# Richten Sie Ihr Netzwerk ein

## Cloud Volumes ONTAP

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/de-de/storage-management-cloud-volumes-ontap/reference-networking-aws.html on February 13, 2026. Always check docs.netapp.com for the latest.

# Inhalt


Richten Sie Ihr Netzwerk ein . . . 1
AWS-Netzwerk für Cloud Volumes ONTAP einrichten . . . 1
Allgemeine Anforderungen . . . 1
Anforderungen für HA-Paare in mehreren AZs . . . 7
Anforderungen für den Konsolenagenten . . . 11
Einrichten eines AWS Transit Gateways für Cloud Volumes ONTAP HA-Paare . . . 12
Stellen Sie Cloud Volumes ONTAP HA-Paare in einem gemeinsam genutzten AWS-Subnetz bereit . . . 17
Konfigurieren Sie die Erstellung von Platzierungsgruppen für Cloud Volumes ONTAP HA-Paare in einzelnen AWS-AZs . . . 19
AWS-Sicherheitsgruppen-Ein- und Ausgangsregeln für Cloud Volumes ONTAP . . . 20
Regeln für Cloud Volumes ONTAP . . . 20
Regeln für die externe Sicherheitsgruppe des HA-Mediators . . . 25
Regeln für die interne Sicherheitsgruppe der HA-Konfiguration . . . 26
Regeln für den Konsolenagenten . . . 26

# Richten Sie Ihr Netzwerk ein

## AWS-Netzwerk für Cloud Volumes ONTAP einrichten

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

### Allgemeine Anforderungen

Stellen Sie sicher, dass Sie die folgenden Anforderungen in AWS erfüllt haben.

#### Ausgehender Internetzugang für Cloud Volumes ONTAP -Knoten

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

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

##### Cloud Volumes ONTAP Endpunkte

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

| Endpunkte | Gilt für | Zweck | Bereitstellungsmodi | Auswirkungen, wenn der Endpunkt nicht verfügbar ist |
|---|---|---|---|---|
| https://netapp-cloud-account.auth0.com | Authentifizierung | Wird zur Authentifizierung in der Konsole verwendet. | Standard- und eingeschränkte Modi. | Die Benutzerauthentifizierung schlägt fehl und die folgenden Dienste sind weiterhin nicht verfügbar:<br>• Cloud Volumes ONTAP Dienste<br>• ONTAP -Dienste<br>• Protokolle und Proxy-Dienste |

| Endpunkte | Gilt für | Zweck | Bereitstellungsmodi | Auswirkungen, wenn der Endpunkt nicht verfügbar ist |
|---|---|---|---|---|
| https://api.bluexp.netapp.com/tenancy | Mietverhältnis | Wird verwendet, um Cloud Volumes ONTAP -Ressourcen von der Konsole abzurufen, um Ressourcen und Benutzer zu autorisieren. | Standard- und eingeschränkte Modi. | Cloud Volumes ONTAP Ressourcen und die Benutzer sind nicht autorisiert. |
| https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup | AutoSupport | Wird verwendet, um AutoSupport Telemetriedaten an den NetApp Support zu senden. | Standard- und eingeschränkte Modi. | AutoSupport -Informationen bleiben unversehrt. |
| Der genaue kommerzielle Endpunkt für den AWS-Dienst (mit dem Zusatz `amazonaws.com` ) hängt von der von Ihnen verwendeten AWS-Region ab. Weitere Informationen finden Sie im "AWS-Dokumentation für Details" . | • CloudFormation<br>• Elastische Compute Cloud (EC2)<br>• Identitäts- und Zugriffsverwaltung (IAM)<br>• Schlüsselverwaltungsdienst (KMS)<br>• Sicherheitstokendienst (STS)<br>• Amazon Simple Storage Service (S3) | Kommunikation mit AWS-Diensten. | Standard- und Privatmodus. | Cloud Volumes ONTAP kann nicht mit dem AWS-Dienst kommunizieren, um bestimmte Vorgänge in AWS auszuführen. |

| Endpunkte | Gilt für | Zweck | Bereitstellungsmodi | Auswirkungen, wenn der Endpunkt nicht verfügbar ist |
|---|---|---|---|---|
| Der genaue Regierungsendpunkt für den AWS-Dienst hängt von der von Ihnen verwendeten AWS-Region ab. Die Endpunkte werden mit dem Suffix `amazonaws.com` Und `c2s.ic.gov` . Siehe "AWS SDK" Und "AWS-Dokumentation" für weitere Informationen. | • CloudFormation<br>• Elastische Compute Cloud (EC2)<br>• Identitäts- und Zugriffsverwaltung (IAM)<br>• Schlüsselverwaltungsdienst (KMS)<br>• Sicherheitstokendienst (STS)<br>• Einfacher Speicherdienst (S3) | Kommunikation mit AWS-Diensten. | Eingeschränkter Modus. | Cloud Volumes ONTAP kann nicht mit dem AWS-Dienst kommunizieren, um bestimmte Vorgänge in AWS auszuführen. |

### Ausgehender Internetzugang für den HA-Mediator

Die HA-Mediatorinstanz muss über eine ausgehende Verbindung zum AWS EC2-Dienst verfügen, damit sie beim Speicherfailover helfen 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 Schnittstellen-VPC-Endpunkt vom Zielsubnetz zum AWS EC2-Dienst sein. Weitere Informationen zu VPC-Endpunkten finden Sie im "AWS-Dokumentation: Schnittstelle für VPC-Endpunkte (AWS PrivateLink)" .

### Netzwerkproxykonfiguration des NetApp Console Agenten

Sie können die Proxyserverkonfiguration des NetApp Console Agenten verwenden, um ausgehenden Internetzugriff von Cloud Volumes ONTAP zu aktivieren. Die Konsole unterstützt zwei Arten von Proxys:

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

Informationen zum Konfigurieren von Proxy-Servern finden Sie im "Konfigurieren des Konsolenagenten zur

Verwendung eines Proxyservers" .

### Private IP-Adressen

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

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

#### IP-Adressen für ein Einzelknotensystem

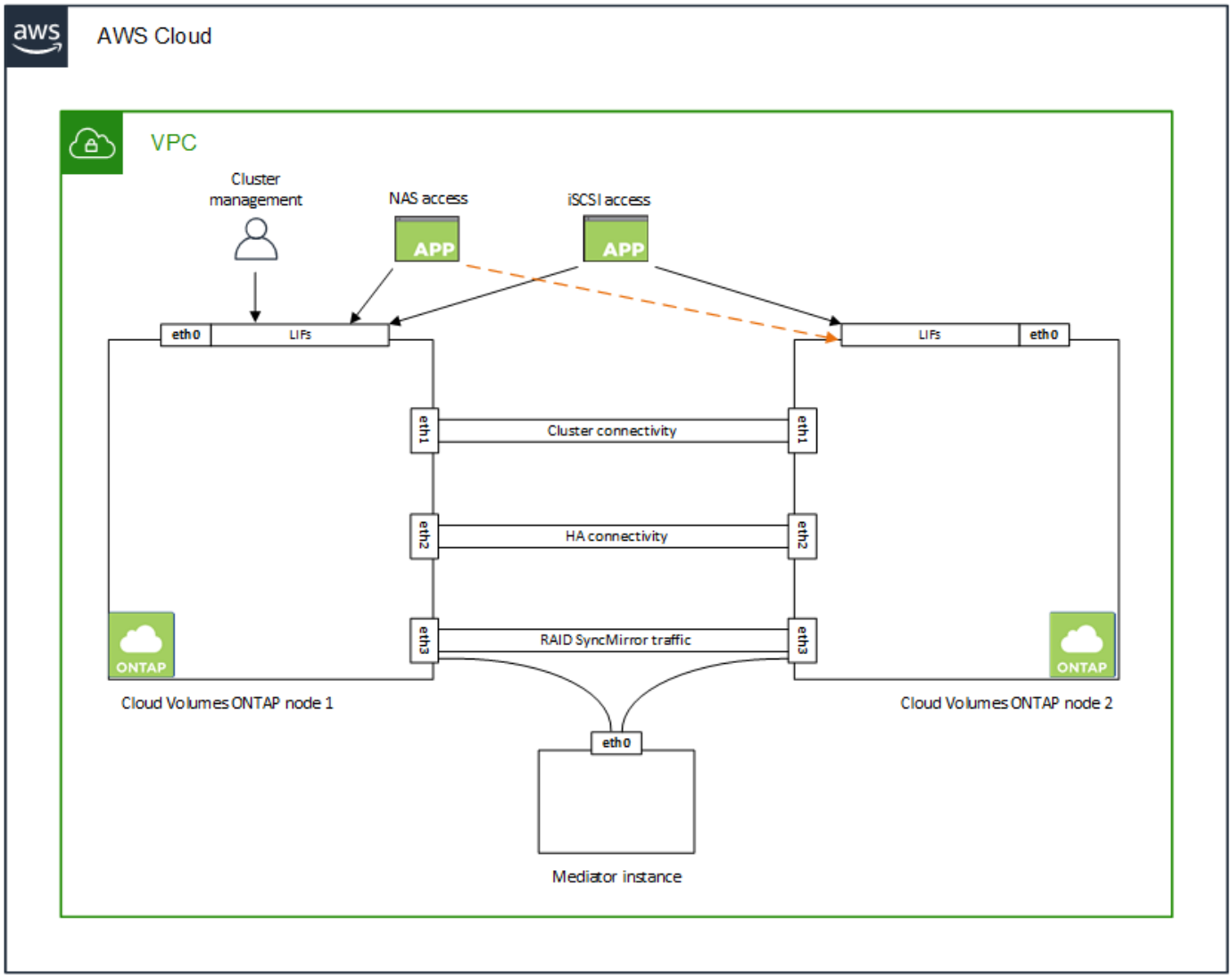
Die Konsole weist einem Einzelknotensystem 6 IP-Adressen zu.

