



Erste Schritte in Amazon Web Services

Cloud Volumes ONTAP

NetApp
June 11, 2024

Inhalt

- Erste Schritte in Amazon Web Services 1
 - Schnellstart für Cloud Volumes ONTAP in AWS 1
 - Planen Sie Ihre Cloud Volumes ONTAP-Konfiguration in AWS 2
 - Richten Sie Ihr Netzwerk ein 6
 - Einrichten des AWS KMS 28
 - Einrichten von IAM-Rollen für Cloud Volumes ONTAP 32
 - Lizenzierung für Cloud Volumes ONTAP in AWS einrichten 41
 - Starten von Cloud Volumes ONTAP in AWS 49
 - Implementieren Sie Cloud Volumes ONTAP in AWS Secret Cloud und Top Secret Cloud-Regionen 63

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 Sie einen Connector in AWS von BlueXP"](#)
- ["Erstellen Sie einen Connector aus dem AWS Marketplace"](#)
- ["Installieren und Einrichten eines Connectors auf dem Gelände"](#)
- ["AWS-Berechtigungen für den Connector"](#)

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 lokale Zone aus

Cloud Volumes ONTAP wird in einigen AWS lokalen Zonen unterstützt, einschließlich Singapur. Die Auswahl einer lokalen Zone ist optional.

["Sehen Sie sich die vollständige Liste der lokalen Zonen an"](#).

Lokale Zonen müssen aktiviert sein, bevor Sie Ressourcen in diesen Zonen erstellen und verwalten können.

["Erfahren Sie, wie Sie eine lokale Zone aktivieren"](#).



Phoenix ist keine unterstützte lokale Zone.

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	
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.

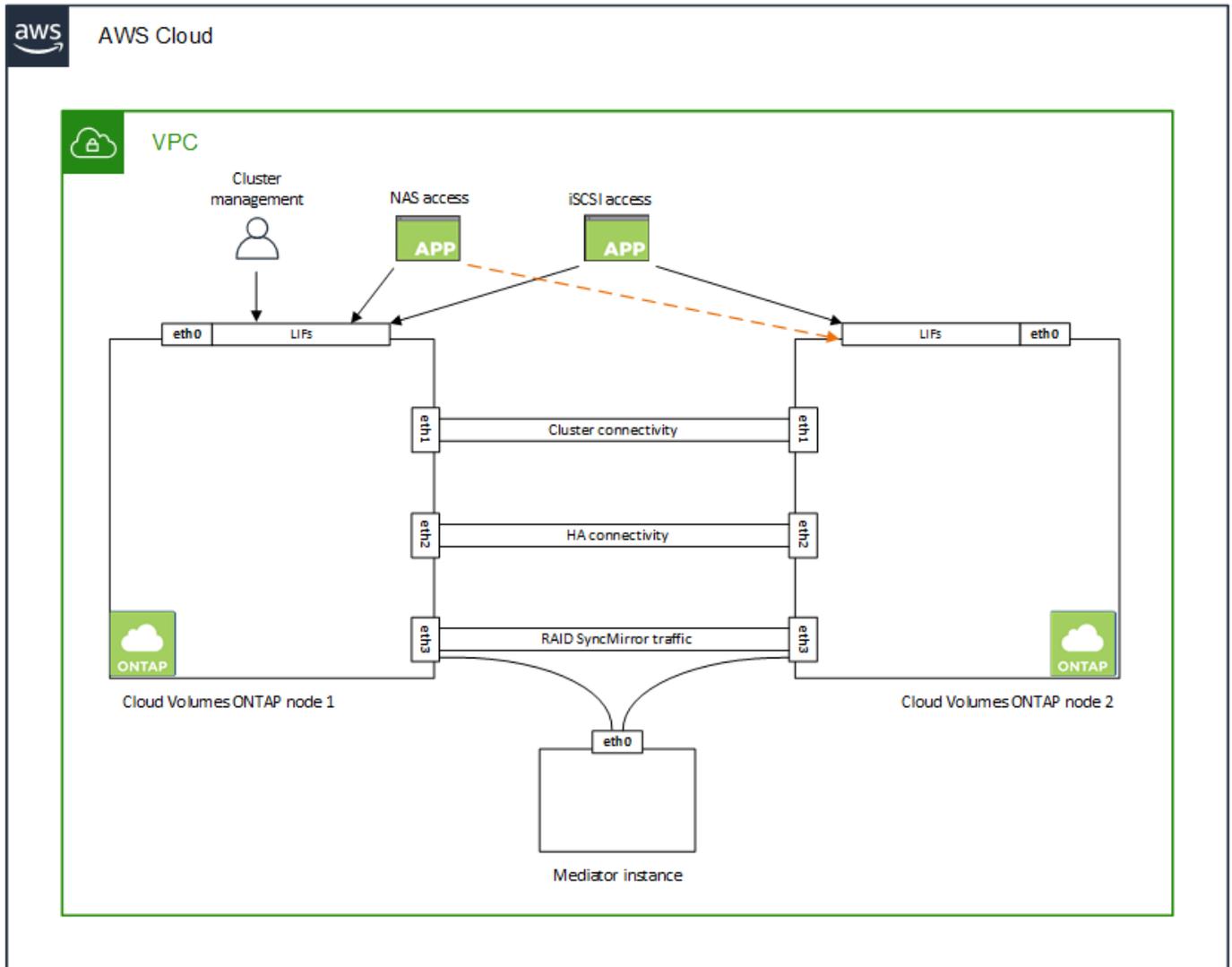
Die folgende Tabelle enthält Details zu den LIFs, die mit jeder privaten IP-Adresse verknüpft sind.

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.

LIF	Zweck
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.
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.

LIF	Schnittstelle	Knoten	Zweck
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.



