



# Erste Schritte in GCP

## Cloud Manager 3.8

NetApp  
March 25, 2024

# Inhalt

- Erste Schritte in GCP ..... 1
  - Erste Schritte mit Cloud Volumes ONTAP für Google Cloud ..... 1
  - Cloud Volumes ONTAP-Konfiguration in Google Cloud planen ..... 2
  - Netzwerkanforderungen für die Implementierung und das Management von Cloud Volumes ONTAP in GCP ..... 5
  - Nutzung von vom Kunden gemanagten Schlüsseln mit Cloud Volumes ONTAP ..... 14
  - Einführung von Cloud Volumes ONTAP in GCP ..... 16

# Erste Schritte in GCP

## Erste Schritte mit Cloud Volumes ONTAP für Google Cloud

### Erste Schritte mit Cloud Volumes ONTAP für GCP



#### Einen Konnektor erstellen

Wenn Sie keine haben ["Stecker"](#) Dennoch muss ein Kontoadministrator einen erstellen. ["Connector in GCP erstellen"](#).

Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von Cloud Manager aufgefordert, einen Connector bereitzustellen, wenn Sie noch keinen haben.



#### Planen Sie Ihre Konfiguration

Cloud Manager bietet vorkonfigurierte Pakete, die Ihren Workload-Anforderungen entsprechen, oder Sie können eine eigene Konfiguration erstellen. Wenn Sie sich für eine eigene Konfiguration entscheiden, sollten Sie sich mit den verfügbaren Optionen vertraut machen. ["Weitere Informationen ."](#)



#### Richten Sie Ihr Netzwerk ein

1. Stellen Sie sicher, dass Ihre VPC und Subnetze die Konnektivität zwischen dem Connector und Cloud Volumes ONTAP unterstützen.
2. Aktivieren Sie den Outbound-Internetzugang über die Ziel-VPC, damit der Connector und der Cloud Volumes ONTAP mehrere Endpunkte kontaktieren können.

Dieser Schritt ist wichtig, da der Connector Cloud Volumes ONTAP nicht ohne Outbound-Internetzugang verwalten kann. Wenn Sie die ausgehende Verbindung begrenzen müssen, lesen Sie die Liste der Endpunkte für ["Anschluss und Cloud Volumes ONTAP"](#).

["Erfahren Sie mehr über Netzwerkanforderungen"](#).



#### GCP für Daten-Tiering einrichten

Für das Tiering von kalten Daten von Cloud Volumes ONTAP auf kostengünstigen Objekt-Storage (ein Google Cloud-Storage-Bucket) müssen zwei Anforderungen erfüllt werden:

1. ["Konfigurieren Sie das Cloud Volumes ONTAP-Subnetz für privaten Google-Zugriff"](#).
2. ["Service-Konto für Daten-Tiering einrichten"](#):
  - Weisen Sie dem Tiering-Service-Konto die vordefinierte Rolle „*Storage Admin*“ zu.
  - Fügen Sie das Connector-Dienstkonto als *Service-Konto-Benutzer* zum Tiering-Dienstkonto hinzu.

Sie können die Benutzerrolle angeben ["In Schritt 3 des Assistenten, wenn Sie das Tiering Service-](#)

[Konto erstellen](#)", Oder ["Geben Sie die Rolle nach der Erstellung des Dienstkontos ein"](#).

Sie müssen das Tiering Service-Konto später auswählen, wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen.

Wenn Sie kein Daten-Tiering aktivieren und bei der Erstellung des Cloud Volumes ONTAP-Systems ein Service-Konto auswählen, müssen Sie das System deaktivieren und das Service-Konto über die GCP-Konsole zu Cloud Volumes ONTAP hinzufügen.



#### Aktivieren Sie Google Cloud-APIs

["Aktivieren Sie die folgenden Google Cloud APIs in Ihrem Projekt"](#). Diese APIs sind für die Implementierung des Connectors und der Cloud Volumes ONTAP erforderlich.

- Cloud Deployment Manager V2-API
- Cloud-ProtokollierungsAPI
- Cloud Resource Manager API
- Compute Engine-API
- IAM-API (Identitäts- und Zugriffsmanagement)



#### Starten Sie Cloud Volumes ONTAP mit Cloud Manager

Klicken Sie auf **Arbeitsumgebung hinzufügen**, wählen Sie den Systemtyp aus, den Sie bereitstellen möchten, und führen Sie die Schritte im Assistenten aus. ["Lesen Sie Schritt-für-Schritt-Anleitungen"](#).

#### Weiterführende Links

- ["Bewertung"](#)
- ["Erstellen eines Connectors über Cloud Manager"](#)
- ["Installieren der Connector-Software auf einem Linux-Host"](#)
- ["Was Cloud Manager mit GCP-Berechtigungen macht"](#)

## Cloud Volumes ONTAP-Konfiguration in Google Cloud planen

Wenn Sie Cloud Volumes ONTAP in Google Cloud implementieren, können Sie entweder ein vorkonfiguriertes System wählen, das Ihren Workload-Anforderungen entspricht, oder Sie erstellen Ihre eigene Konfiguration. Wenn Sie sich für eine eigene Konfiguration entscheiden, sollten Sie sich mit den verfügbaren Optionen vertraut machen.

### Auswahl eines Lizenztyps

Cloud Volumes ONTAP ist in zwei Preisoptionen erhältlich: Nutzungsbasiert und als BYOL-Modell (Bring-Your-Own-License). Für Pay-as-you-go können Sie zwischen drei Lizenzen wählen: Explore, Standard oder Premium. Jede Lizenz bietet verschiedene Kapazitäts- und Computing-Optionen.

