Inizia con Amazon Web Services

Cloud Volumes ONTAP

NetApp
April 23, 2024

Sommario

Inizia con Amazon Web Services

Avvio rapido di Cloud Volumes ONTAP in AWS

Inizia a utilizzare Cloud Volumes ONTAP in AWS in pochi passaggi.

1 Creare un connettore

Se non si dispone di un "Connettore" Tuttavia, un amministratore dell'account deve crearne uno. "Scopri come creare un connettore in AWS"

Se si desidera implementare Cloud Volumes ONTAP in una subnet in cui non è disponibile alcun accesso a Internet, è necessario installare manualmente il connettore e accedere all'interfaccia utente di BlueXP in esecuzione su tale connettore. "Scopri come installare manualmente il connettore in una posizione senza accesso a Internet"

2 Pianificare la configurazione

BlueXP offre pacchetti preconfigurati che soddisfano i requisiti del carico di lavoro, oppure è possibile creare una configurazione personalizzata. Se si sceglie una configurazione personalizzata, è necessario comprendere le opzioni disponibili. "Scopri di più".

3 Configurare la rete

1. Assicurarsi che il VPC e le subnet supportino la connettività tra il connettore e Cloud Volumes ONTAP.
2. Abilitare l'accesso a Internet in uscita dal VPC di destinazione per NetApp AutoSupport.

   Questo passaggio non è necessario se si implementa Cloud Volumes ONTAP in una posizione in cui non è disponibile alcun accesso a Internet.

3. Impostare un endpoint VPC sul servizio S3.

   È necessario un endpoint VPC se si desidera eseguire il tiering dei dati cold da Cloud Volumes ONTAP a uno storage a oggetti a basso costo.

"Scopri di più sui requisiti di rete".

4 Configurare AWS KMS

Se si desidera utilizzare la crittografia Amazon con Cloud Volumes ONTAP, è necessario assicurarsi che esista una chiave master cliente (CMK) attiva. È inoltre necessario modificare il criterio delle chiavi per ogni CMK aggiungendo il ruolo IAM che fornisce le autorizzazioni al connettore come *utente chiave*. "Scopri di più".

5 Avviare Cloud Volumes ONTAP utilizzando BlueXP

Fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro), selezionare il tipo di sistema che si desidera implementare e completare la procedura guidata. "Leggi le istruzioni dettagliate".

Link correlati

- "Creazione di un connettore da BlueXP"
- "Avvio di un connettore da AWS Marketplace"
- "Installazione del software del connettore su un host Linux"
- "Cosa fa BlueXP con le autorizzazioni AWS"

Pianificare la configurazione di Cloud Volumes ONTAP in AWS

Quando si implementa Cloud Volumes ONTAP in AWS, è possibile scegliere un sistema preconfigurato che soddisfi i requisiti del carico di lavoro oppure creare una configurazione personalizzata. Se si sceglie una configurazione personalizzata, è necessario comprendere le opzioni disponibili.

Scegliere una licenza Cloud Volumes ONTAP

Per Cloud Volumes ONTAP sono disponibili diverse opzioni di licenza. Ciascuna opzione consente di scegliere un modello di consumo che soddisfi le proprie esigenze.

- "Scopri le opzioni di licenza per Cloud Volumes ONTAP"
- "Scopri come impostare le licenze"

Scegliere una regione supportata

Cloud Volumes ONTAP è supportato nella maggior parte delle regioni AWS. "Visualizza l'elenco completo delle regioni supportate".

Prima di poter creare e gestire le risorse in tali regioni, è necessario abilitare le regioni AWS più recenti. "Scopri come abilitare una regione".

Scegliere un'istanza supportata

Cloud Volumes ONTAP supporta diversi tipi di istanze, a seconda del tipo di licenza scelto.

"Configurazioni supportate per Cloud Volumes ONTAP in AWS"

Comprendere i limiti dello storage

Il limite di capacità raw per un sistema Cloud Volumes ONTAP è legato alla licenza. Ulteriori limiti influiscono sulle dimensioni degli aggregati e dei volumi. Durante la pianificazione della configurazione, è necessario conoscere questi limiti.

"Limiti di storage per Cloud Volumes ONTAP in AWS"

Dimensionare il sistema in AWS

Il dimensionamento del sistema Cloud Volumes ONTAP può aiutarti a soddisfare i requisiti di performance e capacità. Quando si sceglie un tipo di istanza, un tipo di disco e una dimensione del disco, è necessario tenere presenti alcuni punti chiave:

Tipo di istanza

- Abbina i requisiti di carico di lavoro al throughput massimo e agli IOPS per ogni tipo di istanza EC2.
- Se diversi utenti scrivono nel sistema contemporaneamente, scegliere un tipo di istanza con CPU sufficienti per gestire le richieste.
- Se si dispone di un'applicazione in gran parte in lettura, scegliere un sistema con una quantità di RAM sufficiente.
  - "Documentazione AWS: Tipi di istanze Amazon EC2"
  - "Documentazione AWS: Istanze ottimizzate per Amazon EBS"

Tipo di disco EBS

Ad un livello elevato, le differenze tra i tipi di dischi EBS sono le seguenti. Per ulteriori informazioni sui casi di utilizzo dei dischi EBS, fare riferimento a. "Documentazione AWS: Tipi di volume EBS".

- I dischi *General Purpose SSD (gp3)* sono gli SSD più economici che bilanciano costi e performance per un'ampia gamma di carichi di lavoro. Le performance sono definite in termini di IOPS e throughput. I dischi gp3 sono supportati con Cloud Volumes ONTAP 9.7 e versioni successive.

  Quando si seleziona un disco gp3, BlueXP inserisce i valori di IOPS e throughput predefiniti che forniscono prestazioni equivalenti a un disco gp2 in base alle dimensioni del disco selezionato. È possibile aumentare i valori per ottenere performance migliori a un costo maggiore, ma non supportiamo valori più bassi perché possono portare a performance inferiori. In breve, attenersi ai valori predefiniti o aumentarli. Non abbassarli. "Scopri di più sui dischi gp3 e sulle loro performance".

  Si noti che Cloud Volumes ONTAP supporta la funzione EBS di Amazon Elastic Volumes con i dischi gp3. "Scopri di più sul supporto di Elastic Volumes".

- *I dischi SSD General Purpose (gp2)* bilanciano costi e performance per un'ampia gamma di carichi di lavoro. Le performance sono definite in termini di IOPS.
- I dischi *IOPS SSD (io1)* forniti sono destinati ad applicazioni critiche che richiedono le massime performance a un costo superiore.

  Nota: Cloud Volumes ONTAP supporta la funzione Amazon EBS Elastic Volumes con dischi io1. "Scopri di più sul supporto di Elastic Volumes".

- I dischi *HDD ottimizzati per il throughput (st1)* sono per i carichi di lavoro ad accesso frequente che richiedono un throughput rapido e coerente a un prezzo inferiore.

  > Si sconsiglia di eseguire il tiering dei dati sullo storage a oggetti quando si utilizzano HDD ottimizzati per il throughput (st1).

Dimensione del disco EBS

Se si sceglie una configurazione che non supporta "Funzionalità Amazon EBS Elastic Volumes", Quindi, quando si avvia un sistema Cloud Volumes ONTAP, è necessario scegliere una dimensione iniziale del disco. Dopo di che, è possibile "Lascia che BlueXP gestisca la capacità di un sistema per te", ma se lo si desidera "crea aggregati", tenere presente quanto segue:

- Tutti i dischi di un aggregato devono avere le stesse dimensioni.
- Le prestazioni dei dischi EBS sono legate alle dimensioni dei dischi. La dimensione determina gli IOPS di riferimento e la durata massima del burst per i dischi SSD e il throughput di base e burst per i dischi HDD.

- In definitiva, è necessario scegliere le dimensioni del disco che offrono le *prestazioni sostenute* necessarie.
- Anche se si scelgono dischi più grandi (ad esempio, sei dischi 4 TIB), è possibile che non si ottengano tutti gli IOPS perché l'istanza EC2 può raggiungere il limite di larghezza di banda.

  Per ulteriori informazioni sulle prestazioni dei dischi EBS, fare riferimento a. "Documentazione AWS: Tipi di volume EBS".

  Come indicato in precedenza, la scelta di una dimensione del disco non è supportata con le configurazioni Cloud Volumes ONTAP che supportano la funzione EBS di Amazon Elastic Volumes. "Scopri di più sul supporto di Elastic Volumes".

Visualizzare i dischi di sistema predefiniti

Oltre allo storage per i dati degli utenti, BlueXP acquista anche lo storage cloud per i dati del sistema Cloud Volumes ONTAP (dati di avvio, dati root, dati core e NVRAM). A scopo di pianificazione, potrebbe essere utile esaminare questi dettagli prima di implementare Cloud Volumes ONTAP.

"Visualizzare i dischi predefiniti per i dati di sistema Cloud Volumes ONTAP in AWS".

Il connettore richiede anche un disco di sistema. "Visualizza i dettagli sulla configurazione predefinita del connettore".

Prepararsi a implementare Cloud Volumes ONTAP in un Outpost AWS

Se si dispone di un Outpost AWS, è possibile implementare Cloud Volumes ONTAP in tale Outpost selezionando il VPC Outpost nella procedura guidata ambiente di lavoro. L'esperienza è la stessa di qualsiasi altro VPC che risiede in AWS. Tenere presente che è necessario implementare prima un connettore nell'Outpost AWS.

Vi sono alcune limitazioni da sottolineare:

- Al momento sono supportati solo i sistemi Cloud Volumes ONTAP a nodo singolo
- Le istanze di EC2 che è possibile utilizzare con Cloud Volumes ONTAP sono limitate ai contenuti disponibili nell'Outpost
- Al momento sono supportati solo gli SSD General Purpose (gp2)

Raccogliere informazioni di rete

Quando si avvia Cloud Volumes ONTAP in AWS, è necessario specificare i dettagli della rete VPC. È possibile utilizzare un foglio di lavoro per raccogliere le informazioni dall'amministratore.

Nodo singolo o coppia ha in un singolo AZ

Informazioni AWS	Il tuo valore
Regione	
VPC	
Subnet	

Informazioni AWS	Il tuo valore
Gruppo di sicurezza (se si utilizza il proprio)	

Coppia HA in AZS multipli

Informazioni AWS	Il tuo valore
Regione	
VPC	
Gruppo di sicurezza (se si utilizza il proprio)	
Zona di disponibilità del nodo 1	
Subnet del nodo 1	
Zona di disponibilità del nodo 2	
Subnet del nodo 2	
Area di disponibilità del mediatore	
Subnet del mediatore	
Coppia di chiavi per il mediatore	
Indirizzo IP mobile per la porta di gestione del cluster	
Indirizzo IP mobile per i dati sul nodo 1	
Indirizzo IP mobile per i dati sul nodo 2	
Tabelle di routing per gli indirizzi IP mobili	

Scegliere una velocità di scrittura

BlueXP consente di scegliere un'impostazione della velocità di scrittura per Cloud Volumes ONTAP. Prima di scegliere una velocità di scrittura, è necessario comprendere le differenze tra le impostazioni normali e alte e i rischi e le raccomandazioni quando si utilizza un'elevata velocità di scrittura. "Scopri di più sulla velocità di scrittura".

Scegliere un profilo di utilizzo del volume

ONTAP include diverse funzionalità di efficienza dello storage che consentono di ridurre la quantità totale di storage necessaria. Quando si crea un volume in BlueXP, è possibile scegliere un profilo che attiva queste funzionalità o un profilo che le disattiva. Dovresti saperne di più su queste funzionalità per aiutarti a decidere quale profilo utilizzare.

Le funzionalità di efficienza dello storage NetApp offrono i seguenti vantaggi:

Thin provisioning

Presenta uno storage logico maggiore per gli host o gli utenti rispetto al pool di storage fisico. Invece di preallocare lo spazio di storage, lo spazio di storage viene allocato dinamicamente a ciascun volume durante la scrittura dei dati.

Deduplica

Migliora l'efficienza individuando blocchi di dati identici e sostituendoli con riferimenti a un singolo blocco condiviso. Questa tecnica riduce i requisiti di capacità dello storage eliminando blocchi di dati ridondanti che risiedono nello stesso volume.

Compressione

Riduce la capacità fisica richiesta per memorizzare i dati comprimendo i dati all'interno di un volume su storage primario, secondario e di archivio.

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

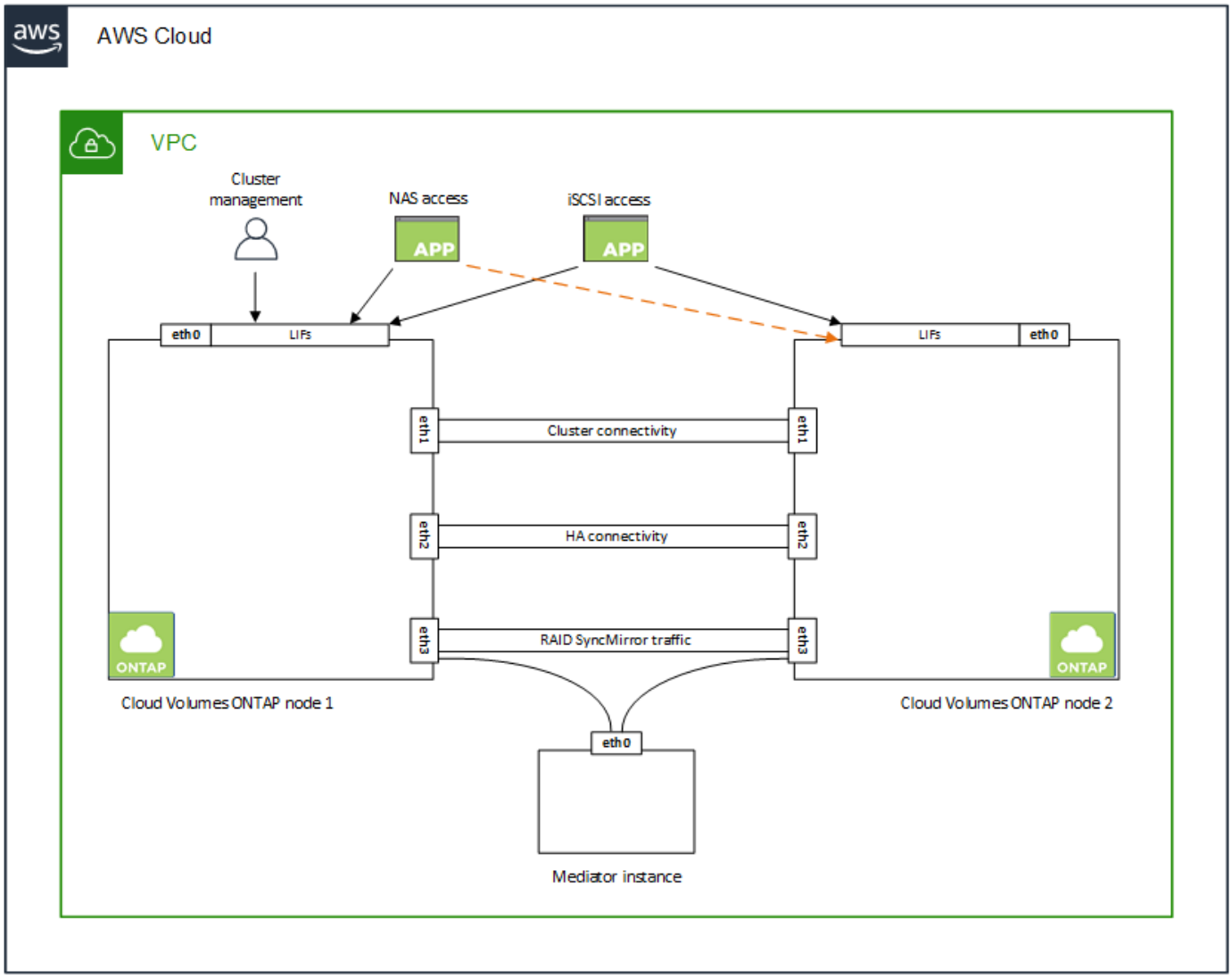
BlueXP assegna 6 indirizzi IP a un sistema a nodo singolo.

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".

