Configurare la rete

Cloud Volumes ONTAP

NetApp
April 23, 2024

This PDF was generated from https://docs.netapp.com/it-it/bluexp-cloud-volumes-ontap/reference-networking-aws.html on April 23, 2024. Always check docs.netapp.com for the latest.

Sommario

Configurare la rete

Requisiti di rete per Cloud Volumes ONTAP in AWS

BlueXP gestisce la configurazione dei componenti di rete per Cloud Volumes ONTAP, come indirizzi IP, netmask e route. È necessario assicurarsi che sia disponibile l'accesso a Internet in uscita, che siano disponibili indirizzi IP privati sufficienti, che siano disponibili le connessioni corrette e altro ancora.

Requisiti generali

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 NetApp AutoSupport, che monitora in modo proattivo lo stato di salute del sistema e invia messaggi al supporto tecnico NetApp.

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

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.

Se non è disponibile una connessione Internet in uscita per l'invio di messaggi AutoSupport, BlueXP configura automaticamente i sistemi Cloud Volumes ONTAP in modo che utilizzino il connettore come server proxy. L'unico requisito è garantire che il gruppo di sicurezza del connettore consenta connessioni *inbound* sulla porta 3128. Dopo aver implementato il connettore, aprire questa porta.

Se sono state definite rigide regole in uscita per Cloud Volumes ONTAP, è necessario anche assicurarsi che il gruppo di sicurezza Cloud Volumes ONTAP consenta connessioni *in uscita* sulla porta 3128.

Dopo aver verificato che l'accesso a Internet in uscita è disponibile, è possibile testare AutoSupport per assicurarsi che sia in grado di inviare messaggi. Per istruzioni, fare riferimento a. "Documenti ONTAP: Configurazione di AutoSupport".

Se BlueXP notifica che non è possibile inviare messaggi AutoSupport, "Risolvere i problemi della configurazione AutoSupport".

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)".

Indirizzi IP privati

BlueXP 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 allocati da BlueXP per Cloud Volumes ONTAP dipende dalla distribuzione di un sistema a nodo singolo o di una coppia ha. LIF è un indirizzo IP associato a una porta fisica.

Indirizzi IP per un sistema a nodo singolo

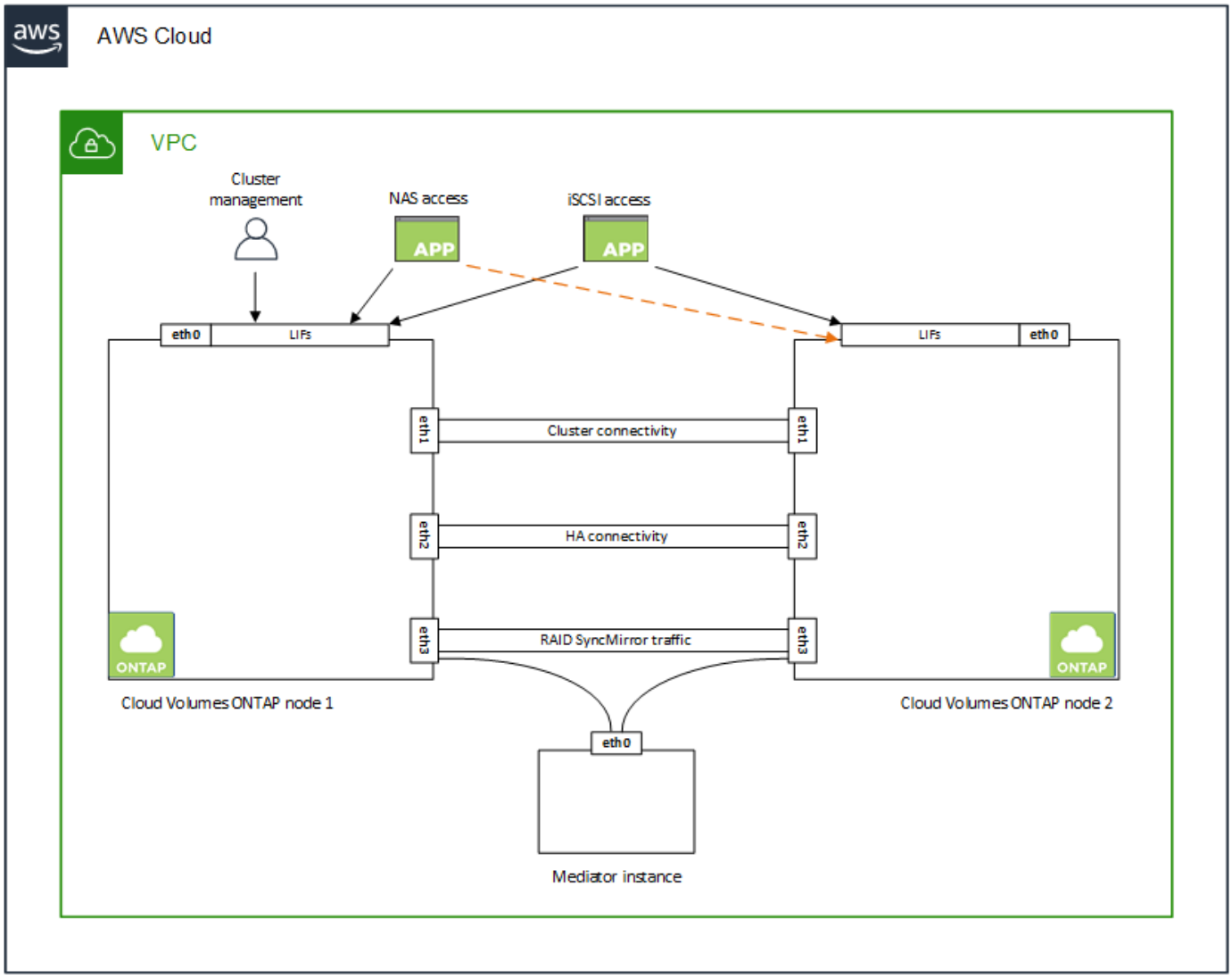
BlueXP assegna 6 indirizzi IP a un sistema a nodo singolo.

