsere Verpflichtung zu Datenschutz und Einhaltung der DSGVO steht in mehreren unserer zahlreichen verfügbar "Kundenverträge", Wie unsere "Ergänzung Zur Kundendatenverarbeitung", Das beinhaltet die "Standardvertragsklauseln" Von der Europäischen Kommission bereitgestellt. Diese Verpflichtungen stellen wir auch in unserer Datenschutzrichtlinie ein, die durch die zentralen Werte unseres Unternehmenskodex eingehalten wird.

Weitere Informationen und Kontaktdaten

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- Google Cloud-Dokumentation für Cloud Volumes Service

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes/"

- Google Private Service-Zugriff

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- NetApp Produktdokumentation

  "https://www.netapp.com/support-and-training/documentation/"

- Kryptografisches Validierungsmodul-Programm – NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- NetApp Lösung gegen Ransomware

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616: NFS Kerberos im ONTAP

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

Kontaktieren Sie uns

Lassen Sie uns wissen, wie wir diesen technischen Bericht verbessern können.

Kontaktieren Sie uns unter doccomments@netapp.com. Nehmen SIE den TECHNISCHEN BERICHT 4918 in die Betreffzeile auf.