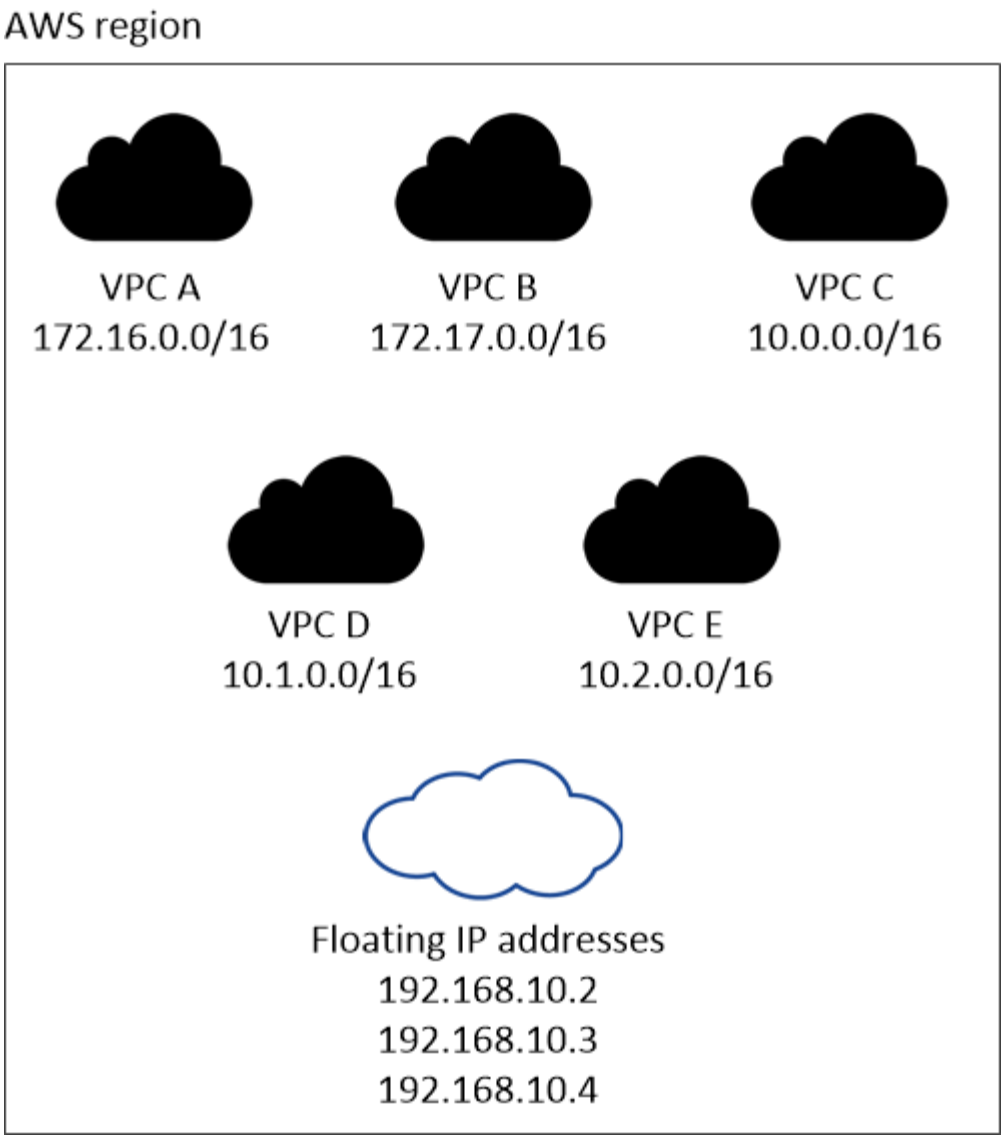
Un indirizzo IP mobile è per la gestione del cluster, uno per i dati NFS/CIFS sul nodo 1 e uno per i dati NFS/CIFS sul nodo 2. Un quarto indirizzo IP mobile per la gestione SVM è opzionale.

> 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".

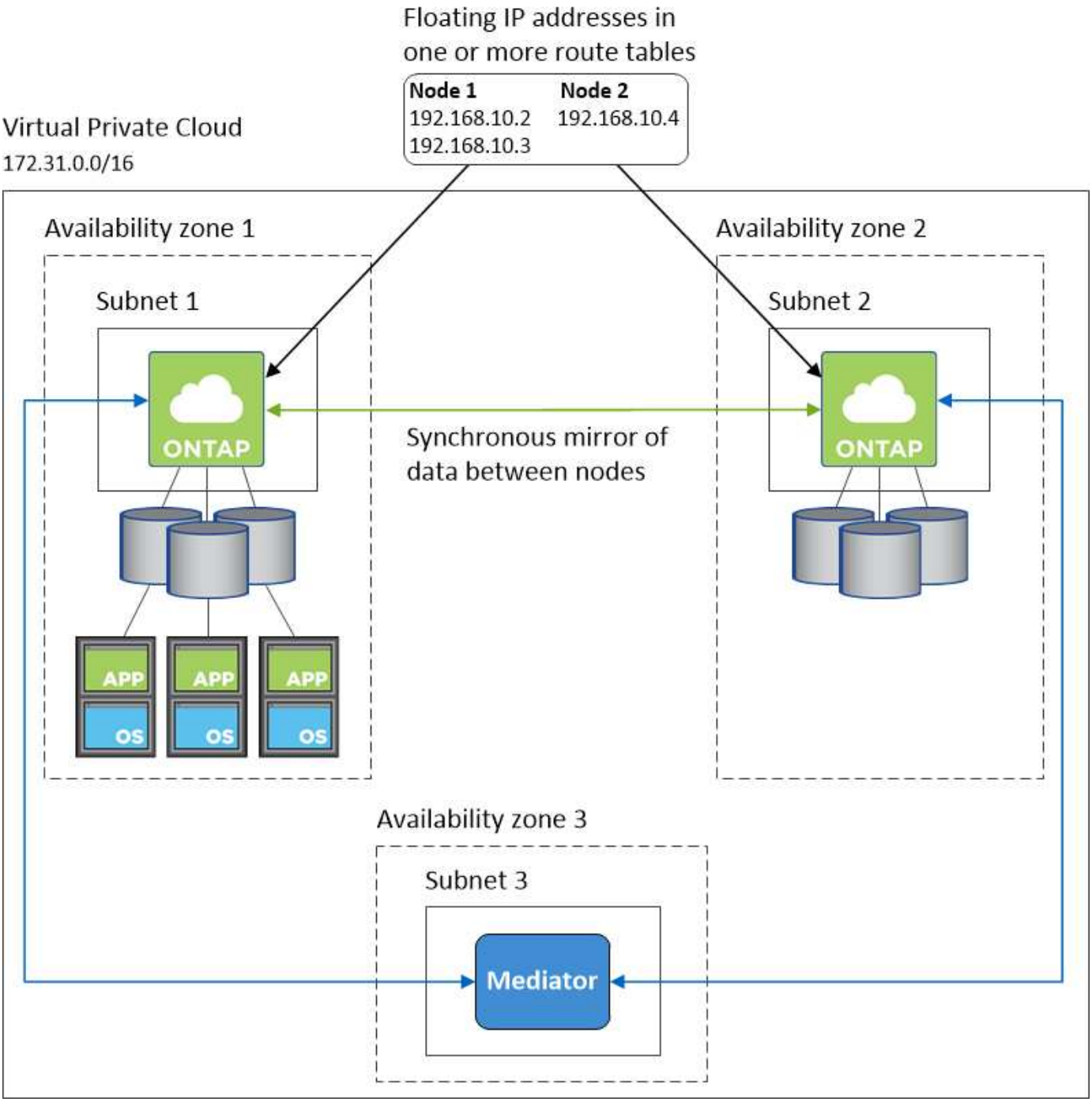
Connessione ai tool di gestione NetApp

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

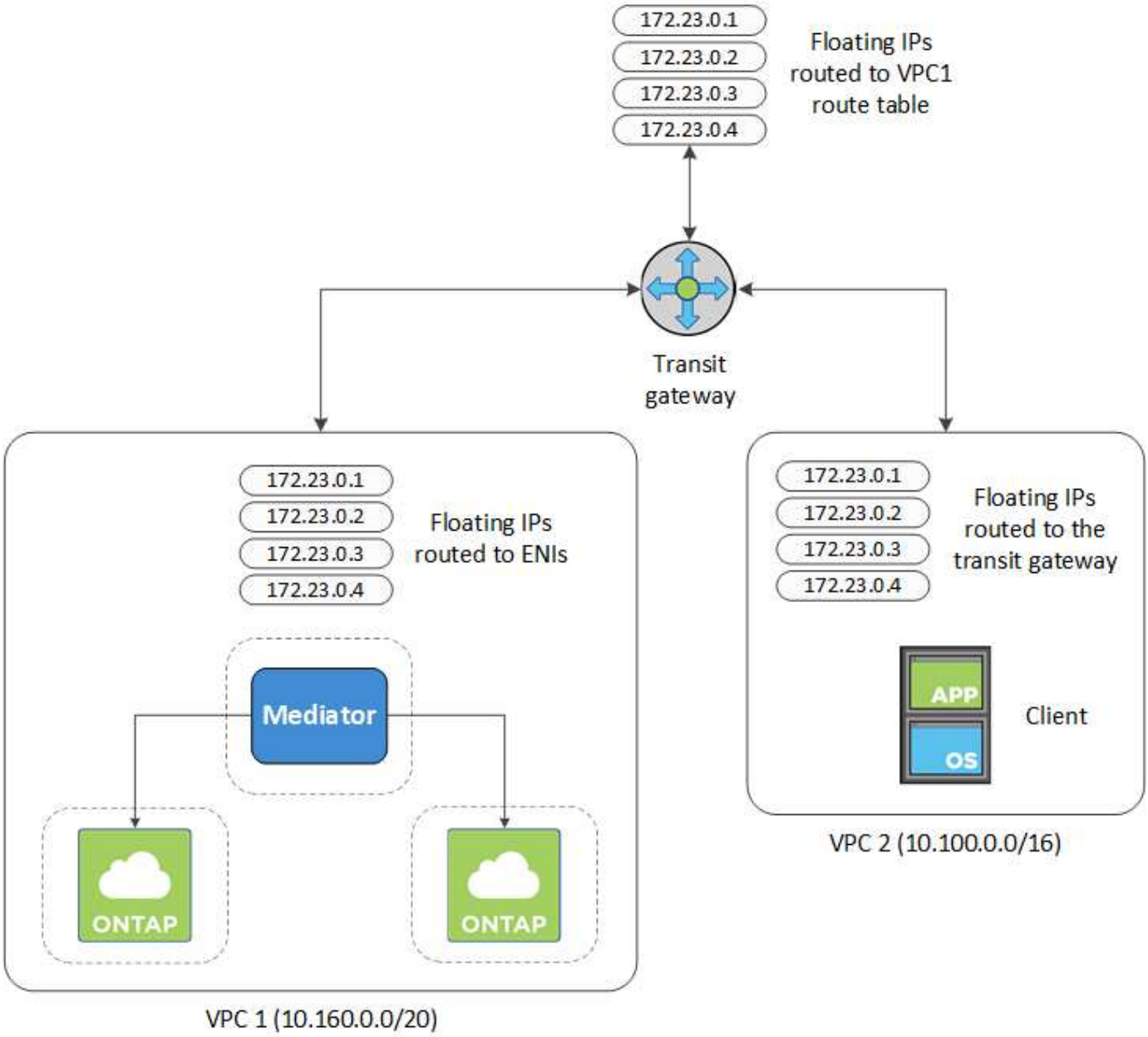
Configurare un gateway di transito AWS per consentire l'accesso a una coppia ha "Indirizzi IP mobili" Dall'esterno del VPC in cui risiede la coppia ha.

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.

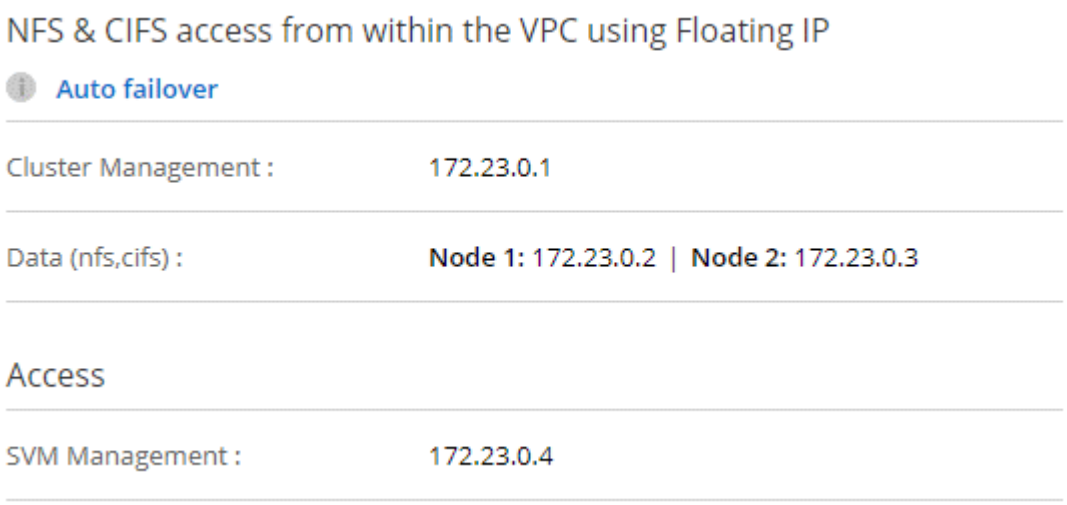


La seguente procedura illustra come configurare una configurazione simile.

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:

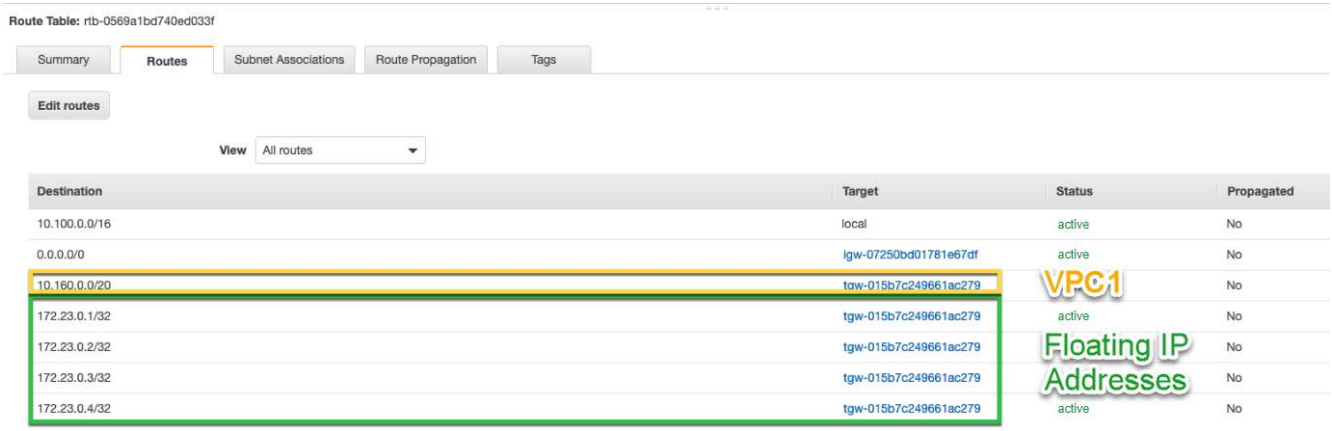


   L'immagine di esempio seguente mostra la tabella di percorso per il gateway di transito. Include le route ai blocchi CIDR dei due VPC e quattro indirizzi IP mobili utilizzati da Cloud Volumes ONTAP.

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.

