



# Netzwerkanforderungen

## Cloud Manager 3.6

NetApp  
March 25, 2024

This PDF was generated from [https://docs.netapp.com/de-de/occm36/reference\\_networking\\_cloud\\_manager.html](https://docs.netapp.com/de-de/occm36/reference_networking_cloud_manager.html) on March 25, 2024. Always check docs.netapp.com for the latest.

# Inhalt

- Netzwerkanforderungen ..... 1
  - Netzwerkanforderungen für Cloud Manager ..... 1
  - Netzwerkanforderungen für Cloud Volumes ONTAP in AWS ..... 4
  - Einrichten eines AWS-Transit-Gateways für HA-Paare in mehreren Verfügbarkeitszonen ..... 11
  - Netzwerkanforderungen für Cloud Volumes ONTAP in Azure ..... 15

# Netzwerkanforderungen

## Netzwerkanforderungen für Cloud Manager

Sie müssen Ihr Netzwerk so einrichten, dass Cloud Manager Cloud Volumes ONTAP Systeme in AWS oder in Microsoft Azure bereitstellen kann. Der wichtigste Schritt besteht darin, ausgehenden Internetzugriff auf verschiedene Endpunkte zu gewährleisten.



Wenn Ihr Netzwerk einen Proxyserver für die gesamte Kommunikation mit dem Internet verwendet, fordert Cloud Manager Sie auf, den Proxy während der Einrichtung anzugeben. Sie können den Proxyserver auch auf der Seite Einstellungen angeben. Siehe "[Konfigurieren von Cloud Manager für die Verwendung eines Proxyservers](#)".

### Verbindung zu Zielnetzwerken

Cloud Manager erfordert eine Netzwerkverbindung zu den AWS VPCs und Azure VNets, in denen Sie Cloud Volumes ONTAP bereitstellen möchten.

Wenn Sie beispielsweise Cloud Manager in Ihrem Unternehmensnetzwerk installieren, müssen Sie eine VPN-Verbindung zum AWS VPC oder Azure VNet einrichten, in dem Sie Cloud Volumes ONTAP starten.

### Outbound-Internetzugang

Cloud Manager erfordert ausgehenden Internetzugang, um Cloud Volumes ONTAP bereitzustellen und zu managen. Outbound-Internetzugang ist auch erforderlich, wenn Sie über Ihren Webbrowser auf Cloud Manager zugreifen und das Cloud Manager-Installationsprogramm auf einem Linux-Host ausführen.

In den folgenden Abschnitten werden die spezifischen Endpunkte beschrieben.

#### Outbound-Internetzugang zum Management von Cloud Volumes ONTAP in AWS

Cloud Manager erfordert ausgehenden Internetzugang, um bei der Implementierung und dem Management von Cloud Volumes ONTAP in AWS die folgenden Endpunkte zu kontaktieren:

Endpunkte	Zweck
<p>AWS-Services (amazonaws.com):</p> <ul style="list-style-type: none"><li>• CloudFormation</li><li>• Elastic Compute Cloud (EC2)</li><li>• Key Management Service (KMS)</li><li>• Security Token Service (STS)</li><li>• Simple Storage Service (S3)</li></ul> <p>Der genaue Endpunkt hängt von der Region ab, in der Sie Cloud Volumes ONTAP implementieren. "<a href="#">Weitere Informationen finden Sie in der AWS-Dokumentation.</a>"</p>	<p>Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in AWS.</p>
<p><a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a></p>	<p>API-Anfragen an NetApp Cloud Central.</p>

Endpunkte	Zweck
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a>	Cloud Manager kann Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images abrufen und herunterladen.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Kommunikation mit dem Cloud Manager-Service, der Cloud Central-Konten einschließt
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
<a href="https://support.netapp.com/aods/asupmessage">https://support.netapp.com/aods/asupmessage</a> <a href="https://support.netapp.com/asupprod/post/1.0/postAsup">https://support.netapp.com/asupprod/post/1.0/postAsup</a>	Kommunikation mit NetApp AutoSupport.
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a>	Kommunikation mit NetApp zur Lizenzierung und Support-Registrierung
<a href="https://packages.cloud.google.com/yum">https://packages.cloud.google.com/yum</a> <a href="https://github.com/NetApp/trident/releases/download/">https://github.com/NetApp/trident/releases/download/</a>	Erforderlich, um Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster zu verbinden. Mit den Endpunkten ist die Installation von NetApp Trident möglich.
Verschiedene Standorte von Drittanbietern, z. B.: <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.org">https://repo.typesafe.org</a></li> </ul> <p>An Standorten von Drittanbietern können Änderungen vorgenommen werden.</p>	Während Upgrades lädt Cloud Manager die neuesten Pakete für Abhängigkeiten von Drittanbietern herunter.