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

LIF	Scopo
Gestione del cluster	Gestione amministrativa dell'intero cluster (coppia ha).
Gestione dei nodi	Gestione amministrativa di un nodo.
Intercluster	Comunicazione tra cluster, backup e replica.
Dati NAS	Accesso client tramite protocolli NAS.
Dati iSCSI	Accesso del client tramite il protocollo iSCSI. Utilizzato anche dal sistema per altri importanti flussi di lavoro di rete. Questa LIF è obbligatoria e non deve essere eliminata.
Gestione delle macchine virtuali dello storage	Una LIF di gestione delle macchine virtuali dello storage viene utilizzata 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 implementazione scelto. Una coppia ha implementata in una *singola* AWS Availability zone (AZ) richiede 15 indirizzi IP privati, mentre una coppia ha implementata in *multiple* AZS richiede 13 indirizzi IP privati.

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

LIF per coppie ha in un singolo AZ

LIF	Interfaccia	Nodo	Scopo
Gestione del 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 tra cluster, backup e replica.
Dati NAS	eth0	nodo 1	Accesso client tramite protocolli NAS.

LIF	Interfaccia	Nodo	Scopo
Dati iSCSI	eth0	nodo 1 e nodo 2	Accesso del client tramite il protocollo iSCSI. Utilizzato anche dal sistema per altri importanti flussi di lavoro di rete. Questi LIF sono obbligatori e non devono essere cancellati.
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 assistere nei processi di acquisizione e giveback dello storage.

LIF per coppie ha in più AZS

LIF	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 tra cluster, backup e replica.
Dati iSCSI	eth0	nodo 1 e nodo 2	Accesso del client tramite il protocollo iSCSI. Queste LIF gestiscono anche la migrazione di indirizzi IP mobili tra nodi. Questi LIF sono obbligatori e non devono essere cancellati.
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 assistere nei processi di acquisizione e giveback dello storage.

Quando viene implementato in più zone di disponibilità, vengono associate diverse LIF "Indirizzi IP mobili", Che non contano rispetto al limite IP privato AWS.

Gruppi di sicurezza

Non è necessario creare gruppi di sicurezza perché BlueXP fa questo per te. Se è necessario utilizzare il proprio, fare riferimento a. "Regole del gruppo di sicurezza".

Cerchi informazioni sul connettore? "Visualizzare le regole del gruppo di protezione per il connettore"

Connessione 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 ai sistemi ONTAP

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 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".

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 le subnet con altri account AWS. Per utilizzare questa configurazione, è necessario configurare l'ambiente AWS e implementare la coppia ha utilizzando l'API.

"Scopri come implementare una coppia ha in una subnet condivisa".

Requisiti per coppie 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 BlueXP quando si crea l'ambiente di lavoro.

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.

In ciascuna zona di disponibilità dovrebbe essere disponibile una subnet.

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".

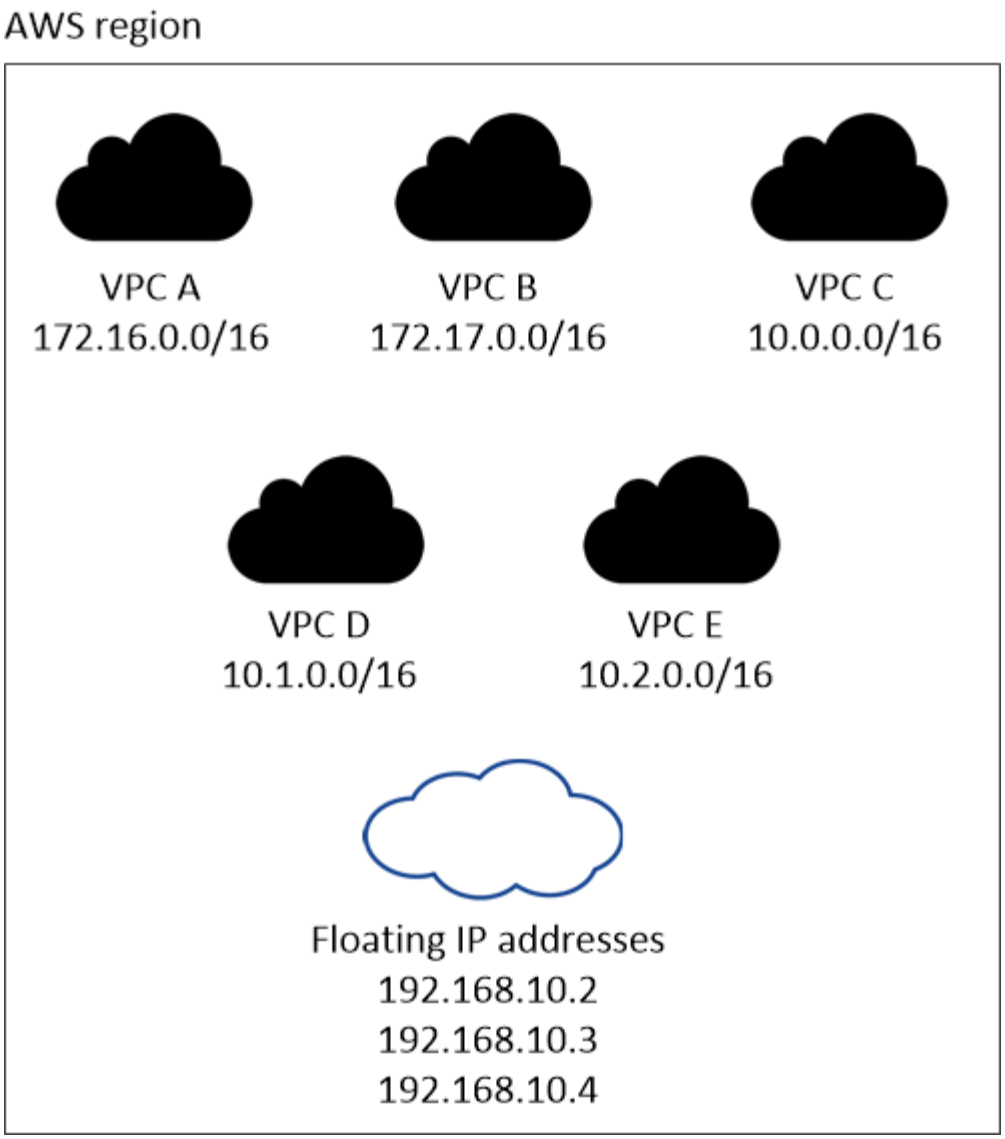
Un indirizzo IP mobile è per la gestione del cluster, uno per i dati NFS/CIFS sul nodo 1 e uno per i dati NFS/CIFS sul nodo 2. Un quarto indirizzo IP mobile per la gestione SVM è opzionale.