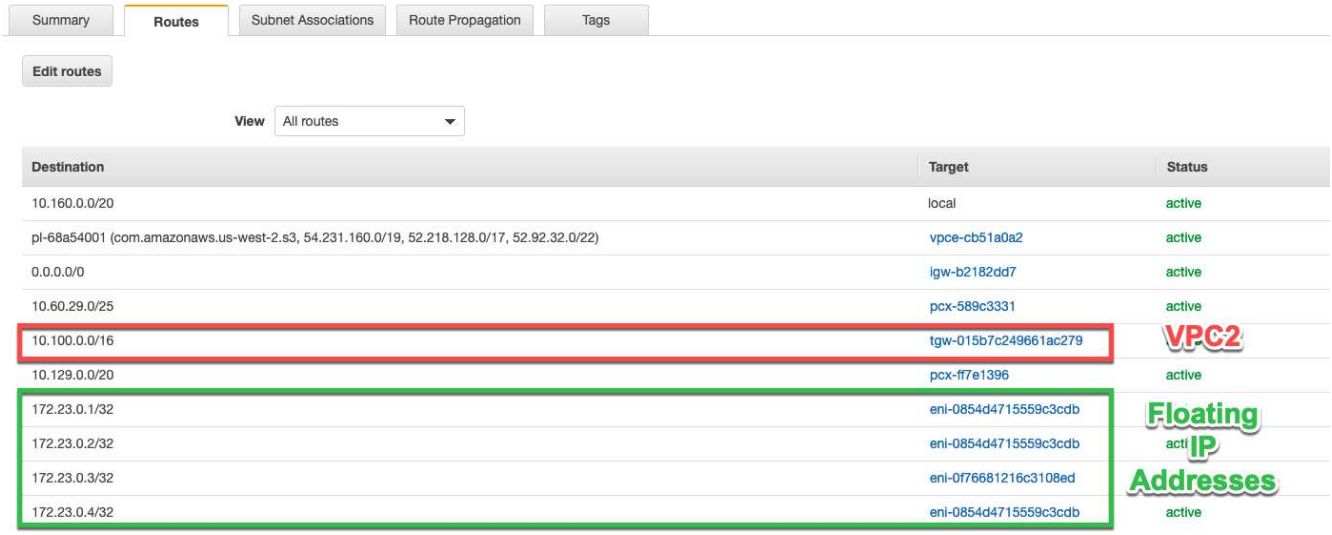
   L'immagine di esempio seguente mostra la tabella di routing per VPC 2, che include i percorsi verso VPC 1 e gli indirizzi IP mobili.



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.



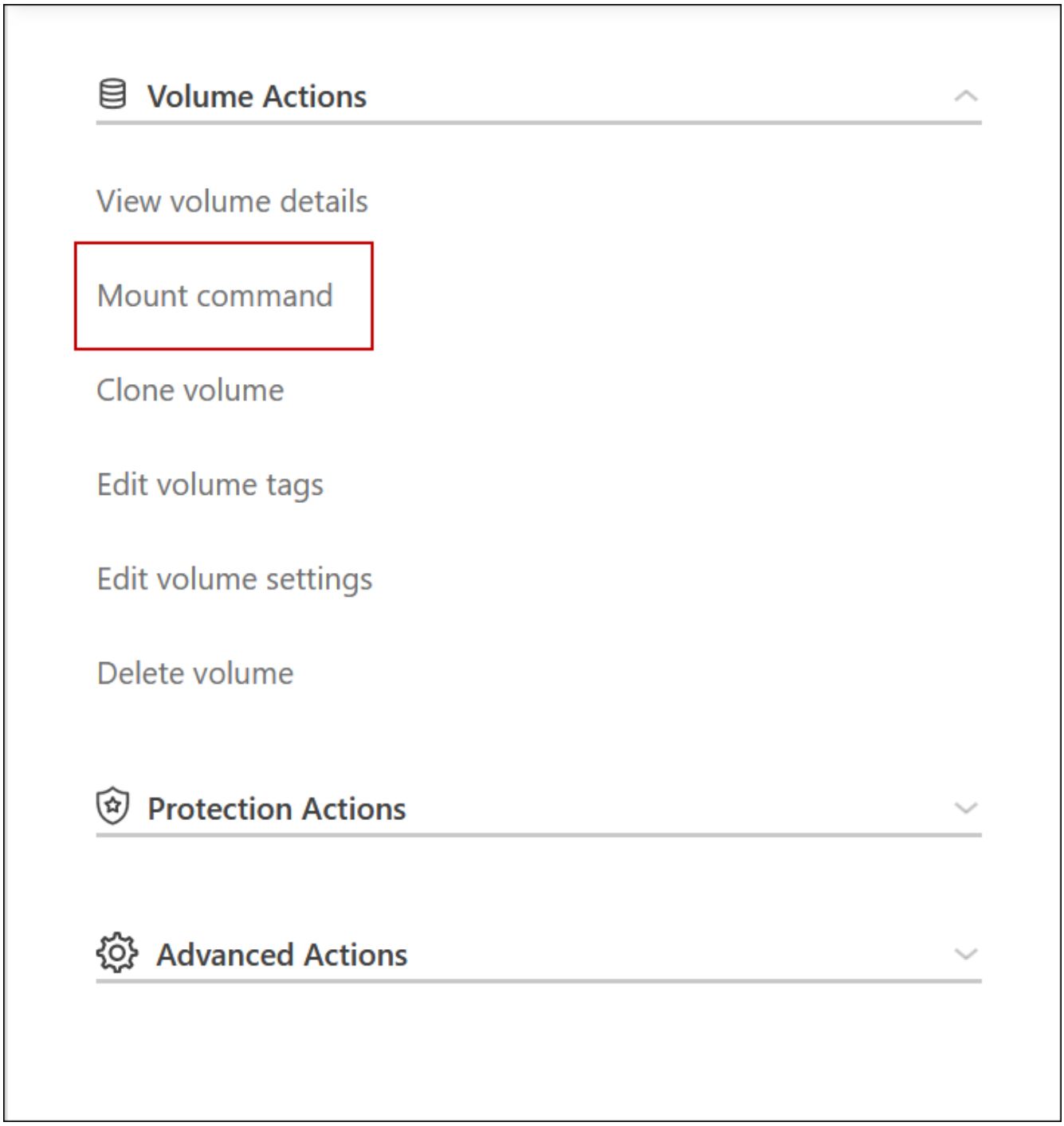
6. Aggiornare le impostazioni dei gruppi di protezione a tutto il traffico per il VPC.
   a. In Virtual Private Cloud, fare clic su **subnet**.
   b. Fare clic sulla scheda **Tabella di instradamento**, selezionare l'ambiente desiderato per uno degli indirizzi IP mobili per una coppia ha.
   c. Fare 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

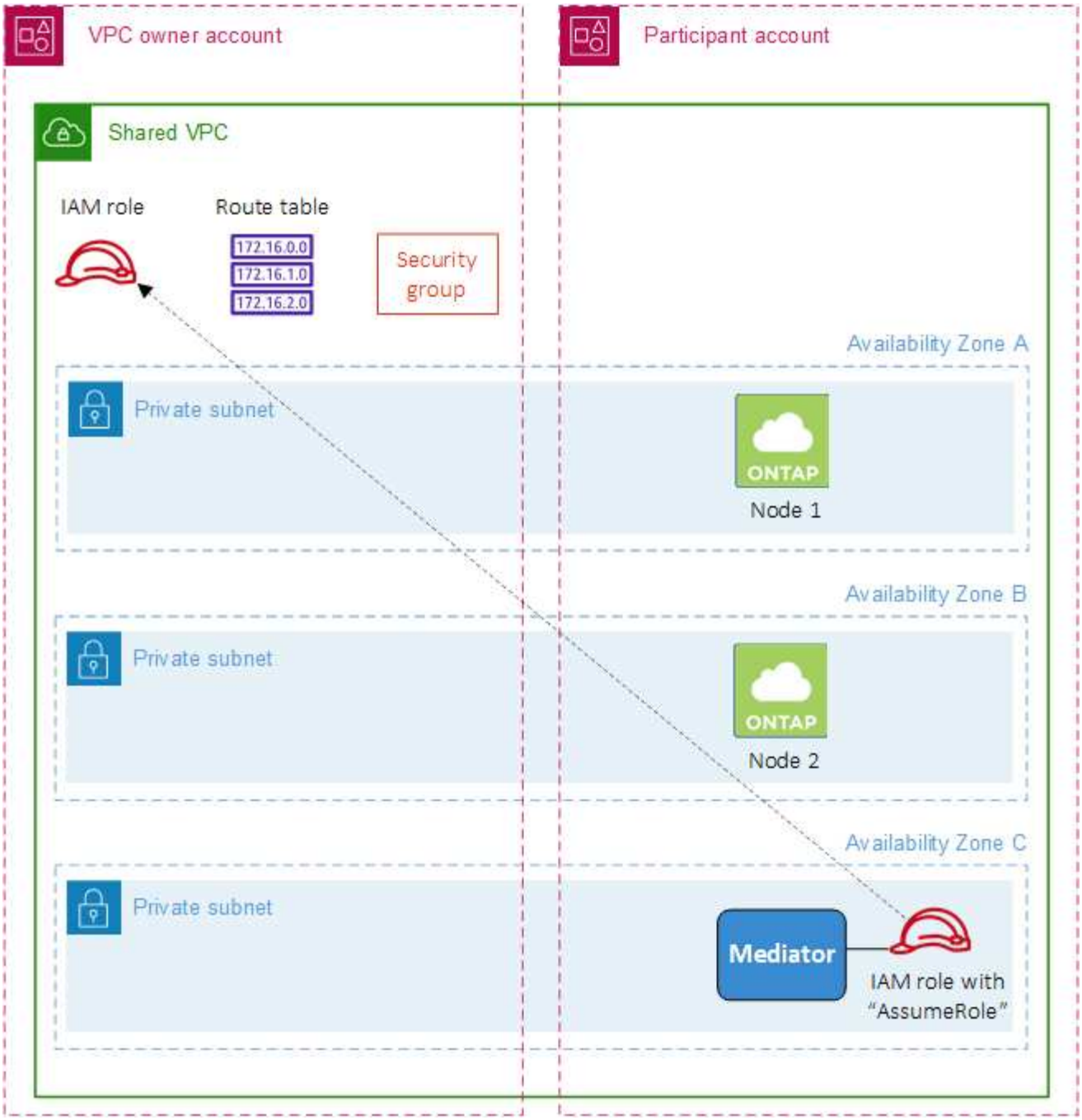
A partire dalla versione 9.11.1, le coppie Cloud Volumes ONTAP ha sono supportate in AWS con condivisione VPC. La condivisione VPC consente alla tua organizzazione di condividere le subnet con altri account AWS. Per utilizzare questa configurazione, è necessario configurare l'ambiente AWS e implementare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

Configurazione di AWS KMS

Se si desidera utilizzare la crittografia Amazon con Cloud Volumes ONTAP, è necessario configurare il servizio di gestione delle chiavi AWS.

Fasi

1. Assicurarsi che esista una chiave master cliente (CMK) attiva.

   Il CMK può essere un CMK gestito da AWS o un CMK gestito dal cliente. Può trovarsi nello stesso account AWS di BlueXP e Cloud Volumes ONTAP o in un altro account AWS.

   "Documentazione AWS: Customer Master Keys (CMK)"

2. Modificare il criterio delle chiavi per ogni CMK aggiungendo il ruolo IAM che fornisce le autorizzazioni a BlueXP come *utente chiave*.

   L'aggiunta del ruolo IAM come utente chiave consente a BlueXP di utilizzare CMK con Cloud Volumes ONTAP.

   "Documentazione AWS: Modifica delle chiavi"

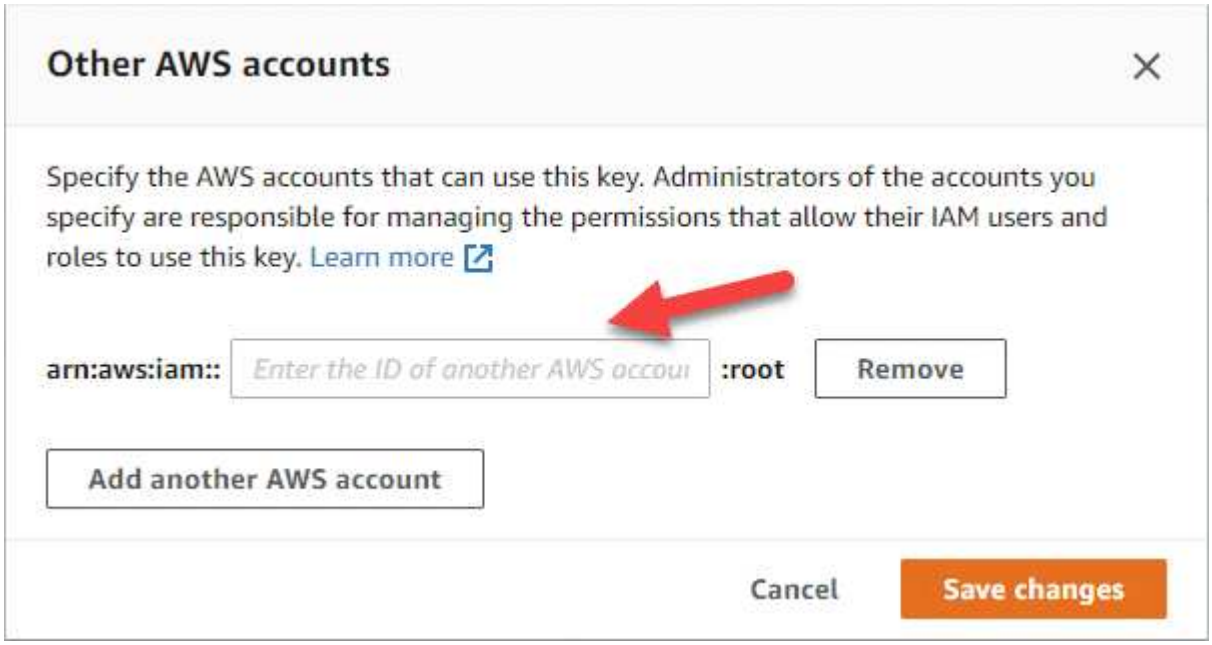
3. Se il CMK si trova in un account AWS diverso, completare la seguente procedura:

   a. Accedere alla console KMS dall'account in cui risiede il CMK.
   b. Selezionare la chiave.
   c. Nel riquadro **General Configuration** (Configurazione generale), copiare l'ARN della chiave.

      Quando si crea il sistema Cloud Volumes ONTAP, è necessario fornire l'ARN a BlueXP.

   d. Nel riquadro **Other AWS accounts** (altri account AWS), aggiungere l'account AWS che fornisce a BlueXP le autorizzazioni necessarie.

      Nella maggior parte dei casi, questo è l'account in cui risiede BlueXP. Se BlueXP non è stato installato in AWS, si tratterebbe dell'account per cui hai fornito le chiavi di accesso AWS a BlueXP.



   e. Passare ora all'account AWS che fornisce a BlueXP le autorizzazioni e aprire la console IAM.
   f. Creare un criterio IAM che includa le autorizzazioni elencate di seguito.

g. Associare il criterio al ruolo IAM o all'utente IAM che fornisce le autorizzazioni a BlueXP.

Il seguente criterio fornisce le autorizzazioni necessarie a BlueXP per utilizzare il CMK dall'account AWS esterno. Assicurarsi di modificare la regione e l'ID account nelle sezioni "risorsa".

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
Per ulteriori informazioni su questo processo, vedere "Documentazione AWS: Consente agli utenti di altri

account di utilizzare una chiave KMS".

4. Se si utilizza una CMK gestita dal cliente, modificare il criterio chiave per la CMK aggiungendo il ruolo IAM Cloud Volumes ONTAP come *utente chiave*.

   Questo passaggio è necessario se si abilita il tiering dei dati su Cloud Volumes ONTAP e si desidera crittografare i dati memorizzati nel bucket S3.

   Sarà necessario eseguire questo passaggio *dopo* l'implementazione di Cloud Volumes ONTAP, in quanto il ruolo IAM viene creato quando si crea un ambiente di lavoro. (Naturalmente, hai la possibilità di utilizzare un ruolo IAM Cloud Volumes ONTAP esistente, quindi è possibile eseguire questo passaggio in precedenza).

   "Documentazione AWS: Modifica delle chiavi"

Impostare i ruoli IAM per Cloud Volumes ONTAP

I ruoli IAM con le autorizzazioni richieste devono essere collegati a ciascun nodo Cloud Volumes ONTAP. Lo stesso vale per il mediatore ha. È più semplice consentire a BlueXP di creare i ruoli IAM, ma è possibile utilizzare i propri ruoli.

Questa attività è facoltativa. Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, l'opzione predefinita è consentire a BlueXP di creare i ruoli IAM. Se le policy di sicurezza della tua azienda richiedono di creare autonomamente i ruoli IAM, segui la procedura riportata di seguito.

> È necessario fornire il proprio ruolo IAM nell'ambiente di servizi cloud commerciali AWS. "Scopri come implementare Cloud Volumes ONTAP in C2S".

