Los geht's

Cloud Volumes ONTAP

NetApp
April 23, 2024

Inhalt

Los geht’s

Weitere Informationen zu Cloud Volumes ONTAP

Mit Cloud Volumes ONTAP können Sie Ihre Cloud Storage-Kosten und -Performance optimieren und gleichzeitig die Datensicherung, -Sicherheit und -Compliance verbessern.

Cloud Volumes ONTAP ist eine rein softwarebasierte Storage Appliance, auf der ONTAP Datenmanagement-Software in der Cloud ausgeführt wird. Das System bietet Storage der Enterprise-Klasse mit den folgenden wichtigen Funktionen:

- Storage-Effizienz

  Nutzen Sie integrierte Datendeduplizierung, Datenkomprimierung, Thin Provisioning und Klonen und minimieren Sie so die Storage-Kosten.

- Hochverfügbarkeit

  Zuverlässigkeit der Enterprise-Klasse und unterbrechungsfreien Betrieb bei Ausfällen in der Cloud-Umgebung sicherstellen.

- Datensicherung

  Cloud Volumes ONTAP nutzt SnapMirror, die branchenführende Replizierungstechnologie von NetApp, um On-Premises-Daten in der Cloud zu replizieren, sodass einfach sekundäre Kopien für diverse Anwendungsfälle verfügbar sind.

  Cloud Volumes ONTAP lässt sich auch in BlueXP Backup und Recovery integrieren, um Backup- und Restore-Funktionen zum Schutz und zur langfristigen Archivierung Ihrer Cloud-Daten zu bieten.

  "Erfahren Sie mehr über Backup und Recovery von BlueXP"

- Daten-Tiering

  Wechseln Sie nach Bedarf zwischen hochperformanten Storage Pools, ohne Applikationen offline zu schalten.

- Applikationskonsistenz

  Konsistenz von NetApp Snapshot Kopien mit NetApp SnapCenter sicherstellen.

  "Weitere Informationen zu SnapCenter"

- Datensicherheit

  Cloud Volumes ONTAP unterstützt die Datenverschlüsselung und bietet Schutz vor Viren und Ransomware.

- Kontrolloptionen für die Einhaltung des Datenschutzes

  Die Integration in die BlueXP Klassifizierung erleichtert Ihnen das Verständnis des Datenkontexts und die Identifizierung sensibler Daten.

  "Weitere Informationen zur BlueXP Klassifizierung"

Lizenzen für ONTAP Funktionen sind im Lieferumfang von Cloud Volumes ONTAP enthalten.

"Anzeigen der unterstützten Cloud Volumes ONTAP Konfigurationen"

"Erfahren Sie mehr über Cloud Volumes ONTAP"

Unterstützte Versionen für neue Bereitstellungen

Mit BlueXP können Sie bei der Erstellung einer neuen Cloud Volumes ONTAP-Arbeitsumgebung aus verschiedenen ONTAP-Versionen auswählen.

Alle anderen Cloud Volumes ONTAP-Versionen werden bei neuen Implementierungen nicht unterstützt.

AWS

Single Node

- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

HA-Paar

- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

- 9.7 P5
- 9.5 P6

Azure

Single Node

- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6
- 9.5 P6

HA-Paar

- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6

Google Cloud

Single Node

- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

HA-Paar

- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

Erste Schritte in Amazon Web Services

Schnellstart für Cloud Volumes ONTAP in AWS

Erste Schritte mit Cloud Volumes ONTAP in AWS

1 **Einen Konnektor erstellen**

Wenn Sie keine haben "Stecker" Dennoch muss ein Kontoadministrator einen erstellen. "Erfahren Sie, wie Sie in AWS einen Connector erstellen können"

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. "Weitere Informationen .".

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. 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.

3. Richten Sie einen VPC-Endpunkt für den S3-Dienst ein.

   Ein VPC-Endpunkt ist erforderlich, wenn Sie kalte Daten von Cloud Volumes ONTAP auf kostengünstigen Objekt-Storage einstufen möchten.

"Erfahren Sie mehr über Netzwerkanforderungen".

4 AWS KMS einrichten

Wenn Sie Amazon Verschlüsselung mit Cloud Volumes ONTAP verwenden möchten, müssen Sie sicherstellen, dass ein aktiver Kundenstammschlüssel (CMK) vorhanden ist. Außerdem müssen Sie die Schlüsselrichtlinie für jedes CMK ändern, indem Sie die IAM-Rolle hinzufügen, die dem Connector Berechtigungen als_Key-Benutzer_ bereitstellt. "Weitere Informationen .".

5 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"
- "Einführen eines Connectors über den AWS Marketplace"
- "Installieren der Connector-Software auf einem Linux-Host"
- "Was BlueXP mit AWS-Berechtigungen macht"

Planen Sie Ihre Cloud Volumes ONTAP-Konfiguration in AWS

Wenn Sie Cloud Volumes ONTAP in AWS 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 AWS Regionen unterstützt. "Hier finden Sie die vollständige Liste der unterstützten Regionen".

Neuere AWS Regionen müssen aktiviert sein, bevor Ressourcen in diesen Regionen erstellt und gemanagt werden können. "Erfahren Sie, wie Sie eine Region aktivieren".

Wählen Sie eine unterstützte Instanz aus

Cloud Volumes ONTAP unterstützt je nach gewähltem Lizenztyp mehrere Instanztypen.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in AWS"

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 AWS"

Größe des Systems in AWS

Mit der Dimensionierung Ihres Cloud Volumes ONTAP Systems können Sie die Anforderungen an Performance und Kapazität erfüllen. Bei der Auswahl eines Instanztyps, des Festplattentyp und der Festplattengröße sollten Sie einige wichtige Punkte beachten:

Instanztyp

- Stimmen Sie die Workload-Anforderungen dem maximalen Durchsatz und IOPS für jeden EC2-Instanztyp ab.
- Wenn mehrere Benutzer gleichzeitig auf das System schreiben, wählen Sie einen Instanztyp aus, der über genügend CPUs verfügt, um die Anforderungen zu verwalten.
- Wenn Sie eine Anwendung haben, die hauptsächlich liest, dann wählen Sie ein System mit genügend RAM.
  - "AWS Dokumentation: Amazon EC2 Instanztypen"
  - "AWS Dokumentation: Für Amazon EBS optimierte Instanzen"

EBS-Festplattentyp

Auf höherer Ebene unterscheiden sich die EBS-Festplattentypen wie folgt. Weitere Informationen zu den Anwendungsfällen für EBS-Festplatten finden Sie unter "AWS Dokumentation: EBS Volume-Typen".

- *General Purpose SSD (gp3)* Festplatten sind die kostengünstigsten SSDs, die ein ausgewogenes Verhältnis zwischen Kosten und Performance für ein breites Spektrum an Workloads bieten. Die Performance wird hinsichtlich IOPS und Durchsatz definiert. gp3-Festplatten werden von Cloud Volumes ONTAP 9.7 und höher unterstützt.

  Wenn Sie eine gp3-Festplatte auswählen, füllt BlueXP die Standard-IOPS- und Durchsatzwerte, die eine Performance liefern, die einer gp2-Festplatte entspricht, die auf der ausgewählten

Festplattengröße basiert. Sie können die Werte erhöhen, um eine bessere Leistung zu einem höheren Preis zu erhalten, aber wir unterstützen keine niedrigeren Werte, weil es zu einer minderwertigen Leistung führen kann. Kurz gesagt: Halten Sie bei den Standardwerten an, oder erhöhen Sie sie. Senken Sie Ihre Storage-Kosten nicht. "Erfahren Sie mehr über gp3-Festplatten und deren Leistung".

Beachten Sie, dass Cloud Volumes ONTAP die Funktion Amazon EBS Elastic Volumes mit gp3-Festplatten unterstützt. "Weitere Informationen zur Unterstützung von Elastic Volumes".

- *General Purpose SSD (gp2)* Festplatten ausgewogenes Verhältnis zwischen Kosten und Performance für ein breites Spektrum an Workloads. Die Performance wird in Bezug auf IOPS definiert.
- *Bereitgestellte IOPS-SSD (io1)* Festplatten sind für kritische Applikationen geeignet, die die höchste Performance zu höheren Kosten erfordern.

  Beachten Sie, dass Cloud Volumes ONTAP die elastische Amazon EBS Volumes-Funktion mit io1-Festplatten unterstützt. "Weitere Informationen zur Unterstützung von Elastic Volumes".

- *Throughput Optimized HDD (st1)* Festplatten sind für häufig abgerufene Workloads, die einen schnellen und konsistenten Durchsatz zu einem niedrigeren Preis erfordern.

  Bei der Verwendung von durchsatzoptimierten HDDs (st1) wird kein Tiering von Daten zu Objekt-Storage empfohlen.

EBS-Festplattengröße

Wenn Sie eine Konfiguration wählen, die das nicht unterstützt "Amazon EBS Elastic Volumes Funktion", Dann müssen Sie eine anfängliche Festplattengröße wählen, wenn Sie ein Cloud Volumes ONTAP-System starten. Danach können Sie "BlueXP verwaltet die Kapazität eines Systems für Sie", Aber wenn Sie wollen "Erstellen Sie Aggregate selbst", Verachten Sie auf folgende Punkte:

- Alle Festplatten in einem Aggregat müssen dieselbe Größe haben.
- Die Performance von EBS-Festplatten ist an die Festplattengröße gebunden. Die Größe bestimmt die IOPS-Basiswerte und die maximale Burst-Dauer für SSD-Festplatten sowie den Baseline- und Burst-Durchsatz für HDD-Festplatten.
- Am Ende sollten Sie die Festplattengröße wählen, die Ihnen die *dauerhafte Performance* bietet, die Sie benötigen.
- Auch wenn Sie größere Festplatten wählen (zum Beispiel sechs 4-tib-Festplatten), erhalten Sie möglicherweise nicht alle IOPS, da die EC2 Instanz ihr Bandbreitenlimit erreichen kann.

  Weitere Informationen zur Performance der EBS Festplatten finden Sie in "AWS Dokumentation: EBS Volume-Typen".

  Wie bereits erwähnt, wird die Auswahl einer Festplattengröße mit Cloud Volumes ONTAP-Konfigurationen, die die Elastic Volumes-Funktion von Amazon EBS unterstützen, nicht unterstützt. "Weitere Informationen zur Unterstützung von Elastic Volumes".

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 AWS an".

Für den Connector ist außerdem eine Systemfestplatte erforderlich. "Zeigen Sie Details zur Standardkonfiguration des Connectors an".

Bereiten Sie sich auf die Implementierung von Cloud Volumes ONTAP in einem AWS-Outpost vor

Wenn Sie einen AWS-Outpost haben, können Sie Cloud Volumes ONTAP in diesem Outpost implementieren, indem Sie die VPC-Outpost im Assistenten zur Arbeitsumgebung auswählen. Die Erfahrung ist mit jeder anderen VPC, die in AWS residiert. Beachten Sie, dass Sie zunächst einen Connector in Ihrem AWS Outpost implementieren müssen.

Es bestehen einige Einschränkungen, die darauf hinweisen:

- Derzeit werden nur Cloud Volumes ONTAP Systeme mit einzelnen Nodes unterstützt
- Die EC2 Instanzen, die Sie mit Cloud Volumes ONTAP verwenden können, sind auf die in Ihrem Outpost verfügbaren EC2-Instanzen beschränkt
- Derzeit werden nur General Purpose SSDs (gp2) unterstützt

Sammeln von Netzwerkinformationen

Wenn Sie Cloud Volumes ONTAP in AWS starten, müssen Sie Details zu Ihrem VPC-Netzwerk angeben. Sie können ein Arbeitsblatt verwenden, um die Informationen von Ihrem Administrator zu sammeln.

Single Node oder HA-Paar in einer einzelnen Verfügbarkeitszone

AWS-Informationen	Ihr Wert
Region	
VPC	
Subnetz	
Sicherheitsgruppe (wenn Sie Ihre eigene verwenden)	

HA-Paar in mehreren AZS

AWS-Informationen	Ihr Wert
Region	
VPC	
Sicherheitsgruppe (wenn Sie Ihre eigene verwenden)	
Verfügbarkeitszone von Node 1	
Subnetz von Node 1	
Verfügbarkeitszone von Node 2	
Subnetz von Node 2	
Mediator Verfügbarkeitszone	
Mediator Subnetz	

AWS-Informationen	Ihr Wert
Schlüsselpaar für den Vermittler	
Floating-IP-Adresse für Cluster-Management-Port	
Unverankerte IP-Adresse für Daten auf Node 1	
Unverankerte IP-Adresse für Daten auf Node 2	
Routing-Tabellen für unverankerte IP-Adressen	

Wählen Sie eine Schreibgeschwindigkeit

Mit BlueXP können Sie eine Schreibgeschwindigkeitseinstellung für Cloud Volumes ONTAP auswählen. 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.

Richten Sie Ihr Netzwerk ein

Netzwerkanforderungen für Cloud Volumes ONTAP in AWS

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

Allgemeine Anforderungen

Die folgenden Anforderungen müssen in AWS erfüllt sein.

Outbound-Internetzugang für Cloud Volumes ONTAP Nodes

Cloud Volumes ONTAP Nodes benötigen Outbound-Internetzugang für NetApp AutoSupport, 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 Sie über eine NAT-Instanz verfügen, müssen Sie eine eingehende Sicherheitsgruppenregel definieren, die HTTPS-Datenverkehr vom privaten Subnetz zum Internet zulässt.

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 Sicherheitsgruppe des Connectors *eingehende* -Verbindungen über Port 3128 zulässt. Nach der Bereitstellung des Connectors müssen Sie diesen Port öffnen.

Wenn Sie strenge ausgehende Regeln für Cloud Volumes ONTAP definiert haben, müssen Sie auch sicherstellen, dass die Cloud Volumes ONTAP-Sicherheitsgruppe *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 von BlueXP darüber informiert werden, dass AutoSupport-Meldungen nicht gesendet werden können, "Fehler bei der AutoSupport Konfiguration beheben".

Outbound-Internetzugang für den HA Mediator

Die HA-Mediatorinstanz muss über eine ausgehende Verbindung zum AWS EC2-Service verfügen, damit sie beim Storage-Failover unterstützt werden kann. Um die Verbindung bereitzustellen, können Sie eine öffentliche IP-Adresse hinzufügen, einen Proxyserver angeben oder eine manuelle Option verwenden.

Die manuelle Option kann ein NAT-Gateway oder ein VPC-Endpunkt der Schnittstelle vom Ziel-Subnetz zum AWS EC2-Dienst sein. Details zu VPC-Endpunkten finden Sie unter "AWS Dokumentation: Interface VPC Endpunkte (AWS PrivateLink)".

Private IP-Adressen

BlueXP weist Cloud Volumes ONTAP automatisch die erforderliche Anzahl privater IP-Adressen zu. Sie müssen sicherstellen, dass Ihrem Netzwerk genügend private IP-Adressen zur Verfügung stehen.

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.

IP-Adressen für ein Single Node-System

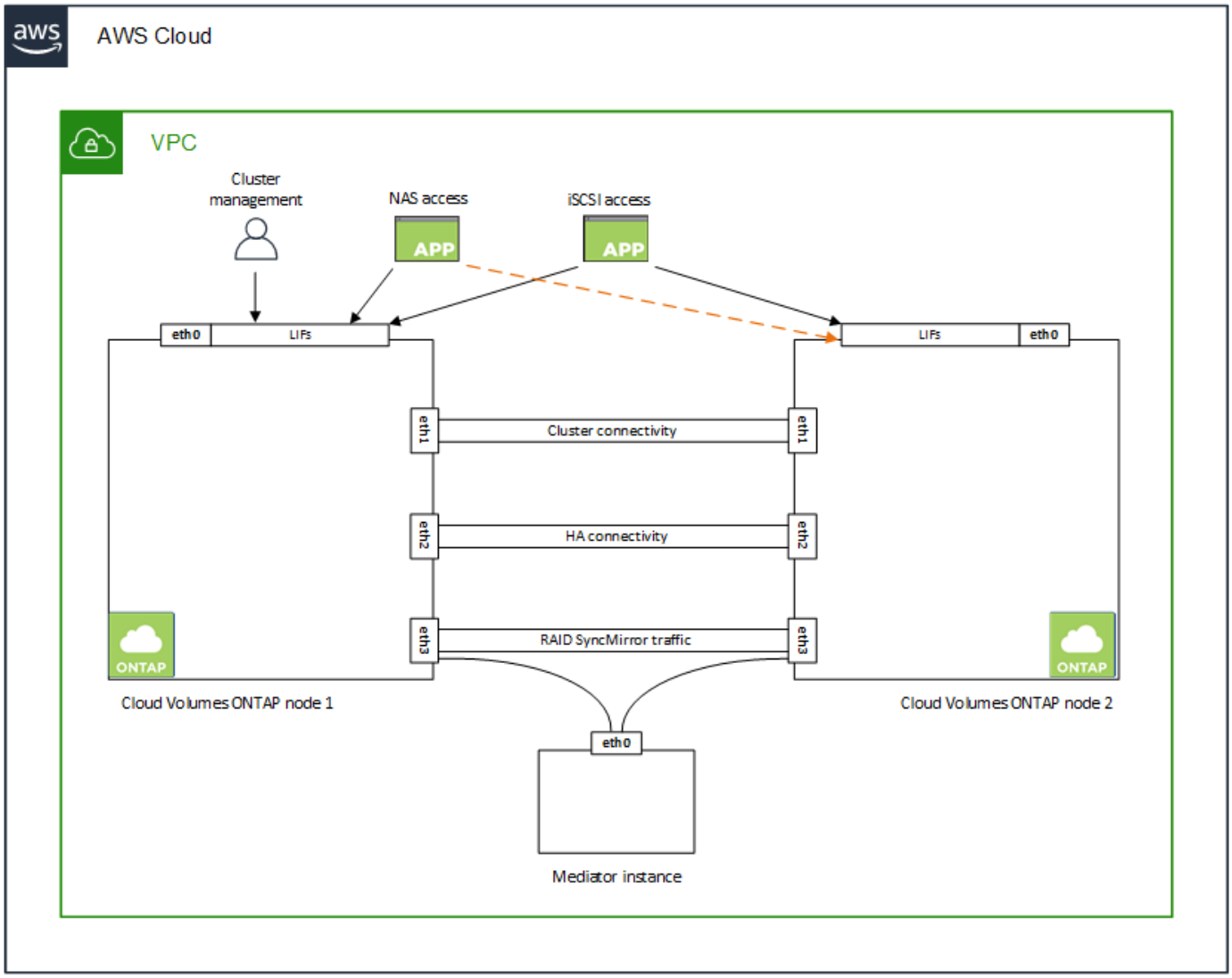
BlueXP weist einem System mit einem einzelnen Node 6 IP-Adressen zu.

Die folgende Tabelle enthält Details zu den LIFs, die mit jeder privaten IP-Adresse verknüpft sind.

LIF	Zweck
Cluster-Management	Administrative Verwaltung des gesamten Clusters (HA-Paar).
Node-Management	Administrationsmanagement eines Node
Intercluster	Cluster-übergreifende Kommunikation, Backup und Replizierung
NAS-Daten	Client-Zugriff über NAS-Protokolle.
ISCSI-Daten	Client-Zugriff über das iSCSI-Protokoll. Wird vom System auch für andere wichtige Netzwerk-Workflows eingesetzt. Dieses LIF ist erforderlich und sollte nicht gelöscht werden.
Storage-VM-Management	Ein Storage-VM-Management-LIF wird mit Managementtools wie SnapCenter verwendet.

IP-Adressen für HA-Paare

HA-Paare benötigen mehr IP-Adressen als ein System mit einem einzelnen Node. Diese IP-Adressen werden über verschiedene ethernet-Schnittstellen verteilt, wie im folgenden Bild dargestellt:



Die Anzahl der für ein HA-Paar erforderlichen privaten IP-Adressen hängt vom ausgewählten Implementierungsmodell ab. Ein in einer *Single* AWS Availability Zone (AZ) implementiertes HA-Paar benötigt 15 Private IP-Adressen, während ein in *multiple* AZS implementiertes HA-Paar 13 Private IP-Adressen erfordert.

Die folgenden Tabellen enthalten Details zu den LIFs, die mit den einzelnen privaten IP-Adressen verknüpft sind.

LIFs für HA-Paare in einer einzelnen Verfügbarkeitszone

LIF	Schnittstelle	Knoten	Zweck
Cluster-Management	Eth0	Knoten 1	Administrative Verwaltung des gesamten Clusters (HA-Paar).
Node-Management	Eth0	Node 1 und Node 2	Administrationsmanagement eines Node
Intercluster	Eth0	Node 1 und Node 2	Cluster-übergreifende Kommunikation, Backup und Replizierung
NAS-Daten	Eth0	Knoten 1	Client-Zugriff über NAS-Protokolle.

LIF	Schnittstelle	Knoten	Zweck
ISCSI-Daten	Eth0	Node 1 und Node 2	Client-Zugriff über das iSCSI-Protokoll. Wird vom System auch für andere wichtige Netzwerk-Workflows eingesetzt. Diese LIFs sind erforderlich und sollten nicht gelöscht werden.
Cluster-Konnektivität	Eth1	Node 1 und Node 2	Ermöglicht die Kommunikation der Nodes und das Verschieben von Daten innerhalb des Clusters.
HA-Konnektivität	Eth2	Node 1 und Node 2	Kommunikation zwischen den beiden Knoten im Failover-Fall.
RSM-iSCSI-Datenverkehr	Eth3	Node 1 und Node 2	RAID SyncMirror iSCSI-Datenverkehr sowie die Kommunikation zwischen den beiden Cloud Volumes ONTAP-Nodes und dem Mediator.
Mediator	Eth0	Mediator	Kommunikationskanal zwischen den Nodes und dem Mediator zur Unterstützung bei Storage-Takeover- und Giveback-Prozessen

LIFs für HA-Paare in mehreren Verfügbarkeitszonen

LIF	Schnittstelle	Knoten	Zweck
Node-Management	Eth0	Node 1 und Node 2	Administrationsmanagement eines Node
Intercluster	Eth0	Node 1 und Node 2	Cluster-übergreifende Kommunikation, Backup und Replizierung
ISCSI-Daten	Eth0	Node 1 und Node 2	Client-Zugriff über das iSCSI-Protokoll. Diese LIFs managen zudem die Migration von fließenden IP-Adressen zwischen Nodes. Diese LIFs sind erforderlich und sollten nicht gelöscht werden.
Cluster-Konnektivität	Eth1	Node 1 und Node 2	Ermöglicht die Kommunikation der Nodes und das Verschieben von Daten innerhalb des Clusters.
HA-Konnektivität	Eth2	Node 1 und Node 2	Kommunikation zwischen den beiden Knoten im Failover-Fall.
RSM-iSCSI-Datenverkehr	Eth3	Node 1 und Node 2	RAID SyncMirror iSCSI-Datenverkehr sowie die Kommunikation zwischen den beiden Cloud Volumes ONTAP-Nodes und dem Mediator.
Mediator	Eth0	Mediator	Kommunikationskanal zwischen den Nodes und dem Mediator zur Unterstützung bei Storage-Takeover- und Giveback-Prozessen

Wenn eine Implementierung in mehreren Verfügbarkeitszonen erstellt wird, werden mehrere LIFs zugeordnet "Floating-IP-Adressen", Die nicht gegen die private IP-Beschränkung von AWS gezählt werden.

Sicherheitsgruppen

Sie müssen keine Sicherheitsgruppen erstellen, weil BlueXP das für Sie tut. Wenn Sie Ihr eigenes verwenden müssen, lesen Sie "Regeln für Sicherheitsgruppen".

Sie suchen Informationen über den Connector? "Zeigen Sie die Sicherheitsgruppenregeln für den Konnektor an"

Verbindung für Daten-Tiering

Wenn Sie EBS als Performance-Tier und AWS S3 als Kapazitäts-Tier verwenden möchten, müssen Sie sicherstellen, dass Cloud Volumes ONTAP eine Verbindung zu S3 hat. Die beste Möglichkeit, diese Verbindung bereitzustellen, besteht darin, einen VPC-Endpunkt für den S3-Dienst zu erstellen. Anweisungen hierzu finden Sie unter "AWS Dokumentation: Erstellen eines Gateway-Endpunkts".

Wenn Sie den VPC-Endpunkt erstellen, wählen Sie die Region, den VPC und die Routing-Tabelle aus, die der Cloud Volumes ONTAP Instanz entspricht. Sie müssen auch die Sicherheitsgruppe ändern, um eine ausgehende HTTPS-Regel hinzuzufügen, die Datenverkehr zum S3-Endpunkt ermöglicht. Andernfalls kann Cloud Volumes ONTAP keine Verbindung zum S3-Service herstellen.

Informationen zu Problemen finden Sie unter "AWS Support Knowledge Center: Warum kann ich mich nicht über einen Gateway VPC Endpunkt mit einem S3-Bucket verbinden?"

Verbindungen zu ONTAP Systemen

Um Daten zwischen einem Cloud Volumes ONTAP System in AWS und ONTAP Systemen in anderen Netzwerken zu replizieren, müssen Sie eine VPN-Verbindung zwischen der AWS VPC und dem anderen Netzwerk herstellen, beispielsweise das Unternehmensnetzwerk. Anweisungen hierzu finden Sie unter "AWS Dokumentation: Einrichten einer AWS VPN-Verbindung".

DNS und Active Directory für CIFS

Wenn Sie CIFS-Storage bereitstellen möchten, müssen Sie DNS und Active Directory in AWS einrichten oder Ihre lokale Einrichtung auf AWS erweitern.

Der DNS-Server muss Namensauflösungsdienste für die Active Directory-Umgebung bereitstellen. Sie können DHCP-Optionssätze so konfigurieren, dass sie den Standard-EC2-DNS-Server verwenden, der nicht der von der Active Directory-Umgebung verwendete DNS-Server sein darf.

Anweisungen finden Sie unter "AWS Dokumentation: Active Directory Domain Services in der AWS Cloud: Quick Start Reference Deployment".

VPC-Sharing

Ab Version 9.11.1 werden Cloud Volumes ONTAP HA-Paare in AWS mit VPC-Sharing unterstützt. Die VPC-Freigabe ermöglicht Ihrem Unternehmen, Subnetze mit anderen AWS Konten gemeinsam zu nutzen. Um diese Konfiguration zu verwenden, müssen Sie Ihre AWS-Umgebung einrichten und dann das HA-Paar mithilfe der API implementieren.

"Erfahren Sie, wie ein HA-Paar in einem gemeinsamen Subnetz implementiert wird".

Anforderungen für HA-Paare in mehreren Verfügbarkeitszonen

Zusätzliche AWS Netzwerkanforderungen gelten für Cloud Volumes ONTAP HA-Konfigurationen, die mehrere Verfügbarkeitszonen (AZS) verwenden. Sie sollten diese Anforderungen überprüfen, bevor Sie ein HA-Paar starten, da Sie beim Erstellen der Arbeitsumgebung die Netzwerkdetails in BlueXP eingeben müssen.

Informationen zur Funktionsweise von HA-Paaren finden Sie unter "Hochverfügbarkeitspaare".

Verfügbarkeitszonen

Dieses HA-Bereitstellungsmodell verwendet mehrere AZS, um eine hohe Verfügbarkeit Ihrer Daten zu gewährleisten. Sie sollten für jede Cloud Volumes ONTAP Instanz und die Mediatorinstanz eine dedizierte AZ verwenden, die einen Kommunikationskanal zwischen dem HA-Paar bereitstellt.

In jeder Verfügbarkeitszone sollte ein Subnetz verfügbar sein.

Fließende IP-Adressen für NAS- und Cluster-/SVM-Management

HA-Konfigurationen in mehreren Verfügbarkeitszonen verwenden fließende IP-Adressen, die bei einem Ausfall zwischen Nodes migriert werden. Außerhalb der VPC ist nicht nativ zugänglich. Es sei denn, Sie können darauf zugreifen "AWS Transit Gateway einrichten".

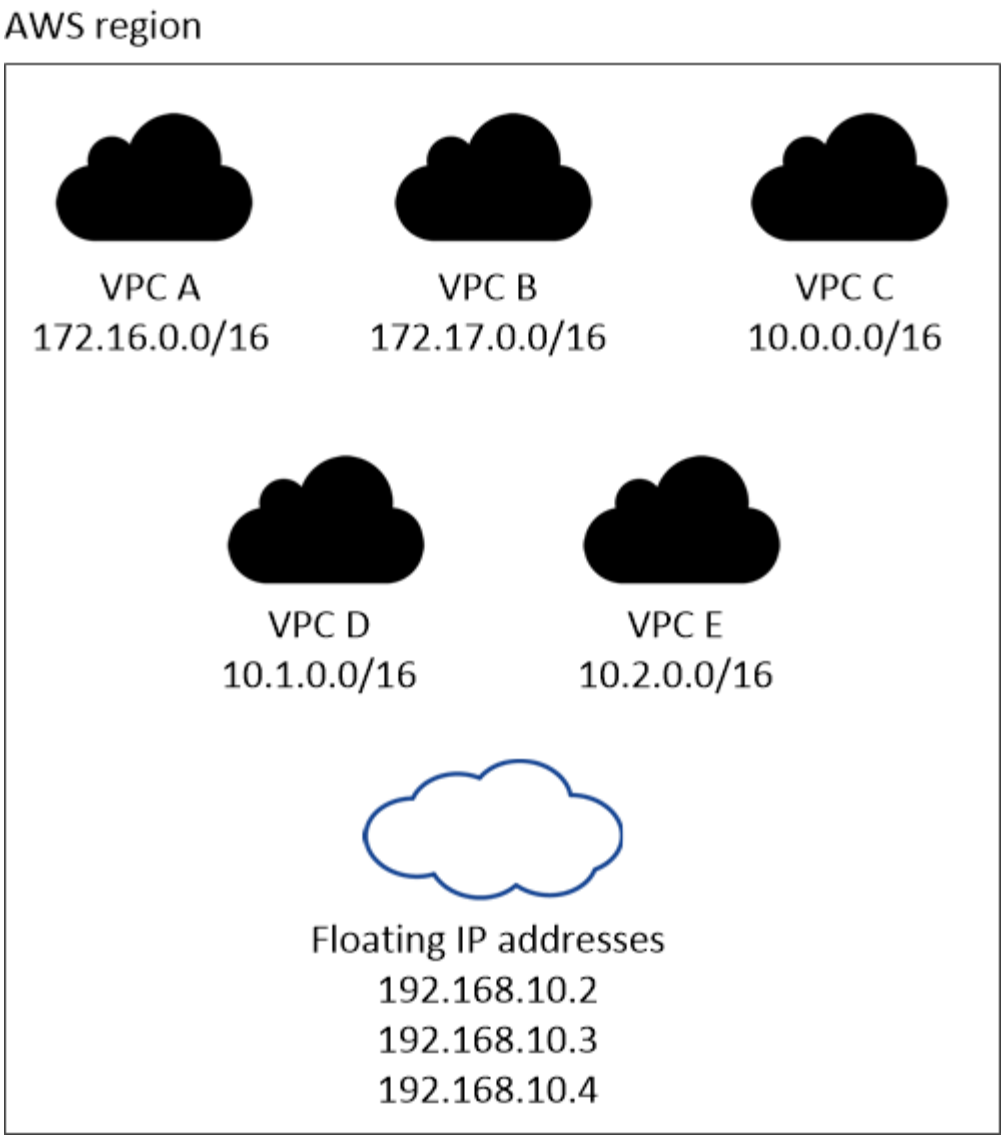
Eine Floating-IP-Adresse ist für das Cluster-Management, eine für NFS/CIFS-Daten auf Node 1 und eine für NFS/CIFS-Daten auf Node 2. Eine vierte Floating IP-Adresse für SVM-Management ist optional.

> Wenn Sie SnapDrive für Windows oder SnapCenter mit dem HA-Paar verwenden, ist eine unverankerte IP-Adresse für die SVM-Management-LIF erforderlich.

Sie müssen die unverankerten IP-Adressen in BlueXP eingeben, wenn Sie eine Arbeitsumgebung mit Cloud Volumes ONTAP HA erstellen. BlueXP weist dem HA-Paar die IP-Adressen zu, wenn das System gestartet wird.

Die fließenden IP-Adressen müssen sich für alle VPCs in der AWS Region, in der Sie die HA-Konfiguration implementieren, außerhalb der CIDR-Blöcke befinden. Stellen Sie sich die fließenden IP-Adressen als logisches Subnetz vor, das sich außerhalb der VPCs in Ihrer Region befindet.

Das folgende Beispiel zeigt die Beziehung zwischen Floating-IP-Adressen und den VPCs in einer AWS-Region. Während sich die fließenden IP-Adressen für alle VPCs außerhalb der CIDR-Blöcke befinden, sind sie über Routing-Tabellen in Subnetze routingfähig.



BlueXP erstellt automatisch statische IP-Adressen für den iSCSI-Zugriff und für NAS-Zugriff von Clients außerhalb der VPC. Für diese Art von IP-Adressen müssen Sie keine Anforderungen erfüllen.

Transit-Gateway zur Aktivierung des Floating IP-Zugriffs von außerhalb der VPC

Bei Bedarf "AWS Transit Gateway einrichten" Um den Zugriff auf die unverankerten IP-Adressen eines HA-Paars von außerhalb der VPC zu ermöglichen, in der sich das HA-Paar befindet.

Routentabellen

Nachdem Sie in BlueXP die unverankerten IP-Adressen angegeben haben, werden Sie dann aufgefordert, die Routingtabellen auszuwählen, die Routen zu den unverankerten IP-Adressen enthalten sollen. Dies ermöglicht den Client-Zugriff auf das HA-Paar.