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

Quando si crea un ambiente di lavoro Cloud Volumes ONTAP ha, è necessario inserire gli indirizzi IP mobili in BlueXP. BlueXP 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.



BlueXP 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

Se necessario, "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 BlueXP, viene richiesto di 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), BlueXP 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".

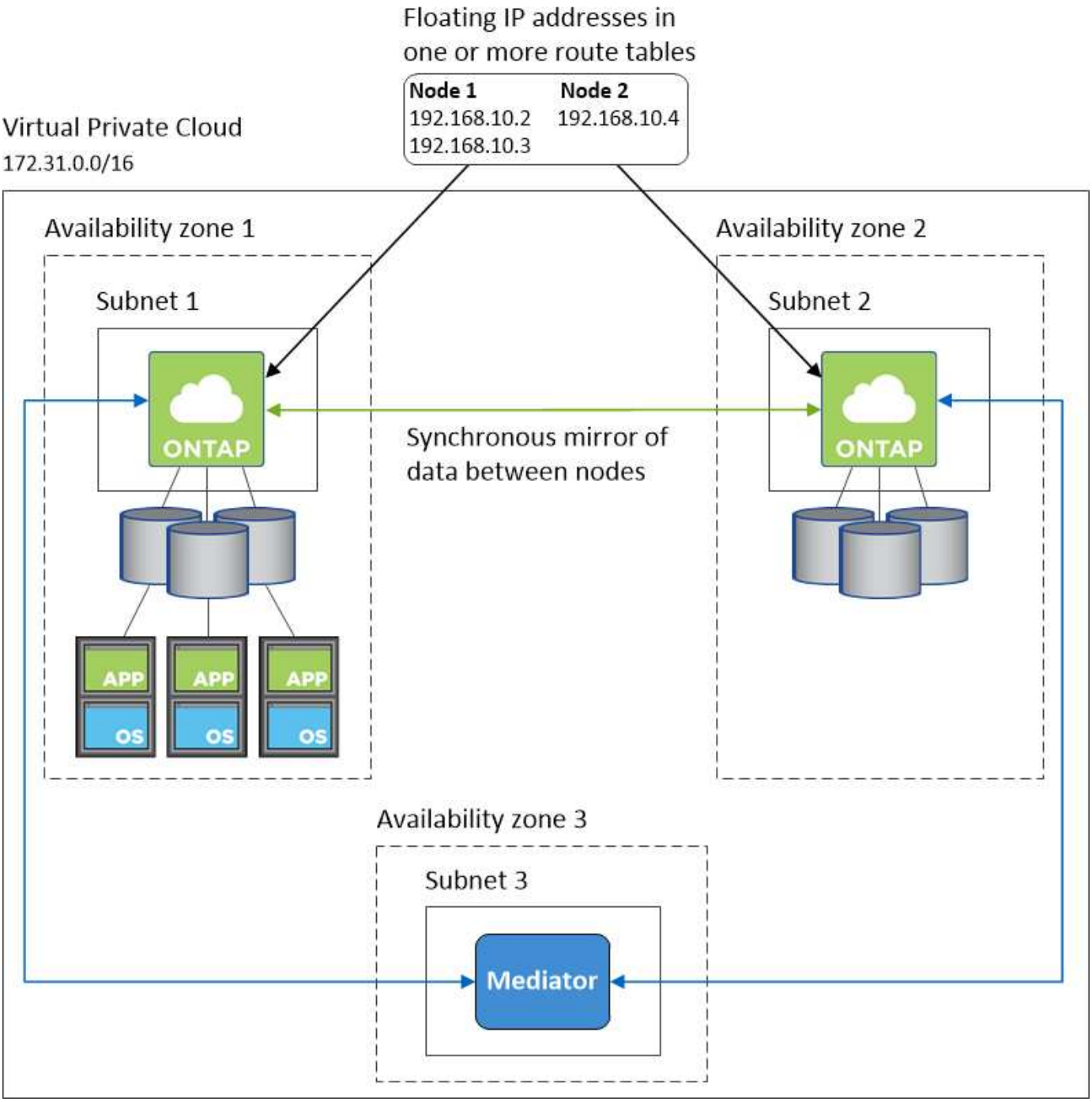
Connessione ai tool di gestione NetApp

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.

Esempio di configurazione ha

La seguente immagine illustra i componenti di rete specifici di una coppia ha in più AZS: Tre zone di disponibilità, tre subnet, indirizzi IP mobili e una tabella di routing.



