Erste Schritte in Google Cloud

Cloud Volumes ONTAP

NetApp
February 17, 2026

Inhalt

Erste Schritte in Google Cloud

Schnellstart für Cloud Volumes ONTAP in Google Cloud

Beginnen Sie in wenigen Schritten mit Cloud Volumes ONTAP in Google Cloud.

1 Erstellen eines Konsolenagenten

Wenn Sie keinen haben "Konsolenagent" Dennoch müssen Sie einen erstellen. "Erfahren Sie, wie Sie einen Konsolenagenten in Google Cloud erstellen"

Beachten Sie: Wenn Sie Cloud Volumes ONTAP in einem Subnetz bereitstellen möchten, in dem kein Internetzugang verfügbar ist, müssen Sie den Konsolenagenten manuell installieren und auf die NetApp Console zugreifen, die auf diesem Konsolenagenten ausgeführt wird. "Erfahren Sie, wie Sie den Konsolenagenten manuell an einem Ort ohne Internetzugang installieren."

2 Planen Sie Ihre Konfiguration

Die Konsole bietet vorkonfigurierte Pakete, die Ihren Workload-Anforderungen entsprechen, oder Sie können Ihre eigene Konfiguration erstellen. Wenn Sie Ihre eigene Konfiguration auswählen, sollten Sie die Ihnen zur Verfügung stehenden Optionen verstehen.

"Erfahren Sie mehr über die Planung Ihrer Konfiguration" .

3 Richten Sie Ihr Netzwerk ein

1. Stellen Sie sicher, dass Ihr VPC und Ihre Subnetze die Konnektivität zwischen dem Konsolenagenten und Cloud Volumes ONTAP unterstützen.
2. Wenn Sie Data Tiering aktivieren möchten, "Konfigurieren Sie das Cloud Volumes ONTAP Subnetz für den privaten Google-Zugriff" .
3. Wenn Sie ein HA-Paar bereitstellen, stellen Sie sicher, dass Sie über vier VPCs verfügen, jede mit ihrem eigenen Subnetz.
4. Wenn Sie eine gemeinsam genutzte VPC verwenden, weisen Sie dem Dienstkonto des Konsolenagenten die Rolle „Compute Network User“ zu.
5. Aktivieren Sie den ausgehenden Internetzugriff vom Ziel-VPC für NetApp AutoSupport.

   Dieser Schritt ist nicht erforderlich, wenn Sie Cloud Volumes ONTAP an einem Standort bereitstellen, an dem kein Internetzugang verfügbar ist.

"Erfahren Sie mehr über die Netzwerkanforderungen" .

4 Einrichten eines Dienstkontos

Cloud Volumes ONTAP erfordert aus zwei Gründen ein Google Cloud-Dienstkonto. Die erste ist, wenn Sie aktivieren"Daten-Tiering" um kalte Daten in kostengünstigen Objektspeicher in Google Cloud zu verschieben. Die zweite Möglichkeit besteht darin, dass Sie die "NetApp Backup and Recovery" um Volumes auf kostengünstigem Objektspeicher zu sichern.

Sie können ein Servicekonto einrichten und es für beide Zwecke verwenden. Das Dienstkonto muss über die Rolle **Storage Admin** verfügen.

"Lesen Sie die Schritt-für-Schritt-Anleitung" .

5 **Google Cloud-APIs aktivieren**

"Aktivieren Sie die folgenden Google Cloud APIs in Ihrem Projekt" . Diese APIs sind für die Bereitstellung des Konsolenagenten und von Cloud Volumes ONTAP erforderlich.

- Cloud Deployment Manager V2 API
- Cloud Logging API
- Cloud Resource Manager-API
- Compute Engine-API
- API für Identitäts- und Zugriffsverwaltung (IAM)

6 **Starten Sie Cloud Volumes ONTAP über die Konsole**

Klicken Sie auf **System hinzufügen**, wählen Sie den Systemtyp aus, den Sie bereitstellen möchten, und führen Sie die Schritte im Assistenten aus. "Lesen Sie die Schritt-für-Schritt-Anleitung" .

Weiterführende Links

- "Erstellen eines Konsolenagenten"
- "Installieren der Konsolenagentensoftware auf einem Linux-Host"
- "Google Cloud-Berechtigungen für den Konsolenagenten"

Planen Sie Ihre Cloud Volumes ONTAP Konfiguration in Google Cloud

Wenn Sie Cloud Volumes ONTAP in Google Cloud bereitstellen, können Sie ein vorkonfiguriertes System auswählen, das Ihren Workload-Anforderungen entspricht, oder Sie können Ihre eigene Konfiguration erstellen. Wenn Sie Ihre eigene Konfiguration auswählen, sollten Sie die Ihnen zur Verfügung stehenden Optionen verstehen.

Wählen Sie eine Cloud Volumes ONTAP -Lizenz

Für Cloud Volumes ONTAP sind mehrere Lizenzierungsoptionen verfügbar. Jede Option ermöglicht Ihnen die Auswahl eines Verbrauchsmodells, das Ihren Anforderungen entspricht.

- "Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP"
- "Erfahren Sie, wie Sie die Lizenzierung einrichten"

Wählen Sie eine unterstützte Region

Cloud Volumes ONTAP wird in den meisten Google Cloud-Regionen unterstützt. "Vollständige Liste der unterstützten Regionen anzeigen" .

Wählen Sie einen unterstützten Maschinentyp

Cloud Volumes ONTAP unterstützt je nach gewähltem Lizenztyp mehrere Maschinentypen.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in Google Cloud"

Speichergrenzen verstehen

Die Rohkapazitätsgrenze für ein Cloud Volumes ONTAP System ist an die Lizenz gebunden. Zusätzliche Beschränkungen wirken sich auf die Größe von Aggregaten und Volumina aus. Sie sollten sich dieser Beschränkungen bewusst sein, wenn Sie Ihre Konfiguration planen.

"Speichergrenzen für Cloud Volumes ONTAP in Google Cloud"

Dimensionieren Sie Ihr System in Google Cloud

Durch die Dimensionierung Ihres Cloud Volumes ONTAP -Systems können Sie die Anforderungen an Leistung und Kapazität erfüllen. Bei der Auswahl eines Maschinentyps, Datenträgertyps und einer Datenträgergröße sollten Sie einige wichtige Punkte beachten:

Maschinentyp

Schauen Sie sich die unterstützten Maschinentypen in der "Versionshinweise zu Cloud Volumes ONTAP" Anschließend können Sie bei Google die Details zu jedem unterstützten Maschinentyp einsehen. Passen Sie Ihre Workload-Anforderungen an die Anzahl der vCPUs und den Arbeitsspeicher für den Maschinentyp an. Beachten Sie, dass jeder CPU-Kern die Netzwerkleistung erhöht.

Weitere Einzelheiten finden Sie im Folgenden:

- "Google Cloud-Dokumentation: N1-Standardmaschinentypen"
- "Google Cloud-Dokumentation: Leistung"

Datenträgertypen

Wenn Sie Volumes für Cloud Volumes ONTAP erstellen, müssen Sie den zugrunde liegenden Cloud-Speicher auswählen, den Cloud Volumes ONTAP für eine Festplatte verwendet. Der Datenträgertyp kann einer der folgenden sein:

- *Zonale persistente SSD-Festplatten*: Persistente SSD-Festplatten eignen sich am besten für Workloads, die hohe zufällige IOPS-Raten erfordern.
- *Zonal Balanced Persistent Disks*: Diese SSDs gleichen Leistung und Kosten aus, indem sie niedrigere IOPS pro GB bereitstellen.
- *Zonale persistente Standarddatenträger*: Persistente Standarddatenträger sind wirtschaftlich und können sequenzielle Lese-/Schreibvorgänge verarbeiten.

  Weitere Einzelheiten finden Sie im "Google Cloud-Dokumentation: Zonale persistente Datenträger (Standard und SSD)" .

Festplattengröße

Sie müssen eine anfängliche Festplattengröße auswählen, wenn Sie ein Cloud Volumes ONTAP -System bereitstellen. Anschließend können Sie die Kapazität eines Systems von der NetApp Console verwalten lassen. Wenn Sie jedoch selbst Aggregate erstellen möchten, beachten Sie Folgendes:

- Alle Festplatten in einem Aggregat müssen die gleiche Größe haben.

- Bestimmen Sie den Platzbedarf unter Berücksichtigung der Leistung.
- Die Leistung persistenter Datenträger skaliert automatisch mit der Datenträgergröße und der Anzahl der dem System zur Verfügung stehenden vCPUs.

  Weitere Einzelheiten finden Sie im Folgenden:

  - "Google Cloud-Dokumentation: Zonale persistente Datenträger (Standard und SSD)"
  - "Google Cloud-Dokumentation: Optimieren der Leistung von persistenten Festplatten und lokalen SSDs"

Standardsystemfestplatten anzeigen

Zusätzlich zum Speicher für Benutzerdaten erwirbt die Konsole auch Cloud-Speicher für Cloud Volumes ONTAP -Systemdaten (Boot-Daten, Root-Daten, Core-Daten und NVRAM). Zu Planungszwecken kann es hilfreich sein, diese Details zu überprüfen, bevor Sie Cloud Volumes ONTAP bereitstellen.

- "Standardfestplatten für Cloud Volumes ONTAP -Systemdaten in Google Cloud anzeigen" .
- "Google Cloud-Dokumentation: Übersicht über Cloud-Kontingente"

  Google Cloud Compute Engine erzwingt Kontingente für die Ressourcennutzung. Stellen Sie daher sicher, dass Sie Ihr Limit nicht erreicht haben, bevor Sie Cloud Volumes ONTAP bereitstellen.

Der Konsolenagent benötigt außerdem eine Systemfestplatte. "Details zur Standardkonfiguration des Konsolenagenten anzeigen" .

Sammeln von Netzwerkinformationen

Wenn Sie Cloud Volumes ONTAP in Google Cloud bereitstellen, müssen Sie Details zu Ihrem virtuellen Netzwerk angeben. Sie können ein Arbeitsblatt verwenden, um die Informationen von Ihrem Administrator zu erfassen.

Netzwerkinformationen für ein Einzelknotensystem

Google Cloud-Informationen	Ihr Wert
Region	
Zone	
VPC-Netzwerk	
Subnetz	
Firewall-Richtlinie (falls Sie Ihre eigene verwenden)	

Netzwerkinformationen für ein HA-Paar in mehreren Zonen

Google Cloud-Informationen	Ihr Wert
Region	
Zone für Knoten 1	

Google Cloud-Informationen	Ihr Wert
Zone für Knoten 2	
Zone für den Mediator	
VPC-0 und Subnetz	
VPC-1 und Subnetz	
VPC-2 und Subnetz	
VPC-3 und Subnetz	
Firewall-Richtlinie (falls Sie Ihre eigene verwenden)	

Netzwerkinformationen für ein HA-Paar in einer einzelnen Zone

Google Cloud-Informationen	Ihr Wert
Region	
Zone	
VPC-0 und Subnetz	
VPC-1 und Subnetz	
VPC-2 und Subnetz	
VPC-3 und Subnetz	
Firewall-Richtlinie (falls Sie Ihre eigene verwenden)	

Wählen Sie eine Schreibgeschwindigkeit

Mit der Konsole können Sie eine Schreibgeschwindigkeitseinstellung für Cloud Volumes ONTAP auswählen, mit Ausnahme von Hochverfügbarkeitspaaren (HA) in Google Cloud. Bevor Sie eine Schreibgeschwindigkeit auswählen, sollten Sie die Unterschiede zwischen den normalen und hohen Einstellungen sowie die Risiken und Empfehlungen bei der Verwendung einer hohen Schreibgeschwindigkeit verstehen. "Erfahren Sie mehr über die Schreibgeschwindigkeit" .

Auswählen eines Volume-Nutzungsprofils

ONTAP umfasst mehrere Speichereffizienzfunktionen, die die von Ihnen benötigte Gesamtspeichermenge reduzieren können. Wenn Sie in der Konsole ein Volume 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.

Die Storage-Effizienzfunktionen von NetApp bieten folgende Vorteile:

Dünne Bereitstellung

Bietet Hosts oder Benutzern mehr logischen Speicher, als Sie tatsächlich in Ihrem physischen Speicherpool haben. Anstatt Speicherplatz vorab zuzuweisen, wird Speicherplatz jedem Volume dynamisch zugewiesen, während Daten geschrieben werden.

Deduplizierung

Verbessert die Effizienz, indem identische Datenblöcke lokalisiert und durch Verweise auf einen einzigen gemeinsamen Block ersetzt werden. Diese Technik reduziert den Speicherkapazitätsbedarf, indem redundante Datenblöcke, die sich auf demselben Datenträger befinden, eliminiert werden.

Komprimierung

Reduziert die zum Speichern von Daten erforderliche physische Kapazität durch Komprimieren von Daten innerhalb eines Volumes auf Primär-, Sekundär- und Archivspeicher.

Einrichten des Google Cloud-Netzwerks für Cloud Volumes ONTAP

Die NetApp Console übernimmt die Einrichtung von Netzwerkkomponenten für Cloud Volumes ONTAP, wie z. B. IP-Adressen, Netzmasken und Routen. Sie müssen sicherstellen, dass ausgehender Internetzugang verfügbar ist, dass genügend private IP-Adressen verfügbar sind, dass die richtigen Verbindungen vorhanden sind und mehr.

Wenn Sie ein HA-Paar einsetzen möchten, sollten Sie"Erfahren Sie, wie HA-Paare in Google Cloud funktionieren." .

Anforderungen für Cloud Volumes ONTAP

Die folgenden Anforderungen müssen in Google Cloud erfüllt sein.

Anforderungen, die speziell für Einzelknotensysteme gelten

Wenn Sie ein Einzelknotensystem bereitstellen möchten, stellen Sie sicher, dass Ihr Netzwerk die folgenden Anforderungen erfüllt.

Eine VPC

Für ein Einzelknotensystem ist eine Virtual Private Cloud (VPC) erforderlich.

Private IP-Adressen

Für ein Einzelknotensystem in Google Cloud weist die Console den folgenden Komponenten private IP-Adressen zu:

- Node
- Cluster
- Speicher-VM
- Daten-NAS-LIF
- Daten-iSCSI-LIF

Sie können die Erstellung des Storage VM (SVM)-Verwaltungs-LIF überspringen, wenn Sie Cloud Volumes ONTAP mithilfe der API bereitstellen und das folgende Flag angeben:

```
skipSvmManagementLif: true
```

Ein LIF ist eine IP-Adresse, die einem physischen Port zugeordnet ist. Für Verwaltungstools wie SnapCenter ist ein Storage VM (SVM)-Verwaltungs-LIF erforderlich.

Spezifische Anforderungen für HA-Paare

Wenn Sie ein HA-Paar bereitstellen möchten, stellen Sie sicher, dass Ihr Netzwerk die folgenden Anforderungen erfüllt.

Eine oder mehrere Zonen

Sie können die hohe Verfügbarkeit Ihrer Daten sicherstellen, indem Sie eine HA-Konfiguration über mehrere oder in einer einzigen Zone bereitstellen. Die Konsole fordert Sie beim Erstellen des HA-Paares auf, mehrere Zonen oder eine einzelne Zone auszuwählen.

- Mehrere Zonen (empfohlen)

  Durch die Bereitstellung einer HA-Konfiguration über drei Zonen hinweg wird eine kontinuierliche Datenverfügbarkeit gewährleistet, wenn innerhalb einer Zone ein Fehler auftritt. Beachten Sie, dass die Schreibleistung im Vergleich zur Verwendung einer einzelnen Zone etwas geringer ist, aber minimal.

- Einzelzone

  Bei der Bereitstellung in einer einzelnen Zone verwendet eine Cloud Volumes ONTAP HA-Konfiguration eine Richtlinie für verteilte Platzierung. Diese Richtlinie stellt sicher, dass eine HA-Konfiguration vor einem einzelnen Fehlerpunkt innerhalb der Zone geschützt ist, ohne dass separate Zonen zur Fehlerisolierung verwendet werden müssen.