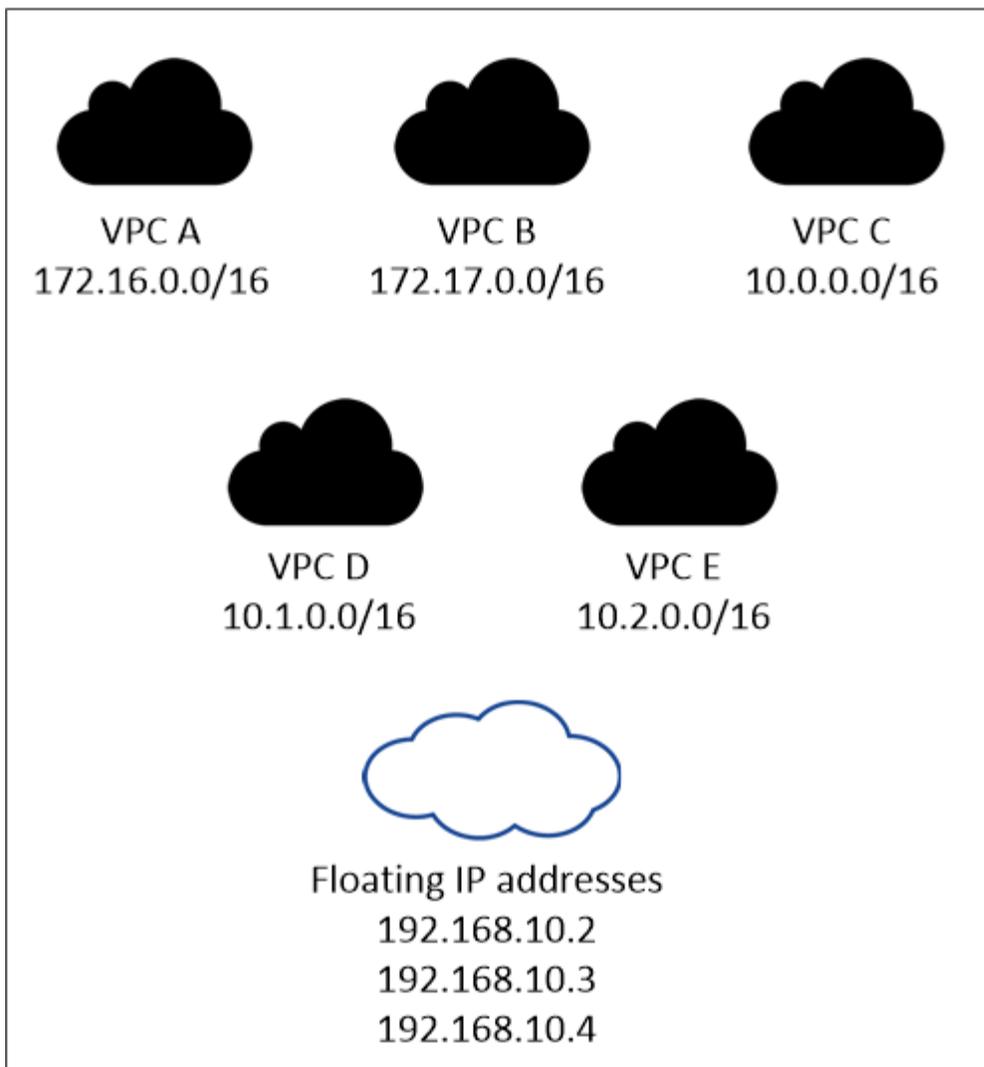
Wenn Sie SnapDrive für Windows oder SnapCenter mit dem HA-Paar verwenden, ist eine unverankerte IP-Adresse für die SVM-Management-LIF erforderlich.

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.

AWS region



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 Routentabellen auszuwählen, die Routen zu den unverankerten IP-Adressen enthalten sollen. Dies ermöglicht den Client-Zugriff auf das HA-Paar.

Wenn Sie nur eine Routentabelle für die Subnetze in Ihrem VPC (der Hauptroutentabelle) haben, fügt BlueXP automatisch die fließenden IP-Adressen zu dieser Routentabelle 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"](#).