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

| LIF | Zweck |
| --- | --- |
| Clusterverwaltung | Administrative Verwaltung des gesamten Clusters (HA-Paar). |
| Knotenverwaltung | Administrative Verwaltung eines Knotens. |
| Intercluster | Clusterübergreifende Kommunikation, Sicherung und Replikation. |
| NAS-Daten | Clientzugriff über NAS-Protokolle. |
| iSCSI-Daten | Clientzugriff über das iSCSI-Protokoll. Wird vom System auch für andere wichtige Netzwerk-Workflows verwendet. Dieses LIF ist erforderlich und sollte nicht gelöscht werden. |
| Speicher-VM-Verwaltung | Ein Storage-VM-Management-LIF wird mit Verwaltungstools wie SnapCenter verwendet. |

#### IP-Adressen für HA-Paare

HA-Paare benötigen mehr IP-Adressen als ein Einzelknotensystem. Diese IP-Adressen sind auf verschiedene Ethernet-Schnittstellen verteilt, wie in der folgenden Abbildung dargestellt:




Die Anzahl der für ein HA-Paar erforderlichen privaten IP-Adressen hängt davon ab, welches Bereitstellungsmodell Sie wählen. Ein in einer *einzelnen* AWS Availability Zone (AZ) bereitgestelltes HA-Paar erfordert 15 private IP-Adressen, während ein in *mehreren* AZs bereitgestelltes HA-Paar 13 private IP-Adressen erfordert.

Die folgenden Tabellen enthalten Details zu den LIFs, die jeder privaten IP-Adresse zugeordnet sind.

| LIF | Schnittstelle | Node | Zweck |
|---|---|---|---|
| Clusterverwaltung | eth0 | Knoten 1 | Administrative Verwaltung des gesamten Clusters (HA-Paar). |
| Knotenverwaltung | eth0 | Knoten 1 und Knoten 2 | Administrative Verwaltung eines Knotens. |
| Intercluster | eth0 | Knoten 1 und Knoten 2 | Clusterübergreifende Kommunikation, Sicherung und Replikation. |
| NAS-Daten | eth0 | Knoten 1 | Clientzugriff über NAS-Protokolle. |

| LIF | Schnittstelle | Node | Zweck |
|---|---|---|---|
| iSCSI-Daten | eth0 | Knoten 1 und Knoten 2 | Clientzugriff über das iSCSI-Protokoll. Wird vom System auch für andere wichtige Netzwerk-Workflows verwendet. Diese LIFs sind erforderlich und sollten nicht gelöscht werden. |
| Cluster-Konnektivität | eth1 | Knoten 1 und Knoten 2 | Ermöglicht den Knoten, miteinander zu kommunizieren und Daten innerhalb des Clusters zu verschieben. |
| HA-Konnektivität | eth2 | Knoten 1 und Knoten 2 | Kommunikation zwischen den beiden Knoten im Falle eines Failovers. |
| RSM-iSCSI-Datenverkehr | eth3 | Knoten 1 und Knoten 2 | RAID SyncMirror iSCSI-Verkehr sowie Kommunikation zwischen den beiden Cloud Volumes ONTAP Knoten und dem Mediator. |
| Vermittler | eth0 | Vermittler | Ein Kommunikationskanal zwischen den Knoten und dem Mediator zur Unterstützung bei Speicherübernahme- und -rückgabeprozessen. |

| LIF | Schnittstelle | Node | Zweck |
|---|---|---|---|
| Knotenverwaltung | eth0 | Knoten 1 und Knoten 2 | Administrative Verwaltung eines Knotens. |
| Intercluster | eth0 | Knoten 1 und Knoten 2 | Clusterübergreifende Kommunikation, Sicherung und Replikation. |
| iSCSI-Daten | eth0 | Knoten 1 und Knoten 2 | Clientzugriff über das iSCSI-Protokoll. Diese LIFs verwalten auch die Migration von Floating-IP-Adressen zwischen Knoten. Diese LIFs sind erforderlich und sollten nicht gelöscht werden. |
| Cluster-Konnektivität | eth1 | Knoten 1 und Knoten 2 | Ermöglicht den Knoten, miteinander zu kommunizieren und Daten innerhalb des Clusters zu verschieben. |
| HA-Konnektivität | eth2 | Knoten 1 und Knoten 2 | Kommunikation zwischen den beiden Knoten im Falle eines Failovers. |
| RSM-iSCSI-Datenverkehr | eth3 | Knoten 1 und Knoten 2 | RAID SyncMirror iSCSI-Verkehr sowie Kommunikation zwischen den beiden Cloud Volumes ONTAP Knoten und dem Mediator. |
| Vermittler | eth0 | Vermittler | Ein Kommunikationskanal zwischen den Knoten und dem Mediator zur Unterstützung bei Speicherübernahme- und -rückgabeprozessen. |

Bei der Bereitstellung in mehreren Availability Zones sind mehrere LIFs verknüpft mit"Floating-IP-Adressen" , die nicht auf das private IP-Limit von AWS angerechnet werden.

### Sicherheitsgruppen

Sie müssen keine Sicherheitsgruppen erstellen, da die Konsole dies für Sie erledigt. Wenn Sie Ihre eigene verwenden müssen, lesen Sie"Sicherheitsgruppenregeln" .

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

### Verbindung für Daten-Tiering

Wenn Sie EBS als Performance-Tier und Amazon S3 als Capacity-Tier verwenden möchten, müssen Sie sicherstellen, dass Cloud Volumes ONTAP eine Verbindung zu S3 hat. Die beste Möglichkeit, diese Verbindung bereitzustellen, ist die Erstellung eines VPC-Endpunkts für den S3-Dienst. Anweisungen finden Sie unter "AWS-Dokumentation: Erstellen eines Gateway-Endpunkts".

Achten Sie beim Erstellen des VPC-Endpunkts darauf, die Region, VPC und Routentabelle auszuwählen, die der Cloud Volumes ONTAP -Instanz entspricht. Sie müssen auch die Sicherheitsgruppe ändern, um eine ausgehende HTTPS-Regel hinzuzufügen, die den Datenverkehr zum S3-Endpunkt ermöglicht. Andernfalls kann Cloud Volumes ONTAP keine Verbindung zum S3-Dienst herstellen.

Wenn Probleme auftreten, lesen Sie die "AWS Support Knowledge Center: Warum kann ich über einen Gateway-VPC-Endpunkt keine Verbindung zu einem S3-Bucket herstellen?"

### Verbindungen zu ONTAP -Systemen

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

### DNS und Active Directory für CIFS

Wenn Sie CIFS-Speicher bereitstellen möchten, müssen Sie DNS und Active Directory in AWS einrichten oder Ihr lokales Setup auf AWS erweitern.

Der DNS-Server muss Namensauflösungsdienste für die Active Directory-Umgebung bereitstellen. Sie können DHCP-Optionssätze so konfigurieren, dass der standardmäßige EC2-DNS-Server verwendet wird. Dabei darf es sich nicht um den von der Active Directory-Umgebung verwendeten DNS-Server handeln.

Anweisungen hierzu finden Sie im "AWS-Dokumentation: Active Directory-Domänendienste in der AWS Cloud: Schnellstart-Referenzbereitstellung" .