### Outbound-Internetzugang zum Management von Cloud Volumes ONTAP in Azure

Cloud Manager erfordert ausgehenden Internetzugang, um bei der Bereitstellung und Verwaltung von Cloud Volumes ONTAP in Microsoft Azure folgende Endpunkte zu kontaktieren:

Endpunkte	Zweck
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den meisten Azure Regionen.
<a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a> <a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a>	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den Azure Germany Regionen.

Endpunkte	Zweck
<a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	Ermöglicht Cloud Manager die Implementierung und das Management von Cloud Volumes ONTAP in den Azure US Gov Regionen.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	API-Anfragen an NetApp Cloud Central.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Bietet Zugriff auf Software-Images, Manifeste und Vorlagen.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a>	Cloud Manager kann Manifeste, Vorlagen und Cloud Volumes ONTAP Upgrade-Images abrufen und herunterladen.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Ermöglicht NetApp das Streamen von Daten aus Audit-Datensätzen.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Kommunikation mit NetApp Cloud Central für zentralisierte Benutzerauthentifizierung
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Kommunikation mit NetApp AutoSupport.
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a>	Kommunikation mit NetApp zur Lizenzierung und Support-Registrierung
<a href="https://packages.cloud.google.com/yum">https://packages.cloud.google.com/yum</a> <a href="https://github.com/NetApp/trident/releases/download/">https://github.com/NetApp/trident/releases/download/</a>	Erforderlich, um Cloud Volumes ONTAP Systeme mit einem Kubernetes Cluster zu verbinden. Mit den Endpunkten ist die Installation von NetApp Trident möglich.
<p>Verschiedene Standorte von Drittanbietern, z. B.:</p> <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.org">https://repo.typesafe.org</a></li> </ul> <p>An Standorten von Drittanbietern können Änderungen vorgenommen werden.</p>	Während Upgrades lädt Cloud Manager die neuesten Pakete für Abhängigkeiten von Drittanbietern herunter.

### Outbound-Internetzugang über Ihren Webbrowser

Benutzer müssen über einen Webbrowser auf Cloud Manager zugreifen. Die Maschine, auf der der Webbrowser ausgeführt wird, muss über Verbindungen zu den folgenden Endpunkten verfügen:

Endpunkte	Zweck
Der Cloud Manager-Host	<p>Sie müssen die IP-Adresse des Hosts aus einem Webbrowser eingeben, um die Cloud Manager-Konsole zu laden.</p> <p>Je nach Ihrer Verbindung mit Ihrem Cloud-Provider können Sie die private IP oder eine dem Host zugewiesene öffentliche IP verwenden:</p> <ul style="list-style-type: none"> <li>• Eine private IP funktioniert, wenn Sie über ein VPN verfügen und direkten Zugriff auf Ihr virtuelles Netzwerk haben</li> <li>• Eine öffentliche IP funktioniert in jedem Netzwerkszenario</li> </ul> <p>In jedem Fall sollten Sie den Netzwerkzugriff sichern, indem Sie sicherstellen, dass die Sicherheitsgruppenregeln den Zugriff nur von autorisierten IPs oder Subnetzen ermöglichen.</p>
<a href="https://auth0.com">https://auth0.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a>	Ihr Webbrowser stellt über NetApp Cloud Central eine Verbindung zu diesen Endpunkten her, um eine zentralisierte Benutzerauthentifizierung zu ermöglichen.
<a href="https://widget.intercom.io">https://widget.intercom.io</a>	Für Ihren Produkt-Chat, der Ihnen das Gespräch mit NetApp Cloud-Experten ermöglicht.

### Outbound-Internetzugang zur Installation von Cloud Manager auf einem Linux-Host

Das Cloud Manager-Installationsprogramm muss während des Installationsvorgangs auf die folgenden URLs zugreifen:

- <http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm>
- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>

### Ports und Sicherheitsgruppen

- Wenn Sie Cloud Manager über Cloud Central oder über Marktplatz-Images bereitstellen, lesen Sie Folgendes:
  - ["Sicherheitsgruppenregeln für Cloud Manager in AWS"](#)
  - ["Sicherheitsgruppenregeln für Cloud Manager in Azure"](#)
- Wenn Sie Cloud Manager auf einem vorhandenen Linux-Host installieren, lesen Sie ["Anforderungen an den Cloud Manager Host"](#).

## Netzwerkanforderungen für Cloud Volumes ONTAP in AWS

Richten Sie das AWS Netzwerk ein, um Cloud Volumes ONTAP Systeme ordnungsgemäß funktionieren zu können.