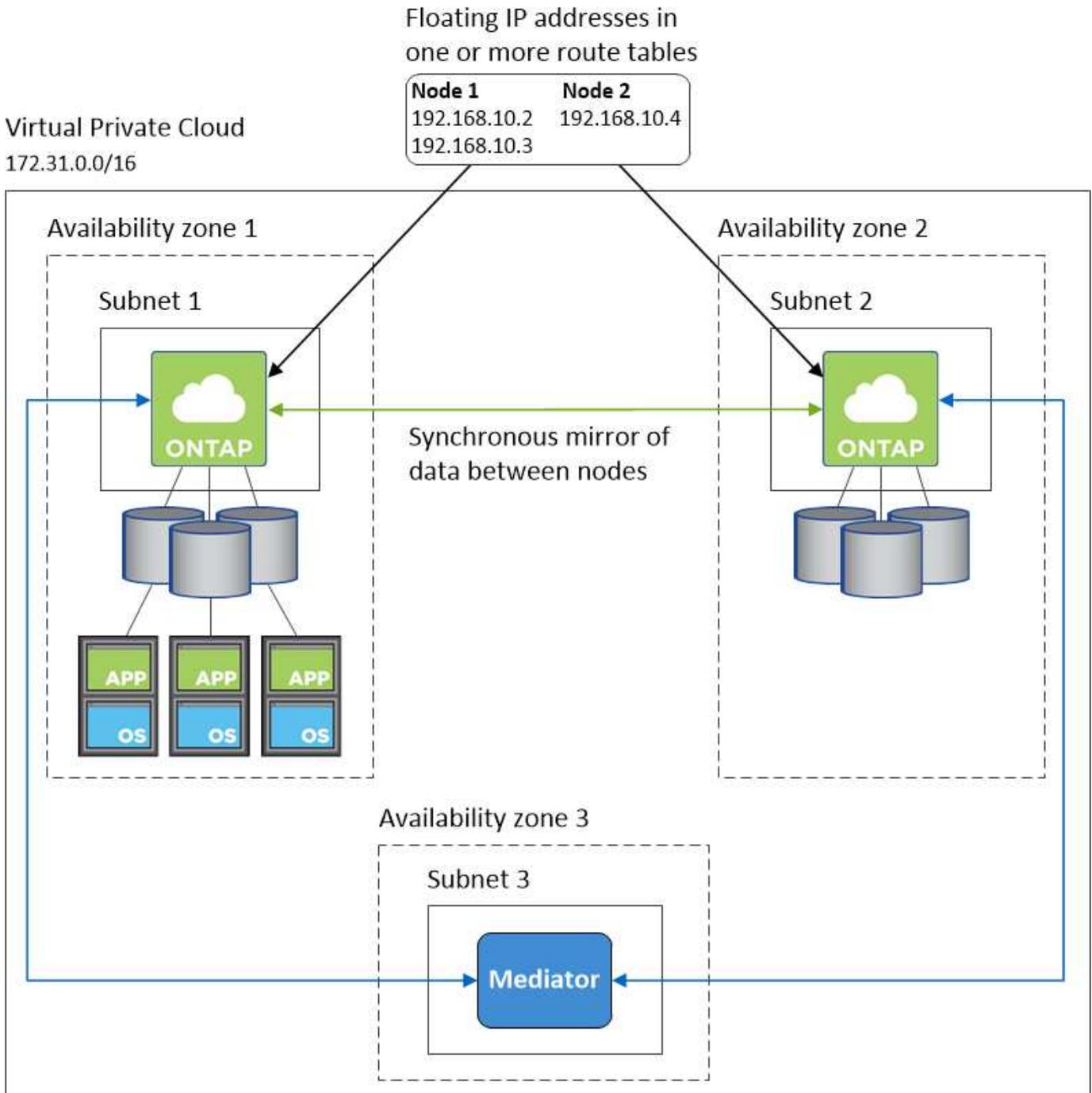
Anbindung an NetApp Management Tools

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-](#)

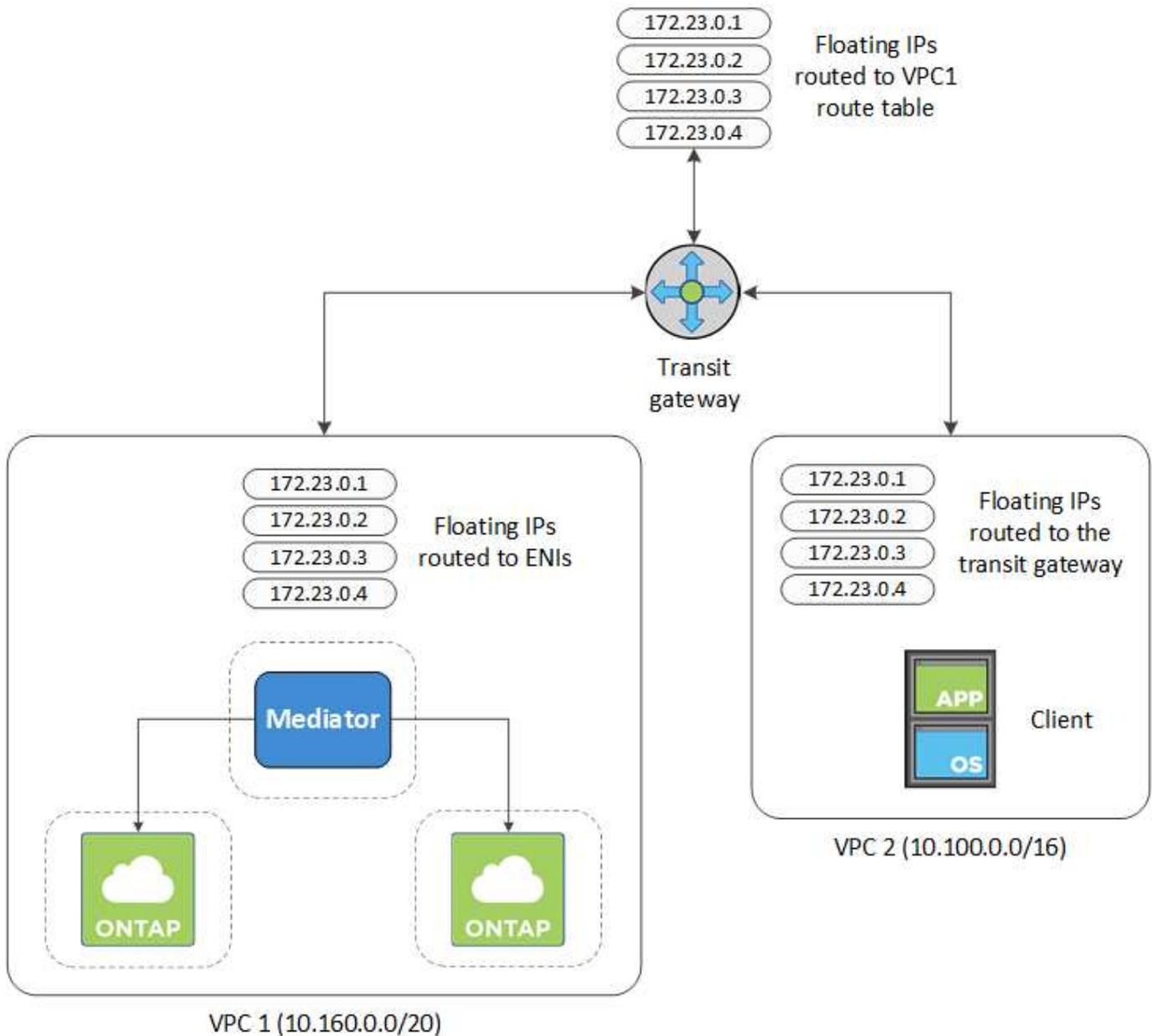
Adressen" Von außerhalb der VPC, wo das HA-Paar residiert.

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:

NFS & CIFS access from within the VPC using Floating IP

Auto failover

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

Access

SVM Management : 172.23.0.4

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.

