Configura la tua rete

Cloud Volumes ONTAP

NetApp
February 13, 2026

Sommario

Configura la tua rete

Configurare la rete AWS per Cloud Volumes ONTAP

La NetApp Console gestisce la configurazione dei componenti di rete per Cloud Volumes ONTAP, come indirizzi IP, maschere di rete e percorsi. È necessario assicurarsi che l'accesso a Internet in uscita sia disponibile, che siano disponibili sufficienti indirizzi IP privati, che siano attive le connessioni giuste e altro ancora.

Requisiti generali

Assicurati di aver soddisfatto i seguenti requisiti in AWS.

Accesso Internet in uscita per i nodi Cloud Volumes ONTAP

I sistemi Cloud Volumes ONTAP necessitano di accesso a Internet in uscita per accedere agli endpoint esterni per varie funzioni. Cloud Volumes ONTAP non può funzionare correttamente se questi endpoint sono bloccati in ambienti con requisiti di sicurezza rigorosi.

L'agente della console contatta diversi endpoint per le operazioni quotidiane. Per informazioni sugli endpoint utilizzati, fare riferimento a "Visualizza gli endpoint contattati dall'agente della console" E "Preparare la rete per l'utilizzo della console" .

Endpoint Cloud Volumes ONTAP

Cloud Volumes ONTAP utilizza questi endpoint per comunicare con vari servizi.

Punti finali	Applicabile per	Scopo	Modalità di distribuzione	Impatto se l'endpoint non è disponibile
\ https://netapp-cloud-account.auth0.com	Autenticazione	Utilizzato per l'autenticazione nella Console.	Modalità standard e limitata.	L'autenticazione dell'utente fallisce e i seguenti servizi rimangono non disponibili: • Servizi Cloud Volumes ONTAP • Servizi ONTAP • Protocolli e servizi proxy
\ https://api.bluexp.netapp.com/tenancy	Locazione	Utilizzato per recuperare la risorsa Cloud Volumes ONTAP dalla Console per autorizzare risorse e utenti.	Modalità standard e limitata.	Le risorse Cloud Volumes ONTAP e gli utenti non sono autorizzati.

Punti finali	Applicabile per	Scopo	Modalità di distribuzione	Impatto se l'endpoint non è disponibile
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	Utilizzato per inviare i dati di telemetria AutoSupport al supporto NetApp .	Modalità standard e limitata.	Le informazioni AutoSupport non vengono recapitate.
L'endpoint commerciale esatto per il servizio AWS (con suffisso `amazonaws.com`) dipende dalla regione AWS che stai utilizzando. Fare riferimento al "Documentazione AWS per i dettagli" .	• Formazione delle nuvole • Elastic Compute Cloud (EC2) • Gestione dell'identità e degli accessi (IAM) • Servizio di gestione delle chiavi (KMS) • Servizio token di sicurezza (STS) • Amazon Simple Storage Service (S3)	Comunicazione con i servizi AWS.	Modalità standard e privata.	Cloud Volumes ONTAP non è in grado di comunicare con il servizio AWS per eseguire operazioni specifiche in AWS.
L'endpoint governativo esatto per il servizio AWS dipende dalla regione AWS utilizzata. Gli endpoint sono suffissi con `amazonaws.com` E `c2s.ic.gov` . Fare riferimento a "Kit di sviluppo software AWS" E "Documentazione AWS" per maggiori informazioni.	• Formazione delle nuvole • Elastic Compute Cloud (EC2) • Gestione dell'identità e degli accessi (IAM) • Servizio di gestione delle chiavi (KMS) • Servizio token di sicurezza (STS) • Servizio di archiviazione semplice (S3)	Comunicazione con i servizi AWS.	Modalità limitata.	Cloud Volumes ONTAP non è in grado di comunicare con il servizio AWS per eseguire operazioni specifiche in AWS.

Accesso Internet in uscita per il mediatore HA

L'istanza del mediatore HA deve disporre di una connessione in uscita al servizio AWS EC2 per poter supportare il failover dell'archiviazione. 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 i dettagli sugli endpoint VPC, fare riferimento a "Documentazione AWS: Endpoint VPC dell'interfaccia (AWS PrivateLink)" .

Configurazione del proxy di rete dell'agente NetApp Console

È possibile utilizzare la configurazione dei server proxy dell'agente NetApp Console per abilitare l'accesso a Internet in uscita da Cloud Volumes ONTAP. La console supporta due tipi di proxy:

- **Proxy esplicito**: il traffico in uscita da Cloud Volumes ONTAP utilizza l'indirizzo HTTP del server proxy specificato durante la configurazione del proxy dell'agente della console. L'amministratore potrebbe anche aver configurato le credenziali utente e i certificati CA radice per un'autenticazione aggiuntiva. Se è disponibile un certificato CA radice per il proxy esplicito, assicurarsi di ottenere e caricare lo stesso certificato sul sistema Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.
- **Proxy trasparente**: la rete è configurata per instradare automaticamente il traffico in uscita da Cloud Volumes ONTAP tramite il proxy per l'agente della console. Quando si configura un proxy trasparente, l'amministratore deve fornire solo un certificato CA radice per la connettività da Cloud Volumes ONTAP, non l'indirizzo HTTP del server proxy. Assicurati di ottenere e caricare lo stesso certificato CA radice sul tuo sistema Cloud Volumes ONTAP utilizzando "ONTAP CLI: installazione del certificato di sicurezza" comando.

Per informazioni sulla configurazione dei server proxy, fare riferimento a "Configurare l'agente della console per utilizzare un server proxy" .

Indirizzi IP privati

La console assegna automaticamente il numero richiesto di indirizzi IP privati a Cloud Volumes ONTAP. È necessario assicurarsi che la rete disponga di un numero sufficiente di indirizzi IP privati.

Il numero di LIF che la Console assegna per Cloud Volumes ONTAP dipende dal fatto che si distribuisca un sistema a nodo singolo o una coppia HA. Un LIF è un indirizzo IP associato a una porta fisica.

Indirizzi IP per un sistema a nodo singolo

La NetApp Console assegna 6 indirizzi IP a un sistema a nodo singolo.

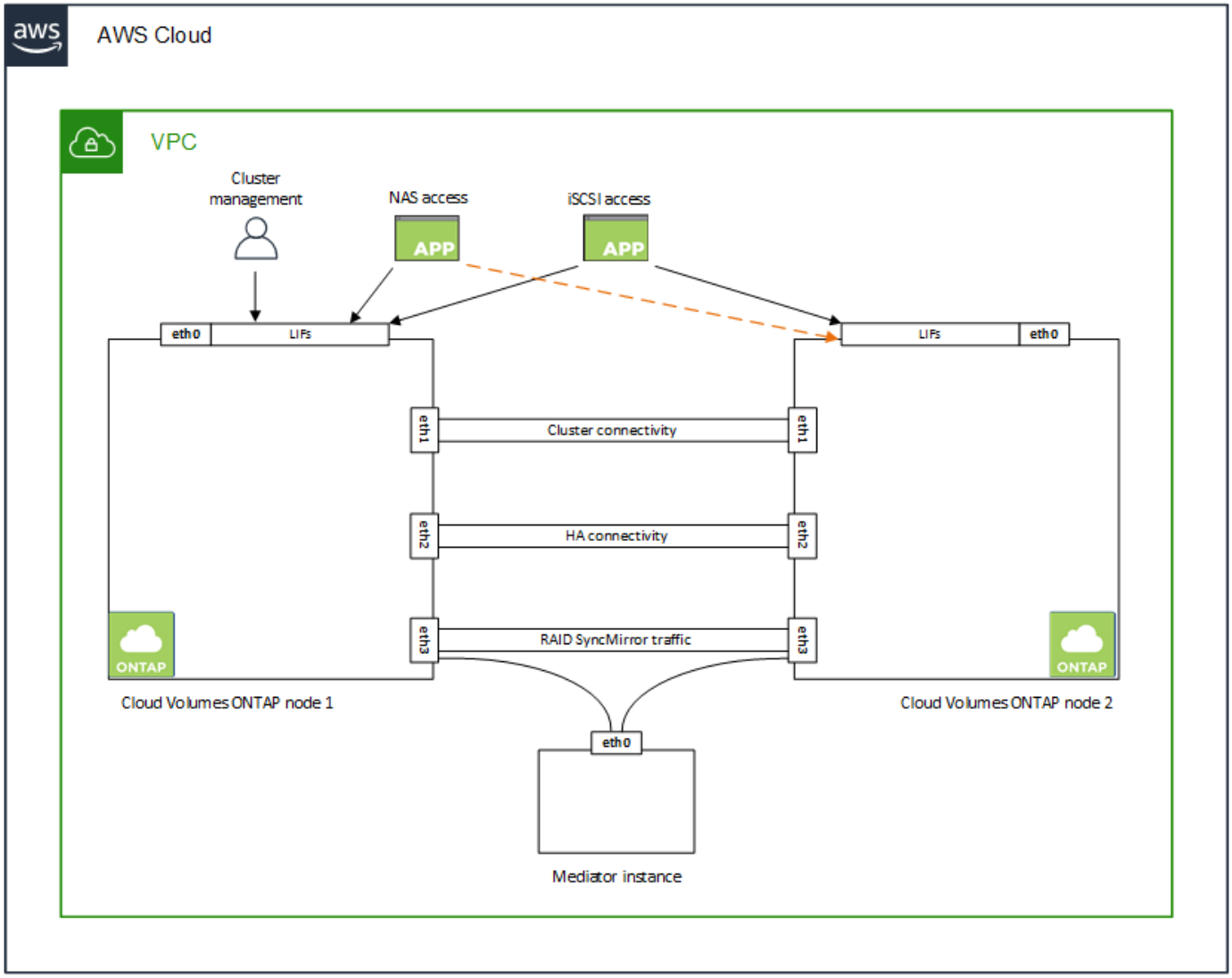
La tabella seguente fornisce dettagli sui LIF associati a ciascun indirizzo IP privato.