Wenn Sie nur eine Routingtabelle für die Subnetze in Ihrem VPC (der Hauptroutingtabelle) haben, fügt BlueXP automatisch die fließenden IP-Adressen zu dieser Routingtabelle hinzu. Wenn Sie mehr als eine Routing-Tabelle haben, ist es sehr wichtig, beim Starten des HA-Paars die richtigen Routing-Tabellen auszuwählen. Andernfalls haben einige Clients möglicherweise keinen Zugriff auf Cloud Volumes ONTAP.

Sie können beispielsweise zwei Subnetze haben, die mit verschiedenen Routing-Tabellen verknüpft sind.

Wenn Sie Routing-Tabelle A auswählen, jedoch nicht Route-Tabelle B, können Clients in der mit Routing-Tabelle A verknüpften Subnetz auf das HA-Paar zugreifen, die Clients im Subnetz der Routing-Tabelle B können jedoch nicht.

Weitere Informationen zu Routingtabellen finden Sie unter "AWS Documentation: Routingtabellen".

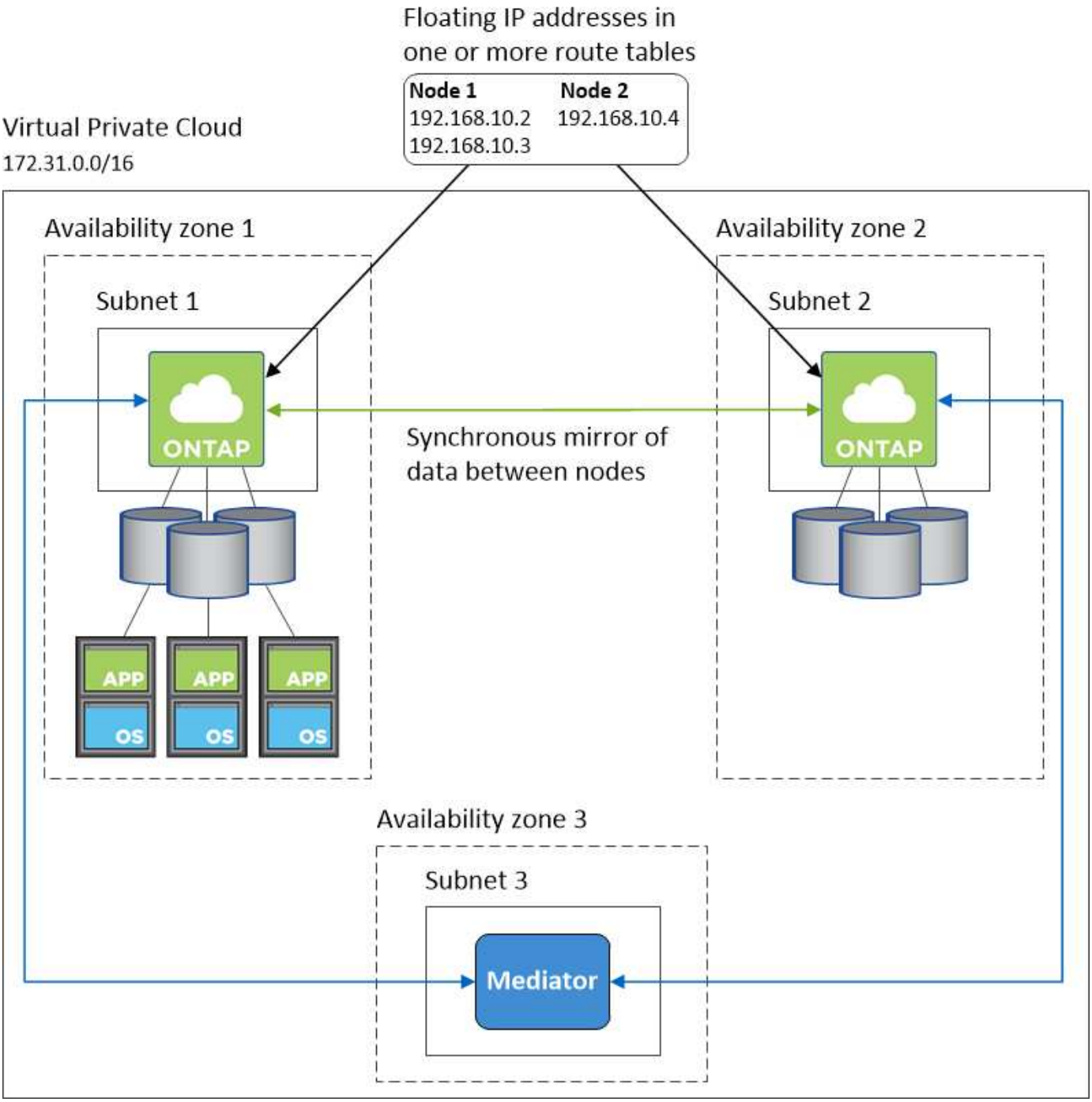
Anbindung an NetApp Management Tools

Für den Einsatz von NetApp Management Tools mit HA-Konfigurationen in mehreren Verfügbarkeitszonen stehen zwei Verbindungsoptionen zur Verfügung:

1. Die NetApp Management Tools in einer anderen VPC und implementieren "AWS Transit Gateway einrichten". Das Gateway ermöglicht den Zugriff auf die unverankerte IP-Adresse für die Cluster-Managementoberfläche von außerhalb der VPC aus.
2. Implementieren Sie die NetApp Management-Tools in derselben VPC mit einer ähnlichen Routing-Konfiguration wie NAS-Clients.

Beispiel für eine HA-Konfiguration

Das folgende Bild zeigt die Netzwerkkomponenten, die für ein HA-Paar in mehreren Verfügbarkeitszonen spezifisch sind: Drei Verfügbarkeitszonen, drei Subnetze, fließende IP-Adressen und eine Routingtabelle.



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"
- "Sicherheitsgruppenregeln in AWS"

Einrichten eines AWS-Transit-Gateways für HA-Paare in mehreren Verfügbarkeitszonen

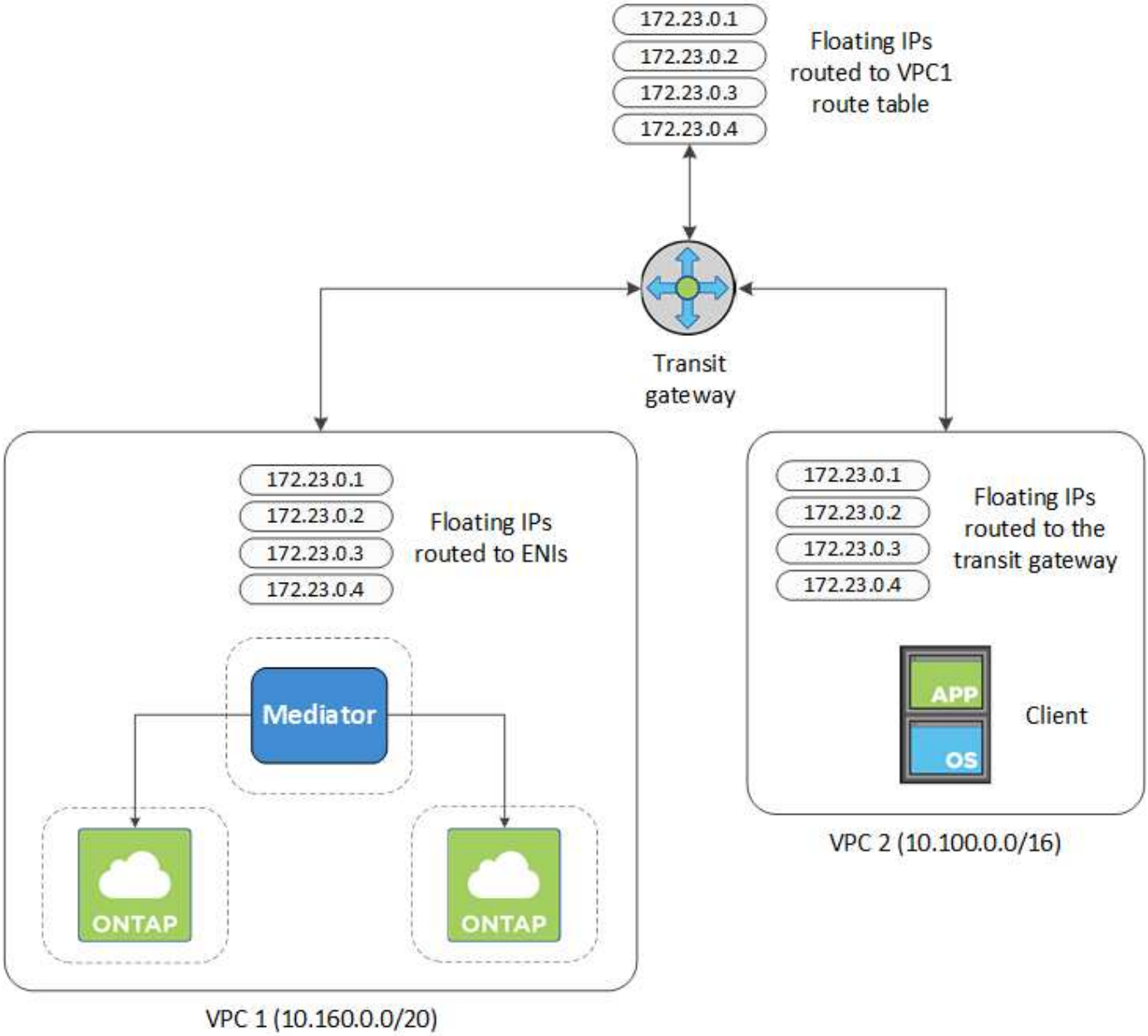
Einrichten eines AWS Transit-Gateways für den Zugriff auf HA-Paare "Floating-IP-Adressen" Von außerhalb der VPC, wo das HA-Paar residiert.

Wenn eine Cloud Volumes ONTAP-HA-Konfiguration über mehrere AWS-Verfügbarkeitszonen verteilt ist, sind unverankerte IP-Adressen für den NAS-Datenzugriff über die VPC erforderlich. Diese fließenden IP-Adressen können bei Ausfällen zwischen Nodes migriert werden, sind aber außerhalb der VPC nicht nativ zugänglich. Separate private IP-Adressen ermöglichen den Datenzugriff von außerhalb der VPC, bieten jedoch kein automatisches Failover.

Floating IP-Adressen sind außerdem für die Cluster-Managementoberfläche und die optionale SVM Management LIF erforderlich.

Wenn Sie ein AWS-Transit-Gateway einrichten, ermöglichen Sie den Zugriff auf die unverankerten IP-Adressen von außerhalb der VPC, wo sich das HA-Paar befindet. Das bedeutet, dass NAS-Clients und NetApp Managementtools außerhalb der VPC auf die fließenden IPs zugreifen können.

Das Beispiel zeigt zwei VPCs, die über ein Transit-Gateway verbunden sind. Ein HA-System befindet sich in einer VPC, während ein Client im anderen befindet. Sie können dann mithilfe der fließenden IP-Adresse ein NAS-Volume auf den Client mounten.

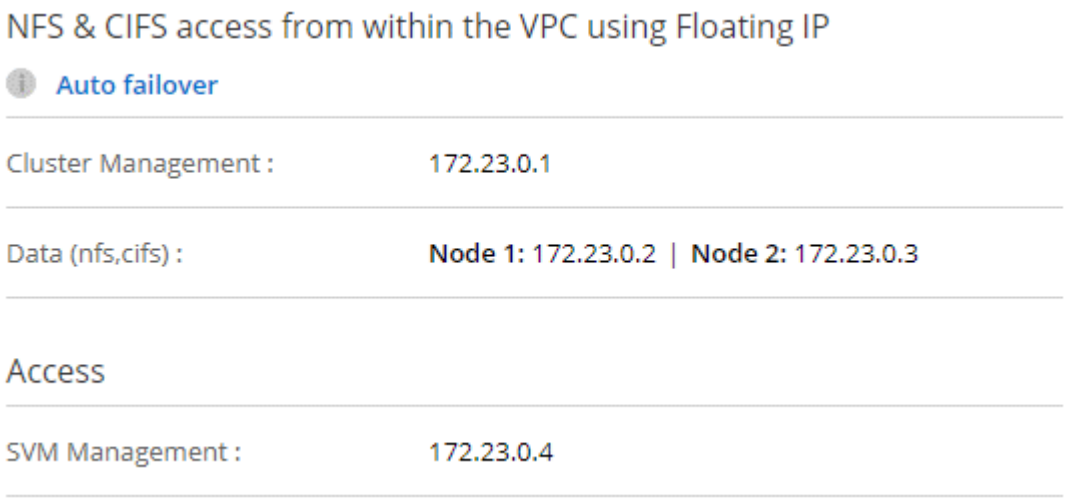


Die folgenden Schritte veranschaulichen die Einrichtung einer ähnlichen Konfiguration.

Schritte

1. "Erstellen Sie ein Transit-Gateway, und verbinden Sie die VPCs mit dem Gateway".
2. Weisen Sie die VPCs der Routing-Gateway-Routingtabelle zu.
   a. Klicken Sie im Dienst * VPC* auf **Transit Gateway Route Tables**.
   b. Wählen Sie die Routentabelle aus.
   c. Klicken Sie auf **Verknüpfungen** und wählen Sie dann **Verknüpfung erstellen** aus.
   d. Wählen Sie die Anhänge (die VPCs) aus, die Sie verknüpfen möchten, und klicken Sie dann auf **Verknüpfung erstellen**.
3. Erstellen Sie Routen in der Routing-Tabelle des Transit-Gateways durch Angabe der Floating-IP-Adressen des HA-Paars.

   Die unverankerten IP-Adressen finden Sie auf der Seite Informationen zur Arbeitsumgebung in BlueXP. Hier ein Beispiel:



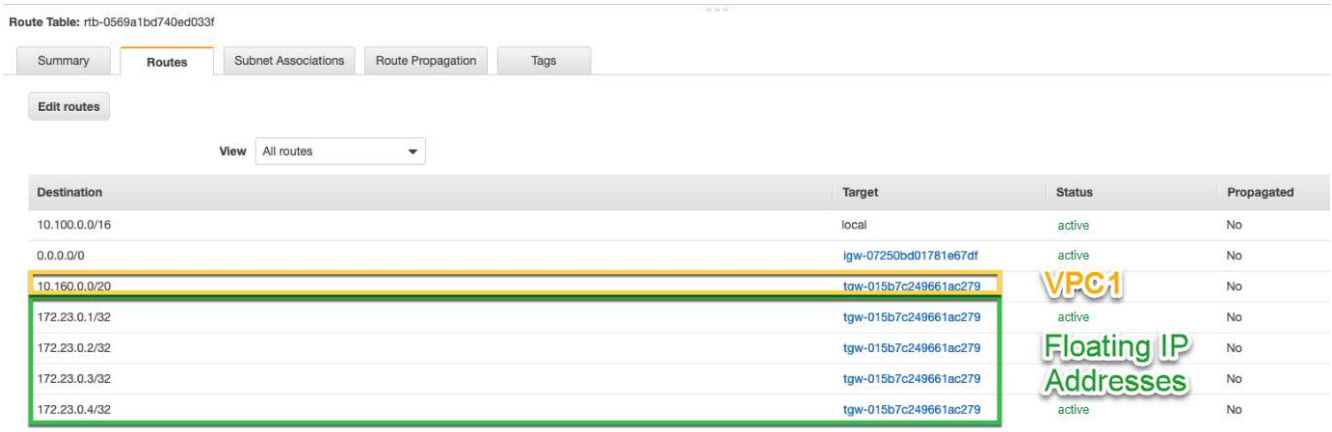
   Das folgende Beispielbild zeigt die Routingtabelle für das Transit Gateway. Er umfasst Routen zu den CIDR-Blöcken der zwei VPCs und vier von Cloud Volumes ONTAP verwendete Floating IP-Adressen.

4. Ändern Sie die Routingtabelle von VPCs, die auf die fließenden IP-Adressen zugreifen müssen.

   a. Fügen Sie den unverankerten IP-Adressen Routeneinträge hinzu.

   b. Fügen Sie einen Routeneintrag zum CIDR-Block des VPC hinzu, wo das HA-Paar residiert.

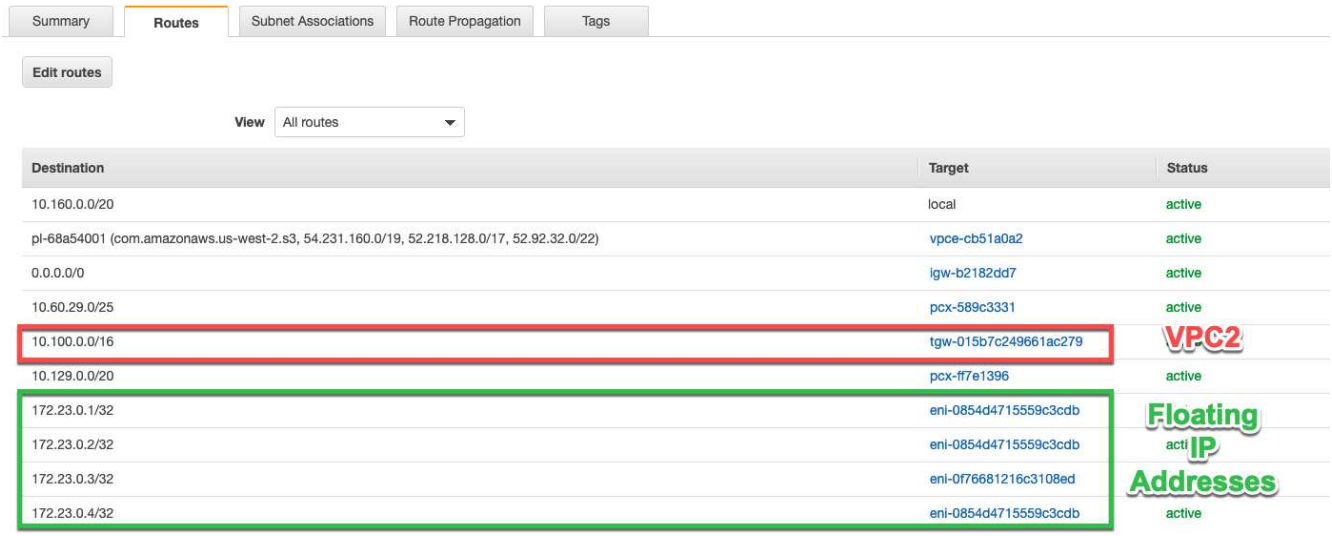
      Das folgende Beispielbild zeigt die Routingtabelle für VPC 2, die auch Routen zu VPC 1 und die fließenden IP-Adressen umfasst.



5. Ändern Sie die Routing-Tabelle für die VPC des HA-Paars, indem Sie der VPC eine Route hinzufügen, die Zugriff auf die fließenden IP-Adressen benötigt.

   Dieser Schritt ist wichtig, da er die Weiterleitung zwischen den VPCs abgeschlossen hat.

   Das folgende Beispielbild zeigt die Routing-Tabelle für VPC 1. Sie umfasst eine Route zu den unverankerten IP-Adressen und zu VPC 2, wo sich der Client befindet. BlueXP hat beim Einsatz des HA-Paars automatisch die unverankerten IPs zur Routingtabelle hinzugefügt.



6. Aktualisieren Sie die Einstellungen der Sicherheitsgruppen auf Alle Daten für die VPC.

   a. Klicken Sie unter Virtual Private Cloud auf **Subnetze**.

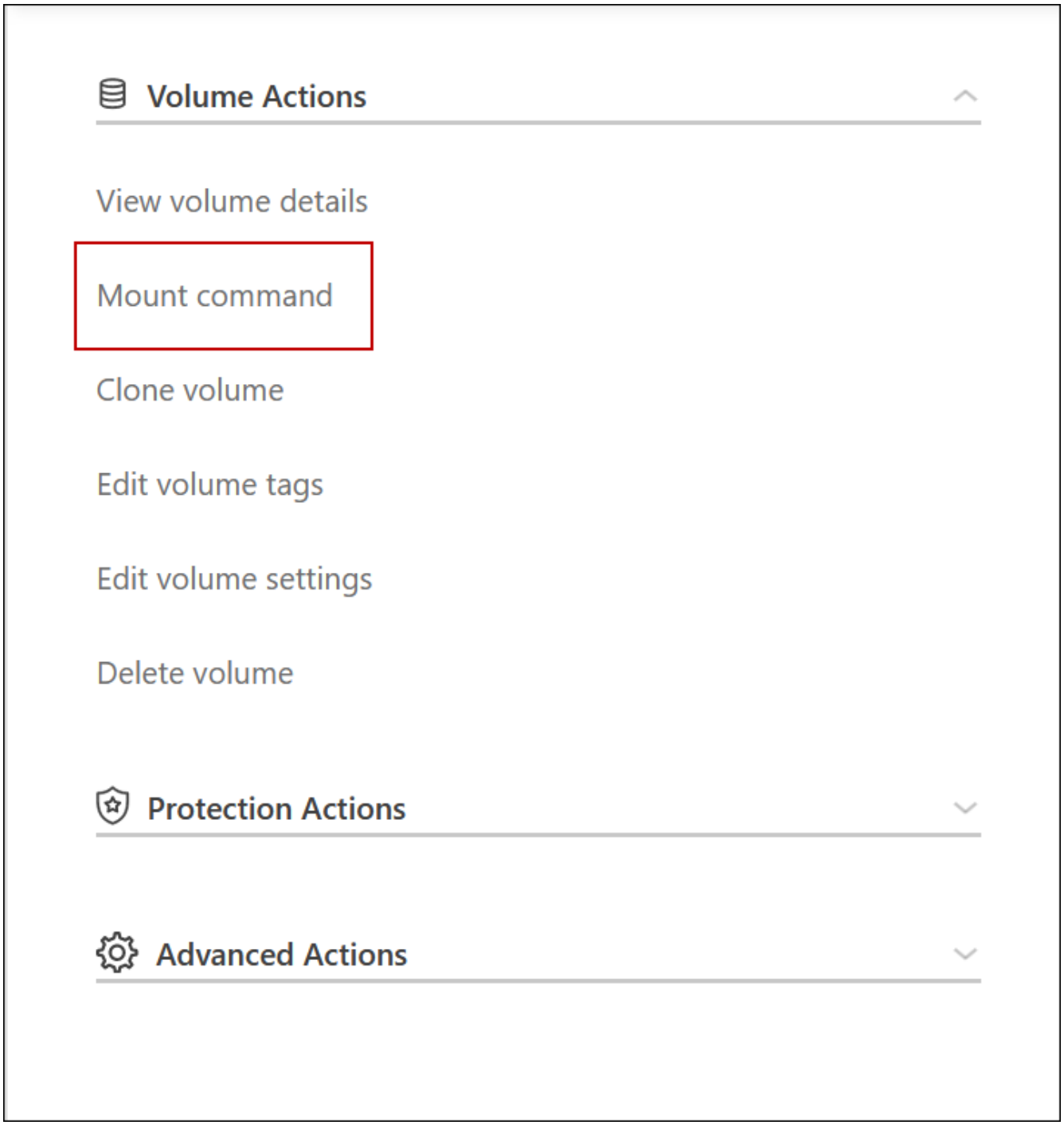
   b. Klicken Sie auf die Registerkarte **Route table** und wählen Sie die gewünschte Umgebung für eine der fließenden IP-Adressen für ein HA-Paar aus.

   c. Klicken Sie auf **Sicherheitsgruppen**.

d. Wählen Sie **Inbound Rules Bearbeiten**.
e. Klicken Sie auf **Regel hinzufügen**.
f. Wählen Sie unter Typ **All Traffic** aus, und wählen Sie dann die VPC-IP-Adresse aus.
g. Klicken Sie auf **Regeln speichern**, um die Änderungen anzuwenden.

7. Volumes werden mithilfe der Floating IP-Adresse an Clients gemountet.

   Die richtige IP-Adresse finden Sie in BlueXP über die Option **Mount Command** im Bereich Volumes verwalten in BlueXP.



8. Wenn Sie ein NFS-Volume mounten, konfigurieren Sie die Exportrichtlinie entsprechend dem Subnetz der Client-VPC.

"Erfahren Sie, wie Sie ein Volume bearbeiten".

Verwandte Links

- "Hochverfügbarkeitspaare in AWS"
- "Netzwerkanforderungen für Cloud Volumes ONTAP in AWS"

Implementieren Sie ein HA-Paar in einem gemeinsamen Subnetz

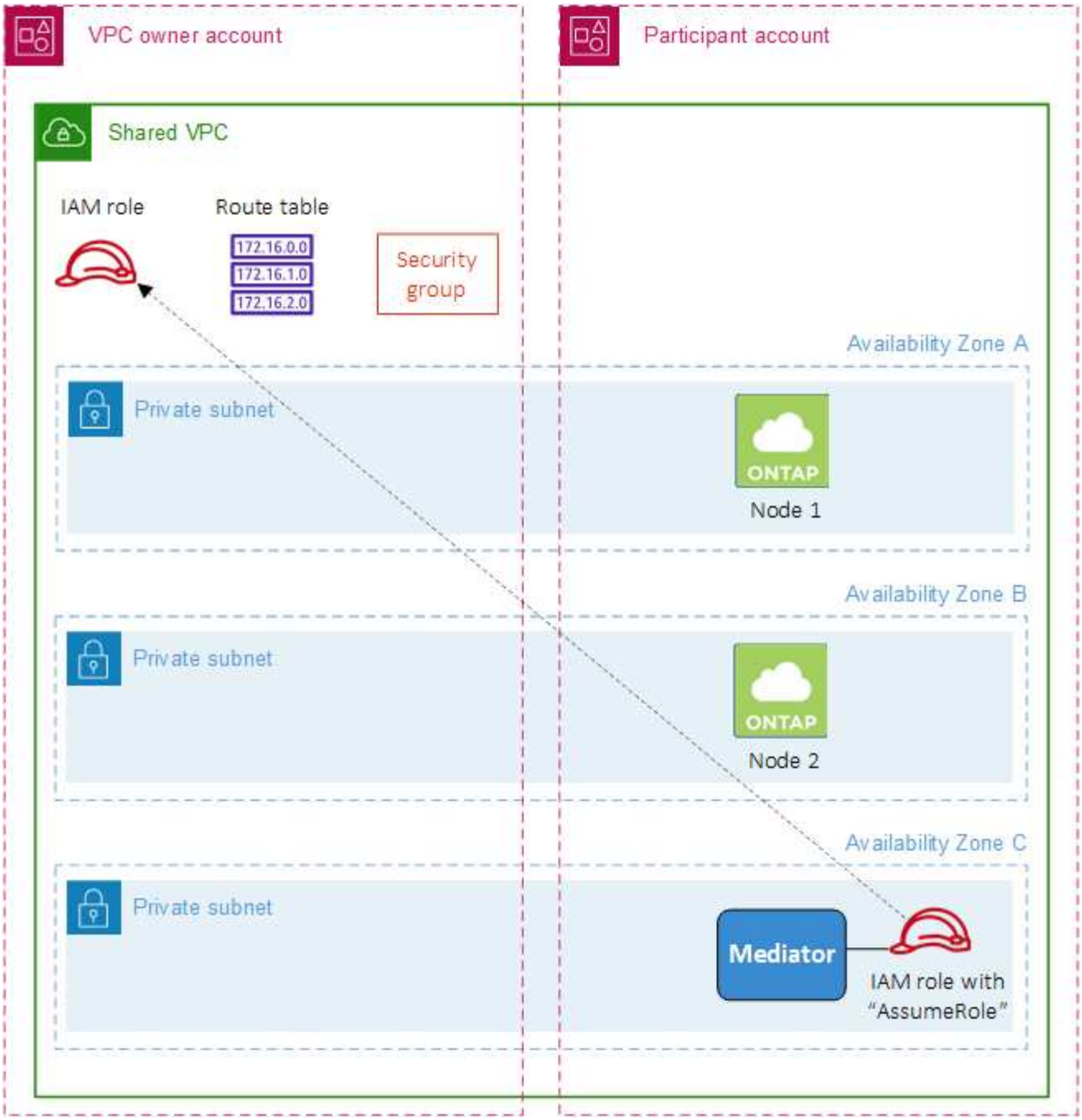
Ab Version 9.11.1 werden Cloud Volumes ONTAP HA-Paare in AWS mit VPC-Sharing unterstützt. Die VPC-Freigabe ermöglicht Ihrem Unternehmen, Subnetze mit anderen AWS Konten gemeinsam zu nutzen. Um diese Konfiguration zu verwenden, müssen Sie Ihre AWS-Umgebung einrichten und dann das HA-Paar mithilfe der API implementieren.

Mit "VPC-Sharing", Eine Cloud Volumes ONTAP HA-Konfiguration ist auf zwei Konten verteilt:

- Das VPC-Owner-Konto, zu dem das Netzwerk gehört (VPC, Subnetze, Routing-Tabellen und Cloud Volumes ONTAP-Sicherheitsgruppe)
- Das Teilnehmerkonto, bei dem die EC2 Instanzen in gemeinsam genutzten Subnetzen implementiert werden (dazu gehören die zwei HA-Nodes und der Mediator)

Bei einer Cloud Volumes ONTAP HA-Konfiguration, die über mehrere Verfügbarkeitszonen hinweg implementiert wird, benötigt der HA-Mediator spezifische Berechtigungen, um die Routing-Tabellen im VPC-Owner-Konto zu schreiben. Sie müssen diese Berechtigungen bereitstellen, indem Sie eine IAM-Rolle einrichten, die der Mediator übernehmen kann.

Das folgende Bild zeigt die betroffenen Komponenten für die Implementierung:



Wie in den unten beschriebenen Schritten beschrieben, müssen Sie die Subnetze dem Teilnehmerkonto teilen und anschließend die IAM-Rolle und Sicherheitsgruppe im VPC-Owner-Konto erstellen.

Beim Erstellen der Arbeitsumgebung von Cloud Volumes ONTAP erstellt BlueXP automatisch eine IAM-Rolle und fügt sie dem Mediator an. Bei dieser Rolle wird die IAM-Rolle angenommen, die Sie im VPC-Owner-Konto erstellt haben, um Änderungen an den Routingtabellen vorzunehmen, die mit dem HA-Paar verknüpft sind.

Schritte

1. Teilen Sie die Subnetze im VPC-Owner-Konto mit dem Teilnehmerkonto.

   Dieser Schritt ist erforderlich, um das HA-Paar in gemeinsam genutzten Subnetzen zu implementieren.

   "AWS Dokumentation: Ein Subnetz gemeinsam nutzen"

2. Erstellen Sie im VPC-Owner-Konto eine Sicherheitsgruppe für Cloud Volumes ONTAP.

   "Beachten Sie die Regeln für Cloud Volumes ONTAP in den Sicherheitsgruppen". Beachten Sie, dass Sie keine Sicherheitsgruppe für den HA Mediator erstellen müssen. BlueXP ist das für Sie.

3. Erstellen Sie im VPC-Owner-Konto eine IAM-Rolle, die die folgenden Berechtigungen enthält:

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. Verwenden Sie die BlueXP API, um eine neue Cloud Volumes ONTAP-Arbeitsumgebung zu erstellen.

   Beachten Sie, dass Sie die folgenden Felder angeben müssen:

   - „SicherheitGruppeID“

     Im Feld „securityGroupID“ sollte die Sicherheitsgruppe angegeben werden, die Sie im VPC-Owner-Konto erstellt haben (siehe Schritt 2 oben).

   - "AssumeeRoleArn" im Objekt "haParams"

     Das Feld „assumeRoleArn“ sollte den ARN der IAM-Rolle enthalten, die Sie im VPC-Owner-Konto erstellt haben (siehe Schritt 3 oben).

     Beispiel:

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

+
"Erfahren Sie mehr über die Cloud Volumes ONTAP-API"

Sicherheitsgruppenregeln für AWS

BlueXP erstellt AWS Sicherheitsgruppen mit den ein- und ausgehenden Regeln, die für den erfolgreichen Betrieb von Cloud Volumes ONTAP erforderlich sind. Sie können sich zu Testzwecken auf die Ports beziehen oder wenn Sie Ihre eigenen Sicherheitsgruppen verwenden möchten.

Regeln für Cloud Volumes ONTAP

Die Sicherheitsgruppe für Cloud Volumes ONTAP erfordert sowohl eingehende als auch ausgehende Regeln.

Regeln für eingehende Anrufe

Wenn Sie eine Arbeitsumgebung erstellen und eine vordefinierte Sicherheitsgruppe auswählen, können Sie den Datenverkehr innerhalb einer der folgenden Optionen zulassen:

- **Nur gewählte VPC**: Die Quelle 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**: Die Quelle für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.

