



Erste Schritte in Google Cloud

Cloud Volumes ONTAP

NetApp
June 27, 2024

Inhalt

- Erste Schritte in Google Cloud 1
 - Schnellstart für Cloud Volumes ONTAP in Google Cloud 1
 - Planen Sie Ihre Cloud Volumes ONTAP-Konfiguration in Google Cloud 2
 - Netzwerkanforderungen für Cloud Volumes ONTAP in Google Cloud 6
 - Planung von VPC-Service-Kontrollen in GCP 16
 - Erstellen eines Servicekontos für Daten-Tiering und Backups 19
 - Nutzung von vom Kunden gemanagten Schlüsseln mit Cloud Volumes ONTAP 22
 - Lizenzierung für Cloud Volumes ONTAP in Google Cloud einrichten 23
 - Cloud Volumes ONTAP in Google Cloud wird gestartet 28
 - Bildüberprüfung Der Google Cloud Platform 42

Erste Schritte in Google Cloud

Schnellstart für Cloud Volumes ONTAP in Google Cloud

Erste Schritte in wenigen Schritten mit Cloud Volumes ONTAP für Google Cloud

1

Einen Konnektor erstellen

Wenn Sie keine haben ["Stecker"](#) Dennoch muss ein Kontoadministrator einen erstellen. ["Erfahren Sie, wie Sie einen Connector in Google Cloud erstellen"](#)

Wenn Sie Cloud Volumes ONTAP in einem Subnetz bereitstellen möchten, in dem kein Internetzugang verfügbar ist, müssen Sie den Connector manuell installieren und auf die BlueXP Benutzeroberfläche zugreifen, die auf diesem Connector ausgeführt wird. ["Erfahren Sie, wie Sie den Connector manuell an einem Ort ohne Internetzugang installieren"](#)

2

Planen Sie Ihre Konfiguration

BlueXP bietet vorkonfigurierte Pakete, die Ihren Workload-Anforderungen entsprechen, oder Sie können eine eigene Konfiguration erstellen. Wenn Sie sich für eine eigene Konfiguration entscheiden, sollten Sie sich mit den verfügbaren Optionen vertraut machen.

["Erfahren Sie mehr über die Planung der Konfiguration"](#).

3

Richten Sie Ihr Netzwerk ein

1. Stellen Sie sicher, dass Ihre VPC und Subnetze die Konnektivität zwischen dem Connector und Cloud Volumes ONTAP unterstützen.
2. Wenn Sie Daten-Tiering aktivieren möchten, ["Konfigurieren Sie das Cloud Volumes ONTAP-Subnetz für privaten Google-Zugriff"](#).
3. Wenn Sie ein HA-Paar implementieren, stellen Sie sicher, dass Sie über vier VPCs verfügen, die jeweils über ein eigenes Subnetz verfügen.
4. Wenn Sie eine gemeinsame VPC verwenden, geben Sie die Rolle „*Compute Network User*“ für das Connector Service-Konto an.
5. Outbound-Internetzugang über die Ziel-VPC für NetApp AutoSupport aktivieren

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

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

4

Erstellen eines Servicekontos

Für Cloud Volumes ONTAP ist ein Google Cloud-Servicekonto aus zwei Gründen erforderlich. Die erste lautet, wenn Sie aktivieren ["Daten-Tiering"](#) Tiering selten genutzter Daten auf kostengünstigen Objekt-Storage in Google Cloud. Die zweite lautet, wenn Sie den aktivieren ["BlueXP Backup und Recovery"](#) Um Volumes auf kostengünstigen Objekt-Storage zu sichern.

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

["Lesen Sie Schritt-für-Schritt-Anleitungen"](#).

5

Aktivieren Sie Google Cloud-APIs

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

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

6

Starten Sie Cloud Volumes ONTAP mit BlueXP

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

Weiterführende Links

- ["Erstellen eines Connectors von BlueXP"](#)
- ["Installieren der Connector-Software auf einem Linux-Host"](#)
- ["Was BlueXP mit Google Cloud-Berechtigungen macht"](#)

Planen Sie Ihre Cloud Volumes ONTAP-Konfiguration in Google Cloud

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

Wählen Sie eine Cloud Volumes ONTAP Lizenz

Für Cloud Volumes ONTAP sind verschiedene Lizenzierungsoptionen verfügbar. Jede Option ermöglicht Ihnen, ein Nutzungsmodell auszuwählen, das Ihren Anforderungen entspricht.

- ["Informieren Sie sich über Lizenzoptionen für Cloud Volumes ONTAP"](#)
- ["Erfahren Sie, wie Sie eine Lizenzierung einrichten"](#)

Wählen Sie eine unterstützte Region aus

Cloud Volumes ONTAP wird in den meisten Google Cloud Regionen unterstützt. ["Hier finden Sie die vollständige Liste der unterstützten Regionen"](#).

Wählen Sie einen unterstützten Maschinentyp aus

Je nach gewähltem Lizenztyp unterstützt Cloud Volumes ONTAP mehrere Maschinentypen.

["Unterstützte Konfigurationen für Cloud Volumes ONTAP in GCP"](#)

Analysieren Sie Ihre Storage-Grenzen

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

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

Dimensionierung Ihres Systems in GCP

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

Maschinentyp

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

Weitere Informationen finden Sie im Folgenden:

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

GCP-Festplattentyp

Bei der Erstellung von Volumes für Cloud Volumes ONTAP müssen Sie den zugrunde liegenden Cloud-Storage auswählen, den Cloud Volumes ONTAP für eine Festplatte verwendet. Der Festplattentyp kann einer der folgenden sein:

- *Zonal SSD persistente Festplatten*: Persistente SSD-Festplatten eignen sich am besten für Workloads, die eine hohe Anzahl an zufälligen IOPS erfordern.
- *Zonal Balance persistente Festplatten*: Diese SSDs sorgen durch niedrigere IOPS pro GB für ein ausgewogenes Verhältnis zwischen Performance und Kosten.
- *Zonal Standard persistente Festplatten* : Standard persistente Festplatten sind wirtschaftlich und können sequenzielle Lese-/Schreibvorgänge verarbeiten.

Weitere Informationen finden Sie unter ["Google Cloud-Dokumentation: Zonal Persistent Disks \(Standard und SSD\)"](#).

GCP-Festplattengröße

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

- Alle Festplatten in einem Aggregat müssen dieselbe Größe haben.

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

Weitere Informationen finden Sie im Folgenden:

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

Anzeigen von Standard-Systemfestplatten

Neben dem Storage für Benutzerdaten erwirbt BlueXP auch Cloud-Storage für Cloud Volumes ONTAP Systemdaten (Boot-Daten, Root-Daten, Core-Daten und NVRAM). Für die Planung können Sie diese Details überprüfen, bevor Sie Cloud Volumes ONTAP implementieren.

- ["Zeigen Sie die Standardfestplatten für Cloud Volumes ONTAP-Systemdaten in Google Cloud an"](#).
- ["Google Cloud Docs: Ressourcenkontingente"](#)

Google Cloud Compute Engine setzt Quoten für die Ressourcenauslastung durch. Damit sollten Sie vor der Implementierung von Cloud Volumes ONTAP sicherstellen, dass Sie das Limit nicht erreicht haben.



Für den Connector ist außerdem eine Systemfestplatte erforderlich. ["Zeigen Sie Details zur Standardkonfiguration des Connectors an"](#).

Sammeln von Netzwerkinformationen

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

Netzwerkinformationen für ein Single-Node-System

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

Netzwerkinformationen für ein HA-Paar in mehreren Zonen

GCP-Informationen	Ihr Wert
Region	
Zone für Knoten 1	

GCP-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	
Firewallrichtlinie (bei Nutzung eigener Richtlinien)	

Netzwerkinformationen für ein HA-Paar in einer einzelnen Zone

GCP-Informationen	Ihr Wert
Region	
Zone	
VPC-0 und Subnetz	
VPC-1 und Subnetz	
VPC-2 und Subnetz	
VPC-3 und Subnetz	
Firewallrichtlinie (bei Nutzung eigener Richtlinien)	

Wählen Sie eine Schreibgeschwindigkeit

Mit BlueXP können Sie eine Schreibgeschwindigkeitseinstellung für Cloud Volumes ONTAP auswählen, außer für HA-Paare in Google Cloud. Bevor Sie sich für eine Schreibgeschwindigkeit entscheiden, sollten Sie die Unterschiede zwischen den normalen und hohen Einstellungen sowie Risiken und Empfehlungen verstehen, wenn Sie eine hohe Schreibgeschwindigkeit verwenden. ["Erfahren Sie mehr über Schreibgeschwindigkeit"](#).

Wählen Sie ein Volume-Auslastungsprofil aus

ONTAP umfasst mehrere Storage-Effizienzfunktionen, mit denen Sie die benötigte Storage-Gesamtmenge reduzieren können. Wenn Sie ein Volume in BlueXP erstellen, können Sie ein Profil auswählen, das diese Funktionen aktiviert oder ein Profil, das sie deaktiviert. Sie sollten mehr über diese Funktionen erfahren, um zu entscheiden, welches Profil Sie verwenden möchten.

NetApp Storage-Effizienzfunktionen bieten folgende Vorteile:

Thin Provisioning

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

Deduplizierung

Verbessert die Effizienz, indem identische Datenblöcke lokalisiert und durch Verweise auf einen einzelnen

gemeinsam genutzten Block ersetzt werden. Durch diese Technik werden die Storage-Kapazitätsanforderungen reduziert, da redundante Datenblöcke im selben Volume eliminiert werden.

Komprimierung

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

Netzwerkanforderungen für Cloud Volumes ONTAP in Google Cloud

Richten Sie Ihr Google-Cloud-Netzwerk ein, damit Cloud Volumes ONTAP-Systeme ordnungsgemäß funktionieren können.

Wenn Sie ein HA-Paar bereitstellen möchten, sollten Sie dies tun ["Funktionsweise von HA-Paaren in Google Cloud"](#).

Anforderungen für Cloud Volumes ONTAP

In Google Cloud müssen die folgenden Anforderungen erfüllt sein:

Spezifische Anforderungen für Single Node-Systeme

Wenn Sie ein Single Node-System implementieren möchten, stellen Sie sicher, dass Ihr Netzwerk die folgenden Anforderungen erfüllt.

Eine VPC

Für ein System mit einem einzelnen Node ist eine Virtual Private Cloud (VPC) erforderlich.

Private IP-Adressen

BlueXP weist 3 oder 4 private IP-Adressen einem System mit einem Knoten in Google Cloud zu.

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

```
skipSvmManagementLif: true
```



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

Spezifischen 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

Durch Implementierung einer HA-Konfiguration für mehrere oder in einer einzelnen Zone werden die Hochverfügbarkeit der Daten gewährleistet. Bei der Erstellung des HA-Paars werden Sie von BlueXP aufgefordert, mehrere Zonen oder eine einzelne Zone auszuwählen.