## Storage-Grenzen kennen

Die Rohkapazitätsgrenze für ein Cloud Volumes ONTAP System ist an die Lizenz gebunden. Zusätzliche Beschränkungen wirken sich auf die Größe von Aggregaten und Volumes aus. Sie sollten sich dieser Grenzen bei der Planung Ihrer Konfiguration bewusst sein.

["Storage-Grenzen für Cloud Volumes ONTAP 9.7 in GCP"](#)

## Dimensionierung Ihres Systems in GCP

Mit der Dimensionierung Ihres Cloud Volumes ONTAP Systems können Sie die Anforderungen an Performance und Kapazität erfüllen. Bei der Auswahl von Maschinentyp, Festplattentyp und Festplattengröße sind einige wichtige Punkte zu beachten:

### Maschinentyp

Sehen Sie sich die unterstützten Maschinentypen im an ["Versionshinweise zu Cloud Volumes ONTAP"](#) Und dann lesen Sie die Details von Google zu jedem unterstützten Maschinentyp durch. Passen Sie Ihre Workload-Anforderungen an die Anzahl an vCPUs und Speicher für den Maschinentyp an. Beachten Sie, dass jeder CPU-Kern die Netzwerk-Performance steigert.

Weitere Informationen finden Sie im Folgenden:

- ["Google Cloud-Dokumentation: N1 Standard-Maschinentypen"](#)
- ["Google Cloud Dokumentation: Performance"](#)

### GCP-Festplattentyp

Bei der Erstellung von Volumes für Cloud Volumes ONTAP müssen Sie den zugrunde liegenden Cloud-Storage auswählen, den Cloud Volumes ONTAP für eine Festplatte verwendet. Der Festplattentyp kann entweder *Zonal SSD Persistent Disks* oder *Zonal Standard Persistent Disks* sein.

Persistente SSD-Festplatten eignen sich ideal für Workloads, die eine hohe Anzahl von zufälligen IOPS erfordern, während Standard-persistente Festplatten wirtschaftlich sind und sequenzielle Lese-/Schreibvorgänge verarbeiten können. Weitere Informationen finden Sie unter ["Google Cloud-Dokumentation: Zonal Persistent Disks \(Standard und SSD\)"](#).

### GCP-Festplattengröße

Sie müssen bei der Implementierung eines Cloud Volumes ONTAP Systems die ursprüngliche Festplattengröße auswählen. Danach können Sie mit Cloud Manager die Kapazität eines Systems für Sie verwalten. Wenn Sie jedoch die Aggregate selbst erstellen möchten, beachten Sie Folgendes:

- Alle Festplatten in einem Aggregat müssen dieselbe Größe haben.
- Ermitteln Sie den Speicherplatz, den Sie benötigen, während Sie gleichzeitig die Performance in Betracht ziehen.
- Die Performance persistenter Festplatten lässt sich automatisch mit der Festplattengröße und der Anzahl der für das System verfügbaren vCPUs skalieren.

Weitere Informationen finden Sie im Folgenden:

- ["Google Cloud-Dokumentation: Zonal Persistent Disks \(Standard und SSD\)"](#)
- ["Google Cloud-Dokumentation: Optimierung von Persistent Disk und lokaler SSD-Performance"](#)

## Informationarbeitsblatt für das GCP-Netzwerk

Bei der Implementierung von Cloud Volumes ONTAP in GCP müssen Details zu Ihrem virtuellen Netzwerk angegeben werden. Sie können ein Arbeitsblatt verwenden, um die Informationen von Ihrem Administrator zu sammeln.

GCP-Informationen	Ihr Wert
Region	
Zone	
VPC-Netzwerk	
Subnetz	
Firewallrichtlinie (bei Nutzung eigener Richtlinien)	

## Auswählen einer Schreibgeschwindigkeit

Mit Cloud Manager können Sie eine Einstellung für die Schreibgeschwindigkeit für Cloud Volumes ONTAP Systeme mit einem Node wählen. Bevor Sie sich für eine Schreibgeschwindigkeit entscheiden, sollten Sie die Unterschiede zwischen den normalen und hohen Einstellungen sowie Risiken und Empfehlungen verstehen, wenn Sie eine hohe Schreibgeschwindigkeit verwenden.

### Unterschied zwischen normaler Schreibgeschwindigkeit und hoher Schreibgeschwindigkeit

Wenn Sie sich für eine normale Schreibgeschwindigkeit entscheiden, werden die Daten direkt auf die Festplatte geschrieben, wodurch die Wahrscheinlichkeit eines Datenverlusts bei einem ungeplanten Systemausfall verringert wird.

Wenn Sie hohe Schreibgeschwindigkeit wählen, werden die Daten vor dem Schreiben auf die Festplatte im Speicher gepuffert, was eine schnellere Schreibleistung ermöglicht. Aufgrund dieses Cachings besteht die Gefahr eines Datenverlusts, wenn ein ungeplanter Systemausfall auftritt.

Die Datenmenge, die bei einem ungeplanten Systemausfall verloren gehen kann, entspricht der Spanne der letzten beiden Konsistenzpunkte. Ein Konsistenzpunkt ist das Schreiben gepufferter Daten auf die Festplatte. Ein Konsistenzpunkt tritt auf, wenn das Schreibprotokoll voll ist oder nach 10 Sekunden (je nachdem, was zuerst eintritt). Die Performance des AWS EBS-Volumes kann sich jedoch auf die Verarbeitungszeit des Konsistenzpunkts auswirken.

### Wann wird hohe Schreibgeschwindigkeit verwendet

Hohe Schreibgeschwindigkeit ist eine gute Wahl, wenn für Ihre Workload eine schnelle Schreibleistung erforderlich ist und Sie das Risiko eines Datenverlusts bei einem ungeplanten Systemausfall überstehen können.