### VPC-Freigabe

Ab der Version 9.11.1 werden Cloud Volumes ONTAP HA-Paare in AWS mit VPC-Sharing unterstützt. Durch die VPC-Freigabe kann Ihre Organisation Subnetze mit anderen AWS-Konten teilen. Um diese Konfiguration zu verwenden, müssen Sie Ihre AWS-Umgebung einrichten und dann das HA-Paar mithilfe der API bereitstellen.

"Erfahren Sie, wie Sie ein HA-Paar in einem gemeinsam genutzten Subnetz bereitstellen" .

## Anforderungen für HA-Paare in mehreren AZs

Für Cloud Volumes ONTAP HA-Konfigurationen, die mehrere Availability Zones (AZs) verwenden, gelten

zusätzliche AWS-Netzwerkanforderungen. Sie sollten diese Anforderungen überprüfen, bevor Sie ein HA-Paar starten, da Sie die Netzwerkdetails in der Konsole eingeben müssen, wenn Sie ein Cloud Volumes ONTAP -System hinzufügen.

Um zu verstehen, wie HA-Paare funktionieren, lesen Sie"Hochverfügbarkeitspaare" .

**Verfügbarkeitszonen**

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

In jeder Availability Zone sollte ein Subnetz verfügbar sein.

**Floating-IP-Adressen für NAS-Daten und Cluster-/SVM-Verwaltung**

HA-Konfigurationen in mehreren AZs verwenden Floating-IP-Adressen, die bei Fehlern zwischen Knoten migrieren. Sie sind von außerhalb der VPC nicht nativ zugänglich, es sei denn, Sie"Einrichten eines AWS Transit Gateways" .

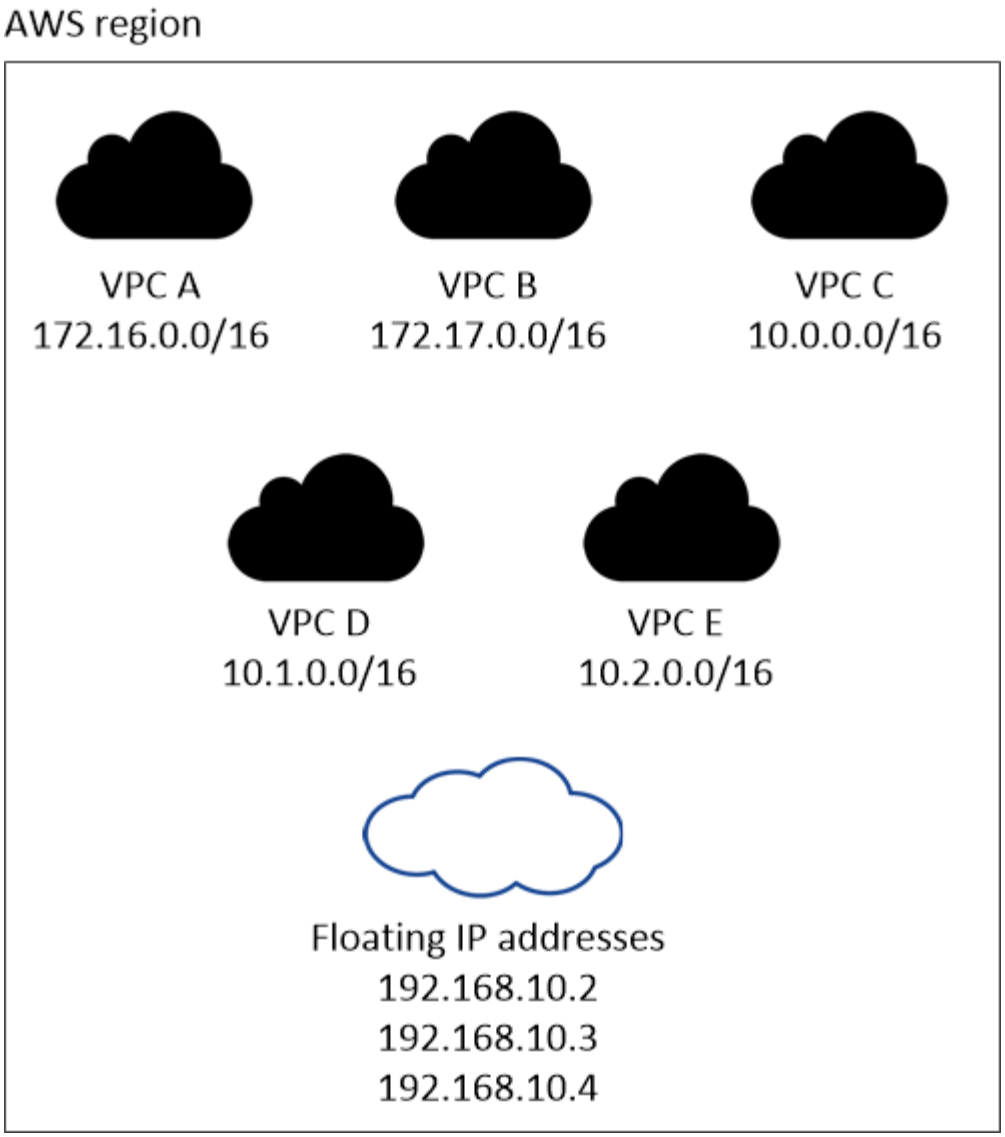
Eine Floating-IP-Adresse dient der Clusterverwaltung, eine für NFS/CIFS-Daten auf Knoten 1 und eine für NFS/CIFS-Daten auf Knoten 2. Eine vierte Floating-IP-Adresse für die SVM-Verwaltung ist optional.

Wenn Sie SnapDrive für Windows oder SnapCenter mit dem HA-Paar verwenden, ist für das SVM-Verwaltungs-LIF eine Floating-IP-Adresse erforderlich.

Sie müssen die Floating-IP-Adressen eingeben, wenn Sie ein Cloud Volumes ONTAP HA-System hinzufügen. Die Konsole weist dem HA-Paar die IP-Adressen zu, wenn sie das System startet.

Die Floating-IP-Adressen müssen außerhalb der CIDR-Blöcke für alle VPCs in der AWS-Region liegen, in der Sie die HA-Konfiguration bereitstellen. Stellen Sie sich die Floating-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 Floating-IP-Adressen für alle VPCs außerhalb der CIDR-Blöcke befinden, können sie über Routentabellen an Subnetze weitergeleitet werden.




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

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

Falls erforderlich,"Einrichten eines AWS Transit Gateways" um den Zugriff auf die Floating-IP-Adressen eines HA-Paares von außerhalb der VPC zu ermöglichen, in der sich das HA-Paar befindet.

**Routentabellen**

Nachdem Sie die Floating-IP-Adressen angegeben haben, werden Sie aufgefordert, die Routentabellen auszuwählen, die Routen zu den Floating-IP-Adressen enthalten sollen. Dies ermöglicht dem Client den Zugriff auf das HA-Paar.

Wenn Sie nur eine Routentabelle für die Subnetze in Ihrer VPC haben (die Hauptroutentabelle), fügt die Konsole die Floating-IP-Adressen automatisch zu dieser Routentabelle hinzu. Wenn Sie mehr als eine Routentabelle haben, ist es sehr wichtig, beim Starten des HA-Paares die richtigen Routentabellen auszuwählen. Andernfalls haben einige Clients möglicherweise keinen Zugriff auf Cloud Volumes ONTAP.

Beispielsweise könnten Sie zwei Subnetze haben, die mit unterschiedlichen Routentabellen verknüpft sind.

Wenn Sie Routentabelle A, aber nicht Routentabelle B auswählen, können Clients im mit Routentabelle A verknüpften Subnetz auf das HA-Paar zugreifen, Clients im mit Routentabelle B verknüpften Subnetz jedoch nicht.

Weitere Informationen zu Routentabellen finden Sie im "AWS-Dokumentation: Routentabellen" .