Requisiti per il connettore

Se non hai ancora creato un connettore, dovresti rivedere anche i requisiti di rete per il connettore.

- "Visualizzare i requisiti di rete per il connettore"
- "Regole del gruppo di sicurezza in AWS"

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

Configurare un gateway di transito AWS per consentire l'accesso a una coppia ha

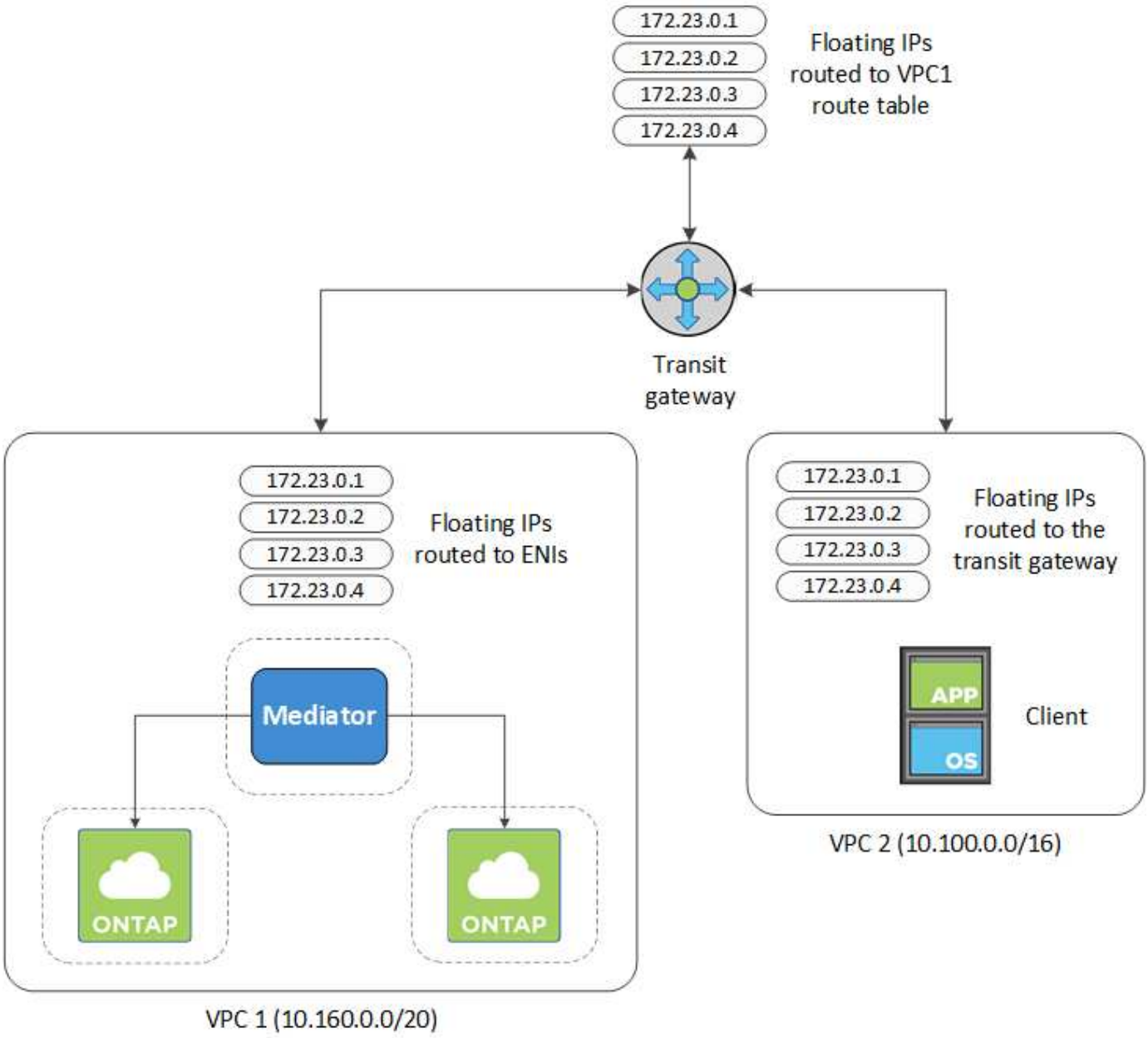
"Indirizzi IP mobili" Dall'esterno del VPC in cui risiede la coppia ha.

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.

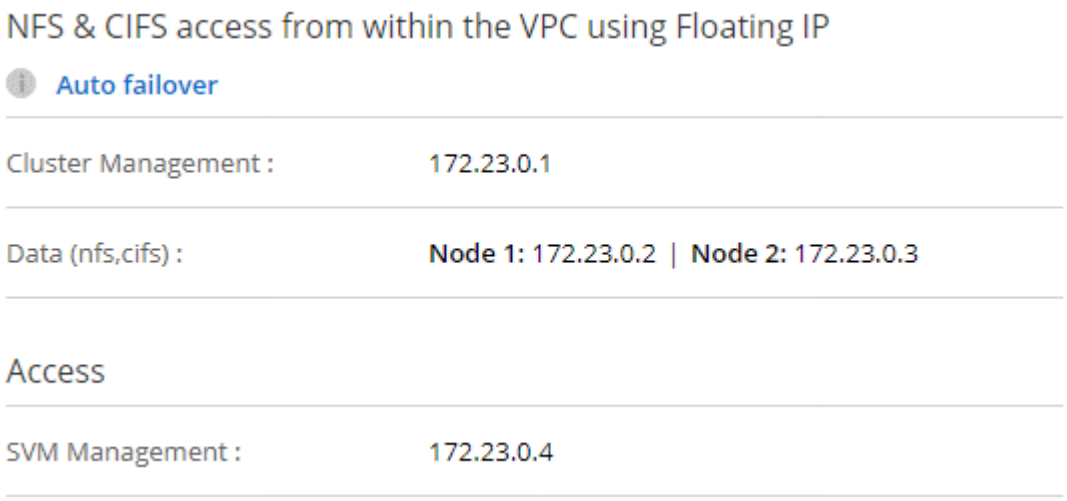


La seguente procedura illustra come configurare una configurazione simile.