Suchen Sie nach der Liste der Endpunkte, auf die Cloud Manager Zugriff benötigt? Sie werden jetzt an einem einzigen Ort gepflegt. ["Details finden Sie hier"](#).

## Allgemeine AWS Netzwerkanforderungen für Cloud Volumes ONTAP

Die folgenden Anforderungen müssen in AWS erfüllt sein.

### Outbound-Internetzugang für Cloud Volumes ONTAP Nodes

Cloud Volumes ONTAP Nodes erfordern ausgehenden Internetzugang, um Nachrichten an NetApp AutoSupport zu senden, der proaktiv den Zustand Ihres Storage überwacht.

Routing- und Firewall-Richtlinien müssen AWS 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.

### 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 \(AWS PrivateLink\)"](#).

### Sicherheitsgruppen

Sie müssen keine Sicherheitsgruppen erstellen, da Cloud Manager dies für Sie tut. Wenn Sie Ihr eigenes verwenden müssen, lesen Sie ["Regeln für Sicherheitsgruppen"](#).

### Verbindung von Cloud Volumes ONTAP zu AWS S3 für Data 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 in anderen Netzwerken

Um Daten zwischen einem Cloud Volumes ONTAP System in AWS und ONTAP Systemen in anderen Netzwerken zu replizieren, müssen Sie eine VPN-Verbindung zwischen AWS VPC und dem anderen Netzwerk haben, z. B. ein Azure VNet oder Ihr 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"](#).

## AWS Netzwerkanforderungen für Cloud Volumes ONTAP HA in mehreren AZS

Zusätzliche AWS Netzwerkanforderungen gelten für Cloud Volumes ONTAP HA-Konfigurationen, die mehrere Verfügbarkeitszonen (AZS) verwenden. Sie sollten diese Anforderungen prüfen, bevor Sie ein HA-Paar starten, da Sie die Netzwerkdetails in Cloud Manager 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.

### 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. Wenn Sie die IP-Adresse nicht angeben, wenn Sie das System implementieren, können Sie später die LIF erstellen. Weitere Informationen finden Sie unter ["Einrichten von Cloud Volumes ONTAP"](#).

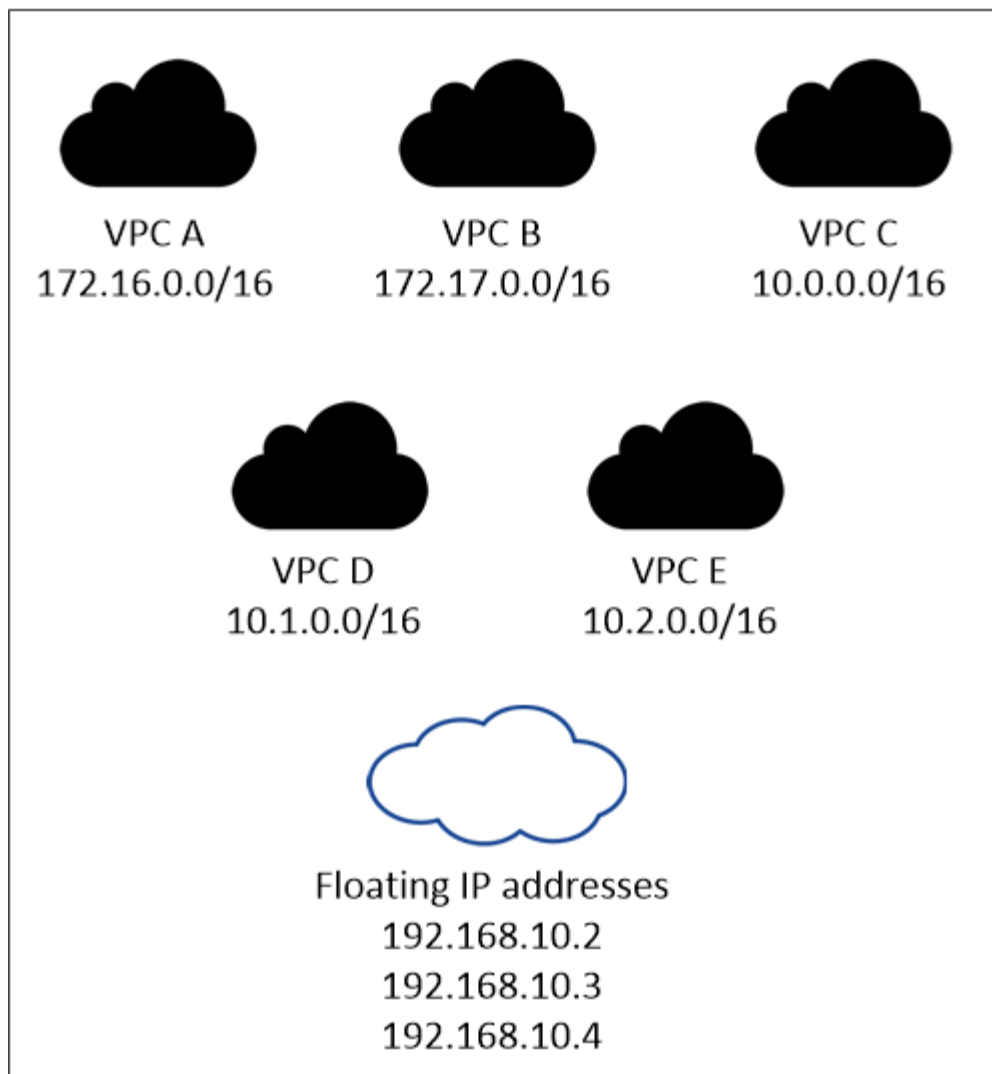
Sie müssen die unverankerten IP-Adressen in Cloud Manager eingeben, wenn Sie eine Cloud Volumes ONTAP HA-Arbeitsumgebung erstellen. Cloud Manager weist dem HA-Paar die IP-Adressen zu, wenn es das System startet.

