Inizia subito

Cloud Volumes ONTAP

NetApp
June 27, 2024

Sommario

Inizia subito 1
Scopri di più su Cloud Volumes ONTAP 1
Versioni supportate per le nuove implementazioni 2
Inizia con Amazon Web Services 4
Inizia a utilizzare Microsoft Azure 72
Inizia a utilizzare Google Cloud 110

Inizia subito

Scopri di più su Cloud Volumes ONTAP

Cloud Volumes ONTAP consente di ottimizzare i costi e le performance del cloud storage, migliorando al contempo protezione, sicurezza e conformità dei dati.

Cloud Volumes ONTAP è un'appliance di storage solo software che esegue il software di gestione dei dati ONTAP nel cloud. Fornisce storage Enterprise con le seguenti funzionalità principali, come segue per il prossimo test:

- Efficienza dello storage

  Sfrutta la deduplica dei dati integrata, la compressione dei dati, il thin provisioning e la clonazione per ridurre al minimo i costi dello storage.

- Alta disponibilità

  Garantisci l'affidabilità aziendale e le operazioni continue in caso di guasti nel tuo ambiente cloud.

- Protezione dei dati

  Cloud Volumes ONTAP sfrutta SnapMirror, la tecnologia di replica leader del settore di NetApp, per replicare i dati on-premise nel cloud, in modo da poter disporre di copie secondarie per diversi casi di utilizzo.

  Cloud Volumes ONTAP si integra anche con il backup e ripristino BlueXP per offrire funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati cloud.

  "Scopri di più sul backup e ripristino BlueXP"

- Tiering dei dati

  Passa tra pool di storage on-demand a performance elevate e basse senza portare le applicazioni offline.

- Coerenza applicativa

  Garantire la coerenza delle copie Snapshot di NetApp con NetApp SnapCenter.

  "Scopri di più su SnapCenter"

- Sicurezza dei dati

  Cloud Volumes ONTAP supporta la crittografia dei dati e fornisce protezione contro virus e ransomware.

- Controlli di conformità alla privacy

  L'integrazione con la classificazione BlueXP consente di comprendere il contesto dei dati e identificare i dati sensibili.

  "Scopri di più sulla classificazione BlueXP"

Le licenze per le funzioni ONTAP sono incluse in Cloud Volumes ONTAP.

"Visualizza le configurazioni Cloud Volumes ONTAP supportate"

"Scopri di più su Cloud Volumes ONTAP"

Versioni supportate per le nuove implementazioni

BlueXP consente di scegliere tra diverse versioni di ONTAP quando si crea un nuovo ambiente di lavoro Cloud Volumes ONTAP.

Tutte le altre versioni di Cloud Volumes ONTAP non sono supportate con le nuove implementazioni.

AWS

Nodo singolo

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9,7 P5
- 9,5 P6

Coppia HA

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9,7 P5
- 9,5 P6

Azure

Nodo singolo

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1

- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9,8 P10
- 9,7 P6
- 9,5 P6

Coppia HA

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9,8 P10
- 9,7 P6

Google Cloud

Nodo singolo

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9,8
- 9,7 P5

Coppia HA

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6

- 9,8

Inizia con Amazon Web Services

Avvio rapido di Cloud Volumes ONTAP in AWS

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

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"

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".

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".

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".

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 nodo 2	
Subnet 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

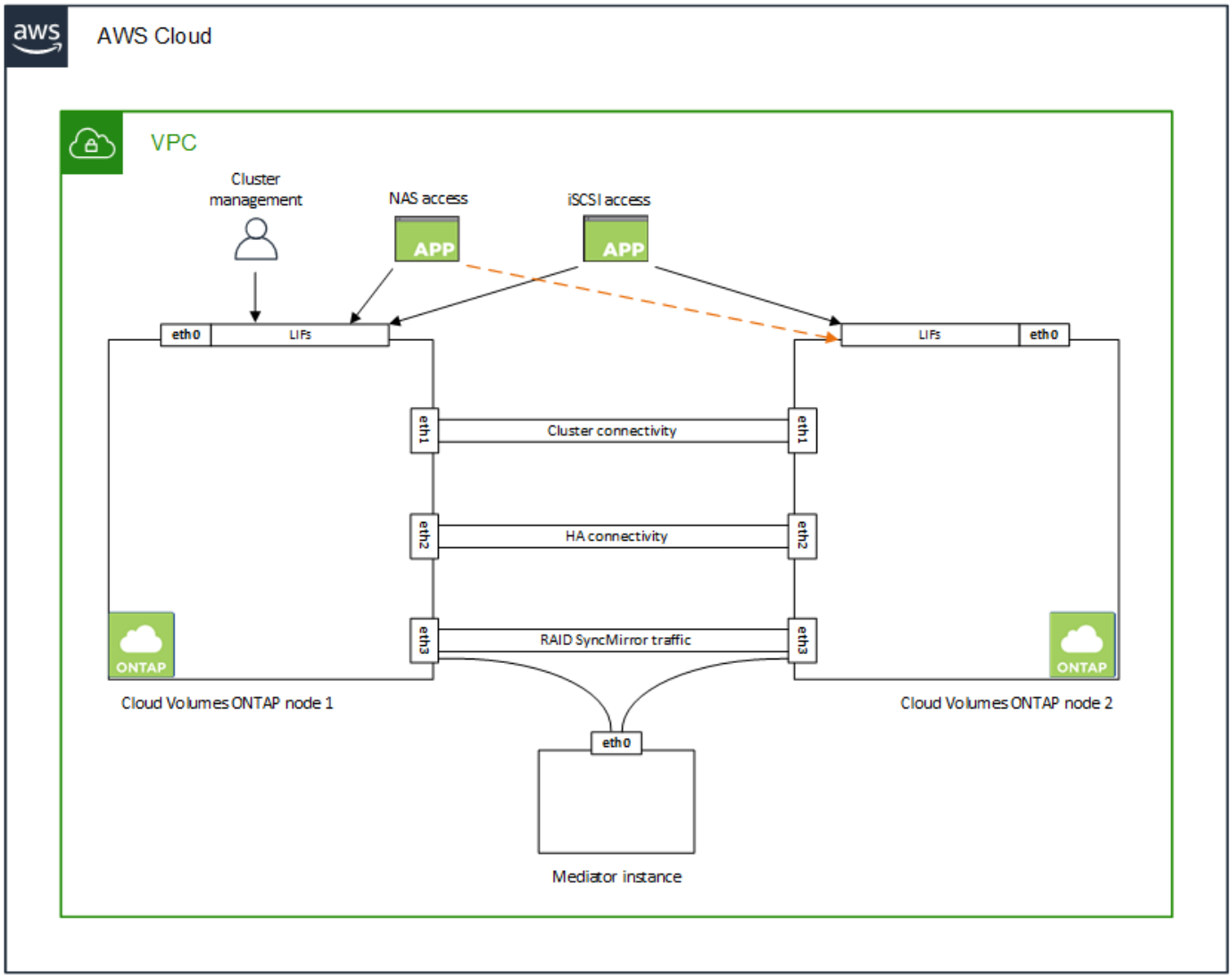
BlueXP assegna 6 indirizzi IP a un sistema a nodo singolo.

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".

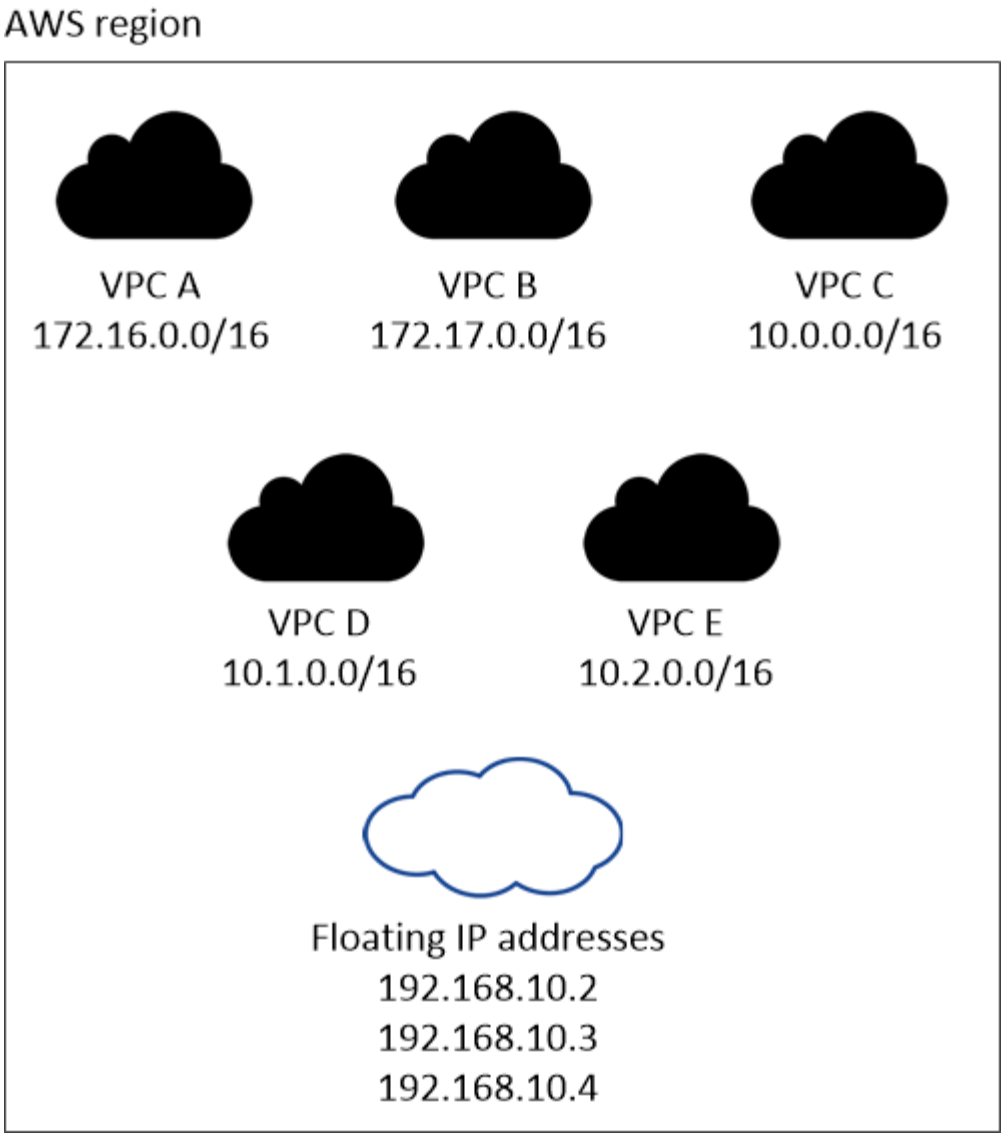
Un indirizzo IP mobile è per la gestione del cluster, uno per i dati NFS/CIFS sul nodo 1 e uno per i dati NFS/CIFS sul nodo 2. Un quarto indirizzo IP mobile per la gestione SVM è opzionale.

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".

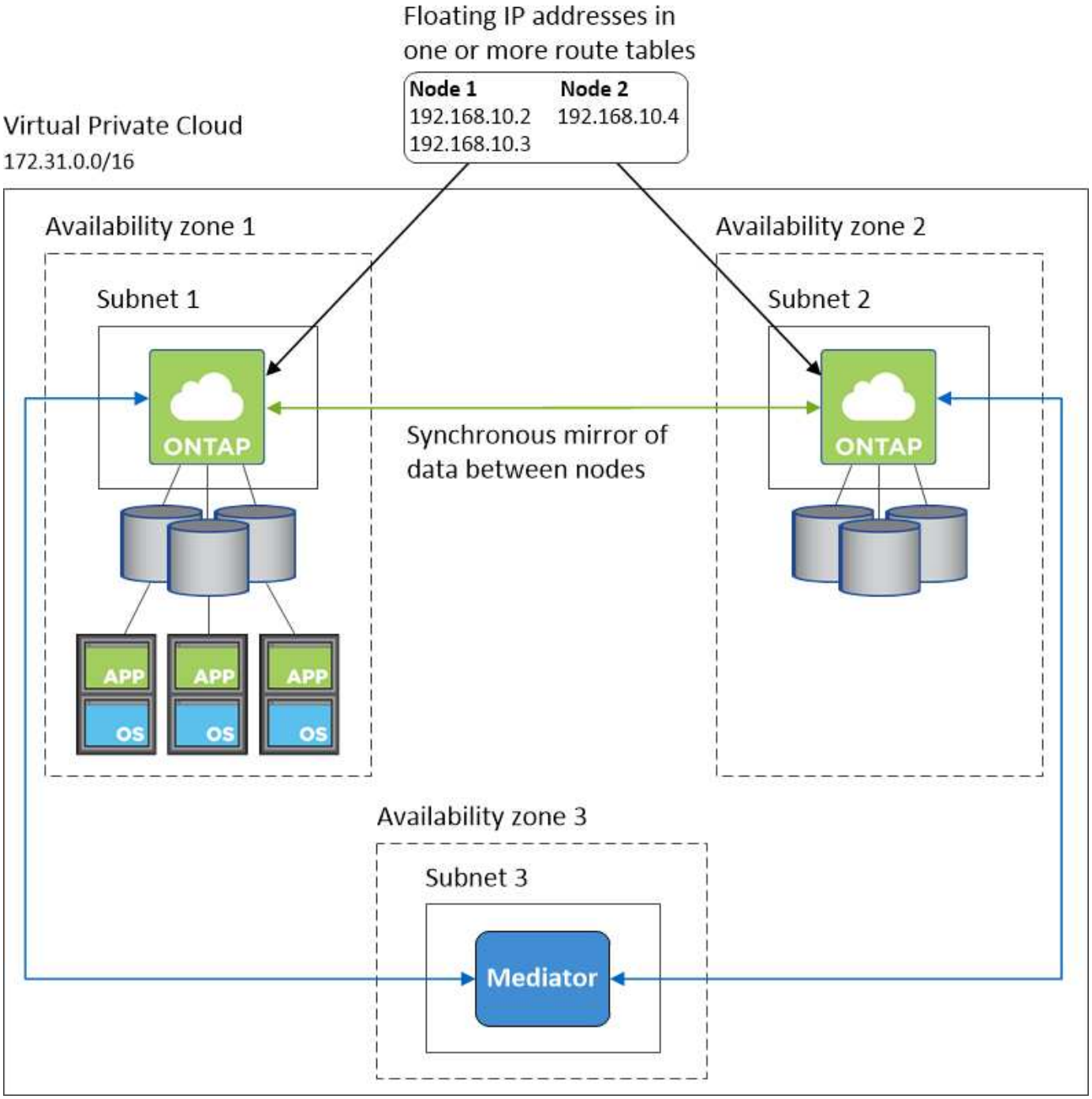
Connessione ai tool di gestione NetApp

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

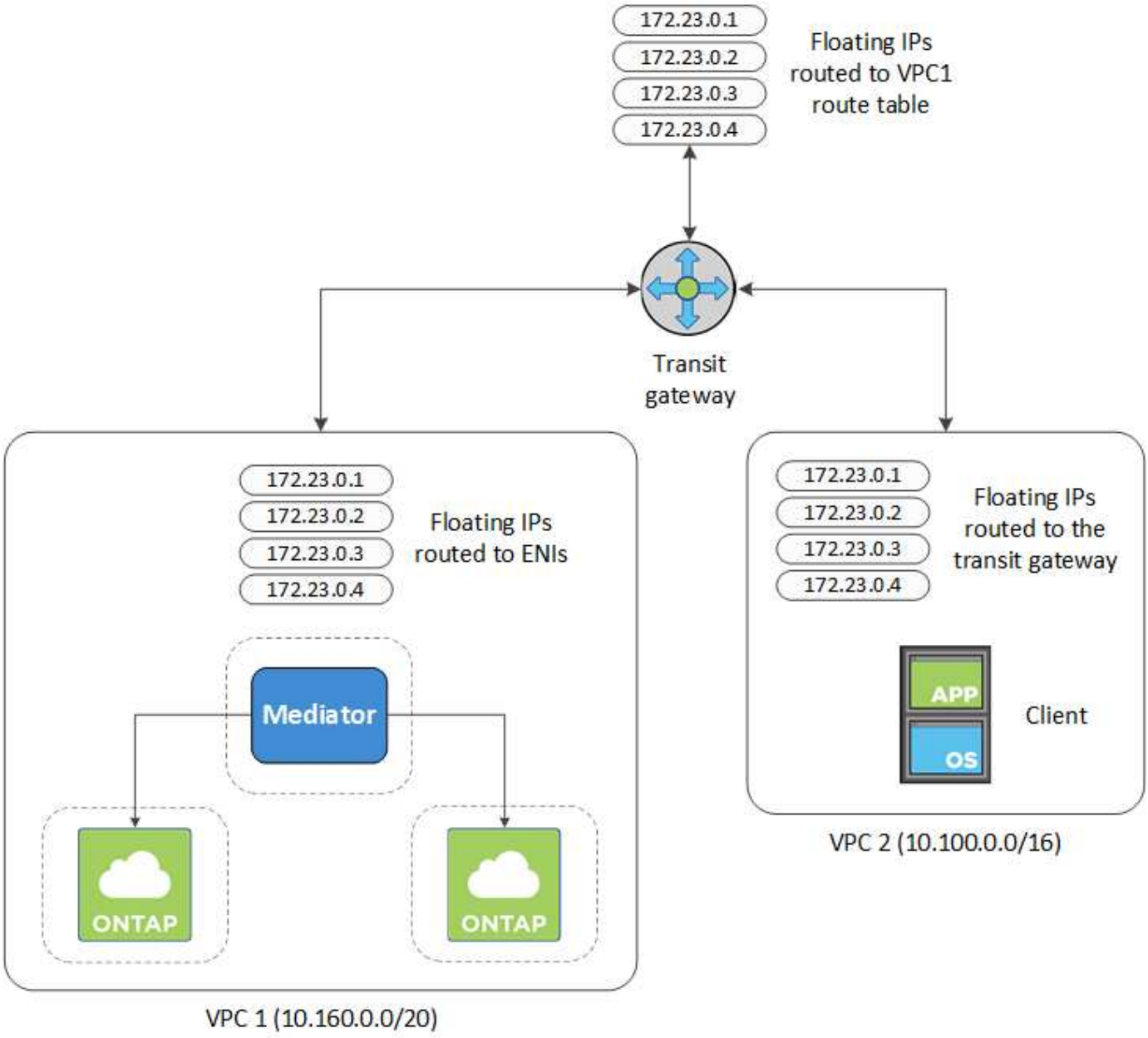
Configurare un gateway di transito AWS per consentire l'accesso a una coppia ha "Indirizzi IP mobili" Dall'esterno del VPC in cui risiede la coppia ha.

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.

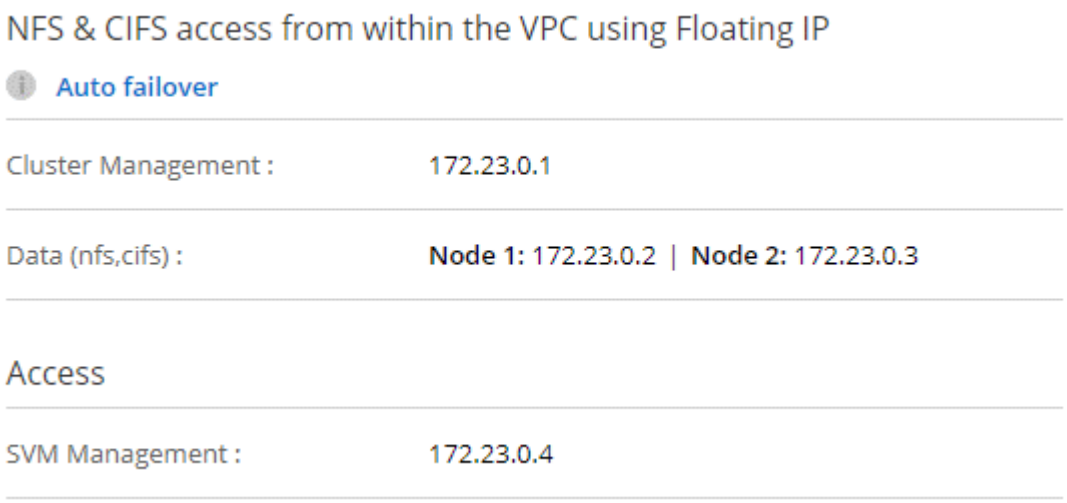


La seguente procedura illustra come configurare una configurazione simile.

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:

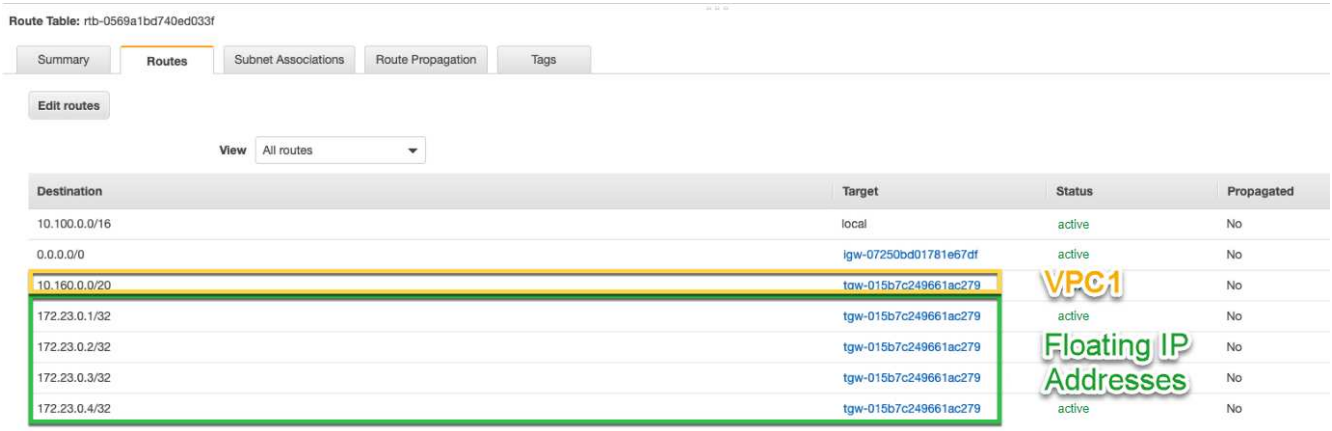


   L'immagine di esempio seguente mostra la tabella di percorso per il gateway di transito. Include le route ai blocchi CIDR dei due VPC e quattro indirizzi IP mobili utilizzati da Cloud Volumes ONTAP.

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.

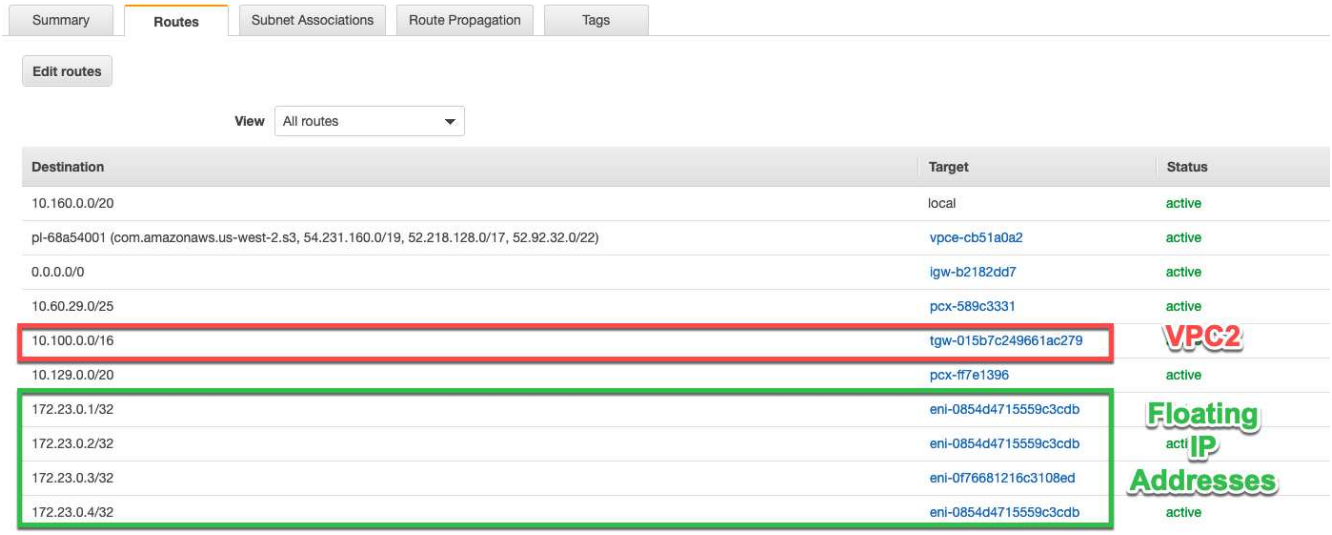
   L'immagine di esempio seguente mostra la tabella di routing per VPC 2, che include i percorsi verso VPC 1 e gli indirizzi IP mobili.



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.

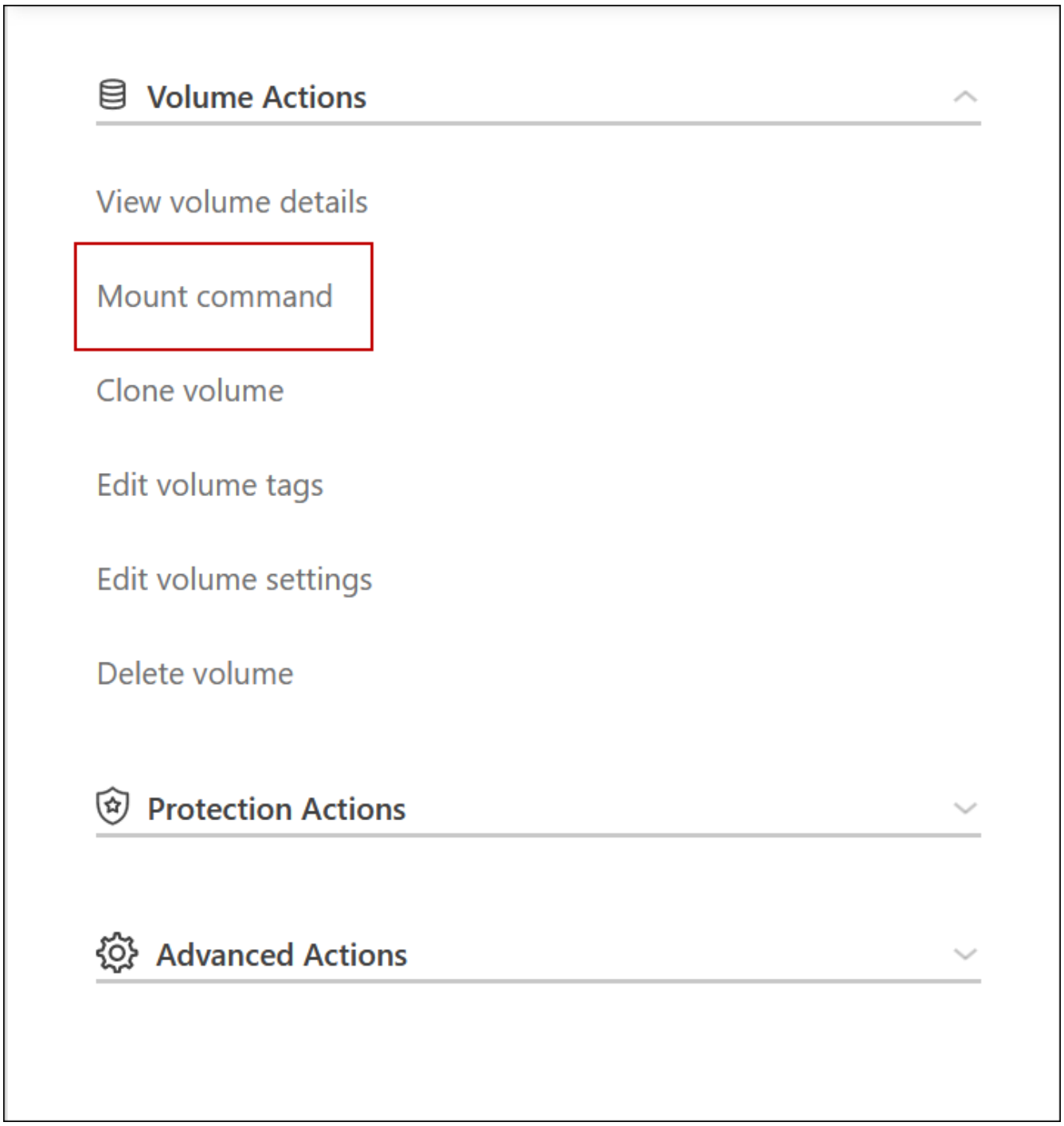
   Questo passaggio è importante perché completa il routing tra i VPC.