Protokoll	Port	Zweck
Alle ICMP	Alle	Pingen der Instanz
HTTP	80	HTTP-Zugriff auf die System Manager Webkonsole mit der IP-Adresse der Cluster-Management-LIF
HTTPS	443	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
TCP	4045	NFS-Sperr-Daemon
TCP	4046	Netzwerkstatusüberwachung für NFS
TCP	10.000	Backup mit NDMP
TCP	11104	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
TCP	11105	SnapMirror Datenübertragung über Cluster-interne LIFs
UDP	111	Remote-Prozeduraufruf für NFS
UDP	161-162	Einfaches Netzwerkverwaltungsprotokoll
UDP	635	NFS-Mount
UDP	2049	NFS-Server-Daemon
UDP	4045	NFS-Sperr-Daemon

Protokoll	Port	Zweck
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
Backup auf S3	TCP	5010	Intercluster-LIF	Backup-Endpunkt oder Wiederherstellungsendpunkt	Backup- und Restore-Vorgänge für die Funktion „Backup in S3“
Cluster	Gesamter Datenverkehr	Gesamter Datenverkehr	Alle LIFs auf einem Node	Alle LIFs auf dem anderen Node	Kommunikation zwischen Clustern (nur Cloud Volumes ONTAP HA)
	TCP	3000	Node Management-LIF	Ha Mediator	ZAPI-Aufrufe (nur Cloud Volumes ONTAP HA)
	ICMP	1	Node Management-LIF	Ha Mediator	Bleiben Sie am Leben (nur Cloud Volumes ONTAP HA)
Konfigurations-Backups	HTTP	80	Node Management-LIF	\Http://<connector-IP-address>/occm/offboxconfig	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	18600-18699	Node Management-LIF	Zielserver	NDMP-Kopie
SMTP	TCP	25	Node Management-LIF	Mailserver	SMTP-Warnungen können für AutoSupport verwendet werden

Service	Protokoll	Port	Quelle	Ziel	Zweck
SNMP	TCP	161	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	UDP	161	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	TCP	162	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	UDP	162	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
SnapMirror	TCP	11104	Intercluster-LIF	ONTAP Intercluster-LIFs	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
	TCP	11105	Intercluster-LIF	ONTAP Intercluster-LIFs	SnapMirror Datenübertragung
Syslog	UDP	514	Node Management-LIF	Syslog-Server	Syslog-Weiterleitungsmeldungen

Regeln für die externe Sicherheitsgruppe des HA Mediators

Die vordefinierte externe Sicherheitsgruppe für den Cloud Volumes ONTAP HA Mediator enthält die folgenden Regeln für ein- und ausgehende Anrufe.

Regeln für eingehende Anrufe

Die vordefinierte Sicherheitsgruppe für den HA-Mediator umfasst die folgende eingehende Regel.

Protokoll	Port	Quelle	Zweck
TCP	3000	CIDR des Connectors	RESTful API-Zugriff über den Connector

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den HA-Vermittler 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 den HA-Vermittler enthält die folgenden Regeln für ausgehende Anrufe.

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

Erweiterte Outbound-Regeln

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

Protokoll	Port	Ziel	Zweck
HTTP	80	IP-Adresse des Connectors auf der AWS EC2 Instanz	Lade Upgrades für den Mediator herunter
HTTPS	443	ec2.amazonaws.com	Unterstützung bei Storage Failover
UDP	53	ec2.amazonaws.com	Unterstützung bei Storage Failover

Anstatt die Ports 443 und 53 zu öffnen, können Sie einen VPC-Endpunkt des Zielsubnetzen zum AWS EC2 Service erstellen.

Regeln für die interne Sicherheitsgruppe der HA-Konfiguration

Die vordefinierte interne Sicherheitsgruppe für eine Cloud Volumes ONTAP HA-Konfiguration umfasst die folgenden Regeln: Diese Sicherheitsgruppe ermöglicht die Kommunikation zwischen den HA-Nodes und zwischen dem Mediator und den Nodes.

BlueXP erstellt diese Sicherheitsgruppe immer. Sie haben nicht die Möglichkeit, Ihre eigenen zu verwenden.

Regeln für eingehende Anrufe

Die vordefinierte Sicherheitsgruppe enthält die folgenden Regeln für eingehende Anrufe.

Protokoll	Port	Zweck
Gesamter Datenverkehr	Alle	Kommunikation zwischen HA-Mediator und HA-Knoten

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Gesamter Datenverkehr	Alle	Kommunikation zwischen HA-Mediator und HA-Knoten

Regeln für den Konnektor

"Zeigen Sie die Sicherheitsgruppenregeln für den Konnektor an"

Einrichten des AWS KMS

Wenn Sie die Amazon Verschlüsselung mit Cloud Volumes ONTAP verwenden möchten, müssen Sie den AWS KMS (Key Management Service) einrichten.

Schritte

1. Stellen Sie sicher, dass ein aktiver Kundenstammschlüssel (CMK) vorhanden ist.

   Bei CMK kann es sich um ein von AWS gemanagtes CMK oder um ein vom Kunden gemanagtes CMK handeln. Sie kann sich im selben AWS Konto wie BlueXP und Cloud Volumes ONTAP oder in einem anderen AWS Konto befinden.

   "AWS Dokumentation: Customer Master Keys (CMKs)"

2. Ändern Sie die Schlüsselrichtlinie für jedes CMK, indem Sie die IAM-Rolle hinzufügen, die BlueXP Berechtigungen als *Key-Benutzer* bereitstellt.

   Wenn Sie die IAM-Rolle als Schlüsselbenutzer hinzufügen, erhalten Sie BlueXP Berechtigungen zur Verwendung des CMK mit Cloud Volumes ONTAP.

   "AWS Dokumentation: Schlüssel bearbeiten"

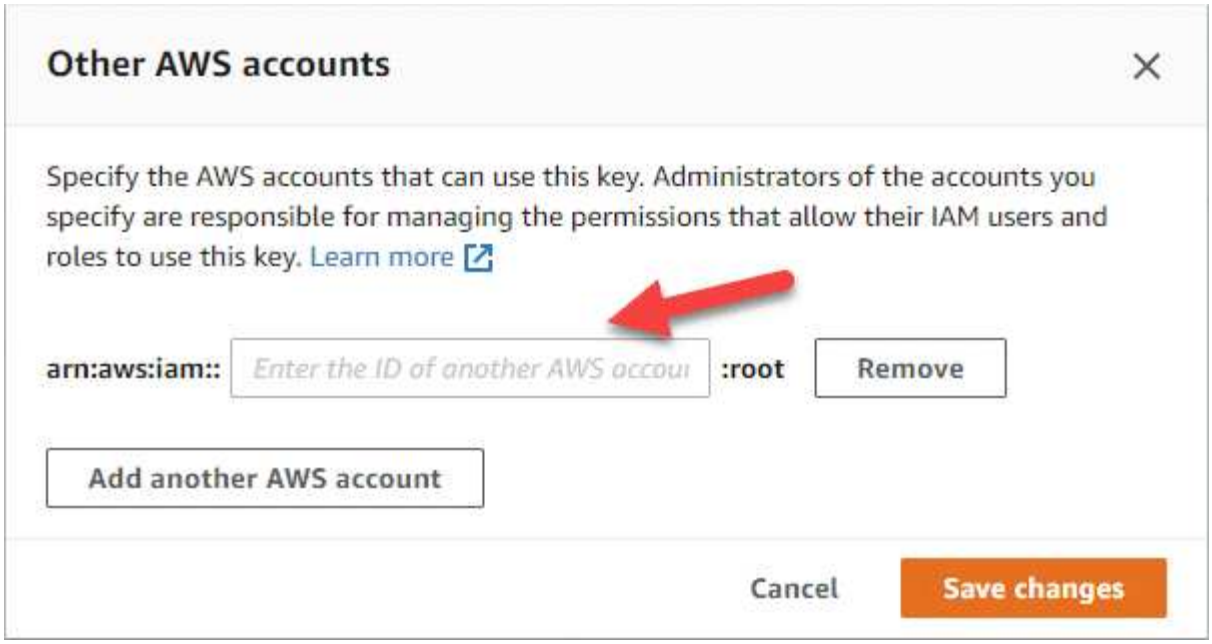
3. Wenn sich das CMK in einem anderen AWS Konto befindet, führen Sie folgende Schritte aus:

   a. Wechseln Sie von dem Konto, in dem sich der CMK befindet, zur KMS-Konsole.
   b. Wählen Sie die Taste.
   c. Kopieren Sie im Fenster **Allgemeine Konfiguration** den ARN des Schlüssels.

      Wenn Sie das Cloud Volumes ONTAP-System erstellen, müssen Sie BlueXP das ARN zur Verfügung stellen.

   d. Fügen Sie im Bereich **andere AWS-Konten** das AWS-Konto hinzu, das BlueXP mit Berechtigungen versorgt.

      In den meisten Fällen ist dies das Konto, in dem sich BlueXP befindet. Wenn BlueXP nicht in AWS installiert wurde, wäre es das Konto, für das Sie AWS-Zugriffsschlüssel für BlueXP zur Verfügung gestellt haben.



e. Wechseln Sie nun zu dem AWS Konto, das BlueXP mit Berechtigungen versorgt, und öffnen Sie die IAM-Konsole.

f. Erstellen Sie eine IAM-Richtlinie, die die unten aufgeführten Berechtigungen enthält.

g. Hängen Sie die Richtlinie an die IAM-Rolle oder den IAM-Benutzer an, der Berechtigungen für BlueXP bereitstellt.

   Die folgende Richtlinie enthält die Berechtigungen, die BlueXP zur Verwendung des CMK über das externe AWS-Konto benötigt. Denken Sie daran, die Region und die Account-ID in den Abschnitten „Ressource“ zu ändern.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
Weitere Details zu diesem Prozess finden Sie unter "AWS Dokumentation: Benutzer in anderen Konten können einen KMS-Schlüssel verwenden".

4. Wenn Sie ein vom Kunden verwaltetes CMK verwenden, ändern Sie die Schlüsselrichtlinie für das CMK, indem Sie die Cloud Volumes ONTAP IAM-Rolle als *Key User* hinzufügen.

Dieser Schritt ist erforderlich, wenn Sie Daten-Tiering auf Cloud Volumes ONTAP aktiviert und die im S3-Bucket gespeicherten Daten verschlüsseln möchten.

Sie müssen diesen Schritt durchführen *nach* Sie implementieren Cloud Volumes ONTAP, da die IAM-Rolle beim Erstellen einer Arbeitsumgebung erstellt wird. (Natürlich haben Sie die Möglichkeit, eine vorhandene Cloud Volumes ONTAP IAM-Rolle zu verwenden, sodass Sie diesen Schritt zuvor ausführen können.)

"AWS Dokumentation: Schlüssel bearbeiten"

Einrichten von IAM-Rollen für Cloud Volumes ONTAP

IAM-Rollen mit den erforderlichen Berechtigungen müssen an jeden Cloud Volumes ONTAP-Knoten angeschlossen sein. Das gleiche gilt für den HA Mediator. Es ist am einfachsten, BlueXP die IAM-Rollen für Sie erstellen zu lassen, aber Sie können Ihre eigenen Rollen verwenden.

Diese Aufgabe ist optional. Wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen, können Sie mit BlueXP standardmäßig die IAM-Rollen für Sie erstellen. Wenn Sie in den Sicherheitsrichtlinien Ihres Unternehmens die IAM-Rollen selbst erstellen müssen, befolgen Sie die folgenden Schritte.

> In der AWS Commercial Cloud Services-Umgebung ist die Bereitstellung Ihrer eigenen IAM-Rolle erforderlich. "Erfahren Sie, wie Cloud Volumes ONTAP in C2S eingesetzt wird".

Schritte

1. Wechseln Sie zur AWS IAM-Konsole.
2. IAM-Richtlinien erstellen, die die folgenden Berechtigungen enthalten:
    - Basisrichtlinie für Cloud Volumes ONTAP-Nodes

Standardregionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud (USA) Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

C2S-Umgebung

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- Backup-Richtlinie für Cloud Volumes ONTAP-Nodes

  Falls Sie BlueXP Backup und Recovery für Ihre Cloud Volumes ONTAP Systeme nutzen möchten, muss die IAM-Rolle für die Nodes die zweite unten dargestellte Richtlinie enthalten.

Standardregionen

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud (USA) Regionen

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

C2S-Umgebung

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- Ha Mediator

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "sts:AssumeRole",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Erstellen Sie eine IAM-Rolle, und hängen Sie die von Ihnen erstellten Richtlinien an die Rolle an.

Ergebnis

Sie können jetzt IAM-Rollen auswählen, wenn Sie eine neue Cloud Volumes ONTAP-Arbeitsumgebung erstellen.

Weitere Informationen

- "AWS Dokumentation: Erstellung von IAM-Richtlinien"
- "AWS Dokumentation: Erstellen von IAM-Rollen"

Lizenzierung für Cloud Volumes ONTAP in AWS 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.

Freimium

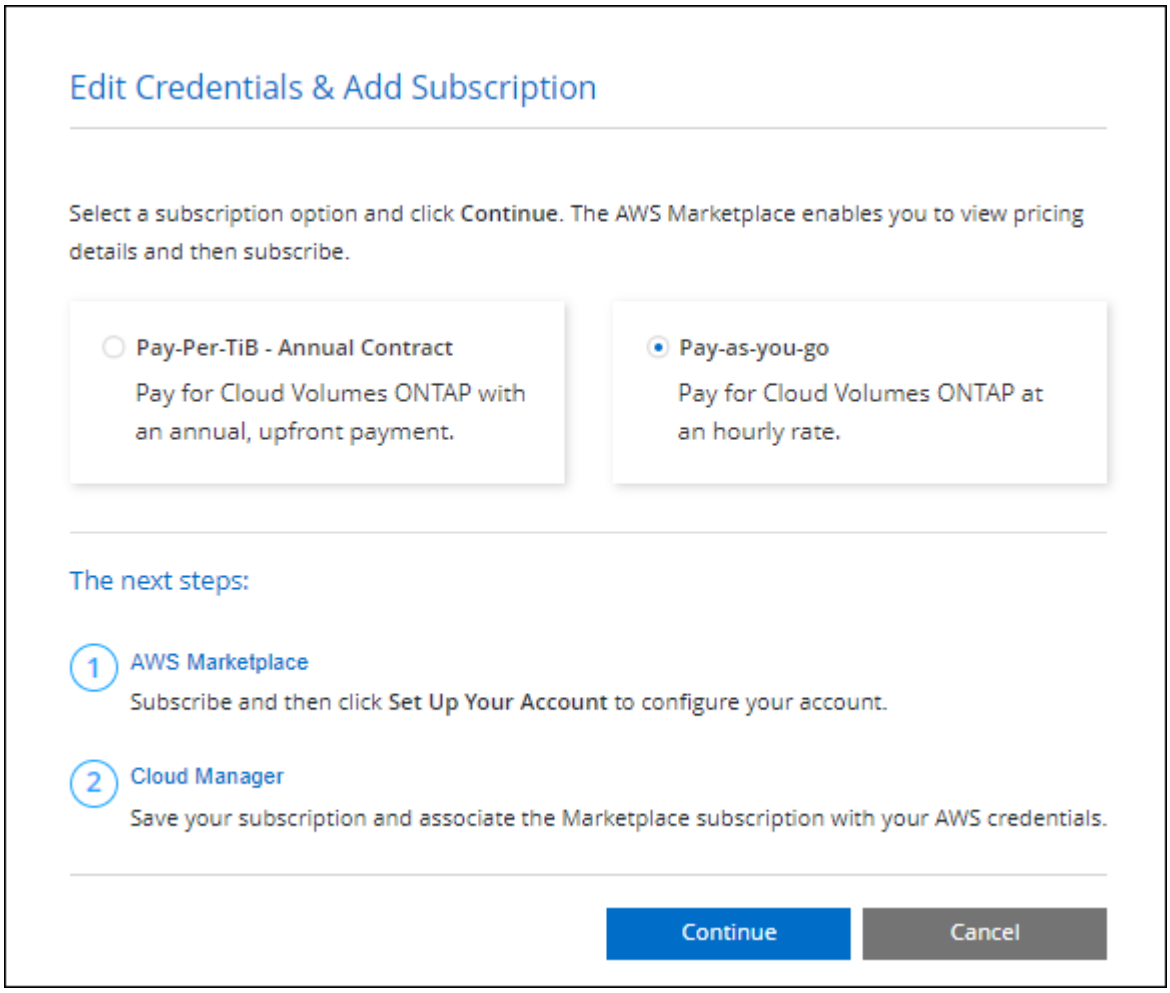
Wählen Sie das Freimium-Angebot aus, um Cloud Volumes ONTAP mit bis zu 500 gib bereitgestellter Kapazität kostenlos zu nutzen. "Erfahren Sie mehr über das Freemium Angebot".

Schritte

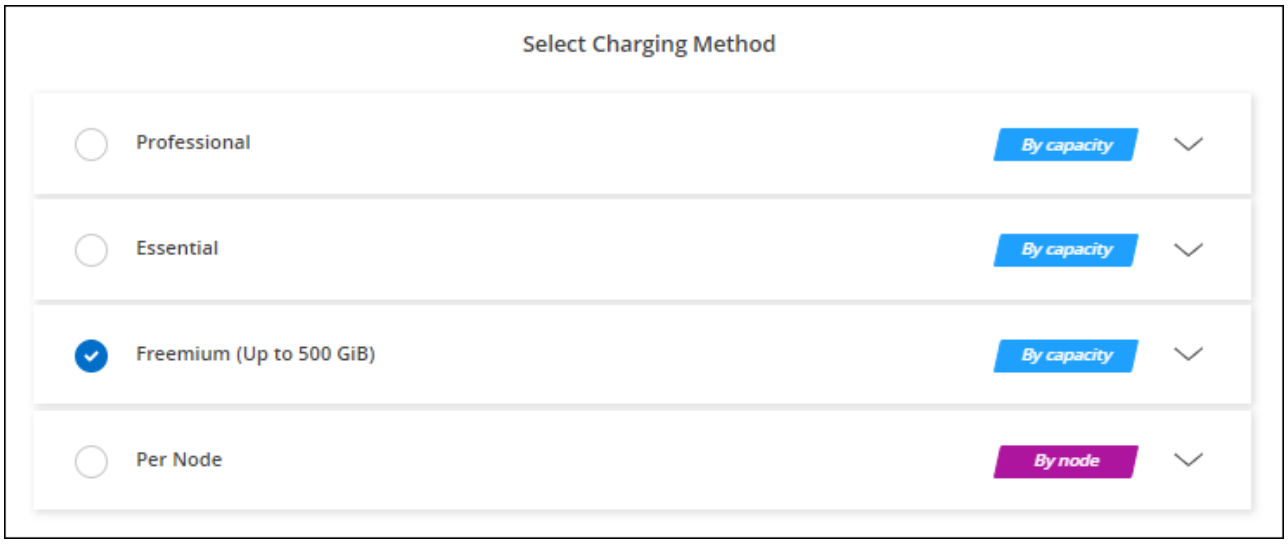
1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.

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 AWS 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".



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



"Sehen Sie sich Schritt-für-Schritt-Anleitungen zum Starten von Cloud Volumes ONTAP in AWS an".

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 AWS Marketplace
- Ein Jahresvertrag aus dem AWS Marketplace

"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.

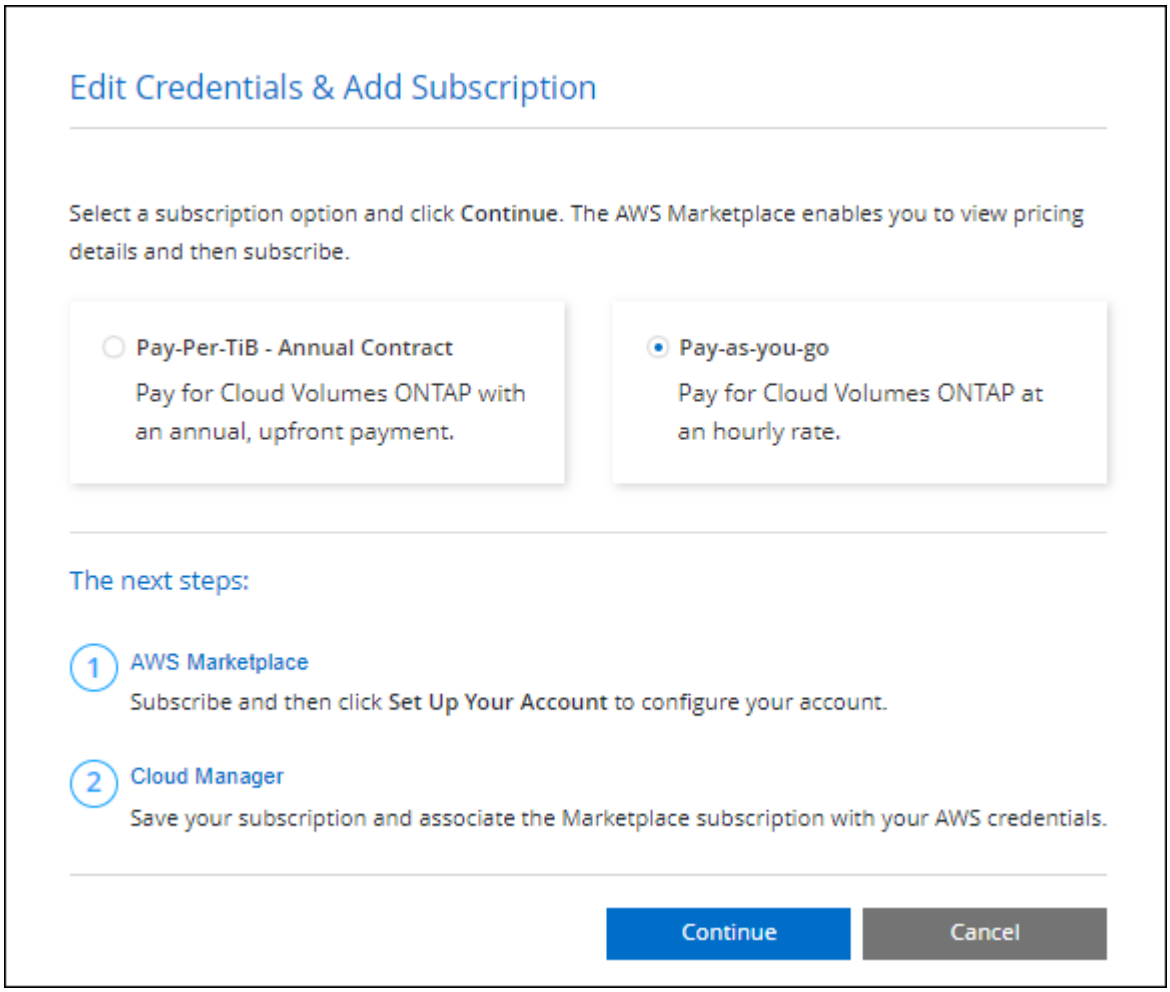
   Bevor Sie Ihre Lizenz mit Cloud Volumes ONTAP verwenden können, muss sie über das Digital Wallet von BlueXP erhältlich sein. Wenn nötig, können Sie "Fügen Sie die Lizenz manuell zum Digital Wallet von BlueXP hinzu".

3. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in

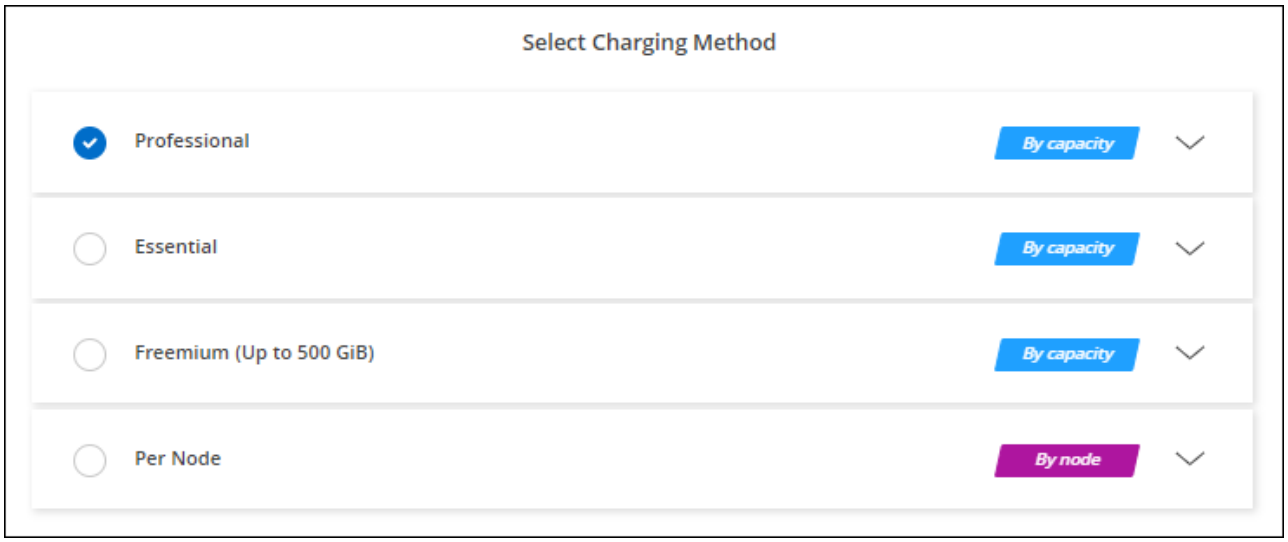
BlueXP.

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 AWS 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.



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



"Sehen Sie sich Schritt-für-Schritt-Anleitungen zum Starten von Cloud Volumes ONTAP in AWS an".

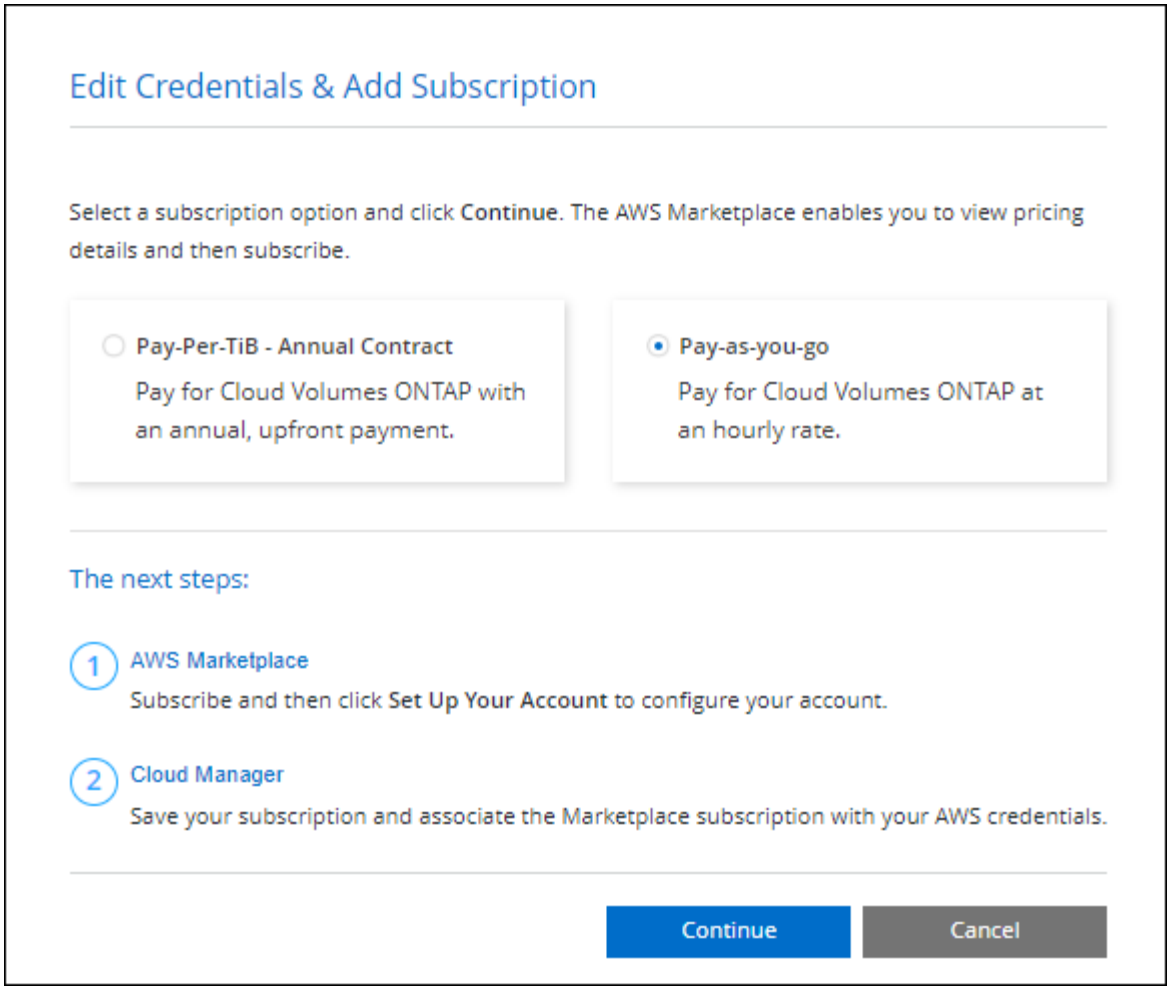
PAYGO-Abonnement

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

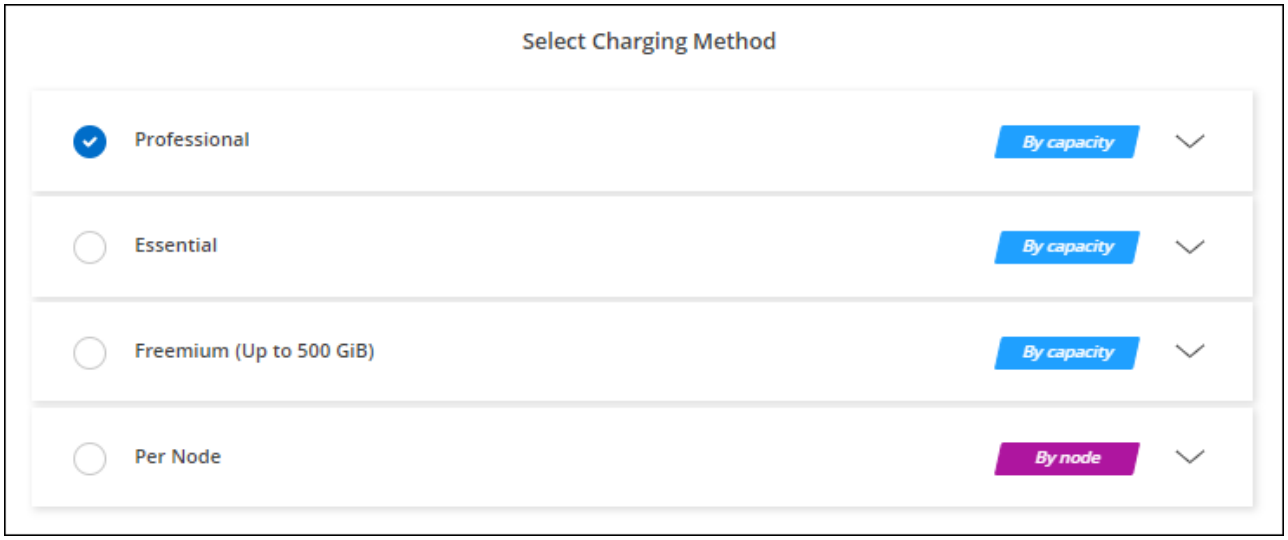
Wenn Sie eine Arbeitsumgebung für Cloud Volumes ONTAP erstellen, werden Sie von BlueXP aufgefordert, den Vertrag im AWS Marketplace zu abonnieren. Dieses Abonnement wird dann zur Verrechnung mit der Arbeitsumgebung verknüpft. Sie können das gleiche Abonnement auch für zusätzliche Arbeitsumgebungen nutzen.

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 AWS Marketplace zu abonnieren.



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



"Sehen Sie sich Schritt-für-Schritt-Anleitungen zum Starten von Cloud Volumes ONTAP in AWS an".

Sie können die mit Ihren AWS-Konten verbundenen AWS Marketplace-Abonnements über die Seite „Einstellungen“ > „Anmeldeinformationen“ managen. "Managen Sie Ihre AWS-Konten und -Abonnements"

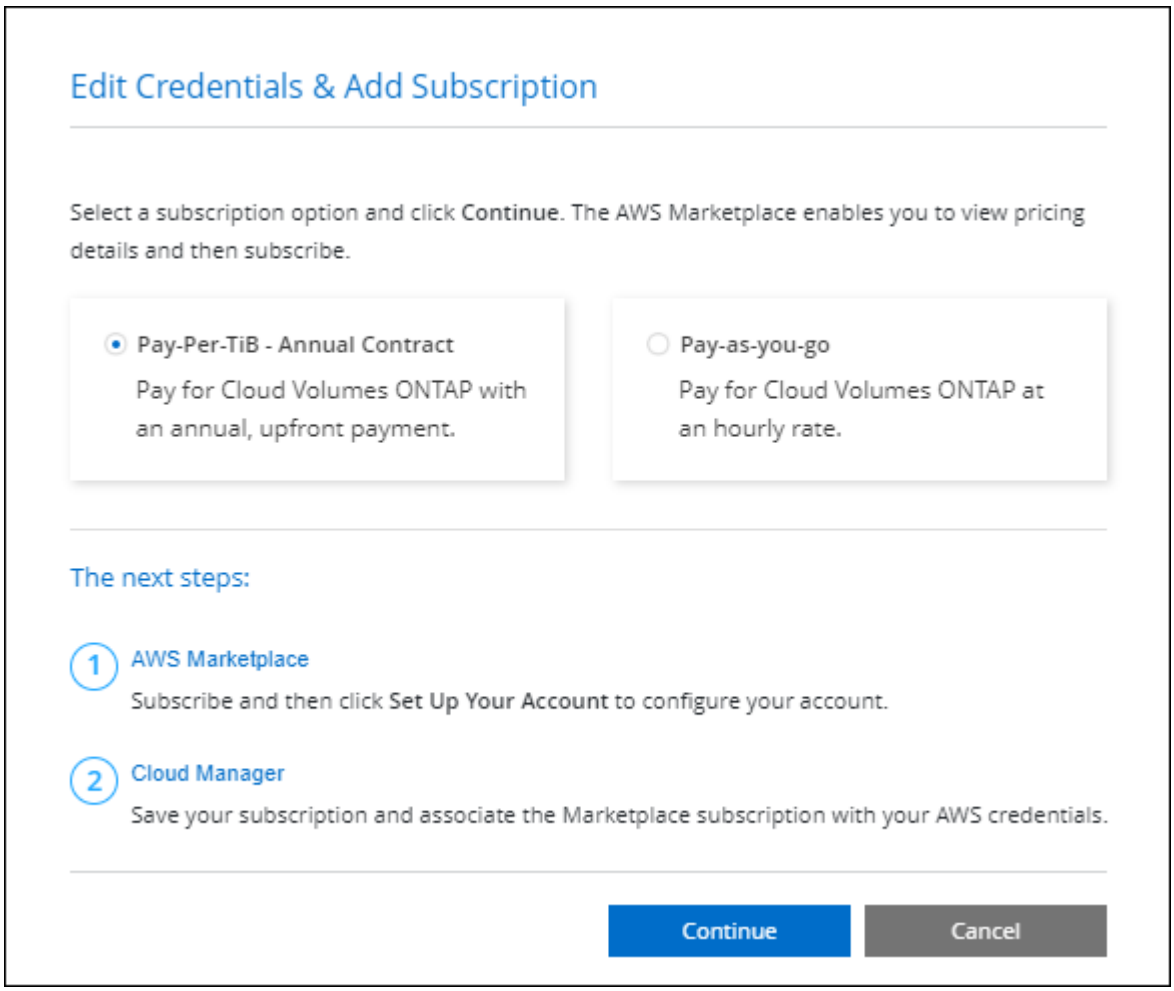
Jahresvertrag

Jährliche Zahlung durch Erwerb eines Jahresvertrags über den Markt Ihres Cloud-Providers.