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aeddd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

CIDR	Attachment	Resource type	Route type	Route state
10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8 vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
10.160.0.0/20	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC1	propagated	active
172.23.0.1/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
172.23.0.2/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
172.23.0.3/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
172.23.0.4/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active

Floating IP Addresses

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

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

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-07250bd01781e67df	active	No
10.160.0.0/20	tgw-015b7c249661ac279	active	No
172.23.0.1/32	tgw-015b7c249661ac279	active	No
172.23.0.2/32	tgw-015b7c249661ac279	active	No
172.23.0.3/32	tgw-015b7c249661ac279	active	No
172.23.0.4/32	tgw-015b7c249661ac279	active	No

VPC1
Floating IP Addresses

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.

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

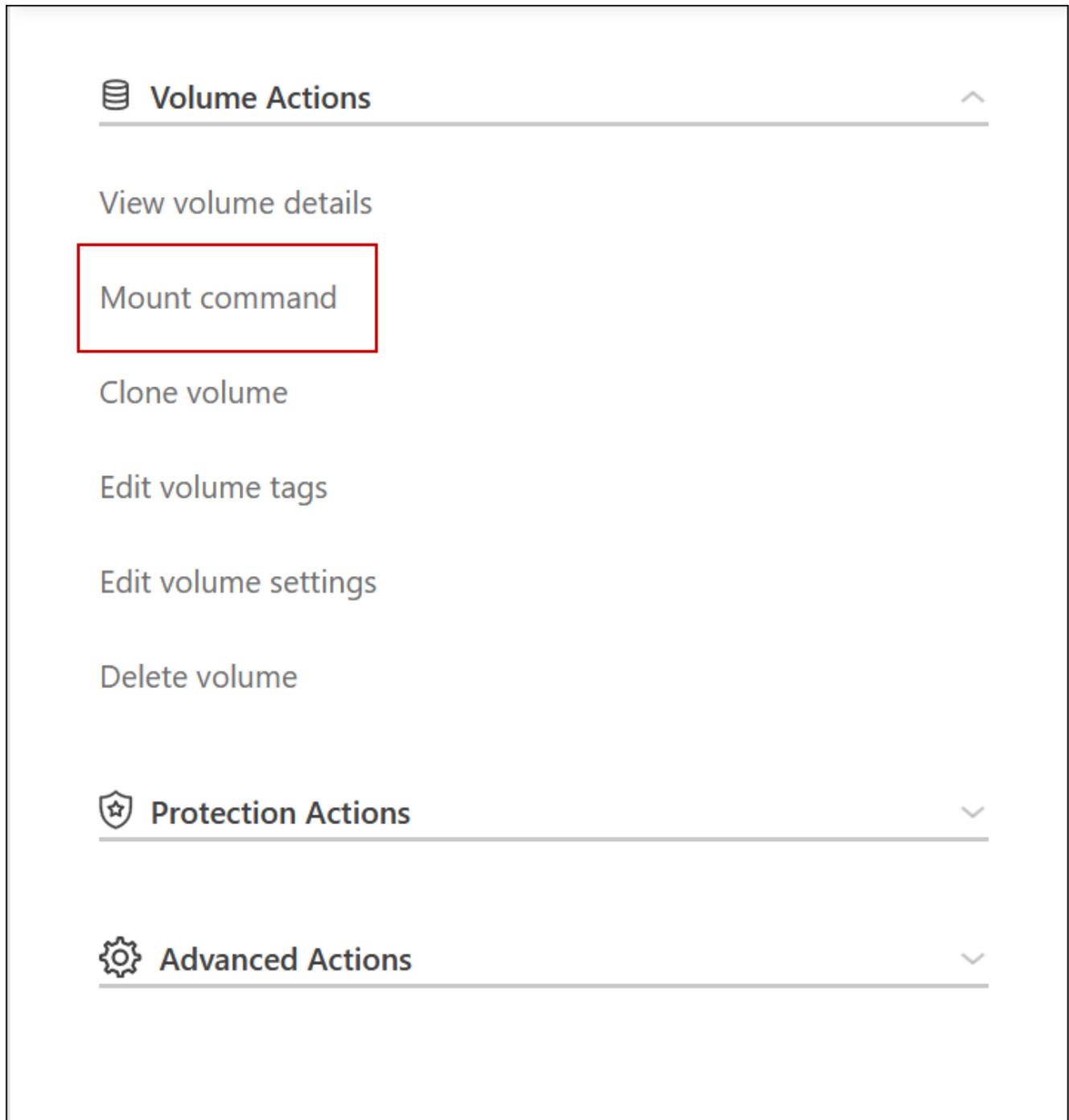
Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-ff7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-076681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

VPC2
Floating act IP Addresses

6. Aktualisieren Sie die Einstellungen der Sicherheitsgruppen auf Alle Daten für die VPC.
- Klicken Sie unter Virtual Private Cloud auf **Subnetze**.
 - Klicken Sie auf die Registerkarte **Route table** und wählen Sie die gewünschte Umgebung für eine der fließenden IP-Adressen für ein HA-Paar aus.
 - Klicken Sie auf **Sicherheitsgruppen**.
 - Wählen Sie **Inbound Rules Bearbeiten**.
 - Klicken Sie auf **Regel hinzufügen**.
 - Wählen Sie unter Typ **All Traffic** aus, und wählen Sie dann die VPC-IP-Adresse aus.
 - 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-Volumen 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