   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. 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.



7. 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

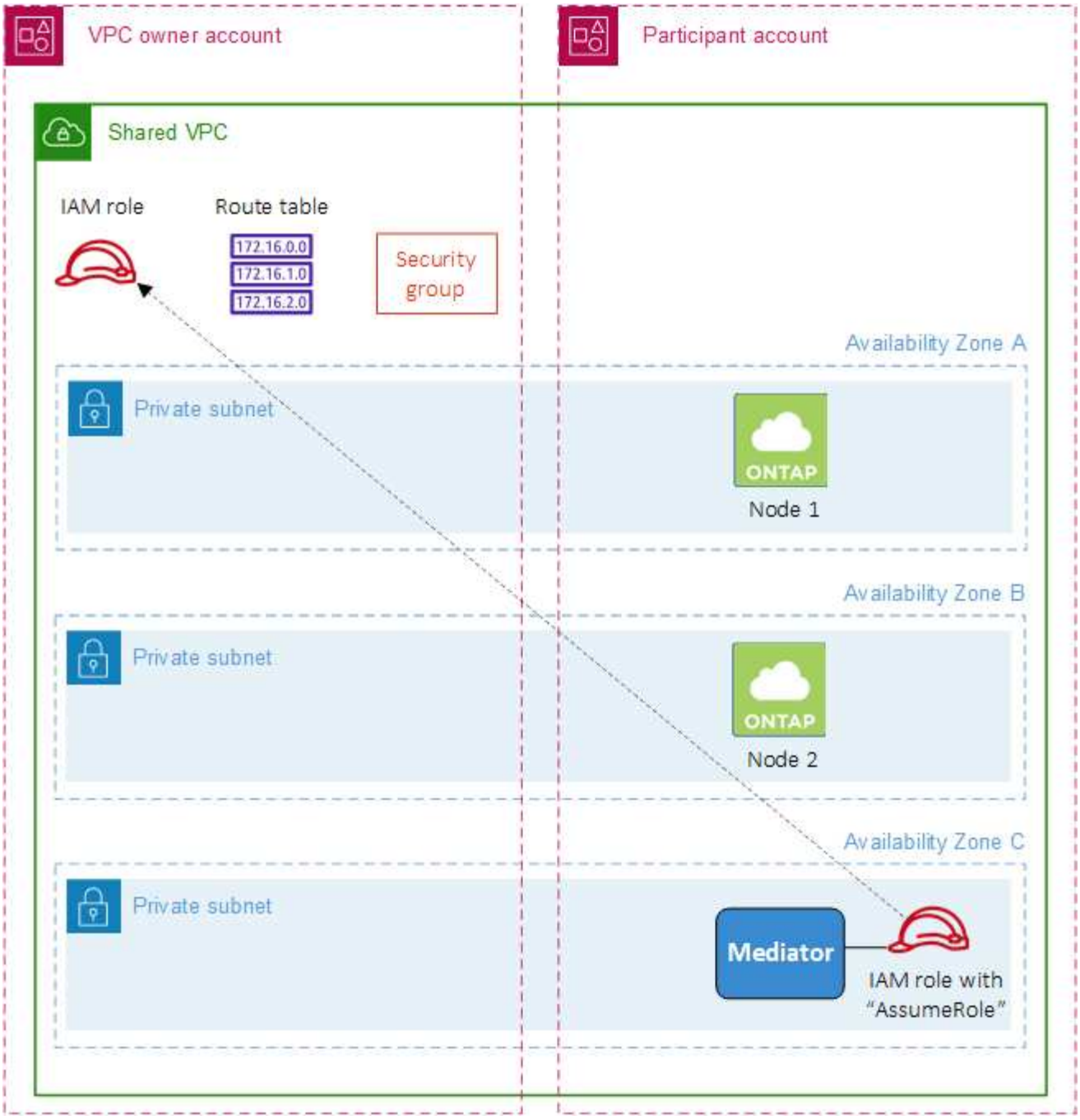
A partire dalla versione 9.11.1, le coppie Cloud Volumes ONTAP ha sono supportate in AWS con condivisione VPC. La condivisione VPC consente alla tua organizzazione di condividere le subnet con altri account AWS. Per utilizzare questa configurazione, è necessario configurare l'ambiente AWS e implementare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

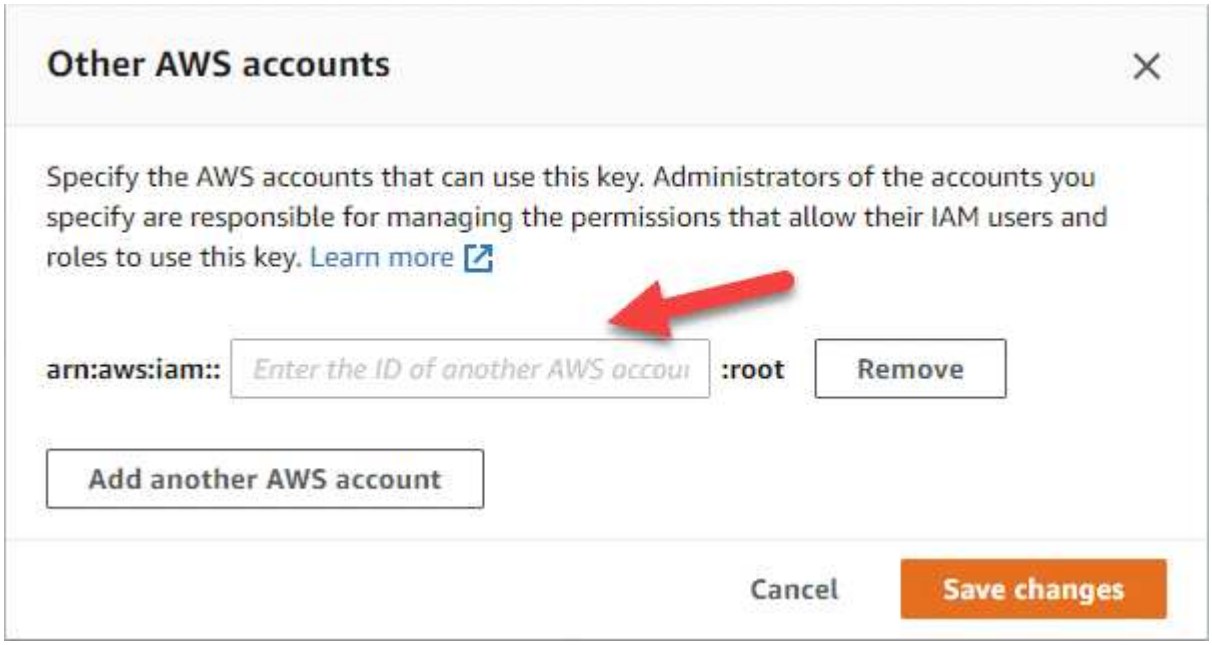
3. Se il CMK si trova in un account AWS diverso, completare la seguente procedura:

   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

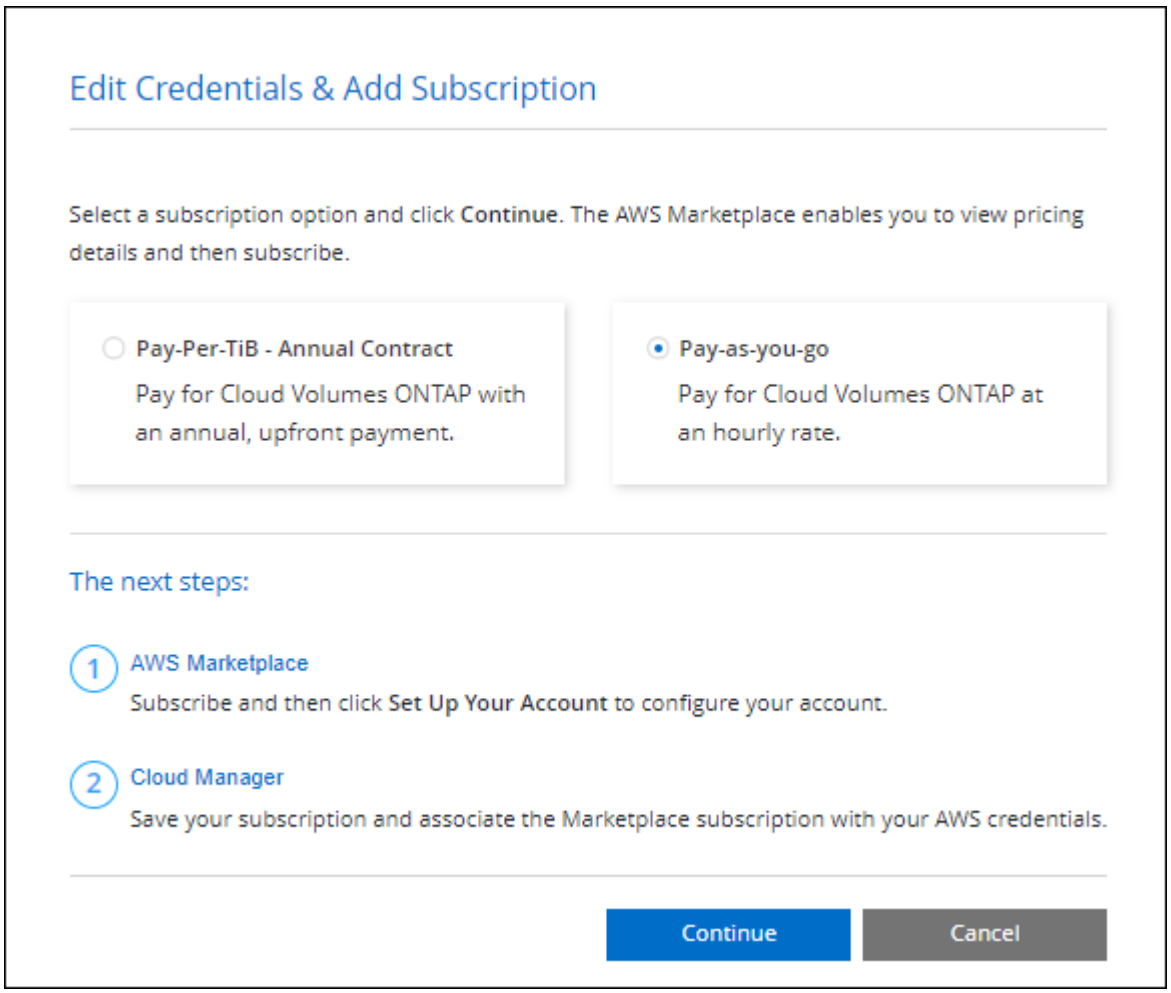
Scegli l'offerta Freemium per utilizzare Cloud Volumes ONTAP gratuitamente con un massimo di 500 GB di capacità fornita. "Scopri di più sull'offerta Freemium".

Fasi

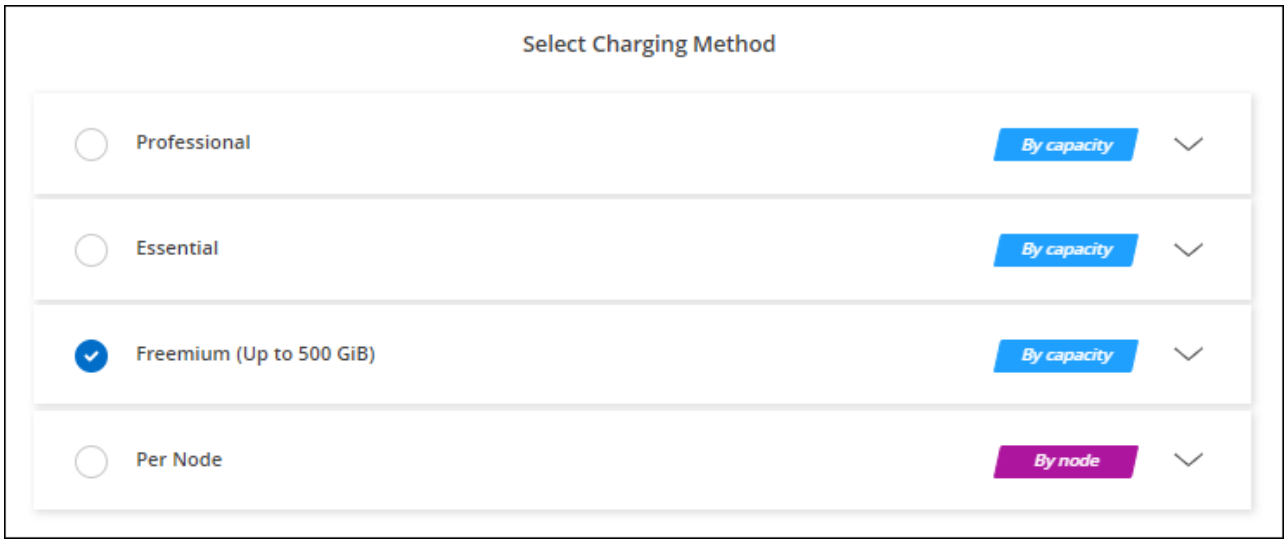
1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.

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"

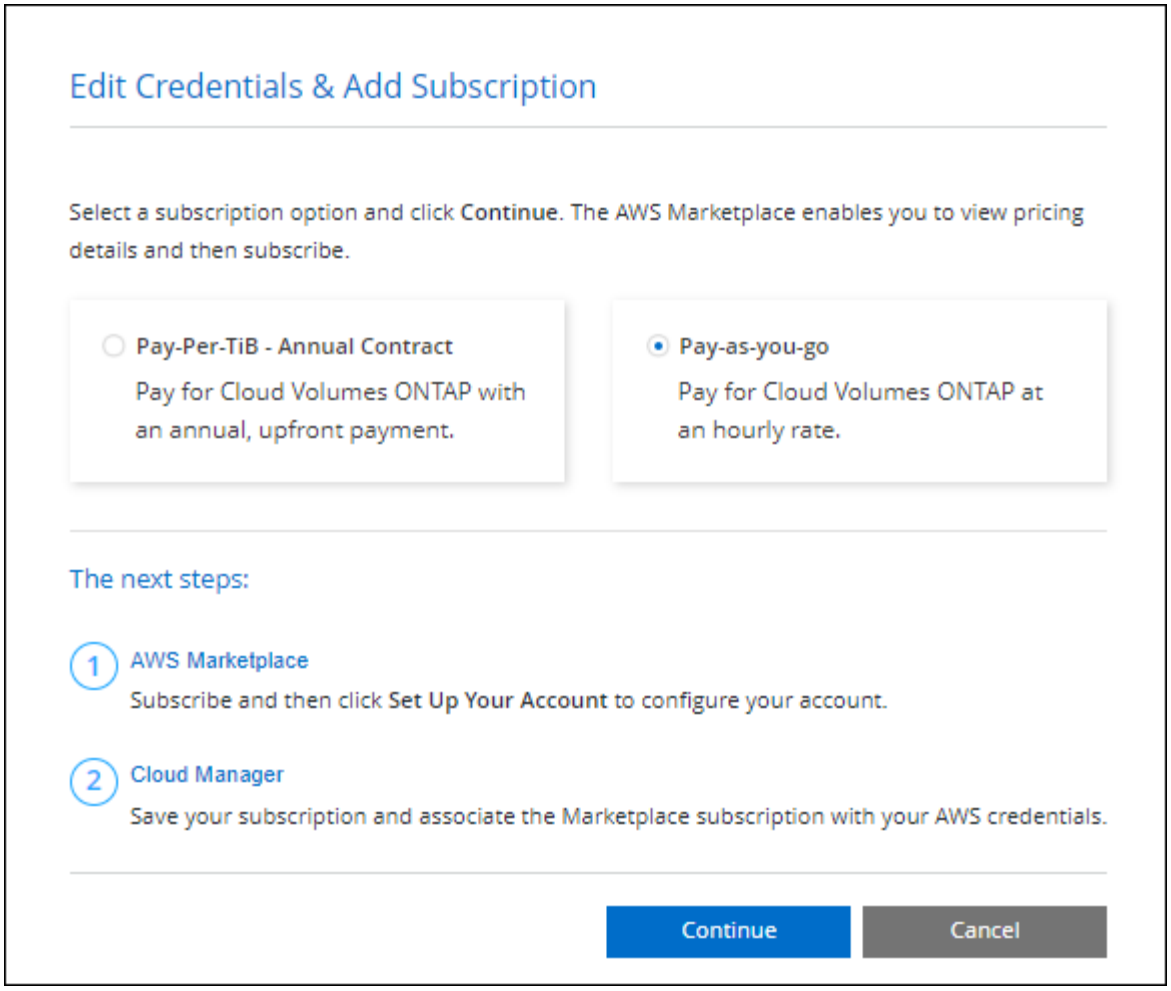
   BlueXP interroga automaticamente il servizio di licensing di NetApp per ottenere dettagli sulle licenze associate al tuo account NetApp Support Site. In assenza di errori, BlueXP aggiunge automaticamente le licenze al portafoglio digitale.

   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".

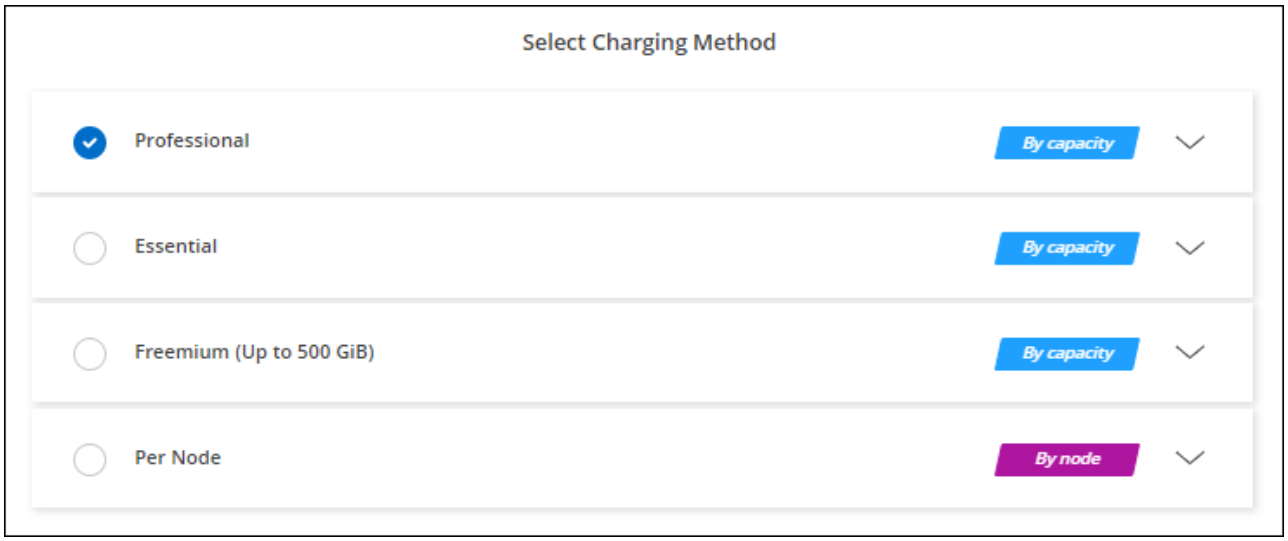
3. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.

   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".

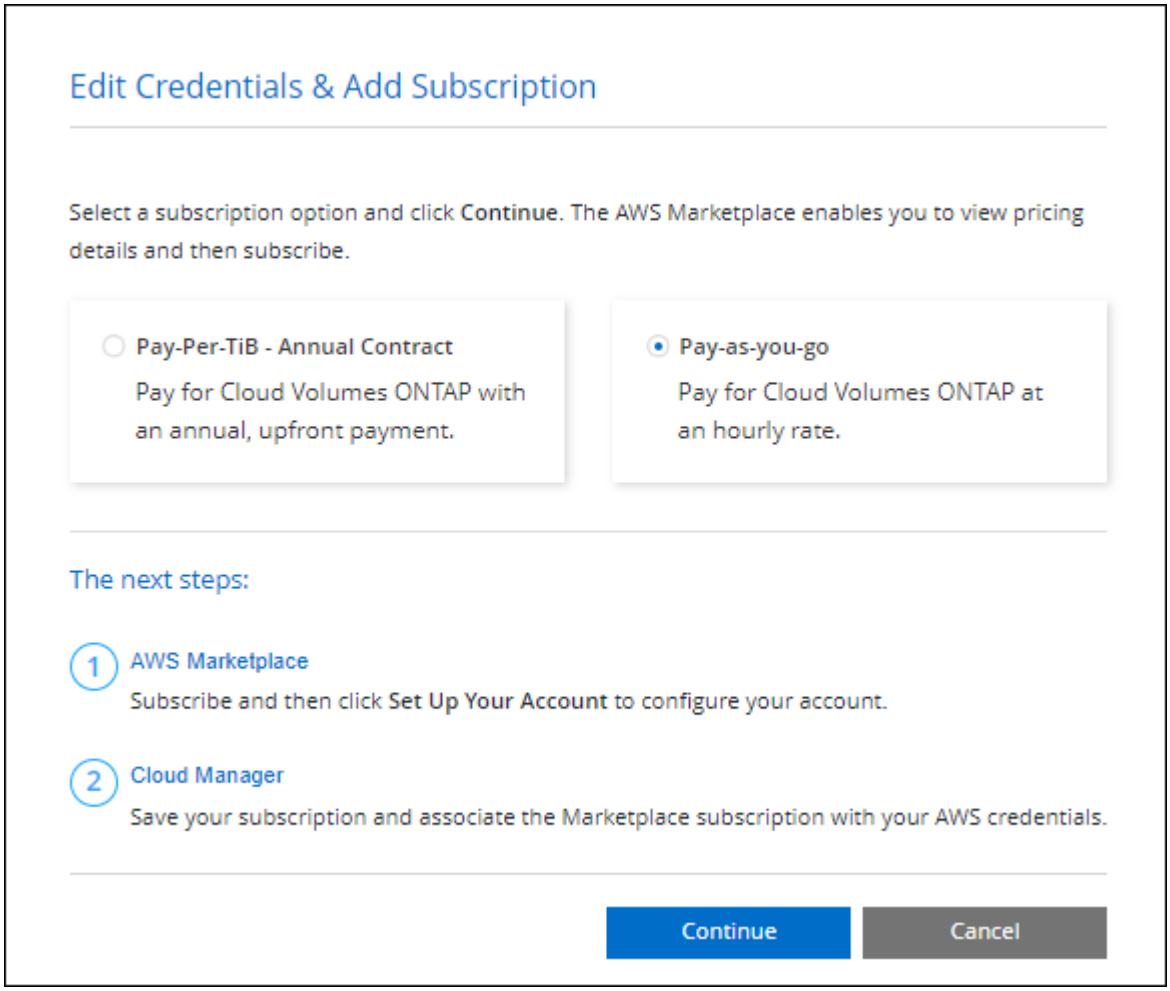
Abbonamento PAYGO

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

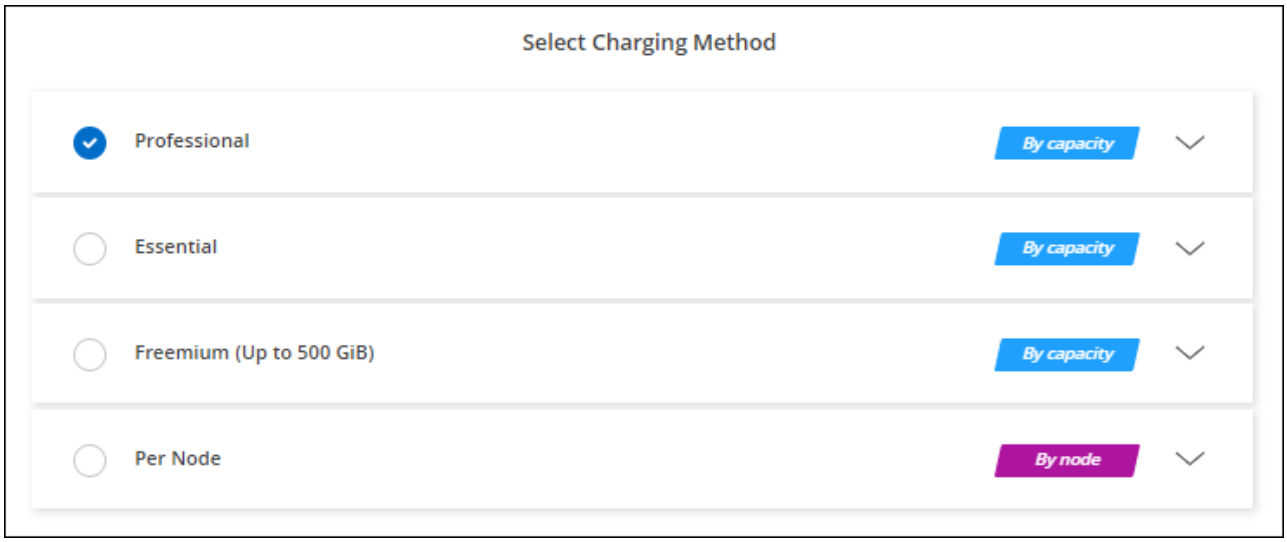
Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, BlueXP richiede di sottoscrivere il contratto disponibile nel marketplace AWS. Tale abbonamento viene quindi associato all'ambiente di lavoro per la ricarica. È possibile utilizzare lo stesso abbonamento per altri ambienti di lavoro.