- Mehrere Zonen (empfohlen)

Durch die Implementierung einer HA-Konfiguration über drei Zonen hinweg wird eine kontinuierliche Datenverfügbarkeit sichergestellt, wenn ein Ausfall innerhalb einer Zone auftritt. Beachten Sie, dass die Schreibleistung im Vergleich zu einer einzelnen Zone etwas geringer ist, aber sie ist minimal.

- Einzelne Zone zu erreichen

Wenn eine Cloud Volumes ONTAP HA-Konfiguration in einer einzelnen Zone implementiert wird, kommt eine Richtlinie zur Platzierung der Verteilung zum Einsatz. Diese Richtlinie sorgt dafür, dass eine HA-Konfiguration innerhalb der Zone vor einem Single Point of Failure geschützt ist, ohne dass zur Fehlereingrenzung separate Zonen erforderlich sind.

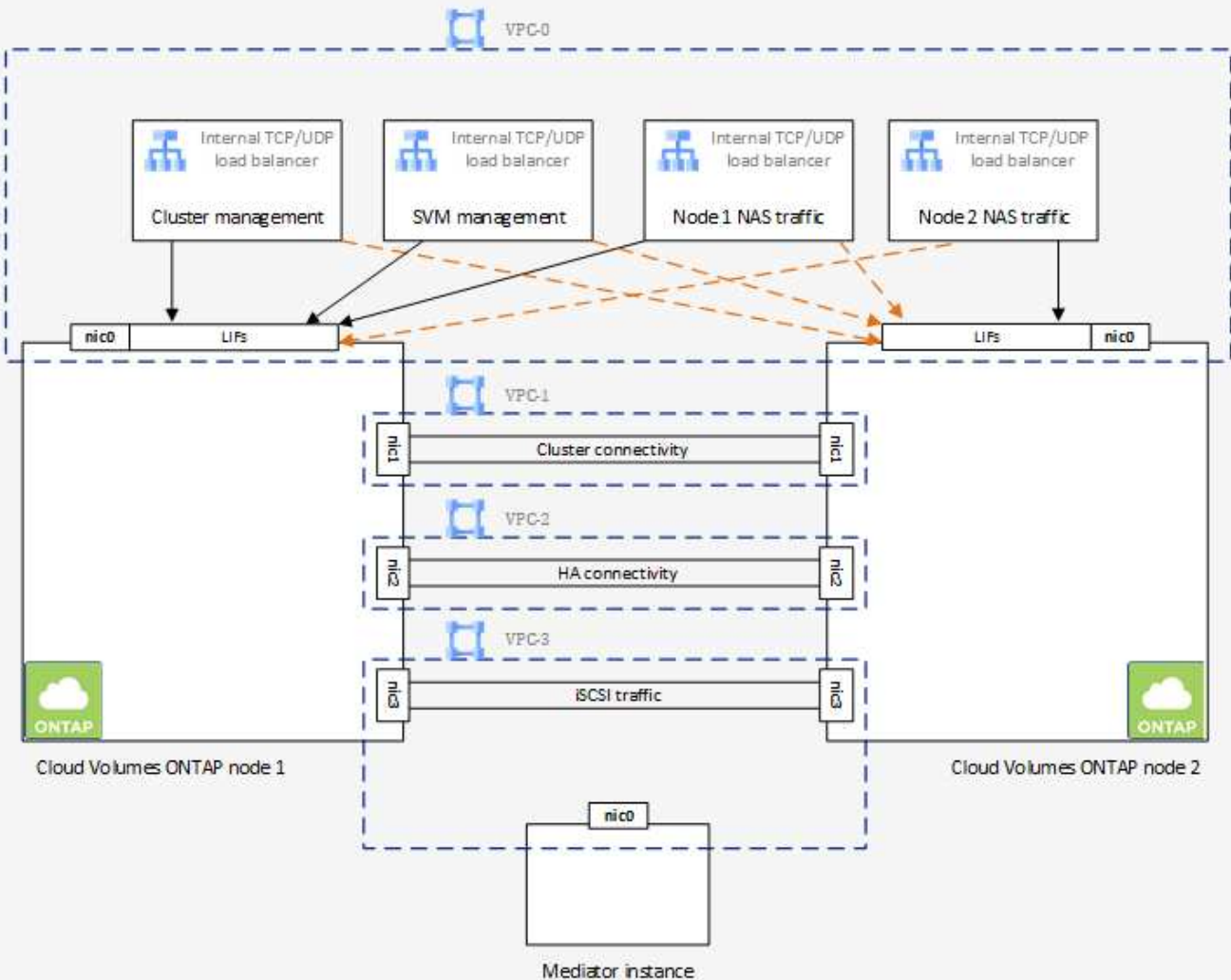
Dieses Implementierungsmodell senkt Ihre Kosten, da zwischen den Zonen keine Kosten für den Datenausgang anfallen.

Vier Virtuelle Private Clouds

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

Bei der Erstellung des HA-Paars werden Sie von BlueXP aufgefordert, vier VPCs auszuwählen:

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



Subnetze

Für jede VPC ist ein privates Subnetz erforderlich.

Wenn Sie den Connector in VPC-0 platzieren, müssen Sie einen privaten Google-Zugriff im Subnetz aktivieren, um auf die APIs zuzugreifen und Daten-Tiering zu ermöglichen.

Die Subnetze in diesen VPCs müssen über unterschiedliche CIDR-Bereiche verfügen. Sie können keine überlappenden CIDR-Bereiche haben.

Private IP-Adressen

BlueXP 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 LIFs, die BlueXP für Cloud Volumes ONTAP zuweist, hängt davon ab, ob Sie ein Single Node-System oder ein HA-Paar implementieren. Ein LIF ist eine IP-Adresse, die einem physischen Port zugewiesen ist. Für Managementtools wie SnapCenter ist eine SVM-Management-LIF erforderlich.

- * Einzelner Knoten*

BlueXP weist einem System mit einem einzelnen Node 4 IP-Adressen zu:

- Node Management-LIF
- Cluster-Management-LIF
- iSCSI-Daten-LIF



Ein iSCSI LIF bietet Client-Zugriff 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 der Storage-VM (SVM)-Management-LIF überspringen, wenn Sie Cloud Volumes ONTAP mithilfe der API implementieren und folgende Flag angeben:

```
skipSvmManagementLif: true
```

• HA-Paar

BlueXP weist 12-13 IP-Adressen einem HA-Paar zu:

- LIFs für das Management von 2 Nodes (e0a)
- 1 LIF zum Cluster-Management (e0a)
- 2 iSCSI LIFs (e0a)



Ein iSCSI LIF bietet Client-Zugriff 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 logische Cluster-Schnittstellen (e0b)
- 2 HA Interconnect IP-Adressen (e0c)
- 2 RSM iSCSI IP-Adressen (e0d)

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

```
skipSvmManagementLif: true
```

Interner Lastausgleich

BlueXP erstellt automatisch vier interne Google Cloud Load Balancer (TCP/UDP), die den eingehenden Datenverkehr zum Cloud Volumes ONTAP HA-Paar verwalten. Am Ende ist keine Konfiguration erforderlich. Diese Anforderung ist lediglich, Sie über den Netzwerkverkehr zu informieren und Sicherheitsbedenken abzumildern.

Ein Load Balancer für das Cluster-Management eignet sich zum Management von Storage-VM (SVM), einer für NAS-Datenverkehr zu Node 1 und der letzte für NAS-Datenverkehr zu Node 2.

Die Einrichtung für die einzelnen Load Balancer lautet wie folgt:

- Eine gemeinsame private IP-Adresse

- Eine globale Zustandsprüfung

Die von der Integritätsprüfung verwendeten Ports sind standardmäßig 63001, 63002 und 63003.

- Ein regionaler TCP-Backend-Service
- Ein regionaler UDP-Backend-Service
- Eine TCP-Weiterleitungsregel
- Eine UDP-Weiterleitungsregel
- Globaler Zugriff ist deaktiviert

Obwohl der globale Zugriff standardmäßig deaktiviert ist, wird die Aktivierung der IT-Bereitstellung unterstützt. Wir haben sie deaktiviert, da der Datenverkehr zwischen Regionen erheblich höhere Latenzen aufweisen wird. Wir wollten sicherstellen, dass Sie keine negativen Erfahrungen durch zufällige, überregionale Montierungen hatten. Wenn Sie diese Option aktivieren, passt sie sich Ihren geschäftlichen Anforderungen an.

Gemeinsam genutzte VPCs

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

Bei einem Single-Node-System kann die VPC entweder eine gemeinsame VPC oder eine Standalone-VPC sein.

Bei einem HA-Paar sind vier VPCs erforderlich. Alle diese VPCs können entweder gemeinsam genutzt oder eigenständig genutzt werden. So könnte es sich beispielsweise um eine gemeinsam genutzte VPC-0, 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 managen. Sie können freigegebene VPC-Netzwerke im `_Host-Projekt_` einrichten und die Instanzen von Connector und Cloud Volumes ONTAP Virtual Machine in einem *Service-Projekt* implementieren. "[Google Cloud-Dokumentation: Gemeinsame VPC-Übersicht](#)".

["Erforderliche gemeinsame VPC-Berechtigungen für die Connector-Implementierung prüfen"](#)

Paketspiegelung in VPCs

"[Paketspiegelung](#)" In der Google Cloud VPC, in der die Cloud Volumes ONTAP implementiert wird, muss deaktiviert werden. Cloud Volumes ONTAP kann nicht ordnungsgemäß ausgeführt werden, wenn die Paketspiegelung aktiviert ist.

Outbound-Internetzugang

Für Cloud Volumes ONTAP ist ein Outbound-Internetzugang für NetApp AutoSupport erforderlich, der den Zustand Ihres Systems proaktiv überwacht und Meldungen an den technischen Support von NetApp sendet.

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

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

Wenn keine ausgehende Internetverbindung zum Senden von AutoSupport-Nachrichten verfügbar ist, konfiguriert BlueXP Ihre Cloud Volumes ONTAP-Systeme automatisch so, dass der Connector als Proxy-Server verwendet wird. Die einzige Anforderung besteht darin, sicherzustellen, dass die Firewall des Connectors *Inbound*-Verbindungen über Port 3128 zulässt. Nach der Bereitstellung des Connectors müssen Sie diesen Port öffnen.

Wenn Sie strenge ausgehende Regeln für Cloud Volumes ONTAP festgelegt haben, müssen Sie auch sicherstellen, dass die Cloud Volumes ONTAP-Firewall *Outbound*-Verbindungen über Port 3128 zulässt.

Nachdem Sie bestätigt haben, dass der ausgehende Internetzugang verfügbar ist, können Sie AutoSupport testen, um sicherzustellen, dass er Nachrichten senden kann. Anweisungen finden Sie unter "[ONTAP Dokumentation: Einrichten von AutoSupport](#)".