Fasi

1. "Creare un gateway di transito e collegare i VPC al gateway".
2. Associare i VPC alla tabella di routing del gateway di transito.
   a. Nel servizio **VPC**, fare clic su **Transit Gateway Route Table**.
   b. Selezionare la tabella dei percorsi.
   c. Fare clic su **Associazioni**, quindi selezionare **Crea associazione**.
   d. Scegliere gli allegati (i VPC) da associare, quindi fare clic su **Crea associazione**.
3. 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 BlueXP. Ecco un esempio:



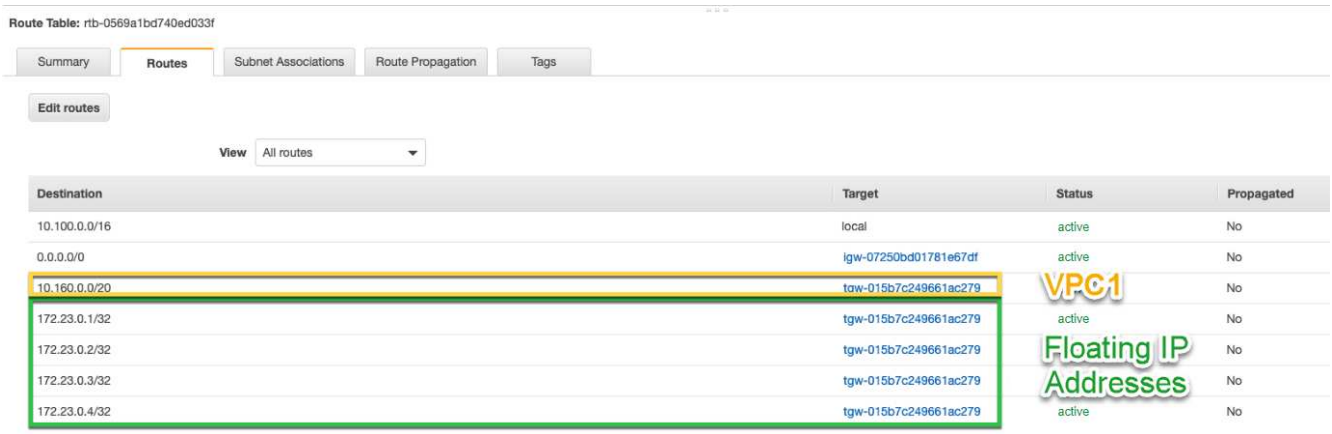
   L'immagine di esempio seguente mostra la tabella di percorso per il gateway di transito. Include le route ai blocchi CIDR dei due VPC e quattro indirizzi IP mobili utilizzati da Cloud Volumes ONTAP.

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

a. Aggiungere voci di routing agli indirizzi IP mobili.

b. Aggiungere una voce di percorso al blocco CIDR del VPC in cui risiede la coppia ha.

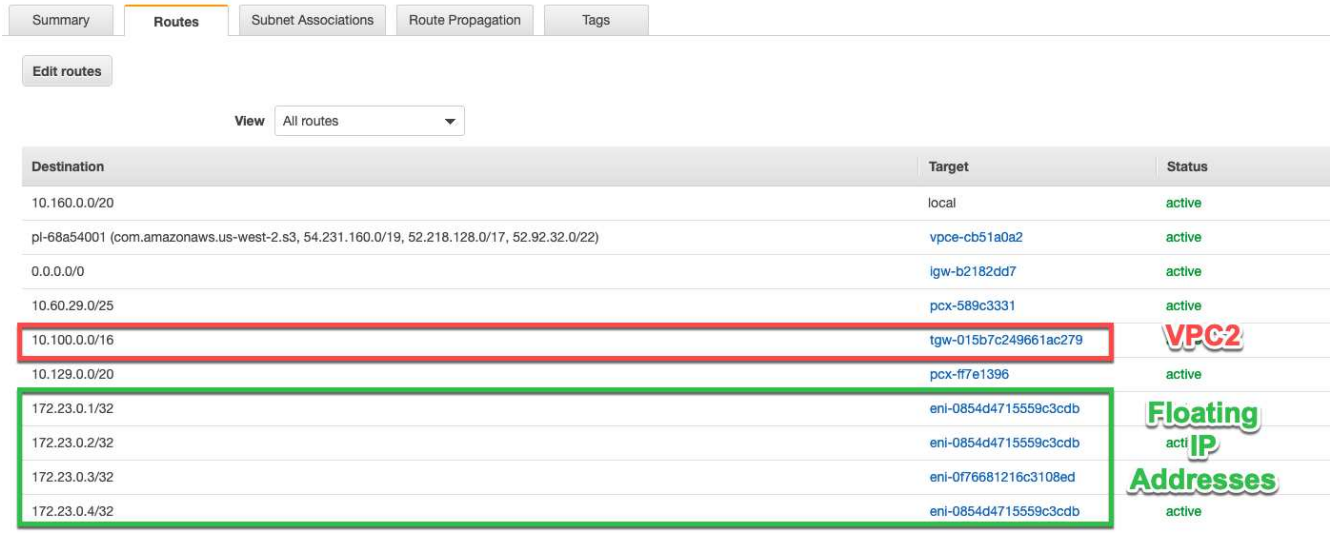
   L'immagine di esempio seguente mostra la tabella di routing per VPC 2, che include i percorsi verso VPC 1 e gli indirizzi IP mobili.