Fasi

1. Accedere alla console AWS IAM.
2. Creare policy IAM che includano le seguenti autorizzazioni:
   - Policy di base per nodi Cloud Volumes ONTAP

Regioni standard

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

Regioni di GovCloud (USA)

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

Ambiente C2S

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- Policy di backup per nodi Cloud Volumes ONTAP

  Se si prevede di utilizzare il backup e il ripristino BlueXP con i sistemi Cloud Volumes ONTAP, il ruolo IAM per i nodi deve includere il secondo criterio mostrato di seguito.

Regioni standard

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Regioni di GovCloud (USA)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

Ambiente C2S

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- MEDIATORE HA

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses",
                "sts:AssumeRole",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Creare un ruolo IAM e allegare al ruolo le policy create.

Risultato

Ora si dispone di ruoli IAM che è possibile selezionare quando si crea un nuovo ambiente di lavoro Cloud Volumes ONTAP.

Ulteriori informazioni

- "Documentazione AWS: Creazione di policy IAM"
- "Documentazione AWS: Creazione di ruoli IAM"

Impostare la licenza per Cloud Volumes ONTAP in AWS

Dopo aver deciso quale opzione di licenza utilizzare con Cloud Volumes ONTAP, è necessario eseguire alcuni passaggi prima di poter scegliere l'opzione di licenza quando si crea un nuovo ambiente di lavoro.

Freemium

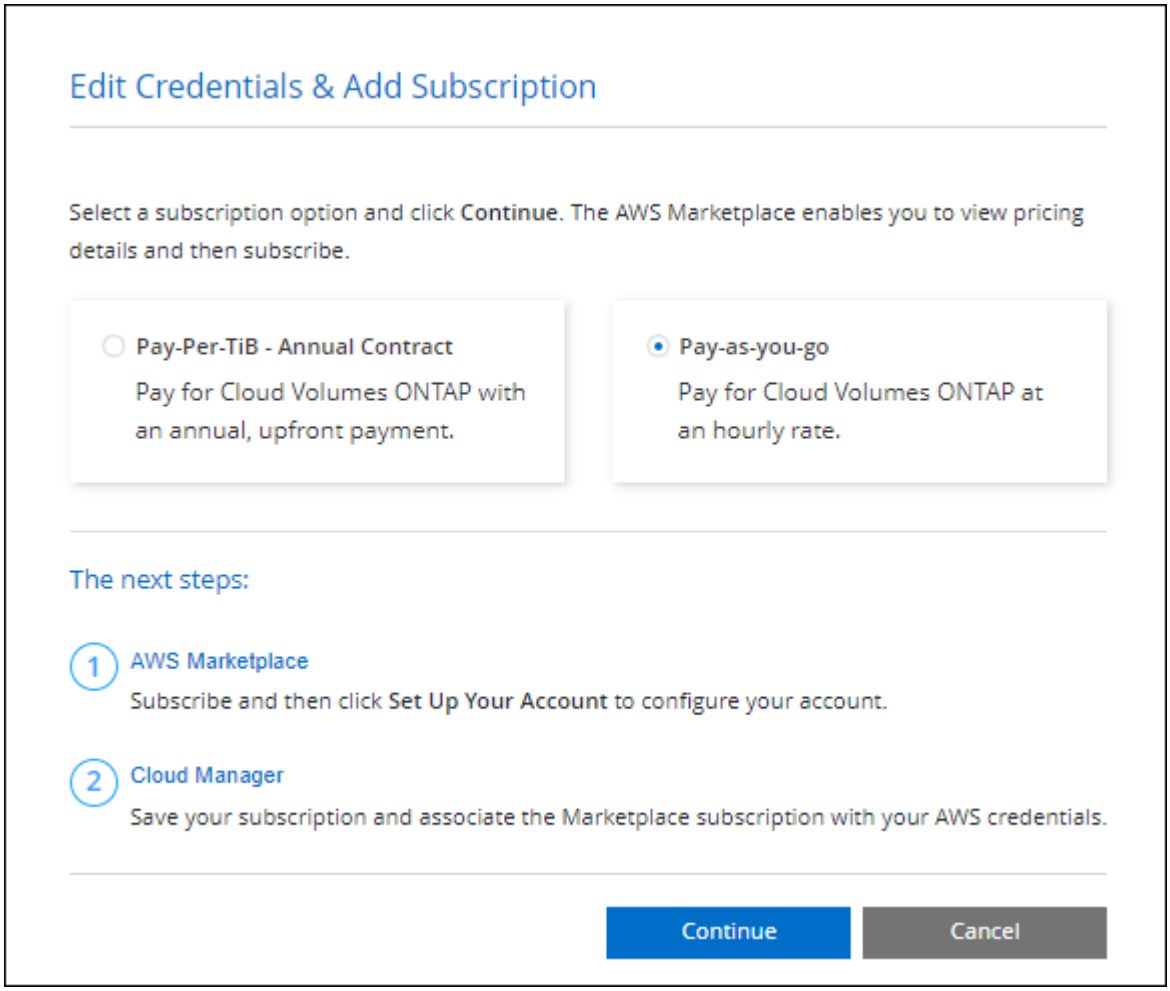
Scegli l'offerta Freemium per utilizzare Cloud Volumes ONTAP gratuitamente con un massimo di 500 GB di capacità fornita. "Scopri di più sull'offerta Freemium".

Fasi

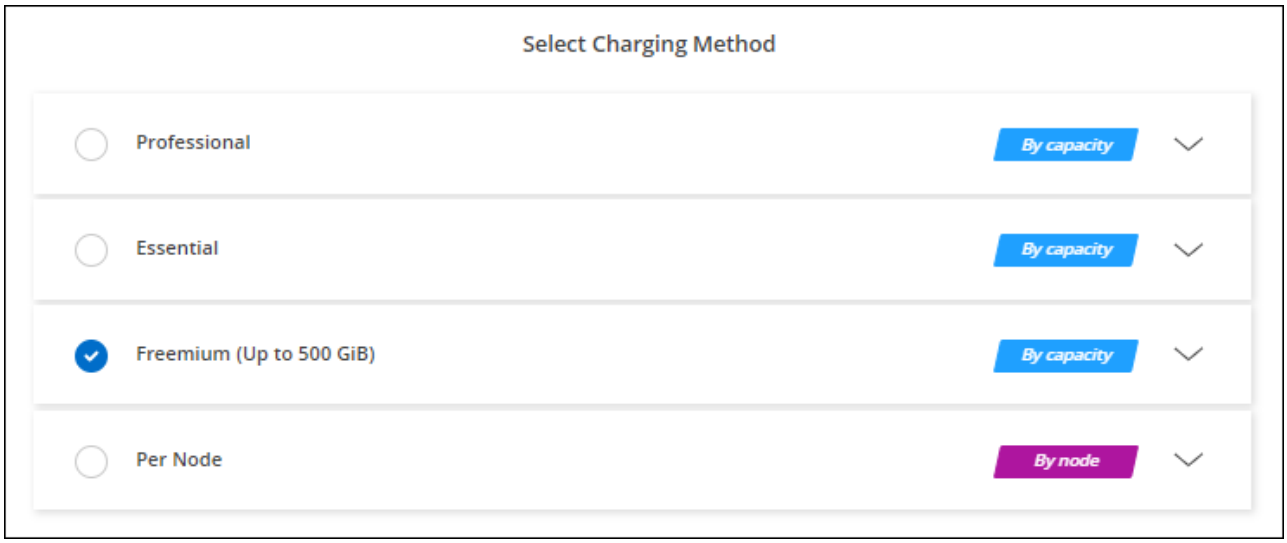
1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.

a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi abbonamento**, quindi seguire le istruzioni per iscriversi all'offerta pay-as-you-go in AWS Marketplace.

   L'abbonamento al marketplace non ti addebiterà alcun costo a meno che non superi i 500 GiB di capacità fornita, dopodiché il sistema viene automaticamente convertito in "Pacchetto Essentials".



a. Una volta visualizzato BlueXP, selezionare **Freemium** quando si accede alla pagina dei metodi di ricarica.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in AWS".

Licenza basata sulla capacità

Le licenze basate sulla capacità consentono di pagare Cloud Volumes ONTAP per TIB di capacità. Le licenze basate sulla capacità sono disponibili sotto forma di un *pacchetto*: Il pacchetto Essentials o il pacchetto Professional.

I pacchetti Essentials e Professional sono disponibili con i seguenti modelli di consumo:

- Una licenza (BYOL) acquistata da NetApp
- Un abbonamento oraria a pagamento (PAYGO) da AWS Marketplace
- Un contratto annuale di AWS Marketplace

"Scopri di più sulle licenze basate sulla capacità".

Le sezioni seguenti descrivono come iniziare a utilizzare ciascuno di questi modelli di consumo.

BYOL

Paga in anticipo acquistando una licenza (BYOL) da NetApp per implementare i sistemi Cloud Volumes ONTAP in qualsiasi cloud provider.

Fasi

1. "Contattare il reparto vendite NetApp per ottenere una licenza"
2. "Aggiungi il tuo account NetApp Support Site a BlueXP"

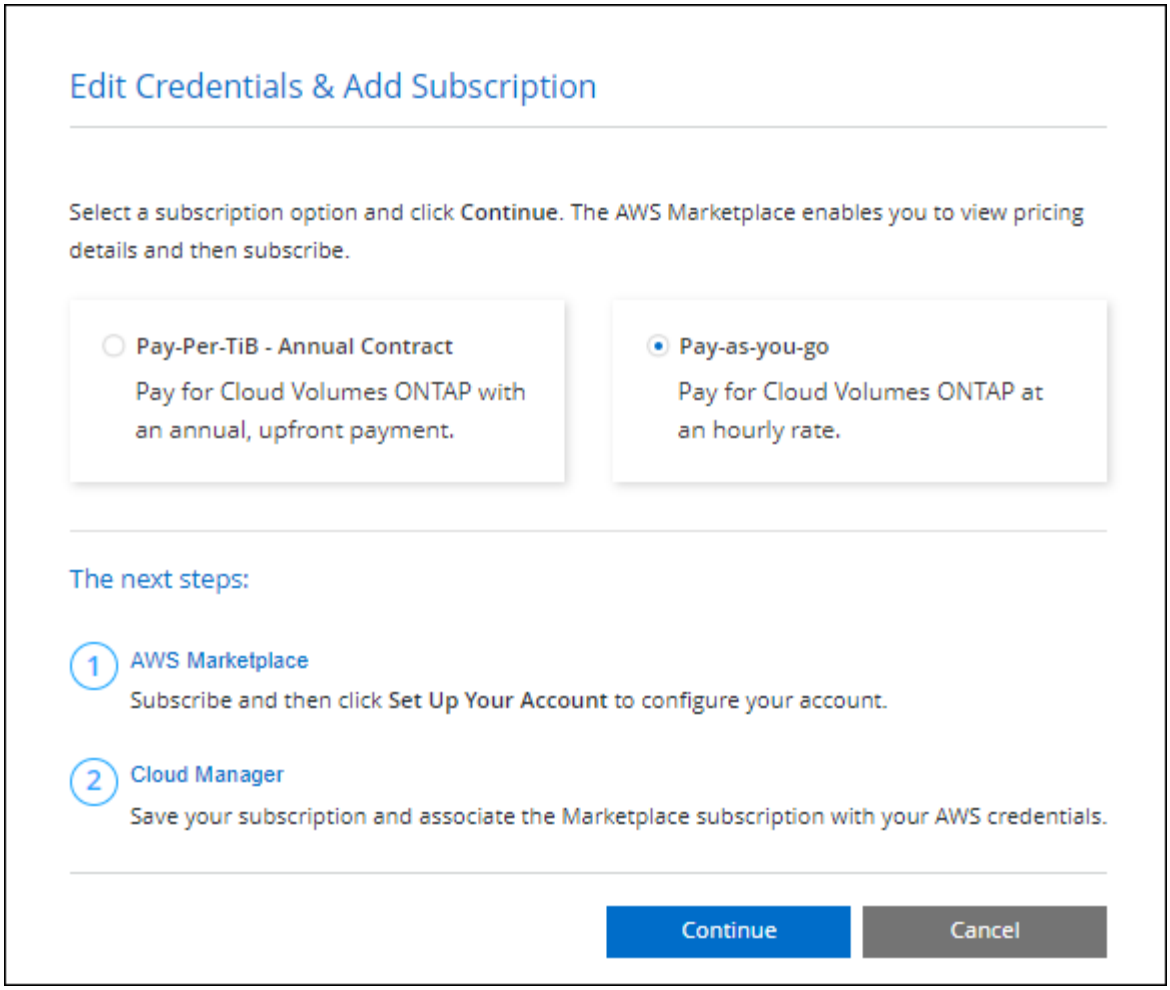
   BlueXP interroga automaticamente il servizio di licensing di NetApp per ottenere dettagli sulle licenze associate al tuo account NetApp Support Site. In assenza di errori, BlueXP aggiunge automaticamente le licenze al portafoglio digitale.

   La licenza deve essere disponibile sul portafoglio digitale BlueXP prima di poter essere utilizzata con Cloud Volumes ONTAP. Se necessario, è possibile "Aggiungere manualmente la licenza al portafoglio digitale BlueXP".

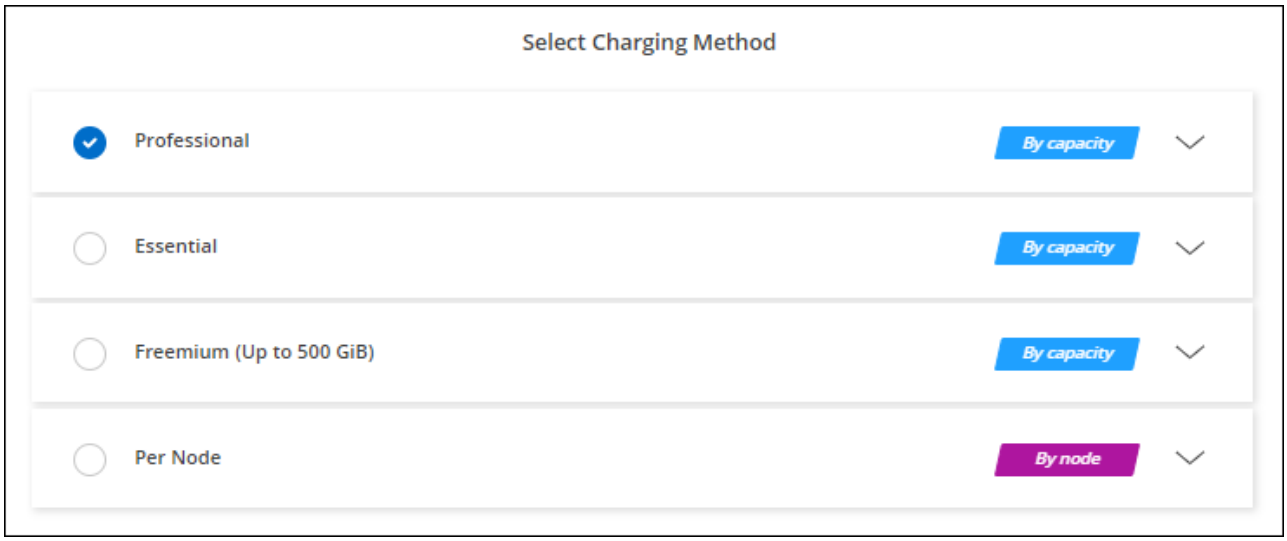
3. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.

   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi abbonamento**, quindi seguire le istruzioni per iscriversi all'offerta pay-as-you-go in AWS Marketplace.

      La licenza acquistata da NetApp viene sempre addebitata per prima, ma verrà addebitato sulla tariffa oraria sul mercato se si supera la capacità concessa in licenza o se scade il termine della licenza.



a. Una volta visualizzato BlueXP, selezionare un pacchetto basato sulla capacità quando si accede alla pagina dei metodi di ricarica.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in AWS".