Wenn Sie ein HA-Paar verwenden, benötigt der HA Mediator keinen Outbound-Internetzugang.

Wenn Sie von BlueXP darüber informiert werden, dass AutoSupport-Meldungen nicht gesendet werden können, "[Fehler bei der AutoSupport Konfiguration beheben](#)".

Firewall-Regeln

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

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

- Ein Regelsatz für HA-Komponenten in VPC-0. Diese Regeln ermöglichen den Datenzugriff auf Cloud Volumes ONTAP. [Weitere Informationen](#) ..
- Weiterer Regelsatz für HA-Komponenten in VPC-1, VPC-2 und VPC-3. Diese Regeln sind für die Kommunikation zwischen den HA-Komponenten ein- und ausgehender Anruf offen. [Weitere Informationen](#) ..

Wenn kalte Daten in einen Google Cloud Storage Bucket verschoben werden sollen, muss das Subnetz, in dem Cloud Volumes ONTAP residiert, für privaten Google Zugriff konfiguriert sein (wenn Sie ein HA-Paar verwenden, ist dies das Subnetz in VPC-0). Anweisungen finden Sie unter "[Google Cloud-Dokumentation: Privaten Google Access konfigurieren](#)".

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

Verbindungen zu ONTAP Systemen in anderen Netzwerken

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

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

Firewall-Regeln

BlueXP erstellt Google Cloud Firewall-Regeln, die die ein- und ausgehenden Regeln enthalten, die Cloud Volumes ONTAP für den erfolgreichen Betrieb benötigt. Sie können sich zu Testzwecken auf die Ports beziehen oder wenn Sie lieber eigene Firewall-Regeln verwenden möchten.

Die Firewall-Regeln für Cloud Volumes ONTAP erfordern sowohl ein- als auch ausgehende Regeln. Bei der Implementierung einer HA-Konfiguration handelt es sich um die Firewall-Regeln für Cloud Volumes ONTAP in

VPC-0.

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

- Ein Regelsatz für HA-Komponenten in VPC-0. Diese Regeln ermöglichen den Datenzugriff auf Cloud Volumes ONTAP.
- Weiterer Regelsatz für HA-Komponenten in VPC-1, VPC-2 und VPC-3. Diese Regeln sind für die Kommunikation zwischen den HA-Komponenten ein- und ausgehender Anruf offen. [Weitere Informationen](#)



Sie suchen Informationen über den Connector? ["Zeigen Sie Firewall-Regeln für den Connector an"](#)

Regeln für eingehende Anrufe

Wenn Sie eine Arbeitsumgebung erstellen, können Sie den Quellfilter für die vordefinierte Firewall-Richtlinie während der Bereitstellung auswählen:

- **Nur gewählte VPC:** Der Quellfilter für eingehenden Datenverkehr ist der Subnetz-Bereich des VPC für das Cloud Volumes ONTAP-System und der Subnetz-Bereich des VPC, in dem sich der Connector 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 Firewallrichtlinie verwenden, stellen Sie sicher, dass Sie alle Netzwerke hinzufügen, die zur Kommunikation mit Cloud Volumes ONTAP erforderlich sind, aber auch sicherstellen, dass beide Adressbereiche hinzugefügt werden, damit der interne Google Load Balancer korrekt funktioniert. Dies sind die Adressen 130.211.0.0/22 und 35.191.0.0/16. Weitere Informationen finden Sie unter ["Google Cloud Dokumentation: Load Balancer Firewall Rules"](#).

Protokoll	Port	Zweck
Alle ICMP	Alle	Pingen der Instanz
HTTP	80	HTTP-Zugriff auf die System Manager Webkonsole mit der IP-Adresse der Cluster-Management-LIF
HTTPS	443	Konnektivität mit dem Connector und HTTPS-Zugriff auf die System Manager Webkonsole unter Verwendung der IP-Adresse der Cluster-Management-LIF
SSH	22	SSH-Zugriff auf die IP-Adresse der Cluster Management LIF oder einer Node Management LIF
TCP	111	Remote-Prozeduraufruf für NFS
TCP	139	NetBIOS-Servicesitzung für CIFS
TCP	161-162	Einfaches Netzwerkverwaltungsprotokoll
TCP	445	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
TCP	635	NFS-Mount
TCP	749	Kerberos
TCP	2049	NFS-Server-Daemon
TCP	3260	ISCSI-Zugriff über die iSCSI-Daten-LIF

Protokoll	Port	Zweck
TCP	4045	NFS-Sperr-Daemon
TCP	4046	Netzwerkstatusüberwachung für NFS
TCP	10000	Backup mit NDMP
TCP	11104	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
TCP	11105	SnapMirror Datenübertragung über Cluster-interne LIFs
TCP	63001-63050	Ports zur Lastausgleichsprobe zur Ermittlung des ordnungsgemäßen Node (nur für HA-Paare erforderlich)
UDP	111	Remote-Prozeduraufruf für NFS
UDP	161-162	Einfaches Netzwerkverwaltungsprotokoll
UDP	635	NFS-Mount
UDP	2049	NFS-Server-Daemon
UDP	4045	NFS-Sperr-Daemon
UDP	4046	Netzwerkstatusüberwachung für NFS
UDP	4049	NFS rquotad-Protokoll

Regeln für ausgehende Anrufe

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

Grundlegende Regeln für ausgehende Anrufe

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

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

Erweiterte Outbound-Regeln

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



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

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

Service	Protokoll	Port	Quelle	Ziel	Zweck
AutoSupport	HTTPS	443	Node Management-LIF	support.netapp.com	AutoSupport (HTTPS ist der Standard)
	HTTP	80	Node Management-LIF	support.netapp.com	AutoSupport (nur wenn das Transportprotokoll von HTTPS zu HTTP geändert wird)
	TCP	3128	Node Management-LIF	Stecker	Senden von AutoSupport-Nachrichten über einen Proxy-Server auf dem Connector, falls keine ausgehende Internetverbindung verfügbar ist
Cluster	Gesamter Datenverkehr	Gesamter Datenverkehr	Alle LIFs auf einem Node	Alle LIFs auf dem anderen Node	Kommunikation zwischen Clustern (nur Cloud Volumes ONTAP HA)
Konfigurations-Backups	HTTP	80	Node Management-LIF	\Http://<connector-IP-address>/occm/offbo xconfig	Senden Sie Konfigurationssicherungen an den Connector. "Informationen zu Backup-Dateien für die Konfiguration" .
DHCP	UDP	68	Node Management-LIF	DHCP	DHCP-Client für die erstmalige Einrichtung
DHCPS	UDP	67	Node Management-LIF	DHCP	DHCP-Server
DNS	UDP	53	Node Management LIF und Daten LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860-1869	Node Management-LIF	Zielservers	NDMP-Kopie
SMTP	TCP	25	Node Management-LIF	Mailserver	SMTP-Warnungen können für AutoSupport verwendet werden
SNMP	TCP	161	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	UDP	161	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	TCP	162	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	UDP	162	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps

Service	Protokoll	Port	Quelle	Ziel	Zweck
SnapMirror	TCP	1110 4	Intercluster-LIF	ONTAP Intercluster-LIFs	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
	TCP	1110 5	Intercluster-LIF	ONTAP Intercluster-LIFs	SnapMirror Datenübertragung
Syslog	UDP	514	Node Management-LIF	Syslog-Server	Syslog-Weiterleitungsmeldungen

Regeln für VPC-1, VPC-2 und VPC-3

In Google Cloud wird eine HA-Konfiguration über vier VPCs hinweg bereitgestellt. Die für die HA-Konfiguration in VPC-0 erforderlichen Firewall-Regeln sind [O. g. für Cloud Volumes ONTAP](#).

Gleichzeitig ermöglichen die vordefinierten Firewall-Regeln, die BlueXP für Instanzen in VPC-1, VPC-2 und VPC-3 erstellt, die Ingress-Kommunikation über *all* Protokolle und Ports. Diese Regeln ermöglichen die Kommunikation zwischen HA-Nodes.

Die Kommunikation zwischen den HA-Nodes und dem HA Mediator erfolgt über Port 3260 (iSCSI).



Um eine hohe Schreibgeschwindigkeit für neue Implementierungen des Google Cloud HA-Paars zu ermöglichen, ist für VPC-1, VPC-2 und VPC-3 eine maximale Übertragungseinheit (MTU) von mindestens 8,896 Byte erforderlich. Wenn Sie ein Upgrade vorhandener VPC-1, VPC-2 und VPC-3 auf eine MTU von 8,896 Byte vornehmen möchten, müssen Sie während des Konfigurationsprozesses alle vorhandenen HA-Systeme mit diesen VPCs herunterfahren.

Anforderungen an den Steckverbinder

Wenn Sie noch keinen Connector erstellt haben, sollten Sie auch die Netzwerkanforderungen für den Connector prüfen.

- ["Zeigen Sie die Netzwerkanforderungen für den Connector an"](#)
- ["Firewall-Regeln in Google Cloud"](#)

Planung von VPC-Service-Kontrollen in GCP

Wenn Sie sich für die Sperrung Ihrer Google Cloud-Umgebung mit VPC-Servicekontrollen entscheiden, sollten Sie verstehen, wie BlueXP und Cloud Volumes ONTAP mit den Google Cloud-APIs interagieren. Außerdem sollten Sie erfahren, wie Sie Ihre Service-Umgebung für die Bereitstellung von BlueXP und Cloud Volumes ONTAP konfigurieren.

Mit den VPC-Service-Kontrollen können Sie den Zugriff auf von Google gemanagte Services außerhalb einer vertrauenswürdigen Umgebung steuern, den Datenzugriff von nicht vertrauenswürdigen Standorten aus blockieren und die Risiken bei nicht autorisierten Datentransfers minimieren. ["Erfahren Sie mehr über Google Cloud VPC Service Controls"](#).

Kommunikation von NetApp Services mit VPC Service Controls

BlueXP 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 dem BlueXP Connector zugewiesenen internen Adresse ausgelöst.

Abhängig vom Bereitstellungsstil des Connectors müssen möglicherweise bestimmte Ausnahmen für Ihren Service-Umfang gemacht werden.

Bilder

Sowohl Cloud Volumes ONTAP als auch BlueXP verwenden Images eines Projekts in GCP, das von NetApp gemanagt wird. Dies kann sich auf die Bereitstellung von BlueXP Connector und Cloud Volumes ONTAP auswirken, wenn Ihr Unternehmen über eine Richtlinie verfügt, die die Verwendung von Bildern blockiert, die nicht im Unternehmen gehostet werden.

Sie können einen Connector manuell mit Hilfe der manuellen Installationsmethode bereitstellen, aber Cloud Volumes ONTAP muss auch Bilder aus dem NetApp Projekt abrufen. Zur Bereitstellung eines Connectors und Cloud Volumes ONTAP müssen Sie eine Liste mit zulässigen Inhalten bereitstellen.