VITA	Scopo
Gestione dei cluster	Gestione amministrativa dell'intero cluster (coppia HA).
Gestione dei nodi	Gestione amministrativa di un nodo.
Intercluster	Comunicazione, backup e replica tra cluster.
Dati NAS	Accesso client tramite protocolli NAS.

VITA	Scopo
dati iSCSI	Accesso client tramite protocollo iSCSI. Utilizzato dal sistema anche per altri importanti flussi di lavoro di rete. Questo LIF è obbligatorio e non deve essere eliminato.
Gestione delle VM di archiviazione	Un LIF di gestione delle VM di storage viene utilizzato con strumenti di gestione come SnapCenter.

Indirizzi IP per coppie HA

Le coppie HA richiedono più indirizzi IP rispetto a un sistema a nodo singolo. Questi indirizzi IP sono distribuiti su diverse interfacce ethernet, come mostrato nell'immagine seguente:



Il numero di indirizzi IP privati richiesti per una coppia HA dipende dal modello di distribuzione scelto. Una coppia HA distribuita in una *singola* zona di disponibilità (AZ) AWS richiede 15 indirizzi IP privati, mentre una coppia HA distribuita in *più* AZ richiede 13 indirizzi IP privati.

Le tabelle seguenti forniscono dettagli sui LIF associati a ciascun indirizzo IP privato.

VITA	Interfaccia	Nodo	Scopo
Gestione dei cluster	eth0	nodo 1	Gestione amministrativa dell'intero cluster (coppia HA).
Gestione dei nodi	eth0	nodo 1 e nodo 2	Gestione amministrativa di un nodo.
Intercluster	eth0	nodo 1 e nodo 2	Comunicazione, backup e replica tra cluster.
Dati NAS	eth0	nodo 1	Accesso client tramite protocolli NAS.
dati iSCSI	eth0	nodo 1 e nodo 2	Accesso client tramite protocollo iSCSI. Utilizzato dal sistema anche per altri importanti flussi di lavoro di rete. Questi LIF sono obbligatori e non devono essere eliminati.
Connettività del cluster	eth1	nodo 1 e nodo 2	Consente ai nodi di comunicare tra loro e di spostare i dati all'interno del cluster.
Connettività HA	eth2	nodo 1 e nodo 2	Comunicazione tra i due nodi in caso di failover.
Traffico iSCSI RSM	eth3	nodo 1 e nodo 2	Traffico iSCSI RAID SyncMirror , nonché comunicazione tra i due nodi Cloud Volumes ONTAP e il mediatore.
Mediatore	eth0	Mediatore	Un canale di comunicazione tra i nodi e il mediatore per facilitare i processi di acquisizione e restituzione dello storage.

VITA	Interfaccia	Nodo	Scopo
Gestione dei nodi	eth0	nodo 1 e nodo 2	Gestione amministrativa di un nodo.
Intercluster	eth0	nodo 1 e nodo 2	Comunicazione, backup e replica tra cluster.
dati iSCSI	eth0	nodo 1 e nodo 2	Accesso client tramite protocollo iSCSI. Questi LIF gestiscono anche la migrazione degli indirizzi IP flottanti tra i nodi. Questi LIF sono obbligatori e non devono essere eliminati.
Connettività del cluster	eth1	nodo 1 e nodo 2	Consente ai nodi di comunicare tra loro e di spostare i dati all'interno del cluster.
Connettività HA	eth2	nodo 1 e nodo 2	Comunicazione tra i due nodi in caso di failover.
Traffico iSCSI RSM	eth3	nodo 1 e nodo 2	Traffico iSCSI RAID SyncMirror , nonché comunicazione tra i due nodi Cloud Volumes ONTAP e il mediatore.
Mediatore	eth0	Mediatore	Un canale di comunicazione tra i nodi e il mediatore per facilitare i processi di acquisizione e restituzione dello storage.

Quando distribuiti in più zone di disponibilità, diversi LIF sono associati a"indirizzi IP flottanti" , che non vengono conteggiati nel limite IP privato di AWS.

Gruppi di sicurezza

Non è necessario creare gruppi di sicurezza perché la Console lo fa per te. Se devi usare il tuo, fai riferimento a"Regole del gruppo di sicurezza" .

Cerchi informazioni sull'agente Console? "Visualizza le regole del gruppo di sicurezza per l'agente della console"

Connessione per la suddivisione in livelli dei dati

Se si desidera utilizzare EBS come livello di prestazioni e Amazon S3 come livello di capacità, è necessario assicurarsi che Cloud Volumes ONTAP disponga di una connessione a S3. Il modo migliore per fornire tale connessione è creare un VPC Endpoint per il servizio S3. Per istruzioni, consultare il "Documentazione AWS: creazione di un endpoint gateway".

Quando crei l'endpoint VPC, assicurati di selezionare la regione, la VPC e la tabella di routing che corrispondono all'istanza Cloud Volumes ONTAP . È inoltre necessario modificare il gruppo di sicurezza per aggiungere una regola HTTPS in uscita che consenta il traffico verso l'endpoint S3. In caso contrario, Cloud Volumes ONTAP non potrà connettersi al servizio S3.

Se riscontri problemi, fai riferimento a "AWS Support Knowledge Center: perché non riesco a connettermi a un bucket S3 tramite un endpoint VPC gateway?"

Collegamenti ai sistemi ONTAP

Per replicare i dati tra un sistema Cloud Volumes ONTAP in AWS e sistemi ONTAP in altre reti, è necessario disporre di una connessione VPN tra AWS VPC e l'altra rete, ad esempio la rete aziendale. Per le istruzioni, fare riferimento al "Documentazione AWS: configurazione di una connessione VPN AWS" .

DNS e Active Directory per CIFS

Se si desidera eseguire il provisioning di storage CIFS, è necessario configurare DNS e Active Directory in AWS oppure estendere la configurazione locale 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 le istruzioni, fare riferimento al "Documentazione AWS: Servizi di dominio Active Directory sul cloud AWS: distribuzione di riferimento rapido" .

Condivisione VPC

A partire dalla versione 9.11.1, le coppie Cloud Volumes ONTAP HA sono supportate in AWS con condivisione VPC. La condivisione VPC consente alla tua organizzazione di condividere subnet con altri account AWS. Per utilizzare questa configurazione, è necessario impostare l'ambiente AWS e quindi distribuire la coppia HA tramite l'API.