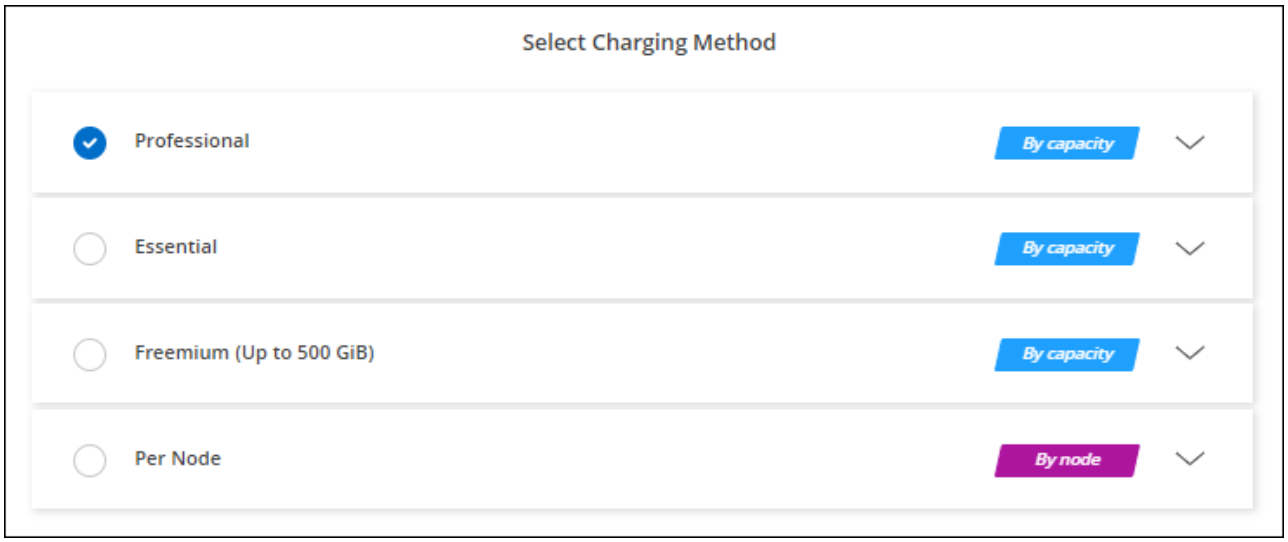
Ähnlich wie bei einem stündlichen Abonnement werden Sie von BlueXP aufgefordert, den Jahresvertrag zu abonnieren, der im AWS Marketplace verfügbar ist.

Schritte

1. 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 Jahresvertrag im AWS Marketplace zu abonnieren.



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



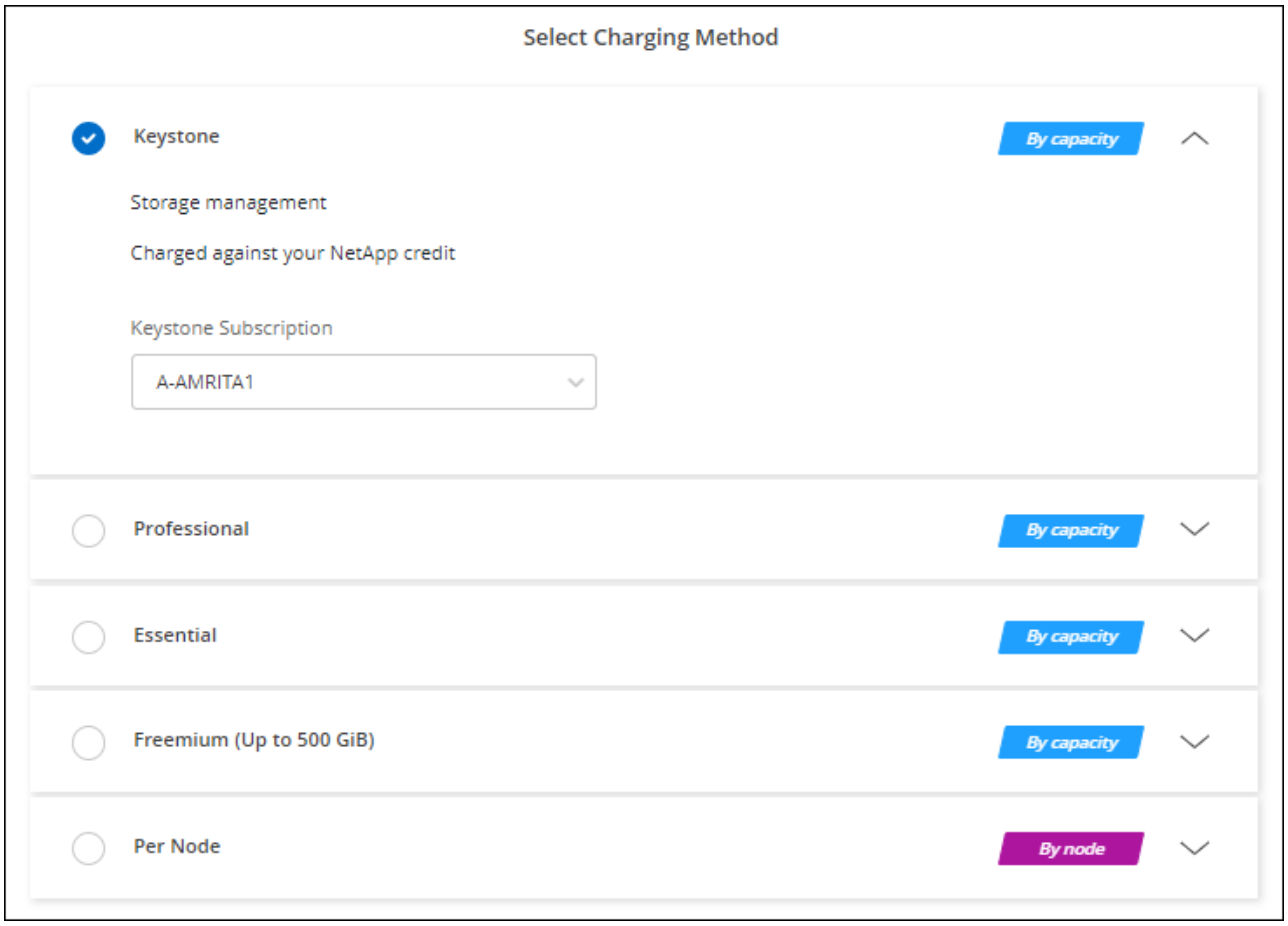
"Sehen Sie sich Schritt-für-Schritt-Anleitungen zum Starten von Cloud Volumes ONTAP in AWS an".

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[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.



"Sehen Sie sich Schritt-für-Schritt-Anleitungen zum Starten von Cloud Volumes ONTAP in AWS an".

Starten von Cloud Volumes ONTAP in AWS

Sie können Cloud Volumes ONTAP in einer Einzelsystemkonfiguration oder als HA-Paar in AWS 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".
- Ein Verständnis der zu verwendenden Konfiguration.

  Sie sollten eine Konfiguration ausgewählt und AWS-Netzwerkinformationen von Ihrem Administrator erhalten haben. 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".

- DNS und Active Directory für CIFS-Konfigurationen.

  Weitere Informationen finden Sie unter "Netzwerkanforderungen für Cloud Volumes ONTAP in AWS".

Starten eines Cloud Volumes ONTAP Systems mit einem Node in AWS

Wenn Sie Cloud Volumes ONTAP in AWS starten möchten, müssen Sie eine neue Arbeitsumgebung in BlueXP schaffen

Über diese Aufgabe

Unmittelbar nach der Erstellung der Arbeitsumgebung startet BlueXP eine Testinstanz in der angegebenen VPC, um die Konnektivität zu überprüfen. Wenn der Vorgang erfolgreich war, beendet BlueXP die Instanz sofort und beginnt dann mit der Bereitstellung des Cloud Volumes ONTAP-Systems. Wenn BlueXP die Verbindung nicht überprüfen kann, schlägt die Erstellung der Arbeitsumgebung fehl. Die Testinstanz ist entweder t2.nano (für Standard-VPC-Mandantenfähigkeit) oder m3.medium (für dedizierte VPC-Mandantenfähigkeit).

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 **Amazon Web Services** und **Cloud Volumes ONTAP Single Node**.
4. Wenn Sie dazu aufgefordert werden, "Einen Konnektor erstellen".
5. **Details und Anmeldeinformationen**: Optional können Sie die AWS-Anmeldeinformationen und das Abonnement ändern, einen Namen der Arbeitsumgebung eingeben, bei Bedarf Tags hinzufügen und dann ein Passwort eingeben.

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

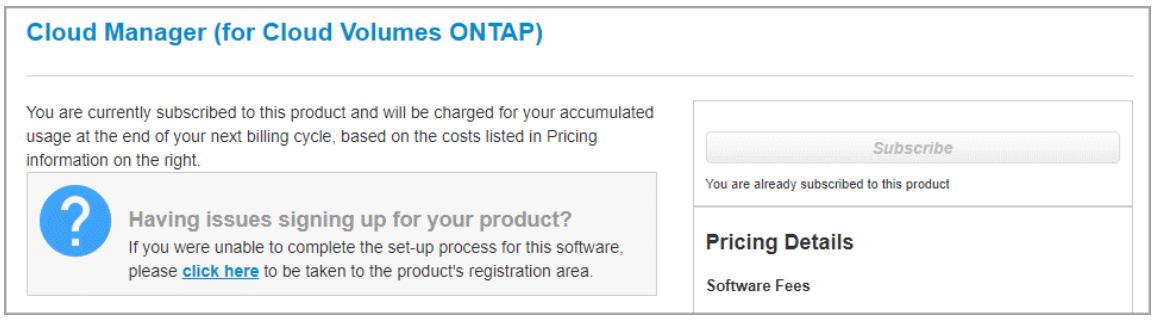
Feld	Beschreibung
Name der Arbeitsumgebung	BlueXP verwendet den Namen der Arbeitsumgebung, um sowohl das Cloud Volumes ONTAP System als auch die Amazon EC2 Instanz zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.
Tags hinzufügen	AWS-Tags sind Metadaten für Ihre AWS-Ressourcen. BlueXP fügt die Tags zur Cloud Volumes ONTAP-Instanz und jeder der Instanz zugeordneten AWS-Ressource hinzu. Sie können bis zu vier Tags aus der Benutzeroberfläche hinzufügen, wenn Sie eine Arbeitsumgebung erstellen. Nach der Erstellung können Sie weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen einer Arbeitsumgebung nicht auf vier Tags beschränkt. Informationen zu Tags finden Sie unter "AWS Dokumentation: Tagging der Amazon EC2 Ressourcen".
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 „*admin*“ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.

Feld	Beschreibung
Anmeldedaten Bearbeiten	Wählen Sie die AWS Zugangsdaten für das Konto aus, in dem Sie dieses System bereitstellen möchten. Sie können das AWS Marketplace Abonnement auch für dieses Cloud Volumes ONTAP-System zuordnen. Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen mit einem neuen AWS Marketplace-Abonnement zu verknüpfen. Bei dem Abonnement kann es sich um einen Jahresvertrag oder um die Bezahlung von Cloud Volumes ONTAP auf Stundenbasis handelt. "Erfahren Sie, wie Sie BlueXP zusätzliche AWS Zugangsdaten hinzufügen".

Im folgenden Video wird gezeigt, wie Sie ein Pay-as-you-go Marketplace Abonnement mit Ihren AWS Zugangsdaten verknüpfen:

Abonnieren Sie BlueXP über den AWS Marketplace

Wenn mehrere IAM-Benutzer im gleichen AWS-Konto arbeiten, muss jeder Benutzer sich anmelden. Wenn der erste Benutzer sich abonniert hat, informiert der AWS Marketplace die nachfolgenden Benutzer, dass sie bereits abonniert sind, wie in der Abbildung unten dargestellt. Während für das AWS *Account* ein Abonnement erfolgt, muss sich jeder IAM-Benutzer mit diesem Abonnement verknüpfen. Wenn Sie die unten angezeigte Meldung sehen, klicken Sie auf den Link **click here**, um zur BlueXP-Website zu gelangen und den Vorgang
abzuschließen.



6. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie nicht mit Cloud Volumes ONTAP verwenden möchten.
   - "Weitere Informationen zur BlueXP Klassifizierung"
   - "Erfahren Sie mehr über Backup und Recovery von BlueXP"

   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.

7. **Standort & Konnektivität**: Geben Sie die Netzwerkinformationen ein, die Sie im aufgezeichnet haben "AWS Worksheet".

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

Feld	Beschreibung
VPC	Wenn Sie über einen AWS Outpost verfügen, können Sie ein Cloud Volumes ONTAP System mit einem einzelnen Node in diesem Outpost implementieren, indem Sie die Outpost VPC auswählen. Die Erfahrung ist mit jeder anderen VPC, die in AWS residiert.
Sicherheitsgruppe wurde generiert	Wenn Sie BlueXP die Sicherheitsgruppe für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Selected VPC Only** wählen, ist die Quelle 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 die Quelle für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene Sicherheitsgruppe verwenden	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".

8. **Datenverschlüsselung**: Wählen Sie keine Datenverschlüsselung oder Verschlüsselung von AWS.

   Für die von AWS gemanagte Verschlüsselung können Sie einen anderen Customer Master Key (CMK) von Ihrem Konto oder einem anderen AWS Konto auswählen.

   Sie können die AWS Datenverschlüsselungsmethode nicht ändern, nachdem Sie ein Cloud Volumes ONTAP System erstellt haben.

   "So richten Sie AWS KMS für Cloud Volumes ONTAP ein".

   "Erfahren Sie mehr über unterstützte Verschlüsselungstechnologien".

9. **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".
10. **Cloud Volumes ONTAP Konfiguration** (nur Jahresvertrag für AWS Marketplace): Überprüfen Sie die Standardkonfiguration und klicken Sie auf **Weiter** oder klicken Sie auf **Konfiguration ändern**, um Ihre eigene Konfiguration auszuwählen.

    Wenn die Standardkonfiguration beibehalten wird, müssen Sie nur ein Volume angeben und anschließend die Konfiguration prüfen und genehmigen.

11. **Vorkonfigurierte Pakete**: Wählen Sie eines der Pakete aus, um schnell Cloud Volumes ONTAP zu starten, oder klicken Sie auf **Konfiguration ändern**, um Ihre eigene Konfiguration auszuwählen.

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

12. **IAM-Rolle**: Es ist am besten, die Standardoption zu behalten, mit der BlueXP die Rolle für Sie erstellen lässt.

Wenn Sie Ihre eigene Richtlinie verwenden möchten, muss diese erfüllen "Richtlinienanforderungen für Cloud Volumes ONTAP-Nodes".

13. **Lizenzierung**: Ändern Sie die Cloud Volumes ONTAP-Version nach Bedarf und wählen Sie einen Instanztyp und die Instanzenfähigkeit aus.

    > 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.

14. **Zugrunde liegende Speicherressourcen**: Wählen Sie einen Festplattentyp, konfigurieren Sie den zugrunde liegenden Speicher und wählen Sie, ob das Daten-Tiering aktiviert bleiben soll.

    Beachten Sie Folgendes:

    - Der Festplattentyp wird für das ursprüngliche Volume (und Aggregat) durchgeführt. Für nachfolgende Volumes (und Aggregate) kann ein anderer Festplattentyp ausgewählt werden.
    - Wenn Sie eine gp3- oder io1-Festplatte auswählen, verwendet BlueXP die Funktion Elastic Volumes in AWS, um bei Bedarf automatisch die zugrunde liegende Storage-Festplattenkapazität zu erhöhen. Sie können die ursprüngliche Kapazität auf Grundlage Ihrer Storage-Anforderungen auswählen und nach der Bereitstellung von Cloud Volumes ONTAP überarbeiten. "Erfahren Sie mehr über die Unterstützung von Elastic Volumes in AWS".
    - Wenn Sie eine gp2- oder st1-Festplatte auswählen, können Sie eine Festplattengröße für alle Festplatten im ursprünglichen Aggregat sowie für alle zusätzlichen Aggregate auswählen, die BlueXP erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuweisungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.
    - 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.

      "So funktioniert Daten-Tiering".

15. **Schreibgeschwindigkeit und WURM**:

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

       "Erfahren Sie mehr über Schreibgeschwindigkeit".

    b. 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.

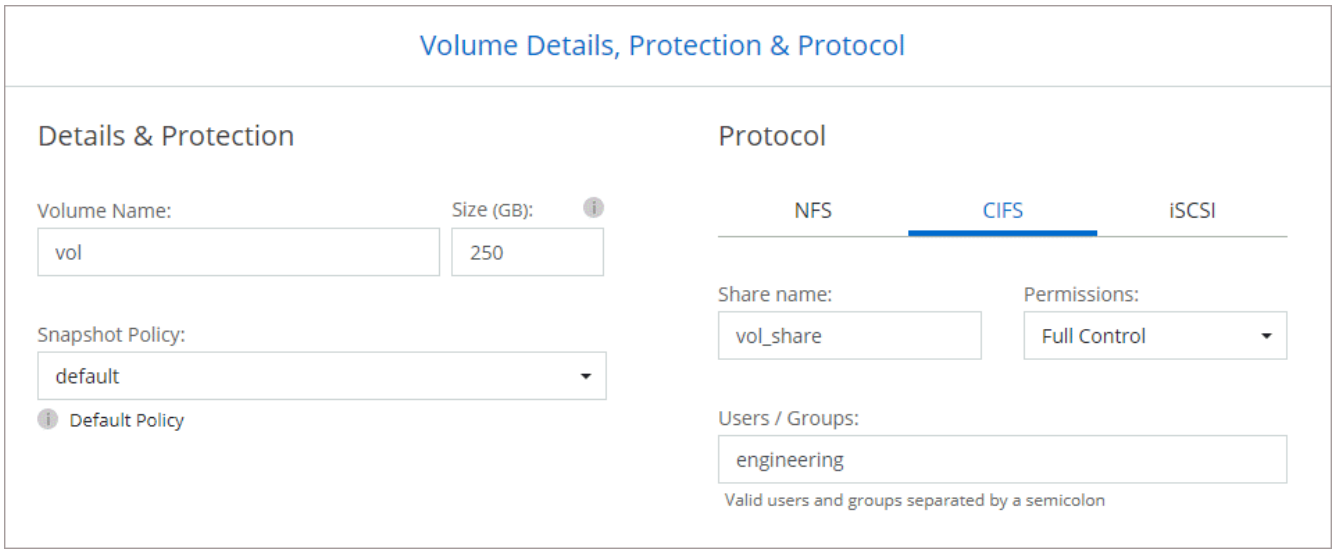
16. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

    "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)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt 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".

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



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

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. Wenn Sie von AWS verwaltete Microsoft AD als AD-Server für Cloud Volumes ONTAP konfigurieren, sollten Sie in diesem Feld **OU=Computers,OU=corp** eingeben.
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.
NTP-Server	Wählen Sie **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. 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.

18. **Nutzungsprofil, Disk Type und Tiering Policy**: Wählen Sie, ob Sie Funktionen für die Storage-Effizienz aktivieren und die Volume Tiering Policy bei Bedarf bearbeiten möchten.

Weitere Informationen finden Sie unter "Allgemeines zu Volume-Nutzungsprofilen" Und "Data Tiering - Übersicht".

19. **Überprüfen & Genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um Details zum Support und den AWS Ressourcen zu erhalten, die BlueXP kaufen wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie Auf **Go**.

Ergebnis

BlueXP startet die Cloud Volumes ONTAP-Instanz. Sie können den Fortschritt in der Timeline verfolgen.

Wenn beim Starten der Cloud Volumes ONTAP Instanz Probleme auftreten, 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 Cloud Volumes ONTAP HA-Paars in AWS

Wenn Sie ein Cloud Volumes ONTAP HA-Paar in AWS starten möchten, müssen Sie eine HA-Arbeitsumgebung in BlueXP erstellen.

Einschränkung

Derzeit werden HA-Paare nicht mit Ausposten von AWS unterstützt.

Über diese Aufgabe

Unmittelbar nach der Erstellung der Arbeitsumgebung startet BlueXP eine Testinstanz in der angegebenen VPC, um die Konnektivität zu überprüfen. Wenn der Vorgang erfolgreich war, beendet BlueXP die Instanz sofort und beginnt dann mit der Bereitstellung des Cloud Volumes ONTAP-Systems. Wenn BlueXP die Verbindung nicht überprüfen kann, schlägt die Erstellung der Arbeitsumgebung fehl. Die Testinstanz ist entweder t2.nano (für Standard-VPC-Mandantenfähigkeit) oder m3.medium (für dedizierte VPC-Mandantenfähigkeit).

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 Anweisungen.
3. **Wählen Sie einen Standort**: Wählen Sie **Amazon Web Services** und **Cloud Volumes ONTAP HA**.
4. **Details und Anmeldeinformationen**: Optional können Sie die AWS-Anmeldeinformationen und das Abonnement ändern, einen Namen der Arbeitsumgebung eingeben, bei Bedarf Tags hinzufügen und dann

ein Passwort eingeben.

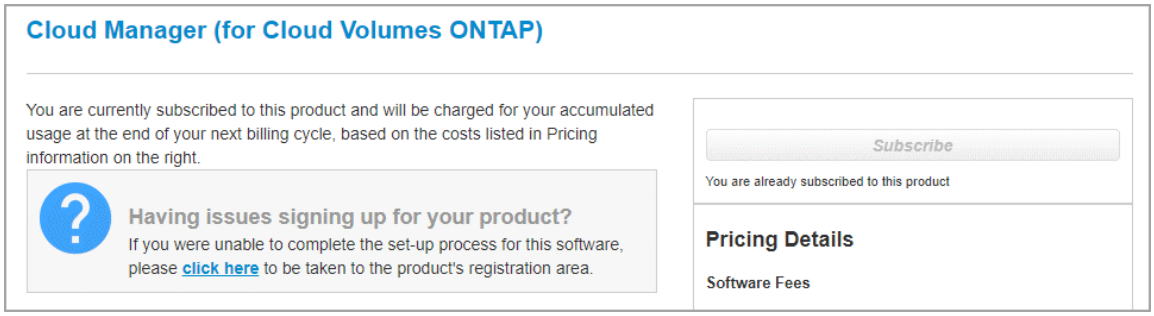
Einige der Felder auf dieser Seite sind selbsterklärend. In der folgenden Tabelle werden Felder beschrieben, für die Sie möglicherweise Hilfe benötigen:

Feld	Beschreibung
Name der Arbeitsumgebung	BlueXP verwendet den Namen der Arbeitsumgebung, um sowohl das Cloud Volumes ONTAP System als auch die Amazon EC2 Instanz zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.
Tags hinzufügen	AWS-Tags sind Metadaten für Ihre AWS-Ressourcen. BlueXP fügt die Tags zur Cloud Volumes ONTAP-Instanz und jeder der Instanz zugeordneten AWS-Ressource hinzu. Sie können bis zu vier Tags aus der Benutzeroberfläche hinzufügen, wenn Sie eine Arbeitsumgebung erstellen. Nach der Erstellung können Sie weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen einer Arbeitsumgebung nicht auf vier Tags beschränkt. Informationen zu Tags finden Sie unter "AWS Dokumentation: Tagging der Amazon EC2 Ressourcen".
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 „*admin*“ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Anmeldedaten Bearbeiten	AWS Zugangsdaten und das Marketplace-Abonnement für dieses Cloud Volumes ONTAP System auswählen Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen mit einem neuen AWS Marketplace-Abonnement zu verknüpfen. Bei dem Abonnement kann es sich um einen Jahresvertrag oder um die Bezahlung von Cloud Volumes ONTAP auf Stundenbasis handelt. Wenn eine Lizenz direkt über NetApp (BYOL) erworben wird, ist kein AWS Abonnement erforderlich. "Erfahren Sie, wie Sie BlueXP zusätzliche AWS Zugangsdaten hinzufügen".

Im folgenden Video wird gezeigt, wie Sie ein Pay-as-you-go Marketplace Abonnement mit Ihren AWS Zugangsdaten verknüpfen:

Abonnieren Sie BlueXP über den AWS Marketplace

Wenn mehrere IAM-Benutzer im gleichen AWS-Konto arbeiten, muss jeder Benutzer sich anmelden. Wenn der erste Benutzer sich abonniert hat, informiert der AWS Marketplace die nachfolgenden Benutzer, dass sie bereits abonniert sind, wie in der Abbildung unten dargestellt. Während für das AWS *Account* ein Abonnement erfolgt, muss sich jeder IAM-Benutzer mit diesem Abonnement verknüpfen. Wenn Sie die unten angezeigte Meldung sehen, klicken Sie auf den Link **click here**, um zur BlueXP-Website zu gelangen und den Vorgang
abzuschließen.



5. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie mit diesem Cloud Volumes ONTAP-System nicht verwenden möchten.
   - "Weitere Informationen zur BlueXP Klassifizierung"
   - "Erfahren Sie mehr über Backup und Recovery von BlueXP"

   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-Bereitstellungsmodelle**: Wählen Sie eine HA-Konfiguration.

   Einen Überblick über die Implementierungsmodelle finden Sie unter "Cloud Volumes ONTAP HA für AWS".

7. **Standort und Konnektivität** (Single AZ) oder **Region & VPC** (Multiple AZS): Geben Sie die Netzwerkinformationen ein, die Sie im AWS-Arbeitsblatt aufgezeichnet haben.

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

Feld	Beschreibung
Sicherheitsgruppe wurde generiert	Wenn Sie BlueXP die Sicherheitsgruppe für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Selected VPC Only** wählen, ist die Quelle 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 die Quelle für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Vorhandene Sicherheitsgruppe verwenden	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".

8. **Konnektivität und SSH Authentifizierung**: Wählen Sie Verbindungsmethoden für das HA-Paar und den Mediator.
9. **Schwebende IPs**: Wenn Sie mehrere AZS gewählt haben, geben Sie die fließenden IP-Adressen an.

   Die IP-Adressen müssen für alle VPCs in der Region außerhalb des CIDR-Blocks liegen. Weitere Informationen finden Sie unter "AWS Netzwerkanforderungen für Cloud Volumes ONTAP HA in mehreren AZS".

10. **Routentabellen**: Wenn Sie mehrere AZS gewählt haben, wählen Sie die Routentabellen aus, die Routen zu den schwimmenden IP-Adressen enthalten sollen.

    Wenn Sie mehr als eine Routentabelle haben, ist es sehr wichtig, die richtigen Routentabellen auszuwählen. Andernfalls haben einige Clients möglicherweise keinen Zugriff auf das Cloud Volumes ONTAP HA-Paar. Weitere Informationen zu Routingtabellen finden Sie unter "AWS Documentation: Routingtabellen".

11. **Datenverschlüsselung**: Wählen Sie keine Datenverschlüsselung oder Verschlüsselung von AWS.

    Für die von AWS gemanagte Verschlüsselung können Sie einen anderen Customer Master Key (CMK) von Ihrem Konto oder einem anderen AWS Konto auswählen.

    > Sie können die AWS Datenverschlüsselungsmethode nicht ändern, nachdem Sie ein Cloud Volumes ONTAP System erstellt haben.

    "So richten Sie AWS KMS für Cloud Volumes ONTAP ein".

    "Erfahren Sie mehr über unterstützte Verschlüsselungstechnologien".

12. **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".
13. **Cloud Volumes ONTAP Konfiguration** (nur Jahresvertrag für AWS Marketplace): Überprüfen Sie die Standardkonfiguration und klicken Sie auf **Weiter** oder klicken Sie auf **Konfiguration ändern**, um Ihre eigene Konfiguration auszuwählen.

    Wenn die Standardkonfiguration beibehalten wird, müssen Sie nur ein Volume angeben und anschließend die Konfiguration prüfen und genehmigen.

14. **Vorkonfigurierte Pakete** (nur stündlich oder BYOL): Wählen Sie eines der Pakete aus, um schnell Cloud Volumes ONTAP zu starten, oder klicken Sie auf **Konfiguration ändern**, um Ihre eigene Konfiguration auszuwählen.

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

15. **IAM-Rolle**: Es ist am besten, die Standardoption zu behalten, mit der BlueXP die Rolle für Sie erstellen lässt.

    Wenn Sie Ihre eigene Richtlinie verwenden möchten, muss diese erfüllen "Richtlinienanforderungen für Cloud Volumes ONTAP-Nodes und den HA-Mediator".

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

Instanztyp und die Instanzenfähigkeit aus.

> 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.

17. **Zugrunde liegende Speicherressourcen**: Wählen Sie einen Festplattentyp, konfigurieren Sie den zugrunde liegenden Speicher und wählen Sie, ob das Daten-Tiering aktiviert bleiben soll.

    Beachten Sie Folgendes:

    - Der Festplattentyp wird für das ursprüngliche Volume (und Aggregat) durchgeführt. Für nachfolgende Volumes (und Aggregate) kann ein anderer Festplattentyp ausgewählt werden.
    - Wenn Sie eine gp3- oder io1-Festplatte auswählen, verwendet BlueXP die Funktion Elastic Volumes in AWS, um bei Bedarf automatisch die zugrunde liegende Storage-Festplattenkapazität zu erhöhen. Sie können die ursprüngliche Kapazität auf Grundlage Ihrer Storage-Anforderungen auswählen und nach der Bereitstellung von Cloud Volumes ONTAP überarbeiten. "Erfahren Sie mehr über die Unterstützung von Elastic Volumes in AWS".
    - Wenn Sie eine gp2- oder st1-Festplatte auswählen, können Sie eine Festplattengröße für alle Festplatten im ursprünglichen Aggregat sowie für alle zusätzlichen Aggregate auswählen, die BlueXP erstellt, wenn Sie die einfache Bereitstellungsoption verwenden. Mithilfe der erweiterten Zuweisungsoption können Sie Aggregate erstellen, die eine andere Festplattengröße verwenden.
    - 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.

      "So funktioniert Daten-Tiering".

18. **Schreibgeschwindigkeit und WURM**:

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

       "Erfahren Sie mehr über Schreibgeschwindigkeit".

    b. 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.

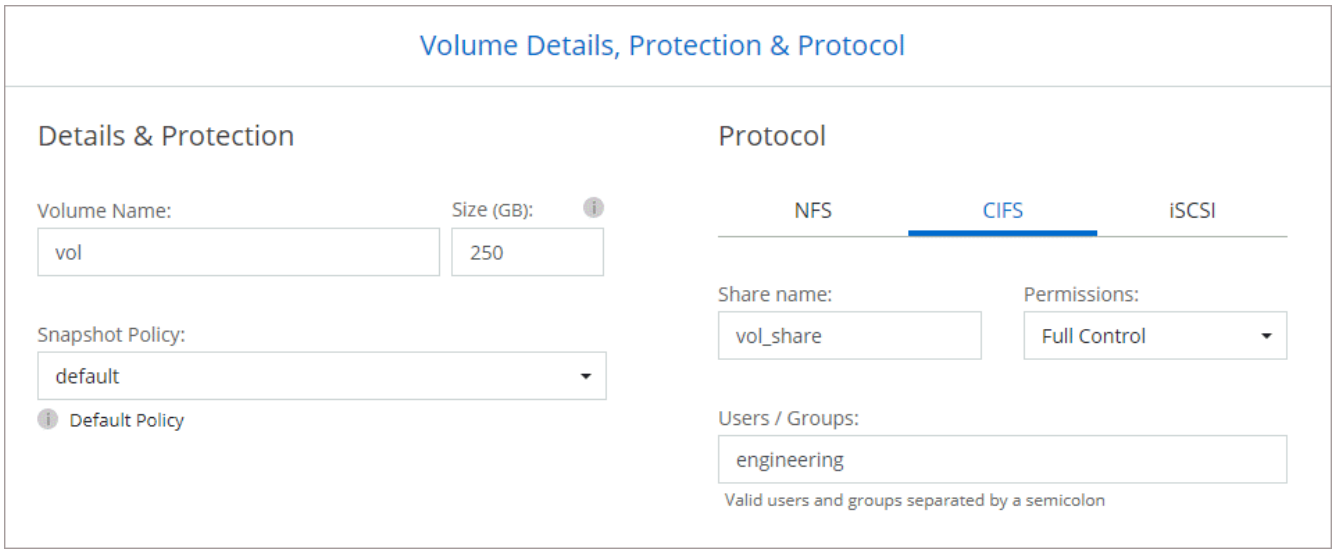
19. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

    "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)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt 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".

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



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

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. Wenn Sie von AWS verwaltete Microsoft AD als AD-Server für Cloud Volumes ONTAP konfigurieren, sollten Sie in diesem Feld **OU=Computers,OU=corp** eingeben.
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.
NTP-Server	Wählen Sie **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. 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.