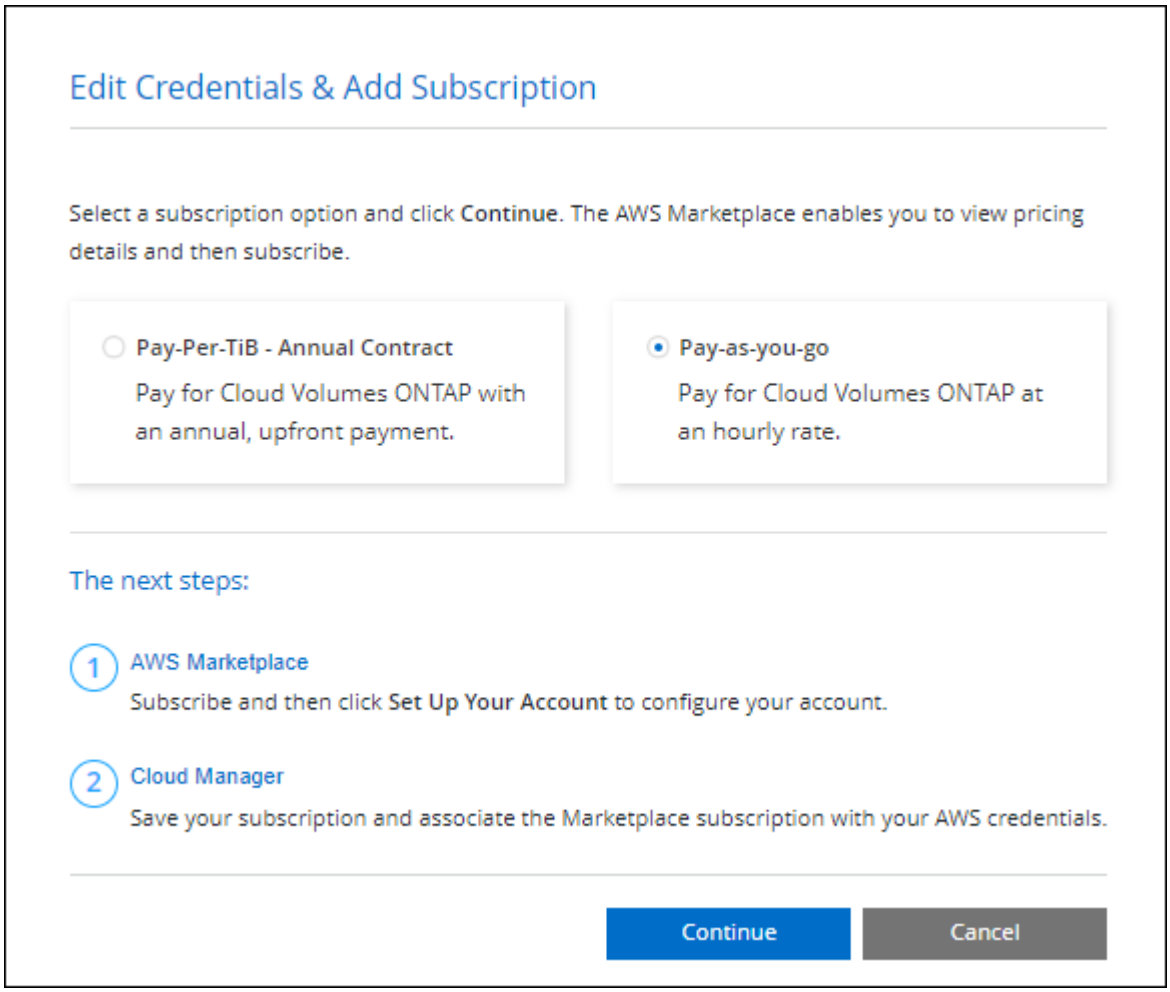
Abbonamento PAYGO

Paga ogni ora sottoscrivendo l'offerta sul mercato del tuo cloud provider.

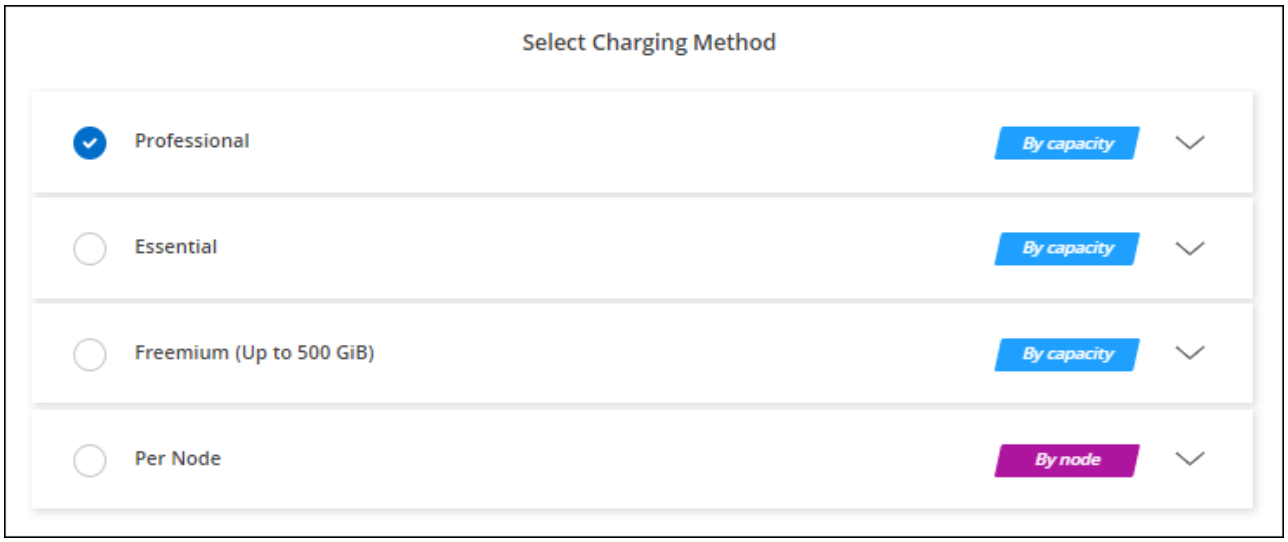
Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, BlueXP richiede di sottoscrivere il contratto disponibile nel marketplace AWS. Tale abbonamento viene quindi associato all'ambiente di lavoro per la ricarica. È possibile utilizzare lo stesso abbonamento per altri ambienti di lavoro.

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.
   a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi abbonamento**, quindi seguire le istruzioni per iscriversi all'offerta pay-as-you-go in AWS Marketplace.



   b. Una volta visualizzato BlueXP, selezionare un pacchetto basato sulla capacità quando si accede alla pagina dei metodi di ricarica.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in AWS".

È possibile gestire gli abbonamenti AWS Marketplace associati agli account AWS dalla pagina Impostazioni > credenziali. "Scopri come gestire gli account e gli abbonamenti AWS"

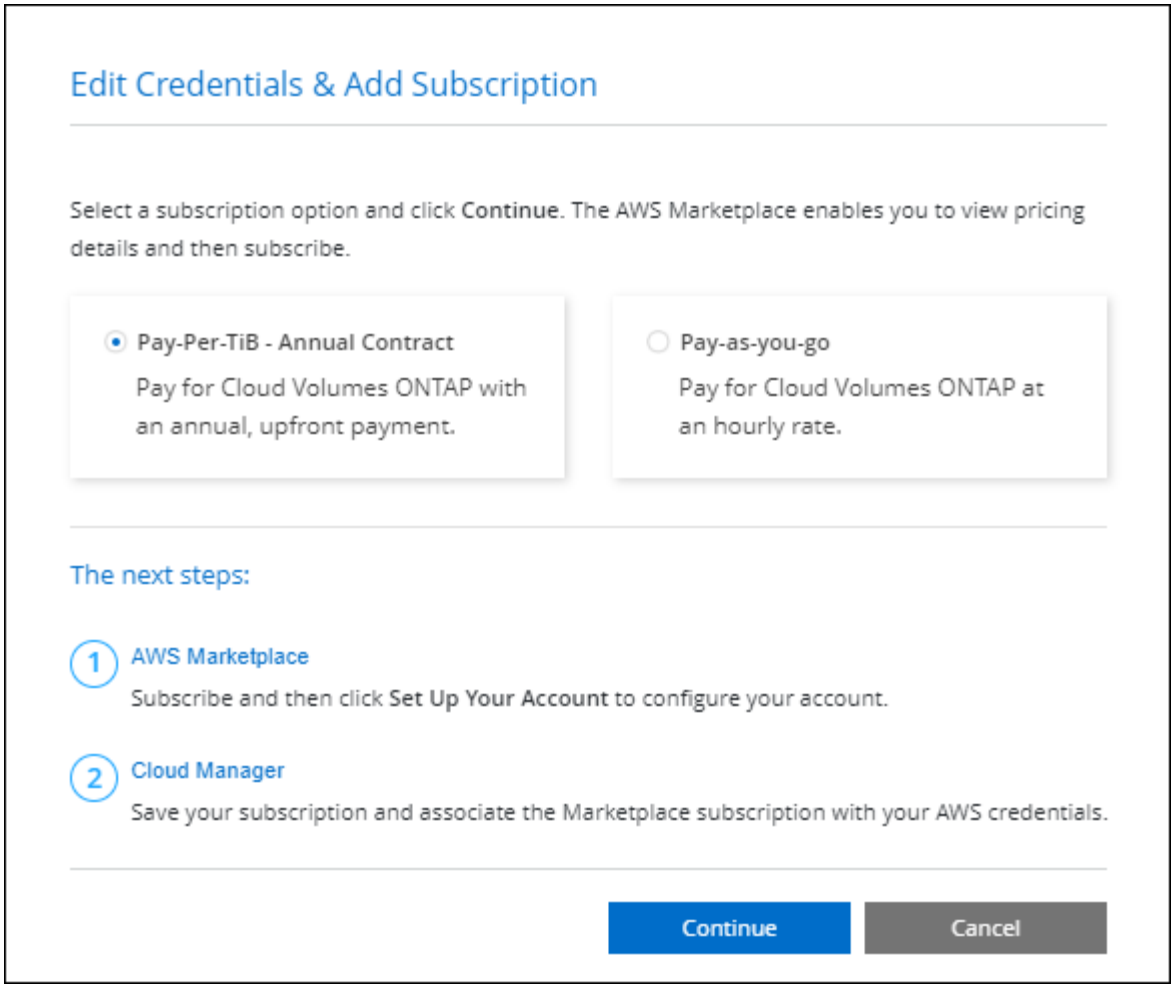
Contratto annuale

Paga ogni anno acquistando un contratto annuale dal mercato del tuo cloud provider.

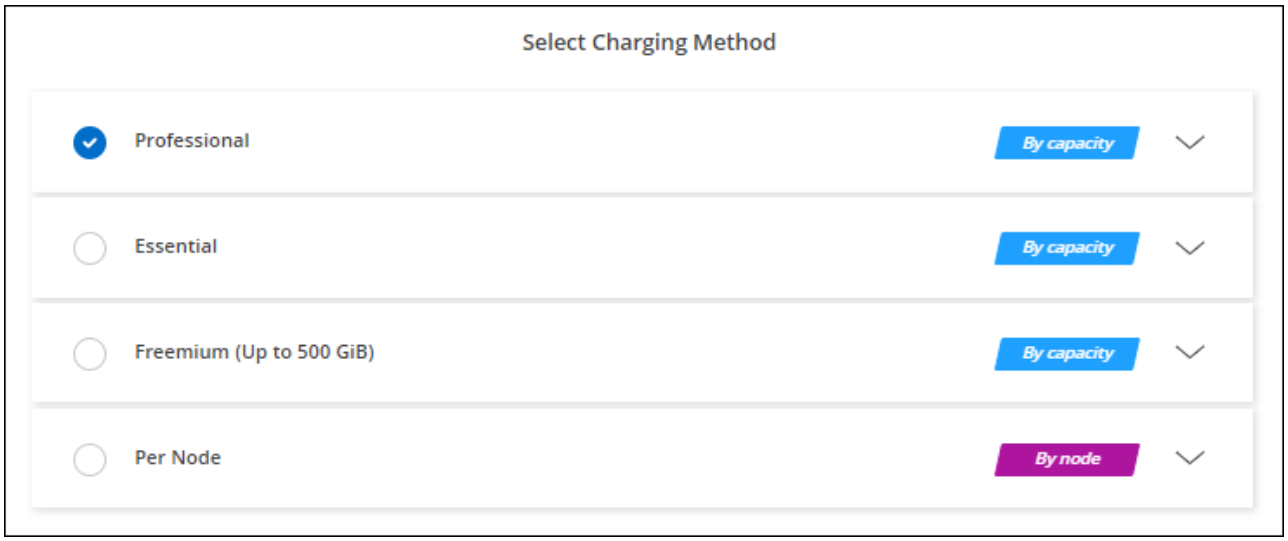
Analogamente a un abbonamento orario, BlueXP richiede di sottoscrivere il contratto annuale disponibile in AWS Marketplace.

Fasi

1. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.
    a. Nella pagina **Dettagli e credenziali**, fare clic su **Modifica credenziali > Aggiungi abbonamento**, quindi seguire le istruzioni per sottoscrivere il contratto annuale in AWS Marketplace.



b. Una volta visualizzato BlueXP, selezionare un pacchetto basato sulla capacità quando si accede alla pagina dei metodi di ricarica.



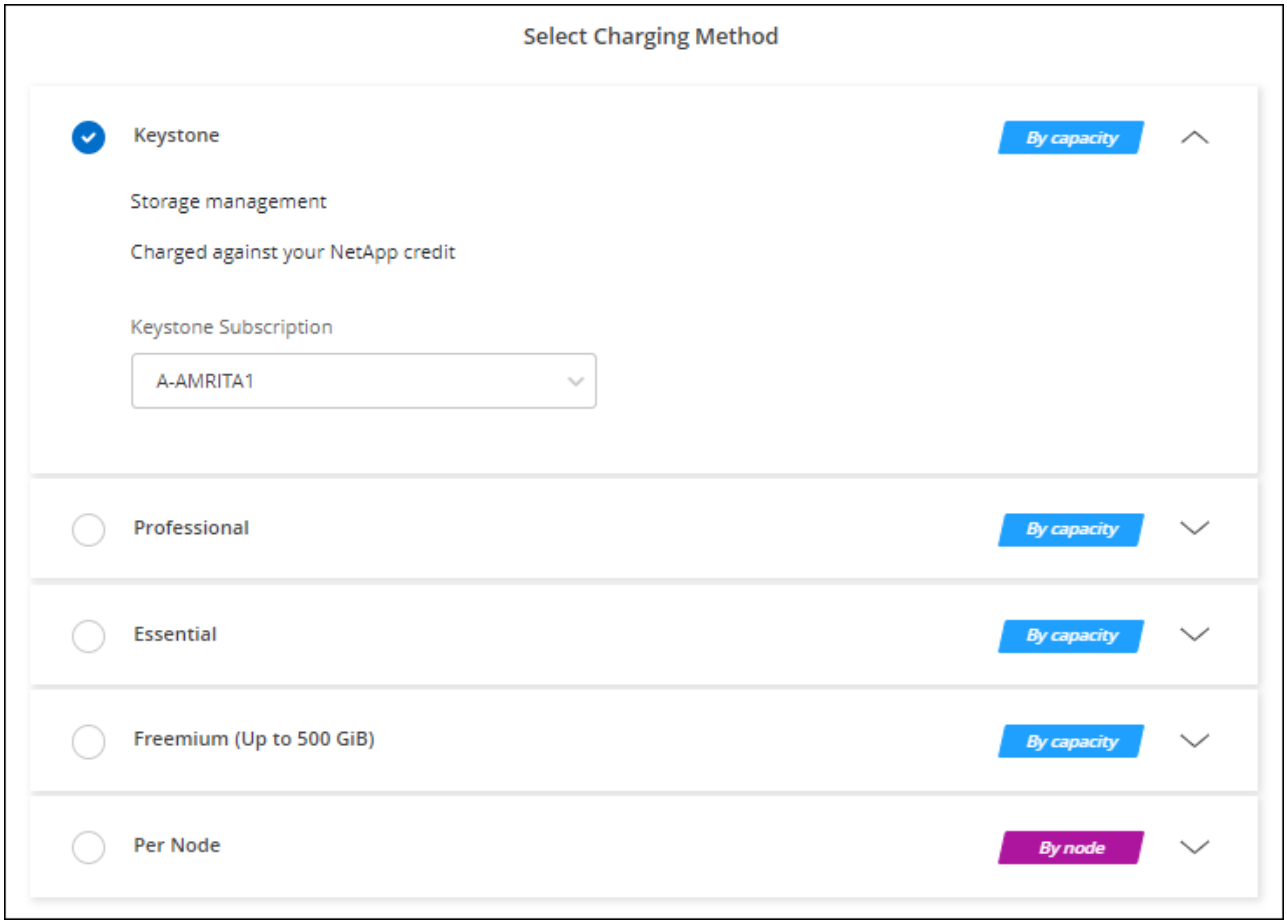
"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in AWS".