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"

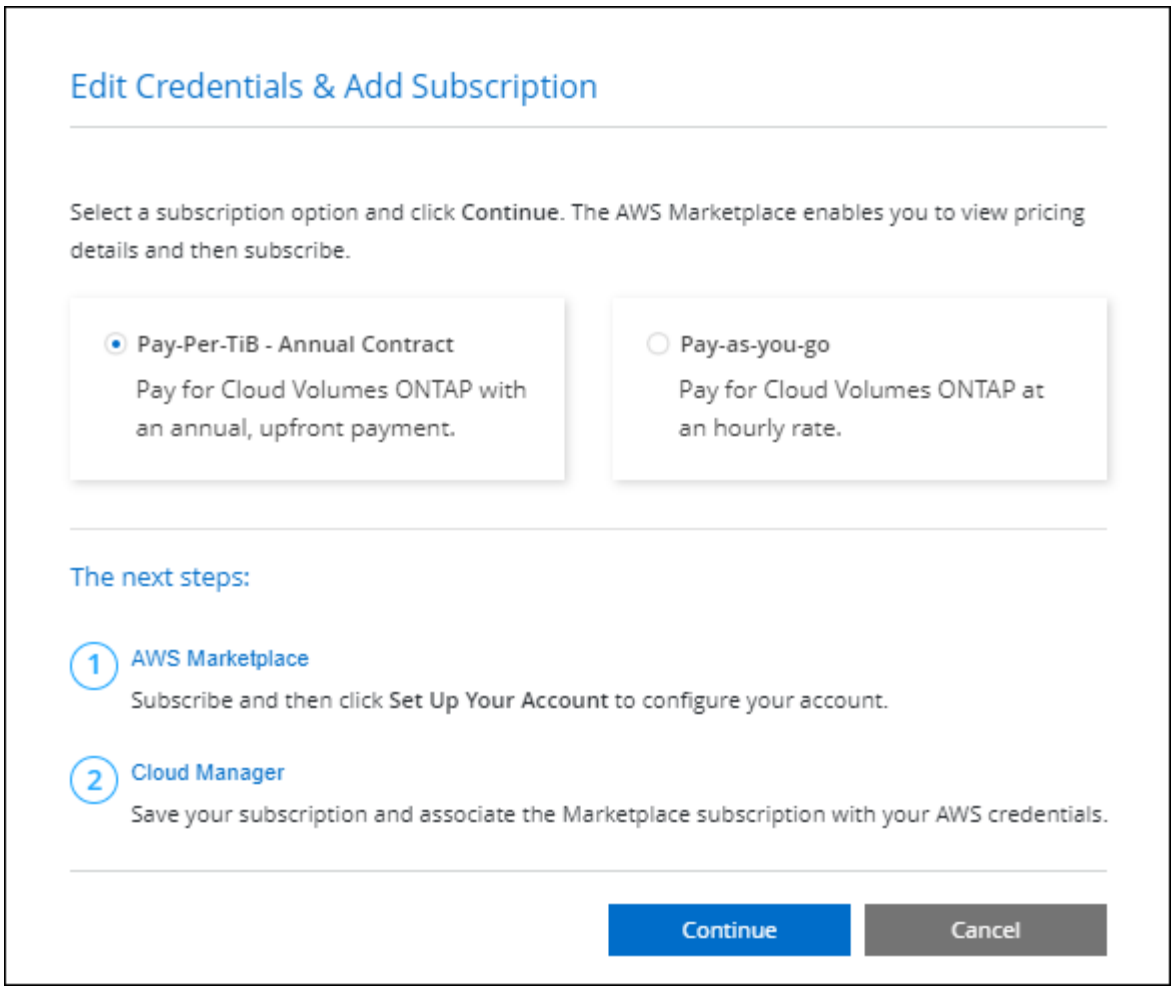
Contratto annuale

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

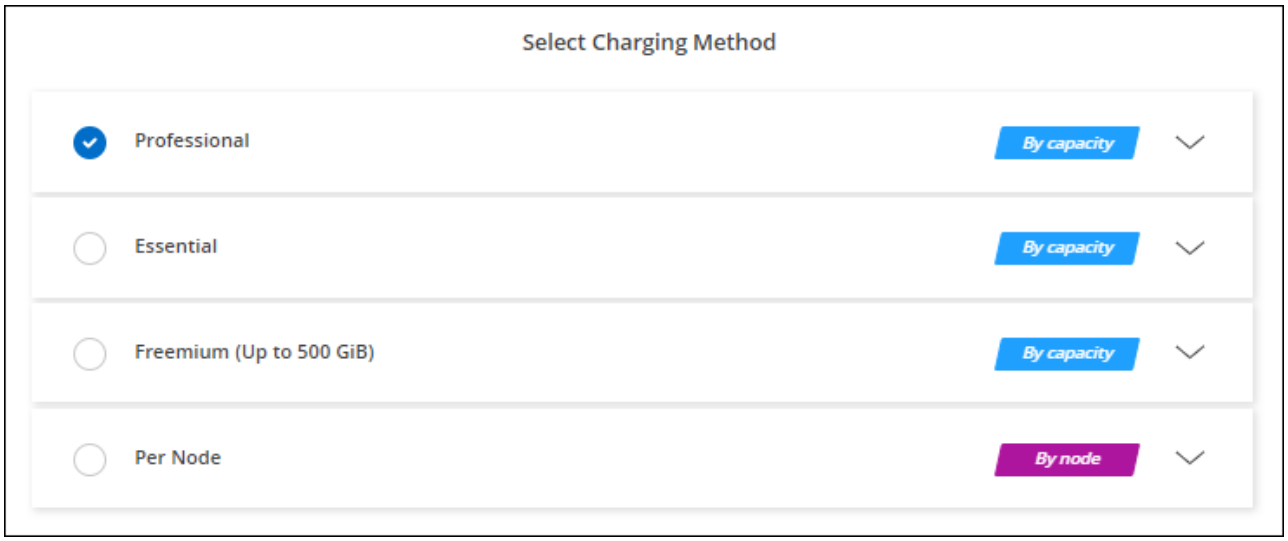
Così come per un abbonamento orario, BlueXP ti richiede di iscriverti al contratto annuale disponibile in AWS Marketplace.

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.



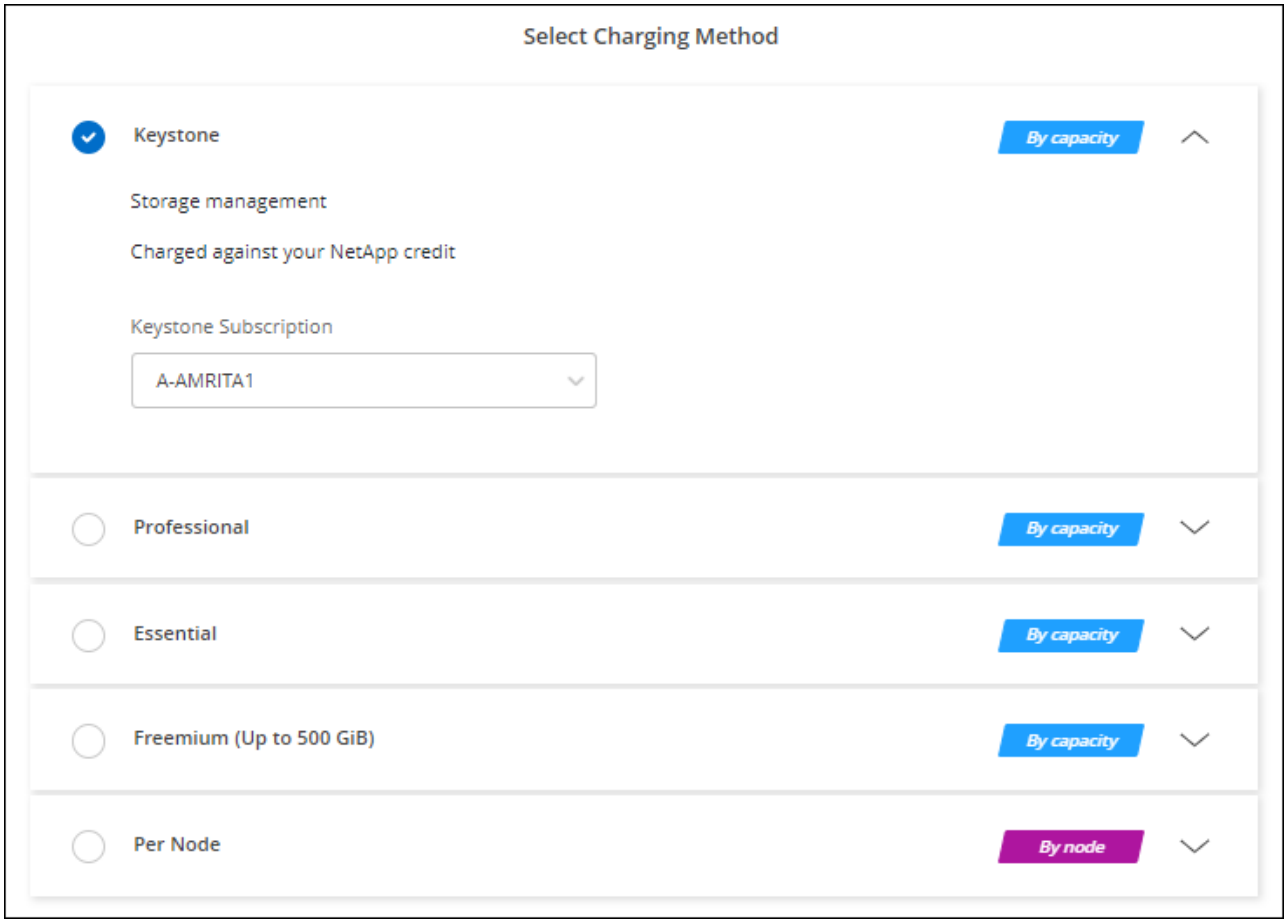
"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in AWS".

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:

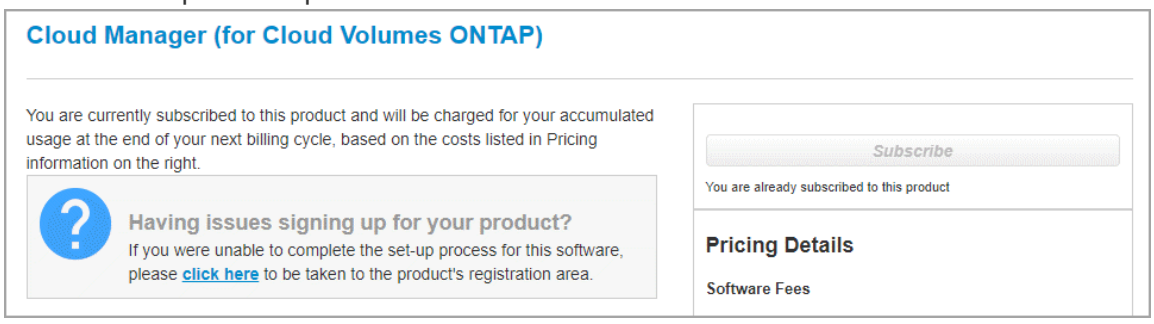
Campo	Descrizione
Nome ambiente di lavoro	BlueXP utilizza il nome dell'ambiente di lavoro per assegnare un nome sia al sistema Cloud Volumes ONTAP che all'istanza di Amazon EC2. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.

Campo	Descrizione
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:

► https://docs.netapp.com/it-it/test//media/video_subscribing_aws.mp4 *(video)*

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 viene eseguito da una versione 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.

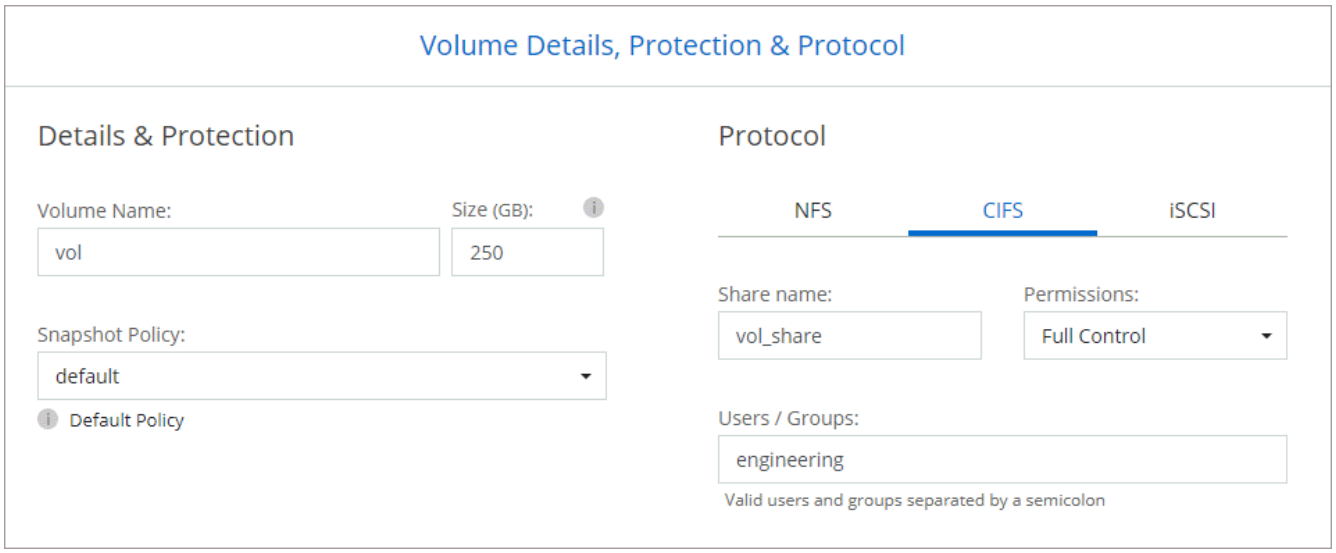
16. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

"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.

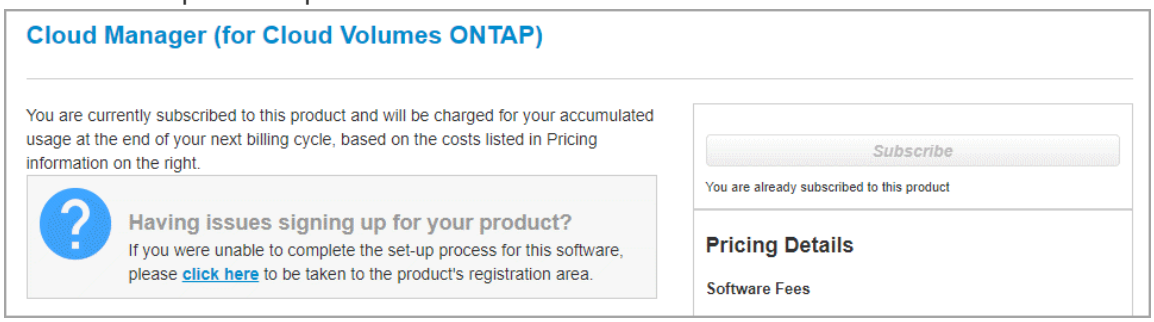
   Alcuni dei campi di questa pagina sono esplicativi. La seguente tabella descrive i campi per i quali potrebbero essere necessarie indicazioni:

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:

► https://docs.netapp.com/it-it/test//media/video_subscribing_aws.mp4 *(video)*

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 viene eseguito da una versione 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.

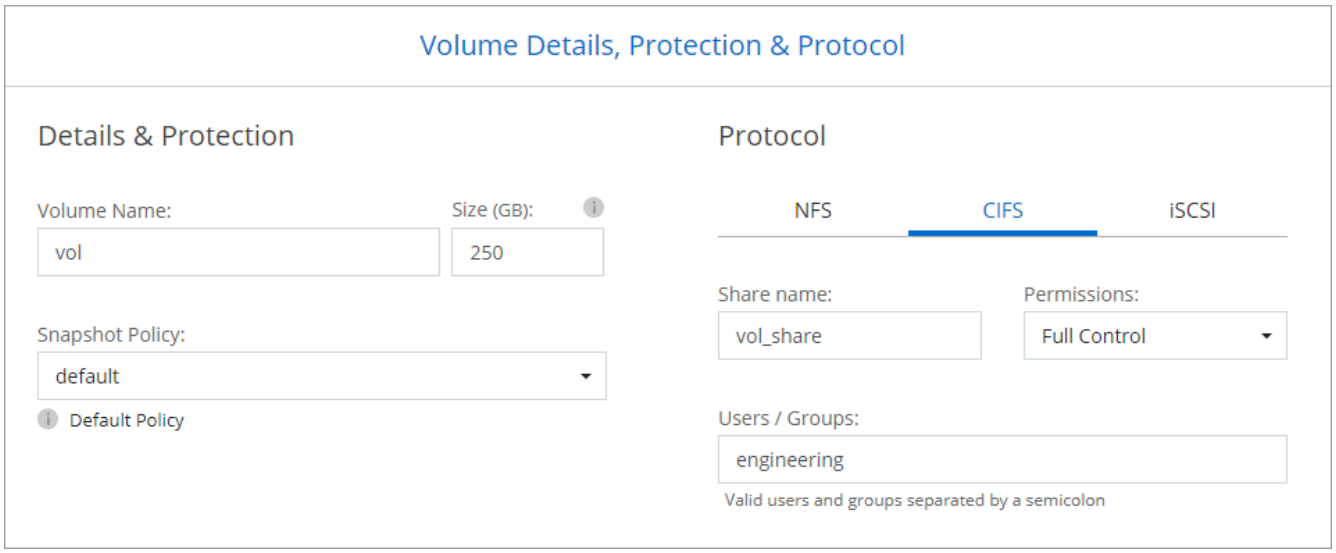
19. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

    "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.
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.
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 performance 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 usando l'indirizzo IP della LIF di gestione 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

Inizia a utilizzare Microsoft Azure

Avvio rapido di Cloud Volumes ONTAP in Azure

Inizia a utilizzare Cloud Volumes ONTAP per Azure in pochi passaggi.

Creare un connettore

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

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 VNET 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.

"Scopri di più sui requisiti di rete".

4 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"
- "Creazione di un connettore da Azure Marketplace"
- "Installazione del software del connettore su un host Linux"
- "Cosa fa BlueXP con le autorizzazioni"

Pianificare la configurazione di Cloud Volumes ONTAP in Azure

Quando si implementa Cloud Volumes ONTAP in Azure, 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 Microsoft Azure. "Visualizza l'elenco completo delle regioni supportate".

Scegliere un tipo di macchina virtuale supportato

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

"Configurazioni supportate per Cloud Volumes ONTAP in Azure"

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 Azure"

Dimensionare il sistema in Azure

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

Tipo di macchina virtuale

Esaminare i tipi di macchine virtuali supportati in "Note di rilascio di Cloud Volumes ONTAP" Quindi, esaminare i dettagli relativi a ciascun tipo di macchina virtuale supportato. Tenere presente che ogni tipo di macchina virtuale supporta un numero specifico di dischi dati.

- "Documentazione di Azure: Dimensioni generali delle macchine virtuali"
- "Documentazione di Azure: Dimensioni delle macchine virtuali ottimizzate per la memoria"

Tipo di disco Azure con sistemi a nodo singolo

Quando crei volumi per Cloud Volumes ONTAP, devi scegliere lo storage cloud sottostante che Cloud Volumes ONTAP utilizza come disco.

I sistemi a nodo singolo possono utilizzare tre tipi di dischi gestiti Azure:

- *Dischi gestiti SSD Premium* offrono performance elevate per carichi di lavoro i/o-intensive a un costo più elevato.
- I *dischi gestiti SSD standard* offrono performance costanti per i carichi di lavoro che richiedono IOPS ridotti.
- *Dischi gestiti HDD standard* sono una buona scelta se non hai bisogno di IOPS elevati e vuoi ridurre i costi.

Per ulteriori informazioni sui casi di utilizzo di questi dischi, vedere "Documentazione di Microsoft Azure: Quali tipi di dischi sono disponibili in Azure?".

Tipo di disco Azure con coppie ha

I sistemi HA utilizzano dischi gestiti condivisi SSD Premium che offrono performance elevate per carichi di lavoro i/o-intensive a un costo superiore. Le implementazioni HA create prima della release 9.12.1 utilizzano i blob di pagina Premium.

Dimensioni del disco Azure

Quando si avviano le istanze di Cloud Volumes ONTAP, è necessario scegliere la dimensione predefinita del disco per gli aggregati. BlueXP utilizza questa dimensione del disco per l'aggregato iniziale e per qualsiasi aggregato aggiuntivo creato quando si utilizza l'opzione di provisioning semplice. È possibile

creare aggregati che utilizzano una dimensione del disco diversa da quella predefinita di "utilizzando l'opzione di allocazione avanzata".

Tutti i dischi di un aggregato devono avere le stesse dimensioni.

Quando si sceglie una dimensione del disco, è necessario prendere in considerazione diversi fattori. Le dimensioni del disco influiscono sul costo dello storage, sulle dimensioni dei volumi che è possibile creare in un aggregato, sulla capacità totale disponibile per Cloud Volumes ONTAP e sulle performance dello storage.

Le prestazioni di Azure Premium Storage sono legate alle dimensioni del disco. I dischi più grandi offrono IOPS e throughput più elevati. Ad esempio, la scelta di 1 disco TIB può offrire prestazioni migliori rispetto a 500 dischi GiB, a un costo superiore.

Non esistono differenze di performance tra le dimensioni dei dischi per lo storage standard. È necessario scegliere le dimensioni del disco in base alla capacità richiesta.

Fare riferimento a Azure per IOPS e throughput in base alle dimensioni del disco:

- "Microsoft Azure: Prezzi dei dischi gestiti"
- "Microsoft Azure: Page Blobs pricing"

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 Azure".

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

Raccogliere informazioni di rete

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

Informazioni su Azure	Il tuo valore
Regione	
Rete virtuale (VNET)	
Subnet	
Gruppo di sicurezza di rete (se si utilizza il proprio)	

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.

Requisiti di rete per Cloud Volumes ONTAP in Azure

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

Requisiti per Cloud Volumes ONTAP

I seguenti requisiti di rete devono essere soddisfatti in Azure.

Accesso a Internet in uscita

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 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".

Indirizzi IP

BlueXP assegna automaticamente il numero richiesto di indirizzi IP privati a Cloud Volumes ONTAP in Azure. 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. Per strumenti di gestione come SnapCenter è necessaria una LIF di gestione SVM.

> Un LIF iSCSI fornisce l'accesso client sul protocollo iSCSI e viene utilizzato dal sistema per altri importanti flussi di lavoro di rete. Questi LIF sono obbligatori e non devono essere cancellati.

Indirizzi IP per un sistema a nodo singolo

BlueXP assegna 5 o 6 indirizzi IP a un sistema a nodo singolo:

- IP di gestione del cluster
- IP di gestione dei nodi
- IP di intercluster per SnapMirror
- IP NFS/CIFS
- IP iSCSI

> L'IP iSCSI fornisce l'accesso del client sul protocollo iSCSI. Viene inoltre utilizzato dal sistema per altri importanti flussi di lavoro di rete. Questa LIF è obbligatoria e non deve essere eliminata.

- Gestione SVM (opzionale - non configurata per impostazione predefinita)

Indirizzi IP per coppie ha

BlueXP assegna gli indirizzi IP a 4 NIC (per nodo) durante l'implementazione.

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

NIC0

- IP di gestione dei nodi
- Intercluster IP
- IP iSCSI

> L'IP iSCSI fornisce l'accesso del client sul protocollo iSCSI. Viene inoltre utilizzato dal sistema per altri importanti flussi di lavoro di rete. Questa LIF è obbligatoria e non deve essere eliminata.

NIC1

- IP della rete del cluster

NIC2

- Cluster Interconnect IP (IC ha)

NIC3

- IP NIC Pageblob (accesso al disco)

NIC3 è applicabile solo alle implementazioni ha che utilizzano lo storage page blob.

Gli indirizzi IP sopra indicati non migrano in caso di eventi di failover.

Inoltre, 4 IP front-end (FIPS) sono configurati per la migrazione in caso di eventi di failover. Questi IP di frontend risiedono nel bilanciamento del carico.

- IP di gestione del cluster
- IP dati NodeA (NFS/CIFS)
- IP dati NodeB (NFS/CIFS)
- IP di gestione SVM

Connessioni sicure ai servizi Azure

Per impostazione predefinita, BlueXP attiva un collegamento privato Azure per le connessioni tra gli account di storage blob di pagina Cloud Volumes ONTAP e Azure.

Nella maggior parte dei casi, non c'è nulla da fare: BlueXP gestisce Azure Private link per te. Tuttavia, se si utilizza Azure Private DNS, sarà necessario modificare un file di configurazione. È inoltre necessario conoscere un requisito per la posizione del connettore in Azure.

È inoltre possibile disattivare la connessione Private link, se richiesto dalle esigenze aziendali. Se si disattiva il collegamento, BlueXP configura Cloud Volumes ONTAP in modo che utilizzi un endpoint del servizio.

"Scopri di più sull'utilizzo di link privati o endpoint di servizio Azure con Cloud Volumes ONTAP".

Connessioni ad altri sistemi ONTAP

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

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

Porta per l'interconnessione ha

Una coppia Cloud Volumes ONTAP ha include un'interconnessione ha, che consente a ciascun nodo di controllare continuamente se il proprio partner funziona e di eseguire il mirroring dei dati di log per la memoria non volatile dell'altro. L'interconnessione ha utilizza la porta TCP 10006 per la comunicazione.

Per impostazione predefinita, la comunicazione tra le LIF di interconnessione ha è aperta e non esistono regole di gruppo di sicurezza per questa porta. Tuttavia, se si crea un firewall tra le LIF di interconnessione ha,

è necessario assicurarsi che il traffico TCP sia aperto per la porta 10006 in modo che la coppia ha possa funzionare correttamente.

Solo una coppia ha in un gruppo di risorse Azure

È necessario utilizzare un gruppo di risorse *dedicato* per ogni coppia di Cloud Volumes ONTAP ha implementata in Azure. In un gruppo di risorse è supportata una sola coppia ha.

BlueXP presenta problemi di connessione se si tenta di implementare una seconda coppia Cloud Volumes ONTAP ha in un gruppo di risorse Azure.

Regole del gruppo di sicurezza

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

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

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

Regole in entrata per sistemi a nodo singolo

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

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
1000 inbound_ssh	22 TCP	Qualsiasi a qualsiasi	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
1001 inbound_http	80 TCP	Qualsiasi a qualsiasi	Accesso HTTP alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
1002 inbound_111_tcp	111 TCP	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
1003 inbound_111_udp	111 UDP	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
1004 inbound_139	139 TCP	Qualsiasi a qualsiasi	Sessione del servizio NetBIOS per CIFS

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
1005 inbound_161-162 _tcp	161-162 TCP	Qualsiasi a qualsiasi	Protocollo di gestione di rete semplice
1006 inbound_161-162 _udp	161-162 UDP	Qualsiasi a qualsiasi	Protocollo di gestione di rete semplice
1007 inbound_443	443 TCP	Qualsiasi a qualsiasi	Connettività con il connettore e accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
1008 inbound_445	445 TCP	Qualsiasi a qualsiasi	Microsoft SMB/CIFS su TCP con frame NetBIOS
1009 inbound_635_tcp	635 TCP	Qualsiasi a qualsiasi	Montaggio NFS
1010 inbound_635_udp	635 UDP	Qualsiasi a qualsiasi	Montaggio NFS
1011 inbound_749	749 TCP	Qualsiasi a qualsiasi	Kerberos
1012 inbound_2049_tcp	2049 TCP	Qualsiasi a qualsiasi	Daemon del server NFS
1013 inbound_2049_udp	2049 UDP	Qualsiasi a qualsiasi	Daemon del server NFS
1014 inbound_3260	3260 TCP	Qualsiasi a qualsiasi	Accesso iSCSI tramite LIF dei dati iSCSI
1015 inbound_4045-4046_tcp	4045-4046 TCP	Qualsiasi a qualsiasi	NFS lock daemon e network status monitor
1016 inbound_4045-4046_udp	4045-4046 UDP	Qualsiasi a qualsiasi	NFS lock daemon e network status monitor
1017 inbound_10000	10000 TCP	Qualsiasi a qualsiasi	Backup con NDMP
1018 inbound_11104-11105	11104-11105 TCP	Qualsiasi a qualsiasi	Trasferimento dei dati SnapMirror
3000 inbound_deny _all_tcp	Qualsiasi porta TCP	Qualsiasi a qualsiasi	Blocca tutto il traffico TCP in entrata
3001 inbound_deny _all_udp	Qualsiasi porta UDP	Qualsiasi a qualsiasi	Bloccare tutto l'altro traffico UDP in entrata
65000 AllowVnetInBound	Qualsiasi porta Qualsiasi protocollo	Da VirtualNetwork a VirtualNetwork	Traffico in entrata dall'interno di VNET

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
65001 AllowAzureLoad BalancerInBound	Qualsiasi porta Qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico di dati dal bilanciamento del carico standard di Azure
65500 DenyAllInBound	Qualsiasi porta Qualsiasi protocollo	Qualsiasi a qualsiasi	Bloccare tutto il traffico in entrata

Regole in entrata per i sistemi ha

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

I sistemi HA hanno meno regole in entrata rispetto ai sistemi a nodo singolo perché il traffico dati in entrata passa attraverso il bilanciamento del carico standard di Azure. Per questo motivo, il traffico proveniente dal bilanciamento del carico deve essere aperto, come mostrato nella regola "AllowAzureLoadBalancerInBound".