21. **Nutzungsprofil, Disk Type und Tiering Policy**: Wählen Sie, ob Sie Funktionen für die Storage-Effizienz aktivieren und die Volume Tiering Policy bei Bedarf bearbeiten möchten.

Weitere Informationen finden Sie unter "Wählen Sie ein Volume-Auslastungsprofil aus" Und "Data Tiering - Übersicht".

22. **Überprüfen & Genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um Details zum Support und den AWS Ressourcen zu erhalten, die BlueXP kaufen wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. Klicken Sie Auf **Go**.

Ergebnis

BlueXP startet das Cloud Volumes ONTAP HA-Paar. Sie können den Fortschritt in der Timeline verfolgen.

Wenn beim Starten des HA-Paars Probleme auftreten, überprüfen 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.

Erste Schritte mit Cloud Volumes ONTAP in der AWS C2S Umgebung

Ähnlich wie eine Standard-Region von AWS können Sie Cloud Manager in verwenden "AWS: Kommerzielle Cloud-Services (C2S)" Umgebung zum Implementieren von Cloud Volumes ONTAP, die Funktionen der Enterprise-Klasse für Ihren Cloud Storage bietet. AWS C2S ist eine geschlossene Region speziell für die USA Intelligence Community; die Anweisungen auf dieser Seite gelten nur für Benutzer der Region AWS C2S.

Unterstützte Versionen in C2S

- Cloud Volumes ONTAP 9.8 wird unterstützt
- Version 3.9.4 des Connectors wird unterstützt

  Der Connector ist eine Software, die für die Implementierung und das Management von Cloud Volumes ONTAP in AWS benötigt wird. Sie melden sich bei Cloud Manager von der Software an, die auf der Connector-Instanz installiert wird. Die SaaS-Website für Cloud Manager wird in der C2S-Umgebung nicht unterstützt.

> Cloud Manager wurde kürzlich in BlueXP umbenannt, doch in C2S wird dieser Begriff weiterhin als Cloud Manager bezeichnet, da die Benutzeroberfläche, die in Version 3.9.4 des Connectors enthalten ist, noch Cloud Manager genannt wird.

Unterstützte Funktionen in C2S

Die folgenden Funktionen sind bei Cloud Manager in der C2S-Umgebung verfügbar:

- Cloud Volumes ONTAP
- Datenreplizierung
- Ein Zeitplan für das Auditing

Für Cloud Volumes ONTAP können Sie ein Single Node-System oder ein HA-Paar erstellen. Beide Lizenzoptionen sind verfügbar: Nutzungsbasiert und als BYOL (Bring-Your-Own-License).

Das Daten-Tiering zu S3 wird auch von Cloud Volumes ONTAP in C2S unterstützt.

Einschränkungen

- Keiner der Cloud-Services von NetApp ist über Cloud Manager verfügbar.
- Da es in der C2S-Umgebung keinen Internetzugang gibt, sind auch die folgenden Funktionen nicht verfügbar:
  - Automatisierte Software-Upgrades von Cloud Manager
  - NetApp AutoSupport
  - AWS Kosteninformationen für Cloud Volumes ONTAP Ressourcen
- Freimium-Lizenzen werden in der C2S-Umgebung nicht unterstützt.

Implementierungsübersicht

Erste Schritte mit Cloud Volumes ONTAP in der C2S sind in wenigen Schritten möglich.

1. Bereiten Sie Ihre AWS-Umgebung vor

   Dazu gehören die Einrichtung des Netzwerks, die Anmeldung bei Cloud Volumes ONTAP, die Einrichtung von Berechtigungen und die optionale Einrichtung des AWS KMS.

2. Installieren des Connectors und Einrichten von Cloud Manager

   Bevor Sie mit Cloud Manager beginnen können, um Cloud Volumes ONTAP zu implementieren, müssen Sie einen *Connector* erstellen. Mit dem Connector kann Cloud Manager Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen (einschließlich Cloud Volumes ONTAP).

   Sie melden sich bei Cloud Manager von der Software an, die auf der Connector-Instanz installiert wird.

3. Cloud Volumes ONTAP über Cloud Manager starten

Jeder dieser Schritte wird im Folgenden beschrieben.

Bereiten Sie Ihre AWS-Umgebung vor

Ihre AWS-Umgebung muss einige Anforderungen erfüllen.

Richten Sie Ihr Netzwerk ein

Richten Sie Ihr AWS Netzwerk ein, um Cloud Volumes ONTAP ordnungsgemäß zu betreiben.

Schritte

1. Wählen Sie die VPC und Subnetze aus, in denen die Connector-Instanz und die Cloud Volumes ONTAP-Instanzen gestartet werden sollen.
2. Stellen Sie sicher, dass Ihre VPC und Subnetze die Konnektivität zwischen dem Connector und Cloud Volumes ONTAP unterstützen.
3. Richten Sie einen VPC-Endpunkt für den S3-Dienst ein.

   Ein VPC-Endpunkt ist erforderlich, wenn Sie kalte Daten von Cloud Volumes ONTAP auf kostengünstigen Objekt-Storage einstufen möchten.

Abonnieren Sie Cloud Volumes ONTAP

Zur Implementierung von Cloud Volumes ONTAP über Cloud Manager ist ein Marketplace-Abonnement erforderlich.

Schritte

1. Gehen Sie im AWS Intelligence Community Marketplace, und suchen Sie nach Cloud Volumes ONTAP.
2. Wählen Sie das zu implementierende Angebot aus.
3. Überprüfen Sie die Bedingungen und klicken Sie auf **Akzeptieren**.
4. Wiederholen Sie diese Schritte für die anderen Angebote, sofern Sie sie implementieren möchten.

   Sie müssen Cloud Volumes ONTAP-Instanzen mit Cloud Manager starten. Sie dürfen Cloud Volumes ONTAP-Instanzen nicht über die EC2-Konsole starten.

Berechtigungen einrichten

Einrichtung von IAM-Richtlinien und -Rollen, die Connector und Cloud Volumes ONTAP die erforderlichen Berechtigungen für Aktionen in der AWS Commercial Cloud Services-Umgebung bieten

Für die folgenden Bereiche benötigen Sie eine IAM-Richtlinie und eine IAM-Rolle:

- Die Instanz des Connectors
- Cloud Volumes ONTAP Instanzen
- Die Cloud Volumes ONTAP HA Mediator Instanz (wenn Sie HA-Paare implementieren möchten)

Schritte

1. Gehen Sie zur AWS IAM-Konsole und klicken Sie auf **Policies**.
2. Erstellen Sie eine Richtlinie für die Connector-Instanz.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
```

```
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
```

```
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

3. Erstellen einer Richtlinie für Cloud Volumes ONTAP

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

4. Wenn Sie ein Cloud Volumes ONTAP HA-Paar implementieren möchten, erstellen Sie eine Richtlinie für den HA Mediator.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Erstellen Sie IAM-Rollen mit dem Rollentyp Amazon EC2 und hängen Sie die Richtlinien an, die Sie in den vorherigen Schritten erstellt haben.

   Ähnlich wie bei den Richtlinien sollten Sie über eine IAM-Rolle für den Connector, eine für die Cloud Volumes ONTAP-Nodes und eine für den HA-Mediator (wenn Sie HA-Paare bereitstellen möchten) verfügen.

   Sie müssen die Connector IAM-Rolle auswählen, wenn Sie die Connector-Instanz starten.

   Beim Erstellen einer Cloud Volumes ONTAP Arbeitsumgebung in Cloud Manager können Sie die IAM-Rollen für Cloud Volumes ONTAP und den HA-Mediator auswählen.

AWS KMS einrichten

Wenn Sie Amazon Verschlüsselung mit Cloud Volumes ONTAP verwenden möchten, stellen Sie sicher, dass die Anforderungen für den AWS Verschlüsselungsmanagement-Service erfüllt sind.

Schritte

1. Stellen Sie sicher, dass ein aktiver Kunden-Master-Schlüssel (CMK) in Ihrem Konto oder in einem anderen AWS-Konto vorhanden ist.

   Bei CMK kann es sich um ein von AWS gemanagtes CMK oder um ein vom Kunden gemanagtes CMK handeln.

2. Wenn sich das CMK in einem AWS Konto befindet und nicht über das Konto, in dem Sie Cloud Volumes ONTAP implementieren möchten, müssen Sie die ARN dieses Schlüssels erhalten.

   Wenn Sie das Cloud Volumes ONTAP-System erstellen, müssen Sie dem Cloud Manager ARN zur Verfügung stellen.

3. Fügen Sie die IAM-Rolle für die Connector-Instanz der Liste der wichtigsten Benutzer für ein CMK hinzu.

   Dadurch erhält Cloud Manager die Berechtigung, CMK mit Cloud Volumes ONTAP zu verwenden.

Installieren des Connectors und Einrichten von Cloud Manager

Bevor Sie Cloud Volumes ONTAP Systeme in AWS starten können, müssen Sie zuerst die Connector-Instanz aus dem AWS Marketplace starten und dann Cloud Manager einloggen und einrichten.

Schritte

1. Sie erhalten ein Root-Zertifikat, das von einer Zertifizierungsstelle (CA) im Format Privacy Enhanced Mail (PEM) Base-64-codiert X.509 signiert ist. Wenden Sie sich an die Richtlinien und Verfahren Ihres Unternehmens, um das Zertifikat zu erhalten.

   Sie müssen das Zertifikat während des Setup-Vorgangs hochladen. Cloud Manager verwendet das vertrauenswürdige Zertifikat für das Senden von Anfragen an AWS über HTTPS.

2. Starten Sie die Connector-Instanz:
   a. Wechseln Sie zur AWS Intelligence Community Marketplace Seite zu Cloud Manager.
   b. Wählen Sie auf der Registerkarte Benutzerdefinierter Start die Option, um die Instanz von der EC2-Konsole aus zu starten.
   c. Befolgen Sie die Anweisungen, um die Instanz zu konfigurieren.

      Beachten Sie beim Konfigurieren der Instanz Folgendes:

      - Wir empfehlen t3.xlarge.
      - Sie müssen die IAM-Rolle auswählen, die Sie bei der Vorbereitung der AWS-Umgebung erstellt haben.
      - Sie sollten die standardmäßigen Speicheroptionen beibehalten.
      - Für den Connector sind folgende Verbindungsmethoden erforderlich: SSH, HTTP und HTTPS.
3. Richten Sie Cloud Manager von einem Host aus ein, der eine Verbindung zur Connector-Instanz hat:
   a. Öffnen Sie einen Webbrowser, und geben Sie ein https://ipaddress Wobei ipaddress die IP-Adresse des Linux-Hosts ist, auf dem Sie den Connector installiert haben.
   b. Geben Sie einen Proxy-Server für die Verbindung zu AWS-Services an.
   c. Laden Sie das Zertifikat, das Sie in Schritt 1 erhalten haben, hoch.
   d. Führen Sie die Schritte im Setup-Assistenten aus, um Cloud Manager einzurichten.
      - **Systemdetails**: Geben Sie einen Namen für diese Instanz von Cloud Manager ein und geben Sie Ihren Firmennamen ein.
      - **Benutzer erstellen**: Erstellen Sie den Admin-Benutzer, den Sie zur Verwaltung von Cloud Manager verwenden.
      - **Review**: Prüfen Sie die Details und genehmigen Sie die Endbenutzer-Lizenzvereinbarung.
   e. Um die Installation des CA-signierten Zertifikats abzuschließen, starten Sie die Connector-Instanz von der EC2-Konsole aus neu.
4. Melden Sie sich nach dem Neustart des Connectors mit dem Administratorkonto an, das Sie im Setup-Assistenten erstellt haben.

Cloud Volumes ONTAP über Cloud Manager starten

Sie können Cloud Volumes ONTAP-Instanzen in der AWS Commercial Cloud Services-Umgebung durch Erstellen neuer Arbeitsumgebungen in Cloud Manager starten.

Was Sie benötigen

- Wenn Sie eine Lizenz erworben haben, müssen Sie über die Lizenzdatei verfügen, die Sie von NetApp erhalten haben. Die Lizenzdatei ist eine NLF-Datei im JSON-Format.
- Um die schlüsselbasierte SSH-Authentifizierung für den HA Mediator zu ermöglichen, ist ein Schlüsselpaar erforderlich.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen**.
2. Wählen Sie unter Erstellen Cloud Volumes ONTAP oder Cloud Volumes ONTAP HA aus.
3. Führen Sie die Schritte im Assistenten aus, um das Cloud Volumes ONTAP-System zu starten.

   Beachten Sie beim Abschließen des Assistenten Folgendes:

   - Wenn Sie Cloud Volumes ONTAP HA in mehreren Verfügbarkeitszonen implementieren möchten, implementieren Sie die Konfiguration wie folgt, da zum Zeitpunkt der Veröffentlichung nur zwei AZS in der AWS Commercial Cloud Services-Umgebung verfügbar waren:
     - Node 1: Verfügbarkeitszone A
     - Node 2: Verfügbarkeitszone B
     - Mediator: Verfügbarkeit Zone A oder B
   - Sie sollten die Standardoption verlassen, um eine generierte Sicherheitsgruppe zu verwenden.

     Die vordefinierte Sicherheitsgruppe enthält die Regeln, die Cloud Volumes ONTAP für den erfolgreichen Betrieb benötigen. Wenn Sie eine Anforderung haben, Ihre eigene zu verwenden, können Sie den folgenden Abschnitt der Sicherheitsgruppe lesen.
   - Sie müssen die IAM-Rolle auswählen, die Sie bei der Vorbereitung der AWS-Umgebung erstellt haben.
   - Der zugrunde liegende AWS Festplattentyp gilt für das erste Cloud Volumes ONTAP Volume.

     Sie können einen anderen Festplattentyp für nachfolgende Volumes auswählen.
   - Die Performance von AWS Festplatten ist an die Festplattengröße gebunden.

     Sie sollten die Festplattengröße wählen, die Ihnen die benötigte kontinuierliche Performance bietet. Weitere Details zur EBS-Performance finden Sie in der AWS Dokumentation.
   - Die Festplattengröße ist die Standardgröße für alle Festplatten im System.

     > Wenn Sie später eine andere Größe benötigen, können Sie die Option Erweiterte Zuweisung verwenden, um ein Aggregat zu erstellen, das Festplatten einer bestimmten Größe verwendet.
   - Storage-Effizienzfunktionen verbessern die Storage-Auslastung und senken die benötigte Storage-Kapazität insgesamt.

Ergebnis

Cloud Manager startet die Cloud Volumes ONTAP Instanz. Sie können den Fortschritt in der Timeline verfolgen.

Regeln für Sicherheitsgruppen

Cloud Manager erstellt Sicherheitsgruppen mit den ein- und ausgehenden Regeln, die Cloud Manager und Cloud Volumes ONTAP für den erfolgreichen Betrieb in der Cloud benötigen. Sie können sich zu Testzwecken auf die Ports beziehen oder wenn Sie Ihre eigenen Sicherheitsgruppen verwenden möchten.

Sicherheitsgruppe für den Konnektor

Die Sicherheitsgruppe für den Konnektor erfordert sowohl ein- als auch ausgehende Regeln.

Regeln für eingehende Anrufe

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

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Connector enthält die folgenden ausgehenden Regeln.

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

Sicherheitsgruppe für Cloud Volumes ONTAP

Für die Sicherheitsgruppe für Cloud Volumes ONTAP-Nodes sind sowohl ein- als auch ausgehende Regeln erforderlich.

Regeln für eingehende Anrufe

Wenn Sie eine Arbeitsumgebung erstellen und eine vordefinierte Sicherheitsgruppe auswählen, können Sie den Datenverkehr innerhalb einer der folgenden Optionen zulassen:

- **Nur gewählte VPC**: Die Quelle 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**: Die Quelle für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.

Protokoll	Port	Zweck
Alle ICMP	Alle	Pingen der Instanz
HTTP	80	HTTP-Zugriff auf die System Manager Webkonsole mit der IP-Adresse der Cluster-Management-LIF

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

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für Cloud Volumes ONTAP 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

Externe Sicherheitsgruppe für den HA Mediator

Die vordefinierte externe Sicherheitsgruppe für den Cloud Volumes ONTAP HA Mediator enthält die folgenden Regeln für ein- und ausgehende Anrufe.

Regeln für eingehende Anrufe

Die Quelle für eingehende Regeln ist der Datenverkehr von der VPC, in der sich der Connector befindet.

Protokoll	Port	Zweck
SSH	22	SSH-Verbindungen zum HA-Vermittler
TCP	3000	RESTful API-Zugriff über den Connector

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den HA-Vermittler enthält die folgenden Regeln für ausgehende Anrufe.

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

Interne Sicherheitsgruppe für den HA Mediator

Die vordefinierte interne Sicherheitsgruppe für den Cloud Volumes ONTAP HA Mediator enthält die folgenden Regeln. Cloud Manager erstellt immer diese Sicherheitsgruppe. Sie haben nicht die Möglichkeit, Ihre eigene zu verwenden.

Regeln für eingehende Anrufe

Die vordefinierte Sicherheitsgruppe enthält die folgenden Regeln für eingehende Anrufe.

Protokoll	Port	Zweck
Gesamter Datenverkehr	Alle	Kommunikation zwischen HA-Mediator und HA-Knoten

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Gesamter Datenverkehr	Alle	Kommunikation zwischen HA-Mediator und HA-Knoten

Erste Schritte in Microsoft Azure

Schnellstart für Cloud Volumes ONTAP in Azure

Erste Schritte mit Cloud Volumes ONTAP für Azure

1 **Einen Konnektor erstellen**

Wenn Sie keine haben "Stecker" Dennoch muss ein Kontoadministrator einen erstellen. "Erfahren Sie, wie Sie

in Azure einen Connector 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. "Weitere Informationen .".

3 Richten Sie Ihr Netzwerk ein

1. Stellen Sie sicher, dass Ihre vnet und Subnetze Verbindungen zwischen dem Connector und Cloud Volumes ONTAP unterstützen.
2. 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 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"
- "Erstellen eines Connectors über den Azure Marketplace"
- "Installieren der Connector-Software auf einem Linux-Host"
- "Was BlueXP mit Berechtigungen macht"

Planen Sie Ihre Cloud Volumes ONTAP-Konfiguration in Azure

Wenn Sie Cloud Volumes ONTAP in Azure 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 Microsoft Azure Regionen unterstützt. "Hier finden Sie die vollständige Liste der unterstützten Regionen".

Wählen Sie einen unterstützten VM-Typ aus

Cloud Volumes ONTAP unterstützt je nach Lizenztyp mehrere VM-Typen.

"Unterstützte Konfigurationen für Cloud Volumes ONTAP in Azure"

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 Azure"

Größe Ihres Systems in Azure

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

Typ der virtuellen Maschine

Sehen Sie sich die unterstützten Typen von Virtual Machines in an "Versionshinweise zu Cloud Volumes ONTAP" Und überprüfen Sie anschließend Details zu jedem unterstützten VM-Typ. Beachten Sie, dass jeder VM-Typ eine bestimmte Anzahl an Datenfestplatten unterstützt.

- "Azure-Dokumentation: Allgemeine Größe virtueller Maschinen"
- "Azure-Dokumentation: Für den Speicher optimierte Größen virtueller Maschinen"

Azure Festplattentyp mit Single-Node-Systemen

Wenn Sie Volumes für Cloud Volumes ONTAP erstellen, müssen Sie den zugrunde liegenden Cloud-Storage auswählen, den Cloud Volumes ONTAP als Festplatte verwendet.

Systeme mit einem Node können drei Typen von Azure Managed Disks verwenden:

- *Premium SSD Managed Disks* bieten hohe Performance für I/O-intensive Workloads zu höheren Kosten.
- *Standard SSD Managed Disks* bieten konsistente Performance für Workloads, die niedrige IOPS erfordern.
- *Standard HDD Managed Disks* sind eine gute Wahl, wenn Sie keine hohen IOPS benötigen und Ihre Kosten senken möchten.

Weitere Details zu den Anwendungsfällen für diese Festplatten finden Sie unter "Microsoft Azure-Dokumentation: Welche Festplattentypen sind in Azure verfügbar?".

Azure-Festplattentyp mit HA-Paaren

HA-Systeme verwenden Shared Managed Disks mit Premium-SSDs, die beide eine hohe Performance für I/O-intensive Workloads mit höheren Kosten bieten. HA-Implementierungen, die vor der Version 9.12.1 erstellt wurden, verwenden Premium-Blobs auf Seite.

Festplattengröße Azure

Wenn Sie Cloud Volumes ONTAP Instanzen starten, müssen Sie die standardmäßige Festplattengröße für Aggregate auswählen. BlueXP verwendet diese Festplattengröße für das anfängliche Aggregat und für alle zusätzlichen Aggregate, die es beim Verwenden der einfachen Bereitstellungsoption erstellt. Sie können Aggregate erstellen, die eine Festplattengröße verwenden, die sich von der Standardgröße unterscheidet "Verwenden der erweiterten Zuweisungsoption".

> Alle Festplatten in einem Aggregat müssen dieselbe Größe haben.

Bei der Auswahl der Festplattengröße sollten Sie mehrere Faktoren berücksichtigen. Die Festplattengröße wirkt sich darauf aus, wie viel Sie für Storage zahlen, wie viele Volumes Sie in einem Aggregat erstellen können, wie viel Kapazität insgesamt für Cloud Volumes ONTAP zur Verfügung steht und wie hoch die Storage-Performance ist.

Die Performance von Azure Premium Storage ist an die Festplattengröße gebunden. Größere Festplatten bieten höhere IOPS und einen höheren Durchsatz. Beispiel: Durch das Auswählen von 1 tib Festplatten kann eine bessere Performance als 500 gib Festplatten zu höheren Kosten erzielt werden.

Es gibt keine Performance-Unterschiede zwischen den Festplattengrößen für Standard-Storage. Sie sollten die Festplattengröße basierend auf der benötigten Kapazität auswählen.

Unter Azure finden Sie IOPS und Durchsatz nach Festplattengröße:

- "Microsoft Azure: Preisgestaltung für Managed Disks"
- "Microsoft Azure: Page Blobs Pricing"

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 Azure an".

> Für den Connector ist außerdem eine Systemfestplatte erforderlich. "Zeigen Sie Details zur Standardkonfiguration des Connectors an".

Sammeln von Netzwerkinformationen

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

Azure Informationen	Ihr Wert
Region	
Virtuelles Netzwerk (VNet)	

Azure Informationen	Ihr Wert
Subnetz	
Netzwerksicherheitsgruppe (wenn Sie Ihre eigene verwenden)	

Wählen Sie eine Schreibgeschwindigkeit

Mit BlueXP können Sie eine Schreibgeschwindigkeitseinstellung für Cloud Volumes ONTAP auswählen. 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 Azure

Richten Sie Ihr Azure Netzwerk ein, um Cloud Volumes ONTAP Systeme ordnungsgemäß funktionieren zu können.

Anforderungen für Cloud Volumes ONTAP

Die folgenden Netzwerkanforderungen müssen in Azure erfüllt werden.

Outbound-Internetzugang

Cloud Volumes ONTAP Nodes benötigen Outbound-Internetzugang für NetApp AutoSupport, 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 Sicherheitsgruppe des Connectors *eingehende* -Verbindungen über Port 3128 zulässt. Nach der Bereitstellung des Connectors müssen Sie diesen Port öffnen.

Wenn Sie strenge ausgehende Regeln für Cloud Volumes ONTAP definiert haben, müssen Sie auch sicherstellen, dass die Cloud Volumes ONTAP-Sicherheitsgruppe *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 von BlueXP darüber informiert werden, dass AutoSupport-Meldungen nicht gesendet werden können, "Fehler bei der AutoSupport Konfiguration beheben".

IP-Adressen

BlueXP weist Cloud Volumes ONTAP in Azure automatisch die erforderliche Anzahl privater IP-Adressen zu. Sie müssen sicherstellen, dass Ihr Netzwerk über genügend private IP-Adressen verfügt.

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.

> 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.

IP-Adressen für ein Single Node-System

BlueXP weist 5 oder 6 IP-Adressen einem System mit einem Knoten zu:

- Cluster-Management-IP
- Node-Management-IP
- Intercluster IP für SnapMirror
- NFS/CIFS-IP
- ISCSI-IP

> Die iSCSI-IP ermöglicht den Client-Zugriff über das iSCSI-Protokoll. Es wird vom System auch für andere wichtige Netzwerk-Workflows verwendet. Dieses LIF ist erforderlich und sollte nicht gelöscht werden.

- SVM-Management (optional – nicht standardmäßig konfiguriert)

IP-Adressen für HA-Paare

BlueXP weist während der Bereitstellung 4 NICs (pro Node) IP-Adressen zu.

Beachten Sie, dass BlueXP in Azure eine SVM Management-LIF auf HA-Paaren erstellt, nicht jedoch auf Systemen mit einzelnen Nodes.

NIC0

- Node-Management-IP
- Intercluster-IP
- ISCSI-IP

> Die iSCSI-IP ermöglicht den Client-Zugriff über das iSCSI-Protokoll. Es wird vom System auch für andere wichtige Netzwerk-Workflows verwendet. Dieses LIF ist erforderlich und sollte nicht gelöscht werden.

NIC1

- Cluster-Netzwerk-IP

NIC2

- Cluster Interconnect IP (HA-IC)

NIC3

- PageBLOB NIC-IP (Festplattenzugriff)

> NIC3 gilt nur für HA-Implementierungen, die BLOB Storage auf Seite verwenden.

Die oben genannten IP-Adressen migrieren nicht bei Failover-Ereignissen.

Zusätzlich werden 4 Frontend-IPs (FIPS) für die Migration bei Failover-Ereignissen konfiguriert. Diese Frontend-IPs sind im Load Balancer aktiv.

- Cluster-Management-IP
- NodeA Daten-IP (NFS/CIFS)
- NodeB-Daten-IP (NFS/CIFS)
- SVM-Management-IP

Sichere Verbindung zu Azure Services

Standardmäßig aktiviert BlueXP einen Azure Private Link für Verbindungen zwischen Blob-Storage-Konten auf der Cloud Volumes ONTAP- und Azure-Seite.

In den meisten Fällen ist nichts für Sie erforderlich – BlueXP managt den Azure Private Link für Sie. Aber wenn Sie Azure Private DNS verwenden, dann müssen Sie eine Konfigurationsdatei bearbeiten. Sie sollten auch eine Anforderung für den Connector-Standort in Azure kennen.

Sie können die Private Link-Verbindung auch deaktivieren, wenn dies von Ihren geschäftlichen Anforderungen erforderlich ist. Wenn Sie den Link deaktivieren, konfiguriert BlueXP stattdessen Cloud Volumes ONTAP für die

Verwendung eines Service-Endpunkts.

"Weitere Informationen zur Verwendung von Azure Private Links oder Service-Endpunkten mit Cloud Volumes ONTAP".

Verbindungen zu anderen ONTAP Systemen

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

Anweisungen finden Sie unter "Microsoft Azure Dokumentation: Erstellen Sie eine Site-to-Site-Verbindung im Azure-Portal".

Port für den HA Interconnect

Ein Cloud Volumes ONTAP HA-Paar enthält einen HA Interconnect, der jedem Knoten erlaubt, kontinuierlich zu überprüfen, ob sein Partner funktioniert und um Protokolldaten für den anderen nichtflüchtigen Speicher zu spiegeln. Das HA Interconnect verwendet TCP Port 10006 für die Kommunikation.

Standardmäßig ist die Kommunikation zwischen den HA Interconnect LIFs offen, und es gibt keine Sicherheitsgruppenregeln für diesen Port. Wenn Sie jedoch eine Firewall zwischen den HA Interconnect LIFs erstellen, müssen Sie sicherstellen, dass TCP Traffic für Port 10006 offen ist, damit das HA-Paar ordnungsgemäß arbeiten kann.

Nur ein HA-Paar in einer Azure-Ressourcengruppe

Sie müssen für jedes Cloud Volumes ONTAP HA-Paar, das Sie in Azure implementieren, eine *dedizierte* Ressourcengruppe verwenden. Es wird nur ein HA-Paar in einer Ressourcengruppe unterstützt.

Bei BlueXP treten Verbindungsprobleme auf, wenn Sie versuchen, ein zweites Cloud Volumes ONTAP HA-Paar in einer Azure Ressourcengruppe bereitzustellen.

Regeln für Sicherheitsgruppen

BlueXP erstellt Azure-Sicherheitsgruppen mit den ein- und ausgehenden Regeln, die für den erfolgreichen Betrieb von Cloud Volumes ONTAP erforderlich sind. Sie können sich zu Testzwecken auf die Ports beziehen oder wenn Sie Ihre eigenen Sicherheitsgruppen verwenden möchten.

Die Sicherheitsgruppe für Cloud Volumes ONTAP erfordert sowohl eingehende als auch ausgehende Regeln.

Sie suchen Informationen über den Connector? "Zeigen Sie die Sicherheitsgruppenregeln für den Konnektor an"

Eingehende Regeln für Single-Node-Systeme

Wenn Sie eine Arbeitsumgebung erstellen und eine vordefinierte Sicherheitsgruppe auswählen, können Sie den Datenverkehr innerhalb einer der folgenden Optionen zulassen:

- **Nur vnet ausgewählt**: Die Quelle für eingehenden Datenverkehr ist der Subnetz-Bereich des vnet für das Cloud Volumes ONTAP-System und der Subnetz-Bereich des vnet, in dem sich der Connector befindet. Dies ist die empfohlene Option.
- **Alle VNets**: Die Quelle für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
1000 Inbound_SSH	22 TCP	Beliebige Art	SSH-Zugriff auf die IP-Adresse der Cluster Management LIF oder einer Node Management LIF
1001 Inbound_http	80 TCP	Beliebige Art	HTTP-Zugriff auf die System Manager Webkonsole mit der IP-Adresse der Cluster-Management-LIF
1002 Inbound_111_tcp	111 TCP	Beliebige Art	Remote-Prozeduraufruf für NFS
1003 Inbound_111_udp	111 UDP	Beliebige Art	Remote-Prozeduraufruf für NFS
1004 eingehend_139	139 TCP	Beliebige Art	NetBIOS-Servicesitzung für CIFS
1005 Inbound_161-162_tcp	161-162 TCP	Beliebige Art	Einfaches Netzwerkverwaltungsprotokoll
1006 Inbound_161-162_udp	161-162 UDP	Beliebige Art	Einfaches Netzwerkverwaltungsprotokoll
1007 eingehend_443	443 TCP	Beliebige Art	Konnektivität mit dem Connector und HTTPS-Zugriff auf die System Manager Webkonsole unter Verwendung der IP-Adresse der Cluster-Management-LIF
1008 eingehend_445	445 TCP	Beliebige Art	Microsoft SMB/CIFS über TCP mit NETBIOS-Framing
1009 Inbound_635_tcp	635 TCP	Beliebige Art	NFS-Mount
1010 Inbound_635_udp	635 UDP	Beliebige Art	NFS-Mount
1011 eingehend_749	749 TCP	Beliebige Art	Kerberos
1012 Inbound_2049_tcp	2049 TCP	Beliebige Art	NFS-Server-Daemon
1013 Inbound_2049_udp	2049 UDP	Beliebige Art	NFS-Server-Daemon
1014 eingehend_3260	3260 TCP	Beliebige Art	ISCSI-Zugriff über die iSCSI-Daten-LIF
1015 Inbound_4045-4046_tcp	4045-4046 TCP	Beliebige Art	NFS Lock Daemon und Network Status Monitor
1016 Inbound_4045-4046_udp	4045-4046 UDP	Beliebige Art	NFS Lock Daemon und Network Status Monitor

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
1017 eingehend_10000	10000 TCP	Beliebige Art	Backup mit NDMP
1018 eingehend_11104-11105	11104-11105 TCP	Beliebige Art	SnapMirror Datenübertragung
3000 Inbound_Deny_all_tcp	Alle TCP-Ports	Beliebige Art	Blockieren Sie den gesamten anderen TCP-eingehenden Datenverkehr
3001 Inbound_Deny_all_udp	Alle Ports UDP	Beliebige Art	Alle anderen UDP-eingehenden Datenverkehr blockieren
65000 AllowVnetInBound	Alle Ports und Protokolle	VirtualNetwork zu VirtualNetwork	Eingehender Verkehr aus dem vnet
65001 AllowAzureLoad BalancerInBound	Alle Ports und Protokolle	AzureLoadBalancer zu jedem	Datenverkehr vom Azure Standard Load Balancer
65500 DenyAllInBound	Alle Ports und Protokolle	Beliebige Art	Alle anderen eingehenden Datenverkehr blockieren

Eingehende Regeln für HA-Systeme

Wenn Sie eine Arbeitsumgebung erstellen und eine vordefinierte Sicherheitsgruppe auswählen, können Sie den Datenverkehr innerhalb einer der folgenden Optionen zulassen:

- **Nur vnet ausgewählt**: Die Quelle für eingehenden Datenverkehr ist der Subnetz-Bereich des vnet für das Cloud Volumes ONTAP-System und der Subnetz-Bereich des vnet, in dem sich der Connector befindet. Dies ist die empfohlene Option.
- **Alle VNets**: Die Quelle für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.

> HA-Systeme weisen weniger eingehende Regeln als Systeme mit einzelnen Nodes auf, da eingehender Datenverkehr durch den Azure Standard Load Balancer geleitet wird. Aus diesem Grund sollte der Verkehr aus dem Load Balancer geöffnet sein, wie in der Regel "AllowAzureLoadBalancerInBound" gezeigt.