"Scopri come distribuire una coppia HA in una subnet condivisa" .

Requisiti per coppie HA in più AZ

Ulteriori requisiti di rete AWS si applicano alle configurazioni Cloud Volumes ONTAP HA che utilizzano più zone di disponibilità (AZ). È opportuno esaminare questi requisiti prima di avviare una coppia HA, poiché è necessario immettere i dettagli di rete nella Console quando si aggiunge un sistema Cloud Volumes ONTAP .

Per comprendere come funzionano le coppie HA, fare riferimento a"Coppie ad alta disponibilità" .

Zone di disponibilità

Questo modello di distribuzione HA utilizza più AZ per garantire un'elevata disponibilità dei dati. È necessario utilizzare una AZ dedicata per ogni istanza Cloud Volumes ONTAP e per l'istanza mediatrice, che fornisce un canale di comunicazione tra la coppia HA.

In ogni zona di disponibilità dovrebbe essere disponibile una subnet.

Indirizzi IP flottanti per dati NAS e gestione cluster/SVM

Le configurazioni HA in più AZ utilizzano indirizzi IP mobili che migrano tra i nodi in caso di guasti. Non sono accessibili in modo nativo dall'esterno della VPC, a meno che tu non"configurare un gateway di transito AWS" .

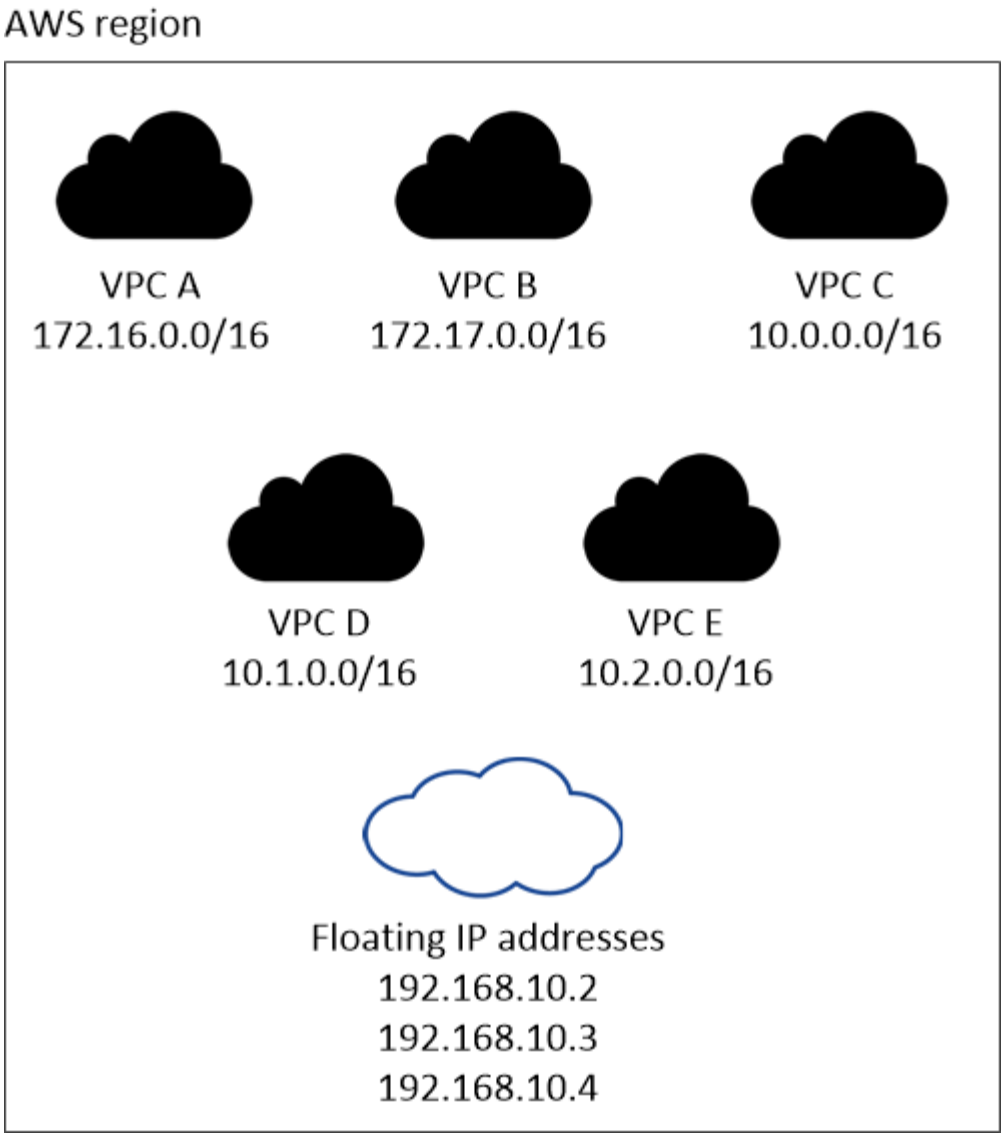
Un indirizzo IP mobile è per la gestione del cluster, uno è per i dati NFS/CIFS sul nodo 1 e uno è per i dati NFS/CIFS sul nodo 2. Un quarto indirizzo IP mobile per la gestione SVM è facoltativo.

> Se si utilizza SnapDrive per Windows o SnapCenter con la coppia HA, è necessario un indirizzo IP mobile per la gestione SVM LIF.

Quando si aggiunge un sistema Cloud Volumes ONTAP HA, è necessario immettere gli indirizzi IP mobili. La console assegna gli indirizzi IP alla coppia HA quando avvia il sistema.

Gli indirizzi IP mobili devono essere esterni ai blocchi CIDR per tutte le VPC nella regione AWS in cui si distribuisce la configurazione HA. Considera gli indirizzi IP mobili come una subnet logica esterna alle VPC nella tua regione.

L'esempio seguente mostra la relazione tra indirizzi IP mobili e VPC in una regione AWS. Sebbene gli indirizzi IP mobili siano al di fuori dei blocchi CIDR per tutte le VPC, sono instradabili verso le subnet tramite tabelle di routing.



La console crea automaticamente indirizzi IP statici per l'accesso iSCSI e per l'accesso NAS da client esterni alla VPC. Per questi tipi di indirizzi IP non è necessario soddisfare alcun requisito.

Gateway di transito per abilitare l'accesso IP flottante dall'esterno della VPC

Se necessario,"configurare un gateway di transito AWS" per consentire l'accesso agli indirizzi IP mobili di una coppia HA dall'esterno della VPC in cui risiede la coppia HA.

Tabelle di routing

Dopo aver specificato gli indirizzi IP mobili, ti verrà chiesto di selezionare le tabelle di routing che devono includere i percorsi verso gli indirizzi IP mobili. Ciò consente al client di accedere alla coppia HA.

Se si dispone di una sola tabella di routing per le subnet nella VPC (la tabella di routing principale), la Console aggiunge automaticamente gli indirizzi IP mobili a tale tabella di routing. Se si dispone di più di una tabella 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, potresti avere due subnet associate a tabelle di routing diverse. Se si seleziona la tabella di routing A, ma non la tabella di routing B, i client nella subnet associata alla tabella di routing A possono

accedere alla coppia HA, ma i client nella subnet associata alla tabella di routing B non possono.

Per ulteriori informazioni sulle tabelle di routing, fare riferimento a "Documentazione AWS: tabelle di routing" .

