



Requisiti di rete

Cloud Manager 3.7

NetApp
March 25, 2024

Sommario

- Requisiti di rete 1
 - Requisiti di rete per Cloud Manager 1
 - Requisiti di rete per Cloud Volumes ONTAP in AWS 5
 - Configurazione di un gateway di transito AWS per coppie ha in più AZS 12
 - Requisiti di rete per Cloud Volumes ONTAP in Azure 16
 - Requisiti di rete per Cloud Volumes ONTAP in GCP 17

Requisiti di rete

Requisiti di rete per Cloud Manager

Configura la tua rete in modo che Cloud Manager possa implementare i sistemi Cloud Volumes ONTAP in AWS, Microsoft Azure o Google Cloud Platform. Il passaggio più importante è garantire l'accesso a Internet in uscita a vari endpoint.



Se la rete utilizza un server proxy per tutte le comunicazioni a Internet, Cloud Manager richiede di specificare il proxy durante la configurazione. È inoltre possibile specificare il server proxy dalla pagina Impostazioni. Fare riferimento a ["Configurazione di Cloud Manager per l'utilizzo di un server proxy"](#).

Connessione alle reti di destinazione

Cloud Manager richiede una connessione di rete ai VPC e ai VNet in cui si desidera implementare Cloud Volumes ONTAP.

Ad esempio, se si installa Cloud Manager nella rete aziendale, è necessario impostare una connessione VPN al VPC o a VNET in cui si avvia Cloud Volumes ONTAP.

Accesso a Internet in uscita

Cloud Manager richiede l'accesso a Internet in uscita per implementare e gestire Cloud Volumes ONTAP. L'accesso a Internet in uscita è necessario anche quando si accede a Cloud Manager dal browser Web e si esegue il programma di installazione di Cloud Manager su un host Linux.

Le sezioni seguenti identificano gli endpoint specifici.

Endpoint per gestire Cloud Volumes ONTAP in AWS

Cloud Manager richiede l'accesso a Internet in uscita per contattare i seguenti endpoint durante l'implementazione e la gestione di Cloud Volumes ONTAP in AWS:

Endpoint	Scopo
<p>Servizi AWS (amazonaws.com):</p> <ul style="list-style-type: none">• CloudFormation• Elastic Compute Cloud (EC2)• Servizio di gestione delle chiavi (KMS)• Servizio token di sicurezza (STS)• S3 (Simple Storage Service) <p>L'endpoint esatto dipende dalla regione in cui viene implementato Cloud Volumes ONTAP. "Per ulteriori informazioni, fare riferimento alla documentazione AWS."</p>	<p>Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP in AWS.</p>

Endpoint	Scopo
https://api.services.cloud.netapp.com:443	Richieste API a NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Fornisce l'accesso a immagini, manifesti e modelli software.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Consente a Cloud Manager di accedere e scaricare manifesti, modelli e immagini di aggiornamento di Cloud Volumes ONTAP.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://cloudmanager.cloud.netapp.com	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Consente di aggiungere l'ID account AWS all'elenco degli utenti autorizzati per Backup in S3.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Comunicazione con NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.
https://ipa-signer.cloudmanager.netapp.com	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.
<p>Varie sedi di terze parti, ad esempio:</p> <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org <p>Le sedi di terze parti sono soggette a modifiche.</p>	Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti.

Endpoint per gestire Cloud Volumes ONTAP in Azure

Cloud Manager richiede l'accesso a Internet in uscita per contattare i seguenti endpoint durante l'implementazione e la gestione di Cloud Volumes ONTAP in Microsoft Azure:

Endpoint	Scopo
https://management.azure.com https://login.microsoftonline.com	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nella maggior parte delle regioni Azure.

Endpoint	Scopo
https://management.microsoftazure.de https://login.microsoftonline.de	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nelle regioni di Azure Germania.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Consente a Cloud Manager di implementare e gestire Cloud Volumes ONTAP nelle regioni di Azure US Gov.
https://api.services.cloud.netapp.com:443	Richieste API a NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Fornisce l'accesso a immagini, manifesti e modelli software.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com	Consente a Cloud Manager di accedere e scaricare manifesti, modelli e immagini di aggiornamento di Cloud Volumes ONTAP.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://cloudmanager.cloud.netapp.com	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
https://mysupport.netapp.com	Comunicazione con NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.
https://ipa-signer.cloudmanager.netapp.com	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.
<p>Varie sedi di terze parti, ad esempio:</p> <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org <p>Le sedi di terze parti sono soggette a modifiche.</p>	Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti.

Endpoint per gestire Cloud Volumes ONTAP in GCP

Cloud Manager richiede l'accesso a Internet in uscita per contattare i seguenti endpoint durante l'implementazione e la gestione di Cloud Volumes ONTAP in GCP:

Endpoint	Scopo
https://www.googleapis.com	Consente a Cloud Manager di contattare le API Google per l'implementazione e la gestione di Cloud Volumes ONTAP in GCP.
https://api.services.cloud.netapp.com:443	Richieste API a NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Fornisce l'accesso a immagini, manifesti e modelli software.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com	Consente a Cloud Manager di accedere e scaricare manifesti, modelli e immagini di aggiornamento di Cloud Volumes ONTAP.
https://kinesis.us-east-1.amazonaws.com	Consente a NetApp di eseguire lo streaming dei dati dai record di audit.
https://cloudmanager.cloud.netapp.com	Comunicazione con il servizio Cloud Manager, che include gli account Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicazione con NetApp Cloud Central per l'autenticazione utente centralizzata.
https://mysupport.netapp.com	Comunicazione con NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Comunicazione con NetApp per la registrazione del supporto e delle licenze di sistema.
https://ipa-signer.cloudmanager.netapp.com	Consente a Cloud Manager di generare licenze (ad esempio, una licenza FlexCache per Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necessario per connettere i sistemi Cloud Volumes ONTAP a un cluster Kubernetes. Gli endpoint consentono l'installazione di NetApp Trident.
<p>Varie sedi di terze parti, ad esempio:</p> <ul style="list-style-type: none"> • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org <p>Le sedi di terze parti sono soggette a modifiche.</p>	Durante gli aggiornamenti, Cloud Manager scarica i pacchetti più recenti per le dipendenze di terze parti.