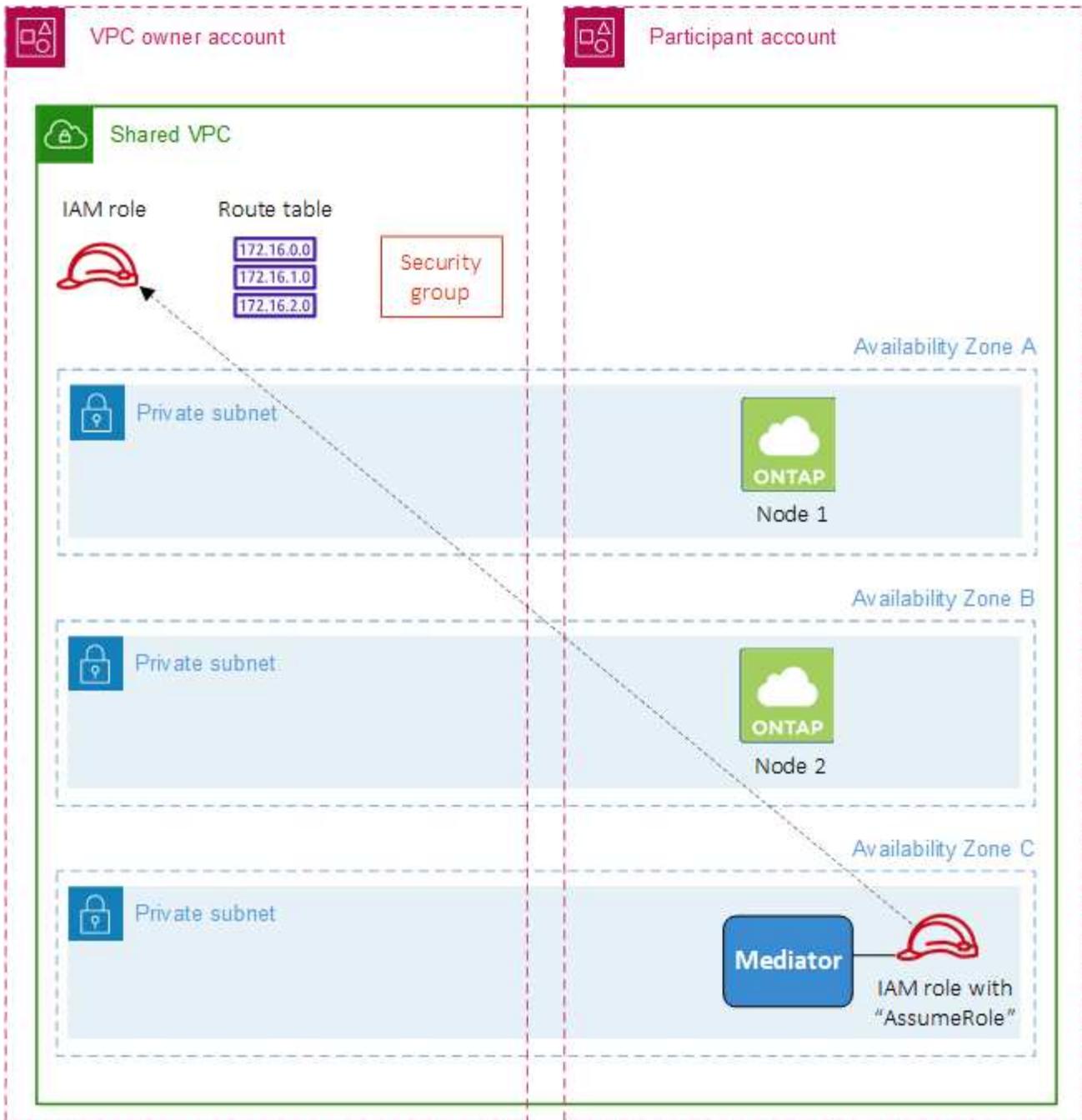
Ab Version 9.11.1 werden Cloud Volumes ONTAP HA-Paare in AWS mit VPC-Sharing unterstützt. Die VPC-Freigabe ermöglicht Ihrem Unternehmen, Subnetze mit anderen AWS Konten gemeinsam zu nutzen. Um diese Konfiguration zu verwenden, müssen Sie Ihre AWS-Umgebung einrichten und dann das HA-Paar mithilfe der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

- "AssumeRoleArn" 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/offbo xconfig	Senden Sie Konfigurationssicherungen an den Connector. "Informationen zu Backup-Dateien für die Konfiguration" .
DHCP	UDP	68	Node Management-LIF	DHCP	DHCP-Client für die erstmalige Einrichtung
DHCPS	UDP	67	Node Management-LIF	DHCP	DHCP-Server
DNS	UDP	53	Node Management LIF und Daten LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	1860-1869	Node Management-LIF	Zielservers	NDMP-Kopie
SMTP	TCP	25	Node Management-LIF	Mailserver	SMTP-Warnungen können für AutoSupport verwendet werden

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.



Other AWS accounts ✕

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#) 

arn:aws:iam:::root

- 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 Secret Cloud muss Ihre eigene IAM-Rolle angegeben werden. ["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"
  }]
}
```

Top Secret Regionen

```
{
  "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"
  }]
}
```

Geheime Regionen