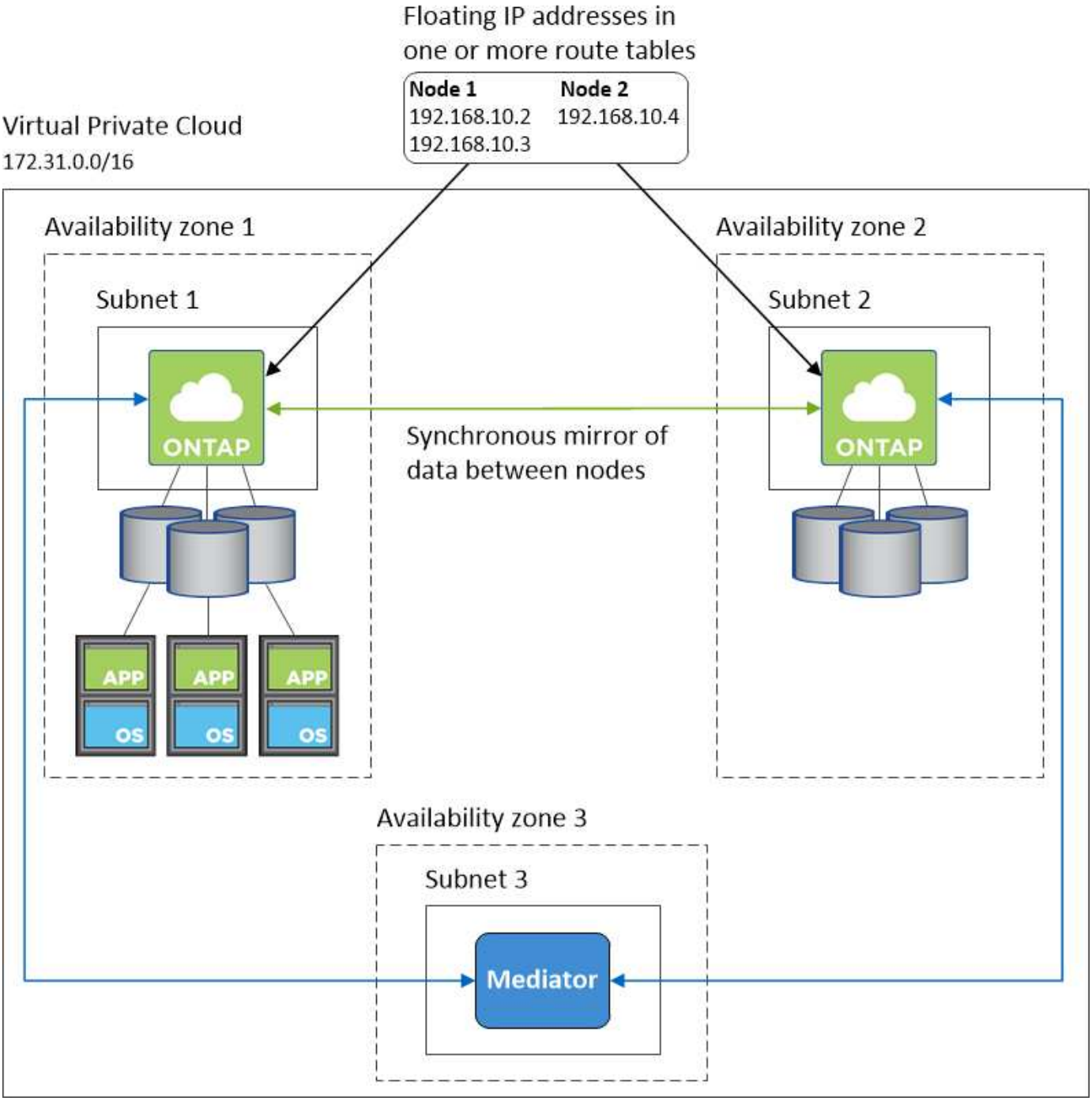
Connessione agli strumenti di gestione NetApp

Per utilizzare gli strumenti di gestione NetApp con configurazioni HA presenti in più AZ, sono disponibili due opzioni di connessione:

1. Distribuire gli strumenti di gestione NetApp in una VPC diversa e"configurare un gateway di transito AWS" . Il gateway consente l'accesso all'indirizzo IP flottante per l'interfaccia di gestione del cluster dall'esterno della VPC.
2. Distribuire gli strumenti di gestione NetApp nella stessa VPC con una configurazione di routing simile a quella dei client NAS.

Esempio di configurazione HA

L'immagine seguente illustra i componenti di rete specifici di una coppia HA in più AZ: tre zone di disponibilità, tre subnet, indirizzi IP mobili e una tabella di routing.



Requisiti per l'agente della console

Se non hai ancora creato un agente Console, dovresti rivedere i requisiti di rete.

- "Visualizza i requisiti di rete per l'agente della console"
- "Regole del gruppo di sicurezza in AWS"

Argomenti correlati

- "Verifica la configurazione AutoSupport per Cloud Volumes ONTAP"
- "Scopri di più sulle porte interne ONTAP" .

Configurare un gateway di transito AWS per coppie Cloud Volumes ONTAP HA

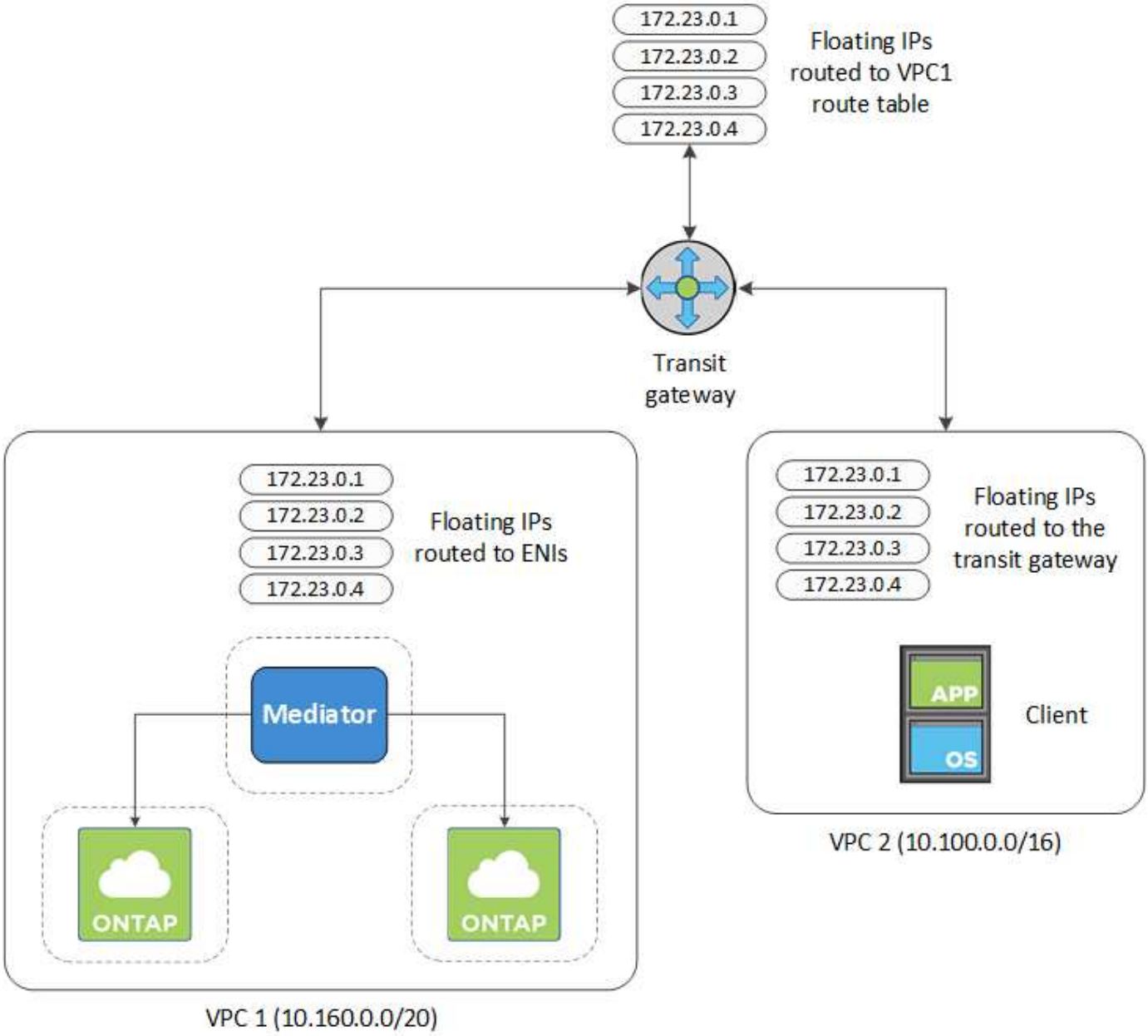
Impostare un gateway di transito AWS per abilitare l'accesso a una coppia HA"indirizzi IP flottanti" dall'esterno della VPC in cui risiede la coppia HA.