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
100 eingehend_443	443 beliebiges Protokoll	Beliebige Art	Konnektivität mit dem Connector und HTTPS-Zugriff auf die System Manager Webkonsole unter Verwendung der IP-Adresse der Cluster-Management-LIF
101 Inbound_111_tcp	111 beliebiges Protokoll	Beliebige Art	Remote-Prozeduraufruf für NFS
102 Inbound_2049_tcp	2049 beliebiges Protokoll	Beliebige Art	NFS-Server-Daemon

Priorität und Name	Port und Protokoll	Quelle und Ziel	Beschreibung
111 Inbound_SSH	22 beliebiges Protokoll	Beliebige Art	SSH-Zugriff auf die IP-Adresse der Cluster Management LIF oder einer Node Management LIF
121 eingehend_53	53 beliebiges Protokoll	Beliebige Art	DNS und CIFS
65000 AllowVnetInBound	Alle Ports und Protokolle	VirtualNetwork zu VirtualNetwork	Eingehender Verkehr aus dem vnet
65001 AllowAzureLoad BalancerInBound	Alle Ports und Protokolle	AzureLoadBalancer zu jedem	Datenverkehr vom Azure Standard Load Balancer
65500 DenyAllInBound	Alle Ports und Protokolle	Beliebige Art	Alle anderen eingehenden Datenverkehr blockieren

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.

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

Service	Port	Protokoll	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
Konfigurations-Backups	HTTP	80	Node Management-LIF	\Http://<connector-IP-address>/occm/offboxconfig	Senden Sie Konfigurationssicherungen an den Connector. "Informationen zu Backup-Dateien für die Konfiguration".
DHCP	68	UDP	Node Management-LIF	DHCP	DHCP-Client für die erstmalige Einrichtung
DHCPS	67	UDP	Node Management-LIF	DHCP	DHCP-Server
DNS	53	UDP	Node Management LIF und Daten LIF (NFS, CIFS)	DNS	DNS
NDMP	18600-18699	TCP	Node Management-LIF	Zielserver	NDMP-Kopie
SMTP	25	TCP	Node Management-LIF	Mailserver	SMTP-Warnungen können für AutoSupport verwendet werden
SNMP	161	TCP	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	161	UDP	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	162	TCP	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
	162	UDP	Node Management-LIF	Server überwachen	Überwachung durch SNMP-Traps
SnapMirror	11104	TCP	Intercluster-LIF	ONTAP Intercluster-LIFs	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
	11105	TCP	Intercluster-LIF	ONTAP Intercluster-LIFs	SnapMirror Datenübertragung
Syslog	514	UDP	Node Management-LIF	Syslog-Server	Syslog-Weiterleitungsmeldungen

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"
- "Für Sicherheitsgruppen gibt es in Azure Regeln"

Cloud Volumes ONTAP einrichten, um einen vom Kunden gemanagten Schlüssel in Azure zu verwenden

Die Daten werden auf Cloud Volumes ONTAP in Azure automatisch verschlüsselt "Azure Storage Service Encryption" Mit einem von Microsoft gemanagten Schlüssel Aber Sie können Ihren eigenen Verschlüsselungsschlüssel verwenden, indem Sie die Schritte auf dieser Seite befolgen.

Übersicht über die Datenverschlüsselung

Cloud Volumes ONTAP-Daten werden in Azure automatisch verschlüsselt "Azure Storage Service Encryption". Bei der Standardimplementierung wird ein von Microsoft verwalteter Schlüssel verwendet. Es ist keine Einrichtung erforderlich.

Wenn Sie einen vom Kunden gemanagten Schlüssel mit Cloud Volumes ONTAP verwenden möchten, müssen Sie folgende Schritte ausführen:

1. Aus Azure erstellen Sie einen Schlüsselspeicher und generieren Sie anschließend einen Schlüssel in diesem Vault
2. Verwenden Sie für BlueXP die API, um eine Cloud Volumes ONTAP-Arbeitsumgebung zu erstellen, in der der Schlüssel zum Einsatz kommt

Rotation von Schlüsseln

Wenn Sie eine neue Version Ihres Schlüssels erstellen, verwendet Cloud Volumes ONTAP automatisch die neueste Schlüsselversion.

Verschlüsselte Daten

BlueXP verwendet einen Satz Festplattenverschlüsselung, der das Management von Verschlüsselungen mit gemanagten Festplatten und nicht mit Page-Blobs ermöglicht. Neue Festplatten verwenden ebenfalls denselben Festplattenverschlüsselungssatz. Bei niedrigeren Versionen wird der von Microsoft verwaltete Schlüssel anstelle des vom Kunden verwalteten Schlüssels verwendet.

Nachdem Sie eine Cloud Volumes ONTAP Arbeitsumgebung erstellt haben, in der ein vom Kunden gemanagter Schlüssel verwendet wird, werden Cloud Volumes ONTAP Daten wie folgt verschlüsselt.

Cloud Volumes ONTAP-Konfiguration	Systemfestplatten, die für die Schlüsselverschlüsselung verwendet werden	Datenfestplatten, die für die Verschlüsselung des Schlüssels verwendet werden
Single Node	• Booten • Kern • NVRAM	• Stamm • Daten
Azure HA, eine einzelne Verfügbarkeitszone mit Page-Blobs	• Booten • Kern • NVRAM	Keine
Azure HA, eine einzelne Verfügbarkeitszone mit gemeinsam genutzten verwalteten Festplatten	• Booten • Kern • NVRAM	• Stamm • Daten
Azure HA mehrere Verfügbarkeitszonen mit gemeinsam genutzten gemanagten Festplatten	• Booten • Kern • NVRAM	• Stamm • Daten

Alle Azure-Storage-Konten für Cloud Volumes ONTAP werden über einen vom Kunden gemanagten Schlüssel verschlüsselt. Wenn Sie Ihre Speicherkonten während ihrer Erstellung verschlüsseln möchten, müssen Sie in der CVO-Erstellungsanforderung die ID der Ressource erstellen und angeben. Dies gilt für alle Implementierungsarten. Wenn Sie es nicht bereitstellen, werden die Speicherkonten immer noch verschlüsselt, aber BlueXP erstellt zuerst die Speicherkonten mit von Microsoft administrierter Verschlüsselungsmethode und aktualisiert dann die Speicherkonten, um den vom Kunden verwalteten Schlüssel zu verwenden.

Erstellen Sie eine vom Benutzer zugewiesene verwaltete Identität

Sie haben die Möglichkeit, eine Ressource zu erstellen, die als benutzerzugewiesene verwaltete Identität bezeichnet wird. Auf diese Weise können Sie Ihre Storage-Konten verschlüsseln, wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen. Wir empfehlen, diese Ressource zu erstellen, bevor Sie einen Schlüsseltresor erstellen und einen Schlüssel erzeugen.

Die Ressource hat die folgende ID: `userassignedidentity`.

Schritte

1. Gehen Sie in Azure zu Azure Services und wählen Sie **verwaltete Identitäten** aus.
2. Klicken Sie Auf **Erstellen**.
3. Geben Sie folgende Informationen an:
    - **Abonnement**: Wählen Sie ein Abonnement. Wir empfehlen, dasselbe Abonnement wie das Connector-Abonnement zu wählen.
    - **Ressourcengruppe**: Verwenden Sie eine vorhandene Ressourcengruppe oder erstellen Sie eine neue.
    - **Region**: Wählen Sie optional die gleiche Region wie der Connector.

    - **Name**: Geben Sie einen Namen für die Ressource ein.
4. Optional können Sie Tags hinzufügen.
5. Klicken Sie Auf **Erstellen**.

Erstellen eines Schlüsselgewölbes und Generieren eines Schlüssels

Der Schlüsselspeicher muss in demselben Azure Abonnement und derselben Region liegen, in der Sie das Cloud Volumes ONTAP System erstellen möchten.

Wenn Sie Eine vom Benutzer zugewiesene verwaltete Identität wurde erstellt, Beim Erstellen des Schlüsseltresors sollten Sie auch eine Zugangsrichtlinie für den Schlüsseltresor erstellen.

Schritte

1. "Erstellen Sie einen Schlüsselspeicher in Ihrem Azure-Abonnement".

   Beachten Sie die folgenden Anforderungen für den Schlüsselspeicher:

   - Der Schlüsselgewölbe muss sich in derselben Region wie das Cloud Volumes ONTAP System befinden.
   - Die folgenden Optionen sollten aktiviert sein:
     - **Soft-delete** (diese Option ist standardmäßig aktiviert, muss aber nicht_ deaktiviert sein)
     - **Schutz löschen**
     - **Azure Festplattenverschlüsselung für Volume Encryption** (für Single Node-Systeme oder HA-Paare in mehreren Zonen)
   - Die folgende Option sollte aktiviert sein, wenn Sie eine vom Benutzer zugewiesene verwaltete Identität erstellt haben:
     - **Vault-Zugangsrichtlinie**
2. Wenn Sie die Vault-Zugriffsrichtlinie ausgewählt haben, klicken Sie auf Erstellen, um eine Zugriffsrichtlinie für den Schlüsseltresor zu erstellen. Falls nicht, fahren sie mit Schritt 3 fort.
   a. Wählen Sie die folgenden Berechtigungen aus:
      - Get
      - Liste
      - Entschlüsseln
      - Verschlüsseln
      - Taste zum Auspacken
      - Umbruch-Taste
      - Verifizieren
      - signieren
   b. Wählen Sie die vom Benutzer zugewiesene verwaltete Identität (Ressource) als Prinzipal aus.
   c. Überprüfen und erstellen Sie die Zugriffsrichtlinie.
3. "Einen Schlüssel im Schlüsselspeicher erzeugen".

   Beachten Sie die folgenden Anforderungen für den Schlüssel:

- Der Schlüsseltyp muss **RSA** sein.
- Die empfohlene RSA-Schlüsselgröße beträgt **2048**, andere Größen werden unterstützt.

Erstellen Sie eine Arbeitsumgebung, in der der Verschlüsselungsschlüssel verwendet wird

Nachdem Sie den Schlüsselspeicher erstellt und einen Verschlüsselungsschlüssel generiert haben, können Sie ein neues Cloud Volumes ONTAP-System erstellen, das für die Verwendung des Schlüssels konfiguriert ist. Diese Schritte werden von der BlueXP API unterstützt.

Erforderliche Berechtigungen

Wenn Sie einen vom Kunden verwalteten Schlüssel mit einem Cloud Volumes ONTAP-System mit einem einzelnen Knoten verwenden möchten, stellen Sie sicher, dass der BlueXP-Connector über die folgenden Berechtigungen verfügt:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"Zeigen Sie die aktuelle Liste der Berechtigungen an"

Schritte

1. Nutzen Sie den folgenden BlueXP API-Aufruf, um die Liste der Schlüsselvaults in Ihrem Azure-Abonnement zu erhalten.

   Bei einem HA-Paar: `GET /azure/ha/metadata/vaults`

   Für Single Node: `GET /azure/vsa/metadata/vaults`

   Notieren Sie sich den **Namen** und die **resourceGroup**. Im nächsten Schritt müssen Sie diese Werte angeben.

   "Weitere Informationen zu diesem API-Aufruf".

2. Rufen Sie die Liste der Schlüssel im Tresor mithilfe des folgenden BlueXP API-Aufrufs ab.

   Bei einem HA-Paar: `GET /azure/ha/metadata/keys-vault`

   Für Single Node: `GET /azure/vsa/metadata/keys-vault`

   Notieren Sie sich den **Keyname**. Im nächsten Schritt müssen Sie diesen Wert (zusammen mit dem Vault-Namen) angeben.

   "Weitere Informationen zu diesem API-Aufruf".

3. Erstellen Sie ein Cloud Volumes ONTAP-System mithilfe des folgenden BlueXP-API-Aufrufs.

   a. Bei einem HA-Paar:

```
POST /azure/ha/working-environments
```

Der Text der Anforderung muss die folgenden Felder enthalten:

```
"azureEncryptionParameters": {
              "key": "keyName",
              "vaultName": "vaultName"
}
```

> Nehmen Sie die auf `"userAssignedIdentity": " userAssignedIdentityId"` Feld, wenn Sie diese Ressource für die Verschlüsselung von Speicherkontos erstellt haben.

"Weitere Informationen zu diesem API-Aufruf".

b. System mit einem einzelnen Node:

```
POST /azure/vsa/working-environments
```

Der Text der Anforderung muss die folgenden Felder enthalten:

```
"azureEncryptionParameters": {
              "key": "keyName",
              "vaultName": "vaultName"
}
```

> Nehmen Sie die auf `"userAssignedIdentity": " userAssignedIdentityId"` Feld, wenn Sie diese Ressource für die Verschlüsselung von Speicherkontos erstellt haben.

"Weitere Informationen zu diesem API-Aufruf".

Ergebnis

Sie verfügen über ein neues Cloud Volumes ONTAP System, das so konfiguriert ist, dass Sie Ihren vom Kunden gemanagten Schlüssel zur Datenverschlüsselung nutzen können.

Lizenzierung für Cloud Volumes ONTAP in Azure 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.

Freimium

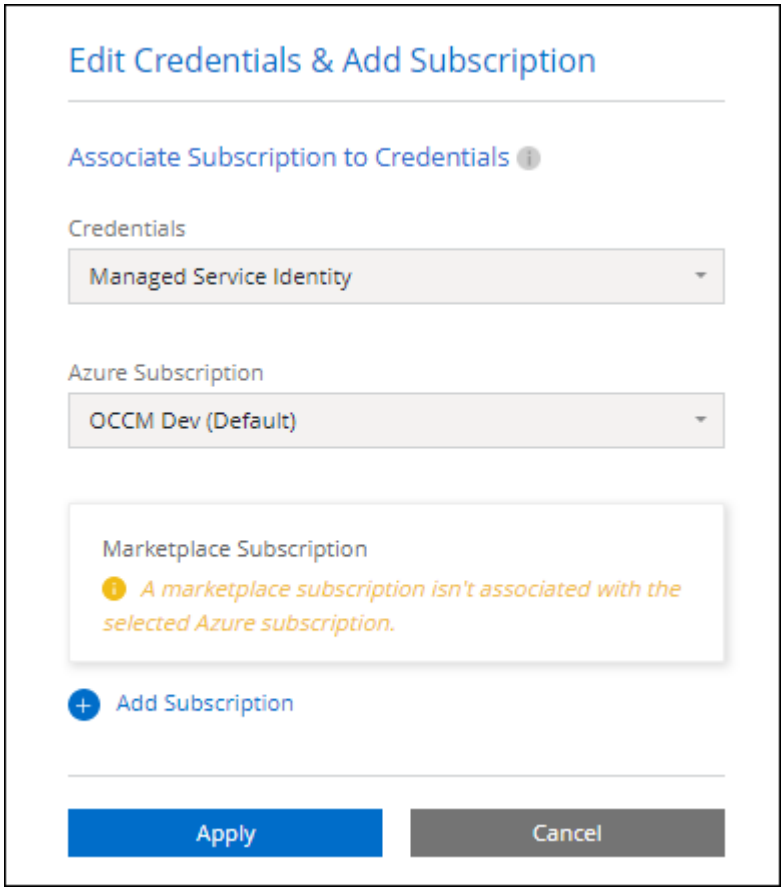
Wählen Sie das Freimium-Angebot aus, um Cloud Volumes ONTAP mit bis zu 500 gib bereitgestellter Kapazität kostenlos zu nutzen. "Erfahren Sie mehr über das Freemium Angebot".

Schritte

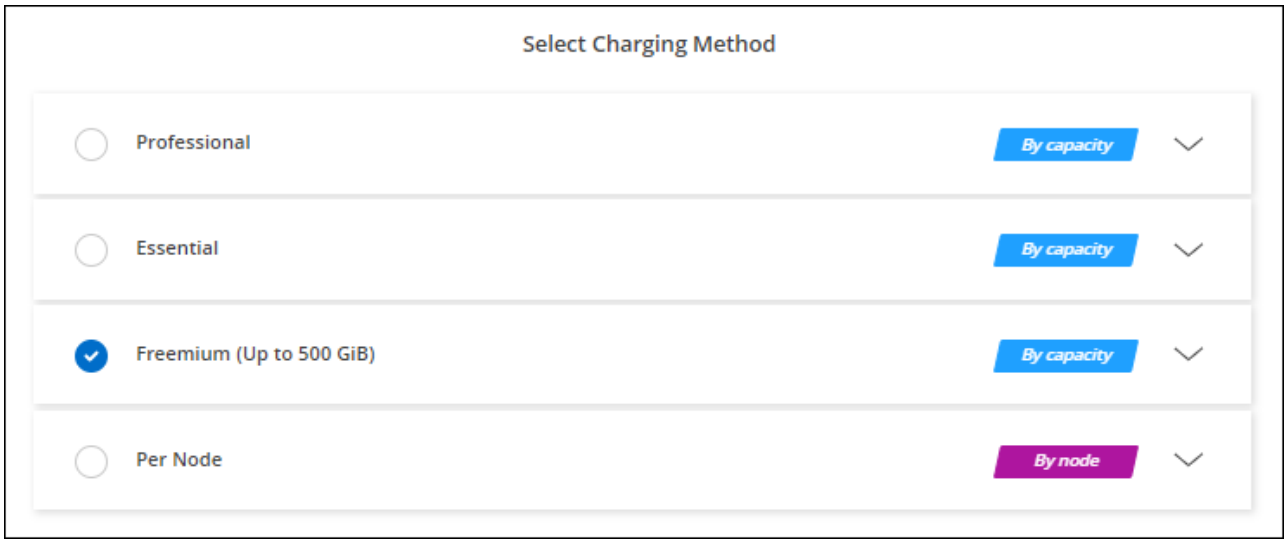
1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in BlueXP.

   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 Azure 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".



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



"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Azure 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) im Azure 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.

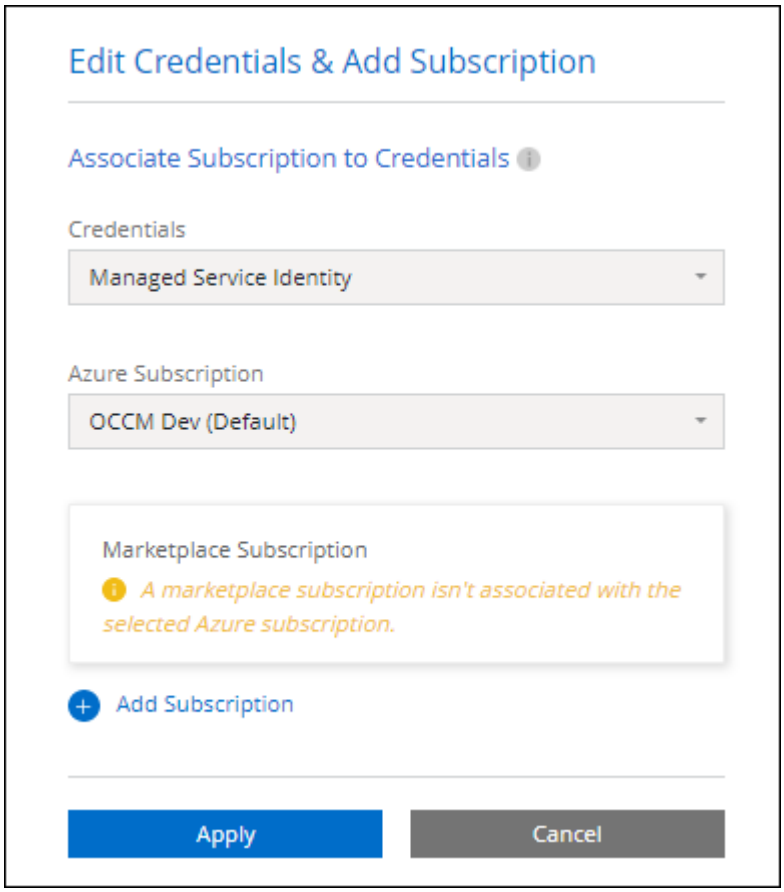
   Bevor Sie Ihre Lizenz mit Cloud Volumes ONTAP verwenden können, muss sie über das Digital Wallet von BlueXP erhältlich sein. Wenn nötig, können Sie "Fügen Sie die Lizenz manuell zum Digital Wallet von BlueXP hinzu".

3. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in

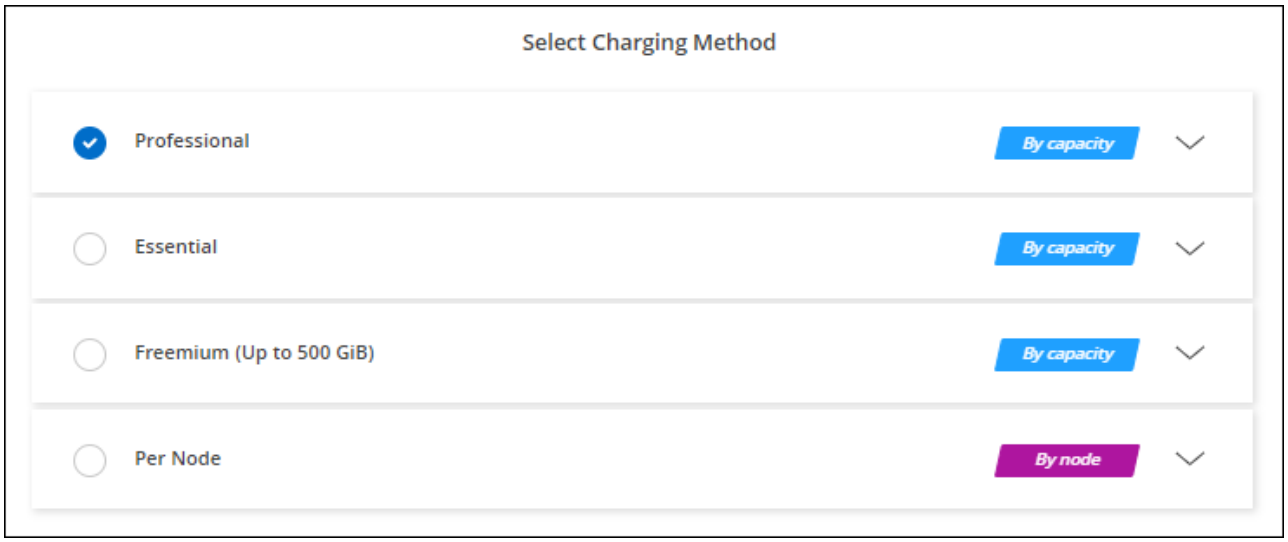
BlueXP.

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 Azure 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.



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



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

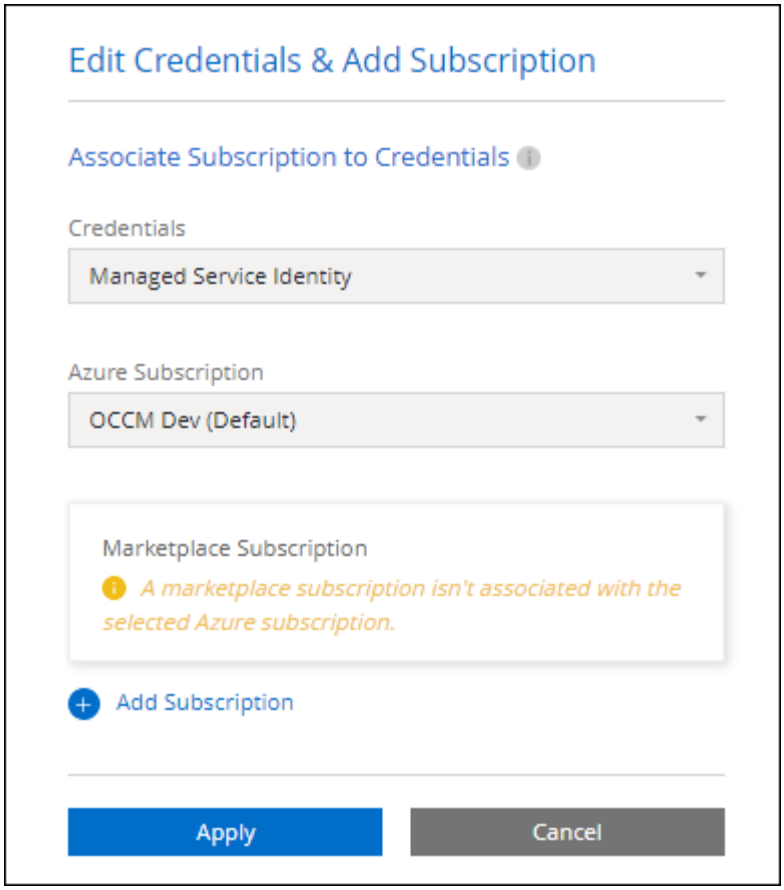
PAYGO-Abonnement

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

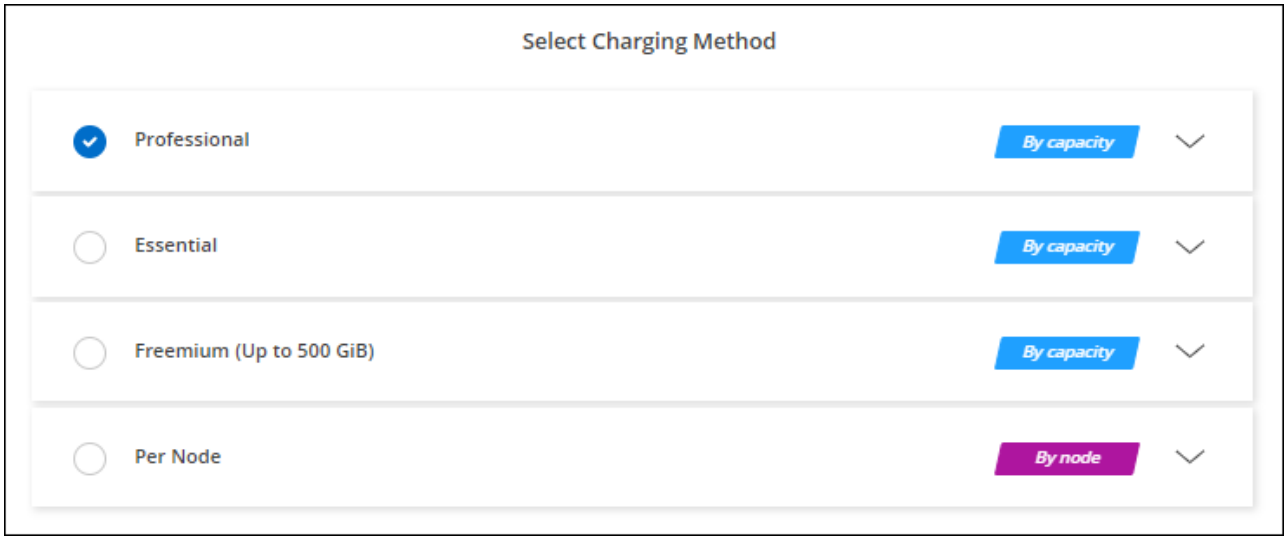
Wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung erstellen, werden Sie von BlueXP aufgefordert, den Vertrag zu abonnieren, der im Azure Marketplace verfügbar ist. Dieses Abonnement wird dann zur Verrechnung mit der Arbeitsumgebung verknüpft. Sie können das gleiche Abonnement auch für zusätzliche Arbeitsumgebungen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



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



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

Sie können die mit Ihren Azure-Konten verbundenen Azure Marketplace-Abonnements auf der Seite „Einstellungen“ > „Anmeldeinformationen“ managen. "Managen Sie Ihre Azure-Konten 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 *privates* Angebot im Azure Marketplace erhältlich.

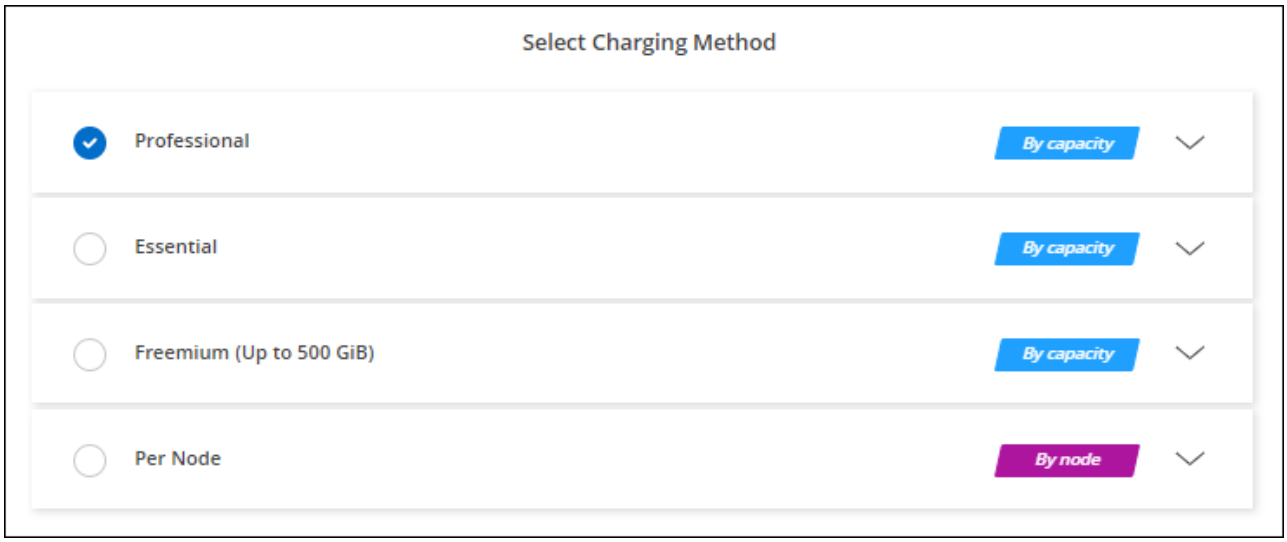
   Wenn NetApp Ihnen das private Angebot teilt, können Sie den Jahresplan auch auswählen, wenn Sie während der Erstellung der Arbeitsumgebung im Azure Marketplace abonnieren.

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 **Anmeldeinformationen bearbeiten > Abonnement hinzufügen > Weiter**.

   b. Wählen Sie im Azure-Portal den Jahresplan aus, der mit Ihrem Azure-Konto geteilt wurde, und klicken Sie anschließend auf **Abonnieren**.

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



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

Keystone Abonnement

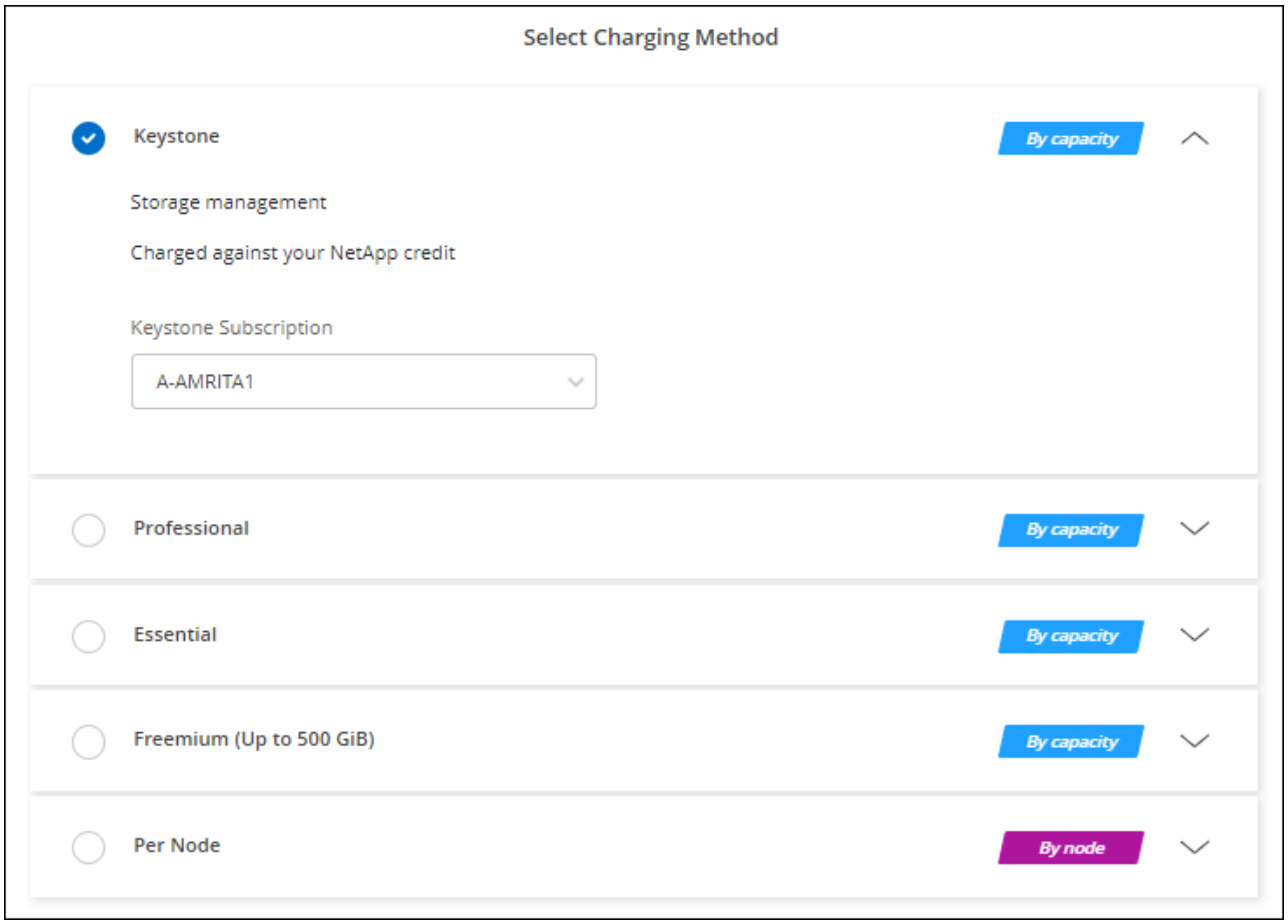
Ein Keystone Abonnement ist ein nutzungsbasierter Abonnementservice. "Weitere Informationen zu NetApp Keystone Abonnements".