Bereitstellen eines Connectors

Der Benutzer, der einen Connector implementiert, muss in der Lage sein, auf ein Image zu verweisen, das im ProjectID `netapp-CloudManager` und der Projektnummer `14190056516` gehostet wird.

Implementierung von Cloud Volumes ONTAP

- Das BlueXP-Servicekonto muss ein im ProjectID `netapp-CloudManager` gehostetes Image und die Projektnummer `14190056516` aus dem Serviceprojekt referenzieren.
- Das Servicekonto für den Google APIs Service Agent muss auf ein Image verweisen, das im ProjectID `netapp-CloudManager` und die Projektnummer `14190056516` aus dem Serviceprojekt gehostet wird.

Im Folgenden sind Beispiele für Regeln aufgeführt, die für das Abrufen dieser Images an VPC-Service-Kontrollen nötig sind.

VPC-Service steuert Perimeterrichtlinien

Richtlinien erlauben Ausnahmen von den VPC Service Controls-Regelsätzen. Weitere Informationen über Richtlinien finden Sie auf der "[Dokumentation der GCP VPC Service Controls Policy](#)".

Um die Richtlinien festzulegen, die für BlueXP erforderlich sind, navigieren Sie zu Ihrem VPC Service Controls Perimeter in Ihrem Unternehmen und fügen Sie die folgenden Richtlinien hinzu. Die Felder sollten mit den Optionen übereinstimmen, die auf der Seite „VPC Service Controls Policy“ angegeben sind. Beachten Sie auch, dass **alle** Regeln erforderlich sind und die **ORDER** Parameter im Regelsatz verwendet werden sollen.