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



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

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

["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 Cloud Manager die unverankerten IP-Adressen angegeben haben, müssen Sie die Routing-Tabellen auswählen, die Routen zu den Floating IP-Adressen enthalten sollen. Dies ermöglicht den Client-Zugriff auf das HA-Paar.

Wenn Sie nur eine Routing-Tabelle für die Subnetze in Ihrem VPC (der Hauptroutingtabelle) haben, fügt Cloud Manager dieser Routing-Tabelle automatisch die unverankerten IP-Adressen 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"](#).

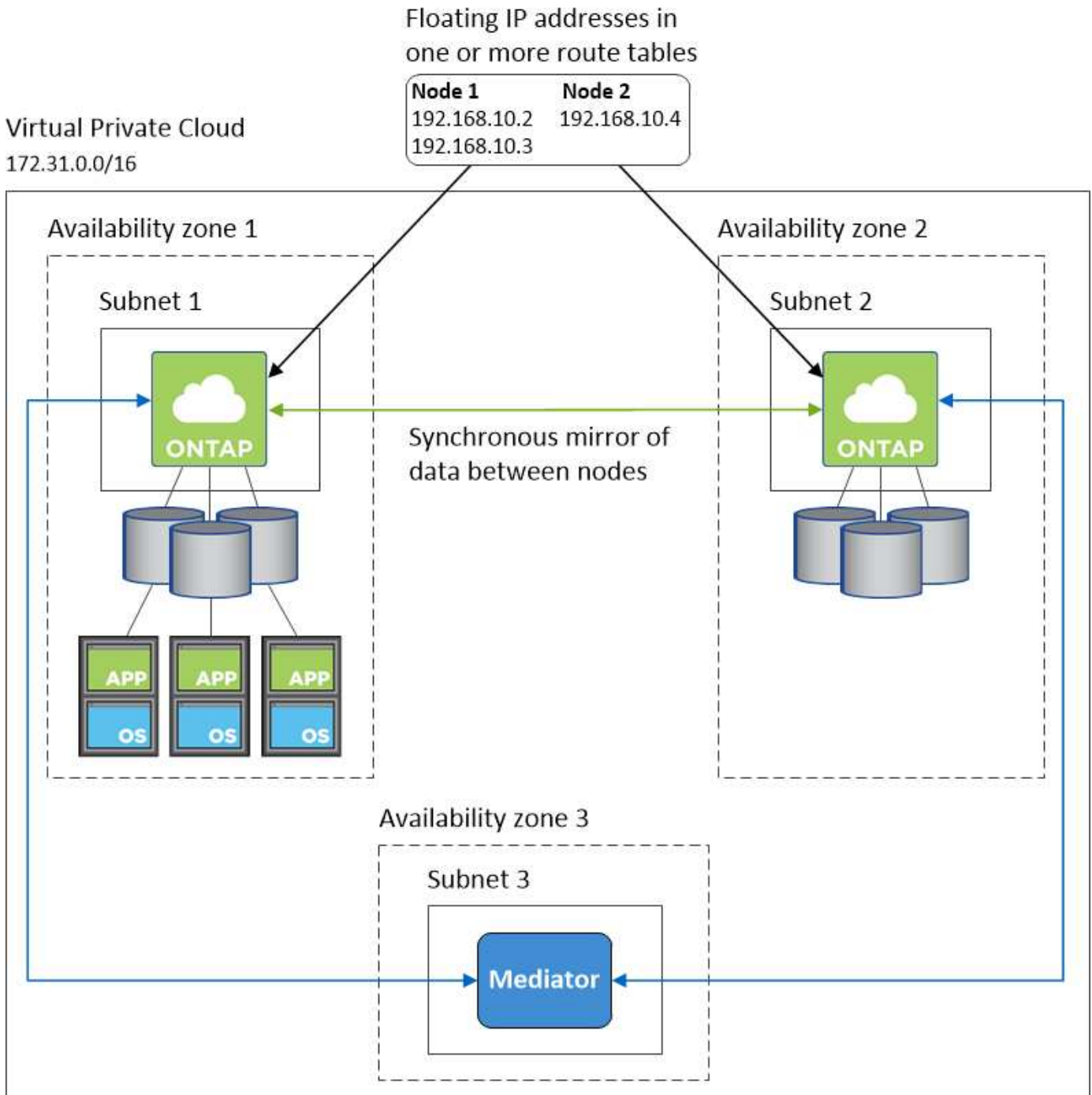
### **Anbindung an NetApp Management Tools**