Schritte

1. Wenn Sie noch kein Abonnement haben, "Kontakt zu NetApp"
2. Mailto:ng-keystone-success@netapp.com[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.



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

Aktivieren Sie den Hochverfügbarkeits-Modus in Azure

Der Hochverfügbarkeits-Modus von Microsoft Azure sollte aktiviert sein, um ungeplante Failover-Zeiten zu verringern und die NFSv4-Unterstützung für Cloud Volumes ONTAP zu aktivieren.

Ab der Version Cloud Volumes ONTAP 9.10.1 reduzierten wir die ungeplante Failover-Zeit für Cloud Volumes ONTAP HA-Paare, die in Microsoft Azure laufen, und fügten Unterstützung für NFSv4 hinzu. Um diese Verbesserungen für Cloud Volumes ONTAP verfügbar zu machen, müssen Sie die Hochverfügbarkeitsfunktion Ihres Azure Abonnements aktivieren.

In BlueXP werden Sie diese Angaben in einer Meldung „Aktion erforderlich“ eingeben, wenn die Funktion auf einem Azure-Abonnement aktiviert werden muss.

Beachten Sie Folgendes:

- Es gibt keine Probleme mit der Hochverfügbarkeit Ihres Cloud Volumes ONTAP HA-Paars. Diese Azure Funktion arbeitet in Kombination mit ONTAP, um die von Clients beobachteten Applikationsausfallzeiten für NFS-Protokolle zu reduzieren, die aus ungeplanten Failover-Ereignissen resultieren.

- Wenn Sie diese Funktion aktivieren, wird für Cloud Volumes ONTAP HA-Paare keine Unterbrechung verursacht.
- Wenn Sie diese Funktion auf Ihrem Azure-Abonnement aktivieren, treten keine Probleme bei anderen VMs auf.

Ein Azure-Benutzer mit „Owner“-Berechtigungen kann die Funktion über die Azure-CLI aktivieren.

Schritte

1. "Greifen Sie über das Azure-Portal auf die Azure Cloud Shell zu"
2. Registrieren der Funktion des Hochverfügbarkeits-Modus:

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. Überprüfen Sie optional, ob die Funktion jetzt registriert ist:

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Die Azure CLI sollte ein Ergebnis wie die folgenden zurückgeben:

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

Starten von Cloud Volumes ONTAP in Azure

Sie können ein Single-Node-System oder ein HA-Paar in Azure starten, indem Sie eine Cloud Volumes ONTAP-Arbeitsumgebung in BlueXP erstellen.

Was Sie benötigen

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".

- Ein Verständnis der zu verwendenden Konfiguration.

  Sie sollten eine Konfiguration auswählen und Azure Netzwerkinformationen von Ihrem Administrator erhalten haben. 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".

Über diese Aufgabe

Wenn BlueXP in Azure ein Cloud Volumes ONTAP-System erstellt, werden mehrere Azure-Objekte erstellt, z. B. eine Ressourcengruppe, Netzwerkschnittstellen und Speicherkonten. Sie können eine Zusammenfassung der Ressourcen am Ende des Assistenten überprüfen.

> **Risiko von Datenverlusten**
>
> Als Best Practice empfiehlt es sich, für jedes Cloud Volumes ONTAP System eine neue, dedizierte Ressourcengruppe zu verwenden.
>
> Aufgrund des Risikos eines Datenverlusts wird die Bereitstellung von Cloud Volumes ONTAP in einer vorhandenen, gemeinsam genutzten Ressourcengruppe nicht empfohlen. Während BlueXP Cloud Volumes ONTAP-Ressourcen im Falle eines Ausfalls oder Löschvorgangs aus einer gemeinsam genutzten Ressourcengruppe entfernen kann, kann ein Azure Benutzer aus Versehen Cloud Volumes ONTAP-Ressourcen aus einer gemeinsam genutzten Ressourcengruppe löschen.

Starten eines Cloud Volumes ONTAP Systems mit einem Node in Azure

Wenn Sie ein Cloud Volumes ONTAP-System mit einem Node in Azure starten möchten, müssen Sie in BlueXP eine Arbeitsumgebung mit einem einzelnen Knoten erstellen.

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 **Microsoft Azure** und **Cloud Volumes ONTAP Single Node**.
4. Wenn Sie dazu aufgefordert werden, "Einen Konnektor erstellen".
5. **Details und Anmeldeinformationen**: Optional können Sie die Azure-Anmeldedaten und das Abonnement ändern, einen Clusternamen angeben, bei Bedarf Tags hinzufügen und dann Anmeldedaten angeben.

   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 virtuelle Azure-Maschine zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.

Feld	Beschreibung
Tags Für Ressourcengruppen	Tags sind Metadaten für Ihre Azure Ressourcen. Wenn Sie in dieses Feld Tags eingeben, fügt BlueXP diese der Ressourcengruppe hinzu, die dem Cloud Volumes ONTAP-System zugeordnet ist. Sie können bis zu vier Tags aus der Benutzeroberfläche hinzufügen, wenn Sie eine Arbeitsumgebung erstellen. Nach der Erstellung können Sie weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen einer Arbeitsumgebung nicht auf vier Tags beschränkt. Informationen zu Tags finden Sie unter "Microsoft Azure-Dokumentation: Verwenden von Tags zur Organisation Ihrer Azure-Ressourcen".
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 „*admin*“ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Anmeldeinformationen bearbeiten	Sie können verschiedene Azure Zugangsdaten und ein anderes Azure Abonnement für dieses Cloud Volumes ONTAP System wählen. Sie müssen ein Azure Marketplace Abonnement mit dem ausgewählten Azure Abonnement verknüpfen, um ein Pay-as-you-go Cloud Volumes ONTAP System zu implementieren. "Hier erfahren Sie, wie Sie Anmeldedaten hinzufügen".

Im folgenden Video wird gezeigt, wie Sie ein Marketplace-Abonnement zu einem Azure-Abonnement verknüpfen:

Abonnieren Sie BlueXP über den Azure Marketplace

6. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie nicht mit Cloud Volumes ONTAP verwenden möchten.
   - "Weitere Informationen zur BlueXP Klassifizierung"
   - "Erfahren Sie mehr über Backup und Recovery von BlueXP"

   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.

7. **Standort**: Wählen Sie eine Region, eine Verfügbarkeitszone, vnet und ein Subnetz aus, und aktivieren Sie dann das Kontrollkästchen, um die Netzwerkverbindung zwischen dem Connector und dem Zielspeicherort zu bestätigen.

   Bei Single-Node-Systemen können Sie die Verfügbarkeitszone auswählen, in der Sie Cloud Volumes ONTAP implementieren möchten. Wenn Sie keine AZ auswählen, wählt BlueXP eine für Sie aus.

8. **Konnektivität**: Wählen Sie eine neue oder bestehende Ressourcengruppe und wählen Sie dann aus, ob Sie die vordefinierte Sicherheitsgruppe verwenden oder Ihre eigene verwenden möchten.

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

Feld	Beschreibung
Ressourcengruppe	Erstellen Sie eine neue Ressourcengruppe für Cloud Volumes ONTAP, oder verwenden Sie eine vorhandene Ressourcengruppe. Als Best Practice empfiehlt es sich, eine neue, dedizierte Ressourcengruppe für Cloud Volumes ONTAP zu verwenden. Es ist zwar möglich, Cloud Volumes ONTAP in einer vorhandenen, gemeinsam genutzten Ressourcengruppe bereitzustellen, jedoch wird dies aufgrund des Risikos eines Datenverlusts nicht empfohlen. Weitere Informationen finden Sie in der oben stehenden Warnung. Wenn im Azure Konto, das Sie verwenden, der angezeigt wird "Erforderliche Berechtigungen", BlueXP entfernt Cloud Volumes ONTAP-Ressourcen aus einer Ressourcengruppe, bei Ausfall oder Löschung der Bereitstellung.
Sicherheitsgruppe wurde generiert	Wenn Sie BlueXP die Sicherheitsgruppe für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Selected vnet Only** wählen, ist die Quelle für eingehenden Datenverkehr der Subnetz-Bereich des ausgewählten vnet und der Subnetz-Bereich des vnet, in dem sich der Connector befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VNets** wählen, ist die Quelle für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Verwenden Sie vorhandene	Wenn Sie eine vorhandene Sicherheitsgruppe auswählen, muss diese die Cloud Volumes ONTAP-Anforderungen erfüllen. "Zeigen Sie die Standardsicherheitsgruppe an".

9. **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".
10. **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.

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

12. **Vom Azure Marketplace abonnieren**: Folgen Sie den Schritten, wenn BlueXP programmatische Bereitstellungen von Cloud Volumes ONTAP nicht aktivieren kann.

13. **Zugrunde liegende Storage-Ressourcen**: Wählen Sie die Einstellungen für das anfängliche Aggregat: Einen Festplattentyp, eine Größe für jede Festplatte und ob Daten-Tiering zu Blob-Storage aktiviert werden soll.

    Beachten Sie Folgendes:

    - 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 "Dimensionierung Ihres Systems in Azure".

    - 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.

      "Weitere Informationen zum Daten-Tiering".

14. **Schreibgeschwindigkeit und WURM**:

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

       "Erfahren Sie mehr über Schreibgeschwindigkeit".

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

       Diese Option ist nur für bestimmte VM-Typen verfügbar. Informationen darüber, welche VM-Typen unterstützt werden, finden Sie unter "Unterstützte Konfigurationen per Lizenz für HA-Paare".

       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.

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

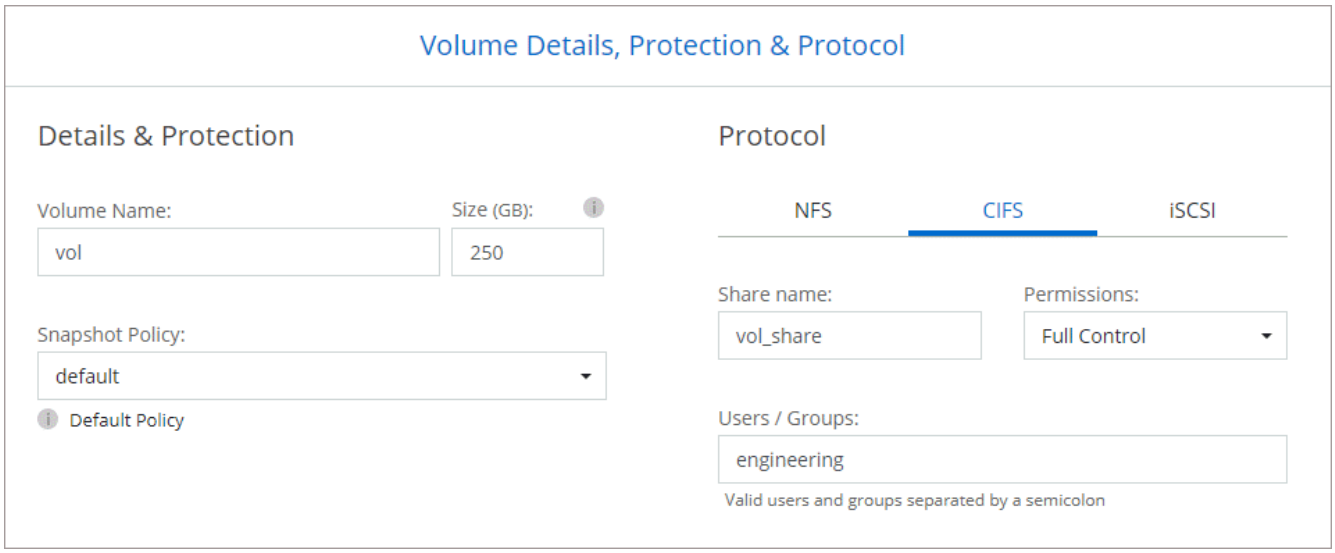
    "Hier erhalten Sie Informationen zu den unterstützten Client-Protokollen und -Versionen".

    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.

Feld	Beschreibung
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)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt 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".

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



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

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. Um Azure AD-Domänendienste als AD-Server für Cloud Volumes ONTAP zu konfigurieren, müssen Sie in diesem Feld **OU=AADDC-Computer** oder **OU=AADDC-Benutzer** eingeben.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure-Dokumentation: Erstellen Sie eine Organisationseinheit (Organisationseinheit, OU) in einer von Azure AD-Domänendiensten gemanagten Domäne"^]
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.
NTP-Server	Wählen Sie **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. 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.

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

    Weitere Informationen finden Sie unter "Allgemeines zu Volume-Nutzungsprofilen" Und "Data Tiering - Übersicht".

18. **Überprüfen & Genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um weitere Informationen zum Support und den Azure-Ressourcen zu erhalten, die BlueXP kaufen wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. 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 Cloud Volumes ONTAP HA-Paars in Azure

Wenn Sie ein Cloud Volumes ONTAP HA-Paar in Azure starten möchten, müssen Sie eine HA-Arbeitsumgebung in BlueXP erstellen.

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. Wenn Sie dazu aufgefordert werden, "Einen Konnektor erstellen".
4. **Details und Anmeldeinformationen**: Optional können Sie die Azure-Anmeldedaten und das Abonnement ändern, einen Clusternamen angeben, bei Bedarf Tags hinzufügen und dann Anmeldedaten angeben.

   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 virtuelle Azure-Maschine zu benennen. Der Name wird auch als Präfix für die vordefinierte Sicherheitsgruppe verwendet, wenn Sie diese Option auswählen.
Tags Für Ressourcengruppen	Tags sind Metadaten für Ihre Azure Ressourcen. Wenn Sie in dieses Feld Tags eingeben, fügt BlueXP diese der Ressourcengruppe hinzu, die dem Cloud Volumes ONTAP-System zugeordnet ist. Sie können bis zu vier Tags aus der Benutzeroberfläche hinzufügen, wenn Sie eine Arbeitsumgebung erstellen. Nach der Erstellung können Sie weitere hinzufügen. Beachten Sie, dass die API Sie beim Erstellen einer Arbeitsumgebung nicht auf vier Tags beschränkt. Informationen zu Tags finden Sie unter "Microsoft Azure-Dokumentation: Verwenden von Tags zur Organisation Ihrer Azure-Ressourcen".
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 „*admin*“ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.

Feld	Beschreibung
Anmeldeinformationen bearbeiten	Sie können verschiedene Azure Zugangsdaten und ein anderes Azure Abonnement für dieses Cloud Volumes ONTAP System wählen. Sie müssen ein Azure Marketplace Abonnement mit dem ausgewählten Azure Abonnement verknüpfen, um ein Pay-as-you-go Cloud Volumes ONTAP System zu implementieren. "Hier erfahren Sie, wie Sie Anmeldedaten hinzufügen".

Im folgenden Video wird gezeigt, wie Sie ein Marketplace-Abonnement zu einem Azure-Abonnement verknüpfen:

Abonnieren Sie BlueXP über den Azure Marketplace

5. **Dienste**: Lassen Sie die Dienste aktiviert oder deaktivieren Sie die einzelnen Dienste, die Sie nicht mit Cloud Volumes ONTAP verwenden möchten.
   - "Weitere Informationen zur BlueXP Klassifizierung"
   - "Erfahren Sie mehr über Backup und Recovery von BlueXP"

   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-Bereitstellungsmodelle*:
   a. Wählen Sie **Single Availability Zone** oder **Multiple Availability Zone** aus.
   b. **Lage und Konnektivität** (Single AZ) und **Region und Konnektivität** (mehrere AZS)
      - Wählen Sie für eine einzelne AZ eine Region, eine Vnet und ein Subnetz aus.
      - Wählen Sie für mehrere AZS eine Region, vnet, Subnetz, Zone für Node 1 und Zone für Node 2 aus.
   c. Aktivieren Sie das Kontrollkästchen * Ich habe die Netzwerkverbindung verifiziert…*.
7. **Konnektivität**: Wählen Sie eine neue oder bestehende Ressourcengruppe und wählen Sie dann aus, ob Sie die vordefinierte Sicherheitsgruppe verwenden oder Ihre eigene verwenden möchten.

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

Feld	Beschreibung
Ressourcengruppe	Erstellen Sie eine neue Ressourcengruppe für Cloud Volumes ONTAP, oder verwenden Sie eine vorhandene Ressourcengruppe. Als Best Practice empfiehlt es sich, eine neue, dedizierte Ressourcengruppe für Cloud Volumes ONTAP zu verwenden. Es ist zwar möglich, Cloud Volumes ONTAP in einer vorhandenen, gemeinsam genutzten Ressourcengruppe bereitzustellen, jedoch wird dies aufgrund des Risikos eines Datenverlusts nicht empfohlen. Weitere Informationen finden Sie in der oben stehenden Warnung. Sie müssen für jedes Cloud Volumes ONTAP HA-Paar, das Sie in Azure implementieren, eine dedizierte Ressourcengruppe verwenden. Es wird nur ein HA-Paar in einer Ressourcengruppe unterstützt. Bei BlueXP treten Verbindungsprobleme auf, wenn Sie versuchen, ein zweites Cloud Volumes ONTAP HA-Paar in einer Azure Ressourcengruppe bereitzustellen. Wenn im Azure Konto, das Sie verwenden, der angezeigt wird "Erforderliche Berechtigungen", BlueXP entfernt Cloud Volumes ONTAP-Ressourcen aus einer Ressourcengruppe, bei Ausfall oder Löschung der Bereitstellung.
Sicherheitsgruppe wurde generiert	Wenn Sie BlueXP die Sicherheitsgruppe für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen: • Wenn Sie **Selected vnet Only** wählen, ist die Quelle für eingehenden Datenverkehr der Subnetz-Bereich des ausgewählten vnet und der Subnetz-Bereich des vnet, in dem sich der Connector befindet. Dies ist die empfohlene Option. • Wenn Sie **Alle VNets** wählen, ist die Quelle für eingehenden Datenverkehr der IP-Bereich 0.0.0.0/0.
Verwenden Sie vorhandene	Wenn Sie eine vorhandene Sicherheitsgruppe auswählen, muss diese die Cloud Volumes ONTAP-Anforderungen erfüllen. "Zeigen Sie die Standardsicherheitsgruppe an".

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 aus, um ein Cloud Volumes ONTAP-System schnell bereitzustellen, oder klicken Sie auf **Konfiguration ändern**.

   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 virtuellen 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. **Vom Azure Marketplace abonnieren**: Folgen Sie den Schritten, wenn BlueXP programmatische Bereitstellungen von Cloud Volumes ONTAP nicht aktivieren kann.
12. **Zugrunde liegende Storage-Ressourcen**: Wählen Sie die Einstellungen für das anfängliche Aggregat: Einen Festplattentyp, eine Größe für jede Festplatte und ob Daten-Tiering zu Blob-Storage aktiviert werden soll.

    Beachten Sie Folgendes:

    - 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 zur Auswahl einer Festplattengröße finden Sie unter "Größe Ihres Systems in Azure".

    - 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.

      "Weitere Informationen zum Daten-Tiering".

13. **Schreibgeschwindigkeit und WURM**:

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

       "Erfahren Sie mehr über Schreibgeschwindigkeit".

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

       Diese Option ist nur für bestimmte VM-Typen verfügbar. Informationen darüber, welche VM-Typen unterstützt werden, finden Sie unter "Unterstützte Konfigurationen per Lizenz für HA-Paare".

       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.
14. **Sichere Kommunikation zu Storage & WORM**: Wählen Sie, ob eine HTTPS-Verbindung zu Azure-Speicherkonten aktiviert und, falls gewünscht, den WORM-Speicher (Write Once, Read Many) aktiviert werden soll.

    Die HTTPS-Verbindung besteht aus einem Cloud Volumes ONTAP 9.7 HA-Paar zu Blob-Storage-Konten auf der Azure-Seite. Beachten Sie, dass die Aktivierung dieser Option sich auf die Schreib-Performance auswirken kann. Sie können die Einstellung nicht ändern, nachdem Sie die Arbeitsumgebung erstellt haben.

"Erfahren Sie mehr über WORM Storage".

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

"Erfahren Sie mehr über WORM Storage".

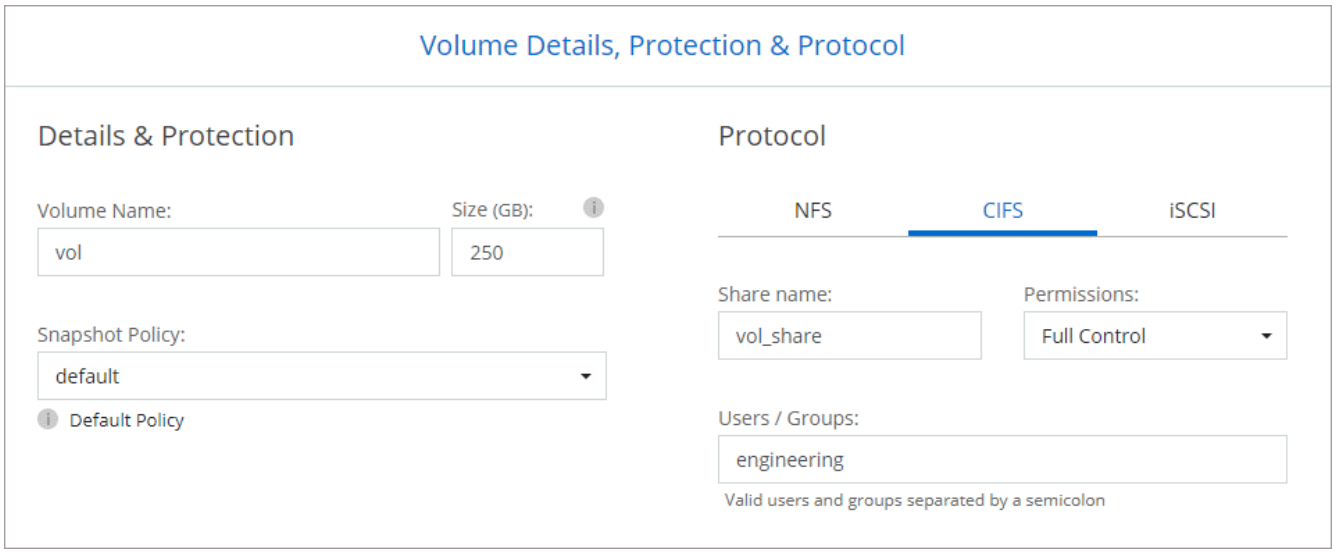
15. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

    "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)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt 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".

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



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

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. Um Azure AD-Domänendienste als AD-Server für Cloud Volumes ONTAP zu konfigurieren, müssen Sie in diesem Feld **OU=AADDC-Computer** oder **OU=AADDC-Benutzer** eingeben.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure-Dokumentation: Erstellen Sie eine Organisationseinheit (Organisationseinheit, OU) in einer von Azure AD-Domänendiensten gemanagten Domäne"^]
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.
NTP-Server	Wählen Sie **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. 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.

17. **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".

18. **Überprüfen & Genehmigen**: Überprüfen und bestätigen Sie Ihre Auswahl.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um weitere Informationen zum Support und den Azure-Ressourcen zu erhalten, die BlueXP kaufen wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. 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.

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	
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	

GCP-Informationen	Ihr Wert
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.

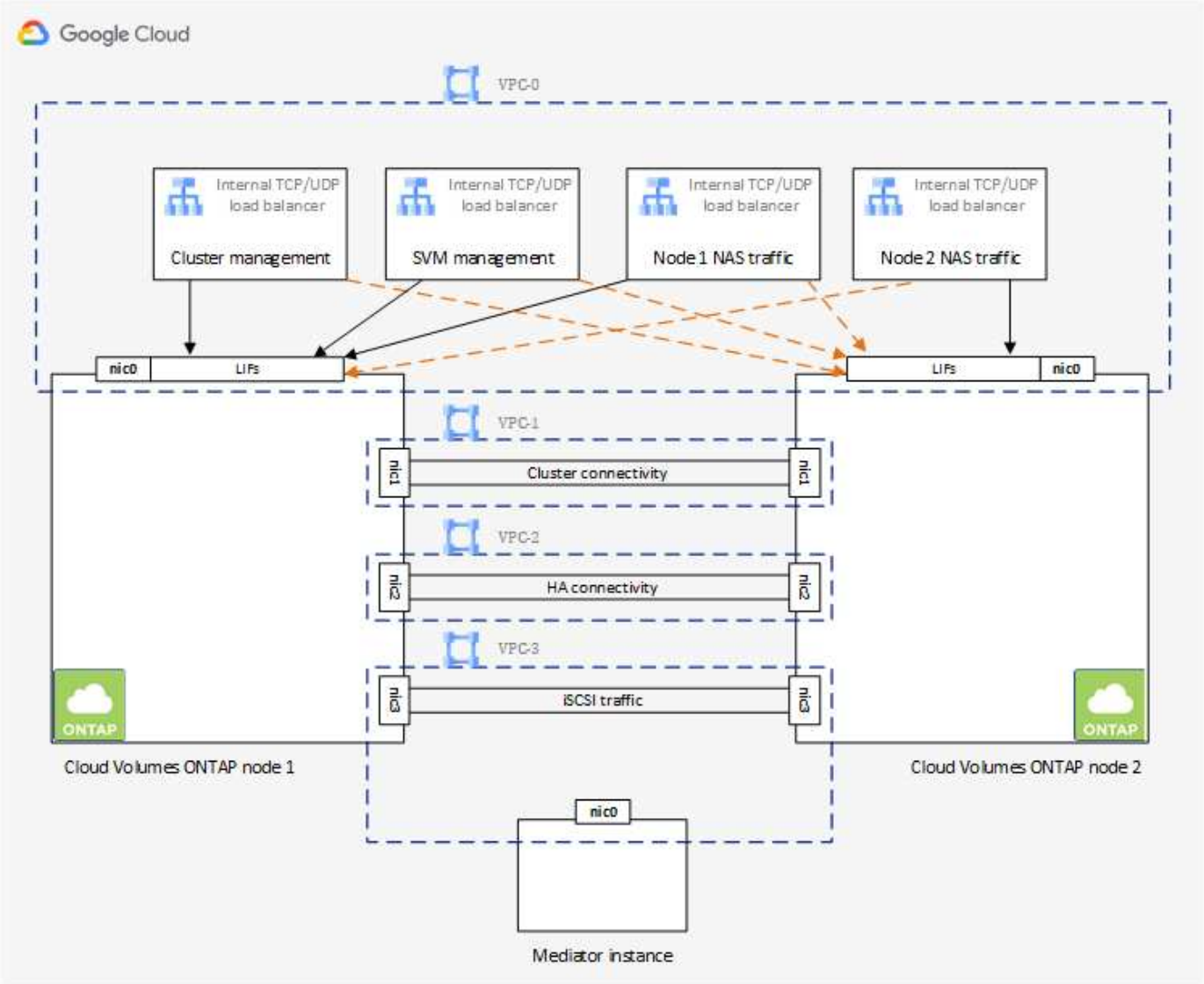
  Dieses Implementierungsmodell senkt Ihre Kosten, da zwischen den Zonen keine Kosten für den Datenausgang anfallen.

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.

- **Single Node** BlueXP weist 4 IP-Adressen einem System mit einem einzigen Knoten 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" Muss im Google Cloud-Subnetz, in dem Sie Cloud Volumes ONTAP bereitstellen, deaktiviert sein. 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 zu Testzwecken auf die Ports verweisen oder Ihre eigenen Firewall-Regeln verwenden.

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	10.000	Backup mit NDMP
TCP	11104	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
TCP	11105	SnapMirror Datenübertragung über Cluster-interne LIFs
TCP	63001-63050	Ports zur Lastausgleichssonde 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/offboxconfig	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	18600-18699	Node Management-LIF	Zielserver	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	11104	Intercluster-LIF	ONTAP Intercluster-LIFs	Management von interclusterübergreifenden Kommunikationssitzungen für SnapMirror
	TCP	11105	Intercluster-LIF	ONTAP Intercluster-LIFs	SnapMirror Datenübertragung
Syslog	UDP	514	Node Management-LIF	Syslog-Server	Syslog-Weiterleitungsmeldungen

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 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 **ODER** 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

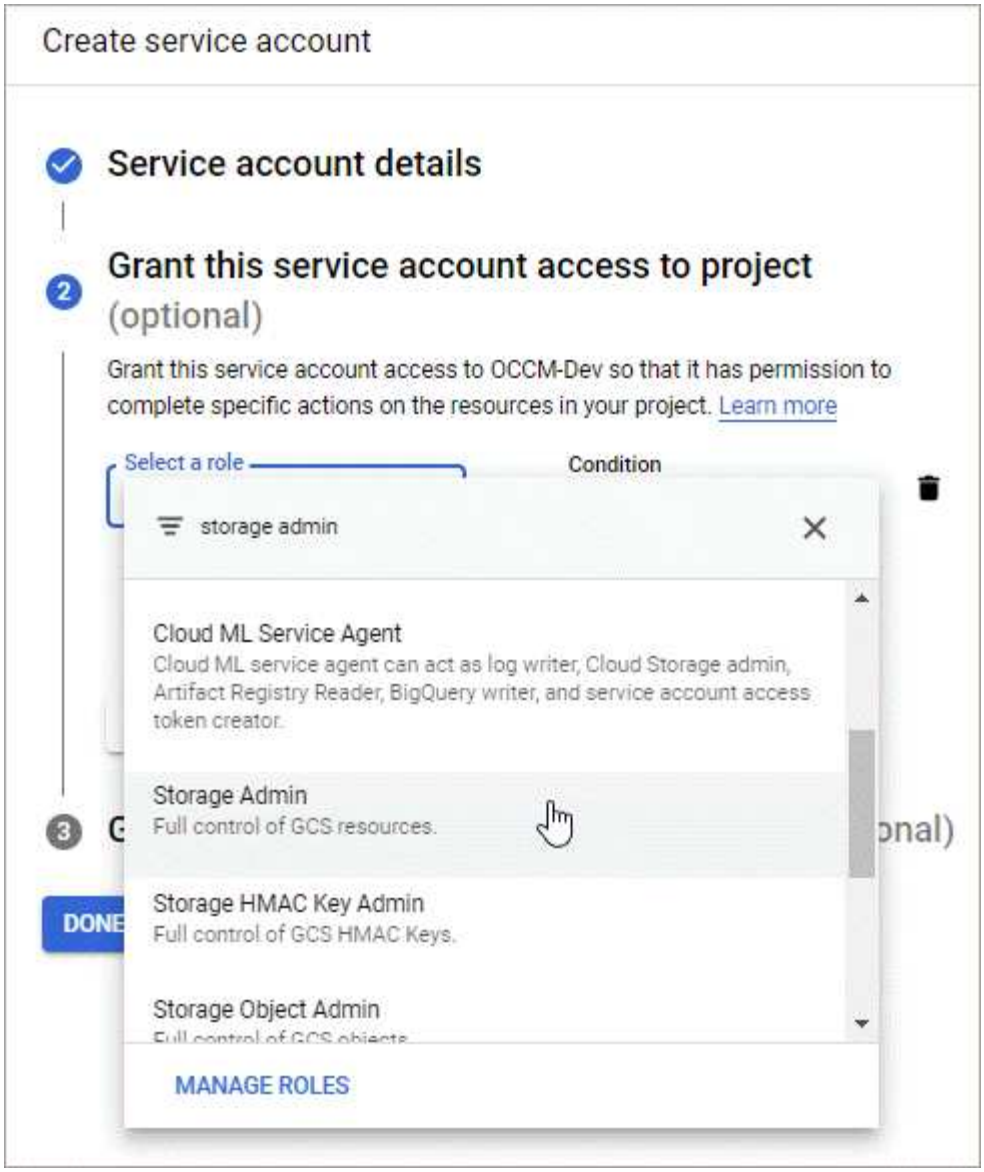
Für Cloud Volumes ONTAP ist ein Google Cloud-Servicekonto aus zwei Gründen erforderlich. Die erste lautet, wenn Sie aktivieren "Daten-Tiering" Tiering selten genutzter Daten auf kostengünstigen Objekt-Storage in Google Cloud. Die zweite lautet, wenn Sie den aktivieren "BlueXP Backup und Recovery" Um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

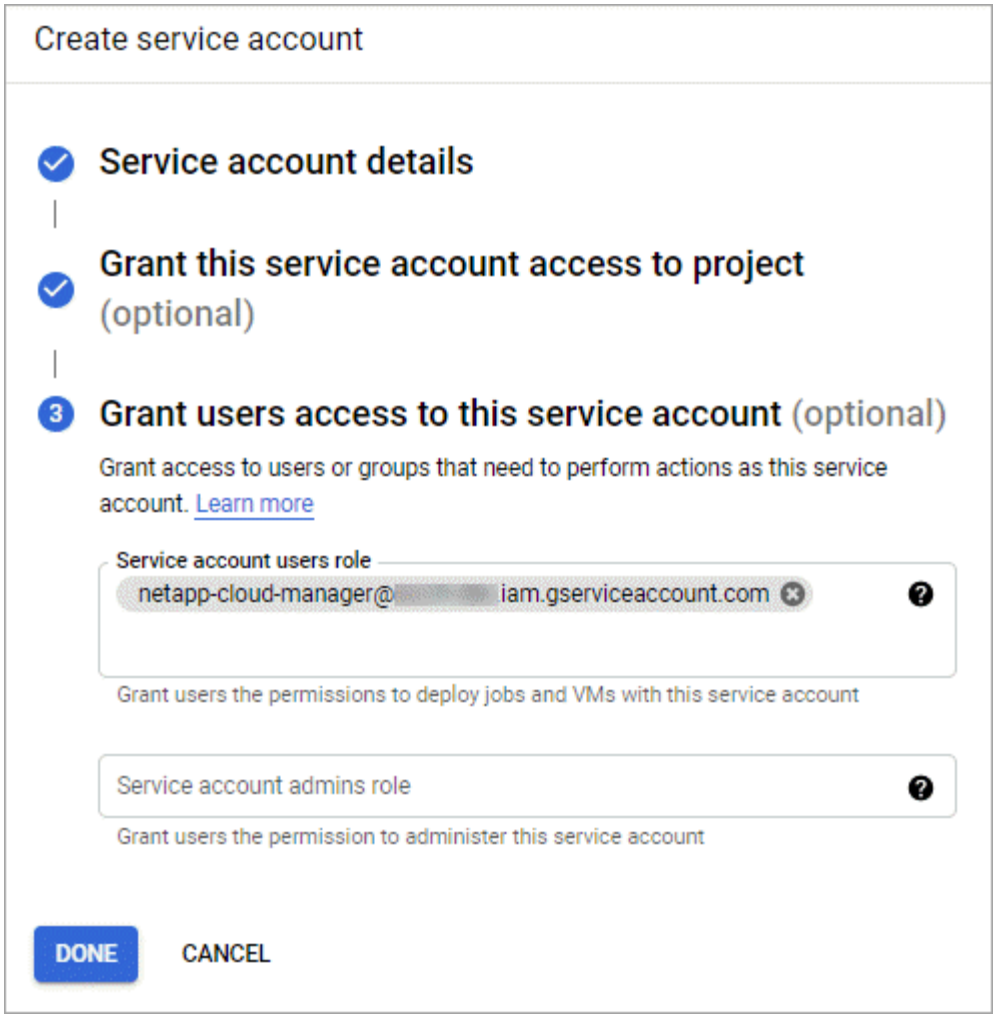
Schritte

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**.