Endpoint a cui si accede dal browser Web

Gli utenti devono accedere a Cloud Manager da un browser Web. Il computer che esegue il browser Web deve disporre di connessioni ai seguenti endpoint:

Endpoint	Scopo
L'host Cloud Manager	<p>Per caricare la console di Cloud Manager, è necessario inserire l'indirizzo IP dell'host da un browser Web.</p> <p>A seconda della connettività con il cloud provider, è possibile utilizzare l'IP privato o un IP pubblico assegnato all'host:</p> <ul style="list-style-type: none"> • Un IP privato funziona se si dispone di una VPN e di un accesso diretto alla rete virtuale • Un IP pubblico funziona in qualsiasi scenario di rete <p>In ogni caso, è necessario proteggere l'accesso alla rete assicurandosi che le regole del gruppo di protezione consentano l'accesso solo da IP o subnet autorizzati.</p>
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Il browser Web si connette a questi endpoint per un'autenticazione utente centralizzata tramite NetApp Cloud Central.
https://widget.intercom.io	Per chat in-product che ti consente di parlare con gli esperti cloud di NetApp.

Endpoint per installare Cloud Manager su un host Linux

Il programma di installazione di Cloud Manager deve accedere ai seguenti URL durante il processo di installazione:

- <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>

Porte e gruppi di sicurezza

- Se si implementa Cloud Manager da Cloud Central o dalle immagini del marketplace, fare riferimento a quanto segue:
 - ["Regole del gruppo di sicurezza per Cloud Manager in AWS"](#)
 - ["Regole del gruppo di sicurezza per Cloud Manager in Azure"](#)
 - ["Regole firewall per Cloud Manager in GCP"](#)
- Se si installa Cloud Manager su un host Linux esistente, vedere ["Requisiti degli host di Cloud Manager"](#).

Requisiti di rete per Cloud Volumes ONTAP in AWS

Configurare la rete AWS in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente.

Requisiti generali di rete AWS per Cloud Volumes ONTAP

I seguenti requisiti devono essere soddisfatti in AWS.

Accesso a Internet in uscita per nodi Cloud Volumes ONTAP

I nodi Cloud Volumes ONTAP richiedono l'accesso a Internet in uscita per inviare messaggi a NetApp AutoSupport, che monitora in modo proattivo lo stato di salute dello storage.

I criteri di routing e firewall devono consentire il traffico HTTP/HTTPS di AWS ai seguenti endpoint in modo che Cloud Volumes ONTAP possa inviare messaggi AutoSupport:

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

Se si dispone di un'istanza NAT, è necessario definire una regola del gruppo di sicurezza in entrata che consenta il traffico HTTPS dalla subnet privata a Internet.

Accesso a Internet in uscita per il mediatore ha

L'istanza di ha mediator deve disporre di una connessione in uscita al servizio AWS EC2 in modo che possa fornire assistenza per il failover dello storage. Per fornire la connessione, è possibile aggiungere un indirizzo IP pubblico, specificare un server proxy o utilizzare un'opzione manuale.

L'opzione manuale può essere un gateway NAT o un endpoint VPC di interfaccia dalla subnet di destinazione al servizio AWS EC2. Per ulteriori informazioni sugli endpoint VPC, fare riferimento a "[Documentazione AWS: Endpoint VPC di interfaccia \(AWS PrivateLink\)](#)".

Numero di indirizzi IP

Cloud Manager assegna il seguente numero di indirizzi IP a Cloud Volumes ONTAP in AWS:

- Nodo singolo: 6 indirizzi IP
- Coppie HA in un singolo AZS: 15 indirizzi
- Coppie HA in più AZS: 15 o 16 indirizzi IP

Si noti che Cloud Manager crea una LIF di gestione SVM su sistemi a nodo singolo, ma non su coppie ha in un singolo AZ. È possibile scegliere se creare una LIF di gestione SVM su coppie ha in più AZS.



LIF è un indirizzo IP associato a una porta fisica. Per strumenti di gestione come SnapCenter è necessaria una LIF di gestione SVM.

Gruppi di sicurezza

Non è necessario creare gruppi di sicurezza perché Cloud Manager fa questo per te. Se è necessario utilizzare il proprio, fare riferimento a "[Regole del gruppo di sicurezza](#)".

Connessione da Cloud Volumes ONTAP ad AWS S3 per il tiering dei dati

Se si desidera utilizzare EBS come Tier di performance e AWS S3 come Tier di capacità, è necessario assicurarsi che Cloud Volumes ONTAP disponga di una connessione a S3. Il modo migliore per fornire tale connessione consiste nella creazione di un endpoint VPC per il servizio S3. Per istruzioni, vedere "[Documentazione AWS: Creazione di un endpoint gateway](#)".

Quando si crea l'endpoint VPC, assicurarsi di selezionare la regione, il VPC e la tabella di routing che corrispondono all'istanza di Cloud Volumes ONTAP. È inoltre necessario modificare il gruppo di protezione per aggiungere una regola HTTPS in uscita che abilita il traffico all'endpoint S3. In caso contrario, Cloud Volumes ONTAP non può connettersi al servizio S3.

In caso di problemi, vedere "[AWS Support Knowledge Center: Perché non è possibile connettersi a un](#)

[bucket S3 utilizzando un endpoint VPC gateway?](#)

Connessioni a sistemi ONTAP in altre reti

Per replicare i dati tra un sistema Cloud Volumes ONTAP in AWS e i sistemi ONTAP in altre reti, è necessario disporre di una connessione VPN tra AWS VPC e l'altra rete, ad esempio Azure VNET o la rete aziendale. Per istruzioni, vedere ["Documentazione AWS: Configurazione di una connessione VPN AWS"](#).