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.

### **Beispielkonfiguration**

Die folgende Abbildung zeigt eine optimale HA-Konfiguration in AWS, die als Aktiv/Passiv-Konfiguration betrieben wird:



## Beispiele für VPC-Konfigurationen

Um besser zu verstehen, wie Sie Cloud Manager und Cloud Volumes ONTAP in AWS implementieren können, sollten Sie sich die gängigsten VPC-Konfigurationen ansehen.

- Ein VPC mit öffentlichen und privaten Subnetzen und einem NAT-Gerät
- Ein VPC mit einem privaten Subnetz und einer VPN-Verbindung zu Ihrem Netzwerk

### Ein VPC mit öffentlichen und privaten Subnetzen und einem NAT-Gerät

Diese VPC-Konfiguration umfasst öffentliche und private Subnetze, ein Internet-Gateway, das den VPC mit dem Internet verbindet, und ein NAT-Gateway oder eine NAT-Instanz im öffentlichen Subnetz, die

ausgehenden Internetverkehr vom privaten Subnetz aus ermöglicht. In dieser Konfiguration können Sie Cloud Manager in einem öffentlichen oder privaten Subnetz ausführen. Das öffentliche Subnetz wird jedoch empfohlen, da es den Zugriff von Hosts außerhalb des VPC ermöglicht. Sie können dann Cloud Volumes ONTAP Instanzen im privaten Subnetz starten.

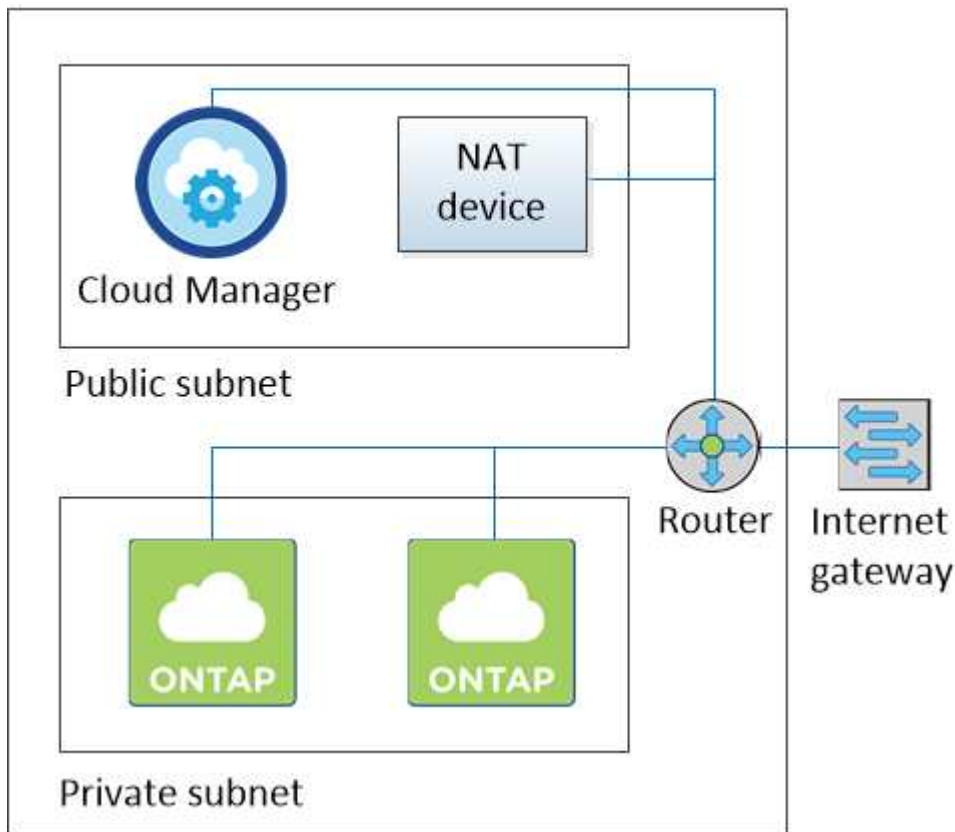


Anstelle eines NAT-Geräts können Sie einen HTTP-Proxy verwenden, um Internetverbindungen bereitzustellen.