```

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

```

Top Secret Regionen

```

{
  "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"
    }
  ]
}

```

Geheime Regionen

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws-iso-b: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-b: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.

Freemium

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

Schritte

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

- a. Klicken Sie auf der Seite **Details und Anmeldeinformationen** auf **Anmeldedaten bearbeiten > Abonnement hinzufügen** und befolgen Sie dann die Anweisungen, um das Pay-as-you-go-Angebot im 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".

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

1 AWS Marketplace
Subscribe and then click **Set Up Your Account** to configure your account.

2 Cloud Manager
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue **Cancel**

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

Select Charging Method

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

["Sehen Sie sich Schritt-für-Schritt-Anleitungen 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.

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 **AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 **Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

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

Select Charging Method

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

"Sehen Sie sich [Schritt-für-Schritt-Anleitungen 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.

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue **Cancel**

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

Select Charging Method

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

"Sehen Sie sich Schritt-für-Schritt-Anleitungen 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.

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue **Cancel**

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

Select Charging Method

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

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

Select Charging Method

Keystone By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1 v

Professional By capacity v

Essential By capacity v

Freemium (Up to 500 GiB) By capacity v

Per Node By node v

["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 „ <i>admin</i> “ bei, oder ändern Sie ihn in einen benutzerdefinierten Benutzernamen.

Feld	Beschreibung
Anmeldedaten Bearbeiten	<p>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.</p> <p>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 handeln.</p> <p>"Erfahren Sie, wie Sie BlueXP zusätzliche AWS Zugangsdaten hinzufügen".</p>

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.



Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

Having issues signing up for your product?
If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

Subscribe

You are already subscribed to this product

Pricing Details

Software Fees

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: <ul style="list-style-type: none"> • 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 WORM:**

- 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:

Volume Details, Protection & Protocol

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

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

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**.

Einige AWS lokale Zonen sind verfügbar.

Bevor Sie AWS Local Zones verwenden können, müssen Sie lokale Zonen aktivieren und in Ihrem AWS-Konto ein Subnetz in der lokalen Zone erstellen. Folgen Sie den Schritten **in einer AWS Local Zone** und **Extend Your Amazon VPC to the Local Zone** im ["AWS Tutorial „erste Schritte mit der Bereitstellung von Anwendungen mit niedriger Latenz mit AWS Local Zones"](#).

Wenn Sie eine Connector-Version 3.9.36 oder niedriger ausführen, müssen Sie die folgende Berechtigung zur AWS Connector-Rolle in der AWS EC2-Konsole hinzufügen: DescribeAvailability Zones.

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 „ <i>admin</i> “ 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 handeln. 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.



Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

?

Having issues signing up for your product?
If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

Subscribe

You are already subscribed to this product

Pricing Details

Software Fees

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	<p>Wenn Sie BlueXP die Sicherheitsgruppe für Sie generieren lassen, müssen Sie festlegen, wie Sie den Datenverkehr zulassen:</p> <ul style="list-style-type: none"> Wenn Sie Selected VPC Only wählen, ist 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	<p>Wenn Sie eine vorhandene Firewallrichtlinie verwenden, stellen Sie sicher, dass diese die erforderlichen Regeln enthält. "Informieren Sie sich über die Firewall-Regeln für Cloud Volumes ONTAP".</p>

8. **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:

Volume Details, Protection & Protocol

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

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

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.

Implementieren Sie Cloud Volumes ONTAP in AWS Secret Cloud und Top Secret Cloud-Regionen

Wie in einer Standardregion von AWS können Sie BlueXP auch einsetzen ["AWS Secret Cloud"](#) Und ein ["Top Secret Cloud von AWS"](#) Zur Implementierung von Cloud Volumes ONTAP mit Funktionen der Enterprise-Klasse für Ihren Cloud-Storage. AWS Secret Cloud und Top Secret Cloud sind geschlossene Regionen speziell für die USA Intelligence Community: Die Anweisungen auf dieser Seite gelten nur für Benutzer der AWS Secret Cloud und der Region Top Secret Cloud.

Bevor Sie beginnen

Bevor Sie beginnen, sehen Sie sich die unterstützten Versionen in AWS Secret Cloud und Top Secret Cloud an, und informieren Sie sich über den Private-Modus in BlueXP.

- Prüfen Sie die folgenden unterstützten Versionen in AWS Secret Cloud und Top Secret Cloud:
 - Cloud Volumes ONTAP 9.12.1 P2
 - Version 3.9.32 des Connectors

Der Connector ist eine Software, die für die Implementierung und das Management von Cloud Volumes ONTAP in AWS benötigt wird. Sie melden sich bei BlueXP über die Software an, die auf der Connector-Instanz installiert wird. Die SaaS-Website für BlueXP wird in AWS Secret Cloud und Top

Secret Cloud nicht unterstützt.

- Weitere Informationen zum privaten Modus

In AWS Secret Cloud und Top Secret Cloud arbeitet BlueXP im *Private Mode*. Im privaten Modus ist keine Konnektivität zur BlueXP SaaS-Ebene vorhanden. Benutzer greifen lokal über die webbasierte Konsole auf BlueXP zu, die über den Connector verfügbar ist und nicht über die SaaS-Schicht.

Weitere Informationen zur Funktionsweise des privaten Modus finden Sie unter ["Privater Implementierungsmodus von BlueXP"](#).

Schritt 1: 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.

Schritt 2: Berechtigungen einrichten

Richten Sie IAM-Richtlinien und -Rollen ein, die dem Connector und Cloud Volumes ONTAP die erforderlichen Berechtigungen für Aktionen in der AWS Secret Cloud oder Top Secret Cloud bieten.

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

- Die Instanz des Connectors
- Cloud Volumes ONTAP Instanzen
- Bei HA-Paaren ist die Cloud Volumes ONTAP HA-Mediatorinstanz (wenn HA-Paare implementiert werden sollen)

Schritte

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



Sie erstellen diese Richtlinien, um die S3-Buckets in Ihrer AWS-Umgebung zu unterstützen. Stellen Sie beim Erstellen der Buckets zu einem späteren Zeitpunkt sicher, dass den Bucket-Namen vorangestellt werden `fabric-pool-`. Diese Anforderung gilt sowohl für die Regionen AWS Secret Cloud als auch Top Secret Cloud.

Geheime Regionen

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

```

Top Secret Regionen

```

{
    "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

Geheime Regionen

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

Top Secret Regionen

```

{
  "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"
  }]
}

```

Wenn Sie bei HA-Paaren 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": "*"
  }
]
}

```

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

Erstellen Sie die Rolle:

Ähnlich wie bei den Richtlinien sollten Sie eine IAM-Rolle für den Konnektor und eine für die Cloud Volumes ONTAP-Knoten haben.

Für HA-Paare: 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 verfügen (wenn Sie HA-Paare implementieren möchten).

Wählen Sie die Rolle aus:

Sie müssen die Connector IAM-Rolle auswählen, wenn Sie die Connector-Instanz starten. Sie können die IAM-Rollen für Cloud Volumes ONTAP auswählen, wenn Sie eine Cloud Volumes ONTAP-Arbeitsumgebung aus BlueXP erstellen.