DNS e Active Directory per CIFS

Se si desidera eseguire il provisioning dello storage CIFS, è necessario configurare DNS e Active Directory in AWS o estendere la configurazione on-premise ad AWS.

Il server DNS deve fornire servizi di risoluzione dei nomi per l'ambiente Active Directory. È possibile configurare i set di opzioni DHCP in modo che utilizzino il server DNS EC2 predefinito, che non deve essere il server DNS utilizzato dall'ambiente Active Directory.

Per istruzioni, fare riferimento a ["Documentazione AWS: Active Directory Domain Services su AWS Cloud: Implementazione di riferimento rapido"](#).

Requisiti di rete AWS per Cloud Volumes ONTAP ha in più AZS

Ulteriori requisiti di rete AWS si applicano alle configurazioni Cloud Volumes ONTAP ha che utilizzano zone di disponibilità multiple (AZS). Prima di avviare una coppia ha, è necessario esaminare questi requisiti perché è necessario inserire i dettagli di rete in Cloud Manager.

Per informazioni sul funzionamento delle coppie ha, vedere ["Coppie ad alta disponibilità"](#).

Zone di disponibilità

Questo modello di implementazione ha utilizza più AZS per garantire un'elevata disponibilità dei dati. È necessario utilizzare un AZ dedicato per ogni istanza di Cloud Volumes ONTAP e per l'istanza del mediatore, che fornisce un canale di comunicazione tra la coppia ha.

Indirizzi IP mobili per dati NAS e gestione cluster/SVM

Le configurazioni HA in più AZS utilizzano indirizzi IP mobili che migrano tra nodi in caso di guasti. Non sono accessibili in modo nativo dall'esterno del VPC, a meno che non si ["Configurare un gateway di transito AWS"](#).

Un indirizzo IP mobile è per la gestione del cluster, uno per i dati NFS/CIFS sul nodo 1 e uno per i dati NFS/CIFS sul nodo 2. Un quarto indirizzo IP mobile per la gestione SVM è opzionale.



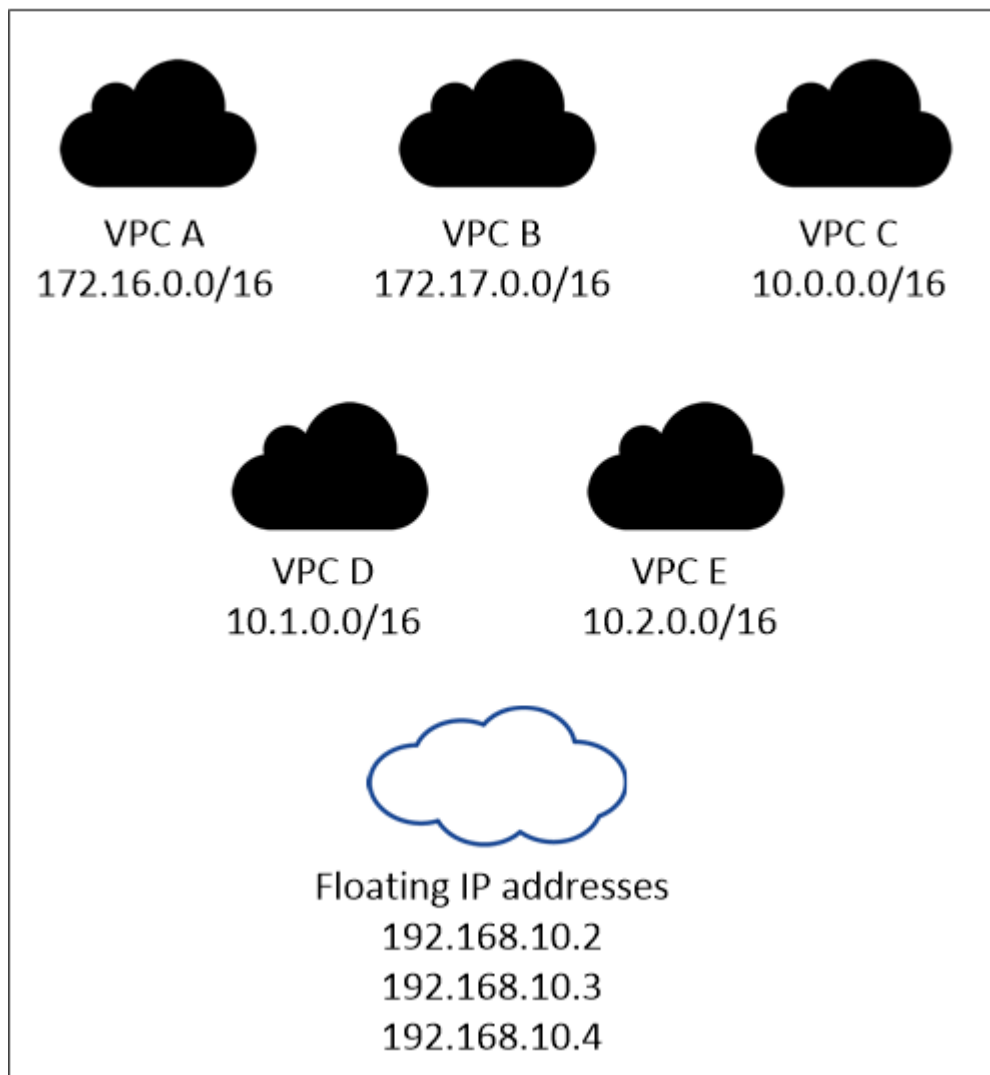
Se si utilizza SnapDrive per Windows o SnapCenter con la coppia ha, è necessario un indirizzo IP mobile per la LIF di gestione SVM. Se non si specifica l'indirizzo IP durante l'implementazione del sistema, è possibile creare la LIF in un secondo momento. Per ulteriori informazioni, vedere ["Configurazione di Cloud Volumes ONTAP"](#).