Weitere Informationen zu diesem Szenario finden Sie unter "[AWS Dokumentation: Szenario 2: VPC mit öffentlichen und privaten Subnetzen \(NAT\)](#)".

Die folgende Grafik zeigt Cloud Manager, der in einem öffentlichen Subnetz und in Einzelknoten-Systemen in einem privaten Subnetz ausgeführt wird:

## Virtual Private Cloud



### Ein VPC mit einem privaten Subnetz und einer VPN-Verbindung zu Ihrem Netzwerk

Bei dieser VPC-Konfiguration handelt es sich um eine Hybrid Cloud-Konfiguration, bei der Cloud Volumes ONTAP zu einer Erweiterung Ihrer privaten Umgebung wird. Die Konfiguration umfasst ein privates Subnetz und ein virtuelles privates Gateway mit einer VPN-Verbindung zu Ihrem Netzwerk. Durch das Routing über den VPN-Tunnel können EC2-Instanzen über das Netzwerk und Firewalls auf das Internet zugreifen. Sie können Cloud Manager im privaten Subnetz oder in Ihrem Datacenter ausführen. Sie starten dann Cloud Volumes ONTAP im privaten Subnetz.

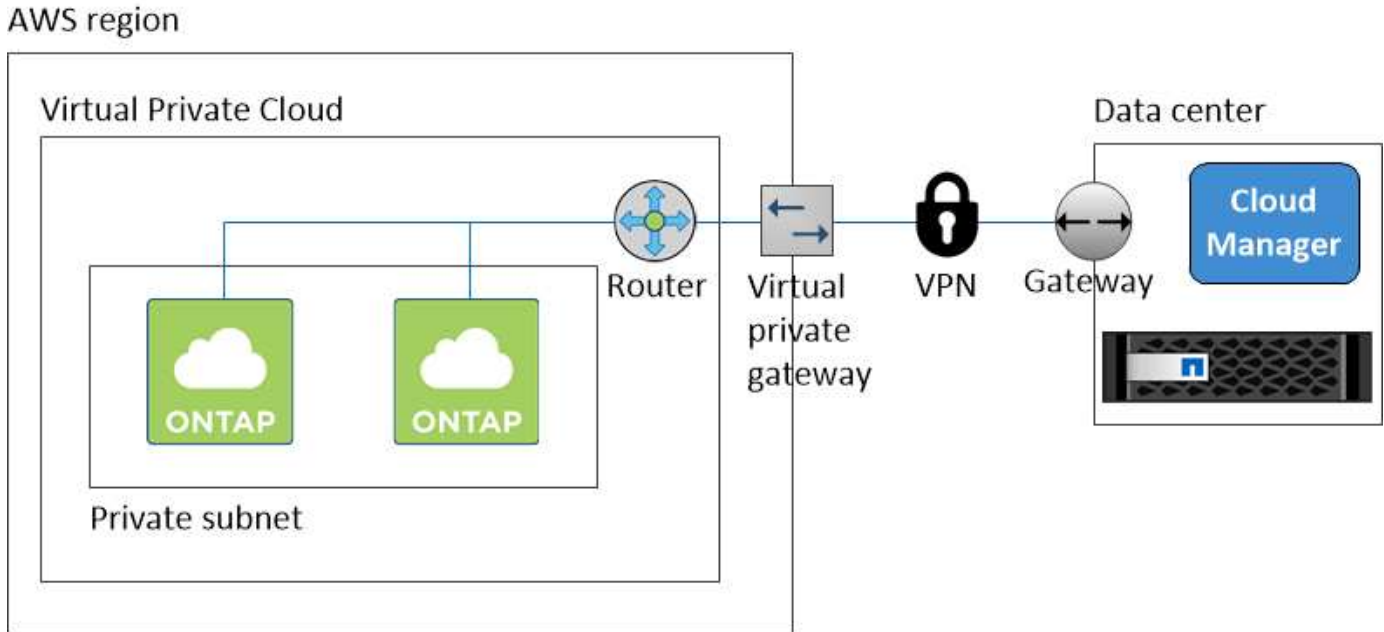


Sie können in dieser Konfiguration auch einen Proxyserver verwenden, um den Internetzugang zu ermöglichen. Der Proxy-Server kann sich in Ihrem Datacenter oder in AWS befinden.