5. 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. BlueXP ha aggiunto automaticamente gli IP mobili alla tabella di routing quando ha implementato la coppia ha.



6. Aggiornare le impostazioni dei gruppi di protezione a tutto il traffico per il VPC.

   a. In Virtual Private Cloud, fare clic su **subnet**.

   b. Fare clic sulla scheda **Tabella di instradamento**, 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**.

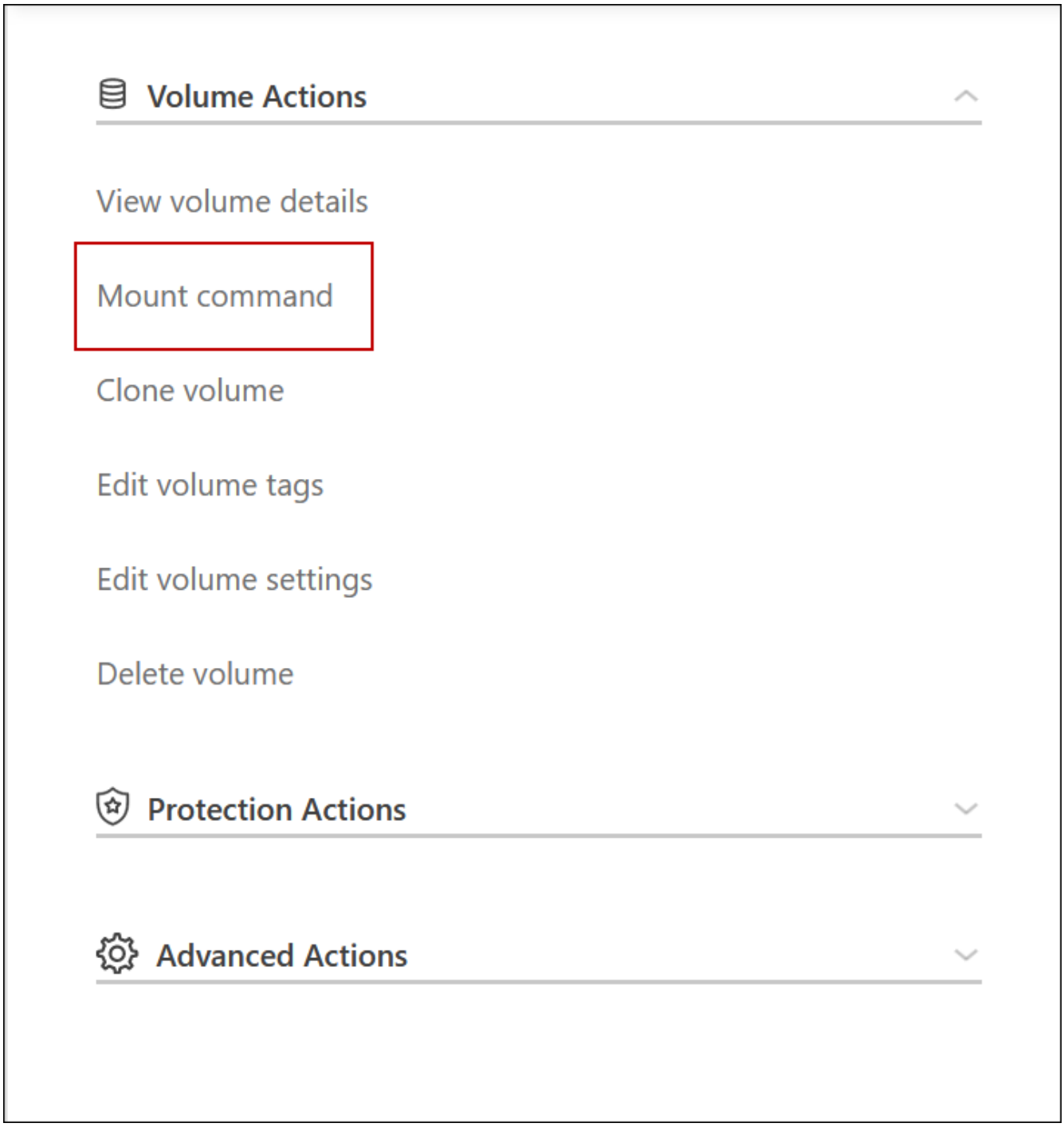
e. Fare clic su **Aggiungi regola**.

f. In tipo, selezionare **tutto il traffico**, quindi selezionare 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 in BlueXP tramite l'opzione **Mount Command** nel pannello Manage Volumes (Gestisci volumi) di BlueXP.