Quando si crea un ambiente di lavoro Cloud Volumes ONTAP ha, è necessario inserire gli indirizzi IP mobili in Cloud Manager. Cloud Manager assegna gli indirizzi IP alla coppia ha quando avvia il sistema.

Gli indirizzi IP mobili devono essere al di fuori dei blocchi CIDR per tutti i VPC nella regione AWS in cui si implementa la configurazione ha. Gli indirizzi IP mobili sono una subnet logica esterna ai VPC della propria regione.

Nell'esempio seguente viene illustrata la relazione tra gli indirizzi IP mobili e i VPC in una regione AWS. Mentre gli indirizzi IP mobili si trovano al di fuori dei blocchi CIDR per tutti i VPC, sono instradabili alle subnet attraverso le tabelle di routing.

AWS region



Cloud Manager crea automaticamente indirizzi IP statici per l'accesso iSCSI e NAS da client esterni al VPC. Non è necessario soddisfare alcun requisito per questi tipi di indirizzi IP.

Gateway di transito per abilitare l'accesso IP mobile dall'esterno del VPC

["Configurare un gateway di transito AWS"](#) Per consentire l'accesso agli indirizzi IP mobili di una coppia ha dall'esterno del VPC in cui risiede la coppia ha.

Tabelle di percorso

Dopo aver specificato gli indirizzi IP mobili in Cloud Manager, è necessario selezionare le tabelle di routing che devono includere i percorsi verso gli indirizzi IP mobili. In questo modo si abilita l'accesso del client alla coppia ha.

Se si dispone di una sola tabella di routing per le subnet nel VPC (la tabella di routing principale), Cloud Manager aggiunge automaticamente gli indirizzi IP mobili alla tabella di routing. Se si dispone di più tabelle di routing, è molto importante selezionare le tabelle di routing corrette quando si avvia la coppia ha. In caso contrario, alcuni client potrebbero non avere accesso a Cloud Volumes ONTAP.

Ad esempio, potrebbero essere presenti due subnet associate a diverse tabelle di routing. Se si seleziona la tabella di route A, ma non la tabella di route B, i client nella subnet associata alla tabella di route A

possono accedere alla coppia ha, ma i client nella subnet associata alla tabella di route B.

Per ulteriori informazioni sulle tabelle di percorso, fare riferimento a. "[Documentazione AWS: Tabelle di percorso](#)".