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
```

Für ausgehenden Datenverkehr

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



Die oben beschriebene Projektnummer gilt als das Projekt *netapp-CloudManager*, das von NetApp zur Speicherung von Bildern für den Connector und für Cloud Volumes ONTAP verwendet wird.

Erstellen eines Servicekontos für Daten-Tiering und Backups

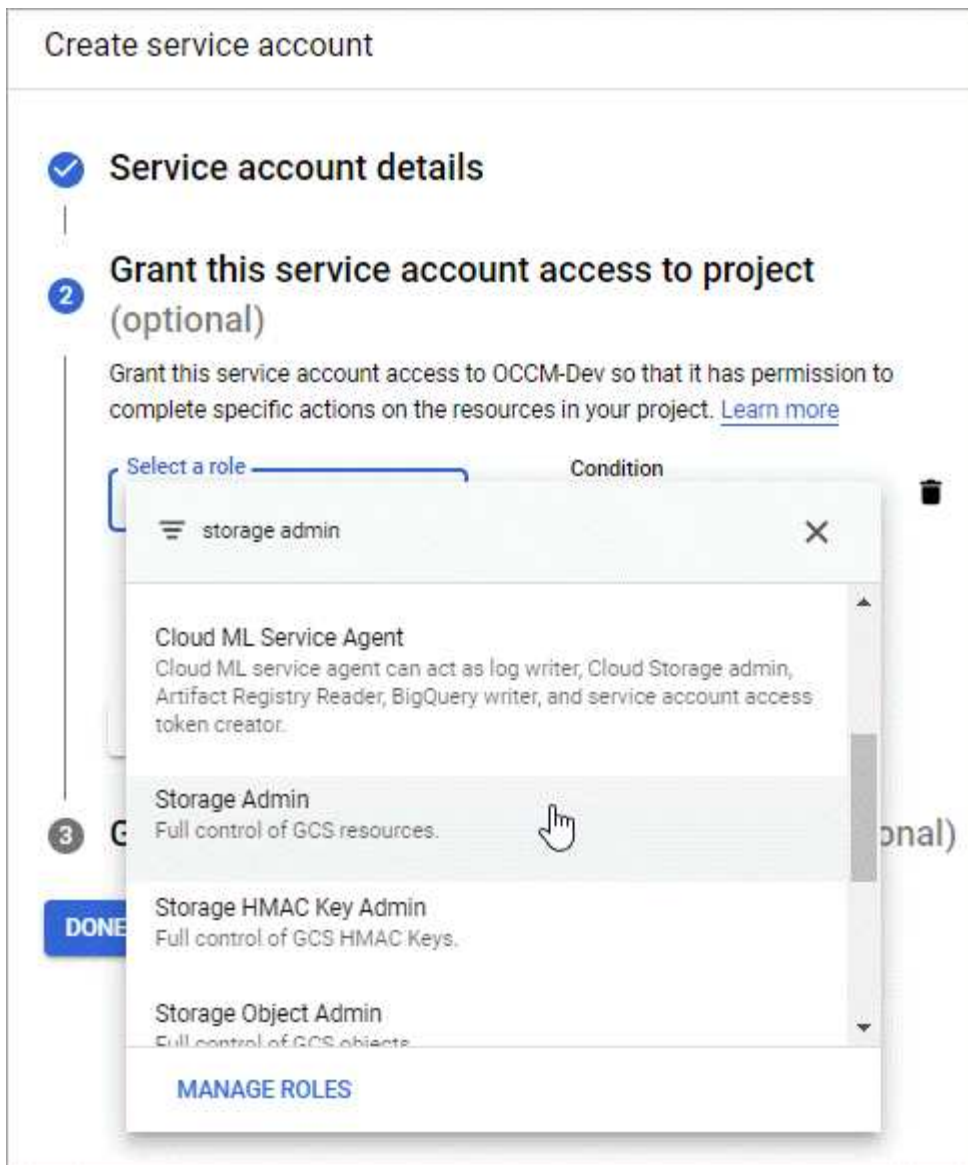
Für Cloud Volumes ONTAP ist ein Google Cloud-Servicekonto aus zwei Gründen erforderlich. Die erste lautet, wenn Sie aktivieren "[Daten-Tiering](#)" Tiering selten genutzter Daten auf kostengünstigen Objekt-Storage in Google Cloud. Die zweite lautet, wenn Sie den aktivieren "[BlueXP Backup und Recovery](#)" Um Volumes auf kostengünstigen Objekt-Storage zu sichern.

Cloud Volumes ONTAP verwendet das Service-Konto, um auf einen Bucket für Tiering-Daten und einen anderen Bucket für Backups zuzugreifen und diese zu verwalten.

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

Schritte

1. In der Google Cloud Konsole "[Rufen Sie die Seite Servicekonten auf](#)".
2. Wählen Sie Ihr Projekt aus.
3. Klicken Sie auf **Dienstkonto erstellen** und geben Sie die erforderlichen Informationen ein.
 - a. **Service Account Details:** Geben Sie einen Namen und eine Beschreibung ein.
 - b. **Begeben Sie diesem Servicekonto Zugriff auf das Projekt:** Wählen Sie die Rolle **Storage Admin**.



- c. **Benutzern Zugriff auf dieses Servicekonto gewähren:** Fügen Sie das Connector Service-Konto als *Service Account User* zu diesem neuen Service-Konto hinzu.

Dieser Schritt ist nur für das Daten-Tiering erforderlich. Sie ist für Backup und Recovery von BlueXP nicht erforderlich.

Create service account

- ✓ Service account details
- ✓ Grant this service account access to project (optional)
- 3 Grant users access to this service account (optional)
Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role

Grant users the permission to administer this service account

DONE CANCEL

Was kommt als Nächstes?

Sie müssen das Servicekonto später auswählen, wenn Sie eine Cloud Volumes ONTAP Arbeitsumgebung erstellen.

Details and Credentials

default-project Google Cloud Project	gcp-sub2 Marketplace Subscription	<div style="border: 1px solid #0070c0; padding: 2px 5px; display: inline-block;">Edit Project</div>
---	--------------------------------------	---

Details

Working Environment Name (Cluster Name)

Service Account

Service Account Name

+ Add Labels Optional Field | Up to four labels

Credentials

User Name

Password

Confirm Password

Nutzung von vom Kunden gemanagten Schlüsseln mit Cloud Volumes ONTAP

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

Schritte

1. Stellen Sie sicher, dass das Servicekonto BlueXP Connector im Projekt, in dem der Schlüssel gespeichert ist, über die entsprechenden Berechtigungen auf Projektebene verfügt.

Die Berechtigungen werden im bereitgestellt "[Standardmäßig sind die Berechtigungen für das Connector-Dienstkonto festgelegt](#)", Kann aber nicht angewendet werden, wenn Sie ein alternatives Projekt für den Cloud Key Management Service verwenden.

Folgende Berechtigungen stehen zur Auswahl:

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

2. Stellen Sie sicher, dass das Servicekonto für das ["Google Compute Engine Service Agent"](#) Hat Cloud KMS-Verschlüsselung/Dekrypter-Berechtigungen auf dem Schlüssel.

Der Name des Dienstkontos verwendet das folgende Format: "Service-[Service_project_number]@compute-system.iam.gserviceaccount.com".

["Google Cloud Documentation: IAM mit Cloud KMS nutzen - Rollenverteilung auf einer Ressource"](#)

3. Rufen Sie die „id“ des Schlüssels ab, indem Sie den Befehl get für das aufrufen `/gcp/vsa/metadata/gcp-encryption-keys` API-Anruf oder durch Auswahl des „Copy Resource Name“ auf dem Schlüssel in der GCP-Konsole.
4. Wenn Sie vom Kunden verwaltete Schlüssel und Tiering-Daten in Objekt-Storage verwenden, versucht BlueXP, dieselben Schlüssel zu verwenden, die zur Verschlüsselung der persistenten Festplatten verwendet werden. Zunächst müssen Sie Google Cloud Storage Buckets aktivieren, um die Schlüssel zu verwenden:
 - a. Suchen Sie den Google Cloud Storage Service Agent, indem Sie den folgenden folgen ["Google Cloud Documentation: Die Bereitstellung des Cloud Storage-Service-Agenten"](#).
 - b. Navigieren Sie zum Verschlüsselungsschlüssel und weisen Sie den Google Cloud Storage Service Agent mit Cloud KMS Verschlüsselungs-/Dekrypter-Berechtigungen zu.

Weitere Informationen finden Sie unter ["Google Cloud Documentation: Nutzung von vom Kunden gemanagten Verschlüsselungsschlüsseln"](#)

5. Verwenden Sie bei der Erstellung einer Arbeitsumgebung den Parameter „GcpEncryption“ in Verbindung mit Ihrer API-Anforderung.

Beispiel

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

Siehe ["BlueXP Automation Dokumentation"](#) Weitere Informationen zur Verwendung des Parameters „GcpEncryption“.

Lizenzierung für Cloud Volumes ONTAP in Google Cloud einrichten

Nachdem Sie sich für die Lizenzoption entschieden haben, die Sie mit Cloud Volumes ONTAP verwenden möchten, sind einige Schritte erforderlich, bevor Sie beim Erstellen einer neuen Arbeitsumgebung die Lizenzoption wählen können.

Freemium

Wählen Sie das Freemium-Angebot aus, 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 die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
 - a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um das Pay-as-you-go-Angebot im Google Cloud Marketplace zu abonnieren.

Sie werden über das Marketplace-Abonnement nicht belastet, es sei denn, Sie überschreiten 500 gib der bereitgestellten Kapazität. Zu dieser Zeit wird das System automatisch in das konvertiert "[Essentials-Paket](#)".

- b. Wenn Sie zu BlueXP zurückkehren, wählen Sie **Freemium**, wenn Sie die Seite mit den Lademethoden aufrufen.

Select Charging Method

<input type="radio"/>	Professional	By capacity	▼
<input type="radio"/>	Essential	By capacity	▼
<input checked="" type="radio"/>	Freemium (Up to 500 GiB)	By capacity	▼
<input type="radio"/>	Per Node	By node	▼

["Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Google Cloud zu starten"](#).

Kapazitätsbasierte Lizenz

Dank der kapazitätsbasierten Lizenzierung können Sie für Cloud Volumes ONTAP pro tib Kapazität bezahlen. Kapazitätsbasierte Lizenzierung ist in Form eines *package*, dem Essentials-Paket oder dem Professional-Paket verfügbar.

Die Essentials- und Professional-Pakete sind mit den folgenden Verbrauchsmodellen erhältlich:

- Eine Lizenz (BYOL) von NetApp erworben
- Ein stündliches PAYGO-Abonnement (Pay-as-you-go) über den Google Cloud Marketplace
- Einem Jahresvertrag

["Hier erhalten Sie weitere Informationen zur kapazitätsbasierten Lizenzierung"](#).

In den folgenden Abschnitten werden die ersten Schritte mit jedem dieser Nutzungsmodelle beschrieben.

BYOL

Bezahlen Sie vorab, indem Sie eine Lizenz (BYOL) von NetApp erwerben und Cloud Volumes ONTAP Systeme bei jedem Cloud-Provider implementieren.

Schritte

1. ["Wenden Sie sich an den NetApp Sales, um eine Lizenz zu erhalten"](#)
2. ["Fügen Sie Ihr Konto für die NetApp Support Website zu BlueXP hinzu"](#)

BlueXP fragt den NetApp Lizenzierungsservice automatisch ab, um Details zu den Lizenzen zu erhalten, die mit Ihrem NetApp Support Site Konto verknüpft sind. Sollte es keine Fehler geben, fügt BlueXP die Lizenzen automatisch zum Digital Wallet hinzu.

Bevor Sie Ihre Lizenz mit Cloud Volumes ONTAP verwenden können, muss sie über das Digital Wallet von BlueXP erhältlich sein. Wenn nötig, können Sie ["Fügen Sie die Lizenz manuell zum Digital Wallet von BlueXP hinzu"](#).

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

Die Lizenz, die Sie bei NetApp erworben haben, wird immer zuerst berechnet. Wenn Sie Ihre lizenzierte Kapazität überschreiten oder die Lizenzlaufzeit abgelaufen ist, werden Sie vom Stundensatz auf dem Markt in Rechnung gestellt.

- b. Wenn Sie zu BlueXP zurückkehren, wählen Sie ein kapazitätsbasiertes Paket aus, wenn Sie die Seite mit den Lademethoden aufrufen.

Select Charging Method	
<input checked="" type="radio"/> Professional	By capacity
<input type="radio"/> Essential	By capacity
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity
<input type="radio"/> Per Node	By node

["Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Google Cloud zu starten"](#).

PAYGO-Abonnement

Sie bezahlen stündlich, indem Sie sich für das Angebot über den Marketplace Ihres Cloud-Providers anmelden.

Wenn Sie eine Arbeitsumgebung von Cloud Volumes ONTAP erstellen, werden Sie von BlueXP aufgefordert, den Vertrag zu abonnieren, der im Google Cloud Marketplace verfügbar ist. Dieses Abonnement wird dann zur Verrechnung mit der Arbeitsumgebung verknüpft. Sie können das gleiche Abonnement auch für zusätzliche Arbeitsumgebungen nutzen.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
 - a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um das Pay-as-you-go-Angebot im Google Cloud Marketplace zu abonnieren.
 - b. Wenn Sie zu BlueXP zurückkehren, wählen Sie ein kapazitätsbasiertes Paket aus, wenn Sie die Seite mit den Lademethoden aufrufen.

The screenshot shows a 'Select Charging Method' dialog box with four rows. The first row is selected and has a blue 'By capacity' button. The other three rows have white 'By capacity' buttons. The last row has a purple 'By node' button.

Charging Method	Button
<input checked="" type="radio"/> Professional	By capacity
<input type="radio"/> Essential	By capacity
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity
<input type="radio"/> Per Node	By node

"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Google Cloud zu starten".



Sie können die mit Ihren Konten verbundenen Google Cloud Marketplace-Abonnements über die Seite Einstellungen > Anmeldeinformationen verwalten. ["So managen Sie Ihre Google Cloud-Anmeldedaten und -Abonnements"](#)

Jahresvertrag

Sie bezahlen jährlich für Cloud Volumes ONTAP durch den Kauf eines Jahresvertrags.

Schritte

1. Wenden Sie sich an Ihren NetApp Ansprechpartner, um einen Jahresvertrag zu erwerben.

Der Vertrag ist als *private* Angebot im Google Cloud Marketplace erhältlich.

Nachdem NetApp das private Angebot mit Ihnen geteilt hat, können Sie den Jahresplan auswählen, wenn Sie während der Erstellung der Arbeitsumgebung den Google Cloud Marketplace abonniert haben.

2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
 - a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die 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. Wenn Sie zu BlueXP zurückkehren, wählen Sie ein kapazitätsbasiertes Paket aus, wenn Sie die Seite mit den Lademethoden aufrufen.

Select Charging Method		
<input checked="" type="radio"/>	Professional	By capacity
<input type="radio"/>	Essential	By capacity
<input type="radio"/>	Freemium (Up to 500 GiB)	By capacity
<input type="radio"/>	Per Node	By node

"Sehen Sie sich [Schritt-für-Schritt-Anleitungen an](#), um Cloud Volumes ONTAP in Google Cloud zu starten".

Keystone Abonnement

Ein Keystone Abonnement ist ein nutzungsbasierter Abonnementservice. "[Weitere Informationen zu NetApp Keystone Abonnements](#)".

Schritte

1. Wenn Sie noch kein Abonnement haben, "[Kontakt zu NetApp](#)"
2. [Mailto:ng-keystone-success@netapp.com](mailto:ng-keystone-success@netapp.com)[NetApp kontaktieren]: Wir autorisieren Ihr BlueXP Benutzerkonto für eine oder mehrere Keystone Abonnements.
3. Nachdem NetApp den Account autorisiert hat, "[Verknüpfen Sie Ihre Abonnements für die Verwendung mit Cloud Volumes ONTAP](#)".
4. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.
 - a. Wählen Sie die Abrechnungsmethode für Keystone Abonnements aus, wenn Sie zur Auswahl einer Lademethode aufgefordert werden.

Select Charging Method

Keystone By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1
▼

Professional By capacity ▼

Essential By capacity ▼

Freemium (Up to 500 GiB) By capacity ▼

Per Node By node ▼

["Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Google Cloud zu starten"](#).

Cloud Volumes ONTAP in Google Cloud wird gestartet

Cloud Volumes ONTAP lässt sich in einer Single-Node-Konfiguration oder als HA-Paar in Google Cloud starten.

Bevor Sie beginnen

Um eine Arbeitsumgebung zu schaffen, benötigen Sie Folgendes.

- Ein Anschluss, der betriebsbereit ist.
 - Sie sollten ein haben ["Anschluss, der Ihrem Arbeitsbereich zugeordnet ist"](#).
 - ["Sie sollten darauf vorbereitet sein, den Konnektor jederzeit in Betrieb zu nehmen"](#).
 - Das mit dem Connector verbundene Servicekonto ["Sollte über die erforderlichen Berechtigungen verfügen"](#)
- Ein Verständnis der zu verwendenden Konfiguration.

Sie sollten sich darauf vorbereiten, indem Sie eine Konfiguration auswählen und die Netzwerkinformationen zu Google Cloud von Ihrem Administrator erhalten. Weitere Informationen finden Sie unter ["Planung Ihrer Cloud Volumes ONTAP Konfiguration"](#).

- Kenntnisse über die erforderlichen Voraussetzungen zur Einrichtung der Lizenzierung für Cloud Volumes

ONTAP.

["Erfahren Sie, wie Sie eine Lizenzierung einrichten"](#).

- Es sollten Google Cloud APIs sein ["In Ihrem Projekt aktiviert"](#):
 - Cloud Deployment Manager V2-API
 - Cloud-ProtokollierungsAPI
 - Cloud Resource Manager API
 - Compute Engine-API
 - IAM-API (Identitäts- und Zugriffsmanagement)

Starten eines Single-Node-Systems in Google Cloud


Schaffen Sie eine Arbeitsumgebung in BlueXP, um Cloud Volumes ONTAP in Google Cloud zu starten.

Schritte

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Bildschirmseite auf **Arbeitsumgebung 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, ["Einen Konnektor erstellen"](#).
5. **Details & Anmeldeinformationen:** Wählen Sie ein Projekt aus, geben Sie einen Cluster-Namen an, wählen Sie optional ein Servicekonto aus, fügen Sie optional Labels hinzu und geben Sie dann Anmeldeinformationen an.

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

Feld	Beschreibung
Name der Arbeitsumgebung	BlueXP verwendet den Namen der Arbeitsumgebung, um sowohl das Cloud Volumes ONTAP System als auch die Google Cloud VM Instanz zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.