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

Sono richiesti anche indirizzi IP flottanti per l'interfaccia di gestione del cluster e per il LIF di gestione SVM opzionale.

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

Ecco un esempio che mostra due VPC connesse tramite un gateway di transito. Un sistema HA risiede in una VPC, mentre un client risiede nell'altra. È quindi possibile montare un volume NAS sul client utilizzando l'indirizzo IP flottante.

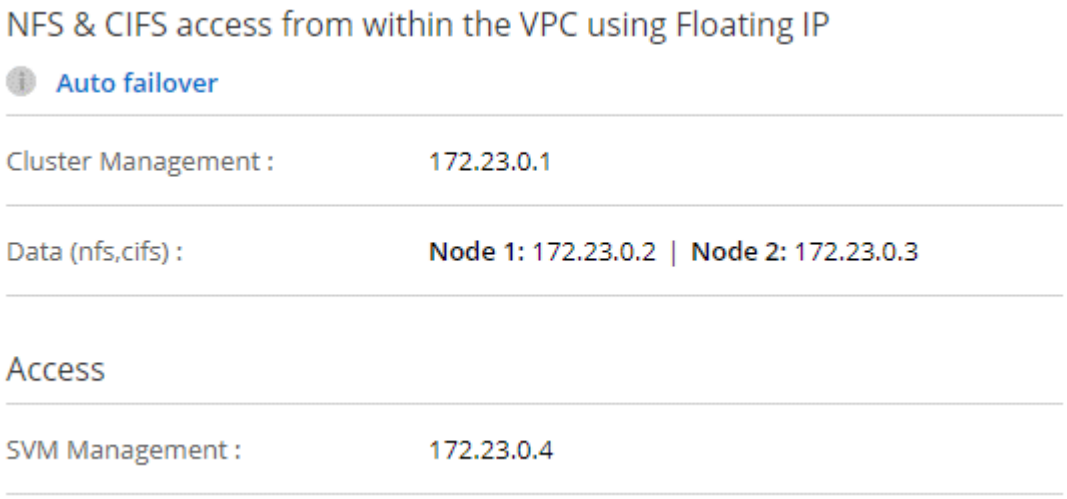


I passaggi seguenti illustrano come impostare una configurazione simile.

Passi

1. "Creare un gateway di transito e collegare le VPC al gateway" .
2. Associare le VPC alla tabella di routing del gateway di transito.
   a. Nel servizio **VPC**, fare clic su **Tabelle di routing del gateway di transito**.
   b. Selezionare la tabella di routing.
   c. Fare clic su **Associazioni** e quindi selezionare **Crea associazione**.
   d. Selezionare gli allegati (VPC) da associare, quindi fare clic su **Crea associazione**.
3. Creare percorsi nella tabella di routing del gateway di transito specificando gli indirizzi IP flottanti della coppia HA.

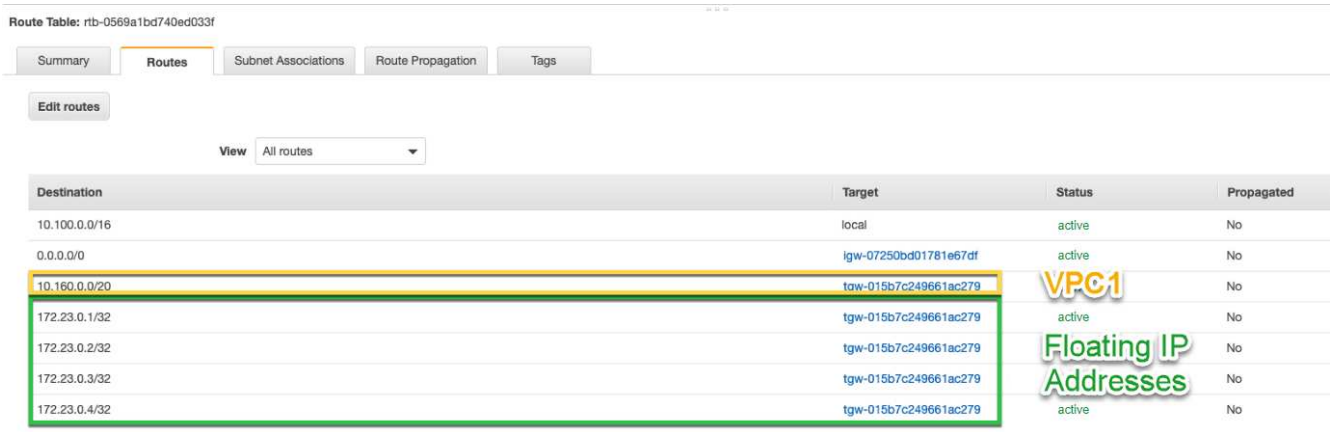
   Puoi trovare gli indirizzi IP mobili nella pagina delle informazioni di sistema nella NetApp Console. Ecco un esempio:



L'immagine di esempio seguente mostra la tabella di routing per il gateway di transito. Include percorsi verso i blocchi CIDR delle due VPC e quattro indirizzi IP mobili utilizzati da Cloud Volumes ONTAP.

4. Modificare la tabella di routing delle VPC che devono accedere agli indirizzi IP mobili.
   a. Aggiungere voci di percorso agli indirizzi IP mobili.
   b. Aggiungere una voce di percorso al blocco CIDR della VPC in cui risiede la coppia HA.

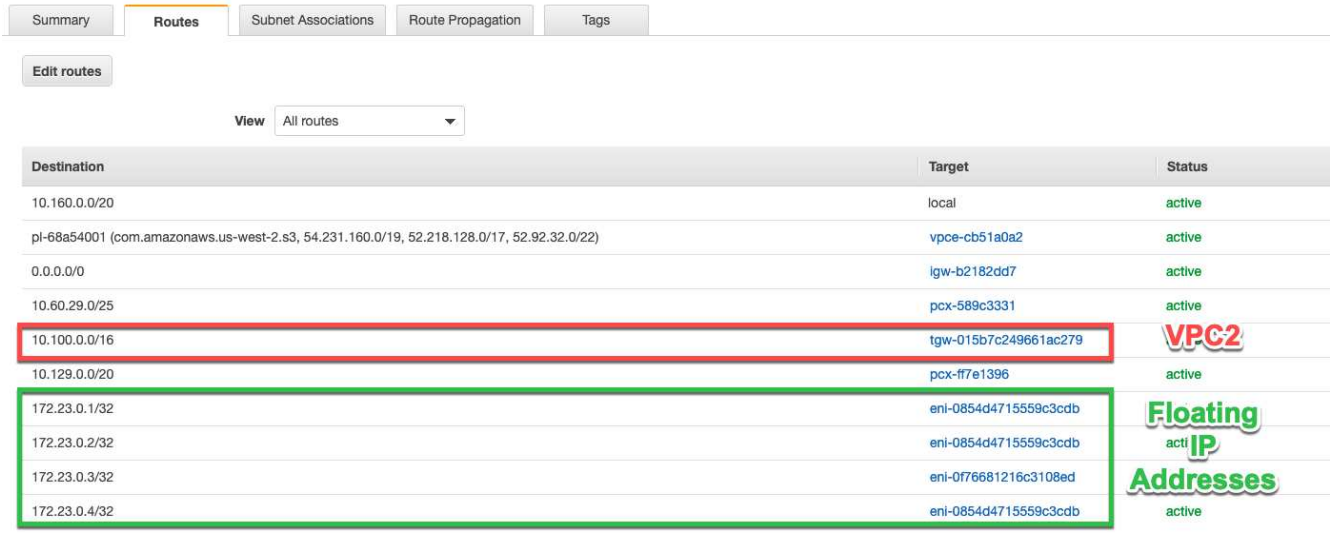
      L'immagine di esempio seguente mostra la tabella di routing per VPC 2, che include i percorsi verso VPC 1 e gli indirizzi IP mobili.