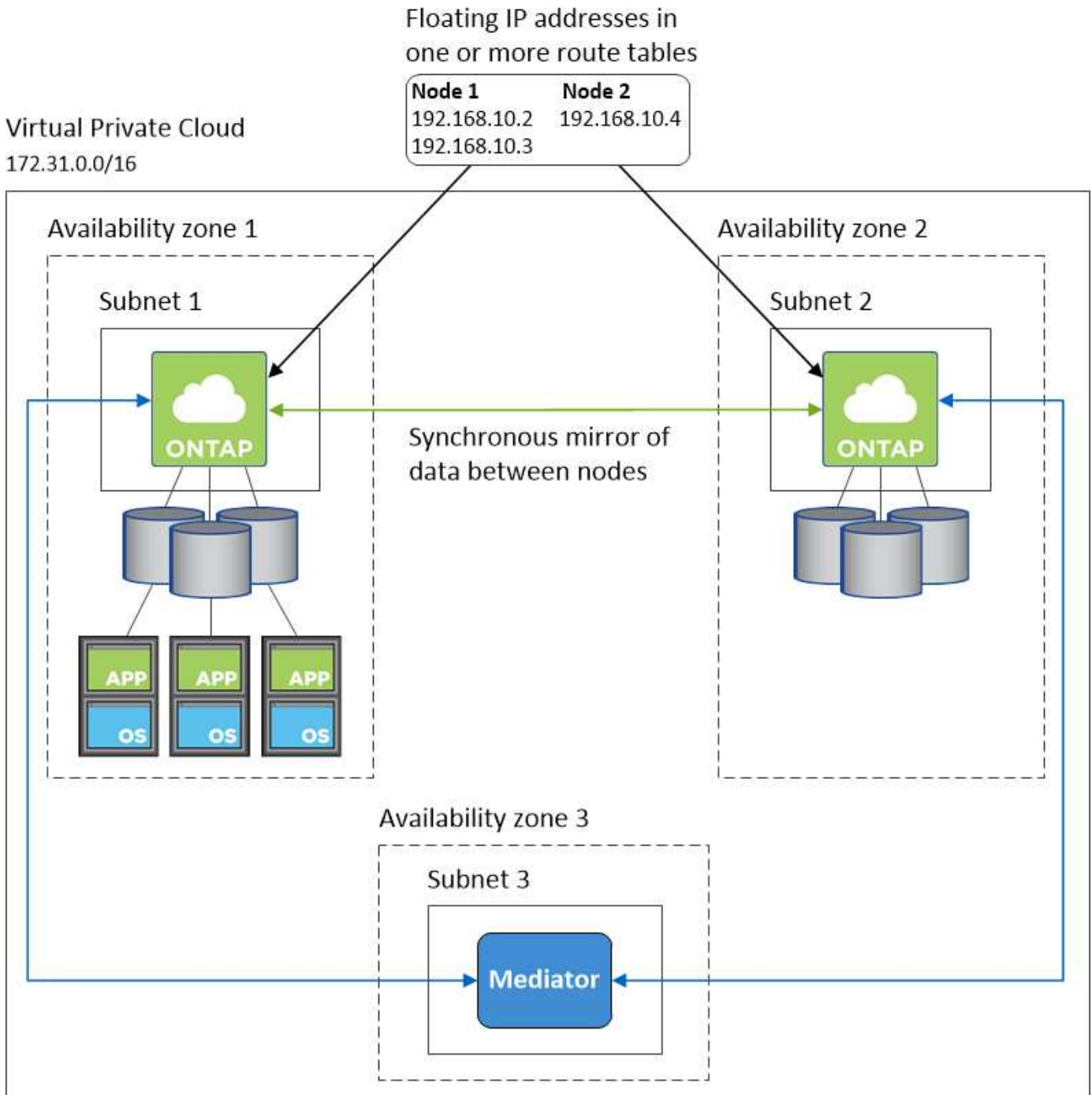
Connessione ai tool di gestione NetApp

Per utilizzare gli strumenti di gestione NetApp con configurazioni ha che si trovano in più AZS, sono disponibili due opzioni di connessione:

1. Implementare gli strumenti di gestione NetApp in un VPC diverso e. "[Configurare un gateway di transito AWS](#)". Il gateway consente l'accesso all'indirizzo IP mobile per l'interfaccia di gestione del cluster dall'esterno del VPC.
2. Implementare gli strumenti di gestione NetApp nello stesso VPC con una configurazione di routing simile a quella dei client NAS.

Configurazione di esempio

La seguente immagine mostra una configurazione ha ottimale in AWS che opera come configurazione Active-passive:



Configurazioni VPC di esempio

Per comprendere meglio come implementare Cloud Manager e Cloud Volumes ONTAP in AWS, è necessario esaminare le configurazioni VPC più comuni.

- Un VPC con subnet pubbliche e private e un dispositivo NAT
- Un VPC con una subnet privata e una connessione VPN alla rete

Un VPC con subnet pubbliche e private e un dispositivo NAT

Questa configurazione VPC include subnet pubbliche e private, un gateway Internet che connette il VPC a Internet e un gateway NAT o istanza NAT nella subnet pubblica che abilita il traffico Internet in uscita dalla

subnet privata. In questa configurazione, è possibile eseguire Cloud Manager in una subnet pubblica o in una subnet privata, ma la subnet pubblica è consigliata perché consente l'accesso da host esterni al VPC. È quindi possibile avviare le istanze di Cloud Volumes ONTAP nella subnet privata.

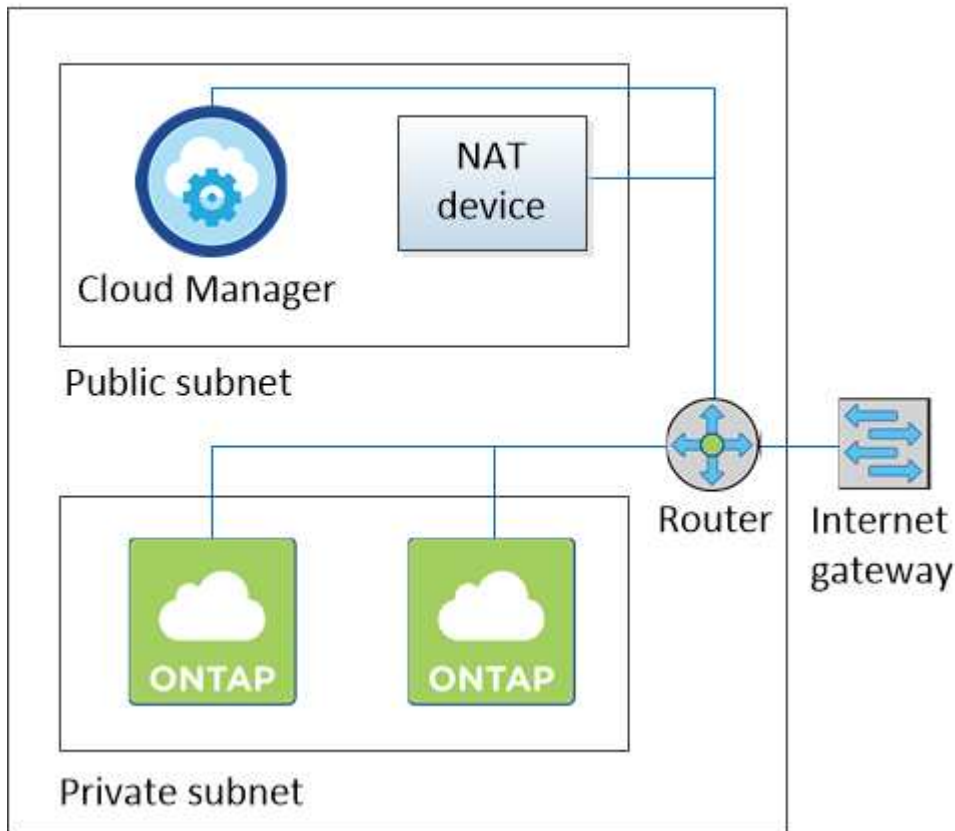


Invece di un dispositivo NAT, è possibile utilizzare un proxy HTTP per fornire la connettività Internet.

Per ulteriori informazioni su questo scenario, fare riferimento a "[Documentazione AWS: Scenario 2: VPC con subnet pubbliche e private \(NAT\)](#)".

La seguente figura mostra Cloud Manager in esecuzione in una subnet pubblica e in sistemi a nodo singolo in esecuzione in una subnet privata:

Virtual Private Cloud



Un VPC con una subnet privata e una connessione VPN alla rete

Questa configurazione VPC è una configurazione di cloud ibrido in cui Cloud Volumes ONTAP diventa un'estensione del tuo ambiente privato. La configurazione include una subnet privata e un gateway privato virtuale con una connessione VPN alla rete. Il routing attraverso il tunnel VPN consente alle istanze EC2 di accedere a Internet attraverso la rete e i firewall. È possibile eseguire Cloud Manager nella subnet privata o nel data center. Quindi, avviare Cloud Volumes ONTAP nella subnet privata.