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
100 inbound_443	443 Qualsiasi protocollo	Qualsiasi a qualsiasi	Connettività con il connettore e accesso HTTPS alla console Web di System Manager utilizzando l'indirizzo IP della LIF di gestione del cluster
101 inbound_111_tcp	111 Qualsiasi protocollo	Qualsiasi a qualsiasi	Chiamata a procedura remota per NFS
102 inbound_2049_tcp	2049 Qualsiasi protocollo	Qualsiasi a qualsiasi	Daemon del server NFS
111 inbound_ssh	22 Qualsiasi protocollo	Qualsiasi a qualsiasi	Accesso SSH all'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi
121 inbound_53	53 Qualsiasi protocollo	Qualsiasi a qualsiasi	DNS e CIFS
65000 AllowVnetInBound	Qualsiasi porta Qualsiasi protocollo	Da VirtualNetwork a VirtualNetwork	Traffico in entrata dall'interno di VNET
65001 AllowAzureLoad BalancerInBound	Qualsiasi porta Qualsiasi protocollo	AzureLoadBalancer a qualsiasi	Traffico di dati dal bilanciamento del carico standard di Azure

Priorità e nome	Porta e protocollo	Origine e destinazione	Descrizione
65500 DenyAllInBound	Qualsiasi porta Qualsiasi protocollo	Qualsiasi a qualsiasi	Bloccare tutto il traffico in entrata

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.

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

Servizio	Porta	Protocollo	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 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	68	UDP	LIF di gestione dei nodi	DHCP	Client DHCP per la prima installazione
DHCPS	67	UDP	LIF di gestione dei nodi	DHCP	DHCP server (Server DHCP)
DNS	53	UDP	LIF di gestione dei nodi e LIF dei dati (NFS, CIFS)	DNS	DNS
NDMP	18600–18699	TCP	LIF di gestione dei nodi	Server di destinazione	Copia NDMP
SMTP	25	TCP	LIF di gestione dei nodi	Server di posta	Gli avvisi SMTP possono essere utilizzati per AutoSupport
SNMP	161	TCP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	161	UDP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	162	TCP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
	162	UDP	LIF di gestione dei nodi	Monitorare il server	Monitoraggio mediante trap SNMP
SnapMirror	11104	TCP	LIF intercluster	ONTAP Intercluster LIF	Gestione delle sessioni di comunicazione tra cluster per SnapMirror
	11105	TCP	LIF intercluster	ONTAP Intercluster LIF	Trasferimento dei dati SnapMirror
Syslog	514	UDP	LIF di gestione dei nodi	Server syslog	Messaggi di inoltro syslog

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 Azure"

Impostare Cloud Volumes ONTAP in modo che utilizzi una chiave gestita dal cliente in Azure

I dati vengono crittografati automaticamente su Cloud Volumes ONTAP in Azure utilizzando "Azure Storage Service Encryption" Con una chiave gestita da Microsoft. Tuttavia, è possibile utilizzare la propria chiave di crittografia seguendo la procedura riportata in questa pagina.

Panoramica sulla crittografia dei dati

I dati Cloud Volumes ONTAP vengono crittografati automaticamente in Azure utilizzando "Azure Storage Service Encryption". L'implementazione predefinita utilizza una chiave gestita da Microsoft. Non è richiesta alcuna configurazione.

Se si desidera utilizzare una chiave gestita dal cliente con Cloud Volumes ONTAP, attenersi alla seguente procedura:

1. Da Azure, creare un vault delle chiavi e quindi generare una chiave in quel vault
2. Da BlueXP, utilizzare l'API per creare un ambiente di lavoro Cloud Volumes ONTAP che utilizza la chiave

Rotazione delle chiavi

Se si crea una nuova versione della chiave, Cloud Volumes ONTAP utilizza automaticamente la versione più recente.

Modalità di crittografia dei dati

Dopo aver creato un ambiente di lavoro Cloud Volumes ONTAP configurato per l'utilizzo di una chiave gestita dal cliente, i dati Cloud Volumes ONTAP vengono crittografati come segue.

Area di disponibilità multipla Azure ha

- Tutti gli account di storage Azure per Cloud Volumes ONTAP vengono crittografati utilizzando una chiave gestita dal cliente.[1]
- Per i dischi root, boot, NVRAM, core e dati, BlueXP utilizza un set di crittografia dei dischi che consente la gestione delle chiavi di crittografia con i dischi gestiti.
- Anche i nuovi dischi dati utilizzano lo stesso set di crittografia del disco.

Area di disponibilità singola Azure ha

- Tutti gli account di storage Azure per Cloud Volumes ONTAP vengono crittografati utilizzando una chiave gestita dal cliente.[1]
- Anche i nuovi account storage (ad esempio, quando si aggiungono dischi o aggregati) utilizzano la stessa chiave.[1]
- A partire da ONTAP 9.10.1P3, per NVRAM e il disco principale, BlueXP utilizza un "crittografia del disco impostata", che consente la gestione delle chiavi di crittografia con dischi gestiti. Le versioni più basse

utilizzeranno la chiave gestita da Microsoft, invece della chiave gestita dal cliente.

Nodo singolo

- Tutti gli account di storage Azure per Cloud Volumes ONTAP vengono crittografati utilizzando una chiave gestita dal cliente. [1]
- Per i dischi root, boot e dati, BlueXP utilizza un "crittografia del disco impostata", che consente la gestione delle chiavi di crittografia con dischi gestiti.
- Anche i nuovi dischi dati utilizzano lo stesso set di crittografia del disco.
- A partire da ONTAP 9.9.1P7, per la NVRAM e il disco principale, BlueXP utilizza un set di crittografia del disco, che consente la gestione delle chiavi di crittografia con i dischi gestiti. Le versioni più basse utilizzeranno la chiave gestita da Microsoft, invece della chiave gestita dal cliente.

Nota a piè di pagina

1. Se si desidera crittografare gli account di storage durante la creazione, è necessario creare e fornire l'ID della risorsa nella richiesta di creazione CVO. Questo vale per tutti i tipi di implementazioni. Se non viene fornito, gli account di storage verranno comunque crittografati, ma BlueXP creerà prima gli account di storage con crittografia a chiave gestita da Microsoft e quindi aggiornerà gli account di storage per utilizzare la chiave gestita dal cliente.

Creare un'identità gestita assegnata dall'utente

È possibile creare una risorsa denominata identità gestita assegnata dall'utente. In questo modo è possibile crittografare gli account storage quando si crea un ambiente di lavoro Cloud Volumes ONTAP. Si consiglia di creare questa risorsa prima di creare un vault delle chiavi e di generare una chiave.

La risorsa ha il seguente ID: `userassignedidentity`.

Fasi

1. In Azure, accedere a servizi Azure e selezionare **identità gestite**.
2. Fare clic su **Create** (Crea).
3. Fornire i seguenti dettagli:
   - **Subscription**: Scegli un abbonamento. Si consiglia di scegliere lo stesso abbonamento di Connector.
   - **Gruppo di risorse**: Utilizzare un gruppo di risorse esistente o crearne uno nuovo.
   - **Regione**: Se si desidera, selezionare la stessa regione del connettore.
   - **Nome**: Immettere un nome per la risorsa.
4. Facoltativamente, aggiungere tag.
5. Fare clic su **Create** (Crea).

Creare un vault delle chiavi e generare una chiave

Il vault delle chiavi deve risiedere nella stessa sottoscrizione Azure e nella stessa regione in cui si intende creare il sistema Cloud Volumes ONTAP.

Se creazione di un'identità gestita assegnata dall'utente, durante la creazione del vault delle chiavi, è necessario creare anche una policy di accesso per il vault delle chiavi.

Fasi

1. "Creare un vault delle chiavi nell'abbonamento Azure".

Tenere presente i seguenti requisiti per il vault delle chiavi:

- Il vault delle chiavi deve risiedere nella stessa regione del sistema Cloud Volumes ONTAP.
- Devono essere attivate le seguenti opzioni:
  - **Soft-delete** (questa opzione è attivata per impostazione predefinita, ma deve *non* essere disattivata)
  - **Protezione da spurgo**
  - **Azure Disk Encryption per la crittografia dei volumi** (per sistemi a nodo singolo o coppie ha in più zone)
- Se è stata creata un'identità gestita assegnata dall'utente, deve essere attivata la seguente opzione:
  - **Policy di accesso al vault**

2. Se è stata selezionata la policy di accesso al vault, fare clic su Create (Crea) per creare una policy di accesso per il vault delle chiavi. In caso contrario, passare alla fase 3.
   a. Selezionare le seguenti autorizzazioni:
      - ottieni
      - elenco
      - decrittare
      - crittografare
      - tasto di savvolgimento
      - tasto di avvolgimento
      - verificare
      - segnale
   b. Selezionare l'identità gestita (risorsa) assegnata dall'utente come principale.
   c. Esaminare e creare la policy di accesso.
3. "Generare una chiave nell'archivio chiavi".

   Tenere presente i seguenti requisiti per la chiave:

   - Il tipo di chiave deve essere **RSA**.
   - La dimensione consigliata della chiave RSA è **2048**, ma sono supportate altre dimensioni.

Creare un ambiente di lavoro che utilizzi la chiave di crittografia

Dopo aver creato l'archivio delle chiavi e aver generato una chiave di crittografia, è possibile creare un nuovo sistema Cloud Volumes ONTAP configurato per l'utilizzo della chiave. Questi passaggi sono supportati dall'API BlueXP.

Autorizzazioni richieste

Se si desidera utilizzare una chiave gestita dal cliente con un sistema Cloud Volumes ONTAP a nodo singolo, assicurarsi che BlueXP Connector disponga delle seguenti autorizzazioni:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"Visualizzare l'elenco più recente delle autorizzazioni"

Fasi

1. Ottenere l'elenco dei vault chiave nell'abbonamento Azure utilizzando la seguente chiamata API BlueXP.

   Per una coppia ha: `GET /azure/ha/metadata/vaults`

   Per nodo singolo: `GET /azure/vsa/metadata/vaults`

   Prendere nota del **nome** e del **resourceGroup**. Sarà necessario specificare questi valori nel passaggio successivo.

   "Scopri di più su questa chiamata API".

2. Ottenere l'elenco delle chiavi all'interno del vault utilizzando la seguente chiamata API BlueXP.

   Per una coppia ha: `GET /azure/ha/metadata/keys-vault`

   Per nodo singolo: `GET /azure/vsa/metadata/keys-vault`

   Prendere nota del **nome chiave**. Nel passaggio successivo, specificare tale valore (insieme al nome del vault).

   "Scopri di più su questa chiamata API".

3. Creare un sistema Cloud Volumes ONTAP utilizzando la seguente chiamata API BlueXP.

   a. Per una coppia ha:

      `POST /azure/ha/working-environments`

      Il corpo della richiesta deve includere i seguenti campi:

      ```
      "azureEncryptionParameters": {
                    "key": "keyName",
                    "vaultName": "vaultName"
      }
      ```

      Includere il `"userAssignedIdentity": " userAssignedIdentityId"` se questa risorsa è stata creata per essere utilizzata per la crittografia dell'account di storage.

"Scopri di più su questa chiamata API".

b. Per un sistema a nodo singolo:

```
POST /azure/vsa/working-environments
```

Il corpo della richiesta deve includere i seguenti campi:

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

Includere il `"userAssignedIdentity": " userAssignedIdentityId"` se questa risorsa è stata creata per essere utilizzata per la crittografia dell'account di storage.

"Scopri di più su questa chiamata API".

Risultato

Si dispone di un nuovo sistema Cloud Volumes ONTAP configurato per utilizzare la chiave gestita dal cliente per la crittografia dei dati.

Impostare la licenza per Cloud Volumes ONTAP in Azure

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

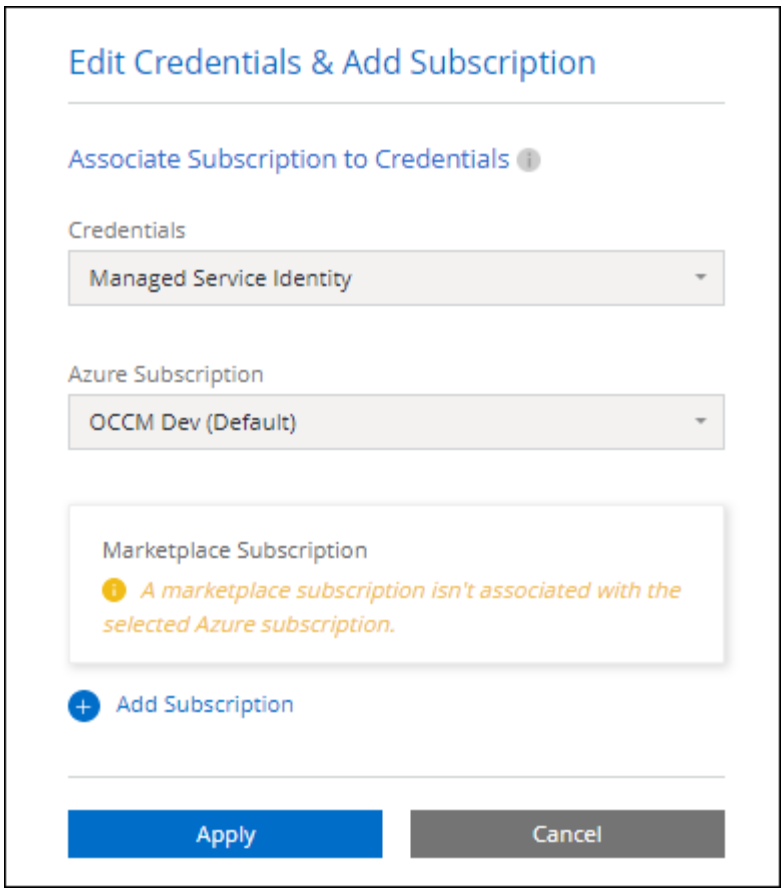
Scegli l'offerta Freemium per utilizzare Cloud Volumes ONTAP gratuitamente con un massimo di 500 GB di capacità fornita. "Scopri di più sull'offerta Freemium".

Fasi

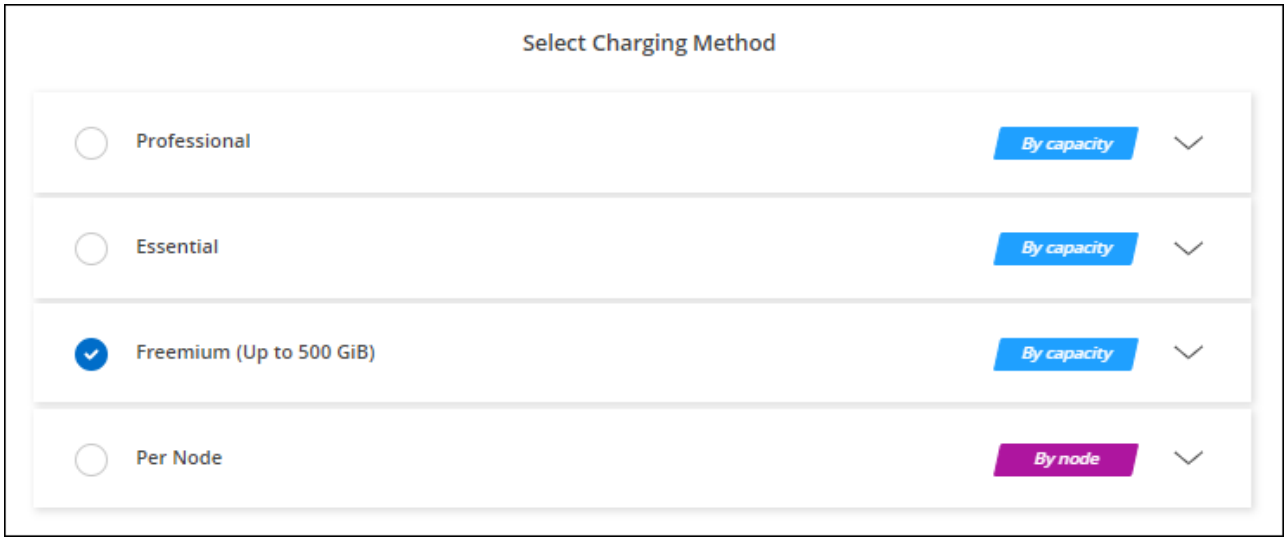
1. Dal menu di navigazione a sinistra, selezionare **Storage > Canvas**.
2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.

   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 Azure 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 Azure".

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 Azure Marketplace
- Un contratto annuale

"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"

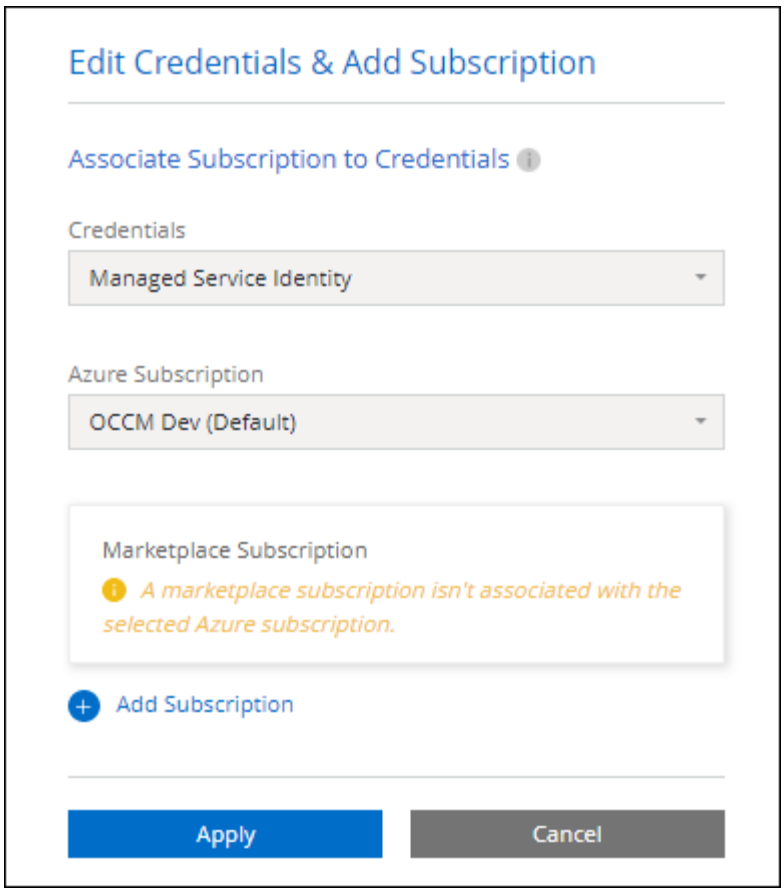
   BlueXP interroga automaticamente il servizio di licensing di NetApp per ottenere dettagli sulle licenze associate al tuo account NetApp Support Site. In assenza di errori, BlueXP aggiunge automaticamente le licenze al portafoglio digitale.

   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".

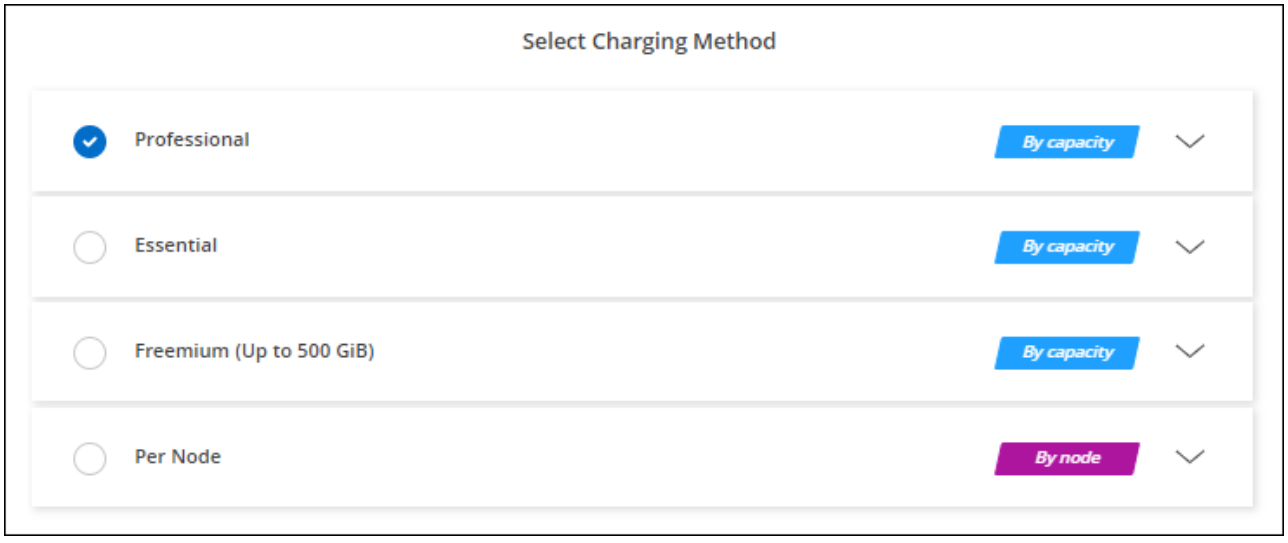
3. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e seguire la procedura in BlueXP.

   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 Azure 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 Azure".

Abbonamento PAYGO

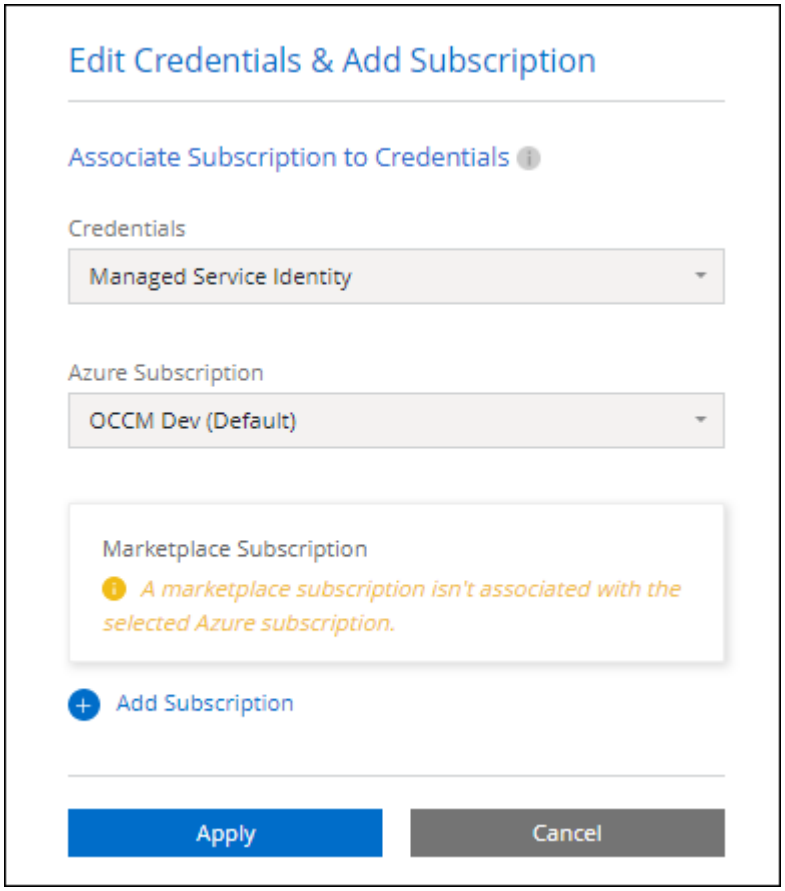
Paga ogni ora sottoscrivendo l'offerta sul mercato del tuo cloud provider.

Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, BlueXP richiede di sottoscrivere il contratto disponibile in Azure Marketplace. Tale abbonamento viene quindi associato all'ambiente di lavoro per la

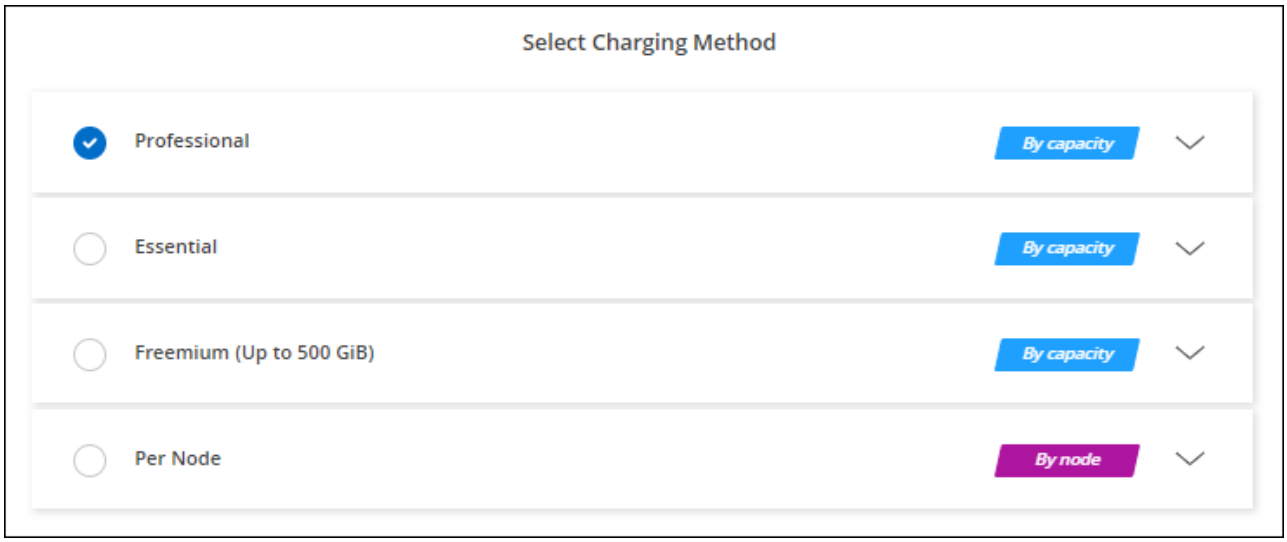
ricarica. È possibile utilizzare lo stesso abbonamento per altri ambienti di lavoro.