5. Modificare la tabella di routing per la VPC della coppia HA aggiungendo una route alla VPC che necessita di accesso agli indirizzi IP flottanti.

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

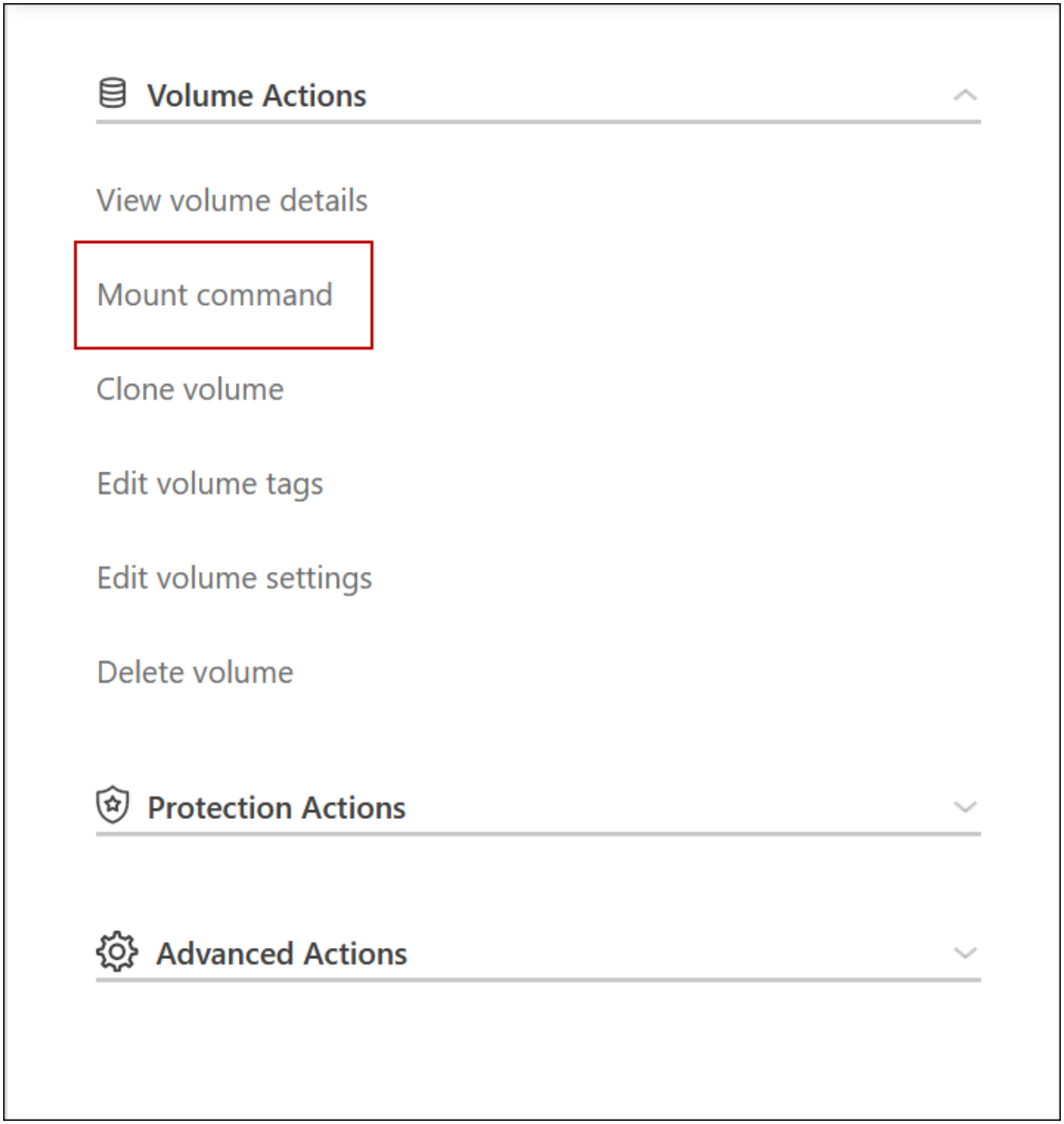
   L'immagine di esempio seguente mostra la tabella di routing per VPC 1. Include un percorso verso gli indirizzi IP mobili e verso VPC 2, dove risiede un client. La console ha aggiunto automaticamente gli IP mobili alla tabella di routing quando ha distribuito la coppia HA.



6. Aggiorna le impostazioni dei gruppi di sicurezza su Tutto il traffico per la VPC.
   a. In Virtual Private Cloud, fare clic su **Sottoreti**.
   b. Fare clic sulla scheda **Tabella di routing** e selezionare l'ambiente desiderato per uno degli indirizzi IP mobili per una coppia HA.
   c. Fare clic su **Gruppi di sicurezza**.
   d. Selezionare **Modifica regole in entrata**.
   e. Fare clic su **Aggiungi regola**.
   f. In Tipo, seleziona **Tutto il traffico**, quindi seleziona l'indirizzo IP VPC.
   g. Fare clic su **Salva regole** per applicare le modifiche.
7. Montare i volumi sui client utilizzando l'indirizzo IP mobile.

   È possibile trovare l'indirizzo IP corretto nella Console tramite l'opzione **Comando di montaggio** nel

pannello Gestisci volumi nella Console.



8. Se si sta montando un volume NFS, configurare la policy di esportazione in modo che corrisponda alla subnet del VPC client.

   "Scopri come modificare un volume" .

Link correlati

- "Coppie ad alta disponibilità in AWS"
- "Requisiti di rete per Cloud Volumes ONTAP in AWS"

Distribuisci coppie Cloud Volumes ONTAP HA in una subnet condivisa AWS

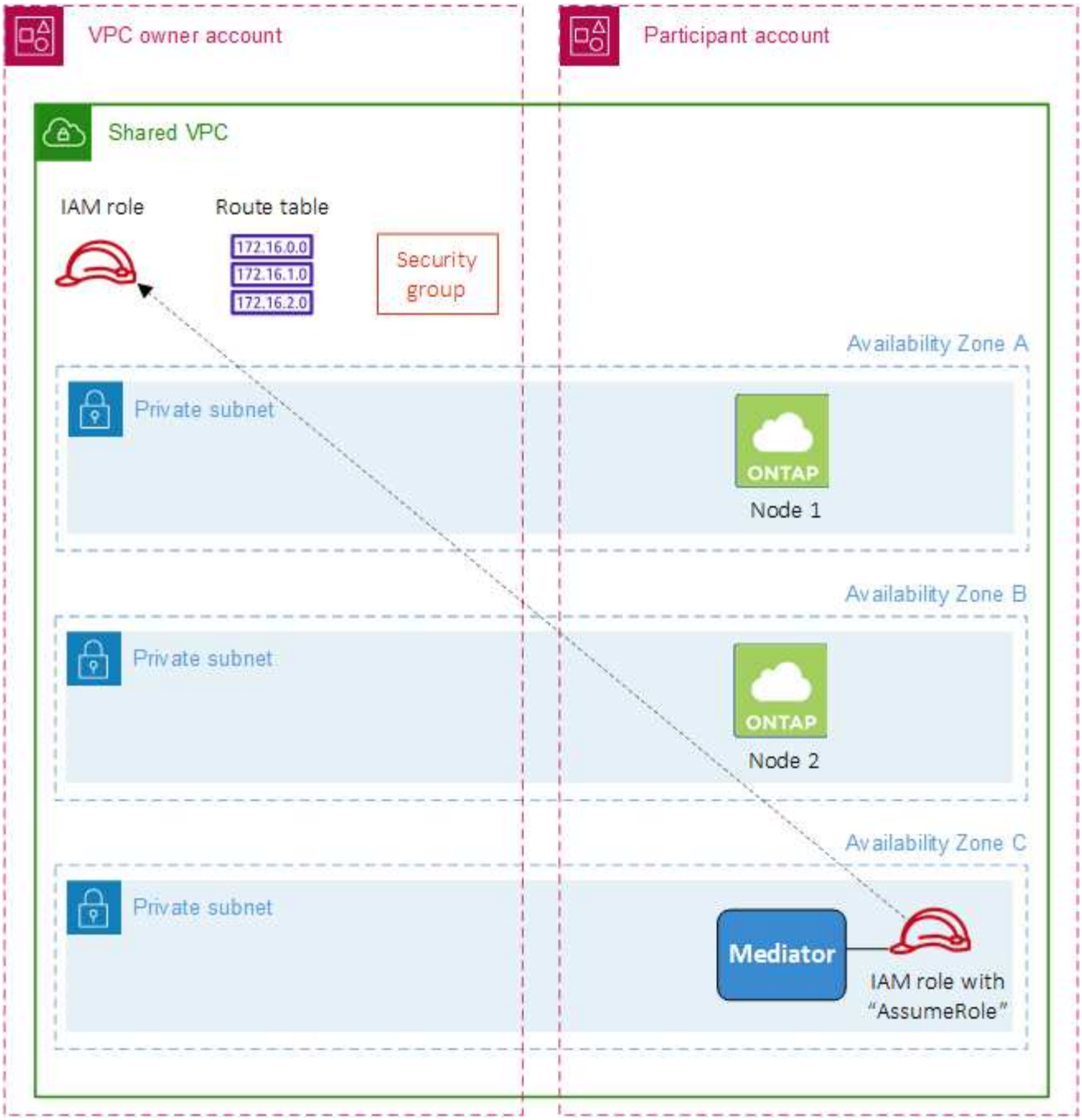
A partire dalla versione 9.11.1, le coppie Cloud Volumes ONTAP HA sono supportate in AWS con condivisione VPC. La condivisione VPC consente alla tua organizzazione di condividere subnet con altri account AWS. Per utilizzare questa configurazione, è necessario impostare l'ambiente AWS e quindi distribuire la coppia HA tramite l'API.