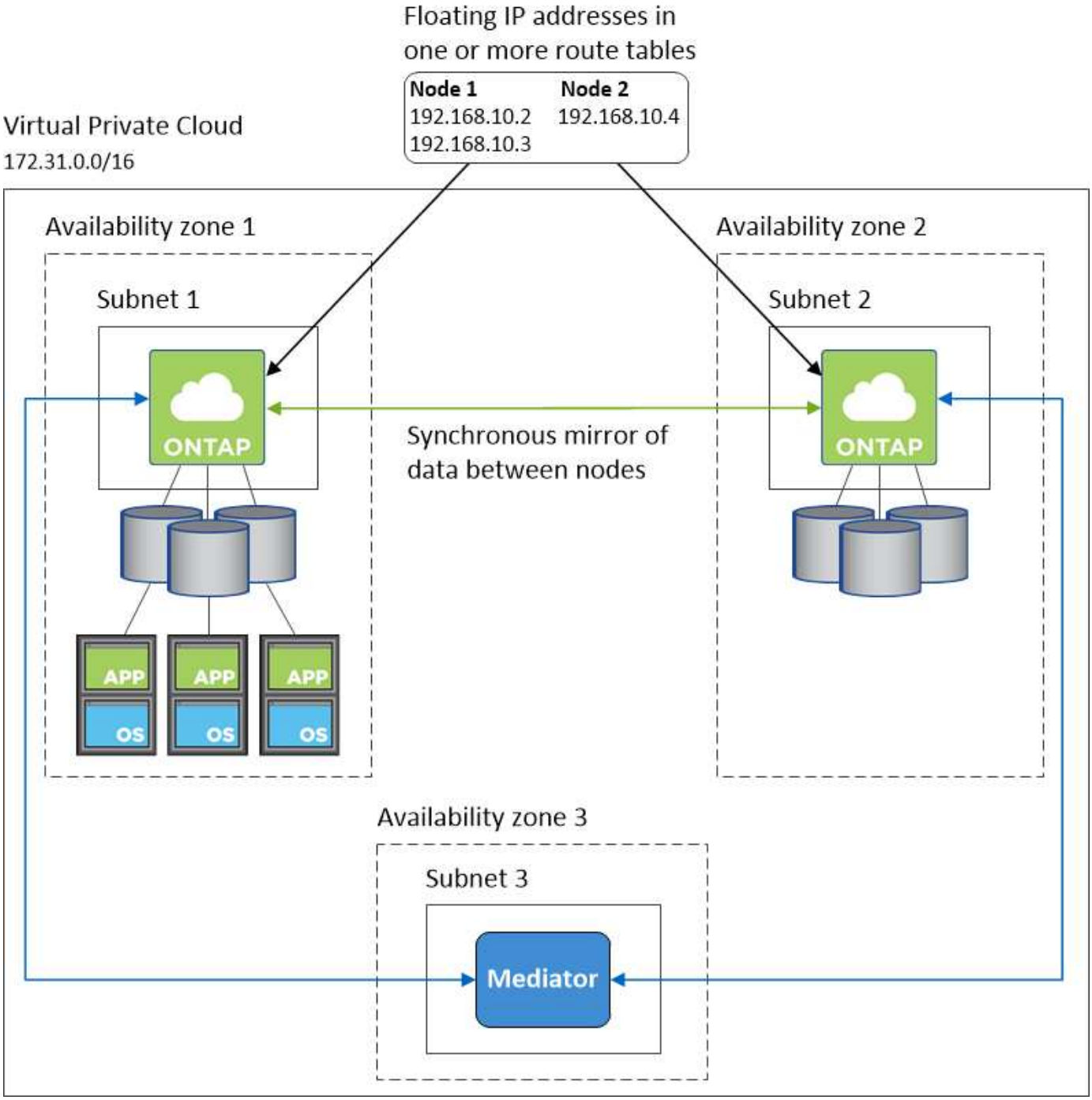
**Anbindung an NetApp Management Tools**

Um NetApp -Verwaltungstools mit HA-Konfigurationen zu verwenden, die sich in mehreren AZs befinden, haben Sie zwei Verbindungsoptionen:

1. Stellen Sie die NetApp -Verwaltungstools in einer anderen VPC bereit und"Einrichten eines AWS Transit Gateways" . Das Gateway ermöglicht den Zugriff auf die Floating-IP-Adresse für die Cluster-Management-Schnittstelle von außerhalb der VPC.
2. Stellen Sie die NetApp -Verwaltungstools im selben VPC mit einer ähnlichen Routing-Konfiguration wie NAS-Clients bereit.

**Beispiel einer HA-Konfiguration**

Das folgende Bild veranschaulicht die Netzwerkkomponenten, die für ein HA-Paar in mehreren AZs spezifisch sind: drei Availability Zones, drei Subnetze, Floating-IP-Adressen und eine Routentabelle.




## Anforderungen für den Konsolenagenten

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

- "Netzwerkanforderungen für den Konsolenagenten anzeigen"
- "Sicherheitsgruppenregeln in AWS"

**Verwandte Themen**

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

# Einrichten eines AWS Transit Gateways für Cloud Volumes ONTAP HA-Paare

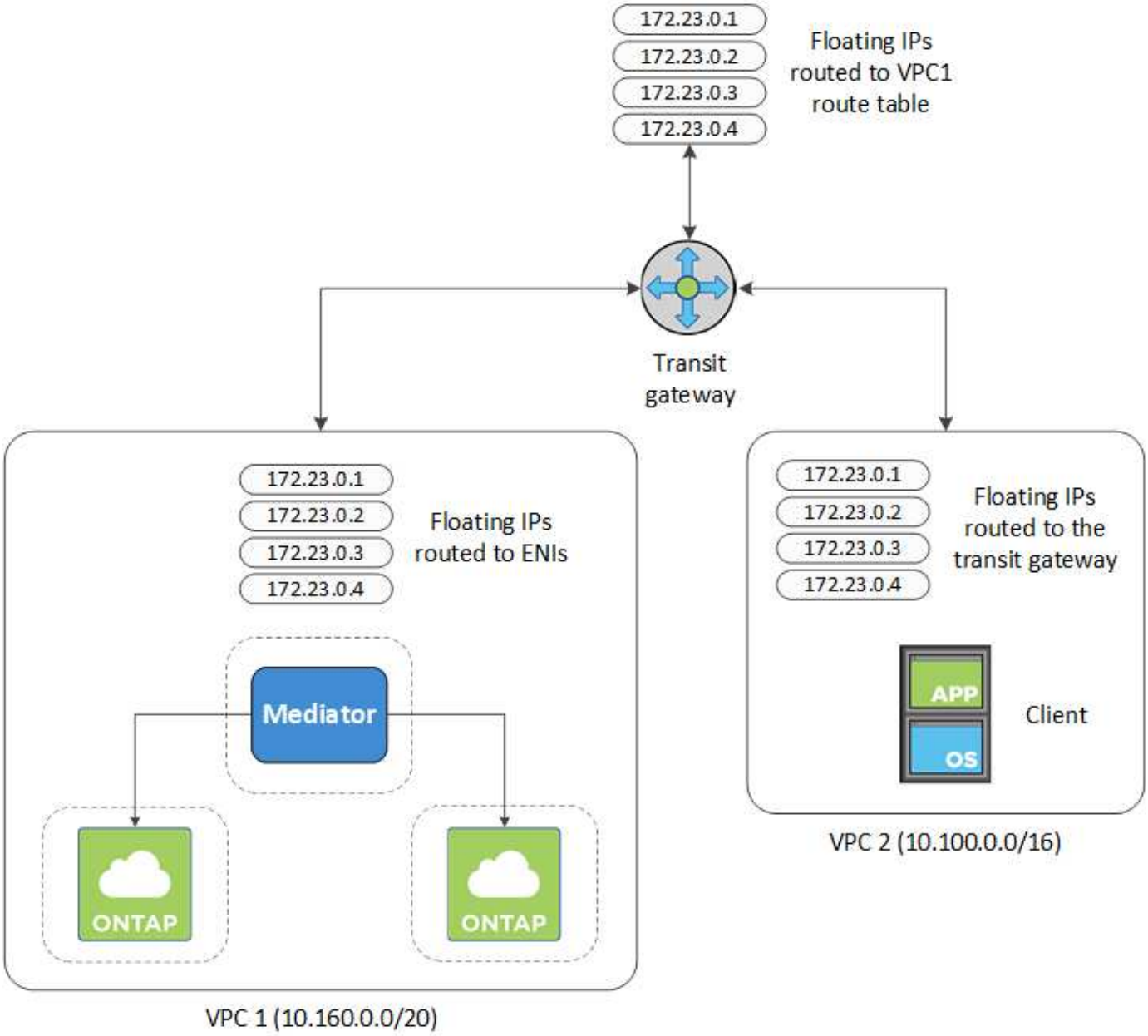
Richten Sie ein AWS Transit Gateway ein, um den Zugriff auf die HA-Paare zu ermöglichen."Floating-IP-Adressen" von außerhalb der VPC, in der sich das HA-Paar befindet.