Bei HA-Paaren können Sie beim Erstellen einer Cloud Volumes ONTAP Arbeitsumgebung aus BlueXP die IAM-Rollen für Cloud Volumes ONTAP und den HA-Mediator auswählen.

Schritt 3: Einrichtung des AWS-KMS

Wenn Sie Amazon Verschlüsselung mit Cloud Volumes ONTAP nutzen möchten, stellen Sie sicher, dass die Anforderungen für den AWS Key Management Service (KMS) 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 BlueXP das ARN zur Verfügung stellen.

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

Dadurch erhalten BlueXP die Berechtigung zur Verwendung des CMK mit Cloud Volumes ONTAP.

Schritt 4: Installieren Sie den Connector und richten Sie BlueXP ein

Bevor Sie BlueXP zur Implementierung von Cloud Volumes ONTAP in AWS nutzen können, müssen Sie den BlueXP Connector installieren und einrichten. Mit dem Connector kann BlueXP Ressourcen und Prozesse in Ihrer Public Cloud-Umgebung managen (einschließlich Cloud Volumes ONTAP).

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.



Laden Sie für AWS Secret Cloud-Regionen die hoch NSS Root CA 2 Zertifikat, und für Top Secret Cloud, die Amazon Root CA 4 Zertifikat: Stellen Sie sicher, dass Sie nur diese Zertifikate und nicht die gesamte Kette hochladen. Die Datei für die Zertifikatskette ist groß, und der Upload kann fehlschlagen. Wenn Sie weitere Zertifikate haben, können Sie diese später hochladen, wie im nächsten Schritt beschrieben.

Sie müssen das Zertifikat während des Setup-Vorgangs hochladen. BlueXP verwendet das vertrauenswürdige Zertifikat, wenn Anfragen über HTTPS an AWS gesendet werden.

2. Starten Sie die Connector-Instanz:
 - a. Besuchen Sie die AWS Intelligence Community Marketplace Seite für BlueXP.
 - 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 beim Einrichten von Berechtigungen erstellt haben.
- Sie sollten die standardmäßigen Speicheroptionen beibehalten.
- Für den Connector sind folgende Verbindungsmethoden erforderlich: SSH, HTTP und HTTPS.

3. Richten Sie BlueXP von einem Host aus, 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. Wählen Sie **Set up New BlueXP** und folgen Sie den Anweisungen, um das System einzurichten.

- **Systemdetails:** Geben Sie einen Namen für den Connector und Ihren Firmennamen ein.
- **Admin-Benutzer erstellen:** Erstellen Sie den Admin-Benutzer für das System.

Dieses Benutzerkonto wird lokal auf dem System ausgeführt. Über BlueXP ist keine Verbindung zum aut0-Service verfügbar.

- **Review:** Überprüfen Sie die Details, akzeptieren Sie die Lizenzvereinbarung und wählen Sie dann **Setup**.

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.

Schritt 5: (Optional) Installieren Sie ein Zertifikat für den privaten Modus

Dieser Schritt ist optional für die Regionen AWS Secret Cloud und Top Secret Cloud und nur erforderlich, wenn Sie neben den im vorherigen Schritt installierten Stammzertifikaten über zusätzliche Zertifikate verfügen.

Schritte

1. Vorhandene installierte Zertifikate auflisten.

a. Führen Sie den folgenden Befehl aus, um die occm Container Docker id (identifizierter Name „ds-occm-1“) zu erfassen:

```
docker ps
```

b. Um in den occm-Container zu gelangen, führen Sie den folgenden Befehl aus:

```
docker exec -it <docker-id> /bin/sh
```

c. Um das Passwort aus der Umgebungsvariable „TRUST_STORE_PASSWORD“ zu erfassen, führen Sie den folgenden Befehl aus:

```
env
```

d. Um alle installierten Zertifikate im Truststore aufzulisten, führen Sie den folgenden Befehl aus und verwenden Sie das im vorherigen Schritt gesammelte Passwort:

```
keytool -list -v -keystore occm.truststore
```

2. Fügen Sie ein Zertifikat hinzu.

a. Führen Sie den folgenden Befehl aus, um die occm Container Docker id (identifizierter Name „ds-occm-1“) zu erfassen:

```
docker ps
```

- b. Um in den occm-Container zu gelangen, führen Sie den folgenden Befehl aus:

```
docker exec -it <docker-id> /bin/sh
```

Speichern Sie die neue Zertifikatdatei in.

- c. Um das Passwort aus der Umgebungsvariable „TRUST_STORE_PASSWORD“ zu erfassen, führen Sie den folgenden Befehl aus:

```
env
```

- d. Um das Zertifikat zum Truststore hinzuzufügen, führen Sie den folgenden Befehl aus und verwenden Sie das Kennwort aus dem vorherigen Schritt:

```
keytool -import -alias <alias-name> -file <certificate-file-name>  
-keystore occm.truststore
```

- e. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob das Zertifikat installiert ist:

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

- f. Führen Sie den folgenden Befehl aus, um den occm-Container zu beenden:

```
exit
```

- g. Führen Sie den folgenden Befehl aus, um den occm-Container zurückzusetzen:

```
docker restart <docker-id>
```

Schritt 6: Erweitern Sie das Digital Wallet von BlueXP um eine Lizenz

Wenn Sie eine Lizenz von NetApp erworben haben, müssen Sie sie zur Digital Wallet von BlueXP hinzufügen, damit Sie bei der Erstellung eines neuen Cloud Volumes ONTAP Systems die Lizenz auswählen können. Die Digital Wallet identifiziert diese Lizenzen als nicht zugewiesen.

Schritte

1. Wählen Sie im Navigationsmenü BlueXP die Option **Governance > Digital Wallet** aus.
2. Wählen Sie im Dropdown-Menü auf der Registerkarte **Cloud Volumes ONTAP** die Option **Node-basierte Lizenzen** aus.