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 Azure 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 Azure".

Puoi gestire gli abbonamenti Azure Marketplace associati ai tuoi account Azure dalla pagina Impostazioni > credenziali. "Scopri come gestire i tuoi account e abbonamenti Azure"

Contratto annuale

Paga Cloud Volumes ONTAP ogni anno acquistando un contratto annuale.

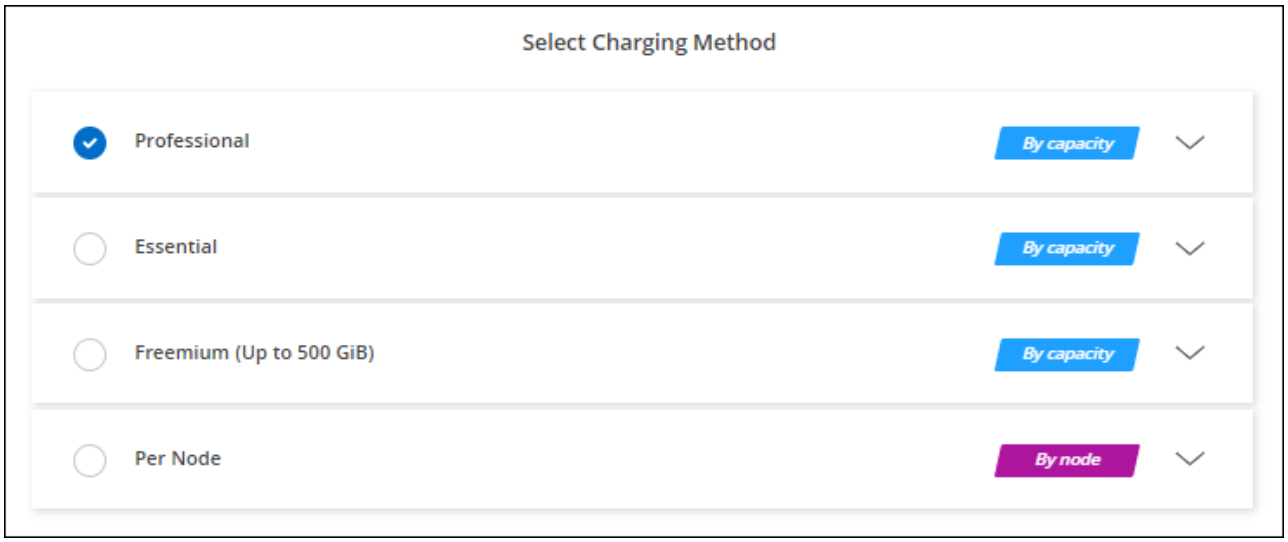
Fasi

1. Contatta il tuo commerciale NetApp per acquistare un contratto annuale.

   Il contratto è disponibile come offerta *privata* in Azure Marketplace.

   Dopo che NetApp condivide l'offerta privata con te, puoi selezionare il piano annuale quando ti iscrivi da Azure Marketplace durante la creazione dell'ambiente di lavoro.

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 > continua**.
   b. Nel portale Azure, seleziona il piano annuale condiviso con il tuo account Azure, quindi fai clic su **Iscriviti**.
   c. Una volta visualizzato BlueXP, selezionare un pacchetto basato sulla capacità quando si accede alla pagina dei metodi di ricarica.



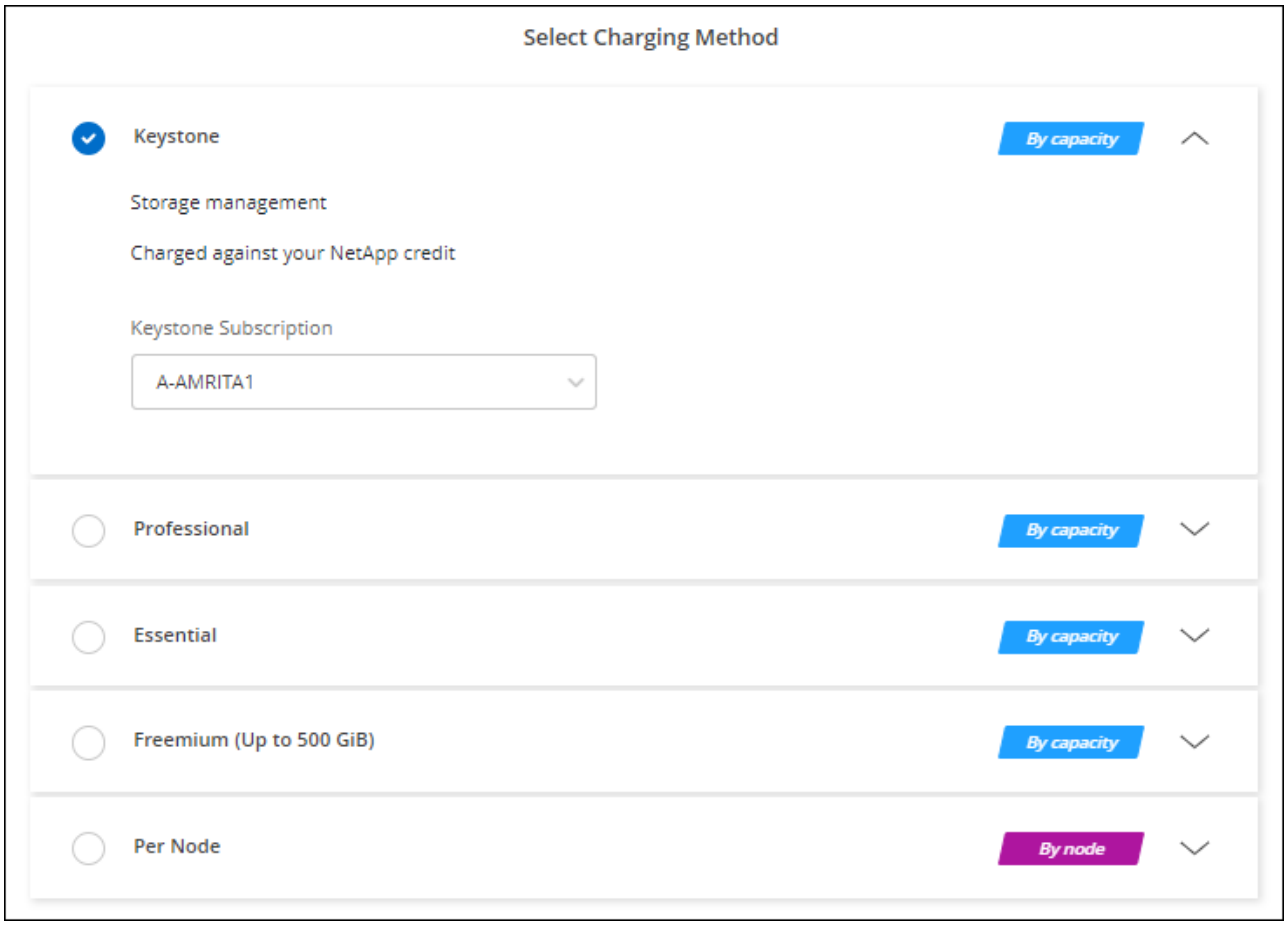
"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Azure".

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 Azure".

Abilitare la modalità ad alta disponibilità in Azure

La modalità ad alta disponibilità di Microsoft Azure deve essere abilitata per ridurre i tempi di failover non pianificati e abilitare il supporto NFSv4 per Cloud Volumes ONTAP.

A partire dalla release Cloud Volumes ONTAP 9.10.1, abbiamo ridotto il tempo di failover non pianificato per le coppie Cloud Volumes ONTAP ha in esecuzione in Microsoft Azure e aggiunto il supporto per NFSv4. Per rendere disponibili questi miglioramenti a Cloud Volumes ONTAP, devi attivare la funzione di disponibilità elevata sul tuo abbonamento Azure.

BlueXP ti chiederà di inserire questi dettagli in un messaggio Action Required (azione richiesta) quando la funzione deve essere attivata con un abbonamento Azure.

Tenere presente quanto segue:

- Non ci sono problemi con l'alta disponibilità della tua coppia Cloud Volumes ONTAP ha. Questa funzionalità di Azure funziona in collaborazione con ONTAP per ridurre il tempo di interruzione dell'applicazione osservato dal client per i protocolli NFS che derivano da eventi di failover non pianificati.
- L'attivazione di questa funzione non comporta interruzioni per le coppie Cloud Volumes ONTAP ha.
- L'attivazione di questa funzione sul tuo abbonamento Azure non causerà problemi ad altre macchine virtuali.

Un utente di Azure che dispone dei privilegi di "Owner" può attivare la funzionalità dalla CLI di Azure.

Fasi

1. "Accedi a Azure Cloud Shell dal portale Azure"
2. Registrare la funzione della modalità ad alta disponibilità:

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. Se si desidera, verificare che la funzione sia ora registrata:

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Azure CLI dovrebbe restituire un risultato simile a quanto segue:

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

Lancio di Cloud Volumes ONTAP in Azure

È possibile avviare un sistema a nodo singolo o una coppia ha in Azure creando un ambiente di lavoro Cloud Volumes ONTAP in BlueXP.

Di cosa hai bisogno

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.

  È necessario aver scelto una configurazione e ottenuto le informazioni di rete di Azure 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".

A proposito di questa attività

Quando BlueXP crea un sistema Cloud Volumes ONTAP in Azure, crea diversi oggetti Azure, ad esempio un gruppo di risorse, interfacce di rete e account di storage. Al termine della procedura guidata, è possibile visualizzare un riepilogo delle risorse.

> **Potenziale perdita di dati**
>
> La Best practice consiste nell'utilizzare un nuovo gruppo di risorse dedicato per ciascun sistema Cloud Volumes ONTAP.
>
> L'implementazione di Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente non è consigliata a causa del rischio di perdita di dati. Mentre BlueXP può rimuovere le risorse Cloud Volumes ONTAP da un gruppo di risorse condiviso in caso di errore di implementazione o di eliminazione, un utente Azure potrebbe accidentalmente eliminare le risorse Cloud Volumes ONTAP da un gruppo di risorse condiviso.

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

Se si desidera avviare un sistema Cloud Volumes ONTAP a nodo singolo in Azure, è necessario creare un ambiente di lavoro a nodo singolo in BlueXP.

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 posizione**: Seleziona **Microsoft Azure** e **nodo singolo Cloud Volumes ONTAP**.
4. Se richiesto, "Creare un connettore".
5. **Dettagli e credenziali**: Se necessario, modificare le credenziali e la sottoscrizione di Azure, specificare un nome del cluster, aggiungere tag, quindi specificare le credenziali.

   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 alla macchina virtuale Azure. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.

Campo	Descrizione
Tag del gruppo di risorse	I tag sono metadati per le risorse Azure. Quando si inseriscono i tag in questo campo, BlueXP li aggiunge al gruppo di risorse associato al sistema Cloud Volumes ONTAP. 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 di Microsoft Azure: Utilizzo di tag per organizzare le risorse di Azure".
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	È possibile scegliere credenziali Azure diverse e un abbonamento Azure diverso da utilizzare con questo sistema Cloud Volumes ONTAP. Per implementare un sistema Cloud Volumes ONTAP pay-as-you-go, devi associare un abbonamento Azure Marketplace all'abbonamento Azure selezionato. "Scopri come aggiungere le credenziali".

Il video seguente mostra come associare un abbonamento Marketplace a un abbonamento Azure:

► https://docs.netapp.com/it-it/test//media/video_subscribing_azure.mp4 *(video)*

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** (posizione): Selezionare una regione, una zona di disponibilità, VNET e una subnet, quindi selezionare la casella di controllo per confermare la connettività di rete tra il connettore e la posizione di destinazione.

   Per i sistemi a nodo singolo, è possibile scegliere l'area di disponibilità in cui si desidera implementare Cloud Volumes ONTAP. Se non si seleziona un AZ, BlueXP ne selezionerà uno.

8. **Connettività**: Scegliere un gruppo di risorse nuovo o esistente, quindi scegliere se utilizzare il gruppo di protezione predefinito o il proprio.

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

Campo	Descrizione
Gruppo di risorse	Creare un nuovo gruppo di risorse per Cloud Volumes ONTAP o utilizzare un gruppo di risorse esistente. La Best practice consiste nell'utilizzare un nuovo gruppo di risorse dedicato per Cloud Volumes ONTAP. Sebbene sia possibile implementare Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente, non è consigliabile a causa del rischio di perdita dei dati. Per ulteriori informazioni, vedere l'avviso riportato sopra. Se l'account Azure in uso dispone di "autorizzazioni richieste", BlueXP rimuove le risorse Cloud Volumes ONTAP da un gruppo di risorse, in caso di errore di implementazione o di eliminazione.
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 VNET Only** (solo VNET selezionato), l'origine del traffico in entrata è l'intervallo di sottorete del VNET selezionato e l'intervallo di sottorete del VNET in cui si trova il connettore. Questa è l'opzione consigliata. • Se si sceglie **All VNets**, l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.
USA esistente	Se si sceglie un gruppo di protezione esistente, questo deve soddisfare i requisiti Cloud Volumes ONTAP. "Visualizzare il gruppo di protezione predefinito".

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. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per implementare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Crea la mia configurazione**.

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

11. **Licenza**: Modificare la versione di Cloud Volumes ONTAP in base alle esigenze e selezionare un tipo di macchina virtuale.

    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 viene eseguito da una versione all'altra, ad esempio da 9,6 a 9,7.

12. **Iscriviti al marketplace Azure**: Segui la procedura se BlueXP non è riuscito ad abilitare le implementazioni programmatiche di Cloud Volumes ONTAP.
13. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco, una

dimensione per ciascun disco e se attivare il tiering dei dati per lo storage Blob.

Tenere presente quanto segue:

- Il tipo di disco è per il volume iniziale. È possibile scegliere un tipo di disco diverso per i volumi successivi.
- Le dimensioni del disco sono 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.

  Per informazioni sulla scelta del tipo e delle dimensioni di un disco, vedere "Dimensionamento del sistema in Azure".

- 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 di più sul tiering dei dati".

14. **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.

       Questa opzione è disponibile solo per alcuni tipi di macchine virtuali. Per scoprire quali tipi di macchine virtuali sono supportati, vedere "Configurazioni supportate dalla licenza per coppie ha".

       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.

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

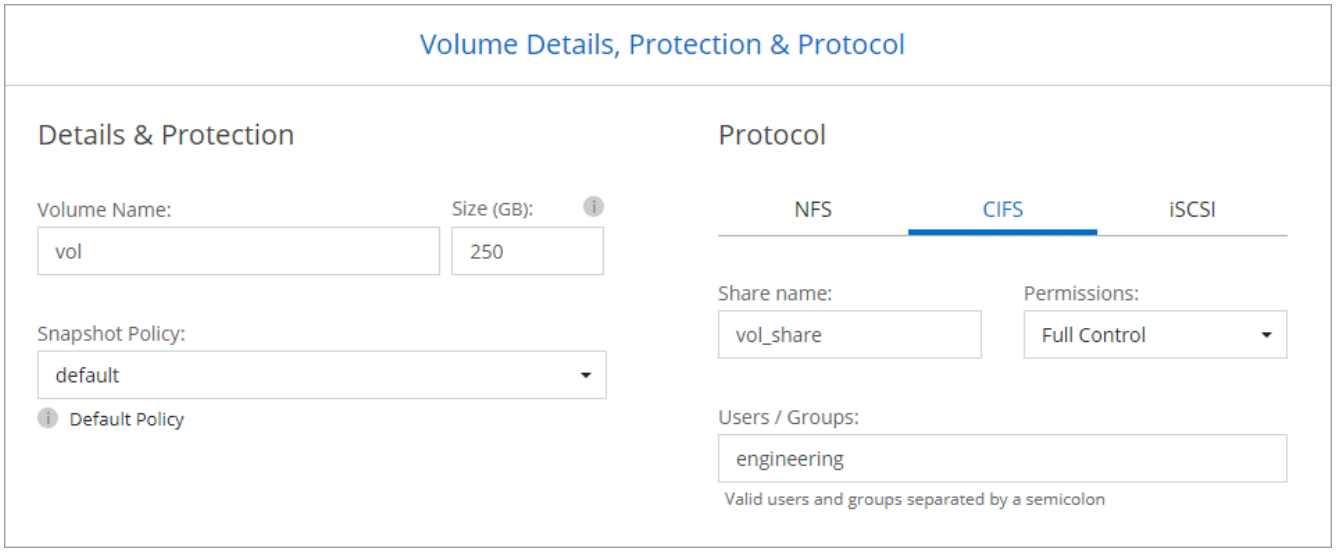
    "Scopri le versioni e i protocolli client supportati".

    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.

Campo	Descrizione
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:



16. **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. Per configurare i servizi di dominio ad Azure come server ad per Cloud Volumes ONTAP, immettere **OU=computer AADDC** o **OU=utenti AADDC** in questo campo. "Documentazione di Azure: Creare un'unità organizzativa (OU) in un dominio gestito dai servizi di dominio ad di Azure"
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.

17. **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".

18. **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 Azure che BlueXP acquisterà.
    c. Selezionare le caselle di controllo **ho capito…**.
    d. Fare clic su **Go**.

Risultato

BlueXP implementa il sistema Cloud Volumes ONTAP. Puoi tenere traccia dei progressi nella timeline.

In caso di problemi durante l'implementazione del sistema Cloud Volumes ONTAP, esaminare il messaggio di

errore. È inoltre possibile selezionare l'ambiente di lavoro e fare clic su **Ricomcreare 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.

Lancio di una coppia Cloud Volumes ONTAP ha in Azure

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

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. Se richiesto, "Creare un connettore".
4. **Dettagli e credenziali**: Se necessario, modificare le credenziali e la sottoscrizione di Azure, specificare un nome del cluster, aggiungere tag, quindi specificare le credenziali.

   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 alla macchina virtuale Azure. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.
Tag del gruppo di risorse	I tag sono metadati per le risorse Azure. Quando si inseriscono i tag in questo campo, BlueXP li aggiunge al gruppo di risorse associato al sistema Cloud Volumes ONTAP. 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 di Microsoft Azure: Utilizzo di tag per organizzare le risorse di Azure".
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.

Campo	Descrizione
Modifica credenziali	È possibile scegliere credenziali Azure diverse e un abbonamento Azure diverso da utilizzare con questo sistema Cloud Volumes ONTAP. Per implementare un sistema Cloud Volumes ONTAP pay-as-you-go, devi associare un abbonamento Azure Marketplace all'abbonamento Azure selezionato. "Scopri come aggiungere le credenziali".

Il video seguente mostra come associare un abbonamento Marketplace a un abbonamento Azure:

► https://docs.netapp.com/it-it/test//media/video_subscribing_azure.mp4 *(video)*

5. **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.

6. **Modelli di implementazione ha**:
   a. Selezionare **Single Availability zone** o **Multiple Availability zone**.
   b. **Posizione e connettività** (AZ singolo) e **Regione e connettività** (AZS multiplo)
      - Per AZ singolo, selezionare una regione, VNET e subnet.
      - Per AZS multipli, selezionare una regione, VNET, subnet, zona per il nodo 1 e zona per il nodo 2.
   c. Selezionare la casella di controllo **ho verificato la connettività di rete…**.
7. **Connettività**: Scegliere un gruppo di risorse nuovo o esistente, quindi scegliere se utilizzare il gruppo di protezione predefinito o il proprio.

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

Campo	Descrizione
Gruppo di risorse	Creare un nuovo gruppo di risorse per Cloud Volumes ONTAP o utilizzare un gruppo di risorse esistente. La Best practice consiste nell'utilizzare un nuovo gruppo di risorse dedicato per Cloud Volumes ONTAP. Sebbene sia possibile implementare Cloud Volumes ONTAP in un gruppo di risorse condiviso esistente, non è consigliabile a causa del rischio di perdita dei dati. Per ulteriori informazioni, vedere l'avviso riportato sopra. È necessario utilizzare un gruppo di risorse dedicato per ogni coppia di Cloud Volumes ONTAP ha implementata in Azure. In un gruppo di risorse è supportata una sola coppia ha. BlueXP presenta problemi di connessione se si tenta di implementare una seconda coppia Cloud Volumes ONTAP ha in un gruppo di risorse Azure. Se l'account Azure in uso dispone di "autorizzazioni richieste", BlueXP rimuove le risorse Cloud Volumes ONTAP da un gruppo di risorse, in caso di errore di implementazione o di eliminazione.
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 VNET Only** (solo VNET selezionato), l'origine del traffico in entrata è l'intervallo di sottorete del VNET selezionato e l'intervallo di sottorete del VNET in cui si trova il connettore. Questa è l'opzione consigliata. • Se si sceglie **All VNets**, l'origine del traffico in entrata è l'intervallo IP 0.0.0.0/0.
USA esistente	Se si sceglie un gruppo di protezione esistente, questo deve soddisfare i requisiti Cloud Volumes ONTAP. "Visualizzare il gruppo di protezione predefinito".

8. **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".
9. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per implementare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Cambia configurazione**.

   Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.
10. **Licenza**: Modificare la versione di Cloud Volumes ONTAP in base alle esigenze e selezionare un tipo di macchina virtuale.

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 viene eseguito da una versione all'altra, ad esempio da 9,6 a 9,7.

11. **Iscriviti al marketplace Azure**: Segui la procedura se BlueXP non è riuscito ad abilitare le implementazioni programmatiche di Cloud Volumes ONTAP.
12. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco, una dimensione per ciascun disco e se attivare il tiering dei dati per lo storage Blob.

    Tenere presente quanto segue:

    - Le dimensioni del disco sono 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.

      Per informazioni sulla scelta delle dimensioni del disco, vedere "Dimensionare il sistema in Azure".

    - 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 di più sul tiering dei dati".

13. **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.

       Questa opzione è disponibile solo per alcuni tipi di macchine virtuali. Per scoprire quali tipi di macchine virtuali sono supportati, vedere "Configurazioni supportate dalla licenza per coppie ha".

       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.

14. **Secure Communication to Storage & WORM**: Scegliere se abilitare una connessione HTTPS agli account di storage Azure e attivare lo storage WORM (Write Once, Read Many), se lo si desidera.

    La connessione HTTPS proviene da una coppia ha di Cloud Volumes ONTAP 9.7 agli account di storage blob di pagina Azure. L'attivazione di questa opzione può influire sulle prestazioni di scrittura. Non è possibile modificare l'impostazione dopo aver creato l'ambiente di lavoro.

    "Scopri di più sullo storage WORM".

    NON è possibile attivare WORM se è stato attivato il tiering dei dati.

"Scopri di più sullo storage WORM".

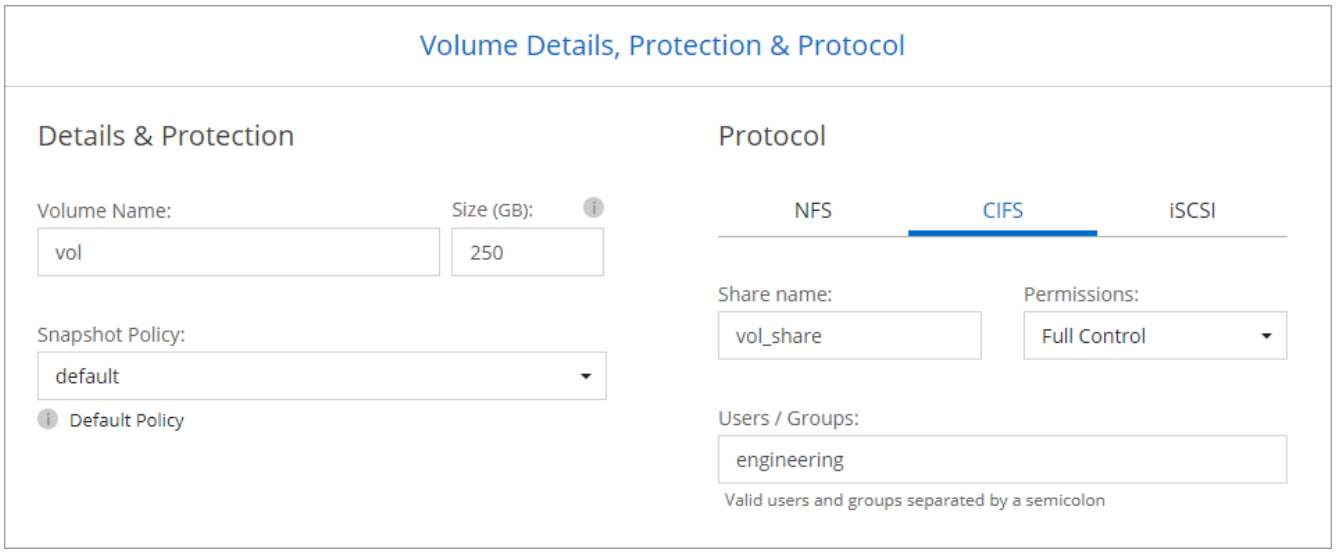
15. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

    "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:



16. **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. Per configurare i servizi di dominio ad Azure come server ad per Cloud Volumes ONTAP, immettere **OU=computer AADDC** o **OU=utenti AADDC** in questo campo. "Documentazione di Azure: Creare un'unità organizzativa (OU) in un dominio gestito dai servizi di dominio ad di Azure"
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.

17. **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".

18. **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 Azure che BlueXP acquisterà.
    c. Selezionare le caselle di controllo **ho capito…**.
    d. Fare clic su **Go**.

Risultato

BlueXP implementa il sistema Cloud Volumes ONTAP. Puoi tenere traccia dei progressi nella timeline.

In caso di problemi durante l'implementazione del sistema Cloud Volumes ONTAP, esaminare il messaggio di errore. È inoltre possibile selezionare l'ambiente di lavoro e fare clic su **Ricomcreare 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 Google Cloud

Guida rapida per Cloud Volumes ONTAP in Google Cloud

Inizia a utilizzare Cloud Volumes ONTAP per Google Cloud 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 Google Cloud"

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 sulla pianificazione della configurazione".

3 Configurare la rete

1. Assicurarsi che il VPC e le subnet supportino la connettività tra il connettore e Cloud Volumes ONTAP.
2. Se si prevede di abilitare il tiering dei dati, "Configurare la subnet Cloud Volumes ONTAP per l'accesso privato a Google".
3. Se si sta implementando una coppia ha, assicurarsi di disporre di quattro VPC, ciascuno con la propria subnet.
4. Se si utilizza un VPC condiviso, fornire il ruolo *Compute Network User* all'account del servizio Connector.
5. 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.

"Scopri di più sui requisiti di rete".

4 Impostare un account di servizio

Cloud Volumes ONTAP richiede un account di servizio cloud Google per due scopi. Il primo è quando si attiva "tiering dei dati" Per tierare i dati cold allo storage a oggetti a basso costo in Google Cloud. Il secondo si verifica quando si attiva "Backup e ripristino BlueXP" per eseguire il backup dei volumi in uno storage a oggetti a basso costo.

È possibile configurare un account di servizio e utilizzarlo per entrambi gli scopi. L'account di servizio deve avere il ruolo **Storage Admin**.

"Leggi le istruzioni dettagliate".

5 Abilitare le API di Google Cloud

"Abilita le seguenti API di Google Cloud nel tuo progetto". Queste API sono necessarie per implementare il connettore e Cloud Volumes ONTAP.