8. Se si sta montando un volume NFS, configurare il criterio 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"

Implementare una coppia ha in una subnet condivisa

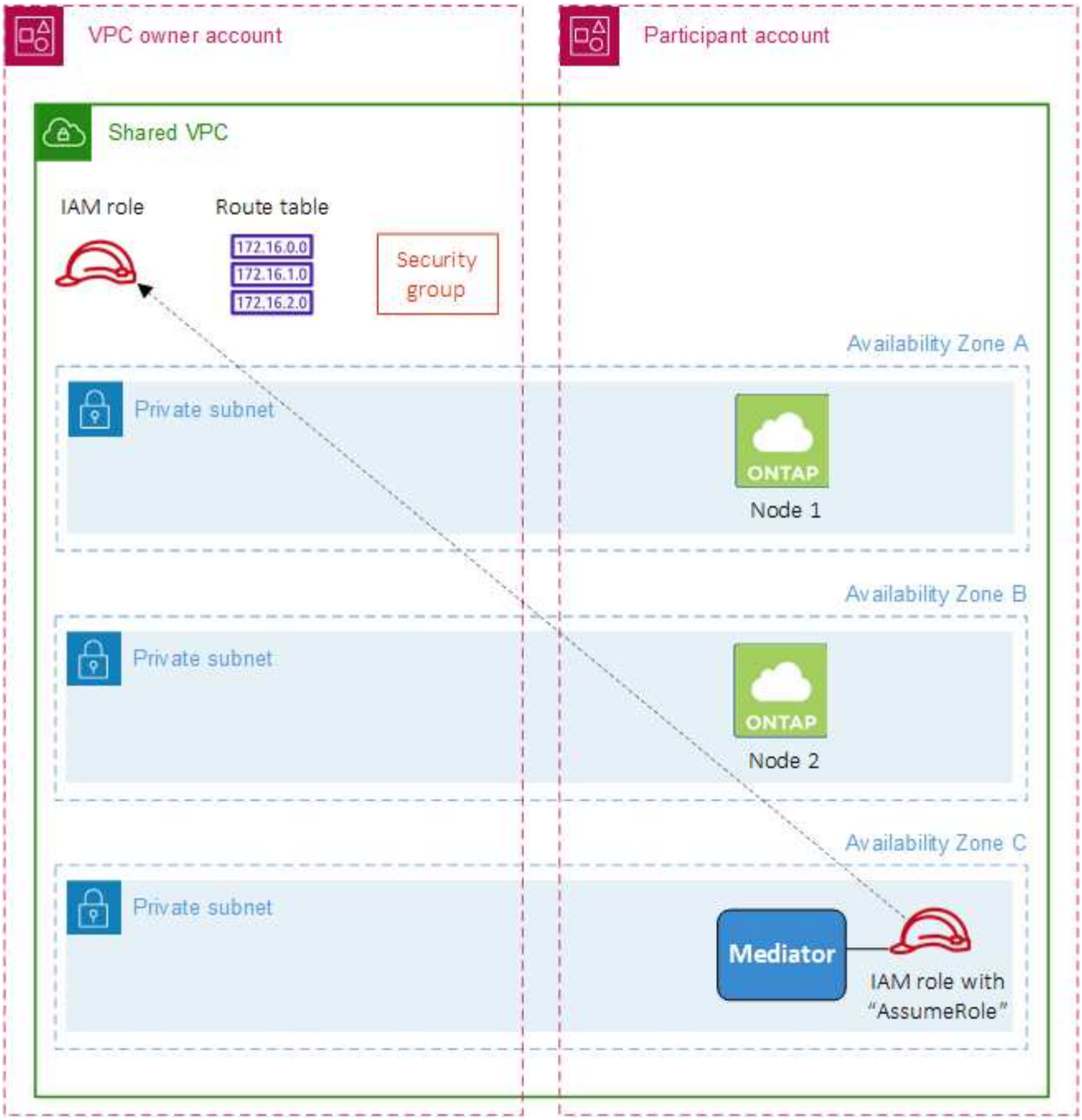
A partire dalla versione 9.11.1, le coppie Cloud Volumes ONTAP ha sono supportate in AWS con condivisione VPC. La condivisione VPC consente alla tua organizzazione di condividere le subnet con altri account AWS. Per utilizzare questa configurazione, è necessario configurare l'ambiente AWS e implementare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

Con "Condivisione VPC", Una configurazione Cloud Volumes ONTAP ha è distribuita su due account:

- L'account proprietario del VPC, proprietario della rete (VPC, subnet, tabelle di routing e gruppo di protezione Cloud Volumes ONTAP)
- L'account partecipante, in cui le istanze EC2 vengono implementate in subnet condivise (inclusi i due nodi ha e il mediatore)

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

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



Come descritto nella procedura riportata di seguito, è necessario condividere le subnet con l'account partecipante, quindi creare il ruolo IAM e il gruppo di protezione nell'account proprietario VPC.

Quando si crea l'ambiente di lavoro Cloud Volumes ONTAP, BlueXP crea e associa automaticamente un ruolo IAM al mediatore. Questo ruolo assume il ruolo IAM creato nell'account proprietario del VPC per apportare modifiche alle tabelle di routing associate alla coppia ha.

Fasi

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

   Questa fase è necessaria per implementare la coppia ha in subnet condivise.

   "Documentazione AWS: Consente di condividere una subnet"

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

   "Fare riferimento alle regole del gruppo di sicurezza per Cloud Volumes ONTAP". Tenere presente che non è necessario creare un gruppo di sicurezza per il mediatore ha. BlueXP fa questo per te.

3. Nell'account proprietario del VPC, creare 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 BlueXP per creare un nuovo ambiente di lavoro Cloud Volumes ONTAP.

   Si noti che è necessario specificare i seguenti campi:

   - "SecurityGroupId"

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

   - "AssumeRoleArn" nell'oggetto "haParams"

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

     Ad esempio:

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

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

Regole del gruppo di sicurezza per AWS

BlueXP crea gruppi di sicurezza AWS che includono le regole in entrata e in uscita di cui Cloud Volumes ONTAP ha bisogno per funzionare correttamente. Si consiglia di fare riferimento alle porte a scopo di test o se si preferisce utilizzare i propri gruppi di protezione.

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 si crea un ambiente di lavoro e si sceglie un gruppo di protezione predefinito, è possibile scegliere di consentire il traffico all'interno di una delle seguenti opzioni:

- **Selezionato solo VPC**: L'origine del traffico in entrata è l'intervallo di sottorete del VPC per il sistema Cloud Volumes ONTAP e l'intervallo di sottorete del VPC in cui si trova il connettore. Questa è l'opzione consigliata.
- **Tutti i VPC**: L'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.