### Empfehlungen bei hoher Schreibgeschwindigkeit

Wenn Sie die hohe Schreibgeschwindigkeit aktivieren, sollten Sie den Schreibschutz auf der Anwendungsebene sicherstellen.

## Auswählen eines Volume-Nutzungsprofils

ONTAP umfasst mehrere Storage-Effizienzfunktionen, mit denen Sie die benötigte Storage-Gesamtmenge

reduzieren können. Wenn Sie ein Volume in Cloud Manager erstellen, können Sie ein Profil auswählen, das diese Funktionen aktiviert, oder ein Profil, das sie deaktiviert. Sie sollten mehr über diese Funktionen erfahren, um zu entscheiden, welches Profil Sie verwenden möchten.

NetApp Storage-Effizienzfunktionen bieten folgende Vorteile:

### **Thin Provisioning**

Bietet Hosts oder Benutzern mehr logischen Storage als in Ihrem physischen Storage-Pool. Anstatt Storage vorab zuzuweisen, wird jedem Volume beim Schreiben von Daten dynamisch Speicherplatz zugewiesen.

### **Deduplizierung**

Verbessert die Effizienz, indem identische Datenblöcke lokalisiert und durch Verweise auf einen einzelnen gemeinsam genutzten Block ersetzt werden. Durch diese Technik werden die Storage-Kapazitätsanforderungen reduziert, da redundante Datenblöcke im selben Volume eliminiert werden.

### **Komprimierung**

Reduziert die physische Kapazität, die zum Speichern von Daten erforderlich ist, indem Daten in einem Volume auf primärem, sekundärem und Archiv-Storage komprimiert werden.

## **Netzwerkanforderungen für die Implementierung und das Management von Cloud Volumes ONTAP in GCP**

Richten Sie das Netzwerk Ihrer Google Cloud-Plattform ein, damit Cloud Volumes ONTAP-Systeme ordnungsgemäß funktionieren können. Dazu gehört auch die Vernetzung von Connector und Cloud Volumes ONTAP.

### **Anforderungen für Cloud Volumes ONTAP**

Die folgenden Anforderungen müssen in GCP erfüllt sein.

#### **Virtuelle Private Cloud**

Cloud Volumes ONTAP und der Connector werden in einer gemeinsamen Google Cloud VPC und auch in nicht-freigegebenen VPCs unterstützt.

Mit einer gemeinsam genutzten VPC können Sie virtuelle Netzwerke über mehrere Projekte hinweg konfigurieren und zentral managen. Sie können freigegebene VPC-Netzwerke im `_Host-Projekt_` einrichten und die Instanzen von Connector und Cloud Volumes ONTAP Virtual Machine in einem *Service-Projekt* implementieren. "[Google Cloud-Dokumentation: Gemeinsame VPC-Übersicht](#)".

Die einzige Anforderung bei der Verwendung einer gemeinsamen VPC ist die "[Benutzerrolle für das Netzwerk wird berechnet](#)" An das Konnektor-Dienstkonto. Cloud Manager benötigt diese Berechtigungen, um Firewalls, VPC und Subnetze im Host-Projekt abzufragen.

#### **Outbound-Internetzugang für Cloud Volumes ONTAP**

Cloud Volumes ONTAP erfordert ausgehenden Internetzugang, um Nachrichten an NetApp AutoSupport zu senden, der proaktiv den Zustand Ihres Storage überwacht.

Routing- und Firewall-Richtlinien müssen HTTP-/HTTPS-Datenverkehr an die folgenden Endpunkte ermöglichen, damit Cloud Volumes ONTAP AutoSupport-Meldungen senden kann:

- <https://support.netapp.com/aods/asupmessage>

- <https://support.netapp.com/asupprod/post/1.0/postAsup>

["Erfahren Sie, wie AutoSupport konfiguriert wird"](#).

## Anzahl der IP-Adressen

Cloud Manager weist Cloud Volumes ONTAP in GCP 5 IP-Adressen zu.

Beachten Sie, dass Cloud Manager keine SVM-Management-LIF für Cloud Volumes ONTAP in GCP erstellt.



Ein LIF ist eine IP-Adresse, die einem physischen Port zugewiesen ist. Für Managementtools wie SnapCenter ist eine SVM-Management-LIF erforderlich.

## Firewall-Regeln

Sie müssen keine Firewall-Regeln erstellen, weil Cloud Manager das für Sie macht. Wenn Sie Ihre eigene verwenden müssen, beachten Sie die unten aufgeführten Firewall-Regeln.

## Verbindung von Cloud Volumes ONTAP zu Google Cloud Storage für Daten-Tiering

Wenn „kalte“ Daten in einen Google Cloud Storage Bucket verschoben werden sollen, muss das Subnetz, in dem Cloud Volumes ONTAP residiert, für privaten Google Zugriff konfiguriert sein. Anweisungen finden Sie unter ["Google Cloud-Dokumentation: Privaten Google Access konfigurieren"](#).

Weitere Schritte zur Einrichtung von Daten-Tiering in Cloud Manager finden Sie unter ["Tiering von kalten Daten auf kostengünstigen Objekt-Storage"](#).

## Verbindungen zu ONTAP Systemen in anderen Netzwerken

Zur Replizierung von Daten zwischen einem Cloud Volumes ONTAP System in GCP und ONTAP Systemen in anderen Netzwerken müssen Sie eine VPN-Verbindung zwischen der VPC und dem anderen Netzwerk herstellen, beispielsweise mit dem Unternehmensnetzwerk.

Anweisungen finden Sie unter ["Google Cloud Dokumentation: Cloud VPN Übersicht"](#).

## Anforderungen an den Steckverbinder

Richten Sie Ihr Netzwerk ein, damit der Connector Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen kann. Der wichtigste Schritt besteht darin, ausgehenden Internetzugriff auf verschiedene Endpunkte zu gewährleisten.