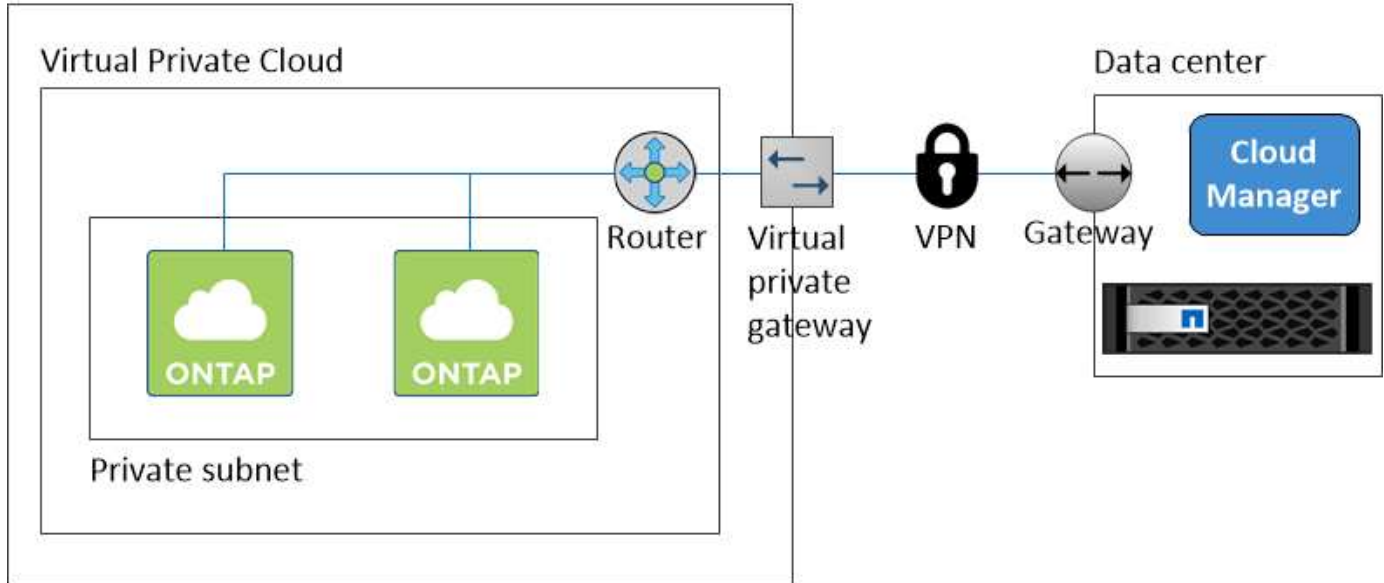
In questa configurazione è anche possibile utilizzare un server proxy per consentire l'accesso a Internet. Il server proxy può trovarsi nel data center o in AWS.

Se si desidera replicare i dati tra i sistemi FAS nel data center e i sistemi Cloud Volumes ONTAP in AWS, è necessario utilizzare una connessione VPN in modo che il collegamento sia sicuro.

Per ulteriori informazioni su questo scenario, fare riferimento a. "[Documentazione AWS: Scenario 4: Solo VPC con subnet privata e accesso VPN gestito da AWS](#)".

La seguente figura mostra Cloud Manager in esecuzione nel data center e nei sistemi a nodo singolo in esecuzione in una subnet privata:

AWS region



Configurazione di un gateway di transito AWS per coppie ha in più AZS

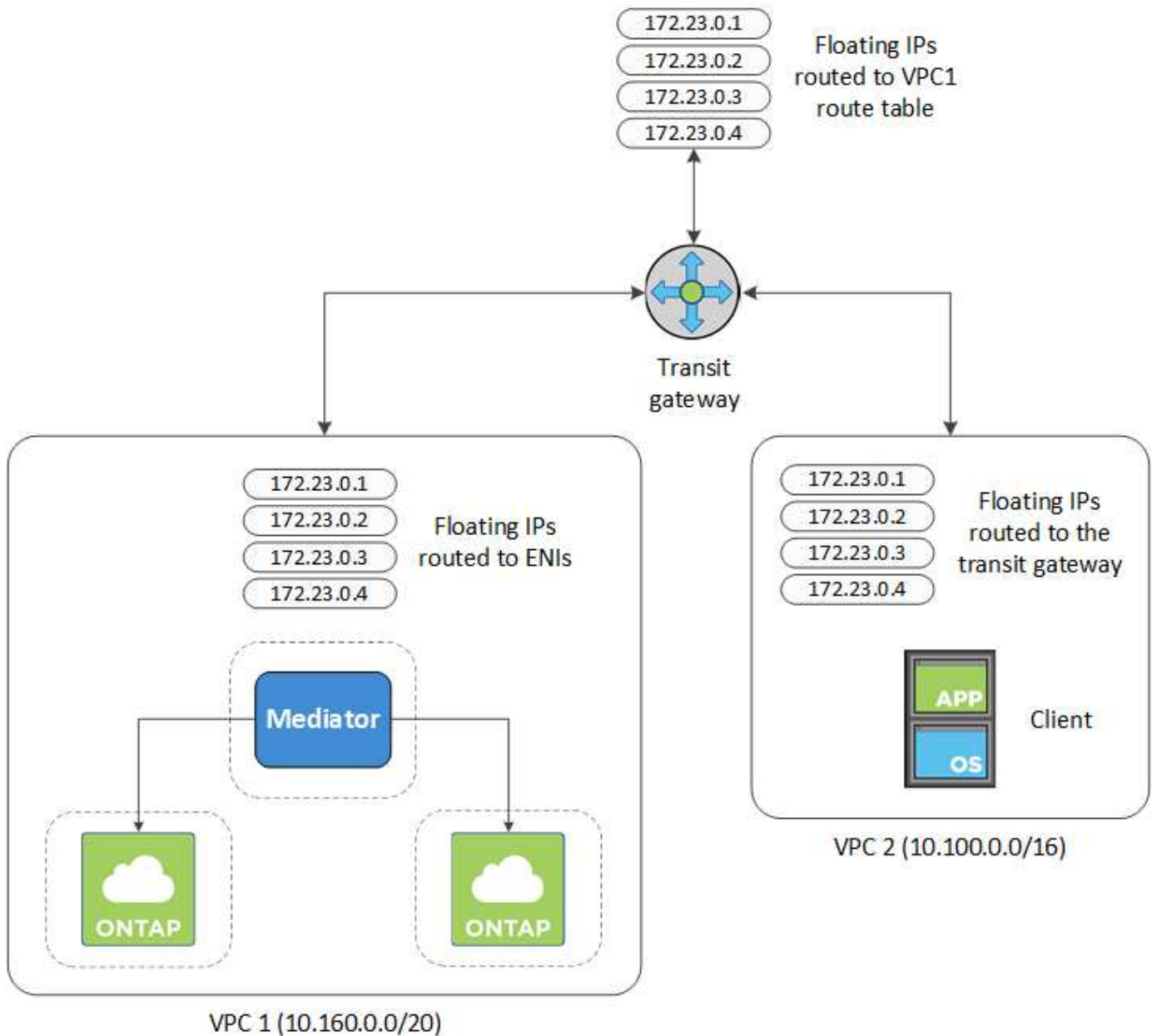
Impostare un gateway di transito AWS per consentire l'accesso agli indirizzi IP mobili di una coppia ha dall'esterno del VPC in cui risiede la coppia ha.