Name Des Servicekontos	Wenn Sie Vorhaben zu verwenden "Daten-Tiering" Oder "BlueXP Backup und Recovery" Mit Cloud Volumes ONTAP müssen Sie dann Dienstkonto aktivieren und ein Servicekonto auswählen, das über die vordefinierte Rolle Speicheradministrator verfügt. "Erfahren Sie, wie Sie ein Servicekonto erstellen" .
Etiketten Hinzufügen	<p>Etiketten sind Metadaten für Ihre Google Cloud-Ressourcen. BlueXP fügt die Etiketten zum Cloud Volumes ONTAP-System und den dem System zugeordneten Google-Cloud-Ressourcen hinzu.</p> <p>Sie können bis zu vier Etiketten von der Benutzeroberfläche hinzufügen, wenn Sie eine Arbeitsumgebung erstellen, und dann können Sie weitere hinzufügen, nachdem sie erstellt wurde. Beachten Sie, dass Sie durch die API beim Erstellen einer Arbeitsumgebung nicht auf vier Labels beschränkt werden.</p> <p>Informationen zu Etiketten finden Sie unter "Google Cloud-Dokumentation: Ressourcen Zur Kennzeichnung".</p>

Feld	Beschreibung
Benutzername und Passwort	Dies sind die Anmeldeinformationen für das Cloud Volumes ONTAP Cluster-Administratorkonto. Sie können diese Anmeldedaten für die Verbindung mit Cloud Volumes ONTAP über System Manager oder dessen CLI verwenden. Behalten Sie den Standardbenutzernamen „ <i>admin</i> “ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Projekt Bearbeiten	<p>Wählen Sie das Projekt aus, in dem Cloud Volumes ONTAP gespeichert werden soll. Das Standardprojekt ist das Projekt, in dem sich BlueXP befindet.</p> <p>Wenn in der Dropdown-Liste keine weiteren Projekte angezeigt werden, haben Sie das BlueXP-Servicekonto noch nicht mit anderen Projekten verknüpft. Rufen Sie die Google Cloud-Konsole auf, öffnen Sie den IAM-Service und wählen Sie das Projekt aus. Fügen Sie dem Projekt das Servicekonto mit der Rolle BlueXP hinzu. Sie müssen diesen Schritt für jedes Projekt wiederholen.</p> <p> Dies ist das Servicekonto, das Sie für BlueXP eingerichtet haben. "Wie auf dieser Seite beschrieben".</p> <p>Klicken Sie auf Abonnement hinzufügen, um die ausgewählten Anmeldeinformationen einem Abonnement zuzuordnen.</p> <p>Um ein Pay-as-you-go Cloud Volumes ONTAP System zu erstellen, müssen Sie im Google Cloud Marketplace ein Google Cloud-Projekt auswählen, das mit einem Abonnement für Cloud Volumes ONTAP verknüpft ist.</p>

Im folgenden Video wird gezeigt, wie Sie Ihrem Google Cloud-Projekt ein Pay-as-you-go Marketplace-Abonnement zuordnen. Sie können auch die Schritte befolgen, um sich im anzumelden "[Verknüpfen eines Marketplace-Abonnements mit Google Cloud-Anmeldedaten](#)" Abschnitt.

► https://docs.netapp.com/de-de/test//media/video_subscribing_gcp.mp4 (video)

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



Wenn SIE WORM und Daten-Tiering nutzen möchten, müssen Sie BlueXP Backup und Recovery deaktivieren und eine Cloud Volumes ONTAP Arbeitsumgebung mit Version 9.8 oder höher implementieren.

- Standort & Konnektivität:** Wählen Sie einen Speicherort, wählen Sie eine Firewall-Richtlinie und bestätigen Sie die Netzwerkverbindung mit Google Cloud Speicher für Daten-Tiering.

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

Feld	Beschreibung
Konnektivitätsprüfung	Für das Tiering selten genutzter Daten auf einen Google Cloud Storage-Bucket muss das Subnetz, in dem Cloud Volumes ONTAP residiert, für privaten Google Zugriff konfiguriert sein. Anweisungen finden Sie unter " Google Cloud Documentation: Configuring Private Google Access ".

Feld	Beschreibung
Generierte Firewallrichtlinie	<p>Wenn Sie BlueXP die Firewall-Richtlinie für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen:</p> <ul style="list-style-type: none"> • Wenn Sie Selected VPC Only wählen, ist der Quellfilter für eingehenden Datenverkehr der Subnetz-Bereich des ausgewählten VPC und der Subnetz-Bereich des VPC, in dem sich der Connector befindet. Dies ist die empfohlene Option. • Wenn Sie Alle VPCs wählen, ist der Quellfilter für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene Firewallrichtlinie verwenden	<p>Wenn Sie eine vorhandene Firewallrichtlinie verwenden, stellen Sie sicher, dass diese die erforderlichen Regeln enthält. Link: Learn über Firewall-Regeln für Cloud Volumes ONTAP.</p>

8. **Charging Methods and NSS Account:** Geben Sie an, welche Ladungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site Konto an.

- ["Informieren Sie sich über Lizenzoptionen für Cloud Volumes ONTAP"](#).
- ["Erfahren Sie, wie Sie eine Lizenzierung einrichten"](#).

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

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

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



Wenn für die ausgewählte Version eine neuere Version von Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert BlueXP das System auf diese Version, wenn die Arbeitsumgebung erstellt wird. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.10.1 und 9.10.1 P4 auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.6 bis 9.7.

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

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

Die Festplattengröße ist für alle Festplatten im ursprünglichen Aggregat und für alle zusätzlichen Aggregate bestimmt, die BlueXP erzeugt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuweisungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

Hilfe bei der Auswahl von Festplattentyp und -Größe finden Sie unter ["Dimensionieren Sie Ihr System in Google Cloud"](#).

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

- Aktivieren Sie **Flash Cache**, falls gewünscht.



Ab Cloud Volumes ONTAP 9.13.1 wird *Flash Cache* auf den Instanztypen n2-Standard-16, n2-Standard-32, n2-Standard-48 und n2-Standard-64 unterstützt. Sie können Flash Cache nach der Bereitstellung nicht deaktivieren.

b. Wählen Sie bei Bedarf * Normal* oder **High** Schreibgeschwindigkeit.

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



Über die Option **High Write Speed** stehen eine hohe Schreibgeschwindigkeit und eine höhere maximale Übertragungseinheit (MTU) von 8,896 Byte zur Verfügung. Darüber hinaus erfordert die höhere MTU von 8,896 die Auswahl von VPC-1, VPC-2 und VPC-3 für die Implementierung. Weitere Informationen zu VPC-1, VPC-2 und VPC-3 finden Sie unter ["Regeln für VPC-1, VPC-2 und VPC-3"](#).

c. Aktivieren Sie auf Wunsch den WORM-Storage (Write Once, Read Many).

WORM kann nicht aktiviert werden, wenn Daten-Tiering für Cloud Volumes ONTAP-Versionen 9.7 und darunter aktiviert wurde. Ein Wechsel- oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach Aktivierung VON WORM und Tiering gesperrt.

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

a. Wenn Sie DEN WORM-Speicher aktivieren, wählen Sie den Aufbewahrungszeitraum aus.

13. **Daten-Tiering in Google Cloud Platform:** Wählen Sie, ob Daten-Tiering auf dem ursprünglichen Aggregat aktiviert werden soll, wählen Sie eine Speicherklasse für die Tiered Data aus und wählen Sie dann entweder ein Servicekonto mit der vordefinierten Storage Admin-Rolle aus (erforderlich für Cloud Volumes ONTAP 9.7 oder höher), Oder wählen Sie ein Google Cloud Konto aus (erforderlich für Cloud Volumes ONTAP 9.6).

Beachten Sie Folgendes:

- BlueXP legt das Servicekonto auf der Cloud Volumes ONTAP-Instanz fest. Dieses Servicekonto bietet Berechtigungen für Daten-Tiering zu einem Google Cloud Storage Bucket. Stellen Sie sicher, dass Sie das Connector-Dienstkonto als Benutzer des Tiering-Dienstkontos hinzufügen, andernfalls können Sie es nicht in BlueXP auswählen
- 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 eine bestimmte Volume-Tiering-Richtlinie auswählen, wenn Sie ein Volume erstellen oder bearbeiten.
- Wenn Sie das Daten-Tiering deaktivieren, können Sie es bei nachfolgenden Aggregaten aktivieren. Sie müssen das System jedoch deaktivieren und ein Service-Konto über die Google Cloud Konsole hinzufügen.

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

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

["Hier erhalten Sie Informationen zu den unterstützten Client-Protokollen und -Versionen"](#).

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

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren, wodurch Sie ein Volume erstellen können, das größer ist als der derzeit verfügbare physische Storage.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt BlueXP einen Wert ein, der Zugriff auf alle Instanzen im Subnetz bietet.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch Zugriffssteuerungslisten oder ACLs genannt). Sie können lokale oder domänenbasierte Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Domain-Windows-Benutzernamen angeben, müssen Sie die Domäne des Benutzers mit dem Format Domain\Benutzername einschließen.
Snapshot-Richtlinie	Eine Snapshot Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot Kopien an. Bei einer NetApp Snapshot Kopie handelt es sich um ein zeitpunktgenaues Filesystem Image, das keine Performance-Einbußen aufweist und minimalen Storage erfordert. Sie können die Standardrichtlinie oder keine auswählen. Sie können keine für transiente Daten auswählen, z. B. tempdb für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume: Entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	<p>ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert.</p> <p>Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben.</p> <p>ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert.</p> <p>Wenn Sie ein iSCSI-Volume erstellen, erstellt BlueXP automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Nachdem Sie das Volume erstellt haben, "Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen".</p>

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

Volume Details, Protection & Protocol

Details & Protection	Protocol
<p>Volume Name: <input style="width: 80%;" type="text" value="vol"/> Size (GB): <input style="width: 50%;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 80%;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> NFS iSCSI </p> <p>Share name: <input style="width: 80%;" type="text" value="vol_share"/> Permissions: <input style="width: 80%;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 80%;" type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>

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

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	<p>Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen.</p> <p>Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.</p> <p>Wenn Sie Google Managed Active Directory konfigurieren, kann standardmäßig mit der IP-Adresse 169.254.169.254 auf AD zugegriffen werden.</p>
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	<p>Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers.</p> <p>Um von Google verwaltete Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in diesem Feld OU=Computer,OU=Cloud ein.</p> <p>"Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD"</p>
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.

Feld	Beschreibung
NTP-Server	<p>Wählen Sie Active Directory-Domäne verwenden aus, um einen NTP-Server mit Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Siehe "BlueXP Automation Dokumentation" Entsprechende Details.</p> <p>Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Er ist nicht konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.</p>

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

Weitere Informationen finden Sie unter "[Wählen Sie ein Volume-Auslastungsprofil aus](#)" Und "[Data Tiering - Übersicht](#)".

17. **Überprüfen & Genehmigen:** Überprüfen und bestätigen Sie Ihre Auswahl.
- Überprüfen Sie die Details zur Konfiguration.
 - Klicken Sie auf **Weitere Informationen**, um weitere Informationen zum Support und den Google Cloud-Ressourcen zu erhalten, die BlueXP kaufen wird.
 - Aktivieren Sie die Kontrollkästchen **Ich verstehe...**
 - Klicken Sie Auf **Go**.

Ergebnis

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

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

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

Nachdem Sie fertig sind

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

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

Starten eines HA-Paars in Google Cloud

Schaffen Sie eine Arbeitsumgebung in BlueXP, um Cloud Volumes ONTAP in Google Cloud zu starten.


Schritte

- Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
- Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.

3. **Wählen Sie einen Standort:** Wählen Sie **Google Cloud** und **Cloud Volumes ONTAP HA**.
4. **Details & Anmeldeinformationen:** Wählen Sie ein Projekt aus, geben Sie einen Cluster-Namen an, wählen Sie optional ein Servicekonto aus, fügen Sie optional Labels hinzu und geben Sie dann Anmeldeinformationen an.

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

Feld	Beschreibung
Name der Arbeitsumgebung	BlueXP verwendet den Namen der Arbeitsumgebung, um sowohl das Cloud Volumes ONTAP System als auch die Google Cloud VM Instanz zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.
Name Des Servicekontos	Wenn Sie die verwenden möchten " BlueXP Tiering " Oder " BlueXP Backup und Recovery " Services. Sie müssen den Schalter Service-Konto aktivieren und dann das Servicekonto auswählen, das die vordefinierte Rolle Storage-Admin hat.
Etiketten Hinzufügen	<p>Etiketten sind Metadaten für Ihre Google Cloud-Ressourcen. BlueXP fügt die Etiketten zum Cloud Volumes ONTAP-System und den dem System zugeordneten Google-Cloud-Ressourcen hinzu.</p> <p>Sie können bis zu vier Etiketten von der Benutzeroberfläche hinzufügen, wenn Sie eine Arbeitsumgebung erstellen, und dann können Sie weitere hinzufügen, nachdem sie erstellt wurde. Beachten Sie, dass Sie durch die API beim Erstellen einer Arbeitsumgebung nicht auf vier Labels beschränkt werden.</p> <p>Informationen zu Etiketten finden Sie unter "Google Cloud-Dokumentation: Ressourcen Zur Kennzeichnung".</p>
Benutzername und Passwort	Dies sind die Anmeldeinformationen für das Cloud Volumes ONTAP Cluster-Administratorkonto. Sie können diese Anmeldedaten für die Verbindung mit Cloud Volumes ONTAP über System Manager oder dessen CLI verwenden. Behalten Sie den Standardbenutzernamen „ <i>admin</i> “ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.

Feld	Beschreibung
