



Richten Sie Ihr Netzwerk ein

Cloud Volumes ONTAP

NetApp
April 23, 2024

Inhalt

- Richten Sie Ihr Netzwerk ein 1
 - Netzwerkanforderungen für Cloud Volumes ONTAP in AWS..... 1
 - Einrichten eines AWS-Transit-Gateways für HA-Paare in mehreren Verfügbarkeitszonen 10
 - Implementieren Sie ein HA-Paar in einem gemeinsamen Subnetz..... 15
 - Sicherheitsgruppenregeln für AWS 17

Richten Sie Ihr Netzwerk ein

Netzwerkanforderungen für Cloud Volumes ONTAP in AWS

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

Allgemeine Anforderungen

Die folgenden Anforderungen müssen in AWS erfüllt sein.

Outbound-Internetzugang für Cloud Volumes ONTAP Nodes

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

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

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

Wenn Sie über eine NAT-Instanz verfügen, müssen Sie eine eingehende Sicherheitsgruppenregel definieren, die HTTPS-Datenverkehr vom privaten Subnetz zum Internet zulässt.

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

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

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

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

Outbound-Internetzugang für den HA Mediator

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

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

Endpunkte (AWS PrivateLink)".

Private IP-Adressen

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

Die Anzahl der LIFs, die BlueXP für Cloud Volumes ONTAP zuweist, hängt davon ab, ob Sie ein Single Node-System oder ein HA-Paar implementieren. Ein LIF ist eine IP-Adresse, die einem physischen Port zugewiesen ist.

IP-Adressen für ein Single Node-System

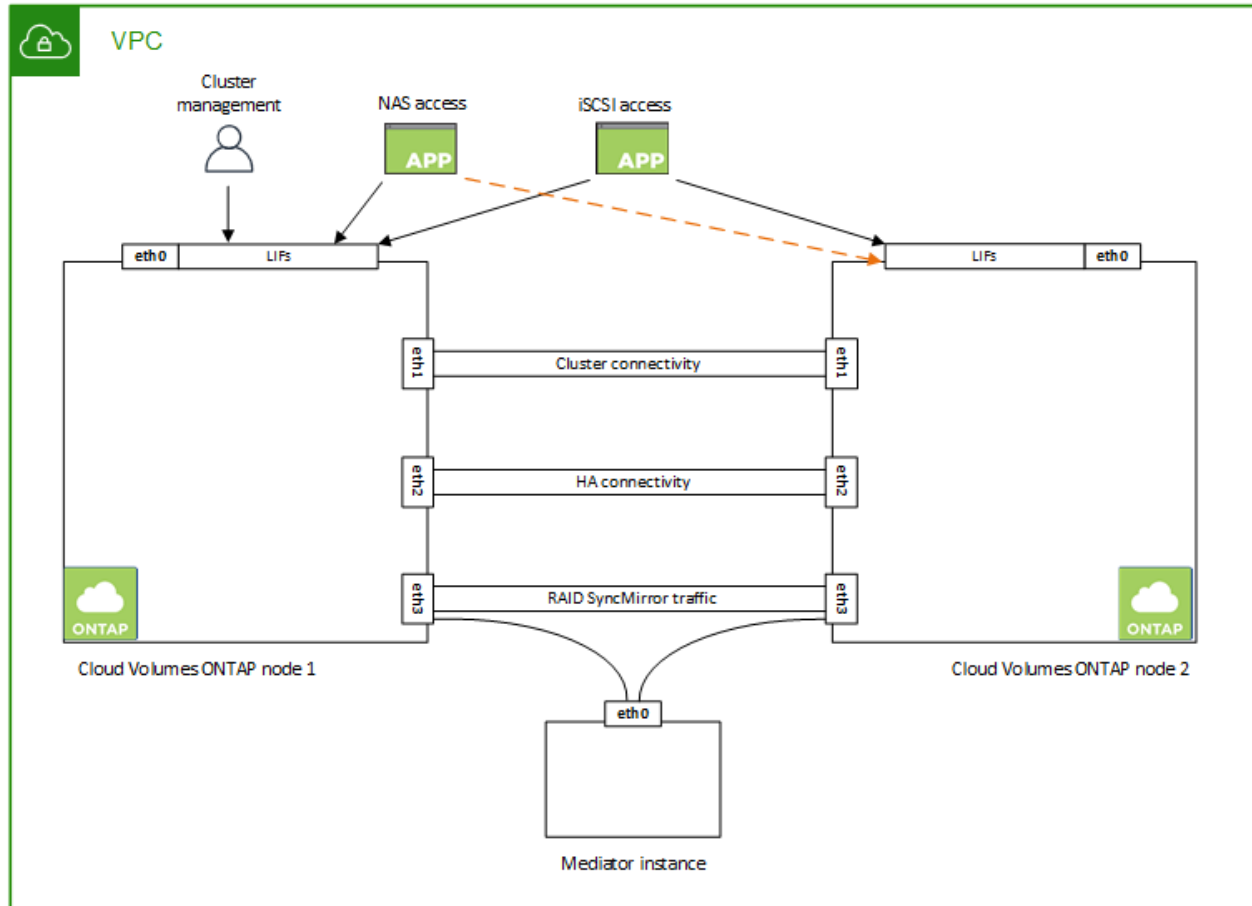
BlueXP weist einem System mit einem einzelnen Node 6 IP-Adressen zu.