- API di Cloud Deployment Manager V2
- API Cloud Logging
- API Cloud Resource Manager
- API di Compute Engine
- API IAM (Identity and Access Management)

6 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"
- "Installazione del software del connettore su un host Linux"
- "Cosa fa BlueXP con le autorizzazioni Google Cloud"

Pianificare la configurazione di Cloud Volumes ONTAP in Google Cloud

Quando si implementa Cloud Volumes ONTAP in Google Cloud, 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 di Google Cloud. "Visualizza l'elenco completo delle regioni supportate".

Scegliere un tipo di computer supportato

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

"Configurazioni supportate per Cloud Volumes ONTAP in GCP"

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 GCP"

Dimensionare il sistema in GCP

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

Tipo di macchina

Esaminare i tipi di computer supportati in "Note di rilascio di Cloud Volumes ONTAP" Quindi, esamina i dettagli di Google relativi a ciascun tipo di computer supportato. Abbina i requisiti di carico di lavoro al numero di vCPU e di memoria per il tipo di computer. Si noti che ogni core della CPU aumenta le performance di rete.

Per ulteriori informazioni, fare riferimento a quanto segue:

- "Documentazione di Google Cloud: Tipi di computer standard N1"
- "Documentazione Google Cloud: Performance"

Tipo di disco GCP

Quando crei volumi per Cloud Volumes ONTAP, devi scegliere lo storage cloud sottostante utilizzato da Cloud Volumes ONTAP per un disco. Il tipo di disco può essere uno dei seguenti:

- *Dischi persistenti SSD Zonal*: I dischi persistenti SSD sono ideali per i carichi di lavoro che richiedono elevati tassi di IOPS casuali.
- *Dischi persistenti bilanciati zonali*: Questi SSD bilanciano le performance e i costi fornendo IOPS per GB inferiori.
- *Dischi persistenti standard zonali* : i dischi persistenti standard sono economici e possono gestire operazioni di lettura/scrittura sequenziali.

  Per ulteriori informazioni, vedere "Documentazione di Google Cloud: Dischi persistenti zonali (Standard e SSD)".

Dimensioni del disco GCP

Quando si implementa un sistema Cloud Volumes ONTAP, è necessario scegliere una dimensione iniziale del disco. Dopodiché, puoi lasciare che BlueXP gestisca la capacità di un sistema per te, ma se vuoi creare aggregati, tieni presente quanto segue:

- Tutti i dischi di un aggregato devono avere le stesse dimensioni.
- Determinare lo spazio necessario, tenendo in considerazione le performance.
- Le performance dei dischi persistenti si ridimensionano automaticamente in base alle dimensioni del disco e al numero di vCPU disponibili per il sistema.

  Per ulteriori informazioni, fare riferimento a quanto segue:

  - "Documentazione di Google Cloud: Dischi persistenti zonali (Standard e SSD)"
  - "Documentazione di Google Cloud: Ottimizzazione delle performance di dischi persistenti e SSD locali"

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 di Cloud Volumes ONTAP in Google Cloud".
- "Documenti di Google Cloud: Quote delle risorse"

  Il motore di calcolo per il cloud di Google applica quote sull'utilizzo delle risorse, in modo da garantire che non sia stato raggiunto il limite prima di implementare Cloud Volumes ONTAP.

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

Raccogliere informazioni di rete

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

Informazioni di rete per un sistema a nodo singolo

Informazioni GCP	Il tuo valore
Regione	
Zona	
Rete VPC	
Subnet	
Policy firewall (se si utilizza il proprio)	

Informazioni di rete per una coppia ha in più zone

Informazioni GCP	Il tuo valore
Regione	
Zona per nodo 1	
Zona per il nodo 2	
Zona per il mediatore	
VPC-0 e subnet	
VPC-1 e subnet	
VPC-2 e subnet	
VPC-3 e subnet	
Policy firewall (se si utilizza il proprio)	

Informazioni di rete per una coppia ha in una singola zona

Informazioni GCP	Il tuo valore
Regione	
Zona	
VPC-0 e subnet	
VPC-1 e subnet	
VPC-2 e subnet	
VPC-3 e subnet	
Policy firewall (se si utilizza il proprio)	

Scegliere una velocità di scrittura

BlueXP consente di scegliere un'impostazione della velocità di scrittura per Cloud Volumes ONTAP, ad eccezione delle coppie ad alta disponibilità (ha) in Google Cloud. 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.

Requisiti di rete per Cloud Volumes ONTAP in Google Cloud

Configura il tuo network Google Cloud in modo che i sistemi Cloud Volumes ONTAP possano funzionare correttamente.

Se si desidera implementare una coppia ha, è necessario "Scopri come funzionano le coppie ha in Google Cloud".

Requisiti per Cloud Volumes ONTAP

I seguenti requisiti devono essere soddisfatti in Google Cloud.

Requisiti specifici per i sistemi a nodo singolo

Se si desidera implementare un sistema a nodo singolo, assicurarsi che la rete soddisfi i seguenti requisiti.

Un VPC

Un Virtual Private Cloud (VPC) è richiesto per un sistema a nodo singolo.

Indirizzi IP privati

BlueXP assegna 3 o 4 indirizzi IP privati a un sistema a nodo singolo in Google Cloud.

È possibile saltare la creazione della LIF di gestione delle VM di storage se si implementa Cloud Volumes ONTAP utilizzando l'API e si specifica il seguente flag:

```
skipSvmManagementLif: true
```

LIF è un indirizzo IP associato a una porta fisica. Per strumenti di gestione come SnapCenter è necessaria una LIF di gestione delle macchine virtuali dello storage (SVM).

Requisiti specifici delle coppie ha

Se si desidera implementare una coppia ha, assicurarsi che la rete soddisfi i seguenti requisiti.

Una o più zone

È possibile garantire l'elevata disponibilità dei dati implementando una configurazione ha in più zone o in una singola zona. BlueXP richiede di scegliere più zone o una singola zona quando si crea la coppia ha.

- Zone multiple (consigliato)

  L'implementazione di una configurazione ha in tre zone garantisce la disponibilità continua dei dati in caso di guasto all'interno di una zona. Si noti che le prestazioni di scrittura sono leggermente inferiori rispetto all'utilizzo di una singola zona, ma sono minime.

- Zona singola

  Quando viene implementato in una singola zona, una configurazione Cloud Volumes ONTAP ha utilizza una policy di posizionamento distribuita. Questa policy garantisce che una configurazione ha sia protetta da un singolo punto di guasto all'interno della zona, senza dover utilizzare zone separate per ottenere l'isolamento degli errori.

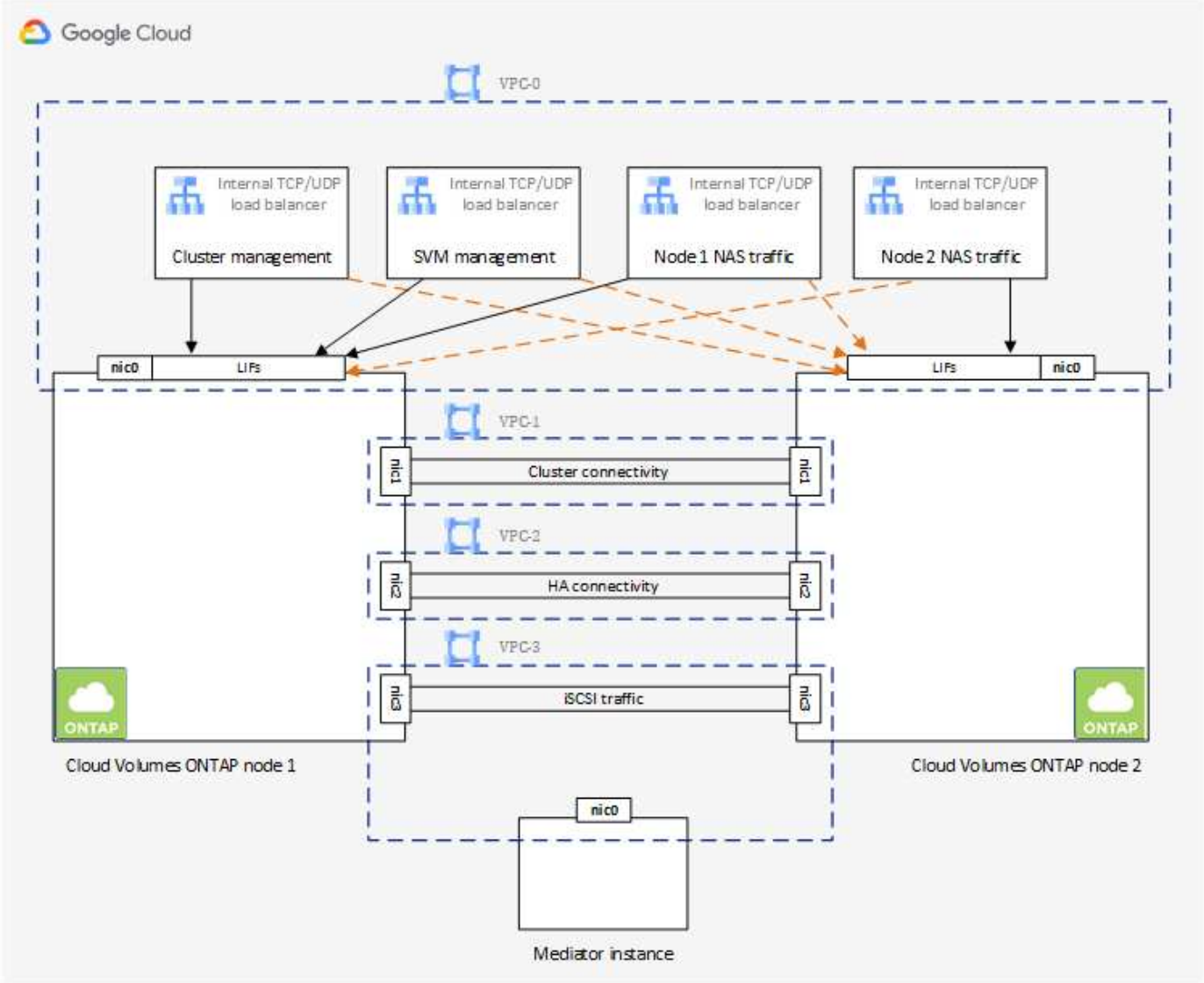
  Questo modello di implementazione riduce i costi perché non sono previsti costi di uscita dei dati tra le zone.

Quattro cloud privati virtuali

Per una configurazione ha sono necessari quattro Virtual Private Clouds (VPC). Sono necessari quattro VPC perché Google Cloud richiede che ogni interfaccia di rete risieda in una rete VPC separata.

BlueXP richiede di scegliere quattro VPC quando si crea la coppia ha:

- VPC-0 per le connessioni in entrata ai dati e ai nodi
- VPC-1, VPC-2 e VPC-3 per la comunicazione interna tra i nodi e il mediatore ha



Subnet

Per ogni VPC è necessaria una subnet privata.

Se si posiziona il connettore in VPC-0, sarà necessario attivare Private Google Access sulla subnet per accedere alle API e abilitare il tiering dei dati.

Le subnet di questi VPC devono avere intervalli CIDR distinti. Non possono avere intervalli CIDR sovrapposti.

Indirizzi IP privati

BlueXP assegna automaticamente il numero richiesto di indirizzi IP privati a Cloud Volumes ONTAP in Google Cloud. È necessario assicurarsi che la rete disponga di un numero sufficiente di indirizzi 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. Per strumenti di gestione come SnapCenter è necessaria una LIF di gestione SVM.

- **Nodo singolo**
  BlueXP alloca 4 indirizzi IP a un sistema con singolo nodo:

- LIF di gestione dei nodi
- LIF gestione cluster
- LIF dati iSCSI

> Un LIF iSCSI fornisce l'accesso client sul protocollo iSCSI e viene utilizzato dal sistema per altri importanti flussi di lavoro di rete. Questi LIF sono obbligatori e non devono essere cancellati.

- LIF NAS

  È possibile saltare la creazione della LIF di gestione delle VM di storage se si implementa Cloud Volumes ONTAP utilizzando l'API e si specifica il seguente flag:

```
skipSvmManagementLif: true
```

- **Coppia ha**
  BlueXP alloca gli indirizzi IP 12-13 a una coppia ha:
  - 2 LIF di gestione dei nodi (e0a)
  - 1 LIF di gestione del cluster (e0a)
  - 2 LIF iSCSI (e0a)

> Un LIF iSCSI fornisce l'accesso client sul protocollo iSCSI e viene utilizzato dal sistema per altri importanti flussi di lavoro di rete. Questi LIF sono obbligatori e non devono essere cancellati.

  - 1 o 2 LIF NAS (e0a)
  - 2 LIF cluster (e0b)
  - 2 indirizzi IP ha Interconnect (e0c)
  - 2 indirizzi IP iSCSI RSM (e0d)

    È possibile saltare la creazione della LIF di gestione delle VM di storage se si implementa Cloud Volumes ONTAP utilizzando l'API e si specifica il seguente flag:

```
skipSvmManagementLif: true
```

Bilanciatori di carico interni

BlueXP crea automaticamente quattro bilanciatori di carico interni di Google Cloud (TCP/UDP) che gestiscono il traffico in entrata verso la coppia ha di Cloud Volumes ONTAP. Non è richiesta alcuna configurazione Questo requisito è stato elencato semplicemente per informarti del traffico di rete e per mitigare eventuali problemi di sicurezza.

Un bilanciamento del carico è per la gestione del cluster, uno per la gestione delle macchine virtuali di storage (SVM), uno per il traffico NAS al nodo 1 e l'altro per il traffico NAS al nodo 2.

La configurazione per ciascun bilanciamento del carico è la seguente:

- Un indirizzo IP privato condiviso

- Un controllo globale dello stato di salute

  Per impostazione predefinita, le porte utilizzate dal controllo dello stato di salute sono 63001, 63002 e 63003.

- Un servizio backend TCP regionale
- Un servizio di backend UDP regionale
- Una regola di inoltro TCP
- Una regola di inoltro UDP
- L'accesso globale è disattivato

  Anche se l'accesso globale è disattivato per impostazione predefinita, è supportata l'abilitazione dell'IT post-implementazione. L'abbiamo disattivata perché il traffico tra regioni avrà latenze significativamente più elevate. Volevamo assicurarci che non avessi avuto un'esperienza negativa a causa di montaggi incrociati accidentali. L'attivazione di questa opzione è specifica per le esigenze aziendali.

VPC condivisi

Cloud Volumes ONTAP e il connettore sono supportati in un VPC condiviso Google Cloud e anche in VPC standalone.

Per un sistema a nodo singolo, il VPC può essere un VPC condiviso o un VPC standalone.

Per una coppia ha, sono necessari quattro VPC. Ciascuno di questi VPC può essere condiviso o standalone. Ad esempio, VPC-0 potrebbe essere un VPC condiviso, mentre VPC-1, VPC-2 e VPC-3 potrebbero essere VPC standalone.

Un VPC condiviso consente di configurare e gestire centralmente le reti virtuali in più progetti. È possibile configurare reti VPC condivise nel *progetto host* e implementare le istanze di connettori e macchine virtuali Cloud Volumes ONTAP in un *progetto di servizio*. "Documentazione di Google Cloud: Panoramica VPC condivisa".

"Esaminare le autorizzazioni VPC condivise richieste e descritte nella sezione implementazione di Connector"

Mirroring dei pacchetti in VPC

"Mirroring dei pacchetti" Deve essere disattivato nel VPC Google Cloud in cui si implementa Cloud Volumes ONTAP. Cloud Volumes ONTAP non può funzionare correttamente se il mirroring dei pacchetti è attivato.

Accesso a Internet in uscita

Cloud Volumes ONTAP richiede 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 di 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 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 firewall 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 firewall 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 si utilizza una coppia ha, il mediatore ha non richiede l'accesso a Internet in uscita.

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

Regole del firewall

Non è necessario creare regole firewall perché BlueXP fa questo per te. Se è necessario utilizzare il proprio, fare riferimento alle regole del firewall elencate di seguito.

Tenere presente che per una configurazione ha sono necessari due set di regole firewall:

- Un set di regole per i componenti ha in VPC-0. Queste regole consentono l'accesso ai dati a Cloud Volumes ONTAP. Scopri di più.
- Un altro insieme di regole per i componenti ha in VPC-1, VPC-2 e VPC-3. Queste regole sono aperte per le comunicazioni in entrata e in uscita tra i componenti ha. Scopri di più.

Se si desidera eseguire il tiering dei dati cold in un bucket di storage Google Cloud, la subnet in cui risiede Cloud Volumes ONTAP deve essere configurata per l'accesso privato Google (se si utilizza una coppia ha, questa è la subnet in VPC-0). Per istruzioni, fare riferimento a. "Documentazione di Google Cloud: Configurazione di Private Google Access".

Per ulteriori passaggi necessari per impostare il tiering dei dati in BlueXP, vedere "Tiering dei dati cold su storage a oggetti a basso costo".

Connessioni a sistemi ONTAP in altre reti

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

Per istruzioni, fare riferimento a. "Documentazione di Google Cloud: Panoramica di Cloud VPN".

Regole del firewall

BlueXP crea regole di Google Cloud Firewall che includono le regole in entrata e in uscita di cui Cloud Volumes ONTAP ha bisogno per funzionare correttamente. È possibile fare riferimento alle porte a scopo di test o se si preferisce utilizzare le proprie regole firewall.

Le regole del firewall per Cloud Volumes ONTAP richiedono regole sia in entrata che in uscita. Se si sta implementando una configurazione ha, queste sono le regole firewall per Cloud Volumes ONTAP in VPC-0.

Tenere presente che per una configurazione ha sono necessari due set di regole firewall:

- Un set di regole per i componenti ha in VPC-0. Queste regole consentono l'accesso ai dati a Cloud Volumes ONTAP.
- Un altro insieme di regole per i componenti ha in VPC-1, VPC-2 e VPC-3. Queste regole sono aperte per le

comunicazioni in entrata e in uscita tra i componenti ha. Scopri di più.

Cerchi informazioni sul connettore? "Visualizzare le regole del firewall per il connettore"

Regole in entrata

Quando si crea un ambiente di lavoro, è possibile scegliere il filtro di origine per la policy firewall predefinita durante l'implementazione:

- **Selezionato solo VPC**: Il filtro di origine per il 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**: Il filtro di origine per il traffico in entrata corrisponde all'intervallo IP 0.0.0.0/0.

Se si utilizza una policy firewall personalizzata, assicurarsi di aggiungere tutte le reti che devono comunicare con Cloud Volumes ONTAP, ma anche di aggiungere entrambi gli intervalli di indirizzi per consentire al bilanciamento del carico interno di Google di funzionare correttamente. Questi indirizzi sono 130.211.0.0/22 e 35.191.0.0/16. Per ulteriori informazioni, fare riferimento a. "Documentazione di Google Cloud: Regole del firewall per il bilanciamento del carico".

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

Protocollo	Porta	Scopo
TCP	63001-63050	Bilanciamento del carico delle porte delle sonde per determinare quale nodo è integro (richiesto solo per coppie ha)
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 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
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)
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	DHCP server (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
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

Servizio	Protocollo	Porta	Origine	Destinazione	Scopo
Syslog	UDP	514	LIF di gestione dei nodi	Server syslog	Messaggi di inoltro syslog

Regole per VPC-1, VPC-2 e VPC-3

In Google Cloud, una configurazione ha viene implementata in quattro VPC. Le regole del firewall necessarie per la configurazione ha in VPC-0 sono Elencato sopra per Cloud Volumes ONTAP.

Nel frattempo, le regole predefinite del firewall create da BlueXP per le istanze in VPC-1, VPC-2 e VPC-3 consentono la comunicazione in ingresso su *tutti* protocolli e porte. Queste regole consentono la comunicazione tra i nodi ha.

La comunicazione dai nodi ha al mediatore ha avviene sulla porta 3260 (iSCSI).

> Per consentire un'elevata velocità di scrittura per le nuove implementazioni di coppie Google Cloud ha, è necessaria un'unità di trasmissione massima (MTU) di almeno 8,896 byte per VPC-1, VPC-2 e VPC-3. Se si sceglie di aggiornare VPC-1, VPC-2 e VPC-3 esistenti a una MTU di 8,896 byte, è necessario arrestare tutti i sistemi ha esistenti che utilizzano questi VPC durante il processo di configurazione.

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 firewall in Google Cloud"

Pianificazione dei controlli dei servizi VPC in GCP

Quando si sceglie di bloccare l'ambiente Google Cloud con i controlli dei servizi VPC, è necessario comprendere come BlueXP e Cloud Volumes ONTAP interagiscono con le API di Google Cloud e come configurare il perimetro dei servizi per implementare BlueXP e Cloud Volumes ONTAP.

I controlli dei servizi VPC consentono di controllare l'accesso ai servizi gestiti da Google all'esterno di un perimetro attendibile, di bloccare l'accesso ai dati da posizioni non attendibili e di ridurre i rischi di trasferimento dei dati non autorizzato. "Scopri di più su Google Cloud VPC Service Controls".

Come i servizi NetApp comunicano con VPC Service Controls

BlueXP comunica direttamente con le API di Google Cloud. Questo viene attivato da un indirizzo IP esterno a Google Cloud (ad esempio, da api.services.cloud.netapp.com) o da un indirizzo interno assegnato a BlueXP Connector all'interno di Google Cloud.

A seconda dello stile di implementazione del connettore, potrebbero essere necessarie alcune eccezioni per il perimetro del servizio.

Immagini

Sia Cloud Volumes ONTAP che BlueXP utilizzano le immagini di un progetto all'interno del GCP gestito da NetApp. Questo può influire sulla distribuzione di BlueXP Connector e Cloud Volumes ONTAP, se l'organizzazione dispone di un criterio che blocca l'utilizzo di immagini non ospitate all'interno dell'organizzazione.

È possibile implementare un connettore manualmente utilizzando il metodo di installazione manuale, ma Cloud Volumes ONTAP dovrà anche estrarre le immagini dal progetto NetApp. È necessario fornire un elenco consentito per implementare un connettore e Cloud Volumes ONTAP.

Implementazione di un connettore

L'utente che implementa un connettore deve essere in grado di fare riferimento a un'immagine ospitata nel projectId *netapp-cloudmanager* e al numero di progetto *14190056516*.

Implementazione di Cloud Volumes ONTAP

- L'account del servizio BlueXP deve fare riferimento a un'immagine ospitata nel projectId *netapp-cloudmanager* e al numero di progetto *14190056516* del progetto del servizio.
- L'account di servizio per l'agente di servizio API di Google predefinito deve fare riferimento a un'immagine ospitata nel projectId *netapp-cloudmanager* e al numero di progetto *14190056516* del progetto di servizio.

Di seguito sono riportati alcuni esempi delle regole necessarie per estrarre queste immagini con VPC Service Controls.

Servizio VPC controlla le policy del perimetro

I criteri consentono eccezioni ai set di regole VPC Service Controls. Per ulteriori informazioni sulle policy, visitare il "GCP VPC Service Controls Policy Documentation".

Per impostare i criteri richiesti da BlueXP, accedere al perimetro dei controlli dei servizi VPC all'interno dell'organizzazione e aggiungere i seguenti criteri. I campi devono corrispondere alle opzioni fornite nella pagina delle policy VPC Service Controls. Si noti inoltre che le regole **all** sono obbligatorie e che i parametri **OR** devono essere utilizzati nel set di regole.

Regole di ingresso

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

OPPURE

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

OPPURE

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

Regole di uscita

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

Il numero di progetto sopra indicato è il progetto *netapp-cloud-manager* utilizzato da NetApp per memorizzare le immagini per il connettore e per Cloud Volumes ONTAP.

Creare un account di servizio per il tiering e i backup dei dati

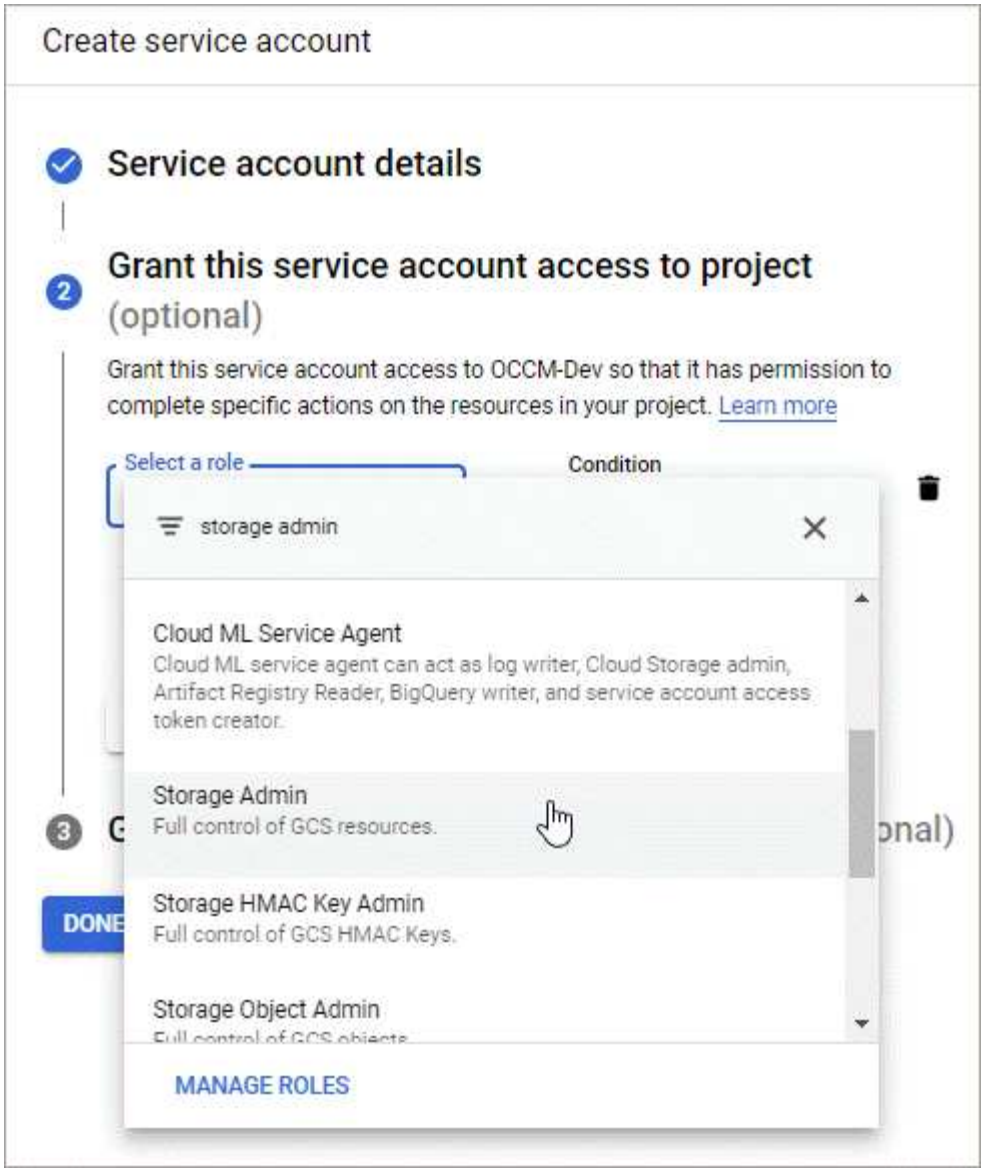
Cloud Volumes ONTAP richiede un account di servizio cloud Google per due scopi. Il primo è quando si attiva "tiering dei dati" Per tierare i dati cold allo storage a oggetti a basso costo in Google Cloud. Il secondo si verifica quando si attiva "Backup e ripristino BlueXP" per eseguire il backup dei volumi in uno storage a oggetti a basso costo.