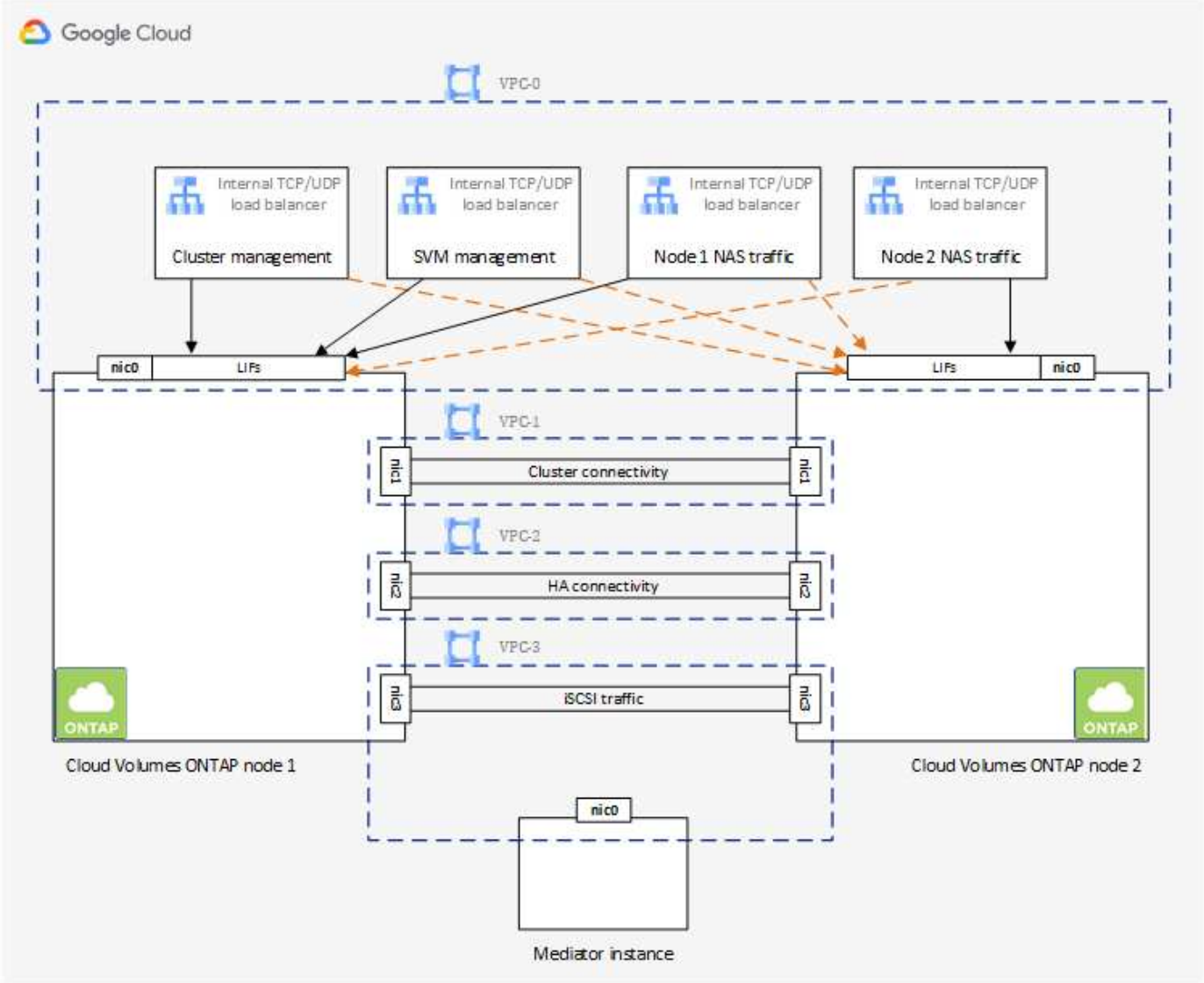
  Dieses Bereitstellungsmodell senkt Ihre Kosten, da zwischen den Zonen keine Gebühren für den Datenausgang anfallen.

Vier virtuelle private Clouds

Für eine HA-Konfiguration werden vier Virtual Private Clouds (VPCs) benötigt. Es sind vier VPCs erforderlich, da Google Cloud erfordert, dass sich jede Netzwerkschnittstelle in einem separaten VPC-Netzwerk befindet.

Die Konsole fordert Sie beim Erstellen des HA-Paares auf, vier VPCs auszuwählen:

- VPC-0 für eingehende Verbindungen zu den Daten und Knoten
- VPC-1, VPC-2 und VPC-3 für die interne Kommunikation zwischen den Knoten und dem HA-Mediator



Subnetze

Für jede VPC ist ein privates Subnetz erforderlich.

Wenn Sie den Konsolenagenten in VPC-0 platzieren, müssen Sie den privaten Google-Zugriff im Subnetz aktivieren, um auf die APIs zuzugreifen und die Datenschichtung zu aktivieren.

Die Subnetze in diesen VPCs müssen unterschiedliche CIDR-Bereiche haben. Sie dürfen keine überlappenden CIDR-Bereiche haben.

Private IP-Adressen

Die Konsole weist Cloud Volumes ONTAP in Google Cloud automatisch die erforderliche Anzahl privater IP-Adressen zu. Sie müssen sicherstellen, dass in Ihrem Netzwerk genügend private Adressen verfügbar sind.

Die Anzahl der für Cloud Volumes ONTAP zugewiesenen LIFs hängt davon ab, ob Sie ein Einzelknotensystem oder ein HA-Paar bereitstellen. Ein LIF ist eine IP-Adresse, die einem physischen Port zugeordnet ist. Ein SVM-Management-LIF ist für Management-Tools wie SnapCenter erforderlich.

- **Einzelknoten** Die NetApp Console weist einem Einzelknotensystem 4 IP-Adressen zu:

- Knotenverwaltung LIF
- Clustermanagement LIF
- iSCSI-Daten-LIF

  Ein iSCSI-LIF bietet Clientzugriff über das iSCSI-Protokoll und wird vom System für andere wichtige Netzwerk-Workflows verwendet. Diese LIFs sind erforderlich und sollten nicht gelöscht werden.

- NAS LIF

  Sie können die Erstellung des Storage VM (SVM)-Verwaltungs-LIF überspringen, wenn Sie Cloud Volumes ONTAP mithilfe der API bereitstellen und das folgende Flag angeben:

```
skipSvmManagementLif: true
```

- **HA-Paar** Die Konsole weist einem HA-Paar 12-13 IP-Adressen zu:
  - 2 Knotenverwaltungs-LIFs (e0a)
  - 1 Clustermanagement LIF (e0a)
  - 2 iSCSI-LIFs (e0a)

    Ein iSCSI-LIF bietet Clientzugriff über das iSCSI-Protokoll und wird vom System für andere wichtige Netzwerk-Workflows verwendet. Diese LIFs sind erforderlich und sollten nicht gelöscht werden.

  - 1 oder 2 NAS-LIFs (e0a)
  - 2 Cluster-LIFs (e0b)
  - 2 HA Interconnect-IP-Adressen (e0c)
  - 2 RSM iSCSI-IP-Adressen (e0d)

    Sie können die Erstellung des Storage VM (SVM)-Verwaltungs-LIF überspringen, wenn Sie Cloud Volumes ONTAP mithilfe der API bereitstellen und das folgende Flag angeben:

```
skipSvmManagementLif: true
```

Interne Lastenausgleichsmodule

Die Konsole erstellt vier interne Google Cloud-Load Balancer (TCP/UDP), die den eingehenden Datenverkehr zum Cloud Volumes ONTAP HA-Paar verwalten. Von Ihrer Seite ist keine Einrichtung erforderlich. Wir haben dies als Anforderung aufgeführt, um Sie lediglich über den Netzwerkverkehr zu informieren und etwaige Sicherheitsbedenken auszuräumen.

Ein Load Balancer dient der Clusterverwaltung, einer der Verwaltung von Storage-VMs (SVM), einer dem NAS-Verkehr zu Knoten 1 und der letzte dem NAS-Verkehr zu Knoten 2.

Die Einrichtung für jeden Load Balancer ist wie folgt:

- Eine gemeinsam genutzte private IP-Adresse
- Ein globaler Gesundheitscheck

Standardmäßig sind die vom Integritätscheck verwendeten Ports 63001, 63002 und 63003.

- Ein regionaler TCP-Backend-Dienst
- Ein regionaler UDP-Backend-Dienst
- Eine TCP-Weiterleitungsregel
- Eine UDP-Weiterleitungsregel
- Der globale Zugriff ist deaktiviert

  Obwohl der globale Zugriff standardmäßig deaktiviert ist, wird die Aktivierung nach der Bereitstellung unterstützt. Wir haben es deaktiviert, da der regionsübergreifende Datenverkehr deutlich höhere Latenzen aufweist. Wir wollten sicherstellen, dass Sie aufgrund versehentlicher regionsübergreifender Mounts keine negativen Erfahrungen machen. Die Aktivierung dieser Option richtet sich nach Ihren Geschäftsanforderungen.

Gemeinsam genutzte VPCs

Cloud Volumes ONTAP und der Konsolenagent werden in einem gemeinsam genutzten Google Cloud VPC und auch in eigenständigen VPCs unterstützt.

Für ein Single-Node-System kann die VPC entweder eine Shared VPC oder eine Standalone VPC sein.

Für ein HA-Paar werden vier VPCs benötigt. Jede dieser VPCs kann entweder gemeinsam genutzt oder eigenständig sein. Beispielsweise könnte VPC-0 eine gemeinsam genutzte VPC sein, während VPC-1, VPC-2 und VPC-3 eigenständige VPCs sein könnten.

Mit einer gemeinsam genutzten VPC können Sie virtuelle Netzwerke über mehrere Projekte hinweg konfigurieren und zentral verwalten. Sie können gemeinsam genutzte VPC-Netzwerke im *Hostprojekt* einrichten und den Konsolenagenten und die virtuellen Maschineninstanzen von Cloud Volumes ONTAP in einem *Serviceprojekt* bereitstellen.

"Google Cloud-Dokumentation: Übersicht über Shared VPC" .

"Überprüfen Sie die erforderlichen freigegebenen VPC-Berechtigungen, die in der Bereitstellung des Konsolenagenten behandelt werden."

Paketspiegelung in VPCs

"Paketspiegelung"muss im Google Cloud-Subnetz deaktiviert werden, in dem Sie Cloud Volumes ONTAP bereitstellen.

Ausgehender Internetzugang

Cloud Volumes ONTAP -Systeme erfordern ausgehenden Internetzugang für den Zugriff auf externe Endpunkte für verschiedene Funktionen. Cloud Volumes ONTAP kann nicht ordnungsgemäß funktionieren, wenn diese Endpunkte in Umgebungen mit strengen Sicherheitsanforderungen blockiert sind.

Der Konsolenagent kontaktiert außerdem mehrere Endpunkte für den täglichen Betrieb. Informationen zu den Endpunkten finden Sie unter "Vom Konsolenagenten kontaktierte Endpunkte anzeigen" Und "Vorbereiten des Netzwerks für die Verwendung der Konsole" .

Cloud Volumes ONTAP Endpunkte

Cloud Volumes ONTAP verwendet diese Endpunkte zur Kommunikation mit verschiedenen Diensten.

Endpunkte	Gilt für	Zweck	Bereitstellungsmodus	Auswirkungen, wenn der Endpunkt nicht verfügbar ist
https://netapp-cloud-account.auth0.com	Authentifizierung	Wird zur Authentifizierung in der Konsole verwendet.	Standard- und eingeschränkte Modi.	Die Benutzerauthentifizierung schlägt fehl und die folgenden Dienste sind weiterhin nicht verfügbar: • Cloud Volumes ONTAP Dienste • ONTAP -Dienste • Protokolle und Proxy-Dienste
https://api.bluexp.netapp.com/tenancy	Mietverhältnis	Wird verwendet, um Cloud Volumes ONTAP -Ressourcen von der Konsole abzurufen, um Ressourcen und Benutzer zu autorisieren.	Standard- und eingeschränkte Modi.	Cloud Volumes ONTAP Ressourcen und die Benutzer sind nicht autorisiert.
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Wird verwendet, um AutoSupport Telemetriedaten an den NetApp Support zu senden.	Standard- und eingeschränkte Modi.	AutoSupport -Informationen bleiben unversehrt.

Endpunkte	Gilt für	Zweck	Bereitstellungsmodus	Auswirkungen, wenn der Endpunkt nicht verfügbar ist
https://cloudbuild.googleapis.com/v1 (nur für private Bereitstellungen) https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud (kommerzielle Nutzung).	Kommunikation mit Google Cloud-Diensten.	Standard-, eingeschränkter und privater Modus.	Cloud Volumes ONTAP kann nicht mit dem Google Cloud-Dienst kommunizieren, um bestimmte Vorgänge für die Konsole in Google Cloud auszuführen.

Verbindungen zu ONTAP -Systemen in anderen Netzwerken

Um Daten zwischen einem Cloud Volumes ONTAP -System in Google Cloud und ONTAP -Systemen in anderen Netzwerken zu replizieren, benötigen Sie eine VPN-Verbindung zwischen der VPC und dem anderen Netzwerk, beispielsweise Ihrem Unternehmensnetzwerk.

"Google Cloud-Dokumentation: Cloud VPN-Übersicht" .

Firewall-Regeln

Die Konsole erstellt Google Cloud-Firewallregeln, die die eingehenden und ausgehenden Regeln enthalten, die Cloud Volumes ONTAP für einen erfolgreichen Betrieb benötigt. Möglicherweise möchten Sie zu Testzwecken auf die Ports verweisen oder wenn Sie lieber Ihre eigenen Firewall-Regeln verwenden möchten.

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

Wenn Sie eine HA-Konfiguration bereitstellen, sind dies die Firewall-Regeln für Cloud Volumes ONTAP in VPC-0.

Beachten Sie, dass für eine HA-Konfiguration zwei Sätze von Firewall-Regeln erforderlich sind:

- Ein Regelsatz für HA-Komponenten in VPC-0. Diese Regeln ermöglichen den Datenzugriff auf Cloud Volumes ONTAP.
- Ein weiterer Regelsatz für HA-Komponenten in VPC-1, VPC-2 und VPC-3. Diese Regeln sind für die eingehende und ausgehende Kommunikation zwischen den HA-Komponenten offen. Mehr erfahren .

Suchen Sie nach Informationen zum Konsolenagenten? "Firewallregeln für den Konsolenagenten anzeigen"

Eingehende Regeln

Wenn Sie ein Cloud Volumes ONTAP -System hinzufügen, können Sie während der Bereitstellung den Quellfilter für die vordefinierte Firewall-Richtlinie auswählen:

- **Nur ausgewählte VPC**: Der Quellfilter für eingehenden Datenverkehr ist der Subnetzbereich der VPC für das Cloud Volumes ONTAP -System und der Subnetzbereich der VPC, in der sich der Konsolenagent befindet. Dies ist die empfohlene Option.
- **Alle VPCs**: Der Quellfilter für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.

Wenn Sie Ihre eigene Firewall-Richtlinie verwenden, stellen Sie sicher, dass Sie alle Netzwerke hinzufügen, die mit Cloud Volumes ONTAP kommunizieren müssen. Achten Sie jedoch auch darauf, beide Adressbereiche hinzuzufügen, damit der interne Google Load Balancer ordnungsgemäß funktioniert. Diese Adressen sind 130.211.0.0/22 und 35.191.0.0/16. Weitere Informationen finden Sie im "Google Cloud-Dokumentation: Load Balancer-Firewallregeln" .