Quando una configurazione Cloud Volumes ONTAP ha viene distribuita in più zone di disponibilità AWS, sono richiesti indirizzi IP mobili per l'accesso ai dati NAS dall'interno del VPC. Questi indirizzi IP mobili possono migrare tra i nodi in caso di guasti, ma non sono accessibili in modo nativo dall'esterno del VPC. Gli indirizzi IP privati separati forniscono l'accesso ai dati dall'esterno del VPC, ma non forniscono il failover automatico.

Gli indirizzi IP mobili sono richiesti anche per l'interfaccia di gestione del cluster e per la LIF di gestione SVM opzionale.

Se si imposta un gateway di transito AWS, si abilita l'accesso agli indirizzi IP mobili dall'esterno del VPC in cui risiede la coppia ha. Ciò significa che i client NAS e gli strumenti di gestione NetApp esterni al VPC possono accedere agli IP mobili.

Ecco un esempio che mostra due VPC connessi da un gateway di transito. Un sistema ha risiede in un VPC, mentre un client risiede nell'altro. È quindi possibile montare un volume NAS sul client utilizzando l'indirizzo IP mobile.



La seguente procedura illustra come configurare una configurazione simile.

Fasi

1. "Creare un gateway di transito e collegare i VPC al gateway".
2. Creare le route nella tabella delle route del gateway di transito specificando gli indirizzi IP mobili della coppia ha.

Gli indirizzi IP mobili sono disponibili nella pagina Working Environment Information (informazioni sull'ambiente di lavoro) di Cloud Manager. Ecco un esempio:

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

L'immagine di esempio seguente mostra la tabella di percorso per il gateway di transito. Include le route ai blocchi CIDR dei due VPC e quattro indirizzi IP mobili utilizzati da Cloud Volumes ONTAP.

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

Floating IP Addresses

3. Modificare la tabella di routing dei VPC che devono accedere agli indirizzi IP mobili.

- Aggiungere voci di routing agli indirizzi IP mobili.
- Aggiungere una voce di percorso al blocco CIDR del VPC in cui risiede la coppia ha.

L'immagine di esempio seguente mostra la tabella di routing per VPC 2, che include i percorsi verso VPC 1 e gli indirizzi IP mobili.

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. Modificare la tabella di routing per il VPC della coppia ha aggiungendo un percorso al VPC che richiede l'accesso agli indirizzi IP mobili.

Questo passaggio è importante perché completa il routing tra i VPC.

L'immagine di esempio seguente mostra la tabella di percorso per VPC 1. Include un routing agli indirizzi IP mobili e a VPC 2, che è dove risiede un client. Cloud Manager ha aggiunto automaticamente gli IP mobili alla tabella di routing quando ha implementato la coppia ha.

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

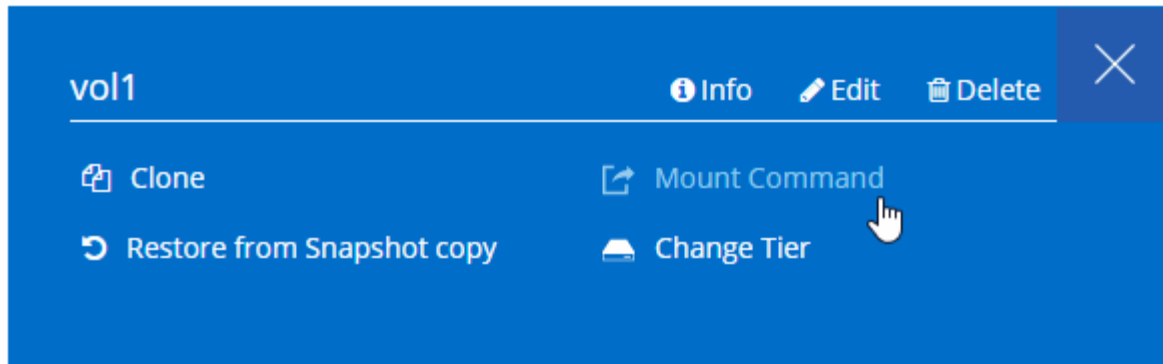
VPC2
Floating act IP Addresses

5. Montare i volumi sui client utilizzando l'indirizzo IP mobile.

È possibile trovare l'indirizzo IP corretto in Cloud Manager selezionando un volume e facendo clic su **Mount Command**.