Cloud Volumes ONTAP utilizza l'account di servizio per accedere e gestire un bucket per i dati a più livelli e un altro bucket per i backup.

È possibile configurare un account di servizio e utilizzarlo per entrambi gli scopi. L'account di servizio deve avere il ruolo **Storage Admin**.

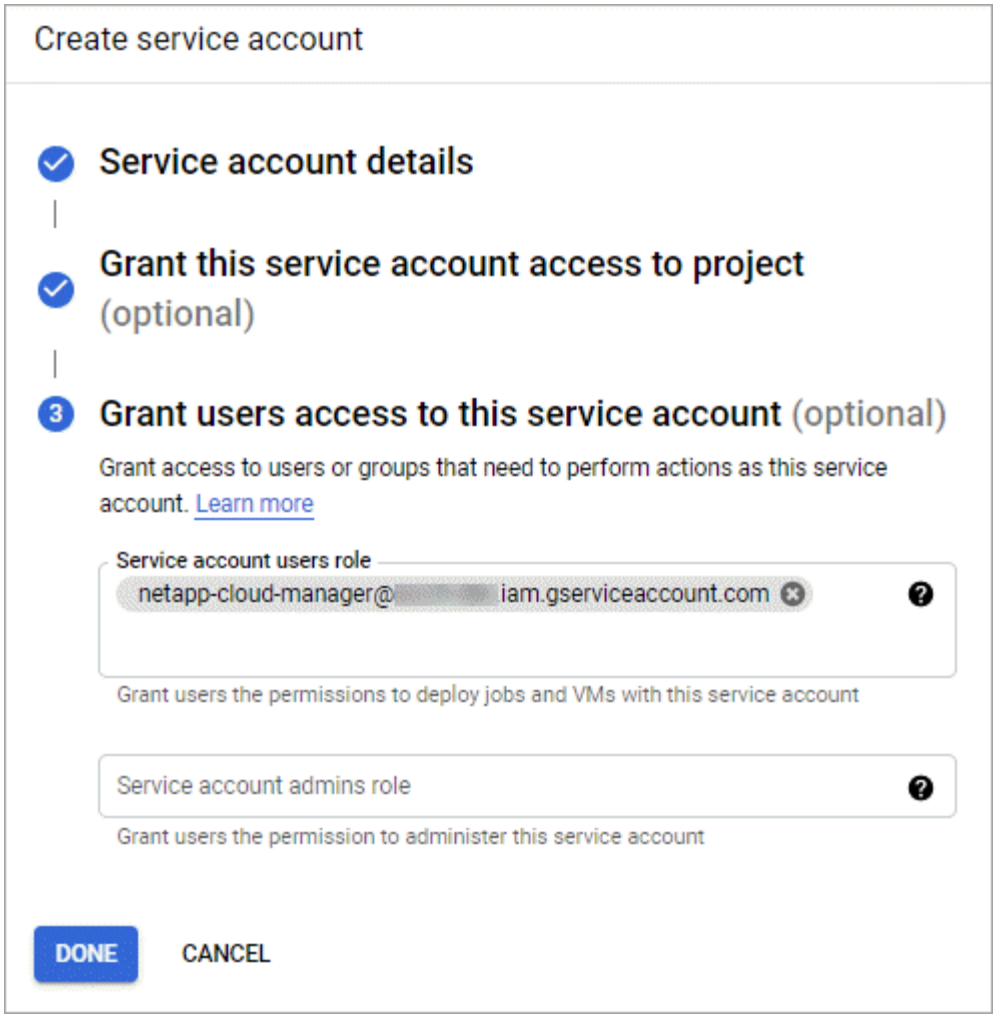
Fasi

1. Nella console di Google Cloud, "Accedere alla pagina Service accounts (account servizio)".
2. Selezionare il progetto.
3. Fare clic su **Create service account** (Crea account servizio) e fornire le informazioni richieste.
    a. **Dettagli account servizio**: Inserire un nome e una descrizione.
    b. **Consenti a questo account di servizio l'accesso al progetto**: Selezionare il ruolo **Storage Admin**.



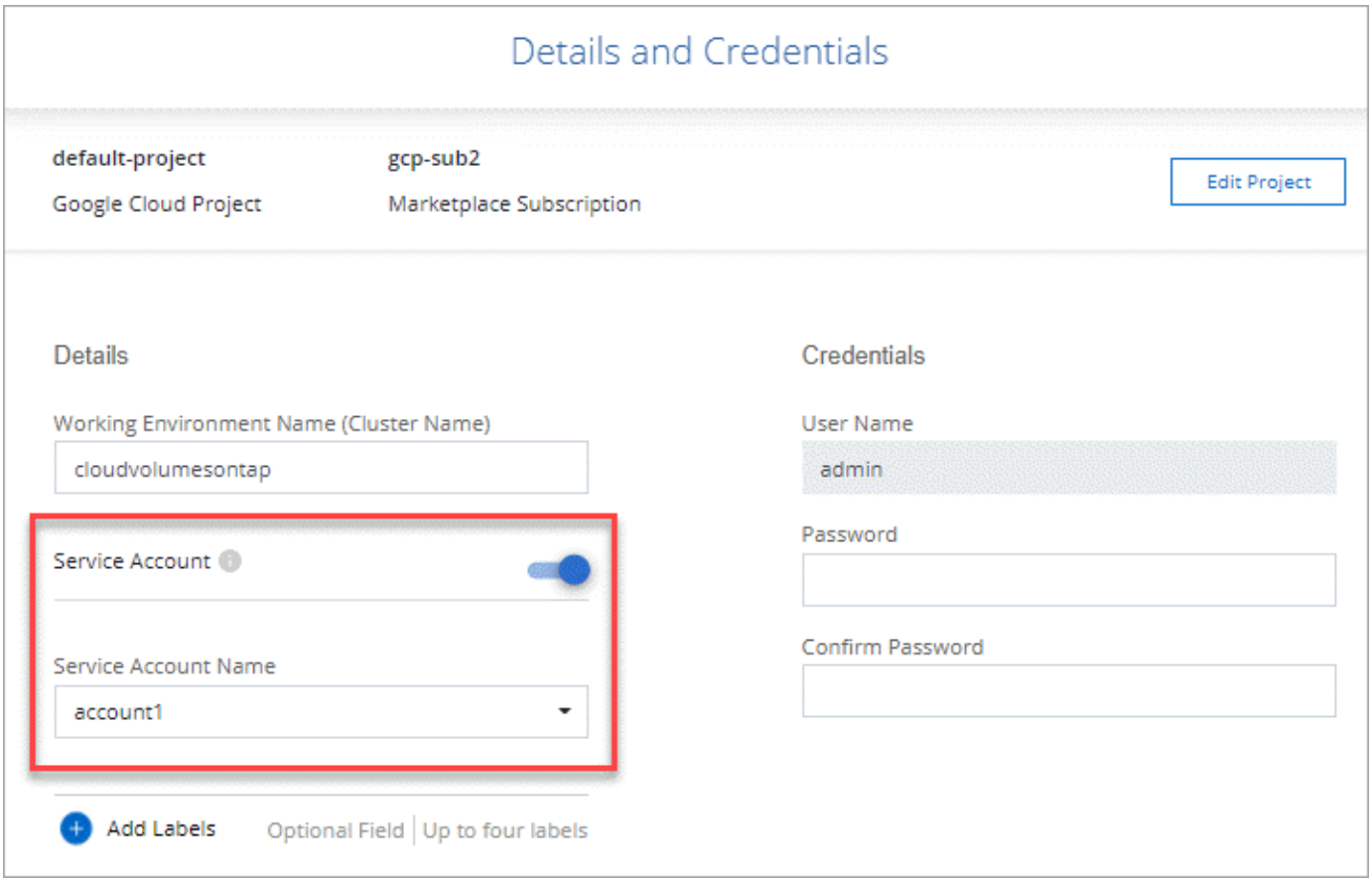
c. **Consenti agli utenti di accedere a questo account del servizio**: Aggiungi l'account del servizio Connector come *utente dell'account del servizio* a questo nuovo account del servizio.

   Questa fase è necessaria solo per il tiering dei dati. Non è necessario per il backup e il ripristino di BlueXP.



Quali sono le prossime novità?

Quando si crea un ambiente di lavoro Cloud Volumes ONTAP, sarà necessario selezionare l'account del servizio in un secondo momento.



Utilizzo di chiavi di crittografia gestite dal cliente con Cloud Volumes ONTAP

Mentre Google Cloud Storage crittografa sempre i tuoi dati prima che vengano scritti su disco, puoi utilizzare l'API BlueXP per creare un sistema Cloud Volumes ONTAP che utilizza *chiavi di crittografia gestite dal cliente*. Si tratta di chiavi che vengono generate e gestite in GCP utilizzando il Cloud Key Management Service.

Fasi

1. Assicurarsi che l'account di servizio di BlueXP Connector disponga delle autorizzazioni corrette a livello di progetto, nel progetto in cui è memorizzata la chiave.

   Le autorizzazioni sono fornite in "Per impostazione predefinita, le autorizzazioni dell'account di servizio del connettore", Ma potrebbe non essere applicato se si utilizza un progetto alternativo per il Cloud Key Management Service.

   Le autorizzazioni sono le seguenti:

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. Assicurarsi che l'account di servizio per "Agente di servizio di Google Compute Engine" Dispone delle autorizzazioni Cloud KMS Encrypter/Decrypter sulla chiave.

Il nome dell'account del servizio utilizza il seguente formato: "Servizio-[numero_progetto_servizio]@compute-system.iam.gserviceaccount.com".

"Documentazione Google Cloud: Utilizzo di IAM con Cloud KMS - assegnazione di ruoli a una risorsa"

3. Ottenere l'id della chiave richiamando il comando get per `/gcp/vsa/metadata/gcp-encryption-keys` Chiamata API o selezionando "Copy Resource Name" (Copia nome risorsa) sulla chiave nella console GCP.
4. Se si utilizzano chiavi di crittografia gestite dal cliente e tiering dei dati per lo storage a oggetti, BlueXP tenta di utilizzare le stesse chiavi utilizzate per crittografare i dischi persistenti. Tuttavia, prima di tutto, dovrai abilitare i bucket di storage Google Cloud per utilizzare le chiavi:

   a. Individuare l'agente del servizio Google Cloud Storage seguendo la "Documentazione Google Cloud: Ottenere l'agente del servizio Cloud Storage".

   b. Accedere alla chiave di crittografia e assegnare all'agente del servizio Google Cloud Storage le autorizzazioni di crittografia/decrypter Cloud KMS.

   Per ulteriori informazioni, fare riferimento a. "Documentazione Google Cloud: Utilizzo di chiavi di crittografia gestite dal cliente"