Wenn eine Cloud Volumes ONTAP HA-Konfiguration über mehrere AWS Availability Zones verteilt ist, sind Floating-IP-Adressen für den NAS-Datenzugriff innerhalb der VPC erforderlich. Diese Floating-IP-Adressen können bei Fehlern zwischen Knoten migrieren, sind jedoch von 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 werden auch für die Cluster-Management-Schnittstelle und das optionale SVM-Management-LIF benötigt.

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

Hier ist ein Beispiel, das zwei VPCs zeigt, die durch ein Transit-Gateway verbunden sind. In einer VPC befindet sich ein HA-System, in der anderen ein Client. Sie könnten dann mithilfe der Floating-IP-Adresse ein NAS-Volume auf dem Client mounten.



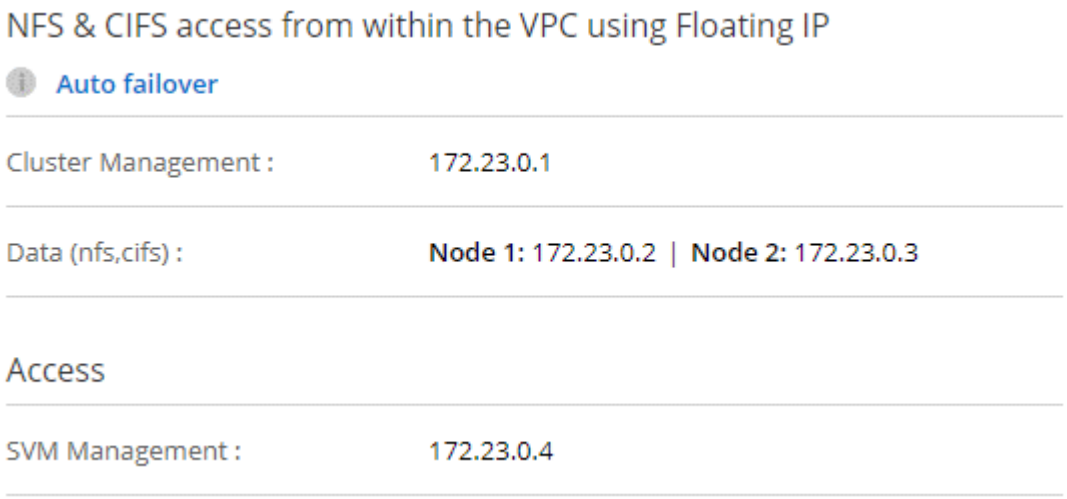

Die folgenden Schritte veranschaulichen, wie eine ähnliche Konfiguration eingerichtet wird.

**Schritte**

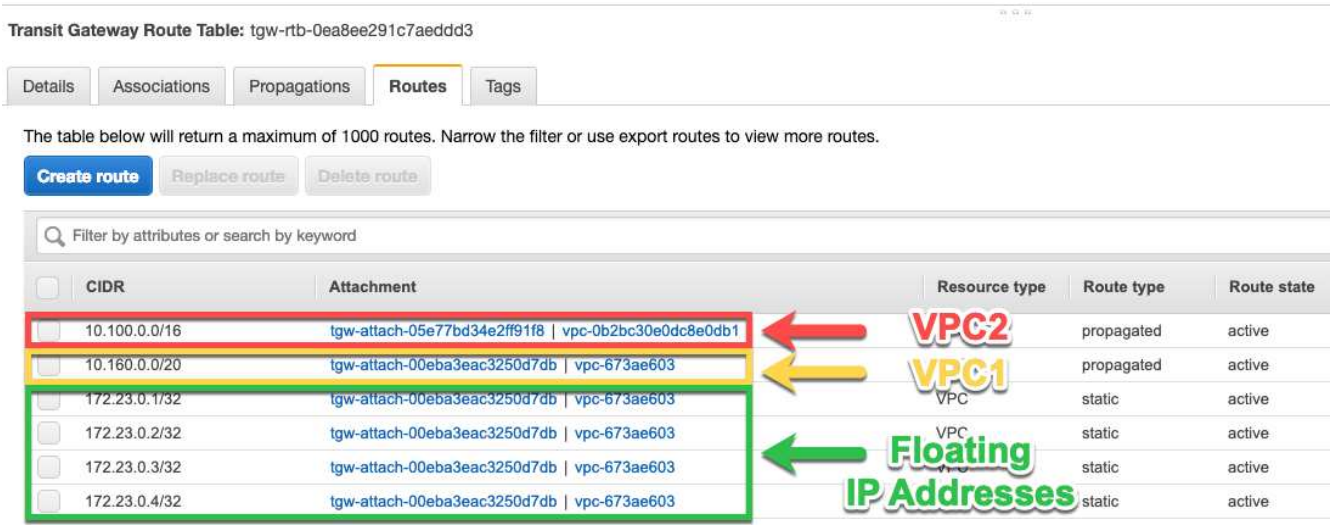
1. "Erstellen Sie ein Transit-Gateway und hängen Sie die VPCs an das Gateway an" .
2. Ordnen Sie die VPCs der Transit-Gateway-Routentabelle zu.
   a. Klicken Sie im **VPC**-Dienst auf **Transit Gateway Route Tables**.
   b. Wählen Sie die Routentabelle aus.
   c. Klicken Sie auf **Verknüpfungen** und wählen Sie dann **Verknüpfung erstellen**.
   d. Wählen Sie die zu verknüpfenden Anhänge (die VPCs) aus und klicken Sie dann auf **Verknüpfung erstellen**.
3. Erstellen Sie Routen in der Routentabelle des Transit-Gateways, indem Sie die Floating-IP-Adressen des HA-Paares angeben.

   Sie finden die Floating-IP-Adressen auf der Systeminformationsseite in der NetApp Console. Hier ist ein

Beispiel:




Das folgende Beispielbild zeigt die Routentabelle für das Transit Gateway. Es umfasst Routen zu den CIDR-Blöcken der beiden VPCs und vier Floating-IP-Adressen, die von Cloud Volumes ONTAP verwendet werden.

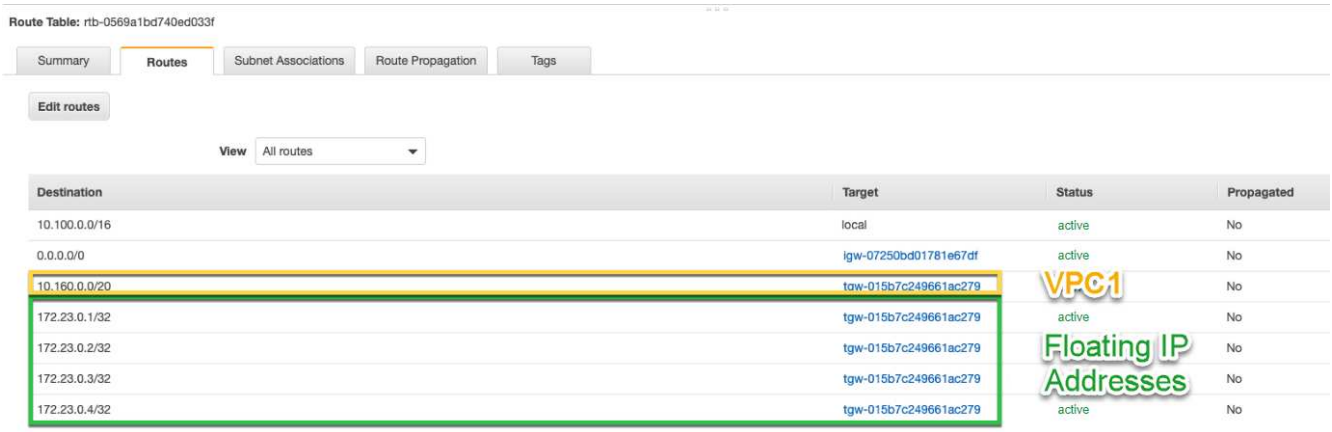



4. Ändern Sie die Routentabelle der VPCs, die auf die Floating-IP-Adressen zugreifen müssen.

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

   b. Fügen Sie dem CIDR-Block der VPC, in der sich das HA-Paar befindet, einen Routeneintrag hinzu.