Iscrizione Keystone

Un abbonamento Keystone è un servizio basato su abbonamento pay-as-you-grow. "Scopri di più sugli abbonamenti NetApp Keystone".

Fasi

1. Se non disponi ancora di un abbonamento, "Contatta NetApp"
2. Mailto:ng-keystone-success@netapp.com[Contatta NetApp] per autorizzare il tuo account utente BlueXP con uno o più abbonamenti Keystone.
3. Dopo che NetApp ha autorizzato il tuo account, "Collega i tuoi abbonamenti per l'utilizzo con Cloud Volumes ONTAP".
4. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.
   a. Quando richiesto, selezionare il metodo di ricarica per l'abbonamento Keystone.



"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in AWS".

Avvio di Cloud Volumes ONTAP in AWS

È possibile avviare Cloud Volumes ONTAP in una configurazione a sistema singolo o come coppia ha in AWS.

Prima di iniziare

Per creare un ambiente di lavoro, è necessario quanto segue.

- Un connettore funzionante.
  - Si dovrebbe avere un "Connettore associato all'area di lavoro".
  - "Si dovrebbe essere pronti a lasciare il connettore sempre in funzione".
- Comprensione della configurazione che si desidera utilizzare.

  Si dovrebbe aver preparato scegliendo una configurazione e ottenendo le informazioni di rete AWS dall'amministratore. Per ulteriori informazioni, vedere "Pianificazione della configurazione di Cloud Volumes ONTAP".

- Comprensione di ciò che è necessario per impostare le licenze per Cloud Volumes ONTAP.

  "Scopri come impostare le licenze".

- Configurazioni DNS e Active Directory per CIFS.

  Per ulteriori informazioni, vedere "Requisiti di rete per Cloud Volumes ONTAP in AWS".

Avvio di un sistema Cloud Volumes ONTAP a nodo singolo in AWS

Se si desidera avviare Cloud Volumes ONTAP in AWS, è necessario creare un nuovo ambiente di lavoro in BlueXP

A proposito di questa attività

Subito dopo aver creato l'ambiente di lavoro, BlueXP avvia un'istanza di test nel VPC specificato per verificare la connettività. Se l'esito è positivo, BlueXP termina immediatamente l'istanza e avvia la distribuzione del sistema Cloud Volumes ONTAP. Se BlueXP non riesce a verificare la connettività, la creazione dell'ambiente di lavoro non riesce. L'istanza di test è t2.nano (per la tenancy VPC predefinita) o m3.medium (per la tenancy VPC dedicata).

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire le istruzioni.
3. **Scegli una località**: Seleziona **Amazon Web Services** e **Cloud Volumes ONTAP nodo singolo**.
4. Se richiesto, "Creare un connettore".
5. **Dettagli e credenziali**: Se si desidera, modificare le credenziali e l'abbonamento AWS, inserire un nome di ambiente di lavoro, aggiungere tag, se necessario, quindi inserire una password.

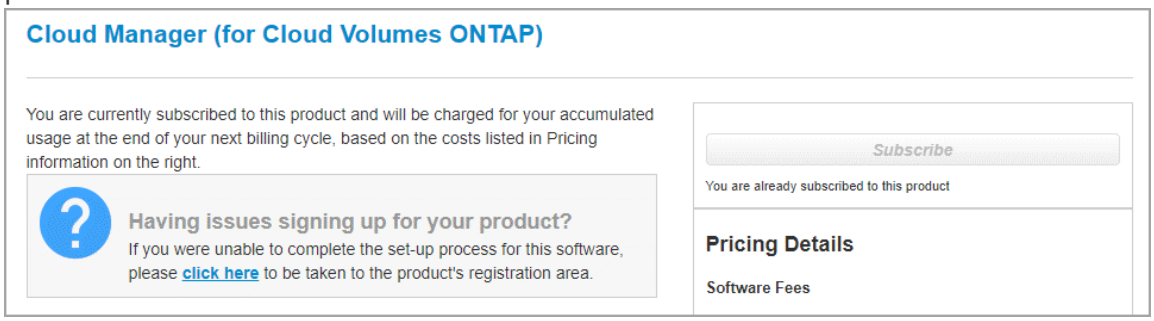
   Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Nome ambiente di lavoro	BlueXP utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che all'istanza di Amazon EC2. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.
Aggiungere tag	I tag AWS sono metadati per le risorse AWS. BlueXP aggiunge i tag all'istanza di Cloud Volumes ONTAP e a ciascuna risorsa AWS associata all'istanza. È possibile aggiungere fino a quattro tag dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altri dopo la creazione. Tenere presente che l'API non si limita a quattro tag durante la creazione di un ambiente di lavoro. Per informazioni sui tag, fare riferimento a. "Documentazione AWS: Contrassegno delle risorse Amazon EC2".
Nome utente e password	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP. È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite Gestore di sistema o la relativa CLI. Mantenere il nome utente predefinito *admin* o modificarlo in un nome utente personalizzato.
Modifica credenziali	Scegliere le credenziali AWS associate all'account in cui si desidera implementare il sistema. È inoltre possibile associare l'abbonamento a AWS Marketplace da utilizzare con questo sistema Cloud Volumes ONTAP. Fare clic su **Add Subscription** (Aggiungi abbonamento) per associare le credenziali selezionate a un nuovo abbonamento AWS Marketplace. L'abbonamento può essere per un contratto annuale o per pagare Cloud Volumes ONTAP a una tariffa oraria. "Scopri come aggiungere ulteriori credenziali AWS a BlueXP".

Il video seguente mostra come associare un abbonamento al Marketplace pay-as-you-go alle tue credenziali AWS:

Iscriviti a BlueXP dal marketplace AWS

Se più utenti IAM lavorano nello stesso account AWS, ciascun utente deve iscriversi. Dopo l'iscrizione, AWS Marketplace informa gli utenti successivi che sono già abbonati, come mostrato nell'immagine seguente. Mentre è in vigore un abbonamento per l' *account* AWS, ciascun utente IAM deve associarsi a tale abbonamento. Se viene visualizzato il messaggio riportato di seguito, fare clic sul collegamento **fare clic qui** per accedere al sito Web di BlueXP e completare la
procedura.



6. **Servizi**: Mantieni abilitati i servizi o disabilita i singoli servizi che non vuoi utilizzare con Cloud Volumes

ONTAP.

- "Scopri di più sulla classificazione BlueXP"
- "Scopri di più sul backup e ripristino BlueXP"

> Se si desidera utilizzare WORM e il tiering dei dati, è necessario disattivare il backup e il ripristino BlueXP e implementare un ambiente di lavoro Cloud Volumes ONTAP con versione 9.8 o superiore.

7. **Location & Connectivity** (posizione e connettività): Inserire le informazioni di rete registrate in "Foglio di lavoro AWS".

   La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
VPC	Se si dispone di un Outpost AWS, è possibile implementare un sistema Cloud Volumes ONTAP a nodo singolo in tale Outpost selezionando il VPC Outpost. L'esperienza è la stessa di qualsiasi altro VPC che risiede in AWS.
Gruppo di sicurezza generato	Se si lascia che BlueXP generi il gruppo di protezione, è necessario scegliere come consentire il traffico: • Se si sceglie **Selected VPC only** (solo VPC selezionato), l'origine del traffico in entrata è l'intervallo di sottorete del VPC selezionato e l'intervallo di sottorete del VPC in cui si trova il connettore. Questa è l'opzione consigliata. • Se si sceglie **All VPC**, l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.
USA gruppo di sicurezza esistente	Se si utilizza un criterio firewall esistente, assicurarsi che includa le regole richieste. "Scopri le regole del firewall per Cloud Volumes ONTAP".

8. **Crittografia dei dati**: Non scegliere alcuna crittografia dei dati o crittografia gestita da AWS.

   Per la crittografia gestita da AWS, è possibile scegliere una chiave Customer Master Key (CMK) diversa dal proprio account o da un altro account AWS.

   > Non è possibile modificare il metodo di crittografia dei dati AWS dopo aver creato un sistema Cloud Volumes ONTAP.

   "Scopri come configurare AWS KMS per Cloud Volumes ONTAP".

   "Scopri di più sulle tecnologie di crittografia supportate".

9. **Charging Methods and NSS account** (metodi di addebito e account NSS): Specificare l'opzione di addebito che si desidera utilizzare con questo sistema, quindi specificare un account NetApp Support Site.
   - "Scopri le opzioni di licenza per Cloud Volumes ONTAP".
   - "Scopri come impostare le licenze".
10. **Configurazione Cloud Volumes ONTAP** (solo contratto annuale AWS Marketplace): Esaminare la configurazione predefinita e fare clic su **continua** o su **Modifica configurazione** per selezionare la propria configurazione.

Se si mantiene la configurazione predefinita, è sufficiente specificare un volume, quindi rivedere e approvare la configurazione.

11. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per avviare rapidamente Cloud Volumes ONTAP oppure fare clic su **Cambia configurazione** per selezionare la propria configurazione.

    Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.

12. **Ruolo IAM**: È meglio mantenere l'opzione predefinita per consentire a BlueXP di creare il ruolo per te.

    Se si preferisce utilizzare la propria policy, è necessario che sia conforme "Requisiti dei criteri per i nodi Cloud Volumes ONTAP".

13. **Licenza**: Modificare la versione di Cloud Volumes ONTAP in base alle necessità e selezionare un tipo di istanza e la tenancy dell'istanza.

    > Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, BlueXP aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.10.1 e 9.10.1 P4 è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.6 a 9.7.

14. **Risorse di storage sottostanti**: Scegliere un tipo di disco, configurare lo storage sottostante e scegliere se mantenere abilitato il tiering dei dati.

    Tenere presente quanto segue:

    - Il tipo di disco è per il volume iniziale (e l'aggregato). È possibile scegliere un tipo di disco diverso per i volumi (e gli aggregati) successivi.
    - Se si sceglie un disco gp3 o io1, BlueXP utilizza la funzionalità Elastic Volumes di AWS per aumentare automaticamente la capacità del disco di storage sottostante in base alle necessità. Puoi scegliere la capacità iniziale in base alle tue esigenze di storage e rivederla dopo l'implementazione di Cloud Volumes ONTAP. "Scopri di più sul supporto per volumi elastici in AWS".
    - Se si sceglie un disco gp2 o st1, è possibile selezionare una dimensione del disco per tutti i dischi nell'aggregato iniziale e per qualsiasi aggregato aggiuntivo creato da BlueXP quando si utilizza l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano una dimensione del disco diversa utilizzando l'opzione di allocazione avanzata.
    - Quando si crea o si modifica un volume, è possibile scegliere un criterio di tiering del volume specifico.
    - Se si disattiva il tiering dei dati, è possibile attivarlo sugli aggregati successivi.

      "Scopri come funziona il tiering dei dati".

15. **Velocità di scrittura e WORM**:

    a. Scegliere **normale** o **alta** velocità di scrittura, se lo si desidera.

       "Scopri di più sulla velocità di scrittura".

    b. Attivare lo storage WORM (Write Once, Read Many), se lo si desidera.

       NON è possibile attivare WORM se il tiering dei dati è stato abilitato per Cloud Volumes ONTAP versione 9.7 e precedenti. Il ripristino o il downgrade a Cloud Volumes ONTAP 9.8 viene bloccato dopo

l'abilitazione DI WORM e tiering.

"Scopri di più sullo storage WORM".

a. Se si attiva lo storage WORM, selezionare il periodo di conservazione.

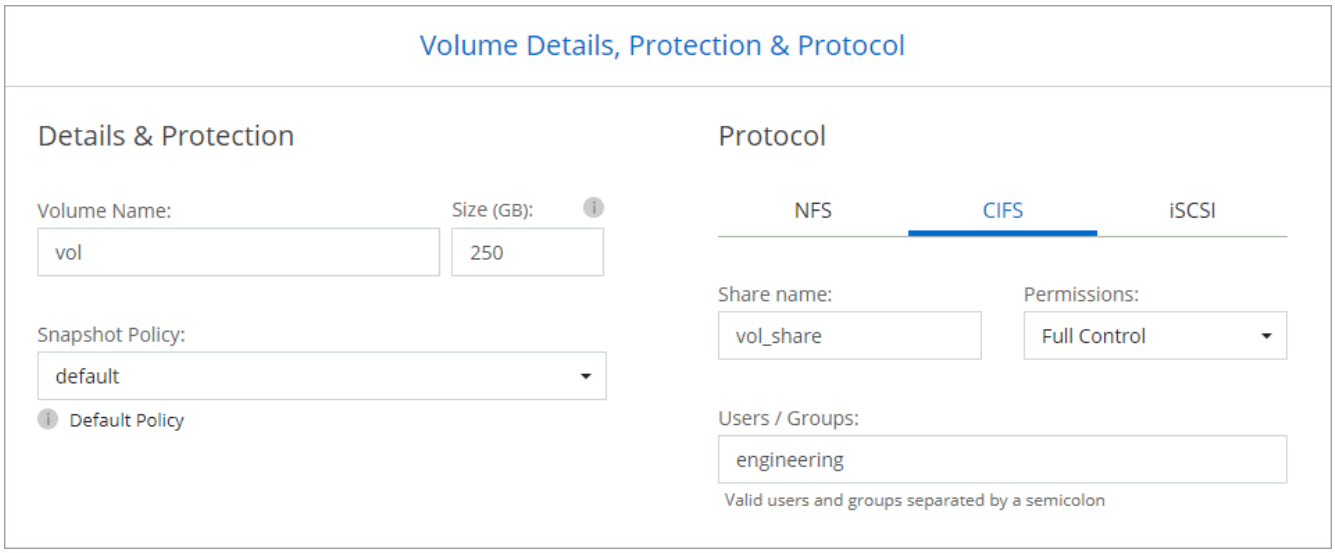
16. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

"Scopri le versioni e i protocolli client supportati".

Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Dimensione	Le dimensioni massime che è possibile inserire dipendono in gran parte dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello storage fisico attualmente disponibile per l'IT.
Controllo degli accessi (solo per NFS)	Un criterio di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, BlueXP inserisce un valore che fornisce l'accesso a tutte le istanze della subnet.
Permessi e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (detti anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio, utenti o gruppi UNIX. Se si specifica un nome utente Windows di dominio, è necessario includere il dominio dell'utente utilizzando il formato dominio/nome utente.
Policy di Snapshot	Una policy di copia Snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot di NetApp è un'immagine del file system point-in-time che non ha alcun impatto sulle performance e richiede uno storage minimo. È possibile scegliere il criterio predefinito o nessuno. È possibile scegliere nessuno per i dati transitori, ad esempio tempdb per Microsoft SQL Server.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.
Initiator group e IQN (solo per iSCSI)	Le destinazioni di storage iSCSI sono denominate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle dei nomi dei nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si collegano alla rete tramite schede di rete Ethernet standard (NIC), schede TOE (TCP offload Engine) con iniziatori software, adattatori di rete convergenti (CNA) o adattatori host busto dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, BlueXP crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è necessario alcun intervento di gestione. Dopo aver creato il volume, "Utilizzare IQN per connettersi al LUN dagli host".

La seguente immagine mostra la pagina Volume compilata per il protocollo CIFS:



17. **CIFS Setup**: Se si sceglie il protocollo CIFS, impostare un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server CIFS si unisce.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate per l'accesso al dominio	Il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata nel dominio ad.
Nome NetBIOS del server CIFS	Un nome server CIFS univoco nel dominio ad.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer. Se si configura AWS Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=corp** in questo campo.
Dominio DNS	Il dominio DNS per la SVM (Storage Virtual Machine) di Cloud Volumes ONTAP. Nella maggior parte dei casi, il dominio è lo stesso del dominio ad.
Server NTP	Selezionare **Use Active Directory Domain** (Usa dominio Active Directory) per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, utilizzare l'API. Vedere "Documenti sull'automazione BlueXP" per ulteriori informazioni. Nota: È possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

18. **Profilo di utilizzo, tipo di disco e policy di tiering**: Scegliere se attivare le funzionalità di efficienza dello storage e modificare la policy di tiering dei volumi, se necessario.

    Per ulteriori informazioni, vedere "Comprensione dei profili di utilizzo dei volumi" e. "Panoramica sul tiering dei dati".

19. **Review & Approve** (Rivedi e approva): Consente di rivedere e confermare le selezioni.
    a. Esaminare i dettagli della configurazione.
    b. Fare clic su **ulteriori informazioni** per visualizzare i dettagli relativi al supporto e alle risorse AWS che BlueXP acquisterà.
    c. Selezionare le caselle di controllo **ho capito…**.
    d. Fare clic su **Go**.