3. Klicken Sie Auf **Nicht Zugewiesen**.
4. Klicken Sie Auf **Nicht Zugewiesene Lizenzen Hinzufügen**.
5. Geben Sie die Seriennummer der Lizenz ein oder laden Sie die Lizenzdatei hoch.
6. Wenn Sie die Lizenzdatei noch nicht besitzen, müssen Sie die Lizenzdatei manuell von netapp.com hochladen.
 - a. Wechseln Sie zum "[NetApp Lizenzdatei-Generator](#)" Und loggen Sie sich mit Ihren Anmeldedaten für die NetApp Support Site ein.
 - b. Geben Sie Ihr Passwort ein, wählen Sie Ihr Produkt aus, geben Sie die Seriennummer ein, bestätigen Sie, dass Sie die Datenschutzrichtlinie gelesen und akzeptiert haben, und klicken Sie dann auf **Absenden**.
 - c. Wählen Sie aus, ob Sie die Datei serialnumber.NLF JSON per E-Mail oder direkt herunterladen möchten.
7. Klicken Sie Auf **Lizenz Hinzufügen**.

Ergebnis

BlueXP erweitert das Digital Wallet um die Lizenz. Die Lizenz wird erst dann als nicht zugewiesen identifiziert, wenn Sie sie einem neuen Cloud Volumes ONTAP-System zuordnen. Anschließend wird die Lizenz auf die Registerkarte BYOL im Digital Wallet verschoben.

Schritt 7: Starten Sie Cloud Volumes ONTAP von BlueXP

Sie können Cloud Volumes ONTAP-Instanzen in der AWS Secret Cloud und Top Secret Cloud starten, indem Sie neue Arbeitsumgebungen in BlueXP erstellen.

Bevor Sie beginnen

Bei HA-Paaren ist ein Schlüsselpaar erforderlich, um eine schlüsslbasierte SSH-Authentifizierung beim HA-Mediator zu aktivieren.

Schritte

1. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen**.
2. Wählen Sie unter **Erstellen** die Option Cloud Volumes ONTAP.

Für HA: 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.



Wählen Sie während der Auswahl über den Assistenten nicht **Data Sense & Compliance** und **Backup in der Cloud** unter **Services** aus. Wählen Sie unter **vorkonfigurierte Pakete** **nur Konfiguration ändern** aus, und stellen Sie sicher, dass Sie keine andere Option ausgewählt haben. Vorkonfigurierte Pakete werden in den Regionen AWS Secret Cloud und Top Secret Cloud nicht unterstützt. Wenn Sie diese Option auswählen, schlägt die Bereitstellung fehl.

Hinweise zur Bereitstellung von Cloud Volumes ONTAP HA in mehreren Verfügbarkeitszonen

Beachten Sie Folgendes, wenn Sie den Assistenten für HA-Paare abschließen.

- Wenn Sie Cloud Volumes ONTAP HA in Multiple Availability Zones (AZS) implementieren, sollten Sie ein Transit-Gateway konfigurieren. Siehe "[AWS Transit Gateway einrichten](#)".

- Implementieren Sie die Konfiguration wie folgt, da zum Zeitpunkt der Veröffentlichung nur zwei AZS in der AWS Top Secret Cloud verfügbar waren:
 - Node 1: Verfügbarkeitszone A
 - Node 2: Verfügbarkeitszone B
 - Mediator: Verfügbarkeit Zone A oder B

Hinweise zur Implementierung von Cloud Volumes ONTAP in Einzel- und HA-Nodes

Beachten Sie beim Abschließen des Assistenten Folgendes:

- 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.

Ergebnis

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

Schritt 8: Sicherheitszertifikate für Data Tiering installieren

Sicherheitszertifikate müssen manuell installiert werden, um Daten-Tiering in den Regionen AWS Secret Cloud und Top Secret Cloud zu aktivieren.

Bevor Sie beginnen

1. Erstellung von S3 Buckets:



Stellen Sie sicher, dass den Bucket-Namen vorangestellt ist `fabric-pool-`. Beispiel `fabric-pool-testbucket`.

2. Behalten Sie die in installierten Stammzertifikate bei `step 4` Praktisch.

Schritte

1. Kopieren Sie den Text aus den Stammzertifikaten, die Sie in installiert haben `step 4`.

2. Stellen Sie über die CLI eine sichere Verbindung zum Cloud Volumes ONTAP System her.
3. Installieren Sie die Stammzertifikate. Drücken Sie möglicherweise die Taste `ENTER` Mehrmals drücken:

```
security certificate install -type server-ca -cert-name <certificate-  
name>
```

4. Wenn Sie dazu aufgefordert werden, geben Sie den gesamten kopierten Text ein, einschließlich und aus
----- BEGIN CERTIFICATE ----- Bis ----- END CERTIFICATE -----.
5. Bewahren Sie eine Kopie des CA-signierten digitalen Zertifikats zur späteren Verwendung auf.
6. Behalten Sie den Namen der Zertifizierungsstelle und die Seriennummer des Zertifikats bei.
7. Konfigurieren Sie den Objektspeicher für AWS Secret Cloud und Top Secret Cloud-Regionen: `set
-privilege advanced -confirmations off`
8. Führen Sie diesen Befehl aus, um den Objektspeicher zu konfigurieren.



Alle Amazon Resource Names (Arns) sollten mit einer Suffix versehen werden `-iso-b`, Wie z. B. `arn:aws-iso-b`. Wenn eine Ressource beispielsweise ein ARN mit einer Region erfordert, verwenden Sie für Top Secret Cloud die Namenskonvention als `us-iso-b` Für das `-server` Flagge. Für AWS Secret Cloud verwenden Sie `us-iso-b-1`.

```
storage aggregate object-store config create -object-store-name  
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-  
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl  
-enabled true -port 443
```

9. Überprüfen Sie, ob der Objektspeicher erfolgreich erstellt wurde: `storage aggregate object-store
show -instance`
10. Fügen Sie den Objektspeicher dem Aggregat zu. Dies sollte für jedes neue Aggregat wiederholt werden:
`storage aggregate object-store attach -aggregate <aggr1> -object-store-name
<S3Bucket>`

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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