Wenn Ihr Netzwerk für die gesamte Kommunikation mit dem Internet einen Proxyserver verwendet, können Sie den Proxyserver über die Seite Einstellungen angeben. Siehe ["Konfigurieren des Connectors für die Verwendung eines Proxy-Servers"](#).

## Verbindung zu Zielnetzwerken

Für einen Connector ist eine Netzwerkverbindung zu den VPCs und VNets erforderlich, in denen Cloud Volumes ONTAP bereitgestellt werden soll.

Wenn Sie beispielsweise einen Connector in Ihrem Unternehmensnetzwerk installieren, müssen Sie eine VPN-Verbindung zur VPC oder vnet einrichten, in der Sie Cloud Volumes ONTAP starten.



## Outbound-Internetzugang

Für den Connector ist ein abgehender Internetzugang erforderlich, um Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung zu managen. Ein Connector kontaktiert die folgenden Endpunkte beim Management von Ressourcen in GCP:

Endpunkte	Zweck
<a href="https://www.googleapis.com">https://www.googleapis.com</a>	Ermöglicht dem Connector den Kontakt zu Google APIs für die Bereitstellung und das Management von Cloud Volumes ONTAP in GCP.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	API-Anfragen an NetApp Cloud Central.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
<a href="https://repo.cloud.support.netapp.com">https://repo.cloud.support.netapp.com</a>	Wird zum Herunterladen der Abhängigkeiten von Cloud Manager verwendet.
<a href="http://repo.mysql.com/">http://repo.mysql.com/</a>	Zum Herunterladen von MySQL.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a>	Ermöglicht dem Connector, auf Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images zuzugreifen und diese herunterzuladen.
<a href="https://cloudmanagerinfraproduct.azurecr.io">https://cloudmanagerinfraproduct.azurecr.io</a>	Zugriff auf Software-Images von Container-Komponenten für eine Infrastruktur, die Docker ausführt und eine Lösung für die Service-Integration mit Cloud Manager bietet.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Kommunikation mit dem Cloud Manager-Service, der Cloud Central-Konten einschließt
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Kommunikation mit NetApp AutoSupport.
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a> <a href="https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com">https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a>	Kommunikation mit NetApp bei Systemlizenzen und Support-Registrierung
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Ermöglicht Cloud Manager die Generierung von Lizenzen (beispielsweise eine FlexCache Lizenz für Cloud Volumes ONTAP)
<a href="https://packages.cloud.google.com/yum">https://packages.cloud.google.com/yum</a> <a href="https://github.com/NetApp/trident/releases/download/">https://github.com/NetApp/trident/releases/download/</a>	Erforderlich, um Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster zu verbinden. Mit den Endpunkten ist die Installation von NetApp Trident möglich.

Endpunkte	Zweck
<p>Verschiedene Standorte von Drittanbietern, z. B.:</p> <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.org">https://repo.typesafe.org</a></li> </ul> <p>An Standorten von Drittanbietern können Änderungen vorgenommen werden.</p>	<p>Während Upgrades lädt Cloud Manager die neuesten Pakete für Abhängigkeiten von Drittanbietern herunter.</p>

Während Sie fast alle Aufgaben über die SaaS-Benutzeroberfläche ausführen sollten, steht auf dem Connector weiterhin eine lokale Benutzeroberfläche zur Verfügung. Die Maschine, auf der der Webbrowser ausgeführt wird, muss über Verbindungen zu den folgenden Endpunkten verfügen:

Endpunkte	Zweck
<p>Der Connector-Host</p>	<p>Sie müssen die IP-Adresse des Hosts aus einem Webbrowser eingeben, um die Cloud Manager-Konsole zu laden.</p> <p>Je nach Ihrer Verbindung mit Ihrem Cloud-Provider können Sie die private IP oder eine dem Host zugewiesene öffentliche IP verwenden:</p> <ul style="list-style-type: none"> <li>• Eine private IP funktioniert, wenn Sie über ein VPN verfügen und direkten Zugriff auf Ihr virtuelles Netzwerk haben</li> <li>• Eine öffentliche IP funktioniert in jedem Netzwerkszenario</li> </ul> <p>In jedem Fall sollten Sie den Netzwerkzugriff sichern, indem Sie sicherstellen, dass die Sicherheitsgruppenregeln den Zugriff nur von autorisierten IPs oder Subnetzen ermöglichen.</p>
<p><a href="https://auth0.com">https://auth0.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>  <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>  <a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a></p>	<p>Ihr Webbrowser stellt über NetApp Cloud Central eine Verbindung zu diesen Endpunkten her, um eine zentralisierte Benutzerauthentifizierung zu ermöglichen.</p>
<p><a href="https://widget.intercom.io">https://widget.intercom.io</a></p>	<p>Für Ihren Produkt-Chat, der Ihnen das Gespräch mit NetApp Cloud-Experten ermöglicht.</p>

## Firewall-Regeln für Cloud Volumes ONTAP

Cloud Manager erstellt die GCP-Firewall-Regeln und enthält die ein- und ausgehenden Regeln, die für den erfolgreichen Betrieb von Cloud Manager und Cloud Volumes ONTAP gelten. Sie können die Ports zu Testzwecken oder zur Verwendung eigener Sicherheitsgruppen verwenden.

Die Firewall-Regeln für Cloud Volumes ONTAP erfordern sowohl ein- als auch ausgehende Regeln.

## Regeln für eingehende Anrufe

Die Quelle für eingehende Regeln in der vordefinierten Sicherheitsgruppe ist 0.0.0.0/0.