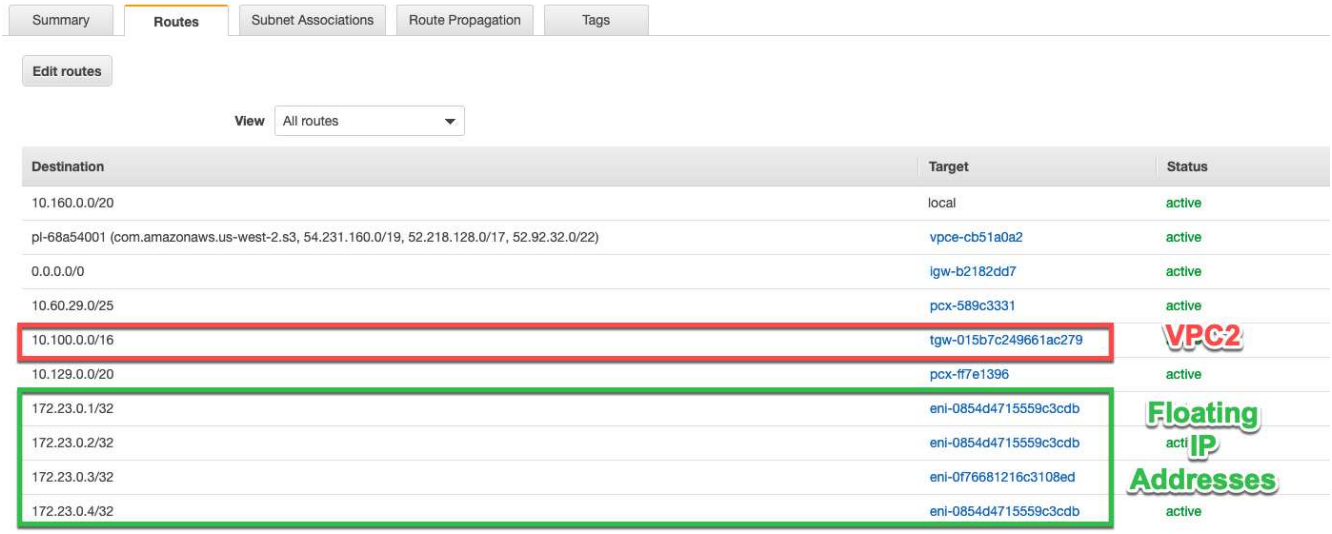
      Das folgende Beispielbild zeigt die Routentabelle für VPC 2, die Routen zu VPC 1 und die Floating-IP-Adressen enthält.




5. Ändern Sie die Routentabelle für die VPC des HA-Paares, indem Sie eine Route zur VPC hinzufügen, die Zugriff auf die Floating-IP-Adressen benötigt.

   Dieser Schritt ist wichtig, da er das Routing zwischen den VPCs abschließt.

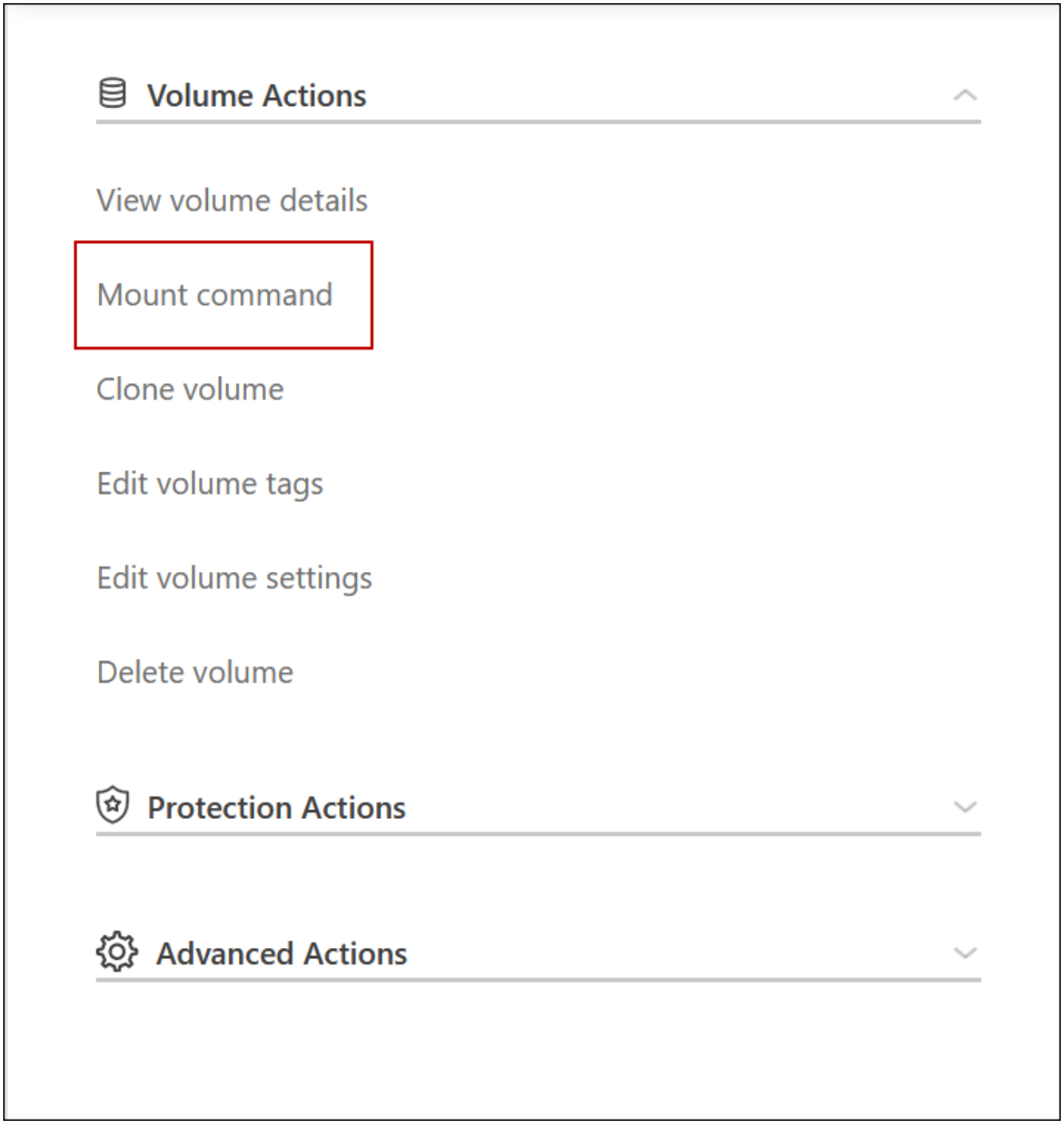
   Das folgende Beispielbild zeigt die Routentabelle für VPC 1. Es enthält eine Route zu den Floating-IP-Adressen und zu VPC 2, wo sich ein Client befindet. Die Konsole hat die Floating-IPs automatisch zur Routentabelle hinzugefügt, als sie das HA-Paar bereitgestellt hat.




6. Aktualisieren Sie die Einstellungen der Sicherheitsgruppen auf „Gesamter Datenverkehr für die VPC“.
   a. Klicken Sie unter „Virtual Private Cloud“ auf **Subnetze**.
   b. Klicken Sie auf die Registerkarte **Routentabelle** und wählen Sie die gewünschte Umgebung für eine der Floating-IP-Adressen für ein HA-Paar aus.
   c. Klicken Sie auf **Sicherheitsgruppen**.
   d. Wählen Sie **Eingehende Regeln bearbeiten**.
   e. Klicken Sie auf **Regel hinzufügen**.
   f. Wählen Sie unter „Typ“ die Option „Gesamter Datenverkehr“ und dann die VPC-IP-Adresse aus.
   g. Klicken Sie auf **Regeln speichern**, um die Änderungen anzuwenden.
7. Hängen Sie Volumes mithilfe der Floating-IP-Adresse an Clients an.

   Sie finden die richtige IP-Adresse in der Konsole über die Option **Mount Command** im Bereich „Volumes

verwalten“ in der Konsole.




8. Wenn Sie ein NFS-Volume mounten, konfigurieren Sie die Exportrichtlinie so, dass sie mit dem Subnetz der Client-VPC übereinstimmt.

   "Erfahren Sie, wie Sie ein Volume bearbeiten" .