Risultato

BlueXP avvia l'istanza di Cloud Volumes ONTAP. Puoi tenere traccia dei progressi nella timeline.

In caso di problemi durante l'avvio dell'istanza di Cloud Volumes ONTAP, esaminare il messaggio di errore. È inoltre possibile selezionare l'ambiente di lavoro e fare clic su Re-create environment (Crea ambiente).

Per ulteriore assistenza, visitare il sito Web all'indirizzo "Supporto NetApp Cloud Volumes ONTAP".

Al termine

- Se è stata fornita una condivisione CIFS, assegnare agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare le quote ai volumi, utilizzare System Manager o l'interfaccia CLI.

  Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

Avvio di una coppia Cloud Volumes ONTAP ha in AWS

Se si desidera avviare una coppia Cloud Volumes ONTAP ha in AWS, è necessario creare un ambiente di lavoro ha in BlueXP.

Limitazione

Al momento, le coppie ha non sono supportate con gli outpost AWS.

A proposito di questa attività

Subito dopo aver creato l'ambiente di lavoro, BlueXP avvia un'istanza di test nel VPC specificato per verificare la connettività. Se l'esito è positivo, BlueXP termina immediatamente l'istanza e avvia la distribuzione del sistema Cloud Volumes ONTAP. Se BlueXP non riesce a verificare la connettività, la creazione dell'ambiente di lavoro non riesce. L'istanza di test è t2.nano (per la tenancy VPC predefinita) o m3.medium (per la tenancy VPC dedicata).

Fasi

1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire le istruzioni.
3. **Scegli una località**: Seleziona **Amazon Web Services** e **Cloud Volumes ONTAP ha**.
4. **Dettagli e credenziali**: Se si desidera, modificare le credenziali e l'abbonamento AWS, inserire un nome di ambiente di lavoro, aggiungere tag, se necessario, quindi inserire una password.

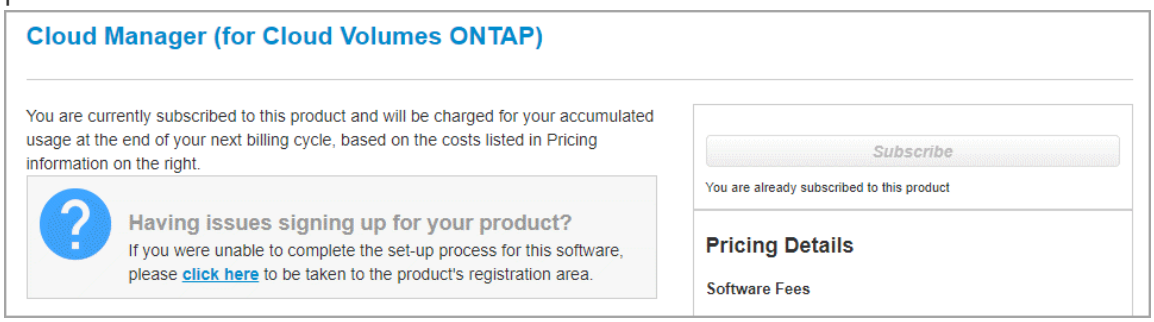
   Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Nome ambiente di lavoro	BlueXP utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che all'istanza di Amazon EC2. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.
Aggiungere tag	I tag AWS sono metadati per le risorse AWS. BlueXP aggiunge i tag all'istanza di Cloud Volumes ONTAP e a ciascuna risorsa AWS associata all'istanza. È possibile aggiungere fino a quattro tag dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altri dopo la creazione. Tenere presente che l'API non si limita a quattro tag durante la creazione di un ambiente di lavoro. Per informazioni sui tag, fare riferimento a. "Documentazione AWS: Contrassegno delle risorse Amazon EC2".
Nome utente e password	Queste sono le credenziali per l'account amministratore del cluster Cloud Volumes ONTAP. È possibile utilizzare queste credenziali per connettersi a Cloud Volumes ONTAP tramite Gestore di sistema o la relativa CLI. Mantenere il nome utente predefinito *admin* o modificarlo in un nome utente personalizzato.
Modifica credenziali	Scegli le credenziali AWS e l'abbonamento al marketplace da utilizzare con questo sistema Cloud Volumes ONTAP. Fare clic su **Add Subscription** (Aggiungi abbonamento) per associare le credenziali selezionate a un nuovo abbonamento AWS Marketplace. L'abbonamento può essere per un contratto annuale o per pagare Cloud Volumes ONTAP a una tariffa oraria. Se si acquista una licenza direttamente da NetApp (BYOL), non è necessario un abbonamento AWS. "Scopri come aggiungere ulteriori credenziali AWS a BlueXP".

Il video seguente mostra come associare un abbonamento al Marketplace pay-as-you-go alle tue credenziali AWS:

Iscriviti a BlueXP dal marketplace AWS

Se più utenti IAM lavorano nello stesso account AWS, ciascun utente deve iscriversi. Dopo l'iscrizione, AWS Marketplace informa gli utenti successivi che sono già abbonati, come mostrato nell'immagine seguente. Mentre è in vigore un abbonamento per l' *account* AWS, ciascun utente IAM deve associarsi a tale abbonamento. Se viene visualizzato il messaggio riportato di seguito, fare clic sul collegamento **fare clic qui** per accedere al sito Web di BlueXP e completare la procedura.



5. **Servizi**: Consente di abilitare o disabilitare i singoli servizi che non si desidera utilizzare con questo sistema Cloud Volumes ONTAP.
   - "Scopri di più sulla classificazione BlueXP"
   - "Scopri di più sul backup e ripristino BlueXP"

   > Se si desidera utilizzare WORM e il tiering dei dati, è necessario disattivare il backup e il ripristino BlueXP e implementare un ambiente di lavoro Cloud Volumes ONTAP con versione 9.8 o superiore.

6. **Modelli di implementazione ha**: Scegliere una configurazione ha.

   Per una panoramica dei modelli di implementazione, vedere "Cloud Volumes ONTAP ha per AWS".

7. **Location and Connectivity** (AZ singolo) o **Region & VPC** (AZS multiplo): Inserire le informazioni di rete registrate nel foglio di lavoro AWS.

   La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Gruppo di sicurezza generato	Se si lascia che BlueXP generi il gruppo di protezione, è necessario scegliere come consentire il traffico: • Se si sceglie **Selected VPC only** (solo VPC selezionato), l'origine del traffico in entrata è l'intervallo di sottorete del VPC selezionato e l'intervallo di sottorete del VPC in cui si trova il connettore. Questa è l'opzione consigliata. • Se si sceglie **All VPC**, l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.
USA gruppo di sicurezza esistente	Se si utilizza un criterio firewall esistente, assicurarsi che includa le regole richieste. "Scopri le regole del firewall per Cloud Volumes ONTAP".

8. **Connettività e autenticazione SSH**: Scegliere i metodi di connessione per la coppia ha e il mediatore.
9. **IP mobili**: Se si sceglie più AZS, specificare gli indirizzi IP mobili.

   Gli indirizzi IP devono essere esterni al blocco CIDR per tutti i VPC della regione. Per ulteriori informazioni, vedere "Requisiti di rete AWS per Cloud Volumes ONTAP ha in più AZS".

10. **Route Table**: Se si sceglie Multiple AZS, selezionare le tabelle di routing che devono includere i percorsi verso gli indirizzi IP mobili.

    Se si dispone di più tabelle di percorso, è molto importante selezionare le tabelle di percorso corrette. In caso contrario, alcuni client potrebbero non avere accesso alla coppia Cloud Volumes ONTAP ha. Per ulteriori informazioni sulle tabelle di percorso, fare riferimento a. "Documentazione AWS: Tabelle di percorso".

11. **Crittografia dei dati**: Non scegliere alcuna crittografia dei dati o crittografia gestita da AWS.

    Per la crittografia gestita da AWS, è possibile scegliere una chiave Customer Master Key (CMK) diversa dal proprio account o da un altro account AWS.

Non è possibile modificare il metodo di crittografia dei dati AWS dopo aver creato un sistema Cloud Volumes ONTAP.

"Scopri come configurare AWS KMS per Cloud Volumes ONTAP".

"Scopri di più sulle tecnologie di crittografia supportate".

12. **Charging Methods and NSS account** (metodi di addebito e account NSS): Specificare l'opzione di addebito che si desidera utilizzare con questo sistema, quindi specificare un account NetApp Support Site.
    - "Scopri le opzioni di licenza per Cloud Volumes ONTAP".
    - "Scopri come impostare le licenze".
13. **Configurazione Cloud Volumes ONTAP** (solo contratto annuale AWS Marketplace): Esaminare la configurazione predefinita e fare clic su **continua** o su **Modifica configurazione** per selezionare la propria configurazione.

    Se si mantiene la configurazione predefinita, è sufficiente specificare un volume, quindi rivedere e approvare la configurazione.

14. **Pacchetti preconfigurati** (solo orario o BYOL): Selezionare uno dei pacchetti per avviare rapidamente Cloud Volumes ONTAP oppure fare clic su **Modifica configurazione** per selezionare la propria configurazione.

    Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.

15. **Ruolo IAM**: È meglio mantenere l'opzione predefinita per consentire a BlueXP di creare il ruolo per te.

    Se si preferisce utilizzare la propria policy, è necessario che sia conforme "Requisiti delle policy per i nodi Cloud Volumes ONTAP e il mediatore ha".

16. **Licenza**: Modificare la versione di Cloud Volumes ONTAP in base alle necessità e selezionare un tipo di istanza e la tenancy dell'istanza.

    Se è disponibile una release Release Candidate, General Availability o patch più recente per la versione selezionata, BlueXP aggiorna il sistema a quella versione durante la creazione dell'ambiente di lavoro. Ad esempio, l'aggiornamento si verifica se si seleziona Cloud Volumes ONTAP 9.10.1 e 9.10.1 P4 è disponibile. L'aggiornamento non si verifica da una release all'altra, ad esempio da 9.6 a 9.7.

17. **Risorse di storage sottostanti**: Scegliere un tipo di disco, configurare lo storage sottostante e scegliere se mantenere abilitato il tiering dei dati.

    Tenere presente quanto segue:

    - Il tipo di disco è per il volume iniziale (e l'aggregato). È possibile scegliere un tipo di disco diverso per i volumi (e gli aggregati) successivi.
    - Se si sceglie un disco gp3 o io1, BlueXP utilizza la funzionalità Elastic Volumes di AWS per aumentare automaticamente la capacità del disco di storage sottostante in base alle necessità. Puoi scegliere la capacità iniziale in base alle tue esigenze di storage e rivederla dopo l'implementazione di Cloud Volumes ONTAP. "Scopri di più sul supporto per volumi elastici in AWS".
    - Se si sceglie un disco gp2 o st1, è possibile selezionare una dimensione del disco per tutti i dischi nell'aggregato iniziale e per qualsiasi aggregato aggiuntivo creato da BlueXP quando si utilizza

l'opzione di provisioning semplice. È possibile creare aggregati che utilizzano una dimensione del disco diversa utilizzando l'opzione di allocazione avanzata.

- Quando si crea o si modifica un volume, è possibile scegliere un criterio di tiering del volume specifico.
- Se si disattiva il tiering dei dati, è possibile attivarlo sugli aggregati successivi.

  "Scopri come funziona il tiering dei dati".

18. **Velocità di scrittura e WORM**:

    a. Scegliere **normale** o **alta** velocità di scrittura, se lo si desidera.

    "Scopri di più sulla velocità di scrittura".

    b. Attivare lo storage WORM (Write Once, Read Many), se lo si desidera.

    NON è possibile attivare WORM se il tiering dei dati è stato abilitato per Cloud Volumes ONTAP versione 9.7 e precedenti. Il ripristino o il downgrade a Cloud Volumes ONTAP 9.8 viene bloccato dopo l'abilitazione DI WORM e tiering.

    "Scopri di più sullo storage WORM".

    a. Se si attiva lo storage WORM, selezionare il periodo di conservazione.

19. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

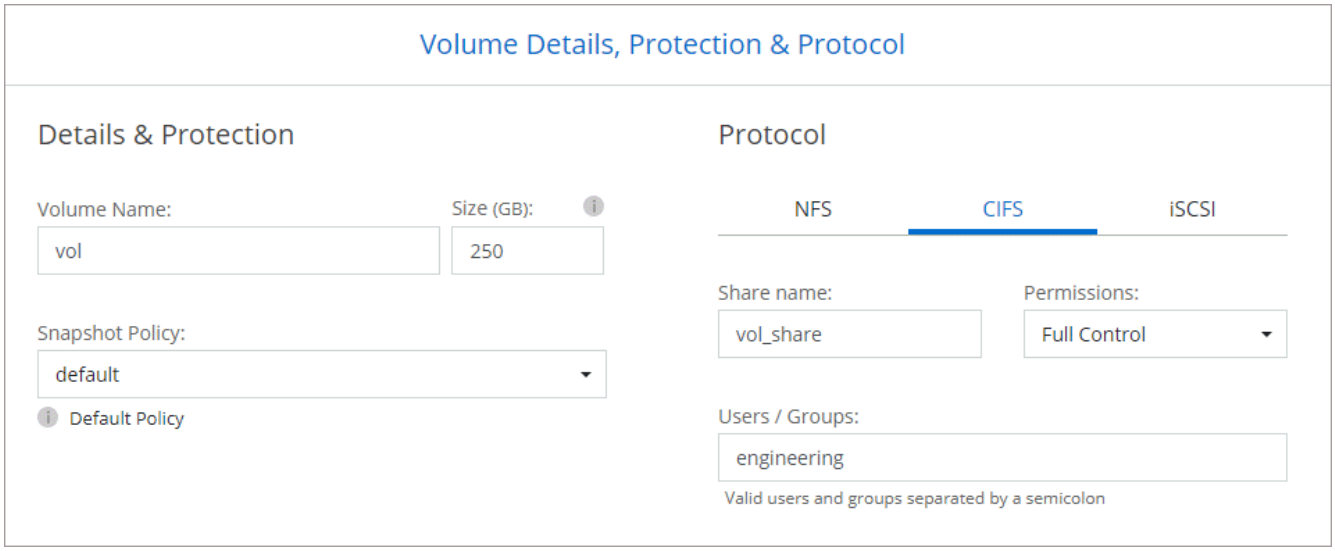
    "Scopri le versioni e i protocolli client supportati".

    Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

Campo	Descrizione
Dimensione	Le dimensioni massime che è possibile inserire dipendono in gran parte dall'attivazione o meno del thin provisioning, che consente di creare un volume più grande dello storage fisico attualmente disponibile per l'IT.
Controllo degli accessi (solo per NFS)	Un criterio di esportazione definisce i client nella subnet che possono accedere al volume. Per impostazione predefinita, BlueXP inserisce un valore che fornisce l'accesso a tutte le istanze della subnet.
Permessi e utenti/gruppi (solo per CIFS)	Questi campi consentono di controllare il livello di accesso a una condivisione per utenti e gruppi (detti anche elenchi di controllo degli accessi o ACL). È possibile specificare utenti o gruppi Windows locali o di dominio, utenti o gruppi UNIX. Se si specifica un nome utente Windows di dominio, è necessario includere il dominio dell'utente utilizzando il formato dominio/nome utente.
Policy di Snapshot	Una policy di copia Snapshot specifica la frequenza e il numero di copie Snapshot NetApp create automaticamente. Una copia Snapshot di NetApp è un'immagine del file system point-in-time che non ha alcun impatto sulle performance e richiede uno storage minimo. È possibile scegliere il criterio predefinito o nessuno. È possibile scegliere nessuno per i dati transitori, ad esempio tempdb per Microsoft SQL Server.
Opzioni avanzate (solo per NFS)	Selezionare una versione NFS per il volume: NFSv3 o NFSv4.

Campo	Descrizione
Initiator group e IQN (solo per iSCSI)	Le destinazioni di storage iSCSI sono denominate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. I gruppi di iniziatori sono tabelle dei nomi dei nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN. Le destinazioni iSCSI si collegano alla rete tramite schede di rete Ethernet standard (NIC), schede TOE (TCP offload Engine) con iniziatori software, adattatori di rete convergenti (CNA) o adattatori host busto dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN). Quando si crea un volume iSCSI, BlueXP crea automaticamente un LUN. Abbiamo semplificato la creazione di un solo LUN per volume, per cui non è necessario alcun intervento di gestione. Dopo aver creato il volume, "Utilizzare IQN per connettersi al LUN dagli host".