Protokoll	Hafen	Zweck
Alle ICMP	Alle	Pingen der Instanz
HTTP	80	HTTP-Zugriff auf die ONTAP System Manager-Webkonsole über die IP-Adresse des Cluster-Management-LIF
HTTPS	443	Konnektivität mit dem Konsolenagenten und HTTPS-Zugriff auf die ONTAP System Manager-Webkonsole unter Verwendung der IP-Adresse des Cluster-Management-LIF
SSH	22	SSH-Zugriff auf die IP-Adresse des Cluster-Management-LIF oder eines Node-Management-LIF
TCP	111	Remote Procedure Call für NFS
TCP	139	NetBIOS-Dienstsitzung 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 das iSCSI-Daten-LIF

Protokoll	Hafen	Zweck
TCP	4045	NFS-Sperrdaemon
TCP	4046	Netzwerkstatusmonitor für NFS
TCP	10000	Sicherung mit NDMP
TCP	11104	Verwaltung von Intercluster-Kommunikationssitzungen für SnapMirror
TCP	11105	SnapMirror Datenübertragung mithilfe von Intercluster-LIFs
TCP	63001-63050	Lastenausgleichs-Testports, um festzustellen, welcher Knoten fehlerfrei ist (nur für HA-Paare erforderlich)
UDP	111	Remote Procedure Call für NFS
UDP	161-162	Einfaches Netzwerkverwaltungsprotokoll
UDP	635	NFS-Mount
UDP	2049	NFS-Server-Daemon
UDP	4045	NFS-Sperrdaemon
UDP	4046	Netzwerkstatusmonitor für NFS
UDP	4049	NFS-Rquotad-Protokoll

Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP öffnet den gesamten ausgehenden Datenverkehr. Wenn das akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Nachrichten. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Ausgangsregeln.

Grundlegende Ausgangsregeln

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

Protokoll	Hafen	Zweck
Alle ICMP	Alle	Der gesamte ausgehende Verkehr
Alle TCP	Alle	Der gesamte ausgehende Verkehr
Alle UDP	Alle	Der gesamte ausgehende Verkehr

Erweiterte Ausgangsregeln

Wenn Sie strenge Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation von Cloud Volumes ONTAP erforderlich sind. Die Cloud Volumes ONTAP -Cluster verwenden die folgenden Ports zur Regulierung des Knotenverkehrs.

Die Quelle ist die Schnittstelle (IP-Adresse) des Cloud Volumes ONTAP Systems.

Service	Protokoll	Hafen	Quelle	Ziel	Zweck
Active Directory	TCP	88	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	NetBIOS-Datagrammdienst
	TCP	139	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	NetBIOS-Dienstsitzung
	TCP und UDP	389	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
	TCP	464	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern & festlegen (SET_CHANGE)
	UDP	464	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Knotenverwaltung LIF	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern und festlegen (RPCSEC_GSS)
	TCP	88	Daten-LIF (NFS, CIFS, iSCSI)	Active Directory-Gesamtstruktur	Kerberos V-Authentifizierung
	UDP	137	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Namensdienst
	UDP	138	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Datagrammdienst
	TCP	139	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	NetBIOS-Dienstsitzung
	TCP und UDP	389	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	LDAP
	TCP	445	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Microsoft SMB/CIFS über TCP mit NetBIOS-Framing
	TCP	464	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern & festlegen (SET_CHANGE)
	UDP	464	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos-Schlüsselverwaltung
	TCP	749	Daten-LIF (NFS, CIFS)	Active Directory-Gesamtstruktur	Kerberos V Passwort ändern & festlegen (RPCSEC_GSS)

Service	Protokoll	Hafen	Quelle	Ziel	Zweck
AutoSupport	HTTPS	443	Knotenverwaltung LIF	mysupport.netapp.com	AutoSupport (HTTPS ist die Standardeinstellung)
	HTTP	80	Knotenverwaltung LIF	mysupport.netapp.com	AutoSupport (nur wenn das Transportprotokoll von HTTPS auf HTTP geändert wird)
	TCP	3128	Knotenverwaltung LIF	Konsolenagent	Senden von AutoSupport -Nachrichten über einen Proxyserver auf dem Konsolenagenten, wenn keine ausgehende Internetverbindung verfügbar ist
Konfigurationssicherungen	HTTP	80	Knotenverwaltung LIF	http://<IP-Adresse des Konsolenagenten>/occm/offboxconfig	Senden Sie Konfigurationssicherungen an den Konsolenagenten."ONTAP-Dokumentation"
DHCP	UDP	68	Knotenverwaltung LIF	DHCP	DHCP-Client für die Ersteinrichtung
DHCPS	UDP	67	Knotenverwaltung LIF	DHCP	DHCP-Server
DNS	UDP	53	Knotenverwaltungs-LIF und Daten-LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	Knotenverwaltung LIF	Zielserver	NDMP-Kopie
SMTP	TCP	25	Knotenverwaltung LIF	Mailserver	SMTP-Benachrichtigungen, können für AutoSupport verwendet werden
SNMP	TCP	161	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
	UDP	161	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
	TCP	162	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
	UDP	162	Knotenverwaltung LIF	Monitorserver	Überwachung durch SNMP-Traps
SnapMirror	TCP	11104	Intercluster LIF	ONTAP Intercluster-LIFs	Verwaltung von Intercluster-Kommunikationssitzungen für SnapMirror
	TCP	11105	Intercluster LIF	ONTAP Intercluster-LIFs	SnapMirror -Datenübertragung
Syslog	UDP	514	Knotenverwaltung LIF	Syslog-Server	Syslog-Weiterleitungsnachrichten

Regeln für VPC-1, VPC-2 und VPC-3

In Google Cloud wird eine HA-Konfiguration über vier VPCs bereitgestellt. Die für die HA-Konfiguration in VPC-0 erforderlichen Firewall-Regeln sindoben für Cloud Volumes ONTAP aufgeführt .

In der Zwischenzeit ermöglichen die vordefinierten Firewall-Regeln, die für die Instanzen in VPC-1, VPC-2 und VPC-3 erstellt wurden, die eingehende Kommunikation über *alle* Protokolle und Ports. Diese Regeln ermöglichen die Kommunikation zwischen HA-Knoten.

Die Kommunikation von den HA-Knoten zum HA-Mediator erfolgt über Port 3260 (iSCSI).

> Um eine hohe Schreibgeschwindigkeit für neue Google Cloud HA-Paarbereitstellungen zu ermöglichen, ist für VPC-1, VPC-2 und VPC-3 eine maximale Übertragungseinheit (MTU) von mindestens 8.896 Bytes erforderlich. Wenn Sie vorhandene VPC-1, VPC-2 und VPC-3 auf eine MTU von 8.896 Bytes aktualisieren möchten, müssen Sie während des Konfigurationsvorgangs alle vorhandenen HA-Systeme herunterfahren, die diese VPCs verwenden.

Anforderungen für den Konsolenagenten

Wenn Sie noch keinen Konsolenagenten erstellt haben, sollten Sie die Netzwerkanforderungen überprüfen.

- "Netzwerkanforderungen für den Konsolenagenten anzeigen"
- "Firewall-Regeln in Google Cloud"

Netzwerkkonfigurationen zur Unterstützung des Konsolenagent-Proxys

Sie können die für den Konsolenagenten konfigurierten Proxyserver verwenden, um ausgehenden Internetzugriff von Cloud Volumes ONTAP zu ermöglichen. Die Konsole unterstützt zwei Arten von Proxys:

- **Expliziter Proxy**: Der ausgehende Datenverkehr von Cloud Volumes ONTAP verwendet die HTTP-Adresse des Proxyservers, der während der Proxy-Konfiguration des Konsolenagenten angegeben wurde. Der Konsolenagent-Administrator hat möglicherweise auch Benutzeranmeldeinformationen und Stamm-CA-Zertifikate für eine zusätzliche Authentifizierung konfiguriert. Wenn ein Stamm-CA-Zertifikat für den expliziten Proxy verfügbar ist, stellen Sie sicher , dass Sie dasselbe Zertifikat erhalten und mithilfe des "ONTAP CLI: Sicherheitszertifikat installieren" Befehl.
- **Transparenter Proxy**: Das Netzwerk ist so konfiguriert, dass ausgehender Datenverkehr von Cloud Volumes ONTAP automatisch über den Proxy des Konsolenagenten geleitet wird. Beim Einrichten eines transparenten Proxys muss der Konsolen-Agent-Administrator nur ein Stamm-CA-Zertifikat für die Konnektivität von Cloud Volumes ONTAP bereitstellen, nicht die HTTP-Adresse des Proxy-Servers. Stellen Sie sicher, dass Sie dasselbe Stamm-CA-Zertifikat erhalten und auf Ihr Cloud Volumes ONTAP System hochladen, indem Sie das "ONTAP CLI: Sicherheitszertifikat installieren" Befehl.

Informationen zum Konfigurieren von Proxy-Servern für den Konsolen-Agenten finden Sie im "Konfigurieren eines Konsolenagenten zur Verwendung eines Proxyservers" .

Konfigurieren Sie Netzwerk-Tags für Cloud Volumes ONTAP in Google Cloud

Während der transparenten Proxy-Konfiguration des Konsolen-Agenten fügt der Administrator ein Netzwerk-Tag für Google Cloud hinzu. Sie müssen dasselbe Netzwerk-Tag für Ihre Cloud Volumes ONTAP Konfiguration abrufen und manuell hinzufügen. Dieses Tag ist für die ordnungsgemäße Funktion des Proxyservers erforderlich.

1. Suchen Sie in der Google Cloud Console Ihr Cloud Volumes ONTAP System.
2. Gehen Sie zu **Details > Netzwerk > Netzwerk-Tags**.

3. Fügen Sie das für den Konsolenagenten verwendete Tag hinzu und speichern Sie die Konfiguration.

Verwandte Themen

- "Überprüfen Sie das AutoSupport -Setup für Cloud Volumes ONTAP"
- "Erfahren Sie mehr über die internen Ports von ONTAP" .

Richten Sie VPC Service Controls ein, um Cloud Volumes ONTAP in Google Cloud bereitzustellen

Wenn Sie Ihre Google Cloud-Umgebung mit VPC Service Controls sperren möchten, sollten Sie verstehen, wie NetApp Console und Cloud Volumes ONTAP mit den Google Cloud-APIs interagieren und wie Sie Ihren Service-Perimeter für die Bereitstellung von Console und Cloud Volumes ONTAP konfigurieren.

Mit VPC Service Controls können Sie den Zugriff auf von Google verwaltete Dienste außerhalb eines vertrauenswürdigen Perimeters steuern, den Datenzugriff von nicht vertrauenswürdigen Standorten blockieren und die Risiken einer nicht autorisierten Datenübertragung mindern. "Erfahren Sie mehr über Google Cloud VPC Service Controls" .

So kommunizieren NetApp -Dienste mit VPC Service Controls

Die Konsole kommuniziert direkt mit den Google Cloud-APIs. Dies wird entweder von einer externen IP-Adresse außerhalb von Google Cloud (z. B. von api.services.cloud.netapp.com) oder innerhalb von Google Cloud von einer internen Adresse ausgelöst, die dem Konsolenagenten zugewiesen ist.

Abhängig vom Bereitstellungsstil des Konsolenagenten müssen möglicherweise bestimmte Ausnahmen für Ihren Service-Perimeter gemacht werden.

Bilder

Sowohl Cloud Volumes ONTAP als auch die Console verwenden Images aus einem Projekt innerhalb von Google Cloud, das von NetApp verwaltet wird. Dies kann die Bereitstellung des Console-Agenten und von Cloud Volumes ONTAP beeinträchtigen, wenn Ihre Organisation eine Richtlinie hat, die die Verwendung von Images blockiert, die nicht innerhalb der Organisation gehostet werden.

Sie können einen Konsolenagenten manuell mithilfe der manuellen Installationsmethode bereitstellen, Cloud Volumes ONTAP muss jedoch auch Bilder aus dem NetApp -Projekt abrufen. Sie müssen eine Zulassungsliste angeben, um einen Konsolenagenten und Cloud Volumes ONTAP bereitzustellen.

Bereitstellen eines Konsolenagenten

Der Benutzer, der einen Konsolenagenten bereitstellt, muss auf ein Image verweisen können, das in der Projekt-ID *netapp-cloudmanager* und der Projektnummer *14190056516* gehostet wird.

Bereitstellen von Cloud Volumes ONTAP

- Das Konsolendienstkonto muss auf ein Image verweisen, das in der Projekt-ID *netapp-cloudmanager* und der Projektnummer *14190056516* aus dem Dienstprojekt gehostet wird.
- Das Dienstkonto für den standardmäßigen Google APIs-Dienstagenten muss auf ein in der Projekt-ID *netapp-cloudmanager* gehostetes Bild und die Projektnummer *14190056516* aus dem Dienstprojekt verweisen.

Beispiele für die Regeln, die zum Abrufen dieser Bilder mit VPC Service Controls erforderlich sind, sind unten definiert.

VPC Service Controls-Perimeterrichtlinien

Richtlinien ermöglichen Ausnahmen von den VPC-Dienststeuerungsregeln. Weitere Informationen zu Richtlinien finden Sie unter "Google Cloud VPC Service Controls Policy Dokumentation".

Um die von der Konsole benötigten Richtlinien festzulegen, navigieren Sie zu Ihrem VPC Service Controls Perimeter innerhalb Ihrer Organisation und fügen Sie die folgenden Richtlinien hinzu. Die Felder sollten mit den Optionen auf der Richtlinienseite „VPC Service Controls“ übereinstimmen. Beachten Sie auch, dass **alle** Regeln erforderlich sind und die **ODER**-Parameter im Regelsatz verwendet werden sollten.

Ingress-Regeln

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

ODER

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

ODER

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

Ausgangsregeln

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

Die oben angegebene Projektnummer ist das Projekt *netapp-cloudmanager*, das von NetApp zum Speichern von Images für den Konsolenagenten und für Cloud Volumes ONTAP verwendet wird.

Erstellen Sie ein Google Cloud-Dienstkonto für Cloud Volumes ONTAP

Cloud Volumes ONTAP erfordert aus zwei Gründen ein Google Cloud-Dienstkonto. Die erste ist, wenn Sie aktivieren"Daten-Tiering" um kalte Daten in kostengünstigen Objektspeicher in Google Cloud zu verschieben. Die zweite Möglichkeit besteht darin, dass Sie die "NetApp Backup and Recovery" um Volumes auf kostengünstigem Objektspeicher zu sichern.

Cloud Volumes ONTAP verwendet das Servicekonto, um auf einen Bucket für mehrstufige Daten und einen anderen Bucket für Backups zuzugreifen und diese zu verwalten.