Protokoll	Port	Zweck
Alle ICMP	Alle	Pingen der Instanz
HTTP	80	HTTP-Zugriff auf die System Manager Webkonsole mit der IP-Adresse der Cluster-Management-LIF
HTTPS	443	HTTPS-Zugriff auf die System Manager-Webkonsole unter Verwendung der IP-Adresse der Cluster-Management-LIF
SSH	22	SSH-Zugriff auf die IP-Adresse der Cluster Management LIF oder einer Node Management LIF
TCP	111	Remote-Prozeduraufruf für NFS
TCP	139	NetBIOS-Servicesitzung für CIFS
TCP	161-162	Einfaches Netzwerkverwaltungsprotokoll
TCP	445	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
TCP	635	NFS-Mount
TCP	749	Kerberos
TCP	2049	NFS-Server-Daemon
TCP	3260	iSCSI-Zugriff über die iSCSI-Daten-LIF
TCP	4045	NFS-Sperr-Daemon
TCP	4046	Netzwerkstatusüberwachung für NFS
TCP	10.000	Backup mit NDMP
TCP	11104	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
TCP	11105	SnapMirror Datenübertragung über Cluster-interne LIFs
UDP	111	Remote-Prozeduraufruf für NFS
UDP	161-162	Einfaches Netzwerkverwaltungsprotokoll
UDP	635	NFS-Mount
UDP	2049	NFS-Server-Daemon
UDP	4045	NFS-Sperr-Daemon
UDP	4046	Netzwerkstatusüberwachung für NFS
UDP	4049	NFS rquotad-Protokoll

## Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

## Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle ICMP	Alle	Gesamter abgehender Datenverkehr
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

## Erweiterte Outbound-Regeln

Wenn Sie strenge Regeln für ausgehenden Datenverkehr benötigen, können Sie mit den folgenden Informationen nur die Ports öffnen, die für die ausgehende Kommunikation durch Cloud Volumes ONTAP erforderlich sind.



Die Quelle ist die Schnittstelle (IP-Adresse) auf dem Cloud Volumes ONTAP System.

Service	Protokoll	Port	Quelle	Ziel	Zweck
Active Directory	TCP	88	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Node Management-LIF	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Node Management-LIF	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	TCP	139	Node Management-LIF	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP UND UDP	389	Node Management-LIF	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Node Management-LIF	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	UDP	464	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Node Management-LIF	Active Directory-Gesamtstruktur	Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	TCP	88	Daten-LIF (NFS, CIFS, iSCSI)	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	TCP	139	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP UND UDP	389	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	UDP	464	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Data LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V - Passwort ändern und festlegen (RPCSEC_GSS)

Service	Protokoll	Port	Quelle	Ziel	Zweck
Cluster	Gesamter Datenverkehr	Gesamter Datenverkehr	Alle LIFs auf einem Node	Alle LIFs auf dem anderen Node	Kommunikation zwischen Clustern (nur Cloud Volumes ONTAP HA)
	TCP	3000	Node Management-LIF	Ha Mediator	ZAPI-Aufrufe (nur Cloud Volumes ONTAP HA)
	ICMP	1	Node Management-LIF	Ha Mediator	Bleiben Sie am Leben (nur Cloud Volumes ONTAP HA)
DHCP	UDP	68	Node Management-LIF	DHCP	DHCP-Client für die erstmalige Einrichtung
DHCPS	UDP	67	Node Management-LIF	DHCP	DHCP-Server
DNS	UDP	53	Node Management LIF und Daten LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860-18699	Node Management-LIF	Zielservers	NDMP-Kopie
SMTP	TCP	25	Node Management-LIF	Mailserver	SMTP-Warnungen können für AutoSupport verwendet werden
SNMP	TCP	161	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	UDP	161	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	TCP	162	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	UDP	162	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
SnapMirror	TCP	11104	Intercluster-LIF	ONTAP Intercluster-LIFs	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
	TCP	11105	Intercluster-LIF	ONTAP Intercluster-LIFs	SnapMirror Datenübertragung
Syslog	UDP	514	Node Management-LIF	Syslog-Server	Syslog-Weiterleitungsmeldungen

## Firewall-Regeln für den Connector

Die Firewall-Regeln für den Connector erfordern sowohl ein- als auch ausgehende Regeln.

## Regeln für eingehende Anrufe

Die Quelle für eingehende Regeln in den vordefinierten Firewall-Regeln ist 0.0.0.0/0.

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche

## Regeln für ausgehende Anrufe

Die vordefinierten Firewall-Regeln für den Connector öffnen den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

### Grundlegende Regeln für ausgehende Anrufe

Die vordefinierten Firewall-Regeln für den Connector enthalten die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

### Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.



Die Quell-IP-Adresse ist der Connector-Host.

Service	Protokoll	Port	Ziel	Zweck
Active Directory	TCP	88	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	TCP	139	Active Directory-Gesamtstruktur	Sitzung für den NETBIOS-Dienst
	TCP	389	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
	TCP	464	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (SET_CHANGE)
	TCP	749	Active Directory-Gesamtstruktur	Active Directory Kerberos V - Kennwort ändern und festlegen (RPCSEC_GSS)
	UDP	137	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Active Directory-Gesamtstruktur	Netbios Datagramm-Dienst
	UDP	464	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API ruft GCP und ONTAP ab und sendet AutoSupport Nachrichten an NetApp
API-Aufrufe	TCP	3000	ONTAP Cluster Management LIF	API-Aufrufe für ONTAP
DNS	UDP	53	DNS	Wird für die DNS-Auflösung durch Cloud Manager verwendet