Wenn Sie Daten zwischen FAS Systemen in Ihrem Datacenter und Cloud Volumes ONTAP Systemen in AWS replizieren möchten, sollten Sie eine VPN-Verbindung verwenden, damit die Verbindung sicher ist.

Weitere Informationen zu diesem Szenario finden Sie unter ["AWS Dokumentation: Szenario 4: VPC mit privatem Subnetz und von AWS gemanagtem VPN-Zugriff"](#).

Die folgende Grafik zeigt Cloud Manager, der in Ihrem Datacenter und in Einzelknotensystemen in einem privaten Subnetz ausgeführt wird:



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

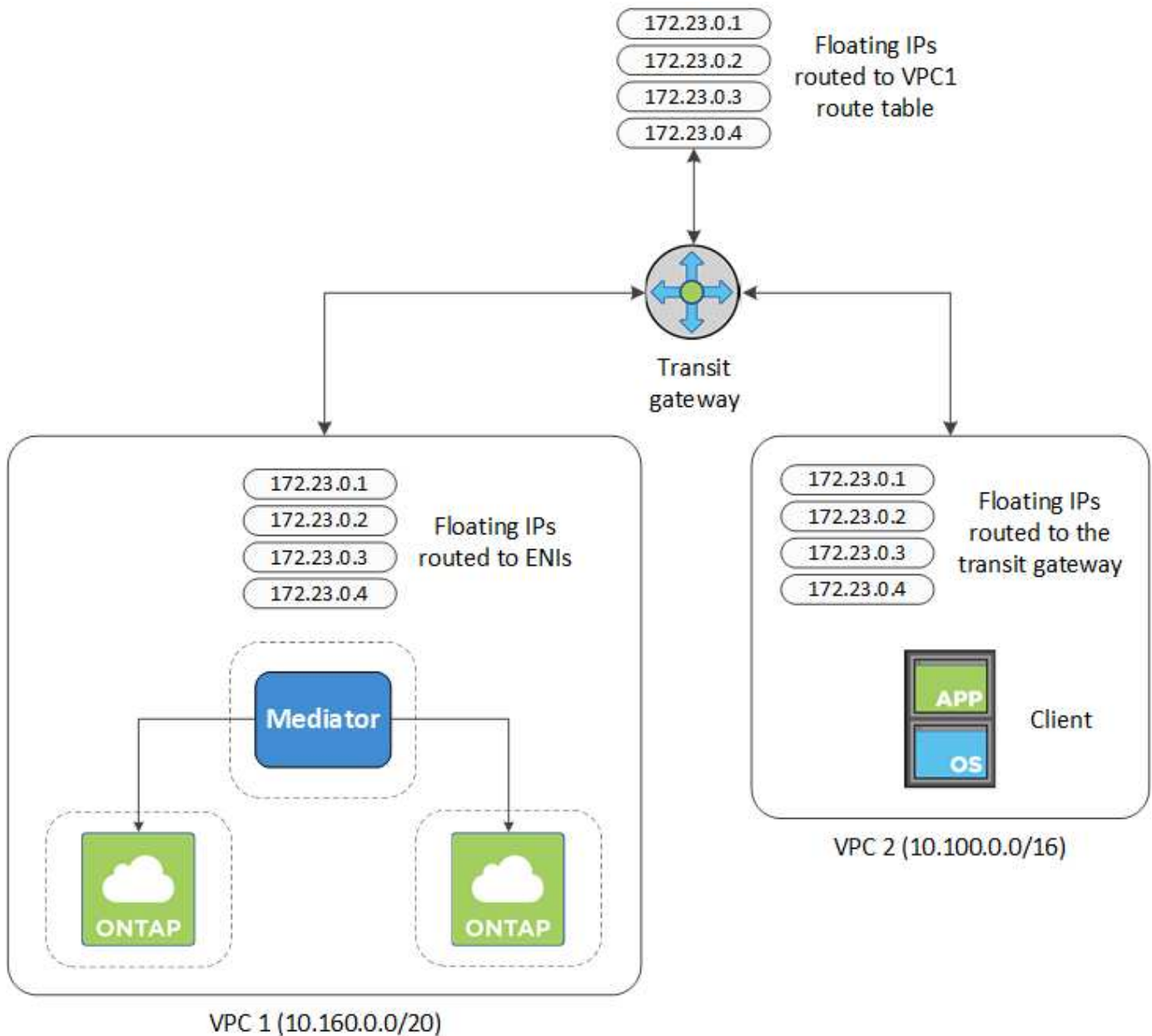
Einrichten eines AWS-Transit-Gateways für den Zugriff auf die unverankerten IP-Adressen eines HA-Paars von außerhalb der VPC aus, wo sich das HA-Paar befindet.