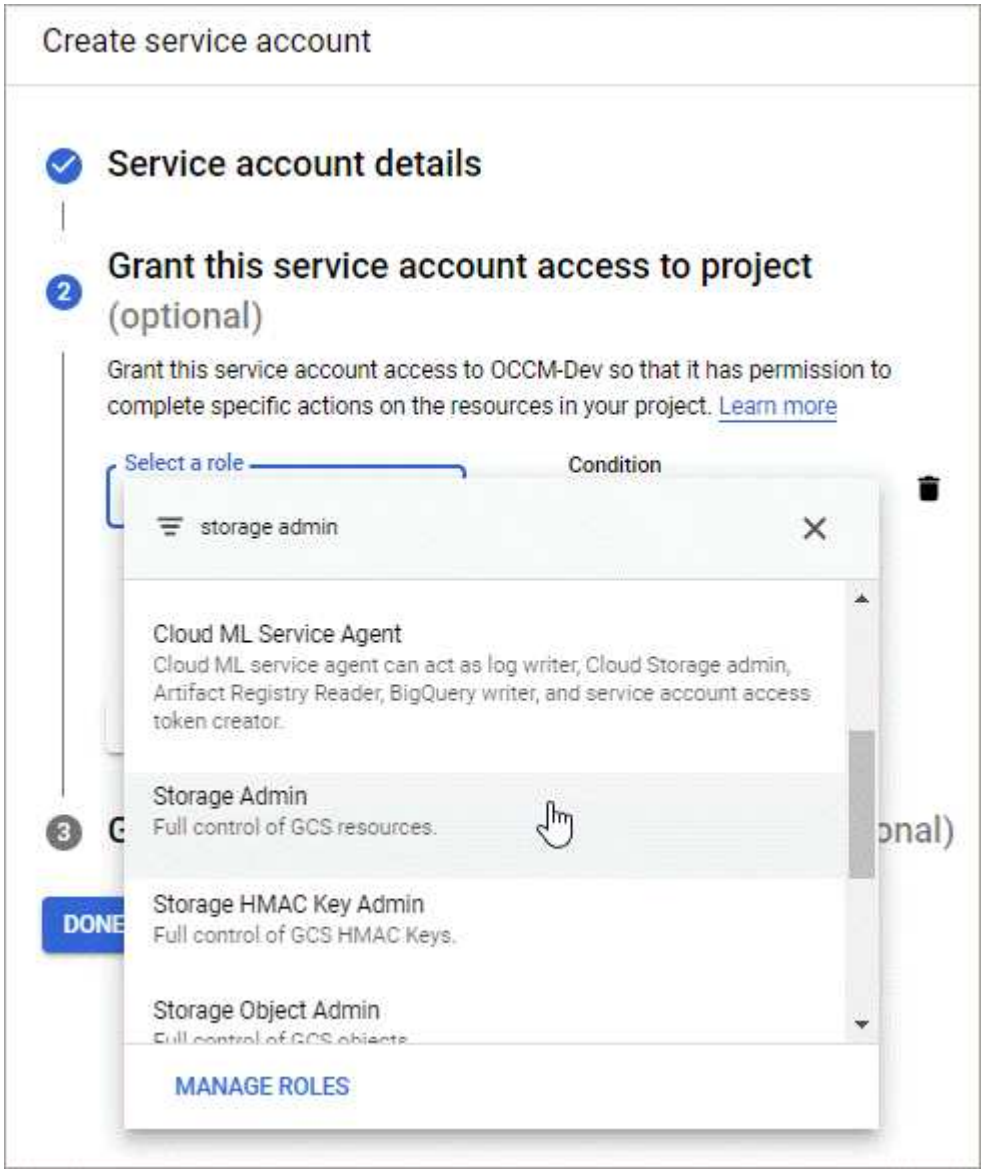
Sie können ein Servicekonto einrichten und es für beide Zwecke verwenden. Das Dienstkonto muss über die Rolle **Storage Admin** verfügen.

Schritte

1. In der Google Cloud Console "Gehen Sie zur Seite „Dienstkonten“".
2. Wählen Sie Ihr Projekt aus.
3. Klicken Sie auf **Dienstkonto erstellen** und geben Sie die erforderlichen Informationen ein.

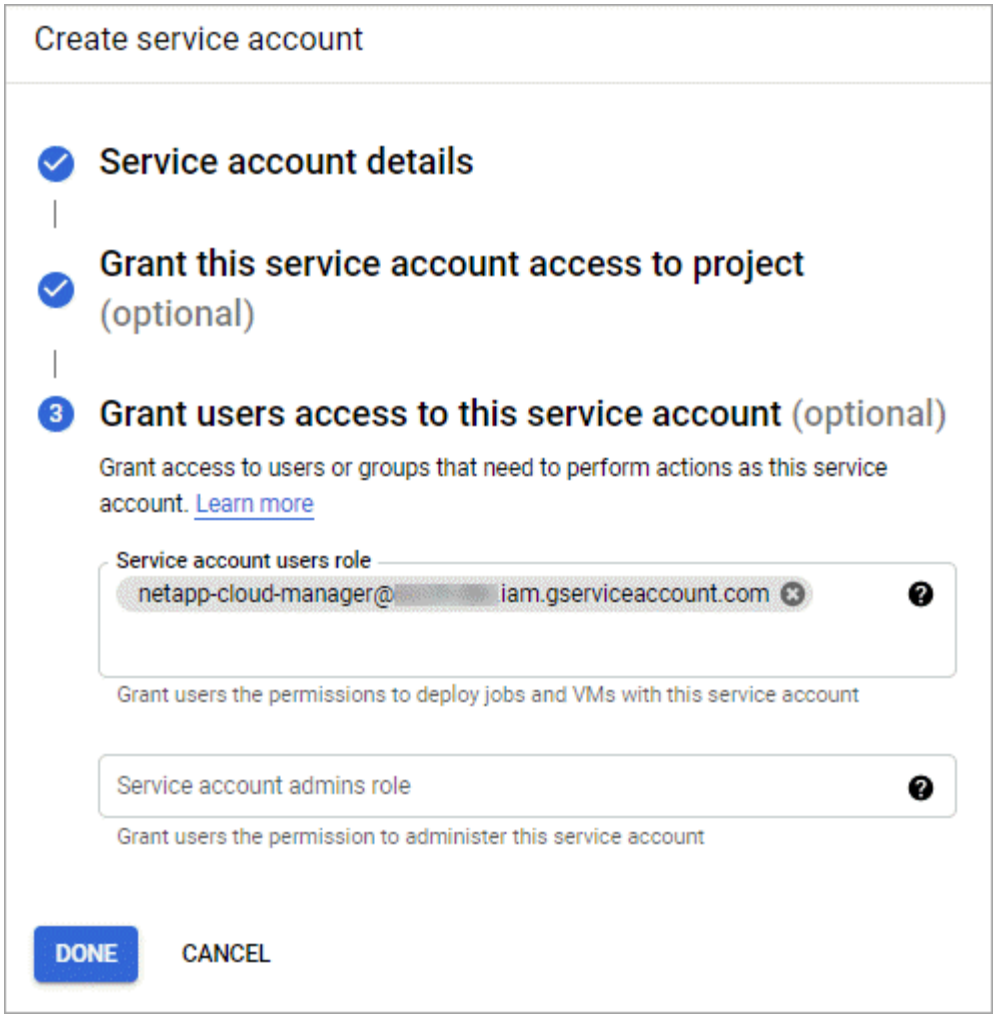
    a. **Servicekontodetails**: Geben Sie einen Namen und eine Beschreibung ein.

    b. **Diesem Dienstkonto Zugriff auf das Projekt gewähren**: Wählen Sie die Rolle **Speicheradministrator** aus.



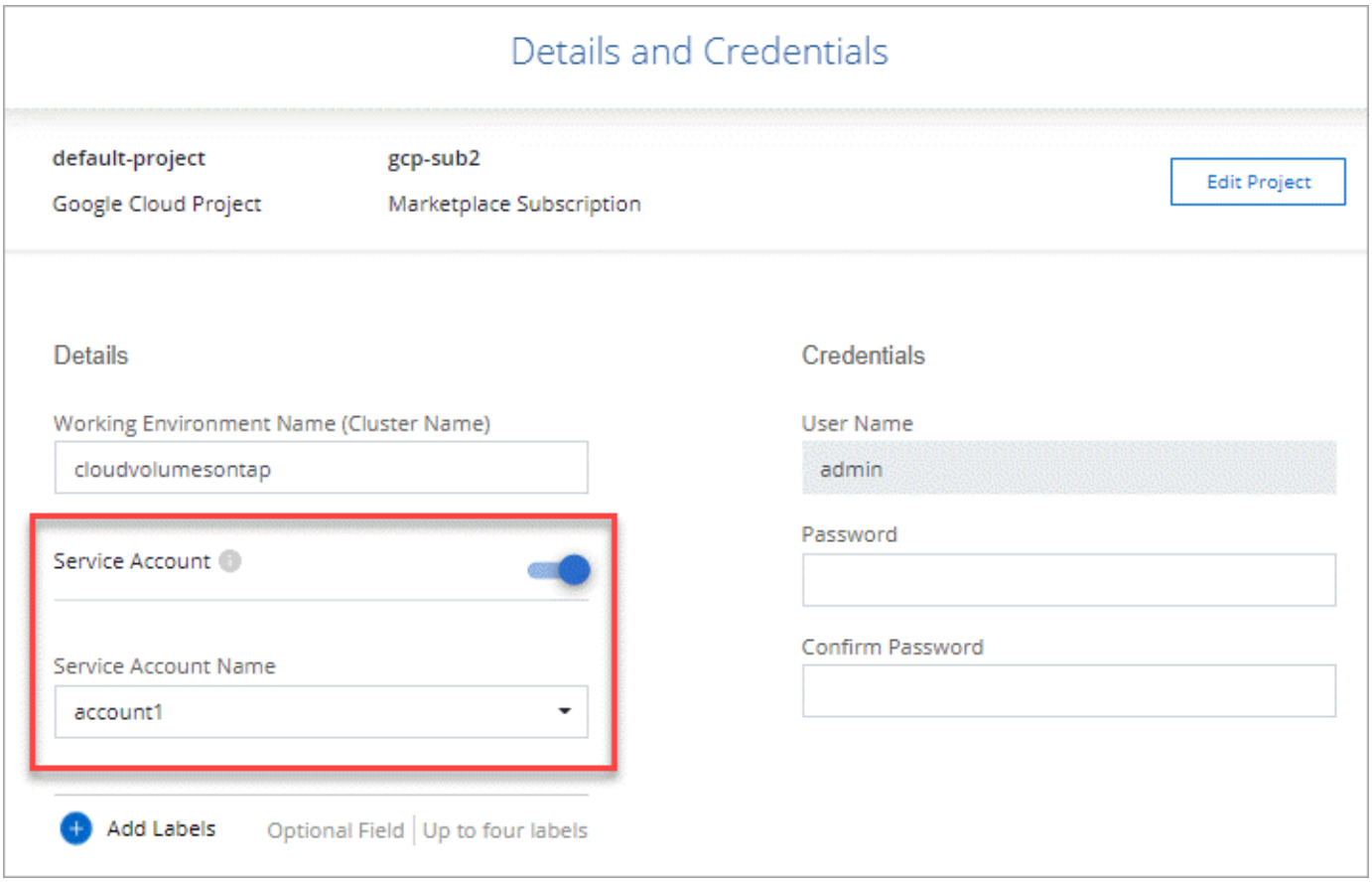
    c. **Benutzern Zugriff auf dieses Dienstkonto gewähren**: Fügen Sie das Dienstkonto des Konsolen-Agenten als *Dienstkontobenutzer* zu diesem neuen Dienstkonto hinzu.

    Dieser Schritt ist nur für die Datenschichtung erforderlich. Für die Sicherung und Wiederherstellung ist es nicht erforderlich.



Wie geht es weiter?

Sie müssen das Dienstkonto später auswählen, wenn Sie ein Cloud Volumes ONTAP -System erstellen.



Verwenden von kundenverwalteten Verschlüsselungsschlüsseln mit Cloud Volumes ONTAP

Während Google Cloud Storage Ihre Daten immer verschlüsselt, bevor sie auf die Festplatte geschrieben werden, können Sie mithilfe der APIs ein Cloud Volumes ONTAP -System erstellen, das *vom Kunden verwaltete Verschlüsselungsschlüssel* verwendet. Dies sind Schlüssel, die Sie mithilfe des Cloud Key Management Service in GCP generieren und verwalten.

Schritte

1. Stellen Sie sicher, dass das Dienstkonto des Konsolen-Agenten über die richtigen Berechtigungen auf Projektebene verfügt, und zwar in dem Projekt, in dem der Schlüssel gespeichert ist.

   Die Berechtigungen werden in der "die Dienstkontoberechtigungen standardmäßig" Dies gilt jedoch möglicherweise nicht, wenn Sie ein alternatives Projekt für den Cloud Key Management Service verwenden.

   Die Berechtigungen lauten wie folgt:

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. Stellen Sie sicher, dass das Dienstkonto für die "Google Compute Engine-Dienstagent" verfügt über Cloud KMS-Verschlüsselungs-/Entschlüsselungsberechtigungen für den Schlüssel.

   Der Name des Dienstkontos verwendet das folgende Format: „service-[service_project_number]@compute-system.iam.gserviceaccount.com“.

   "Google Cloud-Dokumentation: Verwenden von IAM mit Cloud KMS – Zuweisen von Rollen für eine Ressource"

3. Rufen Sie die ID des Schlüssels ab, indem Sie den Befehl „get“ für den `/gcp/vsa/metadata/gcp-encryption-keys` API-Aufruf oder durch Auswahl von „Ressourcennamen kopieren“ auf dem Schlüssel in der GCP-Konsole.
4. Wenn Sie vom Kunden verwaltete Verschlüsselungsschlüssel verwenden und Daten in den Objektspeicher verschieben, versucht die NetApp Console, dieselben Schlüssel zu verwenden, die zum Verschlüsseln der persistenten Datenträger verwendet werden. Sie müssen jedoch zunächst Google Cloud Storage-Buckets aktivieren, um die Schlüssel verwenden zu können:

   a. Suchen Sie den Google Cloud Storage-Dienstagenten, indem Sie den "Google Cloud-Dokumentation: Abrufen des Cloud Storage-Dienstagenten" .
   b. Navigieren Sie zum Verschlüsselungsschlüssel und weisen Sie dem Google Cloud Storage-Dienstagenten die Berechtigungen zum Verschlüsseln/Entschlüsseln von Cloud KMS zu.

   Weitere Informationen finden Sie unter "Google Cloud-Dokumentation: Verwenden von vom Kunden verwalteten Verschlüsselungsschlüsseln"