## Nutzung von vom Kunden gemanagten Schlüsseln mit Cloud Volumes ONTAP

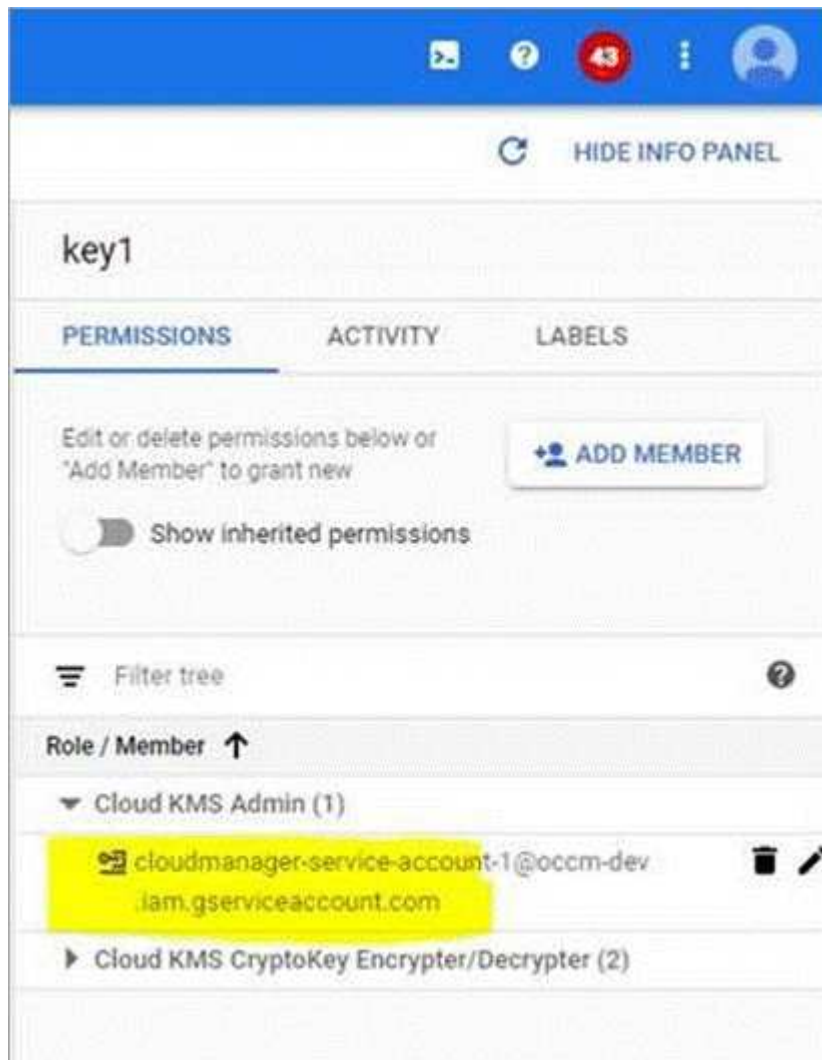
Während Google Cloud Storage immer Ihre Daten verschlüsselt, bevor sie auf die Festplatte geschrieben werden, können Sie Cloud-Manager-APIs verwenden, um ein Cloud Volumes ONTAP-System zu erstellen, das *vom Kunden verwaltete Verschlüsselungsschlüssel* verwendet. Diese Schlüssel werden in GCP mithilfe des



Cloud Key Management Service generiert und gemanagt.

### Schritte

1. Geben Sie dem Connector-Dienstkonto die Berechtigung, den Verschlüsselungsschlüssel zu verwenden.



2. Rufen Sie die „id“ des Schlüssels auf, indem Sie den Befehl get für die API /gcp/vsa/Metadaten/gcp-Encryption-Keys aufrufen.
3. Verwenden Sie bei der Erstellung einer Arbeitsumgebung den Parameter „GcpEncryption“ in Verbindung mit Ihrer API-Anforderung.

### Beispiel

```
"gcpEncryptionParameters": {  
  "key": "projects/tlv-support/locations/us-  
east4/keyRings/Nikiskeys/cryptoKeys/generatedkey1"  
}
```

Siehe "[API-Entwicklerhandbuch](#)" Weitere Informationen zur Verwendung des Parameters „GcpEncryption“.

# Einführung von Cloud Volumes ONTAP in GCP

In der GCP können Sie ein Single-Node-Cloud Volumes ONTAP-System einführen, indem Sie eine Arbeitsumgebung erstellen.

## Was Sie benötigen

- Sie sollten ein haben ["Anschluss, der Ihrem Arbeitsbereich zugeordnet ist"](#).



Sie müssen ein Kontoadministrator sein, um einen Konnektor zu erstellen. Wenn Sie Ihre erste Cloud Volumes ONTAP-Arbeitsumgebung erstellen, fordert Cloud Manager Sie auf, einen Connector zu erstellen, wenn Sie noch keinen haben.


- ["Sie sollten darauf vorbereitet sein, den Konnektor jederzeit in Betrieb zu nehmen"](#).
- Sie sollten eine Konfiguration auswählen und GCP-Netzwerkinformationen von Ihrem Administrator erhalten haben. Weitere Informationen finden Sie unter ["Planung Ihrer Cloud Volumes ONTAP Konfiguration"](#).
- Für die Implementierung eines BYOL-Systems benötigen Sie für jeden Node die 20-stellige Seriennummer (Lizenzschlüssel).
- Die folgenden Google Cloud APIs sollten sein ["In Ihrem Projekt aktiviert"](#):
  - Cloud Deployment Manager V2-API
  - Cloud-ProtokollierungsAPI
  - Cloud Resource Manager API
  - Compute Engine-API
  - IAM-API (Identitäts- und Zugriffsmanagement)

## Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.
2. **Wählen Sie einen Standort:** Wählen Sie **Google Cloud** und **Cloud Volumes ONTAP**.
3. **Details & Anmeldeinformationen:** Wählen Sie ein Projekt aus, geben Sie einen Clusternamen an, fügen Sie optional Labels hinzu und geben Sie dann Anmeldeinformationen an.