Con "Condivisione VPC" , una configurazione Cloud Volumes ONTAP HA è distribuita su due account:

- L'account proprietario della VPC, che possiede la rete (la VPC, le subnet, le tabelle di routing e il gruppo di sicurezza Cloud Volumes ONTAP)
- L'account del partecipante, in cui le istanze EC2 vengono distribuite in subnet condivise (inclusi i due nodi HA e il mediatore)

Nel caso di una configurazione Cloud Volumes ONTAP HA distribuita su più zone di disponibilità, il mediatore HA necessita di autorizzazioni specifiche per scrivere nelle tabelle di routing nell'account proprietario della VPC. È necessario fornire tali autorizzazioni impostando un ruolo IAM che il mediatore può assumere.

L'immagine seguente mostra i componenti coinvolti in questa distribuzione:



Come descritto nei passaggi seguenti, dovrai condividere le subnet con l'account del partecipante e quindi creare il ruolo IAM e il gruppo di sicurezza nell'account del proprietario della VPC.

Quando si crea il sistema Cloud Volumes ONTAP , la NetApp Console crea automaticamente e associa un ruolo IAM al mediatore. Questo ruolo assume il ruolo IAM creato nell'account proprietario VPC per apportare modifiche alle tabelle di routing associate alla coppia HA.

Passi

1. Condividere le subnet nell'account proprietario della VPC con l'account partecipante.

   Questo passaggio è necessario per distribuire la coppia HA in subnet condivise.

   "Documentazione AWS: condividere una sottorete"

2. Nell'account proprietario VPC, creare un gruppo di sicurezza per Cloud Volumes ONTAP.

   "Fare riferimento alle regole del gruppo di sicurezza per Cloud Volumes ONTAP" . Tieni presente che non è necessario creare un gruppo di sicurezza per il mediatore HA. La Console lo fa per te.

3. Nell'account proprietario della VPC, crea un ruolo IAM che includa le seguenti autorizzazioni:

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

4. Utilizzare l'API per creare un nuovo sistema Cloud Volumes ONTAP .

   Si noti che è necessario specificare i seguenti campi:

   - "securityGroupId"

     Il campo "securityGroupId" deve specificare il gruppo di sicurezza creato nell'account proprietario della VPC (vedere il passaggio 2 sopra).

   - "assumeRoleArn" nell'oggetto "haParams"

     Il campo "assumeRoleArn" deve includere l'ARN del ruolo IAM creato nell'account proprietario della VPC (vedere il passaggio 3 sopra).

     Per esempio:

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

+
"Scopri di più sull'API Cloud Volumes ONTAP"

Configurare la creazione di gruppi di posizionamento per coppie Cloud Volumes ONTAP HA nelle singole zone di disponibilità AWS

Le distribuzioni ad alta disponibilità (HA) Cloud Volumes ONTAP nella zona di disponibilità singola (AZ) di AWS possono non riuscire e subire il rollback se la creazione

del gruppo di posizionamento non riesce. Anche la creazione del gruppo di posizionamento fallisce e la distribuzione viene annullata se il nodo Cloud Volumes ONTAP e l'istanza del mediatore non sono disponibili. Per evitare questo problema, è possibile modificare la configurazione per consentire il completamento della distribuzione anche se la creazione del gruppo di posizionamento non riesce.

Se si ignora il processo di rollback, il processo di distribuzione Cloud Volumes ONTAP viene completato correttamente e viene notificato che la creazione del gruppo di posizionamento non è completa.

Passi

1. Utilizzare SSH per connettersi all'host dell'agente NetApp Console ed effettuare l'accesso.
2. Vai a `/opt/application/netapp/cloudmanager/docker_occm/data` .
3. Modificare `app.conf` modificando il valore del `rollback-on-placement-group-failure` parametro a `false` . Il valore predefinito di questo parametro è `true` .

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

4. Salvare il file e disconnettersi dall'agente della console. Non è necessario riavviare l'agente Console.

Regole in entrata e in uscita del gruppo di sicurezza AWS per Cloud Volumes ONTAP

La NetApp Console crea gruppi di sicurezza AWS che includono le regole in entrata e in uscita di cui Cloud Volumes ONTAP ha bisogno per funzionare correttamente. Potresti voler fare riferimento alle porte per scopi di test o se preferisci utilizzare i tuoi gruppi di sicurezza.

Regole per Cloud Volumes ONTAP

Il gruppo di sicurezza per Cloud Volumes ONTAP richiede regole sia in entrata che in uscita.

Regole in entrata

Quando aggiungi un sistema Cloud Volumes ONTAP e scegli un gruppo di sicurezza predefinito, puoi scegliere di consentire il traffico all'interno di uno dei seguenti:

- **Solo VPC selezionata**: l'origine del traffico in entrata è l'intervallo di subnet della VPC per il sistema Cloud Volumes ONTAP e l'intervallo di subnet della VPC in cui risiede l'agente della console. Questa è l'opzione consigliata.
- **Tutte le VPC**: la sorgente del traffico in entrata è l'intervallo IP 0.0.0.0/0.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Ping dell'istanza
HTTP	80	Accesso HTTP alla console Web di ONTAP System Manager tramite l'indirizzo IP del LIF di gestione del cluster
HTTPS	443	Connettività con l'agente Console e accesso HTTPS alla console Web ONTAP System Manager utilizzando l'indirizzo IP del LIF di gestione del cluster
SSH	22	Accesso SSH all'indirizzo IP del LIF di gestione del cluster o di un LIF di gestione del nodo
TCP	111	Chiamata di procedura remota per NFS
TCP	139	Sessione del servizio NetBIOS per CIFS
TCP	161-162	Protocollo semplice di gestione della rete
TCP	445	Microsoft SMB/CIFS su TCP con framing NetBIOS
TCP	635	Montaggio NFS
TCP	749	Kerberos
TCP	2049	Demone del server NFS
TCP	3260	Accesso iSCSI tramite i dati iSCSI LIF
TCP	4045	Demone di blocco NFS
TCP	4046	Monitoraggio dello stato di rete per NFS
TCP	10000	Backup tramite NDMP
TCP	11104	Gestione delle sessioni di comunicazione intercluster per SnapMirror
TCP	11105	Trasferimento dati SnapMirror tramite LIF intercluster
UDP	111	Chiamata di procedura remota per NFS
UDP	161-162	Protocollo semplice di gestione della rete
UDP	635	Montaggio NFS
UDP	2049	Demone del server NFS
UDP	4045	Demone di blocco NFS
UDP	4046	Monitoraggio dello stato di rete per NFS
UDP	4049	Protocollo NFS rquotad

Regole in uscita

Il gruppo di sicurezza predefinito per Cloud Volumes ONTAP apre tutto il traffico in uscita. Se ciò è accettabile, seguite le regole di base per le comunicazioni in uscita. Se hai bisogno di regole più rigide, usa le regole in uscita avanzate.