5. Verwenden Sie den Parameter „gcpEncryption“ bei Ihrer API-Anfrage, wenn Sie ein System erstellen.

   Beispiel

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-1/cryptoKeys/generatedkey1"
  }
```

Weitere Informationen finden Sie im "Dokumentation zur NetApp Console" Weitere Informationen zur Verwendung des Parameters „GcpEncryption“.

Einrichten der Lizenzierung für Cloud Volumes ONTAP in Google Cloud

Nachdem Sie entschieden haben, welche Lizenzierungsoption Sie mit Cloud Volumes ONTAP verwenden möchten, sind einige Schritte erforderlich, bevor Sie diese Lizenzierungsoption beim Erstellen eines neuen Systems auswählen können.

Freemium

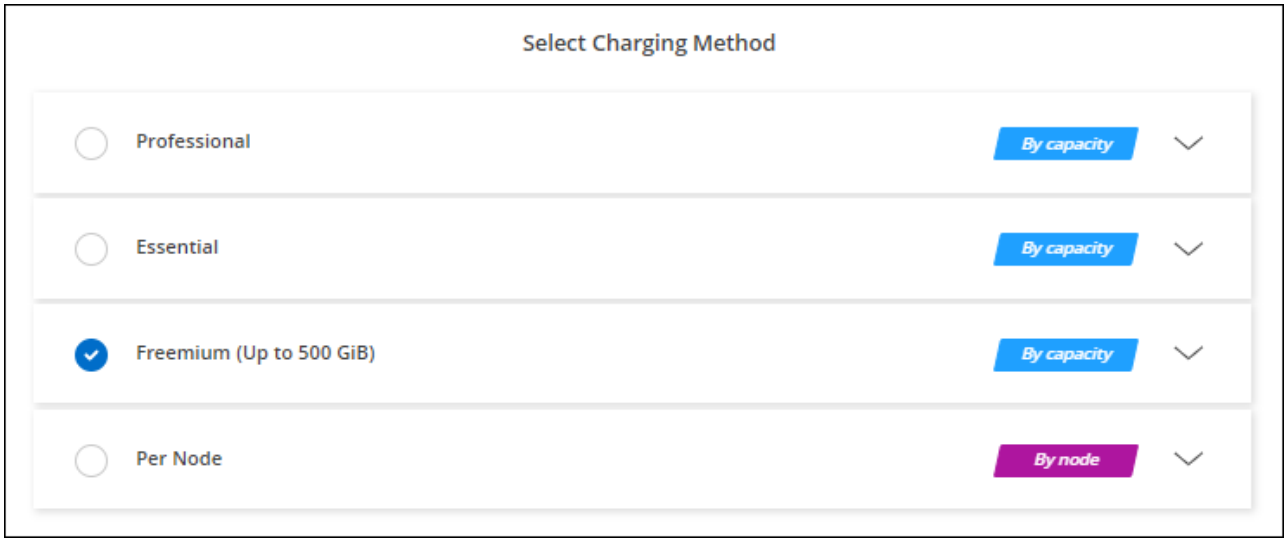
Wählen Sie das Freemium-Angebot, um Cloud Volumes ONTAP mit bis zu 500 GiB bereitgestellter Kapazität kostenlos zu nutzen. "Erfahren Sie mehr über das Freemium-Angebot" .

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten in der NetApp Console.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um das Pay-as-you-go-Angebot im Google Cloud Marketplace zu abonnieren.

      Ihnen werden keine Kosten über das Marktplatz-Abonnement berechnet, es sei denn, Sie überschreiten 500 GiB bereitgestellte Kapazität. Zu diesem Zeitpunkt wird das System automatisch auf das"Essentials-Paket" .

   b. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie **Freemium** aus, wenn Sie die Seite mit den Abrechnungsmethoden erreichen.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Google Cloud an" .

Kapazitätsbasierte Lizenz

Mit der kapazitätsbasierten Lizenzierung können Sie für Cloud Volumes ONTAP pro TiB Kapazität bezahlen. Die kapazitätsbasierte Lizenzierung ist in Form eines *Pakets* verfügbar: dem Essentials- oder Professional-Paket.

Die Pakete Essentials und Professional sind mit folgenden Verbrauchsmodellen bzw. Kaufoptionen erhältlich:

- Eine von NetApp erworbene Lizenz (Bring Your Own License (BYOL))
- Ein stündliches Pay-as-you-go-Abonnement (PAYGO) vom Google Cloud Marketplace
- Ein Jahresvertrag

"Erfahren Sie mehr über kapazitätsbasierte Lizenzierung" .

In den folgenden Abschnitten wird beschrieben, wie Sie mit jedem dieser Verbrauchsmodelle beginnen.

BYOL

Zahlen Sie im Voraus, indem Sie eine Lizenz (BYOL) von NetApp erwerben, um Cloud Volumes ONTAP -Systeme bei jedem Cloud-Anbieter bereitzustellen.

NetApp hat den Erwerb, die Verlängerung und die Erneuerung von BYOL-Lizenzen eingeschränkt. Weitere Informationen finden Sie unter "Eingeschränkte Verfügbarkeit der BYOL-Lizenzierung für Cloud Volumes ONTAP" .

Schritte

1. "Kontaktieren Sie den NetApp -Vertrieb, um eine Lizenz zu erhalten"
2. "Fügen Sie Ihr NetApp Support Site-Konto zur NetApp Console hinzu"

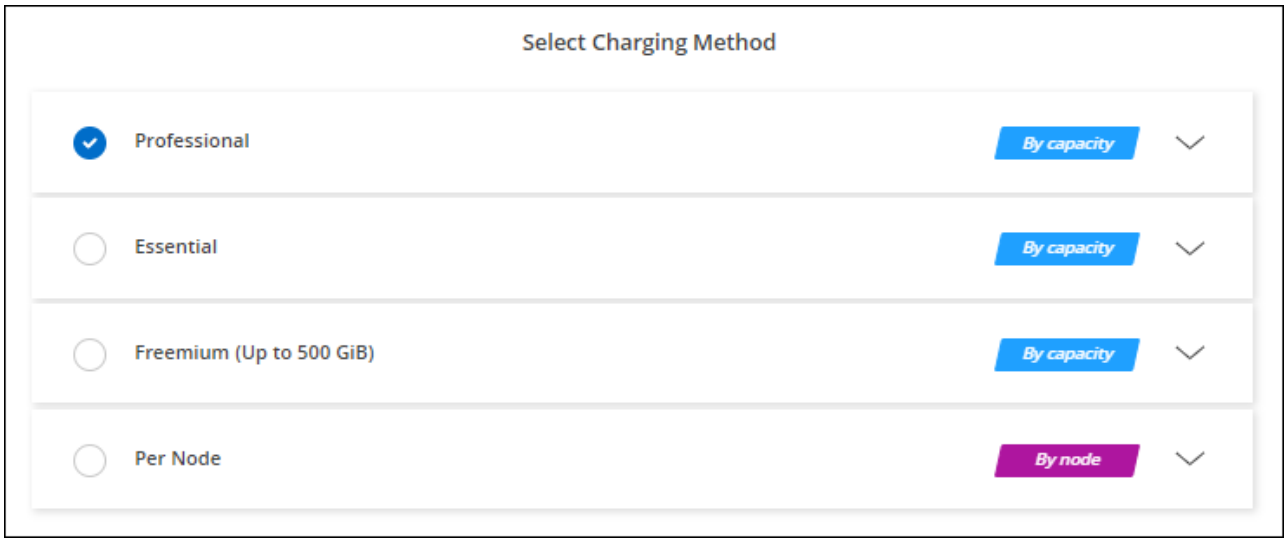
   Die Konsole fragt automatisch den Lizenzierungsdienst von NetApp ab, um Details zu den Lizenzen abzurufen, die mit Ihrem NetApp Support Site-Konto verknüpft sind. Wenn keine Fehler auftreten, fügt die Konsole die Lizenzen hinzu.

   Ihre Lizenz muss in der Konsole verfügbar sein, bevor Sie sie mit Cloud Volumes ONTAP verwenden können. Bei Bedarf können Sie"Fügen Sie die Lizenz manuell zur Konsole hinzu" .

3. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um das Pay-as-you-go-Angebot im Google Cloud Marketplace zu abonnieren.

      Die von Ihnen bei NetApp erworbene Lizenz wird immer zuerst in Rechnung gestellt. Wenn Sie jedoch Ihre lizenzierte Kapazität überschreiten oder die Laufzeit Ihrer Lizenz abläuft, wird Ihnen der Stundensatz auf dem Marktplatz in Rechnung gestellt.

   b. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie auf der Seite mit den Abrechnungsmethoden ein kapazitätsbasiertes Paket aus.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Google Cloud an" .

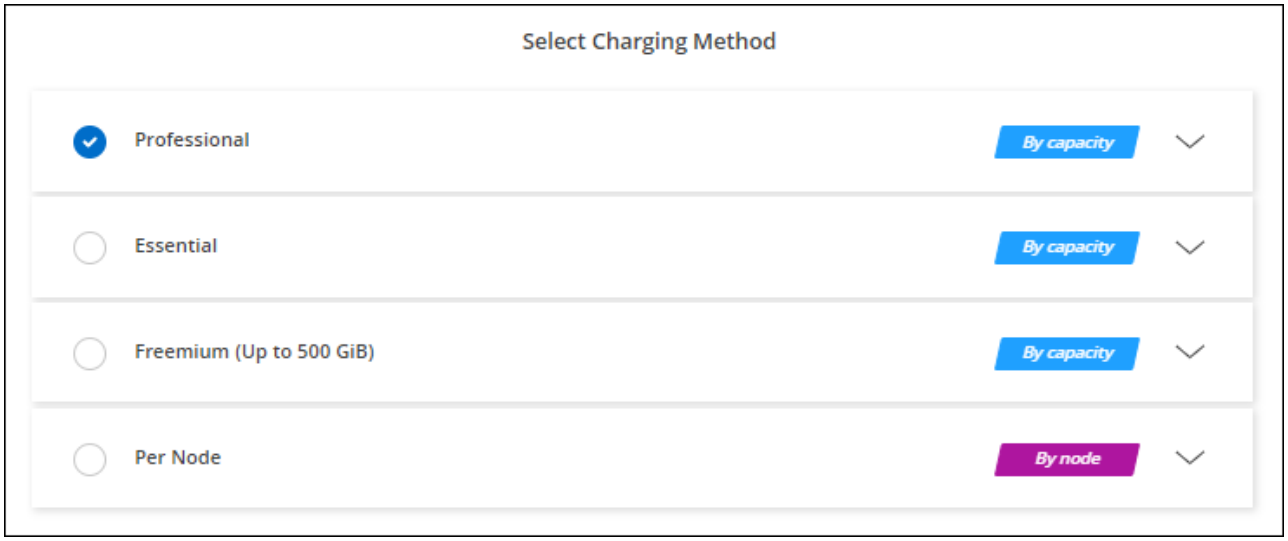
PAYGO-Abonnement

Zahlen Sie stundenweise, indem Sie das Angebot auf dem Marktplatz Ihres Cloud-Anbieters abonnieren.

Wenn Sie ein Cloud Volumes ONTAP -System erstellen, werden Sie von der Konsole aufgefordert, die im Google Cloud Marketplace verfügbare Vereinbarung zu abonnieren. Dieses Abonnement wird dann zum Aufladen mit dem System verknüpft. Sie können dasselbe Abonnement für zusätzliche Systeme verwenden.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um das Pay-as-you-go-Angebot im Google Cloud Marketplace zu abonnieren.
   b. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie auf der Seite mit den Abrechnungsmethoden ein kapazitätsbasiertes Paket aus.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Google Cloud an" .

Sie können die mit Ihren Konten verknüpften Google Cloud Marketplace-Abonnements auf der Seite „Einstellungen > Anmeldeinformationen“ verwalten. "Erfahren Sie, wie Sie Ihre Google Cloud-Anmeldeinformationen und -Abonnements verwalten"

Jahresvertrag

Bezahlen Sie Cloud Volumes ONTAP jährlich, indem Sie einen Jahresvertrag abschließen.

Schritte

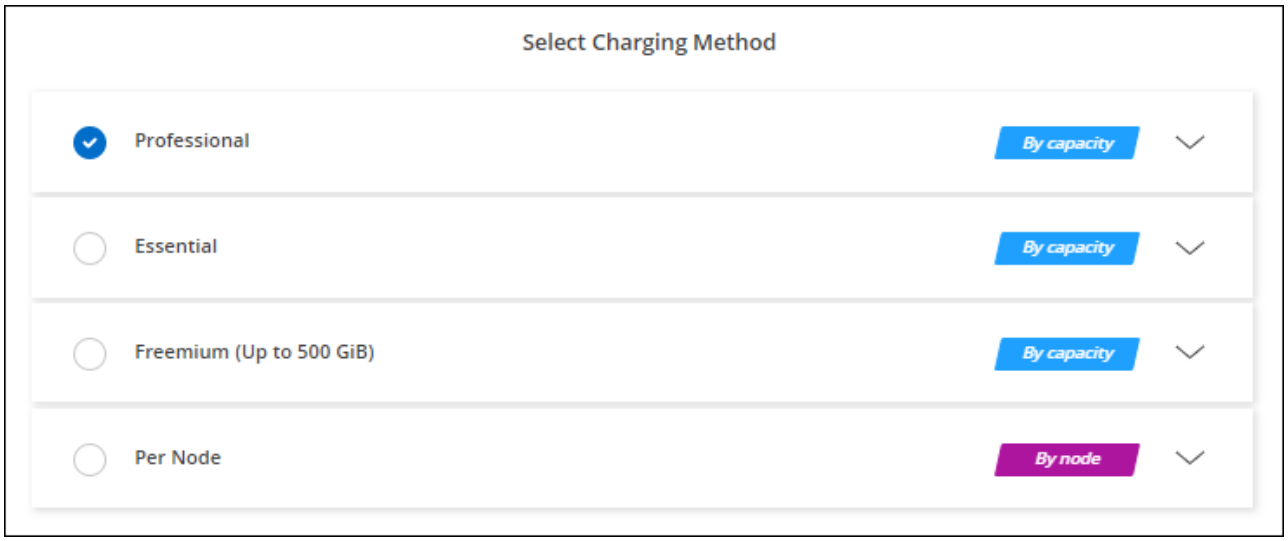
1. Wenden Sie sich an Ihren NetApp Vertriebsmitarbeiter, um einen Jahresvertrag abzuschließen.

   Der Vertrag ist als *privates* Angebot im Google Cloud Marketplace verfügbar.

   Nachdem NetApp Ihnen das private Angebot mitgeteilt hat, können Sie bei der Anmeldung im Google Cloud Marketplace während der Systemerstellung den Jahresplan auswählen.

2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.
   a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldeinformationen bearbeiten > Abonnement hinzufügen** und folgen Sie dann den Anweisungen, um den Jahresplan im Google Cloud Marketplace zu abonnieren.
   b. Wählen Sie in Google Cloud den Jahresplan aus, der mit Ihrem Konto geteilt wurde, und klicken Sie dann auf **Abonnieren**.

c. Nachdem Sie zur Konsole zurückgekehrt sind, wählen Sie auf der Seite mit den Abrechnungsmethoden ein kapazitätsbasiertes Paket aus.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Google Cloud an" .

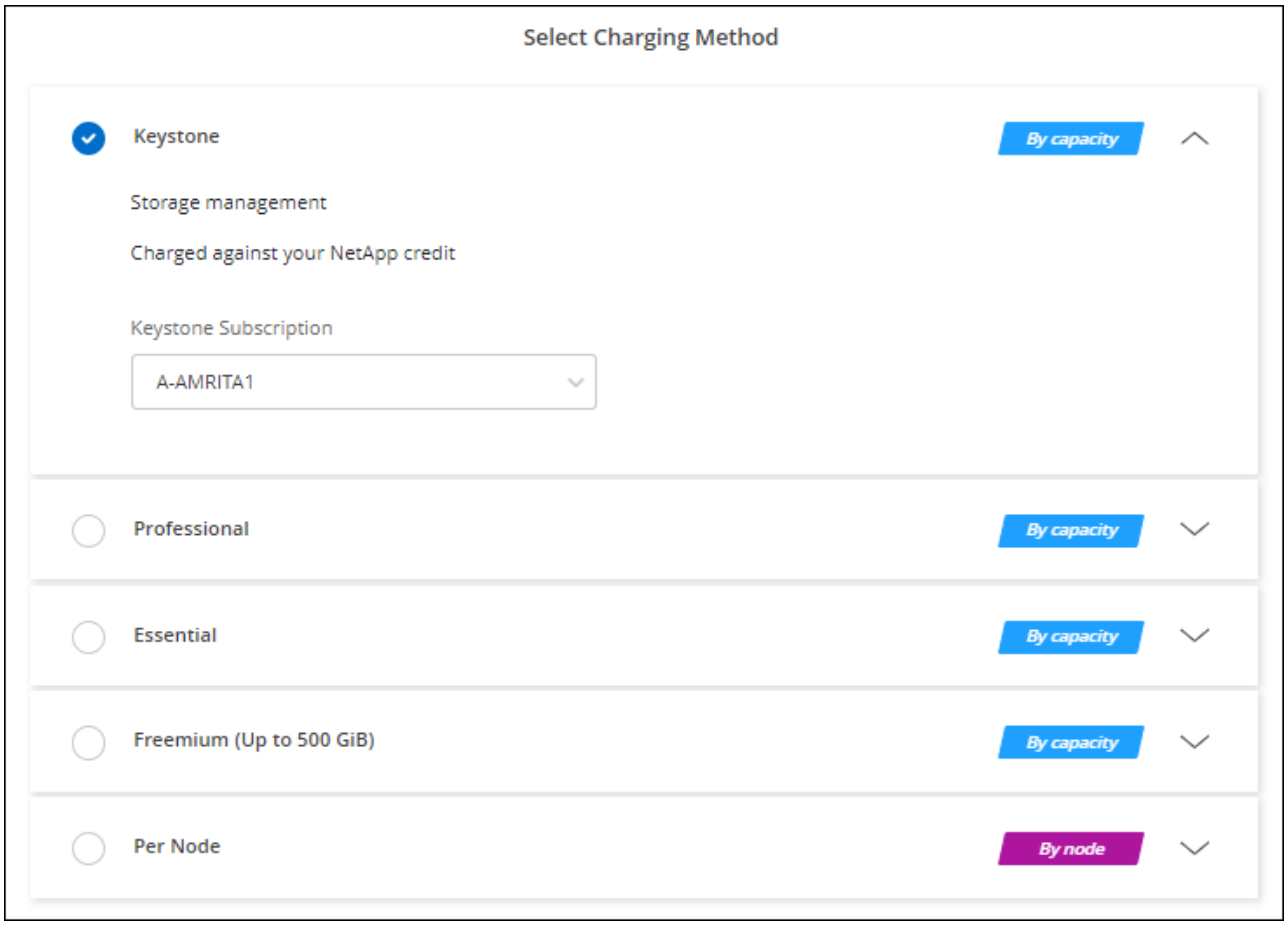
Keystone Abonnement

Bei einem Keystone -Abonnement handelt es sich um einen Abonnementdienst mit nutzungsabhängiger Bezahlung. "Erfahren Sie mehr über NetApp Keystone -Abonnements" .

Schritte

1. Wenn Sie noch kein Abonnement haben, "NetApp kontaktieren"
2. mailto:ng-keystone-success@netapp.com [Kontaktieren Sie NetApp], um Ihr Konsolenbenutzerkonto mit einem oder mehreren Keystone Abonnements zu autorisieren.
3. Nachdem NetApp Ihr Konto autorisiert hat,"Verknüpfen Sie Ihre Abonnements zur Verwendung mit Cloud Volumes ONTAP" .
4. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Schritten.

   a. Wählen Sie die Abrechnungsmethode „Keystone -Abonnement“ aus, wenn Sie zur Auswahl einer Abrechnungsmethode aufgefordert werden.



"Sehen Sie sich die Schritt-für-Schritt-Anleitung zum Starten von Cloud Volumes ONTAP in Google Cloud an" .

Knotenbasierte Lizenz

Eine knotenbasierte Lizenz ist die Lizenz der vorherigen Generation für Cloud Volumes ONTAP. Eine knotenbasierte Lizenz kann von NetApp (BYOL) erworben werden und ist nur in bestimmten Fällen für Lizenzverlängerungen verfügbar. Weitere Informationen finden Sie unter:

- "Ende der Verfügbarkeit knotenbasierter Lizenzen"
- "Ende der Verfügbarkeit von knotenbasierten Lizenzen"
- "Konvertieren Sie eine knotenbasierte Lizenz in eine kapazitätsbasierte Lizenz"

Starten Sie Cloud Volumes ONTAP in Google Cloud

Sie können Cloud Volumes ONTAP in einer Einzelknotenkonfiguration oder als HA-Paar in Google Cloud starten.

Bevor Sie beginnen

Bevor Sie beginnen, benötigen Sie Folgendes.

- Ein NetApp Console-Agent, der betriebsbereit ist.

- Sie sollten über eine "Konsolenagent, der mit Ihrem System verknüpft ist" .
- "Sie sollten darauf vorbereitet sein, den Konsolenagenten immer laufen zu lassen" .
- Das mit dem Console-Agenten verknüpfte Dienstkonto "sollte über die erforderlichen Berechtigungen verfügen"

- Ein Verständnis der Konfiguration, die Sie verwenden möchten.

  Sie sollten sich vorbereitet haben, indem Sie eine Konfiguration ausgewählt und von Ihrem Administrator Informationen zum Google Cloud-Netzwerk eingeholt haben. Weitere Einzelheiten finden Sie unter"Planen Ihrer Cloud Volumes ONTAP Konfiguration" .

- Ein Verständnis dafür, was zum Einrichten der Lizenzierung für Cloud Volumes ONTAP erforderlich ist.

  "Erfahren Sie, wie Sie die Lizenzierung einrichten" .

- Google Cloud APIs sollten "in Ihrem Projekt aktiviert" :
  - Cloud Deployment Manager V2 API
  - Cloud Logging API
  - Cloud Resource Manager-API
  - Compute Engine-API
  - API für Identitäts- und Zugriffsverwaltung (IAM)

Starten Sie ein Einzelknotensystem in Google Cloud

Erstellen Sie in der NetApp Console ein System, um Cloud Volumes ONTAP in Google Cloud zu starten.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **Systeme** auf **System hinzufügen** und folgen Sie den Anweisungen.
3. **Wählen Sie einen Standort**: Wählen Sie **Google Cloud** und * Cloud Volumes ONTAP*.
4. Wenn Sie dazu aufgefordert werden, "Erstellen Sie einen Konsolenagenten" .
5. **Details und Anmeldeinformationen**: Wählen Sie ein Projekt aus, geben Sie einen Clusternamen an, wählen Sie optional ein Dienstkonto aus, fügen Sie optional Bezeichnungen hinzu und geben Sie dann die Anmeldeinformationen an.

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

Feld	Beschreibung
Systemname	Die Konsole verwendet den Systemnamen, um sowohl das Cloud Volumes ONTAP -System als auch die Google Cloud VM-Instanz zu benennen. Wenn Sie diese Option auswählen, wird der Name auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet.
Dienstkontoname	Wenn Sie planen,"Daten-Tiering" oder "NetApp Backup and Recovery" mit Cloud Volumes ONTAP, dann müssen Sie **Servicekonto** aktivieren und ein Servicekonto auswählen, das über die vordefinierte Rolle „Storage Admin“ verfügt. "Erfahren Sie, wie Sie ein Dienstkonto erstellen" .

Feld	Beschreibung
Beschriftungen hinzufügen	Labels sind Metadaten für Ihre Google Cloud-Ressourcen. Die Konsole fügt die Labels dem Cloud Volumes ONTAP -System und den mit dem System verknüpften Google Cloud-Ressourcen hinzu. Sie können beim Erstellen eines Systems bis zu vier Beschriftungen über die Benutzeroberfläche hinzufügen und nach der Erstellung weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen eines Systems nicht auf vier Labels beschränkt. Informationen zu Etiketten finden Sie im "Google Cloud-Dokumentation: Kennzeichnungsressourcen" .