In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Name der Arbeitsumgebung	Cloud Manager verwendet den Namen der Arbeitsumgebung, um sowohl das Cloud Volumes ONTAP System als auch die GCP VM-Instanz zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.

Feld	Beschreibung
Etiketten Hinzufügen	Beschriftungen sind Metadaten für Ihre GCP-Ressourcen. Cloud Manager fügt die Bezeichnungen dem Cloud Volumes ONTAP System und den GCP-Ressourcen hinzu, die dem System zugeordnet sind. Sie können bis zu vier Etiketten von der Benutzeroberfläche hinzufügen, wenn Sie eine Arbeitsumgebung erstellen, und dann können Sie weitere hinzufügen, nachdem sie erstellt wurde. Beachten Sie, dass Sie durch die API beim Erstellen einer Arbeitsumgebung nicht auf vier Labels beschränkt werden. Informationen zu Etiketten finden Sie unter " <a href="#">Google Cloud-Dokumentation: Ressourcen Zur Kennzeichnung</a> ".
Benutzername und Passwort	Dies sind die Anmeldedaten für das Cloud Volumes ONTAP Cluster-Administratorkonto. Sie können diese Anmeldedaten für die Verbindung mit Cloud Volumes ONTAP über System Manager oder dessen CLI verwenden.
Projekt Bearbeiten	<p>Wählen Sie das Projekt aus, in dem Cloud Volumes ONTAP gespeichert werden soll. Das Standardprojekt ist das Projekt, in dem Cloud Manager residiert.</p> <p>Wenn in der Dropdown-Liste keine weiteren Projekte angezeigt werden, ist das Cloud Manager-Servicekonto noch nicht mit anderen Projekten verbunden. Rufen Sie die Google Cloud-Konsole auf, öffnen Sie den IAM-Service und wählen Sie das Projekt aus. Fügen Sie dem Projekt das Service-Konto mit der Rolle Cloud Manager hinzu. Sie müssen diesen Schritt für jedes Projekt wiederholen.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin: 10px 0;">  <p>Dies ist das Service-Konto, das Sie für Cloud Manager eingerichtet haben. "<a href="#">Wie in Schritt 2b auf dieser Seite beschrieben</a>".</p> </div> <p>Klicken Sie auf <b>Abonnement hinzufügen</b>, um die ausgewählten Anmeldeinformationen einem Abonnement zuzuordnen.</p> <p>Zum Erstellen eines nutzungsbasierten Cloud Volumes ONTAP Systems müssen Sie über GCP Marketplace ein GCP-Projekt für ein Cloud Volumes ONTAP Abonnement auswählen.</p>

Das folgende Video zeigt, wie Sie ein Pay-as-you-go Marketplace Abonnement für Ihr GCP-Projekt verknüpfen:

► [https://docs.netapp.com/de-de/occm38//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/de-de/occm38//media/video_subscribing_gcp.mp4) (video)

- Standort & Konnektivität:** Wählen Sie einen Speicherort, wählen Sie eine Firewall-Richtlinie und aktivieren Sie das Kontrollkästchen, um die Netzwerkverbindung zu Google Cloud Storage für Daten-Tiering zu bestätigen.

Wenn „kalte“ Daten in einen Google Cloud Storage Bucket verschoben werden sollen, muss das Subnetz, in dem Cloud Volumes ONTAP residiert, für privaten Google Zugriff konfiguriert sein. Anweisungen finden Sie unter "[Google Cloud Documentation: Configuring Private Google Access](#)".

- Lizenz & Support Site Account:** Geben Sie an, ob Sie Pay-as-you-go oder BYOL verwenden möchten, und legen Sie dann ein NetApp Support Site Konto fest.

Informationen zur Funktionsweise von Lizenzen finden Sie unter "[Lizenzierung](#)".

Ein NetApp Support Site Konto ist optional für „Pay-as-you-go“-Systeme erhältlich, wird aber für BYOL-Systeme benötigt. "[Erfahren Sie, wie Sie Konten der NetApp Support Site hinzufügen](#)".

6. **Vorkonfigurierte Pakete:** Wählen Sie eines der Pakete, um schnell ein Cloud Volumes ONTAP System bereitzustellen, oder klicken Sie auf **eigene Konfiguration erstellen**.

Wenn Sie eines der Pakete auswählen, müssen Sie nur ein Volume angeben und dann die Konfiguration prüfen und genehmigen.

7. **Lizenzierung:** Ändern Sie die Cloud Volumes ONTAP-Version nach Bedarf, wählen Sie eine Lizenz und wählen Sie einen virtuellen Maschinentyp.

The screenshot shows the 'Licensing' section of the NetApp Cloud Manager interface. It displays three license options: 'Explore', 'Standard Improved Functionality' (which is selected and highlighted in blue), and 'Premium Advanced Functionality'. Below the license options, there is a 'Machine Type' dropdown menu currently set to 'n1-standard-8'. The interface also shows the current version to be deployed as 'ONTAP-9.7RC1' with a 'Change version' link.

Wenn sich Ihre Anforderungen nach dem Start des Systems ändern, können Sie die Lizenz oder den Typ der virtuellen Maschine später ändern.



Wenn für die ausgewählte Version ein neuer Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert Cloud Manager das System beim Erstellen der Arbeitsumgebung auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.6 RC1 und 9.6 GA auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.6 bis 9.7.

8. **Zugrunde liegende Speicherressourcen:** Wählen Sie die Einstellungen für das anfängliche Aggregat: Einen Datenträgertyp und die Größe für jede Platte.

Der Festplattentyp ist für das anfängliche Volume. Sie können einen anderen Festplattentyp für nachfolgende Volumes auswählen.