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

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

IP-Adressen für HA-Paare

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



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

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

LIFs für HA-Paare in einer einzelnen Verfügbarkeitszone

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

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

LIFs für HA-Paare in mehreren Verfügbarkeitszonen

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



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

Sicherheitsgruppen

Sie müssen keine Sicherheitsgruppen erstellen, weil BlueXP das für Sie tut. Wenn Sie Ihr eigenes verwenden müssen, lesen Sie "[Regeln für Sicherheitsgruppen](#)".



Sie suchen Informationen über den Connector? "[Zeigen Sie die Sicherheitsgruppenregeln für den Konnektor an](#)"

Verbindung für Daten-Tiering

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

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

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

Verbindungen zu ONTAP Systemen

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

DNS und Active Directory für CIFS

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

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

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

VPC-Sharing

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

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

Anforderungen für HA-Paare in mehreren Verfügbarkeitszonen

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

Informationen zur Funktionsweise von HA-Paaren finden Sie unter "[Hochverfügbarkeitspaare](#)".

Verfügbarkeitszonen

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

In jeder Verfügbarkeitszone sollte ein Subnetz verfügbar sein.

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

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

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



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

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

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

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

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-Table 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"](#).

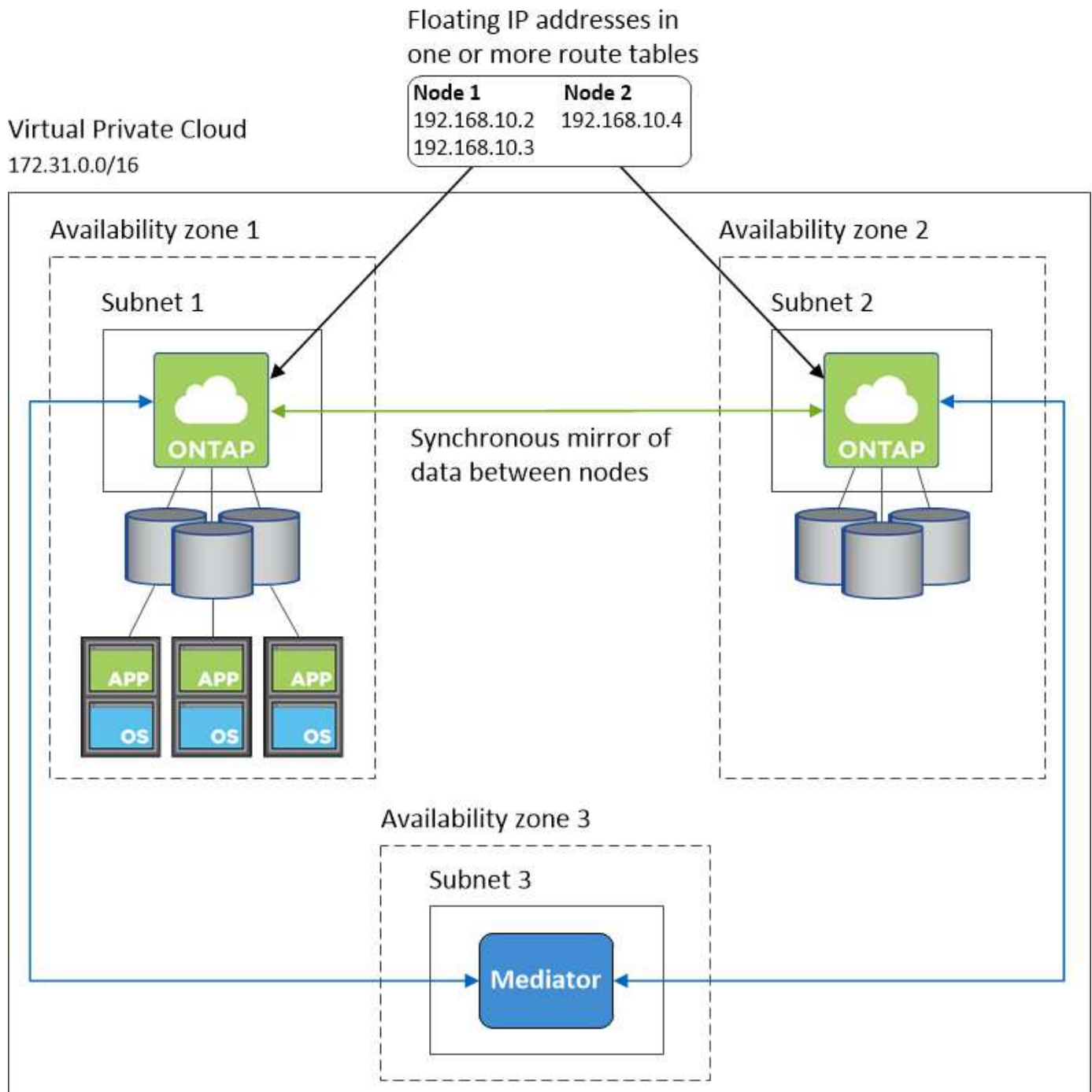
Anbindung an NetApp Management Tools

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-0ea8ee291c7aedd3

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

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

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

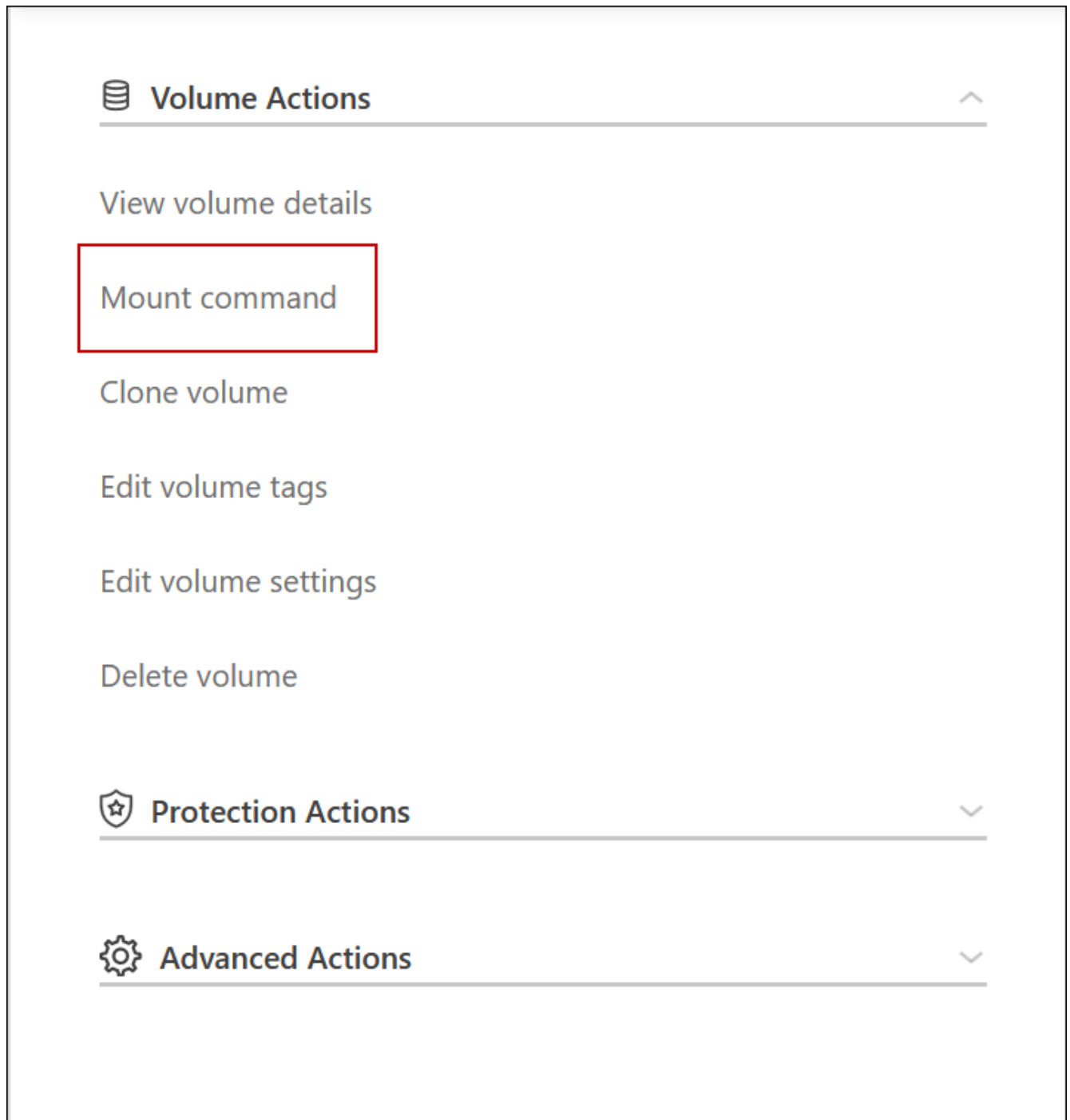
View All routes

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-0f76681216c3108ed	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



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

["Erfahren Sie, wie Sie ein Volume bearbeiten"](#).

Verwandte Links

- ["Hochverfügbarkeitspaare in AWS"](#)
- ["Netzwerkanforderungen für Cloud Volumes ONTAP in AWS"](#)

Implementieren Sie ein HA-Paar in einem gemeinsamen Subnetz

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

Mit "[VPC-Sharing](#)", Eine Cloud Volumes ONTAP HA-Konfiguration ist auf zwei Konten verteilt:

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

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

Das folgende Bild zeigt die betroffenen Komponenten für die Implementierung:



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

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

Schritte

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

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

["AWS Dokumentation: Ein Subnetz gemeinsam nutzen"](#)

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

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

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

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

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

Beachten Sie, dass Sie die folgenden Felder angeben müssen:

- „SicherheitGruppeID“

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

- "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	18600-18699	Node Management-LIF	Zielserver	NDMP-Kopie
SMTP	TCP	25	Node Management-LIF	Mailserver	SMTP-Warnungen können für AutoSupport verwendet werden

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

Regeln für die externe Sicherheitsgruppe des HA Mediators

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

Regeln für eingehende Anrufe

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

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

Regeln für ausgehende Anrufe

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

Grundlegende Regeln für ausgehende Anrufe

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

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

Erweiterte Outbound-Regeln

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

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



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

Regeln für die interne Sicherheitsgruppe der HA-Konfiguration

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

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

Regeln für eingehende Anrufe

Die vordefinierte Sicherheitsgruppe enthält die folgenden Regeln für eingehende Anrufe.

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

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe enthält die folgenden ausgehenden Regeln.

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

Regeln für den Konnektor

["Zeigen Sie die Sicherheitsgruppenregeln für den Konnektor an"](#)

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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