Benutzername und Passwort	Dies sind die Anmeldeinformationen für das Cloud Volumes ONTAP Clusteradministratorkonto. Sie können diese Anmeldeinformationen verwenden, um über ONTAP System Manager oder die ONTAP CLI eine Verbindung zu Cloud Volumes ONTAP herzustellen. Behalten Sie den Standardbenutzernamen *admin* bei oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Projekt bearbeiten	Wählen Sie das Projekt aus, in dem Cloud Volumes ONTAP gespeichert werden soll. Das Standardprojekt ist das Projekt der Konsole. Wenn in der Dropdown-Liste keine weiteren Projekte angezeigt werden, haben Sie das Dienstkonto noch nicht mit anderen Projekten verknüpft. Gehen Sie zur Google Cloud Console, öffnen Sie den IAM-Dienst und wählen Sie das Projekt aus. Fügen Sie das Dienstkonto mit der Rolle, die Sie für die Console verwenden, zu diesem Projekt hinzu. Sie müssen diesen Schritt für jedes Projekt wiederholen. Dies ist das Dienstkonto, das Sie für die Konsole eingerichtet haben."wie auf dieser Seite beschrieben" . Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen einem Abonnement zuzuordnen. Um ein Cloud Volumes ONTAP -System mit nutzungsbasierter Bezahlung zu erstellen, müssen Sie ein Google Cloud-Projekt auswählen, das mit einem Abonnement für Cloud Volumes ONTAP aus dem Google Cloud-Marktplatz verknüpft ist. Siehe "Verknüpfen eines Marktplatz-Abonnements mit Google Cloud-Anmeldeinformationen" .

6. **Dienste**: Wählen Sie die Dienste aus, die Sie auf diesem System verwenden möchten. Um Backup und Recovery auszuwählen oder NetApp Cloud Tiering zu verwenden, müssen Sie in Schritt 3 das Servicekonto angegeben haben.

   Wenn Sie WORM und Daten-Tiering nutzen möchten, müssen Sie Backup und Recovery deaktivieren und ein Cloud Volumes ONTAP System mit Version 9.8 oder höher bereitstellen.

7. **Standort & Konnektivität**: Wählen Sie die Google Cloud-Region und -Zone für Ihr System, wählen Sie eine Firewall-Richtlinie und bestätigen Sie die Netzwerkverbindung zu Google Cloud storage für die Daten-Tiering.

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

Feld	Beschreibung
Konnektivitätsüberprüfung	Um kalte Daten in einen Google Cloud Storage-Bucket zu verschieben, muss das Subnetz, in dem sich Cloud Volumes ONTAP befindet, für den privaten Google-Zugriff konfiguriert werden. Anweisungen hierzu finden Sie unter "Google Cloud-Dokumentation: Konfigurieren des privaten Google-Zugriffs" .
Generierte Firewall-Richtlinie	Wenn Sie die Firewall-Richtlinie von der Konsole erstellen lassen, müssen Sie auswählen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Nur ausgewählte VPC** auswählen, ist der Quellfilter für eingehenden Datenverkehr der Subnetzbereich der ausgewählten VPC und der Subnetzbereich der VPC, in der sich der Konsolenagent befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VPCs** auswählen, ist der Quellfilter für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene Firewall-Richtlinie verwenden	Wenn Sie eine vorhandene Firewall-Richtlinie verwenden, stellen Sie sicher, dass diese die erforderlichen Regeln enthält:"Erfahren Sie mehr über Firewall-Regeln für Cloud Volumes ONTAP"

8. **Abrechnungsmethoden und NSS-Konto**: Geben Sie an, welche Abrechnungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site-Konto an:
   - "Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP"
   - "Erfahren Sie, wie Sie die Lizenzierung einrichten"
9. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete aus, um schnell ein Cloud Volumes ONTAP-System bereitzustellen, oder klicken Sie auf **Eigene Konfiguration erstellen**. Die vorkonfigurierten Pakete variieren je nach gewählter Cloud Volumes ONTAP Version. Zum Beispiel zeigt die Console für Cloud Volumes ONTAP 9.18.1 und höher Pakete mit C3-VMs, einschließlich Hyperdisk Balanced-Festplatten, an. Sie können die Konfigurationen, wie IOPS- und Durchsatzparameter, basierend auf Ihren Workload-Anforderungen anpassen.

   Wenn Sie sich für eines der Pakete entscheiden, müssen Sie lediglich ein Volumen angeben und anschließend die Konfiguration prüfen und freigeben.
10. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP -Version nach Bedarf und wählen Sie einen Maschinentyp aus.

    Wenn für eine ausgewählte Version ein neuerer Release Candidate, eine allgemeine Verfügbarkeit oder ein Patch-Release verfügbar ist, aktualisiert die Konsole das System beim Erstellen auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.13.1 auswählen und 9.13.1 P4 verfügbar ist. Das Update erfolgt nicht von einer Version zur nächsten, beispielsweise von 9.13 auf 9.14.
11. **Zugrunde liegende Speicherressourcen**: Wählen Sie Einstellungen für das anfängliche Aggregat: einen Datenträgertyp und die Größe für jeden Datenträger.

    Der Datenträgertyp ist für das ursprüngliche Volume. Sie können für nachfolgende Volumes einen anderen Datenträgertyp auswählen.

    Die Datenträgergröße gilt für alle Datenträger im anfänglichen Aggregat und für alle zusätzlichen Aggregate, die die Konsole erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der

erweiterten Zuordnungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

Hilfe zur Auswahl von Datenträgertyp und -größe finden Sie unter"Dimensionieren Sie Ihr System in Google Cloud" .

12. **Flash-Cache, Schreibgeschwindigkeit und WORM**:

    a. Aktivieren Sie **Flash Cache** oder wählen Sie **Normal** oder **High** Schreibgeschwindigkeit, wenn Sie es benötigen.

       Erfahren Sie mehr über "Flash-Cache" und "Schreibgeschwindigkeit".

       Eine hohe Schreibgeschwindigkeit und eine höhere maximale Übertragungseinheit (MTU) von 8.896 Bytes sind über die Schreibgeschwindigkeitsoption **Hohe** verfügbar. Darüber hinaus erfordert die höhere MTU von 8.896 die Auswahl von VPC-1, VPC-2 und VPC-3 für die Bereitstellung. Weitere Informationen zu VPC-1, VPC-2 und VPC-3 finden Sie unter "Regeln für VPC-1, VPC-2 und VPC-3" .

    b. Aktivieren Sie bei Bedarf den WORM-Speicher (Write Once, Read Many).

       WORM kann nicht aktiviert werden, wenn die Datenschichtung für Cloud Volumes ONTAP Version 9.7 und darunter aktiviert wurde. Das Zurücksetzen oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach der Aktivierung von WORM und Tiering blockiert.

    "Erfahren Sie mehr über WORM-Speicher" .

    a. Wenn Sie den WORM-Speicher aktivieren, wählen Sie die Aufbewahrungsdauer aus.

13. **Daten-Tiering in Google Cloud Platform**: Wählen Sie, ob das Daten-Tiering für das anfängliche Aggregat aktiviert werden soll, wählen Sie eine Speicherklasse für die gestuften Daten und wählen Sie dann entweder ein Dienstkonto mit der vordefinierten Rolle „Speicheradministrator“ (erforderlich für Cloud Volumes ONTAP 9.7 oder höher) oder ein Google Cloud-Konto (erforderlich für Cloud Volumes ONTAP 9.6).

    Beachten Sie Folgendes:

    - Die Konsole richtet das Dienstkonto auf der Cloud Volumes ONTAP Instanz ein. Dieses Dienstkonto bietet Berechtigungen für die Datenschichtung in einem Google Cloud Storage-Bucket. Stellen Sie sicher, dass Sie das Dienstkonto des Konsolenagenten als Benutzer des Tiering-Dienstkontos hinzufügen, da Sie es sonst nicht aus der Konsole auswählen können.
    - Hilfe zum Hinzufügen eines Google Cloud-Kontos finden Sie unter "Einrichten und Hinzufügen von Google Cloud-Konten für Daten-Tiering mit 9.6" .
    - Sie können beim Erstellen oder Bearbeiten eines Volumes eine bestimmte Volume-Tiering-Richtlinie auswählen.
    - Wenn Sie die Datenschichtung deaktivieren, können Sie sie bei nachfolgenden Aggregaten wieder aktivieren, aber Sie müssen das System ausschalten und ein Dienstkonto aus der Google Cloud Console hinzufügen.

      "Weitere Informationen zum Daten-Tiering" .

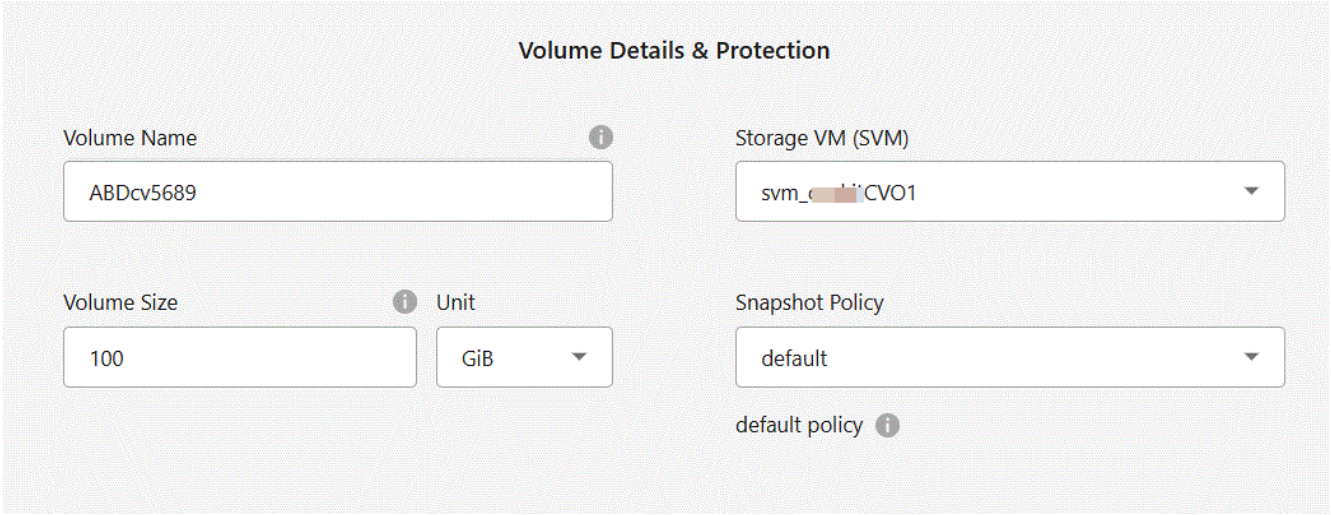
14. **Volume erstellen**: Geben Sie Details für das neue Volume ein oder klicken Sie auf **Überspringen**.

    "Erfahren Sie mehr über unterstützte Clientprotokolle und -versionen" .

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

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren. Dadurch können Sie ein Volume erstellen, das größer ist als der ihm aktuell zur Verfügung stehende physische Speicher.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt die Konsole einen Wert ein, der Zugriff auf alle Instanzen im Subnetz gewährt.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch als Zugriffskontrolllisten oder ACLs bezeichnet). Sie können lokale oder Domänen-Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Windows-Domänenbenutzernamen angeben, müssen Sie die Domäne des Benutzers im Format Domäne\Benutzername angeben.
Snapshot-Richtlinie	Eine Snapshot-Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot-Kopien an. Eine NetApp Snapshot-Kopie ist ein zeitpunktbezogenes Dateisystem-Image, das keine Auswirkungen auf die Leistung hat und nur minimalen Speicherplatz benötigt. Sie können die Standardrichtlinie oder keine auswählen. Für vorübergehende Daten können Sie „Keine“ auswählen, beispielsweise „tempdb“ für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume aus: entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	iSCSI-Speicherziele werden als LUNs (logische Einheiten) bezeichnet und Hosts als Standardblockgeräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Hostknotennamen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. iSCSI-Ziele stellen über Standard-Ethernet-Netzwerkadapter (NICs), TCP-Offload-Engine-Karten (TOE) mit Software-Initiatoren, konvergente Netzwerkadapter (CNAs) oder dedizierte Hostbusadapter (HBAs) eine Verbindung zum Netzwerk her und werden durch iSCSI-qualifizierte Namen (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt die Konsole automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volume erstellt haben, sodass keine Verwaltung erforderlich ist. Nachdem Sie das Volume erstellt haben,"Verwenden Sie den IQN, um von Ihren Hosts aus eine Verbindung zum LUN herzustellen" .

Das folgende Bild zeigt die erste Seite des Assistenten zur Volumeerstellung:



15. **CIFS-Setup**: Wenn Sie das CIFS-Protokoll gewählt haben, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
DNS Primäre und sekundäre IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgelisteten DNS-Server müssen die Service Location Records (SRV) enthalten, die zum Auffinden der Active Directory-LDAP-Server und Domänencontroller für die Domäne erforderlich sind, der der CIFS-Server beitreten wird. Wenn Sie Google Managed Active Directory konfigurieren, kann auf AD standardmäßig mit der IP-Adresse 169.254.169.254 zugegriffen werden.
Beitretende Active Directory-Domäne	Der FQDN der Active Directory (AD)-Domäne, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zum Beitritt zur Domäne berechtigt sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
NetBIOS-Name des CIFS-Servers	Ein CIFS-Servername, der in der AD-Domäne eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domäne, die mit dem CIFS-Server verknüpft werden soll. Der Standardwert ist CN=Computers. Um Google Managed Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in dieses Feld **OU=Computers,OU=Cloud** ein.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud-Dokumentation: Organisationseinheiten in Google Managed Microsoft AD"^]
DNS-Domäne	Die DNS-Domäne für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen ist die Domäne dieselbe wie die AD-Domäne.
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden**, um einen NTP-Server mithilfe des Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Weitere Informationen finden Sie im "Dokumentation zur NetApp Console" für Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Es ist nicht mehr konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