La seguente immagine mostra la pagina Volume compilata per il protocollo CIFS:



20. **CIFS Setup**: Se è stato selezionato il protocollo CIFS, impostare un server CIFS.

Campo	Descrizione
Indirizzo IP primario e secondario DNS	Gli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server CIFS. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server CIFS si unisce.
Dominio Active Directory da unire	L'FQDN del dominio Active Directory (ad) a cui si desidera che il server CIFS si unisca.
Credenziali autorizzate per l'accesso al dominio	Il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer all'unità organizzativa (OU) specificata nel dominio ad.
Nome NetBIOS del server CIFS	Un nome server CIFS univoco nel dominio ad.
Unità organizzativa	L'unità organizzativa all'interno del dominio ad da associare al server CIFS. L'impostazione predefinita è CN=computer. Se si configura AWS Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=corp** in questo campo.

Campo	Descrizione
Dominio DNS	Il dominio DNS per la SVM (Storage Virtual Machine) di Cloud Volumes ONTAP. Nella maggior parte dei casi, il dominio è lo stesso del dominio ad.
Server NTP	Selezionare **Use Active Directory Domain** (Usa dominio Active Directory) per configurare un server NTP utilizzando il DNS di Active Directory. Se è necessario configurare un server NTP utilizzando un indirizzo diverso, utilizzare l'API. Vedere "Documenti sull'automazione BlueXP" per ulteriori informazioni. Nota: È possibile configurare un server NTP solo quando si crea un server CIFS. Non è configurabile dopo aver creato il server CIFS.

21. **Profilo di utilizzo, tipo di disco e policy di tiering**: Scegliere se attivare le funzionalità di efficienza dello storage e modificare la policy di tiering dei volumi, se necessario.

    Per ulteriori informazioni, vedere "Scegliere un profilo di utilizzo del volume" e. "Panoramica sul tiering dei dati".

22. **Review & Approve** (Rivedi e approva): Consente di rivedere e confermare le selezioni.
    a. Esaminare i dettagli della configurazione.
    b. Fare clic su **ulteriori informazioni** per visualizzare i dettagli relativi al supporto e alle risorse AWS che BlueXP acquisterà.
    c. Selezionare le caselle di controllo **ho capito…**.
    d. Fare clic su **Go**.

Risultato

BlueXP lancia la coppia Cloud Volumes ONTAP ha. Puoi tenere traccia dei progressi nella timeline.

In caso di problemi durante l'avvio della coppia ha, esaminare il messaggio di errore. È inoltre possibile selezionare l'ambiente di lavoro e fare clic su Re-create environment (Crea ambiente).

Per ulteriore assistenza, visitare il sito Web all'indirizzo "Supporto NetApp Cloud Volumes ONTAP".

Al termine

- Se è stata fornita una condivisione CIFS, assegnare agli utenti o ai gruppi le autorizzazioni per i file e le cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file.
- Se si desidera applicare le quote ai volumi, utilizzare System Manager o l'interfaccia CLI.

  Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree.

Inizia a utilizzare Cloud Volumes ONTAP nell'ambiente AWS C2S

Analogamente a un'area AWS standard, è possibile utilizzare Cloud Manager in "Servizi cloud commerciali AWS (C2S)" Ambiente per l'implementazione di Cloud Volumes ONTAP, che offre funzionalità di livello Enterprise per il tuo cloud storage. AWS C2S è una regione chiusa specifica per gli Stati Uniti Intelligence Community; le istruzioni

riportate in questa pagina si applicano solo agli utenti della regione AWS C2S.

Versioni supportate in C2S

- Cloud Volumes ONTAP 9.8 è supportato
- È supportata la versione 3.9.4 del connettore

  Il connettore è un software necessario per implementare e gestire Cloud Volumes ONTAP in AWS. Potrai accedere a Cloud Manager dal software installato sull'istanza di Connector. Il sito Web SaaS per Cloud Manager non è supportato nell'ambiente C2S.

> Cloud Manager è stato recentemente rinominato BlueXP, ma continuiamo a chiamarlo Cloud Manager in C2S perché l'interfaccia utente inclusa con la versione 3.9.4 del connettore è ancora chiamata Cloud Manager.

Funzionalità supportate in C2S

Cloud Manager offre le seguenti funzionalità nell'ambiente C2S:

- Cloud Volumes ONTAP
- Replica dei dati
- Una tempistica per il controllo

Per Cloud Volumes ONTAP, è possibile creare un sistema a nodo singolo o una coppia ha. Sono disponibili entrambe le opzioni di licenza: Pay-as-you-go e Bring Your Own License (BYOL).

Il tiering dei dati in S3 è supportato anche con Cloud Volumes ONTAP in C2S.

Limitazioni

- Nessuno dei servizi cloud di NetApp è disponibile da Cloud Manager.
- Poiché l'ambiente C2S non dispone di accesso a Internet, non sono disponibili le seguenti funzionalità:
  - Aggiornamenti software automatici da Cloud Manager
  - NetApp AutoSupport
  - Informazioni sui costi AWS per le risorse Cloud Volumes ONTAP
- Le licenze Freemium non sono supportate nell'ambiente C2S.

Panoramica dell'implementazione

La guida introduttiva a Cloud Volumes ONTAP in C2S include alcuni passaggi.

1. Preparazione dell'ambiente AWS

   Ciò include la configurazione della rete, l'iscrizione a Cloud Volumes ONTAP, la configurazione delle autorizzazioni e, facoltativamente, la configurazione di AWS KMS.

2. Installazione del connettore e configurazione di Cloud Manager

   Prima di iniziare a utilizzare Cloud Manager per implementare Cloud Volumes ONTAP, è necessario creare

un *connettore*. Il connettore consente a Cloud Manager di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico (incluso Cloud Volumes ONTAP).

Potrai accedere a Cloud Manager dal software installato sull'istanza di Connector.

3. Avvio di Cloud Volumes ONTAP da Cloud Manager

Ciascuno di questi passaggi è descritto di seguito.

Preparazione dell'ambiente AWS

L'ambiente AWS deve soddisfare alcuni requisiti.

Configurare la rete

Configurare la rete AWS in modo che Cloud Volumes ONTAP possa funzionare correttamente.

Fasi

1. Scegliere il VPC e le subnet in cui si desidera avviare l'istanza di Connector e le istanze di Cloud Volumes ONTAP.
2. Assicurarsi che il VPC e le subnet supportino la connettività tra il connettore e Cloud Volumes ONTAP.
3. Impostare un endpoint VPC sul servizio S3.

   È necessario un endpoint VPC se si desidera eseguire il tiering dei dati cold da Cloud Volumes ONTAP a uno storage a oggetti a basso costo.

Iscriviti a Cloud Volumes ONTAP

Per implementare Cloud Volumes ONTAP da Cloud Manager è necessario un abbonamento a Marketplace.

Fasi

1. Accedere al marketplace della community di AWS Intelligence e cercare Cloud Volumes ONTAP.
2. Seleziona l'offerta che intendi implementare.
3. Leggere i termini e fare clic su **Accept** (Accetta).
4. Ripetere questi passaggi per le altre offerte, se si prevede di implementarle.

   È necessario utilizzare Cloud Manager per avviare le istanze di Cloud Volumes ONTAP. Non è necessario avviare le istanze di Cloud Volumes ONTAP dalla console EC2.

Impostare le autorizzazioni

Impostare i ruoli e le policy IAM che forniscono a Connector e Cloud Volumes ONTAP le autorizzazioni necessarie per eseguire le azioni nell'ambiente dei servizi cloud commerciali AWS.

È necessario disporre di una policy IAM e di un ruolo IAM per ciascuno dei seguenti elementi:

- L'istanza del connettore
- Istanze di Cloud Volumes ONTAP
- Istanza di Cloud Volumes ONTAP ha Mediator (se si desidera implementare coppie ha)

Fasi

1. Accedere alla console AWS IAM e fare clic su **Policies** (Criteri).
2. Creare un criterio per l'istanza del connettore.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
```

```
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
```

```
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

3. Creare un criterio per Cloud Volumes ONTAP.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

4. Se si prevede di implementare una coppia Cloud Volumes ONTAP ha, creare una policy per il mediatore ha.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Creare ruoli IAM con il tipo di ruolo Amazon EC2 e allegare i criteri creati nei passaggi precedenti.

   Analogamente ai criteri, è necessario disporre di un ruolo IAM per il connettore, uno per i nodi Cloud Volumes ONTAP e uno per il mediatore ha (se si desidera implementare le coppie ha).

   Quando si avvia l'istanza di Connector, è necessario selezionare il ruolo di Connector IAM.

   È possibile selezionare i ruoli IAM per Cloud Volumes ONTAP e il mediatore ha quando si crea un ambiente di lavoro Cloud Volumes ONTAP da Cloud Manager.

Configurare AWS KMS

Se desideri utilizzare la crittografia Amazon con Cloud Volumes ONTAP, assicurati che siano soddisfatti i requisiti per il servizio di gestione delle chiavi AWS.

Fasi

1. Assicurarsi che nel proprio account o in un altro account AWS sia presente una chiave Customer Master Key (CMK) attiva.

   Il CMK può essere un CMK gestito da AWS o un CMK gestito dal cliente.

2. Se il CMK si trova in un account AWS separato dall'account in cui si intende implementare Cloud Volumes ONTAP, è necessario ottenere l'ARN di tale chiave.

   Quando crei il sistema Cloud Volumes ONTAP, dovrai fornire l'ARN a Cloud Manager.

3. Aggiungere il ruolo IAM per l'istanza del connettore all'elenco degli utenti chiave per una CMK.

   In questo modo, Cloud Manager dispone delle autorizzazioni per l'utilizzo del CMK con Cloud Volumes ONTAP.

Installazione del connettore e configurazione di Cloud Manager

Prima di avviare i sistemi Cloud Volumes ONTAP in AWS, è necessario avviare l'istanza di Connector da AWS Marketplace, quindi accedere e configurare Cloud Manager.

Fasi

1. Ottenere un certificato root firmato da un'autorità di certificazione (CA) nel formato X.509 codificato con Privacy Enhanced Mail (PEM) base-64. Per ottenere il certificato, consultare le policy e le procedure della propria organizzazione.

   Durante il processo di configurazione, è necessario caricare il certificato. Cloud Manager utilizza il certificato attendibile per l'invio di richieste ad AWS su HTTPS.

2. Avviare l'istanza di Connector:
   a. Vai alla pagina AWS Intelligence Community Marketplace per Cloud Manager.
   b. Nella scheda Custom Launch (Avvio personalizzato), scegliere l'opzione per avviare l'istanza dalla console EC2.
   c. Seguire le istruzioni per configurare l'istanza.

      Durante la configurazione dell'istanza, tenere presente quanto segue:

      - Si consiglia di utilizzare t3.xlarge.
      - È necessario scegliere il ruolo IAM creato durante la preparazione dell'ambiente AWS.
      - È necessario mantenere le opzioni di storage predefinite.
      - I metodi di connessione richiesti per il connettore sono i seguenti: SSH, HTTP e HTTPS.
3. Configurare Cloud Manager da un host che dispone di una connessione all'istanza del connettore:
   a. Aprire un browser Web e immettere https://ipaddress Dove ipaddress è l’indirizzo IP dell’host Linux in cui è stato installato il connettore.
   b. Specificare un server proxy per la connettività ai servizi AWS.
   c. Caricare il certificato ottenuto al punto 1.
   d. Completare la procedura di installazione guidata per configurare Cloud Manager.
      - **Dettagli sistema**: Immettere un nome per questa istanza di Cloud Manager e fornire il nome della società.
      - **Create User** (Crea utente): Consente di creare l'utente Admin da utilizzare per amministrare Cloud Manager.
      - **Revisione**: Esaminare i dettagli e approvare il contratto di licenza per l'utente finale.
   e. Per completare l'installazione del certificato firmato dalla CA, riavviare l'istanza del connettore dalla console EC2.
4. Una volta riavviato il connettore, accedere utilizzando l'account utente amministratore creato nell'installazione guidata.

Avvio di Cloud Volumes ONTAP da Cloud Manager

È possibile avviare le istanze di Cloud Volumes ONTAP nell'ambiente dei servizi cloud commerciali AWS creando nuovi ambienti di lavoro in Cloud Manager.

Di cosa hai bisogno

- Se è stata acquistata una licenza, è necessario disporre del file di licenza ricevuto da NetApp. Il file di licenza è un file .NLF in formato JSON.
- È necessaria una coppia di chiavi per abilitare l'autenticazione SSH basata su chiave al mediatore ha.

Fasi

1. Nella pagina ambienti di lavoro, fare clic su **Aggiungi ambiente di lavoro**.
2. In Crea, selezionare Cloud Volumes ONTAP o Cloud Volumes ONTAP ha.
3. Completare la procedura guidata per avviare il sistema Cloud Volumes ONTAP.

   Al termine della procedura guidata, tenere presente quanto segue:

   - Se si desidera implementare Cloud Volumes ONTAP ha in più zone di disponibilità, implementare la configurazione come segue, poiché solo due AZS erano disponibili nell'ambiente dei servizi cloud commerciali AWS al momento della pubblicazione:
     - Nodo 1: Zona di disponibilità A.
     - Nodo 2: Zona di disponibilità B
     - Mediatore: Zona di disponibilità A o B.
   - Lasciare l'opzione predefinita per utilizzare un gruppo di protezione generato.

     Il gruppo di protezione predefinito include le regole necessarie per il corretto funzionamento di Cloud Volumes ONTAP. Se hai un requisito per utilizzare il tuo, puoi fare riferimento alla sezione relativa al gruppo di sicurezza riportata di seguito.
   - È necessario scegliere il ruolo IAM creato durante la preparazione dell'ambiente AWS.
   - Il tipo di disco AWS sottostante è per il volume Cloud Volumes ONTAP iniziale.

     È possibile scegliere un tipo di disco diverso per i volumi successivi.
   - Le prestazioni dei dischi AWS sono legate alle dimensioni dei dischi.

     È necessario scegliere le dimensioni del disco in grado di garantire le prestazioni costanti necessarie. Fare riferimento alla documentazione AWS per ulteriori dettagli sulle prestazioni EBS.
   - La dimensione del disco è la dimensione predefinita per tutti i dischi del sistema.

     > Se in un secondo momento è necessaria una dimensione diversa, è possibile utilizzare l'opzione Advanced allocation (allocazione avanzata) per creare un aggregato che utilizza dischi di una dimensione specifica.
   - Le funzionalità di efficienza dello storage possono migliorare l'utilizzo dello storage e ridurre la quantità totale di storage necessaria.

Risultato

Cloud Manager avvia l'istanza di Cloud Volumes ONTAP. Puoi tenere traccia dei progressi nella timeline.

Regole del gruppo di sicurezza

Cloud Manager crea gruppi di sicurezza che includono le regole in entrata e in uscita di cui Cloud Manager e Cloud Volumes ONTAP hanno bisogno per operare con successo nel cloud. Si consiglia di fare riferimento alle

porte a scopo di test o se si preferisce utilizzare i propri gruppi di protezione.

Gruppo di sicurezza per il connettore

Il gruppo di protezione per il connettore richiede regole sia in entrata che in uscita.

Regole in entrata

Protocollo	Porta	Scopo
SSH	22	Fornisce l'accesso SSH all'host del connettore
HTTP	80	Fornisce l'accesso HTTP dai browser Web client all'interfaccia utente locale
HTTPS	443	Fornisce l'accesso HTTPS dai browser Web client all'interfaccia utente locale

Regole in uscita

Il gruppo di protezione predefinito per il connettore 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

Gruppo di sicurezza per Cloud Volumes ONTAP

Il gruppo di sicurezza per i nodi 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	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

Protocollo	Porta	Scopo
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
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 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

Gruppo di sicurezza esterno per il 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

L’origine delle regole in entrata è il traffico proveniente dal VPC in cui si trova il connettore.

Protocollo	Porta	Scopo
SSH	22	Connessioni SSH al mediatore ha
TCP	3000	Accesso API RESTful dal connettore

Regole 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

Gruppo di sicurezza interno per il mediatore ha

Il gruppo di sicurezza interno predefinito per il mediatore ha Cloud Volumes ONTAP include le seguenti regole. Cloud Manager crea sempre questo gruppo di sicurezza. 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