Protocollo	Porta	Scopo
Tutti gli ICMP	Tutto	Eseguire il ping dell'istanza
HTTP	80	Accesso HTTP alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
HTTPS	443	Connettività con il connettore e accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
SSH	22	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
TCP	111	Chiamata a procedura remota per NFS
TCP	139	Sessione del servizio NetBIOS per CIFS
TCP	161-162	Protocollo di gestione di rete semplice
TCP	445	Microsoft SMB/CIFS su TCP con frame NetBIOS
TCP	635	Montaggio NFS
TCP	749	Kerberos
TCP	2049	Daemon del server NFS
TCP	3260	Accesso iSCSI tramite LIF dei dati iSCSI
TCP	4045	Daemon di blocco NFS
TCP	4046	Network status monitor per NFS
TCP	10000	Backup con NDMP
TCP	11104	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
TCP	11105	Trasferimento dei dati SnapMirror con LIF intercluster
UDP	111	Chiamata a procedura remota per NFS
UDP	161-162	Protocollo di gestione di rete semplice
UDP	635	Montaggio NFS
UDP	2049	Daemon del server NFS

Protocollo	Porta	Scopo
UDP	4045	Daemon di blocco NFS
UDP	4046	Network status monitor per NFS
UDP	4049	Protocollo NFS rquotad

Regole in uscita

Il gruppo di protezione predefinito per Cloud Volumes ONTAP apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

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

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

Regole avanzate in uscita

Se sono necessarie regole rigide per il traffico in uscita, è possibile utilizzare le seguenti informazioni per aprire solo le porte richieste per le comunicazioni in uscita da Cloud Volumes ONTAP.

L'origine è l'interfaccia (indirizzo IP) del sistema Cloud Volumes ONTAP.

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
Active Directory	TCP	88	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	UDP	137	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	TCP	139	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP E UDP	389	LIF di gestione dei nodi	Insieme di strutture di Active Directory	LDAP
	TCP	445	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	UDP	464	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	LIF di gestione dei nodi	Insieme di strutture di Active Directory	Kerberos V change & set Password (RPCSEC_GSS)
	TCP	88	Data LIF (NFS, CIFS, iSCSI)	Insieme di strutture di Active Directory	Autenticazione Kerberos V.
	UDP	137	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio nomi NetBIOS
	UDP	138	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Servizio datagramma NetBIOS
	TCP	139	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Sessione del servizio NetBIOS
	TCP E UDP	389	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	LDAP
	TCP	445	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Microsoft SMB/CIFS su TCP con frame NetBIOS
	TCP	464	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (SET_CHANGE)
	UDP	464	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Amministrazione delle chiavi Kerberos
	TCP	749	LIF DATI (NFS, CIFS)	Insieme di strutture di Active Directory	Kerberos V change & set password (RPCSEC_GSS)

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
AutoSupport	HTTPS	443	LIF di gestione dei nodi	support.netapp.com	AutoSupport (HTTPS è l'impostazione predefinita)
	HTTP	80	LIF di gestione dei nodi	support.netapp.com	AutoSupport (solo se il protocollo di trasporto viene modificato da HTTPS a HTTP)
	TCP	3128	LIF di gestione dei nodi	Connettore	Invio di messaggi AutoSupport tramite un server proxy sul connettore, se non è disponibile una connessione Internet in uscita
Backup su S3	TCP	5010	LIF intercluster	Endpoint di backup o endpoint di ripristino	Operazioni di backup e ripristino per la funzione Backup in S3
Cluster	Tutto il traffico	Tutto il traffico	Tutte le LIF su un nodo	Tutte le LIF sull'altro nodo	Comunicazioni tra cluster (solo Cloud Volumes ONTAP ha)
	TCP	3000	LIF di gestione dei nodi	MEDIATORE HA	Chiamate ZAPI (solo Cloud Volumes ONTAP ha)
	ICMP	1	LIF di gestione dei nodi	MEDIATORE HA	Mantieni attivo (solo Cloud Volumes ONTAP ha)
Backup della configurazione	HTTP	80	LIF di gestione dei nodi	Http://<connector-IP-address>/occm/offboxconfig	Inviare i backup della configurazione al connettore. "Informazioni sui file di backup della configurazione".
DHCP	UDP	68	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione
DHCPS	UDP	67	LIF di gestione dei nodi	DHCP	Server DHCP
DNS	UDP	53	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600–18699	LIF di gestione dei nodi	Server di destinazione	Copia NDMP
SMTP	TCP	25	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
SNMP	TCP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	161	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	TCP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	UDP	162	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
SnapMirror	TCP	11104	LIF intercluster	ONTAP Intercluster LIF	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
	TCP	11105	LIF intercluster	ONTAP Intercluster LIF	Trasferimento dei dati SnapMirror
Syslog	UDP	514	LIF di gestione dei nodi	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 inbound.

Protocollo	Porta	Origine	Scopo
TCP	3000	CIDR del connettore	Accesso API RESTful dal connettore

Regole in uscita

Il gruppo di sicurezza predefinito per il mediatore ha apre tutto il traffico in uscita. Se questo è accettabile, attenersi alle regole di base per le chiamate in uscita. Se sono necessarie regole più rigide, utilizzare le regole avanzate in uscita.

Regole di base in uscita

Il gruppo di protezione predefinito per il mediatore ha include le seguenti regole in uscita.

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

Regole avanzate in uscita

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 dal mediatore ha.

Protocollo	Porta	Destinazione	Scopo
HTTP	80	Indirizzo IP del connettore sull'istanza AWS EC2	Scarica gli aggiornamenti per il mediatore
HTTPS	443	ec2.amazonaws.com	Assistenza per il failover dello storage
UDP	53	ec2.amazonaws.com	Assistenza per il failover dello storage

Anziché 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 protezione 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.

BlueXP crea sempre questo gruppo di protezione. Non hai la possibilità di utilizzare 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 protezione 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 il connettore

"Visualizzare le regole del gruppo di protezione per il connettore"

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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.