5. Utilizzare il parametro "GcpEncryption" con la richiesta API durante la creazione di un ambiente di lavoro.

   Esempio

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-1/cryptoKeys/generatedkey1"
  }
```

Fare riferimento a. "Documenti sull'automazione BlueXP" Per ulteriori informazioni sull'utilizzo del parametro "GcpEncryption".

Impostare la licenza per Cloud Volumes ONTAP in Google Cloud

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".

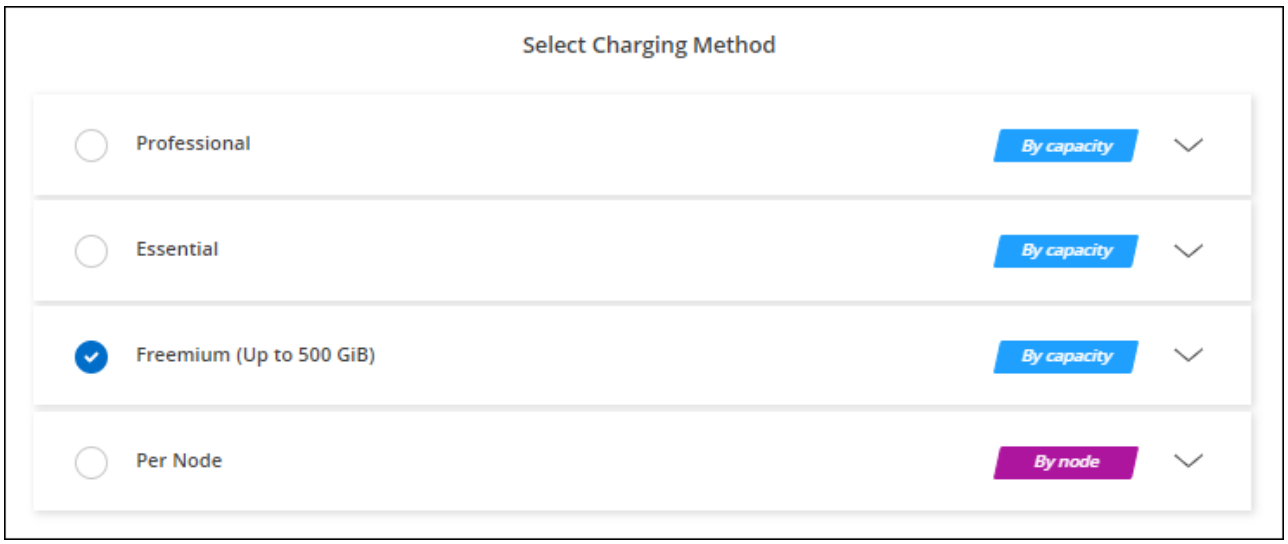
Fasi

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 Google Cloud 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".

b. 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 Google Cloud".

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 Google Cloud Marketplace
- Un contratto annuale

"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"

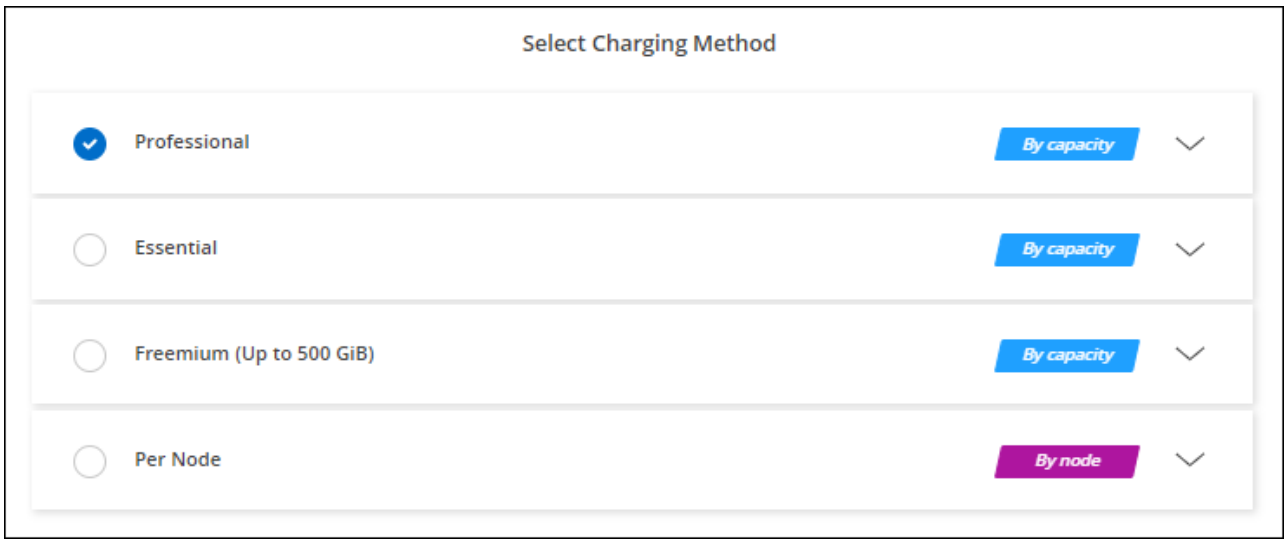
   BlueXP interroga automaticamente il servizio di licensing di NetApp per ottenere dettagli sulle licenze associate al tuo account NetApp Support Site. In assenza di errori, BlueXP aggiunge automaticamente le licenze al portafoglio digitale.

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 Google Cloud 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.

   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 Google Cloud".

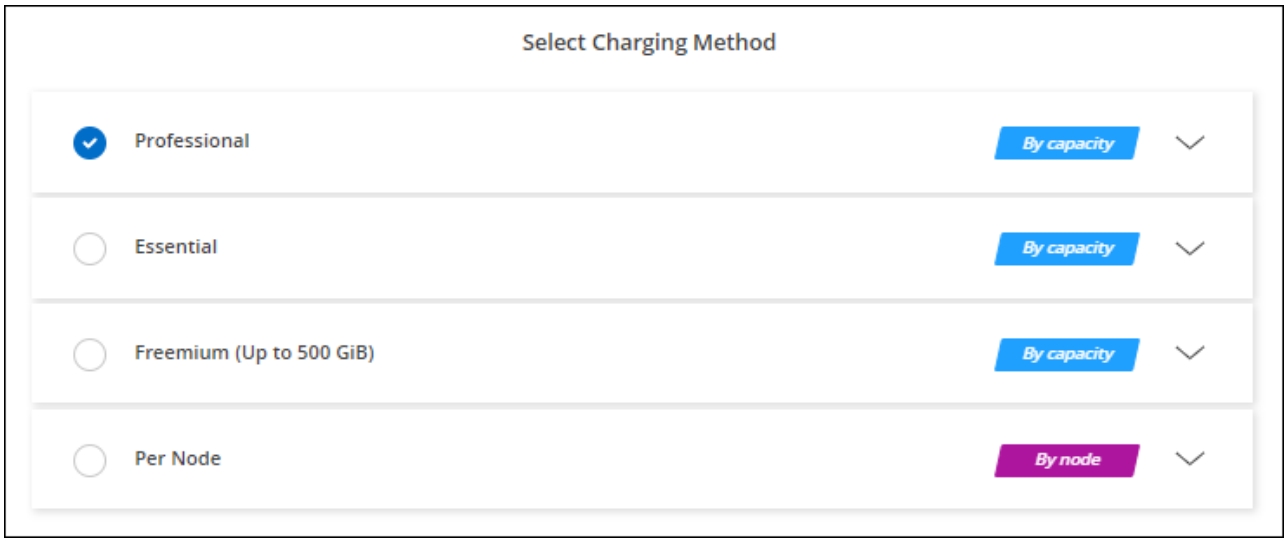
Abbonamento PAYGO

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

Quando crei un ambiente di lavoro Cloud Volumes ONTAP, BlueXP ti chiede di sottoscrivere il contratto disponibile in Google Cloud Marketplace. 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 Google Cloud 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 Google Cloud".

Puoi gestire gli abbonamenti a Google Cloud Marketplace associati ai tuoi account dalla pagina Impostazioni > credenziali. "Scopri come gestire le tue credenziali e sottoscrizioni Google Cloud"

Contratto annuale

Paga Cloud Volumes ONTAP ogni anno acquistando un contratto annuale.

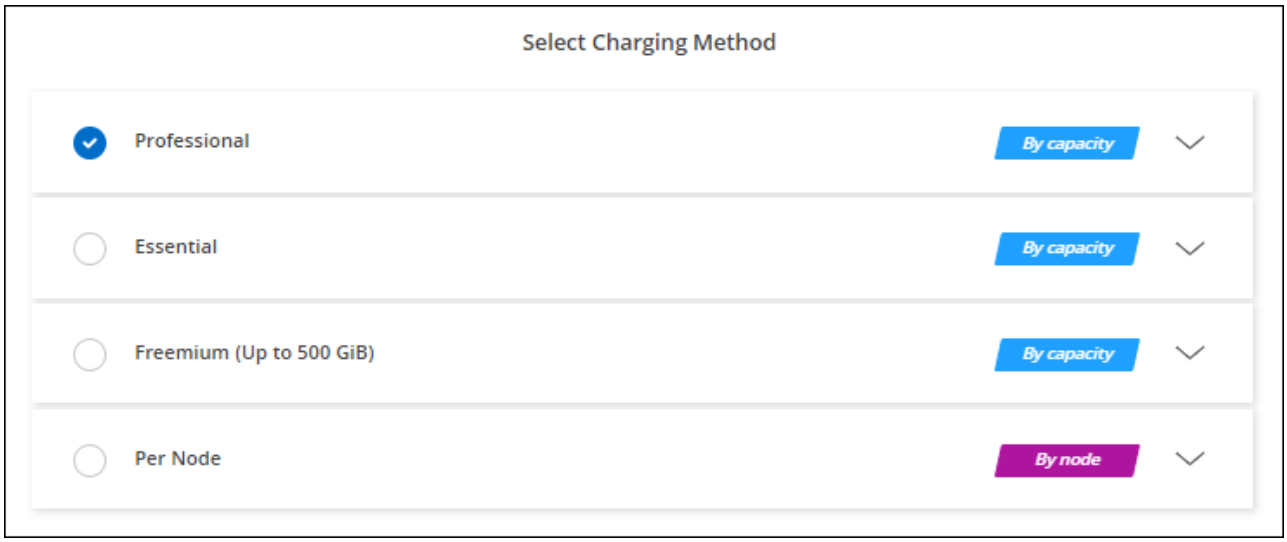
Fasi

1. Contatta il tuo commerciale NetApp per acquistare un contratto annuale.

   Il contratto è disponibile come offerta *privata* in Google Cloud Marketplace.

   Dopo che NetApp condivide l'offerta privata con te, puoi selezionare il piano annuale quando ti iscrivi da Google Cloud Marketplace durante la creazione dell'ambiente di lavoro.

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 al piano annuale in Google Cloud Marketplace.
   b. In Google Cloud, seleziona il piano annuale condiviso con il tuo account, quindi fai clic su **Iscriviti**.
   c. Una volta visualizzato BlueXP, selezionare un pacchetto basato sulla capacità quando si accede alla pagina dei metodi di ricarica.



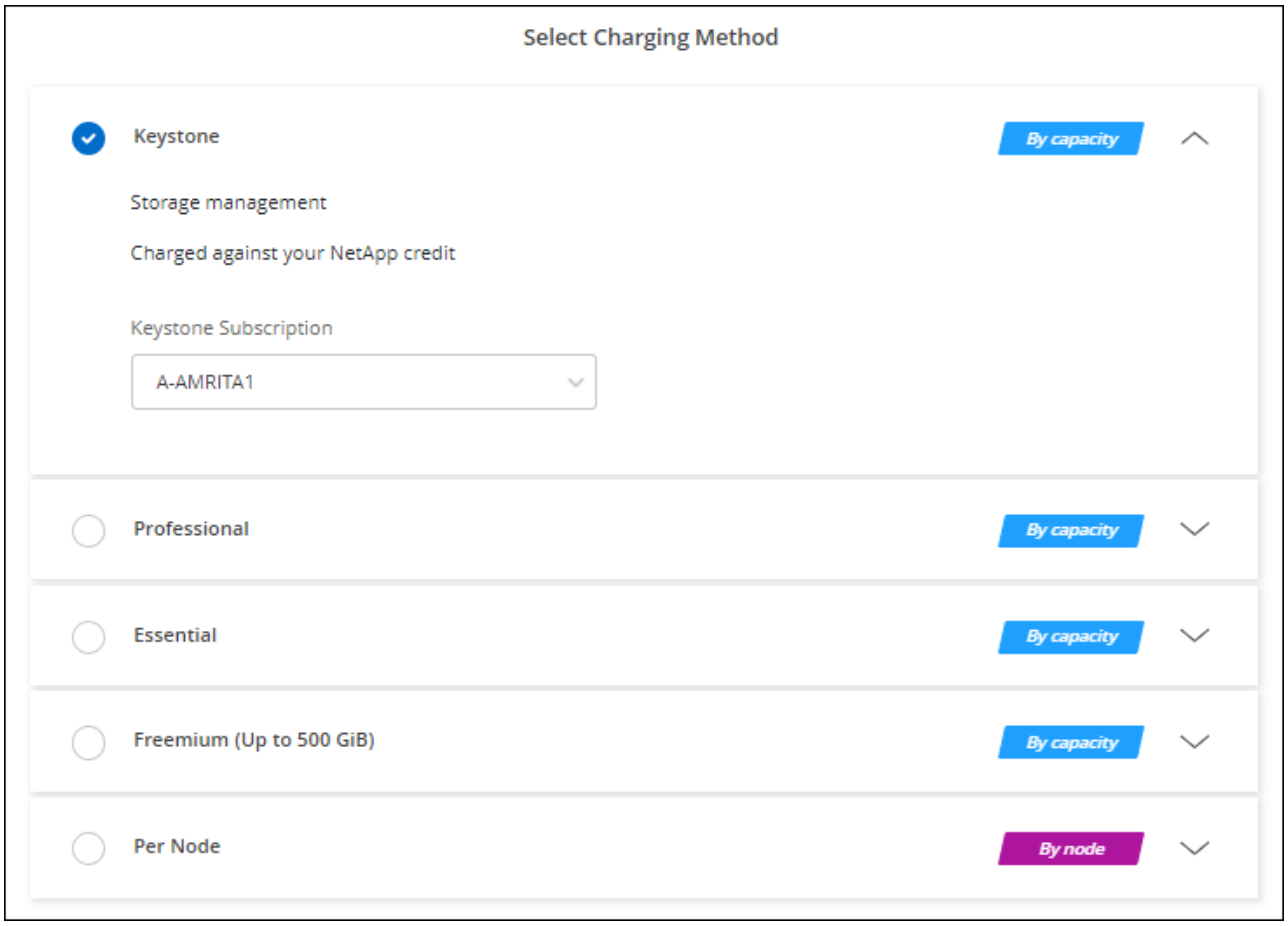
"Visualizza le istruzioni dettagliate per avviare Cloud Volumes ONTAP in Google Cloud".

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 Google Cloud".

Lancio di Cloud Volumes ONTAP in Google Cloud

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

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".
  - L'account del servizio associato al connettore "deve disporre delle autorizzazioni necessarie"
- Comprensione della configurazione che si desidera utilizzare.

  Dovresti aver preparato scegliendo una configurazione e ottenendo le informazioni di rete di Google Cloud dal tuo 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".

- Le API di Google Cloud dovrebbero essere "abilitato nel tuo progetto":
  - API di Cloud Deployment Manager V2
  - API Cloud Logging
  - API Cloud Resource Manager
  - API di Compute Engine
  - API IAM (Identity and Access Management)

Avvio di un sistema a nodo singolo in Google Cloud

Creare un ambiente di lavoro in BlueXP per avviare Cloud Volumes ONTAP in Google Cloud.

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 **Google Cloud** e **Cloud Volumes ONTAP**.
4. Se richiesto, "Creare un connettore".
5. **Dettagli e credenziali**: Selezionare un progetto, specificare un nome di cluster, selezionare un account di servizio, aggiungere etichette e specificare le credenziali.

   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 Google Cloud VM. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.
Nome account servizio	Se si intende utilizzare "tiering dei dati" oppure "Backup e ripristino BlueXP" Con Cloud Volumes ONTAP, è necessario attivare **account di servizio** e selezionare un account di servizio con il ruolo di amministratore dello storage predefinito. "Scopri come creare un account di servizio".
Aggiungi etichette	Le etichette sono metadati per le risorse Google Cloud. BlueXP aggiunge le etichette al sistema Cloud Volumes ONTAP e alle risorse di Google Cloud associate al sistema. È possibile aggiungere fino a quattro etichette dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altre dopo la creazione. Si noti che l'API non limita l'utente a quattro etichette quando crea un ambiente di lavoro. Per informazioni sulle etichette, fare riferimento a. "Documentazione Google Cloud: Risorse per l'etichettatura".
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.

Campo	Descrizione
Modifica progetto	Selezionare il progetto in cui si desidera che Cloud Volumes ONTAP risieda. Il progetto predefinito è il progetto in cui risiede BlueXP. Se nell'elenco a discesa non sono presenti progetti aggiuntivi, l'account del servizio BlueXP non è ancora stato associato ad altri progetti. Accedere alla console di Google Cloud, aprire il servizio IAM e selezionare il progetto. Aggiungere l'account del servizio con il ruolo BlueXP a quel progetto. Dovrai ripetere questo passaggio per ogni progetto. Account di servizio impostato per BlueXP, "come descritto in questa pagina". Fare clic su **Add Subscription** (Aggiungi abbonamento) per associare le credenziali selezionate a un abbonamento. Per creare un sistema Cloud Volumes ONTAP pay-as-you-go, devi selezionare un progetto Google Cloud associato a un abbonamento a Cloud Volumes ONTAP da Google Cloud Marketplace.

Il video seguente mostra come associare un abbonamento a pagamento a Marketplace al progetto Google Cloud. In alternativa, seguire la procedura per effettuare l'iscrizione nella "Associazione di un abbonamento a Marketplace con le credenziali Google Cloud" sezione.

► https://docs.netapp.com/it-it/test//media/video_subscribing_gcp.mp4 *(video)*

6. **Servizi**: Selezionare i servizi che si desidera utilizzare sul sistema. Per selezionare il backup e ripristino BlueXP o per utilizzare il tiering BlueXP, è necessario aver specificato l'account di servizio nel passaggio 3.

   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. **Posizione e connettività**: Selezionare una posizione, scegliere una policy firewall e confermare la connettività di rete allo storage Google Cloud per il tiering dei dati.

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

Campo	Descrizione
Verifica della connettività	Per eseguire il tiering dei dati cold in un bucket di storage cloud Google, la subnet in cui risiede Cloud Volumes ONTAP deve essere configurata per l'accesso privato a Google. Per istruzioni, fare riferimento a. "Documentazione Google Cloud: Configurazione di Private Google Access".

Campo	Descrizione
Policy firewall generata	Se si consente a BlueXP di generare il criterio firewall, è necessario scegliere come consentire il traffico: • Se si sceglie **Selected VPC only** (solo VPC selezionato), il filtro di origine per il traffico in entrata corrisponde all'intervallo di sottorete del VPC selezionato e all'intervallo di sottorete del VPC in cui si trova il connettore. Questa è l'opzione consigliata. • Se si sceglie **All VPC**, il filtro di origine per il traffico in entrata corrisponde all'intervallo IP 0.0.0.0/0.
Utilizza policy firewall esistenti	Se si utilizza un criterio firewall esistente, assicurarsi che includa le regole richieste. Link: Learn About firewall rules for Cloud Volumes ONTAP.

8. **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".
9. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per implementare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Crea la mia configurazione**.

   Se si sceglie uno dei pacchetti, è sufficiente specificare un volume e quindi rivedere e approvare la configurazione.
10. **Licenza**: Modificare la versione di Cloud Volumes ONTAP in base alle esigenze e selezionare un tipo di computer.

    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 viene eseguito da una versione all'altra, ad esempio da 9,6 a 9,7.
11. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco e le dimensioni di ciascun disco.

    Il tipo di disco è per il volume iniziale. È possibile scegliere un tipo di disco diverso per i volumi successivi.

    Le dimensioni del disco sono 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.

    Per informazioni sulla scelta del tipo e delle dimensioni di un disco, vedere "Dimensionare il sistema in Google Cloud".
12. **Flash cache, velocità di scrittura e WORM**:
    a. Attivare **Flash cache**, se lo si desidera.

A partire da Cloud Volumes ONTAP 9.13.1, *Flash cache* è supportato sui tipi di istanze n2-standard-16, n2-standard-32, n2-standard-48 e n2-standard-64. Non è possibile disattivare Flash cache dopo l'implementazione.

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

"Scopri di più sulla velocità di scrittura".

L'opzione **High** write speed (velocità di scrittura elevata) offre un'elevata velocità di scrittura e un'unità MTU (Maximum Transmission Unit) di 8,896 byte. Inoltre, la MTU superiore di 8,896 richiede la selezione di VPC-1, VPC-2 e VPC-3 per l'implementazione. Per ulteriori informazioni su VPC-1, VPC-2 e VPC-3, vedere "Regole per VPC-1, VPC-2 e VPC-3".

c. 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.

13. **Tiering dei dati nella piattaforma cloud di Google**: Scegliere se attivare il tiering dei dati sull'aggregato iniziale, scegliere una classe di storage per i dati a più livelli, quindi selezionare un account di servizio con il ruolo di amministratore dello storage predefinito (richiesto per Cloud Volumes ONTAP 9.7 o versione successiva), Oppure seleziona un account Google Cloud (richiesto per Cloud Volumes ONTAP 9.6).

Tenere presente quanto segue:

- BlueXP imposta l'account del servizio sull'istanza di Cloud Volumes ONTAP. Questo account di servizio fornisce le autorizzazioni per il tiering dei dati a un bucket di storage Google Cloud. Assicurarsi di aggiungere l'account del servizio Connector come utente dell'account del servizio di tiering, altrimenti non è possibile selezionarlo da BlueXP
- Per informazioni sull'aggiunta di un account Google Cloud, vedere "Configurazione e aggiunta di account Google Cloud per il tiering dei dati con 9.6".
- 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 su aggregati successivi, ma è necessario spegnere il sistema e aggiungere un account di servizio dalla console di Google Cloud.

"Scopri di più sul tiering dei dati".

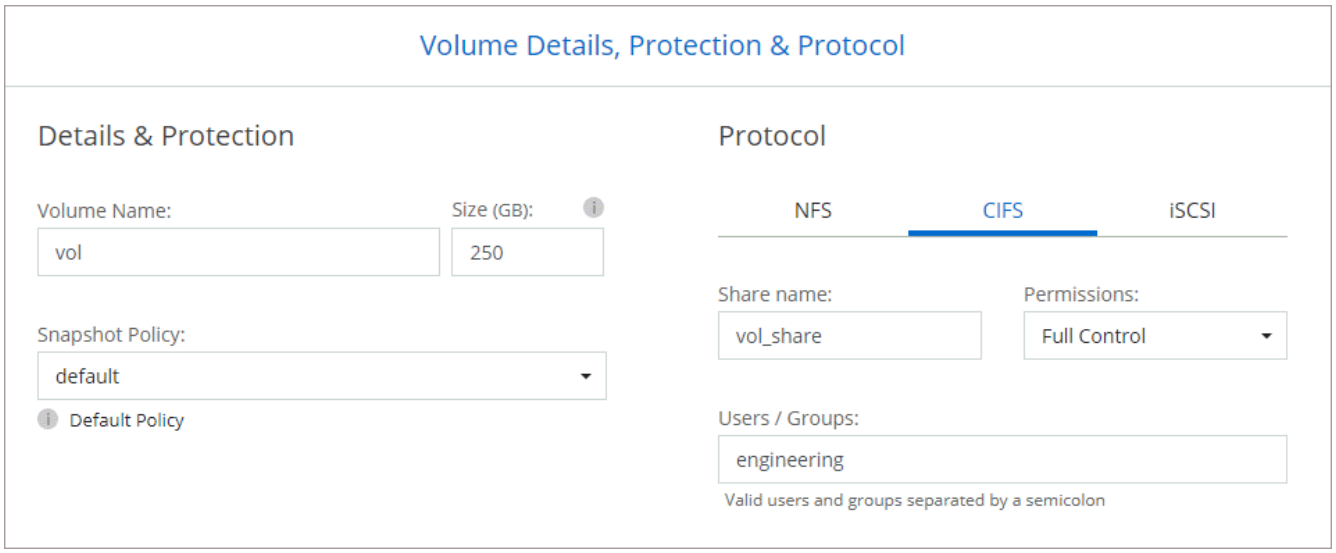
14. **Create Volume** (Crea volume): Inserire i dettagli del nuovo volume o fare clic su **Skip** (Ignora).

"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:



15. **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. Se si configura Google Managed Active Directory, per impostazione predefinita è possibile accedere ad utilizzando l'indirizzo IP 169.254.169.254.
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. Per configurare Google Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=cloud** in questo campo. "Documentazione Google Cloud: Unità organizzative in Google Managed Microsoft ad"
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.

Campo	Descrizione
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.

16. **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".

17. **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 Google Cloud che BlueXP acquisterà.
    c. Selezionare le caselle di controllo **ho capito…**.
    d. Fare clic su **Go**.

Risultato

BlueXP implementa il sistema Cloud Volumes ONTAP. Puoi tenere traccia dei progressi nella timeline.

In caso di problemi durante l'implementazione del sistema Cloud Volumes ONTAP, esaminare il messaggio di errore. È inoltre possibile selezionare l'ambiente di lavoro e fare clic su **Ricomcreare 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.

Lancio di una coppia ha in Google Cloud

Creare un ambiente di lavoro in BlueXP per avviare Cloud Volumes ONTAP in Google Cloud.

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 **Google Cloud** e **Cloud Volumes ONTAP ha**.
4. **Dettagli e credenziali**: Selezionare un progetto, specificare un nome di cluster, selezionare un account di

servizio, aggiungere etichette e specificare le credenziali.

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 Google Cloud VM. Se si seleziona questa opzione, il nome viene utilizzato anche come prefisso per il gruppo di protezione predefinito.
Nome account servizio	Se si intende utilizzare "Tiering BlueXP" oppure "Backup e ripristino BlueXP" Services (servizi), è necessario attivare lo switch **Service account** (account servizio) e selezionare l'account di servizio che ha il ruolo di amministratore dello storage predefinito.
Aggiungi etichette	Le etichette sono metadati per le risorse Google Cloud. BlueXP aggiunge le etichette al sistema Cloud Volumes ONTAP e alle risorse di Google Cloud associate al sistema. È possibile aggiungere fino a quattro etichette dall'interfaccia utente durante la creazione di un ambiente di lavoro e aggiungerne altre dopo la creazione. Si noti che l'API non limita l'utente a quattro etichette quando crea un ambiente di lavoro. Per informazioni sulle etichette, fare riferimento a. "Documentazione Google Cloud: Risorse per l'etichettatura".
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 progetto	Selezionare il progetto in cui si desidera che Cloud Volumes ONTAP risieda. Il progetto predefinito è il progetto in cui risiede BlueXP. Se nell'elenco a discesa non sono presenti progetti aggiuntivi, l'account del servizio BlueXP non è ancora stato associato ad altri progetti. Accedere alla console di Google Cloud, aprire il servizio IAM e selezionare il progetto. Aggiungere l'account del servizio con il ruolo BlueXP a quel progetto. Dovrai ripetere questo passaggio per ogni progetto. Account di servizio impostato per BlueXP, "come descritto in questa pagina". Fare clic su **Add Subscription** (Aggiungi abbonamento) per associare le credenziali selezionate a un abbonamento. Per creare un sistema Cloud Volumes ONTAP pay-as-you-go, devi selezionare un progetto Google Cloud associato a un abbonamento a Cloud Volumes ONTAP da Google Cloud Marketplace.

Il video seguente mostra come associare un abbonamento a pagamento a Marketplace al progetto Google Cloud. In alternativa, seguire la procedura per effettuare l'iscrizione nella "Associazione di un

abbonamento a Marketplace con le credenziali Google Cloud" sezione.

► https://docs.netapp.com/it-it/test//media/video_subscribing_gcp.mp4 *(video)*

5. **Servizi**: Selezionare i servizi che si desidera utilizzare sul sistema. Per selezionare il backup e ripristino BlueXP o per utilizzare BlueXP Tiering, è necessario aver specificato l'account di servizio nel passaggio 3.

   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. **Ha Deployment Models** (modelli di implementazione ha): Scegliere più zone (consigliato) o una singola zona per la configurazione ha. Quindi selezionare una regione e zone.

   "Scopri di più sui modelli di implementazione ha".

7. **Connettività**: Selezionare quattro diversi VPC per la configurazione ha, una subnet in ciascun VPC, quindi scegliere un criterio firewall.

   "Scopri di più sui requisiti di rete".

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

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

8. **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".
9. **Pacchetti preconfigurati**: Selezionare uno dei pacchetti per implementare rapidamente un sistema Cloud Volumes ONTAP oppure fare clic su **Crea la mia configurazione**.

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

10. **Licenza**: Modificare la versione di Cloud Volumes ONTAP in base alle esigenze e selezionare un tipo di computer.

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 viene eseguito da una versione all'altra, ad esempio da 9,6 a 9,7.

11. **Risorse di storage sottostanti**: Scegliere le impostazioni per l'aggregato iniziale: Un tipo di disco e le dimensioni di ciascun disco.

    Il tipo di disco è per il volume iniziale. È possibile scegliere un tipo di disco diverso per i volumi successivi.

    Le dimensioni del disco sono 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.

    Per informazioni sulla scelta del tipo e delle dimensioni di un disco, vedere "Dimensionare il sistema in Google Cloud".

12. **Flash cache, velocità di scrittura e WORM**:

    a. Attivare **Flash cache**, se lo si desidera.

    A partire da Cloud Volumes ONTAP 9.13.1, *Flash cache* è supportato sui tipi di istanze n2-standard-16, n2-standard-32, n2-standard-48 e n2-standard-64. Non è possibile disattivare Flash cache dopo l'implementazione.

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

    "Scopri di più sulla velocità di scrittura".

    L'opzione **High** write speed con i tipi di istanze n2-standard-16, n2-standard-32, n2-standard-48 e n2-standard-64 offre un'elevata velocità di scrittura e un'unità MTU (Maximum Transmission Unit) di 8,896 byte. Inoltre, la MTU superiore di 8,896 richiede la selezione di VPC-1, VPC-2 e VPC-3 per l'implementazione. L'elevata velocità di scrittura e una MTU di 8,896 dipendono dalle funzionalità e non possono essere disabilitate singolarmente all'interno di un'istanza configurata. Per ulteriori informazioni su VPC-1, VPC-2 e VPC-3, vedere "Regole per VPC-1, VPC-2 e VPC-3".

    c. 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.

13. **Data Tiering in Google Cloud**: Scegliere se attivare il tiering dei dati sull'aggregato iniziale, scegliere una classe di storage per i dati a più livelli, quindi selezionare un account di servizio con il ruolo predefinito Storage Admin.

    Tenere presente quanto segue:

- BlueXP imposta l'account del servizio sull'istanza di Cloud Volumes ONTAP. Questo account di servizio fornisce le autorizzazioni per il tiering dei dati a un bucket di storage Google Cloud. Assicurarsi di aggiungere l'account del servizio Connector come utente dell'account del servizio di tiering, altrimenti non è possibile selezionarlo da BlueXP.
- 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 su aggregati successivi, ma è necessario spegnere il sistema e aggiungere un account di servizio dalla console di Google Cloud.

  "Scopri di più sul tiering dei dati".

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

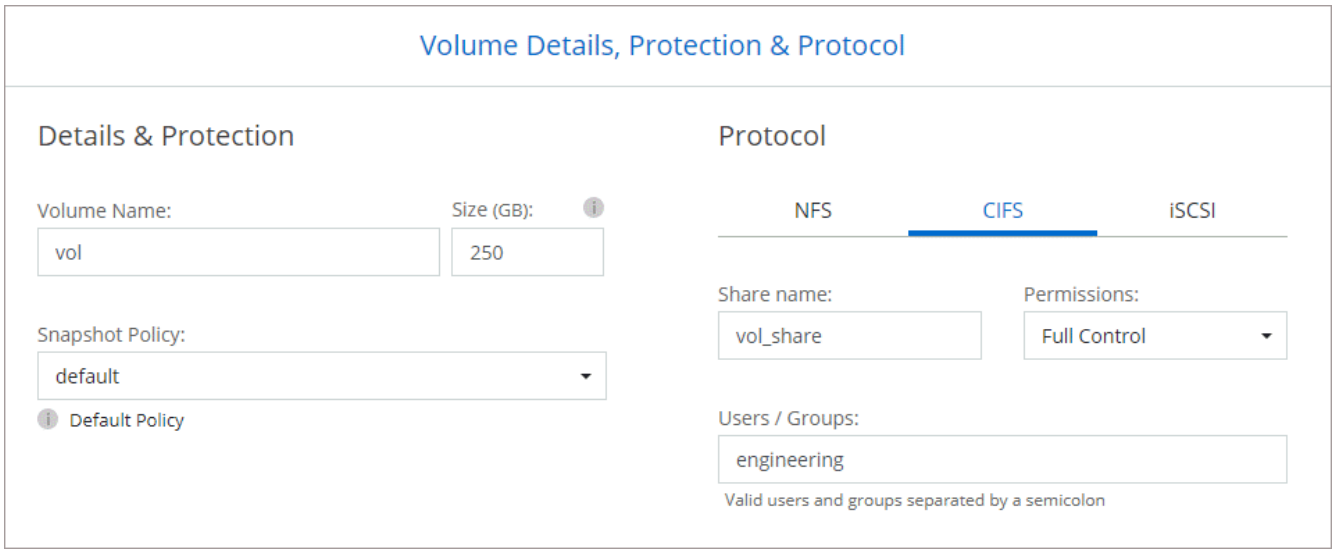
    "Scopri le versioni e i protocolli client supportati".

    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:



15. **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. Se si configura Google Managed Active Directory, per impostazione predefinita è possibile accedere ad utilizzando l'indirizzo IP 169.254.169.254.
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.

Campo	Descrizione
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. Per configurare Google Managed Microsoft ad come server ad per Cloud Volumes ONTAP, immettere **OU=computer,OU=cloud** in questo campo. "Documentazione Google Cloud: Unità organizzative in Google Managed Microsoft ad"
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.

16. **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".

17. **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 Google Cloud che BlueXP acquisterà.
    c. Selezionare le caselle di controllo **ho capito…**.
    d. Fare clic su **Go**.

Risultato

BlueXP implementa il sistema Cloud Volumes ONTAP. Puoi tenere traccia dei progressi nella timeline.

In caso di problemi durante l'implementazione del sistema Cloud Volumes ONTAP, esaminare il messaggio di errore. È inoltre possibile selezionare l'ambiente di lavoro e fare clic su **Ricomcreare 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.

Verifica dell'immagine della piattaforma Google Cloud

Panoramica sulla verifica delle immagini di Google Cloud

La verifica delle immagini di Google Cloud è conforme ai requisiti di sicurezza NetApp avanzati. Sono state apportate modifiche allo script che genera le immagini per firmare l'immagine lungo il percorso utilizzando le chiavi private generate specificamente per questa attività. È possibile verificare l'integrità dell'immagine GCP utilizzando il digest firmato e il certificato pubblico per Google Cloud che possono essere scaricati tramite "NSS" per una release specifica.

La verifica dell'immagine Google Cloud è supportata dal software Cloud Volumes ONTAP versione 9.13.0 o superiore.

Converti l'immagine in formato raw su Google Cloud

L'immagine utilizzata per implementare nuove istanze, aggiornamenti o utilizzata in immagini esistenti verrà condivisa con i client tramite "Il NetApp Support Site (NSS)". Il digest firmato e i certificati saranno disponibili per il download attraverso il portale NSS. Assicurarsi di scaricare il digest e i certificati per la release corretta corrispondente all'immagine condivisa dal supporto NetApp. Ad esempio, 9.13.0 immagini avranno un digest con 9.13.0 firme e certificati disponibili su NSS.

Perché è necessario questo passaggio?

Le immagini di Google Cloud non possono essere scaricate direttamente. Per verificare l'immagine rispetto al digest firmato e ai certificati, è necessario disporre di un meccanismo per confrontare i due file e scaricare l'immagine. Per farlo, devi esportare/convertire l'immagine in un formato disk.raw e salvare i risultati in un bucket di storage su Google Cloud. Il file disk.raw viene archiviato e compresso nel processo.

L'account utente/servizio avrà bisogno di privilegi per eseguire le seguenti operazioni:

- Accesso al bucket di storage Google
- Scrivi al bucket di storage Google
- Creazione di processi di cloud build (utilizzati durante il processo di esportazione)
- Accesso all'immagine desiderata
- Creare attività di esportazione delle immagini

Per verificare l'immagine, è necessario convertirla in un formato disk.raw e quindi scaricarla.

Utilizza la riga di comando di Google Cloud per esportare l'immagine di Google Cloud

Il modo preferito per esportare un'immagine in Cloud Storage è utilizzare "comando di esportazione delle immagini di calcolo di gcloud". Questo comando prende l'immagine fornita e la converte in un file disk.raw che viene tarred e gzippato. Il file generato viene salvato nell'URL di destinazione e può essere scaricato per la verifica.

Per eseguire questa operazione, l'utente/account deve disporre dei privilegi necessari per accedere e scrivere nel bucket desiderato, esportare l'immagine e creare cloud (utilizzati da Google per esportare l'immagine).

Esportare l'immagine di Google Cloud utilizzando gcloud

Fare clic per visualizzare lo script

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

Estrarre i file compressi

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

Vedere "Documento Google Cloud sull'esportazione di un'immagine" Per ulteriori informazioni su come esportare un'immagine tramite Google Cloud.

Verifica della firma dell'immagine

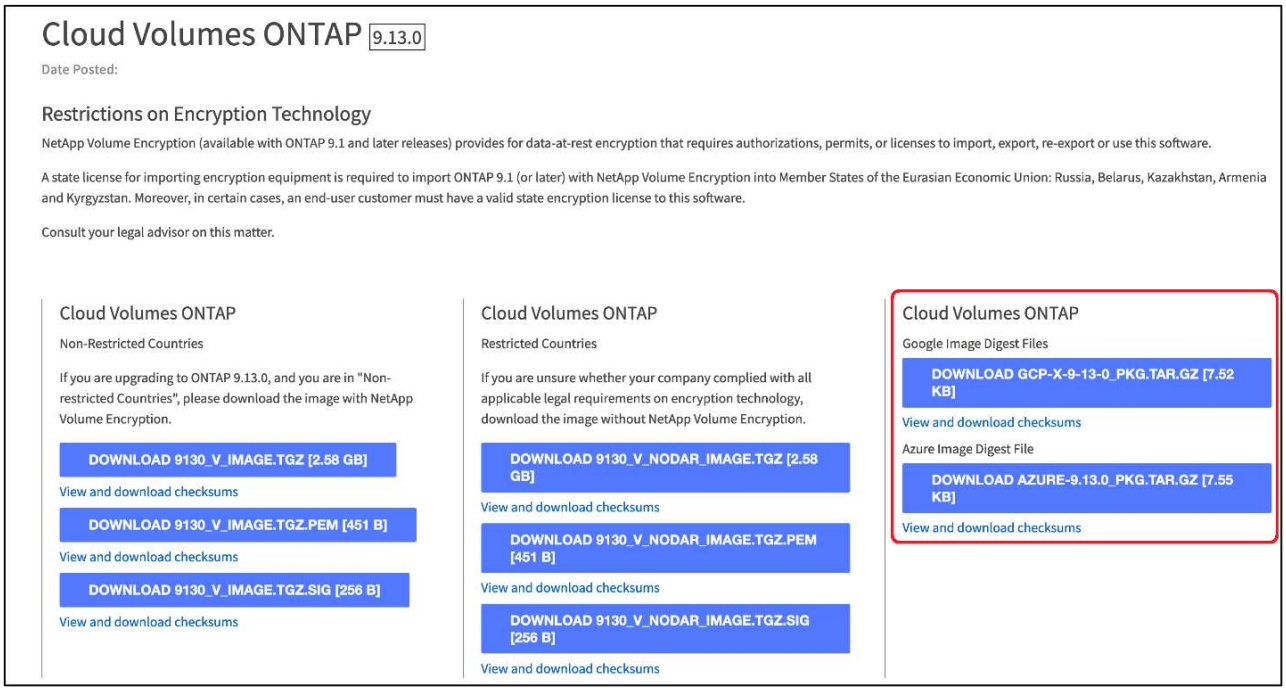
Verificare le immagini firmate di Google Cloud

Per verificare l'immagine firmata Google Cloud esportata, è necessario scaricare il file di digest dell'immagine da NSS per convalidare il file disk.raw e il contenuto del file di digest.

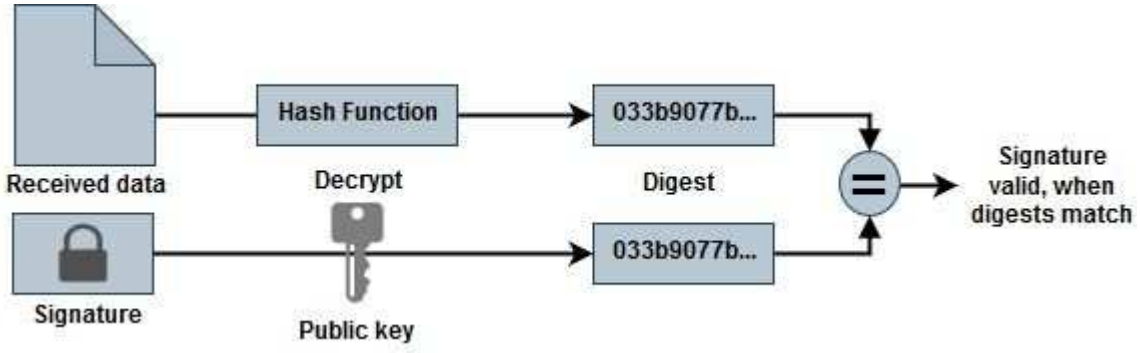
Riepilogo del flusso di lavoro per la verifica dell'immagine firmata

Di seguito viene riportata una panoramica del processo di verifica delle immagini firmato da Google Cloud.

- Dal "NSS", Scaricare l'archivio Google Cloud contenente i seguenti file:
  - Digest firmato (.sig)
  - Certificato contenente la chiave pubblica (.pem)
  - Catena di certificati (.pem)



- Scaricare il file disk.raw convertito
- Validare il certificato utilizzando la catena del certificato
- Validare il digest firmato utilizzando il certificato contenente la chiave pubblica
  - Decrittare il digest firmato utilizzando la chiave pubblica per estrarre il digest del file di immagine
  - Creare un digest del file disk.raw scaricato
  - Confrontare i due file digest per la convalida



Verifica del file disk.raw e del contenuto del file digest con OpenSSL

È possibile verificare il file disk.raw scaricato da Google Cloud rispetto al contenuto del file digest disponibile tramite "NSS" Con OpenSSL.

I comandi OpenSSL per la convalida dell'immagine sono compatibili con macchine Linux, Mac OS e Windows.

Fasi

1. Verificare il certificato utilizzando OpenSSL.

Fare clic per visualizzare lo script

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
         e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
         22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
         38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
         fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
         bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. Inserire il file disk.raw scaricato, la firma e i certificati in una directory.
3. Estrarre la chiave pubblica dal certificato utilizzando OpenSSL.
4. Decrittare la firma utilizzando la chiave pubblica estratta e verificare il contenuto del file disk.raw scaricato.

Fare clic per visualizzare lo script

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

Informazioni sul copyright

Informazioni sul marchio commerciale