16. **Nutzungsprofil, Datenträgertyp und Tiering-Richtlinie**: Wählen Sie aus, ob Sie Speichereffizienzfunktionen aktivieren möchten, und ändern Sie bei Bedarf die Volume-Tiering-Richtlinie.

    Weitere Informationen finden Sie unter"Auswählen eines Volume-Nutzungsprofils" ,"Übersicht über Data Tiering" , Und "KB: Welche Inline-Speichereffizienzfunktionen werden mit CVO unterstützt?"

17. **Überprüfen und genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um Details zum Support und den Google Cloud-Ressourcen anzuzeigen, die über die Konsole erworben werden.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie auf **Los**.

Ergebnis

Die Konsole stellt das Cloud Volumes ONTAP -System bereit. Sie können den Fortschritt auf der Seite **Audit** verfolgen.

Wenn bei der Bereitstellung des Cloud Volumes ONTAP Systems Probleme auftreten, überprüfen Sie die Fehlermeldung. Sie können auch das System auswählen und auf **Umgebung neu erstellen** klicken.

Weitere Hilfe finden Sie unter "NetApp Cloud Volumes ONTAP Unterstützung" .

Nach Abschluss

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

  Mithilfe von Kontingenten können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Dateien beschränken oder verfolgen.

> Nach Abschluss des Bereitstellungsprozesses dürfen die systemgenerierten Cloud Volumes ONTAP Konfigurationen im Google Cloud-Portal, wie zum Beispiel die System-Tags und die in den Google Cloud-Ressourcen festgelegten Labels, nicht verändert werden. Jegliche Änderungen an diesen Konfigurationen können zu unerwartetem Verhalten oder Datenverlust führen.

Starten Sie ein HA-Paar in Google Cloud

Erstellen Sie in der Konsole ein System, um Cloud Volumes ONTAP in Google Cloud zu starten.

Schritte

1. Wählen Sie im linken Navigationsmenü **Speicher > Verwaltung**.
2. Klicken Sie auf der Seite **Systeme** auf **Speicher > System** und folgen Sie den Anweisungen.
3. **Wählen Sie einen Standort**: Wählen Sie **Google Cloud** und * Cloud Volumes ONTAP HA*.
4. **Details und Anmeldeinformationen**: Wählen Sie ein Projekt aus, geben Sie einen Clusternamen an, wählen Sie optional ein Dienstkonto aus, fügen Sie optional Bezeichnungen hinzu und geben Sie dann die Anmeldeinformationen an.

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

Feld	Beschreibung
Systemname	Die Konsole verwendet den Systemnamen, um sowohl das Cloud Volumes ONTAP -System als auch die Google Cloud VM-Instanz zu benennen. Wenn Sie diese Option auswählen, wird der Name auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet.
Dienstkontoname	Wenn Sie die"NetApp Cloud Tiering" oder "Sicherung und Wiederherstellung" Dienste müssen Sie den Schalter **Dienstkonto** aktivieren und dann das Dienstkonto auswählen, das über die vordefinierte Rolle „Speicheradministrator“ verfügt.
Beschriftungen hinzufügen	Labels sind Metadaten für Ihre Google Cloud-Ressourcen. Die Konsole fügt die Labels dem Cloud Volumes ONTAP -System und den mit dem System verknüpften Google Cloud-Ressourcen hinzu. Sie können beim Erstellen eines Systems bis zu vier Beschriftungen über die Benutzeroberfläche hinzufügen und nach der Erstellung weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen eines Systems nicht auf vier Labels beschränkt. Informationen zu Etiketten finden Sie unter "Google Cloud-Dokumentation: Kennzeichnungsressourcen" .
Benutzername und Passwort	Dies sind die Anmeldeinformationen für das Cloud Volumes ONTAP Clusteradministratorkonto. Sie können diese Anmeldeinformationen verwenden, um über ONTAP System Manager oder die ONTAP CLI eine Verbindung zu Cloud Volumes ONTAP herzustellen. Behalten Sie den Standardbenutzernamen *admin* bei oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Projekt bearbeiten	Wählen Sie das Projekt aus, in dem Cloud Volumes ONTAP gespeichert werden soll. Das Standardprojekt ist das Projekt der Konsole. Wenn in der Dropdown-Liste keine weiteren Projekte angezeigt werden, haben Sie das Dienstkonto noch nicht mit anderen Projekten verknüpft. Gehen Sie zur Google Cloud Console, öffnen Sie den IAM-Dienst und wählen Sie das Projekt aus. Fügen Sie das Dienstkonto mit der Rolle, die Sie für die Console verwenden, zu diesem Projekt hinzu. Sie müssen diesen Schritt für jedes Projekt wiederholen. Dies ist das Dienstkonto, das Sie für die Konsole eingerichtet haben."wie auf dieser Seite beschrieben" . Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen einem Abonnement zuzuordnen. Um ein Cloud Volumes ONTAP -System mit nutzungsbasierter Bezahlung zu erstellen, müssen Sie ein Google Cloud-Projekt auswählen, das mit einem Abonnement für Cloud Volumes ONTAP aus dem Google Cloud Marketplace verknüpft ist. Siehe "Verknüpfen eines Marktplatz-Abonnements mit Google Cloud-Anmeldeinformationen" .

5. **Dienste**: Wählen Sie die Dienste aus, die Sie auf diesem System verwenden möchten. Um „Backup und Wiederherstellung“ auszuwählen oder NetApp Cloud Tiering zu verwenden, müssen Sie in Schritt 3 das

Dienstkonto angegeben haben.

Wenn Sie WORM und Daten-Tiering nutzen möchten, müssen Sie Backup und Recovery deaktivieren und ein Cloud Volumes ONTAP System mit Version 9.8 oder höher bereitstellen.

6. **HA-Bereitstellungsmodelle**: Wählen Sie mehrere Zonen (empfohlen) oder eine einzelne Zone für die HA-Konfiguration. Wählen Sie dann eine Region und eine Zone aus.

   "Erfahren Sie mehr über HA-Bereitstellungsmodelle" .

7. **Konnektivität**: Wählen Sie vier verschiedene VPCs für die HA-Konfiguration, ein Subnetz in jedem VPC und dann eine Firewall-Richtlinie aus.

   "Erfahren Sie mehr über die Netzwerkanforderungen" .

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

Feld	Beschreibung
Generierte Richtlinie	Wenn Sie die Firewall-Richtlinie von der Konsole erstellen lassen, müssen Sie auswählen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Nur ausgewählte VPC** auswählen, ist der Quellfilter für eingehenden Datenverkehr der Subnetzbereich der ausgewählten VPC und der Subnetzbereich der VPC, in der sich der Konsolenagent befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VPCs** auswählen, ist der Quellfilter für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene verwenden	Wenn Sie eine vorhandene Firewall-Richtlinie verwenden, stellen Sie sicher, dass diese die erforderlichen Regeln enthält. "Erfahren Sie mehr über Firewall-Regeln für Cloud Volumes ONTAP" .

8. **Abrechnungsmethoden und NSS-Konto**: Geben Sie an, welche Abrechnungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site-Konto an.
   - "Erfahren Sie mehr über die Lizenzierungsoptionen für Cloud Volumes ONTAP" .
   - "Erfahren Sie, wie Sie die Lizenzierung einrichten" .
9. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete aus, um schnell ein Cloud Volumes ONTAP System bereitzustellen, oder klicken Sie auf **Meine eigene Konfiguration erstellen**.

   Wenn Sie sich für eines der Pakete entscheiden, müssen Sie lediglich ein Volumen angeben und anschließend die Konfiguration prüfen und freigeben.

10. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP -Version nach Bedarf und wählen Sie einen Maschinentyp aus.

Wenn für die ausgewählte Version ein neuerer Release Candidate, eine allgemeine Verfügbarkeit oder ein Patch-Release verfügbar ist, aktualisiert die Konsole das System beim Erstellen auf diese Version. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.13.1 auswählen und 9.13.1 P4 verfügbar ist. Das Update erfolgt nicht von einer Version zur nächsten, beispielsweise von 9.13 auf 9.14.

11. **Zugrunde liegende Speicherressourcen**: Wählen Sie Einstellungen für das anfängliche Aggregat: einen Datenträgertyp und die Größe für jeden Datenträger.

    Der Datenträgertyp ist für das ursprüngliche Volume. Sie können für nachfolgende Volumes einen anderen Datenträgertyp auswählen.

    Die Datenträgergröße gilt für alle Datenträger im anfänglichen Aggregat und für alle zusätzlichen Aggregate, die die Konsole erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuordnungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

    Hilfe zur Auswahl von Datenträgertyp und -größe finden Sie unter"Dimensionieren Sie Ihr System in Google Cloud" .

12. **Flash-Cache, Schreibgeschwindigkeit und WORM**:

    a. Aktivieren Sie **Flash Cache** oder wählen Sie **Normal** oder **High** Schreibgeschwindigkeit, wenn Sie es benötigen.

       Erfahren Sie mehr über "Flash-Cache" und "Schreibgeschwindigkeit".

       Eine hohe Schreibgeschwindigkeit und eine höhere maximale Übertragungseinheit (MTU) von 8.896 Bytes sind über die Schreibgeschwindigkeitsoption **Hohe** mit den Instance-Typen n2-standard-16, n2-standard-32, n2-standard-48 und n2-standard-64 verfügbar. Darüber hinaus erfordert die höhere MTU von 8.896 die Auswahl von VPC-1, VPC-2 und VPC-3 für die Bereitstellung. Eine hohe Schreibgeschwindigkeit und eine MTU von 8.896 sind funktionsabhängig und können innerhalb einer konfigurierten Instanz nicht einzeln deaktiviert werden. Weitere Informationen zu VPC-1, VPC-2 und VPC-3 finden Sie unter "Regeln für VPC-1, VPC-2 und VPC-3" .

    b. Aktivieren Sie bei Bedarf den WORM-Speicher (Write Once, Read Many).

       WORM kann nicht aktiviert werden, wenn die Datenschichtung für Cloud Volumes ONTAP Version 9.7 und darunter aktiviert wurde. Das Zurücksetzen oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach der Aktivierung von WORM und Tiering blockiert.

    "Erfahren Sie mehr über WORM-Speicher" .

    a. Wenn Sie den WORM-Speicher aktivieren, wählen Sie die Aufbewahrungsdauer aus.

13. **Daten-Tiering in Google Cloud**: Wählen Sie, ob Sie das Daten-Tiering für das anfängliche Aggregat aktivieren möchten, wählen Sie eine Speicherklasse für die gestuften Daten und wählen Sie dann ein Dienstkonto mit der vordefinierten Rolle „Speicheradministrator“.

    Beachten Sie Folgendes:

    - Die Konsole richtet das Dienstkonto auf der Cloud Volumes ONTAP Instanz ein. Dieses Dienstkonto bietet Berechtigungen für die Datenschichtung in einem Google Cloud Storage-Bucket. Stellen Sie sicher, dass Sie das Dienstkonto des Konsolenagenten als Benutzer des Tiering-Dienstkontos

hinzufügen, da Sie es sonst nicht aus der Konsole auswählen können.

- Sie können beim Erstellen oder Bearbeiten eines Volumes eine bestimmte Volume-Tiering-Richtlinie auswählen.
- Wenn Sie die Datenschichtung deaktivieren, können Sie sie bei nachfolgenden Aggregaten wieder aktivieren, aber Sie müssen das System ausschalten und ein Dienstkonto aus der Google Cloud Console hinzufügen.

"Weitere Informationen zum Daten-Tiering" .

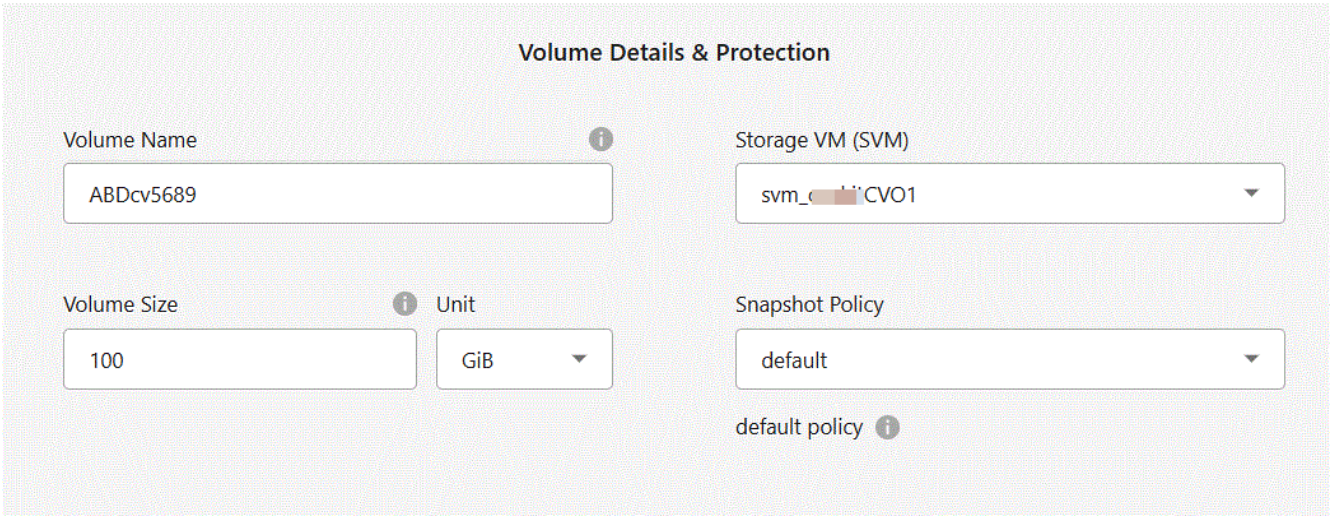
14. **Volume erstellen**: Geben Sie Details für das neue Volume ein oder klicken Sie auf **Überspringen**.

"Erfahren Sie mehr über unterstützte Clientprotokolle und -versionen" .

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