Die Festplattengröße gilt für alle Festplatten im ursprünglichen Aggregat und für alle zusätzlichen Aggregate, die Cloud Manager erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuweisungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

Hilfe bei der Auswahl von Festplattentyp und -Größe finden Sie unter "[Dimensionierung Ihres Systems in GCP](#)".

9. **Schreibgeschwindigkeit & WURM:** Wählen Sie **Normal** oder **hohe** Schreibgeschwindigkeit, und

aktivieren Sie auf Wunsch den Schreib-Speicher, den WORM-Speicher.

Auswahl einer Schreibgeschwindigkeit wird nur bei Single-Node-Systemen unterstützt.

["Erfahren Sie mehr über Schreibgeschwindigkeit"](#).

WORM kann nicht aktiviert werden, wenn Daten-Tiering aktiviert wurde.

["Erfahren Sie mehr über WORM Storage"](#).

10. **Daten-Tiering in der Google Cloud Platform:** Wählen Sie, ob Daten-Tiering auf dem ursprünglichen Aggregat aktiviert werden soll, wählen Sie eine Storage-Klasse für die Tiered Daten, und wählen Sie dann entweder ein Service-Konto mit der vordefinierten Storage-Administratorrolle (erforderlich für Cloud Volumes ONTAP 9.7) oder wählen Sie ein GCP-Konto (erforderlich für Cloud Volumes ONTAP 9.6).

Beachten Sie Folgendes:

- Cloud Manager legt das Service-Konto auf der Cloud Volumes ONTAP Instanz fest. Dieses Servicekonto bietet Berechtigungen für Daten-Tiering zu einem Google Cloud Storage Bucket. Stellen Sie sicher, dass Sie das Cloud Manager-Servicekonto als Benutzer des Tiering-Dienstkontos hinzufügen, andernfalls können Sie es nicht aus Cloud Manager auswählen.
- Hilfe zum Hinzufügen eines GCP-Kontos finden Sie unter ["Einrichten und Hinzufügen von GCP-Konten für Daten-Tiering mit 9.6"](#).
- Sie können eine bestimmte Volume-Tiering-Richtlinie auswählen, wenn Sie ein Volume erstellen oder bearbeiten.
- Wenn Sie das Daten-Tiering deaktivieren, können Sie es auf nachfolgenden Aggregaten aktivieren, jedoch müssen Sie das System deaktivieren und ein Service-Konto über die GCP-Konsole hinzufügen.

["Weitere Informationen zum Daten-Tiering"](#).

11. **Create Volume:** Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren, wodurch Sie ein Volume erstellen können, das größer ist als der derzeit verfügbare physische Storage.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt Cloud Manager einen Wert ein, der Zugriff auf alle Instanzen im Subnetz ermöglicht.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch Zugriffssteuerungslisten oder ACLs genannt). Sie können lokale oder domänenbasierte Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Domain-Windows-Benutzernamen angeben, müssen Sie die Domäne des Benutzers mit dem Format Domain\Benutzername einschließen.

Feld	Beschreibung
Snapshot-Richtlinie	Eine Snapshot Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot Kopien an. Bei einer NetApp Snapshot Kopie handelt es sich um ein zeitpunktgenaues Filesystem Image, das keine Performance-Einbußen aufweist und minimalen Storage erfordert. Sie können die Standardrichtlinie oder keine auswählen. Sie können keine für transiente Daten auswählen, z. B. tempdb für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume: Entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt Cloud Manager automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Nachdem Sie das Volume erstellt haben, <a href="#">"Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen"</a> .

Die folgende Abbildung zeigt die für das CIFS-Protokoll ausgefüllte Volume-Seite:

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy:

Default Policy

#### Protocol

NFS   
 CIFS   
 iSCSI

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

12. **CIFS Setup:** Wenn Sie das CIFS-Protokoll wählen, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.

Feld	Beschreibung
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers.
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.
NTP-Server	Wählen Sie <b>Active Directory-Domäne verwenden</b> aus, um einen NTP-Server mit Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Siehe " <a href="#">Cloud Manager API-Entwicklerleitfaden</a> " Entsprechende Details.

13. **Nutzungsprofil, Festplattentyp und Tiering-Richtlinie:** Wählen Sie aus, ob Sie Funktionen für die Storage-Effizienz aktivieren und gegebenenfalls die Volume Tiering-Richtlinie ändern möchten.

Weitere Informationen finden Sie unter "[Allgemeines zu Volume-Nutzungsprofilen](#)" Und "[Data Tiering - Übersicht](#)".

14. **Überprüfen & Genehmigen:** Überprüfen und bestätigen Sie Ihre Auswahl.
- Überprüfen Sie die Details zur Konfiguration.
  - Klicken Sie auf **Weitere Informationen**, um weitere Informationen zum Support und zu den von Cloud Manager erworbenen GCP-Ressourcen zu erhalten.
  - Aktivieren Sie die Kontrollkästchen **Ich verstehe...**
  - Klicken Sie Auf **Go**.

### Ergebnis

Cloud Manager implementiert das Cloud Volumes ONTAP System. Sie können den Fortschritt in der Timeline verfolgen.

Wenn Sie Probleme bei der Implementierung des Cloud Volumes ONTAP Systems haben, lesen Sie die Fehlermeldung. Sie können auch die Arbeitsumgebung auswählen und auf **Umgebung neu erstellen** klicken.

Weitere Hilfe finden Sie unter "[NetApp Cloud Volumes ONTAP Support](#)".

### Nachdem Sie fertig sind

- Wenn Sie eine CIFS-Freigabe bereitgestellt haben, erteilen Sie Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner, und überprüfen Sie, ob diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.
- Wenn Sie Kontingente auf Volumes anwenden möchten, verwenden Sie System Manager oder die CLI.

Mithilfe von Quotas können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder qtree verwendeten Dateien einschränken oder nachverfolgen.



## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

## Markeninformationen

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