Volumes

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



Link correlati

- ["Coppie ad alta disponibilità in AWS"](#)
- ["Requisiti di rete per Cloud Volumes ONTAP in AWS"](#)

Requisiti di rete per Cloud Volumes ONTAP in Azure

Configura la tua rete Azure in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente.

Accesso a Internet in uscita per Cloud Volumes ONTAP

Cloud Volumes ONTAP richiede l'accesso a Internet in uscita per inviare messaggi a NetApp AutoSupport, che monitora in maniera proattiva lo stato dello storage.

I criteri di routing e firewall devono consentire il traffico HTTP/HTTPS ai seguenti endpoint in modo che Cloud Volumes ONTAP possa inviare messaggi AutoSupport:

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

Gruppi di sicurezza

Non è necessario creare gruppi di sicurezza perché Cloud Manager fa questo per te. Se è necessario utilizzare il proprio, fare riferimento a ["Regole del gruppo di sicurezza"](#).

Numero di indirizzi IP

Cloud Manager assegna il seguente numero di indirizzi IP a Cloud Volumes ONTAP in Azure:

- Nodo singolo: 5 indirizzi IP
- Coppia HA: 16 indirizzi IP

Si noti che Cloud Manager crea una LIF di gestione SVM sulle coppie ha, ma non sui sistemi a nodo singolo in Azure.



LIF è un indirizzo IP associato a una porta fisica. Per strumenti di gestione come SnapCenter è necessaria una LIF di gestione SVM.

Connessione da Cloud Volumes ONTAP a Azure BLOB storage per il tiering dei dati

Se si desidera eseguire il tiering dei dati cold allo storage Azure Blob, non è necessario configurare una connessione tra il Tier di performance e il Tier di capacità, purché Cloud Manager disponga delle autorizzazioni necessarie. Cloud Manager abilita un endpoint del servizio VNET se la policy di Cloud Manager dispone delle seguenti autorizzazioni:

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

Queste autorizzazioni sono incluse nella versione più recente ["Policy di Cloud Manager"](#).

Per ulteriori informazioni sull'impostazione del tiering dei dati, vedere ["Tiering dei dati cold su storage a oggetti a basso costo"](#).

Connessioni a sistemi ONTAP in altre reti

Per replicare i dati tra un sistema Cloud Volumes ONTAP in Azure e i sistemi ONTAP in altre reti, è necessario disporre di una connessione VPN tra Azure VNET e l'altra rete, ad esempio un VPC AWS o la rete aziendale.

Per istruzioni, fare riferimento a ["Documentazione di Microsoft Azure: Crea una connessione Site-to-Site nel portale Azure"](#).

Requisiti di rete per Cloud Volumes ONTAP in GCP

Configura la tua rete della piattaforma cloud Google in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente.

VPC condiviso

Cloud Manager e Cloud Volumes ONTAP sono supportati in un VPC condiviso con la piattaforma cloud Google.

Un VPC condiviso consente di configurare e gestire centralmente le reti virtuali in più progetti. È possibile configurare reti VPC condivise nel *progetto host* e implementare le istanze di Cloud Manager e macchina virtuale Cloud Volumes ONTAP in un *progetto di servizio*. ["Documentazione di Google Cloud: Panoramica VPC condivisa"](#).

L'unico requisito è fornire le seguenti autorizzazioni all'account di servizio Cloud Manager nel progetto host VPC condiviso:

```
compute.firewalls.* compute.networks.* compute.subnetworks.*
```

Cloud Manager necessita di queste autorizzazioni per eseguire query su firewall, VPC e subnet nel progetto host.

Accesso a Internet in uscita per Cloud Volumes ONTAP

Cloud Volumes ONTAP richiede l'accesso a Internet in uscita per inviare messaggi a NetApp AutoSupport, che monitora in maniera proattiva lo stato dello storage.

I criteri di routing e firewall devono consentire il traffico HTTP/HTTPS ai seguenti endpoint in modo che Cloud Volumes ONTAP possa inviare messaggi AutoSupport:

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

Numero di indirizzi IP

Cloud Manager assegna 5 indirizzi IP a Cloud Volumes ONTAP in GCP.

Si noti che Cloud Manager non crea una LIF di gestione SVM per Cloud Volumes ONTAP in GCP.



LIF è un indirizzo IP associato a una porta fisica. Per strumenti di gestione come SnapCenter è necessaria una LIF di gestione SVM.

Regole del firewall

Non è necessario creare regole firewall perché Cloud Manager fa tutto questo per te. Se è necessario utilizzare il proprio, fare riferimento a ["Regole del firewall GCP"](#).

Connessione da Cloud Volumes ONTAP allo storage cloud Google per il tiering dei dati

Se si desidera eseguire il tiering dei dati cold in un bucket di storage cloud Google, la subnet in cui risiede Cloud Volumes ONTAP deve essere configurata per l'accesso privato a Google. Per istruzioni, fare riferimento a ["Documentazione di Google Cloud: Configurazione di Private Google Access"](#).

Per ulteriori passaggi necessari per impostare il tiering dei dati in Cloud Manager, consulta ["Tiering dei dati cold su storage a oggetti a basso costo"](#).

Connessioni a sistemi ONTAP in altre reti

Per replicare i dati tra un sistema Cloud Volumes ONTAP in GCP e i sistemi ONTAP in altre reti, è necessario disporre di una connessione VPN tra il VPC e l'altra rete, ad esempio la rete aziendale.

Per istruzioni, fare riferimento a ["Documentazione di Google Cloud: Panoramica di Cloud VPN"](#).

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.