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-Volumen 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. 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 Cloud Manager. 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

<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	VPC	static	active
<input type="checkbox"/>	172.23.0.3/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.4/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active

3. 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

4. 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. Cloud Manager hat bei der Implementierung des HA-Paars automatisch die Floating IPs zur Routing-Tabelle 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

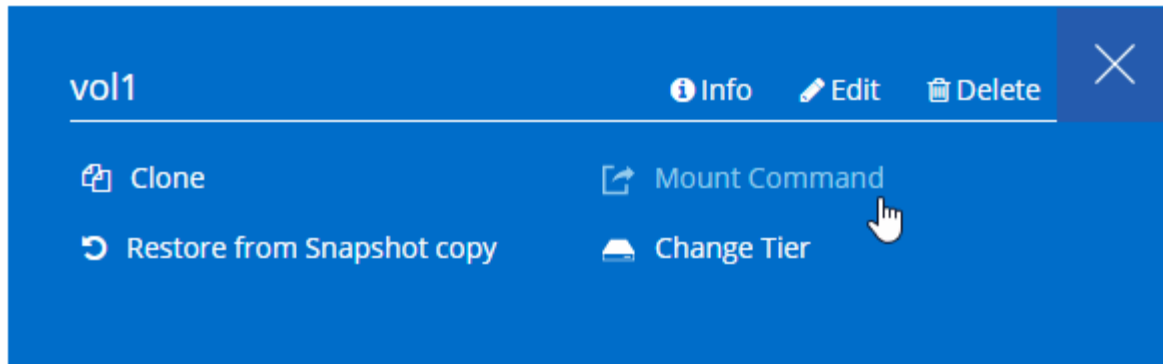
5. Volumes werden mithilfe der Floating IP-Adresse an Clients gemountet.

Die richtige IP-Adresse finden Sie in Cloud Manager, indem Sie ein Volume auswählen und auf **Mount Command** klicken.



# Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



## Verwandte Links

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

## Netzwerkanforderungen für Cloud Volumes ONTAP in Azure

Sie müssen Ihr Azure Networking so einrichten, dass Cloud Volumes ONTAP Systeme ordnungsgemäß funktionieren.

Suchen Sie nach der Liste der Endpunkte, auf die Cloud Manager Zugriff benötigt? Sie werden jetzt an einem einzigen Ort gepflegt. ["Details finden Sie hier"](#).

### Outbound-Internetzugang für Cloud Volumes ONTAP

Cloud Volumes ONTAP erfordert ausgehenden Internetzugang, um Nachrichten an NetApp AutoSupport zu senden, der proaktiv den Zustand Ihres Storage überwacht.

Routing- und Firewall-Richtlinien müssen AWS 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>

### Sicherheitsgruppen

Sie müssen keine Sicherheitsgruppen erstellen, da Cloud Manager dies für Sie tut. Wenn Sie Ihr eigenes verwenden müssen, lesen Sie ["Regeln für Sicherheitsgruppen"](#).

### Verbindung von Cloud Volumes ONTAP zu Azure Blob Storage für Data Tiering

Wenn Sie „kalte“ Daten für Azure Blob Storage Tiering möchten, müssen Sie keinen vnet Service-Endpunkt einrichten, wenn Cloud Manager über die erforderlichen Berechtigungen verfügt:

```
"Microsoft.Network/virtualNetworks/subnets/write",  
"Microsoft.Network/routeTables/join/action",
```

Diese Berechtigungen sind in der neuesten enthalten ["Cloud Manager-Richtlinie"](#).

Weitere Informationen zum Einrichten von Daten-Tiering finden Sie unter ["Tiering von kalten Daten auf kostengünstigen Objekt-Storage"](#).

### **Verbindungen zu ONTAP Systemen in anderen Netzwerken**

Um Daten zwischen einem Cloud Volumes ONTAP System in Azure und ONTAP Systemen in anderen Netzwerken zu replizieren, müssen Sie über eine VPN-Verbindung zwischen Azure VNet und dem anderen Netzwerk verfügen, z. B. einem AWS VPC oder Ihrem Unternehmensnetzwerk.

Anweisungen finden Sie unter ["Microsoft Azure Dokumentation: Erstellen Sie eine Site-to-Site-Verbindung im Azure-Portal"](#).

## 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.