**Weiterführende Links**

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

# Stellen Sie Cloud Volumes ONTAP HA-Paare in einem gemeinsam genutzten AWS-Subnetz bereit

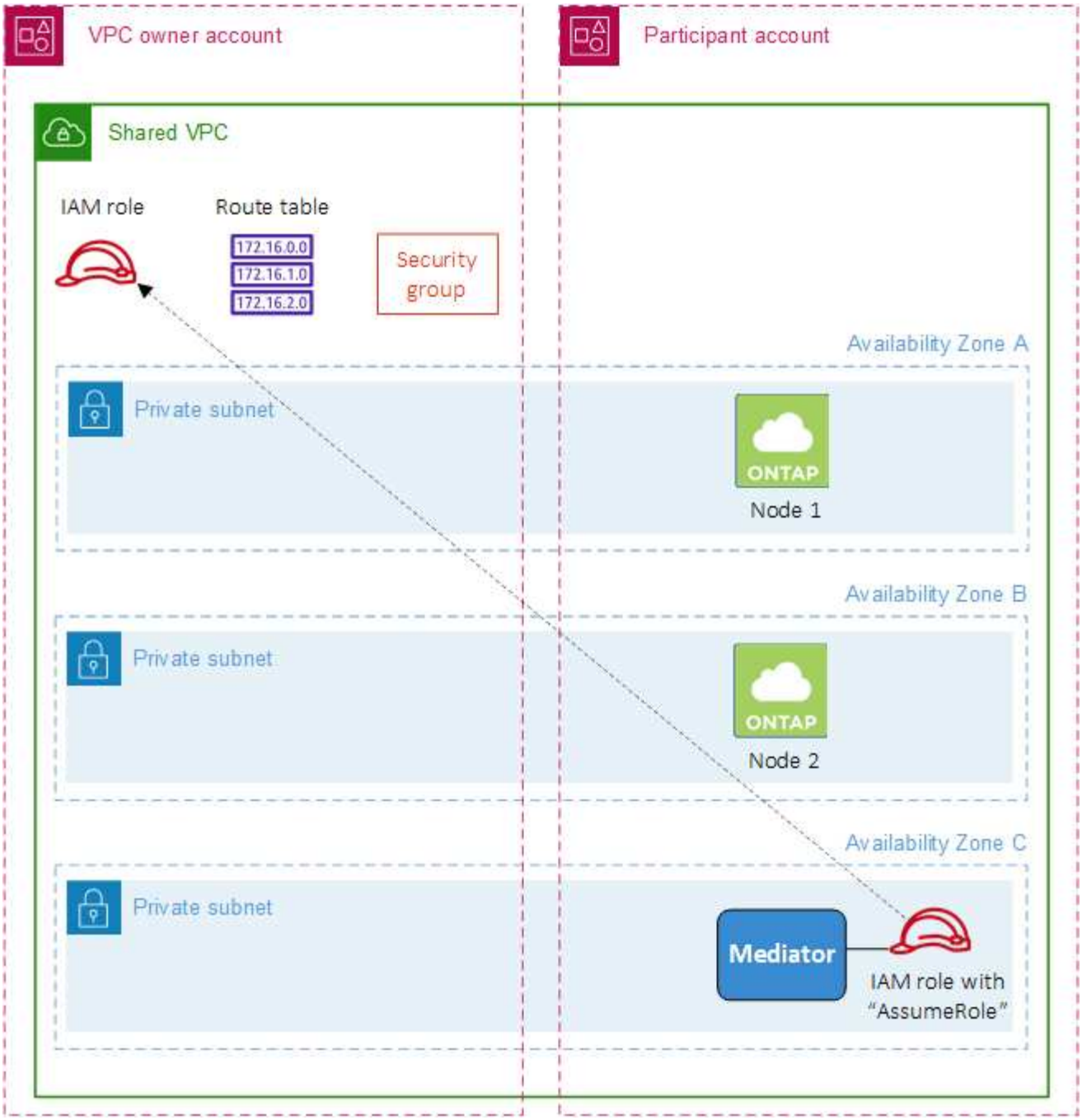
Ab der Version 9.11.1 werden Cloud Volumes ONTAP HA-Paare in AWS mit VPC-Sharing unterstützt. Durch die VPC-Freigabe kann Ihre Organisation Subnetze mit anderen AWS-Konten teilen. Um diese Konfiguration zu verwenden, müssen Sie Ihre AWS-Umgebung einrichten und dann das HA-Paar mithilfe der API bereitstellen.

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

- Das VPC-Eigentümerkonto, dem das Netzwerk gehört (VPC, Subnetze, Routentabellen und Cloud Volumes ONTAP Sicherheitsgruppe)
- Das Teilnehmerkonto, in dem die EC2-Instanzen in gemeinsam genutzten Subnetzen bereitgestellt werden (dazu gehören die beiden HA-Knoten und der Mediator)

Im Fall einer Cloud Volumes ONTAP HA-Konfiguration, die über mehrere Availability Zones hinweg bereitgestellt wird, benötigt der HA-Mediator bestimmte Berechtigungen zum Schreiben in die Routentabellen im VPC-Eigentümerkonto. Sie müssen diese Berechtigungen bereitstellen, indem Sie eine IAM-Rolle einrichten, die der Mediator übernehmen kann.

Das folgende Bild zeigt die an dieser Bereitstellung beteiligten Komponenten:




Wie in den folgenden Schritten beschrieben, müssen Sie die Subnetze mit dem Teilnehmerkonto teilen und dann die IAM-Rolle und Sicherheitsgruppe im VPC-Eigentümerkonto erstellen.

Wenn Sie das Cloud Volumes ONTAP -System erstellen, erstellt die NetApp Console automatisch eine IAM-Rolle und fügt sie dem Mediator hinzu. Diese Rolle übernimmt die IAM-Rolle, die Sie im VPC-Eigentümerkonto erstellt haben, um Änderungen an den mit dem HA-Paar verknüpften Routentabellen vorzunehmen.

**Schritte**

1. Geben Sie die Subnetze im VPC-Eigentümerkonto für das Teilnehmerkonto frei.

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

   "AWS-Dokumentation: Freigeben eines Subnetzes"

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

   "Beachten Sie die Sicherheitsgruppenregeln für Cloud Volumes ONTAP" . Beachten Sie, dass Sie für den HA-Mediator keine Sicherheitsgruppe erstellen müssen. Die Konsole erledigt das für Sie.

3. Erstellen Sie im VPC-Eigentümerkonto eine IAM-Rolle, die die folgenden Berechtigungen umfasst:

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

4. Verwenden Sie die API, um ein neues Cloud Volumes ONTAP System zu erstellen.

   Beachten Sie, dass Sie die folgenden Felder angeben müssen:

   - "Sicherheitsgruppen-ID"

     Das Feld „securityGroupId“ sollte die Sicherheitsgruppe angeben, die Sie im VPC-Eigentümerkonto erstellt haben (siehe Schritt 2 oben).

   - "assumeRoleArn" im "haParams"-Objekt

     Das Feld „assumeRoleArn“ sollte die ARN der IAM-Rolle enthalten, die Sie im VPC-Eigentümerkonto 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"

# Konfigurieren Sie die Erstellung von Platzierungsgruppen für Cloud Volumes ONTAP HA-Paare in einzelnen AWS-AZs

Bei Bereitstellungen mit hoher Verfügbarkeit (HA) von Cloud Volumes ONTAP in einer einzelnen AWS-Verfügbarkeitszone (AZ) kann es zu Fehlern und einem Rollback kommen, wenn die Erstellung der Platzierungsgruppe fehlschlägt. Die Erstellung der

Platzierungsgruppe schlägt ebenfalls fehl und die Bereitstellung wird zurückgesetzt, wenn der Cloud Volumes ONTAP Knoten und die Mediatorinstanz nicht verfügbar sind. Um dies zu vermeiden, können Sie die Konfiguration so ändern, dass die Bereitstellung auch dann abgeschlossen werden kann, wenn die Erstellung der Platzierungsgruppe fehlschlägt.

Wenn Sie den Rollback-Prozess umgehen, wird der Bereitstellungsprozess von Cloud Volumes ONTAP erfolgreich abgeschlossen und Sie werden benachrichtigt, dass die Erstellung der Platzierungsgruppe unvollständig ist.

**Schritte**

1. Verwenden Sie SSH, um eine Verbindung zum NetApp Console Agent-Host herzustellen und sich anzumelden.
2. Navigieren Sie zu `/opt/application/netapp/cloudmanager/docker_occm/data` .
3. Bearbeiten `app.conf` durch Ändern des Wertes der `rollback-on-placement-group-failure` Parameter auf `false` . Der Standardwert dieses Parameters ist `true` .

```
{
    "occm" : {
        "aws" : {
            "rollback-on-placement-group-failure" : false
        }
    }
}
```

4. Speichern Sie die Datei und melden Sie sich vom Konsolenagenten ab. Sie müssen den Konsolenagenten nicht neu starten.

# AWS-Sicherheitsgruppen-Ein- und Ausgangsregeln für Cloud Volumes ONTAP

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

## Regeln für Cloud Volumes ONTAP

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

### Eingehende Regeln

Wenn Sie ein Cloud Volumes ONTAP -System hinzufügen und eine vordefinierte Sicherheitsgruppe auswählen, können Sie den Datenverkehr innerhalb einer der folgenden Gruppen zulassen:

- **Nur ausgewählte VPC**: Die Quelle für eingehenden Datenverkehr ist der Subnetzbereich der VPC für das Cloud Volumes ONTAP -System und der Subnetzbereich der VPC, in der sich der Konsolenagent befindet. Dies ist die empfohlene Option.