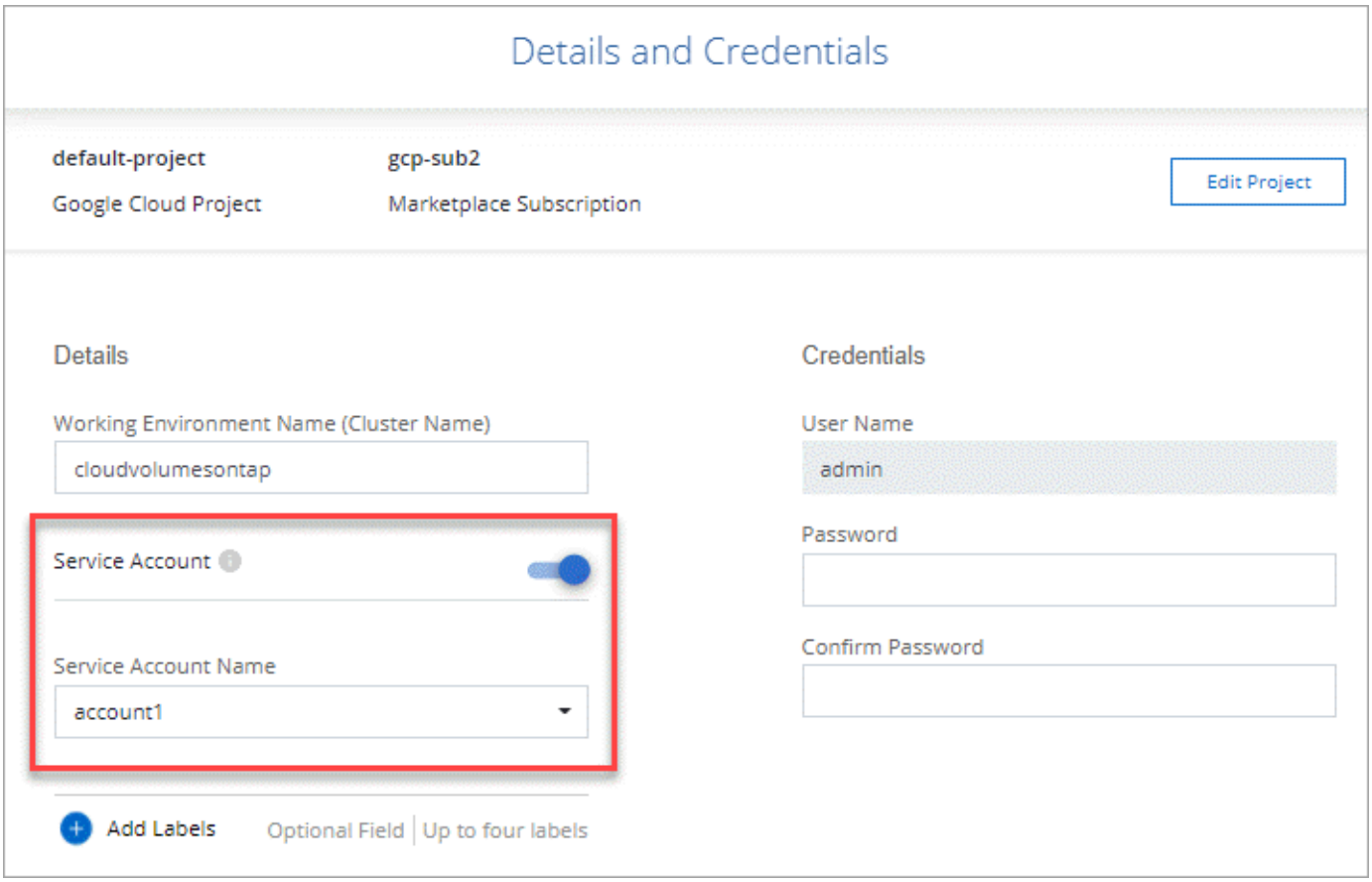
c. **Benutzern Zugriff auf dieses Servicekonto gewähren**: Fügen Sie das Connector Service-Konto als *Service Account User* zu diesem neuen Service-Konto hinzu.

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



Was kommt als Nächstes?

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



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.

Freimium

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

Schritte

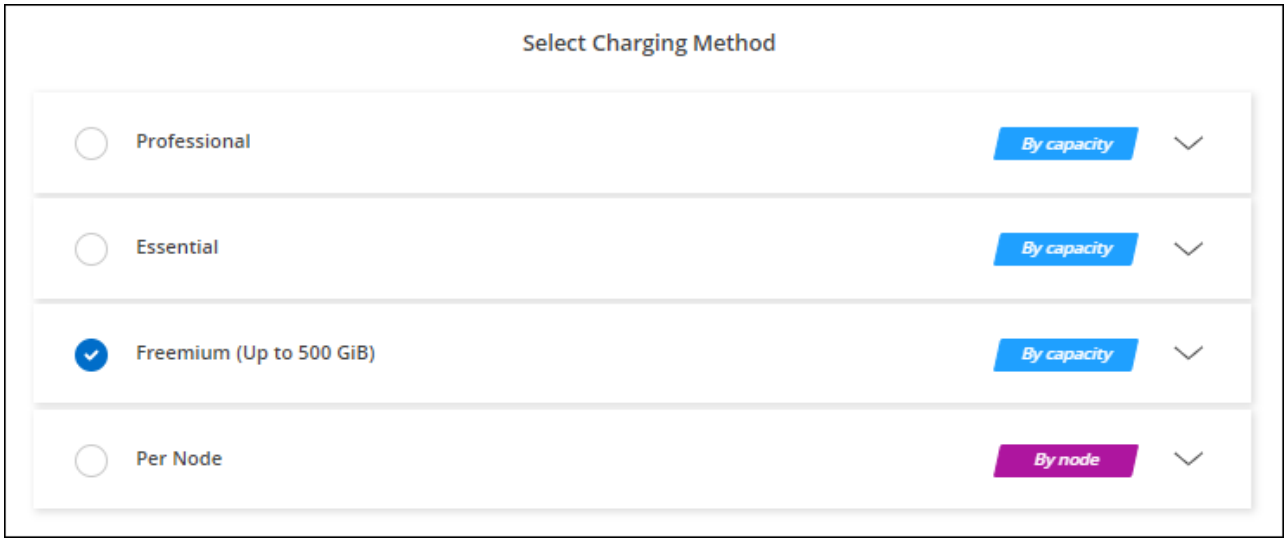
1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. Klicken Sie auf der Seite Arbeitsfläche auf **Arbeitsumgebung hinzufügen** und folgen Sie den Schritten in

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.



"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"

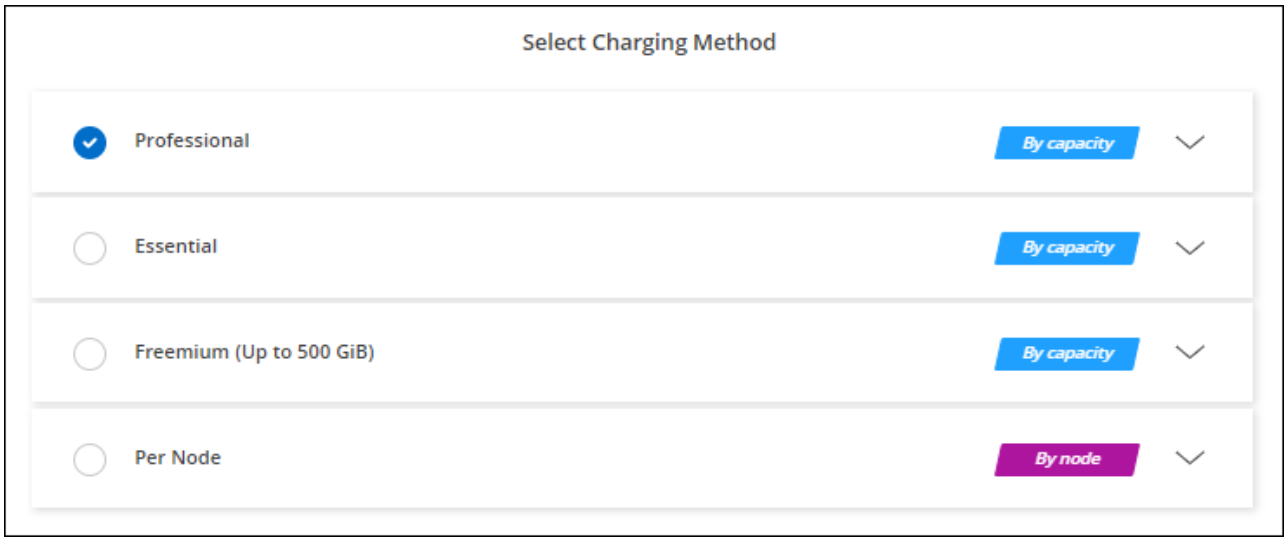
   BlueXP fragt den NetApp Lizenzierungsservice automatisch ab, um Details zu den Lizenzen zu erhalten, die mit Ihrem NetApp Support Site Konto verknüpft sind. Sollte es keine Fehler geben, fügt BlueXP die Lizenzen automatisch zum Digital Wallet hinzu.

   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.



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

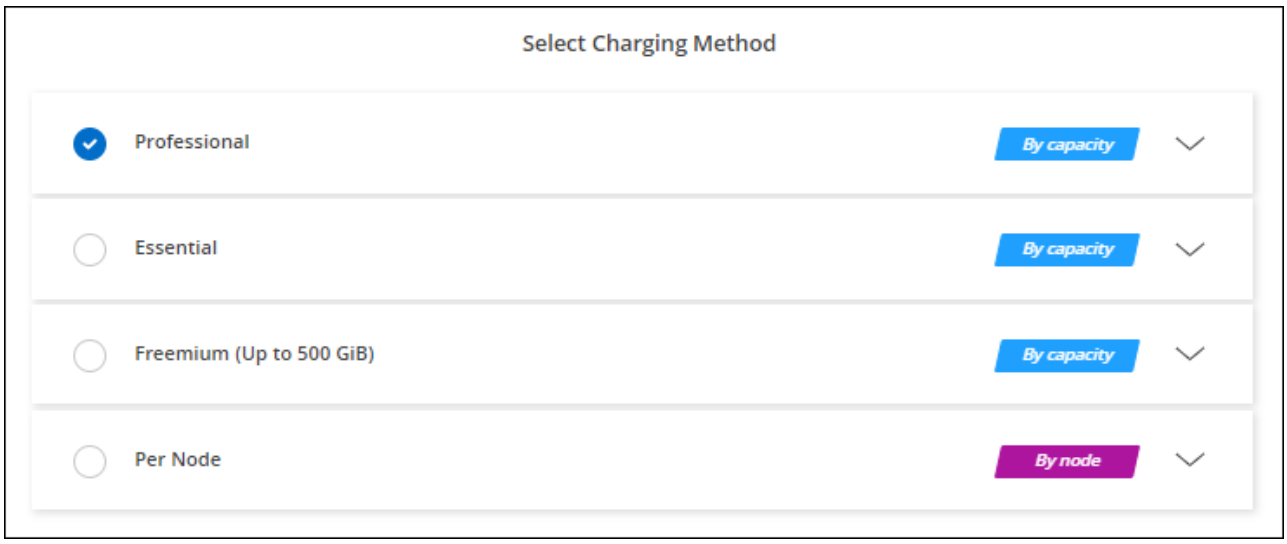
PAYGO-Abonnement

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.



"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

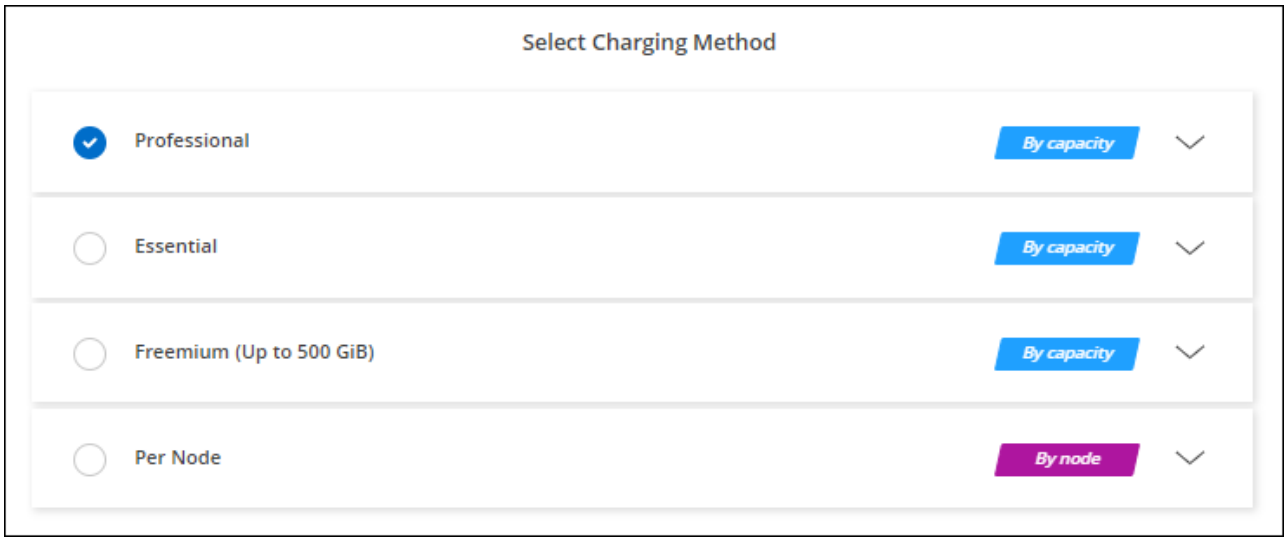
1. Wenden Sie sich an Ihren NetApp Ansprechpartner, um einen Jahresvertrag zu erwerben.

   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.



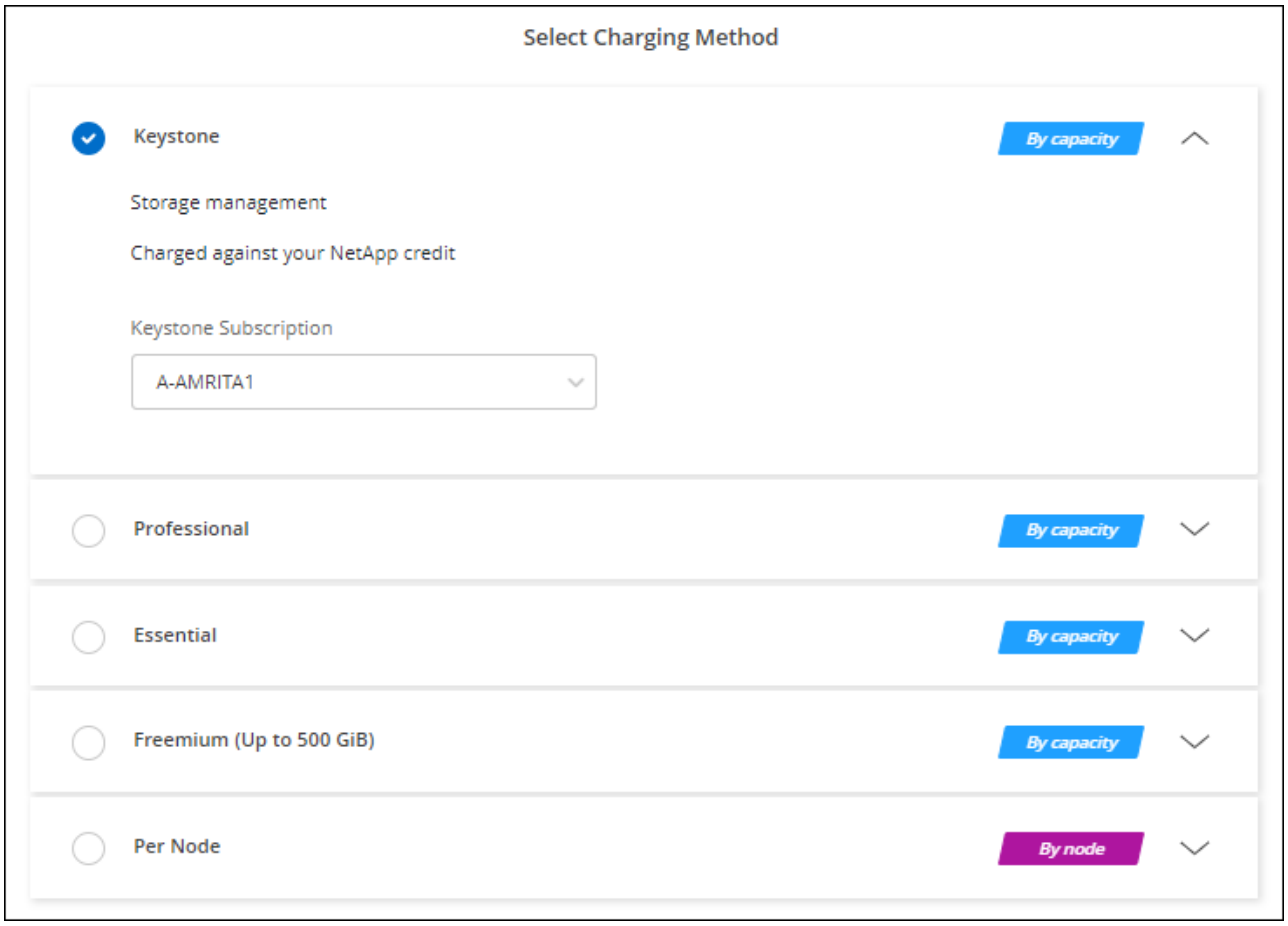
"Sehen Sie sich Schritt-für-Schritt-Anleitungen an, um Cloud Volumes ONTAP in Google Cloud zu starten".

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[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.



"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	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. Sie können bis zu vier Etiketten von der Benutzeroberfläche hinzufügen, wenn Sie eine Arbeitsumgebung erstellen, und dann können Sie weitere hinzufügen, nachdem sie erstellt wurde. Beachten Sie, dass Sie durch die API beim Erstellen einer Arbeitsumgebung nicht auf vier Labels beschränkt werden. Informationen zu Etiketten finden Sie unter "Google Cloud-Dokumentation: Ressourcen Zur Kennzeichnung".

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 „*admin*“ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Projekt Bearbeiten	Wählen Sie das Projekt aus, in dem Cloud Volumes ONTAP gespeichert werden soll. Das Standardprojekt ist das Projekt, in dem sich BlueXP befindet. 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. Dies ist das Servicekonto, das Sie für BlueXP eingerichtet haben. "Wie auf dieser Seite beschrieben". Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen einem Abonnement zuzuordnen. 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.

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.

Abonnieren Sie BlueXP über den Google Cloud Marketplace

6. **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.

7. **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	Wenn Sie BlueXP die Firewall-Richtlinie für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen: • 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	Wenn Sie eine vorhandene Firewallrichtlinie verwenden, stellen Sie sicher, dass diese die erforderlichen Regeln enthält. Link: Learn über Firewall-Regeln für Cloud Volumes ONTAP.

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".

> 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".

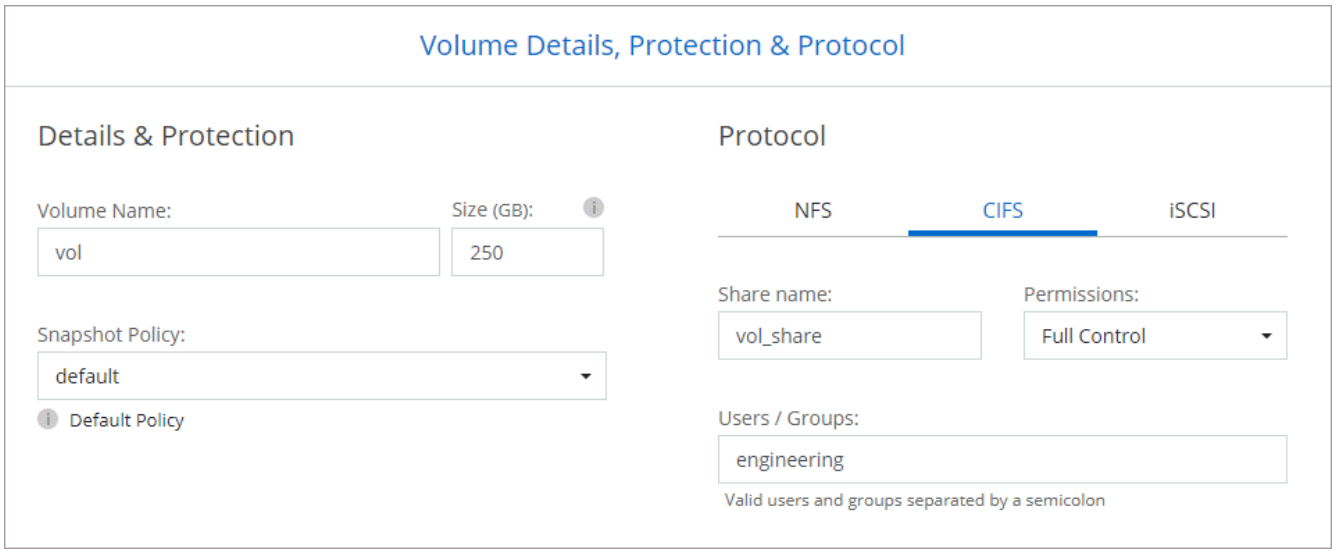
14. **Create Volume**: Geben Sie Details für den neuen Datenträger ein oder klicken Sie auf **Skip**.

"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)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt 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".

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



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

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind. Wenn Sie Google Managed Active Directory konfigurieren, kann standardmäßig mit der IP-Adresse 169.254.169.254 auf AD zugegriffen werden.
Active Directory-Domäne, der Sie beitreten möchten	Der FQDN der Active Directory (AD)-Domain, der der CIFS-Server beitreten soll.
Anmeldeinformationen, die zur Aufnahme in die Domäne autorisiert sind	Der Name und das Kennwort eines Windows-Kontos mit ausreichenden Berechtigungen zum Hinzufügen von Computern zur angegebenen Organisationseinheit (OU) innerhalb der AD-Domäne.
CIFS-Server-BIOS-Name	Ein CIFS-Servername, der in der AD-Domain eindeutig ist.
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. 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.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD"^]
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	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. 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.

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.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um weitere Informationen zum Support und den Google Cloud-Ressourcen zu erhalten, die BlueXP kaufen wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. 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

1. Wählen Sie im linken Navigationsmenü die Option **Speicherung > Leinwand**.
2. 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	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. Sie können bis zu vier Etiketten von der Benutzeroberfläche hinzufügen, wenn Sie eine Arbeitsumgebung erstellen, und dann können Sie weitere hinzufügen, nachdem sie erstellt wurde. Beachten Sie, dass Sie durch die API beim Erstellen einer Arbeitsumgebung nicht auf vier Labels beschränkt werden. Informationen zu Etiketten finden Sie unter "Google Cloud-Dokumentation: Ressourcen Zur Kennzeichnung".
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 „*admin*“ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.
Projekt Bearbeiten	Wählen Sie das Projekt aus, in dem Cloud Volumes ONTAP gespeichert werden soll. Das Standardprojekt ist das Projekt, in dem sich BlueXP befindet. 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. Dies ist das Servicekonto, das Sie für BlueXP eingerichtet haben. "Wie auf dieser Seite beschrieben". Klicken Sie auf **Abonnement hinzufügen**, um die ausgewählten Anmeldeinformationen einem Abonnement zuzuordnen. 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.

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.

Abonnieren Sie BlueXP über den Google Cloud Marketplace

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	Wenn Sie BlueXP die Firewall-Richtlinie für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen: • 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	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".

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**.

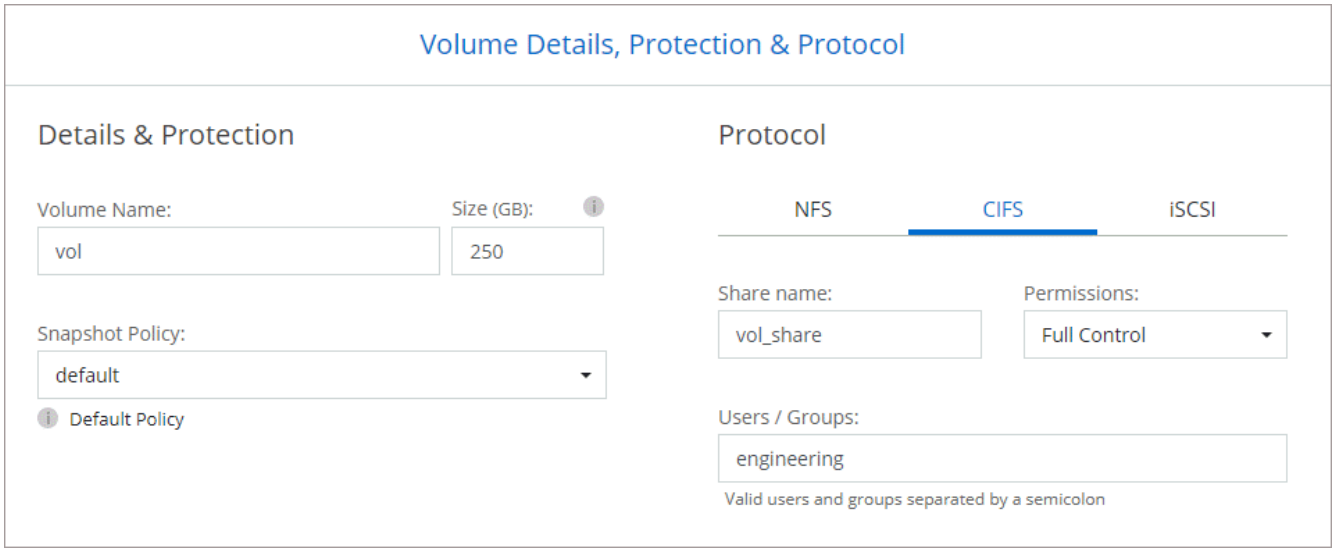
    "Hier erhalten Sie Informationen zu den unterstützten Client-Protokollen und -Versionen".

    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.

Feld	Beschreibung
Initiatorgruppe und IQN (nur für iSCSI)	ISCSI-Storage-Ziele werden LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Initiatorgruppen sind Tabellen mit iSCSI-Host-Node-Namen und steuern, welche Initiatoren Zugriff auf welche LUNs haben. ISCSI-Ziele werden über standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) Karten mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert. Wenn Sie ein iSCSI-Volume erstellen, erstellt 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".

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



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

Feld	Beschreibung
Primäre und sekundäre DNS-IP-Adresse	Die IP-Adressen der DNS-Server, die die Namensauflösung für den CIFS-Server bereitstellen. Die aufgeführten DNS-Server müssen die Servicestandortdatensätze (SRV) enthalten, die zum Auffinden der Active Directory LDAP-Server und Domänencontroller für die Domain, der der CIFS-Server beitreten wird, erforderlich sind. Wenn Sie Google Managed Active Directory konfigurieren, kann standardmäßig mit der IP-Adresse 169.254.169.254 auf AD zugegriffen werden.
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.

Feld	Beschreibung
Organisationseinheit	Die Organisationseinheit innerhalb der AD-Domain, die dem CIFS-Server zugeordnet werden soll. Der Standardwert lautet CN=Computers. 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.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD"^]
DNS-Domäne	Die DNS-Domain für die Cloud Volumes ONTAP Storage Virtual Machine (SVM). In den meisten Fällen entspricht die Domäne der AD-Domäne.
NTP-Server	Wählen Sie **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. 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.

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.
    a. Überprüfen Sie die Details zur Konfiguration.
    b. Klicken Sie auf **Weitere Informationen**, um weitere Informationen zum Support und den Google Cloud-Ressourcen zu erhalten, die BlueXP kaufen wird.
    c. Aktivieren Sie die Kontrollkästchen **Ich verstehe…**.
    d. 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 gzipped 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/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

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

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

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

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


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

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

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

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

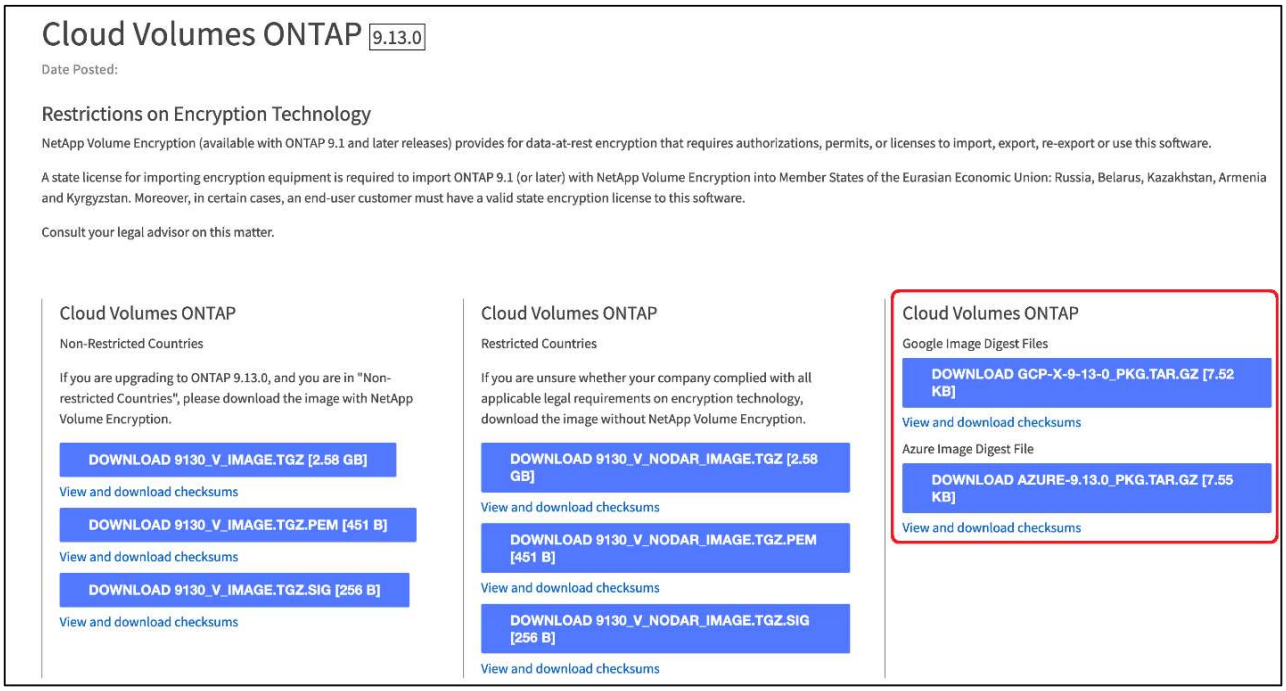
Verifizieren von durch Google Cloud signierten Bildern

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.

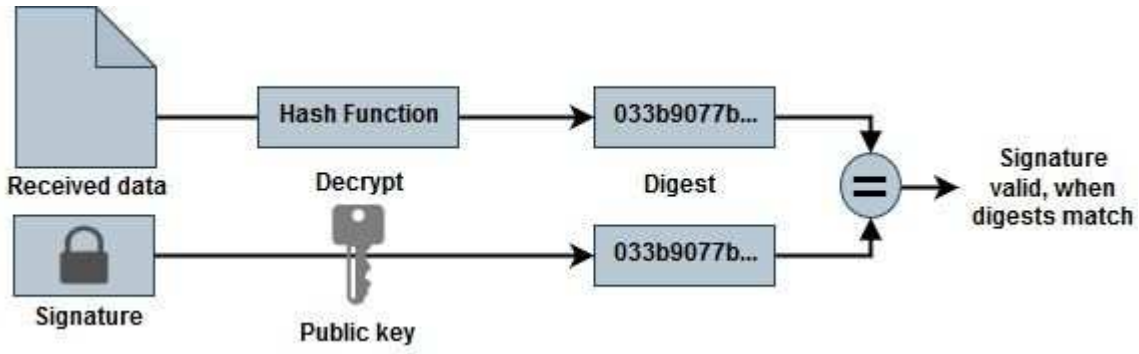
Workflow-Zusammenfassung für die signierte Bildüberprüfung

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)



- 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-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

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

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

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

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

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

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

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

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

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

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

2. Legen Sie die heruntergeladene Datei Disk.RAW, die Signatur und 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
```