Projekt Bearbeiten	<p>Wählen Sie das Projekt aus, in dem Cloud Volumes ONTAP gespeichert werden soll. Das Standardprojekt ist das Projekt, in dem sich BlueXP befindet.</p> <p>Wenn in der Dropdown-Liste keine weiteren Projekte angezeigt werden, haben Sie das BlueXP-Servicekonto noch nicht mit anderen Projekten verknüpft. Rufen Sie die Google Cloud-Konsole auf, öffnen Sie den IAM-Service und wählen Sie das Projekt aus. Fügen Sie dem Projekt das Servicekonto mit der Rolle BlueXP hinzu. Sie müssen diesen Schritt für jedes Projekt wiederholen.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  Dies ist das Servicekonto, das Sie für BlueXP eingerichtet haben. "Wie auf dieser Seite beschrieben". </div> <p>Klicken Sie auf Abonnement hinzufügen, um die ausgewählten Anmeldeinformationen einem Abonnement zuzuordnen.</p> <p>Um ein Pay-as-you-go Cloud Volumes ONTAP System zu erstellen, müssen Sie im Google Cloud Marketplace ein Google Cloud-Projekt auswählen, das mit einem Abonnement für Cloud Volumes ONTAP verknüpft ist.</p>

Im folgenden Video wird gezeigt, wie Sie Ihrem Google Cloud-Projekt ein Pay-as-you-go Marketplace-Abonnement zuordnen. Sie können auch die Schritte befolgen, um sich im anzumelden "[Verknüpfen eines Marketplace-Abonnements mit Google Cloud-Anmeldedaten](#)" Abschnitt.

► https://docs.netapp.com/de-de/test//media/video_subscribing_gcp.mp4 (video)

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



Wenn SIE WORM und Daten-Tiering nutzen möchten, müssen Sie BlueXP Backup und Recovery deaktivieren und eine Cloud Volumes ONTAP Arbeitsumgebung mit Version 9.8 oder höher implementieren.

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

["Weitere Informationen zu den HA-Implementierungsmodellen"](#).

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

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

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

Feld	Beschreibung
Generierte Richtlinie	<p>Wenn Sie BlueXP die Firewall-Richtlinie für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen:</p> <ul style="list-style-type: none"> • Wenn Sie Selected VPC Only wählen, ist der Quellfilter für eingehenden Datenverkehr der Subnetz-Bereich des ausgewählten VPC und der Subnetz-Bereich des VPC, in dem sich der Connector befindet. Dies ist die empfohlene Option. • Wenn Sie Alle VPCs wählen, ist der Quellfilter für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Verwenden Sie vorhandene	<p>Wenn Sie eine vorhandene Firewallrichtlinie verwenden, stellen Sie sicher, dass diese die erforderlichen Regeln enthält. "Informieren Sie sich über die Firewall-Regeln für Cloud Volumes ONTAP".</p>

8. **Charging Methods and NSS Account:** Geben Sie an, welche Ladungsoption Sie mit diesem System verwenden möchten, und geben Sie dann ein NetApp Support Site Konto an.

- ["Informieren Sie sich über Lizenzoptionen für Cloud Volumes ONTAP"](#).
- ["Erfahren Sie, wie Sie eine Lizenzierung einrichten"](#).

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

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

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



Wenn für die ausgewählte Version eine neuere Version von Release Candidate, General Availability oder Patch Release verfügbar ist, aktualisiert BlueXP das System auf diese Version, wenn die Arbeitsumgebung erstellt wird. Das Update erfolgt beispielsweise, wenn Sie Cloud Volumes ONTAP 9.10.1 und 9.10.1 P4 auswählen. Das Update erfolgt nicht von einem Release zum anderen, z. B. von 9.6 bis 9.7.

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

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

Die Festplattengröße ist für alle Festplatten im ursprünglichen Aggregat und für alle zusätzlichen Aggregate bestimmt, die BlueXP erzeugt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuweisungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.

Hilfe bei der Auswahl von Festplattentyp und -Größe finden Sie unter ["Dimensionieren Sie Ihr System in Google Cloud"](#).

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

- a. Aktivieren Sie **Flash Cache**, falls gewünscht.



Ab Cloud Volumes ONTAP 9.13.1 wird *Flash Cache* auf den Instanztypen n2-Standard-16, n2-Standard-32, n2-Standard-48 und n2-Standard-64 unterstützt. Sie können Flash Cache nach der Bereitstellung nicht deaktivieren.

b. Wählen Sie bei Bedarf * Normal* oder **High** Schreibgeschwindigkeit.

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



Hohe Schreibgeschwindigkeit und eine höhere maximale Übertragungseinheit (MTU) von 8,896 Byte sind über die Option **High Write Speed** mit den Instanztypen 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 Implementierung. Hohe Schreibgeschwindigkeit und eine MTU von 8,896 sind funktionsabhängig und können nicht einzeln innerhalb einer konfigurierten Instanz deaktiviert werden. Weitere Informationen zu VPC-1, VPC-2 und VPC-3 finden Sie unter ["Regeln für VPC-1, VPC-2 und VPC-3"](#).

c. Aktivieren Sie auf Wunsch den WORM-Storage (Write Once, Read Many).

WORM kann nicht aktiviert werden, wenn Daten-Tiering für Cloud Volumes ONTAP-Versionen 9.7 und darunter aktiviert wurde. Ein Wechsel- oder Downgrade auf Cloud Volumes ONTAP 9.8 ist nach Aktivierung VON WORM und Tiering gesperrt.

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

a. Wenn Sie DEN WORM-Speicher aktivieren, wählen Sie den Aufbewahrungszeitraum aus.

13. **Daten-Tiering in Google Cloud:** Wählen Sie, ob Daten-Tiering auf dem ursprünglichen Aggregat aktiviert werden soll, wählen Sie eine Speicherklasse für die Tiered-Daten und wählen Sie dann ein Service-Konto aus, das die vordefinierte Storage Admin-Rolle hat.

Beachten Sie Folgendes:

- BlueXP legt das Servicekonto auf der Cloud Volumes ONTAP-Instanz fest. Dieses Servicekonto bietet Berechtigungen für Daten-Tiering zu einem Google Cloud Storage Bucket. Stellen Sie sicher, dass Sie das Connector-Dienstkonto als Benutzer des Tiering-Dienstkontos hinzufügen, andernfalls können Sie es nicht in BlueXP auswählen.
- Sie können eine bestimmte Volume-Tiering-Richtlinie auswählen, wenn Sie ein Volume erstellen oder bearbeiten.
- Wenn Sie das Daten-Tiering deaktivieren, können Sie es bei nachfolgenden Aggregaten aktivieren. Sie müssen das System jedoch deaktivieren und ein Service-Konto über die Google Cloud Konsole hinzufügen.

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

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

["Hier erhalten Sie Informationen zu den unterstützten Client-Protokollen und -Versionen"](#).

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

Feld	Beschreibung
Größe	Die maximale Größe, die Sie eingeben können, hängt weitgehend davon ab, ob Sie Thin Provisioning aktivieren, wodurch Sie ein Volume erstellen können, das größer ist als der derzeit verfügbare physische Storage.
Zugriffskontrolle (nur für NFS)	Eine Exportrichtlinie definiert die Clients im Subnetz, die auf das Volume zugreifen können. Standardmäßig gibt BlueXP einen Wert ein, der Zugriff auf alle Instanzen im Subnetz bietet.
Berechtigungen und Benutzer/Gruppen (nur für CIFS)	Mit diesen Feldern können Sie die Zugriffsebene auf eine Freigabe für Benutzer und Gruppen steuern (auch Zugriffssteuerungslisten oder ACLs genannt). Sie können lokale oder domänenbasierte Windows-Benutzer oder -Gruppen oder UNIX-Benutzer oder -Gruppen angeben. Wenn Sie einen Domain-Windows-Benutzernamen angeben, müssen Sie die Domäne des Benutzers mit dem Format Domain\Benutzername einschließen.
Snapshot-Richtlinie	Eine Snapshot Kopierrichtlinie gibt die Häufigkeit und Anzahl der automatisch erstellten NetApp Snapshot Kopien an. Bei einer NetApp Snapshot Kopie handelt es sich um ein zeitpunktgenaues Filesystem Image, das keine Performance-Einbußen aufweist und minimalen Storage erfordert. Sie können die Standardrichtlinie oder keine auswählen. Sie können keine für transiente Daten auswählen, z. B. tempdb für Microsoft SQL Server.
Erweiterte Optionen (nur für NFS)	Wählen Sie eine NFS-Version für das Volume: Entweder NFSv3 oder NFSv4.
Initiatorgruppe und IQN (nur für iSCSI)	<p>ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert.</p> <p>Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatorgruppen Zugriff auf welche LUNs haben.</p> <p>ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert.</p> <p>Wenn Sie ein iSCSI-Volume erstellen, erstellt BlueXP automatisch eine LUN für Sie. Wir haben es einfach gemacht, indem wir nur eine LUN pro Volumen erstellen, so gibt es keine Verwaltung beteiligt. Nachdem Sie das Volume erstellt haben, "Verwenden Sie den IQN, um von den Hosts eine Verbindung zur LUN herzustellen".</p>

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

Volume Details, Protection & Protocol

Details & Protection	Protocol
<p>Volume Name: <input style="width: 200px;" type="text" value="vol"/> Size (GB): <input style="width: 80px;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 300px;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> <input type="radio"/> NFS <input checked="" type="radio"/> CIFS <input type="radio"/> iSCSI </p> <hr/> <p>Share name: <input style="width: 150px;" type="text" value="vol_share"/> Permissions: <input style="width: 150px;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 300px;" type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>

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

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	<p>Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.</p> <p>Wenn Sie Google Managed Active Directory konfigurieren, kann standardmäßig mit der IP-Adresse 169.254.169.254 auf AD zugegriffen werden.</p>
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	<p>Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers.</p> <p>Um von Google verwaltete Microsoft AD als AD-Server für Cloud Volumes ONTAP zu konfigurieren, geben Sie in diesem Feld OU=Computer,OU=Cloud ein.</p> <p>"Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD"</p>
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.

Feld	Beschreibung
NTP-Server	<p>Wählen Sie Active Directory-Domäne verwenden aus, um einen NTP-Server mit Active Directory-DNS zu konfigurieren. Wenn Sie einen NTP-Server mit einer anderen Adresse konfigurieren müssen, sollten Sie die API verwenden. Siehe "BlueXP Automation Dokumentation" Entsprechende Details.</p> <p>Beachten Sie, dass Sie einen NTP-Server nur beim Erstellen eines CIFS-Servers konfigurieren können. Er ist nicht konfigurierbar, nachdem Sie den CIFS-Server erstellt haben.</p>

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

Weitere Informationen finden Sie unter "[Wählen Sie ein Volume-Auslastungsprofil aus](#)" Und "[Data Tiering - Übersicht](#)".

17. **Überprüfen & Genehmigen:** Überprüfen und bestätigen Sie Ihre Auswahl.
- Überprüfen Sie die Details zur Konfiguration.
 - Klicken Sie auf **Weitere Informationen**, um weitere Informationen zum Support und den Google Cloud-Ressourcen zu erhalten, die BlueXP kaufen wird.
 - Aktivieren Sie die Kontrollkästchen **Ich verstehe...**
 - Klicken Sie Auf **Go**.

Ergebnis

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

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

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

Nachdem Sie fertig sind

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

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

Bildüberprüfung Der Google Cloud Platform

Google Cloud Bild Verifizierung Überblick

Die Google Cloud Image-Verifizierung erfüllt erweiterte NetApp Sicherheitsanforderungen. Es wurden Änderungen am Skript vorgenommen, das die Bilder generiert, um das Bild unterwegs mit privaten Schlüsseln zu signieren, die speziell für diese Aufgabe generiert wurden. Sie können die Integrität des GCP-Images mit dem

signierten Digest und öffentlichen Zertifikat für Google Cloud überprüfen, das über heruntergeladen werden kann ["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 Bild in RAW-Format auf Google Cloud

Das Image, das zur Bereitstellung neuer Instanzen, Upgrades oder zur Verwendung in vorhandenen Images verwendet wird, wird über mit den Clients geteilt ["Die NetApp Support Site \(NSS\)"](#). Der signierte Digest und die Zertifikate können über das NSS-Portal heruntergeladen werden. Laden Sie unbedingt die Digest und Zertifikate für die rechte Version herunter, die dem von NetApp Support geteilten Image entspricht. 9.13.0 Bilder verfügen beispielsweise über einen 9.13.0 signierten Digest und Zertifikate, die auf NSS verfügbar sind.

Warum ist dieser Schritt erforderlich?

Die Bilder von Google Cloud können nicht direkt heruntergeladen werden. Um das Bild mit dem signierten Digest und den Zertifikaten vergleichen zu können, benötigen Sie einen Mechanismus, um die beiden Dateien zu vergleichen und das Bild herunterzuladen. Dazu müssen Sie das Bild in ein Disk.RAW-Format exportieren/konvertieren und die Ergebnisse in einem Storage-Bucket auf Google Cloud speichern. Die Datei Disk.RAW wird getarbt und gzippt.

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

- Zugriff auf Google Storage-Bucket
- In Google Storage-Bucket schreiben
- Erstellen von Cloud-Build-Jobs (während des Exportvorgangs verwendet)
- Zugriff auf das gewünschte Bild
- Erstellen Sie Aufgaben für Exportbilder

Um das Image zu überprüfen, muss es in ein Disk.RAW-Format konvertiert und anschließend heruntergeladen werden.

Verwenden Sie die Google Cloud-Befehlszeile, um Google Cloud-Bild zu exportieren

Die bevorzugte Methode zum Exportieren eines Bildes in Cloud Storage ist die Verwendung von ["Exportbefehl für gcloudCompute-Bilder"](#). Dieser Befehl nimmt das bereitgestellte Image und konvertiert es in eine Disk.RAW-Datei, die tarred und gzippt wird. Die generierte Datei wird unter der Ziel-URL gespeichert und kann zur Überprüfung heruntergeladen werden.

Der Benutzer/das Konto muss über Berechtigungen verfügen, um auf den gewünschten Bucket zuzugreifen und in diesen zu schreiben, das Bild zu exportieren und Cloud-Builds (die von Google zum Exportieren des Bildes verwendet werden) zu erstellen, um diesen Vorgang auszuführen.

Export Google Cloud Bild mit gcloud

Klicken Sie auf, um das Skript 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/xxxxxxxxxxxxx].  
Logs are available at [https://console.cloud.google.com/cloud-  
build/builds;region=us-central1/xxxxxxxxxxxxx?project=xxxxxxxxxxxxx].  
[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
```