- **Alle VPCs**: Die Quelle für eingehenden Datenverkehr ist der IP-Bereich 0.0.0.0/0.

| Protokoll | Hafen | Zweck |
|---|---|---|
| Alle ICMP | Alle | Pingen der Instanz |
| HTTP | 80 | HTTP-Zugriff auf die ONTAP System Manager-Webkonsole über die IP-Adresse des Cluster-Management-LIF |
| HTTPS | 443 | Konnektivität mit dem Konsolenagenten und HTTPS-Zugriff auf die ONTAP System Manager-Webkonsole unter Verwendung der IP-Adresse des Cluster-Management-LIF |
| SSH | 22 | SSH-Zugriff auf die IP-Adresse des Cluster-Management-LIF oder eines Node-Management-LIF |
| TCP | 111 | Remote Procedure Call für NFS |
| TCP | 139 | NetBIOS-Dienstsitzung für CIFS |
| TCP | 161-162 | Einfaches Netzwerkverwaltungsprotokoll |
| TCP | 445 | Microsoft SMB/CIFS über TCP mit NetBIOS-Framing |
| TCP | 635 | NFS-Mount |
| TCP | 749 | Kerberos |
| TCP | 2049 | NFS-Server-Daemon |
| TCP | 3260 | iSCSI-Zugriff über das iSCSI-Daten-LIF |
| TCP | 4045 | NFS-Sperrdaemon |
| TCP | 4046 | Netzwerkstatusmonitor für NFS |
| TCP | 10000 | Sicherung mit NDMP |
| TCP | 11104 | Verwaltung von Intercluster-Kommunikationssitzungen für SnapMirror |
| TCP | 11105 | SnapMirror Datenübertragung mithilfe von Intercluster-LIFs |
| UDP | 111 | Remote Procedure Call für NFS |
| UDP | 161-162 | Einfaches Netzwerkverwaltungsprotokoll |
| UDP | 635 | NFS-Mount |
| UDP | 2049 | NFS-Server-Daemon |
| UDP | 4045 | NFS-Sperrdaemon |
| UDP | 4046 | Netzwerkstatusmonitor für NFS |
| UDP | 4049 | NFS-Rquotad-Protokoll |

#### Ausgangsregeln

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

#### Grundlegende Ausgangsregeln

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

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

#### Erweiterte Ausgangsregeln

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

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

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

| Service | Protokoll | Hafen | Quelle | Ziel | Zweck |
|---|---|---|---|---|---|
| AutoSupport | HTTPS | 443 | Knotenverwaltung LIF | mysupport.netapp.com | AutoSupport (HTTPS ist die Standardeinstellung) |
| | HTTP | 80 | Knotenverwaltung LIF | mysupport.netapp.com | AutoSupport (nur wenn das Transportprotokoll von HTTPS auf HTTP geändert wird) |
| | TCP | 3128 | Knotenverwaltung LIF | Konsolenagent | Senden von AutoSupport -Nachrichten über einen Proxyserver auf dem Konsolenagenten, wenn keine ausgehende Internetverbindung verfügbar ist |
| Sicherung auf S3 | TCP | 5010 | Intercluster LIF | Sicherungsendpunkt oder Wiederherstellungsendpunkt | Sicherungs- und Wiederherstellungsvorgänge für die Funktion „Backup to S3“ |
| Cluster | Der gesamte Verkehr | Der gesamte Verkehr | Alle LIFs auf einem Knoten | Alle LIFs auf dem anderen Knoten | Intercluster-Kommunikation (nur Cloud Volumes ONTAP HA) |
| | TCP | 3000 | Knotenverwaltung LIF | HA-Mediator | ZAPI-Aufrufe (nur Cloud Volumes ONTAP HA) |
| | ICMP | 1 | Knotenverwaltung LIF | HA-Mediator | Keep-Alive (nur Cloud Volumes ONTAP HA) |
| Konfigurationssicherungen | HTTP | 80 | Knotenverwaltung LIF | http://<IP-Adresse des Konsolenagenten>/occm/offboxconfig | Senden Sie Konfigurationssicherungen an den Konsolenagenten."ONTAP-Dokumentation" |
| DHCP | UDP | 68 | Knotenverwaltung LIF | DHCP | DHCP-Client für die Ersteinrichtung |
| DHCPS | UDP | 67 | Knotenverwaltung LIF | DHCP | DHCP-Server |
| DNS | UDP | 53 | Knotenverwaltungs-LIF und Daten-LIF (NFS, CIFS) | DNS | DNS |
| NDMP | TCP | 18600–18699 | Knotenverwaltung LIF | Zielserver | NDMP-Kopie |
| SMTP | TCP | 25 | Knotenverwaltung LIF | Mailserver | SMTP-Benachrichtigungen, können für AutoSupport verwendet werden |

| Service | Protokoll | Hafen | Quelle | Ziel | Zweck |
|---|---|---|---|---|---|
| SNMP | TCP | 161 | Knotenverwaltung LIF | Monitorserver | Überwachung durch SNMP-Traps |
| | UDP | 161 | Knotenverwaltung LIF | Monitorserver | Überwachung durch SNMP-Traps |
| | TCP | 162 | Knotenverwaltung LIF | Monitorserver | Überwachung durch SNMP-Traps |
| | UDP | 162 | Knotenverwaltung LIF | Monitorserver | Überwachung durch SNMP-Traps |
| SnapMirror | TCP | 11104 | Intercluster LIF | ONTAP Intercluster-LIFs | Verwaltung von Intercluster-Kommunikationssitzungen für SnapMirror |
| | TCP | 11105 | Intercluster LIF | ONTAP Intercluster-LIFs | SnapMirror -Datenübertragung |
| Syslog | UDP | 514 | Knotenverwaltung LIF | Syslog-Server | Syslog-Weiterleitungsnachrichten |

## Regeln für die externe Sicherheitsgruppe des HA-Mediators

Die vordefinierte externe Sicherheitsgruppe für den Cloud Volumes ONTAP HA-Mediator umfasst die folgenden eingehenden und ausgehenden Regeln.

### Eingehende Regeln

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

| Protokoll | Hafen | Quelle | Zweck |
|---|---|---|---|
| TCP | 3000 | CIDR des Konsolenagenten | RESTful-API-Zugriff vom Konsolenagenten |

### Ausgangsregeln

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

#### Grundlegende Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für den HA-Mediator umfasst die folgenden ausgehenden Regeln.

| Protokoll | Hafen | Zweck |
|---|---|---|
| Alle TCP | Alle | Der gesamte ausgehende Verkehr |
| Alle UDP | Alle | Der gesamte ausgehende Verkehr |

#### Erweiterte Ausgangsregeln

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

| Protokoll | Hafen | Ziel | Zweck |
|---|---|---|---|
| HTTP | 80 | IP-Adresse des Konsolenagenten auf der AWS EC2-Instanz | Upgrades für den Mediator herunterladen |
| HTTPS | 443 | ec2.amazonaws.com | Unterstützung beim Speicherfailover |
| UDP | 53 | ec2.amazonaws.com | Unterstützung beim Speicherfailover |

Anstatt die Ports 443 und 53 zu öffnen, können Sie einen Schnittstellen-VPC-Endpunkt vom Zielsubnetz zum AWS EC2-Dienst 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-Knoten und zwischen dem Mediator und den Knoten.

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

#### Eingehende Regeln

Die vordefinierte Sicherheitsgruppe umfasst die folgenden eingehenden Regeln.

| Protokoll | Hafen | Zweck |
|---|---|---|
| Der gesamte Verkehr | Alle | Kommunikation zwischen dem HA-Mediator und den HA-Knoten |

#### Ausgangsregeln

Die vordefinierte Sicherheitsgruppe umfasst die folgenden ausgehenden Regeln.

| Protokoll | Hafen | Zweck |
|---|---|---|
| Der gesamte Verkehr | Alle | Kommunikation zwischen dem HA-Mediator und den HA-Knoten |

## Regeln für den Konsolenagenten

"Sicherheitsgruppenregeln für den Konsolenagenten anzeigen"

**Copyright-Informationen**

Copyright © 2026 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 IRGENDEINER 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.