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren. Dadurch können Sie ein Volume erstellen, das größer ist als der ihm aktuell zur Verfügung stehende physische Speicher.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt die Konsole einen Wert ein, der Zugriff auf alle Instanzen im Subnetz gewährt.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch als Zugriffskontrolllisten oder ACLs bezeichnet). Sie können lokale oder Domänen-Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Windows-Domänenbenutzernamen angeben, müssen Sie die Domäne des Benutzers im Format Domäne\Benutzername angeben.
Snapshot-Richtlinie	Eine Snapshot-Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot-Kopien an. Eine NetApp Snapshot-Kopie ist ein zeitpunktbezogenes Dateisystem-Image, das keine Auswirkungen auf die Leistung hat und nur minimalen Speicherplatz benötigt. Sie können die Standardrichtlinie oder keine auswählen. Für vorübergehende Daten können Sie „Keine“ auswählen, beispielsweise „tempdb“ für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume aus: entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	iSCSI-Speicherziele werden als LUNs (logische Einheiten) bezeichnet und Hosts als Standardblockgeräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Hostknotennamen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. iSCSI-Ziele stellen über Standard-Ethernet-Netzwerkadapter (NICs), TCP-Offload-Engine-Karten (TOE) mit Software-Initiatoren, konvergente Netzwerkadapter (CNAs) oder dedizierte Hostbusadapter (HBAs) eine Verbindung zum Netzwerk her und werden durch iSCSI-qualifizierte Namen (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt die Konsole automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volume erstellt haben, sodass keine Verwaltung erforderlich ist. Nachdem Sie das Volume erstellt haben,"Verwenden Sie den IQN, um von Ihren Hosts aus eine Verbindung zum LUN herzustellen" .

Das folgende Bild zeigt die erste Seite des Assistenten zur Volumeerstellung:



15. **CIFS-Setup**: Wenn Sie das CIFS-Protokoll gewählt haben, richten Sie einen CIFS-Server ein.

Feld	Beschreibung
DNS Primäre und sekundäre IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgelisteten DNS-Server müssen die Service Location Records (SRV) enthalten, die zum Auffinden der Active Directory-LDAP-Server und Domänencontroller für die Domäne erforderlich sind, der der CIFS-Server beitreten wird. Wenn Sie Google Managed Active Directory konfigurieren, kann auf AD standardmäßig mit der IP-Adresse 169.254.169.254 zugegriffen werden.
Beitretende Active Directory-Domäne	Der FQDN der Active Directory (AD)-Domäne, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zum Beitritt zur Domäne berechtigt sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
NetBIOS-Name des CIFS-Servers	Ein CIFS-Servername, der in der AD-Domäne eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domäne, die mit dem CIFS-Server verknüpft werden soll. Der Standardwert ist CN=Computers. Um Google Managed Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in dieses Feld **OU=Computers,OU=Cloud** ein.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud-Dokumentation: Organisationseinheiten in Google Managed Microsoft AD"^]
DNS-Domäne	Die DNS-Domäne für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen ist die Domäne dieselbe wie die AD-Domäne.

Feld	Beschreibung
NTP-Server	Wählen Sie **Active Directory-Domäne verwenden**, um einen NTP-Server mithilfe des Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Weitere Informationen finden Sie im "Dokumentation zur NetApp Console" für Details. Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Es ist nicht mehr konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.

16. **Nutzungsprofil, Datenträgertyp und Tiering-Richtlinie**: Wählen Sie aus, ob Sie Speichereffizienzfunktionen aktivieren möchten, und ändern Sie bei Bedarf die Volume-Tiering-Richtlinie.

    Weitere Informationen finden Sie unter"Auswählen eines Volume-Nutzungsprofils" ,"Übersicht über Data Tiering" , Und "KB: Welche Inline-Speichereffizienzfunktionen werden mit CVO unterstützt?"

17. **Überprüfen und genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um Details zum Support und den Google Cloud-Ressourcen anzuzeigen, die über die Konsole erworben werden.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie auf **Los**.

Ergebnis

Die Konsole stellt das Cloud Volumes ONTAP -System bereit. Sie können den Fortschritt auf der Seite **Audit** verfolgen.

Wenn bei der Bereitstellung des Cloud Volumes ONTAP Systems Probleme auftreten, überprüfen Sie die Fehlermeldung. Sie können auch das System auswählen und auf **Umgebung neu erstellen** klicken.

Weitere Hilfe finden Sie unter "NetApp Cloud Volumes ONTAP Unterstützung" .

Nach Abschluss

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

  Mithilfe von Kontingenten können Sie den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Dateien beschränken oder verfolgen.

Nach Abschluss des Bereitstellungsprozesses dürfen die systemgenerierten Cloud Volumes ONTAP Konfigurationen im Google Cloud-Portal, wie zum Beispiel die System-Tags und die in den Google Cloud-Ressourcen festgelegten Labels, nicht verändert werden. Jegliche Änderungen an diesen Konfigurationen können zu unerwartetem Verhalten oder Datenverlust führen.

Weiterführende Links

- "Planen Ihrer Cloud Volumes ONTAP Konfiguration in Google Cloud"

Google Cloud Platform-Bildüberprüfung

Erfahren Sie, wie das Google Cloud-Image in Cloud Volumes ONTAP verifiziert wird

Die Google Cloud-Image-Verifizierung entspricht den erweiterten Sicherheitsanforderungen von NetApp . Am Skript zur Bildgenerierung wurden Änderungen vorgenommen, um das Bild unterwegs mit speziell für diese Aufgabe generierten privaten Schlüsseln zu signieren. Sie können die Integrität des Google Cloud-Images überprüfen, indem Sie den signierten Digest und das öffentliche Zertifikat für Google Cloud verwenden, die über heruntergeladen werden können "NSS" für eine bestimmte Version.

Die Google Cloud-Image-Verifizierung wird auf der Cloud Volumes ONTAP -Softwareversion 9.13.0 oder höher unterstützt.

Konvertieren Sie das Google Cloud-Image in das Rohformat für Cloud Volumes ONTAP

Das Image, das zum Bereitstellen neuer Instanzen, Upgrades oder in vorhandenen Images verwendet wird, wird mit den Clients geteilt durch "die NetApp Support Site (NSS)" . Der signierte Digest und die Zertifikate können über das NSS-Portal heruntergeladen werden. Stellen Sie sicher, dass Sie den Digest und die Zertifikate für die richtige Version herunterladen, die dem vom NetApp Support freigegebenen Image entspricht. Beispielsweise verfügen 9.13.0-Images über einen signierten 9.13.0-Digest und Zertifikate, die auf NSS verfügbar sind.

Warum ist dieser Schritt notwendig?

Die Bilder aus der Google Cloud können nicht direkt heruntergeladen werden. Um das Bild anhand des signierten Digests und der Zertifikate zu überprüfen, benötigen Sie einen Mechanismus zum Vergleichen der beiden Dateien und zum Herunterladen des Bildes. Dazu müssen Sie das Image in ein disk.raw-Format exportieren/konvertieren und die Ergebnisse in einem Speicher-Bucket in Google Cloud speichern. Die Datei disk.raw wird dabei getarnt und gzippt.

Das Benutzer-/Dienstkonto benötigt Berechtigungen, um Folgendes auszuführen:

- Zugriff auf den Google-Speicherplatz
- In den Google Storage-Bucket schreiben
- Cloud-Build-Jobs erstellen (wird während des Exportvorgangs verwendet)
- Zugriff auf das gewünschte Bild
- Erstellen von Aufgaben zum Exportieren von Bildern

Um das Image zu überprüfen, muss es in ein disk.raw-Format konvertiert und dann heruntergeladen werden.

Verwenden Sie die Google Cloud-Befehlszeile, um das Google Cloud-Image zu exportieren

Die bevorzugte Methode zum Exportieren eines Bildes in den Cloud-Speicher ist die Verwendung des "Befehl „gcloud compute images export“" . Dieser Befehl nimmt das bereitgestellte Bild und konvertiert es in eine

disk.raw-Datei, die getarnt und gzippt wird. Die generierte Datei wird unter der Ziel-URL gespeichert und kann anschließend zur Überprüfung heruntergeladen werden.

Der Benutzer/das Konto muss über Berechtigungen zum Zugriff auf und Schreiben in den gewünschten Bucket, zum Exportieren des Bilds und für Cloud-Builds (die von Google zum Exportieren des Bilds verwendet werden) verfügen, um diesen Vorgang auszuführen.

Exportieren Sie das Google Cloud-Image mit gcloud

Klicken Sie hier, um anzuzeigen

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

ZIP-Dateien extrahieren

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

Weitere Informationen zum Exportieren eines Bildes über Google Cloud finden Sie im "Google Cloud-Dokument zum Exportieren eines Bildes" .

Bildsignaturprüfung

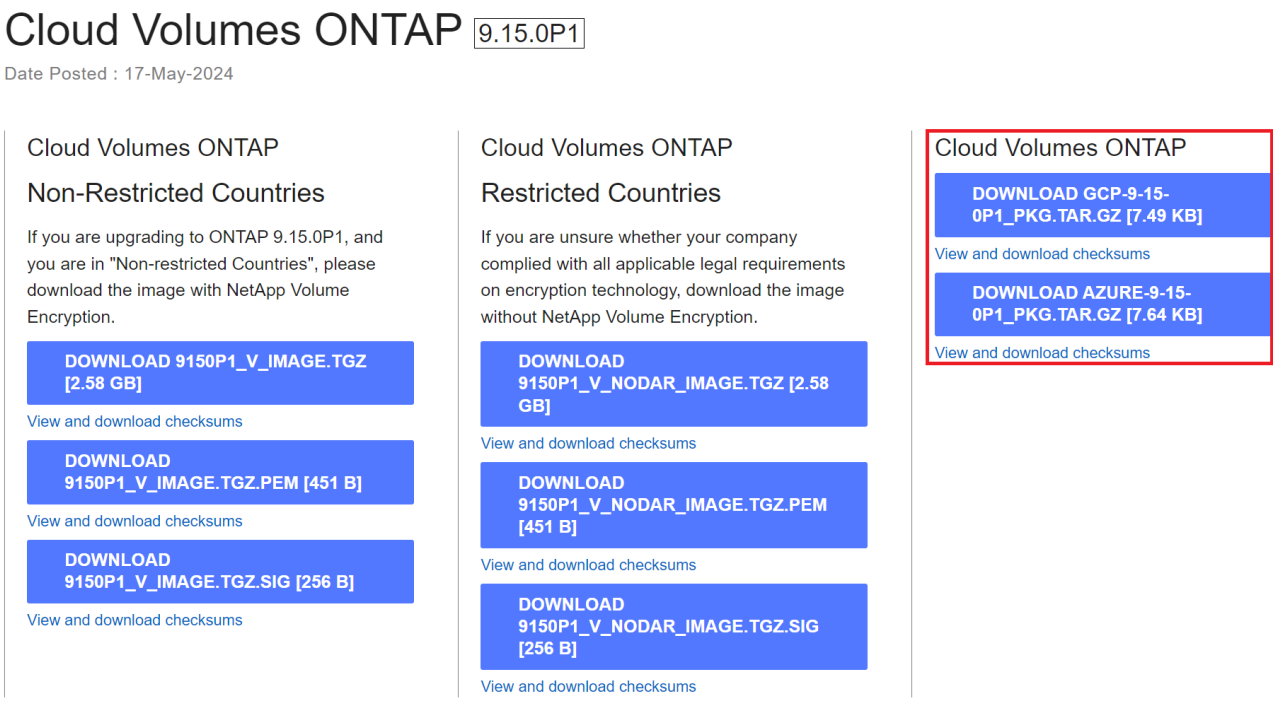
Google Cloud-Image-Signaturprüfung für Cloud Volumes ONTAP

Um das exportierte, von Google Cloud signierte Image zu überprüfen, müssen Sie die Image-Digest-Datei vom NSS herunterladen, um die Datei disk.raw und den Inhalt der Digest-Datei zu validieren.

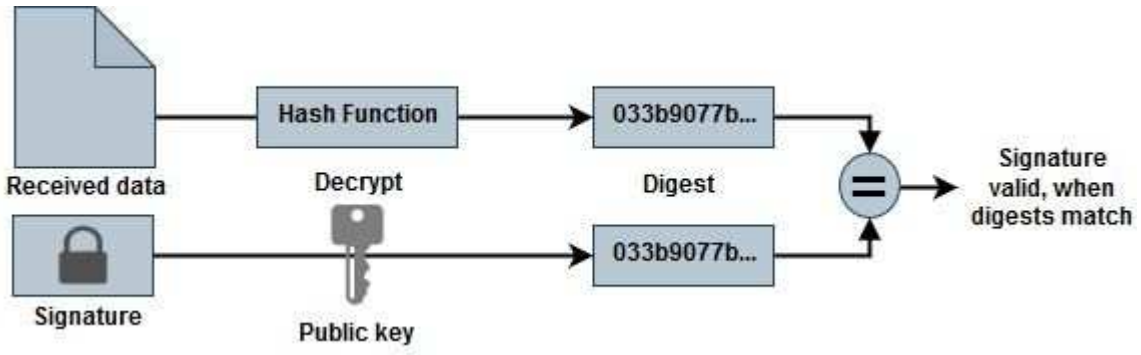
Zusammenfassung des Workflows zur signierten Bildüberprüfung

Nachfolgend finden Sie eine Übersicht über den Workflow-Prozess zur Überprüfung signierter Bilder in Google Cloud.

- Aus dem "NSS" , laden Sie das Google Cloud-Archiv mit den folgenden Dateien herunter:
  - Signierter Digest (.sig)
  - Zertifikat mit dem öffentlichen Schlüssel (.pem)
  - Zertifikatskette (.pem)



- Laden Sie die konvertierte disk.raw-Datei herunter
- Validieren Sie das Zertifikat mithilfe der Zertifikatskette
- Validieren Sie den signierten Digest mithilfe des Zertifikats, das den öffentlichen Schlüssel enthält
  - Entschlüsseln Sie den signierten Digest mit dem öffentlichen Schlüssel, um den Digest der Bilddatei zu extrahieren
  - Erstellen Sie einen Digest der heruntergeladenen disk.raw-Datei
  - Vergleichen Sie die beiden Digest-Dateien zur Validierung



Überprüfen Sie die Google Cloud-Image-Datei disk.raw für Cloud Volumes ONTAP mit OpenSSL

Sie können die von Google Cloud heruntergeladene Datei disk.raw mit dem Inhalt der Digest-Datei vergleichen, der über die "NSS" mit OpenSSL.

Die OpenSSL-Befehle zur Validierung des Images sind mit Linux-, macOS- und Windows-Computern kompatibel.

Schritte

1. Überprüfen Sie das Zertifikat mit OpenSSL.

Klicken Sie hier, um anzuzeigen

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
          e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
          22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
          38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
          fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
          bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. Legen Sie die heruntergeladene Datei disk.raw, die Signatur und die Zertifikate in einem Verzeichnis ab.
3. Extrahieren Sie den öffentlichen Schlüssel mithilfe von OpenSSL aus dem Zertifikat.
4. Entschlüsseln Sie die Signatur mit dem extrahierten öffentlichen Schlüssel und überprüfen Sie den Inhalt der heruntergeladenen Datei disk.raw.

Klicken Sie hier, um anzuzeigen

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```