Extrahiere gezippte Dateien

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



Siehe "[Google Cloud-Dokument beim Exportieren eines Bildes](#)" Weitere Informationen zum Exportieren von Bildern über Google Cloud.

Überprüfung der Bildsignatur

Verifizieren von durch Google Cloud signierten Bildern

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

Workflow-Zusammenfassung für die signierte Bildüberprüfung

Im Folgenden finden Sie eine Übersicht über den Workflow zur Verifizierung von Google Cloud signierten Bildern.

- Von "[NSS](#)", Laden Sie das Google Cloud-Archiv mit den folgenden Dateien herunter:
 - Signierter Digest (.SIG)
 - Zertifikat mit dem öffentlichen Schlüssel (.pem)
 - Zertifikatskette (.pem)

Cloud Volumes ONTAP 9.13.0

Date Posted:

Restrictions on Encryption Technology

NetApp Volume Encryption (available with ONTAP 9.1 and later releases) provides for data-at-rest encryption that requires authorizations, permits, or licenses to import, export, re-export or use this software.

A state license for importing encryption equipment is required to import ONTAP 9.1 (or later) with NetApp Volume Encryption into Member States of the Eurasian Economic Union: Russia, Belarus, Kazakhstan, Armenia and Kyrgyzstan. Moreover, in certain cases, an end-user customer must have a valid state encryption license to this software.

Consult your legal advisor on this matter.

Cloud Volumes ONTAP

Non-Restricted Countries

If you are upgrading to ONTAP 9.13.0, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

[DOWNLOAD 9130_V_IMAGE.TGZ \[2.58 GB\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_V_IMAGE.TGZ.PEM \[451 B\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_V_IMAGE.TGZ.SIG \[256 B\]](#)

[View and download checksums](#)

Cloud Volumes ONTAP

Restricted Countries

If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.

[DOWNLOAD 9130_V_NODAR_IMAGE.TGZ \[2.58 GB\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_V_NODAR_IMAGE.TGZ.PEM \[451 B\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_V_NODAR_IMAGE.TGZ.SIG \[256 B\]](#)

[View and download checksums](#)

Cloud Volumes ONTAP

Google Image Digest Files

[DOWNLOAD GCP-X-9-13-0_PKG.TAR.GZ \[7.52 KB\]](#)

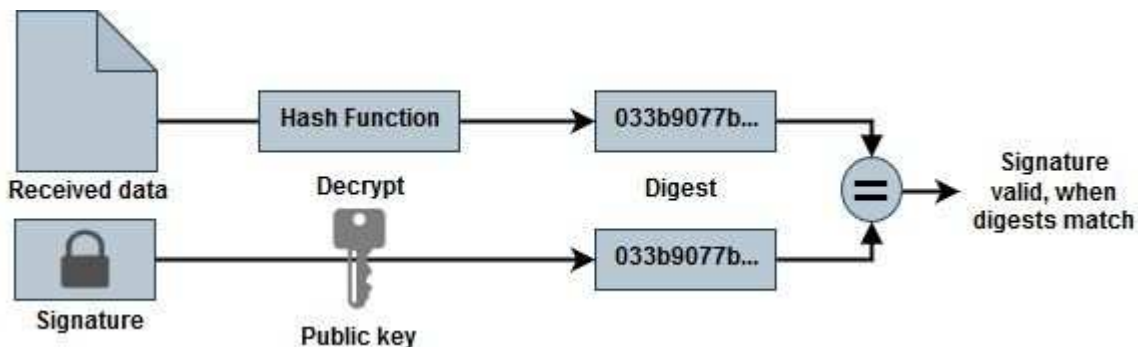
[View and download checksums](#)

Azure Image Digest File

[DOWNLOAD AZURE-9.13.0_PKG.TAR.GZ \[7.55 KB\]](#)

[View and download checksums](#)

- Laden Sie die konvertierte Datei Disk.RAW herunter
- Validieren Sie das Zertifikat mithilfe der Zertifikatskette
- Validieren Sie den signierten Digest mit dem Zertifikat, 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 Datei Disk.RAW
 - Vergleichen Sie die beiden Digest-Dateien zur Validierung



Überprüfung der Datei Disk.RAW und Digest Dateiinhalte mit OpenSSL

Sie können die heruntergeladene Datei „Disk.RAW“ von Google Cloud anhand der über den verfügbaren Inhalte der Digest-Datei überprüfen "NSS" OpenSSL verwenden.



Die OpenSSL-Befehle zur Validierung des Images sind mit Linux, Mac OS und Windows-Maschinen kompatibel.

Schritte

1. Überprüfen Sie das Zertifikat mit OpenSSL.

Klicken Sie auf, um das Skript 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-20230119-0XXXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXXX.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-20230119-0XXXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OSCP request for the certificate
$ openssl ocsf -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsf -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXXX.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-20230119-0XXXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

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

```
$ openssl ocspl -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: CE894F8251AA15A28462CA312361D261F8F8FE78

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 Zertifikate in ein Verzeichnis.
3. Extrahieren Sie den öffentlichen Schlüssel mit 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 auf, um das Skript 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
```

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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