Regole di base in uscita

Il gruppo di sicurezza predefinito per Cloud Volumes ONTAP include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Tutto il traffico in uscita
Tutti gli TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole in uscita avanzate

Se hai bisogno di regole rigide per il traffico in uscita, puoi utilizzare le seguenti informazioni per aprire solo le porte necessarie per la comunicazione in uscita da parte di Cloud Volumes ONTAP.

La sorgente è l'interfaccia (indirizzo IP) sul sistema Cloud Volumes ONTAP .

Servizio	Protocollo	Porta	Fonte	Destinazione	Scopo
Directory attiva	TCP	88	Gestione dei nodi LIF	Foresta di Active Directory	Autenticazione Kerberos V
	UDP	137	Gestione dei nodi LIF	Foresta di Active Directory	Servizio di denominazione NetBIOS
	UDP	138	Gestione dei nodi LIF	Foresta di Active Directory	Servizio datagramma NetBIOS
	TCP	139	Gestione dei nodi LIF	Foresta di Active Directory	Sessione del servizio NetBIOS
	TCP e UDP	389	Gestione dei nodi LIF	Foresta di Active Directory	LDAP
	TCP	445	Gestione dei nodi LIF	Foresta di Active Directory	Microsoft SMB/CIFS su TCP con framing NetBIOS
	TCP	464	Gestione dei nodi LIF	Foresta di Active Directory	Kerberos V cambia e imposta la password (SET_CHANGE)
	UDP	464	Gestione dei nodi LIF	Foresta di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	Gestione dei nodi LIF	Foresta di Active Directory	Kerberos V modifica e imposta password (RPCSEC_GSS)
	TCP	88	Dati LIF (NFS, CIFS, iSCSI)	Foresta di Active Directory	Autenticazione Kerberos V
	UDP	137	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Servizio di denominazione NetBIOS
	UDP	138	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Servizio datagramma NetBIOS
	TCP	139	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Sessione del servizio NetBIOS
	TCP e UDP	389	Dati LIF (NFS, CIFS)	Foresta di Active Directory	LDAP
	TCP	445	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Microsoft SMB/CIFS su TCP con framing NetBIOS
	TCP	464	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Kerberos V cambia e imposta la password (SET_CHANGE)
	UDP	464	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	Dati LIF (NFS, CIFS)	Foresta di Active Directory	Kerberos V modifica e imposta password (RPCSEC_GSS)

Servizio	Protocollo	Porta	Fonte	Destinazione	Scopo
AutoSupport	HTTPS	443	Gestione dei nodi LIF	mysupport.netapp.com	AutoSupport (HTTPS è l'impostazione predefinita)
	HTTP	80	Gestione dei nodi LIF	mysupport.netapp.com	AutoSupport (solo se il protocollo di trasporto viene modificato da HTTPS a HTTP)
	TCP	3128	Gestione dei nodi LIF	Agente console	Invio di messaggi AutoSupport tramite un server proxy sull'agente Console, se non è disponibile una connessione Internet in uscita
Backup su S3	TCP	5010	Intercluster LIF	Backup dell'endpoint o ripristino dell'endpoint	Operazioni di backup e ripristino per la funzionalità Backup su S3
Grappolo	Tutto il traffico	Tutto il traffico	Tutti i LIF su un nodo	Tutti i LIF sull'altro nodo	Comunicazioni intercluster (solo Cloud Volumes ONTAP HA)
	TCP	3000	Gestione dei nodi LIF	Mediatore HA	Chiamate ZAPI (Cloud Volumes ONTAP HA)
	ICMP	1	Gestione dei nodi LIF	Mediatore HA	Mantieni attivo (Cloud Volumes ONTAP HA)
Backup di configurazione	HTTP	80	Gestione dei nodi LIF	http://<indirizzo-IP-agente-console>/occm/offboxconfig	Inviare i backup della configurazione all'agente della console."Documentazione ONTAP"
DHCP	UDP	68	Gestione dei nodi LIF	DHCP	Client DHCP per la prima configurazione
DHCP	UDP	67	Gestione dei nodi LIF	DHCP	server DHCP
DNS	UDP	53	Gestione dei nodi LIF e dati LIF (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	Gestione dei nodi LIF	Server di destinazione	Copia NDMP
SMTP	TCP	25	Gestione dei nodi LIF	Server di posta	Avvisi SMTP, possono essere utilizzati per AutoSupport

Servizio	Protocollo	Porta	Fonte	Destinazione	Scopo
SNMP	TCP	161	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
	UDP	161	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
	TCP	162	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
	UDP	162	Gestione dei nodi LIF	Monitorare il server	Monitoraggio tramite trappole SNMP
SnapMirror	TCP	11104	Intercluster LIF	LIF intercluster ONTAP	Gestione delle sessioni di comunicazione intercluster per SnapMirror
	TCP	11105	Intercluster LIF	LIF intercluster ONTAP	Trasferimento dati SnapMirror
Registro di sistema	UDP	514	Gestione dei nodi LIF	Server Syslog	Messaggi di inoltro Syslog

Regole per il gruppo di sicurezza esterno del mediatore HA

Il gruppo di sicurezza esterno predefinito per il mediatore Cloud Volumes ONTAP HA include le seguenti regole in entrata e in uscita.

Regole in entrata

Il gruppo di sicurezza predefinito per il mediatore HA include la seguente regola in ingresso.

Protocollo	Porta	Fonte	Scopo
TCP	3000	CIDR dell'agente della console	Accesso API RESTful dall'agente Console

Regole in uscita

Il gruppo di sicurezza predefinito per il mediatore HA apre tutto il traffico in uscita. Se ciò è accettabile, seguite le regole di base per le comunicazioni in uscita. Se hai bisogno di regole più rigide, usa le regole in uscita avanzate.

Regole di base in uscita

Il gruppo di sicurezza predefinito per il mediatore HA include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutti gli TCP	Tutto	Tutto il traffico in uscita
Tutti gli UDP	Tutto	Tutto il traffico in uscita

Regole in uscita avanzate

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte necessarie per la comunicazione in uscita da parte del mediatore HA.

Protocollo	Porta	Destinazione	Scopo
HTTP	80	Indirizzo IP dell'agente della console sull'istanza AWS EC2	Scarica gli aggiornamenti per il mediatore
HTTPS	443	ec2.amazonaws.com	Assistenza con il failover dell'archiviazione
UDP	53	ec2.amazonaws.com	Assistenza con il failover dell'archiviazione

Invece di aprire le porte 443 e 53, è possibile creare un endpoint VPC di interfaccia dalla subnet di destinazione al servizio AWS EC2.

Regole per il gruppo di sicurezza interno della configurazione HA

Il gruppo di sicurezza interno predefinito per una configurazione Cloud Volumes ONTAP HA include le seguenti regole. Questo gruppo di sicurezza consente la comunicazione tra i nodi HA e tra il mediatore e i nodi.

La Console crea sempre questo gruppo di sicurezza. Non hai la possibilità di usare il tuo.

Regole in entrata

Il gruppo di sicurezza predefinito include le seguenti regole in entrata.

Protocollo	Porta	Scopo
Tutto il traffico	Tutto	Comunicazione tra il mediatore HA e i nodi HA

Regole in uscita

Il gruppo di sicurezza predefinito include le seguenti regole in uscita.

Protocollo	Porta	Scopo
Tutto il traffico	Tutto	Comunicazione tra il mediatore HA e i nodi HA

Regole per l'agente della console

"Visualizza le regole del gruppo di sicurezza per l'agente della console"

Informazioni sul copyright

Informazioni sul marchio commerciale